Cryptography and Communications (2022) 14:737–782
https://doi.org/10.1007/s12095-022-00570-x

A survey on *p*-ary and generalized bent functions

Wilfried Meidl [1]

Received: 29 September 2021 / Accepted: 27 February 2022 /Published online: 1 April 2022

Abstract
Boolean bent functions have been introduced by Rothaus in 1966, bent functions in odd characteristic were first considered in 1985 by Kumar, Scholtz, and Welch. Two books on bent functions and some surveys on bent functions and related topics mainly deal with the Boolean case. In this survey, we focus on bent and vectorial bent functions in odd characteristic. Lately, one can observe increasing interest in the bentness of functions from elementary abelian into cyclic groups. Following this development, we also survey recent results on this class of functions.

Keywords p-ary bent function · Vectorial bent function · Difference set · Relative difference set · Generalized bent function · $\mathbb{Z}_{p^k}$-bent function

Mathematics Subject Classification (2010) 06E30 · 05B10 · 11T06 · 94C10 · 94D10

1 Introduction

As indicated in the influential PhD thesis of Dillon [49] in 1974, Boolean bent functions have been introduced in 1966 by Rothaus in the paper [110], which in its final version was published 1976. In 1985, Kumar, Scholtz, and Welch [72] generalized the concept to p-ary functions, i.e., to functions which map from elementary abelian p-groups into the prime field $\mathbb{F}_p$[1]. Boosted by applications in cryptography and coding theory, and by rich connections to objects from geometry and combinatorics, bent functions and related functions developed into a lively research area. Two books on bent functions, [92, 117], chapters in books (see e.g. [23, Chapter 6], [45, Chapter 5]), and several surveys on bent functions and functions related to bent functions, testify to this fact (we refer to [26] and [21, 22]).

The books and surveys *mainly* focus on the Boolean case.[2] In this survey, we concentrate on p-ary (vectorial) bent functions, where p is an odd prime. We especially elaborate the differences between bent functions in characteristic 2

[1] More general, in [72], functions from $\mathbb{Z}_q^n$ to $\mathbb{Z}_q$ are considered for arbitrary positive integers q.
[2] Some treatment of the p-ary case can be found e.g. in [92, Chapters 13,14], or in [117, Chapter 15].

✉ Wilfried Meidl
meidlwilfried@gmail.com

[1] Sabancı University, MDBF, Orhanlı, Tuzla, Istanbul 34956, Turkey

and bent functions in odd characteristic, and analyse several properties, which are specific to bent functions in odd characteristic. For instance, whereas all Boolean bent functions are so-called regular bent functions, the class of p-ary bent functions inherits a much larger variety of properties. It contains the class of dual-bent functions introduced in [31] as a proper subclass, which again contains the class of weakly regular bent functions as a proper subclass. To compare the Boolean and the p-ary case, we will also have to shortly recall some classical results on Boolean bent functions.

Lately, one can observe increasing interest in the bentness of functions from elementary abelian into cyclic groups, leading to the concepts of generalized bent functions and $\mathbb{Z}_{p^k}$-bent functions. We follow this development, and survey recent results on these classes of functions.

The objective of this survey article, is to give comprehensive information on the current status of research on p-ary bent functions, generalized bent and $\mathbb{Z}_{p^k}$-bent functions, albeit without claiming to be exhaustive. Parts of the survey (in particular the choice of the problems) reflect aspects about (vectorial) p-ary bent functions, generalized bent and $\mathbb{Z}_{p^k}$-bent functions, in which I am personally most interested.

This survey article is organized as follows. After the introduction, in Chapter 2, we give the definitions and recall the basic properties of p-ary bent functions, vectorial bent functions, and generalized bent and $\mathbb{Z}_{p^k}$-bent functions. In Chapter 3, we review classes and constructions of p-ary and vectorial bent functions. Chapter 4 is dedicated to regularity and duality for p-ary bent functions. For alternative information on this chapter (including also some proofs), we also may refer to the survey [37] on these special aspects. More properties of p-ary bent functions, like algebraic degree, normality, distance between bent functions, and also some theoretical coding results, are dealt with in Chapter 5. In Chapter 6, some approaches to generalize the classical result on the connection between Boolean bent functions and Hadamard difference sets are discussed. Finally, in Chapter 7, recent results on generalized bent and $\mathbb{Z}_{p^k}$ -bent functions are presented.

We finish the introduction with the definition of bent functions between arbitrary finite abelian groups.

In [105], three equivalent characterizations of bent functions[3] between arbitrary finite abelian groups are shown. The first one is a definition via character sums, for the second one, differential properties of a function are considered. The third definition equivalently uses an object from combinatorics, namely relative difference sets, a generalization of a difference set. We therefore first recall the definitions of a difference set and of a relative difference set.

Definition 1 Let H be a finite (abelian) group of order μ. A subset D of H with k elements is called a (μ, k, λ)-difference set in H, if every element $z \in H$ can be written as $z = d_1 - d_2$ with $d_1, d_2 \in D$, in λ ways.

Let H be an abelian group of order $\mu\nu$ with a subgroup N of order ν. A subset R of H with k elements is called a (μ, ν, k, λ)-relative difference set relative to N, if every element $z \in H \setminus N$ can be written as $z = d_1 - d_2$ with $d_1, d_2 \in R$, in λ ways, and there is no such representation for any nonzero element in N. N is then called the forbidden subgroup.

[3] In [105], the term *perfect nonlinear function* is used.

Clearly, a relative difference set with trivial forbidden subgroup is just a difference set.

Definition 2 Let $(A,+_A)$ and $(B,+_B)$ be two finite abelian groups. A function f from A to B is called a bent function, if and only if one (and hence all) of the following equivalent conditions are satisfied.

(i) For every character χ of $A\times B$ which is nontrivial on B we have[4]

$$\left|\sum_{x\in A}\chi(x,f(x))\right| = \sqrt{|A|}. \tag{1}$$

(ii) For all nonzero $a\in A$, the derivative D_af of f in direction a,

$$D_af(x) = f(x+_A a) -_B f(x)$$

is balanced, i.e., every value in B is taken on the same number $|A|/|B|$ of times.

(iii) The graph of f, $G(f)=\{(x,f(x)) : x\in A\}$, is a relative difference set[5] in $A\times B$ relative to $\{0\}\times B$ (see [105, Theorem 1]).

We remark that bent functions can also be defined between finite non-abelian groups. The charaterizarions in Definition 2 (ii), (iii) still apply, see [99] and [100, 101]. For recent results on bentness of functions on a non-abelian group, respectively between non-abelian groups, also on characterizations in terms of adequately defined *Fourier transforms*, we refer to [53, 120], and [121] and references therein.

Relative difference sets of the type given in Definition 2 (iii) are called *splitting relative difference sets*. In contrast, a relative difference set in a group H is *nonsplitting*, if the forbidden subgroup B has no complement, hence the group H cannot be written as $A\times B$ for some group A. Moreover, for the parameters of $G(f)$ we have $k=\mu$, $G(f)$ is then called *semiregular*. Conversely, semiregular splitting relative difference sets in $A\times B$ define bent functions $f : A\to B$, see [105, p.180]. The study of bent functions is therefore also a study of semiregular splitting relative difference sets (and vice versa). For further background on relative difference sets we refer to [104].

We finally remark that in some literature, the term *perfect nonlinear function* is used, e.g. also in [105]. In this survey, we will use the term bent function, and more concretely, depending on the groups involved, the terms *Boolean bent function, p*-ary *bent function, vectorial bent function, $\mathbb{Z}_{p^k}$-bent function*, which we will introduce in the next section.

2 Bent definitions, basic properties

We first fix some notation, which we will use throughout the survey article.

Let q be a prime power. We denote with $\mathbb{F}_q$ the finite field with q elements. The ring of integers respectively the cyclic group (with respect to the addition) of the integers modulo q, we denote by $\mathbb{Z}_q$ (q will here again always be a prime power). For a positive integer n

[4] By Parseval's identity (see [105, Theorem 4]), for a bent function, the maximal value for $|\sum_{x\in A}\chi(x,f(x))|$ over all such characters (which is $\sqrt{|A|}$) is smallest possible.

[5] The parameters of $G(f)$ obviously are $(\mu,\nu,k,\lambda)=(|A|,|B|,|A|,|A|/|B|)$.

and a prime p, we denote by $\mathbb{V}_n^{(p)}$ the vector space of dimension n over the prime field $\mathbb{F}_p$, and with $\langle , \rangle_n$ we denote a non-degenerate inner product of $\mathbb{V}_n^{(p)}$. If $\mathbb{V}_n^{(p)}$ is represented by $\mathbb{F}_p^n$, the vector space of the n-tuples over $\mathbb{F}_p$, then one may take the conventional dot product $u \cdot v$ for $\langle u, v\rangle_n$, the standard inner product for the finite field $\mathbb{F}_{p^n}$ with p^n elements, is $\langle u, v\rangle_n = \mathrm{Tr}_1^n(uv)$, where $\mathrm{Tr}_1^n(z)$ is the absolute trace of $z \in \mathbb{F}_{p^n}$. Accordingly, for a divisor m of n, $\mathrm{Tr}_m^n(z)$ is the relative trace of $z \in \mathbb{F}_{p^n}$ from $\mathbb{F}_{p^n}$ into the subfield $\mathbb{F}_{p^m}$. (The characteristic p of the field is seen from the context, and is not included in the notation for the trace.) Some classes of interesting functions from $\mathbb{V}_n^{(p)}$ to $\mathbb{F}_p$, like some bent functions, can be represented best in bivariate form, where $\mathbb{V}_n^{(p)} = \mathbb{F}_{p^m} \times \mathbb{F}_{p^m}$, $n = 2m$, in which case we can take the inner product $\langle (u_1, u_2), (v_1, v_2)\rangle_n = \mathrm{Tr}_1^m(u_1 v_1 + u_2 v_2)$.

We will have to strictly distinguish between the addition in elementary abelian groups, and the addition in other structures. Addition and subtraction in vector spaces over a prime field $\mathbb{F}_p$ is hence denoted by $\oplus$ and $\ominus$, whereas $+$ and $-$ stands for addition and subtraction in $\mathbb{Z}_q$, in the integers, complex numbers, etc.

2.1 The Boolean and *p*-ary case

Functions f from $\mathbb{V}_n^{(p)}$ into the prime field $\mathbb{F}_p$, we call *p-ary functions*, and when $p = 2$, as usual also *Boolean functions*. A function f from $\mathbb{F}_p^n$ to $\mathbb{F}_p$ can uniquely be expressed with its *algebraic normal form (ANF)*

$$f(x_1, \ldots, x_n) = \sum_{(j_1,\ldots,j_n)\in\mathbb{F}_p^n} a_{(j_1,\ldots,j_n)} \prod_{i=1}^{n} x_i^{j_i}, \tag{2}$$

with coefficients $a_{(j_1,\ldots,j_n)}$ in $\mathbb{F}_p$. The degree of a monomial $\prod_{i=1}^n x_i^{j_i}$ is $j_1 + \ldots + j_n$, and the largest degree of all monomials in (2) with nonzero coefficient $a_{(j_1,\ldots,j_n)}$ is called the *algebraic degree* of f. If f is given as a function from the finite field $\mathbb{F}_{p^n}$ to $\mathbb{F}_p$, then f can be uniquely represented as a polynomial $f(x) = \sum_{j=0}^{p^n-1} a_j x^j$ of polynomial degree at most $p^n - 1$.[6] Every exponent t can be written in base p representation $t = \sum_{i=0}^{n-1} t_i p^i$, the *weight* of t is then $\sum_{i=0}^{n-1} t_i$. The algebraic degree of f equals the largest weight of an exponent t in the polynomial representation of f, for which $a_t \neq 0$. The constant functions therefore are the functions with algebraic degree 0, the functions of algebraic degree 1 are called *affine functions*.

For p-ary functions $f : \mathbb{V}_n^{(p)} \to \mathbb{F}_p$, the character sum in Equation (1), which is called the *Walsh transform* (or *Walsh-Hadamard transform*) of f, denoted by $\mathcal{W}_f$, is the function from $\mathbb{V}_n^{(p)}$ into the complex numbers $\mathbb{C}$ of the form

$$\mathcal{W}_f(b) = \sum_{x\in\mathbb{V}_n^{(p)}} \zeta_p^{f(x)\ominus\langle b,x\rangle_n}, \quad \zeta_p = e^{2\pi i/p}. \tag{3}$$

The multiset $\{\mathcal{W}_f(b) : b \in \mathbb{V}_n^{(p)}\}$ is called the *Walsh spectrum* of the function f.[7]

[6] Recall that all functions from $\mathbb{F}_{p^n}$ to $\mathbb{F}_{p^n}$ (or with values in a subfield) have a unique representation as a univariate polynomial of degree at most $p^n - 1$.

[7] More precisely, the character sum (3) should be of the form $\mathcal{W}_f(a, b) = \sum_{x\in\mathbb{V}_n^{(p)}} \zeta_p^{af(x)\ominus\langle b,x\rangle_n}$ with $a \in \mathbb{F}_p^*$. However, since with a p-ary function f, also af is bent for all $a \in \mathbb{F}_p^*$, in connection with bentness, the Walsh transform of a p-ary function is commonly defined as in (3).

Differently from the exact value of the Walsh transform $\mathcal{W}_f(b)$ at an element $b \in \mathbb{V}_n^{(p)}$, the Walsh spectrum of f is independent from the inner product used in (3). Definition 2 (i) for p-ary bent functions is then of the following form.

Definition 3 A function f from $\mathbb{V}_n^{(p)}$ to $\mathbb{F}_p$ is called a bent function, if the Walsh transform $\mathcal{W}_f(b)$ of f at b, has absolute value $p^{n/2}$ for all $b \in \mathbb{V}_n^{(p)}$.

The first well-known fundamental differences between the Boolean case and the case of odd primes p, we observe at the possible values in the Walsh spectrum.

The Boolean case. If $p = 2$, then $\zeta_2 = -1$ and $\mathcal{W}_f(b)$ is always an integer. For a Boolean bent function we hence have $\mathcal{W}_f(b) = 2^{n/2}(-1)^{f^*(b)}$ for a Boolean function $f^* : \mathbb{V}_n^{(2)} \to \mathbb{F}_2$, called the *dual*[8] of f. Clearly, n must be even. As is well-known, the dual f^* is a bent function as well, and $(f^*)^* := f^{**} = f$.

The p odd case. Differently from the case that $p = 2$, bent functions from $\mathbb{V}_n^{(p)}$ to $\mathbb{F}_p$, p odd, exist for all integers $n \geq 1$[9]. As first shown in [72] (see also [57]), the values of the Walsh transform of a p-ary bent function are also quite restricted. For a p-ary bent function $f : \mathbb{V}_n^{(p)} \to \mathbb{F}_p$, the *Walsh coefficient* $\mathcal{W}_f(b)$ at $b \in \mathbb{V}_n^{(p)}$ always satisfies

$$\mathcal{W}_f(b) = \begin{cases} \pm\zeta_p^{f^*(b)} p^{n/2} & : \quad p^n \equiv 1 \bmod 4; \\ \pm i\zeta_p^{f^*(b)} p^{n/2} & : \quad p^n \equiv 3 \bmod 4, \end{cases} \tag{4}$$

where f^* is a function from $\mathbb{V}_n^{(p)}$ to $\mathbb{F}_p$, which again is called the dual of f (and $i = \sqrt{-1}$).

A bent function $f : \mathbb{V}_n^{(p)} \to \mathbb{F}_p$ is called *weakly regular* if, for all $b \in \mathbb{V}_n^{(p)}$, we have $\mathcal{W}_f(b) = \epsilon\, \zeta_p^{f^*(b)} p^{n/2}$ for some fixed $\epsilon \in \{\pm 1, \pm i\}$, cf. Equation (4). If $\epsilon = 1$ we call f *regular*[10]. If (the sign of) ϵ changes with $b \in \mathbb{V}_n^{(p)}$, then f is called *non-weakly regular* bent. Weakly regular bent functions f belong to the class of *dual-bent functions*, for which the dual f^* is bent as well. Moreover, we then have $f^{**}(x) = f(-x)$, hence $f^{****}(x) = f(x)$, see e.g. [57]. A non-weakly regular bent function can be either dual-bent or *non-dual-bent*, see [31, 34]. As it is shown in [98], the dual of a non-weakly regular dual-bent function is again non-weakly regular.

Boolean bent functions are defined as the Boolean functions in even dimension with the largest possible nonlinearity $\mathcal{N} = 2^{n-1} - 2^{n/2-1}$, i.e., as the Boolean functions with the furthest distance $\mathcal{N}$ from the set of affine functions. The size of the preimage sets $|f^{-1}(i)|$, $i = 0, 1$, are $2^{n-1} \pm 2^{n/2-1}$. In coding theoretical terms, the distance $\mathcal{N}$ of a Boolean bent function from the set of the affine functions is the covering radius of the first order Reed-Muller code $\mathcal{RM}_2(1, n)$. We refer to [21]. This does not apply for p-ary bent functions and the Reed-Muller code $\mathcal{RM}_p(1, n)$. The size of the preimage sets and the Hamming distance of a p-ary bent function from the set of the affine functions is determined in Theorems 3.2–3.5 in [97].

Theorem 1 [97] *Let $f : \mathbb{V}_n^{(p)} \mapsto \mathbb{F}_p$, p odd, be a bent function, and for $\ell \in \mathbb{F}_p$, let $b_\ell = |f^{-1}(\ell)|$, where $f^{-1}(\ell) = \{x \in \mathbb{V}_n^{(p)} \ : \ f(x) = \ell\}$.*

[8] Since the Walsh coefficient $\mathcal{W}_f(b)$ depends also on the inner product used in (3), strictly speaking, f^* is the dual of f with respect to $\langle , \rangle_n$.

[9] As is shown by Hou in [62], the bent functions $f : \mathbb{F}_p \to \mathbb{F}_p$ are the functions $f(x) = ax^2 \oplus bx \oplus c$, $a \neq 0$.

[10] This trivially applies to Boolean bent functions. Hence we can see Boolean bent functions as regular bent functions.

(i) *If n is even, then there exits a unique $c \in \mathbb{F}_p$ such that $b_c = p^{n-1} \pm (p-1)p^{\frac{n}{2}-1}$ and $b_\ell = p^{n-1} \mp p^{\frac{n}{2}-1}$ for all $\ell \in \mathbb{F}_p \setminus \{c\}$. Moreover, if f is regular, then the upper signs have to be attained. The Hamming distance to the nearest affine function from $\mathbb{V}_n^{(p)}$ to $\mathbb{F}_p$ is $(p-1)p^{n-1} - p^{n/2-1}$ or $(p-1)(p^{n-1} - p^{n/2-1})$. If f is regular, then the latter case applies.*

(ii) *If n is odd, then the value distribution is given by $(b_0, b_1, \ldots, b_{p-1})$ or a cyclic shift of $(b_0, b_1, \ldots, b_{p-1})$, where $b_0 = p^{n-1}$ and $b_\ell = p^{n-1} + \left(\frac{\ell}{p}\right) p^{\frac{n-1}{2}}$ for all $\ell \in \mathbb{F}_p \setminus \{0\}$, or $b_\ell = p^{n-1} - \left(\frac{\ell}{p}\right) p^{\frac{n-1}{2}}$ for all $\ell \in \mathbb{F}_p \setminus \{0\}$, and $\left(\frac{*}{*}\right)$ is the Legendre symbol. The Hamming distance to the nearest affine function from $\mathbb{V}_n^{(p)}$ to $\mathbb{F}_p$ is $(p-1)p^{n-1} - p^{(n-1)/2}$.*

We finish this section with the definitions of some related functions. A p-ary function $f : \mathbb{V}_n^{(p)} \to \mathbb{F}_p$ is called *plateaued* (also *s-plateaued*), if $|\mathcal{W}_f(b)| \in \{0, p^{(n+s)/2}\}$ for an integer s, $0 \le s \le n$, depending only on f.[11] Bent functions are exactly the 0-plateaued functions. If $s = 1$, then f is called *semi-bent* (or also *near-bent*). For $p = 2$ the term semi-bent is also used for $s = 2$ if n is even (note that $n \equiv s \bmod 2$ is required when $p = 2$).[12]

A subclass of the plateaued functions is the class of partially bent functions, which are the functions $f : \mathbb{V}_n^{(p)} \to \mathbb{F}_p$, for which the derivative $D_a f(x) = f(x \oplus a) \ominus f(x)$ is either balanced or constant. The set of elements $a \in \mathbb{V}_n^{(p)}$ for which $D_a f$ is constant forms a subspace of $\mathbb{V}_n^{(p)}$, the *linear space of f*, of some dimension s. The function f is then s-plateaued.

2.2 Vectorial bent functions

Let $\mathbb{V}_n^{(p)}$ and $\mathbb{V}_m^{(p)}$ be vector spaces over $\mathbb{F}_p$ of dimension n and m respectively. For a function F from $\mathbb{V}_n^{(p)}$ to $\mathbb{V}_m^{(p)}$, which we call a *vectorial function* (when $m > 1$), the character sum (1), which is also called the Walsh transform, is given by

$$\mathcal{W}_f(a, b) = \sum_{x \in \mathbb{V}_n^{(p)}} \zeta_p^{\langle a, f(x) \rangle_m \ominus \langle b, x \rangle_n}, \quad \zeta_p = e^{2\pi i/p}.$$

Hence, Definition 2 (i) for vectorial functions appears as follows.

Definition 4 A function F from $\mathbb{V}_n^{(p)}$ to $\mathbb{V}_m^{(p)}$ is called a bent function, if the Walsh transform $\mathcal{W}_f(a, b)$ of F at (a, b), has absolute value $p^{n/2}$ for all $b \in \mathbb{V}_n^{(p)}$ and nonzero $a \in \mathbb{V}_m^{(p)}$.

For a vectorial function $F : \mathbb{V}_n^{(p)} \to \mathbb{V}_m^{(p)}$ and a nonzero element $a \in \mathbb{V}_m^{(p)}$ (and some fixed inner product $\langle , \rangle_m$ of $\mathbb{V}_m^{(p)}$), the p-ary function $F_a : \mathbb{V}_n^{(p)} \to \mathbb{F}_p$, $F_a(x) = \langle a, F(x) \rangle_m$, is called a *component function* of the vectorial function F. The algebraic degree of a vectorial function is the largest algebraic degree among its component functions. In terms of the component functions, a vectorial function F is bent, if and only if all of its component functions are p-ary bent functions. The set of the component functions, together with the 0-function, forms then a vector space of p-ary bent functions of dimension m.

[11] Recall that by Parseval's identity we have $\sum_{b \in \mathbb{V}_n^{(p)}} |\mathcal{W}_f|^2 = p^{2n}$. Hence if f is an s-plateaued function, then $\mathcal{W}_f(b) \neq 0$ for p^{n-s} values of b.

[12] The notion of plateaued functions was introduced in [125]. In some literature, the term *three valued function* is used, and semi-bent functions are called *three valued almost optimal*, see for instance [15].

The following fundamental differences between $p = 2$ and p odd are well known.

$p = 2$. Clearly, also vectorial bent functions $F : \mathbb{V}_n^{(2)} \to \mathbb{V}_m^{(2)}$ can only exist for even n. By Theorem 3.2 (and its Corollary) in [96], for a vectorial bent function $F : \mathbb{V}_n^{(2)} \to \mathbb{V}_m^{(2)}$, m can be at most $n/2$. More precisely, in [96] it is shown that for a vectorial bent function $F : \mathbb{V}_n^{(p)} \to \mathbb{V}_m^{(p)}$ of which all component functions are regular bent functions, m can be at most $n/2$.

p ODD. Bent functions from $\mathbb{V}_n^{(p)}$ to $\mathbb{V}_m^{(p)}$ exist for all integers n and $m \leq n$. Vectorial bent functions on $\mathbb{V}_n^{(p)}$ are called *planar functions*. Planar functions attracted a lot of attention in the literature, in particular due to their connections to projective planes and commutative semifields. We may refer to Section 8 (and also Section 3.3) in the survey paper [106], or to [44].

2.3 Bent functions into the cyclic group

Recently, one can observe increasing interest in functions from the vector space $\mathbb{V}_n^{(p)}$ into the cyclic group $\mathbb{Z}_{p^k}$. The character sum in (1) for functions $f : \mathbb{V}_n^{(p)} \to \mathbb{Z}_{p^k}$ is of the form

$$\mathcal{H}_f(c,u) = \sum_{x \in \mathbb{V}_n^{(p)}} \zeta_{p^k}^{cf(x)} \zeta_p^{\langle u,x\rangle_n}, \quad \zeta_q = e^{2\pi i/q},$$

the accordant version of Definition 2 (i) is then

Definition 5 A function f from $\mathbb{V}_n^{(p)}$ to $\mathbb{Z}_{p^k}$ is bent if and only if $|\mathcal{H}_f(c,u)| = p^{n/2}$ for all $u \in \mathbb{V}_n^{(p)}$ and nonzero $c \in \mathbb{Z}_{p^k}$.

Differently from bent functions between elementary abelian groups, bent functions from $\mathbb{V}_n^{(p)}$ to $\mathbb{Z}_{p^k}$, which we will also call $\mathbb{Z}_{p^k}$*-bent functions*, seem to be "rare", see our discussions in Section 7.2.

The class of functions from $\mathbb{V}_n^{(p)}$ to $\mathbb{Z}_{p^k}$ satisfying only the much weaker condition that $|\mathcal{H}_f(1,u)| = p^{n/2}$ for all $u \in \mathbb{V}_n^{(p)}$, is called the class of *generalized bent functions*. Generalized bent functions originally have been introduced in [111] for $p = 2$, in connection with applications in code division multiple access (CDMA) systems when $k = 2$. Satisfying only a much weaker condition, generalized bent functions (in general) do not yield relative difference sets. As easily seen, cf. [61], $f : \mathbb{V}_n^{(p)} \to \mathbb{Z}_{p^k}$ is bent, if and only if $p^t f$ is generalized bent for all $0 \leq t \leq k-1$. Consequently, generalized bent functions play an important role in the research on $\mathbb{Z}_{p^k}$-bent functions respectively relative difference sets in $\mathbb{V}_n^{(p)} \times \mathbb{Z}_{p^k}$.

The possible values of $\mathcal{H}_f(1,u)$ respectively $\mathcal{H}_f(c,u)$ for a generalized bent function respectively a $\mathbb{Z}_{p^k}$-bent function are similar as for bent functions between elementary abelian groups. The following generalizations are shown in [82] for $p = 2$, and in [94, Lemma 3] for odd p. For the special case, $p = 2$ and n is odd we refer to [111, Lemma 3.3].

Theorem 2 *Let $f : \mathbb{V}_n^{(p)} \to \mathbb{Z}_{p^k}$ be a generalized bent function.*

– Let $p = 2$. If n is even or n is odd and $k \neq 2$, then $\mathcal{H}_f(1,u) = 2^{n/2} \zeta_{2^k}^{f^*(u)}$ for all $u \in \mathbb{V}_n^{(2)}$ and some function $f^* : \mathbb{V}_n^{(2)} \to \mathbb{Z}_{2^k}$. If n is odd and $k = 2$, then $\mathcal{H}_f(1,u) = (1+i)2^{(n-1)/2} i^{f^*(u)}$ for all $u \in \mathbb{V}_n^{(2)}$ and some function $f^* : \mathbb{V}_n^{(2)} \to \mathbb{Z}_4$.

– If p is an odd prime, then

$$\mathcal{H}_f(1,u) = \begin{cases} \pm\zeta_{p^k}^{f^*(u)} p^{n/2} & : \quad p^n \equiv 1 \bmod 4; \\ \pm i\zeta_{p^k}^{f^*(u)} p^{n/2} & : \quad p^n \equiv 3 \bmod 4, \end{cases}$$

where f^* is a function from $\mathbb{V}_n^{(p)}$ to $\mathbb{Z}_{p^k}$.

3 *P*-ary bent functions. Examples and constructions

In this chapter, examples and constructions of p-ary (vectorial) bent functions are reviewed. In general, one distinguishes between primary bent function constructions, i.e., bent functions, which are constructed from scratch, and secondary bent function constructions, where new bent functions are constructed from known bent functions or related functions. Crucial for the classification of (vectorial) bent functions is the concept of equivalence.

Extended affine equivalence Two functions $f, g : \mathbb{V}_n^{(p)} \to \mathbb{V}_m^{(p)}$ are called *extended affine equivalent (EA-equivalent)*, if there exist a linear permutation L_1 of $\mathbb{V}_n^{(p)}$, a linear permutation L_2 of $\mathbb{V}_m^{(p)}$, a linear map $L_3 : \mathbb{V}_n^{(p)} \to \mathbb{V}_m^{(p)}$, and an element $c \in \mathbb{V}_m^{(p)}$, such that

$$g(x) = (L_2 \circ f \circ L_1)(x) + L_3(x) + c. \tag{5}$$

If $L_3 = 0$, then f, g are called *affine equivalent*, if further $c = 0$, then *linear equivalent*.

The algebraic degree and essentially the Walsh spectrum are invariant under EA-equivalence.[13] In particular, if f in (5) is bent, so is g. Therefore, for the classification of (vectorial) bent functions, the concept of EA-equivalence is essential, two (vectorial) bent functions are considered different, if they are not EA-equivalent. In general, it is not easy to decide whether two bent functions of the same algebraic degree are EA-equivalent. For a group theoretic approach we refer to [48].

We remark that for classifying (vectorial) functions, the coarser CCZ-equivalence is used, [24]. However for Boolean functions, p-ary functions, and for bent functions, these two equivalence concepts coincide, see [8, 9].

As for Boolean bent functions, a complete classification of p-ary bent functions is illusive. There are plenty of primary classes of p-ary (vectorial) bent functions known, and with the use of the several known secondary constructions (and concatenations of secondary constructions), a huge amount of (vectorial) bent functions can be generated. As shown in Kantor [68, 69, Remark 4], already in the partial spread class from the Desarguesian spread, which will be recalled below, the number of inequivalent p-ary bent functions (which can then serve as ingredients in secondary constructions), grows exponentially with the dimension. In my opinion, due to the numerous possibilities of bent function constructions, presenting further bent formulas is of limited interest, unless one can show that the obtained functions satisfy some exceptional properties. We concentrate here on some major primary constructions, classes of (vectorial) bent functions with a neat representation (monomials,

[13] If p and n are odd and $a \in \mathbb{F}_p$ is a nonsquare, then the signs in the Walsh spectra of the bent functions f and af from $\mathbb{V}_n^{(p)}$ to $\mathbb{F}_p$ are opposite. Hence in this case e.g. a regular bent function and a weakly regular but not regular bent function can be EA-equivalent. The precise effects of EA-equivalence transformations are listed in [31].

binomials), and on some p-ary versions of secondary constructions, which turned out to be useful to generate bent functions with properties that are specific for the case of p odd. We point to the literature on further constructions of p-ary bent functions in Section 3.4.

3.1 Primary constructions

Quadratic bent functions Quadratic functions, i.e., functions of algebraic degree 2, are partially bent, hence plateaued. In the Boolean case, all quadratic s-plateaued functions form an EA-equivalence class. In particular, every quadratic Boolean bent function from $\mathbb{V}_n^{(2)}$ to $\mathbb{F}_2$ is EA-equivalent to the function $x_1x_2 \oplus x_3x_4 \oplus \cdots \oplus x_{n-1}x_n$ from $\mathbb{F}_2^n$ to $\mathbb{F}_2$.

The situation is different when p is odd. Omitting affine terms, every quadratic function $Q(x)$ in multivariate form, i.e., represented as a function Q from $\mathbb{F}_p^n$ to $\mathbb{F}_p$, can be written as

$$Q(x) = (x_1, \ldots, x_n)A(x_1, \ldots, x_n)^T$$

for some symmetric $n \times n$-matrix over $\mathbb{F}_p$ ($(x_1, \ldots, x_n)^T$ denotes the transpose of the vector $(x_1, \ldots, x_n)$). The quadratic function Q is bent, if and only if A is nonsingular. With a coordinate transformation on $\mathbb{F}_p^n$, A can be transformed into diagonal form, with either $(1, \ldots, 1)$ or $(d, 1, \ldots, 1)$ for some nonsquare $d \in \mathbb{F}_p$ in its main diagonal.

Theorem 3 *For an odd prime p and a nonsquare $d \in \mathbb{F}_p$, let $Q_1, Q_2 : \mathbb{F}_p^n \to \mathbb{F}_p$ be the quadratic functions $Q_1(x) = x_1^2 \oplus x_2^2 \oplus \cdots \oplus x_n^2$ and $Q_2(x) = dx_1^2 \oplus x_2^2 \oplus \cdots \oplus x_n^2$.*

(i) *Q_1 and Q_2 are bent functions with*

$$\mathcal{W}_{Q_1}(b) = \begin{cases} p^{n/2}\zeta_p^{Q_1^*(b)} & : \quad p \equiv 1 \bmod 4, \\ i^n p^{n/2}\zeta_p^{Q_1^*(b)} & : \quad p \equiv 3 \bmod 4, \end{cases}$$

$$\mathcal{W}_{Q_2}(b) = \begin{cases} -p^{n/2}\zeta_p^{Q_2^*(b)} & : \quad p \equiv 1 \bmod 4, \\ -i^n p^{n/2}\zeta_p^{Q_2^*(b)} & : \quad p \equiv 3 \bmod 4, \end{cases}$$

where $Q_1^*(x) = -(4)^{-1}Q_1(x)$, and $Q_2^*(x) = -(4)^{-1}(x_1^2/d \oplus x_2^2 \oplus \cdots \oplus x_n^2)$.

(ii) *If n is even, then every quadratic bent function $Q : \mathbb{V}_n^{(p)} \to \mathbb{F}_p$ is EA-equivalent to either Q_1 or to Q_2. If n is odd, then every quadratic bent function $Q : \mathbb{V}_n^{(p)} \to \mathbb{F}_p$ is EA-equivalent to Q_1.*[14]

For vectorial quadratic bent functions, univariate representation seems most convenient. In particular, all in the literature explicitly given quadratic planar functions are in univariate representation (see Section 3.3 below for some examples). We remark that, omitting affine terms, all quadratic functions on $\mathbb{F}_{p^n}$, p odd, have a unique representation of the form

[14] Multiplying Q_2 with a nonsquare $a \in \mathbb{F}_p$ changes the signs in the Walsh spectrum, aQ_2 can then be transformed to Q_1 with a coordinate transformation.

$$Q(x) = \sum_{\substack{i,j=0,\dots,n-1 \\ i \le j}} a_{i,j} x^{p^i+p^j} \in \mathbb{F}_{p^n}[x]. \tag{6}$$

Polynomials of the form (6) *are called Dembowski-Ostrom polynomials*[15].

Maiorana-McFarland (MMF) bent functions As already observed in [72], the Maiorana-McFarland construction for $p = 2$ can be applied in the same way in odd characteristic.[16] The construction is essentially vectorial. Commonly, Maiorana-McFarland bent functions are represented in bivariate form.

Theorem 4 *Let π be a function on the finite field $\mathbb{F}_{p^m}$.*

p-ary version: For $g : \mathbb{F}_{p^m} \to \mathbb{F}_p$, the function $f : \mathbb{F}_{p^m} \times \mathbb{F}_{p^m} \to \mathbb{F}_p$, $f(x, y) = \mathrm{Tr}_1^m(x\pi(y)) + g(y)$ is bent if and only if π is a permutation. The bent function f is then regular, its dual $f^*(x, y) = \mathrm{Tr}_1^m(-y\pi^{-1}(x)) + g(\pi^{-1}(x))$ is also a Maiorana-McFarland bent function.

Vectorial version: For $G : \mathbb{F}_{p^m} \to \mathbb{F}_{p^m}$, the function $F : \mathbb{F}_{p^m} \times \mathbb{F}_{p^m} \to \mathbb{F}_{p^m}$, $F(x, y) = x\pi(y) + G(y)$ is bent if and only if π is a permutation. All component functions are then regular.

Alternatively one can define a Maiorana-McFarland bent function $f : \mathbb{F}_{p^m} \times \mathbb{F}_{p^m} \to \mathbb{F}_p$ by

$$f(x, y) = f_y(x) \oplus g(y),$$

where $f_y : \mathbb{F}_{p^m} \to \mathbb{F}_p$ is linear and $f_y \neq f_{y'}$ if $y \neq y'$, or as

$$f(x, y) = f_y(x), \tag{7}$$

where $f_y : \mathbb{F}_{p^m} \to \mathbb{F}_p$ are affine functions, and the supports of their Walsh spectra are pairwise disjoint. We note that a function from $\mathbb{F}_{p^m} \to \mathbb{F}_p$ is affine, if and only if it is an m-plateaued function, or equivalently, if and only if the support of the Walsh spectrum contains exactly one value. Hence in the version in Equation (7)*, every $c \in \mathbb{F}_{p^m}$ belongs to the support of the Walsh spectrum of exactly one f_y.*

Spread and partial spread (PS) bent functions Generalizations of the partial spread construction as given in Dillon [49] for $p = 2$, have been presented in [69, 76]. First recall that a *partial spread* of the elementary abelian group $\mathbb{V}_n^{(p)}$, $n = 2m$, is a collection $\mathcal{S} = \{U_1, U_2, \dots, U_K\}$ of m-dimensional subspaces of $\mathbb{V}_n^{(p)}$, which pairwise intersect trivially. If $K = p^m + 1$, i.e., every nonzero element of $\mathbb{V}_n^{(p)}$ is in exactly one subspace, then $\mathcal{S}$ is called a *(complete) spread* of $\mathbb{V}_n^{(p)}$. The standard example is the *Desarguesian spread*, which for $\mathbb{V}_n^{(p)} = \mathbb{F}_{p^m} \times \mathbb{F}_{p^m}$ has the representation $\mathcal{S} = \{U, U_s : s \in \mathbb{F}_{p^m}\}$, with $U = \{(0, y) : y \in \mathbb{F}_{p^m}\}$, and for $s \in \mathbb{F}_{p^m}$, $U_s = \{(x, sx) : x \in \mathbb{F}_{p^m}\}$.

[15] For $p = 2$, slightly differently, the sum is over i, j with $i < j$, as the term $x^{2^j+2^j} = x^{2^{j+1}}$ is linear.

[16] Boolean Maiorana-McFarland functions were introduced independently by Maiorana (unpublished) and McFarland [84] as a generalization of Rothaus' bent functions $x \cdot y \oplus g(x)$ in [110].

Theorem 5 [69, 76]

(i) *Let $\mathcal{S}$ be a partial spread of $\mathbb{V}_n^{(p)}$, $n = 2m$, with at least $(p-1)p^{m-1}$ subspaces. Suppose that $f : \mathbb{V}_n^{(p)} \to \mathbb{F}_p$ is a function such that every nonzero element of $\mathbb{F}_p$ has the union of p^{m-1} subspaces in $\mathcal{S}$, without the 0, as the preimage set, and all other elements are mapped to 0. Then f is a bent function, a so called p-ary PS^- bent function.*

(ii) *Let $\mathcal{S}$ be a partial spread of $\mathbb{V}_n^{(p)}$, $n = 2m$, with at least $(p-1)p^{m-1}+1$ subspaces. For some fixed nonzero $c \in \mathbb{F}_p$, we take the union of $p^{m-1}+1$ subspaces (including 0) as the preimage of c. For all remaining nonzero elements of $\mathbb{F}_p$, the preimage is the union of p^{m-1} subspaces, without the 0. All remaining elements of $\mathbb{V}_n^{(p)}$, the function f maps to 0. Then f is a bent function, a so called p-ary PS^+bent function.*

Both classes of partial spread bent functions are regular.

A (complete) spread is a very powerful object for constructing bent functions, not only between elementary abelian groups, but remarkably, for bent functions from $\mathbb{V}_n^{(p)}$ into any abelian group of order p^k, $k \le n/2$. For a proof of the subsequent theorem, we may refer to [89].

Theorem 6 *Let $U_0, U_1, \ldots, U_{p^m}$ be the subspaces of a spread of $\mathbb{V}_n^{(p)}$, $n = 2m$, and let B be an abelian group of order p^k for some $1 \le k \le m$. We obtain a bent function from $\mathbb{V}_n^{(p)}$ to B as follows.*

1. *For every $z \in B$, the nonzero elements of exactly p^{m-k} of the subspaces U_j, $1 \le j \le p^m$, are mapped to z.*
2. *The elements of U_0 are mapped to a fixed $c \in B$.*

We finally remark that one can obtain vectorial bent functions, and bent functions into other abelian groups, also from partial spreads of $\mathbb{V}_n^{(p)}$ with sufficiently many subspaces, see e.g. [3, 87].

Monomials and Binomials Besides from the big MMF and PS classes, there are not many primary constructions of p-ary bent functions. A few (non-quadratic) monomials and binomials are known. As shown in [10], the following examples do not belong to the *completed Maiorana-McFarland class*, i.e., they are not EA-equivalent to any Maiorana-McFarland bent function. One more monomial we will recall in the section on planar functions below.

$$\textbf{(i)}\ \mathbf{f_1(x) = Tr_1^n\left(ax^{\frac{3^n-1}{4}+3^n+1}\right)}$$

The bentness of this monomial over the finite field $\mathbb{F}_{3^n}$ was conjectured in [57], and then shown in [58, Theorem 1.4], see also [56]. In [38, Theorem 1], the vectorial bentness of the monomial is shown, i.e., it is shown that f_1 is a component of an associated vectorial monomial bent function. We summarize the results in the following theorem, giving a p-ary and a vectorial version.

Theorem 7 *Let $n = 2m$, m odd, $a = \alpha^{(3^m+1)/4}$ for a primitive element α of $\mathbb{F}_{3^n}$.*

p -ary version. The function $f_1 : \mathbb{F}_{3^n} \to \mathbb{F}_3$, $f_1(x) = \mathrm{Tr}_1^n\left(ax^{\frac{3^n-1}{4}+3^n+1}\right)$, is a weakly regular but not regular bent function.

Vectorial version. The function $F_1 : \mathbb{F}_{3^n} \to \mathbb{F}_{3^m}$, $F_1(x) = \mathrm{Tr}_m^n\left(ax^{\frac{3^n-1}{4}+3^m+1}\right)$, is a vectorial bent function all of which component functions are weakly regular but not regular.

$$\textbf{(ii) } \mathbf{f_2(x) = Tr_1^n\left(x^{p^{3k}+p^{2k}-p^k+1} \oplus x^2\right)}$$

The bentness of this binomial is shown in [59], *the vectorial version is Theorem* 2 *in* [38].

Theorem 8 *Let $n = 4k$ for an arbitrary positive integer k.*

p -ary version. The function $f_2 : \mathbb{F}_{p^n} \to \mathbb{F}_p$, $f_2(x) = \mathrm{Tr}_1^n\left(x^{p^{3k}+p^{2k}-p^k+1} \oplus x^2\right)$, is a weakly regular but not regular bent function.

Vectorial version. The function $F_2 : \mathbb{F}_{p^n} \to \mathbb{F}_{p^{2k}}$,

$$F_2(x) = \mathrm{Tr}_{2k}^{4k}\left(x^{p^{3k}+p^{2k}-p^k+1} \oplus x^2\right)$$

is a vectorial bent function with all components weakly regular but not regular bent.

(iii) Functions with Dillon type exponents In [57], it is shown that the monomial function $f_3 : \mathbb{F}_{3^n} \to \mathbb{F}_3$, $n = 2m$, $f_3(x) = \mathrm{Tr}_1^n(ax^d)$, $d = r(3^m - 1)$, is bent under a condition on a Kloosterman sum involving the coefficient $a \in \mathbb{F}_{3^n}$. Exponents d of this form are called Dillon type exponents, yielding functions that are constant on the nonzero elements of the subspaces $\gamma\mathbb{F}_{3^m}$, $\gamma \in \mathbb{F}_{3^n}^*$. The collection of such subspaces forms the Desarguesian spread in univariate representation. These functions are included in the class of the partial spread functions, see Theorem 3.3 in [76], and they are a component function of a vectorial spread bent function, see [38]. Further examples of bent functions with Dillon type exponents are dealt with in [66, 108, 114, 116, 124].

3.2 Secondary constructions

Secondary constructions of bent functions, i.e., constructions of new bent functions from known bent (or related) functions, provide the toolkit to generate a huge amount of new bent functions. The very difficult problem however, is to show whether obtained bent functions are new (in terms of EA-equivalence). With secondary constructions, classes of bent functions with special properties can be obtained, which we do not see in the known primary constructions. We present here (the p-ary version[17] for) three constructions in detail,

[17] Several, but not all, of the primary and secondary Boolean bent function construction procedures work for odd primes p as well. For instance, Niho bent functions, i.e., Dillon's H-class [25, 49], only exist for $p = 2$. The secondary construction of Boolean bent functions in [20, 91], does not work in this form for odd primes p.

which turned out to be useful for the construction of bent and vectorial bent functions with properties, which are specific to p-ary bent functions.

Another procedure to obtain an new bent function from a given one, will be discussed in Section 5.3 in connection with the minimal distance between two bent functions. Bent functions obtained with certain partitions of $\mathbb{V}_n^{(p)}$ occur in connections with generalized bent functions and $\mathbb{Z}_{p^k}$-bent functions on Chapter 7. In Section 3.4 below, the further literature on p-ary bent function constructions is overviewed.

Direct sum and semidirect sum The simplest secondary construction is the *direct sum* of two functions $f : \mathbb{V}_m^{(p)} \to \mathbb{F}_p$ and $g : \mathbb{V}_n^{(p)} \to \mathbb{F}_p$ given by $h(x, y) = f(x) \oplus g(y)$. As easily derived, the Walsh transform of h at $(a, b) \in \mathbb{V}_m^{(p)} \times \mathbb{V}_n^{(p)}$ satisfies $\mathcal{W}_h(a, b) = \mathcal{W}_f(a)\mathcal{W}_g(b)$. For the vectorial version of the direct sum, let F, G be two vectorial bent functions from $\mathbb{V}_m^{(p)}$ respectively from $\mathbb{V}_n^{(p)}$ to $\mathbb{F}_{p^k}$ (without loss of generality we represent $\mathbb{V}_k^{(p)}$ with $\mathbb{F}_{p^k}$). Then the function $H : \mathbb{V}_m^{(p)} \times \mathbb{V}_n^{(p)} \to \mathbb{F}_{p^k}$ given as $H(x, y) = F(x) \oplus G(y)$ is a vectorial bent function. The *semi-direct sum* introduced in [34] for p-ary functions, and in [38] as vectorial construction, can be seen as a generalization of the direct sum.

Theorem 9 *p-ary version. Let $f : \mathbb{V}_m^{(p)} \to \mathbb{F}_p$ and $g : \mathbb{V}_n^{(p)} \to \mathbb{F}_p$ be bent, and let φ be a function from $\mathbb{V}_m^{(p)}$ to $\mathbb{V}_n^{(p)}$. The function $h : \mathbb{V}_m^{(p)} \times \mathbb{V}_n^{(p)} \to \mathbb{F}_p$ defined as $h(x, y) = f(x) \oplus g(y \oplus \varphi(x))$ is bent if and only if for all $b \in \mathbb{V}_n^{(p)}$ the function $\Psi_b : \mathbb{V}_m^{(p)} \to \mathbb{F}_p$, $\Psi_b(x) = f(x) \oplus \langle b, \varphi(x)\rangle_n$ is a bent function. The dual h^* of h is then $h^*(x, y) = \Psi_y^*(x) \oplus g^*(y)$.*

Vectorial version. Let $F : \mathbb{V}_m^{(p)} \to \mathbb{F}_{p^k}$ and $G : \mathbb{V}_n^{(p)} \to \mathbb{F}_{p^k}$ be vectorial bent functions, and let φ be a function from $\mathbb{V}_m^{(p)}$ to $\mathbb{V}_n^{(p)}$. The function $H : \mathbb{V}_m^{(p)} \times \mathbb{V}_n^{(p)} \to \mathbb{F}_{p^k}$ defined as

$$H(x, y) = F(x) \oplus G(y \oplus \varphi(x))$$

is vectorial bent if and only if for all $b \in \mathbb{V}_n^{(p)}$ and nonzero $\alpha \in \mathbb{F}_{p^k}$ the function $G_{b,\alpha} : \mathbb{V}_m^{(p)} \to \mathbb{F}_p$

$$\Psi_{b,\alpha}(x) = \mathrm{Tr}_1^k(\alpha F(x)) \oplus \langle b, \varphi(x)\rangle_n$$

is a bent function.

Remark 1 If φ is the zero function, then the condition in Theorem 9 trivially holds, and the semi-direct sum reduces to the direct sum.

The secondary construction of Boolean bent functions in Carlet [17] is the special case of the semidirect sum with $g(x) = x_1x_2 \oplus x_3x_4 \oplus \cdots \oplus x_{n-1}x_n$.

Generalized Maiorana-McFarland In [28, 30], a construction of p-ary bent functions is presented, which can be seen as a p-ary version of the construction of Boolean bent functions from semi-bent functions in [14, 41, 74]. The p-ary version we present here is from [31].

Theorem 10 *Let $g_y : \mathbb{V}_n^{(p)} \to \mathbb{F}_p$, $y \in \mathbb{V}_s^{(p)}$, be a collection of p^s functions all of which are s-plateaued such that the supports of the Walsh spectra $\{b \in \mathbb{V}_n^{(p)} : \mathcal{W}_{g_y}(b) \neq 0\}$ are pairwise disjoint. Then $f : \mathbb{V}_n^{(p)} \times \mathbb{V}_s^{(p)} \to \mathbb{F}_p$*

$$f(x, y) = g_y(x)$$

is a p-ary bent function.

Remark 2 In the extreme case that $s = m$, hence all g_y are affine functions, the construction in Theorem 10 reduces to the Maiorana-McFarland construction as it is described in (7). Hence we refer to the construction in Theorem 10 as the *generalized Maiorana-McFarland construction*.

Remark 3 Looking at the construction from the perspective of the corresponding relative difference sets, it can be seen as an instance of the construction principle of relative difference sets in [47], see [2].

Sets of plateaued functions with the properties required for the generalized Maiorana-McFarland construction, one can obtain starting with bent functions, see [30]. A concrete realization, by which a bent function in $n+2$ variables is obtained from an arbitrary set of p bent functions in n variables, is given in the following theorem, which we give in two versions since Theorem 10 also supports a construction of vectorial bent functions.

Theorem 11 [31, *Theorem* 2], [38, *Theorem* 3]

p -ary version. For $j = 0, \ldots, p-1$, let g_j be bent functions from $\mathbb{V}_n^{(p)}$ to $\mathbb{F}_p$. Then $f : \mathbb{V}_{n+2}^{(p)} \to \mathbb{F}_p$

$$f(x, x_{n+1}, y) = g_y(x) \oplus x_{n+1} y \tag{8}$$

is a bent function. Its dual f^* is

$$f^*(x, x_{n+1}, y) = g^*_{x_{n+1}}(x) \ominus x_{n+1} y. \tag{9}$$

Vectorial version. For every $y \in \mathbb{F}_{p^k}$ let G_y be a vectorial bent function from $\mathbb{F}_{p^k}^n$ to $\mathbb{F}_{p^k}$ (without loss of generality we here use these representations for the vector spaces). Then the function $F : \mathbb{F}_{p^k}^{n+2} \to \mathbb{F}_{p^k}$ defined as

$$F(x_1, \ldots, x_n, x_{n+1}, y) = G_y(x_1, \ldots, x_n) \oplus y x_{n+1}$$

is a vectorial bent function.

Generalized Rothaus construction In [85], a generalization of a construction in Rothaus [110], that also applies to p-ary functions, p odd, is presented. For the construction we need three bent functions $f_1, f_2, f_3 : \mathbb{V}_n^{(p)} \to \mathbb{F}_p$, for which linear combinations (not necessarily all) are also bent. One may simply employ three (linearly independent) components of a vectorial bent function.

Theorem 12 *Let $f_1,f_2,f_3 : \mathbb{V}_n^{(p)} \to \mathbb{F}_p$ be linearly independent component functions of a vectorial bent function, and let a, b, c be elements of $\mathbb{F}_p$. The function g from $\mathbb{V}_n^{(p)} \times \mathbb{F}_p^2$ to $\mathbb{F}_p$ given by*

$$g(x,y,z) = f_1^2(x) \ominus f_1f_2(x) \oplus f_2f_3(x) \ominus f_1f_3(x) \oplus af_1(x) \oplus bf_2(x) \oplus cf_3(x) \\ \oplus (f_2(x) \ominus f_1(x))y \oplus (f_3(x) \ominus f_1(x))z \oplus yz$$

is bent if and only if $a \oplus b \oplus c \neq 0$[18].

For $p = 2$, in which case g is bent whenever $a \oplus b \oplus c = 1$, with the choice $a = 1$, $b = c = 0$, one obtains Rothaus' construction of Boolean bent functions in [110]. *We remark that for this case, it is sufficient that with f_1,f_2,f_3 also $f_1 \oplus f_2 \oplus f_3$ is bent.*

3.3 Planar functions

Bent functions from $\mathbb{V}_n^{(p)}$ to $\mathbb{V}_n^{(p)}$, which only exist for odd primes p, are called planar functions. By the alternative definition of bent functions via derivatives, a function $F : \mathbb{V}_n^{(p)} \to \mathbb{V}_n^{(p)}$ is planar, if for every nonzero $a \in \mathbb{V}_n^{(p)}$ the derivative $D_aF(x) = F(x \oplus a) \ominus F(x)$ is a permutation of $\mathbb{V}_n^{(p)}$. Planar functions are particularly interesting for their connections to projective planes or to commutative semifields. A lot of research therefore focused on planar functions. An excellent survey on the results on planar functions (and on APN functions), is the paper [106]. We hence here solely sketch the connections to *projective planes* and *commutative semifields*, give some examples for planar functions, and refer to the literature.

The graph of a planar function is a relative difference set in $\mathbb{V}_n^{(p)} \times \mathbb{V}_n^{(p)}$ with parameters $(p^n, p^n, p^n, 1)$. Relative difference sets with parameters $(v, v, v, 1)$ induce *divisible (v, v, v, 1)-designs*, which uniquely can be extended to projective planes of order v[19]. For details we refer to [106, Section 3.3], and the references therein.

The only known not quadratic planar functions are the *Coulter-Matthews* functions, [43], $F : \mathbb{F}_{3^n} \to \mathbb{F}_{3^n}$,

$$F(x) = x^{\frac{3^t+1}{2}}, \quad t \text{ is odd, and } \gcd(t,n) = 1. \tag{10}$$

Any quadratic planar function, i.e., planar Dembowski–Ostrom polynomial, describes a commutative (pre)semifield $(\mathbb{F}_{p^n}, +, *)$ (see [70, 73]), and vice versa, any commutative (pre) semifield of odd order can be described by a planar Dembowski–Ostrom polynomial. The corresponding projective planes are then semifield planes, i.e., coordinatised by the commutative semifield. For several results on planar functions and their connections to commutative semifields we refer to [12, 44, 118]. Some examples of quadratic planar functions on $\mathbb{F}_{p^n}$ with neat polynomial representation (and the corresponding semifields) are the *Gold functions* $F(x) = x^2$ (finite field), $F(x) = x^{p^k+1}$, $n/\gcd(n,k)$ odd (generalized twisted fields [1]), and the functions $F(x) = x^{10} \pm x^6 \ominus x^2$, $p = 3$, n odd [43, 51]. Some more examples are in [6] or in [11, 13] respectively in [7].

[18] For the bentness of g it is sufficient that $\lambda_1f_1(x) \oplus \lambda_2f_2(x) \oplus \lambda_3f_3(x)$ is bent for all $\lambda_1, \lambda_2, \lambda_3 \in \mathbb{F}_p$, for which $\lambda_1 \oplus \lambda_2 \oplus \lambda_3 = a \oplus b \oplus c$, see [85, Remark 1].

[19] It is conjectured that v has to be a prime power.

For more detailed information and an exhaustive list, we refer to Chapter 8 in [106], and to the references therein.

3.4 Some more examples

In this section, we point to the further p-ary bent function constructions, which one can find in the literature, without going into the details. I like to emphasize again, that with the large number of bent functions from primary constructions and the rich toolkit provided by secondary constructions (and concatenations of secondary constructions), one can easily generate huge quantities of (p-ary) bent functions, also bent functions, which do not belong to one of the major classes[20] (which is not always easy to see).

As is observed in [102, 103], the construction in Carlet [18] of a new Boolean bent functions by altering the values of a Boolean bent function $f : \mathbb{V}_n^{(2)} \to \mathbb{F}_2$ on an $n/2$-dimensional affine subspace on which f is affine, has a p-ary version. This observation plays the key role in the research on the minimal distance between bent functions, which will be discussed in Section 5.3.

With similar principles, considering subspaces, Mandal et al. [79] presented p-ary generalizations of Carlet's $\mathcal{C}$ and $\mathcal{D}$ class.

In [122, 123], (non-quadratic) p-ary bent functions are obtained by modifying a quadratic bent monomial on a hyperplane

Bent functions of the form

$$f(x) = g(x) \oplus F(\mathrm{Tr}_1^n(u_0 x), \mathrm{Tr}_1^n(u_1 x), \ldots, \mathrm{Tr}_1^n(u_{k-1} x)), \tag{11}$$

where $g : \mathbb{F}_{p^n} \to \mathbb{F}_p$ is a (weakly regular) bent function, $u_i \in \mathbb{F}_{p^n}^*$, $0 \le i \le k-1$, are presented in [109]. We observe that (11) is of the shape (20) in Section 7.1. As we will see, (11) has an interpretation as a bent function with a partition, and can be analysed in connection with the concept of generalized bent functions, which we will discuss in Chapter 7. Large classes of (p-ary) bent and vectorial bent functions can be obtained with partitions corresponding to generalized bent functions and $\mathbb{Z}_{p^k}$-bent functions, as will be presented in Chapter 7.

3.5 Some Questions

The primary constructions of bent functions in Section 3.1 are vectorial. Also for some secondary constructions we have vectorial versions. In fact it has not yet been shown from any Boolean or p-ary bent function to be *lonely*, i.e., to be not a component function of some vectorial bent function.

Question 1 Do lonely p-ary (or Boolean) bent functions exist, or is every p-ary (Boolean) bent function a component function of some vectorial bent function?

A similar question one can ask for vectorial bent functions $F : \mathbb{V}_n^{(p)} \to \mathbb{V}_m^{(p)}$ for $m < n/2$ when $p = 2$, and $m < n$ when p is odd. A related question, motivated by the fact that on the

[20] As we will see in Section 4.1, there are many possibilities to obtain non-weakly regular bent functions, which never belong to any of the primary classes introduced in this section.

one hand some planar functions are known, on the other hand, some vectorial bent functions from $\mathbb{V}_n^{(p)}$ to $\mathbb{V}_{n/2}^{(p)}$ (n even) are known, is the following.

Question 2 Do there exist vectorial bent functions from $\mathbb{V}_n^{(p)}$ to $\mathbb{V}_m^{(p)}$ with $n/2 < m < n$, which are not a projection[21] of a planar function?

Spread bent functions are those bent functions which are constant on the subspaces of a spread (0 is taken out from all but one subspace), the bent functions which are affine on the subspaces of a spread form Dillon's $\mathcal{H}$ class[22], which for the Desarguesian spread in univariate representation is also known as the class of Niho bent functions, see [25]. The latter class only exists for $p = 2$, [33]. On the other hand, some of the explicit examples of (non-quadratic) p-ary bent functions, like f_1 and f_2 in Section 3.1, are quadratic on every subspace of the Desarguesian spread (univariate representation).

Question 3 Can one characterize (non-quadratic) bent functions which are quadratic restricted to the subspaces of a spread?

The perhaps most famous problem on planar functions is

Question 4 [106, Problem 8.21] Find more non-quadratic planar functions, or show that the Coulter-Matthews functions (10) are the only ones.

4 Regularity and duality for *p*-ary bent functions

A Boolean bent function is always regular. The situation is very different for p-ary bent functions, p odd, they inherit a much larger variety of properties. P-ary bent functions contain the class of dual-bent functions as a proper subclass, which again contains the class of weakly regular bent functions as a proper subclass. A considerable amount of research on p-ary bent functions deals hence with regularity and duality. We emphasize that the classes of weakly regular, of non-weakly regular, and of dual-bent functions are invariant under EA-equivalence, cf. [31].

All classical constructions of bent functions presented in Chapter 3, yield weakly regular bent functions. The first sporadic examples of non-weakly regular bent functions, all ternary functions found with computer search, were published in [57, 59, 60, 113]:

1. $g_1 : \mathbb{F}_{3^6} \to \mathbb{F}_3$ with $g_1(x) = \mathrm{Tr}_1^6(\xi^7 x^{98})$, where ξ is a primitive element of $\mathbb{F}_{3^6}$, see [57],
2. $g_2 : \mathbb{F}_{3^4} \to \mathbb{F}_3$ with $g_2(x) = \mathrm{Tr}_1^4(a_0 x^{22} \oplus x^4)$, where for a primitive element ξ of $\mathbb{F}_{3^4}$, $a_0 \in \{\oplus\xi^{10}, \ominus\xi^{10}, \oplus\xi^{30}, \ominus\xi^{30}\}$, see [59],
3. $g_3 : \mathbb{F}_{3^3} \to \mathbb{F}_3$ with $g_3(x) = \mathrm{Tr}_1^3(x^{22} \oplus x^8)$, or alternatively $\tilde{g}_3 : \mathbb{F}_3^3 \to \mathbb{F}_3$ with $\tilde{g}_3(x_1, x_2, x_3) = x_2^2 x_3^2 \oplus 2x_3^2 \oplus x_1 x_3 \oplus x_2^2$, see [113],
4. $g_4, g_5 : \mathbb{F}_{3^6} \to \mathbb{F}_3$ with $g_4(x) = \mathrm{Tr}_1^6(\xi x^{20} \oplus \xi^{41} x^{92})$, $g_5(x) = \mathrm{Tr}_1^6(\xi^7 x^{14} \oplus \xi^{35} x^{70})$, where ξ is a primitive element of $\mathbb{F}_{3^6}$, see [60].

[21] Seen a planar function on $\mathbb{V}_n^{(p)}$ as an n-dimensional vector space of bent functions, one can consider a projection, i.e., delete some coordinates. This results in a vectorial bent function from $\mathbb{V}_n^{(p)}$ to $\mathbb{V}_m^{(p)}$, where $m < n$ can be chosen arbitrarily, which is a vectorial component function of the planar function.

[22] Spread bent functions with an affine term added, which are also affine on the subspaces of a spread, are excluded.

As it was observed in [31], the duals of the bent functions g_1, g_2, g_5 are not bent, hence g_1, g_2, g_5 are non-dual-bent functions, whereas the duals of g_3, g_4 are bent functions, [31].

Since then, some effort has been given to construct examples and classes of p-ary bent functions of various types, and also results on properties of component functions for vectorial bent functions have been presented. We here also refer to the survey paper [37].

4.1 Regularity

The sporadic ternary examples of non-weakly regular bent functions in low dimension, indicate that (as dimension increases) there may be infinitely many of such functions. The first confirmation of this fact has been provided in [113] with a recursive argument employing the direct sum construction.

Proposition 1 [113] *For some odd prime p, let $f : \mathbb{V}_m^{(p)} \to \mathbb{F}_p$ be a non-weakly regular bent function, and let $g : \mathbb{V}_n^{(p)} \to \mathbb{F}_p$ be weakly regular bent. The direct sum $h(x, y) = f(x) \oplus g(y)$ from $\mathbb{V}_m^{(p)} \times \mathbb{V}_n^{(p)}$ to $\mathbb{F}_p$ is then a non-weakly regular bent function.*

Note that this result easily follows from the identity $\mathcal{W}_h(a.b) = \mathcal{W}_f(a)\mathcal{W}_g(b)$. With the sporadic examples and Proposition 1, one can now obtain non-weakly regular ternary bent functions in any dimension $n \geq 3$.

The first explicit construction of non-weakly regular bent functions has been presented in [28], see also [30]. The functions belong to the generalized Maiorana-McFarland class obtained with the secondary construction in Theorem 10, which was established in [28] for the purpose of constructing non-weakly regular bent functions.

The most suitable version for easily obtaining non-weakly regular bent functions, is the version in Theorem 11, in which a bent function f from $\mathbb{V}_{n+2}^{(p)}$ to $\mathbb{F}_p$ is constructed from bent functions f_j, $0 \leq j \leq p-1$, from $\mathbb{V}_n^{(p)}$ to $\mathbb{F}_p$. From the explicit expression (9) of the dual of f,

$$f^*(x, x_{m+1}, y) = f^*_{x_{m+1}}(x) \ominus x_{m+1}y,$$

we see that f is non-weakly regular if some f_j are regular, and some are weakly regular but not regular. This is easily achieved, by picking for f_j, $0 \leq j \leq p-1$, quadratic bent functions. We arrive at

Theorem 13 *The generalized Maiorana-McFarland construction gives weakly regular and non-weakly regular p-ary bent functions*[23] *in any even or odd dimension $n \geq 3$ and for every odd prime p.*

We remark that the dual f^* also belongs to the generalized Maiorana-McFarland class, hence if all f_j^* are bent (i.e., all f_j are dual-bent functions), then also f^* is bent. Therefore f is dual-bent. Several interesting examples of generalized Maiorana-McFarland bent functions are in [31], among others, bent functions f for which the dual f^* has a different algebraic degree, which guarantees that f and f^* are EA-inequivalent.

[23] Note that f is weakly regular only if all of the bent functions f_j are regular, or all are weakly regular but not regular. Hence, mostly one will obtain a non-weakly regular bent function.

Having explicit constructions of non-weakly regular bent functions, the question if non-weakly regular bent functions can be components of vectorial bent functions[24], is natural. It is observed in [38], that the above sporadic example g_1 of a ternary non-weakly regular bent function has the vectorial version $G : \mathbb{F}_{3^6} \to \mathbb{F}_{3^3}$, $G(x) = \mathrm{Tr}_3^6(\xi^7 x^{98})$, ξ is a primitive element of $\mathbb{F}_{3^6}$. Hence G is an example of a vectorial bent function with non-weakly regular component functions. Moreover, the components are also non-dual-bent functions.

The first constructions of vectorial bent functions with non-weakly regular components for any odd prime p, have been presented in [38]. In [38, Section 3], the vectorial version of Theorem 11 has been employed: For every $y \in \mathbb{F}_{p^k}$, choose a vector $(a_{y,1}, a_{y,2}, \ldots, a_{y,n}) \in (\mathbb{F}_{p^k}^*)^n$. The functions G_y from $\mathbb{F}_{p^k}^n$ to $\mathbb{F}_{p^k}$ of the form

$$G_y(x_1, x_2, \ldots, x_n) = a_{y,1}x_1^2 \oplus a_{y,2}x_2^2 \oplus \cdots \oplus a_{y,n}x_n^2,$$

are then vectorial bent. Using results on the Walsh transform for the planar function x^2 (see [57, Corollary 3]) and an iterative argument, it is shown that, under some easy to satisfy condition, all component functions of the vectorial bent functions $F : \mathbb{F}_{p^k}^{n+2} \to \mathbb{F}_{p^k}$ obtained via Theorem 11 with the functions of the form G_y,

$$\begin{aligned} F(x_1, \ldots, x_n, x_{n+1}, y) =& G_y(x_1, \ldots, x_n) \oplus yx_{n+1} \\ =& a_{y,1}x_1^2 \oplus a_{y,2}x_2^2 \oplus \cdots \oplus a_{y,n}x_n^2 \oplus yx_{n+1} \end{aligned} \tag{12}$$

are non-weakly regular, yet dual-bent functions, see [38, Theorem 4].

Theorem 14 *The vectorial version of the generalized Maiorana-McFarland construction in Theorem 11 can produce vectorial bent functions of which all components are non-weakly regular dual-bent functions.*

A different construction of non-weakly regular bent functions in [85] uses the generalized Rothaus construction presented in Theorem 12. We refer to [85] for a comparison with the generalized Maiorana-McFarland construction. In the constructions in [85], planar functions, namely the Gold function and the Coulter-Matthews function, are employed. The following theorem is Corollary 1 and Corollary 2 in [85].

Theorem 15 *Let p be an odd prime and n, k be integers such that $n/\gcd(n,k)$ is odd ($p = 3$ and n, k be integers such that $gcd(2n, k) = 1$), and let $g : \mathbb{F}_{p^n} \to \mathbb{F}_{p^n}$ be the Gold function $g(x) = x^{p^k+1}$ (the Coulter-Matthews function $g(x) = x^{(3^k+1)/2}$). For linearly independent elements $\alpha_1, \alpha_2, \alpha_3$ of $\mathbb{F}_{p^n}$, not all of which are squares respectively nonsquares in $\mathbb{F}_{p^n}$, and $a, b, c \in \mathbb{F}_p$ such that $a \oplus b \oplus c \neq 0$, the function $h : \mathbb{F}_{p^n} \times \mathbb{F}_p^2 \to \mathbb{F}_p$,*

$$\begin{aligned} h(x, y, z) =& (\mathrm{Tr}_1^n(\alpha_1 g(x))^2 \ominus \mathrm{Tr}_1^n(\alpha_1 g(x))\mathrm{Tr}_1^n(\alpha_2 g(x)) \\ &\oplus \mathrm{Tr}_1^n(\alpha_2 g(x))\mathrm{Tr}_1^n(\alpha_3 g(x)) \ominus \mathrm{Tr}_1^n(\alpha_1 g(x))\mathrm{Tr}_1^n(\alpha_3 g(x)) \\ &\oplus \mathrm{Tr}_1^n((a\alpha_1 \oplus b\alpha_2 \oplus c\alpha_3)g(x)) \oplus \mathrm{Tr}_1^n((\alpha_2 \ominus \alpha_1)g(x)y) \\ &\oplus \mathrm{Tr}_1^n((\alpha_3 \ominus \alpha_1)g(x)z) \oplus yz \end{aligned}$$

is a non-weakly regular bent function.

[24] This question is quite opposite to Question 1 on the existence of lonely bent functions.

4.2 Non-dual-bent functions

Similarly as for non-weakly regular bent functions, also non-dual-bent functions can be constructed recursively. As observed in [34, Theorem 3], besides from the direct sum, also the generalized Maiorana-McFarland construction can be used, see also [37, Theorem 2].

Theorem 16

(i) *For $z = 0, \dots, p-1$, let g_z be bent functions from $\mathbb{V}_n^{(p)}$ to $\mathbb{F}_p$. The generalized Maiorana-McFarland bent function $f : \mathbb{V}_n^{(p)} \times \mathbb{F}_p^2 \to \mathbb{F}_p$*

$$f(x, y, z) = g_z(x) \oplus yz$$

is dual-bent, if and only if for all $0 \le z \le p-1$ the function g_z is dual-bent.

(ii) *The direct sum of a dual-bent function and a non-dual-bent function is a non-dual-bent function.*

With Theorem 16, and the non-dual-bent functions g_1, g_2, g_5 presented at the beginning of this chapter, we can now obtain non-dual-bent functions for $p = 3$ and any dimension $n \ge 4$. What is missing, is a generic construction of non-dual-bent functions, possibly also yielding non-dual-bent functions for p other than 3. Such a construction was finally given in [34] using the semi-direct sum. With the vectorial version introduced in [38], we can simultaneously obtain non-dual-bent functions and vectorial bent functions with non-dual component functions.

To apply the semi-direct sum construction in Theorem 9, we identify $\mathbb{V}_m^{(p)}$ with $\mathbb{F}_{p^m}$ and $\mathbb{V}_n^{(p)} = \mathbb{V}_{2k}^{(p)}$ with $\mathbb{F}_{p^k} \times \mathbb{F}_{p^k}$. We employ the Gold planar function x^2, take for $F : \mathbb{F}_{p^m} \to \mathbb{F}_{p^k}$ the function $F(x) = \mathrm{Tr}_k^m(x^2)$, and for some γ_1, γ_2 in $\mathbb{F}_{p^m}$ such that $1, \gamma_1, \gamma_2$ are linearly independent over $\mathbb{F}_{p^k}$, we choose $\varphi : \mathbb{F}_{p^m} \to \mathbb{F}_{p^k} \times \mathbb{F}_{p^k}$ as $\varphi(x) = (\mathrm{Tr}_k^m(\gamma_1 x^2), \mathrm{Tr}_k^m(\gamma_2 x^2))$. The vectorial bent function $G : \mathbb{F}_{p^k} \times \mathbb{F}_{p^k} \to \mathbb{F}_{p^k}$, is the Maiorana-McFarland bent function $G(x, y) = xy$. It is easily seen that the conditions for Theorem 9 are then satisfied. The symbol $\eta(z)$ in the following theorem, denotes the quadratic character of $z \in \mathbb{F}_{p^m}$.

Theorem 17 [34, 38]

p -ary version. Let $1, \gamma_1, \gamma_2 \in \mathbb{F}_{p^m}$ be linearly independent over $\mathbb{F}_p$. If

$$\left| \sum_{y_1, y_2 \in \mathbb{F}_p} \eta(1 + y_1\gamma_1 + y_2\gamma_2) \epsilon_p^{-y_1 y_2} \right| \neq p, \tag{13}$$

then the function $f : \mathbb{F}_{p^m} \times \mathbb{F}_p^2 \to \mathbb{F}_p$

$$f(x, y_1, y_2) = \mathrm{Tr}_1^m(x^2) + (y_1 + \mathrm{Tr}_1^m(\gamma_1 x^2))(y_2 + \mathrm{Tr}_1^m(\gamma_2 x^2))$$

is a non-dual-bent function.

Vectorial version. Let $m = 3k$, and let $\{1, \gamma_1, \gamma_2\}$ be a basis of $\mathbb{F}_{p^m}$ over $\mathbb{F}_{p^k}$. Then the function F from $\mathbb{F}_{p^m} \times \mathbb{F}_{p^k} \times \mathbb{F}_{p^k}$ to $\mathbb{F}_{p^k}$,

$$F(x, y_1, y_2) = \mathrm{Tr}_k^m(x^2) + (y_1 + \mathrm{Tr}_k^m(\gamma_1 x^2))(y_2 + \mathrm{Tr}_k^m(\gamma_2 x^2))$$

is a vectorial bent function. If for some nonzero $\alpha \in \mathbb{F}_{p^k}$ *we have*

$$\left| \sum_{y_1, y_2 \in \mathbb{F}_{p^k}} \eta(\alpha + y_1\gamma_1 + y_2\gamma_2) \epsilon_p^{-\mathrm{Tr}_k(y_1 y_2/\alpha)} \right| \neq p^k, \tag{14}$$

then F_α^* *is not bent, and consequently* F *is a vectorial bent function, which has non-dual-bent component functions.*

The conditions in Theorem 17 are obtained by determining $\mathcal{W}_{f^*}(0)$ respectively $\mathcal{W}_{F_\alpha^*}(0)$. The Walsh transform of f^* respectively of F_α^* at 0 has *not* absolute value $p^{n/2}$, if and only if Condition (13) respectively Condition (14) is satisfied. Note that, therefore, the conditions are sufficient (not even necessary) for f being non-dual-bent respectively F having non-dual-bent components.

Remark 4 Conditions (13), (14) combine the additive and the multiplicative structure of the finite field and are therefore not easy to analyse. With a random choice of α and of γ_1 and γ_2, one would expect a chaotic behaviour of the character sums in (13) and (14). In particular, as experimental results indicate, its absolute value is mostly different from p respectively p^k, so that it is easy to find examples of non-dual-bent functions and vectorial bent functions with non-dual-bent component functions. For examples for $p = 3, 5, 7, 11, 13$ we refer to [34].

Remark 5 Though the classical constructions and explicit representations of p-ary bent functions describe (weakly) regular bent functions, the results on recursive and explicit constructions presented in this chapter indicate that being non-weakly regular and being non-dual-bent is not at all an exceptional property for a p-ary bent function.

4.3 Some questions

The generalized Maiorana-McFarland construction, the Rothaus construction and the semi-direct sum can produce non-weakly regular bent functions.

Question 5 Can one find more secondary constructions of bent functions, which support the generation of non-weakly regular or non-dual-bent functions?

The generalized Maiorana-McFarland vectorial bent function with non-weakly regular components described in Section 4.1 has solely non-weakly regular components, see [38, Theorem 4]. In view of Remark 4, it seems likely that all components of the vectorial bent function in Theorem 17 are not only non-weakly regular, but also non-dual-bent.

Question 6 Do vectorial bent functions of which some component functions are weakly regular and some are non-weakly regular exist?

Question 7 Do vectorial bent functions of which some component functions are dual-bent and some are non-dual bent functions exist?

The vectorial bent function with non-dual-bent components in Theorem 17, obtained with the semi-direct sum, maps from $\mathbb{V}_n^{(p)}$ to $\mathbb{V}_k^{(p)}$ with $k = n/5$. With $n = 1$, the vectorial bent function with non-weakly regular components in (12) is $F(x_1, x_2, y) = a_y x_1^2 \oplus y x_2$, hence maps from $\mathbb{F}_{p^k}^3$ to $\mathbb{F}_{p^k}$.

Question 8 What is the largest dimension k for which vectorial bent functions from $\mathbb{V}_n^{(p)}$ to $\mathbb{V}_k^{(p)}$ with non-weakly regular (non-dual-bent) component functions exist?

By the alternative definition of bent functions, Definition 2 (iii), a function is bent, if and only if its graph is a relative difference set.

Question 9 Can the property of being non-weakly regular respectively non-dual-bent be related to properties of the relative difference set?

5 Further properties of *p*-ary bent functions

Properties of Boolean and p-ary functions, which are frequently investigated in connection with bentness, are the algebraic degree and normality. In this chapter we summarize the main results on these properties for p-ary bent functions, in particular, we highlight the differences between the Boolean and the p-ary case, p odd. We add a short discussion on the minimal distance between bent functions (see [71, 102]), again pointing to some differences between the cases of $p = 2$ and p odd. We finish this chapter with some results on codes related to p-ary (vectorial) bent functions.

5.1 Algebraic degree

It is already shown in the paper of Rothaus [110], that a Boolean bent function $f : \mathbb{V}_n^{(2)} \to \mathbb{F}_2$ can have algebraic degree at most $n/2$. Examples of bent functions attaining this maximal algebraic degree are easy to construct, for instance in the Maiorana-McFarland class. It is also well known, that every Boolean PS^- bent function from $\mathbb{V}_{2m}^{(2)}$ to $\mathbb{F}_2$ attains the maximal possible algebraic degree m. Moreover, a Boolean PS^+ bent function from $\mathbb{V}_{2m}^{(2)}$ to $\mathbb{F}_2$ can have algebraic degree smaller than m, only if the corresponding partial spread with $2^{m-1} + 1$ subspaces cannot be extended to a larger partial spread. An example is the quadratic bent function, see [49, Theorem 6.3.12].

A similar result holds for weakly regular p-ary bent functions.

Theorem 18 [62, *Proposition* 4.5] *Let $f : \mathbb{V}_n^{(p)} \to \mathbb{F}_p$ be a weakly regular bent function, $(n, p) \neq (1, 3)$*[25]*. Then f has algebraic degree at most $(p-1)n/2$.*

[25] The exceptions when $(n, p) = (1, 3)$, are the (quadratic) bent functions cx^2 on $\mathbb{F}_3$ (affine term omitted).

As in the Boolean case, one easily can obtain examples for bent functions of algebraic degree $(p-1)n/2$ (for instance in the Maiorana-McFarland class). A slight difference we see for partial spread bent functions. For odd primes p, every partial spread bent function $f : \mathbb{V}_n^{(p)} \to \mathbb{F}_p$, without exception, attains the maximal possible algebraic degree $(p-1)n/2$, see [3].

The weak regularity plays an important role in Theorem 18. For non-weakly regular bent functions, a slightly larger bound applies.

Theorem 19 [62, *Proposition* 4.4] *For the algebraic degree* $\deg(f)$ *of a non-weakly regular bent function* $f : \mathbb{V}_n^{(p)} \to \mathbb{F}_p$ *we have*

$$\deg(f) \leq \frac{(p-1)n}{2} + 1.$$

The first (and as far as we are aware of, the only) construction of bent functions which attain the bound in Theorem 19, has been given in [29, 30], using the generalized Maiorana-McFarland construction:

With Lagrange interpolation, an explicit formula for (8) consists of sums of algebraic degree $(p-1) + \deg g_y$. If for some $\tilde{y} \in \mathbb{F}_p$, the bent function $g_{\tilde{y}} : \mathbb{V}_n^{(p)} \to \mathbb{F}_p$ has maximal degree $(p-1)n/2 + 1$, and the functions g_y are chosen such that the maximal degree term does not cancel, then the resulting bent function in dimension $n+2$ has maximal possible degree $(p-1)(n+2)/2 + 1$. For $p = 3$, the quadratic bent function $_{cx^2}$ on $\mathbb{F}_3$ has the maximal possible algebraic degree. Hence, recursively we can generate ternary bent functions in odd dimension $1 + 2k$ with maximal possible algebraic degree. For examples and an explicit formula for any odd dimension, see [30].

Question 10 Do (non-weakly regular) bent functions $f : \mathbb{V}_n^{(p)} \to \mathbb{F}_p$ with algebraic degree $(p-1)n/2 + 1$ exist for $p \geq 5$, or for even n?

The (non-weakly regular) ternary bent functions of maximal algebraic degree obtained with the generalized Maiorana-McFarland construction described as above, belong to the class of dual-bent functions.

Question 11 Do bent functions $f : \mathbb{V}_n^{(p)} \to \mathbb{F}_p$ with algebraic degree $(p-1)n/2 + 1$ exist in the class of non-dual-bent functions?

5.2 Normality

The definition of k-normality for p-ary functions below, is based on the accordant definitions for Boolean functions in [40, 52].

Definition 6 A function $f : \mathbb{V}_n^{(p)} \to \mathbb{F}_p$ is called k-normal, if there exists a k-dimensional affine subspace of $\mathbb{V}_n^{(p)}$ restricted to which f is constant. If f is affine on a k-dimensional affine subspace of $\mathbb{V}_n^{(p)}$, then f is called weakly k-normal. When n is even and $k = n/2$, then f is called (weakly) normal.

Remark 6 A function $f : \mathbb{V}_n^{(p)} \to \mathbb{F}_p$ is weakly normal, if and only if there exists an $a \in \mathbb{V}_n^{(p)}$ such that $f(x) \ominus \langle a, x \rangle_n$ is normal. Weak normality is hence in connection with bentness the essential property.

Normality for Boolean bent functions has been thoroughly investigated, see [16, 19, 40, 52, 74]. A Boolean bent function from $\mathbb{V}_n^{(2)}$ to $\mathbb{F}_2$ can be (weakly) k-normal for k at most $n/2$, [40]. Interestingly, most classical examples of Boolean bent functions attain this bound, the existence of non-(weakly) normal Boolean bent functions has been an open question for some time, see [52]. In fact, all Boolean bent functions in dimension 6 are normal, but in the meantime, examples of non-weakly normal bent functions have been found for dimensions $n = 10, 12$ ([74]), and $n = 14$ ([16]), employing an algorithm for testing normality in small dimension, [16]. A recursive procedure in [16] then guarantees that there are non-weakly normal Boolean bent functions in any (even) dimension $n \geq 10$.

The situation is somewhat different for bent functions from $\mathbb{V}_n^{(p)}$ to $\mathbb{F}_p$, p odd. As it is shown in [32], a p-ary bent function, which is weakly regular but not regular, cannot be weakly normal. Together with the observation that for a p-ary function f, which is weakly k-normal, we must have $p^k \leq \max_{b \in \mathbb{V}_n^{(p)}} |\mathcal{W}_f(b)|$ (see [88, Corollary 1] for odd p, and [40, Theorem 1] for $p = 2$), we have the following theorem.

Theorem 20 [32, 88] *Let $f : \mathbb{V}_n^{(p)} \to \mathbb{F}_p$ be a p-ary bent function, and suppose that f is weakly k-normal. If n is even, then k is at most $n/2$, moreover, if f is weakly regular but not regular then k can be at most $n/2 - 1$.*

If n is odd, then k can be at most $(n-1)/2$.

As in the Boolean case, many p-ary bent functions attain these bounds. Note that the large classes of completed Maiorana-McFarland functions and of the PS^+ bent functions are normal by definition.

- A quadratic bent function $Q : \mathbb{V}_n^{(p)} \to \mathbb{F}_p$, p odd, is normal if n is even and Q is regular, $(n/2-1)$-normal if n is even and Q is weakly regular but not regular, and $(n-1)/2$ -normal if n is odd, see [32, 88].
- The regular Coulter-Matthews bent functions are normal, [32, Theorem 7].
- The generalized Maiorana-McFarland construction yields weakly regular and non-weakly regular bent functions which are weakly normal if n is even, and (weakly) $(n-1)/2$-normal if n is odd (if not non-weakly normal bent functions are used for the construction).
- The non-dual-bent function $g_2 : \mathbb{F}_{3^4} \to \mathbb{F}_3$, $g_2(x) = \mathrm{Tr}_1^4(\omega^{10}x^{22} + x^d)$, ω primitive element of $\mathbb{F}_{3^4}$, is normal, [32, Example 1].

Employing a generalization for odd characteristic of the algorithm in [16], in [88] the existence of p-ary bent functions which do not attain the bound on k-normality is confirmed. More precisely, for some weakly regular p-ary bent functions in odd dimension it is shown that they are not $(n-1)/2$-normal, and some non-weakly regular bent functions in even dimension are shown to be not normal (e.g. g_1, g_5 in our list in Chapter 4).

Question 12 Find regular p-ary bent functions in even dimension, which are not weakly normal.[26] Find weakly regular but not regular bent functions in even dimension, that are not $(n/2-1)$-weakly normal.

[26] Recall that for Boolean bent functions, which are always regular, the existence of not weakly normal functions is confirmed for all (even) dimensions $n \geq 10$.

Question 13 Analyse normality for more of the known classes of p-ary bent functions. For instance, confirm that - as experimental results indicate - the weakly regular but not regular Coulter-Matthews bent functions in even dimension n are $(n/2-1)$-normal.

The question on the typical behaviour of p-ary (and Boolean) bent functions with respect to normality seems not easy to be answered. Are (most) bent functions affine on affine subspaces of large dimension, or do they behave like arbitrary p-ary (and Boolean) functions[27], bent functions that are (weakly) k-normal for a large value of k are only easier to find?

5.3 Minimal distance

In [18], Carlet introduced the following secondary construction of Boolean bent functions: Let $f : \mathbb{V}_n^{(2)} \to \mathbb{F}_2$ be a weakly normal bent function, i.e., there exists an $n/2$-dimensional affine subspace E of $\mathbb{V}_n^{(2)}$ restricted to which f is an affine function. Let $\mathcal{I}_E$ denote the characteristic function of E, i.e., $\mathcal{I}_E(x) = 1$ if $x \in E$, otherwise $\mathcal{I}_E(x) = 0$. Then the function $g(x) = f(x) \oplus \mathcal{I}_E(x)$ is bent. This construction was further analysed in [71] for Boolean functions, and then in [102, 103] for p-ary functions, resulting in an analysis of the minimal distance between bent functions. The main results for the Boolean and the p-ary case (in even dimension n) are essentially the same:

Theorem 21 [71, 102, 103] *Let p be a prime and let n be even.*

- The Hamming distance $d(f,g) = |\{x \in \mathbb{V}_n^{(p)} : f(x) \neq g(x)\}|$ between two bent functions $f, g : \mathbb{V}_n^{(p)} \to \mathbb{F}_p$, is at least $p^{n/2}$.
- If two bent functions $f, g : \mathbb{V}_n^{(p)} \to \mathbb{F}_p$ have Hamming distance $d(f,g) = p^{n/2}$, then there exists an affine subspace E of dimension $n/2$, on which f is affine, and $g(x) = f(x) \oplus c\mathcal{I}_E$ for some $c \in \mathbb{F}_p^*$. Conversely, if a bent function $f : \mathbb{V}_n^{(p)} \to \mathbb{F}_p$ is weakly normal, i.e., affine on an $n/2$-dimensional affine subspace E, then $g(x) = f(x) \oplus c\mathcal{I}_E$ is bent.
- If a bent function $f : \mathbb{V}_n^{(p)} \to \mathbb{F}_p$ is weakly normal, hence affine on an $n/2$-dimensional affine subspace E, then there are $p-1$ bent functions which differ from f only on this subspace.

In [71], properties of the graph of the minimal distance between bent functions[28] are investigated, like connectedness and vertices of maximal degree. Apparently, the isolated vertices are the bent functions which are not weakly normal, among which are, in the case of p odd, all bent functions which are weakly regular but not regular.

Question 14 Are there comparable results on the minimal distance between bent functions for weakly regular but not regular bent functions, or for p-ary bent functions in odd dimension n?

[27] In average, Boolean and p-ary functions are deeply non-normal. For details we refer to Theorem 3 and Proposition 1 in [19] for the Boolean case, and to [88, Proposition 1] for the case of odd primes p.

[28] The vertices of this graph are the bent functions from $\mathbb{V}_n^{(p)}$ to $\mathbb{F}_p$, and two bent functions f, g are adjacent if they have Hamming distance $p^{n/2}$.

5.4 Coding theoretical results

For a (vectorial) function $F : \mathbb{V}_n^{(p)} \to \mathbb{V}_m^{(p)}$, let $\mathcal{C}_F$ be the linear code containing the first order Reed-Muller code and the code formed by the component functions of F as a subcode. If F is given in univariate form as a function from $\mathbb{F}_{p^n}$ to $\mathbb{F}_{p^m}$ (for simplicity we then suppose that m divides n), then

$$\begin{aligned} \mathcal{C}_F &= \{c_{\alpha,\beta,c} \ : \ \alpha \in \mathbb{F}_{p^m}, \beta \in \mathbb{F}_{p^n}, c \in \mathbb{F}_p\} \quad \text{with} \\ c_{\alpha,\beta,c} &= \{(\mathrm{Tr}_1^m(\alpha F(x)) \oplus \mathrm{Tr}_1^n(\beta x) \oplus c) \ : \ x \in \mathbb{F}_{p^n}\}. \end{aligned}$$

In the multivariate representation, i.e., if F is given as a function from $\mathbb{F}_p^n$ to $\mathbb{F}_p^m$, the code $\mathcal{C}_F$ is the linear code generated by the rows of the matrix

$$\begin{bmatrix} 1 \\ x \\ F(x) \end{bmatrix}_{x \in \mathbb{F}_p^n}.$$

Clearly, the code $\mathcal{C}_F$ has codewords of length p^n, the dimension of $\mathcal{C}_F$ is at most $k = n + m + 1$. We remark that in some papers, variants of the code $\mathcal{C}_F$ are considered. For instance, in [54, 93], for a function on $\mathbb{F}_{p^n}$, the code

$$\begin{aligned} \tilde{\mathcal{C}}_F = \{\tilde{c}_{\alpha,\beta} = (&\mathrm{Tr}_1^n(\alpha F(1) \oplus \beta), \mathrm{Tr}_1^n(\alpha F(\gamma) \oplus \beta\gamma), \dots \\ &\dots \mathrm{Tr}_1^n(\alpha F(\gamma^{p^n-2}) \oplus \beta\gamma^{p^n-2})) \ : \ \alpha, \beta \in \mathbb{F}_{p^n}\} \end{aligned} \tag{15}$$

for a primitive element γ of $\mathbb{F}_{p^n}$, is considered.[29]

Besides from the parameters of a linear code, length, dimension and minimum distance, which determine the error correcting capabilities of the code, the weight distribution is of interest for calculating the error probabilities of the error detecting and error correcting. Linear codes with few weights have applications in several areas, like sharing schemes, authentication codes (we refer to [75] and references therein).

There are several results on parameters and on the weight distribution of the code $\mathcal{C}_F$ (and variants) for special (classes of) functions F. We summarize below results on codes corresponding to some major classes of functions F in odd characteristic (in which we are interested in this survey), and refer to [54, 93, 119], and some references therein for further reading.

Parameters and weight distribution for codes obtained with (vectorial) bent functions from $\mathbb{V}_n^{(p)}$ to $\mathbb{V}_m^{(p)}$, p odd, with (weakly) regular components can be derived using the value distribution for (weakly) regular bent functions in Theorem 1. For the results on codes obtained from p-ary bent functions we may refer to [93][30].

As it is common, we call a linear code with codewords of length μ, dimension k, and minimal distance d, a (μ, k, d)-linear code. The weight enumerator polynomial for a code $\mathcal{C}$ is the polynomial $W_{\mathcal{C}}(z) = \sum_{i=0}^{\mu} A_j z^j$, where the coefficient A_j is the number of codewords of weight j.

[29] Note that $\tilde{\mathcal{C}}_F$ is a punctured version of the subcode of $\mathcal{C}_F$ with the codewords $c_{\alpha,\beta,0}$.

[30] In [93], the code $\tilde{\mathcal{C}}_F$ is investigated.

Theorem 22 *Let n be even, let p be an odd prime, and let $F : \mathbb{V}_n^{(p)} \to \mathbb{V}_m^{(p)}$ be a (vectorial) bent function.*

(i) *If all component functions of F are regular, then $\mathcal{C}_F$ is a $(p^n, n+m+1, p^n - p^{n-1} - p^{n/2-1})$-linear code with weight enumerator polynomial*

$$W_{\mathcal{C}_F}(z) = 1 + (p^m - 1)p^n z^{(p-1)(p^{n/2}-1)p^{n/2-1}} + p(p^n - 1)z^{(p-1)p^{n-1}} + (p-1)(p^m - 1)p^n z^{p^n - p^{n-1} + p^{n/2-1}} + (p-1)z^{p^n}.$$

(ii) *If all component functions of F are weakly regular but not regular, then $\mathcal{C}_F$ is a $(p^n, n+m+1, p^n - p^{n-1} - p^{n/2-1})$-linear code with weight enumerator polynomial*

$$W_{\mathcal{C}_F}(z) = 1 + (p-1)(p^m - 1)p^n z^{p^n - p^{n-1} - p^{n/2-1}} + p(p^n - 1)z^{(p-1)p^{n-1}} + (p^m - 1)p^n z^{(p-1)(p^{n/2}+1)p^{n/2-1}} + (p-1)z^{p^n}.$$

Theorem 23 *Let n be odd, let p be an odd prime, and let $F : \mathbb{V}_n^{(p)} \to \mathbb{V}_m^{(p)}$ be a (vectorial) bent function. If all component functions of F are weakly regular, then $\mathcal{C}_F$ is a $(p^n, n+m+1, (p-1)p^{n-1} - p^{(n-1)/2})$-linear code with weight enumerator polynomial*

$$\begin{aligned} W_{\mathcal{C}_F}(z) = 1 &+ (p^m - 1)\frac{p-1}{2}p^n z^{(p-1)p^{n-1} - p^{(n-1)/2}} + \\ &((p^n - 1)p + (p^m - 1)p^n)z^{(p-1)p^{n-1}} + \\ &(p^m - 1)\frac{p-1}{2}p^n z^{(p-1)p^{n-1} + p^{(n-1)/2}} + (p-1)z^{p^n}. \end{aligned}$$

In [54], the weight distribution of $\tilde{\mathcal{C}}_F$ for all known planar functions F is determined. We recall that, with the exception of the Coulter-Matthews function, all known planar functions are quadratic, and can - linear and constant term omitted - uniquely be represented by a Dembowski-Ostrom polynomial (6). The component functions of quadratic functions are necessarily weakly regular, the weak regularity of the components of the Coulter-Matthews planar function is shown in [58, 112]. The weight distribution of the corresponding codes hence depends on the quantities of regular and weakly regular but not regular components.

Theorem 24 [54, *Theorem* 2] *Let $F : \mathbb{V}_n^{(p)} \to \mathbb{V}_n^{(p)}$ be any Dembowski-Ostrom planar function, or the Coulter-Matthews planar function ($p = 3$), and let $W_{\tilde{\mathcal{C}}_F}(z)$ be the weight enumerator polynomial for the code $\tilde{\mathcal{C}}_F$ given as in (15).*

(i) *If n is odd, then*

$$\begin{aligned} W_{\tilde{\mathcal{C}}_F}(z) = 1 &+ (p^n - 1)(p^{n-1} + 1)z^{(p-1)p^{n-1}} \\ &+ \frac{p^n - 1}{2}(p^{n-1} + p^{(n-1)/2})(p-1)z^{(p-1)p^{n-1} - p^{(n-1)/2}} \\ &+ \frac{p^n - 1}{2}(p^{n-1} - p^{(n-1)/2})(p-1)z^{(p-1)p^{n-1} + p^{(n-1)/2}}. \end{aligned}$$

(ii) *If n is even, then*

$$
\begin{aligned}
W_{\tilde{C}_F}(z) = 1 &+ (p^n - 1)z^{(p-1)p^{n-1}} \\
&+ \frac{p^n - 1}{2}(p^{n-1} + (p-1)p^{n/2-1})z^{(p-1)(p^{n-1}-p^{n/2-1})} \\
&+ \frac{p^n - 1}{2}(p^{n-1} - (p-1)p^{n/2-1})z^{(p-1)(p^{n-1}+p^{n/2-1})} \\
&+ \frac{p^n - 1}{2}(p^{n-1} + p^{n/2-1})(p-1)z^{(p-1)p^{n-1}-p^{n/2-1}} \\
&+ \frac{p^n - 1}{2}(p^{n-1} - p^{n/2-1})(p-1)z^{(p-1)p^{n-1}+p^{n/2-1}}.
\end{aligned}
$$

Question 15 Prove or disprove that the weight distribution of $W_{\tilde{C}_F}(z)$ must be as in Theorem 24 for every planar function F ($F(0) = 0$).

Note that showing that the Coulter-Matthews planar functions are the only non-quadratic planar functions (Question 4) would also solve Question 15.

A different approach is applied in Ding [50], where cyclic codes with generator polynomial $(x^{p^n-1} - 1)/\gcd(S(x), x^{p^n-1} - 1)$ are investigated, where $S(x) = \sum_{i=0}^{p^n-2} s_i x^i$ with $s_i = \mathrm{Tr}_1^n(F(\gamma^i + 1))$ for a primitive element γ of $\mathbb{F}_{p^n}$ and a function F on $\mathbb{F}_{p^n}$. It is pointed out that some codes from planar functions (and APN functions) F are optimal.

6 Bent functions and difference sets

A main motivation for research on bent functions are their strong connections to difference sets, generalizations of difference sets, and related objects. Recall that, by Definition 2 (iii), a bent function can be seen as a relative difference set.

Another generalization of difference sets are *partial difference sets*.

Definition 7 Let G be a finite group of order v. A k-subset D of G is called a (v, k, λ, μ) partial difference set (PDS) of G, if every nonzero element of D can be written as a difference of two elements of D in exactly λ ways, and every nonzero element of $G \setminus D$ can be written as such a difference in exactly μ ways. If additionally $-D = D$ and $0 \notin D$, then D is called a regular partial difference set.

Note that a partial difference set with $\mu = \lambda$, is a (conventional) difference set. For background on partial difference sets we refer to [77, 78].

Regular partial difference sets yield *strongly regular graphs*.

Definition 8 A k-regular graph $\mathcal{G}$ with v vertices is called strongly regular with parameters (v, k, λ, μ), if any two adjacent vertices have exactly λ common neighbours, and any two non-adjacent vertices have exactly μ common neighbours.

Recall that for a subset D of a finite group G with $-D = D$, the *Cayley graph* of D is the graph of which the vertices are the elements of G, and $x, y \in G$ are adjacent, if and only if $x - y \in D$.

Theorem 25 [78, *Proposition* 1.1] *Let D be a k-subset of a finite group G of order ν. The Cayley graph of D is a strongly regular graph with parameters (ν, k, λ, μ), if and only if D is a regular (ν, k, λ, μ) partial difference set of G.*

Remark 7 Observe that the property $-D = D$ is important to obtain an undirected graph $\mathcal{G}$ as Cayley graph. The condition $0 \notin D$ avoids that $\mathcal{G}$ has loops. However, as is easily seen, if D is a partial difference set, then so are $D \cup \{0\}$ and $D \setminus \{0\}$.

There are rich connections between bent functions and some classes of difference sets. We recall again that a function between two finite abelian groups A and B is a bent function, if and only if its graph is a (splitting) relative difference set in $A \times B$ relative to B. Therefore, the study of bent functions is also a study of relative difference sets.

Remarkable is the following well-known relation between Boolean bent functions and difference sets in the elementary abelian 2-group.

Theorem 26 [49, *Theorem* 6.2.10] *A Boolean function $f : \mathbb{V}_n^{(2)} \to \mathbb{F}_2$ is bent, if and only if the support of f, $supp(f) = \{x \in \mathbb{V}_n^{(2)} : f(x) = 1\}$[31], is a $(2^n, 2^{n-1} \pm 2^{n/2-1}, 2^{n-2} \pm 2^{n/2-1})$ -difference set in $\mathbb{V}_n^{(2)}$.*

Difference sets with these parameters are called *Hadamard difference sets*. It is shown in [80], that every nontrivial difference set[32] in an elementary abelian 2-group $\mathbb{V}_n^{(2)}$ is a Hadamard difference set (n must be even). Therefore, Boolean bent functions and difference sets in the elementary abelian 2-group are the same objects.

Seeing a (Hadamard) difference set of $\mathbb{V}_n^{(2)}$ as a partial difference set with $\lambda = \mu$, with the connection to strongly regular graphs in Theorem 25, Theorem 26 can also be stated in terms of strongly regular graphs. The following corollary is Lemma 12 in [4] and Theorem 3 in [5].

Corollary 1 *A Boolean function $f : \mathbb{V}_n^{(2)} \to \mathbb{F}_2$ is bent, if and only if the Cayley graph of the support of f is a strongly regular graph with the property that $\lambda = \mu$.*

We remark that $-D = D$ trivially holds in characteristic 2, the Cayley graphs considered in [4, 5] may have loops.

Theorem 26 and Corollary 1 do not at all apply in a similar way to p-ary bent functions, $p > 2$. But there are several interesting attempts in the literature to obtain generalizations, p-ary versions - though much weaker type of results - which shall be summarized in this chapter.

6.1 Partial difference sets from p-ary bent functions

Connections between bent functions and partial difference sets were extended to ternary bent functions in 2011 in [112], and then to p-ary bent functions for arbitrary odd

[31] The complementary set, i.e., the set $\{x \in \mathbb{V}_n^{(2)} : f(x) = 0\}$, is then a $(2^n, 2^{n-1} \mp 2^{n/2-1}, 2^{n-2} \mp 2^{n/2-1})$-difference set.

[32] Every finite group G contains the trivial difference sets, G, $\emptyset$, $\{z\}$, $G \setminus \{z\}$, where z is any element of G.

primes p in [42] and [55]. Differently from the Boolean case, special properties have to be imposed to p-ary bent functions in order to yield partial difference sets.

For a p-ary function $f : \mathbb{V}_n^{(p)} \to \mathbb{F}_p$ with $f(0) = 0$ (otherwise we may add a constant), we define

$$\begin{aligned} D_0^f &= \{x \in \mathbb{V}_n^{(p)} \setminus \{0\} \ : \ f(x) = 0\}, \\ D_S^f &= \{x \in \mathbb{V}_n^{(p)} \ : \ f(x) \text{ is a nonzero square in } \mathbb{F}_p\}, \\ D_N^f &= \{x \in \mathbb{V}_n^{(p)} \ : \ f(x) \text{ is a nonsquare in } \mathbb{F}_p\}. \end{aligned} \tag{16}$$

The following theorem is [112, Theorem 1] for the ternary case and [42, Theorem 1,2] respectively [55, Theorem 3.5] for arbitrary odd primes p.

Theorem 27 [42, 55, 112] *Let $n = 2m$ be even, and $f : \mathbb{V}_n^{(p)} \to \mathbb{F}_p$ be a weakly regular p-ary bent function, and suppose that there exists an integer l with $\gcd(p-1, l-1) = 1$, such that*

$$f(\alpha x) = \alpha^l f(x) \tag{17}$$

for all $\alpha \in \mathbb{F}_p$ (which also implies that $f(0) = 0$ and $f(-x) = f(x)$). Then D_0^f, D_S^f and D_N^f are (ν, k, λ, μ) partial difference sets with

$$\begin{aligned} &\nu = p^{2m}, \quad k = (p^m - \epsilon)(p^{m-1} + \epsilon), \\ &\lambda = (p^{m-1} + \epsilon)^2 - 3\epsilon(p^{m-1} + \epsilon) + \epsilon p^m, \quad \mu = (p^{m-1} + \epsilon)p^{m-1}, \end{aligned}$$

for D_0^f, and

$$\begin{aligned} &\nu = p^{2m}, \quad k = \frac{1}{2}(p^m - p^{m-1})(p^m - \epsilon), \\ &\lambda = \frac{1}{4}(p^m - p^{m-1})^2 - \frac{3\epsilon}{2}(p^m - p^{m-1}) + p^m\epsilon, \\ &\mu = \frac{1}{2}(p^m - p^{m-1})\Big(\frac{1}{2}(p^m - p^{m-1}) - \epsilon\Big), \end{aligned}$$

for D_S^f and D_N^f, where $\epsilon = 1$ if f is regular and $\epsilon = -1$ if f is weakly regular but not regular.

Remark 8 For ternary functions f, the sets D_S^f and D_N^f are the preimage sets of 1 and 2, respectively. Hence f is completely determined by D_0^f, D_S^f and D_N^f. This does not at all apply if $p > 3$. There are many other functions, mostly not bent, with the same D_0^f, D_S^f, D_N^f. The conditions in the proposition above are therefore certainly only sufficient.

Remark 9 Though the conditions in Theorem 27 on p-ary bent functions are quite strong, they are satisfied by many of the classical examples (like quadratic bent functions, the Coulter-Matthews bent function, some Maiorana-McFarland functions), see [112].

Remark 10 Strongly regular graphs (or partial difference sets) with parameters $(n^2, r(n-\epsilon), \epsilon n + r^2 - 3\epsilon r, r^2 - \epsilon r)$ are called of Latin square type if $\epsilon = 1$, and of negative Latin square type if $\epsilon = -1$, see [78]. The partial difference sets in Theorem 27 are hence of (negative) Latin square type.

In [65], the results in Theorem 27 have been generalized to some larger classes of sets. In accordance with [65], we call a function satisfying the property (17) an *l-form*.

For an integer l, let $H_l = \{x^l \ : \ x \in \mathbb{F}_p^*\}$ be the multiplicative subgroup of $\mathbb{F}_p^*$ containing all l-th powers of $\mathbb{F}_p^*$, let

$$D^f_{\beta H_l} = \{x \in \mathbb{V}_n^{(p)} \ : \ f(x) \in \beta H_l\},$$

and for some $\beta \in \mathbb{F}_p^*$, let

$$D^f_{\beta H_l} = \{x \in \mathbb{V}_n^{(p)} \ : \ f(x) \in \beta H_l\},$$

where βH_l is the coset of H_l containing β. We state the main results of [65] in terms of partial difference sets. In [65], all results are equivalently given in terms of strongly regular graphs.

Theorem 28 [65] *For an odd prime p, an even integer n, and some $l \in \{1, 2, \ldots, p-1\}$, with $\gcd(l-1, p-1) = 1$ and $l \neq p-1$ if $p > 3$, let $f : \mathbb{V}_n^{(p)} \to \mathbb{F}_p$ be a p-ary bent function and an l-form (hence $f(0) = 0$, $f(-x) = f(x)$).*

$l = 2$. In this case the following is equivalent.

(a) *f is weakly regular.*
(b) *One of D^f_0, $D^f_S = D^f_{H_l}$, $D^f_N = D^f_{\beta H_l}$ for some nonsquare $\beta \in \mathbb{F}_p^*$, is a PDS.*
(c) *All of the sets D^f_0, D^f_S, D^f_N are PDSs.*

$l \neq 2$. In this case the following is equivalent.

(a) *f is regular.*
(b) *One of D^f_0, $D^f_{\beta H_l}$ for some $\beta \in \mathbb{F}_p^*$, is a PDS.*
(c) *All of the sets D^f_0, $D^f_{\beta H_l}$, $\beta \in \mathbb{F}_p^*$ are PDSs.*

Furthermore, any union of sets from $\{D^f_0; D^f_{\beta H_l}, \beta \in \mathbb{F}_p^*\}$ is a PDS.

Remark 11 The parameters for D^f_0 (and for D^f_S, D^f_N) are given in Theorem 27. The parameters for $D_{\beta H_l}$ are $(\nu, k, \lambda, \mu) =$

$$(p^n, h_l(p^{n-1} - \epsilon p^{n/2-1}), h_l^2 p^{n-2} + \epsilon p^{n/2} - 3\epsilon h_l p^{n/2-1}, h_l^2 p^{n-2} - \epsilon h_l p^{n/2-1}),$$

where $h_l = |H_l| = (p-1)/\gcd(l, p-1)$ and $\epsilon = 1$ if f is regular, and $\epsilon = -1$ if f is weakly regular but not regular (only relevant for $l = 2$), see [65, Proposition IV.4]. Again these partial difference sets are of (negative) Latin square type.

Association schemes Another combinatorial object, which one can obtain from some partial difference sets respectively strongly regular graphs from p-ary bent functions, are *association schemes*. Recall that for a set of vertices V and binary relations $R_0 = \mathrm{id}, R_1, \ldots, R_r$, the configuration $(V; R_0, R_1, \ldots, R_r)$ is called an *association scheme of class r* on V, if the following holds:

- $V \times V = R_0 \cup R_1 \cup \cdots \cup R_r$ and $R_i \cap R_j = \emptyset$ for $i \neq j$;
- For each i, there exists a j such that $R_i^\star = R_j$, where $R^\star = \{(x, y) \in V \times V \ : \ (y, x) \in R\}$ (if $R_i^\star = R_i$ for all i, then we call the association scheme symmetric);

– For i, j and $(x, y) \in V \times V$ let

$$\rho_{i,j}(x, y) = |\{z \in V \ : \ (x, z) \in R_i, (z, y) \in R_j\}|.$$

Then for each k and $(x, y) \in R_k$, the integer $\rho_{i,j}(x, y)$ is constant $\rho_{i,j}^k$ (independent from $(x, y) \in R_k$).

The constants $\rho_{i,j}^k$ are called the *intersection numbers* of the association scheme. Given an association scheme, we can take unions of the relations $R_i, i \neq 0$, and form schemes with larger sets, called *fusion*. If any fusion again results in an association scheme, then the association scheme is called *amorphic*.

Let $\{\mathcal{G}_1, \mathcal{G}_2, \ldots, \mathcal{G}_r\}$ be an edge-decomposition of the complete graph on a vertex set V of size v. If all $\mathcal{G}_i, 1 \leq i \leq r$, are strongly regular, all of Latin square type or all of negative Latin square type, then this decomposition is an r-class (symmetric) amorphic association scheme on V, see [46, Theorem 3], (the binary relations are naturally defined via adjacency on the graphs).

As a consequence of these relations, we obtain association schemes from some classes of weakly regular bent functions, see [112, Theorem 3], [42, Theorem 4] and [55, Corollary 3.7]:

Theorem 29 [42, 55, 112] *Let $n = 2m$ be even, and let $f : \mathbb{V}_n^{(p)} \to \mathbb{F}_p$ be a weakly regular p-ary bent function, and suppose that there exists an integer l with $\gcd(p-1, l-1) = 1$, such that $f(\alpha x) = \alpha^l f(x)$ for all $\alpha \in \mathbb{F}_p$. Then the Cayley graphs of D_0^f, D_S^f and D_N^f induce an amorphic association scheme of class 3 on $\mathbb{V}_n^{(p)}$.*

For further results on association schemes from p-ary bent functions we refer to Theorem B in [65] (*obtained from Theorem* 28), *or to* [107].

Vectorial bent functions and PDSs In [36, 39], some attempts were made to extend the connections between bent functions and partial difference sets to vectorial functions. It appears that the concept of duality for vectorial bent functions, which was introduced in [35], plays an important role. Let $F : \mathbb{V}_n^{(p)} \to \mathbb{V}_m^{(p)}$ be a vectorial bent function, i.e., the set of the component functions $\{F_a(x) = \langle a, F(x)\rangle_m \ : \ a \in \mathbb{V}_m^{(p)} \setminus \{0\}\}$ forms - together with the 0-function - an m-dimensional vector space of bent functions. We suppose that all components are weakly regular. Then the set of the duals $\{F_a^* \ : \ a \in \mathbb{V}_m^{(p)} \setminus \{0\}\}$ is a set of bent functions, but in general not a vector space. In general this set is not closed under addition, in general, for two (dual-) bent functions f_1,f_2 for which $f_1 \oplus f_2$ is also bent, the function $f_1^* \oplus f_2^*$ is not even a bent function. On the other hand, there are some classes of vectorial bent functions, for which the dual functions of the components again form a vector space of bent functions.

Definition 9 [35] A vectorial bent function $F : \mathbb{V}_n^{(p)} \to \mathbb{V}_m^{(p)}$ is called a vectorial dual-bent function, if the set of the dual functions of the component functions of F (together with the zero function) forms a vector space of bent functions of the same dimension m. The dual functions of the component functions of F are then the component functions of some vectorial bent function F^* from $\mathbb{V}_n^{(p)}$ to $\mathbb{V}_m^{(p)}$, called a vectorial dual of F.

For some examples of vectorial dual-bent functions we refer to [35].

Theorem 30 [36, 39] *For a prime p and an even integer n, let $F : \mathbb{V}_n^{(p)} \to \mathbb{V}_m^{(p)}$ be a vectorial dual-bent function with $F(0) = 0$ and $F(-x) = F(x)$. If p is odd, suppose that all component functions are regular ($\epsilon = 1$) or weakly regular but not regular ($\epsilon = -1$). The set*

$$D_0^F = \{x \in \mathbb{V}_n^{(p)} \setminus \{0\} \ : \ F(x) = 0\}$$

is a (ν, k, λ, μ) partial difference set in $\mathbb{V}_n^{(p)}$ of (negative) Latin square type, with $k = p^{n-m} + \epsilon(p^{n/2} - p^{n/2-m}) - 1$, $\mu = p^{n-2m} + \epsilon p^{n/2-m}$, $\lambda = p^{n-2m} + \epsilon(p^{n/2} - p^{n/2-m}) - 2$.

Remark 12 A Boolean bent function f, seen as a 1-dimensional vector space of bent functions is trivially vectorial dual-bent, and trivially $f(-x) = f(x)$. The PDS D_0^f (as well as the the complementary set $\{x \in \mathbb{V}_n^{(2)} \ : \ f(x) = 1\}$) reduces then to a Hadamard difference set, and we can see Theorem 26 as a special case[33]. Conversely the partial difference sets D_0^f, D_0^F (and their complementary sets) in Theorems 27, 28, 30 can be seen as some generalization for odd p of the Hadamard difference sets in Theorem 26.

A weakly regular bent function f (of which the dual f^* is always also bent), seen as a vectorial function from $\mathbb{V}_n^{(p)}$ to $\mathbb{F}_p$, has the constant multiples cf, $1 \le c \le p-1$, as component functions. In general, the p-ary bent functions $f^*, (2f)^*, \ldots, ((p-1)f)^*$ are not the component functions (i.e., the multiples) of one of them, say f^*. In general, the sum of two of them is not even a bent function, see Example 3 in [35]. Hence for $p \neq 2$, a p-ary dual-bent function is in general not vectorial dual-bent.

Proposition 2 *Let $f : \mathbb{V}_n^{(p)} \to \mathbb{F}_p$ be a weakly regular bent function which is an l-form, i.e., there exists an integer l with $\gcd(l-1, p-1) = 1$, such that $f(\alpha x) = \alpha^l f(x)$ for all $\alpha \in \mathbb{F}_p$. Then f is a vectorial dual-bent function.*

Proposition 2, by which Theorem 27 for the case D_0^f follows from Theorem 30, indicates that there is a connection between vectorial dual-bentness and l-forms, which we can generalize to vectorial functions as follows. For some divisor s of n, let $\mathbb{V}_n^{(p)}$ be a vector space over the finite field $\mathbb{F}_{p^s}$. For instance, $\mathbb{V}_n^{(p)} = \mathbb{F}_{p^n}$, or $\mathbb{V}_n^{(p)} = \mathbb{F}_{p^m} \times \mathbb{F}_{p^m}$, where s divides m. We call a function F from $\mathbb{V}_n^{(p)}$ to $\mathbb{F}_{p^s}$ a (vectorial) l-form, if $F(\alpha x) = \alpha^l F(x)$ for all $\alpha \in \mathbb{F}_{p^s}$. As pointed out in [39], all known classes of vectorial dual-bent functions F from $\mathbb{V}_n^{(p)}$ to $\mathbb{F}_{p^s}$ are EA-equivalent to such a vectorial version of an l-form.

It is shown in [39, Section 4], that vectorial dual-bentness and the property of inducing partial difference sets are both invariant under linear equivalence. This holds for l-forms solely for p-ary functions, but not necessarily for vectorial l-forms, which indicates that rather than the l-form property, the duality properties of a vectorial bent function decide on the differential properties of D_0^F (and perhaps of D_S^F, D_N^F, defined for $F : \mathbb{V}_n^{(p)} \to \mathbb{F}_{p^s}$ as in (16) with the squares and non-squares of the finite field $\mathbb{F}_{p^s}$).

Some questions on partial difference sets from p-ary bent functions also concern connections between l-forms and vectorial dual-bentness, see also the problems in [39].

[33] Of course, differently from Theorem 26, the Theorems 27, 28, 30 give only sufficient conditions for PDSs.

Question 16 Converse of Proposition 2: Does vectorial dual-bentness of a weakly regular bent function $f : \mathbb{V}_n^{(p)} \to \mathbb{F}_p$ (seen as 1-dimensional vectorial function) imply that f is an l-form for some l?

Question 17 Vectorial version of Proposition 2: Is every vectorial bent function $F : \mathbb{V}_n^{(p)} \to \mathbb{F}_{p^s}$, which is an l-form, always vectorial dual-bent?

Question 18 Let $F : \mathbb{V}_n^{(p)} \to \mathbb{F}_{p^s}$ be a vectorial dual-bent function. Are then D_S^F, D_N^F partial difference sets (a positive answer has been given for one special Maiorana-McFarland bent function in [39]).

Question 19 Is there a generalization of the results on $D_{H_l}^f$, $D_{\beta H_l}^f$ in Theorem 28 for vectorial bent l-forms?

6.2 Bent functions and edge-weighted graphs

Alternative attempts to generalize the connection between Boolean bent functions and (Hadamard) difference sets to p-ary bent functions are made by Joyner and Melles (and co-authors) in the series of papers [27, 67, 90]. Differently from the approach in Section 6.1, where properties are imposed on the bent functions in order to yield partial difference sets, Joyner et al. adapt the definitions of partial difference sets and strongly regular graphs.

Let f be a function from $\mathbb{V}_n^{(p)}$ to $\mathbb{F}_p$ with $f(x) = f(-x)$. The Cayley graph of f is defined to be the regular edge-weighted graph whose vertex set is $\mathbb{V}_n^{(p)}$ and $u, v \in \mathbb{V}_n^{(p)}$ are adjacent with edge weight c if $f(u - v) = c \neq 0$.[34] The definition of edge-weighted strongly regular graphs is more sophisticated. First, for an edge-weighted graph, we denote with $N(u)$ the set of all neighbours of a vertex u, and with $N(u, a)$ the set of all neighbours v of u, for which the edge (u, v) has weight a. With this notation, $|N(u_1, a_1) \cap N(u_2, a_2)|$ is the number of common neighbours v of the vertices u_1, u_2 for which the edge (u_1, v) has weight a_1 and the edge (u_2, v) has weight a_2.

Definition 10 (see Definition 23 in [67]) Let $\mathcal{G}$ be a connected edge-weighted graph, which is regular as an unweighted graph. We let the weight set be $W = \{1, 2, \ldots, p-1\}$. Then $\mathcal{G}$ is called edge-weighted strongly regular with parameters (ν, k, λ, μ), $k = (k_1, k_2, \ldots, k_{p-1})$, $\lambda = (\lambda_{a_1,a_2,a_3})_{a_i \in W}$, $\mu = (\mu_{a_1,a_2})_{a_i \in W}$, if it consists of ν vertices, every vertex u has k_a neighbours v for which the edge (u, v) has weight $a \in W$, and for vertices $u_1 \neq u_2$ and $a_1, a_2 \in W$ we have

$$|N(u_1, a_1) \cap N(u_2, a_2)| = \begin{cases} \lambda_{a_1,a_2,a_3} & : \quad u_1 \in N(u_2, a_3), \\ \mu_{a_1,a_2} & : \quad u_1 \notin N(u_2). \end{cases}$$

Remark 13 [67, Lemma 24] If in Definition 10, the sum $\sum_{a_1,a_2 \in W} \lambda_{a_1,a_2,a_3}$ is a fixed λ, independent from a_3, then the graph $\mathcal{G}$ is strongly regular as unweighted graph with parameters (ν, k, λ, μ) with $k = \sum_{a \in W} k_a$, $\mu = \sum_{a_1,a_2} \mu_{a_1,a_2}$.

An appropriate definition of a weighted partial difference set is given as follows.

[34] Observe that the Cayley graph is k-regular with $k = |supp(f)|$.

Definition 11 (see Definition 21 in [67]) Let G be a finite abelian group of order ν and D be a subset of G, which is a disjoint union $D = D_1 \cup \ldots \cup D_r$, where D_j has order k_j, $1 \le j \le r$, and let $\lambda = (\lambda_{i,j,l})_{1 \le i,j,l \le r}$ and $\mu = (\mu_{i,j})_{1 \le i,j \le r}$. Then D is called a weighted (ν, k, λ, μ) partial difference set, if the following holds:

- For all $1 \le i, j, l \le r$, every nonzero element of D_l can be written as a difference of $d_1 \in D_i$, $d_2 \in D_j$ in exactly $\lambda_{i,j,l}$ ways, and every nonzero element of $G \setminus D$ can be written in $\mu_{i,j}$ ways as such a difference.
- For each i, there exists a j such that $-D_i = D_j$.

If $-D_i = D_i$ for all $1 \le i \le r$, then the weighted partial difference set D is called symmetric.

Remark 14 [67, Lemma 22] If in Definition 11, the sum $\sum_{i,j} \lambda_{i,j,l}$ is a fixed λ, independent from l, then D is a (conventional) partial difference set with parameters (ν, k, λ, μ) with $k = \sum_i k_i$, $\mu = \sum_{i,j} \mu_{i,j}$.

In [27], a one-to-one correspondence between weighted partial difference sets and edge-weighted strongly regular graphs is shown, which generalizes Proposition 1.1 in [78] on the connection between PDSs and strongly regular graphs, and connects weighted partial difference sets with association schemes.

Theorem 31 [27, *Theorem* 29], [67, *Theorem* 31] *Let G be a finite abelian group of order ν, and let D be subset of G, which is the disjoint union $D = D_1 \cup D_2 \cup \cdots \cup D_r$. Suppose that $0 \notin D$ and $-D_i = D_i$ for all $1 \le i \le r$. The following are equivalent*:

(i) *D is a (symmetric) weighted partial difference set with parameters (ν, k, λ, μ), where $k = (k_1, \ldots, k_r)$ with $k_i = |D_i|$, $\lambda = (\lambda_{i,j,l})_{1 \le i,j,l \le r}$ and $\mu = (\mu_{i,j})_{1 \le i,j \le r}$.*

(ii) *The Cayley graph $\mathcal{G}$ of D is a strongly regular edge-weighted graph with parameters (ν, k, λ, μ) as in (i).*

(iii) *For $1 \le i \le r$, let $R_i = \{(x, y) \in G \times G : x - y \in D_i\}$, and let $R_0 = \{(x, y) \in G \times G : x - y = 0\}$, and $R_{r+1} = \{(x, y) \in G \times G : x - y \in G \setminus (D \cup \{0\})\}$. Then $(G; R_0, R_1, \ldots, R_r, R_{r+1})$ is a symmetric association scheme.*

By Theorem 31, again connections between bent functions and weighted partial difference sets can alternatively be formulated in terms of edge-weighted strongly regular graphs.

The following theorem gives - opposite to the results in Section 6.1 - a sufficient condition for the bentness of a p-ary function in terms of properties of weighted partial difference sets.

Theorem 32 [67, *Theorem* 49] *For an odd prime p and an even integer n, let $f : \mathbb{V}_n^{(p)} \to \mathbb{F}_p$ be a p-ary function with $f(x) = f(-x)$ and $f(0) = 0$. Let*

$$D_i^f = \{x \in \mathbb{V}_n^{(p)} : f(x) = i\}, \quad 1 \le i \le p-1,$$
$$D_0^f = \mathbb{V}_n^{(p)} \setminus (\{0\} \cup D_1^f \cup \cdots \cup D_{p-1}^f) = \{x \in \mathbb{V}_n^{(p)}, x \ne 0 : f(x) = 0\}.$$

Suppose that $|D_i^f| = p^{n-1} \pm p^{n/2-1}$ *(hence* $|D_0^f| = p^{n-1} \pm (p-1)p^{n/2-1} - 1$*), and* $D = D_1^f \cup \cdots \cup D_{p-1}^f$ *is a weighted partial difference set, such that the corresponding association scheme is amorphic. Then f is bent.*

Remark 15 In [67], examples are given, which show that there are non-bent functions for which (with the above definitions) the edge-weighted Cayley graph is edge-weighted strongly regular, and that there are (regular) bent functions, whose Cayley graphs are not edge-weighted strongly regular.

7 Generalized and $\mathbb{Z}_{p^k}$-bent functions

In line with the increasing interest in functions from elementary abelian groups $\mathbb{V}_n^{(p)}$ to cyclic groups $\mathbb{Z}_{p^k}$, in this last chapter we present the major results on bentness for this class of functions, which were developed in several papers by several groups of authors. We refer to [3, 61, 81–83, 86, 87, 89, 94, 95, 115], and references therein. We are likewise interested in the case $p = 2$, and in the case of p odd.

Let f be a function from $\mathbb{V}_n^{(p)}$ to the cyclic group $\mathbb{Z}_{p^k}$. Then we can write f as

$$f(x) = a_0(x) + a_1(x)p + \cdots + a_{k-1}(x)p^{k-1}, \tag{18}$$

for some uniquely determined functions $a_i : \mathbb{V}_n^{(p)} \to \mathbb{F}_p$, $i = 0, \ldots, k-1$. As it turned out, the bentness of f and bentness of corresponding Boolean or p-ary functions are strongly related. We start with the more general class of the generalized bent functions.

7.1 Generalized bent functions

Since the introduction of generalized bent functions by Schmidt in [111] (2009), huge progress has been made in the research on this class of functions. By now, generalized bent functions are quite well understood interesting objects, comprising rich structures.

Clearly, for $k = 1$, a generalized bent function is simply a p-ary bent function. For $p = 2$, a function $f : \mathbb{V}_n^{(2)} \to \mathbb{Z}_{2^2}$, $f(x) = a_0(x) + a_1(x)2$, is generalized bent, if and only if a_1 and $a_1 \oplus a_0$ are Boolean bent functions when n is even, and if and only if a_1 and $a_1 \oplus a_0$ are semi-bent with complementary Walsh support when n is odd. In the general case, the situation becomes more complicated.

By several groups of authors it is observed - in various generality - that for a generalized bent function $f : \mathbb{V}_n^{(p)} \to \mathbb{Z}_{p^k}$ given as in (18), the affine space of p-ary (Boolean) functions

$$\mathcal{A}(f) = a_{k-1} \oplus \langle a_0, \ldots, a_{k-2} \rangle$$

is an affine space of bent functions if p is odd or $p = 2$ and n is even, and an affine space of semi-bent functions if $p = 2$ and n is odd. Sufficient conditions for the affine space $\mathcal{A}(f)$ to correspond to a generalized bent function f can be given in terms of Walsh coefficients of the bent respectively semi-bent functions in $\mathcal{A}(f)$. The quite strong conditions are a bit technical. We refer to Theorem 7 in [115], for $p = 2$ (see also [81, Theorems 8, 11]), and to Theorem 8 in [94] for odd p (or $p = 2$ and n even).

Remark 16 The detailed analysis of the Walsh coefficients of the bent respectively semi-bent functions in $\mathcal{A}(f)$ also enables the determination of the dual f^* (as given in Theorem 2) of a generalized bent function f. By [61, Theorem 1], the dual of a generalized bent function $f : \mathbb{V}_n^{(2)} \to \mathbb{Z}_{2^k}$, n even, given as $f(x) = a_0(x) + 2a_1(x) + \cdots + 2^{k-1}a_{k-1}(x)$, is $f^*(x) = b_0(x) + 2b_1(x) + \cdots + 2^{k-1}b_{k-1}(x)$, where

$$b_{k-1}(x) = a_{k-1}^*(x), \text{ and } b_j(x) = a_{k-1}^*(x) \oplus (a_{k-1} \oplus a_j)^*(x), 0 \le j \le k-2.$$

The expression for the dual f^* of a generalized bent function $f : \mathbb{V}_n^{(2)} \to \mathbb{Z}_{2^k}$ when n is odd, is somewhat more involved. We refer to Theorem 29 in [94].

The most comprehensive characterization of generalized bent functions is a description via partitions of $\mathbb{V}_n^{(p)}$, presented by Mesnager et al. in [94, Theorem 16]. For a function $f : \mathbb{V}_n^{(p)} \to \mathbb{Z}_{p^k}$ given as in (18), we obtain the partition $\mathcal{P} = \{A(d) : 0 \le d \le p^{k-1} - 1\}$ of $\mathbb{V}_n^{(p)}$, where

$$A(d) = \left\{ x \in \mathbb{V}_n : \sum_{i=0}^{k-2} a_i(x)p^i = d \right\}, \tag{19}$$

(some of the sets $A(d)$ may be empty). Then we have the following theorem.

Theorem 33 *Let p be an odd prime and n be a positive integer, or let $p = 2$ and n be an even positive integer, and let $f : \mathbb{V}_n^{(p)} \to \mathbb{Z}_{p^k}$ be given as in (18). Then f is generalized bent, if and only if $a_{k-1}(x) \oplus C(x)$ is bent for every p-ary respectively Boolean function $C(x)$, which is constant on the subsets $A(d)$ in (19) of the partition $\mathcal{P}$.*

Remark 17 Theorem 33 can be stated equivalently as follows: The function $f : \mathbb{V}_n^{(p)} \to \mathbb{Z}_{p^k}$ given as $f(x) = a_0(x) + a_1(x)p + \cdots + a_{k-1}(x)p^{k-1}$ is generalized bent, if and only if for very function $F : \mathbb{F}_p^{k-1} \to \mathbb{F}_p$, the p-ary function

$$a_{k-1}(x) \oplus F(a_0(x), \ldots, a_{k-2}(x)) \tag{20}$$

is bent.

Remark 18 For a generalized bent function given in the form (18), the set of p-ary (Boolean) functions $a_{k-1}(x) \oplus C(x)$, $C(x)$ constant on the subsets of the partition $\mathcal{P}$ as described above, forms an affine space of bent functions $\mathcal{A}(a_{k-1}, \mathcal{P})$ of dimension $|\mathcal{P}|$. Hence, one can see the generalized bent function as a p-ary respectively Boolean bent function $a(x)$ with a corresponding partition $\mathcal{P}$[35], which gives rise to a large affine space of bent functions.

Remark 19 As pointed out in [89, Theorem 3], any (nonempty) subset of a partition $\mathcal{P}$ for a bent function $a : \mathbb{V}_n^{(p)} \to \mathbb{F}_p$, n even, must have cardinality at least $p^{n/2}$, and a subset which achieves this lower bound is an affine subspace of $\mathbb{V}_n^{(p)}$. Therefore, the number of subsets in such a partition $\mathcal{P}$ is upper bounded by $p^{n/2}$. It is shown in [89, Theorem 4], that partitions for Maiorana-McFarland bent functions $a(x)$ achieve this upper bound, hence provide affine spaces of bent functions $\mathcal{A}(a, \mathcal{P})$ with maximal possible dimension $p^{n/2}$.

[35] In [95], the bent function $a(x)$ is then called admissible for the partition $\mathcal{P}$.

Remark 20 In [95], results of similar type are presented for generalized plateaued functions, i.e., for functions $f : \mathbb{V}_n^{(p)} \to \mathbb{Z}_{p^k}$ for which $\mathcal{H}_f(1, u)$ has absolute value $p^{(n+s)/2}$ or 0 for all $u \in \mathbb{V}_n^{(p)}$, and a fixed integer s depending on f.

An alternative neat characterization of generalized bent functions for $p = 2$ is given in [61].

Theorem 34 *Let n be even, and $f : \mathbb{V}_n^{(2)} \to \mathbb{Z}_{2^k}$ be given as $f(x) = a_0(x) + 2a_1(x) + \cdots + 2^{k-1}a_{k-1}(x)$ for some Boolean functions a_j, $0 \le j \le k-1$, and let $\mathcal{A}(f)$ be the affine space of Boolean functions,*

$$\mathcal{A}(f) = a_{k-1} \oplus \langle a_{k-2}, \ldots, a_0 \rangle.$$

Then f is generalized bent, if and only if all functions in $\mathcal{A}(f)$ are Boolean bent functions, and for any three functions $b_0, b_1, b_2 \in \mathcal{A}(f)$ we have

$$(b_0 \oplus b_1 \oplus b_2)^* = b_0^* \oplus b_1^* \oplus b_2^*. \tag{21}$$

Remark 21 Triples of Boolean bent functions b_0, b_1, b_2, for which the sum $b_0 \oplus b_1 \oplus b_2$ is bent as well, and the sum of the duals $b_0^* \oplus b_1^* \oplus b_2^*$ equals the dual of the sum $(b_0 \oplus b_1 \oplus b_2)^*$, have been employed in a secondary construction of Boolean bent functions, [20]. In fact, in [91, Theorem 4], it is shown that for three bent functions b_0, b_1, b_2 for which the sum is bent, the Boolean function $b_0b_1 \oplus b_0b_2 \oplus b_1b_2$ is bent if and only (21) applies. It is easily verified that for a generalized bent function $f : \mathbb{V}_n^{(2)} \to \mathbb{Z}_{2^k}$ given as $f(x) = a_0(x) + a_1(x)2 + \ldots + a_{k-1}(x)2^{k-1}$, and three bent functions $b_0, b_1, b_2 \in \mathcal{A}(f)$, the bent function $b_0b_1 \oplus b_0b_2 \oplus b_1b_2$ is in $\mathcal{A}(a_{k-1}, \mathcal{P})$.

Theorems 33 and 34 are not applicable in this form for $p = 2$ and n odd, in which case $\mathcal{A}(f)$ is an affine space of semi-bent functions. A version of Theorem 34 for n odd is given in [61], based on the observation that for three semi-bent functions $b_0, b_1, b_2 : \mathbb{V}_n^{(2)} \to \mathbb{F}_2$, for which the sum is also semi-bent, the Boolean function $b_0b_1 \oplus b_0b_2 \oplus b_1b_2$ is semi-bent, if and only if certain conditions on the Walsh coefficients of b_0, b_1, b_2 are satisfied (see [61, Theorem 2]. The version of Theorem 34 for odd n requires some more detailed conditions on the Walsh transforms of the semi-bent functions in $\mathcal{A}(f)$, see [61, Corollary 3].

In [94], for $p = 2$, a connection between generalized bent functions in even dimension and in odd dimension is given.

Theorem 35 [94, *Theorem* 24] *For a function $f : \mathbb{V}_n^{(2)} \to \mathbb{Z}_{2^k}$, n odd, given in the form (18) as $f(x) = a_0(x) + a_1(x)2 + \cdots + a_{k-1}(x)2^{k-1}$, let $\tilde{f} : \mathbb{V}_n^{(2)} \times \mathbb{F}_2 \to \mathbb{Z}_{2^k}$ be given as*

$$\tilde{f}(x, z) = a_0(x) + a_1(x)2 + \cdots + a_{k-3}(x)2^{k-3} + z2^{k-2} + (a_{k-1}(x) \oplus a_{k-2}(x)z)2^{k-1}.$$

Then f is generalized bent, if and only if $\tilde{f}$ is generalized bent.

With this connection between the case of n odd and n even, one can transfer some results for the case n even to the case n odd, see Theorem 25 and Corollary 26 in [94].

We conclude this section with some remarks on classification of generalized bent functions. Formal expressions (18), which satisfy the condition for generalized bent functions are easy to obtain. For instance, $f(x) = p^{k-1}a(x)$ is a generalized bent function from $\mathbb{V}_n^{(p)}$ to $\mathbb{Z}_{p^k}$ for every p-ary bent function $a : \mathbb{V}_n^{(p)} \to \mathbb{F}_p$. However, one would not consider $a(x)$ and

$p^{k-1}a(x)$ as different objects. Given the affine space $\mathcal{A}(f) = a_{k-1} \oplus \langle a_0, \ldots, a_{k-2} \rangle$ of bent functions corresponding to a generalized bent function f represented as in (18), with any other representation of the same affine space, another formal expression for a generalized bent function is obtained. Many more expressions one should be able to obtain from the much larger affine space $\mathcal{A}(a_{k-1}, \mathcal{P})$[36]. A very general approach to classify generalized bent functions would be via p-ary bent functions $a(x)$ and their corresponding partitions $\mathcal{P}$, i.e., via the affine space $\mathcal{A}(a, \mathcal{P})$.

Question 20 For classes of bent functions other than the Maiorana-McFarland class and the class of spread bent functions[37], find corresponding partitions $\mathcal{P}$ with cardinality $|\mathcal{P}|$ as large as possible. Can the maximal possible cardinality $p^{n/2}$ of a partition be achieved by bent functions other than a Maiorana-McFarland function?

For three bent functions b_0, b_1, b_2 in the affine space $\mathcal{A}(f)$ of a generalized bent function, the bent function $b_0b_1 \oplus b_0b_2 \oplus b_1b_2 \in \mathcal{A}(a_{k-1}, \mathcal{P})$ has in general a different algebraic degree. Hence, in general, $\mathcal{A}(a_{k-1}, \mathcal{P})$ contains bent functions from different EA-equivalence classes.

Question 21 Examine which classes of bent functions are contained in the affine space $\mathcal{A}(a, \mathcal{P})$ of some given bent function $a(x)$ and a corresponding partition $\mathcal{P}$.

The p-ary bent functions corresponding to all so far considered constructions of generalized bent functions are (weakly) regular bent functions.

Question 22 Examine partitions $\mathcal{P}$ for non-weakly regular bent functions a, i.e., for generalized bent functions for which $\mathcal{A}(a, \mathcal{P})$ contains non-weakly regular bent functions. What is the largest cardinality a partition $\mathcal{P}$ for a non-weakly regular bent function $a(x)$ can have?

In many secondary bent function constructions, a new bent function is obtained from some bent functions (sometimes in the same number, sometimes in a larger number of variables).

Question 23 Can we infer information on a partition for a bent function obtained with a secondary construction, from the partitions of the bent functions used in the construction?

7.2 $\mathbb{Z}_{p^k}$-bent functions

$\mathbb{Z}_{p^k}$-bent functions respectively relative difference sets in $\mathbb{V}_n^{(p)} \times \mathbb{Z}_{p^k}$, are much harder to find than bent functions between elementary abelian groups or generalized bent functions.

Clearly, when $k = 1$, then $\mathbb{Z}_{p^k}$-bent functions reduce to conventional p-ary bent functions, if $f(x) = a_0(x) + a_1(x)p + \cdots + a_{k-1}(x)p^{k-1}$ is $\mathbb{Z}_{p^k}$-bent, then $F(x) = (a_0(x), a_1(x), \ldots, a_{k-1}(c))$ is a vectorial bent function, but the converse does not hold.[38]

[36] As easily confirmed, $\mathcal{A}(f)$ is a subspace of $\mathcal{A}(a_{k-1}, \mathcal{P})$.

[37] Partitions for spread bent functions are naturally obtained from the spread, see the discussions in [89].

[38] In the case of $p = 2$, $k = 2$, $f(x) = a_0(x) \oplus a_1(x)2$ is $\mathbb{Z}_4$-bent if and only if $F(x) = (a_0(x), a_1(x))$ is a vectorial bent function.

As is easily observed, $f : \mathbb{V}_n^{(p)} \to \mathbb{Z}_{p^k}$ is $\mathbb{Z}_{p^k}$-bent if and only if $p^t f(x)$ is generalized bent for all $0 \le t \le k-1$. With the sufficient and necessary conditions for generalized bentness in Section 7.1, we get quite strong conditions on a sequence of affine spaces of p-ary respectively Boolean functions.

One construction which yields $\mathbb{Z}_{p^k}$-bent functions, is the ubiquitous spread construction, we recalled in Theorem 6, as with this construction one can generate bent functions from $\mathbb{V}_n^{(p)}$, n even, into any abelian group of order p^k, $k \le n/2$.[39]

In [87], for $p = 2$, and in [3], for odd primes p, a first construction of $\mathbb{Z}_{p^k}$-bent functions is presented, obtained from partitions of $\mathbb{V}_n^{(p)} = \mathbb{F}_{p^m} \times \mathbb{F}_{p^m}$, $m = n/2$, which have similar properties as spreads, but provable[40] do not come from (partial) spreads:

Let m, k be integers such that k divides m and $\gcd(p^m - 1, p^k + p - 1) = 1$. Set $e = p^k + p - 1$, and let d be the multiplicative inverse of e modulo $p^m - 1$. For an element $s \in \mathbb{F}_{p^m}$ define

$$U_s := \{(x, sx^e) \ : \ x \in \mathbb{F}_{p^m}\},\ U_s^* = U_s \setminus \{(0,0)\},\ \text{ and } \ U = \{(0, y) \ : \ y \in \mathbb{F}_{p^m}\}.$$

Then U, U_s^*, $s \in \mathbb{F}_{p^m}$, form a partition of $\mathbb{F}_{p^m} \times \mathbb{F}_{p^m}$.

Similarly, for an element $s \in \mathbb{F}_{p^m}$,

$$V_s := \{(x^d s, x) \ : \ x \in \mathbb{F}_{p^m}\},\ V_s^* = V_s \setminus \{(0,0)\},\ \text{ and } \ V = \{(x, 0) \ : \ x \in \mathbb{F}_{p^m}\}.$$

For an element γ of $\mathbb{F}_{p^k}$, let then

$$\mathcal{A}(\gamma) = \bigcup_{\substack{s \in \mathbb{F}_{p^m} \\ \mathrm{Tr}_k^m(s) = \gamma}} U_s^* \quad \text{and} \quad \mathcal{B}(\gamma) = \bigcup_{\substack{s \in \mathbb{F}_{p^m} \\ \mathrm{Tr}_k^m(s) = \gamma}} V_s^*.$$

With these definitions, we obtain two partitions of $\mathbb{F}_{p^m} \times \mathbb{F}_{p^m}$,

$$\Gamma_1 = \{U, \mathcal{A}(\gamma); \gamma \in \mathbb{F}_{p^k}\}$$
$$\Gamma_2 = \{V, \mathcal{B}(\gamma); \gamma \in \mathbb{F}_{p^k}\},$$

into $p^k + 1$ subsets, which exhibit similar properties as spreads. For $k = m$, both partitions reduce to the Desarguesian spread.

The following theorem summarizes Theorems 2, 3 in [87] for $p = 2$, and Theorem 7, Corollary 4 in [3] for arbitrary p.

Theorem 36 *Let m, k be integers, such that k divides m and $\gcd(p^m - 1, p^k + p - 1) = 1$, let $e = p^k + p - 1$, and d such that $de \equiv 1 \bmod p^m - 1$.*

I. Let f be a p-ary function from $\mathbb{F}_{p^m} \times \mathbb{F}_{p^m}$ to $\mathbb{F}_p$, for which every $c \in \mathbb{F}_p$ has the union of exactly p^{k-1} of the sets $\mathcal{A}(\gamma)$ (respectively $\mathcal{B}(\gamma)$) in its preimage set. Further suppose that f is constant c_0 on U (respectively V) for some $c_0 \in \mathbb{F}_p$. Then f is a regular p-ary bent function. Conversely, every p-ary bent function that is constant on the elements

[39] As pointed out in [87], $\mathbb{Z}_{p^k}$-bent functions can more generally be obtained from partial spreads with sufficiently many subspaces.

[40] The argument is via the algebraic degree of the involved bent functions.

of Γ_1 *(respectively* Γ_2*) is of this form. The duals of the bent functions of* Γ_1 *are bent functions of* Γ_2*, and vice versa.*
II. Let $F : \mathbb{F}_{p^m} \times \mathbb{F}_{p^m} \to \mathbb{Z}_{p^k}$ *such that every* $c \in \mathbb{Z}_{p^k}$ *has exactly one of the sets* $\mathcal{A}(\gamma)$ *(respectively* $\mathcal{B}(\gamma)$*) in its preimage set, and F is constant* c_0 *on U (respectively on V) for some* $c_0 \in \mathbb{Z}_{p^k}$*. Then F is a* $\mathbb{Z}_{p^k}$*-bent function. If* $k < m$*, then F is not obtained from some (partial) spread.*

Remark 22 Similar as for spreads, the partitions Γ_1, Γ_2, not only yield bent functions between elementary abelian groups and $\mathbb{Z}_{p^k}$-bent functions, but also bent functions from $\mathbb{F}_{p^m} \times \mathbb{F}_{p^m}$ into any abelian group B of order p^k. The bentness property is inhered in the partition.

Remark 23 In [3], a partition Ω of $\mathbb{V}_n^{(p)}$ is called a *bent partition*, if every p-ary respectively Boolean function, for which the preimage set of any element of $\mathbb{F}_p$ is the union of exactly $|\Omega|/p$ subsets of Ω, is always bent (in a variant of the definition, one element $\tilde{\ell} \in \mathbb{F}_p$ has one subset more in its preimage set). It is then shown, that from any such bent partition one obtains $\mathbb{Z}_{p^k}$-bent functions.[41]

Question 24 Is the largest possible k for a $\mathbb{Z}_{p^k}$-bent function that one, which is achieved with the spread construction, i.e., $k = n/2$. Is the spread construction the only construction of $\mathbb{Z}_{p^k}$-bent functions for $k = n/2$?

From a $\mathbb{Z}_{p^k}$-bent function f we obtain a sequence of generalized bent functions $p^t f$, $0 \le t \le k-2$, and hence a sequence of affine spaces (of the form $\mathcal{A}(a, \mathcal{P})$ as introduced above). This may give rise to a large variety of (vectorial) bent functions.

Question 25 Can one say something about the classes of (vectorial) bent functions inherent in a given $\mathbb{Z}_{p^k}$-bent function. For instance, the set of p-ary (Boolean) bent functions from Γ_1, Γ_2 contains many Maiorana-McFarland functions. Are there other classes, which ones?

For all so far known $\mathbb{Z}_{p^k}$-bent functions, $k \ge 2$, the inherent bent functions are regular bent functions.

Question 26 Similar as for generalized bent functions, one can ask for existence of $\mathbb{Z}_{p^k}$-bent functions, $k \ge 2$, for which (some of) the corresponding bent functions are non-weakly regular. What would be the largest possible k for such $\mathbb{Z}_{p^k}$-bent functions?

Acknowledgements The author thanks Sabancı University for the hospitality during several research visits. The author also wishes to thank the reviewer and the associate editor for valuable comments, which helped to improve the paper.

[41] Some questions on bent partitions are collected in section "Perspectives" of [3].

References

1. A.A. Albert, Generalied twisted fields. Pac. J. Math. 11 (1961), 1–8
2. N. Anbar, C. Kaşkci, W. Meidl, A. Topuzoğo, Alev Shifted plateaued functions and their differential properties. Cryptogr. Commun. 12 (2020), 1091–1105
3. N. Anbar, W. Meidl, Bent partitions. Des. Codes Cryptogr. 90 (2022), 1081–1101
4. A. Bernasconi, B. Codenotti, Spectral analysis of Boolean functions as a graph eigenvalue problem. IEEE Trans. Comput. 48 (1999), 345–351
5. A. Bernasconi, B. Codenotti, J.M. VanderKam, A characterization of bent functions in terms of strongly regular graphs, IEEE Trans. Comput. 50 (2001), 984–985
6. J. Bierbrauer, New semifields, PN and APN functions. Des. Codes Cryptogr. 54 (2010), 189–200
7. J. Bierbrauer, D. Bartoli, G. Faina, S. Marcugini, F. Pambianco, A family of semifields in odd characteristic. Des. Codes Cryptogr. 86 (2018), 611–621
8. L. Budaghyan, C. Carlet, CCZ-equivalence of single and multi output Boolean functions. In; Finite fields: theory and applications, Contemp. Math., 518, pp. 43–54, Amer. Math. Soc., Providence, RI, 2010
9. L. Budaghyan, C. Carlet, CCZ-equivalence of bent vectorial functions and related constructions. Des. Codes Cryptogr. 59 (2011), 69–87
10. L. Budaghyan, C. Carlet, T. Helleseth, A. Kholosha, Generalized bent functions and their relation to Maiorana-McFarland class, in: Proceedings IEEE Int. Symp. on Inform. Theory, 2012, pp. 1217–1220
11. L. Budaghyan, T. Helleseth, New commutative semifields defined by new PN multinomials. Cryptogr. Commun. 3 (2011), 1–16
12. L. Budaghyan, T. Helleseth, Planar functions and commutative semifields. Tatra Mt. Math. Publ. 45 (2010), 15–25
13. L. Budaghyan, T. Helleseth, New perfect nonlinear multinomials over F_{p2k} for any odd prime p. In: Sequences and their applications–SETA 2008, Lecture Notes in Comput. Sci., 5203, pp. 403–414, Springer, Berlin, 2008
14. A. Canteaut, C. Carlet, P. Charpin, C. Fontaine, On cryptographic properties of the cosets of R(1, m). IEEE Trans. Inform. Theory 47 (2001), 1494–1513
15. A. Canteaut, P. Charpin, Decomposing bent functions. IEEE Trans. Inform. Theory 49 (2003), 2004–2019
16. A. Canteaut, M. Daum, H. Dobbertin, G. Leander, Finding nonnormal bent functions. Discrete Appl. Math. 154 (2006), 202–218
17. C. Carlet, A transformation on Boolean functions, its consequences on some problems related to Reed-Muller codes. In: Eurocode '90 (Udine, 1990), Lecture Notes in Comput. Sci., vol. 514, pp. 42–50, Springer, Berlin, 1991
18. C. Carlet, Two new classes of bent functions. In: Advances in Cryptology - EUROCRYPT 93, Lecture Notes in Computer Science 765, pp. 77–101, Springer-Verlag, Berlin, 1994
19. C. Carlet, On the degree, nonlinearity, algebraic thickness, and nonormality of Boolean functions, with developments on symmetric functions. IEEE Trans. Inform. Theory 50 (2004), 2178–2185
20. C. Carlet, On Bent and Highly Non-linear Balanced/Resilient Functions and their Algebraic Immunities. In: M.P.C. Fossorier et al. (Eds.), AAECC, Lecture Notes in Computer Science 3857, pp. 1–28, Springer-Verlag, New York, 2006
21. C. Carlet, Boolean functions for cryptography and error correcting codes. In: Boolean Models and Methods in Mathematics, Computer Science, and Engineering, pp. 257–397, Cambridge University Press, Cambridge 2010
22. C. Carlet, Vectorial Boolean functions for cryptography. In: Boolean Models and Methods in Mathematics, Computer Science, and Engineering, pp. 398–469, Cambridge University Press, Cambridge 2010
23. C. Carlet, Boolean Functions for Cryptography and Coding Theory. Cambridge University Press 2021
24. C. Carlet, P. Charpin, V. Zinoviev, Codes, bent functions and permutations suitable for DES-like cryptosystems, Des. Codes Cryptogr. 15 (1998), 125–156
25. C. Carlet, S. Mesnager, On Dillon's class H of bent functions, Niho bent functions and o-polynomials. J. Combin. Theory Ser. A 118 (2011), 2392–2410
26. C. Carlet, S. Mesnager, Four decades of research on bent functions. Des. Codes Cryptogr. 78 (2016), 5–50
27. C. Celerier, D. Joyner, C. Melles, D. Phillips, S. Walsh, Edge-weighted Cayley graphs and p-ary bent functions. Integers 16 (2016), Paper No. A35, 56 pp

28. A. Çeşmelioğlu, G. McGuire, W. Meidl, A construction of weakly and non-weakly regular bent functions, J. Comb. Theory, Series A 119 (2012), 420–429
29. A. Çeşmelioğlu, W. Meidl, Bent functions of maximal degree, IEEE Trans. Inform. Theory 58 (2012), 1186–1190
30. A. Çeşmelioğlu, W. Meidl, A construction of bent functions from plateaued functions, Des. Codes Cryptogr. 66 (2013), 231–242
31. A. Çeşmelioğlu, W. Meidl, A. Pott, On the dual of (non)-weakly regular bent functions and self-dual bent functions, Advances in Mathematics of Communications 7 (2013), 425–440
32. A. Çeşmelioğlu, W. Meidl, A. Pott, Generalized Maiorana-McFarland class and normality of p-ary bent functions, Finite Fields Appl. 24 (2013), 105–117
33. A. Çeşmelioğlu, W. Meidl, A. Pott, Bent functions, spreads, and o-polynomials, SIAM J. Discrete Math. 29 (2015), 854–867
34. A. Çeşmelioğlu, W. Meidl, A. Pott, There are infinitely many bent functions for which the dual is not bent, IEEE Trans. Inform. Theory 62 (2016), 5204–5208
35. A. Çeşmelioğlu, W. Meidl, A. Pott, Vectorial bent functions and their duals, Linear Algebra and its Applications 548 (2018), 305–320
36. A. Çeşmelioğlu, W. Meidl, Bent and vectorial bent functions, partial difference sets, and strongly regular graphs. Advances in Mathematics of Communications 12 (2018), 691–705
37. A. Çeşmelioğlu, W. Meidl, A. Pott, A survey on bent functions and their duals. In: Combinatorics and Finite Fields, Radon Series on Computational and Applied Mathematics, pp. 39–56, de Gruyter, Berlin, 2019
38. A. Çeşmelioğlu, W. Meidl, A. Pott, Vectorial bent functions in odd characteristic and their components. Cryptogr. Commun. 12 (2020), 899–912
39. A. Çeşmelioğlu, W. Meidl, I. Pirsic, Vectorial bent functions and partial difference sets. Des. Codes Cryptogr. 89 (2021), 2313–2330
40. P. Charpin, Normal Boolean functions. J. Complexity 20 (2004), 245–265
41. P. Charpin, E. Pasalic, C Tavernier, On bent and semi-bent quadratic Boolean functions. IEEE Trans. Inform. Theory 51 (2005), 4286–4298
42. Y.M. Chee, Y. Tan, X.D. Zhang, Strongly regular graphs constructed from p-ary bent functions, J. Algebr. Comb. 34 (2011), 251–266
43. R.S. Coulter, R.W. Matthews, Planar functions and planes of Lenz-Barlotti class II. Des. Codes Cryptogr. 10 (1997), 167–184
44. R.S. Coulter, M. Henderson, Commutative presemifields and semifields. Adv. Math. 217 (2008), no. 1, 282–304
45. T.W. Cusick, P. Stănică, Cryptographic Boolean functions and applications. Second edition. Elsevier/Academic Press, London, 2017
46. E. van Dam, Strongly regular decompositions of the complete graph. J. Algebraic Combin. 17 (2003), 181–201
47. J.A. Davis, J. Jedwab, A unifying construction for difference sets, J. Combin. Theory Ser. A 80 (1997), 13–78
48. U. Dempwolff, Automorphisms and isomorphisms of some p-ary bent functions. J. Algebraic Combin. 51 (2020), 527–566
49. J.F. Dillon, Elementary Hadamard difference sets, Ph.D. dissertation, University of Maryland, 1974
50. C. Ding, Cyclic codes from APN and planar functions, arXiv:1206.4687v1
51. C. Ding, J. Yuan, A family of skew Hadamard difference sets. J. Comb. Theory A 113 (2006), 1526–1535
52. H. Dobbertin, Construction of bent functions and balanced boolean functions with high nonlinearity. In: Fast Software Encryption: Proceedings of the 1994 Leuven Workshop on Cryptographic Algorithms, Lecture Notes in Computer Science 1008, pp. 61–74, Berlin, Germany, 1995
53. Y. Fan, B. Xu, Fourier transforms and bent functions on finite groups. Des. Codes Cryptogr. 86 (2018), 2091–2113
54. K. Feng, J. Luo, Value distributions of exponential sums from perfect nonlinear functions and their applications, IEEE Trans. Inform. Theory 53 (2007), 3035–3041
55. T. Feng, B. Wen, Q. Xiang, J. Yin, Partial difference sets from quadratic forms and p-ary weakly regular bent functions. ALM 27, 25–40
56. G. Gong, T. Helleseth, H. Hu, A. Kholosha, On the dual of certain ternary weakly regular bent functions, IEEE Trans. Inform. Theory 58 (2012), 2237–2243
57. T. Helleseth, A. Kholosha, Monomial and quadratic bent functions over the finite fields of odd characteristic, IEEE Trans. Inform. Theory 52 (2006), 2018–2032

58. T. Helleseth, H. D. L. Hollmann, A. Kholosha, Z. Wang, Q. Xiang, Proofs of two conjectures on ternary weakly regular bent functions, IEEE Trans. Inform. Theory 55 (2009), 5272–5283
59. T. Helleseth, A. Kholosha, New binomial bent functions over the finite fields of odd characteristic, IEEE Trans. Inform. Theory 56 (2010), 4646–4652
60. T. Helleseth, A. Kholosha, Crosscorrelation of m-sequences, exponential sums, bent functions and Jacobsthal sums, Cryptogr. Commun. 3 (2011), 281–291
61. S. Hodžić, W. Meidl, E. Pasalic, Full characterization of generalized bent functions as (semi)-bent spaced, their dual and the Gray image. IEEE Trans. Inform. Theory 64 (2018), 5432–5440
62. X.D. Hou, p-ary and q-ary versions of certain results about bent functions and resilient functions, Finite Fields Appl. 10 (2004), 566–582
63. H. Hu, Q. Zhang, S. Shao, On the dual of the Coulter-Matthews bent functions. IEEE Trans. Inform. Theory 63 (2017), 2454–2463
64. H. Hu, X. Yang, S. Tang, New classes of ternary bent functions from the Coulter-Matthews bent functions. IEEE Trans. Inform. Theory 64 (2018), 4653–4663
65. J.Y. Hyun, Y. Lee, Characterization of p-ary bent functions in terms of strongly regular graphs. IEEE Trans. Inform. Theory 65 (2019), 676–684
66. W. Jia, X. Zeng, T. Helleseth, C. Li, A class of binomial bent functions over the finite fields of odd characteristic. IEEE Trans. Inform. Theory 58 (2012), 6054–6063
67. D. Joyner, C. Melles, Perspectives on p-ary bent functions. Elementary theory of groups and group rings, and related topics (New York, Nov. 1–2, 2018), pp. 103–126, de Gruyter, Berlin, 2020
68. W. Kantor, Exponential numbers of two-weight codes, difference sets and symmetric designs. Discrete Math. 46 (1983), 95–98
69. W. Kantor, Bent functions generalizing Dillon's partial spread functions, arXiv:1211.2600v1
70. D.E. Knuth, Finite semifields and projective planes. J. Agebra 2 (1965), 182–217
71. N. Kolomeec, The graph of minimal distances of bent functions and its properties. Des. Codes Cryptogr. 85 (2017), 395–410
72. P.V. Kumar, R.A. Scholtz, L.R. Welch, Generalized bent functions and their properties, J. Combin. Theory Ser. A 40 (1985), 90–107
73. M. Lavrauw, O. Polverino, Finite semifields. In: Current research topics in Galois Geometry, pp. 131–159, Nova Science Publishers, New York, 2012
74. G. Leander, G. McGuire, Construction of bent functions from near-bent functions. J. Comb. Theory Ser. A 116 (2009), 960–970
75. N. Li, S. Mesnager, Recent results and problems on constructions of linear codes from cryptographic functions. Cryptogr. Commun. 12 (2020), 965–986
76. P. Lisonek, H.Y. Lu, Bent functions on partial spreads, Des. Codes Cryptogr. 73 (2014), 209–216
77. S.L. Ma, Partial difference sets. Discrete Math. 52 (1984), 75–89
78. S.L. Ma, A survey of partial difference sets. Des. Codes Cryptogr. 4 (1994), 221–261
79. B. Mandal, P. Stănică, S. Gangopadhyay, New classes of p-ary bent functions. Cryptogr. Commun. 11 (2019), 77–92
80. H. B. Mann, Difference sets in elementary Abelian groups. Illinois J. Math. 9 (1965), 212–219
81. T. Martinsen, W. Meidl, S. Mesnager, P. Stănică, Decomposing generalized bent and hyperbent functions. IEEE Trans. Inform. Theory 63 (2017), 7804–7812
82. T. Martinsen, W. Meidl, P. Stănică, Generalized bent functions and their Gray images, in (S. Duquesne, S. Petkova-Nikova, eds.) Arithmetic of Finite Fields, Proceedings of WAIFI 2016, Lecture Notes in Computer Science 10064, pp. 160–173, Springer-Verlag, Berlin Heidelberg, 2017
83. T. Martinsen, W. Meidl, P. Stănică, Partial spread and vectorial generalized bent functions. Designs, Codes, Cryptogr. 85 (2017), 1–13
84. R.L. McFarland, A family of noncyclic difference sets, J. Combin. Theory Ser. A 15 (1973), 1–10
85. W. Meidl, Generalized Rothaus construction and non-weakly regular bent functions, J. Combin. Theory Ser. A 141 (2016), 78–89
86. W. Meidl, A secondary construction of bent functions, octal gbent functions and their duals. Math. Comput. Simulation 143 (2018), 57–64
87. W. Meidl, I. Pirsic, Bent and Z_{2k}-bent functions from spread-like partitions. Des. Codes Cryptogr. 89 (2021), 75–89
88. W. Meidl, I. Pirsic, On the normality of p-ary bent functions. Cryptogr. Commun. 10 (2018), 1037–1049
89. W. Meidl, A. Pott, Generalized bent functions into Z_{2k} from the partial spread and the Maiorana-McFarland class, Cryptogr. Commun. 11 (2019), 1233–1245
90. C. Melles, D. Joyner, On p-ary bent functions and strongly regular graphs, arXiv:1904.09359v1
91. S. Mesnager, Several new infinite families of bent functions and their duals. IEEE Trans. Inform. Theory 60 (2014), 4397–4407
92. S. Mesnager, Bent functions. Fundamentals and results. Springer 2016

93. S. Mesnager, Linear codes with few weights from weakly regular bent functions based on a generic construction. Cryptogr. Commun. 9 (2017), 71–84
94. S. Mesnager, C. Tang, Y. Qi, L. Wang, B. Wu, K. Feng, Further results on generalized bent functions and their complete characterization. IEEE Trans. Inform. Theory 64 (2018), 5441–5452
95. S. Mesnager, C. Tang, Y. Qi, Generalized plateaued functions and admissible (plateaued) functions. IEEE Trans. Inform. Theory 63 (2017), 6139–6148
96. K. Nyberg, Perfect nonlinear S-boxes, In: Advances in cryptology–EUROCRYPT '91 (Brighton, 1991), Lecture Notes in Comput. Sci., 547, pp. 378–386, Springer, Berlin, 1991
97. K. Nyberg, Construction of bent functions and difference sets, In: Advances in cryptology–EUROCRYPT '90 (Aarhus, 1990), Lecture Notes in Comput. Sci., 473, pp. 151–160, Springer, Berlin, 1991
98. R.M. Pelen, F. Özbudak, Duals of non weakly regular bent functions are not weakly regular and generalization to plateaued functions, Finite Fields Appl. 64 (2020), 101668, 16 pp
99. L. Poinsot, Bent functions on a finite nonabelian group. J. Discrete Math. Sci. Cryptogr. 9 (2006), 349–364
100. L. Poinsot, Non Abelian bent functions. Cryptogr. Commun. 4 (2012), 1–23
101. L. Poinsot, A. Pott, Non-Boolean almost perfect nonlinear functions on non-Abelian groups. Internat. J. Found. Comput. Sci. 22 (2011), 1351–1367
102. V. Potapov, On minimal distance between p-ary bent functions. In: Problems of redundancy in information and control systems, pp. 115–116, IEEE, 2016
103. V. Potapov, On q-ary bent and plateaued functions. Des. Codes Cryptogr. 88 (2020), 2037–2049
104. A. Pott, A survey on relative difference sets. Groups, difference sets, and the Monster. In: Ohio State Univ. Math. Res. Inst. Publ., 4, pp. 195–232, de Gruyter, Berlin, 1996
105. A. Pott, Nonlinear functions in abelian groups and relative difference sets. Discrete Appl. Math. 138 (2004), 177–193
106. A. Pott, Almost perfect and planar functions. Des. Codes Cryptogr. 78 (2016), 141–195
107. A. Pott, Y. Tan, T. Feng, S. Ling, Association schemes arising from bent functions. Des. Codes Cryptogr. 59 (2011), 319–331
108. Y. Qi, C. Tang, D Huang, Explicit characterization of two classes of regular bent functions. Appl. Algebra Engrg. Comm. Comput. 29 (2018), 529–544
109. Y. Qi, Yanfeng, C.Tang, Z. Zhou, C. Fan, Several infinite families of p-ary weakly regular bent functions. Adv. Math. Commun. 12 (2018), 303–315
110. O.S. Rothaus, On bent functions, J. Combin. Theory Ser. A 20 (1976), 300–305
111. K.U. Schmidt, Quaternary constant-amplitude codes for multicode CDMA. IEEE Trans. Inf. Theory 55 (2009), 1824–1832
112. Y. Tan, A. Pott, T. Feng, Strongly regular graphs associated with ternary bent functions. J. Comb. Theory, Series A 117 (2010), 668–682
113. Y. Tan, J. Yang, X. Zhang, A recursive approach to construct p-ary bent functions which are not weakly regular, In: Proceedings of IEEE International Conference on Information Theory and Information Security, pp. 156–159, Beijing, 2010
114. C. Tang, Y. Qi, D. Huang, Regular p-ary bent functions with five terms and Kloosterman sums. Cryptogr. Commun. 11 (2019), 1133–1144
115. C. Tang, C. Xiang, Y. Qi, K. Feng, Complete characterization of generalized bent and 2_k-bent Boolean functions. IEEE Trans. Inform. Theory 63 (2017), 4668–4674
116. C. Tang, M. Xu, Y. Qi, M. Zhou, A new class of p-ary regular bent functions. Adv. Math. Commun. 15 (2021), 55–64
117. N. Tokareva, Bent Functions, Results and Applications to Cryptography, Academic Press, San Diego, CA, 2015
118. G. Weng, X. Zeng, Further results on planar DO functions and commutative semifields. Des. Codes Cryptogr. 63 (2012), 413–423
119. Y. Wu, N. Li, X. Zeng, Linear codes from perfect nonlinear functions over finite fields. IEEE Trans. Commun. 68 (2020), 3–11
120. B. Xu, Bentness and nonlinearity of functions on finite groups. Des. Codes Cryptogr. 76 (2015), 409–430
121. B. Xu, Absolute maximum nonlinear functions on finite nonabelian groups. IEEE Trans. Inform. Theory 66 (2020), 5167–5181
122. G. Xu, X. Cao, S. Xu, Constructing new APN functions and bent functions over finite fields of odd characteristic via the switching method. Cryptogr. Commun. 8 (2016), 155–171
123. G. Xu, X. Cao, S. Xu, Two classes of p-ary bent functions and linear codes with three or four weights. Cryptogr. Commun. 9 (2017), 117–131

124. D. Zheng, L. Yu, L. Hu, On a class of binomial bent functions over the finite fields of odd characteristic. Appl. Algebra Engrg. Comm. Comput. 24 (2013), 461–475
125. Y.L. Zheng, X.M. Zhang, On plateaued functions, IEEE Trans. Inf. Theory 47 (2001), 1215–1223