Boolean and Vectorial Functions: A Design-Theoretic Point of View

Dissertation

zur Erlangung des akademischen Grades

doctor rerum naturalium
(Dr. rer. nat.)

von Dipl. Math. Alexandr Polujan

geb. am 01.06.1993 in Minsk

genehmigt durch die Fakultät für Mathematik
der Otto-von-Guericke-Universität Magdeburg

Gutachter: Prof. Dr. Alexander Pott
Prof. Dr. Enes Pasalic

eingereicht am: 14.04.2021

Verteidigung am: 05.07.2021

Zusammenfassung

In der vorliegenden Arbeit untersuchen wir verschiedene Klassen kryptografisch bedeutsamer Funktionen wie beispielsweise *bent*, *plateaued* und *differentially uniform* Funktionen sowie aus diesen Funktionen konstruierte Inzidenzstrukturen.

Zunächst untersuchen wir vektorielle bent Funktionen in wenigen Variablen. Wir klassifizieren und enumerieren alle vektoriellen bent Funktionen in sechs Variablen. Damit vervollständigen wir die Klassifizierung perfekter nichtlinearer Funktionen in sechs Variablen vom algebraischen Grad höchstens drei und die Liste der bent Funktionen in sechs Variablen. Darüber hinaus zeigen wir, dass im Gegensatz zu Booleschen bent Funktionen nicht alle vektoriellen bent Funktionen in sechs Variablen bis auf EA-Äquivalenz durch *Maiorana-McFarland* und Desarguesian *partial spread* Konstruktionen beschrieben werden können.

Wir untersuchen ferner, ob sich bestimmte Eigenschaften von Booleschen und vektoriellen bent Funktionen sowie deren Verallgemeinerungen in den zugehörigen Inzidenzstrukturen widerspiegeln, die in einigen Fällen zur gut erforschten Klasse der kombinatorischen Designs gehören. In diesem Zusammenhang stellen wir eine neue Konstruktion von Inzidenzstrukturen aus Booleschen und vektoriellen Funktionen vor und präsentieren zwei Anwendungen dieser Objekte zur Untersuchung von bent Funktionen. Die erste Anwendung ist eine designtheoretische Charakterisierung von bent Funktionen innerhalb der plateaued Funktionen, die zweite ist eine kombinatorische Interpretation des Erweiterbarkeitsproblems für bent Funktionen. Wir stellen ferner eine große Klasse fast perfekt-nichtlinearer Funktionen (*APN-Funktionen*) vor, deren lineare Codes 2-Designs tragen. Aus diesem Ergebnis entwickeln wir eine neue hinreichende Bedingung für die CCZ-Nichtäquivalenz von APN-Funktionen mit dem klassischen Walsh-Spektrum zu quadratischen Funktionen.

Zum Abschluss untersuchen wir kubische Boolesche bent Funktionen. Wir beweisen, dass im Gegensatz zu den Fällen mit $n = 6$ und $n = 8$ Variablen die Maiorana-McFarland Konstruktion für alle $n \geq 10$ nicht die gesamte Klasse der kubischen bent Funktionen in n Variablen beschreiben kann. Außerdem zeigen wir für unendlich viele $n \geq 10$ die Existenz kubischer bent Funktionen in n Variablen, die homogen sind, keine affinen Ableitungen haben und nicht in der abgeschlossenen Maiorana-McFarland Klasse sind.

Abstract

In this thesis, we investigate various classes of cryptographically significant functions, including bent, plateaued and differentially uniform functions, as well as the incidence structures constructed from these mappings.

First, we investigate vectorial bent functions in a small number of variables. We classify and enumerate all vectorial bent functions in six variables. Thereby, we complete the classification of perfect nonlinear functions in six variables of algebraic degree at most three and the enumeration of bent functions in six variables. Moreover, we show that all vectorial bent functions in six variables, in contrast to the Boolean bent functions, cannot be described, up to EA-equivalence, by Maiorana-McFarland and Desarguesian partial spread constructions.

Furthermore, we investigate whether certain properties of Boolean and vectorial bent functions, as well as their generalizations, may be reflected by the associated incidence structures, which in some cases, fall into the well-studied class of combinatorial designs. In particular, we introduce a new construction of incidence structures from Boolean and vectorial functions called nonvanishing flats and provide two applications of this object to study bent functions. The first is a design-theoretic characterization of bent functions among plateaued functions, and the second is a combinatorial interpretation of the extendability problem for bent functions. We also provide a large class of APN functions, whose linear codes support 2-designs. Using this result, we give a new sufficient condition for APN functions with the classical Walsh spectrum to be CCZ-inequivalent to quadratic functions.

Finally, we investigate cubic Boolean bent functions. We prove that, in contrast to the cases of $n = 6$ and $n = 8$ variables, the Maiorana-McFarland construction does not describe the whole class of cubic bent functions in n variables for all $n \geq 10$. Moreover, we show that cubic bent functions in n variables that are homogeneous, have no affine derivatives and are not in the completed Maiorana-McFarland class exist for infinitely many $n \geq 10$.

Contents

List of Tables

List of Figures

List of Algorithms

Overview

In this dissertation, we study mappings $F\colon \mathbb{F}_2^n \to \mathbb{F}_2^m$ on finite dimensional vector spaces over the binary finite field, which are called (n,m)-functions. In particular, we focus on the classes of (n,m)-functions having perfect nonlinearity and exceptional differential properties, which play an important role in cryptographic applications. Among them are the classes of Boolean and vectorial bent functions, plateaued and differentially uniform functions. Besides the computer search and the tools from linear algebra, we consider a "design-theoretic approach" to (n,m)-functions, which can be explained as follows. From the (n,m)-functions having nice cryptographic properties we construct various incidence structures, which in certain cases belong to the well studied class of combinatorial structures, namely designs. Consequently, we investigate which combinatorial properties of these designs may reflect cryptographic properties of (n,m)-functions. The advantage of the design-theoretic approach is that properly constructed incidence structures may not only characterize the nonlinearity and differential properties of a given function, but also be an invariant under equivalence. This property can be used for distinguishing different functions or even classes of functions.

In Chapter 1, we give a comprehensive survey on Boolean and vectorial bent functions, which includes a summary of the fundamental constructions as well as the known classification and enumeration results. Consequently, we summarize the known constructions of incidence structures from bent functions with the use of difference sets and linear codes. The investigation of Boolean and vectorial bent functions, as well as their generalizations is arranged into three chapters in the following way.

In Chapter 2, we investigate vectorial bent functions in six variables with a computer search. Vectorial bent functions together with Boolean bent functions and almost perfect nonlinear (APN) functions form the set of perfect nonlinear functions, which are referred to as functions with maximum nonlinearity or minimum differential uniformity. While bent functions have simultaneously maximum nonlinearity and minimum differential uniformity, APN functions are characterized by the minimum differential uniformity; this is the reason why they are called almost perfect nonlinear. The complete classification of perfect nonlinear functions seems to be elusive, however, thanks to computer search, this problem can still be solved provided the number of variables is not too large or functions of a special shape are considered. Perfect nonlinear functions up to five variables are completely classified [11], while in the case of six variables the complete classification seems to be possible only for the functions of algebraic degree at most three. Considering the case of six variables in more detail, the classification of perfect nonlinear functions is known only for the Boolean bent functions [103] and APN functions [42, 68]. In Section 2.3, we resolve the open case of vectorial bent functions. Moreover, we enumerate all vectorial bent functions in six variables, thus completing the enumeration of bent functions on $\mathbb{F}_2^6$. We also address the question of the extendability of (n, m)-bent functions, which is closely related to the bent sum decomposition problem [109] in the Boolean case $m = 1$.

Theorem 2.15. *For vectorial bent functions in* 6 *variables the following hold.*

1. *There are* 23,392,233,361,244,160 $\approx 2^{54.37}$ *vectorial* $(6, 2)$*-bent functions, which are divided into* 9 *extended-affine equivalence classes.*
2. *There are* 121,282,113,886,947,901,440 $\approx 2^{66.71}$ *vectorial* $(6, 3)$*-bent functions, which are divided into* 13 *extended-affine equivalence classes.*

Moreover, if a $(6, m)$*-bent function* F *is non-extendable, then* F *is absolutely non-extendable, i.e., it has* $m = 3$.

Based on the analysis of the obtained equivalence classes of vectorial bent functions, we show that any $(6, m)$-bent function with $m < 3$ is extendable to a $(6, m + 1)$-bent function. Besides that, we show that in contrast to Boolean bent functions, vectorial bent functions in six variables can not be described, up to extended-affine equivalence, by Maiorana-McFarland and Desarguesian partial spread constructions.

In Chapter 3, we investigate which design-theoretic properties of Boolean bent functions can be shared by their generalizations: vectorial bent functions, plateaued functions and differentially uniform functions. First, we concentrate on the study of the incidence structures constructed from Boolean and vectorial bent functions. In Theorem 3.10, we observe that the Smith normal form of Boolean and vectorial functions have the same general shape. Consequently, in Theorem 3.25, we prove that from the isomorphism of the addition designs of vectorial bent functions, similarly to the Boolean case, one can deduce extended-affine equivalence of vectorial bent functions. Despite the mentioned similarities, we also observe that certain phenomena, which are "regular" for the incidence structures constructed from Boolean bent functions, can not be observed for the vectorial bent functions. In Theorem 3.19, we show that extended-affine inequivalent bent functions on $\mathbb{F}_2^n$ may give rise to isomorphic translation designs for all $n \geq 6$. In contrast to the Boolean case, there exists no single pair of vectorial bent functions in six variables, which are extended-affine equivalent, but their translation designs are isomorphic, as we show in Theorem 3.22.

Then we focus on vanishing flats of Boolean and vectorial bent functions. For an (n,m)-function F, the incidence structure $\mathcal{VF}(F)$, called vanishing flats, was introduced recently in [73] to study inequivalence of (n,n)-functions. In the following theorem, we give a characterization of (n,m)-bent functions F in terms of the associated vanishing flats $\mathcal{VF}(F)$.

Theorem 3.26. *Let F be an (n,m)-function. The following statements are equivalent.*

1. *The function F is an (n,m)-bent function.*
2. *The incidence structure $\mathcal{VF}(F)$ is a 2-$(2^n, 4, 2^{n-m-1}-1)$ design.*

Motivated by the fact that the proof of this statement works for a larger class of incidence structures, we introduce a combinatorial generalization of the vanishing flats, namely nonvanishing flats $\mathcal{NF}_{\mathbf{v}}(F)$ of an (n,m)-function F with respect to a vector $\mathbf{v} \in \mathbb{F}_2^m \setminus \{\mathbf{0}\}$. While the block set of the vanishing flats $\mathcal{VF}(F)$ is formed by affine two-dimensional subspaces $\{\mathbf{x}, \mathbf{x}\oplus\mathbf{a}, \mathbf{x}\oplus\mathbf{b}, \mathbf{x}\oplus\mathbf{a}\oplus\mathbf{b}\}$ on which the second-derivative $D_{\mathbf{a},\mathbf{b}}F(\mathbf{x})$ vanishes, the block set of the nonvanishing flats $\mathcal{NF}_{\mathbf{v}}(F)$ is formed by those affine two-dimensional subspaces, on which the second-derivative takes the value $\mathbf{v} \in \mathbb{F}_2^m \setminus \{\mathbf{0}\}$, namely $D_{\mathbf{a},\mathbf{b}}F(\mathbf{x}) = \mathbf{v}$. Carlet [28] used the values $N_F(\mathbf{v},\mathbf{x}) = |\{(\mathbf{a},\mathbf{b}) \in \mathbb{F}_2^n \times \mathbb{F}_2^n \colon D_{\mathbf{a},\mathbf{b}}F(\mathbf{x}) = \mathbf{v}\}|$ to characterize plateaued (n,m)-functions F as those (n,m)-functions, for which $N_F(\mathbf{v},\mathbf{x})$ is independent on $\mathbf{x} \in \mathbb{F}_2^n$ for any $\mathbf{v} \in \mathbb{F}_2^m$. In the following statement, we interpret this characterization by means of the regularity of nonvanishing flats.

Theorem 3.36. *Let F be an (n,m)-function and let for $\mathbf{v} \in \mathbb{F}_2^m$ the values $\lambda_{\mathbf{v}} \in \mathbb{N}$ be defined in the following way:*

$$\lambda_{\mathbf{0}} = \frac{N_F(\mathbf{0},\mathbf{x}) - 3\cdot 2^n + 2}{6} \quad \textit{and} \quad \lambda_{\mathbf{v}} = \frac{N_F(\mathbf{v},\mathbf{x})}{6} \quad \textit{for } \mathbf{v} \in \mathbb{F}_2^m \setminus \{\mathbf{0}\}.$$

Then the following statements are equivalent.

1. *The function F is plateaued.*
2. *For all $\mathbf{v} \in \mathbb{F}_2^m \setminus \{\mathbf{0}\}$ the incidence structure $\mathcal{NF}_{\mathbf{v}}(F)$ is a 1-$(2^n, 4, \lambda_{\mathbf{v}})$ design.*

Moreover, if an (n,m)-function F is plateaued, then the incidence structure $\mathcal{VF}(F)$ is a 1-$(2^n, 4, \lambda_{\mathbf{0}})$ design.

An advantage of the design-theoretic approach to plateaued functions is that the collection of all nonvanishing flats contains not only information about nonlinearity but also is an invariant under extended-affine equivalence, as we show in Theorem 3.32. Remarkably, the aforementioned characterization of plateaued functions can be even more strengthened for bent functions. In particular, the nonvanishing flats of (n, m)-bent functions are not only 1-designs but also 2-designs as the following result shows.

Theorem 3.42. *Let F be an (n, m)-function. The following statements are equivalent.*

1. *The function F is (n, m)-bent.*

2. *For any $\mathbf{v} \in \mathbb{F}_2^m \setminus \{\mathbf{0}\}$ the incidence structure $\mathcal{NF}_{\mathbf{v}}(F)$ is a 2-$(2^n, 4, 2^{n-m-1})$ design.*

Moreover, the number of the nonvanishing flats of an (n, m)-bent function F with respect to a nonzero vector $\mathbf{v} \in \mathbb{F}_2^m$ is given by

$$|\mathcal{NF}_{\mathbf{v},F}| = \frac{(2^{n+m} - 2^m) \cdot 2^{2(n-m)}}{24}.$$

Besides characterizations of plateaued and bent functions in terms of nonvanishing and vanishing flats, we give a design-theoretic interpretation of the extendability problem for (n, m)-bent functions, which was studied for p-ary (n, m)-bent functions in [91]. In Theorem 3.46, we show that vanishing flats of extendable bent functions are highly structured combinatorial objects. Consequently, we show that nonexistence of certain subdesigns in the design of vanishing flats implies non-extendability of a given bent function.

Theorem 3.47. *Let F be an (n, s)-bent function.*

1. *If $\mathcal{VF}(F)$ contains no 2-$(2^n, 4, 2^{n-s-2} - 1)$ subdesign, then F is non-extendable.*

2. *If $\mathcal{VF}(F)$ contains no 2-$(2^n, 4, 2^{n-s-2})$ subdesign, then F is non-extendable.*

3. *If $\mathcal{VF}(F)$ contains no 2-$(2^n, 4, 2^{n-s-r-1} - 1)$ subdesign for some integer r, satisfying $1 \leq r \leq n/2 - s - 1$, then F is not the projection of an $(n, n/2)$-bent function.*

We consider a coding-theoretic generalization of the vanishing flats $\mathcal{VF}(F)$ of (n, m)-bent functions F, which can be constructed using the supports of the codewords of weight $w = 4$ in the linear code $\mathcal{C}_F^\perp$. An essential step is to consider the incidence structures supported by the codewords of other weights in the linear codes $\mathcal{C}$ and $\mathcal{C}_F^\perp$. Tang, Ding and Xiong [108] proved that linear codes $\mathcal{C}_F$ and $\mathcal{C}_F^\perp$ constructed from several classes of (n, m)-functions, including (n, m)-bent functions and differentially two-valued s-plateaued (n, n)-functions, support 2-designs. We finish this chapter by providing another large class of (n, n)-functions, whose linear codes $\mathcal{C}_F$ and $\mathcal{C}_F^\perp$ support 2-designs.

Theorem 3.56. *Let F be an APN function on $\mathbb{F}_2^n$ with $n = 2k$, which has the classical Walsh spectrum. If the function F is CCZ-equivalent to a function F' on $\mathbb{F}_2^n$ having $2(2^n - 1)/3$ bent components and $(2^n - 1)/3$ semi-bent components, then the linear codes $\mathcal{C}_F$ and $\mathcal{C}_F^\perp$ support 2-designs.*

To show that an APN function F on $\mathbb{F}_2^n$ is CCZ-inequivalent to a quadratic one is, in general, difficult. With Theorem 3.56, we derive new sufficient conditions for an APN function with the classical Walsh spectrum to be CCZ-inequivalent to a quadratic function.

Theorem 3.61. *Let F be an APN function on $\mathbb{F}_2^n$ with $n = 2k$, which has the classical Walsh spectrum.*

1. *If there exists an integer ℓ, satisfying $1 < \ell < 2^n$ such that the incidence structure $(\mathcal{P}(\mathcal{C}_F), \mathcal{B}_\ell(\mathcal{C}_F))$ is not a 2-design, then the APN function F is CCZ-inequivalent to a quadratic function.*

2. *If there exists an integer $\ell^\perp$, satisfying $6 < \ell^\perp < 2^n$ such that the incidence structure $\left(\mathcal{P}(\mathcal{C}_F^\perp), \mathcal{B}_{\ell^\perp}(\mathcal{C}_F^\perp)\right)$ is not a 2-design, then the APN function F is CCZ-inequivalent to a quadratic function.*

In Chapter 4, we investigate the class of cubic Boolean bent functions, remaining the only class of bent functions (with respect to the algebraic degree), for which it is not known whether it can be described, up to extended-affine equivalence, by the Maiorana-McFarland construction.

So far, the question whether the class of cubic Boolean bent functions is contained in the completed Maiorana-McFarland class, was studied in a small number of variables with the use of computer: Dillon [40] and Bracken [10] showed that all cubic bent functions in $n = 6$ and $n = 8$ variables, respectively, are the members of the completed Maiorana-McFarland class $\mathcal{M}^\#$. However, the same question, addressed for an arbitrary number of variables $n \geq 10$, still remains an open problem. In order to solve this open problem, we study cubic Boolean bent functions, which are homogeneous, i.e., the algebraic normal form of these functions contains only monomials of algebraic degree three.

We begin the study of the known homogeneous cubic bent functions with the analysis of the functions obtained with a computer search [34, 35, 83]. We show that all these functions, which belong to the $\mathcal{M}^\#$ class, are extended-affine inequivalent to the only one known algebraic construction $h^n_{pr.}$ on $\mathbb{F}_2^n$ proposed by Seberry, Xia and Pieprzyk [104]. Using design-theoretic invariants of Boolean functions we show that concatenations of these functions are also extended-affine inequivalent to the primary construction, thus, proving the following result.

Theorem 4.11. *There exist homogeneous cubic bent functions on $\mathbb{F}_2^n$, extended-affine inequivalent to the primary construction $h^n_{pr.}$, whenever $n \geq 8$.*

We also provide an algorithmic approach to the construction of new homogeneous bent functions from old ones. Using Algorithm 4.1, we construct almost twice as the number of previously known homogeneous cubic bent functions in $6 \leq n \leq 12$ variables, and show that some of the constructed functions are extended-affine inequivalent to all of the previously known examples.

Besides that, we show that among the known homogeneous cubic bent functions in ten variables there are a few examples, which do not belong to the completed Maiorana-McFarland class $\mathcal{M}^{\#}$. In order to show that concatenations of these functions do not belong to the $\mathcal{M}^{\#}$ class as well, we provide a sufficient condition for bent functions f on $\mathbb{F}_2^n$ and g on $\mathbb{F}_2^m$, which guaranties that the direct sum $f \oplus g$ is outside $\mathcal{M}^{\#}$ on $\mathbb{F}_2^n \times \mathbb{F}_2^m$. The main idea of the approach is to estimate the maximum dimensions (denoted by r-ind) of the vector subspaces, on which second-order derivatives of the functions f on $\mathbb{F}_2^n$ and g on $\mathbb{F}_2^m$ are constant functions. In the case when the dimensions are small enough, the direct sum $f \oplus g$ is provably outside $\mathcal{M}^{\#}$, as the following statement shows.

Theorem 4.24. *Let $f\colon \mathbb{F}_2^n \to \mathbb{F}_2$ and $g\colon \mathbb{F}_2^m \to \mathbb{F}_2$ be two Boolean bent functions. If f and g satisfy $\text{r-ind}(f) < n/2$ and $\text{r-ind}(g) \leq m/2$, then $f \oplus k \cdot g \notin \mathcal{M}^{\#}$ on $\mathbb{F}_2^{n+km}$ for all $k \in \mathbb{N}$.*

With the help of computer search, we show that certain cubic bent functions in $6 \leq n \leq 12$ variables satisfy the aforementioned sufficient condition and thus lead to infinitely many cubic bent functions outside the $\mathcal{M}^{\#}$ class. In this way, we derive the following series of existence results of cubic bent functions outside the completed Maiorana-McFarland class $\mathcal{M}^{\#}$ possessing various cryptographic properties.

Theorem 4.27. *On $\mathbb{F}_2^n$ there exist:*

1. *Cubic bent functions outside $\mathcal{M}^{\#}$ for all $n \geq 10$.*
2. *Cubic bent functions without affine derivatives outside $\mathcal{M}^{\#}$ for all $n \geq 26$.*
3. *Homogeneous cubic bent functions outside $\mathcal{M}^{\#}$ for all $n \geq 26$.*
4. *Homogeneous cubic bent functions without affine derivatives outside $\mathcal{M}^{\#}$ for all $n \geq 50$.*

With this statement, we conclude that the only class of Boolean bent functions (with respect to the algebraic degree) completely contained in $\mathcal{M}^{\#}$ is the class of quadratic bent functions.

Each chapter concerning the investigation of bent functions is concluded with a list of open problems. In Appendices A and B, we summarize the algebraic normal forms and invariants under extended-affine equivalence for the Boolean and vectorial bent functions used in the thesis.

Finally, we remark that this dissertation is based on three papers by Pott and the present author [92–94] and the work by Meidl, Pott and the present author [80].

Chapter 1

Preliminaries

In this chapter, we present the mathematical background needed in this thesis. The chapter is organized in the following way.

In Section 1.1, we give necessary definitions related to the main object of the dissertation: perfect nonlinear functions. In Subsection 1.1.1, we describe basic notation for Boolean and vectorial functions. In Subsection 1.1.2, we define several important classes of cryptographically significant functions: Boolean and vectorial bent functions as well as their generalizations, namely plateaued and differentially uniform functions. In Subsection 1.1.3, we focus on the fundamental classes of Boolean bent functions as well as their vectorial analogues: quadratic functions, Maiorana-McFarland and partial spread bent functions. We also discuss, how one can check computationally whether a given Boolean bent function can be described by Maiorana-McFarland or partial spread constructions. In Subsection 1.1.4, we summarize some known results about a special class of Boolean bent functions, i.e., cubic bent functions, which will be considered in more detail in the last chapter of this thesis.

In the following, we summarize the known combinatorial and coding theoretic characterizations of perfect nonlinear functions, which we later use for theoretical and computational analysis of these functions. In Section 1.2, we define two important combinatorial objects, namely difference sets and relative difference sets. Consequently, we explain how to construct difference and relative difference sets from bent functions, and give the known characterizations of Boolean and vectorial bent functions in terms of these constructions. In Section 1.3, we introduce linear codes and show how one can use them to characterize perfect nonlinear functions and check their equivalence.

In Section 1.4, we introduce incidence structures, which we further use as one of the main tools for the analysis of Boolean and vectorial functions. Consequently, in Subsections 1.4.1 and 1.4.2, we introduce various constructions of incidence structures using difference sets and linear codes, respectively. With the help of the introduced incidence structures we provide further characterizations of bent functions and define several invariants under equivalence.

1.1 Boolean and vectorial functions

Many conventional cryptographic systems use as a main ingredient Boolean and vectorial functions, which are mappings on finite dimensional vector spaces over the binary finite field. There are several criteria which a given function has to satisfy in order to be considered as a good cryptographic primitive. Two basic properties, which a secure cryptographic system must have, namely confusion and diffusion, were formulated by Claude Shannon [105] in his pioneering work "Communication theory of secrecy systems" and could be formulated as follows:

- *Confusion* refers to making the relationship between the input and the output of a cryptographic system as complex as possible, i.e., changing the input has unpredictable effect on the output.
- *Diffusion* refers to changing few entries in the input in such a way that many entries in the output are changed.

In the following subsection, we consider in detail basic definitions related to Boolean and vectorial functions, describe their various representations and discuss cryptographic concepts, reflecting confusion and diffusion of Boolean and vectorial functions.

1.1.1 Basic definitions

Let $\mathbb{F}_2 = (\{0,1\}, \oplus, \cdot)$ be the finite field with two elements and let $\mathbb{F}_2^n$ be the vector space of dimension n over $\mathbb{F}_2$. A mapping $F\colon \mathbb{F}_2^n \to \mathbb{F}_2^m$ is called an (n,m)-*function*. The single-output case $m = 1$ is called a *Boolean* function, while in the multi-output case $m \geq 2$ one deals with a *vectorial Boolean* function. Since the output of any vectorial (n,m)-function can be described by m Boolean functions (as we will show later), we omit the term "Boolean" and simply say *vectorial* (n,m)*-functions*.

Vectors, matrices and vector spaces. In this dissertation, we will often identify the vector space $(\mathbb{F}_2^n, \oplus)$ with the finite field $(\mathbb{F}_{2^n}, +, \cdot)$. In order to distinguish elements in $\mathbb{F}_2^n$ and $\mathbb{F}_{2^n}$, we will use plain font for the elements of the finite field $x \in \mathbb{F}_{2^n}$ and bold font for the elements of the vector space $\mathbf{x} \in \mathbb{F}_2^n$. Following this notation, we will also use bold font for vectors and matrices. The following vectors and matrices are frequently used throughout this thesis:

- $\mathbf{j}_n$ is the *all-one-vector* of length n;
- $\mathbf{I}_n$ and $\mathbf{J}_n$ are the *identity matrix* and the *all-one-matrix* of order n, respectively;
- $\mathbf{O}_{r,s}$ is the *all-zero-matrix* of size $r \times s$. If $r = s$, we use the notation $\mathbf{O}_r$.

We denote by $\mathbf{A} \otimes \mathbf{B}$ the *Kronecker product* of matrices $\mathbf{A} = \left(a_{i,j}\right)$ and $\mathbf{B} = (b_{k,l})$ with $1 \le i \le n, 1 \le j \le m$ and $1 \le k \le n', 1 \le l \le m'$:

$$\mathbf{A} \otimes \mathbf{B} := \begin{pmatrix} a_{1,1}\mathbf{B} & \dots & a_{1,m}\mathbf{B} \\ \vdots & & \vdots \\ a_{n,1}\mathbf{B} & \dots & a_{n,m}\mathbf{B} \end{pmatrix}, \tag{1.1}$$

which is a matrix of size $nn' \times mm'$.

We will represent vector spaces with the help of the canonical Gauss-Jordan basis, which we define according to the work [22, Subsection 4] using the following notation. For a vector $\mathbf{u} = (u_1, \dots, u_n) \in \mathbb{F}_2^n$, we denote the index of the leftmost 1 in $\mathbf{u}$ by $\nu(\mathbf{u}) = \max\{i \in \{1, \dots, n+1\} \mid u_j = 0 \text{ for } 1 \le j < i\}$. For a vector space $U \subseteq \mathbb{F}_2^n$, we define $\Upsilon(U) := \{\nu(\mathbf{u}) \mid \mathbf{u} \in U \setminus \{\mathbf{0}\}\}$. On $\mathbb{F}_2^n$ we introduce the standard lexicographic ordering $<$ for elements $\mathbf{u} = (u_1, \dots, u_n)$ and $\mathbf{v} = (v_1, \dots, v_n) \in \mathbb{F}_2^n$ as follows:

$$\mathbf{u} > \mathbf{v} \iff \begin{array}{ll} \nu(\mathbf{u}) < \nu(\mathbf{v}) & \text{or} \\ \nu(\mathbf{u}) = \nu(\mathbf{v}) & \text{and} \quad (u_{\nu(\mathbf{u})+1}, \dots, u_n) > (v_{\nu(\mathbf{v})+1}, \dots, v_n) \end{array}.$$

Definition 1.1. An ordered basis $\mathbf{u}_1, \dots, \mathbf{u}_k \in \mathbb{F}_2^n$ of a vector space $U \subseteq \mathbb{F}_2^n$ is called a *Gauss–Jordan basis* of U and denoted by $\mathrm{GJB}(U)$ if

$$\mathbf{u}_1 > \dots > \mathbf{u}_k \text{ and } (u_j)_{\nu(u_i)} = 0 \text{ for all } i \neq j.$$

Since the Gauss-Jordan basis of a vector space U is unique, we will represent U by its Gauss-Jordan basis $\mathrm{GJB}(U)$. A vector space $\bar{U} \subseteq \mathbb{F}_2^n$ is the *complement* of $U \subseteq \mathbb{F}_2^n$, if $\dim(U) + \dim(\bar{U}) = n$ and $U \cap \bar{U} = \{\mathbf{0}\}$. With the help of the introduced notation, the complement $\bar{U}$ of $U \subseteq \mathbb{F}_2^n$ can be computed as follows $\bar{U} = \{\mathbf{a} \in \mathbb{F}_2^n \colon a_i = 0 \text{ for all } i \in \Upsilon(U)\}$. We will call a t-dimensional affine subspace of $\mathbb{F}_2^n$ a *flat*. For a vector space $U \subseteq \mathbb{F}_2^n$, any flat $\mathbf{u} \oplus U$ can be uniquely represented as $\bar{\mathbf{u}} \oplus U$ for some $\bar{\mathbf{u}} \in \bar{U}$.

Representations of Boolean and vectorial functions. First, we consider polynomial representations of (n,m)-functions: the algebraic normal form and trace representations. We will frequently use these polynomial descriptions of (n,m)-functions throughout this dissertation and do not distinguish between polynomials and polynomial mappings.

Any Boolean function $f \colon \mathbb{F}_2^n \to \mathbb{F}_2$ can be uniquely expressed as a multivariate polynomial in the ring $\mathbb{F}_2[x_1, \dots, x_n]/(x_1 \oplus x_1^2, \dots, x_n \oplus x_n^2)$. This representation is unique and called the *algebraic normal form* (denoted as ANF), namely

$$f(\mathbf{x}) = \bigoplus_{\mathbf{a} \in \mathbb{F}_2^n} c_{\mathbf{a}} \mathbf{x}^{\mathbf{a}} = \bigoplus_{\mathbf{a} \in \mathbb{F}_2^n} c_{\mathbf{a}} \left(\prod_{i=1}^{n} x_i^{a_i} \right), \tag{1.2}$$

where $\mathbf{x} = (x_1, \ldots, x_n) \in \mathbb{F}_2^n$, $c_\mathbf{a} \in \mathbb{F}_2$ and $\mathbf{a} = (a_1, \ldots, a_n) \in \mathbb{F}_2^n$. The *complement* of a Boolean function f is defined by $\bar{f} := f \oplus 1$. If an (n, m)-function F and a (k, m)-function G do not have common variables, then the $(n + k, m)$-function H defined by $H(\mathbf{x}, \mathbf{y}) := F(\mathbf{x}) \oplus G(\mathbf{y})$ is called the *direct sum* of functions F and G. Similarly, we define the *k-fold direct sum* $k \cdot F \colon \mathbb{F}_2^{k \cdot n} \to \mathbb{F}_2^m$ in the following way $k \cdot F(\mathbf{x}_1, \ldots, \mathbf{x}_k) := F(\mathbf{x}_1) \oplus \cdots \oplus F(\mathbf{x}_k)$, where $\mathbf{x}_i \in \mathbb{F}_2^n$.

The *algebraic degree* of a Boolean function $f \colon \mathbb{F}_2^n \to \mathbb{F}_2$, denoted by $\deg(f)$, is the algebraic degree of its ANF as a multivariate polynomial, which is formally defined as follows $\deg(f) := \max_{\mathbf{a} \in \mathbb{F}_2^n, c_\mathbf{a} \neq 0} \operatorname{wt}(\mathbf{a})$, where $\operatorname{wt}(\mathbf{a}) = \sum_{i=1}^n a_i \in \mathbb{Z}$ is the *Hamming weight* of $\mathbf{a} \in \mathbb{F}_2^n$. This definition can be essentially extended to the vectorial case using the notion of coordinate functions. Any vectorial function $F \colon \mathbb{F}_2^n \to \mathbb{F}_2^m$ can be uniquely described by *m coordinate Boolean functions* $f_i \colon \mathbb{F}_2^n \to \mathbb{F}_2$ for $1 \leq i \leq m$ as a column vector $F(\mathbf{x}) := (f_1(\mathbf{x}), \ldots, f_m(\mathbf{x}))^T$. In this way, the *algebraic normal form* of a vectorial (n, m)-function F is defined coordinate-wise and its *algebraic degree* is defined as $\deg(F) := \max_{1 \leq i \leq m} \deg(f_i)$. An (n, m)-function F is called *d-homogeneous*, if all the monomials in its ANF have the same degree d, and simply *homogeneous*, if the degree is clear from the context. In the following, we will deal with three important classes of (n, m)-functions:

- *Affine functions*, i.e., (n, m)-functions F with $\deg(F) \leq 1$;
- *Quadratic functions*, i.e., (n, m)-functions F with $\deg(F) = 2$;
- *Cubic functions*, i.e., (n, m)-functions F with $\deg(F) = 3$.

Let F be an (n, m)-function and assume that m divides n. For the univariate trace representation, we endow $\mathbb{F}_2^n$ with the structure of the finite field $(\mathbb{F}_{2^n}, +, \cdot)$ and define the *relative trace* $\operatorname{Tr}_m^n \colon \mathbb{F}_{2^n} \to \mathbb{F}_{2^m}$ as follows $\operatorname{Tr}_m^n(x) = \sum_{i=0}^{\frac{n}{m}-1} x^{2^{i \cdot m}}$. For $m = 1$, we deal with the *absolute trace* and use the notation $\operatorname{Tr}(x) := \operatorname{Tr}_1^n(x)$ for $x \in \mathbb{F}_{2^n}$. Due to Lagrange interpolation, any (n, n)-function F can be uniquely represented as a polynomial $F \colon \mathbb{F}_{2^n} \to \mathbb{F}_{2^n}$ given by $F(x) = \sum_{i=0}^{2^n-1} a_i x^i$ with coefficients $a_i \in \mathbb{F}_{2^n}$. When $m|n$, any (n, m)-function can be written in the form $G(x) = \operatorname{Tr}_m^n \left(\sum_{i=0}^{2^n-1} a_i x^i \right)$. This representation is called the *univariate (trace) representation*, however, it is not unique in general. Similarly, one can obtain a *bivariate (trace) representation* of a $(2k, m)$-function F. It is enough to identify $\mathbb{F}_{2^n}$ with $\mathbb{F}_{2^k} \times \mathbb{F}_{2^k}$ and consider the functions of the form $F(x, y) = \operatorname{Tr}_m^k \left(\sum_{i,j=0}^{2^k-1} a_{i,j} x^i y^j \right)$. In order to compute the algebraic degree for trace representations, we identify an exponent $d \in \mathbb{N}$ with its binary representation $\mathbf{d} = (d_1, \ldots, d_n) \in \mathbb{F}_2^n$ as $d = \sum_{i=1}^n d_i 2^{n-i}$. Then the algebraic degree of an (n, m)-function F, given by a trace representation, is computed in the following way:

- $\deg(F) = \max\limits_{i \colon a_i \neq 0} \operatorname{wt}(i)$ for the univariate representation and

- $\deg(F) = \max\limits_{(i,j)\colon a_{i,j}\neq 0} (\mathrm{wt}(i) + \mathrm{wt}(j))$ for the bivariate representation.

Besides the algebraic normal form and trace representations, we will also use "polynomial-free" representations of Boolean and vectorial functions. We identify a vector $\mathbf{x} = (x_1, \ldots, x_n) \in \mathbb{F}_2^n$ with its integer representation $\mathbf{x} = \sum_{i=1}^n x_i 2^{n-i}$. In this way, any Boolean function f on $\mathbb{F}_2^n$ is uniquely determined by the vector $\mathbf{f} := (f(0), f(1), \ldots, f(2^n - 1)) \in \mathbb{F}_2^{2^n}$, which is called the *truth table* of the Boolean function f. The *(Hamming) weight* $\mathrm{wt}(f)$ of a Boolean function f on $\mathbb{F}_2^n$ is defined as the Hamming weight of its truth table $\mathbf{f}$. The truth table of a vectorial (n,m)-function is defined coordinate-wise. The *support* $\mathcal{D}_f \subseteq \mathbb{F}_2^n$ of a Boolean function f on $\mathbb{F}_2^n$ is the set $\mathcal{D}_f := f^{-1}(1)$. The *graph* $\mathcal{G}_F$ of an (n,m)-function F is the set $\mathcal{G}_F := \{(\mathbf{x}, F(\mathbf{x}))\colon \mathbf{x} \in \mathbb{F}_2^n\} \subseteq \mathbb{F}_2^n \times \mathbb{F}_2^m$.

Nonlinearity and differential uniformity. Now we introduce two concepts, which reflect confusion and diffusion of (n,m)-functions, namely nonlinearity and differential uniformity.

In order to provide a good confusion, a given (n,m)-function F has to be as far away as possible from the set of most predictable functions, i.e., the set of *affine* (n,m)*-functions*, which is denoted by $\mathcal{A}_{n,m}$ in the vectorial case and by $\mathcal{A}_n$ in the case of Boolean functions on $\mathbb{F}_2^n$. The *nonlinearity of a Boolean function* $f\colon \mathbb{F}_2^n \to \mathbb{F}_2$ is a measure of the distance between the function f and the set of all affine functions $\mathcal{A}_n$. Formally, it is defined as $\mathrm{nl}(f) := \min\limits_{l \in \mathcal{A}_n} d_H(f, l)$, where $d_H(f,g)$ is the *Hamming distance* between functions f and g on $\mathbb{F}_2^n$, which is computed as follows $d_H(f,g) := |\{\mathbf{x} \in \mathbb{F}_2^n\colon f(\mathbf{x}) \neq g(\mathbf{x})\}|$. This definition can be extended for the vectorial case using the notion of component functions. For an (n,m)-function F, we define the *component function* $F_{\mathbf{b}}$ as the Boolean function $F_{\mathbf{b}}\colon \mathbb{F}_2^n \to \mathbb{F}_2$, given by $F_{\mathbf{b}}(\mathbf{x}) := \langle \mathbf{b}, F(\mathbf{x})\rangle_m$, where $\langle \cdot, \cdot \rangle_m$ is a nondegenerate bilinear form on $\mathbb{F}_2^m$. Note that for an $(n,1)$-function F (i.e., a Boolean function) we have only one nonzero component function $F_1 := F$. In this way, the *nonlinearity of a vectorial* (n,m)*-function* F is the minimum nonlinearity among its component functions, that is, $\mathrm{nl}(F) := \min\limits_{l \in \mathcal{A}_n, \mathbf{b} \in \mathbb{F}_2^m \setminus \{\mathbf{0}\}} d_H(F_{\mathbf{b}}, l)$. The main tool to compute the nonlinearity of an (n,m)-function F is the *Walsh transform* $\hat{\chi}_F\colon \mathbb{F}_2^n \times \mathbb{F}_2^m \to \mathbb{Z}$ defined by

$$\hat{\chi}_F(\mathbf{a}, \mathbf{b}) := \hat{\chi}_{F_{\mathbf{b}}}(\mathbf{a}) \quad \text{and} \quad \hat{\chi}_{F_{\mathbf{b}}}(\mathbf{a}) := \sum_{\mathbf{x} \in \mathbb{F}_2^n} (-1)^{F_{\mathbf{b}}(\mathbf{x}) \oplus \langle \mathbf{a}, \mathbf{x} \rangle_n} \tag{1.3}$$

for $\mathbf{a} \in \mathbb{F}_2^n$ and $\mathbf{b} \in \mathbb{F}_2^m$. Note that the Walsh transform is a special version of the more general discrete Fourier transform. The multiset

$$\Lambda_F := \{* \; \hat{\chi}_F(\mathbf{a}, \mathbf{b})\colon \mathbf{a} \in \mathbb{F}_2^n, \mathbf{b} \in \mathbb{F}_2^m \setminus \{\mathbf{0}\} \; *\}$$

is called the *Walsh spectrum* of an (n,m)-function F. The *extended Walsh spectrum* is the multiset $|\Lambda_F| := \{* \; |\hat{\chi}_F(\mathbf{a}, \mathbf{b})|\colon \mathbf{a} \in \mathbb{F}_2^n, \mathbf{b} \in \mathbb{F}_2^m \setminus \{\mathbf{0}\} \; *\}$. Using the

Walsh transform, the nonlinearity of an (n, m)-function F can be computed in the following way

$$\mathrm{nl}(F) := 2^{n-1} - \frac{1}{2} \cdot \max_{\mathbf{a} \in \mathbb{F}_2^n, \mathbf{b} \in \mathbb{F}_2^m \setminus \{\mathbf{0}\}} |\hat{\chi}_F(\mathbf{a}, \mathbf{b})| .$$

In the following result, we give a well-known upper bound on the nonlinearity of an arbitrary (n, m)-function F.

Result 1.2 (Covering radius bound). *Let F be an (n, m)-function. The nonlinearity of F is at most*

$$\mathrm{nl}(F) \leq 2^{n-1} - 2^{\frac{n}{2}-1}. \tag{1.4}$$

For n even and $m \leq n/2$, this bound is achieved by (n, m)-bent functions (see [75, 89]), which we introduce in the following subsection. When n is even and $m > n/2$, this bound is not tight. Note that it is a challenging problem to find (n, m)-functions with the best nonlinearity. For some values of n and m, the covering radius bound can be improved, although the expressions of the improved bounds become more complicated; for this reason they are omitted here. The reader can find the exact expressions of these bounds in [29, 30].

In order to provide a good diffusion, an (n, m)-function F must have the following property: any change in the input $\mathbf{x} \mapsto \mathbf{x} \oplus \mathbf{a}$ has to lead to a big change between the values $F(\mathbf{x})$ and $F(\mathbf{x} \oplus \mathbf{a})$; the latter can be formalized with the help of the notions of derivative and differential uniformity. With an (n, m)-function F one can associate the (n, m)-function $D_{\mathbf{a}}F$ defined by $D_{\mathbf{a}}F(\mathbf{x}) := F(\mathbf{x} \oplus \mathbf{a}) \oplus F(\mathbf{x})$, which is called the *first-order derivative* of the function F in the direction $\mathbf{a} \in \mathbb{F}_2^n$. Derivatives of higher orders are defined recursively, i.e., the *k-th order derivative* of an (n, m)-function F is given by $D_{\mathbf{a}_k} D_{\mathbf{a}_{k-1}} \ldots D_{\mathbf{a}_1} F(\mathbf{x}) := D_{\mathbf{a}_k}(D_{\mathbf{a}_{k-1}} \ldots D_{\mathbf{a}_1} F)(\mathbf{x})$.

Using the notion of the first-order derivative, we define differential uniformity as follows. An (n, m)-function F has *differential uniformity* δ, if the value $\delta(F)$ defined as follows

$$\delta(F) := \max_{\mathbf{a} \in \mathbb{F}_2^n \setminus \{\mathbf{0}\}, \mathbf{b} \in \mathbb{F}_2^m} \delta_F(\mathbf{a}, \mathbf{b}), \quad \text{where} \quad \delta_F(\mathbf{a}, \mathbf{b}) := |\{\mathbf{x} \in \mathbb{F}_2^n \colon D_{\mathbf{a}}F(\mathbf{x}) = \mathbf{b}\}|,$$

is equal to δ (see [90]). The multiset $\Delta_F := \{* \, \delta_F(\mathbf{a}, \mathbf{b}) \colon \mathbf{a} \in \mathbb{F}_2^n \setminus \{\mathbf{0}\}, \mathbf{b} \in \mathbb{F}_2^m \, *\}$ is called the *differential spectrum* of the function F. The differential uniformity of an (n, m)-function F is at least

$$\delta(F) \geq 2^{n-m} \tag{1.5}$$

with equality if and only if all derivatives $D_{\mathbf{a}}F$ for nonzero $\mathbf{a} \in \mathbb{F}_2^n$ are balanced. We say that an (n, m)-function F is *balanced* if for any $\mathbf{b} \in \mathbb{F}_2^m$ holds $|F^{-1}(\mathbf{b})| = 2^{n-m}$, i.e., the function F takes each value $\mathbf{b} \in \mathbb{F}_2^m$ equally often.

Equivalence relations for cryptographic functions. Now we define the following three equivalence relations for (n, m)-functions, which preserve nonlinearity and differential properties.

Definition 1.3. Let F and F' be two (n, m)-functions. The functions F and F' are said to be:

- *Affine equivalent*, if there exist two affine permutations $A_1 \colon \mathbb{F}_2^m \to \mathbb{F}_2^m$ and $A_2 \colon \mathbb{F}_2^n \to \mathbb{F}_2^n$ such that $A_1 \circ F \circ A_2 = F'$.

- *Extended-affine equivalent* (*EA-equivalent*), if there exist two affine permutations $A_1 \colon \mathbb{F}_2^m \to \mathbb{F}_2^m, A_2 \colon \mathbb{F}_2^n \to \mathbb{F}_2^n$ and an affine function $A_3 \colon \mathbb{F}_2^n \to \mathbb{F}_2^m$ such that $A_1 \circ F \circ A_2 \oplus A_3 = F'$.

- *Carlet-Charpin-Zinoviev equivalent* (*CCZ-equivalent*), if there exists an affine permutation $\mathcal{L}$ on $\mathbb{F}_2^n \times \mathbb{F}_2^m$ such that $\mathcal{L}\left(\mathcal{G}_F\right) = \mathcal{G}_{F'}$.

It is not difficult to show that affine equivalence implies EA-equivalence, and EA-equivalence implies CCZ-equivalence. The question whether the converse is also true for a given class of (n, m)-functions is in general difficult. In the following subsection, we will give several classes of functions, for which CCZ-equivalence and EA-equivalence coincide.

Definition 1.4. Let F be an (n, m)-function. An affine permutation $\mathcal{L}$ on $\mathbb{F}_2^n \times \mathbb{F}_2^m$ is called an *automorphism* of F if it fixes the graph $\mathcal{G}_F$, i.e., $\mathcal{L}(\mathcal{G}_F) = \mathcal{G}_F$. The set of all automorphisms of an (n, m)-function F forms a group, which is called the *automorphism group of F* and is denoted by $\mathrm{Aut}(F)$.

Remark 1.5. The differential spectrum and the extended Walsh spectrum are invariants under all the aforementioned types of equivalence, and hence the nonlinearity and differential uniformity are invariants as well. The automorphism group $\mathrm{Aut}(F)$ of an (n, m)-function F is invariant under CCZ-equivalence. The algebraic degree $\deg(F)$ of an (n, m)-function F is invariant under affine equivalence and EA-equivalence, but not invariant under CCZ-equivalence [14].

1.1.2 Bent functions

In general, (n, m)-functions with the maximum nonlinearity and (n, m)-functions with the minimum differential uniformity are two different sets of functions. However, as the following result shows in some cases these sets are the same.

Result 1.6. *[81, 89] Let F be an (n, m)-function with n even and $m \leq n/2$. The following statements are equivalent.*

1. *The function F has the maximum nonlinearity* $\mathrm{nl}(F) = 2^{n-1} - 2^{\frac{n}{2}-1}$.

2. *The function F has the minimum differential uniformity* $\delta(F) = 2^{n-m}$.

3. *For all* $\mathbf{a} \in \mathbb{F}_2^n$ *and* $\mathbf{b} \in \mathbb{F}_2^m \setminus \{\mathbf{0}\}$ *the Walsh transform satisfies* $|\hat{\chi}_F(\mathbf{a}, \mathbf{b})| = 2^{n/2}$.

Boolean functions satisfying the condition of the last claim in Result 1.6 are called Boolean bent functions and were introduced by Rothaus [103] as follows.

Definition 1.7. Let n be even. A Boolean function $f \colon \mathbb{F}_2^n \to \mathbb{F}_2$ is called *bent* if the Walsh transform of f satisfies $\hat{\chi}_f(\mathbf{a}) = \pm 2^{n/2}$ for all $\mathbf{a} \in \mathbb{F}_2^n$.

In view of Result 1.6, (n, m)-functions with n even and $m \leq n/2$ having the maximum nonlinearity are called (n, m)-bent functions.

Definition 1.8. Let n be even and $m \leq n/2$. An (n, m)-function F is called *(n, m)-bent,* if it achieves the covering radius bound (1.4) with equality, i.e., $\mathrm{nl}(F) = 2^{n-1} - 2^{\frac{n}{2}-1}$.

Throughout this thesis, we denote the *set of (n, m)-bent functions* by $\mathcal{B}_{n,m}$ and the set of Boolean bent functions on $\mathbb{F}_2^n$ by $\mathcal{B}_n$.

Remark 1.9. Boolean bent functions on $\mathbb{F}_2^n$ exist if and only if n is even, as it was shown by Rothaus [103]. The algebraic degree of a bent function on $\mathbb{F}_2^n$ is at most $n/2$, see [103]. Due to the Nyberg bound [89], (n, m)-bent functions do not exist for $m > n/2$.

Result 1.10 (Nyberg bound)**.** *Let F be an (n, m)-bent function. Then $m \leq n/2$.*

In this thesis, we will be interested in the most general type of equivalence for Boolean and vectorial bent functions, what in view of the following result, reduces the investigation to EA-equivalence.

Result 1.11. *[15, 54, 65] Let f, f' be two Boolean functions on $\mathbb{F}_2^n$ and F, F' be two (n, m)-bent functions. The following hold.*

1. *Boolean functions f and f' are CCZ-equivalent if and only if f and f' are EA-equivalent.*

2. *Bent functions F and F' are CCZ-equivalent if and only if F and F' are EA-equivalent.*

In this way, for a given class $\mathcal{C} \subseteq \mathcal{B}_{n,m}$ of (n, m)-bent functions (and (n, m)-functions in general) it is essential to define the smallest possible class, which contains all functions EA-equivalent to the members of $\mathcal{C}$.

Definition 1.12. A class of (n, m)-functions $\mathcal{C}$ is called *complete* if it is invariant under EA-equivalence. The *completed class* $\mathcal{C}^{\#}$ is the smallest possible class invariant under EA-equivalence, which contains $\mathcal{C}$.

Generalizations of bent functions. Bentness of (n, m)-functions for n even and $m \leq n/2$ is characterized by the minimal cardinality of either the extended Walsh spectrum or of the differential spectrum (both are considered as sets). Further generalizations of bent functions are obtained by relaxing slightly the minimality conditions.

The first important generalization of the class of bent functions is the class of plateaued functions defined in the following way.

Definition 1.13. A Boolean function $f\colon \mathbb{F}_2^n \to \mathbb{F}_2$ is said to be *s-plateaued*, if for all $\mathbf{a} \in \mathbb{F}_2^n$ the absolute value of its Walsh transform takes only two values, i.e., $|\hat{\chi}_f(\mathbf{a})| \in \{0, 2^{\frac{n+s}{2}}\}$. The value $2^{\frac{n+s}{2}}$ is called the *amplitude* of an s-plateaued Boolean function f. An (n, m)-function F is said to be *s-plateaued* if all its component functions $F_{\mathbf{b}}$ with $\mathbf{b} \neq \mathbf{0}$ are s-plateaued. If all the component functions $F_{\mathbf{b}}$ of an (n, m)-function F are $s_{\mathbf{b}}$-plateaued (not necessarily with the same amplitude), then F is called an *(n, m)-plateaued* function. Boolean 1-plateaued functions on $\mathbb{F}_2^n$ with n odd and 2-plateaued functions on $\mathbb{F}_2^n$ with n even are called *semi-bent*. For n odd, an (n, n)-function F is called *almost bent*, or simply *AB*, if for all nonzero $\mathbf{b} \in \mathbb{F}_2^n$ its component functions $F_{\mathbf{b}}$ are semi-bent.

Now we give the following characterization of plateaued Boolean functions by means of second-order derivatives.

Result 1.14. *[31, Theorem 1] A Boolean function f on $\mathbb{F}_2^n$ is s-plateaued if and only if*

$$\sum_{\mathbf{a},\mathbf{b} \in \mathbb{F}_2^n} (-1)^{D_{\mathbf{a},\mathbf{b}} f(\mathbf{x})} = 2^{n+s} \tag{1.6}$$

holds for all $\mathbf{x} \in \mathbb{F}_2^n$.

Proof. The function f satisfies (1.6) if and only if for all $\mathbf{x} \in \mathbb{F}_2^n$ holds

$$\sum_{\mathbf{a},\mathbf{b} \in \mathbb{F}_2^n} (-1)^{f(\mathbf{x} \oplus \mathbf{a}) \oplus f(\mathbf{x} \oplus \mathbf{b}) \oplus f(\mathbf{x} \oplus \mathbf{a} \oplus \mathbf{b})} = 2^{n+s} \cdot (-1)^{f(\mathbf{x})}.$$

Going to the Walsh transform, we have that the identity $\hat{\chi}_f^3(\mathbf{u}) = 2^{n+s} \hat{\chi}_f(\mathbf{u})$ holds for all $\mathbf{u} \in \mathbb{F}_2^n$, which is possible if and only if $\hat{\chi}_f(\mathbf{u}) = \pm 2^{\frac{n+s}{2}}$. The latter is equivalent to the fact that the function f is s-plateaued. □

The characterization of vectorial (n, m)-plateaued functions is similar and can be obtained by applying Result 1.14 coordinate-wise.

Result 1.15. *[28, Theorem 1]. Let F be an (n, m)-function. For $\mathbf{v} \in \mathbb{F}_2^m$ and $\mathbf{x} \in \mathbb{F}_2^m$ we define*

$$N_F(\mathbf{v}, \mathbf{x}) = |\, \{(\mathbf{a}, \mathbf{b}) \in \mathbb{F}_2^n \times \mathbb{F}_2^n \colon D_{\mathbf{a},\mathbf{b}} F(\mathbf{x}) = \mathbf{v}\} \,|. \tag{1.7}$$

Then the following holds.

1. *The function F is plateaued if and only if, for every $\mathbf{v} \in \mathbb{F}_2^m$ the number $N_F(\mathbf{v},\mathbf{x})$ does not depend on $\mathbf{x} \in \mathbb{F}_2^n$.*
2. *The function F is plateaued with single amplitude if and only if the number $N_F(\mathbf{v},\mathbf{x})$ does not depend on $\mathbf{x} \in \mathbb{F}_2^n$, nor on $\mathbf{v} \in \mathbb{F}_2^m$ when $\mathbf{v} \neq \mathbf{0}$.*

Proof. For any $\mathbf{v} \in \mathbb{F}_2^m$, consider the following sum

$$\sum_{\mathbf{u}\in\mathbb{F}_2^m}\sum_{\mathbf{a},\mathbf{b}\in\mathbb{F}_2^n}(-1)^{\langle\mathbf{u},D_{\mathbf{a},\mathbf{b}}F(\mathbf{x})\rangle_m\oplus\langle\mathbf{u},\mathbf{v}\rangle_m} = \sum_{\mathbf{a},\mathbf{b}\in\mathbb{F}_2^n}\sum_{\mathbf{u}\in\mathbb{F}_2^m}(-1)^{\langle\mathbf{u},D_{\mathbf{a},\mathbf{b}}F(\mathbf{x})\oplus\mathbf{v}\rangle_m}, \tag{1.8}$$

which is equal to $2^m \cdot |\{(\mathbf{a},\mathbf{b}) \in \mathbb{F}_2^n \times \mathbb{F}_2^n \colon D_{\mathbf{a},\mathbf{b}}F(\mathbf{x}) = \mathbf{v}\}|$. In this way, for any $\mathbf{x} \in \mathbb{F}_2^n$ and $\mathbf{v} \in \mathbb{F}_2^m$ the number $N_F(\mathbf{v},\mathbf{x})$ can be computed as follows

$$\begin{aligned} N_F(\mathbf{v},\mathbf{x}) =& 2^{-m}\cdot\sum_{\mathbf{u}\in\mathbb{F}_2^m}\sum_{\mathbf{a},\mathbf{b}\in\mathbb{F}_2^n}(-1)^{\langle\mathbf{u},D_{\mathbf{a},\mathbf{b}}F(\mathbf{x})\rangle_m\oplus\langle\mathbf{u},\mathbf{v}\rangle_m} & (1.9)\\ =& 2^{-m}\cdot\sum_{\mathbf{u}\in\mathbb{F}_2^m}(-1)^{\langle\mathbf{u},\mathbf{v}\rangle_m}\cdot\left(\sum_{\mathbf{a},\mathbf{b}\in\mathbb{F}_2^n}(-1)^{D_{\mathbf{a},\mathbf{b}}F_{\mathbf{u}}(\mathbf{x})}\right). & (1.10)\end{aligned}$$

The first claim now follows from the fact that the sum $\sum_{\mathbf{a},\mathbf{b}\in\mathbb{F}_2^n}(-1)^{D_{\mathbf{a},\mathbf{b}}F_{\mathbf{u}}(\mathbf{x})}$ in (1.10) is independent on $\mathbf{x} \in \mathbb{F}_2^n$ for any $\mathbf{u} \in \mathbb{F}_2^m$ if and only if any component function $F_{\mathbf{u}}$ of F is plateaued, or equivalently, if and only if F is (n,m)-plateaued. The second claim follows from the fact that the sum $\sum_{\mathbf{a},\mathbf{b}\in\mathbb{F}_2^n}(-1)^{D_{\mathbf{a},\mathbf{b}}F_{\mathbf{u}}(\mathbf{x})}$ in (1.10) is independent on $\mathbf{x} \in \mathbb{F}_2^n$ and $\mathbf{u} \in \mathbb{F}_2^m \setminus \{\mathbf{0}\}$ if and only if any component function $F_{\mathbf{u}}$ of F is s-plateaued for some $s \in \mathbb{Z}$, or equivalently, if and only if the (n,m)-function F is s-plateaued. □

The following generalizations of bent functions are obtained by allowing the differential spectrum, considered as a set, to take only one different from zero value.

Definition 1.16. An (n,m)-function F is called *differentially two-valued*, if there are only two different values in the differential spectrum, that is, $\Delta_F = \{0, 2^s\}$ (multiplicities are omitted). In particular, (n,n)-functions F with $\Delta_F = \{0,2\}$ are called *almost perfect nonlinear* or simply *APN*.

Example 1.17. [52] Consider Gold APN functions, i.e., power functions on $\mathbb{F}_2^n$, given by $F\colon x \in \mathbb{F}_{2^n} \mapsto x^{2^i+1}$ with $\gcd(i,n) = 1$. If n is odd, then the Walsh spectrum of F is given by

$$\Lambda_F = \left\{*\ 0\ \left[2^{n-1}\cdot(2^n-1)\right],\ \pm 2^{\frac{n+1}{2}}\ \left[(2^n-1)\cdot\left(2^{n-2}\pm 2^{\frac{n-3}{2}}\right)\right]*\right\}. \tag{1.11}$$

In this case, F is AB, since all the nonzero component functions are semi-bent. For n even, the Walsh spectrum of f is given by

$$\begin{aligned}\Lambda_F = \Big\{*\ 0\ \left[2^{n-2}\cdot(2^n-1)\right],\ \pm 2^{\frac{n+2}{2}}\ \left[\tfrac{1}{3}(2^n-1)\cdot\left(2^{n-3}\pm 2^{\frac{n-4}{2}}\right)\right],\\ \pm 2^{\frac{n}{2}}\ \left[\tfrac{2}{3}(2^n-1)\cdot\left(2^{n-1}\pm 2^{\frac{n}{2}-1}\right)\right]\ *\Big\},\end{aligned} \tag{1.12}$$

that is, $2(2^n - 1)/3$ nonzero component functions of F are bent, and $(2^n - 1)/3$ are semi-bent.

The following definition is motivated by the fact that most of the known constructions of APN functions have the Walsh spectrum of Gold APN functions.

Definition 1.18. Let F be an APN function on $\mathbb{F}_2^n$. Without loss of generality we assume that $F(\mathbf{0}) = \mathbf{0}$. We say that APN function F on $\mathbb{F}_2^n$ has *the classical Walsh spectrum*, if it has the Walsh spectrum of Gold APN functions, i.e., Λ_F is given by (1.11) for n odd, and by (1.12) for n even.

Remark 1.19. Any AB function is APN [32]. The converse of this statement is not true in general, as the example of the Dobbertin power APN function $f(x) = x^d$ on $\mathbb{F}_{2^n}$ with $n = 5m$ and $d = 2^{4m} + 2^{3m} + 2^{2m} + 2^m - 1$ shows [19].

Remark 1.20. For (n, n)-functions F with n odd, the covering radius bound (1.4) can be improved, see [29, p. 370]. The upper bound on the nonlinearity of (n, n)-functions F with n odd is given by $\mathrm{nl}(F) \leq 2^{n-1} - 2^{\frac{n-1}{2}}$, and it is achieved by AB functions. In this way, AB functions, similarly to bent functions, have optimal nonlinearity and differential uniformity. This is the reason, why they are called almost bent. To determine the nonlinearity of an arbitrary APN function is, in general, difficult.

Finally, we refer to the paper of Budaghyan and Pott [16] for the study of differentially two-valued and s-plateaued functions.

Perfect nonlinear functions. We will use the term *perfect nonlinear function* to describe those functions, which have either the best nonlinearity or best differential uniformity, i.e., (n, m)-bent functions and APN (almost perfect nonlinear) functions. Although APN functions do not achieve the lower bound on the differential uniformity (1.5), since in the even characteristic with a solution $\mathbf{x} \in \mathbb{F}_2^n$ of the equation $F(\mathbf{x}) \oplus F(\mathbf{x} \oplus \mathbf{a}) = \mathbf{b}$ one always has a solution $\mathbf{x} \oplus \mathbf{a}$, they achieve the minimum possible value of differential uniformity for (n, n)-functions F, i.e., $\delta(F) = 2$. From this point of view, we consider throughout this thesis the class of perfect nonlinear functions as the union of Boolean bent functions, vectorial bent functions and APN functions.

1.1.3 Fundamental classes of bent functions

In this subsection, we summarize several general classes of Boolean and vectorial bent functions: quadratic, Maiorana-McFarland and partial spread bent functions.

Quadratic Boolean bent functions

The class of quadratic Boolean bent functions is, probably, the only one completely understood class of Boolean bent functions. In order to characterize quadratic Boolean bent functions, we first give the general definition of the quadratic form.

Definition 1.21. A *quadratic form* on a vector space V over a field F is a mapping $f : V \to F$ satisfying the following two conditions:

1. $f(c\mathbf{x}) = c^2 f(\mathbf{x})$ for all $c \in F, \mathbf{x} \in V$;
2. The function (form) $Q_f \colon V \times V \to F$ given by

$$Q_f(\mathbf{x},\mathbf{y}) = f(\mathbf{x}+\mathbf{y}) - f(\mathbf{x}) - f(\mathbf{y})$$

is bilinear.

The bilinear form $Q_f \colon V \times V \to F$ is said to be obtained by *polarization* of the function f. The *radical* of a quadratic form $f \colon V \to F$ is defined as

$$\mathcal{W}_f := \{\mathbf{y} \in V \colon Q_f(\mathbf{x},\mathbf{y}) = \mathbf{0} \text{ for all } \mathbf{x} \in V\},$$

which is a linear subspace of V. If $\dim(\mathcal{W}_f) = 0$, i.e., $\mathcal{W}_f = \{\mathbf{0}\}$, then f is called *nondegenerate*, and *degenerate*, otherwise.

In the following statement, we illustrate that one can read off all the differential properties of a quadratic Boolean function from its algebraic normal form and thus characterize perfect nonlinearity of quadratic functions. This is, in general, not the case for an arbitrary class of Boolean functions.

Proposition 1.22. *Let $f \colon \mathbb{F}_2^n \to \mathbb{F}_2$ be a quadratic function, which is given by*

$$f(\mathbf{x}) = \mathbf{x}\mathbf{A}\mathbf{x}^T \oplus l(\mathbf{x}), \tag{1.13}$$

where $\mathbf{A}$ is an upper triangular matrix with a zero diagonal and $l \colon \mathbb{F}_2^n \to \mathbb{F}_2$ is an arbitrary affine function. Then the bilinear form $Q_f \colon \mathbb{F}_2^n \times \mathbb{F}_2^n \to \mathbb{F}_2$ obtained by polarization *of f is given by*

$$Q_f(\mathbf{x},\mathbf{y}) = \mathbf{x}\mathbf{B}\mathbf{y}^T, \tag{1.14}$$

where $\mathbf{B} = \mathbf{A} \oplus \mathbf{A}^T$. Consequently, f on $\mathbb{F}_2^n$ is bent if and only if $\mathrm{rank}_{\mathbb{F}_2}(\mathbf{B}) = n$.

Proof. First, we compute the bilinear form Q_f in the following way:

$$\begin{aligned} Q_f(\mathbf{x},\mathbf{y}) &= (\mathbf{x}\oplus\mathbf{y})\mathbf{A}(\mathbf{x}\oplus\mathbf{y})^T \oplus \mathbf{x}\mathbf{A}\mathbf{x}^T \oplus \mathbf{y}\mathbf{A}\mathbf{y}^T \oplus l(\mathbf{x}\oplus\mathbf{y}) \oplus l(\mathbf{x}) \oplus l(\mathbf{y}) \\ &= \mathbf{x}\mathbf{A}\mathbf{x}^T \oplus \mathbf{x}\mathbf{A}\mathbf{y}^T \oplus \mathbf{y}\mathbf{A}\mathbf{x}^T \oplus \mathbf{x}\mathbf{A}\mathbf{x}^T = \mathbf{x}(\mathbf{A}\oplus\mathbf{A}^T)\mathbf{y}^T = \mathbf{x}\mathbf{B}\mathbf{y}^T = \mathbf{y}\mathbf{B}\mathbf{x}^T. \end{aligned}$$

Since $D_{\mathbf{a}}f(\mathbf{x}) = Q_f(\mathbf{x},\mathbf{a}) \oplus f(\mathbf{a})$, we have that $D_{\mathbf{a}}f$ is balanced for all $\mathbf{a} \in \mathbb{F}_2^n, \mathbf{a} \neq \mathbf{0}$ if and only if the symplectic matrix $\mathbf{B}$ is invertible. □

Corollary 1.23. *Let $f\colon \mathbb{F}_2^n \to \mathbb{F}_2$ be a quadratic Boolean function. Then f is bent if and only if f is nondegenerate.*

Consequently, the fact that homogeneous quadratic Boolean bent functions are in 1-to-1 correspondence with invertible symplectic $n \times n$-matrices over $\mathbb{F}_2$ immediately implies enumeration and classification of quadratic Boolean bent functions.

Result 1.24. *[75, Chapter 15]* 1. *The number of quadratic Boolean bent functions on $\mathbb{F}_2^n$ is given by*

$$|\mathcal{B}_n| = 2^{(k+1)^2-k} \prod_{i=0}^{k-1} \left(2^{2i+1}-1\right). \tag{1.15}$$

2. *Every quadratic Boolean bent function $f\colon \mathbb{F}_2^n \to \mathbb{F}_2$ is equivalent to the function Q_n on $\mathbb{F}_2^n$, given by*

$$Q_n\colon (x_1,\dots,x_n) \mapsto x_1x_2 \oplus x_3x_4 \oplus \cdots \oplus x_{n-1}x_n. \tag{1.16}$$

Remark 1.25. More general, symplectic $n \times n$ matrices of even rank $r \le n$ are in 1-to-1 correspondence with homogeneous quadratic Boolean s-plateaued functions on $\mathbb{F}_2^n$ with $s = n - r$. Let f be a quadratic Boolean function on $\mathbb{F}_2^n$. By *"Dickson's theorem"* [75, p. 438], we have that the function f on $\mathbb{F}_2^n$ is EA-equivalent to the canonical quadratic function

$$Q_r\colon (x_1,\dots,x_n) \mapsto x_1x_2 \oplus x_3x_4 \oplus \cdots \oplus x_{r-1}x_r,$$

whose Hamming weight is equal to $\mathrm{wt}(Q_r) = 2^{n-1} - 2^{n-r/2-1}$. The second-order derivative $D_{\mathbf{a},\mathbf{b}}Q_r$ is a constant function, given by

$$D_{\mathbf{a},\mathbf{b}}Q_r(\mathbf{x}) = a_1b_2 \oplus a_2b_1 \oplus a_3b_4 \oplus a_4b_3 \oplus \cdots \oplus a_{r-1}b_r \oplus a_rb_{r-1},$$

which depends on $\mathbf{a},\mathbf{b} \in \mathbb{F}_2^n$. Considering $D_{\mathbf{a},\mathbf{b}}Q_r(\mathbf{x})$ as a quadratic function on $\mathbb{F}_2^n \times \mathbb{F}_2^n$, we get $\mathrm{wt}(D_{\mathbf{a},\mathbf{b}}Q_r) = 2^{2n-1} - 2^{2n-r-1} = 2^{2n-1} - 2^{n+s-1}$, where $s = n - r$. In this way, for $\epsilon \in \mathbb{F}_2^n$ we have

$$|\{(\mathbf{a},\mathbf{b}) \in \mathbb{F}_2^n \times \mathbb{F}_2^n\colon D_{\mathbf{a},\mathbf{b}}Q_r = \epsilon\}| = 2^{2n-1} + (-1)^{\epsilon} \cdot 2^{n+s-1},$$

and hence for the function f on $\mathbb{F}_2^n$ holds

$$\sum_{\mathbf{a},\mathbf{b} \in \mathbb{F}_2^n} (-1)^{D_{\mathbf{a},\mathbf{b}}f(\mathbf{x})} = 2 \cdot 2^{n+s-1} = 2^{n+s}.$$

By Result 1.14, the quadratic function f on $\mathbb{F}_2^n$ is s-plateaued.

The enumeration of quadratic s-plateaued functions follows from the enumeration of symplectic $n \times n$ matrices of a fixed even rank $r = n - s$, which can be found in [75, p. 436].

Quadratic vectorial bent functions

In view of Proposition 1.22, homogeneous quadratic vectorial (n,m)-bent functions are in 1-to-1 correspondence with the set of all possible representations of m-dimensional vector subspaces of invertible symplectic $n \times n$ matrices over $\mathbb{F}_2$. In general it is an open problem to establish the number of homogeneous quadratic vectorial (n,m)-bent functions for an arbitrary $m \leq n/2$. However, the case $m = 2$ was resolved by Pott, Schmidt and Zhou [99, Theorem 1]. They used tools from character theory to compute the number of pairs $(\mathbf{A}, \mathbf{B})$ of invertible alternating matrices over $\mathbb{F}_q$ such that $\mathbf{A} + \mathbf{B}$ is also invertible. Consequently, according to their result the number of quadratic $(n,2)$-bent functions is given as follows.

Result 1.26. *[99, Theorem 1] Let $n = 2k$. The number of quadratic $(n,2)$-bent functions is given by*

$$|\mathcal{B}_{n,2}| = 2^{(k+1)^2+1} \prod_{j=1}^{k} \left(2^{2j-1} - 1\right) \times \left(\sum_{i=0}^{k} (-1)^i 2^{i(i-1)} \begin{bmatrix} k \\ i \end{bmatrix} \prod_{j=1}^{k-i} \left(2^{2j-1} - 1\right)^2 \right), \tag{1.17}$$

where

$$\begin{bmatrix} x \\ l \end{bmatrix} = \prod_{i=1}^{l} \left(q^{2x-2i+2} - 1\right) / \left(q^{2i} - 1\right)$$

is the q^2-binomial coefficient defined for real x and nonnegative integer l, which is computed here for $q = 2$.

Remark 1.27. Similarly to the Boolean case, the number of quadratic $(n,2)$-bent functions is established for all $n \geq 4$, however, the number of equivalence classes of quadratic (n,m)-bent functions with $2 \leq m \leq n/2$ is not known in general. The classification of quadratic vectorial (n,m)-bent functions is known only for small values of n and m thanks to computer search:

- Up to EA-equivalence, there is only one $(4,2)$-bent function. Its algebraic normal form will be given later in Example 1.31.
- Up to EA-equivalence, there is one $(6,2)$-bent function and three $(6,3)$-bent functions, as it was shown in [1, Theorem 3.1].

In the following proposition, we show that, similarly to the Boolean case, all information about the differential properties of a quadratic vectorial function can be also recovered from its algebraic normal form.

Proposition 1.28. *Let F be a quadratic vectorial (n,m)-function with $2 \leq m \leq n$, which is given in the following way:*

$$F(\mathbf{x}) := \begin{pmatrix} f_1(\mathbf{x}) \\ \vdots \\ f_m(\mathbf{x}) \end{pmatrix} = \begin{pmatrix} \mathbf{x}\mathbf{A}_1\mathbf{x}^T \oplus l_1(\mathbf{x}) \\ \vdots \\ \mathbf{x}\mathbf{A}_m\mathbf{x}^T \oplus l_m(\mathbf{x}) \end{pmatrix}. \tag{1.18}$$

We define $\mathbf{B}_i := \mathbf{A}_i \oplus \mathbf{A}_i^T$ *for all* $1 \leq i \leq m$ *and let* $\mathbf{B} = [\mathbf{B}_1, \dots, \mathbf{B}_m]$ *be a tensor with elements* $\mathbf{B} = (b_{ijk})_{\substack{1\leq i\leq m \\ 1\leq j,k\leq n}}$*, i.e., the entry* b_{ijk} *in* $\mathbf{B}$ *is the entry* b_{jk} *in the matrix* $\mathbf{B}_i$*. We also define a mapping* $Q_F \colon \mathbb{F}_2^n \times \mathbb{F}_2^n \to \mathbb{F}_2^m$*, whose coordinate functions are bilinear forms* $Q_{f_i} \colon \mathbb{F}_2^n \times \mathbb{F}_2^n \to \mathbb{F}_2$*, namely*

$$Q_F(\mathbf{x}, \mathbf{y}) := [Q_{f_1}(\mathbf{x}, \mathbf{y}), \dots, Q_{f_m}(\mathbf{x}, \mathbf{y})]^T.$$

Then $Q_F(\mathbf{x}, \mathbf{y}) = \mathbf{M_y}F \cdot \mathbf{x}^T$*, where* $\mathbf{M_y}F$ *is the* $m \times n$ *matrix defined as follows*

$$\mathbf{M_y}F := \bigoplus_{j=1}^{n} y_j \mathbf{B}'_j,$$

where $\mathbf{y} \in \mathbb{F}_2^n$ *is the vector with coordinates* $\mathbf{y} = (y_1, \dots, y_n)$ *and for* $j = 1, \dots, n$ *the* $m \times n$ *matrix* $\mathbf{B}'_j$ *is defined by* $\mathbf{B}'_j := (b_{ijk})_{\substack{1\leq i\leq m \\ 1\leq k\leq n}}$*.*

Proof. By Proposition 1.22, the bilinear form Q_{f_i} is given by the following expression

$$\begin{aligned} Q_{f_i}(\mathbf{x}, \mathbf{y}) = \mathbf{y}\mathbf{B}_i\mathbf{x}^T &= \left(\bigoplus_{j=1}^{n} y_j b_{ij1}, \quad \dots, \quad \bigoplus_{j=1}^{n} y_j b_{ijn} \right) \mathbf{x}^T \\ &= \bigoplus_{k=1}^{n} x_k \left(\bigoplus_{j=1}^{n} y_j b_{ijk} \right). \end{aligned}$$

Now gathering the coefficient of the term x_k for the bilinear form Q_{f_i} of each coordinate function f_i, we get the following matrix $\mathbf{M_a}F$:

$$\mathbf{M_y}F = \begin{array}{cccccc} x_1 & \cdots & x_k & \cdots & x_n & \\ \bigoplus_{j=1}^{n} y_j b_{1j1} & \cdots & \bigoplus_{j=1}^{n} y_j b_{1jk} & \cdots & \bigoplus_{j=1}^{n} y_j b_{1jn} & f_1 \\ \vdots & \ddots & \vdots & \ddots & \vdots & \vdots \\ \bigoplus_{j=1}^{n} y_j b_{ij1} & \cdots & \bigoplus_{j=1}^{n} y_j b_{ijk} & \cdots & \bigoplus_{j=1}^{n} y_j b_{ijn} & f_i \\ \vdots & \ddots & \vdots & \ddots & \vdots & \vdots \\ \bigoplus_{j=1}^{n} y_j b_{mj1} & \cdots & \bigoplus_{j=1}^{n} y_j b_{mjk} & \cdots & \bigoplus_{j=1}^{n} y_j b_{mjn} & f_m \end{array} = \bigoplus_{j=1}^{n} y_j \mathbf{B}'_j, \tag{1.19}$$

where the matrix $\mathbf{B}'_j$ is defined as follows

$$\mathbf{B}'_j := \begin{array}{cccccc} x_1 & \cdots & x_j & \cdots & x_n & \\ b_{1j1} & \cdots & b_{1jk} & \cdots & b_{1jn} & f_1 \\ \vdots & \ddots & \vdots & \ddots & \vdots & \vdots \\ b_{ij1} & \cdots & b_{ijk} & \cdots & b_{ijn} & f_i \\ \vdots & \ddots & \vdots & \ddots & \vdots & \vdots \\ b_{mj1} & \cdots & b_{mjk} & \cdots & b_{mjn} & f_m \end{array} \cdot \tag{1.20}$$

In this way, the function Q_F is given by $Q_F(\mathbf{x},\mathbf{y}) = \mathbf{M_y}F \cdot \mathbf{x}^T$. □

Now we characterize quadratic vectorial bent functions, similarly to Proposition 1.22 for the Boolean case.

Theorem 1.29. *Let F be a quadratic vectorial (n,m)-function, which has the form* (1.18). *Let for any $\mathbf{a} \in \mathbb{F}_2^n$ with $\mathbf{a} \neq \mathbf{0}$ the matrix $\mathbf{M_a}F$ be defined as in* (1.19). *Then the vectorial (n,m)-function F is bent if and only if for any $\mathbf{a} \in \mathbb{F}_2^n \setminus \{\mathbf{0}\}$ we have $\operatorname{rank}_{\mathbb{F}_2}(\mathbf{M_a}F) = m$.*

Proof. By Proposition 1.22, the function Q_F is given by $Q_F(\mathbf{x},\mathbf{y}) = \mathbf{M_y}F \cdot \mathbf{x}^T$ and, consequently, the first-order derivative of F in direction $\mathbf{a} \in \mathbb{F}_2^n$ is given by

$$D_\mathbf{a}F(\mathbf{x}) = Q_F(\mathbf{x},\mathbf{a}) \oplus F(\mathbf{a}).$$

Then for any nonzero $\mathbf{a} \in \mathbb{F}_2^n$ and for any $\mathbf{b} \in \mathbb{F}_2^m$ the equation $D_\mathbf{a}F(\mathbf{x}) = \mathbf{b}$ has exactly 2^{n-m} solutions if and only if the equation

$$\mathbf{M_a}F \cdot \mathbf{x}^T = \mathbf{b}' \tag{1.21}$$

has 2^{n-m} solutions for any $\mathbf{b}' := \mathbf{b} \oplus F(\mathbf{a})$. The latter is equivalent to the fact that for any nonzero $\mathbf{a} \in \mathbb{F}_2^n$ the matrix $\mathbf{M_a}F$ has full rank, i.e., $\operatorname{rank}_{\mathbb{F}_2}(\mathbf{M_a}F) = m$. □

Remark 1.30. Following the proof of Theorem 1.29, one can characterize differentially 2-valued quadratic (n,n)-functions in the following way. Let F be a differentially 2-valued quadratic (n,n)-function, i.e., for some $s \in \mathbb{Z}$ we have $\Lambda_F = \{0, 2^s\}$ (multiplicities are omitted). In this way, equation (1.21) has 0 or 2^s solutions for any $\mathbf{b}' := \mathbf{b} \oplus F(\mathbf{a})$ if and only if for all $\mathbf{a} \in \mathbb{F}_2^n \setminus \{\mathbf{0}\}$ holds $\operatorname{rank}_{\mathbb{F}_2}(\mathbf{M_a}F) = n - s$.

Example 1.31. Let F be a quadratic $(4,2)$-bent function, given by

$$F(\mathbf{x}) := \begin{pmatrix} f_1(\mathbf{x}) \\ f_2(\mathbf{x}) \end{pmatrix} = \begin{pmatrix} x_1x_2 \oplus x_3x_4 \\ x_1x_2 \oplus x_1x_4 \oplus x_2x_3 \end{pmatrix}.$$

There are two ways to see that this function is vectorial bent. First, we consider the symplectic matrices $\mathbf{B}_i$, corresponding to the coordinate functions f_i:

$$\mathbf{B}_1 = \begin{pmatrix} 0 & 1 & 0 & 0 \\ 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{pmatrix} \quad \text{and} \quad \mathbf{B}_2 = \begin{pmatrix} 0 & 1 & 0 & 1 \\ 1 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 \\ 1 & 0 & 0 & 0 \end{pmatrix}.$$

It is easy to see that the matrices $\mathbf{B}_1, \mathbf{B}_2, \mathbf{B}_1 \oplus \mathbf{B}_2$ are invertible, what means that all the component functions of F are Boolean bent, and hence F is vectorial bent. On the other hand, one can construct the matrices $\mathbf{B}'_i$ as in (1.20) in the following way:

$$\mathbf{B}'_1 = \begin{pmatrix} 0 & 1 & 0 & 0 \\ 0 & 1 & 0 & 1 \end{pmatrix}, \mathbf{B}'_2 = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 1 & 0 & 1 & 0 \end{pmatrix}, \mathbf{B}'_3 = \begin{pmatrix} 0 & 0 & 0 & 1 \\ 0 & 1 & 0 & 0 \end{pmatrix}, \mathbf{B}'_4 = \begin{pmatrix} 0 & 0 & 1 & 0 \\ 1 & 0 & 0 & 0 \end{pmatrix}.$$

Clearly, all matrices $\mathbf{B}'_i$ have full rank. One may check that any nonzero matrix from the linear span $\langle \mathbf{B}'_1, \mathbf{B}'_2, \mathbf{B}'_3, \mathbf{B}'_4 \rangle$ has full rank as well, and hence all nontrivial first-order derivatives of F are balanced, and hence, F is vectorial bent.

Remark 1.32. Although the structure of quadratic vectorial bent functions is understood, similarly to the Boolean case, it is in general a difficult problem to construct these functions.

The Maiorana-McFarland class

The following generalization of quadratic Boolean bent functions was independently suggested by James A. Maiorana and Robert L. McFarland [78]. We identify $\mathbb{F}_2^n$ with $\mathbb{F}_2^k \times \mathbb{F}_2^k$ and consider Boolean functions $f_{\pi,\phi} \colon \mathbb{F}_{2^k} \times \mathbb{F}_{2^k} \to \mathbb{F}_2$ of the form

$$f_{\pi,\phi}(\mathbf{x}, \mathbf{y}) = \langle \mathbf{x}, \pi(\mathbf{y}) \rangle_k \oplus \phi(\mathbf{y}). \tag{1.22}$$

A Boolean function $f_{\pi,\phi}$ of the form (1.22) is bent if and only if the mapping π is a permutation of $\mathbb{F}_2^k$ (one can see it from the proof of Result 1.35 below). Any bent function $f_{\pi,\phi}$ on $\mathbb{F}_2^k \times \mathbb{F}_2^k$ is called a *Maiorana-McFarland* bent function and the set of all Maiorana-McFarland bent functions is called the *(original) Maiorana-McFarland class* and denoted by $\mathcal{M}$.

One of the central problems of research on Boolean bent functions is the construction of bent functions, which are provably outside the *completed Maiorana-McFarland class* $\mathcal{M}^\#$. The motivation behind this problem is the following:

- The truth table of a Maiorana-McFarland bent function on $\mathbb{F}_2^k \times \mathbb{F}_2^k$ is a concatenation of 2^k truth tables of affine functions on $\mathbb{F}_2^k$, since for any fixed $\mathbf{y}^* \in \mathbb{F}_2^k$ the mapping $\mathbf{x} \mapsto f_{\pi,\phi}(\mathbf{x}, \mathbf{y}^*)$ is affine on $\mathbb{F}_2^k$. This property is usually considered as undesirable from the cryptographic point of view, since it may be used for attacks on block ciphers [23].

- Besides the original Maiorana-McFarland class $\mathcal{M}$, there are a few general classes of Boolean bent functions: the Dillon's partial spread class $\mathcal{PS}$ and the $\mathcal{H}$ class [41], Carlet's $\mathcal{C}$ and $\mathcal{D}$ classes [26] as well as the Dobbertin's class $\mathcal{N}$ [48]; for extensive references on the subject we refer to the book of Mesnager [86]. In order to show that a Boolean bent function f on $\mathbb{F}_2^n$ is new in the broadest sense, one needs to show that f is EA-inequivalent to a member of the union of the aforementioned classes, which is a very difficult problem due to the different descriptions of these classes. The standard approach towards the understanding whether a given bent function f on $\mathbb{F}_2^n$ is new, is to consider a weaker statement, namely to prove that f is not a member of the completed version of one of the classes, particularly, the completed Maiorana-McFarland class $\mathcal{M}^\#$.

For the recent advances in construction and analysis of Boolean bent functions, which are provably outside the completed Maiorana-McFarland class, we refer to [116–118].

A further generalization of the Maiorana-McFarland construction may be obtained by considering the functions $f_{\pi,\phi}$ on $\mathbb{F}_2^n$, which is now identified with $\mathbb{F}_2^r \times \mathbb{F}_2^s$. The *generalized Maiorana-McFarland class* of Boolean functions $\mathcal{M}_{r,s}$ is defined in [27, p. 354] as the set of Boolean functions in $n = r + s$ variables, which have the following form

$$f_{\pi,\phi}(\mathbf{x},\mathbf{y}) = \langle \mathbf{x}, \pi(\mathbf{y}) \rangle_r \oplus \phi(\mathbf{y}), \tag{1.23}$$

where $\mathbf{x} \in \mathbb{F}_2^r$, $\mathbf{y} \in \mathbb{F}_2^s$, ϕ is an arbitrary Boolean function on $\mathbb{F}_2^s$ and $\pi\colon \mathbb{F}_2^s \to \mathbb{F}_2^r$ is some mapping. However, in this case it becomes more difficult to characterize the bentness of functions of the form (1.23), for the details we refer to [74, p. 173, Theorem 6.40] or [27, p. 326, Proposition 8.33]. For a given Boolean function f on $\mathbb{F}_2^n$, we define its *Maiorana-McFarland representation* to be a mapping $f_{\pi,\phi}$ on $\mathbb{F}_2^r \times \mathbb{F}_2^s$, given as in (1.23). Note that this representation is not unique in general.

Remark 1.33. Since any affine function on $\mathbb{F}_2^r$ can be decomposed as a concatenation of two affine functions on $\mathbb{F}_2^{r-1}$, we have that if f is a member of *the completed generalized Maiorana-McFarland class* $\mathcal{M}^{\#}_{r,s}$, then $f \in \mathcal{M}^{\#}_{r',s'}$ for all integers $r' < r$ as well. The converse, however, is not true in general.

This observation leads to the following EA-invariant under extended-affine equivalence, which measures the maximal possible number of variables of affine functions in a Maiorana-McFarland representation (1.23) of a Boolean function.

Definition 1.34. [115, p. 82] The *linearity index* $\operatorname{ind}(f)$ of a Boolean function $f\colon \mathbb{F}_2^n \to \mathbb{F}_2$ is the maximal possible r such that $f \in \mathcal{M}^{\#}_{r,s}$.

In general, it seems to be a difficult problem to give an upper bound on the linearity index of a given class of Boolean functions or even to construct an efficient algorithm for calculating or estimating this value [115, p. 70]. For the class of bent functions, an upper bound on the linearity index is known.

Result 1.35. *[24, Proposition 8.33] Let f be a Boolean bent function f on $\mathbb{F}_2^n$. Then* $\operatorname{ind}(f) \leq n/2$ *with equality if and only if* $f \in \mathcal{M}^{\#}$.

Proof. Let $f \in \mathcal{M}^{\#}_{r,s}$ be bent. Then the function f is EA-equivalent to a function $f_{\pi,\phi}$ of the form (1.23). Consider the Walsh transform of the function $f_{\pi,\phi}$, which for $\mathbf{a} \in \mathbb{F}_2^r$ and $\mathbf{b} \in \mathbb{F}_2^s$ is given by

$$\begin{aligned}
\hat{\chi}_{f_{\pi,\phi}}(\mathbf{a},\mathbf{b}) &= \sum_{\mathbf{x}\in\mathbb{F}_2^r}\sum_{\mathbf{y}\in\mathbb{F}_2^s}(-1)^{\langle \mathbf{x},\pi(\mathbf{y})\rangle_r \oplus \phi(\mathbf{y}) \oplus \langle \mathbf{x},\mathbf{a}\rangle_r \oplus \langle \mathbf{y},\mathbf{b}\rangle_s} \\
&= \sum_{\mathbf{y}\in\pi^{-1}(\mathbf{a})}\sum_{\mathbf{x}\in\mathbb{F}_2^r}(-1)^{\langle \mathbf{x},\pi(\mathbf{y})\rangle_r \oplus \phi(\mathbf{y}) \oplus \langle \mathbf{x},\mathbf{a}\rangle_r \oplus \langle \mathbf{y},\mathbf{b}\rangle_s} \\
&+ \sum_{\mathbf{y}\notin\pi^{-1}(\mathbf{a})}\sum_{\mathbf{x}\in\mathbb{F}_2^r}(-1)^{\langle \mathbf{x},\pi(\mathbf{y})\rangle_r \oplus \phi(\mathbf{y}) \oplus \langle \mathbf{x},\mathbf{a}\rangle_r \oplus \langle \mathbf{y},\mathbf{b}\rangle_s}.
\end{aligned} \tag{1.24}$$

Since for a fixed $\mathbf{y} \notin \pi^{-1}(\mathbf{a})$ the function $\mathbf{x} \mapsto \langle \mathbf{x}, \pi(\mathbf{y})\rangle_r \oplus \phi(\mathbf{y}) \oplus \langle \mathbf{x}, \mathbf{a}\rangle_r \oplus \langle \mathbf{y}, \mathbf{b}\rangle_s$ is affine, and hence balanced, the latter term in (1.24) is equal to zero. In this way, the Walsh transform of $f_{\pi,\phi}$ at $\mathbf{a} \in \mathbb{F}_2^r$ and $\mathbf{b} \in \mathbb{F}_2^s$ is equal to

$$\hat{\chi}_{f_{\pi,\phi}}(\mathbf{a}, \mathbf{b}) = 2^r \sum_{\mathbf{y} \in \pi^{-1}(\mathbf{a})} (-1)^{\phi(\mathbf{y}) \oplus \langle \mathbf{y}, \mathbf{b}\rangle_s} = \pm 2^{n/2}, \tag{1.25}$$

since $f_{\pi,\phi}$ is bent on $\mathbb{F}_2^n$. In this way, $r \le n/2$ and the equality is achieved if and only if $f \in \mathcal{M}^\#$. □

The linearity index of a Boolean function is yet another way to measure the distance between a given function f on $\mathbb{F}_2^n$ and the set of all affine functions. For any affine function l on $\mathbb{F}_2^n$, we have $\operatorname{ind}(l) = n$, and hence Boolean functions with a small linearity index are in some sense far away from being affine. So far, we are not aware of any construction methods of bent functions on $\mathbb{F}_2^n$ with a prescribed linearity index $r < n/2$. However, one can use the following proposition to show that a function f on $\mathbb{F}_2^n$ is (not) the member of the $\mathcal{M}^\#_{r,s}$ class for a fixed r.

Proposition 1.36. *Let f be a Boolean function on $\mathbb{F}_2^n$ with $n = r + s$. The following statements are equivalent.*

1. *The function f belongs to the $\mathcal{M}^\#_{r,s}$ class.*
2. *There exists a vector subspace $U \subseteq \mathbb{F}_2^n$ of dimension r such that the second-order derivatives $D_{\mathbf{a},\mathbf{b}}f$ vanish for all $\mathbf{a}, \mathbf{b} \in U$, that is, $D_{\mathbf{a},\mathbf{b}}f = 0$.*
3. *There exists a vector subspace $U \subseteq \mathbb{F}_2^n$ of dimension r such that the function f is affine on every coset of U.*

Proof. 1.⇒2. The proof of this claim follows the original proof of Dillon [41, p. 102] for the completed Maiorana-McFarland class $\mathcal{M}^\#$. Since $f \in \mathcal{M}^\#_{r,s}$, we have $f_{\pi,\phi}(\mathbf{x}, \mathbf{y}) := \langle \mathbf{x}, \pi(\mathbf{y})\rangle_r \oplus \phi(\mathbf{y}) = f(\mathbf{z}\mathbf{A} \oplus \mathbf{b}) \oplus l(\mathbf{z})$ for all $\mathbf{z} \in \mathbb{F}_2^n, \mathbf{x} \in \mathbb{F}_2^r$, $\mathbf{y} \in \mathbb{F}_2^s$, where $\mathbf{A}$ is an invertible $n \times n$-matrix, $\mathbf{b} \in \mathbb{F}_2^n$ and l is an affine function on $\mathbb{F}_2^n$. We observe that for any $\mathbf{a}', \mathbf{b}' \in U' = \{(\mathbf{u}, \mathbf{0}) \colon \mathbf{u} \in \mathbb{F}_2^r\}$ we have $D_{\mathbf{a}',\mathbf{b}'} f_{\pi,\phi} = 0$. In this way, for any $\mathbf{a}, \mathbf{b} \in U = U'A^{-1}$ we have $D_{\mathbf{a},\mathbf{b}}f = 0$.
2.⇒3. Let $U \subseteq \mathbb{F}_2^n$ be an r-dimensional vector subspace such that for all $\mathbf{a}, \mathbf{b} \in U$ we have $D_{\mathbf{a},\mathbf{b}}f(\mathbf{z}) = 0$ for all $\mathbf{z} \in \mathbb{F}_2^n$. Let $\bar{U}$ be a complement of U. Then any vector $\mathbf{z} \in \mathbb{F}_2^n$ can be uniquely represented as $\mathbf{z} = \mathbf{u} \oplus \bar{\mathbf{u}}$ for $\mathbf{u} \in U$ and $\bar{\mathbf{u}} \in \bar{U}$. For a fixed $\bar{\mathbf{u}} \in \bar{U}$, consider the mapping $f|_{U \oplus \bar{\mathbf{u}}} \colon \mathbf{u} \in U \mapsto f(\mathbf{u} \oplus \bar{\mathbf{u}})$. In this way, $D_{\mathbf{a},\mathbf{b}} f|_{U \oplus \bar{\mathbf{u}}}(\mathbf{u}) = 0$ for all $\mathbf{u} \in U$, and thus f is affine on every coset $U \oplus \bar{\mathbf{u}}$.
3.⇒1. Assume that f is affine on each coset of $U \in \mathbb{F}_2^n$. For the r-dimensional vector space U we construct an invertible matrix $\mathbf{A}_U$, which brings f to its Maiorana-McFarland representation (1.23), i.e., $f(\mathbf{z}\mathbf{A}_U) = \langle \mathbf{x}, \pi(\mathbf{y})\rangle_r \oplus \phi(\mathbf{y})$, with $\mathbf{z} \in \mathbb{F}_2^n$, $\mathbf{x} \in \mathbb{F}_2^r$ and $\mathbf{y} \in \mathbb{F}_2^s$, satisfying $\mathbf{z}\mathbf{A}_U = (\mathbf{x}, \mathbf{y})$ in the following way. Since the values of the function $f_{\pi,\phi}(\mathbf{x}, \mathbf{y}) = \langle \mathbf{x}, \pi(\mathbf{y})\rangle_r \oplus \phi(\mathbf{y})$ on the coset $\mathbb{F}_2^r \oplus \mathbf{y}$ for

$\mathbf{y} \in \mathbb{F}_2^s$ coincide with the values of f on the coset $U \oplus \bar{\mathbf{u}}$ for $\bar{\mathbf{u}} \in \bar{U}$, we can construct $\mathbf{A}_U$ using the change of basis formula

$$\mathbf{A}_U = \left(\begin{array}{c|c} \mathbf{O}_{r,s} & \mathbf{I}_r \\ \hline \mathbf{I}_s & \mathbf{O}_{s,r} \end{array} \right) \cdot \left(\begin{array}{c} \mathrm{GJB}(\bar{U}) \\ \hline \mathrm{GJB}(U) \end{array} \right). \tag{1.26}$$

In this way, $f \in \mathcal{M}^{\#}_{r,s}$ by definition of the completed generalized Maiorana-McFarland class $\mathcal{M}^{\#}_{r,s}$. □

In the following chapters, we will frequently use the $n/2$-dimensional vector subspaces U, which satisfy the condition of the second claim in Proposition 1.36, in order to show that certain cubic bent functions do not belong to the completed Maiorana-McFarland class $\mathcal{M}^{\#}$. For the sake of convenience, we will call them $\mathcal{M}$-subspaces and formally define them as follows.

Definition 1.37. We call a vector subspace U of $\mathbb{F}_2^n$ an $\mathcal{M}$*-subspace* of a Boolean function $f\colon \mathbb{F}_2^n \to \mathbb{F}_2$, if for all $\mathbf{a}, \mathbf{b} \in U$ the second-order derivatives $D_{\mathbf{a},\mathbf{b}}f$ are constant zero functions, i.e., $D_{\mathbf{a},\mathbf{b}}f = 0$. We denote by $\mathcal{MS}_r(f)$ the collection of all r-dimensional $\mathcal{M}$-subspaces of f and by $\mathcal{MS}(f)$ the collection

$$\mathcal{MS}(f) := \bigcup_{r=1}^{n} \mathcal{MS}_r(f).$$

In terms of $\mathcal{M}$-subspaces, the linearity index of f is given by

$$\mathrm{ind}(f) = \max_{U \in \mathcal{MS}(f)} \dim(U).$$

In general, a Boolean function may have many different r-dimensional $\mathcal{M}$-subspaces. Using the result of Kolomeec [64, Theorem 2], one can compute the upper bound on the number of $n/2$-dimensional $\mathcal{M}$-subspaces of a bent function f on $\mathbb{F}_2^n$ and also characterize those functions, which achieve this bound with equality.

Proposition 1.38. *Let f be a bent function on $\mathbb{F}_2^n$ and let $n = 2k$. The number of k-dimensional $\mathcal{M}$-subspaces of f is at most*

$$|\mathcal{MS}_k(f)| \leq \prod_{i=1}^{k} \left(2^i + 1\right), \tag{1.27}$$

with equality if and only if the function f is quadratic.

Proof. By [64, Theorem 2], the number of affine k-dimensional vector subspaces L of $\mathbb{F}_2^n$ such that a bent function f is affine on L is at most $2^k \prod_{i=1}^{k} \left(2^i + 1\right)$ with equality if and only if f is quadratic. Moreover, by [64, Lemma 6] the function f is affine on any coset of L. The statement now follows from Proposition 1.36 and the fact that any k-dimensional $\mathcal{M}$-subspace of f on $\mathbb{F}_2^n$ has 2^k different cosets. □

Now we describe a naive algorithm, which one can use to construct the collection $\mathcal{MS}_r(f)$ for a given function f on $\mathbb{F}_2^n$ and a fixed r. For a more efficient algorithm, we refer to [22, Algorithm 2].

Algorithm 1.1. Construct the collection $\mathcal{MS}_r(f)$ for a Boolean function f on $\mathbb{F}_2^n$

```
Require: A Boolean function $D_{\mathbf{a},\mathbf{b}}f : \mathbb{F}_2^n \to \mathbb{F}_2$ and $2 \le r \le n$.
Ensure: The collection $\mathcal{MS}_r(f)$.
Construct $\mathcal{MS}_2(f) := \{\langle \mathbf{a}, \mathbf{b} \rangle : \dim(U) = 2$ and $D_{\mathbf{a},\mathbf{b}}f = 0\}$.
for all subspaces $U \in \mathcal{MS}_2(f)$ do
    repeat
        Determine subspaces $\tilde{U} = \langle U, \tilde{\mathbf{u}} \rangle$ for all $\tilde{\mathbf{u}} \notin U$ such that for any
        two-dimensional vector subspace $\langle \mathbf{a}, \mathbf{b} \rangle \subseteq U$ second-order derivatives
        vanish, i.e., $D_{\mathbf{a},\mathbf{b}}f = 0$.
        Put $U \leftarrow \tilde{U}$ for the obtained subspaces $\tilde{U}$.
    until $\dim(U) = r$.
    Output subspaces $U$ of dimension $r$.
end for
```

Remark 1.39. Algorithm 1.1 can be used to compute the linearity index of a given function f in the following way: $\operatorname{ind}(f)$ is the biggest r, for which $\mathcal{MS}_r(f) \neq \varnothing$.

Example 1.40. Consider the following cubic bent function on $\mathbb{F}_2^6$, given by

$$\begin{aligned} f(\mathbf{z}) = & z_2 \oplus z_4 \oplus z_5 \oplus z_6 \oplus z_1z_2 \oplus z_1z_3 \oplus z_1z_4 \oplus z_2z_4 \oplus z_2z_5 \oplus z_2z_6 \oplus z_3z_4 \\ & \oplus z_3z_6 \oplus z_5z_6 \oplus z_1z_2z_3 \oplus z_1z_3z_5 \oplus z_1z_4z_5 \oplus z_1z_4z_6 \oplus z_2z_3z_4 \oplus z_3z_4z_6. \end{aligned}$$

With Algorithm 1.1, it is possible to check that $\mathcal{MS}_3(f)$ contains exactly five $\mathcal{M}$-subspaces. One of them is the $\mathcal{M}$-subspace U, which is generated by the following three row vectors, forming its Gauss-Jordan basis

$$U = \left\langle \begin{matrix} 1 & 0 & 1 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 \end{matrix} \right\rangle.$$

To verify that the vector subspace U is indeed an $\mathcal{M}$-subspace of the function f on $\mathbb{F}_2^6$, one can compute second-order derivatives $D_{\mathbf{a},\mathbf{b}}f$ corresponding to the different two-dimensional vector subspaces $\langle \mathbf{a}, \mathbf{b} \rangle$ of U and check that all of them are constant zero functions. We list them in the following form $\langle \mathbf{a}, \mathbf{b} \rangle \mapsto D_{\mathbf{a},\mathbf{b}}f$ below:

$$\left\langle \begin{matrix} 0 & 1 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 \end{matrix} \right\rangle \mapsto 0, \left\langle \begin{matrix} 1 & 0 & 1 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 \end{matrix} \right\rangle \mapsto 0, \left\langle \begin{matrix} 1 & 1 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 \end{matrix} \right\rangle \mapsto 0, \left\langle \begin{matrix} 1 & 0 & 1 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 & 1 & 0 \end{matrix} \right\rangle \mapsto 0,$$

$$\left\langle \begin{matrix} 1 & 0 & 1 & 0 & 1 & 1 \\ 0 & 1 & 0 & 0 & 1 & 0 \end{matrix} \right\rangle \mapsto 0, \left\langle \begin{matrix} 1 & 0 & 1 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 & 1 & 1 \end{matrix} \right\rangle \mapsto 0, \left\langle \begin{matrix} 1 & 0 & 1 & 0 & 1 & 1 \\ 0 & 1 & 0 & 0 & 1 & 1 \end{matrix} \right\rangle \mapsto 0.$$

In order to construct for a function f its Maiorana-McFarland representation $f_{\pi,\phi}(\mathbf{x}, \mathbf{y}) = \langle \mathbf{x}, \pi(\mathbf{y}) \rangle_r \oplus \phi(\mathbf{y})$, we need to compute the linear transformation

$\mathbf{A}_U$, whose computation given in (1.26) involves U and its complement $\bar{U}$. First, we compute the complement $\bar{U}$ of the vector space U, as described in the first paragraph of Subsection 1.1.1. Similarly to U, the vector space $\bar{U}$ is generated by the following three row vectors, forming its Gauss-Jordan basis

$$\bar{U} = \left\langle \begin{matrix} 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 \end{matrix} \right\rangle.$$

Now we construct the linear transformation $\mathbf{A}_U$, which brings f to its Maiorana-McFarland representation $f(\mathbf{z}\mathbf{A}_U) = f_{\pi,\phi}(\mathbf{x},\mathbf{y})$, where $\mathbf{z} \in \mathbb{F}_2^6$ and $\mathbf{x},\mathbf{y} \in \mathbb{F}_2^3$, using expression (1.26) as follows

$$\mathbf{A}_U = \begin{pmatrix} 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 \\ 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 \end{pmatrix} \cdot \left(\begin{array}{cccccc} 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 \\ \hline 1 & 0 & 1 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 \end{array}\right) = \begin{pmatrix} 1 & 0 & 1 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 \end{pmatrix}.$$

After the linear transformation of coordinates $\mathbf{z}\mathbf{A}_U = (\mathbf{x},\mathbf{y})$, we get the following Maiorana-McFarland representation of the function f:

$$\begin{aligned} f(\mathbf{z}\mathbf{A}_U) = f_{\pi,\phi}(\mathbf{x},\mathbf{y}) = & x_1(1 \oplus y_2 \oplus y_3 \oplus y_1y_3 \oplus y_2y_3) \oplus x_2(1 \oplus y_2 \oplus y_1y_2 \oplus y_3) \\ & \oplus x_3(1 \oplus y_1 \oplus y_1y_2 \oplus y_3) \oplus y_2 \oplus y_3 \oplus y_1y_2. \end{aligned}$$

In order to generalize the classical Maiorana-McFarland construction to the vectorial case, we endow $\mathbb{F}_2^{n/2}$ with the structure of the finite field $(\mathbb{F}_{2^{n/2}}, +, \cdot)$ and identify $\mathbb{F}_2^n$ with $\mathbb{F}_{2^{n/2}} \times \mathbb{F}_{2^{n/2}}$. The *strict Maiorana-McFarland class* $\mathcal{M}$ of vectorial bent functions is the set of (n,m)-bent functions F of the form

$$F(x,y) = L(x \cdot \pi(y)) + G(y),$$

where $L\colon \mathbb{F}_{2^{n/2}} \to \mathbb{F}_{2^m}$ is a linear or an affine function, $\pi\colon \mathbb{F}_{2^{n/2}} \to \mathbb{F}_{2^{n/2}}$ is a permutation, and $G\colon \mathbb{F}_{2^{n/2}} \to \mathbb{F}_{2^m}$ is an arbitrary $(n/2,m)$-function.

Remark 1.41. Similarly to the Boolean case, one can check with Algorithm 1.1 that a given (n,m)-bent function $F = (f_1(\mathbf{x}),\ldots,f_m(\mathbf{x}))^T$ is a member of the strict Maiorana-McFarland class or its completed version. The (n,m)-function F belongs to the completed Maiorana-McFarland class if and only if all coordinate functions $f_1,\ldots,f_m$ have a common $\mathcal{M}$-subspace $U \subset \mathbb{F}_2^n$ of dimension $n/2$.

The partial spread class

In order to introduce the partial spread construction of bent functions suggested by Dillon in his thesis [41], we first give the definition of a partial spread.

Definition 1.42. A *partial spread of order k* in $\mathbb{F}_2^n$ is a set of k vector subspaces $U_1,\ldots,U_k$ of $\mathbb{F}_2^n$ of dimension d each, such that $U_i \cap U_j = \{\mathbf{0}\}$ for all $i \neq j$.

The $\mathcal{PS}^+$ *class* of bent functions is the set of Boolean bent functions on $\mathbb{F}_2^n$ of the form

$$f(\mathbf{x}) = \mathbb{1}_D(\mathbf{x}), \text{ with } D = \bigcup_{i=1}^{k} U_i, \tag{1.28}$$

where $\{U_1, \ldots, U_k\}$ is a partial spread of order $k = 2^{n/2-1} + 1$ in $\mathbb{F}_2^n$ and the mapping $\mathbb{1}_D : \mathbb{F}_2^n \to \mathbb{F}_2$ is the *indicator function* of $D \subseteq \mathbb{F}_2^n$, i.e., $\mathbb{1}_D(\mathbf{x}) = 1$ for $\mathbf{x} \in D$ and $\mathbb{1}_D(\mathbf{x}) = 0$ for $\mathbf{x} \notin D$. The $\mathcal{PS}^-$ *class* of bent functions is the set of Boolean bent functions on $\mathbb{F}_2^n$ of the form

$$f(\mathbf{x}) = \mathbb{1}_D(\mathbf{x}), \text{ with } D = \bigcup_{i=1}^{k} (U_i \setminus \{\mathbf{0}\}), \tag{1.29}$$

where $\{U_1, \ldots, U_k\}$ is a partial spread of order $k = 2^{n/2-1}$ in $\mathbb{F}_2^n$. The union of these two classes is denoted by $\mathcal{PS} = \mathcal{PS}^+ \cup \mathcal{PS}^-$ and called the *partial spread class* of Boolean bent functions. The *Desarguesian partial spread* class $\mathcal{PS}_{ap} \subset \mathcal{PS}^-$ is the set of Boolean bent functions f on $\mathbb{F}_{2^{n/2}} \times \mathbb{F}_{2^{n/2}}$ of the form $f\colon (x, y) \in \mathbb{F}_{2^{n/2}} \times \mathbb{F}_{2^{n/2}} \mapsto h(x/y)$, where $x/y = 0$ if $y = 0$ for $x, y \in \mathbb{F}_{2^{n/2}}$ and $h\colon \mathbb{F}_{2^{n/2}} \to \mathbb{F}_2$ is a balanced Boolean function. Note that a bent function from the $\mathcal{PS}^+$ class is not necessarily equivalent to the complement of a bent function from $\mathcal{PS}^-$, as it was observed by Dillon, see [41, pp. 96-97]. The complement of a bent function from the $\mathcal{PS}_{ap} \subset \mathcal{PS}^-$ class is a member of the $\mathcal{PS}^+$ class.

Remark 1.43. In general, it is difficult to check whether a given bent function f on $\mathbb{F}_2^n$ belongs to the $\mathcal{PS}$ class due to the combinatorial nature of the partial spread construction. Up to our best knowledge, there are a few constructions of Boolean bent functions provably inside or outside the (completed) partial spread class $\mathcal{PS}$, which we give below.
1. Quadratic bent function $Q_n\colon (x_1, \ldots, x_n) \mapsto x_1x_2 \oplus x_3x_4 \oplus \cdots \oplus x_{n-1}x_n$ is a member of the $\mathcal{PS}^+$ class if $n = 4k$, as it was shown by Dillon [41, Theorems 4.1.1 and 6.3.12]. If $n \neq 4k$, then the quadratic bent function Q_n does not belong to the completed partial spread class $\mathcal{PS}^\#$.
2. Let the function f on $\mathbb{F}_2^m \times \mathbb{F}_2^m$ with $m \geq 5$ be defined as follows

$$f\colon (\mathbf{x}, \mathbf{y}) \in \mathbb{F}_2^m \times \mathbb{F}_2^m \mapsto \prod_{i=1}^{m} x_i \oplus \langle \mathbf{x} \oplus \mathbf{j}_m, \mathbf{y} \rangle_m.$$

Carlet [26] proved by contradiction that the function f does not belong to the completed partial spread class $\mathcal{PS}^\#$.

Remark 1.44. The property of a bent function to be a member of the partial spread class is not invariant under EA-equivalence. If f is a partial spread bent function on $\mathbb{F}_2^n$, then for an invertible $n \times n$-matrix $\mathbf{A}$, the function g on $\mathbb{F}_2^n$ given by $g\colon \mathbf{x} \mapsto f(\mathbf{xA})$ is also a partial spread bent function. However, translations of the input $\mathbf{x} \mapsto \mathbf{x} \oplus \mathbf{b}$ for $\mathbf{b} \in \mathbb{F}_2^n$ and additions of affine functions l on $\mathbb{F}_2^n$ to the output of a partial spread bent function f on $\mathbb{F}_2^n$ may lead to bent functions $g\colon \mathbf{x} \mapsto f(\mathbf{x} \oplus \mathbf{b})$ and $h\colon \mathbf{x} \mapsto f(\mathbf{x}) \oplus l(\mathbf{x})$ on $\mathbb{F}_2^n$, respectively, which do not belong to the partial spread class $\mathcal{PS}$, as we will show in Example 1.45.

In Algorithm 1.2, we describe how to check computationally the membership of a given bent function f on $\mathbb{F}_2^n$ in the $\mathcal{PS}$ class. Note that it is also possible to establish with Algorithm 1.2 whether a bent function f on $\mathbb{F}_2^n$ belongs to the completed partial spread class $\mathcal{PS}^\#$. If for a vector $\mathbf{b} \in \mathbb{F}_2^n$ and an affine function l on $\mathbb{F}_2^n$ the function $g\colon \mathbf{x} \mapsto f(\mathbf{x} \oplus \mathbf{b}) \oplus l(\mathbf{x})$ on $\mathbb{F}_2^n$ is a member of the $\mathcal{PS}$ class, we have $f \in \mathcal{PS}^\#$, otherwise $f \notin \mathcal{PS}^\#$.

Algorithm 1.2. Membership in the partial spread class $\mathcal{PS}$

```
Require: Bent function $f : \mathbb{F}_2^n \to \mathbb{F}_2$.
Ensure: True, if $f \in \mathcal{PS}$ and false, otherwise.
 1: if $f(\mathbf{0}) = 1$ then                                   ▷ The case $\mathcal{PS}^+$
 2:     Assign $k := 2^{n/2-1} + 1$ and $s(f) := \mathcal{D}_f$ (the support of $f$).
 3: else                                                         ▷ The case $\mathcal{PS}^-$
 4:     Assign $k := 2^{n/2-1}$    and $s(f) := \mathcal{D}_f \bigcup \{\mathbf{0}\}$.
 5: end if
 6: Construct the graph $G = (V, E)$, with $V = s(f)$ and the set of edges $E$ is
    determined by the incidence matrix $[f(\mathbf{x} \oplus \mathbf{y})]_{\mathbf{x},\mathbf{y} \in V}$.
 7: Find the set $S$ of cliques of the size $2^{n/2}$ in $G$.
 8: if $S = \varnothing$ then
 9:     Return false.
10: end if
11: Construct the set $V'$ of cliques in $S$, whose elements form a vector space of
    dimension $n/2$.
12: if $V' = \varnothing$ then
13:     Return false.
14: end if
15: Construct the graph $G' = (V', E')$, where the set of edges $E'$ is deter-
    mined by the incidence matrix $(a_{i,j})$, where $a_{i,j} = 1$, if for $U_i, U_j \in S$ holds
    $U_i \cap U_j = \{\mathbf{0}\}$, and 0 otherwise.
16: Return true, $f \in \mathcal{PS}$, if the graph $G'$ contains a clique of size $k$, and false
    otherwise.
```

Example 1.45. Consider the cubic bent function f on $\mathbb{F}_2^n$ with $n = 6$ from Example 1.40. With Algorithm 1.2, it is possible to show that $f \notin \mathcal{PS}$. Since $f(\mathbf{0}) = 0$, the function f can potentially belong only to $\mathcal{PS}^-$. However, this is not the case, since the graph G' defined in step 15 of Algorithm 1.2 does not contain a clique of size $4 = 2^{n/2-1}$. On the other hand, f belongs to the completed $\mathcal{PS}^-$ class, since for the vector $\mathbf{b} = (0,0,0,1,0,1) \in \mathbb{F}_2^6$ the function $g\colon \mathbf{x} \mapsto f(\mathbf{x} \oplus \mathbf{b})$ belongs to $\mathcal{PS}^-$. The function g can be written in the form

$g(\mathbf{x}) = \mathbb{1}_D(\mathbf{x})$, with $D = \bigcup_{i=1}^{4} (U_i \setminus \{\mathbf{0}\})$, where the elements U_i of the partial spread $\{U_1, U_2, U_3, U_4\}$ are given by

$$U_1 = \left\langle \begin{matrix} 1 & 0 & 0 & 1 & 1 & 1 \\ 0 & 1 & 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 & 1 & 0 \end{matrix} \right\rangle, U_2 = \left\langle \begin{matrix} 1 & 0 & 0 & 1 & 0 & 0 \\ 0 & 1 & 0 & 1 & 0 & 1 \\ 0 & 0 & 1 & 0 & 0 & 0 \end{matrix} \right\rangle,$$

$$U_3 = \left\langle \begin{matrix} 1 & 0 & 1 & 0 & 1 & 1 \\ 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 \end{matrix} \right\rangle, U_4 = \left\langle \begin{matrix} 0 & 1 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 \end{matrix} \right\rangle,$$

and can be can be obtained with Algorithm 1.2. Similarly, one can show that the function f belongs to the completed $\in \mathcal{PS}^+$ class, since the function h on $\mathbb{F}_2^6$ defined by $h\colon \mathbf{x} \mapsto f(\mathbf{x}) \oplus x_5 \oplus 1$ belongs to $\mathcal{PS}^+$. The function h can be written in the form $h(\mathbf{x}) = \mathbb{1}_D(\mathbf{x})$, with $D = \bigcup_{i=1}^{5} U_i$, where the elements U_i of the partial spread $\{U_1, U_2, U_3, U_4, U_5\}$ are obtained with Algorithm 1.2 and are given by

$$U_1 = \left\langle \begin{matrix} 1 & 0 & 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 & 1 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 \end{matrix} \right\rangle, U_2 = \left\langle \begin{matrix} 1 & 0 & 0 & 0 & 1 & 1 \\ 0 & 1 & 0 & 1 & 1 & 0 \\ 0 & 0 & 1 & 1 & 1 & 1 \end{matrix} \right\rangle, U_3 = \left\langle \begin{matrix} 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 1 & 0 & 1 & 1 \\ 0 & 0 & 0 & 1 & 0 & 1 \end{matrix} \right\rangle,$$

$$U_4 = \left\langle \begin{matrix} 1 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 & 1 & 1 \end{matrix} \right\rangle, U_5 = \left\langle \begin{matrix} 1 & 1 & 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 \end{matrix} \right\rangle.$$

Remark 1.46. Similarly to the maximum number of $\mathcal{M}$-subspaces of a Boolean bent function $f \in \mathcal{M}^\#$ on $\mathbb{F}_2^n$ (see Proposition 1.38), it is an interesting problem to establish an upper bound on the number of different representations (1.28) and (1.29) of a bent function f on $\mathbb{F}_2^n$ from the $\mathcal{PS}$ class and characterize the functions with the maximum number of such representations. Using a modification of Algorithm 1.2, it is possible to compute the maximum possible number of representations (1.28) for partial spread bent functions in 8 variables, which are known and were obtained by Langevin and Hou [69]. For instance, at the last step of Algorithm 1.2 it is enough to return all cliques (provided they exist) of size k. According to our computations for $n = 8$, the maximum number of different representations (1.28), which a partial spread bent function on $\mathbb{F}_2^8$ may have, equals to $1920 = 2^7 \cdot 3^1 \cdot 5^1$ and is attained by quadratic bent functions from the $\mathcal{PS}^+$ class.

Finally, we note that the $\mathcal{PS}_{ap}$ class of Boolean bent functions can be generalized to the vectorial case as follows. The *Desarguesian* $\mathcal{PS}_{ap}$ *class* of vectorial (n,m)-bent functions is the set of (n,m)-bent functions F of the form $F(x,y) := H\left(x \cdot y^{2^{n/2}-2}\right) = H(x/y)$, where $x/y = 0$ if $y = 0$ for $x, y \in \mathbb{F}_{2^{n/2}}$ and H is a balanced $(n/2, m)$-function (or, equivalently, permutation if $m = n/2$).

1.1.4 Cubic bent functions

Cubic Boolean bent functions, i.e., bent functions of algebraic degree three, attracted a lot of attention from researchers, partly because the small algebraic degree of these functions allows investigating them exhaustively, provided the number of variables is not too large.

All cubic bent functions in six and eight variables are well-understood:

- The classification of cubic bent functions in six variables was obtained by Rothaus [103], and the case of eight variables was resolved by Braeken [10, p. 102]. We list the representatives of the EA-equivalence classes in Table 1.1, since in the following chapters we will analyze their cryptographic properties, which are invariant under EA-equivalence.

Table 1.1. EA-inequivalent cubic bent functions up to 8 variables

1.1(a) EA-inequivalent cubic bent functions on $\mathbb{F}_2^6$

c_i^6	Algebraic normal form of c_i^6
c_1^6	$x_1x_4 \oplus x_2x_5 \oplus x_3x_6 \oplus x_1x_2x_3$
c_2^6	$x_1x_2 \oplus x_1x_4 \oplus x_2x_6 \oplus x_3x_5 \oplus x_4x_5 \oplus x_1x_2x_3 \oplus x_2x_4x_5$
c_3^6	$x_1x_4 \oplus x_2x_6 \oplus x_3x_4 \oplus x_3x_5 \oplus x_3x_6 \oplus x_4x_5 \oplus x_4x_6 \oplus x_1x_2x_3 \oplus x_2x_4x_5 \oplus x_3x_4x_6$

1.1(b) EA-inequivalent cubic bent functions on $\mathbb{F}_2^8$

c_i^8	Algebraic normal form of c_i^8	B_j
c_1^8	$x_1x_4 \oplus x_2x_5 \oplus x_3x_6 \oplus x_7x_8 \oplus x_1x_2x_3$	B_1
c_2^8	$x_1x_4 \oplus x_2x_6 \oplus x_3x_7 \oplus x_5x_8 \oplus x_1x_2x_3 \oplus x_2x_4x_5$	B_2
c_3^8	$x_1x_4 \oplus x_2x_6 \oplus x_3x_7 \oplus (x_1 \oplus x_5 \oplus x_7)x_8 \oplus x_1x_2x_3 \oplus x_2x_4x_5$	B_3
c_4^8	$x_1x_2 \oplus x_1x_4 \oplus x_2x_6 \oplus x_5x_7 \oplus (x_2 \oplus x_3 \oplus x_4 \oplus x_7)x_8 \oplus x_1x_2x_3 \oplus x_2x_4x_5 \oplus x_3x_4x_6$	B_6
c_5^8	$x_1x_4 \oplus x_2x_7 \oplus x_5x_6 \oplus x_3x_8 \oplus x_1x_2x_3 \oplus x_2x_4x_5 \oplus x_3x_4x_6$	B_7
c_6^8	$x_1x_4 \oplus x_2x_7 \oplus x_5x_6 \oplus (x_3 \oplus x_4 \oplus x_6)x_8 \oplus x_1x_2x_3 \oplus x_2x_4x_5 \oplus x_3x_4x_6$	B_4, B_5
c_7^8	$x_1x_2 \oplus x_1x_3 \oplus x_2x_5 \oplus x_4x_6 \oplus x_7x_8 \oplus x_1x_2x_7 \oplus x_3x_4x_7 \oplus x_5x_6x_7$	B_8
c_8^8	$x_1x_5 \oplus x_1x_6 \oplus x_2x_6 \oplus x_3x_7 \oplus x_4x_8 \oplus x_1x_2x_3 \oplus x_2x_4x_5 \oplus x_3x_4x_6 \oplus x_1x_4x_7$	B_9

In general, it is a difficult problem to find a set of invariants, which can distinguish all EA-inequivalent functions with a given property. From Table 1.2, one can see that all EA-equivalence classes of cubic bent functions in $n \leq 8$ variables can be distinguished by the order of the automorphism group.

Table 1.2. Orders of automorphism groups of EA-inequivalent cubic bent functions up to 8 variables

1.2(a) $n = 6$ variables

c_i^6	$\lvert \mathrm{Aut}(c_i^6)\rvert$
c_1^6	$2^{15} \cdot 3^1 \cdot 7^1$
c_2^6	$2^{13} \cdot 3^1 \cdot 5^1$
c_3^6	$2^{11} \cdot 3^1 \cdot 7^1$

1.2(b) $n = 8$ variables

c_i^8	$\lvert \mathrm{Aut}(c_i^8)\rvert$	c_i^8	$\lvert \mathrm{Aut}(c_i^8)\rvert$
c_1^8	$2^{24} \cdot 3^2 \cdot 7^1$	c_5^8	$2^{20} \cdot 3^1$
c_2^8	$2^{22} \cdot 3^1$	c_6^8	$2^{18} \cdot 3^1$
c_3^8	$2^{18} \cdot 3^2 \cdot 5^1$	c_7^8	$2^{17} \cdot 3^2 \cdot 7^1$
c_4^8	$2^{14} \cdot 3^2 \cdot 7^1$	c_8^8	$2^{17} \cdot 7^1$

- The enumeration of cubic bent functions up to 8 variables is also known. There are exactly $42{,}372{,}288 \cdot 2^7 \approx 2^{25.33}$ cubic bent functions in 6 variables, as it was shown by Preneel in his thesis [100, p. 258], and there are exactly $5{,}386{,}705{,}781{,}653{,}504 \cdot 2^9 \approx 2^{61.25}$ cubic bent functions in 8 variables. The latter result was obtained by Langevin and Leander [70].

- All cubic bent functions up to $n \leq 8$ variables belong to the completed Maiorana-McFarland class $\mathcal{M}^\#$. The case $n = 6$ was resolved by Dillon [40], while the case $n = 8$ was shown by Braeken [10, p. 103].

Remark 1.47. Leopardi [72, Theorem 6] observed that the Braeken's list of affine inequivalent cubic bent functions in 8 variables given in [10, p. 102] contains a computational mistake. He showed that the representatives B_4 and B_5 on $\mathbb{F}_2^8$ given by

$$\begin{aligned} B_4(\mathbf{x}) =& x_1x_2x_3 \oplus x_2x_4x_5 \oplus x_3x_4x_6 \oplus x_3x_5 \oplus x_2x_6 \oplus x_2x_5 \oplus x_1x_7 \oplus x_4x_8, \\ B_5(\mathbf{x}) =& x_1x_2x_3 \oplus x_2x_4x_5 \oplus x_3x_4x_6 \oplus x_3x_5 \oplus x_1x_3 \oplus x_1x_4 \oplus x_2x_7 \oplus x_6x_8, \end{aligned}$$

are in fact affine equivalent, since $B_5(L(\mathbf{x})) = B_4(\mathbf{x})$, where the invertible linear transformation L on $\mathbb{F}_2^8$ is given by $L(\mathbf{x}) = (x_5, x_4, x_2, x_3, x_6, x_1, x_8, x_7)$. In view of this fact, we revised the classification of cubic bent functions in 8 variables as described in [10, p. 102] using the implementation of Result 1.60 (which we explain later) in Magma [9]. In Table 1.1(b), we list our representatives of equivalence classes c_i^8 and point out to which representatives B_j of Braeken [10, p. 120] they are equivalent to. In this way, we get the following result.

Theorem 1.48. *There are 8 extended-affine equivalence classes of cubic Boolean bent functions on $\mathbb{F}_2^8$.*

Although cubic bent function are not far away from quadratic from the algebraic degree point of view, it seems elusive to classify or enumerate them completely as well as to provide a unifying construction approach. So far, the current research on cubic bent functions is mostly focused on the construction of these functions and investigation of their cryptographic properties, among which are the following:

- being outside the competed Maiorana-McFarland class $\mathcal{M}^{\#}$;
- having no affine derivatives.

The class of cubic Boolean bent functions remains the only class of bent functions (w.r.t. the algebraic degree) for which it is not known whether it can (not) be completely described by the Maiorana-McFarland construction. As we mentioned previously, all cubic bent functions in six and eight variables are the members of the completed Maiorana-McFarland class $\mathcal{M}^{\#}$. On the other hand, a couple of infinite families of cubic bent functions constructed with the use of finite fields [21, 49, 71, 85] are either proved to be members of $\mathcal{M}^{\#}$ or have not been studied so far. For instance, Canteaut-Charpin-Kyureghyan and Leander power functions [21, 71] are proved to be members of the $\mathcal{M}^{\#}$ class, while the Niho cubic bent function [49] as well as Mesnager's infinite family with multiple trace terms [85] have not been analyzed yet. At the same time, all quadratic Boolean bent functions on $\mathbb{F}_2^n$ belong to the $\mathcal{M}^{\#}$ class (see Result 1.24) and bent functions of algebraic degrees $d \geq 4$, which are outside $\mathcal{M}^{\#}$, exist on $\mathbb{F}_2^n$ for all $n \geq 8$, as it was shown by Dillon in [41]. His proof will be considered in more detail in Result 4.16. In this way, the question whether a cubic bent function on $\mathbb{F}_2^n$ can be outside the $\mathcal{M}^{\#}$ class whenever $n \geq 10$ still remains an open problem.

The property of having no affine derivatives is closely related to the notion of fast points, which were introduced in [51] motivated by applications in cryptanalysis. The point $\mathbf{a} \in \mathbb{F}_2^n$ is called a *fast point* of a function $f\colon \mathbb{F}_2^n \to \mathbb{F}_2$ if it satisfies $\deg(D_{\mathbf{a}}f) < \deg(f) - 1$ and a *slow point*, if $\deg(D_{\mathbf{a}}f) = \deg(f) - 1$. The *set of fast points* of a Boolean function f on $\mathbb{F}_2^n$, denoted by $\mathbb{FP}_f$, is a vector space and its dimension is bounded by $\dim(\mathbb{FP}_f) \leq n - \deg(f)$, as it was shown in [51]. A cubic function f on $\mathbb{F}_2^n$ has *no affine derivatives*, if $\dim(\mathbb{FP}_f) = 0$, i.e., all its nontrivial first-order derivatives are quadratic functions.

Cryptographic systems having component functions without fast points are more resistant to certain differential attacks, as it was shown in [50, 66]. The question about the existence of cubic bent functions without affine derivatives on $\mathbb{F}_2^n$ was firstly addressed by Hou [58]. Consequently, Canteaut and Charpin [20, Lemma 1] provided a positive answer by showing that such cubic bent functions exist for all even $n \geq 6$ with $n \neq 8$. Mandal, Gangopadhyay and Stănică [77] constructed two classes of cubic bent functions without affine derivatives inside $\mathcal{M}^{\#}$ and proved their mutual inequivalence. They also suggested to find such functions outside the $\mathcal{M}^{\#}$ class and evaluate their significance for cryptographic applications [77, Section 1.6].

In comparison to the Boolean case, the class of cubic vectorial bent functions seems to be a less understood object. There are no computational results about classification and enumeration of these functions in a small number of variables. The known theoretical constructions are mostly generalizations of the Boolean analogues. For extensive references on the subject, we refer to [86, Chapter 12].

1.2 Difference and relative difference sets

Here we provide two remarkable characterizations of Boolean and vectorial bent functions by means of difference sets and relative difference sets.

Definition 1.49. Let $(G,+)$ be a finite group of order v. A subset $D \subseteq G$ is called a (v,k,λ)*-difference set*, if $|D| = k$ and the list of differences $d - d'$ with $d, d' \in D$ contains every non-identity element of G exactly λ times.

The following fundamental connection between Boolean bent functions and difference sets was established by Dillon in his thesis.

Result 1.50. *[41, p. 74, Theorem 6.2.2] Let f be a Boolean function on $\mathbb{F}_2^n$. The following statements are equivalent.*

1. *The function f is bent.*
2. *The support $\mathcal{D}_f$ is a $\left(2^n, 2^{n-1} \pm 2^{n/2-1}, 2^{n-2} \pm 2^{n/2-1}\right)$-difference set in $\mathbb{F}_2^n$.*

There are various generalizations of classical difference sets. One of them is the notion of relative difference sets.

Definition 1.51. Let $(G,+)$ be a finite group of order $\mu \cdot \nu$ and N be a normal subgroup of order ν of G. A subset $R \subseteq G$ is called a *relative* (μ,ν,k,λ)*-difference set* relative to the *forbidden subgroup* N if $|R| = k$ and the list of differences $r - r'$ with $r, r' \in R$ contains all elements of $G \setminus N$ exactly λ times. Moreover, no nonzero element in N occurs in this list of differences.

Remark 1.52. Any relative $(\mu,1,k,\lambda)$-difference set is a (v,k,λ)-difference set with $v = \mu$.

The following connection between perfect nonlinear functions and relative difference sets was observed by Pott [97, Theorem 1] within a more general framework of perfect nonlinearity of functions on arbitrary finite groups.

Result 1.53. *[97, Theorem 1] Let n be even. The following statements are equivalent.*

1. *An (n,m)-function F is bent.*
2. *The graph $\mathcal{G}_F \subseteq \mathbb{F}_2^n \times \mathbb{F}_2^m$ is a relative $(2^n, 2^m, 2^n, 2^{n-m})$-difference set in $\mathbb{F}_2^n \times \mathbb{F}_2^m$ relative to the subgroup $N = \{(\mathbf{0}, \mathbf{y}) \colon \mathbf{y} \in \mathbb{F}_2^m\}$.*

1.2.1 Group rings

Now we introduce group rings, which serve as a powerful tool used to formally translate combinatorial properties of subsets of finite groups into the language of equations.

Definition 1.54. Let G be a finite multiplicatively written group with the identity element 1_G. The integral *group ring* $\mathbb{Z}[G]$ consists of formal sums $\sum_{g \in G} a_g g$, where $a_g \in \mathbb{Z}$. Addition of group ring elements is defined componentwise

$$\sum_{g \in G} a_g g + \sum_{g \in G} b_g g = \sum_{g \in G} (a_g + b_g) g$$

and the multiplication is a convolution

$$\sum_{g \in G} a_g g \sum_{g \in G} b_g g = \sum_{g \in G} (\sum_{h \in G} a_h b_{h^{-1} g}) g.$$

Here we identify a subset $S \subseteq G$ with the group ring element $\sum_{g \in S} g$. In order to proceed with the application of group rings to the characterizations of Boolean and vectorial functions in terms of group ring equations, one needs to associate a certain set with a given function. First, we identify a Boolean function f on $\mathbb{F}_2^n$ with its support $\mathcal{D}_f \subseteq \mathbb{F}_2^n$. Since the support $\mathcal{D}_f \subseteq \mathbb{F}_2^n$ of a Boolean bent function f on $\mathbb{F}_2^n$ is a $\left(2^n, 2^{n-1} \pm 2^{n/2-1}, 2^{n-2} \pm 2^{n/2-1}\right)$ difference set, the set $\mathcal{D}_f$ satisfies the following group ring equation

$$D_f^2 = \left(2^{n-1} \pm 2^{n/2-1}\right) \cdot 1_G + \left(2^{n-2} \pm 2^{n/2-1}\right) \cdot (G - 1_G)$$

with $G = \mathbb{F}_2^n$. In a similar manner, one can identify an (n, m)-function F with its graph $\mathcal{G}_F \subset G = \mathbb{F}_2^n \times \mathbb{F}_2^m$. Thus, (n, m)-bent functions, being $(2^n, 2^m, 2^n, 2^{n-m})$ relative difference sets in $G = \mathbb{F}_2^n \times \mathbb{F}_2^m$ relative to the forbidden subgroup $N = \{(\mathbf{0}, \mathbf{y}) \colon \mathbf{y} \in \mathbb{F}_2^m\}$, can be described by the following group ring equation,

$$\mathcal{G}_F^2 = 2^n \cdot 1_G + 2^{n-m} \cdot (G - N).$$

Similarly, Budaghyan and Pott [16, Theorem 5], characterized s-plateaued (n, n)-functions F using the group ring equations in the following way,

$$\mathcal{G}_F^3 = 2^{n+s} \cdot \mathcal{G}_F + (2^n - 2^s) \cdot G. \tag{1.30}$$

Graphs of APN functions F on $\mathbb{F}_2^n$ satisfy the following group ring equation [54]

$$\mathcal{G}_F^2 = 2^n \cdot 1_G + 2 \cdot S_F, \tag{1.31}$$

where S_F corresponds to a subset of $\mathbb{F}_2^n \times \mathbb{F}_2^n$, which is disjoint from the set $\{(\mathbf{0}, \mathbf{y}) : \mathbf{y} \in \mathbb{F}_2^n\}$. Note that if F is an AB function on $\mathbb{F}_2^n$, then $S_F = \mathcal{D}_f$ for some bent function f on $\mathbb{F}_2^{2n}$, see [25].

For background on group rings, we refer to [95, 96] and for further applications of the group ring equations to the study of perfect nonlinear functions we refer to [97, 98].

1.3 Linear codes

In the following chapters, we will investigate equivalence of Boolean and vectorial functions with the help of linear codes, therefore we give some necessary definitions from coding theory.

Definition 1.55. A *linear code $\mathcal{C}$ of length n* over $\mathbb{F}_2$ is a vector subspace $\mathcal{C} \subseteq \mathbb{F}_2^n$. The elements of a linear code $\mathcal{C} \subseteq \mathbb{F}_2^n$ are called *codewords* and said to have *length* n.

The number of nonzero coordinates of a codeword $\mathbf{c} \in \mathcal{C}$ is called the *weight* of $\mathbf{c}$ and is denoted by $\mathrm{wt}(\mathbf{c})$. We also denote by A_i the number of codewords of weight i in the code $\mathcal{C}$. For a linear code $\mathcal{C} \subseteq \mathbb{F}_2^n$ we call the polynomial $W_{\mathcal{C}}(z) := \sum_{i=0}^{n} A_i z^i$ the *weight enumerator* of $\mathcal{C}$. The *minimum distance* of a linear code is the minimum weight of its nonzero codewords. We also say that a linear code $\mathcal{C} \subseteq \mathbb{F}_2^n$ is an

- $[n,k]$*-linear* code, if $\mathcal{C}$ has dimension k;
- $[n,k,d]$*-linear* code, if $\mathcal{C}$ is an $[n,k]$-linear code, which has the minimum distance d.

The *dual* of an $[n,k]$-linear $\mathcal{C}$ code is the $[n,n-k]$-linear code $\mathcal{C}^{\perp}$ defined by

$$\mathcal{C}^{\perp} := \{\mathbf{u} \in \mathbb{F}_2^n \colon \mathbf{u} \cdot \mathbf{w} = u_1 w_1 \oplus \cdots \oplus u_n w_n = 0 \text{ for all } \mathbf{w} \in \mathcal{C}\}.$$

There are two ways to define an $[n,k]$-linear code: with the help of a generator matrix and a parity-check matrix. We say that a $k \times n$-matrix G is a *generator matrix* of an $[n,k]$-linear code $\mathcal{C}$, if the rows of G form a basis for $\mathcal{C}$. An $(n-k) \times n$-matrix H is called a *parity-check matrix* of an $[n,k]$-linear code $\mathcal{C}$, if every vector in $\mathcal{C}$ is orthogonal to the rows of the matrix H. It is easy to see that an $[n,k]$-linear code $\mathcal{C}$ is specified by a generator matrix G and a parity-check matrix H, if and only if the dual $[n,n-k]$-linear code $\mathcal{C}^{\perp}$ is specified by a generator matrix H and a parity-check matrix G.

Definition 1.56. Two linear codes $\mathcal{C}$ and $\mathcal{C}'$ are *permutation equivalent* provided there exists a permutation of coordinates which maps the code $\mathcal{C}$ to $\mathcal{C}'$.

In the following, we will omit the word "permutation" and simply say that two codes are equivalent. Clearly, two linear codes $\mathcal{C}$ and $\mathcal{C}'$ are equivalent if and only if the dual codes $\mathcal{C}^{\perp}$ and $\mathcal{C}'^{\perp}$ are equivalent. The *automorphism group* $\mathrm{Aut}(\mathcal{C})$ of a linear code $\mathcal{C}$ is the set of all permutations of coordinates, which fix the code $\mathcal{C}$.

Definition 1.57. Let G be a group, S be a set and let $\cdot \colon G \times S \to S$ be a group action. The *group action* is called:

- *free* if for given $g_1, g_2 \in G$ the existence of an element $s \in S$ satisfying $g_1 \cdot s = g_2 \cdot s$ implies $g_1 = g_2$;
- *t-transitive* if for any two ordered t-tuples $(x_1, \dots, x_t)$ and $(y_1, \dots, y_t)$ of pairwise distinct elements of S, there exists an element $g \in G$ such that for all $i \in \{1, \dots, t\}$ holds $g \cdot x_i = y_i$;
- *regular* if it is both free and 1-transitive.

We also say that a group is *free/ t-transitive/ regular* if it acts on the set S freely/ t-transitively/ regularly.

Definition 1.58. The *r-th order binary Reed-Muller code* $\mathcal{RM}(r,n)$ of length 2^n, for $0 \le r \le n$, is the set of truth tables of Boolean functions on $\mathbb{F}_2^n$ with algebraic degree at most r, i.e., $\mathcal{RM}(r,n) = \{\mathbf{f} \mid f \colon \mathbb{F}_2^n \to \mathbb{F}_2, \deg(f) \le r\}$.

Since the elements of the first-order Reed-Muller code $\mathcal{RM}(1,n)$ are the truth tables of all affine functions on $\mathbb{F}_2^n$, we have that $\mathcal{RM}(1,n)$ is a $[2^n, n+1, 2^{n-1}]$-linear code with the weight enumerator $W_{\mathcal{RM}(1,n)}(z) = 1 + (2^{n+1} - 2)z^{2^{n-1}} + z^{2^n}$. Moreover, its generator matrix G can be given by

$$G = \begin{pmatrix} 1 \\ \mathbf{x} \end{pmatrix}_{\mathbf{x} \in \mathbb{F}_2^n},$$

where $\mathbf{x} = (x_1, \dots, x_n)^T$ is a column vector.

Equivalence of functions and equivalence of linear codes

In the following, we interpret the equivalence of Boolean functions in terms of code equivalence, which can be easily verified with the help of computer algebra systems, e.g., Magma [9] or GAP [106], provided that the number of variables is not too large. For a given (n,m)-function F, we define the following generator matrices:

$$C_1(F) := \begin{pmatrix} 1 \\ \mathbf{x} \\ F(\mathbf{x}) \end{pmatrix}_{\mathbf{x} \in \mathbb{F}_2^n}, \qquad C_2(F) := \begin{pmatrix} 1 & 0 \\ \mathbf{x} & \mathbf{0} \\ F(\mathbf{x}) & \mathbf{y} \end{pmatrix}_{\substack{\mathbf{x} \in \mathbb{F}_2^n \\ \mathbf{y} \in \mathbb{F}_2^m \setminus \{\mathbf{0}\}}}, \tag{1.32}$$

where $\mathbf{x}, \mathbf{y}$ and $F(\mathbf{x})$ are column vectors.

Definition 1.59. We define a linear code $\mathcal{C}_i(F)$ of an (n,m)-function F as a linear code, whose generator matrix is the matrix $C_i(F)$ from (1.32). In this way, a linear code $\mathcal{C}_i^{\perp}(F)$ of an (n,m)-function F is a linear code, whose parity-check matrix is the matrix $C_i(F)$ from (1.32).

With the help of linear codes $\mathcal{C}_i(F)$ given in Definition 1.59, one can check various types of equivalence relations for (n,m)-functions F and F' due to the following result.

Result 1.60. *Let F and F' be two (n,m)-functions. The following hold.*

1. *Functions F and F' are CCZ-equivalent if and only if the linear codes $\mathcal{C}_1(F)$ and $\mathcal{C}_1(F')$ are equivalent.*

2. *Functions F and F' are EA-equivalent if and only if the linear codes $\mathcal{C}_2(F)$ and $\mathcal{C}_2(F')$ are equivalent.*

For the proof of the first claim, we refer to the work of Browning, Dillon, Kibler and McQuistan [12, Theorem 6.2] and for the proof of the second claim, we refer to the work of Edel and Pott [54, Theorems 10]. For the methods of checking affine equivalence with linear codes, we refer to [17, 54].

Remark 1.61. Since EA-equivalence and CCZ-equivalence coincide for (n,m)-bent functions (see Result 1.11), it is more convenient from the computational point of view to check equivalence of the codes $\mathcal{C}_1(F)$ and $\mathcal{C}_1(F')$ instead of $\mathcal{C}_2(F)$ and $\mathcal{C}_2(F')$ for (n,m)-bent functions F and F'. For this reason and due to the fact that further we will be concentrated only on EA-equivalence of (n,m)-bent functions, we denote throughout the thesis $\mathcal{C}_F := \mathcal{C}_1(F)$ for an (n,m)-function F.

Remark 1.62. The automorphism group $\mathrm{Aut}(F)$ of an (n,m)-bent function F (see Definition 1.4) and the automorphism group of the corresponding linear code $\mathrm{Aut}(\mathcal{C}_F)$ are isomorphic. Any automorphism of $\mathcal{C}_F$ corresponds to a permutation matrix $\mathbf{Q} \in \mathbb{F}_2^{(2^n,2^n)}$ such that $\mathbf{M} \cdot C_1(F) = C_1(F) \cdot \mathbf{Q}$ for an invertible matrix $\mathbf{M} \in \mathbb{F}_2^{(n+m+1,n+m+1)}$, which is uniquely determined by $\mathbf{Q}$, since all columns of $C_1(F)$ are distinct. Without loss of generality, the matrix $\mathbf{M}$ has the form

$$\mathbf{M} = \begin{pmatrix} 1 & \mathbf{0} & \mathbf{0} \\ \mathbf{a} & \mathbf{A}_{11} & \mathbf{A}_{12} \\ \mathbf{b} & \mathbf{A}_{21} & \mathbf{A}_{22} \end{pmatrix},$$

where $\mathbf{a} \in \mathbb{F}_2^n$, $\mathbf{b} \in \mathbb{F}_2^m$, $\mathbf{A}_{11} \in \mathbb{F}_2^{(n,n)}$, $\mathbf{A}_{12} \in \mathbb{F}_2^{(n,m)}$, $\mathbf{A}_{21} \in \mathbb{F}_2^{(m,n)}$ and $\mathbf{A}_{22} \in \mathbb{F}_2^{(m,m)}$. Then the affine function $\mathcal{L}(\mathbf{x},\mathbf{y}) := (\mathbf{A}_{11}\mathbf{x} \oplus \mathbf{A}_{12}F(\mathbf{x}) \oplus \mathbf{a}, \mathbf{A}_{21}\mathbf{x} \oplus \mathbf{A}_{22}F(\mathbf{x}) \oplus \mathbf{b})^T$ is a permutation on $\mathbb{F}_2^n \times \mathbb{F}_2^m$, which fixes the graph of F, i.e., $\mathcal{L}(\mathcal{G}_F) = \mathcal{G}_F$.

Characterization of perfect nonlinearity in terms of linear codes

In this subsection, we provide a characterization of (n,m)-bent functions and APN functions in terms of linear codes $\mathcal{C}_F$ and $\mathcal{C}_F^\perp$, which contain information about nonlinearity and differential properties of a given (n,m)-function F. First, we give a connection between the number of codewords of weight 4 in the linear code $\mathcal{C}_F^\perp$ of an (n,m)-function F and the fourth power moment of the Walsh transform.

Result 1.63. *[1, Theorem 2.5.] Let F be an (n, m)-function. Then the number of codewords of weight 4 in $\mathcal{C}_F^\perp$ is given by*

$$A_4 = \frac{1}{24}\left(\frac{1}{2^{n+m}}\left(\sum_{\mathbf{a}\in\mathbb{F}_2^n,\mathbf{b}\in\mathbb{F}_2^m}(\hat{\chi}_F(\mathbf{a},\mathbf{b}))^4\right) - 3\cdot 2^{2n} + 2^{n+1}\right). \tag{1.33}$$

Using this statement and definitions of linear codes $\mathcal{C}_F$ and $\mathcal{C}_F^\perp$, we derive the following characterizations of bent and APN functions.

Corollary 1.64. *Let $n = 2k$. The following statements are equivalent.*

1. *An (n, m)-function F is bent.*
2. *The linear code $\mathcal{C}_F$ is a $[2^n, n+m+1, 2^{n-1}-2^{k-1}]$-linear code with the weight enumerator*

$$\begin{aligned} W_{\mathcal{C}_F}(z) =& 1 + (2^m-1)\,2^n z^{2^{n-1}-2^{k-1}} + (2^{n+1}-2)z^{2^{n-1}} \\ &+ (2^m-1)\,2^n z^{2^{n-1}+2^{k-1}} + z^{2^n}. \end{aligned} \tag{1.34}$$

3. *The linear code $\mathcal{C}_F^\perp$ is a $[2^n, 2^n-n-m-1, 4]$-linear code with the number of weight 4 codewords given by*

$$A_4 = \frac{1}{3}\left(2^{3n-m-3} - 2^{2n-m-3} - 2^{2n-2} + 2^{n-2}\right), \tag{1.35}$$

which is the minimum possible value for an (n, m)-function F with n even and $m \le n/2$.

Proof. The claim *1.* ⇔ *2.* follows from the definition of nonlinearity and the fact that bent functions achieve the covering radius bound (1.4) with equality. The claim *1.* ⇔ *3.* follows from Result 1.63 and the fact a Boolean function f on $\mathbb{F}_2^n$ is bent if and only if the fourth power moment of the Walsh transform achieves the bound $\sum_{\mathbf{a}\in\mathbb{F}_2^n}(\hat{\chi}_F(\mathbf{a}))^4 \ge 2^{3n}$ with equality, see [87, Theorem 3]. □

Corollary 1.65. *An (n, n)-function F is APN if and only if $\mathcal{C}_F^\perp$ is a $[2^n, 2^n-2n-1, 6]$-linear code or, equivalently, if the number of weight 4 codewords in $\mathcal{C}_F^\perp$ is $A_4 = 0$.*

Proof. Follows from Result 1.63 and the fact an (n, n)-function F is APN if and only if the fourth power moment of the Walsh transform achieves the bound $\sum_{\mathbf{a}\in\mathbb{F}_2^n,\mathbf{b}\in\mathbb{F}_2^m\setminus\{\mathbf{0}\}}(\hat{\chi}_F(\mathbf{a},\mathbf{b}))^4 \ge (2^n-1)2^{3n+1}$ with equality, see [6, Corollary 1]. □

1.4 Incidence structures

In the following chapters, we will analyze equivalence of bent functions with the help of incidence structures arising from (relative) difference sets and linear codes.

Definition 1.66. An *incidence structure* is a triple $S = (\mathcal{P}, \mathcal{B}, \mathcal{R})$, where:

- $\mathcal{P}$ is the *point set* of S and its elements are called *points*;
- $\mathcal{B}$ is the *block set* of S and its elements are called *blocks*;
- $\mathcal{R} \subseteq \mathcal{P} \times \mathcal{B}$ is a binary relation, called an *incidence relation*.

If $(p, B) \in \mathcal{R}$, we say that point p and block B are *incident*.

Remark 1.67. In this thesis, we consider only incidence structures $S = (\mathcal{P}, \mathcal{B}, \mathcal{R})$ with the incidence relation $\mathcal{R}$ being set inclusion. For this reason, we omit $\mathcal{R}$ and simply write $S = (\mathcal{P}, \mathcal{B})$.

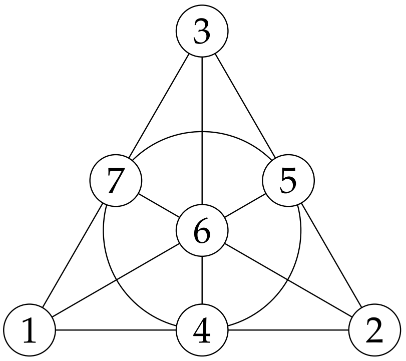
An *isomorphism* from incidence structure S onto S' is a bijection between point sets of S and S', which induces a bijection between their block sets. If such an isomorphism from S to S' exist, we call these incidence structures *isomorphic*. Any isomorphism of an incidence structure onto itself is called an *automorphism*. Clearly, the set of all automorphisms of an incidence structure S is a group, which is called the *automorphism group* of S and denoted by $\mathrm{Aut}(S)$.

All information about an incidence structure S is contained in its *incidence matrix* $\mathbf{M}(S) = (m_{i,j})$, which is a binary $b \times v$ matrix with $m_{ij} = 1$ if $p_j \in B_i$ and $m_{ij} = 0$ otherwise. In terms of incidence matrices, two incidence structures S and S' are isomorphic if there exist permutation matrices $\mathbf{P}$ and $\mathbf{Q}$ such that $\mathbf{P} \cdot \mathbf{M}(S) \cdot \mathbf{Q} = \mathbf{M}(S')$.

Example 1.68. Let $S = (\mathcal{P}, \mathcal{B})$ be the *Fano plane*, where $\mathcal{P} = \{1,2,3,4,5,6,7\}$ and $\mathcal{B} = \{\{1,2,4\},\{2,3,5\},\{3,4,6\},\{4,5,7\},\{5,6,1\},\{6,7,2\},\{7,1,3\}\}$. In Figure 1.1, we give a graphical representation of the Fano plane together with its incidence matrix.

Figure 1.1. Fano plane

(a) Blocks and points



(b) Incidence matrix

$$\begin{array}{cc} & \begin{matrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \end{matrix} \\ \begin{matrix} B_1 \\ B_2 \\ B_3 \\ B_4 \\ B_5 \\ B_6 \\ B_7 \end{matrix} & \begin{pmatrix} 1 & 1 & 0 & 1 & 0 & 0 & 0 \\ 0 & 1 & 1 & 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 1 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 & 1 & 0 & 1 \\ 1 & 0 & 0 & 0 & 1 & 1 & 0 \\ 0 & 1 & 0 & 0 & 0 & 1 & 1 \\ 1 & 0 & 1 & 0 & 0 & 0 & 1 \end{pmatrix} \end{array}$$

We will use invariants of incidence matrices in order to distinguish non-isomorphic incidence structures; among them are the Smith normal form and p-rank.

Definition 1.69. A diagonal matrix $\mathbf{D}$ with nonnegative entries $d_1, d_2, \ldots, d_n$ such that $d_1|d_2|\cdots|d_n$ is called the *Smith normal form* of an integral matrix $\mathbf{A}$ of order n, if there exist integral matrices $\mathbf{U}$ and $\mathbf{V}$ with $\det(\mathbf{U}), \det(\mathbf{V}) = \pm 1$ such that $\mathbf{UAV} = \mathbf{D}$. The diagonal entries d_i are called *elementary divisors* of $\mathbf{A}$. The *p-rank* of $\mathbf{A}$ is the rank of $\mathbf{A}$ over the field $\mathbb{F}_p$. The Smith normal form $\mathrm{SNF}(S)$ and the p-rank(S) of an incidence structure S are defined as the Smith normal form and the p-rank of its incidence matrix $\mathbf{M}(S)$, respectively.

Remark 1.70. *1.* The Smith normal form of a matrix is unique [38, Section 7.5]. It can be computed using elementary row and column operations. The p-rank of a matrix $\mathbf{A}$ is the number of elementary divisors coprime with p. The Smith normal form and the p-rank of an incidence structure S are unique as well. Let $\mathbf{M}_1$ and $\mathbf{M}_2$ be two different incidence matrices of S, i.e., there exist permutation matrices $\mathbf{P}$ and $\mathbf{Q}$ such that $\mathbf{M}_1 = \mathbf{P} \cdot \mathbf{M}_2 \cdot \mathbf{Q}$. Assume that the Smith normal form $\mathbf{D}$ of $\mathbf{M}_1$ is given by $\mathbf{U}\mathbf{M}_1\mathbf{V} = \mathbf{D}$, where $\mathbf{U}, \mathbf{V}$ are integral matrices with $\det(\mathbf{U}), \det(\mathbf{V}) = \pm 1$. Then the SNF of $\mathbf{M}_2$ is given by $\mathbf{U}'\mathbf{M}_2\mathbf{V}' = \mathbf{D}$, where $\mathbf{U}' = \mathbf{UP}$ and $\mathbf{V}' = \mathbf{QV}$ are integral matrices, satisfying $\det(\mathbf{U}'), \det(\mathbf{V}') = \pm 1$.
2. In the following chapters, we will be interested only in elementary divisors of the Smith normal form of incidence structures. For this reason, we define $\mathrm{SNF}(S)$ as the multiset $\mathrm{SNF}(S) = \{* d_1^{m_1}, \ldots, d_k^{m_k} *\}$, where consecutive elementary divisors d_i and d_{i+1} satisfy $d_i | d_{i+1}$, and m_i is the multiplicity of the elementary divisor d_i. For extensive references about the Smith normal form and p-ranks, we refer to [56, p. 494] and [38, Section 7.5].

Example 1.71. With the help of a computer algebra system, one can check that the Smith normal form of the Fano plane S considered in Example 1.68 is given by $\mathrm{SNF}(S) = \{*1^4, 2^2, 6^1*\}$. Since the number of elementary divisors coprime with 2 equals to 4, we have $2\text{-rank}(S) = 4$.

In the following, we define two important classes of incidence structures, namely t-designs and divisible designs, and give explicit constructions of these incidence structures with the help of (n, m)-bent functions.

Definition 1.72. An incidence structure $D = (\mathcal{P}, \mathcal{B})$ is called a *t-(v, k, λ) design*, if the cardinality of the point set $\mathcal{P}$ is v, the set of blocks $\mathcal{B}$ of cardinality $|B| = b$ is a collection of *k-subsets* of $\mathcal{P}$ and every t-subset of points is contained in exactly λ blocks of $\mathcal{B}$. A t-(v, k, λ) design D is called *symmetric*, if the number of points and blocks coincide.

Any t-(v, k, λ) design $D = (\mathcal{P}, \mathcal{B})$ with $|B| = b$ is a *regular* incidence structure, i.e., any point of D is contained in the same number of blocks r, which is called the *replication number* of D. The replication number r can be computed from the following relation between parameters of D, namely $bk = vr$. The parameter λ is called the *covalency*. For a t-(v, k, λ) design $D = (\mathcal{P}, \mathcal{B})$ with $|B| = b$, the following relations between parameters t, v, k, λ, b holds

$$\binom{v}{t}\lambda = \binom{k}{t}b. \tag{1.36}$$

We call a t-(v,k,λ) design $D = (\mathcal{P},\mathcal{B})$ *trivial*, if $B = \varnothing$ or $k < t$. In the case of 1-(v,k,λ) designs, the parameters r and λ coincide, for this reason we will call 1-designs regular incidence structures. If two 1-designs have the same replication number r, we will call them *equiregular*. We say that a t'-(v',k,λ') design $D' = (\mathcal{P}',\mathcal{B}')$ is a *subdesign* of a t-(v,k,λ) design $D = (\mathcal{P},\mathcal{B})$, if $\mathcal{P}' \subseteq \mathcal{P}$ and $\mathcal{B}' \subseteq \mathcal{B}$. Finally, if for a design $D = (\mathcal{P},\mathcal{B})$ there exist n subdesigns $D_i = (\mathcal{P},\mathcal{B}_i)$ such that $\mathcal{B} = \bigsqcup_{i=1}^{n}\mathcal{B}_i$, we say that that *$D$ is partitioned into subdesigns $D_1,\dots,D_n$* and write $D = \bigsqcup_{i=1}^{n} D_i$.

A divisible design is a generalization of a 2-(v,k,λ) design, which is based on the partitioning of the point set into point classes (i.e., equivalence classes of points) and requiring, that points in distinct classes are incident with the same number of blocks.

Definition 1.73. An incidence structure $D = (\mathcal{P},\mathcal{B})$ is called a *(μ,ν,k,λ)-divisible design*, if the point set $\mathcal{P}$ with $|\mathcal{P}| = v = \mu\cdot\nu$ elements is divided into μ *point classes* of size ν each, the block set $\mathcal{B}$ is a collection of k-subsets of $\mathcal{P}$ and the number of blocks containing any subset $\{p,q\} \subset \mathcal{P}$ depends on the relation between points p and q in the following way:

- If p and q are in the same point class, the subset $\{p,q\}$ is not contained in a block.
- Otherwise it is contained in exactly λ blocks.

For extensive references on incidence structures, we refer to [7, 8, 59] and for the results on p-ranks and Smith normal forms of 2-(v,k,λ) designs we refer to [114]. In the following subsections, we will survey some well-known constructions of incidence structures from Boolean and vectorial functions with the use of graphs, supports and linear codes. We also explain, how one may use these incidence structures to characterize perfect nonlinearity and distinguish inequivalent classes of functions.

1.4.1 Developments

We begin with a general construction approach of incidence structures from subsets of finite groups.

Definition 1.74. For a subset $A \subseteq G$ of a finite group $(G,+)$, the *development* $\mathrm{dev}(A)$ of A is an incidence structure, whose points are the elements in G, and whose blocks are the translates $A + g := \{a + g : a \in A\}$, where $g \in G$.

In order to distinguish Boolean and vectorial functions with the help of their supports and graphs, we introduce the equivalence relation for the subsets of finite groups in the following way.

Definition 1.75. We say that two subsets $A, A' \subseteq G$ of a finite group $(G, +)$ are *equivalent*, if there is a group automorphism $\phi\colon G \to G$ such that $\phi(A) = A + h$ for some $h \in G$, where $A + h = \{a + h\colon a \in A\}$.

Remark 1.76. If two subsets $A, A' \subseteq G$ are equivalent in the sense of Definition 1.75, then the developments $\operatorname{dev}(A)$ and $\operatorname{dev}(A')$ are isomorphic. In this way, since affine equivalence of Boolean functions f and f' of $\mathbb{F}_2^n$ is equivalence of their supports $\mathcal{D}_f$ and $\mathcal{D}_{f'}$, we have that for a Boolean function f on $\mathbb{F}_2^n$ the incidence structure $\operatorname{dev}(\mathcal{D}_f)$ is invariant under affine equivalence. Similarly, since CCZ-equivalence of (n, m)-functions F and F' is equivalence of their graphs $\mathcal{G}_F$ and $\mathcal{G}_{F'}$, we have that for an (n, m)-function F the incidence structure $\operatorname{dev}(\mathcal{G}_F)$ is invariant under CCZ-equivalence.

With the following fundamental result, one can always construct symmetric 2-designs and divisible designs as developments of difference sets and relative difference sets, respectively.

Result 1.77. 1. *A subset $D \subseteq G$ of a group G is a (v, k, λ)-difference set in G if and only if the incidence structure* $\operatorname{dev}(D)$ *is a symmetric* 2-(v, k, λ) *design with a regular automorphism group.*
2. *A subset $R \subseteq G$ of a group G is a relative (μ, ν, k, λ)-difference set in G relative to some normal subgroup N of G with $|N| = \nu$ if and only if the incidence structure* $\operatorname{dev}(R)$ *is a (μ, ν, k, λ)-divisible design with the automorphism group G, acting regularly on both the point and block sets of* $\operatorname{dev}(R)$.

For the proofs of the first and the second claims, we refer to the Lander's book [67, Chapter 4] and the article of Jungnickel [60, Theorem 2.7], respectively.

Example 1.78. The Fano plane $S = (\mathcal{P}, \mathcal{B})$, considered in Example 1.68, is a symmetric 2-$(7, 3, 1)$ design. First, we observe that the set $A = \{1, 2, 4\}$ is a $(7, 3, 1)$-difference set in group $(\mathbb{Z}_7, +)$, since any nonzero element of $\mathbb{Z}_7$ can be uniquely represented as a difference of two residues modulo 7. We also note that any block B_i has the form $B_i = A + i \mod 7$, thus $S = \operatorname{dev}(A)$. In this way, by Result 1.77, the Fano plane is a symmetric 2-$(7, 3, 1)$-design.

Applying Result 1.77 to supports of Boolean bent functions f on $\mathbb{F}_2^n$, which are $(2^n, 2^{n-1} \pm 2^{n/2-1}, 2^{n-2} \pm 2^{n/2-1})$-difference sets according to Result 1.50, we get the following design-theoretic characterization of Boolean bent functions.

Result 1.79. *Let f be a Boolean function on $\mathbb{F}_2^n$. The following statements are equivalent.*

1. *The function f is bent.*

2. *The incidence structure* $\mathrm{dev}(\mathcal{D}_f)$ *is a symmetric*
$$2\text{-}(2^n, 2^{n-1} \pm 2^{n/2-1}, 2^{n-2} \pm 2^{n/2-1}) \tag{1.37}$$
design.

In the same way, applying Result 1.77 to graphs of (n,m)-bent functions, which are $(2^n, 2^m, 2^n, 2^{n-m})$-relative difference sets according to Result 1.53, we obtain the following characterization of (n,m)-bent functions.

Result 1.80. *Let F be an (n,m)-function. The following statements are equivalent.*

1. *The function F is (n,m)-bent.*
2. *The incidence structure* $\mathrm{dev}(\mathcal{G}_F)$ *is a* $(2^n, 2^m, 2^n, 2^{n-m})$ *divisible design.*

Definition 1.81. Let f be a Boolean bent function on $\mathbb{F}_2^n$ and F be an (n,m)-bent function. We will call the designs $\mathrm{dev}(\mathcal{D}_f)$, $\mathrm{dev}(\mathcal{G}_f)$ and $\mathrm{dev}(\mathcal{G}_F)$ *translation designs* of bent functions f and F, since the blocks of these designs are the translates of difference and relative difference sets.

For extensive references on the incidence structures constructed from difference sets and relative difference sets, we refer to [7, 8, 60, 95, 96].

Geometric invariants of Boolean and vectorial functions. We will frequently use the following invariants of Boolean and vectorial functions, which arise from incidence structures $\mathrm{dev}(\mathcal{D}_f)$ and $\mathrm{dev}(\mathcal{G}_F)$ of Boolean functions f on $\mathbb{F}_2^n$ and (n,m)-functions F, respectively; throughout the thesis they will be referred to as *geometric invariants.*

Definition 1.82. Let f be a Boolean function on $\mathbb{F}_2^n$ and F be an (n,m)-function. We define the $\mathrm{rank}(f)$ as the 2-rank of $\mathbf{M}(\mathrm{dev}(\mathcal{D}_f))$. For an (n,m)-function F, we define the Γ-$\mathrm{rank}(F)$ as the 2-rank of $\mathbf{M}(\mathrm{dev}(\mathcal{G}_F))$ and $\mathrm{SNF}(F)$ as the Smith normal form of the incidence matrix $\mathbf{M}(\mathrm{dev}(\mathcal{G}_F))$, which is given by a multiset $\mathrm{SNF}(F) = \{* d_1^{m_1}, \dots, d_k^{m_k} *\}$, where $d_i | d_{i+1}$ and m_i is the multiplicity of d_i.

Remark 1.83. In view of Remark 1.76, we have that Γ-$\mathrm{rank}(F)$ and $\mathrm{SNF}(F)$ are invariant under CCZ-equivalence for all (n,m)-functions F, while $\mathrm{rank}(f)$ is invariant under EA-equivalence only for Boolean functions f on $\mathbb{F}_2^n$ with $\deg(f) \geq 2$, as it was shown in [110]. For the study of inequivalence of bent functions with the help of ranks, we refer to [110, 111], and for the applications of Γ-ranks to inequivalence of (n,m)-functions, we refer to [53, 54].

1.4.2 Supports of codewords of the fixed weight

Let $\mathcal{C}$ be a linear code of length v. The *support* of a codeword $\mathbf{c} = (c_1, \ldots, c_v) \in \mathcal{C}$ is the set of nonzero coordinate positions in $\mathbf{c}$, which is denoted by $\mathrm{suppt}(\mathbf{c})$ and formally defined as $\mathrm{suppt}(\mathbf{c}) = \{i : 1 \leq i \leq v \text{ and } c_i \neq 0\}$. For an integer w satisfying $A_w \neq 0$ in $W_{\mathcal{C}}(z)$, we define the collection of the supports of codewords of the fixed weight w as $\mathcal{B}_w(\mathcal{C}) := \{\mathrm{suppt}(\mathbf{c}) : \mathbf{c} \in \mathcal{C} \text{ and } \mathrm{wt}(\mathbf{c}) = w\}$. Finally, we denote by $\mathcal{P}(\mathcal{C}) := \{1, \ldots, v\}$ the set of all possible coordinate positions of the linear code $\mathcal{C}$ of length v.

Definition 1.84. An incidence structure $S = (\mathcal{P}(\mathcal{C}), \mathcal{B}_w(\mathcal{C}))$ is said to be *supported* by codewords of weight w in $\mathcal{C}$. If S is a t-(v,k,λ) design, we say that the codewords of weight w in $\mathcal{C}$ *hold* a t-(v,k,λ) design. If the codewords of the weight w hold t-designs for any $0 \leq w \leq v$, we say that the code $\mathcal{C}$ *supports t-designs.*

The constructed in such a way incidence structures may be used to distinguish inequivalent linear codes. If $\mathcal{C}$ and $\mathcal{C}'$ are two equivalent binary linear codes of length v, then there exists a permutation π on the set $\mathcal{P}(\mathcal{C})$ such that for any $\mathbf{c} \in \mathcal{C}$ we have $\pi(\mathbf{c}) \in \mathcal{C}'$. In this way, for any fixed weight w satisfying $1 \leq w \leq v$, the permutation π induces a permutation from $\mathcal{B}_w(\mathcal{C})$ to $\mathcal{B}_w(\mathcal{C}')$. This observation proves the following statement.

Proposition 1.85. *Let $\mathcal{C}$ and $\mathcal{C}'$ be two equivalent binary linear codes of length v. Then for any integer w satisfying $1 \leq w \leq v$ the incidence structures $S = (\mathcal{P}(\mathcal{C}), \mathcal{B}_w(\mathcal{C}))$ and $S' = (\mathcal{P}(\mathcal{C}'), \mathcal{B}_w(\mathcal{C}'))$ are isomorphic.*

In general, it is a nontrivial problem to construct t-designs. One of the standard ways to construct t-designs from linear codes is to consider the supports of the codewords of a fixed weight, and check whether either the automorphism group of the given code is t-transitive (see Definition 1.57), or the conditions of the original Assmus-Mattson theorem are fulfilled. Below we formulate these results for binary linear codes, since these are the only codes considered in this thesis, however, the original statements are valid for linear codes over $\mathbb{F}_q$ with q being a prime power.

Result 1.86 (Transitivity theorem). *[2]. Let $\mathcal{C}$ be a linear code of length v over $\mathbb{F}_2$ with a t-transitive automorphism group* $\mathrm{Aut}(\mathcal{C})$. *Then for any $w \geq t$ the incidence structures $(\mathcal{P}(\mathcal{C}), \mathcal{B}_w(\mathcal{C}))$ and $\left(\mathcal{P}\left(\mathcal{C}^{\perp}\right), \mathcal{B}_w\left(\mathcal{C}^{\perp}\right)\right)$ are t-designs.*

Result 1.87 (Original Assmus-Mattson Theorem). *[3] Let $\mathcal{C}$ be a linear code over $\mathbb{F}_2$ of length v and minimum distance d. Let $\mathcal{C}^{\perp}$ be the dual code of $\mathcal{C}$ and have minimum distance $d^{\perp}$. Let t with $1 \leq t < \min\left\{d, d^{\perp}\right\}$ be an integer such that there are at most $d^{\perp} - t$ weights of $\mathcal{C}$ in $\{1, 2, \ldots, v-t\}$. Then $(\mathcal{P}(\mathcal{C}), \mathcal{B}_w(\mathcal{C}))$ and $\left(\mathcal{P}\left(\mathcal{C}^{\perp}\right), \mathcal{B}_w\left(\mathcal{C}^{\perp}\right)\right)$ are t-designs for all $w \in \{0, 1, \ldots, v\}$.*

Remark 1.88. *1.* If a linear code $\mathcal{C}$ satisfies the conditions of Result 1.86 or Result 1.87, then by relation (1.36), the parameters of t-designs $(\mathcal{P}(\mathcal{C}), \mathcal{B}_w(\mathcal{C}))$ and $\left(\mathcal{P}\left(\mathcal{C}^\perp\right), \mathcal{B}_w\left(\mathcal{C}^\perp\right)\right)$ are t-$\left(v, w, A_w \cdot \binom{w}{t}/\binom{v}{t}\right)$ and t-$\left(v, w, B_w \cdot \binom{w}{t}/\binom{v}{t}\right)$, respectively, where A_w is the number of codewords of weight w of $\mathcal{C}$ and B_w is the number of codewords of weight w of $\mathcal{C}^\perp$.
2. If $w < t$ or there are no codewords of weight w in $\mathcal{C}$ or $\mathcal{C}^\perp$, then t-designs $(\mathcal{P}(\mathcal{C}), \mathcal{B}_w(\mathcal{C}))$ or $\left(\mathcal{P}\left(\mathcal{C}^\perp\right), \mathcal{B}_w\left(\mathcal{C}^\perp\right)\right)$, respectively, are trivial.

Example 1.89. *1.* Let $\mathcal{H}$ be the binary $[7,4,3]$-*Hamming code*, whose weight enumerator is given by $W_{\mathcal{H}}(z) = 1 + 7z^3 + 7z^4 + z^7$. The dual of $\mathcal{H}$ is the $[7,3,4]$-linear code $\mathcal{H}^\perp$, whose weight enumerator is given by $W_{\mathcal{H}^\perp}(z) = 1 + 7z^4$. With Magma [9], it is possible to check that automorphism groups of $\mathcal{H}$ and $\mathcal{H}^\perp$ are 2-transitive. In this way, by Result 1.86, for any weight $w \geq 2$ the codewords of weight w in linear codes $\mathcal{H}$ and $\mathcal{H}^\perp$ hold 2-designs with parameters 2-$(7, w, \lambda_w)$, where λ_w can be determined with relation (1.36). From the code $\mathcal{H}$, we have three nontrivial designs with parameters 2-$(7,3,1)$, 2-$(7,4,2)$ and 2-$(7,7,1)$, while from the code $\mathcal{H}^\perp$ we have only one nontrivial design with parameters 2-$(7,4,2)$.
2. Let $\mathcal{G}$ be the *extended binary* $[24,12,8]$-*Golay code*, whose weight enumerator is given by $W_{\mathcal{G}}(z) = 1 + 759z^8 + 2576z^{12} + 759z^{16} + z^{24}$. This code is self-dual, i.e., $\mathcal{G}^\perp = \mathcal{G}$. We show that codewords of weight w in $\mathcal{G}$ hold 5-designs using Result 1.87. Let $\mathcal{C} = \mathcal{G}$, then $v = 24$, $d = d^\perp = 8$. Set $t = 5$, which satisfies $1 \leq t < \min\left\{d, d^\perp\right\} = 8$. Then there are $3 < 8 - 2$ weights of $\mathcal{G}$ in the set $\{1, 2, \ldots, 22\}$ and thus incidence structures $(\mathcal{P}(\mathcal{C}), \mathcal{B}_w(\mathcal{C}))$ are 2-designs for all $w \in \{0, 1, \ldots, v\}$. The nontrivial 2-$(24, w, \lambda_w)$ designs $(\mathcal{P}(\mathcal{C}), \mathcal{B}_w(\mathcal{C}))$ have the following parameters: 5-$(24,8,1)$, 5-$(24,12,48)$, 5-$(24,16,78)$ and 5-$(24,24,1)$.

On the other hand, considering incidence matrices as generator matrices, one can construct linear codes from incidence structures in the following way.

Definition 1.90. The *linear code $\mathcal{C}(S)$ of an incidence structure $S = (\mathcal{P}, \mathcal{B})$* with $|\mathcal{P}| = v$ is the vector subspace of $\mathbb{F}_2^v$, which is spanned by the row vectors of the incidence matrix $\mathbf{M}(S)$.

Example 1.91. The Fano plane $S = (\mathcal{P}, \mathcal{B})$ considered in Example 1.78 is a 2-$(7,3,1)$ design. The incidence matrix $\mathbf{M}(S)$ from Example 1.78 is a generator matrix of the binary Hamming code $\mathcal{H}$ from Example 1.89. In this way, we have $\mathcal{H} = \mathcal{C}(S)$. Alternatively, since all 7 row vectors of the incidence matrix $\mathbf{M}(S)$ have weight 3, which is the minimum weight of $\mathcal{H}$, we have that codewords of the minimum weight of $\mathcal{H}$ hold the 2-$(7,3,1)$ design S.

Now we consider incidence structures supported by codewords of the minimum weight in the linear codes $\mathcal{C}_F$ and $\mathcal{C}_F^\perp$ of (n, m)-functions F, which reflect nonlinearity and differential properties of F, respectively.

Addition designs

First, we consider the incidence structures supported by codewords of the minimum weight in linear codes $\mathcal{C}_F$ of (n,m)-functions F.

Definition 1.92. For an (n,m)-function F, we define $\mathbb{D}(F) = (\mathcal{P},\mathcal{B})$ as the incidence structure, supported by codewords of the minimum weight in $\mathcal{C}_F$.

The incidence structures $\mathbb{D}(f)$ for Boolean bent functions f on $\mathbb{F}_2^n$ were considered by Dillon and Schatz [43] and by Bending in his thesis [5]. Remarkably, they showed that incidence structures $\mathbb{D}(f)$ of Boolean bent functions f on $\mathbb{F}_2^n$ are symmetric 2-designs with the *symmetric difference property*, i.e., the symmetric difference of any two blocks is either a block or the complement of a block. Moreover, they showed that EA-equivalence of Boolean bent functions f and f' on $\mathbb{F}_2^n$ and isomorphism of incidence structures $\mathbb{D}(f)$ and $\mathbb{D}(f')$, respectively, are the same concepts.

Result 1.93. *Let f and f' be Boolean functions on $\mathbb{F}_2^n$. The following statements are equivalent.*

1. *The function f is bent.*
2. *The incidence structure $\mathbb{D}(f)$ is a symmetric*

$$2\text{-}(2^n,2^{n-1}-2^{n/2-1},2^{n-2}-2^{n/2-1}) \tag{1.38}$$

design with the symmetric difference property.

Moreover, Boolean bent functions f and f' on $\mathbb{F}_2^n$ are EA-equivalent if and only if the designs $\mathbb{D}(f)$ and $\mathbb{D}(f')$ are isomorphic.

Proof. For the proofs of the claim *1.⇒2.* and the statement about equivalence of bent functions and isomorphism of designs, we refer to the paper of Dillon and Schatz [43] and Bending's thesis [5, Chapters 9, 10].
2.⇒1. Let $\mathbb{D}(f)$ be a symmetric 2-design with parameters (1.38). Since $\mathbb{D}(f)$ is supported by codewords of the minimum weight $2^{n-1}-2^{n/2-1}$ in $\mathcal{C}_f$, we have that 2^n blocks of $\mathbb{D}(f)$ have the form $f \oplus l$, where $l \in \mathcal{A}_n$, and thus $d_H(f,l) = 2^{n-1}-2^{n/2-1}$. Consequently, for the affine functions of the form $l \oplus 1$ we have $d_H(f,l\oplus 1) = 2^{n-1}+2^{n/2-1}$. In this way, the function f on $\mathbb{F}_2^n$ is at the distance $2^{n-1}-2^{n/2-1}$ from the set of all affine functions $\mathcal{A}_n$ and, hence, bent. □

The incidence structures $\mathbb{D}(F)$ arising from vectorial (n,m)-bent functions F were considered recently by Ding, Munemasa and Tonchev [44]. They generalized Result 1.93 by showing that incidence structures $\mathbb{D}(F)$ of vectorial (n,m)-bent functions F are 2-designs and, moreover, invariants under EA-equivalence. They also asked whether for (n,m)-bent functions F and F', similarly to the

Boolean case, isomorphism of 2-designs $\mathbb{D}(F)$ and $\mathbb{D}(F')$ defines EA-equivalence of functions F and F'. The positive answer on this question will be given in Chapter 3, Section 3.4.

Result 1.94. *Let F be an (n,m)-function. The following statements are equivalent.*

1. *The function F is (n,m)-bent.*
2. *The incidence structure $\mathbb{D}(F)$ is a*
$$2\text{-}(2^n, 2^{n-1}-2^{n/2-1}, (2^m-1)\cdot(2^{n-2}-2^{n/2-1})) \tag{1.39}$$
design.

Moreover, if (n,m)-bent functions F and F' are EA-equivalent, then the designs $\mathbb{D}(F)$ and $\mathbb{D}(F')$ are isomorphic.

Proof. 1.⇒2. Follows from the fact that the incidence structure $\mathbb{D}(F)$ is obtained by a disjoint union of incidence structures $\mathbb{D}(F_{\mathbf{b}})$ for $\mathbf{b} \in \mathbb{F}_2^m \setminus \{\mathbf{0}\}$, which are 2-$(2^n, 2^{n-1}-2^{n/2-1}, 2^{n-2}-2^{n/2-1})$ designs by Result 1.93, and do not have common blocks since F is (n,m)-bent.
2.⇒1. Let $\mathbb{D}(F)$ be a 2-design with parameters (1.39). We will show that $\mathcal{C}_F$ is a $[2^n, n+m+1, 2^{n-1}-2^{n/2-1}]$-linear code with the weight enumerator given by (1.34). From (1.36), we have that the number of blocks of $\mathbb{D}(F)$ is equal to $(2^m-1)\cdot 2^n$. Since any row of the incidence matrix $\mathbf{M}(\mathbb{D}(F))$ is described by the truth table of a function $F_{\mathbf{b}} \oplus l$ for $\mathbf{b} \in \mathbb{F}_2^m \setminus \{\mathbf{0}\}$ and $l \in \mathcal{RM}(1,n)$, we have that the linear code $\mathcal{C}_F$ contains exactly $(2^m-1)\cdot 2^n$ codewords of weight $2^{n-1}-2^{n/2-1}$. Clearly, the truth tables of the complements $F_{\mathbf{b}} \oplus l \oplus 1$ for $\mathbf{b} \in \mathbb{F}_2^m \setminus \{\mathbf{0}\}$ and $l \in \mathcal{RM}(1,n)$ also belong to the code $\mathcal{C}_F$, and hence there are $(2^m-1)\cdot 2^n$ codewords of weight $2^{n-1}+2^{n/2-1}$ in $\mathcal{C}_F$. Since $\mathcal{RM}(1,n) \subseteq \mathcal{C}_F$, the code $\mathcal{C}_F$ contains 2^n-2 codewords of weight 2^{n-1} as well as all-one-vector and all-zero-vector. In total, $\mathcal{C}_F$ contains $(2^m-1)2^{n+1}+2^{n+1} = 2^{n+m+1}$ codewords, which is the maximum number for a linear code $\mathcal{C}_F$ of an (n,m)-function F. In this way, $\mathcal{C}_F$ is a $[2^n, n+m+1, 2^{n-1}-2^{n/2-1}]$-linear code with the weight enumerator given by (1.34). By Corollary 1.64, the function F is (n,m)-bent.

Now we show that if (n,m)-bent functions F and F' are EA-equivalent, then the designs $\mathbb{D}(F)$ and $\mathbb{D}(F')$ are isomorphic. By definition of the addition design, we have that $\mathbb{D}(F) = (\mathcal{P}(\mathcal{C}_F), \mathcal{B}_w(\mathcal{C}_F))$ and $\mathbb{D}(F') = (\mathcal{P}(\mathcal{C}_{F'}), \mathcal{B}_w(\mathcal{C}_{F'}))$ for $w = 2^{n-1}-2^{n/2-1}$. By Result 1.11 and Result 1.60, we have that functions F and F' are EA-equivalent if and only if linear codes $\mathcal{C}_F$ and $\mathcal{C}_{F'}$ are equivalent. The statement now follows from Proposition 1.85, since for linear codes $\mathcal{C}_F$ and $\mathcal{C}_{F'}$ the incidence structures $(\mathcal{P}(\mathcal{C}_F), \mathcal{B}_w(\mathcal{C}_F))$ and $(\mathcal{P}(\mathcal{C}_{F'}), \mathcal{B}_w(\mathcal{C}_{F'}))$ are isomorphic for all $1 \leq w \leq 2^n$. □

Remark 1.95. We will call 2-designs $\mathbb{D}(F)$ of (n,m)-bent functions F *addition designs*, motivated by the terminology introduced by Bending in his thesis [5] for the designs $\mathbb{D}(f)$ of Boolean bent functions f on $\mathbb{F}_2^n$. The term "addition" has the following meaning. For an (n,m)-bent function F, any block of $\mathbb{D}(F)$ is formed by supports of Boolean bent functions, obtained via addition of the component functions $F_{\mathbf{b}}\colon \mathbb{F}_2^n \to \mathbb{F}_2$ to those affine functions $l\colon \mathbb{F}_2^n \to \mathbb{F}_2$, which satisfy $\mathrm{wt}(F_{\mathbf{b}} \oplus l) = 2^{n-1} - 2^{n/2-1}$.

Vanishing flats

In this subsection, we proceed with incidence structures supported by codewords of the minimum weight in the linear code $\mathcal{C}_F^\perp$ for (n,m)-functions F.

Recall that four distinct elements $\mathbf{x}_1, \mathbf{x}_2, \mathbf{x}_3, \mathbf{x}_4 \in \mathbb{F}_2^n$, which satisfy the condition $\mathbf{x}_1 \oplus \mathbf{x}_2 \oplus \mathbf{x}_3 \oplus \mathbf{x}_4 = \mathbf{0}$, form an affine two-dimensional subspace of $\mathbb{F}_2^n$, also called a flat. By definition of the linear code $\mathcal{C}_F^\perp$ of an (n,m)-function F (see Definition 1.59), a codeword $\mathbf{c} \in \mathcal{C}_F^\perp$ has weight 4 if and only if there exist 4 different elements $\mathbf{x}_1, \mathbf{x}_2, \mathbf{x}_3, \mathbf{x}_4 \in \mathbb{F}_2^n$ with $\mathbf{x}_1 \oplus \mathbf{x}_2 \oplus \mathbf{x}_3 \oplus \mathbf{x}_4 = \mathbf{0}$ such that $F(\mathbf{x}_1) \oplus F(\mathbf{x}_2) \oplus F(\mathbf{x}_3) \oplus F(\mathbf{x}_4) = \mathbf{0}$. In this way, for an (n,m)-function F, supports of the codewords of the weight 4 in $\mathcal{C}_F^\perp$, are in 1-to-1 correspondence with the elements of the set

$$\mathcal{VF}_F = \left\{ \{\mathbf{x}_1, \mathbf{x}_2, \mathbf{x}_3, \mathbf{x}_4\} \colon \bigoplus_{i=1}^{4} \begin{pmatrix} \mathbf{x}_i \\ F(\mathbf{x}_i) \end{pmatrix} = \begin{pmatrix} \mathbf{0} \\ \mathbf{0} \end{pmatrix} \text{ for } \mathbf{x}_i \in \mathbb{F}_2^n \right\}, \tag{1.40}$$

which is called the set of *vanishing flats* in $\mathbb{F}_2^n$ with respect to a function F. Motivated by the fact that many inequivalent (n,m)-functions F may have the same number of vanishing flats, or equivalently the number of weight 4 vectors in the code $\mathcal{C}_F^\perp$ (see Result 1.35), Li et al. [73] introduced an incidence structure, called vanishing flats, aimed to provide a more detailed combinatorial information about the function, than just the number of vanishing flats.

Definition 1.96. For an (n,m)-function F, the incidence structure $\mathcal{VF}(F)$ defined as $\mathcal{VF}(F) = (\mathbb{F}_2^n, \mathcal{VF}_F)$ is called *vanishing flats* of F.

Remark 1.97. In the original paper [73], the incidence structure $\mathcal{VF}(F)$ was introduced for (n,n)-functions F, however, we define it for a more general class of (n,m)-functions.

By Result 1.60 and Proposition 1.85, the incidence structure $\mathcal{VF}(F)$ of an (n,m)-function F is invariant under CCZ-equivalence. For a combinatorial proof of this fact, we refer to [73, Theorem II.1].

Corollary 1.98. *Let F and F' be two CCZ-equivalent (n,m)-functions. Then $\mathcal{VF}(F)$ and $\mathcal{VF}(F')$ are isomorphic. Consequently, the cardinalities of the block sets of $\mathcal{VF}(F)$ and $\mathcal{VF}(F')$ are the same, i.e., $|\mathcal{VF}_F| = |\mathcal{VF}_{F'}|$.*

In this way, the vanishing flats may be used to distinguish inequivalent (n,m)-functions and even classes of (n,m)-functions. On the other hand, the combinatorial structure of the vanishing flats may be used to characterize certain classes of (n,m)-functions.

Result 1.99. *Let F be an (n,n)-function and $\mathcal{VF}(F) = (\mathbb{F}_2^n, \mathcal{VF}_F)$ be the vanishing flats of F. The following hold.*

1. *The function F is APN if and only if $\mathcal{VF}_F = \varnothing$.*
2. *The function F is differentially 2-valued, that is, $\Delta_F = \{0, 2^s\}$ for some $s \in \mathbb{N}$ if and only if $\mathcal{VF}(F)$ is a 2-$(2^n, 4, 2^{s-1} - 1)$ design.*

Proof. The first claim is a reformulation of the well-known characterization of APN functions, given in [57]: an (n,n)-function $F\colon \mathbb{F}_2^n \to \mathbb{F}_2^n$ is APN if and only if F is not affine on any 2-dimensional affine subspace of $\mathbb{F}_2^n$. For the proof of the second claim, we refer to [108, Theorem 6.1]. □

A similar characterization of (n,m)-bent functions F in terms of the vanishing flats $\mathcal{VF}(F)$ will be considered in Chapter 3. For extensive references on the connections between designs and linear codes, we refer to [2, 18, 45, 46, 75].

Chapter 2

Vectorial bent functions in six variables

In this chapter, we classify and enumerate vectorial bent functions in six variables. In this way, we complete the classification of perfect nonlinear functions in six variables of algebraic degree at most three and the enumeration of bent functions in six variables. We also show that in contrast to Boolean bent functions, vectorial bent functions in six variables can not be described, up to equivalence, by Maiorana-McFarland and Desarguesian partial spread constructions.

This chapter is based on the paper by Polujan and Pott [94].

2.1 Introduction

In general, it seems elusive to classify and enumerate all perfect nonlinear functions completely. Nevertheless, these problems could be solved with the help of computer search provided the number of variables is small enough. For instance, up to five variables classification and enumeration of perfect nonlinear functions are known: for the discussion on Boolean and vectorial bent functions we refer to Subsection 1.1.3, and for the case of APN functions, we refer to the work of Brinkmann and Leander [11]. However, these problems become very challenging in dimension six due to significantly larger search space. Therefore, one may expect to obtain only partial results within certain subclasses of perfect nonlinear functions, e.g., bent functions or perfect nonlinear functions of algebraic degree at most three.

2.1.1 Known classification results on perfect nonlinear functions in six variables

In this subsection, we summarize the known computational results on the classification and enumeration of perfect nonlinear functions in six variables.

The classification and enumeration of all Boolean bent functions in six variables are well known and have been summarized in Subsection 1.1.3 in the context of classification and enumeration of cubic bent functions. So far, the enumeration of APN functions of algebraic degree at most three did not attract much attention to the best of our knowledge, while the classification problem (up to CCZ-equivalence) was solved as follows. First, Dillon, Browning and McQuistan showed that there are 13 equivalence classes of quadratic APN functions, as it was reported in [42]. Later on, Brinkmann and Leander [11] confirmed their results and also provided a new equivalence class of APN functions, which was later proven to be nonquadratic (cubic, to be more precise) by Edel and Pott [52]. In this way, the number of known CCZ-equivalence classes of APN functions of algebraic degree at most three in six variables is at least 14. Finally, Langevin [68] showed that the obtained list of 14 equivalence classes is complete up to CCZ-equivalence and, consequently, any new, up to CCZ-equivalence, APN function must have the algebraic degree at least four.

We summarize the representatives of the obtained CCZ-equivalence classes in Table 2.1. We endow $\mathbb{F}_2^6$ with the structure of the finite field $(\mathbb{F}_{2^6}, +, \cdot)$ in such a way that the multiplicative group $\mathbb{F}_{2^6}^*$ is given by $\mathbb{F}_{2^6}^* = \langle a \rangle$ and the minimal polynomial of α over $\mathbb{F}_2$ is $p(x) = x^6 + x^4 + x^3 + x + 1$. We denote by D_i quadratic APN functions from the Banff list [42], and by EP the Edel-Pott's cubic APN function from [52].

Table 2.1. Representatives of CCZ-equivalence classes of APN functions in six variables of algebraic degree at most three

f	Univariate representation of f
D_1	x^3
D_2	$x^3 + \alpha^{11}x^6 + \alpha x^9$
D_3	$\alpha x^5 + x^9 + \alpha^4 x^{17} + \alpha x^{18} + \alpha^4 x^{20} + \alpha x^{24} + \alpha^4 x^{34} + \alpha x^{40}$
D_4	$\alpha^7 x^3 + x^5 + \alpha^3 x^9 + \alpha^4 x^{10} + x^{17} + \alpha^6 x^{18}$
D_5	$x^3 + \alpha x^{24} + x^{10}$
D_6	$x^3 + \alpha^{17}(x^{17} + x^{18} + x^{20} + x^{24})$
D_7	$x^3 + \alpha^{11}x^5 + \alpha^{13}x^9 + x^{17} + \alpha^{11}x^{33} + x^{48}$
D_8	$\alpha^{25}x^5 + x^9 + \alpha^{38}x^{12} + \alpha^{25}x^{18} + \alpha^{25}x^{36}$
D_9	$\alpha^{40}x^5 + \alpha^{10}x^6 + \alpha^{62}x^{20} + \alpha^{35}x^{33} + \alpha^{15}x^{34} + \alpha^{29}x^{48}$
D_{10}	$\alpha^{34}x^6 + \alpha^{52}x^9 + \alpha^{48}x^{12} + \alpha^6 x^{20} + \alpha^9 x^{33} + \alpha^{23}x^{34} + \alpha^{25}x^{40}$
D_{11}	$x^9 + \alpha^4(x^{10} + x^{18}) + \alpha^9(x^{12} + x^{20} + x^{40})$
D_{12}	$\alpha^{52}x^3 + \alpha^{47}x^5 + \alpha x^6 + \alpha^9 x^9 + \alpha^{44}x^{12} + \alpha^{47}x^{33} + \alpha^{10}x^{34} + \alpha^{33}x^{40}$
D_{13}	$\alpha(x^6 + x^{10} + x^{24} + x^{33}) + x^9 + \alpha^4 x^{17}$
EP	$x^3 + a^{17}(x^{17} + x^{18} + x^{20} + x^{24}) + a^{14}(a^{18}x^9 + a^{36}x^{18} + a^9 x^{36} + x^{21} + x^{42}$ $+ \mathrm{Tr}(a^{27}x + a^{52}x^3 + a^6 x^5 + a^{19}x^7 + a^{28}x^{11} + a^2 x^{13}))$

2.1.2 Objectives

Summarizing the discussion above, perfect nonlinear $(6,m)$-functions with algebraic degree at most three are completely classified for $m \in \{1,6\}$. At the same time, to the best of our knowledge, the classification problem for vectorial bent functions still remains unsolved. Moreover, among the class of $(6,m)$-bent functions, vectorial bent functions are the only bent functions, for which the enumeration is not known. In this way, the main aim of this chapter is to classify and enumerate vectorial bent functions in six variables.

The rest of the chapter is organized in the following way. In Section 2.2, we introduce a series of invariants under equivalence for bent functions and explain how one can use them in order to enumerate vectorial bent functions. In Section 2.3, we describe a recursive algorithm, which we consequently use to obtain the main result of the chapter, namely the classification and enumeration of vectorial bent functions in six variables. In Section 2.4, we analyze, which of the obtained equivalence classes can be described by Maiorana-McFarland and Desarguesian partial spread constructions. In Section 2.5, we conclude the chapter and raise some open problems on the extendability of Boolean and vectorial bent functions.

2.2 Extension invariants of bent functions

In this chapter, we call EA-equivalent (n,m)-bent functions simply equivalent, since EA-equivalence is the most general equivalence relation for (n,m)-bent functions in view of Result 1.11. Recall that $\mathcal{B}_{n,m}$ denotes the set of all (n,m)-bent functions and $\mathcal{A}_{n,m}$ denotes the *set of* (n,m)*-affine functions*. In the following, we denote by $\mathcal{AB}_{n,m}$ the *set of affine-free* (n,m)*-bent functions* , i.e., any function $F \in \mathcal{AB}_{n,m}$ contains no affine terms in its ANF. For the sake of convenience, we denote by C_i^m an i-th EA-equivalence class of (n,m)-bent functions. On the set $\bigcup_{m=1}^{n/2} \mathcal{B}_{n,m}$ we introduce the order relation "$\prec$" in the following way. Let $m < l$ and C_i^m and C_j^l be two equivalence classes of (n,m)- and (n,l)-bent functions, respectively. We say that a function $F \in C_i^m$ *is contained* in $G \in C_j^l$ and write $F \prec G$, if the first m coordinate functions of $G(\mathbf{x}) = (g_1(\mathbf{x}),\dots,g_l(\mathbf{x}))^T$ form the function F, that is, $F(\mathbf{x}) = (g_1(\mathbf{x}),\dots,g_m(\mathbf{x}))^T$. Similarly, we say that $F \in C_i^m$ *is contained* in the equivalence class C_j^l and write $F \prec C_j^l$, if there exist a representative $G \in C_j^l$ such that $F \prec G$. Finally, we say that the equivalence class C_i^m *is contained* in C_j^l and denote it by $C_i^m \prec C_j^l$, if there exist $F \in C_i^m$ such that $F \prec C_j^l$.

Definition 2.1. An (n,m)-bent function F is called *extendable*, if the there exists a Boolean bent function $f\colon \mathbb{F}_2^n \to \mathbb{F}_2$ such that the $(n,m+1)$-function G defined by $G\colon \mathbf{x} \in \mathbb{F}_2^n \mapsto (F(\mathbf{x}), f(\mathbf{x}))^T$ is $(n,m+1)$-bent. If no such a bent function f exists, the function F is called *non-extendable*.

Remark 2.2. The problem of the existence of non-extendable bent functions $F\colon \mathbb{F}_p^n \to \mathbb{F}_p^m$ has mostly been studied for the case p odd, see [91, Section 4]. The particular case of this problem, namely $p = 2$ and $m = 1$, is closely related to the Tokareva's conjecture, also known as the *bent sum decomposition problem*, which is formulated in the following way. Any Boolean function on $\mathbb{F}_2^n$ of degree at most $n/2$ can be represented as the sum of two Boolean bent functions on $\mathbb{F}_2^n$, see [109, Hypothesis 1]. Note that a single example of a non-extendable Boolean bent function would disprove the Tokareva's conjecture. If a bent function f on $\mathbb{F}_2^n$ is non-extendable, then there exists no bent function f' on $\mathbb{F}_2^n$ such that $(f, f')^T$ is a vectorial bent function. Equivalently, the function f can not be written as a sum of two bent functions f' and $f \oplus f'$ on $\mathbb{F}_2^n$.

Definition 2.3. Let F be an (n, m)-bent function. We define the following two sets

$$\begin{aligned} \mathcal{F}(F) :=& \{f \in \mathcal{AB}_{n,1}\colon (F, f)^T \text{ is } (n, m+1)\text{-bent}\} \text{ and} \\ \mathrm{Ext}(F) :=& \{(F, f)^T\colon f \in \mathcal{F}(F)\}, \end{aligned} \tag{2.1}$$

namely $\mathcal{F}(F)$ is the set of affine-free Boolean bent functions, which can extend an (n, m)-bent function F to an $(n, m+1)$-bent function, and $\mathrm{Ext}(F)$ is the set of extensions of a function F. Clearly, different extensions may lead to different equivalence classes. In this way, we define

$$\mathcal{F}(F, C_j^{m+1}) := \{f \in \mathcal{AB}_{n,1}\colon (F, f)^T \in C_j^{m+1} \text{ is } (n, m+1)\text{-bent}\} \tag{2.2}$$

as the set of affine-free Boolean bent functions, which can extend an (n, m)-bent function F to the equivalence class C_j^{m+1}. Similarly, we define the set of extensions of the function F, which belong to the equivalence class C_j^{m+1}, that is,

$$\mathrm{Ext}(F, C_j^{m+1}) := \{(F, f)^T\colon f \in \mathcal{F}(F, C_j^{m+1})\}. \tag{2.3}$$

Clearly, the collection of sets $\mathrm{Ext}(F, C_j^{m+1})$ forms a partition of $\mathrm{Ext}(F)$, namely

$$\mathrm{Ext}(F) = \bigsqcup_{j : F \prec C_j^{m+1}} \mathrm{Ext}(F, C_j^{m+1}). \tag{2.4}$$

Remark 2.4. Non-extendable (n, m)-bent functions F are also called *lonely* [79]. In this way, it is essential to call the following sets:

- $\mathcal{F}(F)$ — the *set of bent friends* of a bent function F;
- $\mathcal{F}(F, C_j^{m+1})$ — the *set of bent friends* of F, *leading to the equivalence class* C_j^{m+1}.

Indeed, according to Definition 2.3, a bent function F is lonely, if it has no bent friends, that is, $|\mathcal{F}(F)| = 0$. We also call $(n, n/2)$-bent functions *absolutely non-extendable (lonely)*, since (n, m)-bent functions do not exist for $m > n/2$ due to the Nyberg bound (see Result 1.10).

Definition 2.5. Let $G(\mathbf{x}) = (g_1(\mathbf{x}), \ldots, g_{m+1}(\mathbf{x}))^T$ be an $(n, m+1)$-bent function. From any $(n, m+1)$-function $G(\mathbf{x}) = (g_1(\mathbf{x}), \ldots, g_{m+1}(\mathbf{x}))^T$ we construct a vector space $U_G = \langle \mathbf{g}_1, \ldots, \mathbf{g}_{m+1} \rangle$ of dimension $m+1$, spanned by the truth tables $\mathbf{g}_i \in \mathbb{F}_2^{2^n}$ of coordinate functions g_i on $\mathbb{F}_2^n$. For the vector space U_G, we denote by $\mathcal{S}(U_G)$ the collection of m-dimensional vector subspaces of U_G, which contains exactly $|\mathcal{S}(U_G)| = \left[{m+1 \atop m}\right]_2 = 2^{m+1} - 1$ elements. Assuming that every m-dimensional vector subspace U_F of U_G is given by its Gauss-Jordan basis $\mathrm{GJB}(U_F)$, we identify U_F with an (n, m)-bent function $F(\mathbf{x}) = (f_1(\mathbf{x}), \ldots, f_m(\mathbf{x}))^T$ in such a way that truth tables of coordinate functions of F are row vectors in the Gauss-Jordan basis $\mathrm{GJB}(U_F)$. With this identification, we define the *set of different (n, m)-bent spaces $\mathcal{S}(G)$* of a function G in the following way

$$\mathcal{S}(G) = \{(n, m)\text{-bent functions } H\colon U_H \in \mathcal{S}(U_G)\}.$$

For an (n, m)-bent function F, with $U_F \in \mathcal{S}(U_G)$, we define

$$\mathcal{S}(F, G) := \{H \in \mathcal{S}(G)\colon H \text{ is EA-equivalent to } F\}$$

as the set of different (n, m)-bent spaces of G, which are EA-equivalent to F.

Example 2.6. Consider the following cubic vectorial (6,3)-bent function

$$G(\mathbf{x}) = \begin{pmatrix} g_1(\mathbf{x}) \\ g_2(\mathbf{x}) \\ g_3(\mathbf{x}) \end{pmatrix} = \begin{pmatrix} x_1x_4 \oplus x_2x_5 \oplus x_3x_6 \\ x_1x_5 \oplus x_1x_6 \oplus x_2x_4 \oplus x_2x_5 \oplus x_3x_4 \\ x_1x_4 \oplus x_1x_5 \oplus x_2x_4 \oplus x_2x_5 \oplus x_2x_6 \oplus x_3x_5 \oplus x_1x_2x_3 \end{pmatrix}.$$

The set of different $(6, 2)$-bent spaces $\mathcal{S}(G)$ of the function G consists of the following $(6, 2)$-bent functions F_i:

$$F_1(\mathbf{x}) = \begin{pmatrix} g_1(\mathbf{x}) \\ g_2(\mathbf{x}) \end{pmatrix}, F_2(\mathbf{x}) = \begin{pmatrix} g_1(\mathbf{x}) \\ g_3(\mathbf{x}) \end{pmatrix}, F_3(\mathbf{x}) = \begin{pmatrix} g_1(\mathbf{x}) \\ g_2(\mathbf{x}) \oplus g_3(\mathbf{x}) \end{pmatrix}, F_4(\mathbf{x}) = \begin{pmatrix} g_2(\mathbf{x}) \\ g_3(\mathbf{x}) \end{pmatrix},$$

$$F_5(\mathbf{x}) = \begin{pmatrix} g_1(\mathbf{x}) \oplus g_2(\mathbf{x}) \\ g_3(\mathbf{x}) \end{pmatrix}, F_6(\mathbf{x}) = \begin{pmatrix} g_1(\mathbf{x}) \oplus g_2(\mathbf{x}) \\ g_2(\mathbf{x}) \oplus g_3(\mathbf{x}) \end{pmatrix}, F_7(\mathbf{x}) = \begin{pmatrix} g_1(\mathbf{x}) \oplus g_3(\mathbf{x}) \\ g_2(\mathbf{x}) \end{pmatrix}.$$

First, we observe that the function F_1 is EA-inequivalent to the functions F_i for $i = 2, \ldots, 7$, since $\deg(F_1) = 2$ and $\deg(F_i) = 3$ for all $i = 2, \ldots, 7$. In this way, we have $\mathcal{S}(F_1, G) = \{F_1\}$. It is possible to check with Magma [9] that all functions $F_2, \ldots, F_8$ are pairwise EA-equivalent. In this way, we have $\mathcal{S}(F_2, G) = \{F_2, F_3, F_4, F_5, F_6, F_7\}$.

Now we show that cardinalities of the sets $\mathcal{F}(F, C_j^{m+1})$ and $\mathcal{S}(F, G)$ do not depend on representatives of equivalence classes and thus are invariants under extended-affine equivalence.

Proposition 2.7. *Let $F, F' \in C_i^m$ be two (n, m)-bent functions and $G, G' \in C_j^{m+1}$ be two $(n, m+1)$-bent functions. If $C_i^m \prec C_j^{m+1}$, then the following hold.*

1. $|\mathcal{F}(F, C_j^{m+1})| = |\mathcal{F}(F', C_j^{m+1})|$.

2. *If* $F \in \mathcal{S}(G)$ *and* $F' \in \mathcal{S}(G')$, *then* $|\mathcal{S}(F,G)| = |\mathcal{S}(F',G')|$.

Proof. 1. Let F and F' be EA-equivalent, i.e., $F = A_1 \circ F' \circ A_2 \oplus A_3$. Clearly, if f is a bent friend of F, then $f' := f \circ A_2$ is a bent friend of F'. Moreover, the nondegenerate affine transformation A_2 maps different bent friends to different ones.

2. Let $H \in \mathcal{S}(F,G)$, i.e., there exist a surjective linear mapping $A_H \colon \mathbb{F}_2^{m+1} \to \mathbb{F}_2^m$ such that $H = A_H \circ G$. From the function H we construct a unique function $H' \in \mathcal{S}(F', G')$ as follows. Since $G, G' \in C_j^{m+1}$ we have $G' = A_1 \circ G \circ A_2 \oplus A_3$ for affine permutations A_1, A_2 and an affine function A_3. Multiplying the latter equality by $A_H \circ A_1^{-1}$ from left and substituting it in $H = A_H \circ G$, we get $A_H \circ A_1^{-1} \circ G' = H \circ A_2 \oplus A_H \circ A_1^{-1} \circ A_3$. Denoting by $A_{H'} := A_H \circ A_1^{-1}$, we get $H' := A_{H'} \circ G'$ for a surjective linear mapping $A_{H'} \colon \mathbb{F}_2^{m+1} \to \mathbb{F}_2^m$. In this way, $H' \in \mathcal{S}(G')$. Since H' and $H \in \mathcal{S}(F,G)$ are EA-equivalent, and $F, F' \in C_i^m$, we have that the functions H and H' are EA-equivalent, and thus $H' \in \mathcal{S}(F', G')$. □

In this way, for two equivalence classes $C_i^m \prec C_j^{m+1}$, we denote by $|\mathcal{F}(C_i^m, C_j^{m+1})|$ the number of Boolean bent functions, which can extend any representative of C_i^m to the class C_j^{m+1}, and by $|\mathcal{S}(C_i^m, C_j^{m+1})|$ the number of different bent spaces contained in C_j^{m+1}, which represent the equivalence class C_i^m, that is,

$$\begin{aligned} |\mathcal{F}(C_i^m, C_j^{m+1})| &:= |\mathcal{F}(F, C_j^{m+1})| \text{ and} \\ |\mathcal{S}(C_i^m, C_j^{m+1})| &:= |\mathcal{S}(F, C_j^{m+1})| \text{ for } F \in C_i^m. \end{aligned} \tag{2.5}$$

In the following section, we will use the number of bent friends $|\mathcal{F}(C_i^m, C_j^{m+1})|$ in order to enumerate all vectorial bent functions in six variables and the number of bent spaces $|\mathcal{S}(C_i^m, C_j^{m+1})|$ in order to verify these computations. Now we describe how to determine the cardinality of the equivalence class C_j^{m+1}, provided its structure is known.

Proposition 2.8. *Let* $C_1^m, \ldots, C_k^m \prec C_j^{m+1}$ *be all equivalence classes of* (n,m)*-bent functions, contained in* C_j^{m+1}*. Then the cardinality of the class* C_j^{m+1} *is equal to*

$$|C_j^{m+1}| = 2^{n+1} \cdot \sum_{i=1}^{k} |C_i^m| \cdot |\mathcal{F}(C_i^m, C_j^{m+1})|. \tag{2.6}$$

Proof. Any function $G \in C_j^{m+1}$ can be considered as an extension of a function $F \in C_i^m \prec C_j^{m+1}$, that is, $G = (F, f)^T \in C_j^{m+1}$ for $f \in \mathcal{F}(F, C_j^{m+1})$. There are k ways to select an equivalence class $C_i^m \prec C_j^{m+1}$ such that $F \in C_i^m$, and there are $|C_i^m|$ ways to choose a representative F. Finally, for any representative $F \in C_i^m$ there exist exactly $2^{n+1} \cdot |\mathcal{F}(C_i^m, C_j^{m+1})|$ ways to extend it to a function $G \in C_j^{m+1}$, since bentness is invariant with respect to addition of affine terms. □

Now we show a connection between the extendability of an (n,m)-bent function F and the metric complement of the linear code $\mathcal{C}_F$. The *covering radius* $\rho = \rho(\mathcal{C})$ of the linear code $\mathcal{C}$ of length v is defined in the following way $\rho := \max\limits_{\mathbf{x}\in\mathbb{F}_2^v}\min\limits_{\mathbf{c}\in\mathcal{C}} d_H(\mathbf{x},\mathbf{c})$. The set $\widehat{\mathcal{C}} = \{\mathbf{x} \in \mathbb{F}_2^v \colon d_H(\mathbf{x},\mathcal{C}) = \rho(\mathcal{C})\}$ is called the *metric complement* of $\mathcal{C}$. In the following, for a fixed $\mathbf{a} \in \mathbb{F}_2^n$ we define a linear function $l_{\mathbf{a}} \colon \mathbb{F}_2^n \to \mathbb{F}_2$ given by $l(\mathbf{x}) = \langle \mathbf{a},\mathbf{x}\rangle_n$ for $\mathbf{x} \in \mathbb{F}_2^n$. First, we need the following technical lemmas[1].

Lemma 2.9. *Let f,g be two Boolean functions on $\mathbb{F}_2^n$, which are not necessarily bent. Then their sum $f\oplus g$ is bent on $\mathbb{F}_2^n$ if and only if $d_H(f\oplus l_{\mathbf{a}},g) = 2^{n-1}\pm 2^{n/2-1}$ holds for all $\mathbf{a}\in\mathbb{F}_2^n$.*

Proof. Let f,g be two Boolean functions on $\mathbb{F}_2^n$, then $f\oplus g$ is bent if and only if for all $\mathbf{a}\in\mathbb{F}_2^n$ holds $d_H(f\oplus g,l_{\mathbf{a}}) = 2^{n-1}-2^{n/2-1}$ or $d_H(f\oplus g,l_{\mathbf{a}}) = 2^{n-1}+2^{n/2-1}$, since then $d_H(f\oplus g,l_{\mathbf{a}}\oplus 1) = 2^{n-1}+2^{n/2-1}$ or $d_H(f\oplus g,l_{\mathbf{a}}\oplus 1) = 2^{n-1}-2^{n/2-1}$, respectively. In this way, since $d_H(f\oplus g,l_{\mathbf{a}}) = \mathrm{wt}(f\oplus g\oplus l_{\mathbf{a}}) = d_H(f\oplus l_{\mathbf{a}},g)$, we have that $f\oplus g$ is bent on $\mathbb{F}_2^n$ if and only if $d_H(f\oplus l_{\mathbf{a}},g) = 2^{n-1}\pm 2^{n/2-1}$ holds for all $\mathbf{a}\in\mathbb{F}_2^n$. □

The following lemma shows that we can relax the condition in Lemma 2.9. We will use this fact to show a connection between extendability of bent functions and the covering radii of their codes.

Lemma 2.10. *Let f,g be two Boolean functions on $\mathbb{F}_2^n$, which satisfy the following inequality*

$$2^{n-1}-2^{n/2-1} \leq d_H(f\oplus l_{\mathbf{a}},g) \leq 2^{n-1}+2^{n/2-1} \tag{2.7}$$

for all $\mathbf{a}\in\mathbb{F}_2^n$. Then we have $d_H(f\oplus l_{\mathbf{a}},g) = 2^{n-1}\pm 2^{n/2-1}$ for all $\mathbf{a}\in\mathbb{F}_2^n$.

Proof. We prove the lemma by contradiction. Recall that by Parseval's identity, for every Boolean function h on $\mathbb{F}_2^n$ we have $\sum_{\mathbf{a}\in\mathbb{F}_2^n}\hat{\chi}_h(\mathbf{a})^2 = 2^{2n}$. Suppose that for all $\mathbf{a}\in\mathbb{F}_2^n$ we have $d_H(f\oplus l_{\mathbf{a}},g) = 2^{n-1}-2^{n/2-1}+\epsilon_{\mathbf{a}}$ with $0\leq\epsilon_{\mathbf{a}}\leq 2^{n/2}$, and suppose that for at least one $\tilde{\mathbf{a}}$ we have $0<\epsilon_{\tilde{\mathbf{a}}}<2^{n/2}$. Then the Walsh transform of $f\oplus g$ at $\mathbf{a}\in\mathbb{F}_2^n$ is given by

$$\begin{aligned}\hat{\chi}_{f\oplus g}(\mathbf{a}) &= \sum_{\mathbf{x}\in\mathbb{F}_2^n}(-1)^{g(\mathbf{x})\oplus f(\mathbf{x})\oplus\mathbf{a}\cdot\mathbf{x}} = 2^n - 2d_H(f\oplus l_{\mathbf{a}},g)\\ &= 2^n - 2(2^{n-1}-2^{n/2-1}+\epsilon_{\mathbf{a}}) = 2^{n/2}-2\epsilon_{\mathbf{a}}.\end{aligned}$$

With $0\leq\epsilon_{\mathbf{a}}\leq 2^{n/2}$, we have $\hat{\chi}_{f\oplus g}(\mathbf{a})^2 = (2^{n/2}-2\epsilon_{\mathbf{a}})^2 \leq 2^n$ with equality if and only if $\epsilon_{\mathbf{a}} = 0$ or $\epsilon_{\mathbf{a}} = 2^{n/2}$. However, by assumption for $\tilde{\mathbf{a}}$, we then have $\hat{\chi}_{f\oplus g}(\tilde{\mathbf{a}})^2 < 2^n$. This contradicts Parseval's identity for the Boolean function $f\oplus g$ on $\mathbb{F}_2^n$. □

[1] The proofs of Lemmas 2.9, 2.10 and Theorem 2.13 are due to Wilfried Meidl.

Lemma 2.9 and Lemma 2.10 can be extended to the vectorial bent case, by considering the necessary and sufficient conditions component-wise.

Lemma 2.11. *Let n be even and F, G be two (n,m)-functions, which are not necessarily bent. The following statements are equivalent.*

1. *The sum $F \oplus G$ is an (n,m)-bent function.*
2. *For all nonzero $\mathbf{v} \in \mathbb{F}_2^m$ the equality $d_H(F_\mathbf{v} \oplus l_\mathbf{a}, G_\mathbf{v}) = 2^{n-1} \pm 2^{n/2-1}$ holds for all $\mathbf{a} \in \mathbb{F}_2^n$.*
3. *For all nonzero $\mathbf{v} \in \mathbb{F}_2^m$ the inequality*
$$2^{n-1} - 2^{n/2-1} \leq d_H(F_\mathbf{v} \oplus l_\mathbf{a}, G_\mathbf{v}) \leq 2^{n-1} + 2^{n/2-1}$$
holds for all $\mathbf{a} \in \mathbb{F}_2^n$.

Remark 2.12. In the following, we identify the first-order Reed-Muller code $\mathcal{RM}(n,1)$ with the set of affine functions $\mathcal{A}_n$, since any codeword of $\mathcal{RM}(n,1)$ is a truth table of a function from $\mathcal{A}_n$. Consequently, since for an (n,m)-function F the linear code $\mathcal{C}_F$ contains the first-order Reed-Muller code $\mathcal{RM}(n,1)$ as a subcode, we identify the code $\mathcal{C}_F$ with the set $\{F_\mathbf{b} \oplus l \colon l \in \mathcal{RM}(n,1), \mathbf{b} \in \mathbb{F}_2^m\}$.

In the following statement, we provide a coding-theoretic characterization of extendable and lonely bent functions.

Theorem 2.13. *Let F be an (n,m)-bent function with $m \leq n/2-1$. Then F is extendable if and only if the linear code $\mathcal{C}_F$ has the covering radius*
$$\rho(\mathcal{C}_F) = 2^{n-1} - 2^{n/2-1}.$$
The metric complement $\widehat{\mathcal{C}_F}$ of $\mathcal{C}_F$ for an extendable (n,m)-bent function F is
$$\widehat{\mathcal{C}_F} = \{f \in \mathcal{B}_{n,1} \ : \ f \oplus F_\mathbf{v} \textit{ is bent for all } \mathbf{v} \in \mathbb{F}_2^m\}. \tag{2.8}$$

Proof. Let f be a Boolean function on $\mathbb{F}_2^n$ and $\tilde{F}$ be an $(n,m+1)$-function defined as follows $\tilde{F} \colon \mathbf{x} \mapsto (F(\mathbf{x}), f(\mathbf{x}))$. Clearly, for any such a function $\tilde{F}$, the following inequality holds,
$$\rho(\mathcal{C}_{\tilde{F}}) \leq \rho(\mathcal{C}_F) = 2^{n-1} - 2^{n/2-1}$$
with equality if only if $f \notin \mathcal{C}_F$ is bent (so that the distance from $\mathcal{RM}(n,1)$ is kept) and satisfies $d_H(f, F_\mathbf{v} \oplus l) \geq 2^{n-1} - 2^{n/2-1}$ for all $l \in \mathcal{RM}(n,1)$ and $\mathbf{v} \in \mathbb{F}_2^m$. Note that then f also satisfies $d_H(f, F_\mathbf{v} \oplus l) \leq 2^{n-1} + 2^{n/2-1}$ for all $l \in \mathcal{RM}(n,1)$ and $\mathbf{v} \in \mathbb{F}_2^m$. With Lemma 2.11, we then conclude that F is not extendable if and only if $\rho(\mathcal{C}_F) < 2^{n-1} - 2^{n/2-1}$. Finally, the metric complement $\widehat{\mathcal{C}_F}$ is given by (2.8). □

Remark 2.14. Let F be an (n, m)-bent function, which is extendable by a Boolean bent function f on $\mathbb{F}_2^n$. Then F is extendable by any bent function f' on $\mathbb{F}_2^n$ from the set $f \oplus \langle f_1, \dots f_m \rangle$. In general, the metric complement of the linear code $\mathcal{C}_F$ for an extendable (n, m)-bent function $F(\mathbf{x}) = (f_1(\mathbf{x}), \dots, f_m(\mathbf{x}))^T$ has the following structure

$$\widehat{\mathcal{C}_F} = \mathrm{Ext}(F) \oplus \mathcal{RM}(n, 1), \text{ where } \mathrm{Ext}(F) = \left(\bigsqcup_{f'} f' \oplus \langle f_1, \dots f_m \rangle \right) \tag{2.9}$$

and f' runs through all different coset leaders, which extend F.

2.3 Classification and enumeration of vectorial bent functions in six variables

Now we give a recursive algorithm, which one can use to classify and enumerate vectorial bent functions.

Algorithm 2.1. Classification and enumeration of all (n, m)-bent functions

```
Require: All pairs $(F_i^1 \in C_i^1, |C_i^1|)$, where $\mathcal{B}_{n,1} = \bigsqcup_i \{f \colon f \in C_i^1\}$.
Ensure: All pairs $(F_i^m \in C_i^m, |C_i^m|)$, where $\mathcal{B}_{n,m} = \bigsqcup_i \{f \colon f \in C_i^m\}$ for all
    $2 \le m \le n/2$.
for $m = 1$ to $n/2 - 1$ do
    for all equivalence classes $C_i^m$ do
        Construct the set of extensions $\mathrm{Ext}(F_i^m)$.
        Classify all $(n, m+1)$-bent functions from the set $\mathrm{Ext}(F_i^m)$ by
        constructing the partition $\mathrm{Ext}(F_i^m) = \bigsqcup_{j_i : F_i^m \prec C_{j_i}^{m+1}} \mathrm{Ext}(F_i^m, C_{j_i}^{m+1})$.
        Compute the number of bent friends
            $|\mathcal{F}(C_i^m, C_{j_i}^{m+1})| := |\mathcal{F}(F_i^m, C_{j_i}^{m+1})|$.
    end for
    Identify all equivalence classes $C_{j_i}^{m+1}$ with the class $C_j^{m+1}$ and set
    $F_j^{m+1}$ to be a random representative of the equivalence class $C_j^{m+1}$.
    Compute the number of bent spaces $|\mathcal{S}(C_i^m, C_j^{m+1})| := |\mathcal{S}(C_i^m, C_{j_i}^{m+1})|$
    and cardinalities of equivalence classes
        $|C_j^{m+1}| = 2^{n+1} \cdot \sum_{i=1}^{k} |C_i^m| \cdot |\mathcal{F}(C_i^m, C_{j_i}^{m+1})|$.
end for
Return pairs $(F_i^m \in C_i^m, |C_i^m|)$ for all $2 \le m \le n/2$.
```

Applying Algorithm 2.1 for Boolean bent functions in six variables, we obtain the following result.

Theorem 2.15. *For vectorial bent functions in* 6 *variables the following hold.*

1. *There are* 23,392,233,361,244,160 $\approx 2^{54.37}$ *vectorial* $(6,2)$*-bent functions, which are divided into* 9 *extended-affine equivalence classes.*
2. *There are* 121,282,113,886,947,901,440 $\approx 2^{66.71}$ *vectorial* $(6,3)$*-bent functions, which are divided into* 13 *extended-affine equivalence classes.*

Moreover, if a $(6,m)$*-bent function* F *is non-extendable, then* F *is absolutely non-extendable, that is,* $m = 3$*.*

Proof. Now we consider the main steps of Algorithm 2.1 in more detail and explain how one can verify our computational results.
Input. For the input of Algorithm 2.1, one has to provide the pairs $(F_i^1, |C_i^1|)$ with $F_i^1 \in C_i^1$ for all equivalence classes C_i^1, which form a partition of the set of Boolean bent functions $\mathcal{B}_{6,1}$. The representatives of 4 equivalence classes are given in Table 1.1(a). For the cardinalities of the equivalence classes, we refer to Table A.4(a).
Output. In order to compute the collections $\mathcal{F}(F_i^m)$, one first has to construct all affine-free Boolean bent functions $\mathcal{AB}_{6,1}$, which can be efficiently listed as described in [70, 83]. Consequently, for a given representative $F_i^m \in C_i^m$ we construct the set $\mathcal{F}(F_i^m)$, by checking directly the characteristic property in (2.1). The classification of functions $G \in \mathrm{Ext}(F_i^m)$ is carried out with Magma [9], by checking the equivalence of linear codes $\mathcal{C}_G$ with the help of Result 1.60.

In this way, Algorithm 2.1 constructs $n/2-1$ layers of the weighted Hasse diagram given in Figure 2.1 as follows. For all $2 \le m \le n/2-1$, we draw an edge between equivalence classes C_i^m and C_j^{m+1} if $C_i^m \prec C_j^{m+1}$ and assign two weights with it. The first number, closer to the equivalence class C_i^m, is the number of bent spaces $|\mathcal{S}(C_i^m, C_j^{m+1})|$, and the second number, closer to C_j^{m+1}, is the number of bent friends $|\mathcal{F}(C_i^m, C_j^{m+1})|$. Note that, if $C_1^m, \dots, C_k^m \prec C_j^{m+1}$ are all equivalence classes contained in C_j^{m+1}, then the following relation holds

$$\sum_{i=1}^{k} |\mathcal{S}(C_i^m, C_j^{m+1})| = \begin{bmatrix} m+1 \\ m \end{bmatrix}_2 = 2^{m+1} - 1.$$

In Figure 2.1, we list exact cardinalities $|C_i^1|$ for all equivalence classes C_i^1, while for equivalence classes $C_i^{m\ge 2}$, due to the lack of a space, we give only approximate values. The exact values $|C_i^{m\ge 2}|$ are given in Table A.4 and can be verified with Proposition 2.8. Finally, we give the total number of bent functions in six variables in Table 2.2 and provide algebraic normal forms of representatives of the equivalence classes together with their invariants (orders of automorphism groups and Smith normal forms) in Appendix A.

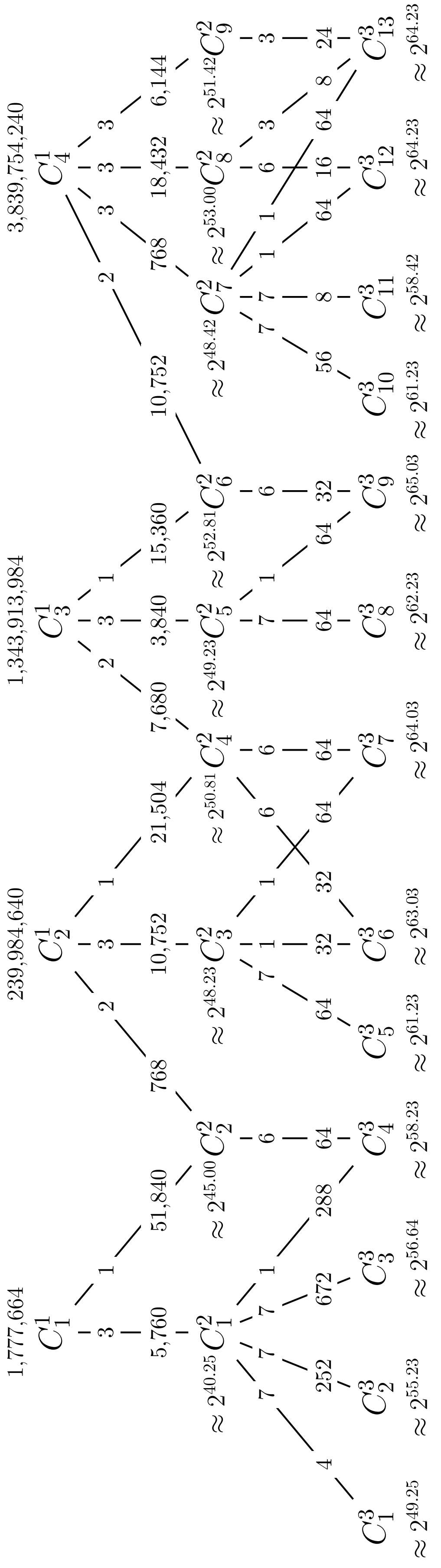


Figure 2.1. The structure of EA-equivalence classes of vectorial bent functions in six variables

Table 2.2. Classification and count of bent functions in six variables

(n,m)	$\lvert\mathcal{AB}_{n,m}\rvert$	$\lvert\mathcal{B}_{n,m}\rvert = \lvert\mathcal{AB}_{n,m}\rvert \cdot 2^{m(n+1)}$	# Eq. cl.
$(6,1)$	$48{,}386{,}176 \approx 2^{25.33}$	$5{,}425{,}430{,}528 \approx 2^{32.33}$	4
$(6,2)$	$1{,}427{,}748{,}618{,}240 \approx 2^{40.37}$	$23{,}392{,}233{,}361{,}244{,}160 \approx 2^{54.37}$	9
$(6,3)$	$57{,}831{,}818{,}526{,}720 \approx 2^{45.71}$	$121{,}282{,}113{,}886{,}947{,}901{,}440 \approx 2^{66.71}$	13

Verification. First, one may observe that cardinalities of all equivalence classes and hence of the sets $\mathcal{B}_{6,m}$ are divisible by the order of the *general linear group* $\mathrm{GL}(m, \mathbb{F}_2)$, which is given by $\lvert \mathrm{GL}(m, \mathbb{F}_2)\rvert = \prod_{k=0}^{m-1} \left(2^m - 2^k\right)$. We also observe that the number of quadratic $(6,2)$-bent functions established with Algorithm 2.1 coincides with the theoretically computed value $\lvert\mathcal{AB}_{n,2}\rvert$ given in Result 1.26. Moreover, we note that for equivalence classes $C_i^m, C_{i'}^m \prec C_j^{m+1}$ the following relation holds

$$\frac{|C_i^m| \cdot |\mathcal{F}(C_i^m, C_j^{m+1})|}{|\mathcal{S}(C_i^m, C_j^{m+1})|} = \frac{|C_{i'}^m| \cdot |\mathcal{F}(C_{i'}^m, C_j^{m+1})|}{|\mathcal{S}(C_{i'}^m, C_j^{m+1})|},$$

since the portion of (n,m)-bent functions from the class C_i^m, contained in the equivalence class C_j^{m+1} equals to

$$\frac{|\mathcal{S}(C_i^m, C_j^{m+1})|}{(2^{m+1}-1) \cdot 2^{n+1} \cdot |\mathcal{F}(C_i^m, C_j^{m+1})|}.$$

Finally, from Figure 2.1 one can see that the only non-extendable bent functions in 6 variables are those, which achieve the Nyberg bound, i.e., $(6,3)$-bent functions. □

2.4 Explanation by the known constructions

It is well-known that all Boolean bent functions in six variables, up to extended-affine equivalence, can be described by the classical Maiorana-McFarland $\mathcal{M}$ construction, while some of the functions may also be represented by the Desarguesian partial spread $\mathcal{PS}_{ap}$ construction. Since both constructions have a direct generalization to the vectorial case, as we have mentioned in Subsection 1.1.3, it is essentially to check whether all vectorial bent functions in six variables can be covered, up to equivalence, by the vectorial versions of $\mathcal{M}$ and $\mathcal{PS}_{ap}$ constructions.

In Table 2.3, we list equivalence classes C_i^m of $(6,3)$-bent functions, which can be described by vectorial $\mathcal{M}$ and $\mathcal{PS}_{ap}$ classes. Note that $(6,2)$-bent functions from $\mathcal{M}$ and $\mathcal{PS}_{ap}$ can be constructed as proper bent subspaces of $(6,3)$-bent from $\mathcal{M}$ and $\mathcal{PS}_{ap}$ classes.

Table 2.3. EA-equivalence classes of $(6,3)$-bent functions, described by classical constructions

2.3(a) Permutations of $\mathbb{F}_2^3$

π_i	$z \mapsto \pi_i(z)$
π_1	z
π_2	z^3
π_3	$z + z^3 + z^5$
π_4	$z^2 + z^3 + z^4 + z^5 + z^6$

2.3(b) $\mathcal{M}$ class

C_i^3	$x \cdot \pi_i(y) + G(y)$
C_1^3	$x \cdot \pi_1(y)$
C_2^3	$x \cdot \pi_1(y) + (y + y^2 + y^3 + y^6)$
C_4^3	$x \cdot \pi_1(y) + (y^3 + y^5 + y^6 + y^7)$
C_5^3	$x \cdot \pi_4(y)$
C_8^3	$x \cdot \pi_3(y)$
C_{10}^3	$x \cdot \pi_2(y) + (y + y^2 + y^3 + y^6)$
C_{11}^3	$x \cdot \pi_2(y)$

2.3(c) $\mathcal{PS}_{ap}$ class

C_i^3	$H(x/y)$
C_{11}^3	$\pi_1(x/y)$
C_{12}^3	$\pi_3(x/y)$
C_{13}^3	$\pi_4(x/y)$

In this way, from Figure 2.1 and Table 2.3 one can see that the only "missing" equivalence classes of $(6,3)$-bent functions are $C_3^3, C_6^3, C_7^3, C_9^3$ and of $(6,2)$-bent functions are C_4^2, C_6^2. In view of this observation, we conclude that in contrast to the Boolean case, vectorial versions of the classical Maiorana-McFarland and Desarguesian partial spread constructions do not cover the whole set of vectorial bent functions in six variables.

2.5 Conclusion and open problems

In this chapter, we classified and enumerated vectorial bent functions in six variables. Besides that, we provided the structure of the obtained equivalence classes (see Figure 2.1) and explained, which of the equivalence classes can be covered by Maiorana-McFarland $\mathcal{M}$ and Desarguesian partial spread $\mathcal{PS}_{ap}$ constructions (see Table 2.3). Considering the structure of equivalence classes of bent functions in a small number of variables, we would like to point the reader's attention on the following two observations based on Remark 1.27 and Figure 2.1.

First, we observe that in $n = 4$ and $n = 6$ variables the only non-extendable bent functions are those, which achieve the Nyberg bound, i.e., $(n, n/2)$-bent functions. In this way, it is reasonable to ask the following question.

Open Problem 2.16. Do non-extendable (n,m)-bent functions (with $m < n/2$) exist?

Since in general it is most likely very difficult to solve this problem theoretically as well as computationally, one may try to attack the relaxed version of this problem, by considering the non-extendability problem for a certain subclass of bent functions (e.g., quadratic, Maiorana-McFarland, Desarguesian partial spread). As a starting point, one can address the question of the non-extendability of quadratic (n,m)-bent functions, following the work of Özbudak and Pott [91].

Open Problem 2.17. Do non-extendable quadratic (n, m)-bent functions (with $m < n/2$) exist?

Second, as one can see from Figure 2.1, for a representative F of an equivalence class C_i^m, there exist many bent functions f, which can extend F to a representative of a class C_j^{m+1}. A theoretical reason behind that, as it was explained recently in Remark 2.14, is the following: if an (n, m)-bent function $F = (f_1(\mathbf{x}), \ldots, f_m(\mathbf{x}))^T$ is extendable by a Boolean bent function f on $\mathbb{F}_2^n$, then F is also extendable by any bent function f' on $\mathbb{F}_2^n$ from the set $f \oplus \langle f_1, \ldots f_m \rangle$. Taking into account this observation, one can see that the only equivalence classes $C_i^m \prec C_j^{m+1}$ of bent functions in six variables with the property "any representative $F \in C_i^m$ is uniquely extendable, up to the choice of the coset leader, to a representative $(F, f)^T \in C_j^{m+1}$" are the classes C_1^2 and C_1^3. In this way, bent functions with this property are exceptionally rare in a small number of variables. Based on this observation, we think it is reasonable to address the following problem.

Open Problem 2.18. Which $(n, n/2)$-bent functions can be characterized by the property to be "unique" extensions of $(n, n/2 - 1)$-bent functions.

As a starting point, one can consider the following $(2m, m)$-bent function F defined by

$$F \colon (x, y) \in \mathbb{F}_{2^m} \times \mathbb{F}_{2^m} \mapsto x \cdot y \in \mathbb{F}_{2^m},$$

since for $m = 3$ this function represents the equivalence class C_1^3.

Chapter 3

Design-theoretic aspects of bent functions

Vectorial bent functions, plateaued and differentially uniform functions, being generalizations of Boolean bent functions, inherit many of their cryptographic and combinatorial properties. In this chapter, we investigate, which design-theoretic properties of Boolean bent functions can be shared with their generalizations.

This chapter summarizes various design-theoretic aspects of Boolean and vectorial bent functions appeared in papers by Polujan and Pott [92–94]. The parts of this chapter concerning various generalizations of the concept of vanishing flats, introduced by Li, Meidl, Pott, Riera, Stănică and the author of this dissertation in [73], are based on the work by Meidl, Polujan and Pott [80].

3.1 Introduction

The interaction between design theory and the theory of perfect nonlinear functions is of special interest. For instance, any new construction of bent functions may lead to a new construction of certain incidence structures. On the other hand, combinatorial invariants of incidence structures constructed from functions over finite fields serve as good distinguishers between inequivalent functions and even classes of functions [54, 73, 110]. Recently there has been a lot of work related with (n,m)-functions and incidence structures [44, 47, 73, 94, 108]. In this chapter, we continue the study of the interaction between Boolean as well as vectorial functions and combinatorial designs.

3.1.1 Perfect nonlinear functions and combinatorial designs

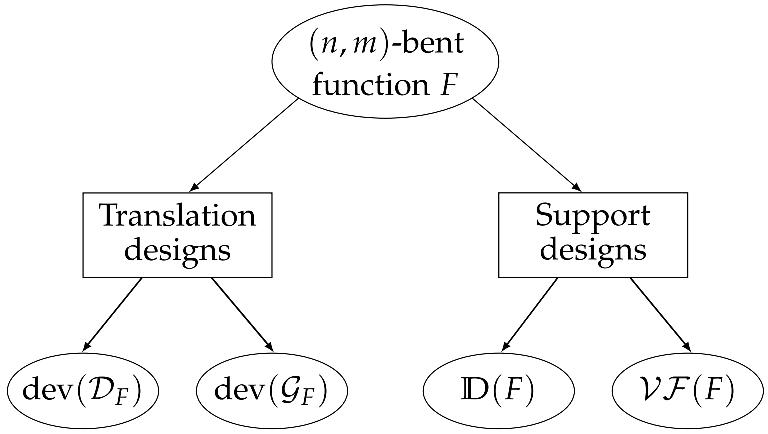
In this subsection, we consider in more detail the following constructions of incidence structures from Boolean and vectorial functions, which constitute the following two groups:

- Developments of supports $\mathrm{dev}(\mathcal{D}_f)$ for Boolean functions f on $\mathbb{F}_2^n$ and developments of graphs $\mathrm{dev}(\mathcal{G}_F)$ for (n, m)-functions F.

- Supports of codewords of the minimum weight of linear codes $\mathcal{C}_F$ and $\mathcal{C}_F^\perp$ for (n, m)-functions F, also known as addition designs $\mathbb{D}(F)$ and the vanishing flats $\mathcal{VF}(F)$, respectively.

In general, for an arbitrary (n, m)-function F the aforementioned incidence structures do not necessarily have nice combinatorial properties, i.e., are regular or even form a t-design. However, for Boolean and vectorial bent functions, the incidence structures summarized in Figure 3.1 are either 2-designs or divisible designs, as we mentioned in Section 1.4. Moreover, they can be used to characterize bentness of (n, m)-functions F. For the characterizations of (n, m)-bent functions F in terms of incidence structures $\mathrm{dev}(\mathcal{D}_F)$ (for $\mathcal{D}_F$ the function F is must be a Boolean function), $\mathrm{dev}(\mathcal{G}_F)$ and $\mathbb{D}(F)$ we refer to Section 1.4 of the first chapter. A characterization of (n, m)-bent functions F by means of vanishing flats $\mathcal{VF}(F)$ will be given in Section 3.5.

Figure 3.1. Designs from bent functions


(n, m)-bent function F
Translation designs
Support designs
$\mathrm{dev}(\mathcal{D}_F)$
$\mathrm{dev}(\mathcal{G}_F)$
$\mathbb{D}(F)$
$\mathcal{VF}(F)$

Besides that, we investigate a coding-theoretic generalization of vanishing flats, i.e., incidence structures supported by codewords of an arbitrary weight of linear codes $\mathcal{C}_F$ and $\mathcal{C}_F^\perp$ for (n, m)-functions F. We also introduce a combinatorial generalization of the vanishing flats, namely the incidence structure called non-vanishing flats, and provide characterizations of plateaued and bent functions by means of combinatorial properties of this object.

3.1.2 Objectives

The main aim of this chapter is to figure out, which design-theoretic properties of Boolean bent functions (within the framework of developments and supports of the codewords of the minimum weight, see Figure 3.1), can be shared with their generalizations: the classes of vectorial bent functions, (n, m)-plateaued functions and differentially uniform functions.

The rest of the chapter is organized in the following way. In Section 3.2, we study geometric invariants of Boolean and vectorial functions, which were introduced in Subsection 1.4.1. In Subsection 3.2.1, we provide a connection between the rank and linearity index of a Boolean function. Consequently, we give an upper bound on the linearity index of a Boolean function using its rank. In Subsection 3.2.2, we study relations between different notions of ranks for Boolean functions. We show that ranks and Γ-ranks coincide for all non-constant Boolean functions. Finally, in Subsection 3.2.3, we explain how one can compute the Smith normal form of Boolean functions more efficiently and specify the shape of the Smith normal form for Boolean and vectorial bent functions.

In Section 3.3, we provide examples of extended-affine inequivalent Boolean bent functions f, f' on $\mathbb{F}_2^n$, whose translation designs $\operatorname{dev}(\mathcal{G}_f)$ and $\operatorname{dev}(\mathcal{G}_{f'})$ are isomorphic. Consequently, we prove that for any $n \geq 6$ isomorphism of translation designs $\operatorname{dev}(\mathcal{G}_f)$ and $\operatorname{dev}(\mathcal{G}_{f'})$ of Boolean bent functions f and f' on $\mathbb{F}_2^n$ is a coarser equivalence relation than extended-affine equivalence. However, based on the analysis of vectorial bent functions in a small number of variables, we indicate that this phenomenon may not occur in general for vectorial bent functions. We observe that, in contrast to the Boolean case, vectorial bent functions F and F' on $\mathbb{F}_2^6$ are extended-affine equivalent if and only if their translation designs $\operatorname{dev}(\mathcal{G}_F)$ and $\operatorname{dev}(\mathcal{G}_{F'})$ are isomorphic.

In Section 3.4, we study the same question, but in the context of addition designs. We show that extended-affine equivalence of vectorial bent functions, similarly to the Boolean case, coincides with the isomorphism of addition designs, in this way, answering a recent question, addressed by Ding, Munemasa and Tonchev [44, Note 24].

In Section 3.5, we consider in detail the vanishing flats of Boolean and vectorial bent functions. As it was shown in [108, Example 4], linear codes $\mathcal{C}_F$ and $\mathcal{C}_F^\perp$ of all (n, m)-bent functions F support 2-designs and hence vanishing flats are 2-designs as well. Using a connection between bent functions and relative difference sets we show that this condition (being a 2-design) is actually sufficient for the perfect nonlinearity.

In Section 3.6, we generalize the original concept of vanishing flats. In Subsection 3.6.1, we introduce the notion of nonvanishing flats $\mathcal{NF}_{\mathbf{v}}(F)$ for (n, m)-functions F and consequently show that the collection of all nonvanishing flats for an (n, m)-function F is an invariant under EA-equivalence. In Subsection 3.6.2, we give a design-theoretic interpretation of the well-known characterization of plateaued functions, given by Carlet [28]. In particular, we show that nonvanishing flats $\mathcal{NF}_{\mathbf{v}}(F)$ of (n, m)-plateaued functions F are regular incidence structures, i.e., 1-$(2^n, 4, \lambda_{\mathbf{v}})$ designs (with not necessarily the same $\lambda_{\mathbf{v}}$). Moreover, we show that the regularity condition is also sufficient for plateauedness, and explain how one can compute the value $\lambda_{\mathbf{v}}$. Furthermore, we show that the equiregularity condition, i.e., nonvanishing flats $\mathcal{NF}_{\mathbf{v}}(F)$ are 1-$(2^n, 4, \lambda_{\mathbf{v}})$ designs with $\lambda_{\mathbf{v}} = \lambda$ for all $\mathbf{v} \in \mathbb{F}_2^m \setminus \{\mathbf{0}\}$, is necessary and sufficient for s-plateauedness of (n,m)-functions F. Finally, in Subsection 3.6.3, we consider nonvanishing flats of bent functions, in particular, we characterize (n,m)-bent functions F among the class of plateaued functions as those, for which the nonvanishing flats $\mathcal{NF}_{\mathbf{v}}(F)$ are 2-$(2^n, 4, 2^{n-m-1})$ designs for all $\mathbf{v} \in \mathbb{F}_2^m \setminus \{\mathbf{0}\}$.

In Section 3.7, we consider extendable and lonely bent functions. Particularly, we provide a design-theoretic framework for studying the extendability of bent functions by means of vanishing and nonvanishing flats.

In Section 3.8, we provide new applications of extended Assmus-Mattson theorem. First, in Subsection 3.8.1, we show that extended Assmus-Mattson theorem, applied to the linear codes of Boolean bent functions may also outperform the transitivity theorem. We show that the automorphism groups of linear codes $\mathcal{C}_f$ and $\mathcal{C}_f^{\perp}$ of Boolean bent functions f on $\mathbb{F}_2^n$ are 2-transitive if and only if f is quadratic. However, by extended Assmus-Mattson theorem, the linear codes $\mathcal{C}_f$ and $\mathcal{C}_f^{\perp}$ of all Boolean bent functions f on $\mathbb{F}_2^n$ support 2-designs. In Subsection 3.8.2, we show that the linear codes of certain APN functions with the classical Walsh spectrum support 2-designs similarly to AB functions; the latter was shown in [108]. We also provide new sufficient conditions for an APN function with the classical Walsh spectrum to be CCZ-inequivalent to a quadratic one.

Finally, in Section 3.9, we give concluding remarks and raise some further questions and open problems on (n,m)-functions and their incidence structures.

3.2 On geometric invariants of Boolean and vectorial functions

Throughout the chapter, we will use the following notation for incidence matrices of translation designs of Boolean functions f on $\mathbb{F}_2^n$, which were introduced in Subsection 1.4.1:

$$\mathbf{M}_f := \mathbf{M}(\mathrm{dev}(\mathcal{D}_f)) = (f(\mathbf{x} \oplus \mathbf{y}))_{\mathbf{x},\mathbf{y} \in \mathbb{F}_2^n} \quad \text{and} \quad \mathbf{N}_f := \mathbf{M}(\mathrm{dev}(\mathcal{G}_f)).$$

Note that $(\mathbf{x} \oplus \mathbf{y}, 1) \in \mathcal{G}_f \Leftrightarrow f(\mathbf{x} \oplus \mathbf{y}) = 1$ and $(\mathbf{x} \oplus \mathbf{y}, 0) \in \mathcal{G}_f \Leftrightarrow \bar{f}(\mathbf{x} \oplus \mathbf{y}) = 1$, consequently, the matrix $\mathbf{N}_f$ can be written without loss of generality as the following block matrix

$$\mathbf{N}_f = \begin{array}{cc} \begin{matrix} V_1 & V_0 \end{matrix} & \\ \begin{pmatrix} \mathbf{M}_f & \mathbf{M}_{\bar{f}} \\ \mathbf{M}_{\bar{f}} & \mathbf{M}_f \end{pmatrix} & \begin{matrix} V_0 \\ V_1 \end{matrix} \end{array}, \tag{3.1}$$

where $V_i := \{(\mathbf{x}, i) \colon \mathbf{x} \in \mathbb{F}_2^n\}$ for a fixed $i \in \mathbb{F}_2$. Similarly to the Boolean case, we also denote by $\mathbf{N}_F$ an incidence matrix of the translation design $\mathrm{dev}(\mathcal{G}_F)$ for a vectorial (n, m)-function F.

3.2.1 Linearity index and rank of Boolean functions

In general, one has to use Algorithm 1.1 in order to compute the linearity index $\mathrm{ind}(f)$ of a Boolean function f on $\mathbb{F}_2^n$. In the following statement, we show that one can estimate the linearity index $\mathrm{ind}(f)$ by means of $\mathrm{rank}(f)$ without enumeration of $\mathcal{M}$-subspaces of f.

Theorem 3.1. *The linearity index* $\mathrm{ind}(f)$ *of a nonzero Boolean function on* $\mathbb{F}_2^n$ *is at most* $n + 1 - \log_2(\mathrm{rank}(f))$.

Proof. Let $f_{\pi,\phi} \colon \mathbb{F}_2^r \times \mathbb{F}_2^s \to \mathbb{F}_2$ be a Maiorana-McFarland representation (1.23) of the function $f \colon \mathbb{F}_2^n \to \mathbb{F}_2$ satisfying $r = \mathrm{ind}(f)$ and $s = n - r$. Let $\mathbf{a}, \mathbf{x} \in \mathbb{F}_2^r$ and $\mathbf{b}, \mathbf{y} \in \mathbb{F}_2^s$. Then $\mathbf{M}_f$ is given by $\mathbf{M}_f((\mathbf{a}, \mathbf{b}), (\mathbf{x}, \mathbf{y})) = f(\mathbf{a} \oplus \mathbf{x}, \mathbf{b} \oplus \mathbf{y})$. Following Weng et al. [110], we add the row $(\mathbf{0}, \mathbf{b})$ to the row $(\mathbf{a}, \mathbf{b})$, for all $\mathbf{a} \in \mathbb{F}_2^r, \mathbf{b} \in \mathbb{F}_2^s$ with $\mathbf{a} \neq \mathbf{0}$, and add the column $(\mathbf{0}, \mathbf{y})$ to the column $(\mathbf{x}, \mathbf{y})$, for all $\mathbf{x} \in \mathbb{F}_2^r, \mathbf{y} \in \mathbb{F}_2^s$ with $\mathbf{x} \neq \mathbf{0}$. In this way, we get a matrix $\mathbf{A}$ which has the same rank as $\mathbf{M}_f$, and whose $((\mathbf{a}, \mathbf{b}), (\mathbf{x}, \mathbf{y}))$-th entry is given by

$$\begin{cases} \bigoplus\limits_{\mathbf{z} \in \langle \mathbf{a}, \mathbf{x} \rangle} f_{\pi,\phi}(\mathbf{z}, \mathbf{b} \oplus \mathbf{y}), & \text{if } \mathbf{a} \neq \mathbf{0},\ \mathbf{x} \neq \mathbf{0}, \\ f_{\pi,\phi}(\mathbf{a}, \mathbf{b} \oplus \mathbf{y}) \oplus f_{\pi,\phi}(\mathbf{0}, \mathbf{b} \oplus \mathbf{y}), & \text{if } \mathbf{a} \neq \mathbf{0},\ \mathbf{x} = \mathbf{0}, \\ f_{\pi,\phi}(\mathbf{x}, \mathbf{b} \oplus \mathbf{y}) \oplus f_{\pi,\phi}(\mathbf{0}, \mathbf{b} \oplus \mathbf{y}), & \text{if } \mathbf{a} = \mathbf{0},\ \mathbf{x} \neq \mathbf{0}, \\ f_{\pi,\phi}(\mathbf{0}, \mathbf{b} \oplus \mathbf{y}), & \text{if } \mathbf{a} = \mathbf{x}. \end{cases}$$

With the definition of the function $f_{\pi,\phi}$, we get the following values

$$\begin{cases} \mathbf{0}, & \text{if } \mathbf{a} \neq \mathbf{0},\ \mathbf{x} \neq \mathbf{0}, \\ \langle \mathbf{a}, \pi(\mathbf{b} \oplus \mathbf{y}) \rangle_r, & \text{if } \mathbf{a} \neq \mathbf{0},\ \mathbf{x} = \mathbf{0}, \\ \langle \mathbf{x}, \pi(\mathbf{b} \oplus \mathbf{y}) \rangle_r, & \text{if } \mathbf{a} = \mathbf{0},\ \mathbf{x} \neq \mathbf{0}, \\ \phi(\mathbf{b} \oplus \mathbf{y}), & \text{if } \mathbf{a} = \mathbf{x} = \mathbf{0}. \end{cases}$$

In this way, the matrix $\mathbf{A}$ can be expressed in the following block form

$$\mathbf{A} = \begin{array}{cc} \mathbb{F}_2^s & \mathbb{F}_2^n \setminus \mathbb{F}_2^s \\ \left(\begin{array}{c} \mathbf{M}_\phi \\ \mathbf{L}_\pi \end{array}\right. & \left.\begin{array}{c} \mathbf{L}_\pi^T \\ \mathbf{O}_{2^n - 2^s, 2^n - 2^s} \end{array}\right) \end{array} \begin{array}{c} \\ \mathbb{F}_2^s \\ \mathbb{F}_2^n \setminus \mathbb{F}_2^s \end{array}, \tag{3.2}$$

where $\mathbf{L}_\pi$ is a $(2^n - 2^s) \times 2^s$-matrix over $\mathbb{F}_2$, whose $((\mathbf{a}, \mathbf{b}), \mathbf{y})$-th entry with $\mathbf{a} \neq \mathbf{0}$ is given by $\mathbf{L}_\pi((\mathbf{a}, \mathbf{b}), \mathbf{y}) = \langle \mathbf{a}, \pi(\mathbf{b} \oplus \mathbf{y}) \rangle_r$, and $\mathbf{M}_\phi$ is a $2^s \times 2^s$-matrix over $\mathbb{F}_2$

given by $\mathbf{M}_\phi(\mathbf{b},\mathbf{y}) = \phi(\mathbf{b} \oplus \mathbf{y})$ for all $\mathbf{b},\mathbf{y} \in \mathbb{F}_2^s$. From decomposition (3.2), we get the following upper bound for the rank of the function $f_{\pi,\phi}$

$$\mathrm{rank}(f_{\pi,\phi}) \leq 2^s + \mathrm{rank}(\mathbf{M}_\phi\ \mathbf{L}_\pi) \leq 2 \cdot 2^s = 2^{s+1} = 2^{n-r+1}, \tag{3.3}$$

since $\mathrm{rank}(\mathbf{M}_\phi\ \mathbf{L}_\pi) \leq 2^s$ and $r = n - s$. Taking the logarithm of both sides, we get $\log_2(\mathrm{rank}(f_{\pi,\phi})) \leq n - r + 1$, or equivalently, $r \leq n + 1 - \log_2(\mathrm{rank}(f_{\pi,\phi}))$. Since functions $f_{\pi,\phi}$ and f are EA-equivalent, we get $r = \mathrm{ind}(f_{\pi,\phi}) = \mathrm{ind}(f)$ and $\mathrm{rank}(f_{\pi,\phi}) = \mathrm{rank}(f)$. In this way, we have $\mathrm{ind}(f) \leq n + 1 - \log_2(\mathrm{rank}(f))$. □

Remark 3.2. *1.* In Theorem 3.1, we consider only nonzero Boolean functions in order to omit the trivial case: if $f = 0$, then $\log_2(\mathrm{rank}(f))$ is not defined, since $\mathrm{rank}(f) = 0$. Note that $\mathrm{ind}(f) = n$ since f is affine.
2. It seems that many Boolean functions f on $\mathbb{F}_2^n$ achieve the bound from Theorem 3.1 with equality. An example of such functions are monomials m_d on $\mathbb{F}_2^n$ given by $m_d \colon (x_1, \ldots, x_n) \mapsto x_1 \cdots x_d$. Since monomials m_d belong to the generalized Maiorana-McFarland class $\mathcal{M}_{n+1-d,d-1}$, as the following computation shows

$$m_d(x_1, \ldots, x_n) = \langle (x_1, x_{d+1}, \ldots, x_n), (x_2 \cdots x_d, 0, \ldots, 0) \rangle_{n+1-d},$$

we have $\mathrm{ind}(m_d) = n + 1 - d$. On the other hand, Weng et al. [111] showed that $\mathrm{rank}(m_d) = 2^d$ on $\mathbb{F}_2^n$. Substituting $\mathrm{ind}(m_d) = n + 1 - d$ and $\mathrm{rank}(m_d) = 2^d$ into $\mathrm{ind}(m_d) \leq n + 1 - \log_2(\mathrm{rank}(m_d))$, we get an equality.
3. Boolean bent functions $f \in \mathcal{M}^\#$ on $\mathbb{F}_2^n$ do not achieve the bound of Theorem 3.1 with equality, since $\mathrm{ind}(f) = n/2$ and $\mathrm{rank}(f) \leq 2^{n/2+1} - 2 < 2^{n/2+1}$, see [110]. The question whether a bent function $f \notin \mathcal{M}^\#$ on $\mathbb{F}_2^n$ can achieve this bound with equality, seems to be difficult in general.

3.2.2 On the ranks of Boolean functions

In this subsection, we show that Γ-rank(f) and $\mathrm{rank}(f)$ coincide for all nonconstant Boolean functions f on $\mathbb{F}_2^n$. First, we summarize some well-known statements about higher-order derivatives, which we will use to show the connection between the ranks of Boolean functions.

Result 3.3. *[66] Let f be a Boolean function on $\mathbb{F}_2^n$ and $\mathbf{a}_1, \ldots, \mathbf{a}_k \in \mathbb{F}_2^n$.*

1. *If $\mathbf{a}_1, \ldots, \mathbf{a}_k$ are linearly dependent, then $D_{\mathbf{a}_k} D_{\mathbf{a}_{k-1}} \ldots D_{\mathbf{a}_1} f = 0$.*

2. *Let now $\mathbf{a}_1, \ldots, \mathbf{a}_k$ be linearly independent. The derivatives of f are independent of the order in which the derivation is taken, i.e., the equality*

$$D_{\mathbf{a}_k} D_{\mathbf{a}_{k-1}} \ldots D_{\mathbf{a}_1} f(\mathbf{x}) = D_{\mathbf{a}_{\pi(k)}} D_{\mathbf{a}_{\pi(k-1)}} \ldots D_{\mathbf{a}_{\pi(1)}} f(\mathbf{x}) = \bigoplus_{\mathbf{a} \in \langle \mathbf{a}_1, \ldots, \mathbf{a}_k \rangle} f(\mathbf{x} \oplus \mathbf{a})$$

   holds for any permutation π on $\{1, \ldots, k\}$.

In the following theorem, we prove that for Boolean functions of degree at least one, the Γ-rank and rank coincide and show that all information about the SNF(f) can be recovered from a matrix obtained through a small modification of the matrix $\mathbf{M}_f$.

Theorem 3.4. *Let f be a Boolean function on $\mathbb{F}_2^n$. Then the following hold.*

1. *If* $\deg(f) \geq 1$, *then the all-one-vector* $\mathbf{j}_{2^n}$ *can be expressed as a sum of an even number of vectors from the linear code* $\mathcal{C}(\mathrm{dev}(\mathcal{D}_f))$.

2. *If* $\deg(f) < 1$, *then* $\Gamma\text{-rank}(f) = 2$, *otherwise* $\Gamma\text{-rank}(f) = \mathrm{rank}(f)$.

Proof. 1. It was shown in [110, Lemma 3.1] that $\mathbf{j}_{2^n} \in \mathcal{C}(\mathrm{dev}(\mathcal{D}_f))$. We will prove this statement, by expressing $\mathbf{j}_{2^n}$ as a sum of an even number of vectors from the linear code $\mathcal{C}(\mathrm{dev}(\mathcal{D}_f))$. First, we observe that the number of slow points of a function f is bounded from below by $2^n - 2^{n-d}$, where d is the degree of the function f. Thus, there exist a sequence of slow points $\mathbf{a}_1, \ldots, \mathbf{a}_d$ such that the d-th order derivative $D_{\mathbf{a}_d} D_{\mathbf{a}_{d-1}} \ldots D_{\mathbf{a}_1} f$ is the constant one function. Finally, since the following equality holds for all $\mathbf{x} \in \mathbb{F}_2^n$ due to Result 3.3

$$D_{\mathbf{a}_d} D_{\mathbf{a}_{d-1}} \ldots D_{\mathbf{a}_1} f(\mathbf{x}) = \bigoplus_{\mathbf{a} \in \langle \mathbf{a}_1, \ldots, \mathbf{a}_d \rangle} f(\mathbf{x} \oplus \mathbf{a}) = 1,$$

one can see, the all-one-vector $\mathbf{j}_{2^n}$ is the sum of 2^d elements of $\mathcal{C}(\mathrm{dev}(\mathcal{D}_f))$.
2. Assume that the matrix $\mathbf{N}_f$ is of the form (3.1). Performing elementary row and column operations, one can bring the matrix N_f to the form

$$\mathbf{N}_f \overset{\text{(I)}}{\rightsquigarrow} \begin{pmatrix} \mathbf{M}_f & \mathbf{M}_{\bar{f}} \\ \mathbf{J}_{2^n} & \mathbf{J}_{2^n} \end{pmatrix} \overset{\text{(II)}}{\rightsquigarrow} \begin{pmatrix} \mathbf{M}_f & \mathbf{J}_{2^n} \\ \mathbf{J}_{2^n} & \mathbf{O}_{2^n} \end{pmatrix}.$$

Note that elementary column operations change the linear code $\mathcal{C}(\mathrm{dev}(\mathcal{D}_f))$, however, its dimension, which is equal to Γ-rank(f), remains the same. If f is a constant function, i.e., $\deg(f) < 1$, then clearly $\Gamma\text{-rank}(f) = 2$. By the previous claim, $\mathbf{j}_{2^n}$ can be expressed as a sum of an even number of rows of $\mathbf{M}_f$. Since the matrix $\mathbf{M}_f$ is symmetric, the vector $\mathbf{j}_{2^n}^T$ can be expressed as a sum of an even number of columns of the matrix $\mathbf{M}_f$. In this way, the matrix $\mathbf{N}_f$ can be brought to the form

$$\mathbf{N}_f \overset{\text{(I)-(II)}}{\rightsquigarrow} \begin{pmatrix} \mathbf{M}_f & \mathbf{J}_{2^n} \\ \mathbf{J}_{2^n} & \mathbf{O}_{2^n} \end{pmatrix} \overset{\text{(III)}}{\rightsquigarrow} \begin{pmatrix} \mathbf{M}_f & \mathbf{O}_{2^n} \\ \mathbf{O}_{2^n} & \mathbf{O}_{2^n} \end{pmatrix}$$

and hence $\Gamma\text{-rank}(f) = \mathrm{rank}(f)$. □

From the previous statement, one can see that Γ-rank of a non-constant Boolean function is an even number. Now we show that Γ-rank of any (n,m)-function is always even as well.

Proposition 3.5. *Let F be an (n,m)-function. Then* $\Gamma\text{-rank}(F)$ *is even.*

Proof. The $(\mathbf{x},\mathbf{y})$-th entry in the matrix $\mathbf{N}_F$ is 1 if and only if $\mathbf{x}\oplus\mathbf{y}\in\mathcal{G}_F$. In this way, $\mathbf{N}_F$ is symmetric. Without loss of generality we assume that $F(\mathbf{0})=\mathbf{0}$ (otherwise we consider $F := F\oplus F(\mathbf{0})$ and this transformation leaves Γ-rank invariant), then we conclude that $\mathbf{N}_F$ is symplectic. Finally, any symplectic matrix has even rank, see [75, p. 436]. □

3.2.3 The Smith normal form of bent functions

As a corollary of Theorem 3.4, the Smith normal form of a Boolean function can be computed in a more efficient way due to the following modification of the incidence matrix $\mathbf{M}_f$.

Corollary 3.6. *Let f be a Boolean function on $\mathbb{F}_2^n$. The Smith normal form of f is given by*

$$\mathrm{SNF}(f)=\{*d_1^{m_1},\ldots,d_k^{m_k},0^{2^n-1}*\},$$

where all d_i's are elementary divisors of the matrix $\begin{pmatrix}\mathbf{M}_f & \mathbf{j}_{2^n}^T\\ \mathbf{j}_{2^n} & 2\end{pmatrix}$.

Proof. Performing elementary row and column operations, as in the proof of Theorem 3.4, but over the ring $\mathbb{Z}$, one can bring the matrix $\mathbf{N}_f$ to the form

$$\mathbf{N}_f \rightsquigarrow \left(\begin{array}{c|c}\begin{matrix}\mathbf{M}_f & \mathbf{j}_{2^n}^T\\ \mathbf{j}_{2^n} & 2\end{matrix} & \mathbf{O}_{2^n+1,2^n-1}\\ \hline \mathbf{O}_{2^n-1,2^n+1} & \mathbf{O}_{2^n-1,2^n-1}\end{array}\right).$$

In this way, $\mathrm{SNF}(f)=\{*d_1^{m_1},\ldots,d_k^{m_k},0^{2^n-1}*\}$, where the d_i's are the elementary divisors of the matrix $\begin{pmatrix}\mathbf{M}_f & \mathbf{j}_{2^n}^T\\ \mathbf{j}_{2^n} & 2\end{pmatrix}$. □

In general, the Smith normal form of an (n,m)-function does not necessarily have a certain pattern. In order to specify the general shape of the Smith normal form of Boolean and vectorial bent functions, we give the following auxiliary statements.

Result 3.7. *[95, Lemma 1.1.4] The matrix*

$$(r-\lambda_1)\mathbf{I}_{\mu\nu}+(\lambda_1-\lambda_2)\mathbf{J}_\nu\otimes\mathbf{I}_\mu+\lambda_2\mathbf{J}_{\mu\nu} \tag{3.4}$$

has eigenvalues

- $r+\lambda_1(\nu-1)+\lambda_2(\mu\nu-\nu)$ *(multiplicity 1);*
- $r-\lambda_1$ *(multiplicity $\mu(\nu-1)$);*
- $r+\lambda_1(\nu-1)-\lambda_2\nu$ *(multiplicity $\mu-1$).*

Remark 3.8. *1.* In Definition 1.73, we considered (μ, ν, k, λ) divisible designs, which belong to a more general class of incidence structures called $(\mu, \nu, k, \lambda_1, \lambda_2)$ divisible designs. An incidence structure $D = (\mathcal{P}, \mathcal{B})$ is called a $(\mu, \nu, k, \lambda_1, \lambda_2)$ *divisible design*, if the point set $\mathcal{P}$ with $|\mathcal{P}| = v = \mu \cdot \nu$ elements is divided into μ *point classes* of size ν each, the block set $\mathcal{B}$ is a collection of k-subsets of $\mathcal{P}$ and the number of blocks containing any subset $\{p, q\} \subset \mathcal{P}$ depends on the relation between points p and q in the following way:

- If p and q are in the same point class, the subset $\{p, q\}$ is contained in λ_1 blocks.

- Otherwise it is contained in exactly λ_2 blocks.

In this way, a (μ, ν, k, λ) design in the sense of Definition 1.73 is a $(\mu, \nu, k, 0, \lambda)$ design.
2. For a $(\mu, \nu, k, \lambda_1, \lambda_2)$ divisible design D, there exists an incidence matrix $\mathbf{N}$, satisfying

$$\mathbf{N}^T\mathbf{N} = (r - \lambda_1)\mathbf{I}_{\mu\nu} + (\lambda_1 - \lambda_2)\mathbf{J}_\nu \otimes \mathbf{I}_\mu + \lambda_2\mathbf{J}_{\mu\nu}, \tag{3.5}$$

where k is the block size and r is the replication number. The value r can be determined from the equation $r(k-1) = \lambda_1(\nu - 1) + \lambda_2(\mu\nu - \nu)$. In this way, for a (μ, ν, k, λ) divisible design D, there exists an incidence matrix $\mathbf{N}$, which satisfies

$$\mathbf{N}^T\mathbf{N} = r\mathbf{I}_{\mu\nu} - \lambda\mathbf{J}_\nu \otimes \mathbf{I}_\mu + \lambda\mathbf{J}_{\mu\nu}, \tag{3.6}$$

where r satisfies $r(k-1) = \lambda_2(\mu\nu - \nu)$.

The following result gives a relation between elementary divisors and eigenvalues of a square matrix over a ring of algebraic integers.

Result 3.9. *[88, Theorem 6] Let the $n \times n$ matrix A have eigenvalues $\alpha_1, \cdots, \alpha_n$ and elementary divisors $d_1 | \cdots | d_n$. Then $d_1 \cdots d_k \mid \alpha_{i_1} \cdots \alpha_{i_k}$ whenever $1 \leqslant i_1 < \cdots < i_k \leqslant n, k = 1, \cdots, n-1$, and $d_1 \cdots d_n$ is an associate of $\alpha_1 \cdots \alpha_n$.*

With these results, the Smith normal form of an (n, m)-bent function F can be described in the following way.

Theorem 3.10. *Let F be an (n, m)-bent function and its Smith normal form be given by $\mathrm{SNF}(F) = \{*d_1^{l_1}, \ldots, d_k^{l_k}*\}$. Then the following hold.*

1. *All nonzero elementary divisors d_i in the $\mathrm{SNF}(F)$ are powers of two.*

2. *Γ-rank$(F) = l_1$, where l_1 is the multiplicity of one in the $\mathrm{SNF}(F)$.*

Proof. 1. Let $\mathrm{SNF}(F) = \{*d_1^{l_1}, \ldots, d_k^{l_k}*\}$ be the Smith normal form of the function F, i.e., $d_1 | d_2 | \ldots | d_{2^{n+m}}$ are the elementary divisors of an incidence matrix $\mathbf{N}_F$ satisfying (3.6), since $\mathrm{dev}(\mathcal{G}_F)$ is a $(2^n, 2^m, 2^n, 2^{n-m})$-divisible design. Let

$\alpha_1, \alpha_2, \ldots, \alpha_{2^{n+m}}$ be the eigenvalues of the matrix $\mathbf{N}_F$ and $\beta_1, \beta_2, \ldots, \beta_{2^{n+m}}$ be the eigenvalues an incidence matrix $\mathbf{N}_F^2$, which is equal to $\mathbf{N}_F^T\mathbf{N}_F$, since the matrix $\mathbf{N}_F$ is symmetric. By Result 3.7 and Remark 3.8, we have that the matrix $\mathbf{N}_F^T\mathbf{N}_F$ has eigenvalue 2^{2n} (multiplicity 1), 2^n (multiplicity $2^n(2^m-1)$) and 0 (multiplicity 2^n-1). By Result 3.9, for all $1 \leq i_1 < \cdots < i_k \leq 2^{n+m}$ and $k = 1, \ldots, 2^{n+m}-1$ the following relation between products of elementary divisors and eigenvalues of $\mathbf{N}_F$ holds $d_1 \cdots d_k \mid \alpha_{i_1} \cdots \alpha_{i_k}$. Moreover, we have $d_1 \cdots d_k \mid \alpha_{i_1}^2 \cdots \alpha_{i_k}^2$, since $\alpha_{i_1} \cdots \alpha_{i_k} \mid \alpha_{i_1}^2 \cdots \alpha_{i_k}^2$. From the following equation

$$\det(\mathbf{N}_F^2 - \alpha_i^2\mathbf{I}_{2^{n+m}}) = \det(\mathbf{N}_F - \alpha_i\mathbf{I}_{2^{n+m}}) \cdot \det(\mathbf{N}_F + \alpha_i\mathbf{I}_{2^{n+m}}),$$

we have that if $\pm\alpha_i$ is an eigenvalue of $\mathbf{N}_F$, then α_i^2 is an eigenvalue of $\mathbf{N}_F^2$. Suppose that the eigenvalue β_i of $\mathbf{N}_F^2 = \mathbf{N}_F^T\mathbf{N}_F$ is $\beta_i = \alpha_i^2$. In this way, for nonzero elementary divisors $d_1, \ldots, d_k$ we have $d_1 \cdots d_k \mid \beta_{i_1}^2 \cdots \beta_{i_k}^2 \mid 2^s$ for some s, and hence all nonzero d_i are powers of two.
2. By definition of Γ-rank(F), we have Γ-rank$(F) = \operatorname{rank}_{\mathbb{F}_2}(\mathbf{N}_F)$. By Remark 1.70, we have that $\operatorname{rank}_{\mathbb{F}_2}(\mathbf{N}_F)$ is the number of elementary divisors coprime with 2, which is given by l_1. In this way, we conclude that Γ-rank$(F) = l_1$. □

Remark 3.11. We computed SNF(f) for many Boolean bent functions of different degrees on $\mathbb{F}_2^n$ with $6 \leq n \leq 12$. Based on our numerical experiments, we observe the following kind of symmetry in the Smith normal form SNF(f) of a Boolean bent function f on $\mathbb{F}_2^n$:

1. SNF$(f) = \{*d_1^{m_1}, \ldots, d_n^{m_n}, 0^{2^n-1}*\}$, where all elementary divisors d_i are of the form $d_i = 2^{i-1}$ for $i = 1, \ldots, n$.

2. Multiplicities of elementary divisors m_i satisfy $m_n = 1$, $m_{n-1} = m_1 - 2$ and $m_{n/2-i} = m_{n/2+i}$ for $i = 1, \ldots, n/2-2$.

Conjecture 3.12. *The* SNF(f) *of a Boolean bent function f on $\mathbb{F}_2^n$ has the form, described in Remark 3.11.*

For examples of Smith normal forms of vectorial bent functions, we refer to Appendix A.3.

3.3 Translation designs of inequivalent Boolean and vectorial bent functions

In this section, we prove that isomorphism of translation designs dev$(\mathcal{G}_f)$ and dev$(\mathcal{G}_{f'})$ of Boolean bent functions $f, f' \colon \mathbb{F}_2^n \to \mathbb{F}_2$ is a coarser equivalence relation for Boolean bent functions than extended-affine equivalence. In the following proposition, we observe that from isomorphism of incidence structures dev$(\mathcal{D}_f)$ and dev$(\mathcal{D}_{f'})$ of Boolean (not necessarily bent) functions f, f' on $\mathbb{F}_2^n$ follows the isomorphism of incidence structures dev$(\mathcal{G}_f)$ and dev$(\mathcal{G}_{f'})$.

Proposition 3.13. *Let $f, f' \colon \mathbb{F}_2^n \to \mathbb{F}_2$ be two Boolean functions. If* $\operatorname{dev}(\mathcal{D}_f)$ *and* $\operatorname{dev}(\mathcal{D}_{f'})$ *are isomorphic, then* $\operatorname{dev}(\mathcal{G}_f)$ *and* $\operatorname{dev}(\mathcal{G}_{f'})$ *are isomorphic too.*

Proof. Since $\operatorname{dev}(\mathcal{D}_f)$ and $\operatorname{dev}(\mathcal{D}_{f'})$ are isomorphic, there exist permutation matrices $\mathbf{P}$ and $\mathbf{Q}$ such that $\mathbf{M}_f = \mathbf{P} \cdot \mathbf{M}_{f'} \cdot \mathbf{Q}$. Clearly, $\operatorname{dev}(\mathcal{D}_{\bar{f}})$ and $\operatorname{dev}(\mathcal{D}_{\bar{f}'})$ are isomorphic with the same permutation matrices $\mathbf{P}$ and $\mathbf{Q}$, as one can see from the following calculations

$$\mathbf{M}_{\bar{f}} = \mathbf{M}_f \oplus \mathbf{J}_{2^n} = \mathbf{P} \cdot \mathbf{M}_{f'} \cdot \mathbf{Q} \oplus \mathbf{J}_{2^n} = \mathbf{P} \cdot (\mathbf{M}_{f'} \oplus \mathbf{J}_{2^n}) \cdot \mathbf{Q} = \mathbf{P} \cdot \mathbf{M}_{\bar{f}'} \cdot \mathbf{Q}.$$

Let the incidence matrices $\mathbf{N}_f$ and $\mathbf{N}_{f'}$ of the incidence structures $\operatorname{dev}(\mathcal{G}_f)$ and $\operatorname{dev}(\mathcal{G}_{f'})$ be defined as in (3.1). Since $\mathbf{N}_f = (\mathbf{I}_2 \otimes \mathbf{P}) \cdot \mathbf{N}_{f'} \cdot (\mathbf{I}_2 \otimes \mathbf{Q})$, we conclude that $\operatorname{dev}(\mathcal{G}_f)$ and $\operatorname{dev}(\mathcal{G}_{f'})$ are isomorphic. □

Remark 3.14. The converse of the previous statement is not true in general. A simple argument supporting this observation, is that the incidence structure $\operatorname{dev}(\mathcal{D}_f)$ of a Boolean function f on $\mathbb{F}_2^n$ is invariant under affine equivalence [110], i.e., $f(\mathbf{x}) = f'(\mathbf{x}A \oplus \mathbf{b})$ for a non-degenerate $n \times n$ matrix A, but not extended-affine equivalence, see [63, Example 9.3.28]. In general, there are many examples of non-isomorphic translation designs $\operatorname{dev}(\mathcal{D}_f)$ and $\operatorname{dev}(\mathcal{D}_{f \oplus l})$, obtained by addition of an affine (and even linear) function l to a bent function f on $\mathbb{F}_2^n$.

Motivated by the fact that the incidence structure $\operatorname{dev}(\mathcal{G}_F)$ of an (n, m)-function F is invariant under CCZ-equivalence and, hence EA-equivalence, see Remark 1.76, we define isomorphic (n, m)-functions in the following way.

Definition 3.15. Two (n, m)-functions F, F' are called *isomorphic*, if the incidence structures $\operatorname{dev}(\mathcal{G}_F)$ and $\operatorname{dev}(\mathcal{G}_{F'})$ are isomorphic.

Example 3.16. Let f be a quadratic and f' be a cubic Maiorana-McFarland bent functions on $\mathbb{F}_2^6$, given by their ANFs

$$f(\mathbf{x}) = x_1x_2 \oplus x_3x_4 \oplus x_5x_6 \quad \text{and} \quad f'(\mathbf{x}) = x_1x_2 \oplus x_3x_4 \oplus x_5x_6 \oplus x_1x_3x_5.$$

Edel and Pott [53, Example 1] observed that the designs $\operatorname{dev}(\mathcal{D}_f)$ and $\operatorname{dev}(\mathcal{D}_{f'})$ are isomorphic. By Proposition 3.13, the divisible designs $\operatorname{dev}(\mathcal{G}_f)$ and $\operatorname{dev}(\mathcal{G}_{f'})$ are isomorphic too, and hence the functions f and f' are isomorphic in the sense of Definition 3.15.

Remark 3.17. With Magma [9], we checked that if two Boolean bent functions g and g' on $\mathbb{F}_2^6$ are EA-inequivalent but isomorphic, then g is EA-equivalent to f and g' is EA-equivalent to f', where f and f' are Boolean bent functions from Example 3.16.

In the following proposition, we show that using the direct sum construction one can always extend a pair of isomorphic incidence structures derived from Boolean and vectorial functions to an infinite family.

Proposition 3.18. *Let $f, f' \colon \mathbb{F}_2^n \to \mathbb{F}_2$ be two Boolean functions and let F, F' be two (n, m)-functions. Let also h be a Boolean function on $\mathbb{F}_2^k$ and H be a (k, m)-function.*

1. *If the incidence structures $\operatorname{dev}(\mathcal{D}_f)$ and $\operatorname{dev}(\mathcal{D}_{f'})$ are isomorphic, then the incidence structures $\operatorname{dev}(\mathcal{D}_{f\oplus h})$ and $\operatorname{dev}(\mathcal{D}_{f'\oplus h})$ of the direct sums $f \oplus h$ and $f' \oplus h$ on $\mathbb{F}_2^n \times \mathbb{F}_2^k$ are isomorphic too.*
2. *If the incidence structures $\operatorname{dev}(\mathcal{G}_F)$ and $\operatorname{dev}(\mathcal{G}_{F'})$ are isomorphic, then the incidence structures $\operatorname{dev}(\mathcal{G}_{F\oplus H})$ and $\operatorname{dev}(\mathcal{G}_{F'\oplus H})$ of the direct sums $F \oplus H$ and $F' \oplus H$, which are $(n + k, m)$-functions, are isomorphic too.*

Proof. We recall that $\oplus$ denotes the addition modulo 2 and $\otimes$ denotes the Kronecker product of two matrices.
1. Let $\mathbf{x}, \mathbf{y} \in \mathbb{F}_2^n$ and $\mathbf{w}, \mathbf{z} \in \mathbb{F}_2^k$. For any fixed $\mathbf{w}, \mathbf{z} \in \mathbb{F}_2^k$, the entry of the incidence matrix $\mathbf{M}_{f\oplus h}$ of $\operatorname{dev}(\mathcal{D}_{f\oplus h})$ labeled by $((\mathbf{x}, \mathbf{w}), (\mathbf{y}, \mathbf{z}))$ is $f(\mathbf{x} \oplus \mathbf{y}) \oplus h(\mathbf{w} \oplus \mathbf{z})$. In this way, the incidence matrix $\mathbf{M}_{f\oplus h}$ has the following form

$$\mathbf{M}_{f\oplus h} = (\mathbf{J}_{2^k} \otimes \mathbf{M}_f) \oplus (\mathbf{M}_h \otimes \mathbf{J}_{2^n}).$$

Since $\operatorname{dev}(\mathcal{D}_f)$ and $\operatorname{dev}(\mathcal{D}_{f'})$ are isomorphic, there exist permutation matrices $\mathbf{P}$ and $\mathbf{Q}$ such that $\mathbf{M}_f = \mathbf{P} \cdot \mathbf{M}_{f'} \cdot \mathbf{Q}$. Finally, from the following equation

$$\mathbf{M}_{f\oplus h} = (\mathbf{I}_{2^k} \otimes \mathbf{P}) \cdot \mathbf{M}_{f'\oplus h} \cdot (\mathbf{I}_{2^k} \otimes \mathbf{Q})$$

one can see that that incidence structures $\operatorname{dev}(\mathcal{D}_{f\oplus h})$ and $\operatorname{dev}(\mathcal{D}_{f'\oplus h})$ are isomorphic.
2. Let $\mathbf{a}, \mathbf{b} \in \mathbb{F}_2^n$, $\mathbf{c}, \mathbf{d} \in \mathbb{F}_2^k$ and $\mathbf{e}, \mathbf{f} \in \mathbb{F}_2^m$. The point $(\mathbf{a}, \mathbf{c}, \mathbf{e})$ is incident with the block $(\mathbf{b}, \mathbf{d}, \mathbf{f}) \oplus \mathcal{G}_{F\oplus H}$ of $\operatorname{dev}(\mathcal{G}_{F\oplus H})$ if and only if the point $(\mathbf{a}, \mathbf{e})$ is incident with the block $(\mathbf{b}, \mathbf{f} \oplus H(\mathbf{c} \oplus \mathbf{d})) \oplus \mathcal{G}_F$ of $\operatorname{dev}(\mathcal{G}_F)$. The statement now follows from the fact that for a block B the mapping $\rho : B \mapsto B \oplus (\mathbf{0}, H(\mathbf{c} \oplus \mathbf{d}))$ is an automorphism of the incidence structures $\operatorname{dev}(\mathcal{G}_F)$ and $\operatorname{dev}(\mathcal{G}_{F'})$, which are isomorphic. □

Now we show that isomorphism of divisible designs for Boolean bent functions is a coarser equivalence relation than extended-affine equivalence.

Theorem 3.19. *Boolean bent functions, which are extended-affine inequivalent but isomorphic exist on $\mathbb{F}_2^n$ for all $n \geq 6$.*

Proof. Let g be a quadratic bent function on $\mathbb{F}_2^k$ and let f and f' be bent functions from the Example 3.16. By Proposition 3.18 Boolean functions $f \oplus g$ and $f' \oplus g$ on $\mathbb{F}_2^n$ with $n = k + 6$ are isomorphic. Clearly, direct sums $f \oplus g$ and $f' \oplus g$ are bent, since all the functions f, f' and g are bent. Finally, since $\deg(f \oplus g) = 2$ and $\deg(f' \oplus g) = 3$, we get that functions $f \oplus g$ and $f' \oplus g$ are extended-affine inequivalent on $\mathbb{F}_2^n$. □

Remark 3.20. Extended-affine inequivalent Boolean bent functions f and f' on $\mathbb{F}_2^6$ from Example 3.16 define isomorphic designs $\operatorname{dev}(\mathcal{D}_f)$ and $\operatorname{dev}(\mathcal{D}_{f'})$ with a 2-transitive automorphism group. According to Kantor [62, Theorem 1], any 2-$(2^n, 2^{n-1}-2^{n/2-1}, 2^{n-2}-2^{n/2-1})$ design with a 2-transitive automorphism group is unique, up to isomorphism. In general, if a design has a large automorphism group, it is more likely that it can be represented by several inequivalent difference sets (bent functions) due to the large symmetry. In this way, one may think that the reason why functions from Example 3.16 have isomorphic translation designs is the 2-transitivity of the automorphism group. In the following example, we show that isomorphic translation designs $\operatorname{dev}(\mathcal{D}_f)$ and $\operatorname{dev}(\mathcal{D}_{f'})$ of EA-inequivalent bent functions f and f' do not necessarily need to have a 2-transitive automorphism group.

Example 3.21. Let f, f' be two Maiorana-McFarland bent functions on $\mathbb{F}_2^{10}$ given by their algebraic normal forms as follows:

$$\begin{aligned} f(\mathbf{x}) =& x_1x_6 \oplus x_2x_7 \oplus x_3x_8 \oplus x_4x_9 \oplus x_5x_{10} \oplus x_1x_2x_3x_4x_5, \\ f'(\mathbf{x}) =& f(\mathbf{x}) \oplus x_4 \oplus x_6 \oplus x_8 \oplus x_{10} \oplus x_1x_2 \oplus x_2x_3 \oplus x_1x_2x_3 \oplus \\ & x_2x_4x_5 \oplus x_1x_2x_4x_5 \oplus x_2x_3x_4x_5. \end{aligned}$$

With Magma [9], one can check that orders of the automorphism groups of bent functions f and f' are equal to

$$|\operatorname{Aut}(\mathcal{C}_f)| = 2^{30} \cdot 3^2 \cdot 5 \cdot 7 \cdot 31 \text{ and } |\operatorname{Aut}(\mathcal{C}_{f'})| = 2^{30} \cdot 3^2 \cdot 7,$$

what implies that functions f and f' are extended-affine inequivalent. However, the designs $\operatorname{dev}(\mathcal{D}_f)$ and $\operatorname{dev}(\mathcal{D}_{f'})$ are isomorphic. First, we observe that in general designs $\operatorname{dev}(\mathcal{D}_f)$ and $\operatorname{dev}(\mathcal{D}_{f'})$ are isomorphic if and only if there exist a pair of permutations $\rho, \sigma\colon \mathbb{F}_2^n \to \mathbb{F}_2^n$ such that $f(\rho(\mathbf{x}) \oplus \sigma(\mathbf{y})) = f'(\mathbf{x} \oplus \mathbf{y})$ holds for all $\mathbf{x}, \mathbf{y} \in \mathbb{F}_2^n$, since an incidence matrix $\mathbf{M}_f$ of the translation design $\operatorname{dev}(\mathcal{D}_f)$ can be computed as $\mathbf{M}_f := (f(\mathbf{x} \oplus \mathbf{y}))_{\mathbf{x},\mathbf{y} \in \mathbb{F}_2^n}$. It is easy to check that the following nonlinear functions $\rho, \sigma\colon \mathbb{F}_2^{10} \to \mathbb{F}_2^{10}$, given by algebraic normal forms

$$\begin{aligned} \rho(\mathbf{x}) =& (x_1, x_2, x_3, x_4, x_1 \oplus x_5, x_1 \oplus x_{10} \oplus x_2x_3 \oplus x_5 \oplus x_6, \\ & x_1x_3 \oplus x_7, x_1x_2 \oplus x_8, x_9, x_1 \oplus x_{10}), \\ \sigma(\mathbf{y}) =& \mathbf{y} \oplus (1, 0, 1, 0, y_1, y_1 \oplus y_{10} \oplus y_2 \oplus y_2y_3 \oplus y_5, \\ & y_1 \oplus y_3 \oplus y_1y_3, y_2 \oplus y_1y_2, 1, 1 \oplus y_1), \end{aligned}$$

are permutations and satisfy $f(\rho(\mathbf{x}) \oplus \sigma(\mathbf{y})) = f'(\mathbf{x} \oplus \mathbf{y})$ for all $\mathbf{x}, \mathbf{y} \in \mathbb{F}_2^{10}$. In this way, designs $\operatorname{dev}(\mathcal{D}_f)$ and $\operatorname{dev}(\mathcal{D}_{f'})$ are isomorphic. We also observe that the 2-rank of any 2-$(2^n, 2^{n-1}-2^{n/2-1}, 2^{n-2}-2^{n/2-1})$ design D with a 2-transitive automorphism group equals $n+2$: any such a design is unique, up to isomorphism [62], it can be constructed as $\operatorname{dev}(\mathcal{D}_g)$ of a quadratic bent function g on $\mathbb{F}_2^n$, and $\operatorname{rank}(g) = n+2$ as it was shown in [111, Corollary 3.8]. Since

f is a Maiorana-McFarland bent function of the form $\langle \mathbf{x}', \mathbf{x}'' \rangle_{n/2} \oplus h(\mathbf{y})$, where $\mathbf{x}', \mathbf{x}'' \in \mathbb{F}_2^{n/2}$ and h is a monomial function with $\deg(h) > 3$ on $\mathbb{F}_2^{n/2}$, we have $\operatorname{rank}(f) = n - 2\deg(h) + 2^{\deg(h)}$ by [111, Corollary 3.8]. In this way, we have

$$\operatorname{rank}(D) = 12 \text{ and } \operatorname{rank}(\operatorname{dev}(\mathcal{D}_f)) = \operatorname{rank}(\operatorname{dev}(\mathcal{D}_{f'})) = 32,$$

consequently, the automorphism groups of designs $\operatorname{dev}(\mathcal{D}_f)$ and $\operatorname{dev}(\mathcal{D}_{f'})$ are not 2-transitive.

From Example 3.16 and Remark 3.17, we know that on $\mathbb{F}_2^6$ there exist EA-inequivalent bent functions f and f', whose translation designs $\operatorname{dev}(\mathcal{G}_f)$ and $\operatorname{dev}(\mathcal{G}_f)$ are isomorphic. Surprisingly, in contrast to the Boolean case, one cannot observe the same phenomenon for EA-inequivalent vectorial bent functions in six variables.

Theorem 3.22. *Let F and F' be two $(6, m)$-bent functions with $m \geq 2$. The following statements are equivalent.*

1. *Bent functions F and F' are extended-affine equivalent.*
2. *Divisible designs $\operatorname{dev}(\mathcal{G}_F)$ and $\operatorname{dev}(\mathcal{G}_{F'})$ are isomorphic.*

Proof. All computations about equivalence and isomorphism are carried out with Magma [9]. Invariants of equivalence classes and their translation designs are listed in Table A.5. □

3.4 Equivalence of bent functions via isomorphism of addition designs

Dillon and Schatz [43] and Bending [5, Corollary 10.6] proved that Boolean bent functions f and f' on $\mathbb{F}_2^n$ are extended-affine equivalent if and only if their addition designs $\mathbb{D}(f)$ and $\mathbb{D}(f')$ are isomorphic. In this section, we show that, similarly to the Boolean case, vectorial (n, m)-bent functions F and F' are extended-affine equivalent if and only if their addition designs $\mathbb{D}(F)$ and $\mathbb{D}(F')$ are isomorphic. We also use the result of Bending [5, Theorem 9.6] to show, how one can construct an incidence matrix of the addition design of a vectorial (n, m)-bent function F with the help of its component functions and their duals.

Remark 3.23. The entries of an incidence matrix of the addition design $\mathbb{D}(F)$ of a vectorial (n, m)-bent function F, introduced in Definition 1.92, similarly to the Boolean case, can be constructed directly from the values of the component functions $F_{\mathbf{b}}$ and their duals $\tilde{F}_{\mathbf{b}}$. The *dual* of a Boolean bent function $f \colon \mathbb{F}_2^n \to \mathbb{F}_2$ is a bent function $\tilde{f} \colon \mathbb{F}_2^n \to \mathbb{F}_2$, which is defined by the Walsh transform of the function f in the following way: $\hat{\chi}_f(\mathbf{a}) = 2^{n/2}(-1)^{\tilde{f}(\mathbf{a})}$ holds for all $\mathbf{a} \in \mathbb{F}_2^n$.

Bending [5, Theorem 9.6] proved that an incidence matrix of the design $\mathbb{D}(f)$ can be constructed with the help of the dual function $\tilde{f}$ as follows (without loss of generality we assume that $f(\mathbf{0}) = 0$):

$$\mathbf{M}(\mathbb{D}(f)) = (a_{\mathbf{x},\mathbf{y}})_{\mathbf{x},\mathbf{y}\in\mathbb{F}_2^n}, \quad \text{where } a_{\mathbf{x},\mathbf{y}} = \tilde{f}(\mathbf{x}) \oplus f(\mathbf{y}) \oplus \langle \mathbf{x}, \mathbf{y}\rangle_n \oplus \tilde{f}(\mathbf{0}). \tag{3.7}$$

With this result, and the observation that an incidence matrix of the addition design $\mathbb{D}(F)$ of an (n, m)-bent function F (without loss of generality we assume $F(\mathbf{0}) = \mathbf{0}$) can be constructed as the concatenation of incidence matrices of addition designs $\mathbb{D}(F_\mathbf{b})$ of nonzero component functions $F_\mathbf{b}$ of F, we prove the following statement.

Proposition 3.24. *Let F be an (n, m)-bent function. Then an incidence matrix of the addition design $\mathbb{D}(F)$ can be constructed as follows*

$$\mathbf{M}(\mathbb{D}(F)) = \begin{bmatrix} \mathbf{M}(\mathbb{D}(F_{\mathbf{b}_1})) \\ \mathbf{M}(\mathbb{D}(F_{\mathbf{b}_2})) \\ \vdots \\ \mathbf{M}(\mathbb{D}(F_{\mathbf{b}_{2^m-1}})) \end{bmatrix}, \tag{3.8}$$

where the value $a_{\mathbf{x},\mathbf{y}}$ of the submatrix $\mathbf{M}(\mathbb{D}(F_{\mathbf{b}_i})) = (a_{\mathbf{x},\mathbf{y}})_{\mathbf{x},\mathbf{y}\in\mathbb{F}_2^n}$ for $i = 1, \ldots, 2^m - 1$ is given by $a_{\mathbf{x},\mathbf{y}} = \tilde{F}_{\mathbf{b}_i}(\mathbf{x}) \oplus F_{\mathbf{b}_i}(\mathbf{y}) \oplus \langle \mathbf{x}, \mathbf{y}\rangle_n \oplus \tilde{F}_{\mathbf{b}_i}(\mathbf{0})$.

Recently, Ding, Munemasa and Tonchev conjectured [44, Note 24] that extended-affine equivalence of vectorial bent functions, similarly to the Boolean case [5, 43], coincides with the isomorphism of their addition designs. In the following theorem, we show that this conjecture is true.

Theorem 3.25. *Let F and F' be two (n, m)-bent functions. Bent functions F and F' are extended-affine equivalent if and only if addition designs $\mathbb{D}(F)$ and $\mathbb{D}(F')$ are isomorphic.*

Proof. By Result 1.11, two (n, m)-bent functions F, F' are EA-equivalent if and only they are CCZ-equivalent. By Result 1.60, functions F and F' are CCZ-equivalent if and only if the linear codes $\mathcal{C}_F$ and $\mathcal{C}_{F'}$ are permutation equivalent. We observe that the $[2^n, 1 + n + m, 2^{n-1} - 2^{n/2-1}]$-linear code $\mathcal{C}_F$ is spanned by the set of codewords of minimum weight. First, for an element $\mathbf{a} \in \mathbb{F}_2^n$ we denote by $l_\mathbf{a}$ the affine function given by $l_{\mathbf{a},\epsilon}(\mathbf{x}) = \langle \mathbf{a}, \mathbf{y}\rangle_n \oplus \epsilon$. Since the (n, m)-bent function $F(\mathbf{x}) = (f_1(\mathbf{x}), \ldots, f_m(\mathbf{x}))^T$ is bent, we have that for any choice of $\mathbf{a}_i$ and ϵ_i for $i = 1, \ldots, m$, the subcode $S \subseteq \mathcal{C}_F$ given by $S = \{\mathbf{f}_1 \oplus \mathbf{l}_{\mathbf{a}_1,\epsilon_1}, \ldots, \mathbf{f}_m \oplus \mathbf{l}_{\mathbf{a}_m,\epsilon_m}\}$ satisfies $\dim\langle S\rangle = m$. Choosing affine functions $l_{\mathbf{a},\epsilon}(\mathbf{x})$ as in Proposition 3.24, we get that S is spanned by codewords of the minimum weight. The first-order Reed-Muller code $\mathcal{RM}(1, n)$ is also spanned by codewords of minimum weight of $\mathcal{C}_F$, since for a nonzero component function $F_\mathbf{b}$ of F, its addition design $\mathbb{D}(F_\mathbf{b})$ is formed by the minimum weight codewords in $\mathcal{C}_{F_\mathbf{b}}$, see [43]. In this way, the incidence matrix $\mathbf{M}(\mathbb{D}(F))$ of the addition design $\mathbb{D}(F)$ given in (3.8) is a generator matrix of the code $\mathcal{C}_F$, and hence, the linear codes $\mathcal{C}(F)$ and $\mathcal{C}(F')$ are equivalent if and only if the addition designs $\mathbb{D}(F)$ and $\mathbb{D}(F')$ are isomorphic. This completes the proof. □

3.5 Vanishing flats of bent functions

Vanishing flats $\mathcal{VF}(F)$ of (n,m)-bent functions F, being supports of codewords of weight 4 in the linear code $\mathcal{C}_F^{\perp}$, are 2-designs, as it was observed in [108, Example 4]. In this section, we explain the combinatorial structure of vanishing flats of bent functions and, consequently, compute the parameters of these designs, i.e., we show that vanishing flats $\mathcal{VF}(F)$ of (n,m)-bent functions F are 2-$(2^n, 4, 2^{n-m-1}-1)$ designs. Moreover, we show that this design-theoretic condition is also sufficient for the perfect nonlinearity. The key ingredient of the proof is the characterization of (n,m)-bent functions in terms of relative difference sets (see Result 1.53).

Theorem 3.26. *Let F be an (n,m)-function. The following statements are equivalent.*

1. *The function F is an (n,m)-bent function.*
2. *The incidence structure $\mathcal{VF}(F)$ is a 2-$(2^n, 4, 2^{n-m-1}-1)$ design.*

Proof. 1.⇒2. Let F be an (n,m)-bent function and let $\mathcal{VF}(F) = (\mathcal{P}, \mathcal{B})$ be the vanishing flats of F. We will show that any two different points $\mathbf{x}_1, \mathbf{x}_2$ of $\mathcal{P}$ are contained in exactly $2^{n-m-1}-1$ blocks of $\mathcal{B}$. We define $\mathbf{a} := \mathbf{x}_1 \oplus \mathbf{x}_2$ and let $\mathbf{v} := F(\mathbf{x}_1) \oplus F(\mathbf{x}_2)$. Since the graph $\mathcal{G}_F$ is a $(2^n, 2^m, 2^n, 2^{n-m})$-difference set in the group $G = \mathbb{F}_2^n \times \mathbb{F}_2^m$ relative to the forbidden subgroup $N = \{(\mathbf{0}, \mathbf{y}) \colon \mathbf{y} \in \mathbb{F}_2^m\}$, the element $g := \begin{pmatrix} \mathbf{a} \\ \mathbf{v} \end{pmatrix} \in G \setminus N$ has $2^{n-m}-2$ further representations

$$\begin{pmatrix} \mathbf{x}_1 \\ F(\mathbf{x}_1) \end{pmatrix} \oplus \begin{pmatrix} \mathbf{x}_2 \\ F(\mathbf{x}_2) \end{pmatrix} = g = \begin{pmatrix} \mathbf{x}_3 \\ F(\mathbf{x}_3) \end{pmatrix} \oplus \begin{pmatrix} \mathbf{x}_4 \\ F(\mathbf{x}_4) \end{pmatrix} \tag{3.9}$$

with $\{\mathbf{x}_3, \mathbf{x}_4\} \neq \{\mathbf{x}_1, \mathbf{x}_2\}$. In this way, any 2-subset $\{\mathbf{x}_1, \mathbf{x}_2\}$ is contained in exactly $2^{n-m-1}-1$ blocks $\{\mathbf{x}_1, \mathbf{x}_2, \mathbf{x}_3, \mathbf{x}_4\}$, satisfying

$$\begin{pmatrix} \mathbf{x}_1 \\ F(\mathbf{x}_1) \end{pmatrix} \oplus \begin{pmatrix} \mathbf{x}_2 \\ F(\mathbf{x}_2) \end{pmatrix} \oplus \begin{pmatrix} \mathbf{x}_3 \\ F(\mathbf{x}_3) \end{pmatrix} \oplus \begin{pmatrix} \mathbf{x}_4 \\ F(\mathbf{x}_4) \end{pmatrix} = \begin{pmatrix} \mathbf{0} \\ \mathbf{0} \end{pmatrix}, \tag{3.10}$$

consequently, the incidence structure $\mathcal{VF}(F)$ is a 2-$(2^n, 4, 2^{n-m-1}-1)$ design.
2.⇒1. Let the incidence structure $\mathcal{VF}(F)$ be a 2-$(2^n, 4, 2^{n-m-1}-1)$ design. By relation (1.36), the number of blocks b of a t-(v,k,λ) design is given by

$$b = \lambda \binom{v}{t} / \binom{k}{t}.$$

Since $\mathcal{VF}(F)$ is a 2-$(2^n, 4, 2^{n-m-1} - 1)$ design, the number of blocks of $\mathcal{VF}(F)$ is given by

$$|\mathcal{VF}_F| = \frac{(2^{n-m-1} - 1) \cdot 2^n \cdot (2^n - 1)}{12}.$$

Since blocks of $\mathcal{VF}(F)$ are in 1-to-1 correspondence with codewords of weight 4 in the linear code $\mathcal{C}_F^{\perp}$, we get that $A_4 = |\mathcal{VF}_F|$. Expanding the obtained value, we get

$$A_4 = |\mathcal{VF}_F| = \frac{1}{3}\left(2^{3n-m-3} - 2^{2n-m-3} - 2^{2n-2} + 2^{n-2}\right). \tag{3.11}$$

By Corollary 1.64, the value A_4 given in (3.11) is the minimum possible value for an (n, m)-function F with n even and $m \leq n/2$, which is attained if and only if F is an (n, m)-bent function. □

Remark 3.27. The proof of the previous statement gives a constructive combinatorial way to determine the number of vanishing flats $|\mathcal{VF}_F|$ of F as follows:

- there are $2^{n+m} - 2^m$ ways to pick an element $g \in G \setminus N$;
- for a selected element g there exist 2^{n-m} ways to choose the left-hand side in (3.9), what gives $2^{n-m} - 2$ remaining choices of the right-hand side;
- in this way, we have $(2^{n+m} - 2^m) \cdot 2^{n-m} \cdot (2^{n-m} - 2)$ "ordered" vanishing flats of F, i.e., quadruples $(\mathbf{x}_1, \mathbf{x}_2, \mathbf{x}_3, \mathbf{x}_4)$ with the property (3.10) .

Dividing this number by $4! = 24$, we get that the number of blocks of $\mathcal{VF}(F)$ is equal to

$$|\mathcal{VF}_F| = \frac{(2^{n+m} - 2^m) \cdot 2^{n-m} \cdot (2^{n-m} - 2)}{24}, \tag{3.12}$$

which after expanding and simplifying coincides with the value in (3.11).

As it was mentioned in Proposition 1.85, the incidence structure $\mathcal{VF}(F)$ is invariant under CCZ-equivalence for (n, m)-functions F. Conversely, two (n, m)-functions F, F' for which the vanishing flats $\mathcal{VF}(F)$ and $\mathcal{VF}(F')$ are isomorphic, are not necessarily CCZ-equivalent, as the case of APN functions shows, since the obtained incidence structures are trivial. However, according to our computational results, the converse is also true for $(6, m)$-bent functions.

Theorem 3.28. *Let F and F' be two $(6, m)$-bent functions. The following statements are equivalent.*

1. *Bent functions F and F' are extended-affine equivalent.*
2. *Vanishing flats $\mathcal{VF}(F)$ and $\mathcal{VF}(F')$ are isomorphic.*

Moreover, for any $(6, m)$-bent function F the linear code $\mathcal{C}_F^{\perp}$ is spanned by the codewords of minimum weight.

Proof. All computations about equivalence and isomorphism are carried out with Magma [9] using the representatives of the equivalence classes of $(6, m)$-bent functions, given in Appendix A.5. □

3.6 Nonvanishing flats of plateaued functions

In this section, we introduce a combinatorial generalization of vanishing flats by modifying the definition of the block set in (1.40). Consequently, we use this generalization in order to derive new characterizations of plateaued and bent functions.

3.6.1 Definition and invariance under EA-equivalence

First, we give a formal definition of nonvanishing flats and show that the collection of all nonvanishing flats of an (n,m)-function is invariant under EA-equivalence.

Definition 3.29. Let F be an (n,m)-function. We define a partial quadruple system, called the *nonvanishing flats of the (n,m)-function F with respect to the nonzero vector* $\mathbf{v} \in \mathbb{F}_2^m$, as the incidence structure $\mathcal{NF}_{\mathbf{v}}(F) := (\mathcal{P}, \mathcal{NF}_{\mathbf{v},F})$ where the point set is given by $\mathcal{P} = \{\mathbf{x} \colon \mathbf{x} \in \mathbb{F}_2^n\}$ and the block set $\mathcal{NF}_{\mathbf{v},F}$ is defined as follows

$$\mathcal{NF}_{\mathbf{v},F} = \left\{ \{\mathbf{x}_1, \mathbf{x}_2, \mathbf{x}_3, \mathbf{x}_4\} \colon \bigoplus_{i=1}^{4} \begin{pmatrix} \mathbf{x}_i \\ F(\mathbf{x}_i) \end{pmatrix} = \begin{pmatrix} \mathbf{0} \\ \mathbf{v} \end{pmatrix} \text{ for } \mathbf{x}_i \in \mathbb{F}_2^n \right\}. \tag{3.13}$$

Remark 3.30. For an arbitrary (n,m)-function F, the collection of incidence structures $\{\mathcal{VF}(F)\} \cup \{\mathcal{NF}_{\mathbf{v}}(F) \colon \mathbf{v} \in \mathbb{F}_2^m \setminus \{\mathbf{0}\}\}$ forms a partition of *the affine Steiner quadruple system $SQS(2^n) := (\mathcal{P}, \mathcal{B})$* with point and block sets being defined as follows

$$\mathcal{P} = \{\mathbf{x} \colon \mathbf{x} \in \mathbb{F}_2^n\} \quad \text{and} \quad \mathcal{B} = \{\{\mathbf{x}_1, \mathbf{x}_2, \mathbf{x}_3, \mathbf{x}_4\} \colon \mathbf{x}_1 \oplus \mathbf{x}_2 \oplus \mathbf{x}_3 \oplus \mathbf{x}_4 = \mathbf{0} \text{ for } \mathbf{x}_i \in \mathbb{F}_2^n\},$$

which is a 3-$(2^n, 4, 1)$ design.

As we mentioned in Proposition 1.85, the incidence structure $\mathcal{VF}(F)$ is invariant under CCZ-equivalence for (n,m)-functions. Now we show that the collection of all nonvanishing flats $\{\mathcal{NF}_{\mathbf{v}}(F) \colon \mathbf{v} \in \mathbb{F}_2^m \setminus \{\mathbf{0}\}\}$ is invariant under EA-equivalence for (n,m)-functions. First, we recall the following characterization of EA-equivalence for perfect nonlinear functions.

Result 3.31. *[54] Let F and F' be two (n,m)-functions. Then F and F' are extended-affine equivalent if and only if there exists an affine permutation $\mathcal{L}$ of $\mathbb{F}_2^n \times \mathbb{F}_2^m$ of the form*

$$\mathcal{L} \colon \begin{pmatrix} \mathbf{x} \\ \mathbf{y} \end{pmatrix} \mapsto \begin{pmatrix} \mathbf{A}_{11} & \mathbf{O} \\ \mathbf{A}_{21} & \mathbf{A}_{22} \end{pmatrix} \begin{pmatrix} \mathbf{x} \\ \mathbf{y} \end{pmatrix} \oplus \begin{pmatrix} \mathbf{a} \\ \mathbf{b} \end{pmatrix} \tag{3.14}$$

such that $\mathcal{L}(\mathcal{G}_F) = \mathcal{G}_{F'}$.

Following the original proof of the invariance of vanishing flats under CCZ-equivalence [73, Theorem II.1.] and using the mentioned characterization of EA-equivalence, we proof the following result.

Theorem 3.32. *Let F and F' be two EA-equivalent (n,m)-functions and let $\mathcal{L}$ be an affine permutation of $\mathbb{F}_2^n \times \mathbb{F}_2^m$ of the form* (3.14) *such that $\mathcal{L}(\mathcal{G}_F) = \mathcal{G}_{F'}$. Then for any nonzero $\mathbf{v} \in \mathbb{F}_2^m$ the block $\{\mathbf{x}_1, \mathbf{x}_2, \mathbf{x}_3, \mathbf{x}_4\} \in \mathcal{NF}_{\mathbf{v}}(F)$ if and only if the block $\{\mathbf{x}'_1, \mathbf{x}'_2, \mathbf{x}'_3, \mathbf{x}'_4\} \in \mathcal{NF}_{\mathbf{v}'}(F')$, where $\mathbf{x}'_i = \mathbf{A}_{11}\mathbf{x}_i \oplus \mathbf{c}$ and $\mathbf{v}' = \mathbf{A}_{22}\mathbf{v}$.*

Proof. Let $\{\mathbf{x}_1, \mathbf{x}_2, \mathbf{x}_3, \mathbf{x}_4\}$ be a block of $\mathcal{NF}_{\mathbf{v}}(F)$. Then the following holds

$$\begin{pmatrix} \mathbf{x}_1 \\ F(\mathbf{x}_1) \end{pmatrix} \oplus \begin{pmatrix} \mathbf{x}_2 \\ F(\mathbf{x}_2) \end{pmatrix} \oplus \begin{pmatrix} \mathbf{x}_3 \\ F(\mathbf{x}_3) \end{pmatrix} \oplus \begin{pmatrix} \mathbf{x}_4 \\ F(\mathbf{x}_4) \end{pmatrix} = \begin{pmatrix} \mathbf{0} \\ \mathbf{v} \end{pmatrix}.$$

Let π be a mapping from $\mathbb{F}_2^n$ to $\mathbb{F}_2^n$ such that $\pi(\mathbf{x}) = \mathbf{A}_{11}\mathbf{x} \oplus \mathbf{c}$. By definition of EA-equivalence, π induces a permutation on $\mathbb{F}_2^n$. Let also $\mathbf{x}'_i := \pi(\mathbf{x}_i)$ and $F'(\mathbf{x}'_i) = \mathbf{A}_{21}\mathbf{x}_i \oplus \mathbf{A}_{22}F(\mathbf{x}_i) \oplus \mathbf{b}$. We then have

$$\begin{pmatrix} \mathbf{x}'_1 \\ F'(\mathbf{x}'_1) \end{pmatrix} \oplus \begin{pmatrix} \mathbf{x}'_2 \\ F'(\mathbf{x}'_2) \end{pmatrix} \oplus \begin{pmatrix} \mathbf{x}'_3 \\ F'(\mathbf{x}'_3) \end{pmatrix} \oplus \begin{pmatrix} \mathbf{x}'_4 \\ F'(\mathbf{x}'_4) \end{pmatrix} = \begin{pmatrix} \mathbf{0} \\ \mathbf{A}_{22} \bigoplus_{i=1}^{4} F(\mathbf{x}_i) \end{pmatrix} = \begin{pmatrix} \mathbf{0} \\ \mathbf{v}' \end{pmatrix},$$

where $\mathbf{v}' := \mathbf{A}_{22}\mathbf{v}$. In this way, $\{\mathbf{x}'_1, \mathbf{x}'_2, \mathbf{x}'_3, \mathbf{x}'_4\}$ is a block of $\mathcal{NF}_{\mathbf{v}'}(F')$ and π induces an injective mapping, which maps blocks of $\mathcal{NF}_{\mathbf{v}}(F)$ to the blocks of $\mathcal{NF}_{\mathbf{v}'}(F')$. Let now $\{\mathbf{x}'_1, \mathbf{x}'_2, \mathbf{x}'_3, \mathbf{x}'_4\}$ be a block of $\mathcal{NF}_{\mathbf{v}'}(F')$. Clearly, the inverse of $\mathcal{L}$ has the form

$$\mathcal{L}^{-1}\colon \begin{pmatrix} \mathbf{x} \\ \mathbf{y} \end{pmatrix} \mapsto \begin{pmatrix} \mathbf{A}'_{11} & \mathbf{O} \\ \mathbf{A}'_{21} & \mathbf{A}'_{22} \end{pmatrix} \begin{pmatrix} \mathbf{x} \\ \mathbf{y} \end{pmatrix} \oplus \begin{pmatrix} \mathbf{a} \\ \mathbf{b} \end{pmatrix},$$

with $\mathbf{A}'_{11} = \mathbf{A}_{11}^{-1}, \mathbf{A}'_{21} = \mathbf{A}_{22}^{-1}\mathbf{A}_{21}\mathbf{A}_{11}$ and $\mathbf{A}'_{22} = \mathbf{A}_{22}^{-1}$. Let $\mathbf{x}_i \in \mathbb{F}_2^n$ be defined as follows $\mathbf{x}_i := \pi^{-1}(\mathbf{x}'_i) = \mathbf{A}_{11}^{-1}\mathbf{x}'_i \oplus \mathbf{a}$, and thus its image $F(\mathbf{x}_i)$ is given by $F(\mathbf{x}_i) = \mathbf{A}'_{21}\mathbf{x}'_i \oplus \mathbf{A}'_{22}F'(\mathbf{x}'_i) \oplus \mathbf{b}$. In this way, the following equation holds

$$\bigoplus_{i=1}^{4} \begin{pmatrix} \mathbf{x}_i \\ F(\mathbf{x}_i) \end{pmatrix} = \begin{pmatrix} \mathbf{0} \\ \mathbf{A}'_{22} \bigoplus_{i=1}^{4} F'(\mathbf{x}'_i) \end{pmatrix} = \begin{pmatrix} \mathbf{0} \\ \mathbf{A}'_{22}\mathbf{v}' \end{pmatrix} = \begin{pmatrix} \mathbf{0} \\ \mathbf{v} \end{pmatrix},$$

consequently, $\{\mathbf{x}_1, \mathbf{x}_2, \mathbf{x}_3, \mathbf{x}_4\}$ is a block of $\mathcal{NF}_{\mathbf{v}}(F)$. Hence, π induces a bijection between the block sets of $\mathcal{NF}_{\mathbf{v}}(F)$ and $\mathcal{NF}_{\mathbf{v}'}(F')$. Thus the incidence structures $\mathcal{NF}_{\mathbf{v}}(F)$ and $\mathcal{NF}_{\mathbf{v}'}(F')$ are isomorphic. □

Remark 3.33. In general, the collection of all nonvanishing flats is not a CCZ-invariant for (n,m)-functions, as the following example shows. We endow $\mathbb{F}_2^6$ with the structure of the finite field $(\mathbb{F}_{2^6}, +, \cdot)$ in such a way that the multiplicative group $\mathbb{F}_{2^6}^*$ is given by $\mathbb{F}_{2^6}^* = \langle a \rangle$, where a is a root of the primitive polynomial $p(x) = x^6 + x^4 + x^3 + x + 1$. Consider the following CCZ-equivalent but not EA-equivalent functions on $\mathbb{F}_{2^6}$: Kim's APN function D_5 on $\mathbb{F}_{2^6}$ from Table 2.1 and the Dillon's APN permutation F on $\mathbb{F}_{2^6}$ from [13], which is defined as follows. Let $w \in \mathbb{F}_{2^6}$ be defined as $w := a^{-2}$. Then the univariate representation of the APN permutation $F(x)$ is given by:

$$\begin{aligned} F(x) = {} & w^{45}x^{60} + w^{41}x^{58} + w^{43}x^{57} + w^{4}x^{56} + w^{50}x^{54} + w^{20}x^{53} + w^{45}x^{52} + w^{20}x^{51} \\ & + w^{23}x^{50} + w^{36}x^{49} + w^{56}x^{48} + w^{21}x^{46} + w^{5}x^{45} + w^{21}x^{44} + w^{28}x^{43} + w^{3}x^{42} \\ & + w^{59}x^{41} + w^{58}x^{40} + w^{57}x^{39} + w^{53}x^{38} + w^{37}x^{37} + w^{40}x^{36} + w^{18}x^{35} + w^{41}x^{34} \\ & + w^{54}x^{33} + w^{3}x^{32} + w^{49}x^{30} + w^{41}x^{29} + w^{42}x^{28} + w^{50}x^{27} + w^{53}x^{26} + w^{58}x^{25} \\ & + w^{9}x^{24} + x^{23} + w^{28}x^{22} + w^{3}x^{21} + w^{21}x^{20} + w^{52}x^{19} + w^{60}x^{17} + w^{59}x^{16} \\ & + w^{10}x^{15} + w^{42}x^{13} + w^{8}x^{12} + w^{35}x^{11} + w^{44}x^{10} + w^{45}x^{8} + w^{8}x^{7} + w^{61}x^{6} \\ & + w^{59}x^{5} + w^{20}x^{4} + w^{12}x^{3} + w^{37}x^{2} + w^{2}x. \end{aligned}$$

It is possible to check with a computer that for the Kim's APN function D_5 there exist:

- 42 elements $v \in \mathbb{F}_{2^6}$ such that $\mathcal{NF}_v(D_5)$ is a 1-$(64,4,9)$ design;
- 21 elements $v \in \mathbb{F}_{2^6}$ such that $\mathcal{NF}_v(D_5)$ is a 1-$(64,4,13)$ design.

On the other hand, among the nonvanishing flats of Dillon's APN permutation only 7 of them, namely $\mathcal{NF}_v(F)$ for $v \in V = \{1, a^7, a^8, a^{29}, a^{44}, a^{50}, a^{53}\}$, are 1-$(64,4,13)$ designs.

3.6.2 Characterization of plateaued functions

As it was mentioned in Theorem 3.26, (n,m)-bent functions are exactly those (n,m)-functions which have the minimum possible number of vanishing flats $|\mathcal{VF}_F|$. In this way, the property of the vanishing flats to be a 2-design is in some sense redundant with respect to the characterization of bentness. In the following, we will show that in contrast to the bent case, one indeed needs information about all nonvanishing flats in order to characterize the class of plateaued functions. First, we give a formula for the number of vanishing flats for an arbitrary plateaued (n,m)-function.

Remark 3.34. Let F be an (n,m)-plateaued function. For each nonzero $\mathbf{b} \in \mathbb{F}_2^m$ let $s_{\mathbf{b}}$ be an integer with $0 \leq s_{\mathbf{b}} \leq n$ such that the component function $F_{\mathbf{b}}$ is $s_{\mathbf{b}}$-plateaued. Then according to (1.33), the number of vanishing flats $|\mathcal{VF}_F|$ is given by

$$|\mathcal{VF}_F| = \frac{1}{3}\left(2^{3n-m-3} + 2^{2n-m-3}\sum_{\mathbf{b}\in\mathbb{F}_2^m\setminus\{\mathbf{0}\}} 2^{s_{\mathbf{b}}} - 3\cdot 2^{2n-3} + 2^{n-2}\right). \qquad (3.15)$$

In particular, if F is an s-plateaued (n,m)-function, then

$$|\mathcal{VF}_F| = \frac{1}{3}\left(2^{3n-m-3} + 2^{2n+s-3} - 2^{2n+s-m-3} - 3\cdot 2^{2n-3} + 2^{n-2}\right). \qquad (3.16)$$

However, this information, namely the number of vanishing flats $|\mathcal{VF}_F|$ is not enough to characterize the class of all plateaued functions, as it follows from [87, Section 5.2]. There exist infinite families of nonplateaued Boolean functions having the fourth power moments of the Walsh transform of plateaued functions and, hence, the same number of vanishing flats $|\mathcal{VF}_F|$, as one can see from Result 1.33. In this way, the same characterization in terms of the number of vanishing flats is no longer possible for (n,m)-plateaued functions.

In the following statements, we show that one has to analyze the combinatorial structure of nonvanishing flats of (n,m)-functions in order to characterize the plateauedness. First, we proceed with the Boolean case.

Theorem 3.35. *Let f be a Boolean function on $\mathbb{F}_2^n$. The following statements are equivalent.*

1. *The function f is s-plateaued.*
2. *The incidence structure $\mathcal{VF}(f)$ is a* 1-$\left(2^n, 4, \frac{2^{n+s-1}(2^{n-s}+1)-3\cdot 2^n+2}{6}\right)$ *design.*
3. *The incidence structure $\mathcal{NF}_1(f)$ is a* 1-$\left(2^n, 4, \frac{2^{n+s-1}(2^{n-s}-1)}{6}\right)$ *design.*

Proof. 1.⇒2. Let f be an s-plateaued Boolean function on $\mathbb{F}_2^n$. For $v \in \mathbb{F}_2$ and $\mathbf{x} \in \mathbb{F}_2^n$ we define the set

$$\mathfrak{N}_f(v,\mathbf{x}) = \{(\mathbf{a},\mathbf{b}) \in \mathbb{F}_2^n \times \mathbb{F}_2^n \colon D_{\mathbf{a},\mathbf{b}}f(\mathbf{x}) = v\}$$

and denote its cardinality by $N_f(v,\mathbf{x}) = |\mathfrak{N}_f(v,\mathbf{x})|$. A given point $\mathbf{x} \in \mathbb{F}_2^n$ is incident with the block $B = \{\mathbf{x}, \mathbf{x}\oplus\mathbf{a}, \mathbf{x}\oplus\mathbf{b}, \mathbf{x}\oplus\mathbf{a}\oplus\mathbf{b}\} \in \mathcal{VF}_F$ if and only if there exists a 2-dimensional vector subspace $\langle\mathbf{a},\mathbf{b}\rangle$ with $\mathbf{a},\mathbf{b} \in \mathbb{F}_2^n$ such that $D_{\mathbf{a},\mathbf{b}}f(\mathbf{x}) = 0$. In order to determine the number of such 2-dimensional vector subspaces, it is enough to exclude from the set $\mathfrak{N}_f(0,\mathbf{x})$ the pairs $(\mathbf{a},\mathbf{0})$, $(\mathbf{0},\mathbf{b})$ and $(\mathbf{a},\mathbf{a})$, which do not correspond to the affine two-dimensional vector spaces, and divide the cardinality of the obtained set by 6, since any 2-dimensional vector subspace $\langle\mathbf{a},\mathbf{b}\rangle$ can be represented by 6 different pairs $(\mathbf{a},\mathbf{b})$ with $\mathbf{a},\mathbf{b} \in \mathbb{F}_2^n$. In this way, any point $\mathbf{x} \in \mathbb{F}_2^n$ is incident with exactly

$$\lambda_0 = \frac{N_f(0,\mathbf{x}) - (2\cdot(2^n-1)+2^n)}{6} \tag{3.17}$$

blocks of $\mathcal{VF}(f)$. By Result 1.15, we have that for an arbitrary Boolean function f on $\mathbb{F}_2^n$ the value $N_f(0,\mathbf{x})$ for $\mathbf{x} \in \mathbb{F}_2^n$ can be computed in the following way

$$N_f(0,\mathbf{x}) = \frac{1}{2}\left(\sum_{u\in\mathbb{F}_2}\sum_{\mathbf{a},\mathbf{b}\in\mathbb{F}_2^n}(-1)^{u\cdot D_{\mathbf{a},\mathbf{b}}f(\mathbf{x})}\right) = \frac{1}{2}\left(2^{2n} + \sum_{\mathbf{a},\mathbf{b}\in\mathbb{F}_2^n}(-1)^{D_{\mathbf{a},\mathbf{b}}f(\mathbf{x})}\right). \tag{3.18}$$

By Result 1.14, the function f on $\mathbb{F}_2^n$ is s-plateaued if and only if for all $\mathbf{x} \in \mathbb{F}_2^n$ holds

$$\sum_{\mathbf{a},\mathbf{b} \in \mathbb{F}_2^n} (-1)^{D_{\mathbf{a},\mathbf{b}} f(\mathbf{x})} = 2^{n+s}. \tag{3.19}$$

In this way, from (3.18) and (3.19) we deduce that for an s-plateaued Boolean function f on $\mathbb{F}_2^n$ the value $N_f(0, \mathbf{x})$ for all $\mathbf{x} \in \mathbb{F}_2^n$ is given by

$$N_f(0, \mathbf{x}) = 2^{n-1}(2^n + 2^s), \tag{3.20}$$

and hence any point $\mathbf{x} \in \mathbb{F}_2^n$ is incident with exactly

$$\lambda_0 = \frac{2^{n-1}(2^n + 2^s) - 3 \cdot 2^n + 2}{6} \tag{3.21}$$

blocks of $B \in \mathcal{VF}_F$, or equivalently the incidence structure $\mathcal{VF}(f)$ is a 1-$(2^n, 4, \lambda_0)$ design, with λ_0 being defined in (3.21).

2.⇒3. Let the incidence structure $\mathcal{VF}(f)$ be a 1-$(2^n, 4, \lambda_0)$ design with the covalency $\lambda_0 = (2^{n+s-1}(2^{n-s} + 1) - 3 \cdot 2^n + 2)/6$. Then any point $\mathbf{x} \in \mathbb{F}_2^n$ is incident with exactly λ_0 blocks of the form $B = \mathbf{x} \oplus \langle \mathbf{a}, \mathbf{b} \rangle \in \mathcal{VF}_F$, where $\langle \mathbf{a}, \mathbf{b} \rangle$ is a 2-dimensional vector subspace of $\mathbb{F}_2^n$ such that $D_{\mathbf{a},\mathbf{b}} f(\mathbf{x}) = 0$. In this way, for the remaining

$$\lambda_1 := \frac{(2^n - 1) \cdot (2^n - 2)}{6} - \lambda_0 = \frac{2^{n-1}(2^n - 2^s)}{6} \tag{3.22}$$

2-dimensional vector subspaces $\langle \mathbf{a}', \mathbf{b}' \rangle$ of $\mathbb{F}_2^n$, the second-order derivative satisfies $D_{\mathbf{a}',\mathbf{b}'} f(\mathbf{x}) = 1$. Equivalently, the incidence structure $\mathcal{NF}_1(f)$ is a 1-$(2^n, 4, \lambda_1)$ design, with λ_1 being defined in (3.22).

3.⇒1. Now we reverse the arguments used in the proofs of the previous two claims. Since the incidence structure $\mathcal{NF}_1(f)$ is a 1-$(2^n, 4, \lambda_1)$ design, with λ_1 being defined in (3.22), then the incidence structure $\mathcal{VF}(f)$ is a 1-$(2^n, 4, \lambda_0)$ design, with λ_0 being defined in (3.21). Substituting λ_0 into the equation (3.17), we get $N_f(0, \mathbf{x}) = 2^{n-1}(2^n + 2^s)$. From equation (3.18), we get

$$\sum_{\mathbf{a},\mathbf{b} \in \mathbb{F}_2^n} (-1)^{D_{\mathbf{a},\mathbf{b}} f(\mathbf{x})} = 2N_f(0, \mathbf{x}) - 2^{2n} = 2^{n+s}.$$

By Result 1.14, we have that the function f on $\mathbb{F}_2^n$ is s-plateaued. □

In the following statement, we characterize plateaued (n, m)-functions F as those (n, m)-functions, for which the collection of nonvanishing and vanishing flats $\{\mathcal{NF}_{\mathbf{v}}(F) \colon \mathbf{v} \in \mathbb{F}_2^n \setminus \{\mathbf{0}\}\} \sqcup \{\mathcal{VF}(F)\}$ is a partition of the affine Steiner quadruple system into 1-designs. First, similarly to the Boolean case, for an (n, m)-function F and fixed elements $\mathbf{v} \in \mathbb{F}_2^m$ and $\mathbf{x} \in \mathbb{F}_2^n$ we define the set

$$\mathfrak{N}_F(\mathbf{v}, \mathbf{x}) = \{(\mathbf{a}, \mathbf{b}) \in \mathbb{F}_2^n \times \mathbb{F}_2^n \colon D_{\mathbf{a},\mathbf{b}} F(\mathbf{x}) = \mathbf{v}\}$$

and denote its cardinality by $N_F(\mathbf{v}, \mathbf{x}) = |\mathfrak{N}_F(\mathbf{v}, \mathbf{x})|$.

Theorem 3.36. *Let F be an (n,m)-function and let for $\mathbf{v} \in \mathbb{F}_2^m$ the values $\lambda_{\mathbf{v}} \in \mathbb{N}$ be defined in the following way:*

$$\lambda_{\mathbf{0}} = \frac{N_F(\mathbf{0},\mathbf{x}) - 3 \cdot 2^n + 2}{6} \quad \text{and} \quad \lambda_{\mathbf{v}} = \frac{N_F(\mathbf{v},\mathbf{x})}{6} \quad \text{for } \mathbf{v} \in \mathbb{F}_2^m \setminus \{\mathbf{0}\}. \tag{3.23}$$

Then the following statements are equivalent.

1. *The function F is plateaued.*
2. *For all $\mathbf{v} \in \mathbb{F}_2^m \setminus \{\mathbf{0}\}$ the incidence structure $\mathcal{NF}_{\mathbf{v}}(F)$ is a 1-$(2^n,4,\lambda_{\mathbf{v}})$ design.*

Moreover, if an (n,m)-function F is plateaued, then the incidence structure $\mathcal{VF}(F)$ is a 1-$(2^n,4,\lambda_{\mathbf{0}})$ design.

Proof. 1.⇒2. Let F be (n,m)-plateaued. For a nonzero $\mathbf{v} \in \mathbb{F}_2^m$, a given point $\mathbf{x} \in \mathbb{F}_2^n$ is incident with the block $B = \{\mathbf{x}, \mathbf{x} \oplus \mathbf{a}, \mathbf{x} \oplus \mathbf{b}, \mathbf{x} \oplus \mathbf{a} \oplus \mathbf{b}\} \in \mathcal{NF}_{\mathbf{v},F}$ if and only if there exists a 2-dimensional vector subspace $\langle \mathbf{a}, \mathbf{b} \rangle$ with $\mathbf{a}, \mathbf{b} \in \mathbb{F}_2^n$ such that $D_{\mathbf{a},\mathbf{b}}F(\mathbf{x}) = \mathbf{v}$. In order to determine the number of such 2-dimensional vector subspaces, we divide the cardinality of the set $\mathfrak{N}_F(\mathbf{v},\mathbf{x})$ by 6, since any 2-dimensional vector subspace $\langle \mathbf{a}, \mathbf{b} \rangle$ can be represented by 6 different pairs $(\mathbf{a}, \mathbf{b})$ with $\mathbf{a}, \mathbf{b} \in \mathbb{F}_2^n$. In this way, any point $\mathbf{x} \in \mathbb{F}_2^n$ is incident with exactly

$$\lambda_{\mathbf{v}} = \frac{N_F(\mathbf{v},\mathbf{x})}{6} \tag{3.24}$$

blocks of $\mathcal{NF}_{\mathbf{v}}(F)$. Since the function F is plateaued, we have by Result 1.15 that for every $\mathbf{v} \in \mathbb{F}_2^m$ the number $N_F(\mathbf{v},\mathbf{x})$ does not depend on $\mathbf{x} \in \mathbb{F}_2^n$. In this way, for all $\mathbf{v} \in \mathbb{F}_2^m \setminus \{\mathbf{0}\}$ the incidence structure $\mathcal{NF}_{\mathbf{v}}(F)$ is a 1-$(2^n,4,\lambda_{\mathbf{v}})$ design, where $\lambda_{\mathbf{v}}$ is defined in (3.24).
2.⇒1. We show that regularity of all nonvanishing flats implies the regularity of vanishing flats and, consequently, the plateauedness of the (n,m)-function F. Assume that for all $\mathbf{v} \in \mathbb{F}_2^m \setminus \{\mathbf{0}\}$ the incidence structure $\mathcal{NF}_{\mathbf{v}}(F)$ is a 1-$(2^n,4,\lambda_{\mathbf{v}})$ design, where $\lambda_{\mathbf{v}}$ is defined in (3.23). Then by (3.24) for all $\mathbf{v} \in \mathbb{F}_2^m \setminus \{\mathbf{0}\}$ we have $N_F(\mathbf{v},\mathbf{x}) = 6\lambda_{\mathbf{v}}$, and hence $N_F(\mathbf{v},\mathbf{x})$ is independent on $\mathbf{x} \in \mathbb{F}_2^n$. Now we show that $N_F(\mathbf{0},\mathbf{x})$ is independent on $\mathbf{x} \in \mathbb{F}_2^n$ as well. Since the collection of nonvanishing and vanishing flats $\{\mathcal{NF}_{\mathbf{v}}(F) \colon \mathbf{v} \in \mathbb{F}_2^n \setminus \{\mathbf{0}\}\} \sqcup \{\mathcal{VF}(F)\}$ is a partition of the affine Steiner quadruple system $SQS(2^n)$, any point $\mathbf{x} \in \mathbb{F}_2^n$ is incident with exactly

$$\lambda_{\mathbf{0}} = \frac{(2^n-1)\cdot(2^n-2)}{6} - \sum_{\mathbf{v} \in \mathbb{F}_2^m \setminus \{\mathbf{0}\}} \lambda_{\mathbf{v}} \tag{3.25}$$

blocks of $\mathcal{NF}_{\mathbf{v}}(F)$. In this way, the incidence structure $\mathcal{VF}(F)$ is a 1-$(2^n,4,\lambda_{\mathbf{0}})$ design. Counting the value $\lambda_{\mathbf{0}}$ as in the proof of Theorem 3.35, we get

$$\lambda_{\mathbf{0}} = \frac{N_F(\mathbf{0},\mathbf{x}) - 3 \cdot 2^n + 2}{6} \quad . \tag{3.26}$$

From equations (3.25) and (3.25), we conclude that $N_F(\mathbf{0},\mathbf{x})$ is independent on $\mathbf{x} \in \mathbb{F}_2^n$. Since for every $\mathbf{v} \in \mathbb{F}_2^m$ the number $N_F(\mathbf{v},\mathbf{x})$ does not depend on $\mathbf{x} \in \mathbb{F}_2^n$, the function F is (n,m)-plateaued by Result 1.7. □

Remark 3.37. For an (n,m)-function F, with the following expression of $N_F(\mathbf{v},\mathbf{x})$ for any $\mathbf{x} \in \mathbb{F}_2^n, \mathbf{v} \in \mathbb{F}_2^m$ by means of the second-order derivatives of the component functions from Result 1.15

$$N_F(\mathbf{v},\mathbf{x}) = 2^{-m} \cdot \sum_{\mathbf{u} \in \mathbb{F}_2^m} (-1)^{\langle \mathbf{u},\mathbf{v} \rangle_m} \cdot \left(\sum_{\mathbf{a},\mathbf{b} \in \mathbb{F}_2^n} (-1)^{D_{\mathbf{a},\mathbf{b}} F_{\mathbf{u}}(\mathbf{x})} \right), \tag{3.27}$$

we make the following observations on the vanishing and nonvanishing flats of plateaued (n,m)-functions F.

1. For the incidence structure $\mathcal{VF}(F)$, which is a 1-$(2^n,4,\lambda_{\mathbf{0}})$ design, the value $\lambda_{\mathbf{0}}$ is determined by the distribution of the component functions $F_{\mathbf{u}}$ of F. Denoting by $p_s(F) = |\{F_{\mathbf{u}} \colon F_{\mathbf{u}} \text{ is } s\text{-plateaued}\}|$ the number of s-plateaued components of the function F, we compute from (3.23) and (3.27) the covalency of the vanishing flats as follows

$$\lambda_{\mathbf{0}} = \frac{\sum_{s=0}^{n} p_s(F) 2^{n+s-m} - 3 \cdot 2^n + 2}{6}. \tag{3.28}$$

2. In general, for the incidence structures $\mathcal{VF}_{\mathbf{v}}(F)$, which are 1-$(2^n,4,\lambda_{\mathbf{v}})$ designs for $\mathbf{v} \in \mathbb{F}_2^m \setminus \{\mathbf{0}\}$, the value $\lambda_{\mathbf{v}}$ is not determined by the distribution of the component functions $F_{\mathbf{u}}$ of F, as the following example shows.

Example 3.38. Consider the quadratic (and hence plateaued) APN functions D_i on $\mathbb{F}_{2^6}$ from Table 2.1. The functions D_i with $i \in C = \{1,\dots,13\} \setminus \{7\}$ have the classical Walsh spectrum, since $2/3$ of their nonzero components are bent, and $1/3$ are semi-bent. In this way, for any D_i with $i \in C$, we have $p_0(D_i) = 42, p_2(D_i) = 21$ and $p_6(D_i) = 1$. The Walsh spectrum of the function D_7 is nonclassical: the distribution of component functions of D_7 is given by $p_0(D_7) = 46, p_2(D_7) = 16$, $p_4(D_7) = 1$ and $p_6(D_7) = 1$. Below we give the multisets $C(D_i) := \{\!*\ \lambda_{\mathbf{v}} \colon \lambda_{\mathbf{v}} \text{ is a covalency of } \mathcal{NF}_{\mathbf{v}}(D_i)\ *\!\}$ containing the covalencies of all nonvanishing flats for quadratic APN functions D_i on $\mathbb{F}_{2^6}$.

Functions D_i	Multisets $C(D_i)$
D_1, D_2, D_4, D_5	$\{* \ 9^{42}, 13^{21} \ *\}$
$D_3, D_6, D_8,$ D_9, D_{10}, D_{13}	$\{* \ 5^1, 7^5, 9^{20}, 11^{26}, 13^{10}, 15^1 \ *\}$
D_{11}, D_{12}	$\{* \ 7^6, 9^{22}, 11^{24}, 13^9, 15^2 \ *\}$
D_7	$\{* \ 5^6, 7^{10}, 9^{10}, 11^{16}, 13^{15}, 15^6 \ *\}$

For example, for the function D_1 there exists 42 elements $v \in \mathbb{F}_{2^6}^*$ such that $\mathcal{NF}_v(D_1)$ is a 1-$(64,4,9)$ design and 21 elements $v \in \mathbb{F}_{2^6}^*$ such that $\mathcal{NF}_v(D_1)$ is a 1-$(64,4,13)$ design. In this way, we conclude that (n,m)-plateaued functions with the same distribution of component functions may have different collections of nonvanishing flats.

In general, it seems to be a difficult problem to compute the covalencies $\lambda_{\mathbf{v}}$ of the nonvanishing flats $\mathcal{NF}_{\mathbf{v}}(F)$ of a given plateaued (n,m)-function F explicitly. From Theorem 3.36, for $\mathbf{v} \in \mathbb{F}_2^m \setminus \{\mathbf{0}\}$ we have $\lambda_{\mathbf{v}} = N_F(\mathbf{v},\mathbf{x})/6$, where $N_F(\mathbf{v},\mathbf{x})$ is the number of solutions $(\mathbf{a},\mathbf{b}) \in \mathbb{F}_2^n \times \mathbb{F}_2^n$ of the equation $D_{\mathbf{a},\mathbf{b}}F(\mathbf{x}) = \mathbf{v}$. With this expression of the covalency, it may be possible to compute the numbers $N_F(\mathbf{v},\mathbf{x})$, provided that the algebraic representation of F is not too complicated.

Example 3.39. Consider Gold APN functions $F(x) = x^{2^i+1}$ on $\mathbb{F}_{2^n}$ with n even and $\gcd(i,n) = 1$, which are quadratic and hence plateaued. Carlet [28] determined the values $N_F(v,x)$ for Gold APN functions for all $x, v \in \mathbb{F}_{2^n}$. For all $x \in \mathbb{F}_{2^n}$, their values are equal to: $3 \cdot 2^n - 2$ for $v = 0$, $2^n + 2^{n/2+1} - 2$ for v being a nonzero cube (there are $(2^n-1)/3$ such elements) and $2^n - 2^{n/2} - 2$ for v being a non-cube (there are $2 \cdot (2^n-1)/3$ such elements). With these values, the nonvanishing flats $\mathcal{NF}_v(F)$ of Gold APN functions are 1-$(2^n, 4, \mathcal{NF}_v(F)/6)$ designs.

In the following result, we show that for (n,m)-plateaued functions with a single amplitude it is also possible to establish the covalency for nonvanishing flats.

Theorem 3.40. *Let F be an (n,m)-function. The following statements are equivalent.*

1. *The function F is s-plateaued.*
2. *For all $\mathbf{v} \in \mathbb{F}_2^m \setminus \{\mathbf{0}\}$ the incidence structure $\mathcal{NF}_{\mathbf{v}}(F)$ is a*
$$1\text{-}\left(2^n, 4, \frac{2^{n+s-m}(2^{n-s}-1)}{6}\right)$$
design.

Moreover, the vanishing flats $\mathcal{VF}(F)$ of an s-plateaued (n,m)-function F is a
$$1\text{-}\left(2^n, 4, \frac{2^{n+s-m}(2^{n-s}+2^m-1) - 3 \cdot 2^n + 2}{6}\right)$$
design.

Proof. The proof of this statement follows from Theorem 3.36. First, using the expression of $N_F(\mathbf{x},\mathbf{v})$ by means of the second-order derivatives of component functions of F given in (3.27), we compute $N_F(\mathbf{0},\mathbf{v}) = 2^{n+s-m}(2^{n-s} + 2^m - 1)$, which after the substitution into (3.23) gives the following value of covalency $\lambda_{\mathbf{0}} = \left(2^{n+s-m}(2^{n-s} + 2^m - 1) - 3 \cdot 2^n + 2\right)/6$. Since vanishing and nonvanishing flats form a partition of the affine Steiner quadruple system $SQS(2^n)$, we have that any $\lambda_{\mathbf{v}}$ for $\mathbf{v} \in \mathbb{F}_2^m \setminus \{\mathbf{0}\}$ satisfies $(2^m - 1) \cdot \lambda_{\mathbf{v}} = (2^n-1) \cdot (2^n-2)/6 - \lambda_{\mathbf{0}}$. With the obtained value $\lambda_{\mathbf{0}}$, we then have $\lambda_{\mathbf{v}} = 2^{n+s-m} \cdot (2^{n-s}-1)/6$ for all $\mathbf{v} \in \mathbb{F}_2^m \setminus \{\mathbf{0}\}$. □

Group ring interpretation. As we mentioned in Subsection 1.2.1, (n,m)-bent functions, s-plateaued (n,n)-functions and APN functions F can be characterized in terms of group ring equations, which their graph $\mathcal{G}_F$ has to satisfy. Now we prove a similar characterization for the class of (n,m)-plateaued functions and in particular for s-plateaued (n,m)-functions.

Theorem 3.41. *An (n,m)-function F is plateaued if and only if its graph $\mathcal{G}_F$ satisfies the following group ring equation*

$$\mathcal{G}_F^3 = \sum_{\mathbf{v}\in\mathbb{F}_2^m} N_F(\mathbf{v},\mathbf{x}) \cdot \left[\mathcal{G}_F \oplus \begin{pmatrix}\mathbf{0}\\ \mathbf{v}\end{pmatrix}\right].$$

In particular, an (n,m)-function F is s-plateaued if and only if its graph $\mathcal{G}_F$ satisfies the following group ring equation,

$$\mathcal{G}_F^3 = 2^{n+s}\cdot\mathcal{G}_F + (2^{2n-m} - 2^{n+s-m})\cdot G,$$

where $G = \mathbb{F}_2^n \times \mathbb{F}_2^m$.

Proof. Let $\mathbf{x} \in \mathbb{F}_2^n$ and $\mathbf{y} \in \mathbb{F}_2^m$ be two fixed elements. Consider the following system of equations

$$\begin{cases} \mathbf{x}_1 \oplus \mathbf{x}_2 \oplus \mathbf{x}_3 = \mathbf{x} \\ F(\mathbf{x}_1) \oplus F(\mathbf{x}_2) \oplus F(\mathbf{x}_3) = \mathbf{y} \end{cases},$$

which is equivalent to the system of equations

$$\begin{cases} \mathbf{x}_1 \oplus \mathbf{x}_2 \oplus \mathbf{x}_3 \oplus \mathbf{x} = \mathbf{0} \\ F(\mathbf{x}_1) \oplus F(\mathbf{x}_2) \oplus F(\mathbf{x}_3) \oplus F(\mathbf{x}) = \mathbf{v} \end{cases},$$

where $\mathbf{v} := F(\mathbf{x}) \oplus \mathbf{y}$. In this way, for an arbitrary (n,m)-function F, we have

$$\mathcal{G}_F^3 = \sum_{\mathbf{v}\in\mathbb{F}_2^m}\sum_{\mathbf{x}\in\mathbb{F}_2^n} \left[N_F(\mathbf{v},\mathbf{x}) \cdot \begin{pmatrix}\mathbf{x}\\ F(\mathbf{x})\oplus\mathbf{v}\end{pmatrix}\right].$$

By Result 1.15, for an (n,m)-function F the values $N_F(\mathbf{v},\mathbf{x})$ are independent of $\mathbf{x} \in \mathbb{F}_2^n$ for all $\mathbf{v} \in \mathbb{F}_2^m$ if and only if the function F is plateaued. In this way, the graph $\mathcal{G}_F$ satisfies the group ring equation

$$\mathcal{G}_F^3 = \sum_{\mathbf{v}\in\mathbb{F}_2^m} N_F(\mathbf{v},\mathbf{x}) \cdot \left[\sum_{\mathbf{x}\in\mathbb{F}_2^n}\begin{pmatrix}\mathbf{x}\\ F(\mathbf{x})\end{pmatrix} \oplus \begin{pmatrix}\mathbf{0}\\ \mathbf{v}\end{pmatrix}\right] \tag{3.29}$$

$$= \sum_{\mathbf{v}\in\mathbb{F}_2^m} N_F(\mathbf{v},\mathbf{x}) \cdot \left[\mathcal{G}_F \oplus \begin{pmatrix}\mathbf{0}\\ \mathbf{v}\end{pmatrix}\right]. \tag{3.30}$$

if and only if the function F is (n,m)-plateaued. Now we proceed with the case when F is s-plateaued. By Theorem 3.40, we have that the (n,m)-function

F is s-plateaued if and only if $N_F(\mathbf{0},\mathbf{v}) = 2^{n+s-m}(2^{n-s}+2^m-1)$ and for all $\mathbf{v} \in \mathbb{F}_2^m \setminus \{\mathbf{0}\}$ holds $N_F(\mathbf{x},\mathbf{v}) = 2^{n+s-m} \cdot (2^{n-s}-1)$. Substituting these values into equation (3.30), we get that the (n,m)-function F is s-plateaued if and only if its graph $\mathcal{G}_F$ satisfies the following group ring equation

$$\begin{aligned}\mathcal{G}_F^3 =& N_F(\mathbf{0},\mathbf{x}) \cdot \mathcal{G}_F + N_F(\mathbf{v},\mathbf{x}) \cdot (G-\mathcal{G}_F)\\ =& 2^{n+s-m}(2^{n-s}+2^m-1) \cdot \mathcal{G}_F + 2^{n+s-m} \cdot (2^{n-s}-1) \cdot (G-\mathcal{G}_F)\\ =& 2^{n+s} \cdot \mathcal{G}_F + (2^{2n-m}-2^{n+s-m}) \cdot G,\end{aligned}$$

where $G = \mathbb{F}_2^n \times \mathbb{F}_2^m$. □

3.6.3 Characterization of bent functions among plateaued functions

By Theorem 3.40, we conclude that the nonvanishing flats $\mathcal{NF}_{\mathbf{v}}(F)$ of an (n,m)-function F are 1-$(2^n, 4, 2^{n-m}(2^n-1)/6)$ designs for all $\mathbf{v} \in \mathbb{F}_2^m \setminus \{\mathbf{0}\}$ if and only if the (n,m)-function F is bent, since (n,m)-bent functions are s-plateaued (n,m)-functions with $s=0$. Now we show that for bent functions this characterization can be even more strengthened. We prove that all nonvanishing flats of (n,m)-bent functions are not only 1-designs, but also 2-designs. The proof is based on the connection between bent functions and relative difference sets and follows the proof of Theorem 3.26.

Theorem 3.42. *Let F be an (n,m)-function. The following statements are equivalent.*

1. *The function F is (n,m)-bent.*
2. *For any $\mathbf{v} \in \mathbb{F}_2^m \setminus \{\mathbf{0}\}$ the incidence structure $\mathcal{NF}_{\mathbf{v}}(F)$ is a 2-$(2^n, 4, 2^{n-m-1})$ design.*

Moreover, the number of the nonvanishing flats of an (n,m)-bent function F with respect to a nonzero vector $\mathbf{v} \in \mathbb{F}_2^m$ is given by

$$|\mathcal{NF}_{\mathbf{v},F}| = \frac{(2^{n+m}-2^m) \cdot 2^{2(n-m)}}{24}. \tag{3.31}$$

Proof. 1.⇒2. Let F be an (n,m)-bent function, $\mathbf{v}$ be a nonzero element of $\mathbb{F}_2^m$ and $\mathcal{NF}_{\mathbf{v}}(F) = (\mathcal{P},\mathcal{B})$ be the nonvanishing flats of F with respect to $\mathbf{v}$. We will show that any two different points $\mathbf{x}_1, \mathbf{x}_2$ of $\mathcal{P}$ are contained in exactly 2^{n-m-1} blocks of $\mathcal{B}$. We define $\mathbf{a} := \mathbf{x}_1 \oplus \mathbf{x}_2$ and let $\mathbf{v}' := F(\mathbf{x}_1) \oplus F(\mathbf{x}_2)$ and $\mathbf{v}'' := \mathbf{v}' \oplus \mathbf{v}$. Then the following holds

$$\begin{pmatrix}\mathbf{x}_1\\ F(\mathbf{x}_1)\end{pmatrix} \oplus \begin{pmatrix}\mathbf{x}_2\\ F(\mathbf{x}_2)\end{pmatrix} = \begin{pmatrix}\mathbf{a}\\ \mathbf{v}'\end{pmatrix} = \begin{pmatrix}\mathbf{0}\\ \mathbf{v}\end{pmatrix} \oplus \begin{pmatrix}\mathbf{a}\\ \mathbf{v}''\end{pmatrix}. \tag{3.32}$$

Since the graph $\mathcal{G}_F$ is a $(2^n, 2^m, 2^n, 2^{n-m})$-difference set in the group $G = \mathbb{F}_2^n \times \mathbb{F}_2^m$ relative to the forbidden subgroup $N = \{(\mathbf{0}, \mathbf{y}) \colon \mathbf{y} \in \mathbb{F}_2^m\}$, then every element $g := \begin{pmatrix} \mathbf{a} \\ \mathbf{v}'' \end{pmatrix} \in G \setminus N$ has 2^{n-m} representations of the form

$$g = \begin{pmatrix} \mathbf{x}_3 \\ F(\mathbf{x}_3) \end{pmatrix} \oplus \begin{pmatrix} \mathbf{x}_4 \\ F(\mathbf{x}_4) \end{pmatrix} \tag{3.33}$$

with $\{\mathbf{x}_3, \mathbf{x}_4\} \neq \{\mathbf{x}_1, \mathbf{x}_2\}$. In this way, any 2-subset $\{\mathbf{x}_1, \mathbf{x}_2\}$ is contained in exactly 2^{n-m-1} blocks $\{\mathbf{x}_1, \mathbf{x}_2, \mathbf{x}_3, \mathbf{x}_4\}$ of the form (3.13), consequently, the incidence structure $\mathcal{NF}_\mathbf{v}(F)$ is a 2-$(2^n, 4, 2^{n-m-1})$ design.
2.⇒1. Let the incidence structures $\mathcal{NF}_\mathbf{v}(F)$ be 2-$(2^n, 4, 2^{n-m-1})$ designs for all $\mathbf{v} \in \mathbb{F}_2^m \setminus \{\mathbf{0}\}$. By equation (1.36), the number of blocks b of a t-(v, k, λ) design is given by

$$b = \lambda \binom{v}{t} / \binom{k}{t}.$$

In this way, for all $\mathbf{v} \in \mathbb{F}_2^m \setminus \{\mathbf{0}\}$ the number of blocks of the nonvanishing flats $\mathcal{NF}_\mathbf{v}(F)$ is given by

$$|\mathcal{NF}_{\mathbf{v},F}| = \frac{(2^{n+m} - 2^m) \cdot 2^{2(n-m)}}{24}.$$

Since for an (n, m)-function F the nonvanishing flats $\mathcal{NF}_\mathbf{v}(F)$ together with vanishing flats $\mathcal{VF}(F)$ form a partition of the affine Steiner quadruple system $SQS(2^n)$, we have $(2^m - 1) \cdot |\mathcal{NF}_{\mathbf{v},F}| + |\mathcal{VF}(F)| = 2^{n-2} \cdot (2^n - 1) \cdot (2^n - 2)\,/6$, and hence the number of vanishing flats of F is given by

$$|\mathcal{VF}_F| = \frac{(2^{n+m} - 2^m) \cdot 2^{n-m} \cdot (2^{n-m} - 2)}{24}. \tag{3.34}$$

By Theorem 3.26 and Remark 3.27, the value $|\mathcal{VF}_F|$ given in (3.34) is the minimum possible value for an (n, m)-function F with n even and $m \leq n/2$, which is attained if and only if F is an (n, m)-bent function. □

Corollary 3.43. *For an (n, m)-bent function F, the collection of incidence structures $\{\mathcal{VF}(F)\} \cup \{\mathcal{NF}_\mathbf{v}(F) \colon \mathbf{v} \in \mathbb{F}_2^m \setminus \{\mathbf{0}\}\}$ forms a partition of the affine Steiner quadruple system $SQS(2^n)$ into 2-designs.*

3.7 Combinatorial interpretation of the extendability problem

In general, it is difficult to decide whether a given (n, m)-bent function F with $m < n/2$ is extendable (for details see Section 2.2). In this section, we provide a purely combinatorial description of the extendability problem of bent functions by means of the subdesign problem using the theory of vanishing and nonvanishing flats, developed in previous sections. Using nonvanishing flats, we show that vanishing flats of extendable bent functions must be highly structured combinatorial objects. This implies that the existence of certain subdesigns in $\mathcal{VF}(F)$ is a measure of extendability of an (n,m)-bent function F.

For a vectorial (n,m)-bent function $F(\mathbf{x}) = (f_1(\mathbf{x}),\dots,f_m(\mathbf{x}))^T$, we define the *projections* $F_s(\mathbf{x}) := (f_1(\mathbf{x}),\dots,f_s(\mathbf{x}))^T$ and $F_{m-s}(\mathbf{x}) := (f_{s+1}(\mathbf{x}),\dots,f_m(\mathbf{x}))^T$, which are (n,s)- and $(n,m-s)$-bent functions, respectively. Let $\mathcal{VF}_F$, $\mathcal{VF}_{F_s}$ and $\mathcal{VF}_{F_{m-s}}$ be the block sets of the vanishing flats of F, F_s and F_{m-s}, respectively, and let

$$\mathcal{NF}_F := \bigsqcup_{\mathbf{v}\in\mathbb{F}_2^m\setminus\{\mathbf{0}\}} \mathcal{NF}_{\mathbf{v},F}$$

be the (disjoint) union of the block sets of the nonvanishing flats of the vectorial bent function F. Define the collection of the vanishing flats of the projection F_s, disjoint from the vanishing flats of F_{m-s} in the following way

$$\mathcal{DF}_{F/F_{m-s}} := \mathcal{VF}_{F_s} \cap \mathcal{NF}_{F_{m-s}}.$$

We can associate the incidence structures with the defined collections of 4-subsets as follows

$$\mathcal{DF}(F/F_{m-s}) := (\mathbb{F}_2^n, \mathcal{DF}_{F/F_{m-s}}) \quad \text{and} \quad \mathcal{NF}(F) := (\mathbb{F}_2^n, \mathcal{NF}_F).$$

In order to analyze the combinatorial structure of the introduced incidence structures, we need the following obvious lemma, which summarizes the relations between parameters of designs having no common blocks.

Lemma 3.44. *Let $D_1 = (\mathcal{P},\mathcal{B}_1)$ and $D_2 = (\mathcal{P},\mathcal{B}_2)$ be t-(v,k,λ_1) and t-(v,k,λ_2) designs, respectively, and suppose that $\mathcal{B}_1 \cap \mathcal{B}_2 = \varnothing$.*

1. *Then $D = (\mathcal{P},\mathcal{B}_1 \cup \mathcal{B}_2)$ is a t-$(v,k,\lambda_1+\lambda_2)$ design.*
2. *Conversely, if $D_1 = (\mathcal{P},\mathcal{B}_1)$ is a t-(v,k,λ_1) design and $D = (\mathcal{P},\mathcal{B}_1 \cup \mathcal{B}_2)$ is a t-$(v,k,\lambda_1+\lambda_2)$ design, then D_2 is a t-(v,k,λ_2) subdesign of D.*

Using the Lemma 3.44, we show that the incidence structures $\mathcal{DF}(F/F_{m-s})$ and $\mathcal{NF}(F)$ of vectorial bent functions are 2-designs and determine their parameters.

Proposition 3.45. *For a vectorial (n,m)-bent function $F(\mathbf{x}) = (f_1(\mathbf{x}),\dots,f_m(\mathbf{x}))^T$ consider the projections*

$$F_s(\mathbf{x}) = (f_1(\mathbf{x}),\dots,f_s(\mathbf{x}))^T \quad \text{and} \quad F_{m-s}(\mathbf{x}) = (f_{s+1}(\mathbf{x}),\dots,f_m(\mathbf{x}))^T. \tag{3.35}$$

With the notation above, the following hold.

1. *$\mathcal{VF}_F = \mathcal{VF}_{F_s} \cap \mathcal{VF}_{F_{m-s}}$ and $\mathcal{VF}_{F_s} = \mathcal{VF}_F \sqcup \mathcal{DF}_{F/F_{m-s}}$, where $\sqcup$ denotes a disjoint union.*

2. *$\mathcal{DF}(F/F_{m-s})$ is a 2-$(2^n, 4, (2^{m-s}-1)\cdot 2^{n-m-1})$ design.*

3. *$\mathcal{NF}(F)$ is a 2-$(2^n, 4, (2^m-1)\cdot 2^{n-m-1})$ design.*

Proof. The set $\{\mathbf{x}_1, \mathbf{x}_2, \mathbf{x}_3, \mathbf{x}_4\}$ is a vanishing flat of F if and only if it is a vanishing flat of both, F_s and F_{m-s}, hence $\mathcal{VF}_F = \mathcal{VF}_{F_s} \cap \mathcal{VF}_{F_{m-s}}$. On the other hand, for F_s seen as a projection of F we can distinguish two kinds of vanishing flats, those which are also in $\mathcal{VF}_F$ (note that $\mathcal{VF}_F \subset \mathcal{VF}_{F_s}$), and those which are in $\mathcal{VF}_{F_s}$, but not in $\mathcal{VF}_{F_{m-s}}$. The latter is exactly the set $\mathcal{DF}_{F/F_{m-s}}$, and we obtain that $\mathcal{VF}_{F_s} = \mathcal{VF}_F \sqcup \mathcal{DF}_{F/F_{m-s}}$. With Lemma 3.44, $\mathcal{DF}(F/F_{m-s})$ is then a 2-$(2^n, 4, (2^{m-s}-1)\cdot 2^{n-m-1})$ design. Finally, $\mathcal{NF}(F)$ is a 2-$(2^n, 4, (2^m-1)\cdot 2^{n-m-1})$ design by Lemma 3.44. □

By Proposition 3.45, the 2-$(2^n, 4, 2^{n-s-1}-1)$ design $\mathcal{VF}(F)$ of a (vectorial) (n,s)-bent function F, which is a projection of a vectorial (n,m)-bent function $\tilde{F}$ for some $m > s$, has certain structural properties. With these observations, we can give a connection between extendability of a (vectorial) bent function and vanishing flats. In this way, instead of extending a given (n,s)-bent function F to an $(n, s+r)$-bent function $\tilde{F}$ by consequently searching for suitable coordinate bent functions $f_{s+1}, \dots, f_{s+r}$ from $\mathcal{B}_{n,1}$ (as in Chapter 2), one can analyze the internal combinatorial information containing in vanishing flats $\mathcal{VF}(F)$ in order to find proper extensions.

Theorem 3.46. *Let F be an (n,s)-bent function.*

1. *If F is extendable, then there exist subdesigns $D = (\mathbb{F}_2^n, \mathcal{B})$ and $D_1 = (\mathbb{F}_2^n, \mathcal{B}_1)$ of $\mathcal{VF}(F)$ with parameters 2-$(2^n, 4, 2^{n-s-2}-1)$ and 2-$(2^n, 4, 2^{n-s-2})$, respectively, such that $\mathcal{VF}(F) = D \sqcup D_1$.*

2. *If F is a projection of a vectorial $(n, s+r)$-bent function $\tilde{F}$ for some $s + r \le n/2$, then there exists a partition*

$$\mathcal{VF}(F) = D \sqcup \left(\bigsqcup_{i=1}^{r} D_i \right),$$

where $D = \mathcal{VF}(\tilde{F})$ is a 2-$(2^n, 4, 2^{n-s-r-1}-1)$ design, and for all $1 \le i \le r$ the incidence structures $D_i = (\mathbb{F}_2^n, \mathcal{B}_i)$ are 2-$(2^n, 4, 2^{n-s-1-i})$ designs with the number of blocks $|\mathcal{B}_i| = (2^{3n-s-3-i} - 2^{2n-s-3-i})/3$.

Proof. Note that the first statement follows as the special case $r = 1$ from the second. Let F and $\tilde{F}$ be given as in (3.35). By Proposition 3.45, the block set $\mathcal{VF}_F$ of the vanishing flats $\mathcal{VF}(F)$ of F, seen as a projection of the function $F_1(\mathbf{x}) = (f_1(\mathbf{x}), \dots, f_s(\mathbf{x}), f_{s+1}(\mathbf{x}))^T$, is a (disjoint) union of the vanishing flats $\mathcal{VF}_{F_1}$ of F_1 and the set $\mathcal{B}_1 = \mathcal{DF}_{F_1/f_{s+1}}$, which has the cardinality $|\mathcal{B}_1| = |\mathcal{VF}_F| - |\mathcal{VF}_{F_1}| = (2^{3n-s-4} - 2^{2n-s-4})$. By Proposition 3.45 and by Lemma 3.44, we have that $D_1 = (\mathbb{F}_2^n, \mathcal{B}_1)$ is a 2-$(2^n, 4, 2^{n-s-2})$ design. As F_1 is a projection of $F_2(\mathbf{x}) = (f_1(\mathbf{x}), \ldots, f_{s+1}(\mathbf{x}), f_{s+2}(\mathbf{x}))^T$, $\mathcal{VF}_{F_1}$ is a (disjoint) union of $\mathcal{VF}_{F_2}$ and $\mathcal{B}_2 = \mathcal{DF}_{F_2/f_{s+2}}$. The cardinality of $\mathcal{B}_2$ is given by $|\mathcal{B}_2| = |\mathcal{VF}_{F_1}| - |\mathcal{VF}_{F_2}| = (2^{3n-s-5} - 2^{2n-s-5})$, and hence, $D_2 = (\mathbb{F}_2^n, \mathcal{B}_2)$ is a 2-$(2^n, 4, 2^{n-s-3})$ design. With a recursive argument, the second statement is shown. □

In Chapter 2, we observed that in $n = 4$ and $n = 6$ variables the only non-extendable bent functions are those, which achieve the Nyberg bound with equality, i.e., $(n, n/2)$-bent functions. To the best of the author's knowledge, the question of the non-extendability of (n, m)-bent functions with $n \geq 8$ and $m < n/2$ has not been studied so far. In order to search for non-extendable bent functions computationally, one may try to use the following sufficient condition for the non-extendability of bent functions, which follows from Theorem 3.46.

Theorem 3.47. *Let F be an (n, s)-bent function.*

1. *If $\mathcal{VF}(F)$ contains no 2-$(2^n, 4, 2^{n-s-2} - 1)$ subdesign, then F is non-extendable.*
2. *If $\mathcal{VF}(F)$ contains no 2-$(2^n, 4, 2^{n-s-2})$ subdesign, then F is non-extendable.*
3. *If $\mathcal{VF}(F)$ contains no 2-$(2^n, 4, 2^{n-s-r-1} - 1)$ subdesign for some integer r, satisfying $1 \leq r \leq n/2 - s - 1$, then F is not the projection of an $(n, n/2)$-bent function.*

Finally, we refer to the DESIGN package [106] of the system for computational discrete algebra GAP [55], which can be used to solve subdesign problems. For an example of the use of this package, we refer to [107].

3.8 Extended Assmus-Mattson theorem and its applications

One of the standard ways to prove that codewords of a fixed weight in a linear code $\mathcal{C}$ hold t-designs is to check whether $\mathcal{C}$ satisfies the conditions of the transitivity theorem (see Result 1.86) or of the original Assmus-Mattson theorem (see Result 1.87). Tang, Ding and Xiong [108] introduced a new powerful tool, which was shown to outperform the original Assmus-Mattson theorem on the linear codes constructed from certain (n, m)-functions.

Result 3.48 (Extended Assmus-Mattson Theorem). *[108, Theorem 5.3] Let $\mathcal{C}$ be a linear code over $\mathbb{F}_2$ with length v and minimum weight d. Let $\mathcal{C}^\perp$ denote the dual code of $\mathcal{C}$ with minimum weight $d^\perp$. Let s and t be two positive integers and let t satisfy $t < \min\{d, d^\perp\}$. Let S be an s-subset of $\{d, d+1, \ldots, v-t\}$. Suppose* *that the incidence structures $(\mathcal{P}(\mathcal{C}), \mathcal{B}_\ell(\mathcal{C}))$ and $\left(\mathcal{P}\left(\mathcal{C}^\perp\right), \mathcal{B}_{\ell^\perp}\left(\mathcal{C}^\perp\right)\right)$ are t-designs for $\ell \in \{d, d+1, \ldots, v-t\} \setminus S$ and $\ell^\perp$ satisfying $0 \leq \ell^\perp \leq s+t-1$. Then $(\mathcal{P}(\mathcal{C}), \mathcal{B}_w(\mathcal{C}))$ and $\left(\mathcal{P}\left(\mathcal{C}^\perp\right), \mathcal{B}_w\left(\mathcal{C}^\perp\right)\right)$ are t-designs for any $t \leq w \leq v$.*

Example 3.49. Let F be an (n, m)-bent function with $n = 2k$. By Corollary 1.64, the linear code $\mathcal{C}_F$ is a $[2^n, n+m+1, d]$-linear code with the minimum distance $d = 2^{n-1} - 2^{k-1}$ and the weight enumerator

$$\begin{aligned} W_{\mathcal{C}_F}(z) =& 1 + (2^m - 1)\, 2^n z^{2^{n-1}-2^{k-1}} + (2^{n+1}-2) z^{2^{n-1}} \\ &+ (2^m-1)\, 2^n z^{2^{n-1}+2^{k-1}} + z^{2^n}. \end{aligned}$$

The dual code $\mathcal{C}_F^\perp$ has the minimum distance $d^\perp = 4$.
1. For $t = 2$, the linear codes $\mathcal{C}_F$ and $\mathcal{C}_F^\perp$ of (n, m)-bent functions F do not satisfy the conditions of the original Assmus-Mattson theorem, given in Result 1.86.
2. Tang, Ding and Xiong [108] used extended Assmus-Mattson Theorem to show that the linear codes $\mathcal{C}_F$ and $\mathcal{C}_F^\perp$ of (n, m)-bent functions F support 2-designs. Set $t = 2$, which satisfies $t < \min\left\{d, d^\perp\right\}$ and let $s = 2$. Consider the set $S = \{2^{n-1} \pm 2^{k-1}\}$. We show that for any $\ell \in \{2^{n-1} - 2^{k-1}, \ldots, 2^n - 2\} \setminus S$ the incidence structures $(\mathcal{P}(\mathcal{C}_F), \mathcal{B}_\ell(\mathcal{C}_F))$ are 2-designs. If $\ell = 2^{n-1}$, then the blocks of $(\mathcal{P}(\mathcal{C}_F), \mathcal{B}_{2^{n-1}}(\mathcal{C}_F))$ are truth tables of all non-constant affine functions, which generate the first-order Reed-Muller code $\mathcal{RM}(1, n)$. By original Assmus-Mattson Theorem (see Result 1.87), the first-order Reed-Muller code $\mathcal{RM}(1, n)$ supports 2-designs, and hence the incidence structure $(\mathcal{P}(\mathcal{C}_F), \mathcal{B}_{2^{n-1}}(\mathcal{C}_F))$ is a 2-design. If $\ell \neq 2^{n-1}$, then the incidence structures $(\mathcal{P}(\mathcal{C}_F), \mathcal{B}_\ell(\mathcal{C}_F))$ are trivial 2-designs, due to the weight enumerator of $\mathcal{C}_F$. Moreover, for any $\ell^\perp$ satisfying $0 \leq \ell^\perp \leq s+t-1 = 3$, we have that incidence structures $\left(\mathcal{P}\left(\mathcal{C}_F^\perp\right), \mathcal{B}_{\ell^\perp}\left(\mathcal{C}_F^\perp\right)\right)$ are trivial 2-designs, since $d^\perp = 4$. In this way, the conditions of the extended Assmus-Mattson theorem are fulfilled, and hence the for (n, m)-bent functions the incidence structures $(\mathcal{P}(\mathcal{C}_F), \mathcal{B}_w(\mathcal{C}_F))$ and $\left(\mathcal{P}\left(\mathcal{C}_F^\perp\right), \mathcal{B}_w\left(\mathcal{C}_F^\perp\right)\right)$ for are 2-designs for any $2 \leq w \leq 2^n$.

Remark 3.50. Since the weight enumerator $W_{\mathcal{C}_F}(z) := \sum_{i=0}^n A_i z^i$ of the $[v, k]$-linear code $\mathcal{C}_F$ for (n, m)-bent functions F is known, the weight enumerator $W_{\mathcal{C}_F^\perp}(z) := \sum_{i=0}^n B_i z^i$ of the dual code $\mathcal{C}_F^\perp$ is uniquely determined by the following linear equations, called *MacWilliams identities* [76]:

$$\text{for all } 0 \leq i \leq v \text{ holds} \quad \sum_{j=0}^{v-i} \binom{v-j}{i} A_j = 2^{k-i} \sum_{j=0}^{i} \binom{v-j}{v-i} B_j. \tag{3.36}$$

With these weight distributions $\{A_j\}$ and $\{B_j\}$, we have that by Remark 1.88, the parameters of t-designs $(\mathcal{P}(\mathcal{C}_F), \mathcal{B}_w(\mathcal{C}_F))$ and $\left(\mathcal{P}\left(\mathcal{C}_F^\perp\right), \mathcal{B}_w\left(\mathcal{C}_F^\perp\right)\right)$ are equal to t-$\left(v, w, A_w \cdot \binom{w}{t}/\binom{v}{t}\right)$ and t-$\left(v, w, B_w \cdot \binom{w}{t}/\binom{v}{t}\right)$, respectively.

Example 3.51. Following Remark 3.50, we compute the parameters of nontrivial 2-designs supported by codewords of weight $1 \leq w \leq 64$ in the linear codes

$\mathcal{C}_F$ and $\mathcal{C}_F^\perp$ of (6,3)-bent functions F. We list the parameters 2-$(64, w, \lambda)$ for all nontrivial 2-designs $(\mathcal{P}(\mathcal{C}_F), \mathcal{B}_w(\mathcal{C}_F))$ constructed from the code $\mathcal{C}_F$, while for the linear code $\mathcal{C}_F^\perp$, we list the parameters 2-$(64, w, \lambda)$ only for some of the 2-designs $\left(\mathcal{P}\left(\mathcal{C}_F^\perp\right), \mathcal{B}_w\left(\mathcal{C}_F^\perp\right)\right)$.

$(\mathcal{P}(\mathcal{C}_F), \mathcal{B}_w(\mathcal{C}_F))$	$\left(\mathcal{P}\left(\mathcal{C}_F^\perp\right), \mathcal{B}_w\left(\mathcal{C}_F^\perp\right)\right)$
	2-(64,4,3)
	2-(64,6,1120)
	2-(64,8,119575)
	2-(64,10,6608160)
	$\vdots$
2-(64, 28, 84)	2-(64,30,682843048315520)
2-(64, 32, 31)	2-(64,32,880632444631427)
2-(64, 36, 140)	2-(64,34,880632069206912)
2-(64, 64, 1)	2-(64,36,682843360300745)
	$\vdots$
	2-(64,56,6576625)
	2-(64,58,123424)
	2-(64,60,885)
	2-(64,64,1)

Note that since all weights w in $\mathcal{C}_F^\perp$ are even and the minimum distance of $\mathcal{C}_F^\perp$ is $d^\perp = 4$, we have that for any $4 \leq w \leq 64$ the 2-designs $\left(\mathcal{P}\left(\mathcal{C}_F^\perp\right), \mathcal{B}_w\left(\mathcal{C}_F^\perp\right)\right)$ are nontrivial if and only if w is even.

In the following subsections, we investigate further applications of the extended Assmus-Mattson theorem to the linear codes constructed from Boolean and vectorial functions.

3.8.1 Extended Assmus-Mattson theorem can outperform transitivity theorem

Now we use Result 1.86 and connections between translation and addition designs, in order to characterize quadratic Boolean bent functions in terms of the 2-transitivity of the automorphism group.

Theorem 3.52. *Let f be a Boolean bent function on $\mathbb{F}_2^n$. The automorphism groups of linear codes $\mathcal{C}_f$ and $\mathcal{C}_f^\perp$ are 2-transitive if and only if f is quadratic.*

Proof. Let f be a quadratic Boolean bent function on $\mathbb{F}_2^n$. Without loss of generality we assume that $\mathrm{wt}(f) = 2^{n-1} - 2^{n/2-1}$, in this way, by Result 1.79 we have that $\mathrm{dev}(\mathcal{D}_f)$ is a 2-$(2^n, 2^{n-1} - 2^{n/2-1}, 2^{n-2} - 2^{n/2-1})$ design. By [39, Lemma 2.3] any two quadratic Boolean functions g and g' on $\mathbb{F}_2^n$ are affine equivalent if and only if $\mathrm{wt}(g) = \mathrm{wt}(g')$. Consequently, for a quadratic Boolean bent function f on

$\mathbb{F}_2^n$ with $\mathrm{wt}(f) = 2^{n-1} - 2^{n/2-1}$ its translation design $\mathrm{dev}(\mathcal{D}_f)$ is isomorphic to the symplectic 2-$(2^n, 2^{n-1} - 2^{n/2-1}, 2^{n-2} - 2^{n/2-1})$ design S, which is realized as the translation design of the quadratic bent function $Q_n(\mathbf{x}) = x_1x_2 \oplus \cdots \oplus x_{n-1}x_n$ on $\mathbb{F}_2^n$, see [67, Chapter 3]. Up to isomorphism, for any even n there is only one 2-$(2^n, 2^{n-1} - 2^{n/2-1}, 2^{n-2} - 2^{n/2-1})$ design with a 2-transitive automorphism group, and that is the symplectic design S, as it was shown by Kantor [61, 62]. The automorphism group of S is a semidirect product of the translation group Σ of the affine space $\mathrm{AG}(n, 2)$ with the symplectic group $\mathrm{Sp}(n, 2)$. Furthermore, for a quadratic bent function f on $\mathbb{F}_2^n$ its translation $\mathrm{dev}(\mathcal{D}_f)$ and addition $\mathbb{D}(f)$ designs are isomorphic, as it was shown by Bending [5, Theorem 11.9]. The characterization of quadratic Boolean bent functions now follows from the fact that the automorphism groups $\mathrm{Aut}(\mathbb{D}(f))$ and $\mathrm{Aut}(\mathcal{C}_f)$ are isomorphic, since the incidence matrix $\mathbf{M}(\mathbb{D}(f))$ of the addition design $\mathbb{D}(f)$ is a generator matrix of the linear code $\mathcal{C}_f$. □

Corollary 3.53. *Let f be a quadratic bent function on $\mathbb{F}_2^n$ with $n = 2k$. Then the order of the automorphism group of the function f is given by*

$$|\mathrm{Aut}(f)| = 2^n \cdot 2^{k^2} \prod_{i=1}^{k} (2^{2i} - 1). \tag{3.37}$$

Remark 3.54. In general, an (n, m)-bent function does not necessarily have a 2-transitive automorphism group. Using a Magma program [9] and the list of representatives F_i^m of the equivalence classes C_i^m of $(6, m)$-bent functions from Appendix A.1, it is possible to check that, up to EA-equivalence, the only $(6, m)$-bent functions, which have a 2-transitive automorphism group, are the following quadratic functions: F_1^1, F_1^2, F_1^3 and F_3^3. Since the automorphism group of the quadratic function F_2^3 is not 2-transitive, we conclude that the property of an (n, m)-bent function to be quadratic does not in general imply the 2-transitivity of its automorphism group.

With Theorem 3.52 and Remark 3.54, we conclude that extended Assmus-Mattson theorem can also outperform the transitivity theorem (Result 1.86). By extended Assmus-Mattson theorem, the linear codes $\mathcal{C}_F$ and $\mathcal{C}_F^\perp$ for all (n, m)-bent functions F support 2-designs. On the other hand, the only Boolean bent function on $\mathbb{F}_2^n$ with a 2-transitive automorphism group is quadratic, and only few examples of vectorial bent functions in six variables have a 2-transitive automorphism group.

3.8.2 Designs from APN functions with the classical Walsh spectrum

Tang, Ding and Xiong [108] proved that not only the vanishing flats $\mathcal{VF}(F)$ of differentially two-valued s-plateaued (n, n)-functions F are 2-designs, but that the linear codes $\mathcal{C}_F$ and $\mathcal{C}_F^\perp$ support 2-designs.

Result 3.55. *[108, Theorem 6.4] Let F be a differentially two-valued s-plateaued (n,n)-function. Then the code $\mathcal{C}_F$ and its dual $\mathcal{C}_F^{\perp}$ support 2-designs.*

As a corollary, this result implies that the linear codes $\mathcal{C}_F$ and $\mathcal{C}_F^{\perp}$ of all AB functions F on $\mathbb{F}_2^n$, which belong to the class of APN functions with the classical Walsh spectrum, support 2-designs. In the following statement, we provide another subclass of APN functions F on $\mathbb{F}_2^n$ with the classical spectrum, whose linear codes $\mathcal{C}_F$ and $\mathcal{C}_F^{\perp}$ support 2-designs.

Theorem 3.56. *Let F be an APN function on $\mathbb{F}_2^n$ with $n = 2k$, which has the classical Walsh spectrum. If the function F is CCZ-equivalent to a function F' on $\mathbb{F}_2^n$ having $2(2^n-1)/3$ bent components and $(2^n-1)/3$ semi-bent components, then the linear codes $\mathcal{C}_F$ and $\mathcal{C}_F^{\perp}$ support 2-designs.*

Proof. First, we recall that by Result 1.60, functions F and F' are CCZ-equivalent if and only if linear codes $\mathcal{C}_F$ and $\mathcal{C}_{F'}$ (or $\mathcal{C}_F^{\perp}$ and $\mathcal{C}_{F'}^{\perp}$, respectively) are equivalent. By Proposition 1.85, for linear codes $\mathcal{C}_F$ and $\mathcal{C}_{F'}$ of CCZ-equivalent functions F and F', the incidence structures $(\mathcal{P}(\mathcal{C}_F), \mathcal{B}_\ell(\mathcal{C}_F))$ and $(\mathcal{P}(\mathcal{C}_{F'}), \mathcal{B}_\ell(\mathcal{C}_{F'}))$ are isomorphic for all $1 \le \ell \le 2^n$. Similarly, for linear codes $\mathcal{C}_F^{\perp}$ and $\mathcal{C}_{F'}^{\perp}$ the incidence structures $\left(\mathcal{P}(\mathcal{C}_F^{\perp}), \mathcal{B}_{\ell^\perp}(\mathcal{C}_F^{\perp})\right)$ and $\left(\mathcal{P}(\mathcal{C}_{F'}^{\perp}), \mathcal{B}_{\ell^\perp}(\mathcal{C}_{F'}^{\perp})\right)$ are isomorphic for all $1 \le \ell^\perp \le 2^n$ as well. Consequently, it is enough to prove that linear codes $\mathcal{C}_{F'}$ and $\mathcal{C}_{F'}^{\perp}$ support 2-designs.

We show that the conditions of the extended Assmus-Mattson theorem (Result 3.48) are fulfilled for linear codes $\mathcal{C}_F$ and $\mathcal{C}_{F'}^{\perp}$ with integers $t = 2$ and $s := |S| = 3$, where the set S is defined as follows $S := \{2^{n-1}, 2^{n-1} \pm 2^{n/2}\}$. Since the function F' has $2(2^n-1)/3$ bent components and $(2^n-1)/3$ semi-bent components, we have that for any codeword $\mathbf{c} \in \mathcal{C}_{F'} \setminus \{\mathbf{0}, \mathbf{j}_{2^n}\}$ holds

$$\mathrm{wt}(\mathbf{c}) \in W := \{2^{n-1} \pm 2^{n/2-1}, 2^{n-1}, 2^{n-1} \pm 2^{n/2}\},$$

since possible Hamming weights of bent functions are $2^{n-1} \pm 2^{n/2-1}$ and possible Hamming weights of semi-bent functions are 2^{n-1} and $2^{n-1} \pm 2^{n/2}$, respectively. By Remark 3.23, from any component function $F'_{\mathbf{b}}$ of F', which is bent, one can construct 2-designs $(\mathcal{P}(\mathcal{C}_{F'_{\mathbf{b}}}), \mathcal{B}_\ell(\mathcal{C}_{F'_{\mathbf{b}}}))$ with $\ell \in W \setminus S = \{2^{n-1} \pm 2^{n/2-1}\}$ using the dual function $\tilde{F'}_{\mathbf{b}}$ as described in Remark 3.23. Clearly, any two component bent functions $F'_{\mathbf{b}}$ and $F'_{\mathbf{b}'}$ with $\mathbf{b} \neq \mathbf{b}'$ do not differ by an affine function. In this way, we have that for $\ell \in \{2^{n-1} \pm 2^{n/2-1}\}$ the incidence structures $(\mathcal{P}(\mathcal{C}_{F'}), \mathcal{B}_\ell(\mathcal{C}_{F'}))$ are 2-$(2^n, 2^{n-1} \pm 2^{n/2-1}, \frac{2}{3}(2^n-1) \cdot (2^{n-2} \pm 2^{n/2-1}))$ designs by Lemma 3.44, since they are obtained by a disjoint union of 2-$(2^n, 2^{n-1} \pm 2^{n/2-1}$, $2^{n-2} \pm 2^{n/2-1})$ designs $(\mathcal{P}(\mathcal{C}_{F'_{\mathbf{b}}}), \mathcal{B}_w(\mathcal{C}_{F'_{\mathbf{b}}}))$ having no repeated blocks. Since the function F' is APN, the minimum distance $d^\perp$ of $\mathcal{C}_{F'}^{\perp}$ is equal to $d^\perp = 6$. In this way, for any $0 \le \ell^\perp \le s + t - 1 = 4$ we have $\mathcal{B}_{\ell^\perp}(\mathcal{C}_{F'}^{\perp}) = \varnothing$ and thus $(\mathcal{P}(\mathcal{C}_{F'}^{\perp}), \mathcal{B}_{\ell^\perp}(\mathcal{C}_{F'}^{\perp}))$ are trivial 2-designs. Since for all $\ell \in W \setminus S$ and $\ell^\perp$ with $0 \le \ell^\perp \le 4$, the incidence structures $(\mathcal{P}(\mathcal{C}_{F'}), \mathcal{B}_\ell(\mathcal{C}_{F'}))$ and $\left(\mathcal{P}\left(\mathcal{C}_{F'}^{\perp}\right), \mathcal{B}_{\ell^\perp}\left(\mathcal{C}_{F'}^{\perp}\right)\right)$ are 2-designs, we have that the linear codes $\mathcal{C}_{F'}$ and $\mathcal{C}_{F'}^{\perp}$ support 2-designs. □

Remark 3.57. The question whether linear codes $\mathcal{C}_F$ and $\mathcal{C}_F^\perp$ of APN functions F on $\mathbb{F}_2^n$ with a nonclassical Walsh spectrum support 2-designs is, in general, difficult. There are no known algebraic constructions of these functions, and the known examples are sporadic.

Example 3.58. Consider the quadratic APN function D_7 from Table 2.1. As we mentioned in Example 3.38, one component function of D_7 is 4-plateaued, and hence the Walsh spectrum of D_7 is nonclassical. It is possible to check with a computer that the incidence structures supported by the codewords of the minimum weight in the codes $\mathcal{C}_{D_7}$ and $\mathcal{C}_{D_7}^\perp$ are 1-designs, but not 2-designs. For instance, we have that:

- $(\mathcal{P}(\mathcal{C}_{D_7}), \mathcal{B}_{16}(\mathcal{C}_{D_7}))$ is a 1-$(64, 16, 1)$ design with 4 blocks;
- $(\mathcal{P}(\mathcal{C}_{D_7}^\perp), \mathcal{B}_6(\mathcal{C}_{D_7}^\perp))$ is a 1-$(64, 6, 1986)$ design with 21184 blocks.

Now we describe a big class of APN functions with the classical Walsh spectrum, satisfying the conditions of Theorem 3.56. Note that this class contains most of the known examples and constructions of APN functions.

Theorem 3.59. *Let F be an APN function on $\mathbb{F}_2^n$ with $n = 2k$, which has the classical Walsh spectrum. If the function F is CCZ-equivalent to a quadratic APN function, then the linear codes $\mathcal{C}_F$ and $\mathcal{C}_F^\perp$ support 2-designs.*

Proof. Let F' be a quadratic APN function on $\mathbb{F}_2^n$ such that F and F' are CCZ-equivalent. From the fact that the extended Walsh spectrum is invariant under CCZ-equivalence, we have that $|\hat{\chi}_{F'}(\mathbf{a}, \mathbf{b})| \in \left\{0, 2^{\frac{n}{2}}, 2^{\frac{n+2}{2}}\right\}$ for all $\mathbf{a} \in \mathbb{F}_2^n$, $\mathbf{b} \in \mathbb{F}_2^m \setminus \{\mathbf{0}\}$. Since the function F' is quadratic, it is plateaued, and thus for any component function $F'_{\mathbf{b}}$ with $\mathbf{b} \in \mathbb{F}_2^m \setminus \{\mathbf{0}\}$, we have $|\hat{\chi}_{F'_{\mathbf{b}}}(\mathbf{a})| \in \left\{2^{\frac{n}{2}}\right\}$ for all $\mathbf{a} \in \mathbb{F}_2^n$ if and only if $F'_{\mathbf{b}}$ is bent, and $|\hat{\chi}_{F'_{\mathbf{b}}}(\mathbf{a})| \in \left\{0, 2^{\frac{n+2}{2}}\right\}$ for all $\mathbf{a} \in \mathbb{F}_2^n$ if and only if $F'_{\mathbf{b}}$ is semi-bent. From the extended Walsh spectrum of F', which is classical, we get that the number of bent components is $2(2^n - 1)/3$ and the number of semi-bent components is $(2^n - 1)/3$. By Proposition 1.85 and Theorem 3.56, the linear codes $\mathcal{C}_F$ and $\mathcal{C}_F^\perp$ support 2-designs, since functions F and F' are CCZ-equivalent. □

Example 3.60. Consider the APN permutation F on $\mathbb{F}_{2^6}$, whose univariate representation is given in Remark 3.33 and which is CCZ-equivalent to the quadratic APN function D_5 on $\mathbb{F}_{2^6}$ from Table 2.1 having the classical Walsh spectrum. By Theorem 3.59, the incidence structures $(\mathcal{P}(\mathcal{C}_F), \mathcal{B}_w(\mathcal{C}_F))$ and $\left(\mathcal{P}\left(\mathcal{C}_F^\perp\right), \mathcal{B}_w\left(\mathcal{C}_F^\perp\right)\right)$ are 2-designs for all $1 \leq w \leq 64$. We give the parameters 2-$(64, w, \lambda)$ for all nontrivial 2-designs $(\mathcal{P}\left(\mathcal{C}_F\right), \mathcal{B}_w\left(\mathcal{C}_F\right))$ constructed from the code $\mathcal{C}_F$, while for the linear code $\mathcal{C}_F^\perp$, we list the parameters only for some of the 2-designs

$\left(\mathcal{P}\left(\mathcal{C}_F^{\perp}\right), \mathcal{B}_w\left(\mathcal{C}_F^{\perp}\right)\right)$. With a computer program, it is possible to check that the weight enumerator $W_{\mathcal{C}_F}(z) := \sum_{i=0}^{n} A_i z^i$ of $\mathcal{C}_F$ is given by

$$W_{\mathcal{C}_F}(z) = 1 + 336z^{24} + 2688z^{28} + 2142z^{32} + 2688z^{36} + 336z^{40} + z^{64}.$$

Using MacWilliams identities (3.36), it is possible to determine the weight enumerator $W_{\mathcal{C}_F^{\perp}}(z) := \sum_{i=0}^{n} B_i z^i$ of the linear code $\mathcal{C}_F^{\perp}$. In this way, by Remark 3.50 the parameters of 2-designs $(\mathcal{P}(\mathcal{C}_F), \mathcal{B}_w(\mathcal{C}_F))$ and $\left(\mathcal{P}\left(\mathcal{C}_F^{\perp}\right), \mathcal{B}_w\left(\mathcal{C}_F^{\perp}\right)\right)$ are equal 2-$\left(64, w, A_w \cdot \binom{w}{2}/2016\right)$ and 2-$\left(64, w, B_w \cdot \binom{w}{2}/2016\right)$, respectively, and given in the following table.

$(\mathcal{P}(\mathcal{C}_F), \mathcal{B}_w(\mathcal{C}_F))$	$\left(\mathcal{P}\left(\mathcal{C}_F^{\perp}\right), \mathcal{B}_w\left(\mathcal{C}_F^{\perp}\right)\right)$
	2-(64,6,150)
	2-(64,8,14827)
	2-(64,10,827050)
	2-(64,12,26239400)
	$\vdots$
2-(64,24,46)	2-(64,28,51213339251088)
2-(64,28,504)	2-(64,30,85355243664120)
2-(64,32,527)	2-(64,32,110079229195587)
2-(64,36,840)	2-(64,34,110078831484072)
2-(64,40,130)	2-(64,36,85355565418480)
2-(64,64,1)	2-(64,38,51213131016218)
	$\vdots$
	2-(64,54,26300190)
	2-(64,56,815485)
	2-(64,58,16530)
	2-(64,64,1)

Note that since all weights w in $\mathcal{C}_F^{\perp}$ are even and the minimum distance of $\mathcal{C}_F^{\perp}$ is $d^{\perp} = 6$, we have that for any $6 \leq w \leq 64$ the 2-designs $\left(\mathcal{P}\left(\mathcal{C}_F^{\perp}\right), \mathcal{B}_w\left(\mathcal{C}_F^{\perp}\right)\right)$ are nontrivial if and only if w is even.

With Theorem 3.59, we derive the following sufficient conditions for an APN function with the classical Walsh spectrum to be CCZ-inequivalent to a quadratic function.

Theorem 3.61. *Let F be an APN function on $\mathbb{F}_2^n$ with $n = 2k$, which has the classical Walsh spectrum.*

1. *If there exists an integer ℓ, satisfying $1 < \ell < 2^n$ such that the incidence structure $(\mathcal{P}(\mathcal{C}_F), \mathcal{B}_\ell(\mathcal{C}_F))$ is not a 2-design, then the APN function F is CCZ-inequivalent to a quadratic function.*

2. *If there exists an integer $\ell^{\perp}$, satisfying $6 < \ell^{\perp} < 2^n$ such that the incidence structure $\left(\mathcal{P}(\mathcal{C}_F^{\perp}), \mathcal{B}_{\ell^{\perp}}(\mathcal{C}_F^{\perp})\right)$ is not a 2-design, then the APN function F is CCZ-inequivalent to a quadratic function.*

Remark 3.62. To prove that an APN function F on $\mathbb{F}_2^n$ is CCZ-inequivalent to a quadratic one is, in general, difficult. Edel and Pott [52] provided several sufficient conditions for an APN function F on $\mathbb{F}_2^n$ (not necessarily having the classical Walsh spectrum) to be CCZ-inequivalent to a quadratic one by means of the automorphism groups of incidence structures constructed from F. For instance, they showed that if for an APN function F on $\mathbb{F}_2^n$ the automorphism group $\mathrm{Aut}(\mathrm{dev}(\mathcal{G}_F))$ does not contain an elementary abelian group of order 2^{3n}, then F is CCZ-inequivalent to a quadratic function. Practically, the computation of the automorphism group of $\mathrm{dev}(\mathcal{G}_F)$ is computationally difficult and can be performed, provided the number of variables is not too large. Moreover, the computation of an automorphism group requires a special software, e.g., Magma [9] or GAP [55].

On the other hand, for a given APN function with the classical Walsh spectrum, the sufficient conditions given in Theorem 3.61 are easy to check without the use of a special software, due to the following algebraic interpretation of the 2-design property. It is well-known that if $\mathbf{N}$ is an incidence matrix of a 2-(v,k,λ) design with the replication number r, then the following holds

$$\mathbf{N}^T\mathbf{N} = (r-\lambda)\mathbf{I}_v + \lambda\mathbf{J}_v. \tag{3.38}$$

One can check first whether equation (3.38) holds for incidence matrices $\mathbf{N}$ of the incidence structures $(\mathcal{P}(\mathcal{C}_F), \mathcal{B}_w(\mathcal{C}_F))$, since rows of $\mathbf{N}$ are formed by the truth tables of the functions $F_{\mathbf{b}} \oplus l$, where $\mathbf{b} \in \mathbb{F}_2^m$, $l \in \mathcal{RM}(1,n)$ and $\mathrm{wt}(F_{\mathbf{b}} \oplus l) = w$.

Example 3.63. Consider the Edel-Pott APN function F on $\mathbb{F}_{2^6}$, which has the classical Walsh spectrum and whose univariate representation is given in Table 2.1.

1. Edel and Pott [52] showed that the function F is CCZ-inequivalent to a quadratic one, since $|\mathrm{Aut}(\mathrm{dev}(\mathcal{G}_F))| = 2^{15}$, and hence the automorphism group $\mathrm{Aut}(\mathrm{dev}(\mathcal{G}_F))$ can not contain an elementary abelian group of order 2^{18}.

2. Now we show that the function F is CCZ-inequivalent to a quadratic one using Theorem 3.59. First, we observe that the function F has the classical Walsh spectrum. The weight distribution of the linear code $\mathcal{C}_F$ is given by

$$W_{\mathcal{C}_F}(z) = 1 + 336z^{24} + 2688z^{28} + 2142z^{32} + 2688z^{36} + 336z^{40} + z^{64}.$$

We observe that the incidence structure $(\mathcal{P}(\mathcal{C}_F), \mathcal{B}_{24}(\mathcal{C}_F))$ supported by the codewords of the minimum weight of $\mathcal{C}_F$ is a 1-(64, 24, 126) design with 336 blocks, but not a 2-design, since the equation (3.38) does not hold. Computing $\mathbf{N}^T\mathbf{N}$ for an incidence matrix $\mathbf{N}$ of the incidence structure $(\mathcal{P}(\mathcal{C}_F), \mathcal{B}_{24}(\mathcal{C}_F))$, we get that the elements of $\mathbf{N}^T\mathbf{N}$ are in the set $S = \{38, 42, 46, 50, 54, 126\}$. However, by equation (3.38) for a 2-design 2-(v,k,λ) design with the replication number r and an incidence matrix $\mathbf{N}$, we have that the elements of $\mathbf{N}^T\mathbf{N}$ are in the set $S = \{r-\lambda, \lambda\}$. By Theorem 3.59, the function F is CCZ-inequivalent to a quadratic one.

3.9 Conclusion and open problems

In this chapter, we studied whether certain design-theoretic properties of Boolean bent functions can be shared by their generalizations. Particularly, we compared different concepts of equivalence relations for Boolean and vectorial bent functions: extended-affine equivalence of functions, isomorphism of translation designs, isomorphism of addition designs and isomorphism of vanishing flats. We summarize our results in the following table.

Table 3.1. EA-equivalence vs. isomorphism of designs for bent functions

Does isomorphism of designs coincide with EA-equivalence for (n,m)-bent functions?	Translation designs $\operatorname{dev}(\mathcal{G}_F)$	Addition designs $\mathbb{D}(F)$	Vanishing flats $\mathcal{VF}(F)$
$m = 1$	No, isomorphism is coarser for all $n \geq 6$	Yes, for all n	Yes, for $n = 4, 6$
$m \geq 2$	Yes, for $n = 4, 6$		

As one can see from Examples 3.16 and 3.21, it is possible to construct EA-inequivalent but isomorphic Boolean bent functions, by taking proper Maiorana-McFarland bent functions and extending them to infinite families using the Proposition 3.18. So far, this approach does not seem to work for vectorial bent functions:

- There is only one, up to EA-equivalence, vectorial bent function in 4 variables. Consequently, all derived translation designs are isomorphic.
- By Theorem 3.22, all isomorphic vectorial bent functions in 6 variables are also EA-equivalent.

Moreover, from Proposition 3.18, a single example of EA-inequivalent but isomorphic vectorial bent functions will lead to an infinite family and, consequently, will prove that for vectorial bent functions the isomorphism of translation designs is a coarser equivalence relation than EA-equivalence. However, since one still does not have an example of such functions, it is essential to ask the following question.

Open Problem 3.64. Do extended-affine inequivalent but isomorphic vectorial bent functions in general exist?

As we mentioned in Corollary 1.98, from the CCZ-equivalence of (n,m)-functions F and F' follows isomorphism of vanishing flats $\mathcal{VF}(F)$ and $\mathcal{VF}(F')$. In general, the converse is not true, since all APN functions lead to the incidence structure with the empty block set. However, our computational results in small dimensions show that for vectorial bent functions isomorphic vanishing flats $\mathcal{VF}(F)$ and $\mathcal{VF}(F')$ define CCZ-equivalent (and hence EA-equivalent) (n,m)-bent functions F and F'. In this way, we suggest to attack the following problem.

Open Problem 3.65. Show that Theorem 3.28 is valid for all even n.

The following problem is related to a potential characterization of bent functions, which are either quadratic or "very close" to quadratic. Kantor [62] showed that, there are 4 types of symmetric designs with a 2-transitive automorphism group. One of them is a 2-$(2^n, 2^{n-1} - 2^{k-1}, 2^{n-2} - 2^{k-1})$ design S with a 2-transitive automorphism group, which is unique for any $n = 2k$, up to isomorphism, and can be constructed using bent functions f on $\mathbb{F}_2^n$ in the following two ways. First, one can construct S as the addition design $\mathbb{D}(f)$ of a bent function f on $\mathbb{F}_2^n$, which must be quadratic by Theorem 3.52. Second, one can construct S as the translation design $\operatorname{dev}(\mathcal{D}_f)$ of a bent function f on $\mathbb{F}_2^n$, which is not necessarily quadratic, as one can see from Example 3.16. In the following problem, we suggest to describe all bent functions f on $\mathbb{F}_2^n$ such that $\operatorname{Aut}(\operatorname{dev}(\mathcal{D}_f))$ is 2-transitive.

Open Problem 3.66. Prove that the translation design $\operatorname{dev}(\mathcal{D}_f)$ of a Boolean bent function f on $\mathbb{F}_2^n$ with $n = 2k$ has a 2-transitive automorphism group if and only if function f is EA-equivalent to a Maiorana-McFarland bent function of the form $\langle \mathbf{x}, \mathbf{y} \rangle_k \oplus g(\mathbf{y})$ with $\deg(g) \leq 3$.

Li et al. [73] and Tang, Ding and Xiong [108] showed that the covalency of vanishing flats reflects differential uniformity. In this way, differentially two-valued (n,n)-functions F can be characterized in terms of vanishing flats $\mathcal{VF}(F)$ having the property to be 2-designs. In this chapter, we showed that regularity of nonvanishing flats reflects another important cryptographic property, namely plateauedness, and consequently we derived a new characterization of (n,m)-bent functions in terms of nonvanishing flats having the property to be 2-designs.

In Table 3.2, we summarize various design-theoretic characterizations of cryptographically significant classes of (n,m)-functions and mention, what kind of incidence structures one gets from the supports of codewords of a fixed weight. We denote by " $\iff$ " a condition or combination of conditions, which characterizes a certain class of (n,m)-functions, and by "$\Longrightarrow$" the properties of the supported incidence structures of a certain class of (n,m)-functions. One may observe a remarkable property of bent functions: all three constructions of incidence structures (vanishing flats, nonvanishing flats and supports of the codewords of a fixed weight) always lead to 2-designs. This is, in general, not the case for differentially two-valued (n,n)-functions and (n,m)-plateaued functions: one can see from Table 3.2 which combinatorial properties of a bent function one may lose, if one considers various generalizations.

Table 3.2. Bent functions and their generalizations from a design-theoretic point of view

Classes of (n, m)-functions F	Vanishing flats $\mathcal{VF}(F)$	Nonvanishing flats $\mathcal{NF}_{\mathbf{v}}(F)$	Supports $(\mathcal{P}(\mathcal{C}_F), \mathcal{B}_\ell(\mathcal{C}_F))$ and $(\mathcal{P}(\mathcal{C}_F^\perp), \mathcal{B}_k(\mathcal{C}_F^\perp))$
(n, m)-Bent functions	2-design $\Longleftrightarrow$ By Theorem 3.26	2-designs $\Longleftrightarrow$ By Theorem 3.42	2-designs $\Longrightarrow$ By [108, Example 4]
Differentially two-valued s-plateaued (n, n)-functions	2-design $\Longleftrightarrow$ By [108, Theorem 6.1] and Corollary 3.40	Equiregular 1-designs	2-designs $\Longrightarrow$ By [108, Theorem 6.4]
Differentially two-valued (n, n)-functions	2-design $\Longleftrightarrow$ By [108, Theorem 6.1]	Not necessarily 1-designs By Remark 3.33	TBD*
s-Plateaued (n, m)-functions	Nonvanishing flats are equiregular 1-designs $\Longleftrightarrow$ By Corollary 3.40		TBD**
Plateaued (n, m)-functions	Nonvanishing flats are 1-designs $\Longleftrightarrow$ By Theorem 3.36		TBD**

Finally, we would like to give a list of open problems, which, we think, deserve further investigations.

Open Problem 3.67. What are the incidence structures, supported by the codewords of a fixed weight arising from differentially two-valued (n, n)-functions and (n, m)-plateaued functions, marked by TBD* and TBD** (to be determined) in Table 3.2? We give some further insights.

1. Consider the TBD* entry. In general, it is difficult to say under which conditions the linear codes $\mathcal{C}_F$ and $\mathcal{C}_F^\perp$ of differentially two-valued (n, n)-functions F support 2-designs. In Theorem 3.56, we specified such a condition for APN functions having the classical Walsh spectrum in terms of the distribution of the component functions. It would be interesting to find out whether it is an if and only if condition. Another interesting problem is to investigate whether linear codes $\mathcal{C}_F$ and $\mathcal{C}_F^\perp$ of APN functions F on $\mathbb{F}_2^n$ with a nonclassical Walsh spectrum support 2-designs. A good starting point can be to look at the new instances of quadratic APN functions on $\mathbb{F}_2^8$ with a nonclassical spectrum constructed by Beierle and Leander, see [4].

2. Now we consider TBD** entries. Deleting a coordinate function from quadratic APN functions from Table 2.1, it is possible to get 1-designs from the obtained projections. However, it is not clear theoretically, why it happens, since the extended Assmus-Mattson Theorem is not applicable any more. In this way, a more careful analysis of this case is needed, although

we do not expect that one can get interesting incidence structures out of this construction (we expect at most 1-designs).

The following series of open problems is related to the design-theoretic interpretation of the extendability of bent functions.

Open Problem 3.68. Based on Theorem 3.47, develop an algorithm for the search of non-extendable bent functions and compute theoretically the complexity of the extendability problem. As a starting point, we refer to [37], where complexity of the subdesign problem is established for several classes of designs and subdesigns.

Let F be an (n,s)-bent function. Taking into account that non-existence of a 2-$(2^n,4,2^{n-s-r-1}-1)$ subdesign of a 2-$(2^n,4,2^{n-s-1}-1)$ design $\mathcal{VF}(F)$ gives information about non-extendability of F (by Theorem 3.47), it is essential to ask the following questions.

Open Problem 3.69. In general, can a 2-$(2^n,4,2^{n-s-1}-1)$ design without a 2-$(2^n,4,2^{n-s-r-1}-1)$ subdesign exist? On the other hand, assume one can find (computationally) a 2-$(2^n,4,2^{n-s-r-1}-1)$ subdesign D of $\mathcal{VF}(F)$ for an (n,s)-bent function F. Can this subdesign D be realized as $\mathcal{VF}(\tilde{F})$ of an $(n,s+r)$ function $\tilde{F}$, which contains F as a projection?

Chapter 4

Homogeneous cubic bent functions

In this chapter, we prove the existence of cubic bent functions which have simultaneously the following three properties: homogeneous, have no affine derivatives and do not belong to the completed Maiorana-McFarland class. Consequently, we show that in opposite to the cases of 6 and 8 variables, the Maiorana-McFarland construction does not describe, up to equivalence, the whole class of cubic bent functions in n variables for all $n \geq 10$.

This chapter is based on the papers by Polujan and Pott [92, 93].

4.1 Introduction

Recall that a Boolean function is called *d-homogeneous*, if all the monomials in its algebraic normal form have the same algebraic degree d. The question about existence of homogeneous cubic, i.e., 3-homogeneous, bent functions may be traced back to the Dillon's survey article [40, p. 36, Question 7], where in the context of the analysis of inequivalent cubic bent functions in six variables he asked whether every bent function must contain a quadratic term.

Considering this question regarding cubic bent functions and taking into account that affine terms do not affect the bentness, this question becomes essentially equivalent to the question of the existence of homogeneous cubic bent functions. From this point of view, homogeneous cubic bent functions may be considered as generalizations of nondegenerate quadratic forms.

Further investigations of homogeneous functions were mostly motivated by cryptographic applications. Qu, Seberry, and Pieprzyk [101] observed that homogeneous Boolean functions may have a "nice symmetry group", what may lead to faster evaluation in certain cryptographic systems. In [101], they found the first examples of homogeneous cubic bent functions on $\mathbb{F}_2^6$ and extended them to infinite families on $\mathbb{F}_2^{6n}$ using the following result, see [102].

Result 4.1. *The direct sum $h(\mathbf{x}, \mathbf{y}) = f(\mathbf{x}) \oplus g(\mathbf{y})$ is d-homogeneous bent on $\mathbb{F}_2^n \times \mathbb{F}_2^m$ if and only if the functions f and g are d-homogeneous bent on $\mathbb{F}_2^n$ and $\mathbb{F}_2^m$ respectively.*

4.1.1 The known examples and constructions

Existence of homogeneous cubic bent functions on $\mathbb{F}_2^n$ for all $n \geq 6$ was shown in two independent ways. The first approach is based on the algebraic construction of homogeneous cubic bent functions, which was proposed by Seberry, Xia and Pieprzyk [104, Theorem 8]. The second approach is based on the concatenation of homogeneous cubic bent functions in a small number of variables via direct sum using Result 4.1. The known computational construction methods of homogeneous cubic bent functions in a small number of variables include:

- Tools from the polynomial invariant theory, as it was shown by Charnes, Rötteler and Beth [34, 35].
- Exhaustive computer search, which is based on the significant reduction of the search space, suggested by Meng, Zhang, Yang and Cui [82].

In the following paragraphs, we briefly survey the mentioned above approaches.

The algebraic construction of homogeneous cubic bent functions

Seberry, Xia and Pieprzyk [104, Theorem 8] proved that one can construct homogeneous cubic bent functions on $\mathbb{F}_2^n$ for all even $n \geq 6$ with $n \neq 8$, from special Maiorana-McFarland functions by a proper linear transformation of coordinates. So far, this is the only one known algebraic construction of homogeneous cubic bent functions. For this reason, we will call this construction *primary* and denote any n-variable homogeneous cubic bent function of this type by $h^n_{pr.}$.

Result 4.2. *[104, Theorem 6] Let $\mathbb{F}_2^n$ be identified with $\mathbb{F}_2^m \times \mathbb{F}_2^m$ and let $f_{id,\phi}$ be a Maiorana-McFarland bent function on $\mathbb{F}_2^n$ where ϕ is a homogeneous cubic function without affine derivatives on $\mathbb{F}_2^m$. Then there exists a nonsingular $n \times n$-matrix $\mathbf{T}$ such that $h^n_{pr.}(\mathbf{x}, \mathbf{y}) := f_{id,\phi}((\mathbf{x}, \mathbf{y})\mathbf{T})$ is a homogeneous cubic bent function.*

Below we give an example of a homogeneous cubic bent function in six variables constructed according to Result 4.2.

Example 4.3. Let $f_{id,\phi} \colon \mathbb{F}_2^6 \to \mathbb{F}_2$ be a cubic Maiorana-McFarland bent function, given by $f_{id,\phi}(\mathbf{x}, \mathbf{y}) = x_1y_1 \oplus x_2y_2 \oplus x_3y_3 \oplus y_1y_2y_3$ and let $\mathbf{T} \in GL(6, \mathbb{F}_2)$ be given as follows

$$\mathbf{T} = \left(\begin{array}{c|c} \mathbf{I}_3 & \mathbf{I}_3 \oplus \mathbf{J}_3 \\ \hline \mathbf{O}_3 & \mathbf{I}_3 \end{array}\right).$$

Then the function $h^6_{pr.}(\mathbf{x}, \mathbf{y}) := f_{id,\phi}((\mathbf{x}, \mathbf{y})\mathbf{T})$ is a cubic bent function, since $\mathbf{T}$ is a nondegenerate linear transformation of the input preserving bentness and degree, and it is homogeneous, since its algebraic normal form is given by

$$\begin{aligned} h^6_{pr.}(\mathbf{x}, \mathbf{y}) =& x_1x_2y_1 \oplus x_1x_3y_1 \oplus x_2x_3y_1 \oplus x_1x_2y_2 \oplus x_1x_3y_2 \oplus x_2x_3y_2 \\ &\oplus x_1y_1y_2 \oplus x_2y_1y_2 \oplus x_1x_2y_3 \oplus x_1x_3y_3 \oplus x_2x_3y_3 \oplus x_1y_1y_3 \\ &\oplus x_3y_1y_3 \oplus x_2y_2y_3 \oplus x_3y_2y_3 \oplus y_1y_2y_3. \end{aligned}$$

Computer search: Polynomial invariant theory

The first computer search technique of homogeneous bent functions, which is based on the tools from polynomial invariant theory, was suggested by Charnes, Rötteler and Beth [34, 35]. The main idea of this approach is to find the set of Boolean functions, which are invariant with respect to the action of a given subgroup $G \leq \mathrm{GL}(n, \mathbb{F}_2)$, namely

$$\mathbb{F}_2 \left[x_1, \ldots, x_n\right]^G := \{f \colon f^g = f \text{ for all } g \in G\}, \tag{4.1}$$

where the operation f^g is defined as follows

$$f^g \left(x_1, \ldots, x_n\right) := f\left(\left(x_1, \ldots, x_n\right) \cdot g\right).$$

Notably, the set $\mathbb{F}_2 \left[x_1, \ldots, x_n\right]^G$ forms a ring and its elements are called *invariant polynomials*. Finally, one has to consider the subring of $\mathbb{F}_2 \left[x_1, \ldots, x_n\right]^G$, formed by d-homogeneous polynomials and search for bent functions in it. The main advantage of this approach is that the obtained subring has a significantly smaller size compared to the whole search space $\mathbb{F}_2 \left[x_1, \ldots, x_n\right]$, and the computation of the invariant polynomials can be performed very efficiently, e.g., with the help of Magma [9]. The only drawback of this approach is the following: it is not known theoretically whether a given subgroup $G \leq \mathrm{GL}(n, \mathbb{F}_2)$ necessarily leads to the ring $\mathbb{F}_2 \left[x_1, \ldots, x_n\right]^G$, containing homogeneous bent functions.

Using this approach, Charnes, Rötteler and Beth [34, 35] constructed a lot of homogeneous cubic bent functions in $6 \leq n \leq 12$ variables, however, cryptographic properties of the constructed functions in 10 and 12 variables have not been studied so far.

Computer search: Exhaustive search for the small number of variables

The second computer search technique of bent functions, which are not necessarily homogeneous, was suggested by Meng, Zhang, Yang and Cui [83]. The main idea of this approach consists of two steps. First, they introduced the following decomposition of a given bent function f on $\mathbb{F}_2^n$ into 2^k subfunctions f_i on $\mathbb{F}_2^{n-k}$.

Result 4.4. *[83] Let k, n be two positive integers such that $k \leq n$. Consider the following decomposition of a Boolean bent function $f \colon \mathbb{F}_2^n \to \mathbb{F}_2$ into the 2^k subfunctions f_i, where $i \in \mathbb{N}$ is identified with its binary representation from $\mathbb{F}_2^k$ as follows*

$$f\left(x_1, x_2, \ldots, x_n\right) = \sum_{i=0}^{2^k-1} \delta_i\left(\mathbf{x}'\right) f_i\left(\mathbf{x}''\right), \tag{4.2}$$

where $\mathbf{x}' = \left(x_1, x_2, \ldots, x_k\right), \mathbf{x}'' = \left(x_{k+1}, x_{k+2}, \ldots, x_n\right)$, and functions $\delta_i \colon \mathbb{F}_2^k \to \mathbb{F}_2$, $f_i \colon \mathbb{F}_2^{n-k} \to \mathbb{F}_2$ are defined in the following way

$$f_i\left(\mathbf{x}''\right) := f\left(i, \mathbf{x}''\right) \quad \textit{and} \quad \delta_i\left(\mathbf{x}'\right) := \begin{cases} 1, & \mathbf{x}' = i \\ 0, & \mathbf{x}' \neq i \end{cases}.$$

Then the Walsh transform of any subfunction f_i can take the following 2^k+1 values

$$\hat{\chi}_{f_i}(\mathbf{a}'') \in \{(2^k-2j)2^{n/2-k} \colon j=0,1,\ldots,2^k\}. \tag{4.3}$$

Secondly, they used the decomposition (4.2) to construct bent functions from those Boolean functions, which satisfy the condition (4.3). In this way, many Boolean functions, which do not behave like subfunctions of bent functions are eliminated, what significantly reduces the search space. Using this approach, they enumerated all homogeneous cubic bent functions in eight variables and constructed many examples in ten variables, with 2 of them being listed in [82]. Later, Charnes, Dempwolff and Pieprzyk [33] classified all homogeneous cubic bent functions in eight variables using the invariants of difference sets, however, the cryptographic properties of these 2 examples in 10 variables have not been analyzed.

Quadratic and cubic bent functions vs. their homogeneous analogues

In the following table, we summarize the known computational results about the number of cubic and homogeneous cubic bent functions in six and eight variables, as well as the number of extended-affine equivalence classes.

Table 4.1. Cubic bent vs. homogeneous cubic bent functions in 6 and 8 variables

n	Cubic bent functions on $\mathbb{F}_2^n$		Hom. cubic bent functions on $\mathbb{F}_2^n$	
	# of functions	# of eq. cl.	# of functions	# of eq. cl.
6	$42{,}372{,}288 \cdot 2^7 \approx 2^{25.33}$, [100, p. 258]	3, [103]	$30 \approx 2^{4.90}$, [102]	1, [102]
8	$5{,}386{,}705{,}781{,}653{,}504 \cdot 2^9 \approx 2^{61.25}$, [70]	8, Theorem 1.48	$293{,}760 \approx 2^{18.16}$, [83]	2, [33]

Remark 4.5. Comparing the known facts about quadratic and homogeneous quadratic bent functions with the results from Table 4.1 about cubic and homogeneous cubic bent functions, we observe the following principal differences between quadratic and cubic bent functions from the homogeneity point of view:

1. By Result 1.24, every quadratic Boolean bent function $f\colon \mathbb{F}_2^n \to \mathbb{F}_2$ is EA-equivalent to the canonical quadratic homogeneous bent function Q_n on $\mathbb{F}_2^n$, given by $Q_n\colon (x_1,\ldots,x_n) \mapsto x_1x_2 \oplus x_3x_4 \oplus \cdots \oplus x_{n-1}x_n$. However, not every cubic bent function is EA-equivalent to a homogeneous one.

2. Homogeneous quadratic bent functions form the core of all quadratic bent functions, since addition of affine terms does not affect bentness. However, in a small number of variables homogeneous cubic bent functions constitute only a tiny portion of all cubic bent functions, moreover, its asymptotic behavior is also not known.

The known non-existence results on d-homogeneous bent functions

Despite the fact that computer search techniques described in the previous paragraphs were successfully used to generate a lot of 3-homogeneous bent functions, they do not seem to work for the search of d-homogeneous bent functions with $d \geq 4$. Moreover, it is not known whether these functions can in general exist.

Open Problem 4.6. Find examples of d-homogeneous bent functions with $d \geq 4$ or prove that they do not exist.

Now we give the known non-existence results of d-homogeneous bent functions. The following result gives an upper bound on the degree of a homogeneous bent function.

Result 4.7. *[113] Homogeneous bent functions $f\colon \mathbb{F}_2^{2m} \to \mathbb{F}_2$ of degree m do not exist for $m \geq 4$. Consequently, the degree of a homogeneous bent function f on $\mathbb{F}_2^{2m}$ is at most* $\deg(f) \leq m - 1$.

Meng, Zhang, Yang and Cui [83, Theorem 3] observed that this upper bound is not tight by showing that 4-homogeneous bent functions do not exist on $\mathbb{F}_2^{10}$. Based on this observation, they suggested the following improvement of the upper bound from Result 4.7, which remains the best known so far.

Result 4.8. *[84, Theorem 1] For any non-negative integer k, there exists a positive integer N such that for $m \geqslant N$, there exist no $2m$-variable homogeneous bent functions having degree $m - k$ or more, where N is the least integer satisfying the following inequality* $2^{N-1} > \sum_{i=0}^{k+1} \binom{N+1}{i}$.

With these non-existence results, it is possible that only non-quadratic homogeneous bent functions are cubic. Moreover, among the known homogeneous cubic bent functions the only bent functions, whose cryptographic properties are note analyzed, are homogeneous cubic bent functions in ten and twelve variables constructed with computer search techniques and their concatenations. In the following subsections, we proceed with the analysis of these functions.

4.1.2 Objectives

The aim of this chapter is two-fold. First, we analyze the known homogeneous cubic bent functions in ten and twelve variables from [35, 82] and show that some of these functions do not belong to the $\mathcal{M}^\#$ class and all of them are different from the primary construction of Seberry, Xia and Pieprzyk [104]. Moreover, some of them have no affine derivatives. We also provide a construction method aimed to generate a lot of homogeneous bent functions from a single given example. Using this approach we construct 2^{21} new homogeneous cubic bent functions in 12 variables (which is almost twice as the number of previously known homogeneous cubic bent functions in $6 \leq n \leq 12$ variables), and show that some of them are new, i.e., not equivalent to all the previously known ones.

Secondly, we extend these results for infinite families by showing that proper direct sums of these functions inherit the properties of its summands. Consequently, we prove that for any $n \geq 8$ there exist cubic bent functions inside $\mathcal{M}^{\#}$, but different from the primary construction [104]. Further, we consider cubic bent functions with respect to the following three properties: outside $\mathcal{M}^{\#}$, without affine derivatives, and homogeneous. We show that n-variable cubic bent functions with at least two of the three mentioned properties exist for all $n \geq n_0$, where n_0 depends on the selected combination of properties. Moreover, we prove that in general the whole class of cubic bent functions in n variables is not described by the $\mathcal{M}^{\#}$ class, whenever $n \geq 10$. This result implies that the smallest possible degree of a bent function outside the $\mathcal{M}^{\#}$ class equals to three. From this point of view, we conclude that cubic bent functions behave like bent functions of higher degrees rather than quadratic. Finally, we show existence of cubic bent functions without affine derivatives outside $\mathcal{M}^{\#}$, thus solving an open problem addressed by Mandal, Gangopadhyay and Stănică in [77, Section 1.6].

The rest of the chapter is organized in the following way. In Section 4.2, we use design-theoretic invariants from Section 3.2 of the previous chapter to prove that proper concatenations of the homogeneous cubic functions constructed via computer search can never be equivalent to the primary construction. In Section 4.3, we introduce an algorithm aimed to produce many homogeneous functions from a single given one without increasing the number of variables and illustrate its application for homogeneous cubic bent functions in 12 variables. In Section 4.4, we consider the problem of the construction of bent functions outside the $\mathcal{M}^{\#}$ class using the direct sum. In Subsection 4.4.1, we provide a sufficient condition, explaining how one should select bent functions f and g such that the direct sum $f \oplus g$ is outside $\mathcal{M}^{\#}$. In Subsection 4.4.2, we show that certain cubic bent functions in $6 \leq n \leq 12$ variables satisfy our new sufficient condition and thus lead to infinitely many cubic bent functions outside the $\mathcal{M}^{\#}$ class, which are homogeneous or do not have affine derivatives. In Section 4.5, we conclude the chapter and raise some open problems. Finally, we list used in the chapter cubic bent functions together with their invariants in Appendix B.

4.2 Analysis of the known examples

In this section, we classify the known examples of homogeneous cubic bent functions in 10 and 12 variables constructed in [35, 82] and show that:

- Some of them are not covered, up to EA-equivalence, by the Maiorana-

McFarland construction.

- All of them are EA-inequivalent to the only one known analytic construction of Seberry, Xia and Pieprzyk, given in Result 4.4.

First, we proceed with the analysis of the homogeneous cubic bent functions in a small number of variables.

Theorem 4.9. *For homogeneous cubic bent functions in $n = 10$ and $n = 12$ variables from [35, p. 149] and [82, p. 15], respectively, the following hold.*

1. *If $n = 10$, there are 4 equivalence classes, with 2 of them being outside the completed Maiorana-McFarland class $\mathcal{M}^{\#}$.*
2. *If $n = 12$, there are 5 equivalence classes, which are subclasses of $\mathcal{M}^{\#}$.*

Proof. For the mentioned homogeneous cubic bent functions, we compute the Smith normal form and check whether the functions having the same ones are EA-equivalent. We check equivalence of bent functions via equivalence of linear codes and isomorphism of addition designs according to Result 1.60 and Result 1.94, respectively, with a Magma [9] program. Consequently, we found 4 and 5 equivalence classes in 10 and 12 variables, respectively. We denote representatives of the obtained classes by h_i^n and list them in Appendix B.1. We provide only the first $n/2$ elementary divisors for the Smith normal forms of bent functions due to Remark 3.11.

Table 4.2. First $n/2$ elementary divisors of the known homogeneous cubic bent functions in $n = 10, 12$ variables

4.2(a) $n = 10$ variables

h_i^{10}	SNF(h_i^{10})
h_1^{10}	$\{*1^{20}, 2^{86}, 4^{130}, 8^{143}, 16^{268}, \cdots *\}$
h_2^{10}	$\{*1^{20}, 2^{78}, 4^{138}, 8^{147}, 16^{260}, \cdots *\}$
h_3^{10}	$\{*1^{20}, 2^{108}, 4^{110}, 8^{129}, 16^{292}, \cdots *\}$
h_4^{10}	$\{*1^{22}, 2^{154}, 4^{90}, 8^{81}, 16^{332}, \cdots *\}$

4.2(b) $n = 12$ variables

h_i^{12}	SNF(h_i^{12})
h_1^{12}	$\{*1^{22}, 2^{142}, 4^{276}, 8^{493}, 16^{630}, 32^{972}, \cdots *\}$
h_2^{12}	$\{*1^{22}, 2^{126}, 4^{276}, 8^{517}, 16^{646}, 32^{924}, \cdots *\}$
h_3^{12}	$\{*1^{24}, 2^{127}, 4^{260}, 8^{525}, 16^{674}, 32^{878}, \cdots *\}$
h_4^{12}	$\{*1^{22}, 2^{104}, 4^{256}, 8^{525}, 16^{698}, 32^{888}, \cdots *\}$
h_5^{12}	$\{*1^{26}, 2^{196}, 4^{392}, 8^{419}, 16^{490}, 32^{1052}, \cdots *\}$

We used a parallel implementation of Algorithm 1.1 in Mathematica [112] in order to check whether the functions h_i^n belong to $\mathcal{M}^{\#}$. As a result, only functions h_3^{10} and h_4^{10} in ten variables do not belong to the $\mathcal{M}^{\#}$ class, while all functions h_i^{12} in twelve variable are in $\mathcal{M}^{\#}$. Finally, we list all $\mathcal{M}$-subspaces of functions h_i^n from $\mathcal{M}^{\#}$ in Appendix B.2. □

Using the facts about ranks of bent functions and the relation between Γ-rank and rank, obtained in the previous chapter, we derive the following corollary.

Corollary 4.10. *Let f and g be Boolean functions on $\mathbb{F}_2^n$ and $\mathbb{F}_2^m$, respectively, with* $\deg(f) \geq 1$ *and* $\deg(g) \geq 1$.

1. *Let h be a Boolean function on $\mathbb{F}_2^n \times \mathbb{F}_2^m$ defined as the direct sum of functions f on $\mathbb{F}_2^n$ and g on $\mathbb{F}_2^m$, then*

$$\Gamma\text{-rank}(h) = \Gamma\text{-rank}(f) + \Gamma\text{-rank}(g) - 2. \tag{4.4}$$

2. *Let $f_{id,\phi}$ be a Maiorana-McFarland bent function on $\mathbb{F}_2^n$, then*

$$\Gamma\text{-rank}(f_{id,\phi}) = n + 2 \textit{ if and only if } \deg(\phi) \leq 3. \tag{4.5}$$

3. *For the primary construction of homogeneous cubic bent functions $h^n_{pr.}$ on $\mathbb{F}_2^n$ we have $\Gamma\text{-rank}(h^n_{pr.}) = n + 2$.*

Proof. The first and the second claims hold, since the statements (4.4) and (4.5) were proven in [110, 111] for ranks, and by Theorem 3.4 we know that ranks and Γ-ranks coincide for all non-constant Boolean functions. Finally, the third claim follows from (4.5) and the definition of the primary construction. □

Now we prove the existence of homogeneous cubic bent functions on $\mathbb{F}_2^n$, which are EA-inequivalent to the primary construction for any $n \geq 8$.

Theorem 4.11. *There exist homogeneous cubic bent functions on $\mathbb{F}_2^n$, extended-affine inequivalent to the primary construction $h^n_{pr.}$, whenever $n \geq 8$.*

Proof. We construct a homogeneous cubic bent function h_n in n variables with $n = 6i + 8j + 10k + 12l$ and $j + k + l \neq 0$ as the following concatenation:

$$h_n := i \cdot h^6_* \oplus j \cdot h^8_* \oplus k \cdot h^{10}_* \oplus l \cdot h^{12}_*, \tag{4.6}$$

where h^6_* and h^8_* are arbitrary homogeneous cubic bent functions in 6 and 8 variables respectively, and h^{10}_*, h^{12}_* are arbitrary homogeneous cubic bent functions in 10 and 12 variables from Table 4.2. Since any homogeneous cubic bent function in 6 variables is equivalent to the primary construction $h^6_{pr.}$, we have $\Gamma\text{-rank}(h^6_*) = 8$. One can check that for any cubic bent function h^8_* in 8 variables we have $\Gamma\text{-rank}(h^8_*) \in \{14, 16\}$. By Theorem 3.10, we have that Γ-ranks of functions h^{10}_* and h^{12}_* are multiplicities of the entry one in Table 4.2. Finally, comparing the lower bound of the $\Gamma\text{-rank}(h_n)$ with $\Gamma\text{-rank}(h^n_{pr.})$, one can see that

$$\begin{aligned}\Gamma\text{-rank}(h_n) &\geq 8i + 14j + 20k + 22l - 2(i + j + k + l - 1) \\ &= n + 2 + 4(j + 2(k + l)) > n + 2 = \Gamma\text{-rank}(h^n_{pr.})'\end{aligned}$$

and hence the function h_n is EA-inequivalent to $h^n_{pr.}$ for all $n \geq 8$. □

4.3 Constructing new homogeneous bent functions from old

In this section, we show that in some cases it is possible to use the power of the Maiorana-McFarland construction in order to construct a lot of homogeneous bent functions from a single one, which is a member of the $\mathcal{M}^{\#}$ class. Our approach is based on a generalization of the following observation.

Observation 4.12. Let $f := h_3^{12}$ and $g := h_4^{12}$. Using Algorithm 1.1, it is possible to show that homogeneous cubic bent functions f and g have a common $\mathcal{M}$-subspace U of dimension 6. The vector space U and its complement $\bar{U}$ are generated by the row vectors, forming their Gauss-Jordan bases as follows

$$U = \left\langle \begin{array}{c|c|c} 1\,1 & \multicolumn{2}{c}{\mathbf{O}_{1,10}} \\ \hline \mathbf{O}_{5,2} & \mathbf{I}_5 & \mathbf{I}_5 \end{array} \right\rangle \quad \text{and} \quad \bar{U} = \left\langle \begin{array}{c|c|c} 0\,1 & \multicolumn{2}{c}{\mathbf{O}_{1,10}} \\ \hline \mathbf{O}_{5,2} & \mathbf{O}_5 & \mathbf{I}_5 \end{array} \right\rangle . \tag{4.7}$$

It is possible to bring functions f and g to their Maiorana-McFarland representations (1.23) using the same linear invertible transformation $\mathbf{A}_U$, given by (1.26):

$$f(\mathbf{z}\mathbf{A}_U) = f_{\pi,\phi}(\mathbf{x},\mathbf{y}) \quad \text{and} \quad g(\mathbf{z}\mathbf{A}_U) = g_{\pi,\psi}(\mathbf{x},\mathbf{y}),$$

where $\pi\colon \mathbb{F}_2^6 \to \mathbb{F}_2^6$ is a permutation and $\phi, \psi\colon \mathbb{F}_2^6 \to \mathbb{F}_2$ are Boolean functions. In this way, one can construct homogeneous function g from the function f in the following way

$$g(\mathbf{z}) := f_{\pi,\phi\oplus\omega}((\mathbf{x},\mathbf{y})\mathbf{T}), \text{ where } \omega := \phi \oplus \psi \text{ and } \mathbf{T} := \mathbf{A}_U^{-1}. \tag{4.8}$$

Let $h_{\pi,\phi}\colon \mathbb{F}_2^n \to \mathbb{F}_2$ be a bent function from the $\mathcal{M}^{\#}_{r,s}$ class, which is EA-equivalent to a d-homogeneous one, i.e., there exist an invertible matrix $\mathbf{T}$ of order n such that $h_{\pi,\phi}((\mathbf{x},\mathbf{y})\mathbf{T})$ is d-homogeneous. The following set

$$\Omega_{\mathbf{T}}(h_{\pi,\phi}) := \{\omega\colon \mathbb{F}_2^s \to \mathbb{F}_2 \mid h_{\pi,\phi\oplus\omega}((\mathbf{x},\mathbf{y})\mathbf{T}) \text{ is } d\text{-homogeneous bent}\}$$

contains all Boolean functions ω on $\mathbb{F}_2^s$, which preserve d-homogeneity and bentness of the function $h_{\pi,\phi\oplus\omega}$ with respect to the linear transformation $\mathbf{T}$.

Proposition 4.13. *Let $h_{\pi,\phi}$ be a Maiorana-McFarland bent function on $\mathbb{F}_2^{2m}$, which is EA-equivalent to a d-homogeneous bent function, i.e., there exist an invertible matrix $\mathbf{T}$ such that $h_{\pi,\phi}((\mathbf{x},\mathbf{y})\mathbf{T})$ is d-homogeneous bent. Then the set $\Omega_{\mathbf{T}}(h_{\pi,\phi})$ is a vector space over $\mathbb{F}_2$.*

Proof. Let $\omega_1, \omega_2 \in \Omega_{\mathbf{T}}(h_{\pi,\phi})$ with $\omega_1 \neq \omega_2$ and $\omega := \omega_1 \oplus \omega_2$. We will show that $\omega \in \Omega_{\mathbf{T}}(h_{\pi,\phi})$. Let the invertible matrix $\mathbf{T}$ be of the form $\mathbf{T} = \begin{pmatrix} \mathbf{A} & \mathbf{B} \\ \mathbf{C} & \mathbf{D} \end{pmatrix}$, where all submatrices have order m. First, we observe that $0 \in \Omega_{\mathbf{T}}(h_{\pi,\phi})$ and for any $\omega_i \in \Omega_{\mathbf{T}}(h_{\pi,\phi})$ we have

$$h_{\pi,\phi\oplus\omega_i}((\mathbf{x},\mathbf{y})\mathbf{T}) = h_{\pi,\phi}((\mathbf{x},\mathbf{y})\mathbf{T}) \oplus \omega_i(\mathbf{xB} \oplus \mathbf{yD}),$$

consequently, $\omega_i(\mathbf{xB} \oplus \mathbf{yD})$ is either d-homogeneous or constant zero function, since $h_{\pi,\phi}((\mathbf{x},\mathbf{y})\mathbf{T})$ is d-homogeneous. Thus $\omega \in \Omega_{\mathbf{T}}(h_{\pi,\phi})$, since bentness of $h_{\pi,\phi\oplus\omega}$ is independent of the choice of a function ω on $\mathbb{F}_2^m$ and, hence, the function $(\mathbf{x},\mathbf{y}) \mapsto \omega(\mathbf{xB} \oplus \mathbf{yD})$ is d-homogeneous. □

Note that for a homogeneous bent function $h_{\pi,\phi} \in \mathcal{M}^{\#}_{r,s}$, the set $\Omega_{\mathbf{T}}(h_{\pi,\phi})$ is not a vector space in general. Nevertheless, for a given homogeneous bent function $h \in \mathcal{M}^{\#}_{r,s}$ one can still construct the set $\Omega_{\mathbf{T}}(h_{\pi,\phi})$, in order to get more (possibly inequivalent) homogeneous functions. We summarize these ideas in the form of an algorithm below.

Algorithm 4.1. New d-homogeneous bent functions from a single one in $\mathcal{M}^{\#}_{r,s}$

```
Require: Homogeneous bent function $h : \mathbb{F}_2^n \to \mathbb{F}_2, h \in \mathcal{M}^{\#}_{r,s}$ of degree $d$.
Ensure: The set $H$ of new $d$-homogeneous bent functions from $\mathcal{M}^{\#}_{r,s}$.
Put $H \leftarrow \{\}$.
for all $\mathcal{M}$-subspaces $U \in \mathcal{MS}_r(h)$ do
    Construct the linear mapping $\mathbf{A}_U$ (1.26), in order to get the
    Maiorana-McFarland representation (1.23), i.e., $h_{\pi,\phi}(\mathbf{x},\mathbf{y}) := h(\mathbf{z}\mathbf{A}_U)$.
    Put $H \leftarrow H \cup \{h_{\pi,\phi\oplus\omega}((\mathbf{x},\mathbf{y})\mathbf{T}) \colon \omega \in \Omega_{\mathbf{T}}(h_{\pi,\phi})\}$, where $\mathbf{T} := \mathbf{A}_U^{-1}$.
end for
```

Remark 4.14. Using Algorithm 4.1 and the mapping $\mathbf{T}$ defined in (4.8), one can construct $2^{\binom{6}{3}}$, i.e., the maximum number of new homogeneous cubic bent functions from each of the functions h_3^{12} and h_5^{12}, members of the $\mathcal{M}^{\#}$ class, thus 2^{21} in total. The maximality of the number of new functions can be explained in the following way. Let $h \in \{h_3^{12}, h_5^{12}\}$. First, we observe that the image of $\mathbf{y}$ after the linear transformation $\mathbf{y} \mapsto \mathbf{y}' = \mathbf{xB} \oplus \mathbf{yD}$ is given by:

$$\mathbf{y} \mapsto \mathbf{y}' = (x_1 \oplus x_2, x_3 \oplus y_2, x_4 \oplus y_3, x_5 \oplus y_4, x_6 \oplus y_5, y_1 \oplus y_6). \tag{4.9}$$

Since any two coordinates of the vector $\mathbf{y}'$ do not contain common variables x_i and y_j, the linear transformation defined in (4.9) is homogeneity-preserving. Thus, $\Omega_{\mathbf{T}}(h_{\pi,\phi})$ is generated by monomials $\omega \colon \mathbb{F}_2^6 \to \mathbb{F}_2$ of degree 3, and hence $|\Omega_{\mathbf{T}}(h_{\pi,\phi})| = 2^{\binom{6}{3}}$. Taking into the account that the total number of the known homogeneous cubic bent functions in $6 \le n \le 12$ equals to

$$\underbrace{30 + 293{,}760}_{\text{total \# in 6,8 variables}} + \underbrace{200 + 480 + 2}_{\text{constructed in [35, 82]}} + \underbrace{868 + 992{,}496}_{\text{primary construction for } n = 10, 12} \approx 2^{20.3},$$

we conclude that with our approach we constructed almost twice the total number of the known homogeneous cubic bent functions. Finally, we note that some of the constructed homogeneous cubic bent functions are EA-inequivalent to all the known ones, since their Smith normal forms listed in Table 4.3 are different from those given in Table 4.2.

Table 4.3. First $n/2$ elementary divisors of the new homogeneous cubic bent functions in $n = 12$ variables

h_i^{12}	$\mathrm{SNF}(h_i^{12})$
h_6^{12}	$\{*1^{24}, 2^{123}, 4^{292}, 8^{497}, 16^{674}, 32^{878}, \cdots *\}$
h_7^{12}	$\{*1^{24}, 2^{123}, 4^{272}, 8^{516}, 16^{674}, 32^{880}, \cdots *\}$

Theorem 4.15. *There are at least 7 pairwise EA-inequivalent homogeneous cubic bent functions on $\mathbb{F}_2^{12}$, which are EA-inequivalent to $h_{pr.}^{12}$.*

4.4 Bent functions outside the $\mathcal{M}^{\#}$ class via direct sum construction

The existence of Boolean bent functions of all degrees $d \geq 4$ outside the completed Maiorana-McFarland class $\mathcal{M}^{\#}$ was firstly shown by Dillon in his thesis. For the sake of reader's convenience, we give a sketch of his proof below.

Result 4.16. *[41, p. 104] For all $m > 3$ there exist bent functions of degree $d \geq 4$ on $\mathbb{F}_2^{2m}$ which are not equivalent to any bent function in $\mathcal{M}^{\#}$.*

Proof. Consider the following $\mathcal{PS}_{ap}$ bent function f on $\mathbb{F}_{2^8}$ in cyclotomic form, which has the algebraic degree 4:

$$f\colon x \in \mathbb{F}_{2^8} \mapsto \mathrm{Tr}(x^{15}).$$

Since the second-order derivative of f has the form

$$D_{a,b}f(x) = \mathrm{Tr}((a^6 + b^6 + (a+b)^6)x^9) + q_{a,b}(x),$$

where $q_{a,b}$ is a quadratic function on $\mathbb{F}_{2^8}$ depending on $a, b \in \mathbb{F}_{2^8}$, one concludes that $\deg(D_{a,b}f) = 2$ for all $a, b \in \mathbb{F}_{2^8}$ with $a, b \neq 0$ simultaneously. In this way, for any nonzero $a, b \in \mathbb{F}_{2^8}$ the second-order derivative $D_{a,b}f$ is never a constant function and by Proposition 1.36 the direct sum $f + g \notin \mathcal{M}^{\#}$, where g is a bent function of degree d on $\mathbb{F}_{2^{2m-8}}$. □

In this way, a single bent function without constant second-order derivatives gives a rise to infinitely many bent functions outside the completed Maiorana-McFarland class having all possible degrees $d \geq 4$. In the following proposition we show that the same argument can not be used to prove the existence of cubic bent functions outside $\mathcal{M}^\#$, since any cubic bent function has nontrivial constant second-order derivatives.

Proposition 4.17. *Let f be a cubic bent function on $\mathbb{F}_2^n$. Then there exist linearly independent $\mathbf{a}, \mathbf{b} \in \mathbb{F}_2^n$ such that $D_{\mathbf{a},\mathbf{b}} f = const.$*

Proof. We prove this statement by contradiction. Recall that by Result 1.14, a Boolean function f on $\mathbb{F}_2^n$ is bent if and only if the following condition holds

$$\sum_{\mathbf{a},\mathbf{b},\mathbf{x} \in \mathbb{F}_2^n} (-1)^{D_{\mathbf{a},\mathbf{b}} f(\mathbf{x})} = 2^{2n}. \tag{4.10}$$

Now we assume that for all linearly independent $\mathbf{a}, \mathbf{b} \in \mathbb{F}_{2^n}$ holds $D_{\mathbf{a},\mathbf{b}} f \neq$ const. In this way, all second-order derivatives are non-constant affine functions, and hence balanced. Consequently, we have that

$$\sum_{\mathbf{a},\mathbf{b},\mathbf{x} \in \mathbb{F}_2^n} (-1)^{D_{\mathbf{a},\mathbf{b}} f(\mathbf{x})} = (2 \cdot (2^n - 1) + 2^n) \cdot 2^n. \tag{4.11}$$

This leads to a contradiction to (4.10). □

From this point of view, cubic bent functions behave similarly to quadratic bent functions, since they always have constant second-order derivatives. Consequently, this property can potentially lead to the situation that constant second-order derivatives of bent functions f on $\mathbb{F}_2^n$ and g on $\mathbb{F}_2^m$ may "balance each other" and thus the direct sum $f \oplus g$ may be inside $\mathcal{M}^\#$ class by Proposition 1.36. Let us illustrate the problem in more detail on the following example.

Example 4.18. Consider bent functions f on $\mathbb{F}_2^4$ and g on $\mathbb{F}_2^2$, which are given by $f(\mathbf{x}) := x_1x_2 \oplus x_3x_4$ and $g(\mathbf{y}) := y_1y_2$. Let $V \subset \mathbb{F}_2^4$ and $W = \mathbb{F}_2^2$ be two vector subspaces of dimension 3 and 2, respectively, which are given by

$$V = \left\langle \begin{array}{cccc} 1 & 0 & 0 & 1 \\ 0 & 1 & 0 & 1 \\ 0 & 0 & 1 & 1 \end{array} \right\rangle \quad \text{and} \quad W = \left\langle \begin{array}{cc} 1 & 0 \\ 0 & 1 \end{array} \right\rangle.$$

Consider also the following 3-dimensional vector subspace $U \subset V \times W$, given by its generators as follows.

$$U = \left\langle \begin{array}{cccccc} 1 & 0 & 0 & 1 & 0 & 1 \\ 0 & 1 & 0 & 1 & 1 & 0 \\ 0 & 0 & 1 & 1 & 1 & 1 \end{array} \right\rangle \subset V \times W$$

One can observe that the vector subspace U is an $\mathcal{M}$-subspace of the function $h := f \oplus g$ on $\mathbb{F}_2^4 \times \mathbb{F}_2^2$, since the second-order derivatives $D_{\mathbf{a},\mathbf{b}} h$ corresponding to two-dimensional vector subspaces $\langle \mathbf{a}, \mathbf{b} \rangle$ of U are constant zero functions. We list them in the following form $\langle \mathbf{a}, \mathbf{b} \rangle \mapsto D_{\mathbf{a},\mathbf{b}}h$ below

$$\left\langle \begin{array}{cccccc} 0 & 1 & 0 & 1 & 1 & 0 \\ 0 & 0 & 1 & 1 & 1 & 1 \end{array} \right\rangle \mapsto 0, \left\langle \begin{array}{cccccc} 1 & 0 & 0 & 1 & 0 & 1 \\ 0 & 0 & 1 & 1 & 1 & 1 \end{array} \right\rangle \mapsto 0, \left\langle \begin{array}{cccccc} 1 & 1 & 0 & 0 & 1 & 1 \\ 0 & 0 & 1 & 1 & 1 & 1 \end{array} \right\rangle \mapsto 0, \left\langle \begin{array}{cccccc} 1 & 0 & 0 & 1 & 0 & 1 \\ 0 & 1 & 0 & 1 & 1 & 0 \end{array} \right\rangle \mapsto 0,$$
$$\left\langle \begin{array}{cccccc} 1 & 0 & 1 & 0 & 1 & 0 \\ 0 & 1 & 0 & 1 & 1 & 0 \end{array} \right\rangle \mapsto 0, \left\langle \begin{array}{cccccc} 1 & 0 & 0 & 1 & 0 & 1 \\ 0 & 1 & 1 & 0 & 0 & 1 \end{array} \right\rangle \mapsto 0, \left\langle \begin{array}{cccccc} 1 & 0 & 1 & 0 & 1 & 0 \\ 0 & 1 & 1 & 0 & 0 & 1 \end{array} \right\rangle \mapsto 0.$$

Identifying vectors $\mathbf{a}, \mathbf{b} \in \mathbb{F}_2^6$ with pairs $\mathbf{a} = (\mathbf{a_x}, \mathbf{a_y})$ and $\mathbf{b} = (\mathbf{b_x}, \mathbf{b_y})$, where $\mathbf{a_x}, \mathbf{b_x} \in \mathbb{F}_2^4$ and $\mathbf{a_y}, \mathbf{b_y} \in \mathbb{F}_2^2$, we compute the second-order derivatives of functions f and g, namely $\langle \mathbf{a_x}, \mathbf{b_x} \rangle \mapsto D_{\mathbf{a_x},\mathbf{b_x}}f$ and $\langle \mathbf{a_y}, \mathbf{b_y} \rangle \mapsto D_{\mathbf{a_y},\mathbf{b_y}}g$ as follows.

$\langle \mathbf{a_x}, \mathbf{b_x} \rangle \mapsto D_{\mathbf{a_x},\mathbf{b_x}}f$	$\langle \mathbf{a_y}, \mathbf{b_y} \rangle \mapsto D_{\mathbf{a_y},\mathbf{b_y}}g$
$\left\langle \begin{array}{cccc} 0 & 1 & 0 & 1 \\ 0 & 0 & 1 & 1 \end{array} \right\rangle \mapsto 1$	$\left\langle \begin{array}{cc} 1 & 0 \\ 1 & 1 \end{array} \right\rangle \mapsto 1$
$\left\langle \begin{array}{cccc} 1 & 0 & 0 & 1 \\ 0 & 0 & 1 & 1 \end{array} \right\rangle \mapsto 1$	$\left\langle \begin{array}{cc} 0 & 1 \\ 1 & 1 \end{array} \right\rangle \mapsto 1$
$\left\langle \begin{array}{cccc} 1 & 1 & 0 & 0 \\ 0 & 0 & 1 & 1 \end{array} \right\rangle \mapsto 0$	$\left\langle \begin{array}{cc} 1 & 1 \\ 1 & 1 \end{array} \right\rangle \mapsto 0$
$\left\langle \begin{array}{cccc} 1 & 0 & 0 & 1 \\ 0 & 1 & 0 & 1 \end{array} \right\rangle \mapsto 1$	$\left\langle \begin{array}{cc} 0 & 1 \\ 1 & 0 \end{array} \right\rangle \mapsto 1$
$\left\langle \begin{array}{cccc} 1 & 0 & 1 & 0 \\ 0 & 1 & 0 & 1 \end{array} \right\rangle \mapsto 0$	$\left\langle \begin{array}{cc} 1 & 0 \\ 1 & 0 \end{array} \right\rangle \mapsto 0$
$\left\langle \begin{array}{cccc} 1 & 0 & 0 & 1 \\ 0 & 1 & 1 & 0 \end{array} \right\rangle \mapsto 0$	$\left\langle \begin{array}{cc} 0 & 1 \\ 0 & 1 \end{array} \right\rangle \mapsto 0$
$\left\langle \begin{array}{cccc} 1 & 0 & 1 & 0 \\ 0 & 1 & 1 & 0 \end{array} \right\rangle \mapsto 1$	$\left\langle \begin{array}{cc} 1 & 0 \\ 0 & 1 \end{array} \right\rangle \mapsto 1$

From this example, one can see that although the vector subspace V is not an $\mathcal{M}$-subspace of the function f, one can still find a suitable vector subspace W for a function g such that the product $V \times W$ contains an $\mathcal{M}$-subspace U of the direct sum $h := f \oplus g$ and, hence the function h is a member of the completed Maiorana-McFarland class.

In the following subsection, we show how one can avoid the situation in Example 4.18 and choose bent functions f and g such that the direct sum $f \oplus g$ is not a member of the completed Maiorana-McFarland class $\mathcal{M}^{\#}$. Using this recursive approach, we prove the series of results about the existence of cubic bent functions outside the $\mathcal{M}^{\#}$ class, which can simultaneously be homogeneous and have no affine derivatives.

4.4.1 The sufficient condition in terms of relaxed $\mathcal{M}$-subspaces

Now we identify $\mathbb{F}_2^{n+m}$ with $\mathbb{F}_2^n \times \mathbb{F}_2^m$. In this way, any vector $\mathbf{v} \in \mathbb{F}_2^{n+m}$ is uniquely represented by a pair $(\mathbf{v_x}, \mathbf{v_y})$, where $\mathbf{v_x} \in \mathbb{F}_2^n$ and $\mathbf{v_y} \in \mathbb{F}_2^m$. Let f be a bent function on $\mathbb{F}_2^n$, g be a bent function on $\mathbb{F}_2^m$ and $h := f \oplus g$ be defined as the direct sum of f and g on $\mathbb{F}_2^{n+m}$. Assume that h is a Maiorana-McFarland bent function, i.e., there exists $U \in \mathcal{MS}(h)$ such that for all $\mathbf{a}, \mathbf{b} \in U$ we have that second-order derivatives satisfy $D_{\mathbf{a},\mathbf{b}}h = 0$. This takes place if and only if $D_{\mathbf{a}_\mathbf{x},\mathbf{b}_\mathbf{x}}f = D_{\mathbf{a}_\mathbf{y},\mathbf{b}_\mathbf{y}}g = c_{\mathbf{a},\mathbf{b}}$, where $c_{\mathbf{a},\mathbf{b}} \in \mathbb{F}_2$ is a constant, depending on $\mathbf{a}$ and $\mathbf{b}$, since f and g do not have common variables. This observation leads to the following generalization of $\mathcal{M}$-subspaces, introduced in Definition 1.37.

Definition 4.19. We call a vector subspace U of $\mathbb{F}_2^n$ a *relaxed $\mathcal{M}$-subspace* of a Boolean function $f\colon \mathbb{F}_2^n \to \mathbb{F}_2$, if for all $\mathbf{a}, \mathbf{b} \in U$ second-order derivatives $D_{\mathbf{a},\mathbf{b}}f$ are either constant zero or constant one functions, i.e., $D_{\mathbf{a},\mathbf{b}}f = 0$ or $D_{\mathbf{a},\mathbf{b}}f = 1$. We denote by $\mathcal{RMS}_r(f)$ the collection of all r-dimensional relaxed $\mathcal{M}$-subspaces of the function f and by $\mathcal{RMS}(f)$ the collection of relaxed $\mathcal{M}$-subspaces

$$\mathcal{RMS}(f) := \bigcup_{r=1}^{n} \mathcal{RMS}_r(f).$$

Since the linearity index of a Boolean function (see Definition 1.34) is defined as the maximal possible dimension of its $\mathcal{M}$-subspace, it is reasonable to define its analogue for relaxed $\mathcal{M}$-subspaces.

Definition 4.20. For a Boolean function $f\colon \mathbb{F}_2^n \to \mathbb{F}_2$ its *relaxed linearity index* r-ind(f) is defined by r-ind$(f) := \max\limits_{U \in \mathcal{RMS}(f)} \dim(U)$.

Example 4.21. Consider the following cubic Maiorana-McFarland bent function on $\mathbb{F}_2^6$, given by $f(\mathbf{x}) := x_1x_4 \oplus x_2x_5 \oplus x_3x_6 \oplus x_1x_2x_3$. One can check that the subspace $U = \langle (0,1,0,0,0,1), (0,0,0,1,0,0), (0,0,0,0,1,1) \rangle$ is a relaxed $\mathcal{M}$-subspace of f, since its second-order derivatives $D_{\mathbf{a},\mathbf{b}}f$, corresponding to all two-dimensional vector subspaces $\langle \mathbf{a}, \mathbf{b} \rangle$ of U, are constant zero or constant one functions. We list them in the following form $\langle \mathbf{a}, \mathbf{b} \rangle \mapsto D_{\mathbf{a},\mathbf{b}}f$ below

$$\left\langle \begin{matrix} 0&0&0&1&0&0 \\ 0&0&0&0&1&1 \end{matrix} \right\rangle \mapsto 0, \left\langle \begin{matrix} 0&1&0&0&0&1 \\ 0&0&0&0&1&1 \end{matrix} \right\rangle \mapsto 1, \left\langle \begin{matrix} 0&1&0&1&0&1 \\ 0&0&0&0&1&1 \end{matrix} \right\rangle \mapsto 1, \left\langle \begin{matrix} 0&1&0&0&0&1 \\ 0&0&0&1&0&0 \end{matrix} \right\rangle \mapsto 0,$$

$$\left\langle \begin{matrix} 0&1&0&0&1&0 \\ 0&0&0&1&0&0 \end{matrix} \right\rangle \mapsto 0, \left\langle \begin{matrix} 0&1&0&0&0&1 \\ 0&0&0&1&1&1 \end{matrix} \right\rangle \mapsto 1, \left\langle \begin{matrix} 0&1&0&0&1&0 \\ 0&0&0&1&1&1 \end{matrix} \right\rangle \mapsto 1.$$

Now we present some properties of collections of $\mathcal{M}$-subspaces as well as of the relaxed ones.

Proposition 4.22. *Let $f\colon \mathbb{F}_2^n \to \mathbb{F}_2$ be a Boolean function and let $n = r + s$. Then the following hold.*

1. $\mathcal{MS}(f) \subseteq \mathcal{RMS}(f)$.

2. $|\mathcal{MS}_r(f)|$ *and* $|\mathcal{RMS}_r(f)|$ *as well as* ind(f) *and* r-ind(f) *are invariants under equivalence.*

3. ind$(f) \leq$ r-ind(f) *and* $f \notin \mathcal{M}^{\#}_{r,s}$ *for all* $r >$ r-ind(f).

Proof. 1. This follows from the definitions of collections $\mathcal{MS}(f)$ and $\mathcal{RMS}(f)$.
2. Let f and f' be equivalent, i.e., $f'(\mathbf{x}) = f(\mathbf{x}\mathbf{A}) \oplus l(\mathbf{x})$. Assume $U \in \mathcal{RMS}_r(f)$ and let $U' = U\mathbf{A}^{-1}$ with $\mathbf{a}', \mathbf{b}' \in U'$. Denoting $\mathbf{y} = \mathbf{x}\mathbf{A}$, one can see from the following computations

$$\begin{aligned} D_{\mathbf{a}',\mathbf{b}'}f'(\mathbf{x}) &= f'(\mathbf{x} \oplus \mathbf{a}' \oplus \mathbf{b}') \oplus f'(\mathbf{x} \oplus \mathbf{a}') \oplus f'(\mathbf{x} \oplus \mathbf{b}') \oplus f'(\mathbf{x}') \\ &= f(\mathbf{y} \oplus \mathbf{a} \oplus \mathbf{b}) \oplus f(\mathbf{y} \oplus \mathbf{a}) \oplus f(\mathbf{y} \oplus \mathbf{b}) \oplus f(\mathbf{y}) = D_{\mathbf{a},\mathbf{b}}f(\mathbf{y}) \end{aligned}$$

that $U' \in \mathcal{RMS}_r(f')$. Since $\mathbf{A}^{-1}$ maps different subspaces to different ones, we have that $|\mathcal{RMS}_r(f)| = |\mathcal{RMS}_r(f')|$ and $|\mathcal{MS}_r(f)| = |\mathcal{MS}_r(f')|$. Since $\dim(U) = \dim(U')$, we have $\text{ind}(f) = \text{ind}(f')$ and $\text{r-ind}(f) = \text{r-ind}(f')$.
3. First, since $\mathcal{MS}(f) \subseteq \mathcal{RMS}(f)$ the inequality $\text{ind}(f) \leq \text{r-ind}(f)$ holds. The statement $f \notin \mathcal{M}^\#_{r,s}$ for all $r > \text{r-ind}(f)$ now follows from the maximality of the linearity index. □

In the next theorem, we show that each relaxed $\mathcal{M}$-subspace of $f \oplus g$ is contained in another relaxed $\mathcal{M}$-subspace from $\mathcal{RMS}(f \oplus g)$, which is constructed as the direct product of relaxed $\mathcal{M}$-subspaces of f and g.

Theorem 4.23. *Let $h(\mathbf{x}, \mathbf{y}) := f(\mathbf{x}) \oplus g(\mathbf{y})$, for $\mathbf{x} \in \mathbb{F}_2^n$ and $\mathbf{y} \in \mathbb{F}_2^m$.*

1. *If $V \in \mathcal{RMS}(f)$ and $W \in \mathcal{RMS}(g)$, then $V \times W \in \mathcal{RMS}(h)$.*
2. *For any $U \in \mathcal{RMS}(h)$ there exist $V \in \mathcal{RMS}(f)$ and $W \in \mathcal{RMS}(g)$ such that $U \subseteq V \times W$.*
3. $\text{r-ind}(h) \leq \text{r-ind}(f) + \text{r-ind}(g)$.

Proof. 1. Let $U = V \times W$. Since $V \in \mathcal{RMS}(f)$ and $W \in \mathcal{RMS}(g)$, then for all $\mathbf{v}_1, \mathbf{v}_2 \in V$ holds $D_{\mathbf{v}_1,\mathbf{v}_2}f = c_{\mathbf{v}_1,\mathbf{v}_2}$ and for all $\mathbf{w}_1, \mathbf{w}_2 \in W$ holds $D_{\mathbf{w}_1,\mathbf{w}_2}g = c_{\mathbf{w}_1,\mathbf{w}_2}$, where $c_{\mathbf{v}_1,\mathbf{v}_2}$ and $c_{\mathbf{w}_1,\mathbf{w}_2}$ are some constants. In this way, for all pairs $\mathbf{u}_1 = (\mathbf{v}_1, \mathbf{w}_1)$ and $\mathbf{u}_2 = (\mathbf{v}_2, \mathbf{w}_2)$ holds $D_{\mathbf{u}_1,\mathbf{u}_2}h = D_{\mathbf{v}_1,\mathbf{v}_2}f \oplus D_{\mathbf{w}_1,\mathbf{w}_2}g = c_{\mathbf{v}_1,\mathbf{v}_2} \oplus c_{\mathbf{w}_1,\mathbf{w}_2}$ and, hence, $U \in \mathcal{RMS}(h)$.
2. Recall that any vector $\mathbf{v} \in \mathbb{F}_2^{n+m}$ is identified with a pair $(\mathbf{v}_\mathbf{x}, \mathbf{v}_\mathbf{y})$, where $\mathbf{v}_\mathbf{x} \in \mathbb{F}_2^n$ and $\mathbf{v}_\mathbf{y} \in \mathbb{F}_2^m$. We define two vector subspaces $V \subseteq \mathbb{F}_2^n$ and $W \subseteq \mathbb{F}_2^m$ as follows:

$$V = \text{span}(\{\mathbf{u}_\mathbf{x} \colon \mathbf{u} \in U\}) \text{ and } W = \text{span}(\{\mathbf{u}_y \colon \mathbf{u} \in U\}).$$

We will show that $V \in \mathcal{RMS}(f)$ and $W \in \mathcal{RMS}(g)$. We define two functions $f', g' \colon \mathbb{F}_2^{n+m} \to \mathbb{F}_2^{n+m}$ as $f'(\mathbf{x}, \mathbf{y}) := f(\mathbf{x})$ for all $\mathbf{y} \in \mathbb{F}_2^m$ and $g'(\mathbf{x}, \mathbf{y}) := g(\mathbf{y})$ for all $\mathbf{x} \in \mathbb{F}_2^n$. Since $U \in \mathcal{RMS}(h)$, then for all $\mathbf{u}_1, \mathbf{u}_2 \in U$ the equation

$$D_{\mathbf{u}_1,\mathbf{u}_2}h(\mathbf{x}, \mathbf{y}) = D_{\mathbf{u}_1,\mathbf{u}_2}f'(\mathbf{x}, \mathbf{y}) \oplus D_{\mathbf{u}_1,\mathbf{u}_2}g'(\mathbf{x}, \mathbf{y}) = c_{\mathbf{u}_1,\mathbf{u}_2} \tag{4.12}$$

holds for all $(\mathbf{x}, \mathbf{y}) \in \mathbb{F}_2^{n+m}$. Let $\mathbf{x}_1, \mathbf{x}_2 \in \mathbb{F}_2^n$ and consider the following equations

$$D_{\mathbf{u}_1,\mathbf{u}_2}f'(\mathbf{x}_1, \mathbf{y}) \oplus D_{\mathbf{u}_1,\mathbf{u}_2}g'(\mathbf{x}_1, \mathbf{y}) = c_{\mathbf{u}_1,\mathbf{u}_2} \tag{4.13}$$

$$D_{\mathbf{u}_1,\mathbf{u}_2}f'(\mathbf{x}_2, \mathbf{y}) \oplus D_{\mathbf{u}_1,\mathbf{u}_2}g'(\mathbf{x}_2, \mathbf{y}) = c_{\mathbf{u}_1,\mathbf{u}_2}, \tag{4.14}$$

which hold for any $\mathbf{y} \in \mathbb{F}_2^m$ due to (4.12). Adding equation (4.13) to (4.14), one gets $D_{\mathbf{u}_1,\mathbf{u}_2} f'(\mathbf{x}_1, \mathbf{y}) = D_{\mathbf{u}_1,\mathbf{u}_2} f'(\mathbf{x}_2, \mathbf{y})$ since g' depends on the variable $\mathbf{x}$ "fictively". Now, since f' depends on the variable $\mathbf{y}$ "fictively", we get that for all $\mathbf{v}_1, \mathbf{v}_2 \in V$ the equation $D_{\mathbf{v}_1,\mathbf{v}_2} f(\mathbf{x}_1) = D_{\mathbf{v}_1,\mathbf{v}_2} f(\mathbf{x}_2)$ holds for all $\mathbf{x}_1, \mathbf{x}_2 \in \mathbb{F}_2^n$ and hence $D_{\mathbf{v}_1,\mathbf{v}_2} f = c_{\mathbf{v}_1,\mathbf{v}_2}$ (one can think about $\mathbf{v}_1$ and $\mathbf{v}_2$ as $(\mathbf{u}_1)_{\mathbf{x}}$ and $(\mathbf{u}_2)_{\mathbf{x}}$, respectively). Thus, we have shown that $V \in \mathcal{RMS}(f)$. Since f and g are interchangeable, we get $W \in \mathcal{RMS}(g)$. Clearly, $U \subseteq V \times W$ and by the previous claim we have $V \times W \in \mathcal{RMS}(h)$.

3. Let $U \in \mathcal{RMS}(h)$ and $\dim(U) = \text{r-ind}(h)$. By the previous claim, there exist $V \in \mathcal{RMS}(f)$ and $W \in \mathcal{RMS}(g)$ such that $U \subseteq V \times W$. Now, using the following series of inequalities

$$\begin{aligned}\text{r-ind}(h) = \dim(U) &\leq \dim(V \times W) = \dim(V) + \dim(W)\\ &\leq \max_{V \in \mathcal{RMS}(f)} \dim(V) + \max_{W \in \mathcal{RMS}(g)} \dim(W)\\ &= \text{r-ind}(f) + \text{r-ind}(g),\end{aligned}$$

we complete the proof. □

In the following theorem, we give a sufficient condition on bent functions f and g by means of relaxed $\mathcal{M}$-subspaces such that the direct sum $f \oplus g$ is outside the $\mathcal{M}^\#$ class.

Theorem 4.24. *Let $f\colon \mathbb{F}_2^n \to \mathbb{F}_2$ and $g\colon \mathbb{F}_2^m \to \mathbb{F}_2$ be two Boolean bent functions. If f and g satisfy* r-ind$(f) < n/2$ *and* r-ind$(g) \leq m/2$, *then $f \oplus k \cdot g \notin \mathcal{M}^\#$ on $\mathbb{F}_2^{n+km}$ for all $k \in \mathbb{N}$.*

Definition 4.25. We will call a Boolean function f on $\mathbb{F}_2^n$ *strongly extendable*, if r-ind$(f) < n/2$ and *weakly extendable*, if r-ind$(f) = n/2$. In this way, if one wants to extend a strongly extendable function f with Theorem 4.24, it is enough to take a weakly extendable function g, while for the extension of a weakly extendable function f one has to take a strongly extendable function g.

Remark 4.26. For a given function f on $\mathbb{F}_2^n$, one can compute the relaxed linearity index r-ind(f) in the same way as the linearity index ind(f), but with only one change. Instead of the second-order derivative $D_{\mathbf{a},\mathbf{b}} f$ given by its ANF

$$D_{\mathbf{a},\mathbf{b}} f(\mathbf{x}) = \bigoplus_{\mathbf{v} \in \mathbb{F}_2^n} c_{\mathbf{v}}(\mathbf{a}, \mathbf{b}) \left(\prod_{i=1}^{n} x_i^{v_i} \right),$$

where coefficients $c_{\mathbf{v}}$ depend on $\mathbf{a}$ and $\mathbf{b}$, one considers the *"relaxed" second-order derivative* $RD_{\mathbf{a},\mathbf{b}} f$ defined by $RD_{\mathbf{a},\mathbf{b}} f(\mathbf{x}) := D_{\mathbf{a},\mathbf{b}} f(\mathbf{x}) \oplus c_{\mathbf{0}}(\mathbf{a}, \mathbf{b})$ and use it as the input of Algorithm 1.1 in the way already described in Remark 1.39.

4.4.2 Application to homogeneous cubic bent functions without affine derivatives

In order to use Theorem 4.24 for the construction of cubic bent functions outside $\mathcal{M}^{\#}$, which can be homogeneous or have no affine derivatives, we need to find such functions in a small number of variables and check whether they are weakly or strongly extendable.

First, we check whether the equivalence classes of cubic bent functions in six and eight variables given in Table 1.1, contain functions with the mentioned properties. Since all cubic bent functions in 6 and 8 variables are members of the $\mathcal{M}^{\#}$ class (see Subsection 1.1.4), the best what one expects to find is a weakly extendable cubic bent function. In this way:

- The only, up to equivalence, weakly extendable cubic bent function in 6 variables is the third Rothaus' function, denoted in Table 1.1 by c_3^6. It has no affine derivatives and is not equivalent to any homogeneous cubic bent function.

- An example of a weakly extendable homogeneous cubic bent function in 8 variables is given by the function h_1^8. Like any other cubic bent function in eight variables, it has affine derivatives [58].

Now we analyze homogeneous cubic bent functions in 10 and 12 variables.

- An example of a strongly extendable cubic bent function in 10 variables is represented by the function h_4^{10}, which is simultaneously homogeneous and has no affine derivatives.

- Since all the mentioned functions in 12 variables belong to the $\mathcal{M}^{\#}$ class, they can not be strongly extendable. Nevertheless, among them we found a weakly extendable homogeneous function h_5^{12} without affine derivatives.

We summarize these results in Table 4.4 and list all the used homogeneous cubic bent functions h_i^n in Appendix B.

Table 4.4. Weakly and strongly extendable cubic Boolean bent functions in a small number of variables

# of variables, n	6	8	10	12
r-ind	3	4	4	6
Is homogeneous?	×	✓	✓	✓
Has no aff. derivatives?	✓	×	✓	✓
Example	c_3^6	h_1^8	h_4^{10}	h_5^{12}

Now we proceed to the proof of our main theorem: the series of existence results about cubic bent functions with nice cryptographic properties.

Theorem 4.27. *On $\mathbb{F}_2^n$ there exist:*

1. *Cubic bent functions outside $\mathcal{M}^\#$ for all $n \geq 10$.*
2. *Cubic bent functions without affine derivatives outside $\mathcal{M}^\#$ for all $n \geq 26$.*
3. *Homogeneous cubic bent functions outside $\mathcal{M}^\#$ for all $n \geq 26$.*
4. *Homogeneous cubic bent functions without affine derivatives outside $\mathcal{M}^\#$ for all $n \geq 50$.*

Proof. In all the four cases the idea of the proof is the same: construct a strongly extendable Boolean function h_n in $n = 6i + 8j + 10k + 12l$ variables of the form

$$h_n := i \cdot c_3^6 \oplus j \cdot h_1^8 \oplus k \cdot h_4^{10} \oplus l \cdot h_5^{12} \tag{4.15}$$

and find the minimal value n_0 such that for all $n \geq n_0$ the function h_n inherits the properties of its components from Table 4.4. Since the only strongly extendable function is h_4^{10} in 10 variables, we require that in all the four cases below $k \neq 0$.
Case 1. Since the first case has nothing to do with homogeneity and having no affine derivatives, one can use all the components from Table 4.4. Clearly, the smallest value of n is $n_0 = 16$ and in order to cover the missing values of $n \in \{12, 14\}$, we construct a function h'_n of the form

$$h'_n(x_1, \ldots, x_n) := h_4^{10}(x_1, \ldots, x_{10}) \oplus Q_k(x_{11}, \ldots, x_n) \text{ with } k = n - 10.$$

Here Q_k is the quadratic bent function on $\mathbb{F}_2^k$, given by $Q_k \colon (x_1, \ldots, x_k) \mapsto x_1x_2 \oplus x_3x_4 \oplus \cdots \oplus x_{k-1}x_k$. Since for the quadratic bent function Q_k its relaxed linearity index $\text{r-ind}(Q_k) = k$, we can not use Theorem 4.24. However, with the second part of Theorem 4.23, it is possible to check with a computer that $h'_n \notin \mathcal{M}^\#$ by showing that none of the vector subspaces U of the form

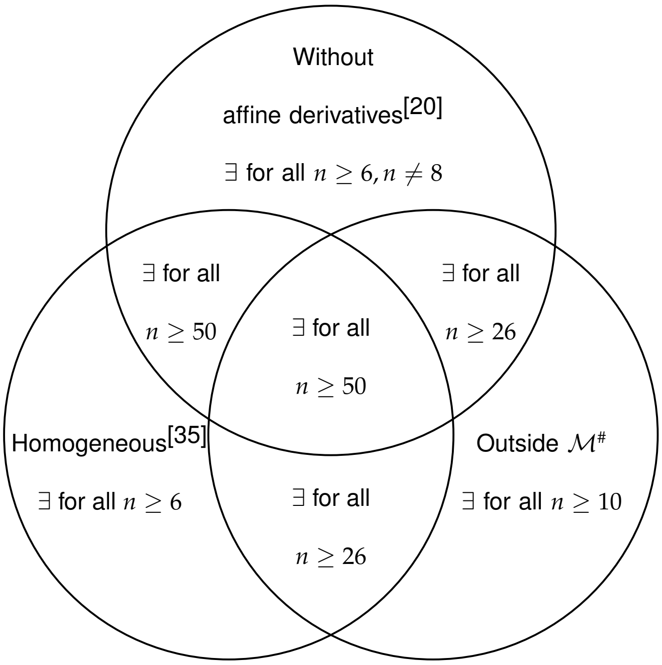
$$\{U \subseteq V \times W \colon V \in \mathcal{RMS}(h_4^{10}), W \in \mathcal{RMS}(Q_k)\}$$

is an $\mathcal{M}$-subspace of the function h'_n.
Case 2. Since there are no weakly extendable homogeneous cubic bent functions in six variables, we can use only components $h_1^8, h_4^{10}, h_5^{12}$ in (4.15). One can see that the smallest value of n is $n_0 = 26$ and the missing values are in the set $\{14, 16, 24\}$.
Case 3. First, we observe that the direct sum of two functions has no affine derivatives, if and only if both of them have no affine derivatives. Hence, the only functions we can use are $c_3^6, h_4^{10}, h_5^{12}$. In this way, the smallest value of n is $n_0 = 26$ and the missing values are in the set $\{12, 14, 18, 24\}$.
Case 4. Finally, since the only extendable functions, which are simultaneously homogeneous and have no affine derivatives are h_4^{10} and h_5^{12}, we observe that the smallest value of n is $n_0 = 50$ and the missing values of n are in the set $\{12, 14, 16, 18, 24, 26, 28, 36, 38, 48\}$, what completes the proof. □

4.5 Conclusion and open problems

In this chapter, we proved the existence of cubic bent functions outside the completed Maiorana-McFarland class $\mathcal{M}^{\#}$ on $\mathbb{F}_2^n$ for all $n \geq 10$ and showed that for almost all values of n these functions can simultaneously be homogeneous and have no affine derivatives. The reason, why some values of n are not covered by our proof is explained by the non-existence of examples with desired properties in 6 and 8 variables, which are necessary for the used recursive framework. We summarize these results in the following Venn diagram.

Figure 4.1. Existence of cubic bent functions which are: homogeneous, without affine derivatives, outside the completed Maiorana-McFarland class


Without
affine derivatives[20]
$\exists$ for all $n \geq 6, n \neq 8$
$\exists$ for all $n \geq 50$
$\exists$ for all $n \geq 26$
$\exists$ for all $n \geq 50$
Homogeneous[35]
$\exists$ for all $n \geq 6$
$\exists$ for all $n \geq 26$
Outside $\mathcal{M}^{\#}$
$\exists$ for all $n \geq 10$

In general, we expect that homogeneous cubic bent functions without affine derivatives outside $\mathcal{M}^{\#}$ exist for all even $n \geq 10$ and we leave this conjecture as an open problem. Since our proof technique is based on the direct sum construction of functions, some of them being members of $\mathcal{M}^{\#}$, the functions constructed in such a way will presumably have bad cryptographic primitives, see [27, p. 330] for details. Thus, we suggest the following problem.

Open Problem 4.28. Construct homogeneous cubic bent functions without affine derivatives outside the $\mathcal{M}^{\#}$ class without the use of the direct sum.

The next problem, which we would like to address, is related to the normality of cubic bent functions. Recall that a Boolean function f on $\mathbb{F}_2^n$ is said to be normal (weakly normal), when it is constant (affine, but not constant) respectively, on some affine subspace U of $\mathbb{F}_2^n$ of dimension $\lceil n/2 \rceil$. In this case f is said to be normal (weakly normal) with respect to the flat U. It is well-known that all quadratic bent functions are normal. Moreover, one can also construct non-normal as well as non-weakly normal bent functions of all degrees $d \geq 4$, as it follows from [22, Fact 22]. At the same time, all cubic bent functions in $n = 6$ variables are normal or weakly-normal, while for $n = 8$ they are proved to be normal [36].

Since the functions h_3^{10} and h_4^{10} do not belong to the completed Maiorana-McFarland class, they are good candidates to be checked for the normality. Based on our parallel implementation of [22, Algorithm 1] in Mathematica [112] we observe that the function h_3^{10} is normal on the flat $48 \oplus \langle \mathrm{g3}, \mathrm{8p}, \mathrm{4q}, \mathrm{2m}, \mathrm{1j} \rangle$ and the function h_4^{10} is normal on the flat $5 \oplus \langle \mathrm{i5}, \mathrm{8h}, \mathrm{6n}, \mathrm{1g}, \mathrm{f} \rangle$. Here we describe each binary vector of a flat by 32-base representation using the following alphabet

$$0 \mapsto 0, \ldots, \mathrm{f} \mapsto 15, \mathrm{g} \mapsto 16, \ldots, \mathrm{v} \mapsto 31. \tag{4.16}$$

In this way, since one still has no examples of non-weakly normal cubic bent functions, it is reasonable to ask the following question.

Open Problem 4.29. Do non-weakly normal cubic bent functions exist?

In Remark 4.14, we found homogeneous cubic bent functions in twelve variables of the form $h\colon (\mathbf{x}, \mathbf{y}) \mapsto f_{\pi,\phi}((\mathbf{x}, \mathbf{y})\mathbf{T})$. Most notably, for a fixed permutation π and a nondegenerate linear transformation $\mathbf{T}$ these functions are homogeneous independently of the choice of a homogeneous cubic function ϕ. The principal difference between the primary construction $h^n_{pr.}$ and functions constructed in Remark 4.14 is the following. For the primary construction of homogeneous cubic bent function $h^n_{pr.}$, one needs to find a special Boolean function ϕ of degree 3 such that the nonhomogeneous cubic Maiorana-McFarland function $f_{id,\phi}$ is homogeneous after the change of coordinates. In some sense, the identity permutation id has a "defect", which makes $f_{id,0}$ never equivalent to a homogeneous cubic function. But the specific choice of a cubic function ϕ helps to repair it. Since the functions constructed in Remark 4.14 are in that sense "defect free", it is essential to search for such functions systematically.

Open Problem 4.30. Construct infinite families of permutations $\pi\colon \mathbb{F}_2^m \to \mathbb{F}_2^m$ such that for some nondegenerate linear transformation $\mathbf{T}$ the bent function $h\colon \mathbb{F}_2^m \times \mathbb{F}_2^m \to \mathbb{F}_2$ defined by

$$h\colon (\mathbf{x}, \mathbf{y}) \mapsto f_{\pi,\phi}((\mathbf{x}, \mathbf{y})\mathbf{T})$$

is homogeneous cubic bent for all homogeneous cubic functions $\phi\colon \mathbb{F}_2^m \to \mathbb{F}_2$.

The final problem is related to the non-existence of d-homogeneous vectorial bent functions (note that vectorial (n,m)-function $F(\mathbf{x}) = (f_1(\mathbf{x}), \ldots, f_m(\mathbf{x}))^T$ is said to be d-homogeneous, if all the coordinate functions f_i are d-homogeneous).

Using computer search, we observe that the only existing homogeneous vectorial bent functions in 6 and 8 variables are quadratic ones. This observation leads to the following question, which we leave as an open problem.

Open Problem 4.31. Do non-quadratic homogeneous vectorial bent functions exist?

Finally, we list in Appendix B all homogeneous cubic bent functions used in this chapter.

Appendix A

Vectorial bent functions in six variables

Here we list algebraic normal forms of representatives of EA-equivalence classes of bent functions in 6 variables. The representatives $F_i^m \in C_i^m$ and $F_j^{m+1} \in C_j^{m+1}$ are selected in such a way that $F_i^m \prec F_j^{m+1}$ as in Figure 2.1. Note that we abbreviate $1 \leq i \leq 6$ for the variable x_i.

A.1 Algebraic normal forms

Table A.1. Algebraic normal forms of EA-inequivalent $(6, 1)$-bent functions

F_i^1	Algebraic normal form of $F_i^1 \in C_i^1$
F_1^1	$14 \oplus 25 \oplus 36$
F_2^1	$14 \oplus 25 \oplus 36 \oplus 123$
F_3^1	$12 \oplus 14 \oplus 26 \oplus 35 \oplus 45 \oplus 123 \oplus 245$
F_4^1	$14 \oplus 26 \oplus 34 \oplus 35 \oplus 36 \oplus 45 \oplus 46 \oplus 123 \oplus 245 \oplus 346$

Table A.2. Algebraic normal forms of EA-inequivalent $(6, 2)$-bent functions

F_i^2	Algebraic normal form of $F_i^2 \in C_i^2$
F_1^2	$\begin{pmatrix} 14 \oplus 25 \oplus 36 \\ 15 \oplus 16 \oplus 24 \oplus 25 \oplus 34 \end{pmatrix}$
F_2^2	$\begin{pmatrix} 14 \oplus 25 \oplus 36 \oplus 123 \\ 15 \oplus 16 \oplus 24 \oplus 25 \oplus 34 \end{pmatrix}$
F_3^2	$\begin{pmatrix} 14 \oplus 25 \oplus 36 \oplus 123 \\ 13 \oplus 15 \oplus 23 \oplus 46 \oplus 124 \end{pmatrix}$
F_4^2	$\begin{pmatrix} 14 \oplus 25 \oplus 36 \oplus 123 \\ 12 \oplus 13 \oplus 16 \oplus 26 \oplus 45 \oplus 56 \oplus 156 \oplus 235 \end{pmatrix}$
F_5^2	$\begin{pmatrix} 12 \oplus 14 \oplus 26 \oplus 35 \oplus 45 \oplus 123 \oplus 245 \\ 13 \oplus 23 \oplus 24 \oplus 35 \oplus 56 \oplus 126 \oplus 235 \end{pmatrix}$

Continued on the next page

Table A.2. Continued from the previous page

F_i^2	Algebraic normal form of $F_i^2 \in C_i^2$
F_6^2	$\begin{pmatrix} 14 \oplus 26 \oplus 34 \oplus 35 \oplus 36 \oplus 45 \oplus 46 \oplus 123 \oplus 245 \oplus 346 \\ 13 \oplus 23 \oplus 24 \oplus 35 \oplus 56 \oplus 126 \oplus 235 \end{pmatrix}$
F_7^2	$\begin{pmatrix} 14 \oplus 26 \oplus 34 \oplus 35 \oplus 36 \oplus 45 \oplus 46 \oplus 123 \oplus 245 \oplus 346 \\ 12 \oplus 35 \oplus 46 \oplus 124 \oplus 134 \oplus 235 \oplus 236 \oplus 245 \end{pmatrix}$
F_8^2	$\begin{pmatrix} 14 \oplus 26 \oplus 34 \oplus 35 \oplus 36 \oplus 45 \oplus 46 \oplus 123 \oplus 245 \oplus 346 \\ 12 \oplus 16 \oplus 23 \oplus 35 \oplus 46 \oplus 56 \oplus 124 \oplus 134 \oplus 156 \oplus 235 \oplus 236 \oplus 245 \end{pmatrix}$
F_9^2	$\begin{pmatrix} 14 \oplus 26 \oplus 34 \oplus 35 \oplus 36 \oplus 45 \oplus 46 \oplus 123 \oplus 245 \oplus 346 \\ 12 \oplus 15 \oplus 16 \oplus 25 \oplus 36 \oplus 45 \oplus 46 \oplus 125 \oplus 126 \oplus 135 \oplus 136 \oplus 145 \oplus 256 \end{pmatrix}$

Table A.3. Algebraic normal forms of EA-inequivalent $(6,3)$-bent functions

F_i^3	Algebraic normal form of $F_i^3 \in C_i^3$
F_1^3	$\begin{pmatrix} 14 \oplus 25 \oplus 36 \\ 15 \oplus 16 \oplus 24 \oplus 25 \oplus 34 \\ 14 \oplus 15 \oplus 24 \oplus 25 \oplus 26 \oplus 35 \end{pmatrix}$
F_2^3	$\begin{pmatrix} 14 \oplus 25 \oplus 36 \\ 15 \oplus 16 \oplus 24 \oplus 25 \oplus 34 \\ 12 \oplus 14 \oplus 15 \oplus 24 \oplus 25 \oplus 26 \oplus 35 \end{pmatrix}$
F_3^3	$\begin{pmatrix} 14 \oplus 25 \oplus 36 \\ 15 \oplus 16 \oplus 24 \oplus 25 \oplus 34 \\ 13 \oplus 14 \oplus 26 \oplus 45 \end{pmatrix}$
F_4^3	$\begin{pmatrix} 14 \oplus 25 \oplus 36 \\ 15 \oplus 16 \oplus 24 \oplus 25 \oplus 34 \\ 14 \oplus 15 \oplus 24 \oplus 25 \oplus 26 \oplus 35 \oplus 123 \end{pmatrix}$
F_5^3	$\begin{pmatrix} 14 \oplus 25 \oplus 36 \oplus 123 \\ 13 \oplus 15 \oplus 23 \oplus 46 \oplus 124 \\ 13 \oplus 24 \oplus 25 \oplus 56 \oplus 125 \end{pmatrix}$
F_6^3	$\begin{pmatrix} 14 \oplus 25 \oplus 36 \oplus 123 \\ 13 \oplus 15 \oplus 23 \oplus 46 \oplus 124 \\ 12 \oplus 14 \oplus 16 \oplus 34 \oplus 46 \oplus 56 \oplus 126 \oplus 136 \oplus 246 \end{pmatrix}$
F_7^3	$\begin{pmatrix} 14 \oplus 25 \oplus 36 \oplus 123 \\ 13 \oplus 15 \oplus 23 \oplus 46 \oplus 124 \\ 12 \oplus 13 \oplus 24 \oplus 25 \oplus 35 \oplus 45 \oplus 56 \oplus 125 \oplus 345 \end{pmatrix}$
F_8^3	$\begin{pmatrix} 12 \oplus 14 \oplus 26 \oplus 35 \oplus 45 \oplus 123 \oplus 245 \\ 13 \oplus 23 \oplus 24 \oplus 35 \oplus 56 \oplus 126 \oplus 235 \\ 16 \oplus 23 \oplus 26 \oplus 35 \oplus 45 \oplus 56 \oplus 123 \oplus 124 \oplus 256 \end{pmatrix}$
F_9^3	$\begin{pmatrix} 12 \oplus 14 \oplus 26 \oplus 35 \oplus 45 \oplus 123 \oplus 245 \\ 13 \oplus 23 \oplus 24 \oplus 35 \oplus 56 \oplus 126 \oplus 235 \\ 16 \oplus 25 \oplus 26 \oplus 35 \oplus 36 \oplus 45 \oplus 56 \oplus 123 \oplus 124 \oplus 234 \oplus 256 \oplus 346 \end{pmatrix}$
F_{10}^3	$\begin{pmatrix} 14 \oplus 26 \oplus 34 \oplus 35 \oplus 36 \oplus 45 \oplus 46 \oplus 123 \oplus 245 \oplus 346 \\ 12 \oplus 35 \oplus 46 \oplus 124 \oplus 134 \oplus 235 \oplus 236 \oplus 245 \\ 12 \oplus 13 \oplus 25 \oplus 35 \oplus 36 \oplus 45 \oplus 123 \oplus 134 \oplus 236 \oplus 246 \oplus 345 \end{pmatrix}$
F_{11}^3	$\begin{pmatrix} 14 \oplus 26 \oplus 34 \oplus 35 \oplus 36 \oplus 45 \oplus 46 \oplus 123 \oplus 245 \oplus 346 \\ 12 \oplus 35 \oplus 46 \oplus 124 \oplus 134 \oplus 235 \oplus 236 \oplus 245 \\ 12 \oplus 13 \oplus 24 \oplus 25 \oplus 34 \oplus 35 \oplus 36 \oplus 45 \oplus 123 \oplus 134 \oplus 236 \oplus 246 \oplus 345 \end{pmatrix}$
F_{12}^3	$\begin{pmatrix} 14 \oplus 26 \oplus 34 \oplus 35 \oplus 36 \oplus 45 \oplus 46 \oplus 123 \oplus 245 \oplus 346 \\ 12 \oplus 35 \oplus 46 \oplus 124 \oplus 134 \oplus 235 \oplus 236 \oplus 245 \\ 14 \oplus 15 \oplus 16 \oplus 23 \oplus 26 \oplus 35 \oplus 56 \oplus 124 \oplus 125 \oplus 126 \oplus 136 \oplus 145 \oplus 156 \oplus 236 \oplus 246 \oplus 345 \end{pmatrix}$
F_{13}^3	$\begin{pmatrix} 14 \oplus 26 \oplus 34 \oplus 35 \oplus 36 \oplus 45 \oplus 46 \oplus 123 \oplus 245 \oplus 346 \\ 12 \oplus 35 \oplus 46 \oplus 124 \oplus 134 \oplus 235 \oplus 236 \oplus 245 \\ 13 \oplus 14 \oplus 24 \oplus 34 \oplus 35 \oplus 36 \oplus 46 \oplus 56 \oplus 123 \oplus 125 \oplus 145 \oplus 146 \oplus 235 \oplus 256 \oplus 356 \oplus 456 \end{pmatrix}$

A.2 Cardinalities of equivalence classes

In the following table, we list the cardinalities of EA-equivalence classes of Boolean and vectorial bent functions in 6 variables.

Table A.4. Cardinalities of EA-equivalence classes of $(6, m)$-bent functions

A.4(a) Boolean $(6, 1)$-bent functions

C_i^1	$\lvert C_i^1\rvert$	$\lvert C_i^1\rvert$ Approx.
C_1^1	1,777,664	$2^{20.76}$
C_2^1	239,984,640	$2^{27.83}$
C_3^1	1,343,913,984	$2^{30.32}$
C_4^1	3,839,754,240	$2^{31.83}$
Total	5,425,430,528	$2^{32.33}$

A.4(b) Vectorial $(6, 2)$-bent functions

C_i^2	$\lvert C_i^2\rvert$	$\lvert C_i^2\rvert$ Approx.
C_1^2	1,310,636,113,920	$2^{40.25}$
C_2^2	35,387,175,075,840	$2^{45.00}$
C_3^2	330,280,300,707,840	$2^{48.23}$
C_4^2	1,981,681,804,247,040	$2^{50.81}$
C_5^2	660,560,601,415,680	$2^{49.23}$
C_6^2	7,926,727,216,988,160	$2^{52.81}$
C_7^2	377,463,200,808,960	$2^{48.42}$
C_8^2	9,059,116,819,415,040	$2^{53.00}$
C_9^2	3,019,705,606,471,680	$2^{51.42}$
Total	23,392,233,361,244,160	$2^{54.37}$

A.4(c) Vectorial $(6, 3)$-bent functions

C_i^3	$\lvert C_i^3\rvert$	$\lvert C_i^3\rvert$ Approx.
C_1^3	671,045,690,327,040	$2^{49.25}$
C_2^3	42,275,878,490,603,520	$2^{55.23}$
C_3^3	112,735,675,974,942,720	$2^{56.64}$
C_4^3	338,207,027,924,828,160	$2^{58.23}$
C_5^3	2,705,656,223,398,625,280	$2^{61.23}$
C_6^3	9,469,796,781,895,188,480	$2^{63.03}$
C_7^3	18,939,593,563,790,376,960	$2^{64.03}$
C_8^3	5,411,312,446,797,250,560	$2^{62.23}$
C_9^3	37,879,187,127,580,753,920	$2^{65.03}$
C_{10}^3	2,705,656,223,398,625,280	$2^{61.23}$
C_{11}^3	386,522,317,628,375,040	$2^{58.42}$
C_{12}^3	21,645,249,787,189,002,240	$2^{64.23}$
C_{13}^3	21,645,249,787,189,002,240	$2^{64.23}$
Total	121,282,113,886,947,901,440	$2^{66.71}$

A.3 Invariants under extended-affine equivalence

For an equivalence class C_i^m of $(6,m)$-bent functions with the representative $F_i^m \in C_i^m$ listed in Appendix A.1, we compute the following invariants under extended-affine equivalence: $|\operatorname{Aut}(C_i^m)| := |\operatorname{Aut}(\mathcal{C}_{F_i^m})|$, $|\operatorname{Aut}(\operatorname{dev}(\mathcal{G}_{C_i^m}))| := |\operatorname{Aut}(\operatorname{dev}(\mathcal{G}_{F_i^m}))|$ and $\operatorname{SNF}(C_i^m) := \operatorname{SNF}(F_i^m)$.

Table A.5. Invariants of EA-inequivalent $(6,m)$-bent functions

A.5(a) Boolean $(6,1)$-bent functions

C_i^1	$\lvert\operatorname{Aut}(C_i^1)\rvert$	$\dfrac{\lvert\operatorname{Aut}(\operatorname{dev}(C_i^1))\rvert}{\lvert\operatorname{Aut}(C_i^1)\rvert}$	$\operatorname{SNF}(C_i^1)$
C_1^1	$2^{15}\cdot 3^4\cdot 5^1\cdot 7^1$	$2^{13}\cdot 7^1\cdot 31^1$	$\{*1^8, 2^{15}, 4^{20}, 8^{15}, 16^6, 32^1*\}$
C_2^1	$2^{15}\cdot 3^1\cdot 7^1$	$2^{13}\cdot 3^3\cdot 5^1\cdot 7^1\cdot 31^1$	$\{*1^8, 2^{15}, 4^{20}, 8^{15}, 16^6, 32^1*\}$
C_3^1	$2^{13}\cdot 3^1\cdot 5^1$	$2^{11}\cdot 3^1$	$\{*1^{12}, 2^9, 4^{24}, 8^9, 16^{10}, 32^1*\}$
C_4^1	$2^{11}\cdot 3^1\cdot 7^1$	2^7	$\{*1^{14}, 2^7, 4^{24}, 8^7, 16^{12}, 32^1*\}$

A.5(b) Vectorial $(6,2)$-bent functions

C_i^2	$\lvert\operatorname{Aut}(C_i^2)\rvert$	$\operatorname{SNF}(C_i^2)$
C_1^2	$2^9\cdot 3^3\cdot 7^1$	$\{*1^{28}, 2^{26}, 4^{42}, 8^{64}, 16^{19}, 32^{12}, 64^2*\}$
C_2^2	$2^9\cdot 7^1$	$\{*1^{30}, 2^{28}, 4^{40}, 8^{54}, 16^{27}, 32^{12}, 64^2*\}$
C_3^2	$2^7\cdot 3^1$	$\{*1^{36}, 2^{22}, 4^{39}, 8^{50}, 16^{32}, 32^{12}, 64^2*\}$
C_4^2	2^6	$\{*1^{38}, 2^{24}, 4^{33}, 8^{56}, 16^{20}, 32^{20}, 64^2*\}$
C_5^2	$2^6\cdot 3^1$	$\{*1^{38}, 2^{24}, 4^{37}, 8^{48}, 16^{24}, 32^{20}, 64^2*\}$
C_6^2	2^4	$\{*1^{42}, 2^{20}, 4^{37}, 8^{48}, 16^{20}, 32^{24}, 64^2*\}$
C_7^2	$2^4\cdot 3^1\cdot 7^1$	$\{*1^{36}, 2^{34}, 4^{23}, 8^{58}, 16^{16}, 32^{24}, 64^2*\}$
C_8^2	$2^1\cdot 7^1$	$\{*1^{42}, 2^{22}, 4^{41}, 8^{34}, 16^{28}, 32^{24}, 64^2*\}$
C_9^2	$2^1\cdot 3^1\cdot 7^1$	$\{*1^{42}, 2^{22}, 4^{41}, 8^{34}, 16^{28}, 32^{24}, 64^2*\}$

A.5(c) Vectorial $(6,3)$-bent functions

C_i^3	$\lvert\operatorname{Aut}(C_i^3)\rvert$	$\operatorname{SNF}(C_i^3)$
C_1^3	$2^9\cdot 3^3\cdot 7^2$	$\{*1^{64}, 2^{48}, 4^{72}, 8^{163}, 16^{54}, 32^{30}, 64^{18}*\}$
C_2^3	$2^9\cdot 3^1\cdot 7^1$	$\{*1^{78}, 2^{44}, 4^{68}, 8^{139}, 16^{62}, 32^{38}, 64^{20}*\}$
C_3^3	$2^6\cdot 3^2\cdot 7^1$	$\{*1^{88}, 2^{32}, 4^{68}, 8^{137}, 16^{68}, 32^{32}, 64^{24}*\}$
C_4^3	$2^6\cdot 3^1\cdot 7^1$	$\{*1^{80}, 2^{40}, 4^{70}, 8^{145}, 16^{54}, 32^{36}, 64^{24}*\}$
C_5^3	$2^3\cdot 3^1\cdot 7^1$	$\{*1^{88}, 2^{48}, 4^{48}, 8^{145}, 16^{48}, 32^{48}, 64^{24}*\}$
C_6^3	$2^4\cdot 3^1$	$\{*1^{98}, 2^{44}, 4^{38}, 8^{153}, 16^{38}, 32^{44}, 64^{34}*\}$
C_7^3	$2^3\cdot 3^1$	$\{*1^{98}, 2^{40}, 4^{46}, 8^{145}, 16^{46}, 32^{40}, 64^{34}*\}$
C_8^3	$2^2\cdot 3^1\cdot 7^1$	$\{*1^{100}, 2^{36}, 4^{36}, 8^{169}, 16^{36}, 32^{36}, 64^{36}*\}$
C_9^3	$2^2\cdot 3^1$	$\{*1^{106}, 2^{36}, 4^{30}, 8^{169}, 16^{30}, 32^{36}, 64^{42}*\}$
C_{10}^3	$2^3\cdot 3^1\cdot 7^1$	$\{*1^{100}, 2^{36}, 4^{36}, 8^{169}, 16^{36}, 32^{36}, 64^{36}*\}$
C_{11}^3	$2^3\cdot 3^1\cdot 7^2$	$\{*1^{100}, 2^{36}, 4^{36}, 8^{169}, 16^{36}, 32^{36}, 64^{36}*\}$
C_{12}^3	$3^1\cdot 7^1$	$\{*1^{106}, 2^{42}, 4^{18}, 8^{181}, 16^{18}, 32^{42}, 64^{42}*\}$
C_{13}^3	$3^1\cdot 7^1$	$\{*1^{106}, 2^{36}, 4^{30}, 8^{169}, 16^{30}, 32^{36}, 64^{42}*\}$

Note that any two different equivalence classes C_i^m and C_j^m of bent functions in six variables have different pairs of invariants

$$(|\operatorname{Aut}(C_i^m)|, \operatorname{SNF}(C_i^m)) \neq (|\operatorname{Aut}(C_j^m)|, \operatorname{SNF}(C_j^m)).$$

In this way, the reader can be sure that all the representatives of equivalence classes listed in Appendix A are EA-inequivalent.

Finally, for quadratic vectorial bent functions from equivalence classes C_1^m with $m = 2, 3$, we have $|\operatorname{Aut}(\operatorname{dev}(C_1^m))| = 2^{n+m} \cdot |\operatorname{Aut}(C_1^m)| \cdot 7^1$, where $n = 6$. For the rest of vectorial (n, m)-bent functions in six variables, we have

$$|\operatorname{Aut}(\operatorname{dev}(C_i^m))| = 2^{n+m} \cdot |\operatorname{Aut}(C_i^m)|.$$

In this way, translation designs of vectorial bent functions from equivalence classes C_{10}^3 and C_{11}^3 can be distinguished by the orders of their automorphism groups, despite the Smith normal forms coincide.

Appendix B

The known homogeneous cubic bent functions

Here we list algebraic normal forms of the known EA-inequivalent n-variable homogeneous cubic bent functions used in Chapter 4. We abbreviate $1 \leq i \leq 9$ for the variable x_i, the variables x_{10}, x_{11} and x_{12} are replaced by a, b and c, respectively.

B.1 Algebraic normal forms

Table B.1. Algebraic normal forms of the known EA-inequivalent homogeneous cubic bent functions

h_i^n	ANFs of EA-inequivalent homogeneous cubic bent functions h_i^n on $\mathbb{F}_2^n$
h_1^6	$123 \oplus 124 \oplus 125 \oplus 134 \oplus 136 \oplus 145 \oplus 146 \oplus 156 \oplus 235 \oplus 236 \oplus 245 \oplus 246 \oplus 256 \oplus 345 \oplus 346 \oplus 356$
h_1^8	$125 \oplus 127 \oplus 134 \oplus 136 \oplus 137 \oplus 138 \oplus 148 \oplus 156 \oplus 157 \oplus 158 \oplus 178 \oplus 234 \oplus 237 \oplus 246 \oplus 258 \oplus 268 \oplus 346 \oplus 347 \oplus 356 \oplus 357 \oplus 368 \oplus 457 \oplus 458 \oplus 467 \oplus 468 \oplus 478 \oplus 567 \oplus 568$
h_2^8	$123 \oplus 124 \oplus 126 \oplus 127 \oplus 134 \oplus 146 \oplus 148 \oplus 157 \oplus 158 \oplus 236 \oplus 247 \oplus 256 \oplus 257 \oplus 267 \oplus 348 \oplus 356 \oplus 358 \oplus 367 \oplus 368 \oplus 378 \oplus 457 \oplus 458 \oplus 468 \oplus 578$
h_1^{10}	$126 \oplus 128 \oplus 129 \oplus 12a \oplus 134 \oplus 137 \oplus 138 \oplus 139 \oplus 145 \oplus 149 \oplus 14a \oplus 157 \oplus 159 \oplus 15a \oplus 178 \oplus 179 \oplus 236 \oplus 237 \oplus 239 \oplus 23a \oplus 26a \oplus 279 \oplus 289 \oplus 28a \oplus 29a \oplus 347 \oplus 34a \oplus 356 \oplus 357 \oplus 358 \oplus 359 \oplus 367 \oplus 369 \oplus 36a \oplus 37a \oplus 38a \oplus 456 \oplus 457 \oplus 467 \oplus 468 \oplus 46a \oplus 478 \oplus 489 \oplus 48a \oplus 49a \oplus 568 \oplus 56a \oplus 578 \oplus 579 \oplus 58a \oplus 69a \oplus 789 \oplus 78a$
h_2^{10}	$123 \oplus 124 \oplus 125 \oplus 126 \oplus 127 \oplus 128 \oplus 129 \oplus 12a \oplus 134 \oplus 135 \oplus 136 \oplus 13a \oplus 147 \oplus 148 \oplus 149 \oplus 156 \oplus 159 \oplus 15a \oplus 167 \oplus 16a \oplus 178 \oplus 179 \oplus 189 \oplus 18a \oplus 234 \oplus 237 \oplus 238 \oplus 239 \oplus 245 \oplus 246 \oplus 24a \oplus 256 \oplus 259 \oplus 25a \oplus 267 \oplus 26a \oplus 278 \oplus 279 \oplus 289 \oplus 28a \oplus 345 \oplus 346 \oplus 347 \oplus 348 \oplus 349 \oplus 34a \oplus 356 \oplus 359 \oplus 35a \oplus 367 \oplus 36a \oplus 378 \oplus 379 \oplus 389 \oplus 38a \oplus 456 \oplus 459 \oplus 45a \oplus 467 \oplus 46a \oplus 478 \oplus 479 \oplus 489 \oplus 48a \oplus 567 \oplus 589 \oplus 59a \oplus 679 \oplus 68a \oplus 78a$

Continued on the next page

Table B.1. Continued from the previous page

h_i^n	ANFs of EA-inequivalent homogeneous cubic bent functions h_i^n on $\mathbb{F}_2^n$
h_3^{10}	$123 \oplus 126 \oplus 128 \oplus 12a \oplus 135 \oplus 136 \oplus 139 \oplus 13a \oplus 145 \oplus 14a \oplus 157 \oplus 15a \oplus 169 \oplus 178 \oplus 189 \oplus 19a \oplus 236 \oplus 237 \oplus 239 \oplus 23a \oplus 26a \oplus 279 \oplus 289 \oplus 28a \oplus 29a \oplus 347 \oplus 34a \oplus 356 \oplus 357 \oplus 358 \oplus 359 \oplus 367 \oplus 369 \oplus 36a \oplus 37a \oplus 38a \oplus 456 \oplus 457 \oplus 467 \oplus 468 \oplus 46a \oplus 478 \oplus 489 \oplus 48a \oplus 49a \oplus 568 \oplus 56a \oplus 578 \oplus 579 \oplus 58a \oplus 69a \oplus 789 \oplus 78a$
h_4^{10}	$126 \oplus 127 \oplus 128 \oplus 12a \oplus 134 \oplus 135 \oplus 137 \oplus 139 \oplus 13a \oplus 145 \oplus 146 \oplus 148 \oplus 149 \oplus 14a \oplus 157 \oplus 167 \oplus 168 \oplus 16a \oplus 179 \oplus 17a \oplus 19a \oplus 235 \oplus 238 \oplus 239 \oplus 23a \oplus 246 \oplus 247 \oplus 248 \oplus 256 \oplus 259 \oplus 267 \oplus 269 \oplus 26a \oplus 278 \oplus 27a \oplus 289 \oplus 28a \oplus 29a \oplus 347 \oplus 349 \oplus 356 \oplus 357 \oplus 358 \oplus 35a \oplus 368 \oplus 369 \oplus 37a \oplus 389 \oplus 38a \oplus 39a \oplus 457 \oplus 459 \oplus 45a \oplus 468 \oplus 46a \oplus 478 \oplus 479 \oplus 47a \oplus 48a \oplus 49a \oplus 568 \oplus 569 \oplus 56a \oplus 579 \oplus 57a \oplus 589 \oplus 58a \oplus 59a \oplus 678 \oplus 68a \oplus 69a \oplus 78a$
h_1^{12}	$135 \oplus 138 \oplus 13b \oplus 13c \oplus 145 \oplus 149 \oplus 157 \oplus 15a \oplus 167 \oplus 16b \oplus 179 \oplus 17c \oplus 189 \oplus 19b \oplus 1ab \oplus 234 \oplus 238 \oplus 246 \oplus 249 \oplus 24c \oplus 256 \oplus 25a \oplus 268 \oplus 26b \oplus 278 \oplus 27c \oplus 28a \oplus 29a \oplus 2ac \oplus 2bc \oplus 346 \oplus 347 \oplus 348 \oplus 35c \oplus 36c \oplus 37c \oplus 389 \oplus 39a \oplus 3ab \oplus 457 \oplus 458 \oplus 459 \oplus 49a \oplus 4ab \oplus 4bc \oplus 568 \oplus 569 \oplus 56a \oplus 5ab \oplus 5bc \oplus 679 \oplus 67a \oplus 67b \oplus 6bc \oplus 78a \oplus 78b \oplus 78c \oplus 89b \oplus 89c \oplus 9ac$
h_2^{12}	$135 \oplus 136 \oplus 138 \oplus 13a \oplus 13b \oplus 13c \oplus 145 \oplus 147 \oplus 149 \oplus 14b \oplus 157 \oplus 158 \oplus 15a \oplus 15c \oplus 167 \oplus 169 \oplus 16b \oplus 179 \oplus 17a \oplus 17c \oplus 189 \oplus 18b \oplus 19b \oplus 19c \oplus 1ab \oplus 234 \oplus 236 \oplus 238 \oplus 23a \oplus 246 \oplus 247 \oplus 249 \oplus 24b \oplus 24c \oplus 256 \oplus 258 \oplus 25a \oplus 25c \oplus 268 \oplus 269 \oplus 26b \oplus 278 \oplus 27a \oplus 27c \oplus 28a \oplus 28b \oplus 29a \oplus 29c \oplus 2ac \oplus 2bc \oplus 348 \oplus 34a \oplus 34b \oplus 356 \oplus 358 \oplus 35a \oplus 367 \oplus 368 \oplus 36b \oplus 37c \oplus 389 \oplus 38a \oplus 38b \oplus 39c \oplus 3ac \oplus 459 \oplus 45b \oplus 45c \oplus 467 \oplus 469 \oplus 46b \oplus 478 \oplus 479 \oplus 47c \oplus 49a \oplus 49b \oplus 49c \oplus 56a \oplus 56c \oplus 578 \oplus 57a \oplus 57c \oplus 589 \oplus 58a \oplus 5ab \oplus 5ac \oplus 67b \oplus 689 \oplus 68b \oplus 69a \oplus 69b \oplus 6bc \oplus 78c \oplus 79a \oplus 79c \oplus 7ab \oplus 7ac \oplus 8ab \oplus 8bc \oplus 9bc$
h_3^{12}	$134 \oplus 135 \oplus 137 \oplus 138 \oplus 139 \oplus 13b \oplus 146 \oplus 149 \oplus 14c \oplus 156 \oplus 157 \oplus 159 \oplus 15a \oplus 15b \oplus 168 \oplus 16b \oplus 178 \oplus 179 \oplus 17b \oplus 17c \oplus 18a \oplus 19a \oplus 19b \oplus 1ac \oplus 1bc \oplus 235 \oplus 238 \oplus 23b \oplus 23c \oplus 245 \oplus 246 \oplus 248 \oplus 249 \oplus 24a \oplus 24c \oplus 257 \oplus 25a \oplus 267 \oplus 268 \oplus 26a \oplus 26b \oplus 26c \oplus 279 \oplus 27c \oplus 289 \oplus 28a \oplus 28c \oplus 29b \oplus 2ab \oplus 2ac \oplus 345 \oplus 346 \oplus 348 \oplus 34a \oplus 34c \oplus 357 \oplus 35b \oplus 35c \oplus 367 \oplus 37c \oplus 389 \oplus 39b \oplus 39c \oplus 3ab \oplus 3bc \oplus 456 \oplus 457 \oplus 459 \oplus 45b \oplus 468 \oplus 46c \oplus 478 \oplus 49a \oplus 4ac \oplus 4bc \oplus 567 \oplus 568 \oplus 56a \oplus 56c \oplus 579 \oplus 589 \oplus 5ab \oplus 678 \oplus 679 \oplus 67b \oplus 68a \oplus 69a \oplus 6bc \oplus 789 \oplus 78a \oplus 78c \oplus 79b \oplus 7ab \oplus 89a \oplus 89b \oplus 8ac \oplus 8bc \oplus 9ab \oplus 9ac \oplus abc$
h_4^{12}	$134 \oplus 136 \oplus 137 \oplus 138 \oplus 139 \oplus 13a \oplus 147 \oplus 149 \oplus 14b \oplus 156 \oplus 158 \oplus 159 \oplus 15a \oplus 15b \oplus 15c \oplus 169 \oplus 16b \oplus 178 \oplus 17a \oplus 17b \oplus 17c \oplus 18b \oplus 19a \oplus 19c \oplus 1bc \oplus 236 \oplus 238 \oplus 23a \oplus 23c \oplus 245 \oplus 247 \oplus 248 \oplus 249 \oplus 24a \oplus 24b \oplus 258 \oplus 25a \oplus 25c \oplus 267 \oplus 269 \oplus 26a \oplus 26b \oplus 26c \oplus 27a \oplus 27c \oplus 289 \oplus 28b \oplus 28c \oplus 29c \oplus 2ab \oplus 345 \oplus 346 \oplus 348 \oplus 34a \oplus 34c \oplus 357 \oplus 35b \oplus 35c \oplus 367 \oplus 37c \oplus 389 \oplus 39b \oplus 39c \oplus 3ab \oplus 3bc \oplus 456 \oplus 457 \oplus 459 \oplus 45b \oplus 468 \oplus 46c \oplus 478 \oplus 49a \oplus 4ac \oplus 4bc \oplus 567 \oplus 568 \oplus 56a \oplus 56c \oplus 579 \oplus 589 \oplus 5ab \oplus 678 \oplus 679 \oplus 67b \oplus 68a \oplus 69a \oplus 6bc \oplus 789 \oplus 78a \oplus 78c \oplus 79b \oplus 7ab \oplus 89a \oplus 89b \oplus 8ac \oplus 8bc \oplus 9ab \oplus 9ac \oplus abc$
h_5^{12}	$135 \oplus 136 \oplus 138 \oplus 13b \oplus 149 \oplus 14b \oplus 157 \oplus 158 \oplus 15a \oplus 16b \oplus 179 \oplus 17a \oplus 17c \oplus 19b \oplus 19c \oplus 238 \oplus 23a \oplus 246 \oplus 247 \oplus 249 \oplus 24c \oplus 25a \oplus 25c \oplus 268 \oplus 269 \oplus 26b \oplus 27c \oplus 28a \oplus 28b \oplus 2ac \oplus 345 \oplus 346 \oplus 34a \oplus 34b \oplus 34c \oplus 356 \oplus 358 \oplus 35a \oplus 35c \oplus 367 \oplus 368 \oplus 36b \oplus 38a \oplus 38b \oplus 39c \oplus 3ab \oplus 3ac \oplus 3bc \oplus 456 \oplus 457 \oplus 45b \oplus 45c \oplus 467 \oplus 469 \oplus 46b \oplus 478 \oplus 479 \oplus 47c \oplus 49b \oplus 49c \oplus 4bc \oplus 567 \oplus 568 \oplus 56c \oplus 578 \oplus 57a \oplus 57c \oplus 589 \oplus 58a \oplus 5ac \oplus 678 \oplus 679 \oplus 689 \oplus 68b \oplus 69a \oplus 69b \oplus 789 \oplus 78a \oplus 79a \oplus 79c \oplus 7ab \oplus 7ac \oplus 89a \oplus 89b \oplus 8ab \oplus 8bc \oplus 9ab \oplus 9ac \oplus 9bc \oplus abc$

Continued on the next page

Table B.1. Continued from the previous page

h_i^n	ANFs of EA-inequivalent homogeneous cubic bent functions h_i^n on $\mathbb{F}_2^n$
h_6^{12}	$138 \oplus 13a \oplus 13b \oplus 13c \oplus 148 \oplus 149 \oplus 14b \oplus 14c \oplus 158 \oplus 159 \oplus 15a \oplus 15c \oplus$ $168 \oplus 169 \oplus 16a \oplus 16b \oplus 179 \oplus 17a \oplus 17b \oplus 17c \oplus 189 \oplus 18c \oplus 19a \oplus 1ab \oplus$ $1bc \oplus 234 \oplus 237 \oplus 238 \oplus 239 \oplus 23a \oplus 23b \oplus 245 \oplus 249 \oplus 24a \oplus 24b \oplus 24c \oplus$ $256 \oplus 258 \oplus 25a \oplus 25b \oplus 25c \oplus 267 \oplus 268 \oplus 269 \oplus 26b \oplus 26c \oplus 278 \oplus 279 \oplus$ $27a \oplus 27c \oplus 348 \oplus 34b \oplus 34c \oplus 359 \oplus 35b \oplus 369 \oplus 36c \oplus 37a \oplus 37b \oplus 37c \oplus$ $389 \oplus 39a \oplus 39c \oplus 3ab \oplus 3ac \oplus 458 \oplus 459 \oplus 45c \oplus 46a \oplus 46c \oplus 478 \oplus 47a \oplus$ $48a \oplus 48b \oplus 49a \oplus 4ab \oplus 4bc \oplus 567 \oplus 568 \oplus 569 \oplus 56a \oplus 56c \oplus 578 \oplus 58c \oplus$ $59b \oplus 59c \oplus 5ab \oplus 679 \oplus 67b \oplus 689 \oplus 68a \oplus 68c \oplus 6bc \oplus 789 \oplus 78b \oplus 78c \oplus$ $79a \oplus 79b \oplus 7ab \oplus abc$
h_7^{12}	$138 \oplus 13a \oplus 13b \oplus 13c \oplus 148 \oplus 149 \oplus 14b \oplus 14c \oplus 158 \oplus 159 \oplus 15a \oplus 15c \oplus$ $168 \oplus 169 \oplus 16a \oplus 16b \oplus 179 \oplus 17a \oplus 17b \oplus 17c \oplus 189 \oplus 18c \oplus 19a \oplus 1ab \oplus$ $1bc \oplus 234 \oplus 237 \oplus 238 \oplus 239 \oplus 23a \oplus 23b \oplus 245 \oplus 249 \oplus 24a \oplus 24b \oplus 24c \oplus$ $256 \oplus 258 \oplus 25a \oplus 25b \oplus 25c \oplus 267 \oplus 268 \oplus 269 \oplus 26b \oplus 26c \oplus 278 \oplus 279 \oplus$ $27a \oplus 27c \oplus 348 \oplus 34b \oplus 34c \oplus 359 \oplus 35b \oplus 369 \oplus 36c \oplus 37a \oplus 37b \oplus 37c \oplus$ $389 \oplus 39a \oplus 39c \oplus 3ab \oplus 3ac \oplus 458 \oplus 459 \oplus 45c \oplus 467 \oplus 46a \oplus 478 \oplus 47a \oplus$ $47b \oplus 48a \oplus 48b \oplus 49a \oplus 4ab \oplus 568 \oplus 569 \oplus 56a \oplus 578 \oplus 57b \oplus 58c \oplus 59b \oplus$ $59c \oplus 5ab \oplus 5bc \oplus 67a \oplus 67b \oplus 689 \oplus 68a \oplus 68c \oplus 69c \oplus 6ac \oplus 6bc \oplus 789 \oplus$ $78b \oplus 78c \oplus 79a \oplus 9bc$

B.2 Invariants under extended-affine equivalence

The functions h_1^6 and h_1^8, h_2^8 describe, up to EA-equivalence, all homogeneous functions in 6 and 8 variables, respectively. Functions h_3^{10} and h_1^{10} are the first and the second 10-variable functions from [82, p. 15], respectively. Functions h_2^{10} and h_4^{10} are representatives of equivalence classes of functions constructed in [35, p. 149]. Functions h_i^{12} for $1 \leq i \leq 5$ are representatives of EA-equivalence classes of functions constructed in [35, p. 149]. Functions h_6^{12} and h_7^{12} were constructed in Section 4.3.

Table B.2. Invariants of the known EA-inequivalent homogeneous cubic bent functions h_i^n on $\mathbb{F}_2^n$ in a small number of variables

B.2(a) $6 \leq n \leq 10$ variables

h_i^n	$\mathrm{ind}(h_i^n)$	r-$\mathrm{ind}(h_i^n)$	$\dim(\mathbb{FP}_{h_i^n})$
h_1^6	3	4	3
h_1^8	4	**4**	1
h_2^8	4	5	2
h_1^{10}	5	5	1
h_2^{10}	5	5	1
h_3^{10}	**4**	**4**	1
h_4^{10}	**2**	**4**	**0**

B.2(b) $n = 12$ variables

h_i^n	$\mathrm{ind}(h_i^n)$	r-$\mathrm{ind}(h_i^n)$	$\dim(\mathbb{FP}_{h_i^n})$
h_1^{12}	6	**6**	2
h_2^{12}	6	**6**	2
h_3^{12}	6	7	1
h_4^{12}	6	7	2
h_5^{12}	6	**6**	**0**
h_6^{12}	6	≥ 7	1
h_7^{12}	6	≥ 7	1

In Table B.2, we use bold font to indicate that a function h_i^n on $\mathbb{F}_2^n$:

- Is outside the completed Maiorana-McFarland class, i.e., $\text{ind}(h_i^n) < n/2$ (the second column).
- Is strongly extendable, i.e., $\text{r-ind}(h_i^n) < n/2$, or weakly extendable, i.e., $\text{r-ind}(h_i^n) = n/2$ (the third column).
- Has no affine derivatives, i.e., $\dim(\mathbb{FP}_{h_i^n}) = 0$ (the fourth column).

For each homogeneous cubic bent function $h_i^n \in \mathcal{M}^\#$ on $\mathbb{F}_2^n$, we list the collection $\mathcal{M}_{n/2}(h_i^n)$ as a $|\mathcal{M}_{n/2}(h_i^n)| \times n/2$ matrix in the following way. Each row of $\mathcal{M}_{n/2}(h_i^n)$ describes the Gauss-Jordan basis of an $\mathcal{M}$-subspace of h_i^n. Each element of a basis is given by 32-base number, which can be converted to the binary vector of length n using the following alphabet

$$0 \mapsto 0, \dots, \text{f} \mapsto 15, \text{g} \mapsto 16, \dots, \text{v} \mapsto 31, \tag{4.16}$$

which has already been used in Chapter 4 to describe normal flats of homogeneous cubic bent functions in 10 variables. Using this conversion, it is possible to check that the first row of the matrix $\mathcal{MS}_6(h_3^{12})$ describes the $\text{GJB}(U)$ of the $\mathcal{M}$-subspace U, given in (4.7).

Table B.3. Collections of $n/2$-dimensional $\mathcal{M}$-subspaces of homogeneous cubic bent functions h_i^n on $\mathbb{F}_2^n$ from the completed Maiorana-McFarland class

h_i^n	The collection $\mathcal{MS}_{n/2}(h_i^n)$
h_1^{10}	$\begin{pmatrix} \text{o2} & \text{4l} & \text{2m} & \text{1j} & \text{f} \end{pmatrix}$
h_2^{10}	$\begin{pmatrix} \text{o0} & \text{60} & \text{12} & \text{o} & \text{5} \end{pmatrix}$
h_1^{12} h_2^{12}	$\begin{pmatrix} \text{22r} & \text{10m} & \text{it} & \text{8e} & \text{66} & \text{17} \\ \text{20q} & \text{12o} & \text{in} & \text{af} & \text{4s} & \text{1p} \\ \text{21c} & \text{10d} & \text{gs} & \text{9n} & \text{5r} & \text{2e} \\ \text{20b} & \text{11u} & \text{gj} & \text{9t} & \text{47} & \text{33} \\ \text{20v} & \text{11k} & \text{hh} & \text{9o} & \text{5f} & \text{3i} \end{pmatrix}$
h_3^{12} h_4^{12} h_6^{12} h_7^{12}	$\begin{pmatrix} \text{300} & \text{gg} & \text{88} & \text{44} & \text{22} & \text{11} \\ \text{21u} & \text{10v} & \text{hh} & \text{99} & \text{55} & \text{33} \\ \text{20v} & \text{11u} & \text{hh} & \text{99} & \text{55} & \text{33} \end{pmatrix}$
h_5^{12}	$\begin{pmatrix} \text{300} & \text{gg} & \text{88} & \text{44} & \text{22} & \text{11} \end{pmatrix}$

Bibliography

[1] R. Arshad, Contributions to the theory of almost perfect nonlinear functions, PhD thesis, Otto-von-Guericke-Universität Magdeburg, 2018 (cited on pages 14, 34).

[2] E. Assmus and J. Key, Designs and Their Codes, ser. Cambridge Tracts in Mathematics. Cambridge University Press, 1992 (cited on pages 40, 45).

[3] E. Assmus and H. Mattson, New 5-designs, *Journal of Combinatorial Theory*, vol. 6, no. 2, pp. 122–151, 1969 (cited on page 40).

[4] C. Beierle and G. Leander, New instances of quadratic APN functions, *arXiv Preprint*, 2020 (cited on page 101).

[5] T. D. Bending, Bent functions, SDP designs and their automorphism groups, PhD thesis, Queen Mary and Westfield College, 1993 (cited on pages 42, 43, 74, 75, 94).

[6] T. P. Berger, A. Canteaut, P. Charpin, and Y. Laigle-Chapuy, On almost perfect nonlinear functions over $\mathbb{F}_2^n$, *IEEE Trans. Information Theory*, vol. 52, no. 9, pp. 4160–4170, 2006 (cited on page 34).

[7] T. Beth, D. Jungnickel, and H. Lenz, Design Theory, 2nd ed., ser. Encyclopedia of Mathematics and its Applications. Cambridge University Press, 1999, vol. 2 (cited on pages 37, 39).

[8] T. Beth, D. Jungnickel, and H. Lenz, Design Theory, 2nd ed., ser. Encyclopedia of Mathematics and its Applications. Cambridge University Press, 1999, vol. 1 (cited on pages 37, 39).

[9] W. Bosma, J. Cannon, and C. Playoust, The Magma algebra system. I. The user language, *J. Symbolic Comput.*, vol. 24, no. 3-4, pp. 235–265, 1997, Computational algebra and number theory (London, 1993) (cited on pages 27, 32, 41, 51, 56, 71, 73, 74, 77, 94, 98, 105, 109).

[10] A. Braeken, Cryptographic properties of Boolean functions and S-Boxes, PhD thesis, Katholieke Universiteit Leuven, 2006 (cited on pages xvii, 26, 27).

[11] M. Brinkmann and G. Leander, On the classification of APN functions up to dimension five, *Designs, Codes and Cryptography*, vol. 49, no. 1, pp. 273–288, 2008 (cited on pages xiv, 47, 48).

[12] K. A. Browning, J. F. Dillon, R. E. Kibler, and M. T. McQuistan, APN polynomials and related codes, *Special volume of Journal of Combinatorics, Information and System Sciences*, vol. 34, pp. 135–159, 2009 (cited on page 33).

[13] K. A. Browning, J. F. Dillon, M. T. McQuistan, and A. J. Wolfe, An APN permutation in dimension six, in *Finite Fields: Theory and Applications - Fq9*, G. McGuire, G. L. Mullen, D. Panario, and I. E. Shparlinski, Eds., ser. Contemporary Mathematics, vol. 518, American Mathematical Society, 2010, pp. 33–42 (cited on page 80).

[14] L. Budaghyan, Construction and Analysis of Cryptographic Functions. Springer, 2014 (cited on page 7).

[15] L. Budaghyan and C. Carlet, On CCZ-equivalence and its use in secondary constructions of bent functions, in *Preproceedings of the International Workshop on Coding and Cryptography, WCC 2009*, Ullensvang, Norway, 2009, pp. 19–36 (cited on page 8).

[16] L. Budaghyan and A. Pott, On differential uniformity and nonlinearity of functions, *Discret. Math.*, vol. 309, no. 2, pp. 371–384, 2009 (cited on pages 11, 30).

[17] M. Calderini, On the EA-classes of known APN functions in small dimensions, *Cryptography and Communications*, 2020 (cited on page 33).

[18] P. J. Cameron and J. H. v. Lint, Designs, Graphs, Codes and their Links, ser. London Mathematical Society Student Texts. Cambridge University Press, 1991 (cited on page 45).

[19] A. Canteaut, P. Charpin, and H. Dobbertin, Weight divisibility of cyclic codes, highly nonlinear functions on $\mathbb{F}_{2^m}$, and crosscorrelation of maximum-length sequences, *SIAM J. Discret. Math.*, vol. 13, pp. 105–138, 2000 (cited on page 11).

[20] A. Canteaut and P. Charpin, Decomposing bent functions, *IEEE Trans. Information Theory*, vol. 49, pp. 2004–2019, 2003 (cited on pages 28, 121).

[21] A. Canteaut, P. Charpin, and G. M. Kyureghyan, A new class of monomial bent functions, *Finite Fields and Their Applications*, vol. 14, no. 1, pp. 221–241, 2008 (cited on page 28).

[22] A. Canteaut, M. Daum, H. Dobbertin, and G. Leander, Finding nonnormal bent functions, *Discrete Applied Mathematics*, vol. 154, no. 2, pp. 202–218, 2006 (cited on pages 3, 21, 122).

[23] A. Canteaut and M. Videau, Degree of composition of highly nonlinear functions and applications to higher order differential cryptanalysis, in *Advances in Cryptology — EUROCRYPT 2002*, L. R. Knudsen, Ed., Berlin, Heidelberg: Springer Berlin Heidelberg, 2002, pp. 518–533 (cited on page 17).

[24] C. Carlet, Boolean functions for cryptography and error-correcting codes, in *Boolean Models and Methods in Mathematics, Computer Science, and Engineering*, Y. Crama and P. L. Hammer, Eds., Cambridge University Press, 2010, pp. 257–397 (cited on page 18).

[25] C. Carlet, P. Charpin, and V. Zinoviev, Codes, bent functions and permutations suitable for DES-like cryptosystems, *Design Codes Cryptography*, vol. 15, no. 2, pp. 125–156, 1998 (cited on page 30).

[26] C. Carlet, Two new classes of bent functions, in *Advances in Cryptology — EUROCRYPT '93*, T. Helleseth, Ed., Berlin, Heidelberg: Springer Berlin Heidelberg, 1994, pp. 77–101 (cited on pages 17, 23).

[27] C. Carlet, Boolean functions for cryptography and error-correcting codes, in *Boolean Models and Methods in Mathematics, Computer Science, and Engineering*, ser. Encyclopedia of Mathematics and its Applications, Y. Crama and P. L. Hammer, Eds., Cambridge University Press, 2010, pp. 257–397 (cited on pages 18, 121).

[28] C. Carlet, Boolean and vectorial plateaued functions and APN functions, *IEEE Transactions on Information Theory*, vol. 61, no. 11, pp. 6272–6289, 2015 (cited on pages xv, 9, 63, 85).

[29] C. Carlet, Boolean Functions for Cryptography and Coding Theory. Cambridge University Press, 2021 (cited on pages 6, 11).

[30] C. Carlet and C. Ding, Nonlinearities of S-boxes, *Finite Fields and Their Applications*, vol. 13, no. 1, pp. 121–135, 2007 (cited on page 6).

[31] C. Carlet and E. Prouff, On plateaued functions and their constructions, in *Fast Software Encryption, 10th International Workshop, FSE 2003, Lund, Sweden, February 24-26, 2003, Revised Papers*, 2003, pp. 54–73 (cited on page 9).

[32] F. Chabaud and S. Vaudenay, Links between differential and linear cryptanalysis, in *Advances in Cryptology — EUROCRYPT'94*, Springer,Berlin, 1995, pp. 356–365 (cited on page 11).

[33] C. Charnes, U. Dempwolff, and J. Pieprzyk, The eight variable homogeneous degree three bent functions, *Journal of Discrete Algorithms*, vol. 6, no. 1, pp. 66–72, 2008 (cited on page 106).

[34] C. Charnes, M. Rötteler, and T. Beth, On homogeneous bent functions, in *Applied Algebra, Algebraic Algorithms and Error-Correcting Codes*, S. Boztaş and I. E. Shparlinski, Eds., Berlin, Heidelberg: Springer Berlin Heidelberg, 2001, pp. 249–259 (cited on pages xvii, 104, 105).

[35] C. Charnes, M. Rötteler, and T. Beth, Homogeneous bent functions, invariants, and designs, *Designs, Codes and Cryptography*, vol. 26, no. 1, pp. 139–154, 2002 (cited on pages xvii, 104, 105, 107–109, 112, 121, 133).

[36] P. Charpin, Normal boolean functions, *J. Complexity*, vol. 20, no. 2-3, pp. 245–265, 2004 (cited on page 122).

[37] C. J. Colbourn, M. J. Colbourn, and D. R. Stinson, The computational complexity of finding subdesigns in combinatorial designs, in *Annals of Discrete Mathematics (26): Algorithms in Combinatorial Design Theory*, ser. North-Holland Mathematics Studies, C. Colbourn and M. Colbourn, Eds., vol. 114, North-Holland, 1985, pp. 59 –65 (cited on page 102).

[38] C. J. Colbourn and J. H. Dinitz, Handbook of Combinatorial Designs, Second Edition (Discrete Mathematics and Its Applications). Chapman & Hall/CRC, 2006 (cited on page 36).

[39] T. W. Cusick, Affine equivalence of cubic homogeneous rotation symmetric functions, *Information Sciences*, vol. 181, no. 22, pp. 5067–5083, 2011 (cited on page 93).

[40] J. F. Dillon, A survey of bent functions, *NSA Technical Journal*, vol. Special Issue, pp. 191–215, 1972 (cited on pages xvii, 27, 103).

[41] J. F. Dillon, Elementary Hadamard difference sets, PhD thesis, University of Maryland, 1974 (cited on pages 17, 19, 22, 23, 28, 29, 113).

[42] J. F. Dillon, Slides from talk given at "Polynomials over finite fields and applications", held at Banff International Research Station, 2006 (cited on pages xiv, 48).

[43] J. F. Dillon and J. R. Schatz, Block designs with the symmetric difference property, *R.L. Ward (Ed.), Proc. NSA Mathematical Sciences Meetings, U.S. Government Printing Office, Washington, DC*, pp. 159–164, 1987 (cited on pages 42, 74, 75).

[44] C. Ding, A. Munemasa, and V. D. Tonchev, Bent vectorial functions, codes and designs, *IEEE Transactions on Information Theory*, vol. 65, no. 11, pp. 7533–7541, 2019 (cited on pages 42, 61, 63, 75).

[45] C. Ding, Codes from Difference Sets. World Scientific, 2014 (cited on page 45).

[46] C. Ding, Designs from Linear Codes. World Scientific, 2018 (cited on page 45).

[47] C. Ding and C. Tang, Combinatorial t-designs from special functions, *Cryptography and Communications*, vol. 12, no. 5, pp. 1011–1033, 2020 (cited on page 61).

[48] H. Dobbertin, Construction of bent functions and balanced Boolean functions with high nonlinearity, in *Fast Software Encryption*, B. Preneel, Ed., Berlin, Heidelberg: Springer Berlin Heidelberg, 1995, pp. 61–74 (cited on page 17).

[49] H. Dobbertin, G. Leander, A. Canteaut, C. Carlet, P. Felke, and P. Gaborit, Construction of bent functions via niho power functions, *J. Comb. Theory, Ser. A*, vol. 113, no. 5, pp. 779–798, 2006 (cited on page 28).

[50] M. Duan and X. Lai, Higher order differential cryptanalysis framework and its applications, in *International Conference on Information Science and Technology*, 2011, pp. 291–297 (cited on page 28).

[51] M. Duan, X. Lai, M. Yang, X. Sun, and B. Zhu, Distinguishing properties of higher order derivatives of Boolean functions, Cryptology ePrint Archive, Report 2010/417, 2010 (cited on page 28).

[52] Y. Edel and A. Pott, A new almost perfect nonlinear function which is not quadratic, *Advances in Mathematics of Communications*, vol. 3, no. 1, pp. 59–81, 2009 (cited on pages 10, 48, 98).

[53] Y. Edel and A. Pott, On designs and multiplier groups constructed from almost perfect nonlinear functions, in *Cryptography and Coding, 12th IMA International Conference, Cryptography and Coding 2009, Cirencester, UK, December 15-17, 2009. Proceedings*, 2009, pp. 383–401 (cited on pages 39, 71).

[54] Y. Edel and A. Pott, On the equivalence of nonlinear functions, in *Enhancing Cryptographic Primitives with Techniques from Error Correcting Codes*, 2009, pp. 87–103 (cited on pages 8, 30, 33, 39, 61, 78).

[55] GAP – Groups, Algorithms, and Programming, Version 4.11.0, The GAP Group, 2020 (cited on pages 91, 98).

[56] M. S. Gockenbach, Finite-dimensional linear algebra, ser. Discrete mathematics and its applications. Hoboken, NJ: CRC Press, 2010 (cited on page 36).

[57] X.-D. Hou, Affinity of permutations of $\mathbb{F}_2^n$, *Discrete Applied Mathematics*, vol. 154, no. 2, pp. 313 –325, 2006 (cited on page 45).

[58] X. Hou, Cubic bent functions, *Discrete Mathematics*, vol. 189, no. 1, pp. 149–161, 1998 (cited on pages 28, 119).

[59] Y. J. Ionin and M. S. Shrikhande, Combinatorics of Symmetric Designs, ser. New Mathematical Monographs. Cambridge University Press, 2006 (cited on page 37).

[60] D. Jungnickel, On automorphism groups of divisible designs, *Canadian Journal of Mathematics*, vol. 34, no. 2, pp. 257–297, 1982 (cited on pages 38, 39).

[61] W. M. Kantor, Symplectic groups, symmetric designs, and line ovals, *Journal of Algebra*, vol. 33, no. 1, pp. 43–58, 1975 (cited on page 94).

[62] W. M. Kantor, Classification of 2-transitive symmetric designs, *Graphs and Combinatorics*, vol. 1, no. 1, pp. 165–166, 1985 (cited on pages 73, 94, 100).

[63] A. Kholosha and A. Pott, Bent and related functions, in *Handbook of Finite Fields*, G. L. Mullen and D. Panario, Eds., 1st, Chapman & Hall/CRC, 2013, pp. 262–273 (cited on page 71).

[64] N. Kolomeec, The graph of minimal distances of bent functions and its properties, *Des. Codes Cryptogr.*, vol. 85, no. 3, pp. 395–410, 2017 (cited on page 20).

[65] G. M. Kyureghyan and A. Pott, Some theorems on planar mappings, in *Arithmetic of Finite Fields*, J. von zur Gathen, J. L. Imaña, and Ç. K. Koç, Eds., Berlin, Heidelberg: Springer Berlin Heidelberg, 2008, pp. 117–122 (cited on page 8).

[66] X. Lai, Higher order derivatives and differential cryptanalysis, in *Communications and Cryptography: Two Sides of One Tapestry*, R. E. Blahut, D. J. Costello, U. Maurer, and T. Mittelholzer, Eds., Boston, MA: Springer US, 1994, pp. 227–233 (cited on pages 28, 66).

[67] E. S. Lander, Symmetric Designs: An Algebraic Approach, ser. London Mathematical Society Lecture Note Series. Cambridge University Press, 1983 (cited on pages 38, 94).

[68] P. Langevin, Classification of APN cubics in dimension 6 over GF(2) (cited on pages xiv, 48).

[69] P. Langevin and X.-D. Hou, Counting partial spread functions in eight variables, *IEEE Transactions on Information Theory*, vol. 57, pp. 2263–2269, 2011 (cited on page 25).

[70] P. Langevin and G. Leander, Counting all bent functions in dimension eight 99270589265934370305785861242880, *Designs, Codes and Cryptography*, vol. 59, no. 1, pp. 193–205, 2011 (cited on pages 27, 56, 106).

[71] G. Leander, Monomial bent functions, *IEEE Trans. Information Theory*, vol. 52, no. 2, pp. 738–743, 2006 (cited on page 28).

[72] P. Leopardi, Classifying bent functions by their cayley graphs, *arXiv Preprint*, 2017 (cited on page 27).

[73] S. Li, W. Meidl, A. A. Polujan, A. Pott, C. Riera, and P. Stănică, Vanishing flats: A combinatorial viewpoint on the planarity of functions and their application, *IEEE Transactions on Information Theory*, vol. 66, no. 11, pp. 7101–7112, 2020 (cited on pages xv, 44, 61, 79, 100).

[74] O. Logachev, A. Salnikov, and V. Yashchenko, Boolean Functions in Coding Theory and Cryptography, ser. Translations of mathematical monographs. American Mathematical Soc. (cited on page 18).

[75] F. MacWilliams and N. Sloane, The Theory of Error-Correcting Codes, 2nd. North-holland Publishing Company, 1978 (cited on pages 6, 13, 45, 68).

[76] J. Macwilliams, A theorem on the distribution of weights in a systematic code, *The Bell System Technical Journal*, vol. 42, no. 1, pp. 79–94, 1963 (cited on page 92).

[77] B. Mandal, S. Gangopadhyay, and P. Stănică, Cubic Maiorana-McFarland bent functions with no affine derivative, *International Journal of Computer Mathematics: Computer Systems Theory*, vol. 2, no. 1, pp. 14–27, 2017 (cited on pages 28, 108).

[78] R. L. McFarland, A family of difference sets in non-cyclic groups, *Journal of Combinatorial Theory, Series A*, vol. 15, no. 1, pp. 1–10, 1973 (cited on page 17).

[79] W. Meidl, Slides from talk given at "Boolean Functions and their Applications", 2019 (cited on page 50).

[80] W. Meidl, A. A. Polujan, and A. Pott, Linear codes and incidence structures of bent functions and their generalizations, *Submitted*, 2020 (cited on pages xviii, 61).

[81] W. Meier and O. Staffelbach, Nonlinearity criteria for cryptographic functions, in *Advances in Cryptology — EUROCRYPT '89*, J.-J. Quisquater and J. Vandewalle, Eds., Berlin, Heidelberg: Springer Berlin Heidelberg, 1990, pp. 549–562 (cited on page 7).

[82] Q. Meng, M. Yang, H. Zhang, and J. Cui, A novel algorithm enumerating bent functions, Cryptology ePrint Archive, Report 2004/274, 2004 (cited on pages 104, 106–109, 112, 133).

[83] Q. Meng, M. Yang, H. Zhang, and J. Cui, A novel algorithm enumerating bent functions, *Discrete Mathematics*, vol. 308, no. 23, pp. 5576–5584, 2008 (cited on pages xvii, 56, 105–107).

[84] Q. Meng, H. Zhang, M. Yang, and J. Cui, On the degree of homogeneous bent functions, *Discrete Applied Mathematics*, vol. 155, no. 5, pp. 665 –669, 2007 (cited on page 107).

[85] S. Mesnager, Several new infinite families of bent functions and their duals, *IEEE Transactions on Information Theory*, vol. 60, no. 7, pp. 4397–4407, 2014 (cited on page 28).

[86] S. Mesnager, Bent Functions. Fundamentals and Results, 1st ed. Springer International Publishing, 2016 (cited on pages 17, 28).

[87] S. Mesnager, F. Özbudak, and A. Sinak, On the p-ary (cubic) bent and plateaued (vectorial) functions, *Des. Codes Cryptography*, vol. 86, no. 8, pp. 1865–1892, 2018 (cited on pages 34, 81).

[88] M. Newman and R. C. Thompson, Matrices over rings of algebraic integers, *Linear Algebra and its Applications*, vol. 145, pp. 1–20, 1991 (cited on page 69).

[89] K. Nyberg, Perfect nonlinear S-Boxes, in *Advances in Cryptology — EUROCRYPT '91*, D. W. Davies, Ed., Berlin, Heidelberg: Springer Berlin Heidelberg, 1991, pp. 378–386 (cited on pages 6–8).

[90] K. Nyberg, Differentially uniform mappings for cryptography, in *Workshop on the Theory and Application of Cryptographic Techniques on Advances in Cryptology*, T. Helleseth, Ed., ser. Advances in Cryptology — EUROCRYPT '93, Lofthus, Norway: Springer-Verlag, 1994, pp. 55–64 (cited on page 6).

[91] F. Özbudak and A. Pott, Non-extendable $\mathbb{F}_q$-Quadratic perfect nonlinear maps, in *Open Problems in Mathematics and Computational Science*, Ç. K. Koç, Ed., Cham: Springer International Publishing, 2014, pp. 91–110 (cited on pages xvi, 50, 59).

[92] A. A. Polujan and A. Pott, Homogeneous cubic bent functions without affine derivatives outside the completed Maiorana-McFarland class, in *Proceedings of the Eleventh International Workshop on Coding and Cryptography*, 2019 (cited on pages xviii, 61, 103).

[93] A. A. Polujan and A. Pott, Cubic bent functions outside the completed Maiorana-McFarland class, *Designs, Codes and Cryptography*, vol. 88, no. 9, pp. 1701–1722, 2020 (cited on pages xviii, 61, 103).

[94] A. A. Polujan and A. Pott, On design-theoretic aspects of Boolean and vectorial bent functions, *IEEE Transactions on Information Theory*, vol. 67, no. 2, pp. 1027–1037, 2021 (cited on pages xviii, 47, 61).

[95] A. Pott, Finite geometry and character theory, ser. Lecture Notes in Mathematics. Berlin: Springer, 1995, vol. 1601 (cited on pages 30, 39, 68).

[96] A. Pott, A survey on relative difference sets, in *Proceedings of a special research quarter on Groups, difference sets, and the monster*, Walter de Gruyter & Co., 1996, pp. 195–232 (cited on pages 30, 39).

[97] A. Pott, Nonlinear functions in abelian groups and relative difference sets, *Discret. Appl. Math.*, vol. 138, no. 1-2, pp. 177–193, 2004 (cited on pages 29, 30).

[98] A. Pott, Almost perfect and planar functions, *Des. Codes Cryptography*, vol. 78, no. 1, pp. 141–195, 2016 (cited on page 30).

[99] A. Pott, K.-U. Schmidt, and Y. Zhou, Pairs of quadratic forms over finite fields, *Electr. J. Comb.*, vol. 23, no. 2, P2.8, 2016 (cited on page 14).

[100] B. Preneel, Analysis and design of cryptographic hash functions, PhD thesis, Katholieke Universiteit Leuven, 1993 (cited on pages 27, 106).

[101] C. Qu, J. Seberry, and J. Pieprzyk, On the symmetric property of homogeneous Boolean functions, in *Information Security and Privacy, 4th Australasian Conference*, 1999, pp. 26–35 (cited on page 103).

[102] C. Qu, J. Seberry, and J. Pieprzyk, Homogeneous bent functions, *Discrete Applied Mathematics*, vol. 102, no. 1, pp. 133 –139, 2000 (cited on pages 103, 106).

[103] O. S. Rothaus, On "bent" functions, *Journal of Combinatorial Theory, Series A*, vol. 20, no. 3, pp. 300–305, 1976 (cited on pages xiv, 8, 26, 106).

[104] J. Seberry, T. Xia, and J. Pieprzyk, Construction of cubic homogeneous Boolean bent functions, *Australasian Journal of Combinatorics*, vol. 22, pp. 233–245, Jan. 2000 (cited on pages xvii, 104, 107, 108).

[105] C. E. Shannon, Communication theory of secrecy systems, *The Bell System Technical Journal*, vol. 28, no. 4, pp. 656–715, 1949 (cited on page 2).

[106] L. H. Soicher, DESIGN, The design package for GAP, 2019 (cited on pages 32, 91).

[107] L. H. Soicher, Designs, groups and computing, in *Probabilistic Group Theory, Combinatorics, and Computing: Lectures from the Fifth de Brún Workshop*, A. Detinko, D. Flannery, and E. O'Brien, Eds. London: Springer London, 2013, pp. 83–107 (cited on page 91).

[108] C. Tang, C. Ding, and M. Xiong, Codes, differentially δ-uniform functions, and t-designs, *IEEE Transactions on Information Theory*, vol. 66, no. 6, pp. 3691–3703, 2020 (cited on pages xvi, 45, 61, 63, 64, 76, 91, 92, 94, 95, 100, 101).

[109] N. Tokareva, On the number of bent functions from iterative constructions: Lower bounds and hypotheses, *Advances in Mathematics of Communications*, vol. 5, pp. 609–621, 2011 (cited on pages xiv, 50).

[110] G. Weng, R. Feng, and W. Qiu, On the ranks of bent functions, *Finite Fields and Their Applications*, vol. 13, no. 4, pp. 1096–1116, 2007 (cited on pages 39, 61, 65–67, 71, 110).

[111] G. Weng, R. Feng, W. Qiu, and Z. Zheng, The ranks of Maiorana-McFarland bent functions, *Science in China Series A: Mathematics*, vol. 51, no. 9, pp. 1726–1731, 2008 (cited on pages 39, 66, 73, 74, 110).

[112] Wolfram Research, Inc., Mathematica, Version 11.2, Champaign, IL, 2017 (cited on pages 109, 122).

[113] T. Xia, J. Seberry, J. Pieprzyk, and C. Charnes, Homogeneous bent functions of degree n in $2n$ variables do not exist for $n > 3$, *Discrete Applied Mathematics*, vol. 142, no. 1, pp. 127–132, 2004, Boolean and Pseudo-Boolean Functions (cited on page 107).

[114] Q. Xiang, Recent results on p-ranks and smith normal forms of some 2-(v,k,λ) designs, *Coding theory and quantum computing, Contemp. Math.*, vol. 381, pp. 53–67, 2005 (cited on page 37).

[115] V. V. Yashchenko, On the propagation criterion for Boolean functions and on bent functions, *Probl. Peredachi Inf.*, vol. 33, no. 1, pp. 75–86, 1997, In Russian (cited on page 18).

[116] F. Zhang, N. Cepak, E. Pasalic, and Y. Wei, Further analysis of bent functions from $\mathcal{C}$ and $\mathcal{D}$ which are provably outside or inside $\mathcal{M}^{\#}$, *Discrete Applied Mathematics*, vol. 285, pp. 458–472, 2020 (cited on page 18).

[117] F. Zhang, E. Pasalic, N. Cepak, and Y. Wei, Bent functions in $\mathcal{C}$ and $\mathcal{D}$ outside the completed Maiorana-McFarland class, in *Codes, Cryptology and Information Security - Second International Conference, C2SI 2017, Rabat, Morocco, April 10-12, 2017, Proceedings - In Honor of Claude Carlet*, S. E. Hajji, A. Nitaj, and E. M. Souidi, Eds., ser. Lecture Notes in Computer Science, vol. 10194, Springer, 2017, pp. 298–313 (cited on page 18).

[118] F. Zhang, E. Pasalic, Y. Wei, and N. Cepak, Constructing bent functions outside the Maiorana-McFarland class using a general form of rothaus, *IEEE Trans. Inf. Theory*, vol. 63, no. 8, pp. 5336–5349, 2017 (cited on page 18).

Index

Notation

(n, m)-Functions

$\mathrm{Aut}(F)$ automorphism group of F, 7

$\mathbb{D}(F)$ addition design of an (n, m)-bent function F, 43

$\deg(F)$ algebraic degree of F, 4

$\delta(F)$ differential uniformity of F, 6

Δ_F differential spectrum of F, 6

$\mathcal{G}_F$ graph of F, 5

$\hat{\chi}_F$ Walsh transform of F, 5

Λ_F Walsh spectrum of F, 5

$|\Lambda_F|$ extended Walsh spectrum of F, 5

$\mathcal{AB}_{n,m}$ set of affine free (n, m)-bent functions, 49

$\mathcal{A}_{n,m}$ set of (n, m)-affine functions, 49

$\mathcal{B}_{n,m}$ set of (n, m)-bent functions, 8

$\mathcal{C}_F$ linear code spanned by codewords of $\mathcal{RM}(1, n)$ and
the truth table of F, 33

$\mathcal{M}$ strict Maiorana-McFarland class of vectorial bent functions, 22

$\mathcal{NF}_{\mathbf{v},F}$ set of nonvanishing flats in F_2^n w.r.t. F and nonzero $\mathbf{v} \in \mathbb{F}_2^m$, 78

$\mathcal{NF}_{\mathbf{v}}(F)$ nonvanishing flats of F w.r.t. nonzero $\mathbf{v} \in \mathbb{F}_2^m$
(incidence structure), 78

$\mathcal{PS}_{ap}$ Desarguesian partial spread class of vectorial bent functions, 25

$\mathcal{VF}_F$ set of vanishing flats in F_2^n w.r.t. F, 44

$\mathrm{nl}(F)$ nonlinearity of F, 5