Designs, Codes and Cryptography
https://doi.org/10.1007/s10623-022-01029-z

Bent partitions

Nurdagül Anbar[1] · Wilfried Meidl[1]

Received: 13 June 2021 / Revised: 27 February 2022 / Accepted: 1 March 2022

Abstract

Spread and partial spread constructions are the most powerful bent function constructions. A large variety of bent functions from a $2m$-dimensional vector space $\mathbb{V}_{2m}^{(p)}$ over $\mathbb{F}_p$ into $\mathbb{F}_p$ can be generated, which are constant on the sets of a partition of $\mathbb{V}_{2m}^{(p)}$ obtained with the subspaces of the (partial) spread. Moreover, from spreads one obtains not only bent functions between elementary abelian groups, but bent functions from $\mathbb{V}_{2m}^{(p)}$ to B, where B can be any abelian group of order p^k, $k \le m$. As recently shown (Meidl, Pirsic 2021), partitions from spreads are not the only partitions of $\mathbb{V}_{2m}^{(2)}$, with these remarkable properties. In this article we present first such partitions—other than (partial) spreads—which we call bent partitions, for $\mathbb{V}_{2m}^{(p)}$, p odd. We investigate general properties of bent partitions, like number and cardinality of the subsets of the partition. We show that with bent partitions we can construct bent functions from $\mathbb{V}_{2m}^{(p)}$ into a cyclic group $\mathbb{Z}_{p^k}$. With these results, we obtain the first constructions of bent functions from $\mathbb{V}_{2m}^{(p)}$ into $\mathbb{Z}_{p^k}$, p odd, which provably do not come from (partial) spreads.

Keywords Bent function · Difference set · Partial spread · Partition · Relative difference set · Vectorial bent function · $\mathbb{Z}_{p^k}$-bent function

Mathematics Subject Classification 06E30 · 05B10 · 94C10

1 Introduction

Boolean bent functions, introduced by Rothaus in [34] attract a lot of attention since several decades (see [2]), due to applications in coding and cryptography—they are the functions of furthest distance from the set of affine functions—and due to rich connections to objects from geometry and combinatorics. In [19], the concept of bent functions has been gener-

Communicated by A. Pott.

✉ Nurdagül Anbar
nurdagulanbar2@gmail.com

Wilfried Meidl
meidlwilfried@gmail.com

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

Published online: 15 March 2022

alized to p-ary functions, i.e., to functions from an n-dimensional vector space $\mathbb{V}_n^{(p)}$ over the prime field $\mathbb{F}_p$ to $\mathbb{F}_p$. Meanwhile, many constructions of bent functions are known, like the Maiorana-McFarland construction and the partial spread construction, and numerous secondary constructions, i.e., constructions of bent functions from known bent or related functions.

The most powerful construction seems to be the construction via (partial) spreads, which for the Boolean case has already been studied comprehensively in Dillon's thesis [9]. The generalization of the (partial) spread construction to p-ary functions is then given in [15, 21]. The construction for the Boolean case (with a complete spread) can be described as follows:

Let $\mathcal{S}$ be a spread of $\mathbb{V}_{2m}^{(2)}$, i.e., a collection of $2^m + 1$ subspaces of $\mathbb{V}_{2m}^{(2)}$, each of dimension m, which pairwise intersect trivially. The union of 2^{m-1} of subspaces from $\mathcal{S}$, the 0-element excluded, is the support $supp(f)$ of a Boolean bent function f, where $supp(f) = \{x \in \mathbb{V}_{2m}^{(2)} : f(x) = 1\}$. Likewise, the union of $2^{m-1} + 1$ of subspaces from $\mathcal{S}$ (with the 0 element), is the support of a bent function. For more details, we refer to Sect. 2.

As shown in [14,Theorem 2], with the Desarguesian spread, one obtains exponentially many pairwise inequivalent Boolean bent functions. Furthermore, differently from other constructions, with (partial) spreads one can generate bent functions from $\mathbb{V}_{2m}^{(2)}$ (respectively $\mathbb{V}_{2m}^{(p)}$) into arbitrary abelian groups of order 2^k (respectively p^k), $k \le m$. For the definition of bent functions between arbitrary abelian groups, we refer to Sect. 2.

Very recently, in the paper [26], the second author and Pirsic showed that spreads are not the only partitions of $\mathbb{V}_{2m}^{(2)}$ with these remarkable properties. (The main objective in [26] has been to construct bent functions from $\mathbb{V}_n^{(2)}$ into the cyclic group $\mathbb{Z}_{2^k}$ which do not come from the partial spread construction.) A class of partitions is constructed, for which the union of a fixed number of its elements is again always the support of a Boolean bent function. The partitions in [26] can be seen as a generalization of the Desarguesian spread, in fact, the Desarguesian spread is a special case.

Motivated by the construction of the partitions of $\mathbb{V}_{2m}^{(2)}$ in [26], we introduce the new concept of *bent partitions*, roughly speaking as partitions of $\mathbb{V}_{2m}^{(p)}$, which have similar properties as (partial) spreads, with respect to the construction of bent functions. Exact definitions are provided in Sect. 3. As we believe, bent partitions are quite significant objects, (partial) spreads are examples, but, as we now know, not the only ones—at least not for characteristic 2.

This article is organized as follows. In Sect. 2, we first recall some basics on bent functions. Then we discuss in detail the construction of bent functions from spreads and partial spreads, and from the partitions presented in [26]. This detailed discussion is fundamental for understanding the significance of the concept of bent partitions, which we introduce in Sect. 3. We analyse general properties of bent partitions, such as the number of the subsets in the partition, properties of their subsets, like the cardinality, and properties of the resulting bent functions. In Sect. 4, we point out that vectorial bent functions, and most notably, bent functions from $\mathbb{V}_n^{(p)}$ to cyclic groups $\mathbb{Z}_{p^k}$ can be constructed from bent partitions of $\mathbb{V}_n^{(p)}$. As a major result, in Sect. 5 we present the first bent partitions of $\mathbb{V}_n^{(p)}$ for odd primes p, which do not arise from any (partial) spread. This also yields the first bent functions from $\mathbb{V}_n^{(p)}$ into a cyclic group $\mathbb{Z}_{p^k}$, p odd, different from (partial) spread functions. To show that the partitions we obtain for odd characteristic do not arise from any (partial) spread, hence are new, we generalize a classical result by Dillon [9] on the algebraic degree of Boolean partial spread bent functions to odd characteristic. Finally, motivated by the connection between Boolean bent functions and Hadamard difference sets, we introduce the concept of difference set partitions, and we give some perspectives for future research.

2 Preliminaries

In this preliminaries, after providing the necessary background on bent functions, we recall in detail the very powerful construction of bent functions based on (partial) spreads of $\mathbb{V}_n^{(p)}$, $n = 2m$. We then describe a main result from [26] on bent functions obtained from partitions of $\mathbb{F}_{2^m} \times \mathbb{F}_{2^m}$, which have properties similar to spreads. This detailed analysis of bent constructions obtained from these classes of partitions is crucial to capture the significance of the concept of bent partitions, which we will introduce in Sect. 3.

Let $(A, +_A)$, $(B, +_B)$ be finite abelian groups. A function f from A to B is called a *bent function* if

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

for every character χ of $A \times B$ which is nontrivial on B. Alternatively, $f : A \to B$ is bent if and only if for all nonzero $a \in A$, the function $D_a f(x) = f(x +_A a) -_B f(x)$ is balanced, i.e., every value in B is taken on the same number $|A|/|B|$ of times. The graph of f, $G = \{(x, f(x)) : x \in A\}$, is then a relative difference set in $A \times B$ relative to B, see [32]. For background on relative difference sets we refer to [33].

In the classical case, $A = \mathbb{V}_n^{(p)}$ and $B = \mathbb{V}_m^{(p)}$ are elementary abelian p-groups, i.e., they are vector spaces of dimension n and m respectively over the prime field $\mathbb{F}_p$ for some prime p. In this case the character sum in (1), called *Walsh transform* of f at $(a, b) \in \mathbb{V}_m^{(p)} \times \mathbb{V}_n^{(p)}$, $a \neq 0$, is of the form

$$\mathcal{W}_f(a, b) = \sum_{x \in \mathbb{V}_n^{(p)}} \epsilon_p^{\langle a, f(x)\rangle_m \ominus \langle b, x\rangle_n},$$

where $\langle , \rangle_k$ denotes an inner product in $\mathbb{V}_k^{(p)}$, ϵ_p is a primitive p-th root of unity, and $\oplus$ (respectively $\ominus$) denotes the addition (respectively subtraction) modulo p. If $\mathbb{V}_k^{(p)} = \mathbb{F}_p^k$, we may use the conventional dot product as inner product. If $\mathbb{V}_k^{(p)} = \mathbb{F}_{p^k}$, the finite field of order p^k, we may use the absolute trace $\mathrm{Tr}_k(bx)$ as the inner product $\langle b, x\rangle_k$. A function $f : \mathbb{V}_n^{(p)} \to \mathbb{V}_m^{(p)}$ is bent, if $m > 1$ also called *vectorial bent*, if and only if $|\mathcal{W}_f(a, b)| = p^{n/2}$ for all nonzero $a \in \mathbb{V}_m^{(p)}$ and $b \in \mathbb{V}_n^{(p)}$. If $p = 2$, then $\epsilon_2 = -1$, hence $\mathcal{W}_f(a, b)$ is an integer, and for a bent function we have $\mathcal{W}_f(a, b) = \pm 2^{n/2}$. Therefore, (vectorial) bent functions from $\mathbb{V}_n^{(2)}$ to $\mathbb{V}_m^{(2)}$ only exist for even dimensions n. Furthermore, by Nyberg's bound [30], m can be at most $n/2$. For odd p, (vectorial) bent functions exist for integers n, even and odd, and $m \leq n$.

Bent functions from $\mathbb{V}_n^{(p)}$ to $\mathbb{F}_p$ are also called *p -ary bent functions*, and *Boolean bent functions* if $p = 2$. The Walsh transform is then of the form

$$\mathcal{W}_f(1, b) = \mathcal{W}_f(b) = \sum_{x \in \mathbb{V}_n^{(p)}} \epsilon_p^{f(x) \ominus \langle b, x\rangle_n}.$$

(We remark that the coefficient $a \in \mathbb{F}_p^*$ of f in the exponent is w.l.o.g. set to $a = 1$, as with f also af, $a \in \mathbb{F}_p^*$, is bent.) In the Boolean case, $\mathcal{W}_f(b) = 2^{n/2}(-1)^{f^*(b)}$ for a Boolean function f^*, called the *dual* of f. For p-ary bent functions f from $\mathbb{V}_n^{(p)}$ to $\mathbb{F}_p$, p odd, the

Walsh coefficient $\mathcal{W}_f(b)$ at $b \in \mathbb{V}_n^{(p)}$ of f always satisfies (see [11, 19])

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

where i is a complex primitive 4-th root of unity, and f^* is a function from $\mathbb{V}_n^{(p)}$ to $\mathbb{F}_p$, which again is called the dual of f.

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 $\mathcal{W}_f(b) = \zeta\ \epsilon_p^{f^*(b)} p^{n/2}$ for some $\zeta \in \{\pm 1, \pm i\}$, cf. Equation (2). If $\zeta = 1$, we call f *regular*, which trivially applies if $p = 2$. If (the sign of) ζ 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. In particular, the dual of a Boolean bent function is always bent. A non-weakly regular bent function can be either dual-bent or *non-dual-bent*, see [5, 6].

For a vectorial function $f : \mathbb{V}_n^{(p)} \to \mathbb{V}_m^{(p)}$ and a nonzero element $a \in \mathbb{V}_m^{(p)}$, the function $f_a : \mathbb{V}_n^{(p)} \to \mathbb{F}_p$ given as $f_a(x) = \langle a, f(x)\rangle_m$ is called a *component function* of f. Observe that f is a vectorial bent function if and only if all component functions are bent. Hence, adding the 0-function, we can see a vectorial bent function as an m-dimensional vector space of p-ary (Boolean) bent functions.

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

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

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

The class of functions satisfying 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*, which meanwhile is quite intensively studied in the literature. Several results on generalized bent functions point to connections with partitions of $\mathbb{V}_n^{(p)}$, see [23, 27, 28].

Satisfying only a much weaker condition, generalized bent functions (in general) do not yield relative difference sets. However, in the research on bent functions into the cyclic group they play an important role, since $f : \mathbb{V}_n^{(p)} \to \mathbb{Z}_{p^k}$ is bent if and only if $p^t f$ is generalized bent for every t, $0 \le t \le k - 1$, see for instance [12].

Many of the classical examples and constructions of Boolean and p-ary bent functions also have a vectorial version, i.e., yield also vectorial bent functions, see [7]. 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".

Among the many classical constructions, it seems it is only the partial spread construction that can produce bent functions that map into the cyclic group, and moreover (based on a spread of $\mathbb{V}_{2m}^{(p)}$), bent functions from $\mathbb{V}_{2m}^{(p)}$ into arbitrary abelian groups of order p^k, $k \le m$. Only recently, the first examples of bent functions from $\mathbb{V}_n^{(2)}$ to $\mathbb{Z}_{2^k}$ have been found, which do not come from the ubiquitous spread construction, see the discussion below.

In the remainder of this section, we describe in detail bent constructions obtained from spreads, partial spreads, and the partition presented in [26].

First recall that a partial spread $\mathcal{S}$ of $\mathbb{V}_n^{(p)}$, $n = 2m$, is a set of m-dimensional subspaces of $\mathbb{V}_n^{(p)}$, which pairwise intersect trivially. If $|\mathcal{S}| = p^m + 1$, hence every nonzero element of

$\mathbb{V}_n^{(p)}$ is in exactly one of those subspaces, then $\mathcal{S}$ is called a (complete) spread. 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 $s \in \mathbb{F}_{p^m}$, $U_s = \{(x, sx) \, : \, x \in \mathbb{F}_{p^m}\}$.

Construction with a spread 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 $c \in B$.

From the spread construction one obtains a large variety of bent functions into various abelian groups. In [14,Theorem 2], a lower bound on the number of pairwise inequivalent Boolean bent functions obtained with the Desarguesian spread of $\mathbb{V}_n^{(2)}$ is shown. By this bound, the number of pairwise inequivalent Desarguesian spread Boolean bent functions grows exponentially with n. One can infer from Theorem 1 in [14] similar results for odd p. We remark that a weaker bound on this number for arbitrary spreads is given in [15,Corollary 2.9] (see also [15,Remark 4]).

Construction with a partial spread We restrict ourselves to the case that $p = 2$, the case of odd p is similar. The proofs for Construction I and Construction II below, are in [26], following the approach in [21] for p-ary bent functions from partial spreads, p odd.

CONSTRUCTION I

For some k, $1 \le k \le m$, let $\mathcal{S} = \{U_j, \ 1 \le j \le (2^k - 1)2^{m-k}\}$ be a partial spread of $\mathbb{V}_n^{(2)}$, $n = 2m$, and B an abelian group of order 2^k. We define $f : \mathbb{V}_n^{(2)} \to B$ as follows.

- Every nonzero element γ of B has as preimage the union of exactly 2^{m-k} elements of $\mathcal{S}$ except from $0 \in \mathbb{V}_n^{(2)}$, i.e., $f^{-1}(\gamma) = \bigcup_{i=1}^{2^{m-k}} U^*_{\gamma,i}$, where $U_j^* = U_j \setminus \{0\}$.
- All other elements are mapped to $0 \in B$, i.e., $f^{-1}(0) = \mathbb{V}_n^{(2)} \setminus \bigcup_j U_j^*$.

CONSTRUCTION II

For some k, $1 \le k \le m$, let $\mathcal{S} = \{U_j, \ 1 \le j \le (2^k - 1)2^{m-k} + 1\}$ be a partial spread of $\mathbb{V}_n^{(2)}$ and B an abelian group of order 2^k. We define $f : \mathbb{V}_n^{(2)} \to B$ as follows.

- All elements which are not in U_j for all $1 \le j \le (2^k - 1)2^{m-k} + 1$ are w.l.o.g mapped to $0 \in B$, i.e., $f^{-1}(0) = \mathbb{V}_n^{(2)} \setminus \bigcup_j U_j$.
- For an element $\tilde{\gamma} \in B^*$ we have $g^{-1}(\tilde{\gamma}) = \bigcup_{i=1}^{2^{m-k}+1} U_{\tilde{\gamma},i}$, i.e., $\tilde{\gamma}$ has the union of $2^{m-k} + 1$ elements of a partial spread as preimage (note that also $f(0) = \tilde{\gamma}$).
- If $\gamma \in B^*$, $\gamma \neq \tilde{\gamma}$, then $g^{-1}(\gamma) = \bigcup_{i=1}^{2^{m-k}} U^*_{\gamma,i}$, i.e., the preimage of γ consists of the nonzero elements of 2^{m-k} elements of a partial spread.

Though from (partial) spreads we can obtain bent functions from elementary abelian groups into various abelian groups, mostly Boolean partial spread bent functions, as already introduced in Dillon's thesis [9], are considered in the literature. Since bent partitions will be defined via Boolean (and p-ary) bent functions, we review this important special case.

PS^- BOOLEAN BENT FUNCTIONS AND THEIR COMPLEMENT. A Boolean function f from $\mathbb{V}_n^{(2)}$ to $\mathbb{F}_2$, $n = 2m$, of which the support, $supp(f) = \{x \in \mathbb{V}_n^{(2)} \ : \ f(x) = 1\}$, is the union of 2^{m-1} elements of a (partial) spread, with the 0 excluded, is called a PS^- bent function. The complement $g = f + 1$ of a PS^- bent function is then a bent function for which exactly the nonzero elements of 2^{m-1} elements of a (partial) spread are mapped to 0. The bent functions in Construction I above for $k=1$, are PS^- bent functions.

PS^+ Boolean bent functions and their complement. A Boolean function f from $\mathbb{V}_n^{(2)}$ to $\mathbb{F}_2$, $n=2m$, of which the support is the union of $2^{m-1}+1$ elements of a (partial) spread (the 0 is now included), is called a PS^+ bent function. A Boolean bent function f obtained with Construction II when $k=1$, is a PS^+ bent function, since w.l.o.g., the elements which are not in one of the subspaces of the spread are mapped to 0 (hence $\tilde{\gamma}=1$). If we choose the other way round, then f is the complement of a PS^+ bent function.

Observe that the complement of a PS^- bent function defined with a partial spread which is a part of a complete spread, is a PS^+ bent function (and vice versa).

Finally we also describe the partial spread versions for p-ary functions, see [15, 21].

p-ary PS^- bent functions from $\mathbb{V}_n^{(p)}$ to $\mathbb{F}_p$, $n=2m$, are the functions with the following property: Every nonzero element of $\mathbb{F}_p$ has the union of p^{m-1} subspaces, without the 0, as the preimage set. All other elements are mapped to 0. Observe that this requires a partial spread with at least $(p-1)p^{m-1}$ subspaces.

p-ary PS^+ bent functions from $\mathbb{V}_n^{(p)}$ to $\mathbb{F}_p$, $n=2m$, are the functions with the following property: 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 $\mathbb{V}_n^{(p)}$ are mapped to 0. Note that a partial spread with at least $(p-1)p^{m-1}+1$ subspaces is required.

Until very recently, the (partial) spread construction has been the only construction which yields also bent functions into the cyclic group $\mathbb{Z}_{p^k}$, $k\ge 3$. In [26], a construction of bent functions from $\mathbb{V}_n^{(2)}$ to $\mathbb{Z}_{2^k}$ is proposed, which is based on partitions Γ_1,Γ_2 of $\mathbb{F}_{2^m}\times\mathbb{F}_{2^m}$, which have similar properties as a spread of $\mathbb{F}_{2^m}\times\mathbb{F}_{2^m}$.

The construction in [26] Let m,k be integers such that k divides m and $\gcd(2^m-1,2^k+1)=1$, let $e=2^k+1$ and d such that $de\equiv 1 \bmod 2^m-1$. For an element $s\in\mathbb{F}_{2^m}$ define

$$U_s := \{(x, sx^e)\ :\ x\in\mathbb{F}_{2^m}\},\ U_s^* = U_s\setminus\{(0,0)\},\ \text{and}\ U=\{(0,y)\ :\ y\in\mathbb{F}_{2^m}\}.$$

Then U, U_s^*, $s\in\mathbb{F}_{2^m}$, form a partition of $\mathbb{F}_{2^m}\times\mathbb{F}_{2^m}$.

Similarly, for an element $s\in\mathbb{F}_{2^m}$ we define

$$V_s := \{(x^d s, x)\ :\ x\in\mathbb{F}_{2^m}\},\ V_s^* = V_s\setminus\{(0,0)\},\ \text{and}\ V=\{(x,0)\ :\ x\in\mathbb{F}_{2^m}\}.$$

For the divisor k of m and an element γ of $\mathbb{F}_{2^k}$ let

$$\mathcal{A}(\gamma)=\bigcup_{\substack{s\in\mathbb{F}_{2^m}\\ \mathrm{Tr}_k^m(s)=\gamma}} U_s^* \quad\text{and}\quad \mathcal{B}(\gamma)=\bigcup_{\substack{s\in\mathbb{F}_{2^m}\\ \mathrm{Tr}_k^m(s)=\gamma}} V_s^*.$$

With these definitions we obtain two partitions of $\mathbb{F}_{2^m}\times\mathbb{F}_{2^m}$,

$$\Gamma_1=\{U,\mathcal{A}(\gamma);\ \gamma\in\mathbb{F}_{2^k}\}$$
$$\Gamma_2=\{V,\mathcal{B}(\gamma);\ \gamma\in\mathbb{F}_{2^k}\},$$

into 2^k+1 subsets, that have similar properties as spreads have. In fact, for $k=m$, both partitions reduce to the Desarguesian spread.

Remark 1 In [26], the partitions Γ_1,Γ_2 are introduced slightly different, as there e is set as $e=2^m-2^k-2$, and therefore (modulo 2^m-1) $-e=2^k+1$. Hence, in [26] U_s and V_s are represented as $U_s=\{(x,sx^{-e})\ :\ x\in\mathbb{F}_{2^m}\}$ and $V_s=\{(x^{-d}s,x)\ :\ x\in\mathbb{F}_{2^m}\}$.

Theorem 1 [26] *Let m, k be integers such that k divides m and* $\gcd(2^m - 1, 2^k + 1) = 1$, *and let U, $\mathcal{A}(\gamma)$, V, $\mathcal{B}(\gamma)$ be defined as above.*

I. *Every Boolean function of which the support is the union of 2^{k-1} of the sets $\mathcal{A}(\gamma)$ is a bent function. Likewise, their complements, i.e., the Boolean functions with U and 2^{k-1} of the sets $\mathcal{A}(\gamma)$ as their support, are bent.*

II. *Every Boolean function of which the support is the union of 2^{k-1} of the sets $\mathcal{B}(\gamma)$ is a bent function. Likewise the Boolean functions with V and 2^{k-1} of the sets $\mathcal{B}(\gamma)$ as their support, are bent.*

The duals of the bent functions of the class in I are in the class in II (and vice versa).

As for spreads, we also obtain bent functions from $\mathbb{V}_n^{(2)}$ into various abelian groups B, in particular into cyclic groups.

Theorem 2 [26] *Let m, k be integers such that k divides m and* $\gcd(2^m - 1, 2^k + 1) = 1$, *and let $\pi(i) = \gamma_i$ be a one-to-one map from $\mathbb{Z}_{2^k}$ to $\mathbb{F}_{2^k}$. Then the function $f : \mathbb{F}_{2^m} \times \mathbb{F}_{2^m} \to \mathbb{Z}_{2^k}$ given as*

- $f(x, y) = i$ *if* $(x, y) \in \mathcal{A}(\gamma_i)$ $((x, y) \in \mathcal{B}(\gamma_i))$,
- $f(0, y) = 0$ w.l.o.g. $(f(x, 0) = 0$ w.l.o.g.$)$ *for all* $y \in \mathbb{F}_{2^m}$ $(x \in \mathbb{F}_{2^m})$,

is a $\mathbb{Z}_{2^k}$-bent function.

With an argument via the algebraic degree, it is shown in [26] that the bent functions in Theorems 1, 2 do not come from the (partial) spread construction if $k < m$. For $k = m$, the partitions Γ_1, Γ_2 reduce to the Desarguesian spread.

3 Bent partitions of elementary abelian groups

Motivated by the observations in the previous section, we introduce a class of partitions of an elementary abelian p-group $\mathbb{V}_n^{(p)}$, which possess similar properties as partitions from spreads.

Definition 1 For an integer K divisible by p, let $\Omega = \{A_1, \ldots, A_K\}$ be a partition of $\mathbb{V}_n^{(p)}$. Suppose that every function for which every $c \in \mathbb{F}_p$ has exactly K/p of sets A_j in Ω in its preimage, is a p-ary bent function. Then we call Ω a bent partition of $\mathbb{V}_n^{(p)}$ of depth K.

Example 1 Let $\mathcal{S} = \{U_0, U_1, \ldots, U_{p^m}\}$ be a spread of $\mathbb{V}_n^{(p)}$, $n = 2m$. W.l.o.g. we set $A_1 = U_0 \cup U_1$ and $A_j = U_j^*, 2 \le j \le p^m$. Then $\{A_1, \ldots, A_{p^m}\}$ is a bent partition of $\mathbb{V}_n^{(p)}$. Observe that we can obtain $\binom{p^m+1}{2}$ bent partitions from a spread of $\mathbb{V}_n^{(p)}$.

Example 2 From a partial spread of $\mathbb{V}_n^{(2)}$ with $(2^k - 1)2^{m-k}$ subspaces, as used also for Construction I in the previous section, we get a bent partition $\Omega = \{A_1, A_2, \ldots, A_{2^k}\}$ of $\mathbb{V}_n^{(2)}$ as follows: A_j, $2 \le j \le 2^k$, is the union of 2^{m-k} elements of the partial spread—the 0-element excluded. The remaining elements form A_1.

Note that then $|A_j| = (2^m - 1)2^{m-k}$ for $2 \le j \le 2^k$, and $|A_1| = 2^m + |A_j|$ $(2 \le j \le 2^k)$.

We observe that a Boolean function that maps exactly half of the sets in Ω to 1 (the other to 0), is a partial spread bent function. It is a PS^- bent function if A_1 is mapped to 0, otherwise it is the complement of a PS^- bent function.

Example 3 From a partial spread of $\mathbb{V}_n^{(2)}$ with $(2^k - 1)2^{m-k} + 1$ elements, as used also for Construction II in the previous section, we get the following bent partitions $\Omega = \{A_1, A_2, \dots, A_{2^k}\}$ of $\mathbb{V}_n^{(2)}$: A_1 is the union of $2^{m-k} + 1$ elements of the partial spread, including 0, A_j, $3 \le j \le 2^k$ is the union of 2^{m-k} of them, the remaining elements of $\mathbb{V}_n^{(2)}$ form A_2.

The cardinalities of the sets A_j are as in Example 2.

As easily observed, again a Boolean function f that maps exactly half of the sets in Ω to 1, is a partial spread bent function. If both (none of), A_1 and A_2 are mapped to 0, then f is a PS^- bent function (the complement of a PS^- bent function), if A_1 is mapped to 1 and A_2 to 0 (A_1 is mapped to 0 and A_2 to 1), then f is a PS^+ bent function (the complement of a PS^+ bent function).

Example 4 For a divisor k of m with $\gcd(2^m - 1, 2^k + 1) = 1$, consider the partition $\Gamma_1 = \{U, \mathcal{A}(\gamma); \gamma \in \mathbb{F}_{2^k}\}$ of $\mathbb{F}_{2^m} \times \mathbb{F}_{2^m}$ given as above. Let $A_1 = U \cup \mathcal{A}(0)$, w.l.o.g. (we may pick any other $\mathcal{A}(\gamma)$ for $\mathcal{A}(0)$ - 2^k choices). Then $\Omega = \{A_1, \mathcal{A}(\gamma); \gamma \in \mathbb{F}_{2^k}^*\}$ is a bent partition of $\mathbb{F}_{2^m} \times \mathbb{F}_{2^m}$. Similarly we obtain bent partitions from Γ_2.

We recall that for $k = m$ both partitions, Γ_1 and Γ_2, reduce to the Desarguesian spread. When $k < m$ the partitions do not come from any (partial) spread at all. For integers m with several divisors, several constructions of bent partitions of $\mathbb{F}_{2^m} \times \mathbb{F}_{2^m}$ emerge.

Our first objective is to determine the possible cardinalities of the sets in a bent partition. We therefore recall a result of Nyberg that gives the value distribution of a bent function, see [29].

Lemma 1 *Let p be an odd prime and $f : \mathbb{V}_n^{(p)} \mapsto \mathbb{F}_p$ a bent function. For $\ell \in \mathbb{F}_p$, we set $b_\ell = |f^{-1}(\ell)|$, where $f^{-1}(\ell) = \{x \in \mathbb{V}_n^{(p)} \ : \ f(x) = \ell\}$.*

(i) *If n is even, then there exists 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.*

(ii) *If n is odd, then $b_0 = p^{n-1}$ 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 $\ell \in \mathbb{F}_p \setminus \{0\}$, where $\left(\frac{*}{*}\right)$ is the Legendre symbol.*

Theorem 3 *Let $\Omega = \{A_1, \dots, A_K\}$ be a bent partition of $\mathbb{V}_n^{(p)}$. Then the following holds.*

(i) *n must be an even integer.*

(ii) *Besides from one set, without loss of generality the set A_1, all sets A_j have the same cardinality, namely*

$$|A_j| = \frac{p^{n/2}(p^{n/2} \mp 1)}{K}, 2 \le j \le K, \text{ and}$$

$$|A_1| = \frac{p^{n/2}(p^{n/2} \mp 1)}{K} \pm p^{n/2}.$$

(iii) *If $p = 2$ then $K \le 2(2^{n/2} \mp 1)$, and $|A_j| \ge 2^{n/2-1}$. For odd p we have $K \le 2p^{n/2} - p$, and $|A_j| \ge \frac{p^{n/2}+1}{2}$.*

Proof (i) Trivially, n must be even if $p = 2$. In the case of odd p and odd n, by Lemma 1(ii), the cardinality b_ℓ depends whether ℓ is a quadratic residue modulo p or not. However, once we choose the sets of a preimage partition for a bent function as unions of the sets A_j, by the definition of a bent partition, we may arbitrarily assign which set shall be mapped to which value. This contradicts the fact that for odd n, the cardinality of the preimage set of ℓ depends on properties of ℓ.

(ii) We use the fact that the preimage sets of a bent function in even dimension n attain exactly two different cardinalities, $2^{n-1} \pm 2^{n/2-1}$ in the Boolean case, the two cardinalities for p odd are given in Lemma 1(i). Consequently, any union of K/p sets of $\{A_1, A_2, \ldots, A_K\}$ must have one of the two cardinalities (and both cardinalities appear). It is easily seen that this applies if and only if all sets A_j have the same cardinality, except from one, w.l.o.g. A_1.

First suppose that $|A_1| > |A_j|$, $2 \leq j \leq K$. Then for $p = 2$, any union of half of the sets A_j, which does not in include A_1, has cardinality $2^{n-1} - 2^{n/2-1}$. Consequently, $|A_j| = (2^n - 2^{n/2})/K, 2 \leq j \leq K$. A union of $K/2$ of the sets $|A_j|$ which includes A_1 has cardinality $2^{n-1} + 2^{n/2-1}$. Therefore $|A_1| = |A_j| + 2^{n/2}$ $(j \neq 1)$.

If on the other hand $|A_1| < |A_j|$, $2 \leq j \leq K$, then with the same argument we see that $|A_j| = (2^n + 2^{n/2})/K, 2 \leq j \leq K$, and $|A_1| = |A_j| - 2^{n/2}$ $(j \neq 1)$.

Similarly for odd p, the union of K/p sets A_j has cardinality $p^{n-1} \mp p^{n/2-1}$ if it does not include A_1, and cardinality $p^{n-1} \pm (p-1)p^{n/2-1}$ if it does include A_1. With the same arguments as for $p = 2$, we infer the claimed cardinalities for A_1 and A_j, $2 \leq j \leq K$.

(iii) We recall that the distance between two bent functions $f, g : \mathbb{V}_n^{(p)} \to \mathbb{F}_p$ is at least $p^{n/2}$, see [17], Proposition 1 in [18], and [31] for odd p (and even n). Exchanging two sets A_{j_1} and A_{j_2} in the preimages of c_1 and c_2 we get two bent functions f, g with distance $d(f, g) = 2|A_j| = 2\frac{p^{n/2}(p^{n/2} \mp 1)}{K} \geq p^{n/2}$, and $K \leq 2(p^{n/2} \mp 1)$, $|A_j| \geq p^{n/2}/2$ follows. The value for $|A_j|$ for odd p is imposed by $|A_j|$ being an integer. Since p must divide K, the values for K follow. □

Remark 2 For all our examples of bent partitions we have $|A_1| > |A_j|, 2 \leq j \leq K$, and K is always a power of p. Note that K must divide $p^{n/2}(p^{n/2} \pm 1)$. The question of the existence of bent partitions with other values of K, or of the bent partitions for which one of the sets in the partition is smaller than the other sets is open.

Remark 3 For a bent partition obtained from a complete spread, we have $K = p^{n/2}$ and $|A_j| = p^{n/2} - 1, 2 \leq j \leq K$. One may expect that in fact this is the largest possible value for K, respectively the smallest possible value for $|A_j|$.

In the light of Theorem 3, from now on we suppose that n is even.

Observe that for the partitions Γ_1 and Γ_2, the subgroups U and V play a special role, see Eq. (6). In a corresponding bent partition described as in Example 4, together with an arbitrary $\mathcal{A}_j$ (respectively $\mathcal{B}_j$), they form the set A_1 with the larger cardinality. In this way, several bent partitions (precisely p^k) can be obtained from Γ_1 respectively Γ_2 (note that with a spread one has even more freedom, as A_1 is the union of two arbitrary subspaces). These observations motivate to refine the definition of a bent partition as follows.

Definition 2 Let $\Omega = \{U, A_1, \ldots, A_K\}$ be a partition of $\mathbb{V}_n^{(p)}$. Suppose that every function with the following properties is bent:

I Every $c \in \mathbb{F}_p$ has exactly K/p of the sets $A_1, \ldots, A_K$ in its preimage set,
II $f(x) = c_0$ for all $x \in U$ and some fixed $c_0 \in \mathbb{F}_p$.

Then we call Ω a normal bent partition of $\mathbb{V}_n^{(p)}$ of depth K.

Remark 4 Recall that a bent function $f : \mathbb{V}_n^{(p)} \to \mathbb{F}_p$ is called *normal* if there exists an $n/2$-dimensional subspace U of $\mathbb{V}_n^{(p)}$ on which f is constant, see [1, 8, 25]. By Theorem 4(ii) below, every bent function obtained from a normal bent partition is a normal bent function.

Similar as Theorem 3 for bent partitions, Theorem 4 below presents the possible cardinalities for the sets in a normal bent partition.

Theorem 4 *Let $\Omega = \{U, A_1, \ldots, A_K\}$ be a normal bent partition of $\mathbb{V}_n^{(p)}$. Then p divides K, and*

(i) $|U| = p^{n/2}$ *and* $|A_j| = \frac{p^{n/2}(p^{n/2}-1)}{K}$, $1 \le j \le K$,
(ii) *U is an affine subspace of $\mathbb{V}_n^{(p)}$, $K \le 2p^{n/2} - p$, and $|A_j| \ge 2^{n/2-1}$ if $p = 2$ and $|A_j| \ge \frac{p^{n/2}+1}{2}$ if p is odd.*

Proof (i) We can order the sets A_j so that we have

$$|A_1| \le |A_2| \le \cdots \le |A_{K-1}| \le |A_K|.$$

Suppose that the cardinalities of the sets A_j are not all the same, i.e., we have $\sum_{j=0}^{K/2} |A_j| < \sum_{j=K/2+1}^{K} |A_j|$.

We first consider the case that $p = 2$. Since any union of $K/2$ of the sets A_j, $1 \le j \le K$, forms the support of a bent function we have

$$\sum_{j=0}^{K/2} |A_j| = 2^{n-1} - 2^{n/2-1} \quad \text{and} \quad \sum_{j=K/2+1}^{K} |A_j| = 2^{n-1} + 2^{n/2-1}. \tag{3}$$

By the definition of a normal bent partition, also $U \cup \bigcup_{j=K/2+1}^{K} A_j$ is the support of a bent function f. However, by Eq. (3), we then have $|supp(f)| > 2^{n-1} + 2^{n/2-1}$, which is a contradiction. Therefore, $|A_i| = |A_j|$ for any $i, j \in \{1, \ldots, K\}$. Since $\bigcup_{j=1}^{K/2} A_j$ and $U \cup \bigcup_{j=1}^{K/2} A_j$, both form the support of bent functions, we conclude that $|U| = 2^{n/2}$, hence $|A_j| = (2^n - 2^{n/2})/K$ for all $j = 1, \ldots, K$.

A similar argument applies for odd p. Let f be a p-ary bent function f obtained from a normal bent partition. By Lemma 1(i), $b_c = p^{n-1} \pm (p-1)p^{\frac{n}{2}-1}$ for a unique $c \in \mathbb{F}_p$ and $b_\ell = p^{n-1} \mp p^{\frac{n}{2}-1}$ for all $\ell \in \mathbb{F}_p \setminus \{c\}$. By the definition of a normal bent partition, U must be mapped to c, $b_c > b_\ell$, hence $|U| = b_c - b_\ell = p^{\frac{n}{2}}$. Furthermore, as any union of K/p sets A_j can be the preimage of an element ℓ, we must have $|A_1| = |A_2| = \cdots = |A_k|$, and the claim for the cardinalities follows.

(ii) The bounds on K and A_j are given in Theorem 3(iii). By the definition of a normal bent partition Ω we can obtain bent functions f, g which only differ on the set U of cardinality $p^{n/2}$. Then f and g have the minimal possible distance between bent functions, and U must be an affine subspace of $\mathbb{V}_n^{(p)}$, see [17], Proposition 1 in [18], and [31] for odd p. □

All bent functions obtained from a (partial) spread of $\mathbb{V}_n^{(p)}$ are regular bent functions, see [21]. The following corollary of Theorem 4 indicates that this is the situation for any normal bent partition.

Corollary 1 *All bent functions constructed from a normal bent partition of $\mathbb{V}_n^{(p)}$ are regular or non-weakly regular.*

Proof Boolean bent functions are always regular, hence we have to consider the case of p odd. From the cardinalities given in Theorem 4, we see that for a bent function f obtained from a normal bent partition we have $\mathcal{W}_f(0) = \sum_{\ell \in \mathbb{F}_p} |f^{-1}(\ell)|\epsilon_p^\ell = p^{n/2}\epsilon_p^c$ if U is mapped to c. Hence if f is weakly regular then it is regular. □

Corollary 2 *Let $\Omega = \{A_1, A_2, \ldots, A_K\}$ be a bent partition of $\mathbb{V}_n^{(p)}$ and suppose that $|A_1| = p^{n/2} + |A_j|$, $2 \le j \le K$. Then Ω can be transformed into a normal bent partition $\Omega' = \{U, A_1', A_2, \ldots, A_K\}$ if and only if A_1 contains an $n/2$-dimensional subspace U.*

Proof Clearly, if A_1 does not contain an $n/2$-dimensional subspace U, then we cannot obtain such a normal bent partition Ω'. Suppose now that U is an $n/2$-dimensional subspace of A_1 and consider the partition Ω' (with $A_1' = A_1 \setminus U$). Observe that every potential bent function f obtained from Ω' is either a bent function obtained from Ω (if f takes on the same value on U and on A_1'), or a function that differs from a bent function obtained from Ω solely on the subspace U by a constant. Hence, by Proposition 1 in [18] for $p = 2$, and the analog result for odd p in [31], the function f is bent as well. Therefore Ω' is a normal bent partition. □

The Examples 1, 3, 4 of bent partitions obviously give rise to normal bent partitions. This may be different for Example 2, as the following immediate consequence of Corollary 2 points out.

Corollary 3 *The bent partition of $\mathbb{V}_n^{(2)}$ given in Example 2 cannot be altered to a normal bent partition if and only if the corresponding partial spread with $(2^k - 1)2^{m-k}$ subspaces is not included in a larger partial spread.*

We remark that it is difficult to construct a partial spread of a given size, which is not extendable to a larger partial spread, see for instance [16]. A potential construction of a partial spread from linear recurring sequences is in the recent article [10]. So far we do not know an example of a bent partition, which cannot be transformed into a normal bent partition, besides from the trivial example of the partition of $\mathbb{V}_n^{(2)}$ into two sets, the support of a Boolean bent function f, and its complement. This partition cannot be transformed into a (trivial) normal bent partition if and only if f is not normal.

4 Bent partitions, vectorial bent functions and $\mathbb{Z}_{p^k}$-bent functions

As pointed out in the preliminaries, with spreads and partial spreads one can generate bent functions from the elementary abelian group to abelian groups B (of some prime power cardinality). For the proof for partial spreads we refer to the preliminaries in [26]. In particular, bent functions mapping into cyclic groups $\mathbb{Z}_{p^k}$ can be obtained. The main objective in [26] has been to show the existence of bent functions into the cyclic group $\mathbb{Z}_{2^k}$, which do not come from the spread construction. From the construction found in [26], the partition of $\mathbb{F}_{2^m} \times \mathbb{F}_{2^m}$ in Example 4 emerged. In this section we point out that this is a general property for (normal) bent partitions. More precisely, as a main result, we will show that bent partitions of $\mathbb{V}_n^{(p)}$ of depth p^k yield bent functions from $\mathbb{V}_n^{(p)}$ to the cyclic group $\mathbb{Z}_{p^k}$.

We first show that vectorial bent functions arise from (normal) bent partitions. As all our concrete examples are potentially normal bent partitions, we state the result in terms of normal bent partitions. The argument applies in the same way also to bent partitions which are not normal.

Theorem 5 *Let $\Omega = \{U, A_1, \ldots, A_K\}$ be a normal bent partition of $\mathbb{V}_n^{(p)}$, and suppose that $K = p^k$. Then every function $F : \mathbb{V}_n^{(p)} \to \mathbb{V}_k^{(p)}$ such that every element $c \in \mathbb{V}_k^{(p)}$ has the elements of exactly one of the sets A_j, $1 \le j \le K$, in its preimage, and U is mapped to some element c_0, is a vectorial bent function.*

Proof It suffices to show that for every nonzero $v \in \mathbb{V}_k^{(p)}$ the component function $F_v(x) = \langle v, F(x)\rangle_k$ is a p-ary (Boolean) bent function. For $x \in A_j$ we have $F_v(x) = \langle v, c_j\rangle_k$ if F maps A_j to c_j. Since the inner product $\langle , \rangle_k$ on $\mathbb{V}_k^{(p)}$ is balanced, every element of $\mathbb{F}_p$ has exactly p^{k-1} of the sets A_j, $1 \le j \le K$, in its preimage. As F_v is also constant on U, by the definition of a bent partition, F_v is bent. □

Remark 5 Given a (normal) bent partition of depth $K = p^k H$ for some $H > 1$ not divisible by p (if exists), one of course can form many bent partitions of depth p^k by forming unions.

To show that a bent function from $\mathbb{V}_n^{(p)}$ into the cyclic group $\mathbb{Z}_{p^k}$ can be obtained from a bent partition with $K = p^k$, we recall that a function $f : \mathbb{V}_n^{(p)} \to \mathbb{Z}_{p^k}$ can be uniquely written as

$$f(x) = a_0(x) + a_1(x)p + \cdots + a_{k-1}(x)p^{k-1} \tag{4}$$

for some p-ary functions a_i, $0 \le i \le k-1$. The following lemma will be our essential tool.

Lemma 2 (i) *$f : \mathbb{V}_n^{(p)} \to \mathbb{Z}_{p^k}$ is bent if and only if $p^t f$ is generalized bent for every t, $0 \le t \le k-1$, see e.g.* [12].

(ii) [28] *$f : \mathbb{V}_n^{(p)} \to \mathbb{Z}_{p^k}$ given as in (4) is generalized bent if and only if every p-ary function of the form $a_{k-1}(x) \oplus C(x)$ is bent, where C is a p-ary function which is constant on the sets of the partition $\mathcal{P}_f = \{A(d) : 0 \le d \le p^{k-1} - 1\}$ with*

$$A(d) = \left\{x \in \mathbb{V}_n^{(p)} : \sum_{i=0}^{k-2} a_i(x)p^i = d\right\}. \tag{5}$$

Let $\Omega = \{U, A_0, \ldots, A_{p^k-1}\}$ be a normal bent partition of $\mathbb{V}_n^{(p)}$. By adding a constant to $f(x)$ and reordering the partition, we can without loss of generality suppose that $f(x) = j$ if $x \in A_j$ and $f(x) = 0$ if $x \in U$. With this convention we first show that f is a generalized bent function.

Proposition 1 *Let $\Omega = \{U, A_0, \ldots, A_{p^k-1}\}$ be a normal bent partition of $\mathbb{V}_n^{(p)}$. Then the function $f : \mathbb{V}_n^{(p)} \mapsto \mathbb{Z}_{p^k}$ such that $f(x) = j$ if $x \in A_j$ and $f(x) = 0$ if $x \in U$, is generalized bent.*

Proof We use Lemma 2 (ii), and show that every function $a_{k-1} \oplus C(x)$ is bent, if C is constant on every set $A(d)$. More precisely we show that $a_{k-1} \oplus C(x)$ is a bent function that can be obtained from the (normal) bent partition Ω. We therefore express the preimage sets of a_{k-1} and the sets $A(d)$ in Eq. (5) in terms of the sets in Ω. For $j \in \{0, \ldots, p^k - 1\}$, we can write $j = d + \ell p^{k-1}$ for some $d \in \{0, \ldots, p^{k-1} - 1\}$ and $\ell \in \{0, \ldots, p-1\}$. As easily observed, $a_{k-1}(x) = \ell$ if and only if $x \in A_j$ with $j = d + \ell p^{k-1}$ for some $d = 0, \ldots, p^{k-1} - 1$. On the other hand, for $d = 1, \ldots, p^{k-1} - 1$, the sets $A(d)$ are given by

$$A(d) = \{A_{d+\ell p^{k-1}} : \ell = 0, \ldots, p-1\} \text{ and}$$
$$A(0) = \{U, A_{\ell p^{k-1}} : \ell = 0, \ldots, p-1\}.$$

Suppose $C(x) = c_d$ on $A(d)$ for some $c_d \in \mathbb{F}_p$. We fix $d \in \{0, \ldots, p^{k-1} - 1\}$. Then every element of $\mathbb{F}_p$ is attained as an image of $a_{k-1}(x) \oplus C(x)$ on exactly one A_j lying in $A(d)$ while ℓ runs through $\{0, \ldots, p-1\}$. Therefore, for each $d \in \{0, \ldots, p^{k-1} - 1\}$ and $b \in \mathbb{F}_p$, there exists a unique $A_j \in A(d)$ such that $a_{k-1}(x) \oplus C(x) = b$ for all $x \in A_j$. Moreover, $a_{k-1}(x) \oplus C(x) = c_0$ for all $x \in U$. Hence, the preimage of $b \in \mathbb{F}_p \setminus \{c_0\}$ consists of the union of p^{k-1} sets A_j in Ω, and the preimage of c_0 consists of the union of p^{k-1} sets A_j in Ω and U. Since Ω is a bent partition, $a_{k-1}(x) \oplus C(x)$ is a bent function. □

Theorem 6 *Let $\Omega = \{U, A_0, \ldots, A_{p^k-1}\}$ be a normal bent partition of $\mathbb{V}_n^{(p)}$, then the functions given by $f(x) = j$ if $x \in A_j$ and $f(x) = 0$ (w.l.o.g.) if $x \in U$, is a bent function from $\mathbb{V}_n^{(p)}$ to $\mathbb{Z}_{p^k}$.*

Proof By Lemma 2 (i), we have to show that $p^t f(x)$ is generalized bent for any $0 \le t \le k-1$. By Proposition 1, this holds for $t = 0$. It remains to show the case that $t \ge 1$. The argument is similar. We first observe that

$$\mathcal{H}_f(c,u) = \sum_{x \in \mathbb{V}_n^{(p)}} \epsilon_{p^k}^{cp^t f(x)} \epsilon_p^{\langle u,x\rangle_n} = \sum_{x \in \mathbb{V}_n^{(p)}} \epsilon_{p^{k-t}}^{c\tilde{f}(x)} \epsilon_p^{\langle u,x\rangle_n},$$

where

$$\tilde{f}(x) = a_0(x) + \cdots + a_{k-t-1}(x)p^{k-t-1}.$$

Hence, f is generalized bent as a function into $\mathbb{Z}_{p^k}$ if and only if $\tilde{f}$ is generalized bent as a function mapping into $\mathbb{Z}_{p^{k-t}}$. Consequently, it suffices to show that $a_{k-t-1} \oplus C(x)$ is bent for every p-ary function which is constant on the sets

$$A(d) = \left\{ x \in \mathbb{V}_n^{(p)} : \sum_{i=0}^{k-t-2} a_i(x)p^i = d \right\}, \quad d = 0, \ldots, p^{k-t} - 1.$$

Suppose that $C(x) = c_d$ on $A(d)$. Writing $j \in \{0, \ldots, p^k - 1\}$ as

$$j = d + \ell p^{k-t-1} + s_t p^{k-t} + \cdots + s_1 p^{k-1}$$

for some $d \in \{0, \ldots, p^{k-t-1} - 1\}$ and $\ell, s_t, \ldots, s_1 \in \{0, \ldots, p-1\}$, we see that A_j is included in $A(d)$, i.e., $C(x) = c_d$ on A_j, and $a_{k-t-1}(x) = \ell$. For a fixed d and $s_t, \ldots, s_1$ running over $\mathbb{F}_p$, every element of $\mathbb{F}_p$ is attained as the image of $a_{k-t-1}(x) \oplus C(x)$ on exactly p^t sets A_j as ℓ runs over $\mathbb{F}_p$. Moreover, $a_{k-t-1}(x) \oplus C(x) = c_0$ on U. With the same argument as in Proposition 1, $a_{k-t-1} \oplus C(x)$ is a bent function obtained from the (normal) bent partition Ω. □

Remark 6 With MAGMA we confirmed that for some sporadic examples of bent functions from $\mathbb{F}_{2^6} \times \mathbb{F}_{2^6}$, into the (small) cyclic group $\mathbb{Z}_8$, obtained with Corollary 2 in [24], the collection of the preimage sets do not form a bent partition. The converse of Theorem 6 does hence not hold.

5 Bent partitions for odd characteristic

In characteristic 2, besides from the bent partitions obtained from (partial) spreads, we know the class of partitions Γ_1, Γ_2 in Example 4. The partitions Γ_1, Γ_2 have been found in [26] by using a property of Boolean bent functions that are connected with some $\mathbb{Z}_{2^k}$-bent functions, see [12,Corollary 1]. This property does in general not hold for $\mathbb{Z}_{p^k}$-bent functions, hence per se, it is not clear that a generalization of Γ_1, Γ_2 for odd p exists. In this section we establish generalizations for odd primes p. The proof with character sums is naturally more elaborate than for the case $p = 2$.

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 an integer such that $de \equiv 1 \bmod p^m - 1$. 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 $s \in \mathbb{F}_{p^m}$ we define

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

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

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

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

$$\begin{aligned} \Gamma_1 &= \{U, \mathcal{A}(\gamma); \gamma \in \mathbb{F}_{p^k}\} \\ \Gamma_2 &= \{V, \mathcal{B}(\gamma); \gamma \in \mathbb{F}_{p^k}\}, \end{aligned} \tag{6}$$

into $p^k + 1$ subsets, that have similar properties as spreads have. In fact, for $k = m$, both partitions reduce to the Desarguesian spread.

Theorem 7 *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 of Γ_1 (respectively Γ_2) is of this form.*
II. *Let $F : \mathbb{F}_{p^m} \times \mathbb{F}_{p^m} \to \mathbb{Z}_{p^k}$ be 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 $F(x) = c_0$ for all $x \in U$ (respectively $x \in V$), for some $c_0 \in \mathbb{Z}_{p^k}$. Then F is a $\mathbb{Z}_{p^k}$-bent function.*

Proof *I* We will show that for any $(\alpha, \beta) \in \mathbb{F}_{p^m} \times \mathbb{F}_{p^m} \setminus \{(0,0)\}$ we have $W_f(\alpha, \beta) = p^m \epsilon_p^c$ for some c depending on α and β. We use the notation $\gamma^{(c)}$ for elements γ for which $\mathcal{A}(\gamma)$ lies in the preimage of c under f, i.e., we have

$$f^{-1}(c) = \{\mathcal{A}(\gamma_1^{(c)}), \ldots, \mathcal{A}(\gamma_{p^{k-1}}^{(c)})\}$$

for some $\gamma_1^{(c)}, \ldots, \gamma_{p^{k-1}}^{(c)} \in \mathbb{F}_{p^k}$. Then for $(\alpha, \beta) \in \mathbb{F}_{p^m} \times \mathbb{F}_{p^m}$ we have the following equalities.

$$\begin{aligned}
W_f(\alpha, \beta) &= \sum_{(x,y)\in\mathbb{F}_{p^m}\times\mathbb{F}_{p^m}} \epsilon_p^{f(x,y)\oplus \mathrm{Tr}_m(\alpha x\oplus\beta y)} = \sum_{c\in\mathbb{F}_p}\sum_{(x,y)\in f^{-1}(c)} \epsilon_p^{c\oplus\mathrm{Tr}_m(\alpha x\oplus\beta y)}\\
&= \sum_{c\in\mathbb{F}_p}\sum_{i=1,\ldots,p^{k-1}}\sum_{(x,y)\in\mathcal{A}(\gamma_i^{(c)})} \epsilon_p^{c\oplus\mathrm{Tr}_m(\alpha x\oplus\beta y)} + \sum_{(x,y)\in U} \epsilon_p^{c_0\oplus\mathrm{Tr}_m(\alpha x\oplus\beta y)}\\
&= \sum_{c\in\mathbb{F}_p}\sum_{i=1,\ldots,p^{k-1}}\sum_{\substack{s\in\mathbb{F}_{p^m}\\ \mathrm{Tr}_k^m(s)=\gamma_i^{(c)}}}\sum_{x\in\mathbb{F}_{p^m}^*} \epsilon_p^{c\oplus\mathrm{Tr}_m(\alpha x\oplus\beta s x^e)} + \sum_{x\in\mathbb{F}_{p^m}} \epsilon_p^{c_0\oplus\mathrm{Tr}_m(\beta x)}\\
&= \sum_{c\in\mathbb{F}_p}\sum_{i=1,\ldots,p^{k-1}}\sum_{\substack{s\in\mathbb{F}_{p^m}\\ \mathrm{Tr}_k^m(s)=\gamma_i^{(c)}}}\left(\sum_{x\in\mathbb{F}_{p^m}} \epsilon_p^{c\oplus\mathrm{Tr}_m(\alpha x\oplus\beta s x^e)} - \epsilon_p^c\right)\\
&\quad + \sum_{x\in\mathbb{F}_{p^m}} \epsilon_p^{c_0\oplus\mathrm{Tr}_m(\beta x)}\\
&= -p^{k-1}p^{m-k}\sum_{c\in\mathbb{F}_p}\epsilon_p^c + \sum_{c\in\mathbb{F}_p}\epsilon_p^c\sum_{i=1,\ldots,p^{k-1}}\sum_{\substack{s\in\mathbb{F}_{p^m}\\ \mathrm{Tr}_k^m(s)=\gamma_i^{(c)}}}\sum_{x\in\mathbb{F}_{p^m}} \epsilon_p^{\mathrm{Tr}_m(\alpha x\oplus\beta s x^e)}\\
&\quad + \sum_{x\in\mathbb{F}_{p^m}} \epsilon_p^{c_0\oplus\mathrm{Tr}_m(\beta x)}\\
&= \sum_{c\in\mathbb{F}_p}\epsilon_p^c\sum_{i=1,\ldots,p^{k-1}}\sum_{\substack{s\in\mathbb{F}_{p^m}\\ \mathrm{Tr}_k^m(s)=\gamma_i^{(c)}}}\sum_{x\in\mathbb{F}_{p^m}} \epsilon_p^{\mathrm{Tr}_m(\alpha x\oplus\beta s x^e)} + \sum_{x\in\mathbb{F}_{p^m}} \epsilon_p^{c_0\oplus\mathrm{Tr}_m(\beta x)} \qquad (7)
\end{aligned}$$

Note that in the last equality we used the fact that $\sum_{c\in\mathbb{F}_p}\epsilon_p^c = 0$. Recall that

$$\sum_{x\in\mathbb{F}_{p^m}} \epsilon_p^{\mathrm{Tr}_m(\alpha x)} = \begin{cases} 0, & \text{if } \alpha \neq 0\\ p^m, & \text{if } \alpha = 0. \end{cases} \qquad (8)$$

Hence for the case $\beta = 0$ (and hence $\alpha \neq 0$) by Eqs. (7) and (8) we have $W_f(\alpha, \beta) = p^m\epsilon_p^{c_0}$.

Now we consider the case $\beta \neq 0$. Let $s_i^{(c)} \in \mathbb{F}_{p^m}$ such that $\mathrm{Tr}_k^m(s_i^{(c)}) = \gamma_i^{(c)}$. Set $\mathcal{Z} := \{y \in \mathbb{F}_{p^m} \mid \mathrm{Tr}_k^m(y) = 0\}$. Then

$$\{s \in \mathbb{F}_{p^m} \mid \mathrm{Tr}_k^m(s) = \gamma_i^{(c)}\} = s_i^{(c)} \oplus \mathcal{Z}.$$

Then by Eq. (8) we can write Eq. (7) as follows.

$$\begin{aligned}
W_f(\alpha, \beta) &= \sum_{c\in\mathbb{F}_p}\sum_{i=1,\ldots,p^{k-1}}\sum_{y\in\mathcal{Z}}\sum_{x\in\mathbb{F}_{p^m}} \epsilon_p^{c\oplus\mathrm{Tr}_m(\alpha x\oplus\beta(s_i^{(c)}\oplus y)x^e)}\\
&= \sum_{c\in\mathbb{F}_p}\epsilon_p^c\sum_{x\in\mathbb{F}_{p^m}}\epsilon_p^{\mathrm{Tr}_m(\alpha x)}\sum_{i=1,\ldots,p^{k-1}}\epsilon_p^{\mathrm{Tr}_m(\beta s_i^{(c)}x^e)}\sum_{y\in\mathcal{Z}}\epsilon_p^{\mathrm{Tr}_m(\beta x^e y)}. \qquad (9)
\end{aligned}$$

Note that if $\beta x^e \in \mathbb{F}_{p^k}$, then $\mathrm{Tr}_m(\beta x^e y) = \mathrm{Tr}_k(\beta x^e \mathrm{Tr}_k^m(y)) = 0$ as $y \in \mathcal{Z}$. That is, $\sum_{y\in\mathcal{Z}}\epsilon_p^{\mathrm{Tr}_m(\beta x^e y)} = p^{m-k}$. By Theorem 5.6 in [20], we know that the number of characters of $\mathbb{F}_{p^m}$ annihilating $\mathcal{Z}$ is $[\mathbb{F}_{p^m} : \mathcal{Z}] = p^k$ since $|\mathcal{Z}| = p^{m-k}$. That is, $x \in \mathbb{F}_{p^m}$ such that $\beta x^e \notin \mathbb{F}_{p^k}$ results in a non-trivial character. In particular, we have $\sum_{y \in \mathcal{Z}} \epsilon_p^{\mathrm{Tr}_m(\beta x^e y)} = 0$ if $\beta x^e \notin \mathbb{F}_{p^k}$. Therefore we can write Eq. (9) as

$$W_f(\alpha, \beta) = p^{m-k} \sum_{c \in \mathbb{F}_p} \epsilon_p^c \sum_{\substack{x \in \mathbb{F}_{p^m} \\ \beta x^e \in \mathbb{F}_{p^k}}} \epsilon_p^{\mathrm{Tr}_m(\alpha x)} \sum_{i=1,\ldots,p^{k-1}} \epsilon_p^{\mathrm{Tr}_m(\beta x^e s_i^{(c)})}. \tag{10}$$

Set $y = \beta x^e$. Since $de \equiv 1 \mod (p^m - 1)$ we have $x = (\beta^{-1} y)^d$. Set $\tilde{\beta} = \mathrm{Tr}_k^m(\alpha \beta^{-d})$. Then by Eq. (10) we obtain the following equalities.

$$\begin{aligned} W_f(\alpha, \beta) &= p^{m-k} \sum_{c \in \mathbb{F}_p} \epsilon_p^c \sum_{y \in \mathbb{F}_{p^k}} \epsilon_p^{\mathrm{Tr}_m(\alpha \beta^{-d} y^d)} \sum_{i=1,\ldots,p^{k-1}} \epsilon_p^{\mathrm{Tr}_m(y s_i^{(c)})} \\ &= p^{m-k} \sum_{c \in \mathbb{F}_p} \epsilon_p^c \sum_{y \in \mathbb{F}_{p^k}} \epsilon_p^{\mathrm{Tr}_k(\tilde{\beta} y^d)} \sum_{i=1,\ldots,p^{k-1}} \epsilon_p^{\mathrm{Tr}_k(y \gamma_i^{(c)})} \\ &= p^{m-k} \sum_{c \in \mathbb{F}_p} \epsilon_p^c \sum_{i=1,\ldots,p^{k-1}} \sum_{y \in \mathbb{F}_{p^k}} \epsilon_p^{\mathrm{Tr}_k(\tilde{\beta} y^d \oplus \gamma_i^{(c)} y)}. \end{aligned} \tag{11}$$

Note that $e \equiv p \mod (p^k - 1)$ and $de \equiv 1 \mod (p^k - 1)$, i.e., $dp \equiv 1 \mod (p^k - 1)$. Then we have

$$\begin{aligned} \sum_{y \in \mathbb{F}_{p^k}} \epsilon_p^{\mathrm{Tr}_k(\tilde{\beta} y^d \oplus \gamma_i^{(c)} y)} &= \sum_{y \in \mathbb{F}_{p^k}} \epsilon_p^{\mathrm{Tr}_k(\tilde{\beta}^p y^{dp} \oplus \gamma_i^{(c)} y)} \\ = \sum_{y \in \mathbb{F}_{p^k}} \epsilon_p^{\mathrm{Tr}_k((\tilde{\beta}^p \oplus \gamma_i^{(c)}) y)} &= \begin{cases} p^k, & \text{if } \gamma_i^{(c)} = \ominus \tilde{\beta}^p \\ 0, & \text{otherwise.} \end{cases} \end{aligned}$$

Since there exists a unique $\gamma_i^{(\tilde{c})} \in \mathbb{F}_{p^k}$ such that $\gamma_i^{(\tilde{c})} = \ominus \tilde{\beta}^p$, by Eq. (11) we have $W_f(\alpha, \beta) = p^m \epsilon_p^{\tilde{c}}$, which gives the desired conclusion.

The fact that every bent function which is constant on the elements of Γ_1 (respectively Γ_2) is of the form described as in the theorem, easily follows from the cardinalities of the sets U and A_j and Lemma 1.

II follows from I together with Theorem 6. □

We recall that the dual f^* of a regular bent function f is also bent. We have observed that for f given as in Theorem 7, $W_f(\alpha, \beta) = p^m \epsilon^{c_0}$ if $\beta = 0$, i.e., f^* is constant c_0 on V. Also, for $(\alpha, \beta) \in V_s^*$, the value $f^*(\alpha, \beta)$ is uniquely determined by $\tilde{\beta} = \mathrm{Tr}_k^m(\alpha \beta^{-d})$. That is, $f^*(\alpha, \beta) = c$ if and only if $\tilde{\beta}^p = \ominus \gamma_i^{(c)}$. By definition of V_s, we have $\tilde{\beta} = \mathrm{Tr}_k^m(s) = \gamma$, and hence f^* is constant on $B(\gamma)$. This implies that f^* is a bent function obtained by Γ_2, which gives the following corollary.

Corollary 4 *The duals of the bent functions of* Γ_1 *are in* Γ_2 *and vice versa.*

In [26] it is shown that for $p = 2$, the partitions Γ_1, Γ_2 do not come from any (partial) spread. One may suspect that this also holds for odd primes.

The argument in [26] uses the known results on the algebraic degree of Boolean partial spread bent functions, see [9,p. 96]: 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 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 [9,Theorem 6.3.12].

For an explicit argument for Γ_1, Γ_2 when p is odd, we first have to show a p-ary version for the algebraic degree result for partial spread bent functions. As it is shown in [13], a p-ary bent functions f from $\mathbb{V}_n^{(p)}$ to $\mathbb{F}_p$ can have algebraic degree at most $n(p-1)/2$ if f is weakly regular, the algebraic degree of non-weakly regular bent functions is upper bounded by $n(p-1)/2+1$ (the only yet known examples attaining this bound are ternary bent functions in odd dimension n, see [3, 4]). The following theorem shows that differently from $p=2$, all p-ary partial spread bent functions (without the exception) do attain the maximal possible algebraic degree.

Theorem 8 *Let p be an odd prime, $n=2m$ an even integer, and let $f:\mathbb{V}_n^{(p)}\rightarrow\mathbb{F}_p$ be a partial spread bent function. Then f has algebraic degree* $\deg(f)=(p-1)m$.

Proof Without loss of generality we consider $\mathbb{V}_n^{(p)}=\mathbb{F}_p^n$ and $f(0,\ldots,0)=0$. Let U be a subspace of the spread such that $f(x_1,\ldots,x_n)=c$ on $U\setminus\{(0,\ldots,0)\}$ for some nonzero $c\in\mathbb{F}_p$. Note that differently from the case of a PS^+ bent function when $p=2$, such a subspace always exists. By a coordinate transformation A of $\mathbb{F}_p^n$, we have

$$A(U)=\{(\alpha_1,\ldots,\alpha_m,0\ldots,0)\}=\mathbb{F}_p^m\times\{(0,\ldots,0)\}=:H$$

Set $g=f\circ A^{-1}$. Then $g(x_1,\ldots,x_n)=c$ on $H\setminus\{(0,\ldots,0)\}$. Set

$$\tilde{g}(x_1,\ldots,x_m):=g(x_1,\ldots,x_m,0,\ldots,0).$$

Note that $\deg(f)=\deg(g)\geq\deg(\tilde{g})$. Hence, it is enough to observe that $\deg(\tilde{g})=(p-1)m$. By Lagrange interpolation, we can write

$$\tilde{g}(x_1,\ldots,x_m)=\sum_{(\alpha_1,\ldots,\alpha_m)\in\mathbb{F}_p^m}\tilde{g}(\alpha_1,\ldots,\alpha_m)\prod_{i=0}^{m}\left(1-(x_i-\alpha_i)^{p-1}\right). \tag{12}$$

Since $\tilde{g}(0,\ldots,0)=0$ and $\tilde{g}(x_1,\ldots,x_m)=c$ on $H\setminus\{(0,\ldots,0)\}$, Eq. (12) becomes

$$\begin{aligned}\tilde{g}(x_1,\ldots,x_m)&=\sum_{(\alpha_1,\ldots,\alpha_m)\in\mathbb{F}_p^m\setminus\{(0,\ldots,0)\}}\prod_{i=0}^{m}c\left(1-(x_i-\alpha_i)^{p-1}\right)\\&=(p^m-1)x_1^{p-1}\cdots x_m^{p-1}+h(x_1,\ldots,x_m)\end{aligned}$$

for some $h\in\mathbb{F}_p[x_1,\ldots,x_m]$ of degree less than $(p-1)m$. Hence $\tilde{g}$ has algebraic degree $(p-1)m$. Therefore f has algebraic degree at least $(p-1)m$. Since every partial spread bent function is a regular bent function, see [21], f has algebraic degree at most $(p-1)m$, which shows the desired result. □

Remark 7 The proof of Theorem 8 also applies for $p=2$. Solely for a Boolean PS^+ bent function the existence of a subspace with the required properties is only guaranteed if the partial spread of $2^{n-1}+1$ subspaces, which defines the function, is extendable to a larger partial spread.

Lemma 3 *Let m,k be integers such that k divides m and* $\gcd(p^m-1,p^k+p-1)=1$ *and set $e=p^k+p-1$. Then $f(x,y):\mathbb{F}_{p^m}\times\mathbb{F}_{p^m}\rightarrow\mathbb{F}_p$ defined by* $f(x,y)=\mathrm{Tr}_1^m(\alpha x^{-e}y)$, *for a nonzero $\alpha\in\mathbb{F}_{p^k}$, is a bent function obtained from the normal bent partition $\Gamma_1=\{U,\mathcal{A}(\gamma);\gamma\in\mathbb{F}_{p^k}\}$ defined by Eq. (6).*

Proof For any nonzero $(x, y) \in U_s = \{(x, sx^e) : x \in \mathbb{F}_{p^m}\}$, we have

$$f(x, y) = \mathrm{Tr}_1^m(\alpha x^{-e} y) = \mathrm{Tr}_1^m(\alpha x^{-e} s x^e) = \mathrm{Tr}_1^m(s\alpha) = \mathrm{Tr}_1^k(\mathrm{Tr}_k^m(s)\alpha) = \mathrm{Tr}_1^k(\gamma\alpha),$$

where $U_s \in \mathcal{A}(\gamma)$. Also, for $(x, y) \in U = \{(0, y) : y \in \mathbb{F}_{p^m}\}$, we have $f(x, y) = 0$. Consequently, f is constant on each element of Γ_1. Since $\alpha \neq 0$ and γ runs over $\mathbb{F}_{p^k}$, there are exactly p^{k-1} elements $\mathcal{A}(\gamma)$ such that $f(x, y) = i$ for all $i \in \mathbb{F}_p$. Therefore, by Theorem 7, f is a bent function obtained from Γ_1. □

Similarly, one can observe that $f(x, y) : \mathbb{F}_{p^m} \times \mathbb{F}_{p^m} \to \mathbb{F}_p$ defined by $f(x, y) = \mathrm{Tr}_1^m(\alpha x y^{-d})$, for a nonzero $\alpha \in \mathbb{F}_{p^k}$ and $de \equiv 1 \mod (p^m - 1)$, is a bent function obtained from the bent partition $\Gamma_2 = \{V, \mathcal{B}(\gamma); \gamma \in \mathbb{F}_{p^k}\}$ defined by Eq. (6).

Proposition 2 *The function $f(x, y) = \mathrm{Tr}_m(\alpha x^{-e} y)$ given in Lemma 3 is not a function obtained from a partial spread.*

Proof By Theorem 8, it is enough to show that the degree of f is less than $(p-1)m$. We have the following equalities:

$$\begin{aligned}
-e &= p^m - p^k - p = p(p^{k-1} - 1) + p^k(p^{m-k} - 2)\\
&= p\left((p-1) + \cdots + (p-1)p^{k-2}\right)\\
&\quad + p^k\left((p-2) + (p-1)p + \cdots + (p-1)p^{m-k-1}\right)\\
&= (p-1)p + \cdots + (p-1)p^{k-1} + (p-2)p^k + (p-1)p^{k+1} \cdots + (p-1)p^{m-1}.
\end{aligned} \tag{13}$$

Hence by Eq. (13), the degree of x^{-e} is equal to

$$(p-1)(k-1) + p - 2 + (p-1)(m-k-1) = (p-1)(m-2) + (p-2).$$

Consequently, the degree of $x^{-e}y$ is equal to $(p-1)(m-1)$, which gives the desired conclusion. □

6 Difference set partitions

Boolean bent functions are in one-to-one correspondence with difference sets in the elementary abelian 2-group. Let us first recall the definition of a difference set in a finite group A.

Definition 3 Let A be a finite group of order v and let D be a subset of A. Then D is called a (v, k, λ)-difference set in A if every nonzero element of A can be written as a difference of two elements in D in exactly λ ways.

As is well known, see [9], a Boolean function $f : \mathbb{V}_n^{(2)} \to \mathbb{F}_2$ is bent if and only if the support of f, $supp(f) = \{x \in \mathbb{V}_n^{(2)} : f(x) = 1\}$, is a $(2^n, 2^{n-1} \pm 2^{n/2-1}, 2^{n-1} \pm 2^{n/2-2})$-difference set in $\mathbb{V}_n^{(2)}$, a so-called *Hadamard difference set*. By a result in [22], such difference sets are the only (nontrivial) difference sets in the elementary abelian 2-group.

With this connection between Boolean bent functions and difference sets, with bent partitions of $\mathbb{V}_n^{(2)}$ one equivalently can generate a large variety of difference sets. This motivates the definition of a difference set partition, which can be seen as a generalization of a difference set.

Definition 4 Let A be an abelian group of order v and let Θ be a partition of A into K subsets. Then Θ is called a (v, K, d)-difference set partition of A if every union of d subsets of Θ is a difference set of A.

Note that then difference sets are exactly the $(v, 2, 1)$-difference set partitions of A (the set complement of a (v, k, λ)-difference set is a $(v, v-k, v-2k+\lambda)$-difference set).

Clearly, in elementary abelian 2-groups, the difference set partitions are exactly the bent partitions (we do not consider the trivial difference sets—the empty set, sets with one element, and their complementary sets). We remark that we can interpret a Boolean bent function f as a trivial bent partition of $\mathbb{V}_n^{(2)}$ into two sets, the support of f, and its complement (both Hadamard difference sets). Our nontrivial Examples 1–4 are difference set partitions of $\mathbb{V}_n^{(2)}$ with parameters $(v, K, d) = (2^n, 2^m, 2^{m-1})$ respectively $(v, K, d) = (2^n, 2^k, 2^{k-1})$. Which groups allow nontrivial difference set partitions, we find an interesting question.

Remark 8 Depending on necessities, one may consider refined definitions of difference set partitions. For instance, for a normal bent partition $\{U, A_1, \ldots, A_K\}$ of $\mathbb{V}_n^{(2)}$, half of the sets A_j with or without U form a difference set.

7 Perspectives

Having similar properties as spreads, bent partitions, which we introduced in this article, are powerful objects for the construction of bent functions. We showed that with a (normal) bent partition of $\mathbb{V}_n^{(p)}$ of depth p^k, we do not only obtain Boolean respectively p-ary bent functions and vectorial bent functions, but also bent functions from $\mathbb{V}_n^{(p)}$ into the cyclic group $\mathbb{Z}_{p^k}$.

Classes of bent partitions, which are different from (partial) spreads have been presented in [26] for characteristic 2, and in this article for arbitrary characteristic p. These bent partitions reduce to the Desarguesian spread in some special case, but in general yield several different ones. Using group theoretical arguments, it is shown in [14] (see also Remark 4 in [15]), that the number of pairwise inequivalent PS_{ap} bent functions (see [9]), which one can obtain with the Desarguesian spread of $\mathbb{V}_n^{(p)}$, grows exponentially with n, more precisely is lower bounded by

$$\binom{p^m+1}{p^{m-1}} \Big/ 2m(p^m+1)p^m(p^m-1)^2. \tag{14}$$

It is an interesting question, whether one can obtain a bound similar to (14) for the bent partitions Γ_1, Γ_2, generalizations of the Desarguesian spread. A generalization of the argumentation in [14] to Γ_1, Γ_2 is not at all obvious.

We believe that there is a variety of bent partitions, also besides from the partitions Γ_1, Γ_2 for different divisors k of m, and that there is also considerable potential for future research on general properties of these powerful objects. We pointed to several open questions on bent partitions $\Omega = \{A_1, \ldots, A_K\}$ and normal bent partitions $\bar{\Omega} = \{U, A_1, \ldots, A_K\}$ of $\mathbb{V}_n^{(p)}$ (e.g. in Remarks 2 and 3), which we summarize below.

- Is K always a power of p?
- Do bent partitions exist with $|A_1| < |A_i|$, $2 \le i \le K$?
- Do bent partitions exist which are not coming from a normal bent partition (bent partitions with either $|A_1| < |A_i|$, $2 \le i \le K$, or with a larger A_1, which does not contain a subspace U of dimension $n/2$)?

- Do normal bent partitions always yield regular bent functions, or can there be normal bent partitions that generate non-weakly regular bent functions?
- Improve the bounds for K, $|A_j|$. One may assume that the parameters we see for bent partitions from spreads are the best possible (the largest possible K, hence the smallest value for $|A_j|$). If so, can only bent partitions from spreads achieve these values?

Acknowledgements The second author thanks Dr. N. Anbar and Sabancı University for their hospitality during several research visits. N. A. is supported by TÜBİTAK Project under Grant 120F309. The authors like to thank Tekgül Kalaycı for the discussions and the MAGMA calculations. We are grateful to the reviewers for their comments that improved the presentation and quality of this paper.

References

1. Canteaut A., Daum M., Dobbertin H., Leander G.: Finding nonnormal bent functions. Discret. Appl. Math. **154**, 202–218 (2006).
2. Carlet C., Mesnager S.: Four decades of research on bent functions. Des. Codes Cryptogr. **78**, 5–50 (2016).
3. Çeşmelioğlu A., Meidl W.: Bent functions of maximal degree. IEEE Trans. Inf. Theory **58**, 1186–1190 (2012).
4. Çeşmelioğlu A., Meidl W.: A construction of bent functions from plateaued functions. Des. Codes Cryptogr. **66**, 231–242 (2013).
5. Çeşmelioğlu A., Meidl W., Pott A.: On the dual of (non)-weakly regular bent functions and self-dual bent functions. Adv. Math. Commun. **7**, 425–440 (2013).
6. Çeşmelioğlu A., Meidl W., Pott A.: There are infinitely many bent functions for which the dual is not bent. IEEE Trans. Inf. Theory **62**, 5204–5208 (2016).
7. Çeşmelioğlu A., Meidl W., Pott A.: Vectorial bent functions in odd characteristic and their components. Cryptogr. Commun. **12**, 899–912 (2020).
8. Charpin P.: Normal Boolean functions. J. Complex. **20**, 245–265 (2004).
9. Dillon J.F: Elementary Hadamard Difference sets. Ph.D. dissertation, University of Maryland (1974).
10. Gadouleau M., Mariot L., Picek S.: Bent functions in the partial spread class generated by linear recurring sequences. arXiv:2112.08705.
11. Helleseth T., Kholosha A.: Monomial and quadratic bent functions over the finite fields of odd characteristic. IEEE Trans. Inf. Theory **52**(5), 2018–2032 (2006).
12. Hodžić S., Meidl W., Pasalic E.: Full characterization of generalized bent functions as (semi)-bent spaces, their dual, and the Gray image. IEEE Trans. Inf. Theory **64**, 5432–5440 (2018).
13. Hou X.D.: p-ary and q-ary versions of certain results about bent functions and resilient functions. Finite Fields Appl. **10**, 566–582 (2004).
14. Kantor W.: Exponential numbers of two-weight codes, difference sets and symmetric designs. Discret. Math. **46**, 95–98 (1983).
15. Kantor W.: Bent functions generalizing Dillon's partial spread functions. arXiv:1211.2600v1.
16. Kantor W.: On maximal symplectic partial spreads. Adv. Geom. **17**, 453–471 (2017).
17. Kolomeec N.: Enumeration of bent functions on the minimum distance from the quadratic bent function. J. Appl. Ind. Math. **6**, 306–317 (2012).
18. Kolomeec N.: The graph of minimal distances of bent functions and its properties. Des. Codes Cryptogr. **85**, 395–410 (2017).
19. Kumar P.V., Scholtz R.A., Welch L.R.: Generalized bent functions and their properties. J. Comb. Theory Ser. A **40**, 90–107 (1985).
20. Lidl R., Niederreiter H.: Finite Fields, 2nd edn Cambridge University Press, Cambridge (1997).
21. Lisonek P., Lu H.Y.: Bent functions on partial spreads. Des. Codes Cryptogr. **73**, 209–216 (2014).
22. Mann H.B.: Difference sets in elementary Abelian groups. Ill. J. Math. **9**, 212–219 (1965).
23. Martinsen T., Meidl W., Stanica P.: Partial spread and vectorial generalized bent functions. Des. Codes Cryptogr. **85**, 1–13 (2017).
24. Meidl W.: A secondary construction of bent functions, octal gbent functions and their duals. Math. Comput. Simul. **143**, 57–64 (2018).
25. Meidl W., Pirsic I.: On the normality of p-ary bent functions. Cryptogr. Commun. **10**, 1037–1049 (2018).
26. Meidl W., Pirsic I.: Bent and $\mathbb{Z}_{2^k}$-bent functions from spread-like partitions. Des. Codes Cryptogr. **89**, 75–89 (2021).

27. Meidl W., Pott A.: Generalized bent functions into $\mathbb{Z}_{p^k}$ from the partial spread and the Maiorana–McFarland class. Cryptogr. Commun. **11**, 1233–1245 (2019).
28. Mesnager S., Tang C., Qi Y., Wang L., Wu B., Feng K.: Further results on generalized bent functions and their complete characterization. IEEE Trans. Inf. Theory **64**, 5441–5452 (2018).
29. Nyberg K.: Construction of bent functions and difference sets, In: Advances in cryptology–EUROCRYPT '90 (Aarhus, 1990), Lecture Notes in Comput. Sci. 473, Springer, Berlin, pp. 151–160 (1991).
30. Nyberg K.: Perfect nonlinear S-boxes, In: Advances in cryptology–EUROCRYPT'91 (Brighton, 1991), Lecture Notes in Comput. Sci. 547, Springer, Berlin, pp. 378–386 (1991).
31. Potapov V.: On minimal distance of q-ary bent functions. In: Problems of redundancy in information and control systems. IEEE, pp. 115–116 (2016).
32. Pott A.: Nonlinear functions in abelian groups and relative difference sets. Discret. Appl. Math. **138**, 177–193 (2004).
33. Pott A.: A survey on relative difference sets. Groups, difference sets, and the Monster. In: Ohio State Univ. Math. Res. Inst. Publ. 4. de Gruyter, Berlin, pp. 195–232 (1996).
34. Rothaus O.S.: On "bent" functions. J. Comb. Theory Ser. A **20**, 300–305 (1976).

Publisher's Note Springer Nature remains neutral with regard to jurisdictional claims in published maps and institutional affiliations.