BENT PARTITIONS AND LP-PACKINGS

by
SEZEL ALKAN

Submitted to the Graduate School of Engineering and Natural Sciences
in partial fulfilment of
the requirements for the degree of Doctor of Philosophy

Sabancı University
July 2025

BENT PARTITIONS AND LP-PACKINGS

Approved by:

Asst. Prof. NURDAGÜL ANBAR MEIDL .....
(Dissertation Supervisor)

Asst. Prof. AYESHA ASLOOB QURESHI .....

Asst. Prof. MOHAMED DABAGH .....

Asst. Prof. SÜHA ORHUN MUTLUERGİL .....

Prof. SEHER TUTDERE KAVUT .....

Date of Approval: July 17, 2025

ABSTRACT

BENT PARTITIONS AND LP-PACKINGS

SEZEL ALKAN

Ph.D Dissertation, July 2025

Dissertation Supervisor: Asst. Prof. NURDAGÜL ANBAR MEIDL

Keywords: Bent function, bent partition, LP-packing, partial difference set, vectorial dual-bent function

This thesis investigates the recently introduced concepts of bent partitions, LP-packings, and their interrelations, including their connection to vectorial dual-bent functions. We begin by showing that LP-packings give rise to (normal) bent partitions. Using examples involving ternary bent functions, we demonstrate that LP-packings and bent partitions represent fundamentally different concepts.

We then extend a known lifting procedure from Desarguesian spreads to LP-packings in non-elementary abelian groups to a lifting procedure from generalized Desarguesian spreads to LP-packings in non-elementary abelian groups as well as larger elementary abelian groups. This generalization broadens the scope of known constructions of LP-packings.

In the final part, we explore secondary constructions of a class of vectorial dual-bent functions corresponding to bent partitions with a specific property. One construction is based on the direct sum of vectorial functions, while the other generalizes a method originally introduced by Wang, Fu, and Wei in [34]. These approaches yield a wide variety of vectorial bent functions, bent partitions, and LP-packings.

ÖZET

BÜKÜLMÜŞ PARÇALANMALAR VE LP-PAKETLEMELER

SEZEL ALKAN

Doktora Tezi, Temmuz 2025

Tez Danışmanı: Asst. Prof. Dr. NURDAGÜL ANBAR MEIDL

Anahtar Kelimeler: Bükülmüş fonksiyon, bükülmüş parçalanma, LP-paketleme, parçalı fark kümesi, vektörel bükülmüş fonksiyon

Bu tez, yakın zamanda literatüre kazandırılan bükülmüş parçalanmalar, LP-paketlemeleri ve bunların birbirleriyle olan ilişkilerinin yanı sıra, vektörel devrik bükülmüş fonksiyonlarla olan bağlantılarını kapsamlı bir biçimde incelemektedir.

Çalışmanın ilk aşamasında, LP-paketlemelerin (normal) bükülmüş parçalanmalar oluşturduğunu göstermekteyiz. Karakteristik 3'teki bükülmüş fonksiyon örnekleri aracılığıyla, LP-paketlemeler ile bükülmüş parçalanmaların farklı yapılar olduklarını ortaya koymaktayız.

Devamında, literatürde mevcut olan ve Desarguesian parçalanmalardan LP-paketlemelere yönelik tanımlanmış kaldırma yöntemini, genelleştirilmiş Desarguesian parçalanmalardan, hem elemanter olmayan hem de elemanter değişmeli gruplara LP-paketlemeler elde edecek şekilde genelleştiriyoruz. Bu genelleştirme, LP-paketlemelerin bilinen inşa yöntemlerinin kapsamını önemli ölçüde genişletmektedir.

Tezin son bölümünde ise, belirli bir yapısal özelliği sağlayan bükülmüş parçalanmalara karşılık gelen bir sınıf vektörel devrik bükülmüş fonksiyonun ikincil inşa yöntemleri ele alınmaktadır. Bu bağlamda, birinci yöntem vektörel fonksiyonların doğrudan toplamına, ikinci yöntem ise Wang, Fu ve Wei tarafından [34] çalışmada önerilen yapının daha genel bir biçimine dayanmaktadır. Bu inşa teknikleri aracılığıyla, geniş bir yelpazede vektörel bükülmüş fonksiyonlar, bükülmüş parçalanmalar ve LP-paketlemeler elde edilebilmektedir.

ACKNOWLEDGEMENTS

First, I would like to express my appreciation to my advisor Prof. Nurdagül Anbar Meidl for patiently guiding and motivating me throughout this study. I also want to thank Tekgül Kalaycı and Wilfried Meidl for their great support and suggestions of open problems.

I would like to thank my jury members, Prof. Ayesha Asloob Qureshi, Prof. Seher Tutdere Kavut, Prof. Mohamed Dabagh, and Prof. Süha Orhun Mutluergil for their time and valuable comments.

I would like to extend my thanks to Sabancı University for providing financial support and a friendly environment.

I also want to thank my parents for unconditionally supporting me throughout my life.

I was supported by the Scientific and Technological Research Institution of Turkey (TUBITAK) under projects 120F309 and 123F360.

PREFACE

Boolean bent functions have been introduced in the 1960s by Rothaus in (Rothaus, 1976). They are the functions of maximum possible distance from all linear and affine functions. In (Kumar, Scholtz & Welch, 1985), Kumar, Scholtz and Welch generalized this concept to p-ary bent functions, that is, to functions from a vector space $\mathbb{V}_n^{(p)}$ of dimension n to the finite field $\mathbb{F}_p$, where p is an odd prime. Bent functions have been an active field of research for their applications in coding and cryptography, and also for their rich connections to objects from combinatorics like difference sets and strongly regular graphs.

There are two main primary construction of bent functions; one is the class of Maiorana-McFarland bent functions, and the other is the class of (partial) spread bent functions. A partial spread of a vector space $\mathbb{V}_n^{(p)}$ (over $\mathbb{F}_p$), $n = 2m$, is a collection $\mathcal{S} = \{U_1, U_2, \ldots, U_K\}$ of m-dimensional subspaces of $\mathbb{V}_n^{(p)}$, which pairwise intersects trivially. If $K = p^m + 1$, hence every nonzero element of $\mathbb{V}_n^{(p)}$ is in exactly one subspace, then $\mathcal{S}$ is called a (complete) spread. Recently, a class of partitions of $\mathbb{V}_n^{(p)}$, which have properties similar to spreads, have been introduced. The first non-spread construction of bent partitions is presented in (Meidl & Pirsic, 2021) by Pirsic and Meidl for $p = 2$. It is extended to odd primes by Anbar and Meidl in (Anbar & Meidl, 2022). Moreover, a large class of bent partitions can be obtained from semifields with certain properties, called generalized semifield spreads; see (Anbar, Kalaycı & Meidl, 2023). Very recently, Jedwab and Li have introduced the concept of Latin square partial difference set packings (LP-packings) in finite abelian groups, which is strongly related to the notion of bent partitions; see (Jedwab & Li, 2021). In fact, LP-packings yield bent partitions. In this thesis, we study mainly bent partitons, LP-packings and their connections with each other, and vectorial dual-bent functions.

The outline of this thesis is as follows. In Chapter 1, we first give definitions, basic properties, and classification of (vectorial) bent functions. Then we recall the construction of bent partitions and LP-packings and some preliminary results to be used in this work. In Chapter 2, we consider ternary bent functions. The question of

whether there exists a nonnormal bent partition for $p > 2$ is open in (Anbar & Meidl, 2022). We show that nonnormal bent partitions can be obtained from preimage sets of ternary bent functions, that is, from preimage sets of bent functions from $\mathbb{V}_n^{(3)}$ to $\mathbb{F}_3$. More precisely, we show that ternary bent functions yield bent partitions. Some of these bent partitions give LP-packings, some do not.

In (Jedwab & Li, 2021), a recursive method is given to produce LP-packings in certain nonelementary abelian groups using spreads in elementary abelian groups as a "base case". In Chapter 3, we show that the generalized Desarguesian spreads can also be applied in the lifting procedure. The concept of LP-partitions is essential in this method. In Section 3.1, we obtain some LP-partitions from generalized Desarguesian spreads for p is odd and even. In Section 3.2, using these LP-partitions we extend the lifting procedure given in (Jedwab & Li, 2021). As a result, we can obtain possibly new LP-packings in elementary abelian groups, and also LP-packings in nonelementary abelian groups from a base case different from a spread.

In Chapter 4, we analyze some secondary constructions of vectorial dual-bent functions satisfying a certain property called Condition $\mathcal{A}$, which is introduced in (Wang, Fu & Wei, 2023). In Section 4.1, we examine the direct sum of two vectorial dual-bent functions satisfying this condition, and also the bent partitions and LP-packings (in some cases) corresponding to this construction. In (Wang et al., 2023), using the PS_{ap} bent functions, a secondary construction of vectorial dual-bent functions is presented. In Section 4.2, we show a more general version of this construction to obtain new bent partitions, LP-packings and vectorial dual-bent functions satisfying Condition $\mathcal{A}$.

TABLE OF CONTENTS

1. PRELIMINARIES

In this chapter, we will give the definitions and fundamental properties of bent functions, vectorial bent functions, and related concepts. There are a number of equivalent characterizations of bent functions. Throughout this work, we will use characterization via character sums.

A character χ of a finite abelian group G is a homomorphism from G to the multiplicative group of complex numbers $\mathbb{C}$. For a positive integer n and a prime number p, if we denote the vector space of dimension n over the finite field $\mathbb{F}_p$ by $\mathbb{V}_n^{(p)}$, then we may describe the characters of $\mathbb{V}_n^{(p)}$ in the following possible ways.

If we identify $\mathbb{V}_n^{(p)}$ with the additive group of the finite field $\mathbb{F}_{p^n}$, then every character of $\mathbb{V}_n^{(p)}$ is given by $x \to \zeta_p^{\mathrm{Tr}(ux)}$ for some $u \in \mathbb{F}_{p^n}$, where $\mathrm{Tr}(.)$ is the absolute trace function and ζ_p is a primitive p-th root of unity. Otherwise, the characters of $\mathbb{V}_n^{(p)}$ are simply the functions $x \to \zeta_p^{\langle b,x\rangle_n}$, $b \in \mathbb{V}_n^{(p)}$, where $\langle .\rangle_n$ is a nondegenerate inner product of $\mathbb{V}_n^{(p)}$. For further background on characters, we refer to (Lidl & Niederreiter, 1997).

1.1 Definitions and Some Basic Properties of Bent Functions

A function $f : \mathbb{V}_n^{(p)} \to \mathbb{F}_p$ is called a Boolean function if $p = 2$ and a p-ary function if p is odd. In this section, we will mainly give the characteristic properties of Boolean and p-ary bent functions. However, bent functions can also be defined between arbitrary finite abelian groups.

Definition 1. *Let $(A, +_A)$ and $(B, +_B)$ be finite abelian groups. A function f from A to B is called a bent function if for every character χ of $A \times B$ which is nontrivial on B we have*

$$\sum_{x\in A} |\chi(x, f(x))| = \sqrt{|A|}. \tag{1.1}$$

In the case $A = \mathbb{V}_n^{(p)}$ and $B = \mathbb{F}_p$, the character sum in (1.1) gives rise to a function $\mathcal{W}_f$ from $B \times A$ to the complex numbers $\mathbb{C}$, which is called the Walsh transform of f, defined by

$$\mathcal{W}_f(b, a) = \sum_{x\in\mathbb{V}_n^{(p)}} \zeta_p^{bf(x)-\langle a,x\rangle_n}$$

for all $(b, a) \in \mathbb{F}_p^* \times \mathbb{V}_n^{(p)}$, where $\langle .\rangle_n$ is a nondegenerate inner product of $\mathbb{V}_n^{(p)}$ and ζ_p is a primitive p-th root of unity.

Definition 2. *A function f from $\mathbb{V}_n^{(p)}$ to $\mathbb{F}_p$ is called a bent function if the absolute value of*

$$\mathcal{W}_f(a) := \mathcal{W}_f(1, a) = \sum_{x\in\mathbb{V}_n^{(p)}} \zeta_p^{f(x)-\langle a,x\rangle_n} \tag{1.2}$$

is $p^{n/2}$ for all $a \in \mathbb{V}_n^{(p)}$.

Note that since if f is bent, then bf is also bent for any nonzero element b of $\mathbb{F}_p$, the Walsh transform of $f : \mathbb{V}_n^{(p)} \to \mathbb{F}_p$ is in general defined as in (1.2), and the set $\{\mathcal{W}_f(a) : a \in \mathbb{V}_n^{(p)}\}$ is called the *Walsh spectrum* of f.

In the case $p = 2$, we have $\zeta_2 = -1$, so $\mathcal{W}_f(a)$ is an integer for any $a \in \mathbb{V}_n^{(p)}$. Then if $f : \mathbb{V}_n^{(2)} \to \mathbb{F}_2$ is bent, using the definition of Walsh transform, one can conclude n must be even and

$$\mathcal{W}_f(a) = 2^{n/2}(-1)^{f^*(a)} \tag{1.3}$$

for some Boolean function $f^* : \mathbb{V}_n^{(2)} \to \mathbb{F}_2$. The function f^* is called the *dual* of f. For the p-ary case, the Walsh transform of a bent function $f : \mathbb{V}_n^{(p)} \to \mathbb{F}_p$ satisfies

$$\mathcal{W}_f(a) = \begin{cases} \pm\zeta_p^{f^*(a)} p^{n/2} & : \quad p^n \equiv 1 \bmod 4, \\ \pm i\zeta_p^{f^*(a)} p^{n/2} & : \quad p^n \equiv 3 \bmod 4, \end{cases} \tag{1.4}$$

where $i = \sqrt{-1}$, and f^* is a function from $\mathbb{V}_n^{(p)}$ to $\mathbb{F}_p$, which is again called the *dual* of f, see (Helleseth & Kholosha, 2006).

A bent function $f : \mathbb{V}_n^{(p)} \to \mathbb{F}_p$ is called *weakly regular* if for all $a \in \mathbb{V}_n^{(p)}$ we have $\mathcal{W}_f(a) = \varepsilon\, \zeta_p^{f^*(a)} p^{n/2}$ for some (fixed) $\varepsilon \in \{\pm 1, \pm i\}$. In particular, if $\varepsilon = 1$ we call f *regular*. Boolean bent functions are always regular by Equation (1.3). If the sign of ε changes with $a \in \mathbb{V}_n^{(p)}$, then f is called *non-weakly regular* bent. If $f : \mathbb{V}_n^{(p)} \to \mathbb{F}_p$ is a weakly regular bent function, then its dual f^* is also weakly regular bent. To see this, let a be an arbitrary element of $\mathbb{V}_n^{(p)}$. Then we have

$$\begin{aligned} \sum_{y \in \mathbb{V}_n^{(p)}} \zeta_p^{\langle y,a\rangle_n} \mathcal{W}_f(y) &= \sum_{y \in \mathbb{V}_n^{(p)}} \zeta_p^{\langle y,a\rangle_n} \sum_{x \in \mathbb{V}_n^{(p)}} \zeta_p^{f(x)-\langle y,x\rangle_n} \\ &= \sum_{x \in \mathbb{V}_n^{(p)}} \zeta_p^{f(x)} \sum_{y \in \mathbb{V}_n^{(p)}} \zeta_p^{\langle y,a-x\rangle_n} \\ &= p^n \zeta_p^{f(a)}, \end{aligned} \tag{1.5}$$

where in the last equality we used the property that $\sum_{y \in \mathbb{V}_n^{(p)}} \zeta_p^{\langle y,a-x\rangle_n} = 0$ for $x \neq a$. Since f is weakly regular bent, we have $\mathcal{W}_f(y) = \varepsilon\, \zeta_p^{f^*(y)} p^{n/2}$ for some $\varepsilon \in \{\pm 1, \pm i\}$, which does not change with $y \in \mathbb{V}_n^{(p)}$. Then using Equation (1.5), we obtain

$$p^n \zeta_p^{f(a)} = \sum_{y \in \mathbb{V}_n^{(p)}} \zeta_p^{\langle y,a\rangle_n} \varepsilon \zeta_p^{f^*(y)} p^{n/2} = \varepsilon p^{n/2} \sum_{y \in \mathbb{V}_n^{(p)}} \zeta_p^{f^*(y)-\langle -a,y\rangle_n} = \varepsilon p^{n/2} \mathcal{W}_{f^*}(-a),$$

which implies $\mathcal{W}_{f^*}(-a) = \varepsilon^{-1} p^{n/2} \zeta_p^{f(a)}$. Thus, f^* is also a weakly regular bent function. However, in the case where $f : \mathbb{V}_n^{(p)} \to \mathbb{F}_p$ is a non-weakly regular bent function, the dual f^* of f may not be a bent function; see (Çeşmelioğlu, Meidl & Pott, 2013b).

Finally, a function $f : \mathbb{V}_n^{(p)} \to \mathbb{F}_p$ is called *plateaued* (or *s-plateaued*) if for all $a \in \mathbb{V}_n^{(p)}$, we have $|\mathcal{W}_f(a)|$ is either 0 or $p^{\frac{n+s}{2}}$ for some fixed integer $0 \leq s \leq n$. Then bent functions are 0-plateaued functions, and by Parseval's identity, there is no 0-plateaued function which is not bent. Moreover, f is called *near-bent* (or *semi-bent*), if $s = 1$.

1.2 Vectorial Bent Functions

A function $F : \mathbb{V}_n^{(p)} \to \mathbb{V}_m^{(p)}$ is called a vectorial function if $m > 1$, where $\mathbb{V}_n^{(p)}$ and $\mathbb{V}_m^{(p)}$ are vector spaces of dimensions n and m, respectively, over the prime field $\mathbb{F}_p$. Then the character sum in (1.1) induces a function $\mathcal{W}_F$ on $\mathbb{V}_m^{(p)} \setminus \{0\} \times \mathbb{V}_n^{(p)}$ of the

form

$$\mathcal{W}_F(b,a) = \sum_{x \in \mathbb{V}_n^{(p)}} \zeta_p^{\langle b, F(x)\rangle_m - \langle a,x\rangle_n},$$

which is also called the Walsh transform of F.

Definition 3. *A function F from $\mathbb{V}_n^{(p)}$ to $\mathbb{V}_m^{(p)}$, $m > 1$, is called a vectorial bent function if $|\mathcal{W}_f(b,a)| = p^{n/2}$ for all nonzero $b \in \mathbb{V}_m^{(p)}$ and $a \in \mathbb{V}_n^{(p)}$.*

For a vectorial function $F : \mathbb{V}_n^{(p)} \to \mathbb{V}_m^{(p)}$ and $v \in \mathbb{V}_m^{(p)} \setminus \{0\}$, the function $F_v : \mathbb{V}_n^{(p)} \to \mathbb{F}_p$ defined by $F_v(x) = \langle v, F(x)\rangle_m$ is called a *component function* of F. Using the definition, one can observe that F is vectorial bent if and only if all component functions of F are bent.

Lemma 1. *Let $F : \mathbb{V}_n^{(p)} \to \mathbb{V}_m^{(p)}$ be a vectorial bent function. The set of component functions, together with the zero function, forms an m-dimensional vector space of bent functions over $\mathbb{F}_p$.*

Proof. Let $\{v_1, v_2, \ldots, v_m\}$ be a basis of $\mathbb{V}_m^{(p)}$ over $\mathbb{F}_p$. For $i = 1, 2, \ldots, m$, we define $f_i(x) = \langle v_i, F(x)\rangle_m$, where $\langle . \rangle_m$ is a fixed inner product of $\mathbb{V}_m^{(p)}$. Suppose that $f_1, f_2 \ldots, f_m$ are linearly dependent over $\mathbb{F}_p$. Then by definition of f_i

$$c_1\langle v_1, F(x)\rangle_m + c_2\langle v_2, F(x)\rangle_m + \ldots + c_m\langle v_m, F(x)\rangle_m = 0$$

for some $c_i \in \mathbb{F}_p$, $i = 1, 2, \ldots, m$, not all zero, which implies

$$\langle c_1 v_1 + c_2 v_2 + \ldots c_m v_m, F(x)\rangle_m = 0, \tag{1.6}$$

by linearity of $\langle . \rangle_m$ in the first argument. The sum $v := c_1 v_1 + c_2 v_2 + \ldots c_m v_m$ is a nonzero element of $\mathbb{V}_m^{(p)}$ since $c_i \neq 0$ for at least one i, $1 \leq i \leq m$. Hence, $f(x) := \langle v, F(x)\rangle_m$ is a bent function (since $F : \mathbb{V}_n^{(p)} \to \mathbb{V}_m^{(p)}$ is vectorial bent). By (1.6), f is zero on $\mathbb{V}_m^{(p)}$. Then the Walsh spectrum of f is $\{0, p^n\}$, which is not possible as f is bent. Therefore, $f_1, f_2 \ldots, f_m$ are linearly independent over $\mathbb{F}_p$, i.e., $\{f_1, f_2 \ldots, f_m\}$ forms a basis for the set of component functions (together with the zero function). □

In (Nyberg, 1991b), it is shown that for a vectorial bent function $F : \mathbb{V}_n^{(p)} \to \mathbb{V}_m^{(p)}$, with n being even, if all component functions are regular bent, then m can be at most $n/2$. In particular, for $p = 2$, we have the bound $m \leq n/2$. In the case where p is odd, n can be even or odd, and m can take the value n (at most). Vectorial bent

functions with $m = n$ are called planar functions (or perfect nonlinear functions).

Example 1. *Let p be an odd prime, and let $F : \mathbb{F}_{p^n} \to \mathbb{F}_{p^n}$ be a function given by $F(x) = x^2$. We can fix an inner product on $\mathbb{F}_{p^n}$ as $\langle a, b\rangle_n = \mathrm{Tr}_1^n(ab)$, where $a, b \in \mathbb{F}_{p^n}$ and $\mathrm{Tr}_1^n(.)$ denotes the trace map from the finite field $\mathbb{F}_{p^n}$ to $\mathbb{F}_p$. Then by (Helleseth & Kholosha, 2006, Corollary 3), for any nonzero $a \in \mathbb{F}_{p^n}$ the component function $F_a(x) = \mathrm{Tr}_1^n(ax^2)$ is a (weakly) regular bent function with the dual $(F_a)^*(x) = \mathrm{Tr}_1^n(-\frac{x^2}{4a})$. Therefore, F is a bent function, which is also planar.*

For a vectorial bent function $F : \mathbb{V}_n^{(p)} \to \mathbb{V}_m^{(p)}$, the set of duals of the component functions may not be closed under addition.

Example 2. *(Çeşmelioğlu, Meidl & Pott, 2018) Let π be a permutation on $\mathbb{V}_m^{(p)}$, $m > 1$. We consider the function $F : \mathbb{F}_{p^m} \times \mathbb{F}_{p^m} \to \mathbb{F}_{p^m}$ defined by*

$$F(x, y) = x\pi(y).$$

Since F is represented in bivariate form, we can take the inner product for the vector space $\mathbb{F}_{p^m} \times \mathbb{F}_{p^m}$ as $\langle (u_1, u_2), (v_1, v_2)\rangle_{2m} = \mathrm{Tr}_1^m(u_1v_1 + u_2v_2)$, where $u_1, u_2, v_1, v_2 \in \mathbb{F}_{p^m}$. Then for any $c \in \mathbb{F}_{p^m}^*$ and $(u, v) \in \mathbb{F}_{p^m} \times \mathbb{F}_{p^m}$ we get

$$\begin{aligned} W_{F_c}(u, v) &= \sum_{x\in\mathbb{F}_{p^m}, y\in\mathbb{F}_{p^m}} \zeta_p^{F_c(x,y)-\mathrm{Tr}_1^m(ux+vy)} \\ &= \sum_{x\in\mathbb{F}_{p^m}, y\in\mathbb{F}_{p^m}} \zeta_p^{\mathrm{Tr}_1^m(cx\pi(y))-\mathrm{Tr}_1^m(ux+vy)} \\ &= \sum_{y\in\mathbb{F}_{p^m}} \zeta_p^{\mathrm{Tr}_1^m(-vy)} \sum_{x\in\mathbb{F}_{p^m}} \zeta_p^{\mathrm{Tr}_1^m((c\pi(y)-u)x)} \\ &= p^m \zeta_p^{\mathrm{Tr}_1^m(-v\pi^{-1}(\frac{u}{c}))}, \end{aligned}$$

which implies that the component function F_c of F is a bent function with the dual $(F_c)^*(x, y) = \mathrm{Tr}_1^m(-y\pi^{-1}(\frac{x}{c}))$. Therefore, the vectorial function $F(x, y) = x\pi(y)$ is bent, which is called a Maiorana-McFarland bent function.

For m is odd, the Dickson polynomial $p(x) := D_5(x, -1) = x^5 + 2x^3 + 5x \in \mathbb{F}_7[x]$ is a permutation on $\mathbb{F}_{7^m}$, so $F(x, y) = xp^{-1}(y)$ is a Maiorana-McFarland bent function from $\mathbb{F}_{7^m} \times \mathbb{F}_{7^m}$ to $\mathbb{F}_{7^m}$. The sum of duals of the component functions F_1 and F_2 are

$$(F_1)^*(x, y) + (F_2)^*(x, y) = \mathrm{Tr}_1^m(-yp(x)) + \mathrm{Tr}_1^m(-yp\left(\frac{x}{2}\right)) = \mathrm{Tr}_1^m(-yq(x)),$$

where $q(x) = 3x^5 + 4x^3 + 4x \in \mathbb{F}_7[x]$. *This is not a permutation on* $\mathbb{F}_{7^m}$ *as* $q(1) = q(5) = 4$. *Then by Theorem 1 (in Section 1.4), the sum* $\mathrm{Tr}_1^m(-yq(x))$ *is not bent.*

Definition 4. *A vectorial bent function* $F : \mathbb{V}_n^{(p)} \to \mathbb{V}_m^{(p)}$ *is called vectorial dual-bent if the set of duals of the component functions of* F *together with the zero function forms a vector space of dimension* m.

Remark 1. *Using the definition, one can conclude that if* $F : \mathbb{V}_n^{(p)} \to \mathbb{V}_m^{(p)}$ *is vectorial dual-bent function, then the duals of the component functions of* F *are component functions of some vectorial bent function, i.e., there exists a vectorial bent function* $G : \mathbb{V}_n^{(p)} \to \mathbb{V}_m^{(p)}$ *such that* $(F_c)^* = G_{\sigma(c)}$ *for* $c \in \mathbb{V}_m^{(p)} \backslash \{0\}$, *where* $(F_c)^*$ *is the dual of the component function* $\langle c, F(x)\rangle_m$ *and* σ *is a permutation on* $\mathbb{V}_m^{(p)} \backslash \{0\}$. *The vectorial bent function* G *is then called a vectorial dual of* F *and denoted by* F^*. *Note that being vectorial dual-bent is a property of the vector space (of the duals of the component functions of* F*), so* F^* *is not unique.*

1.3 EA-Equivalence and Algebraic Degree

For the classification of (vectorial) bent functions, the concept of equivalence is important.

Definition 5. *Let* $f, g : \mathbb{V}_n^{(p)} \to \mathbb{V}_m^{(p)}$ *be two functions. They are called extended affine equivalent (EA-equivalent) if one is obtained from another with an affine coordinate transformation on* $\mathbb{V}_n^{(p)}$ *or* $\mathbb{V}_m^{(p)}$ *and an addition of an affine function.*

In particular, for $\mathbb{V}_n^{(p)} = \mathbb{F}_p^n$, $\mathbb{V}_m^{(p)} = \mathbb{F}_p$, *taking the conventional dot product as inner product, we conclude that* f *and* g *are EA-equivalent if*

$$g(x) = cf(Ax + u) + v.x + d,$$

where A *is an invertible* $n \times n$ *matrix,* $u, v \in \mathbb{F}_p^n$, $c \in \mathbb{F}_p^*$ *and* $d \in \mathbb{F}_p$.

It is well known that if f is bent, then g is also bent, where f and g are as above. More generally, the absolute value of elements in the Walsh spectrum does not change under EA-Equivalence. To see this in the particular case $\mathbb{V}_n^{(p)} = \mathbb{F}_p^n$ and $\mathbb{V}_m^{(p)} = \mathbb{F}_p$, we give the following lemma, which is stated in (Çeşmelioğlu & Meidl,

2013).

Lemma 2. *Let $f : \mathbb{F}_p^n \to \mathbb{F}_p$ be a p-ary (or Boolean) function. Then for $u, v \in \mathbb{F}_p^n$ and $d \in \mathbb{F}_p$ we have the following properties of Walsh transform.*

(i) $\mathcal{W}_{f+d}(b) = \zeta_p^d \mathcal{W}_f(b)$.

(ii) If $f_v(x) = f(x) + v.x$ *then* $\mathcal{W}_{f_v}(b) = \mathcal{W}_f(b - v)$.

(iii) Given $g(x) = f(x+u)$*, the Walsh transform of* g *at* $b \in \mathbb{F}_p^n$ *is* $\mathcal{W}_g(b) = \zeta_p^{b.u} \mathcal{W}_f(b)$

(iv) If $L(x) = Ax$ *for an invertible matrix* A*, then* $\mathcal{W}_{f \circ L}(b) = \mathcal{W}_f((A^{-1})^T b)$*, where* A^T *is the transpose of the matrix* A.

Proof. (i) For any $b \in \mathbb{F}_p^n$, by the definition of Walsh transform, we have

$$\mathcal{W}_{f+d}(b) = \sum_{x \in \mathbb{F}_p^n} \zeta_p^{f(x)+d-b.x} = \zeta_p^d \sum_{x \in \mathbb{F}_p^n} \zeta_p^{f(x)-b.x} = \zeta_p^d \mathcal{W}_f(b).$$

(ii) For $v \in \mathbb{F}_p^n$, the Walsh transform of f_v at $b \in \mathbb{F}_p^n$ is

$$\mathcal{W}_{f_v}(b) = \sum_{x \in \mathbb{F}_p^n} \zeta_p^{f(x)+v.x-b.x} = \sum_{x \in \mathbb{F}_p^n} \zeta_p^{f(x)-(b-v).x} = \mathcal{W}_f(b-v)$$

(iii) If we replace $x+u$ with y, for any $b \in \mathbb{F}_p^n$ we obtain

$$\mathcal{W}_g(b) = \sum_{x \in \mathbb{F}_p^n} \zeta_p^{f(x+u)-b.x} = \sum_{y \in \mathbb{F}_p^n} \zeta_p^{f(y)-b.(y-u)} = \zeta_p^{b.u} \sum_{y \in \mathbb{F}_p^n} \zeta_p^{f(y)-b.y}.$$

Hence, we conclude that $\mathcal{W}_g(b) = \zeta_p^{b.u} \mathcal{W}_f(b)$.

(iv) If we make the change of variable $y = Ax$, then for $b \in \mathbb{F}_p^n$ we get

$$\mathcal{W}_{f \circ L} = \sum_{x \in \mathbb{F}_p^n} \zeta_p^{f(Ax)-b.x} = \sum_{y \in \mathbb{F}_p^n} \zeta_p^{f(y)-b.A^{-1}y} = \sum_{y \in \mathbb{F}_p^n} \zeta_p^{f(y)-((A^{-1})^T b).y} = \mathcal{W}_f((A^{-1})^T b).$$

□

In addition to preserving the absolute value of the Walsh transform, the transformations given in Lemma 2 preserve also the sign. This is not always true when we multiply f with a nonzero constant c. More precisely, if $f : \mathbb{F}_p^n \to \mathbb{F}_p$ is a weakly regular bent function, then cf is a weakly regular bent function with opposite sign

whenever n is odd and c is a non-square in $\mathbb{F}_p$, see (Çeşmelioğlu & Meidl, 2013, Theorem 1).

It is also well known that the algebraic degree of a function $f : \mathbb{V}_n^{(p)} \to \mathbb{F}_p$ is invariant under EA-equivalence, which is defined as follows.

If f is a function from the finite field $\mathbb{F}_{p^n}$ to $\mathbb{F}_p$, then f can be represented uniquely in polynomial form $f(x) = \sum_{j=0}^{p^n-1} c_j x^j$, where $c_j \in \mathbb{F}_{p^n}$. Each exponent l can be written in base p as $l = \sum_{i=0}^{n-1} l_i p^i$ with $0 \leq l_i \leq p-1$. Then the sum $\sum_{i=0}^{n-1} l_i$ is called the weight of l, and considering the terms with nonzero coefficient in the representation of f, the largest weight of the exponents is called the algebraic degree of f .

In the case that f is a function from $\mathbb{F}_p^n$ to $\mathbb{F}_p$, similarly f can be represented uniquely using polynomials in $\mathbb{F}_p[x_1, \ldots, x_n]/(x_1 - x_1^p, \ldots, x_n - x_n^p)$. To be precise, f is uniquely expressed in the form

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

where $c_{(j_1,\ldots,j_n)} \in \mathbb{F}_p$. This representation is called the algebraic normal form (ANF) of f. Then the largest degree of all monomials with a nonzero coefficient is called the algebraic degree of f, which will be denoted by $deg(f)$. Hence, we have $deg(f) = max\{j_1 + \ldots + j_n : c_{(j_1,\cdots,j_n)} \neq 0\}$. Affine functions are of algebraic degree 1, and functions with algebraic degree 2 are called quadratic functions.

We know that any quadratic bent function $f : \mathbb{F}_2^n \to \mathbb{F}_2$ is EA-equivalent to the function

$$q(x_1, \ldots, x_n) = x_1x_2 + x_3x_4 + \cdots + x_{n-1}x_n.$$

It is not valid for odd p. In this case, using properties (i) and (ii) given in Lemma 2 we leave out the affine part and consider the functions $f : \mathbb{F}_p^n \to \mathbb{F}_p$ of the form $f(x_1, \ldots, x_n) = \sum_{1 \leq i,j \leq n} c_{ij} x_i x_j$, where $c_{ij} \in \mathbb{F}_p$. Then f can be represented by

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

where A is a symmetric $n \times n$ matrix over $\mathbb{F}_p$. Every such matrix can be transformed into a diagonal matrix with a coordinate transformation. Then by (Çeşmelioğlu & Meidl, 2013, Proposition 1) and its proof, bent functions of this form are exactly as follows.

Proposition 1. *A quadratic function $q(x_1, \ldots, x_n) = d_1x_1^2 + \cdots + d_nx_n^2$ from $\mathbb{F}_p^n$ to*

$\mathbb{F}_p$ is bent if and only if $d_i \neq 0$ for all i. In this case, the Walsh transform of q at any $b \in \mathbb{F}_p^n$ is

$$\mathcal{W}_q(b) = \begin{cases} \eta(\Delta) p^{n/2} \zeta_p^{q^*(b)} & : \quad p \equiv 1 \bmod 4, \\ \eta(\Delta) i^n p^{n/2} \zeta_p^{q^*(b)} & : \quad p \equiv 3 \bmod 4, \end{cases} \tag{1.7}$$

where $\Delta = \prod_i^n d_i$, which is called the discriminant of q, and η denotes the quadratic character over $\mathbb{F}_p$. Moreover, the dual q^* of q is

$$q^*(x_1, \ldots, x_n) = -\frac{x_1^2}{4d_1} - \cdots - \frac{x_n^2}{4d_n}.$$

By (Serre, 1973, pp. 34-35) every quadratic function q, given as in Proposition 1, is EA-equivalent to $q_1(x_1, \ldots, x_n) = x_1^2 + \cdots + x_n^2$ or to the quadratic function $q_2(x_1, \ldots, x_n) = x_1^2 + \cdots + a x_n^2$ for some nonsquare a in $\mathbb{F}_p$. More precisely, if n is odd, any quadratic bent function is EA-equivalent to q_1, and for even n a quadratic bent function q is EA-equivalent to q_2 in the case the discriminant of q is a nonsquare and is EA-equivalent to q_1 otherwise.

1.4 Primary Constructions of Bent Functions

There are two big primary construction of bent functions, one is the class of Maiorana-McFarland bent functions, and the other is the class of bent functions obtained from spreads and partial spreads.

1.4.1. Maiorana-McFarland bent functions

The p-ary (and also Boolean) version of the Maiorana-McFarland bent functions is as follows:

Theorem 1. *Let $\pi : \mathbb{F}_{p^m} \to \mathbb{F}_{p^m}$ and $g : \mathbb{F}_{p^m} \to \mathbb{F}_p$ be two functions. Then the function f from $\mathbb{F}_{p^m} \times \mathbb{F}_{p^m}$ to $\mathbb{F}_p$ defined by*

$$f(x, y) = \mathrm{Tr}_1^m(x\pi(y)) + g(y),$$

is bent if and only if π is a permutation of $\mathbb{F}_{p^m}$.

Proof. Suppose π is a permutation. We can take the inner product for $\mathbb{F}_{p^m} \times \mathbb{F}_{p^m}$ as $\langle (x_1, x_2), (y_1, y_2) \rangle_{2m} = \mathrm{Tr}_1^m(x_1 y_1 + x_2 y_2)$. Then for any $(u, v) \in \mathbb{F}_{p^m} \times \mathbb{F}_{p^m}$, we have

$$\begin{aligned} W_f(u,v) &= \sum_{x \in \mathbb{F}_{p^m}, y \in \mathbb{F}_{p^m}} \zeta_p^{f(x,y) - \mathrm{Tr}_1^m(ux+vy)} \\ &= \sum_{x \in \mathbb{F}_{p^m}, y \in \mathbb{F}_{p^m}} \zeta_p^{\mathrm{Tr}_1^m(x\pi(y)) + g(y) - \mathrm{Tr}_1^m(ux+vy)} \\ &= \sum_{y \in \mathbb{F}_{p^m}} \zeta_p^{g(y) - \mathrm{Tr}_1^m(vy)} \sum_{x \in \mathbb{F}_{p^m}} \zeta_p^{\mathrm{Tr}_1^m((\pi(y)-u)x)} \\ &= p^m \zeta_p^{g(\pi^{-1}(u)) - \mathrm{Tr}_1^m(v\pi^{-1}(u))}. \end{aligned}$$

Hence, f is a regular bent function with dual $f^*(x, y) = g(\pi^{-1}(x)) - \mathrm{Tr}_1^m(y\pi^{-1}(x))$. Conversely, let $t \in \mathbb{F}_{p^m}$ be such that $\pi(y) \neq t$ for any $y \in \mathbb{F}_{p^m}$, that is, π is not a permutation. Then for any $w \in \mathbb{F}_{p^m}$ the Walsh coefficient of f at (t, w) is

$$\begin{aligned} W_f(t,w) &= \sum_{x \in \mathbb{F}_{p^m}, y \in \mathbb{F}_{p^m}} \zeta_p^{\mathrm{Tr}_1^m(x\pi(y)) + g(y) - \mathrm{Tr}_1^m(tx+wy)} \\ &= \sum_{y \in \mathbb{F}_{p^m}} \zeta_p^{g(y) - \mathrm{Tr}_1^m(wy)} \sum_{x \in \mathbb{F}_{p^m}} \zeta_p^{\mathrm{Tr}_1^m((\pi(y)-t)x)} \\ &= 0. \end{aligned}$$

Hence, f is not bent. □

Maiorana-McFarland bent functions defined in the previous theorem have the following equivalent characterization.

Let $f : \mathbb{F}_{p^m} \times \mathbb{F}_{p^m} \to \mathbb{F}_p$ be a Maiorana-McFarland bent function given by

$$f(x, y) = \mathrm{Tr}_1^m(x\pi(y)) + g(y),$$

where $\pi : \mathbb{F}_{p^m} \to \mathbb{F}_{p^m}$ is a permutation and $g : \mathbb{F}_{p^m} \to \mathbb{F}_p$ is an arbitrary function. Then for each (fixed) $y \in \mathbb{F}_{p^m}$, we have

$$f(x, y) = L_y(x) + c_y =: f_y(x),$$

where $L_y(x) = \mathrm{Tr}_1^m(x\pi(y))$ and $c_y = g(y)$ (that is, f_y is affine). Hence, for any

$b \in \mathbb{F}_{p^m}$, the Walsh transform of f_y at b is

$$\mathcal{W}_{f_y}(b) = \sum_{x \in \mathbb{F}_{p^m}} \zeta_p^{L_y(x)+c_y-\mathrm{Tr}_1^m(bx)} = \zeta_p^{c_y} \sum_{x \in \mathbb{F}_{p^m}} \zeta_p^{\mathrm{Tr}_1^m(x(\pi(y)-b))},$$

which implies $\mathcal{W}_{f_y}(b) = 0$ if and only if $b \neq \pi(y)$. In other words, the support of $\mathcal{W}_{f_y}$ is the set $supp(\mathcal{W}_{f_y}) = \{\pi(y)\}$ with one element. Since π is a permutation, we also have $supp(\mathcal{W}_{f_y}) \cap supp(\mathcal{W}_{f_z}) = \emptyset$ if $y \neq z$.

Conversely, for each $y \in \mathbb{F}_{p^m}$, let $f_y : \mathbb{F}_{p^m} \to \mathbb{F}_p$ be an affine function with the property $supp(\mathcal{W}_{f_y}) \cap supp(\mathcal{W}_{f_z}) = \emptyset$ whenever $y \neq z$. Since for $y \in \mathbb{F}_{p^m}$ the function f_y is affine, we have $f_y(x) = \mathrm{Tr}_1^m(a_y x) + c_y$ for some $a_y \in \mathbb{F}_{p^m}$ and $c_y \in \mathbb{F}_p$ (depending on y). Then the Walsh transform of f_y at $b \in \mathbb{F}_{p^m}$ is

$$\mathcal{W}_{f_y}(b) = \sum_{x \in \mathbb{F}_{p^m}} \zeta_p^{\mathrm{Tr}_1^m(a_y x)+c_y-\mathrm{Tr}_1^m(bx)} = \zeta_p^{c_y} \sum_{x \in \mathbb{F}_{p^m}} \zeta_p^{\mathrm{Tr}_1^m(x(a_y-b))}.$$

Hence, the support of $\mathcal{W}_{f_y}$ is the one-element set $supp(\mathcal{W}_{f_y}) = \{a_y\}$. Accordingly, we can define a function $\pi : \mathbb{F}_{p^m} \to \mathbb{F}_{p^m}$ by $\pi(y) = a_y$, which is a permutation of $\mathbb{F}_{p^m}$, as $supp(\mathcal{W}_{f_y}) \cap supp(\mathcal{W}_{f_z}) = \emptyset$ if $y \neq z$. Then the function $f(x, y) = f_y(x) = \mathrm{Tr}_1^m(\pi(y)x) + g(y)$, with $g(y) = c_y$, is a Maiorana-McFarland bent function.

One can also show the vectorial version of the Maiorana-McFarland bent functions, the special case of which was shown in Example 2.

Theorem 2. *Let $\pi : \mathbb{F}_{p^m} \to \mathbb{F}_{p^m}$ and $G : \mathbb{F}_{p^m} \to \mathbb{F}_{p^m}$ be two functions. Then the function $F : \mathbb{F}_{p^m} \times \mathbb{F}_{p^m} \to \mathbb{F}_{p^m}$ defined by*

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

is bent if and only if π is a permutation.

Proof. Let π be a permutation of $\mathbb{F}_{p^m}$. For a nonzero element c of $\mathbb{F}_{p^m}$, the component function F_c of F is given by $F_c(x, y) = \mathrm{Tr}_1^m(cx\pi(y) + cG(y))$. Then for any

$u, v \in \mathbb{F}_{p^m}$, the Walsh coefficient of F_c at (u, v) is

$$\begin{aligned} W_{F_c}(u,v) &= \sum_{x\in\mathbb{F}_{p^m}, y\in\mathbb{F}_{p^m}} \zeta_p^{F_c(x,y)-\mathrm{Tr}_1^m(ux+vy)} \\ &= \sum_{x\in\mathbb{F}_{p^m}, y\in\mathbb{F}_{p^m}} \zeta_p^{\mathrm{Tr}_1^m(cx\pi(y)+cG(y))-\mathrm{Tr}_1^m(ux+vy)} \\ &= \sum_{y\in\mathbb{F}_{p^m}} \zeta_p^{\mathrm{Tr}_1^m(cG(y)-vy)} \sum_{x\in\mathbb{F}_{p^m}} \zeta_p^{\mathrm{Tr}_1^m((c\pi(y)-u)x)} \\ &= p^m \zeta_p^{\mathrm{Tr}_1^m(cG(\pi^{-1}(\frac{u}{c}))-v\pi^{-1}(\frac{u}{c}))}. \end{aligned}$$

Therefore, any component function F_c of F is bent, which implies that F is bent. The converse is almost the same as the proof of Theorem 1, so it is omitted. □

1.4.2. Partial spread bent functions

Definition 6. *A partial spread of a vector space $\mathbb{V}_n^{(p)}$ (over $\mathbb{F}_p$), $n = 2m$, is a collection $\mathcal{S} = \{U_1, U_2, \ldots, U_K\}$ of m-dimensional subspaces of $\mathbb{V}_n^{(p)}$, which pairwise intersects trivially. If $K = p^m + 1$, hence every nonzero element of $\mathbb{V}_n^{(p)}$ is exactly in one subspace, then $\mathcal{S}$ is called a (complete) spread.*

Let $\mathbb{V}_n^{(p)} = \mathbb{F}_{p^m} \times \mathbb{F}_{p^m}$. Then the collection $\mathcal{S} = \{U, U_s : s \in \mathbb{F}_{p^m}\}$, with $U = \{(0, y) : y \in \mathbb{F}_{p^m}\}$ and $U_s = \{(x, sx) : x \in \mathbb{F}_{p^m}\}$ for $s \in \mathbb{F}_{p^m}$, forms a spread, called Desarguesian spread.

Suppose that $\mathcal{S} = \{U_0, U_1, \ldots, U_{p^m}\}$ is a spread of a vector space $\mathbb{V}_n^{(p)}$ (over $\mathbb{F}_p$), $n = 2m$. We get bent functions into an arbitrary abelian group G of order p^k with $1 \le k \le m$ as follows:

(i) For every $c \in G$, nonzero elements of exactly p^{m-k} of the subspaces U_i, $1 \le i \le p^m$, are mapped to c.

(ii) The elements of U_0 are mapped to some fixed $c_0 \in G$.

To see this, let us take $\mathbb{V}_n^{(p)} = \mathbb{F}_{p^m} \times \mathbb{F}_{p^m}$ and $G = \mathbb{V}_m^{(p)}$, an elementary abelian group of order p^m (for simplicity). Suppose that $F : \mathbb{F}_{p^m} \times \mathbb{F}_{p^m} \to \mathbb{V}_m^{(p)}$ is such that for every element $c \neq c_0$, of $\mathbb{V}_m^{(p)}$, the preimage set of c is $F^{-1}(c) =: U_c^*$, and $F^{-1}(c_0) =: U_0 \cup U_{c_0}^*$, where U_c and U_{c_0} are elements of $\mathcal{S}$. Then for any $\beta \in \mathbb{V}_m^{(p)} \setminus \{0_{\mathbb{V}_m^{(p)}}\}$ and

$(u,v) \in \mathbb{F}_{p^m} \times \mathbb{F}_{p^m}$, we have

$$\begin{aligned}
W_{F_\beta}(u,v) &= \sum_{x\in\mathbb{F}_{p^m}, y\in\mathbb{F}_{p^m}} \zeta_p^{F_\beta(x,y)-\mathrm{Tr}_1^m(ux+vy)} \\
&= \sum_{x\in\mathbb{F}_{p^m}, y\in\mathbb{F}_{p^m}} \zeta_p^{\langle\beta,F(x,y)\rangle_m-\mathrm{Tr}_1^m(ux+vy)} \\
&= \sum_{c\in\mathbb{V}_m^{(p)}} \sum_{(x,y)\in U_c^*} \zeta_p^{\langle\beta,c\rangle_m-\mathrm{Tr}_1^m(ux+vy)} + \sum_{(x,y)\in U_0} \zeta_p^{\langle\beta,c_0\rangle_m-\mathrm{Tr}_1^m(ux+vy)} \\
&= \sum_{c\in\mathbb{V}_m^{(p)}} \sum_{(x,y)\in U_c} \zeta_p^{\langle\beta,c\rangle_m-\mathrm{Tr}_1^m(ux+vy)} - \sum_{c\in\mathbb{V}_m^{(p)}} \zeta_p^{\langle\beta,c\rangle_m} \\
&\quad + \sum_{(x,y)\in U_0} \zeta_p^{\langle\beta,c_0\rangle_m-\mathrm{Tr}_1^m(ux+vy)} \\
&= \sum_{c\in\mathbb{V}_m^{(p)}} \sum_{(x,y)\in U_c} \zeta_p^{\langle\beta,c\rangle_m-\mathrm{Tr}_1^m(ux+vy)} + \sum_{(x,y)\in U_0} \zeta_p^{\langle\beta,c_0\rangle_m-\mathrm{Tr}_1^m(ux+vy)}, \qquad (1.8)
\end{aligned}$$

where the last equality comes from the fact that $\sum_{c\in\mathbb{V}_m^{(p)}} \zeta_p^{\langle\beta,c\rangle_m} = 0$ for $\beta \neq 0_{\mathbb{V}_m^{(p)}}$. In the case $(u,v) = (0,0)$, using Equation (1.8), we get

$$\begin{aligned}
W_{F_\beta}(0,0) &= \sum_{c\in\mathbb{V}_m^{(p)}} \sum_{(x,y)\in U_c} \zeta_p^{\langle\beta,c\rangle_m} + \sum_{(x,y)\in U_0} \zeta_p^{\langle\beta,c_0\rangle_m} \\
&= p^m \sum_{c\in\mathbb{V}_m^{(p)}} \zeta_p^{\langle\beta,c\rangle_m} + p^m \zeta_p^{\langle\beta,c_0\rangle_m} = p^m \zeta_p^{\langle\beta,c_0\rangle_m}.
\end{aligned}$$

Since $\mathcal{S}$ is a (complete) spread, in the case $(u,v) \neq (0,0)$ the inner product $\langle(u,v),(x,y)\rangle_{2m} = \mathrm{Tr}_1^m(ux+vy)$ is zero on exactly one spread element, say U_t, $0 \leq t \leq p^m$, and is balanced on the remaining spread elements. Hence, in this case, using Equation (1.8), we obtain

$$\begin{aligned}
W_{F_\beta}(u,v) &= \sum_{c\in\mathbb{V}_m^{(p)}} \zeta_p^{\langle\beta,c\rangle_m} \sum_{(x,y)\in U_c} \zeta_p^{-\mathrm{Tr}_1^m(ux+vy)} + \zeta_p^{\langle\beta,c_0\rangle_m} \sum_{(x,y)\in U_0} \zeta_p^{-\mathrm{Tr}_1^m(ux+vy)} \\
&= p^m \zeta_p^{\langle\beta,t\rangle_m}.
\end{aligned}$$

Then any component function F_β of F is (regular) bent, so F is bent.

Similarly, one can obtain bent functions into various abelian groups from partial spreads of $\mathbb{V}_n^{(p)}$ with sufficiently many subspaces as follows.

Theorem 3. *Suppose that $n = 2m$, $\mathbb{V}_n^{(p)}$ is a vector space over $\mathbb{F}_p$ and G is an arbitrary abelian group of order p^k, where $1 \leq k \leq m$.*

(i) Let $\mathcal{S} = \{U_1, U_2, \ldots, U_{(p^k-1)p^{m-k}}\}$ be a partial spread of $\mathbb{V}_n^{(p)}$, and let the func-

tion $F : \mathbb{V}_n^{(p)} \to G$ *be defined so that every nonzero element of* G *has as a preimage the union of exactly* p^{m-k} *subspaces of* $\mathcal{S}$*, without* $0 \in \mathbb{V}_n^{(p)}$*, and all other elements are mapped to* $0 \in G$*. Then* F *is a bent function.*

(ii) Similarly, let $\mathcal{S} = \{U_1, U_2, \ldots, U_{(p^k-1)p^{m-k}+1}\}$ *be a partial spread of* $\mathbb{V}_n^{(p)}$*. Then the function* $F : \mathbb{V}_n^{(p)} \to G$ *that is defined as below is a bent function.*

- *For some fixed* $c_0 \in G^*$*, the preimage of* c_0 *is the union of* $p^{m-k}+1$ *subspaces of* $\mathcal{S}$*, including* $0 \in \mathbb{V}_n^{(p)}$*.*
- *For any other element* $c \in G^*$ *with* $c \neq c_0$*, the preimage of* c *is the union of* p^{m-k} *subspaces of* $\mathcal{S}$*, without* $0 \in \mathbb{V}_n^{(p)}$*.*
- *The remaining elements of* $\mathbb{V}_n^{(p)}$ *are mapped to* $0 \in G$*.*

Note that with the above notation, for $k = 1$ the function $F : \mathbb{V}_n^{(p)} \to \mathbb{F}_p$ which is defined in Theorem 3(i) is called PS^- bent, and which is given in Theorem 3(ii) is called a PS^+ bent function.

The proof of Theorem 3(i) for $p = 2$ is given in (Meidl & Pirsic, 2021). We will present the proof of Theorem 3(ii) for $k = 1$, that is, for PS^+ bent functions using the same method.

Let $f : \mathbb{V}_n^{(p)} \to \mathbb{F}_p$ be a function defined as in Theorem 3(ii), that is, we have $f^{-1}(c_0) = \bigcup_{i=1}^{p^{m-1}} U_{c_0,i} \cup U_{c_0,0}$, and for any other nonzero element c of $\mathbb{F}_p$ the preimage is $f^{-1}(c) = \bigcup_{i=1}^{p^{m-1}} U_{c,i}^*$ (after reindexing the elements of $\mathcal{S}$), and the remaining elements of $\mathbb{V}_n^{(p)}$ are mapped to 0. Then for any $u \in \mathbb{V}_n^{(p)}$ the Walsh coefficient of f at u is

$$W_f(u) = \sum_{x \in \mathbb{V}_n^{(p)}} \zeta_p^{f(x)-\langle u,x\rangle_n}$$

(1.9)

$$= \sum_{c \in \mathbb{F}_p^*} \sum_{i=1}^{p^{m-1}} \sum_{x \in U_{c,i}^*} \zeta_p^{c-\langle u,x\rangle_n} + \sum_{x \in U_{c_0,0}} \zeta_p^{c_0-\langle u,x\rangle_n} + \sum_{x \in \mathbb{V}_n^{(p)} \setminus \bigcup \mathcal{S}} \zeta_p^{-\langle u,x\rangle_n}$$

(1.10)

$$= \sum_{c \in \mathbb{F}_p^*} \sum_{i=1}^{p^{m-1}} \sum_{x \in U_{c,i}} \zeta_p^{c-\langle u,x\rangle_n} - \sum_{c \in \mathbb{F}_p^*} \sum_{i=1}^{p^{m-1}} \zeta_p^{c} + \sum_{x \in U_{c_0,0}} \zeta_p^{c_0-\langle u,x\rangle_n} + \sum_{x \in \mathbb{V}_n^{(p)} \setminus \bigcup \mathcal{S}} \zeta_p^{-\langle u,x\rangle_n}.$$

In the case $u = 0$, using Equation (1.9) we obtain

$$\begin{aligned} W_f(0) &= (p^m-1)p^{m-1}\sum_{c\in\mathbb{F}_p^*}\zeta_p^c + p^m\zeta_p^{c_0} \\ &\quad + p^{2m} - ((p-1)p^{m-1}(p^m-1)+p^m) \\ &= (p^m-1)p^{m-1}(-1) + p^m\zeta_p^{c_0} + (p^{2m-1}-p^{m-1}) \\ &= p^m\zeta_p^{c_0}. \end{aligned}$$

Since $\mathcal{S}$ is a partial spread, in the case $u \neq 0$ the inner product $\langle u, x\rangle_n$ is zero on at most one of the elements of $\mathcal{S}$ and is balanced on the remaining (partial) spread elements. If $L(x) := \langle u, x\rangle_n$ is not zero on any of the spread elements, then using Equation (1.10), we get

$$\begin{aligned} W_f(u) &= \sum_{c\in\mathbb{F}_p^*}\zeta_p^c\sum_{i=1}^{p^{m-1}}\sum_{x\in U_{c,i}}\zeta_p^{-\langle u,x\rangle_n} - p^{m-1}(-1) + \zeta_p^{c_0}\sum_{x\in U_{c_0,0}}\zeta_p^{-\langle u,x\rangle_n} \\ &\quad + \sum_{x\in\mathbb{V}_n^{(p)}\setminus\bigcup\mathcal{S}}\zeta_p^{-\langle u,x\rangle_n} \\ &= p^{m-1} + \sum_{x\in\mathbb{V}_n^{(p)}\setminus\cup_{c\in\mathbb{F}_p^*}\cup_{i=1}^{p^{m-1}}U_{c,i}^*\cup U_{c_0,0}}\zeta_p^{-\langle u,x\rangle_n} \\ &= p^{m-1} + (0 - ((p-1)p^{m-1}(-1)+0)) = p^m. \end{aligned}$$

Note that here we used the fact that $\langle u, x\rangle_n$ is balanced on any of the (partial) spread elements (and on $V_n^{(p)}$), that is $\sum_{x\in U_{c_0,0}}\zeta_p^{-\langle u,x\rangle_n} = 0$ and $\sum_{x\in U_{c,i}^*}\zeta_p^{-\langle u,x\rangle_n} = -1$ for all $c \in \mathbb{F}_p^*$ and $i = 1, \ldots, p^{m-1}$.

Finally, in the case $L(x) = \langle u, x\rangle_n = 0$ on some $U_{t,j}$, where $t \in \mathbb{F}_p^*$ and $j \in \{0, 1, \ldots, p^{m-1}\}$, observing that $\bigcup\mathcal{S} = \bigcup_{\substack{c\in\mathbb{F}_p^*\setminus\{t\} \\ or\ i\neq j}} U_{c,i}^*\bigcup U_{t,j}$ and using Equation (1.10), we get

$$\begin{aligned} W_f(u) &= \sum_{c\in\mathbb{F}_p^*}\zeta_p^c\sum_{i=1}^{p^{m-1}}\sum_{x\in U_{c,i}}\zeta_p^{-\langle u,x\rangle_n} - p^{m-1}(-1) + \zeta_p^{c_0}\sum_{x\in U_{c_0,0}}\zeta_p^{-\langle u,x\rangle_n} \\ &\quad + \sum_{x\in\mathbb{V}_n^{(p)}\setminus\bigcup\mathcal{S}}\zeta_p^{-\langle u,x\rangle_n} \\ &= p^m\zeta_p^t + p^{m-1} - ((p-1)p^{m-1}(-1)+p^m) = p^m\zeta_p^t \end{aligned}$$

Hence, we have $|W_f(u)| = p^m$ for any $u \in \mathbb{V}_n^{(p)}$, which implies that f is a bent function.

Partial spread bent functions obtained from the Desarguesian spread are called PS_{ap} bent functions. For this class of bent functions, we have an explicit representation. Let $B : \mathbb{F}_{p^m} \to \mathbb{F}_p$ be a balanced function, that is, for each $i \in \mathbb{F}_p$, the preimage set of i contains exactly p^{m-1} elements of F_{p^m}, and let $B(0) = 0$. Then the function $F : \mathbb{F}_{p^m} \times \mathbb{F}_{p^m} \to \mathbb{F}_p$, which is given by

$$F(x, y) = B(yx^{p^m-2})$$

is a PS_{ap} bent function, and every PS_{ap} bent function is of this form.

1.5 Secondary Constructions of Bent Functions

In this section, we will present some constructions of bent functions from known bent functions or some other functions like plateaued functions.

1.5.1. Direct sum of bent functions

Given two bent functions $f : \mathbb{V}_n^{(p)} \to \mathbb{F}_p$ and $g : \mathbb{V}_m^{(p)} \to \mathbb{F}_p$, where n and m are some positive integers, we can construct a function h from $\mathbb{V}_n^{(p)} \times \mathbb{V}_m^{(p)}$ to $\mathbb{F}_p$ via

$$h(x, y) = f(x) + g(y).$$

In this way, we obtain a bent function on a larger dimensional vector space.

Proposition 2. *Let $h : \mathbb{V}_n^{(p)} \times \mathbb{V}_m^{(p)} \to \mathbb{F}_p$ be a function defined as above. Then $h(x, y) = f(x) + g(y)$ is a bent function if and only if $f : \mathbb{V}_n^{(p)} \to \mathbb{F}_p$ and $g : \mathbb{V}_m^{(p)} \to \mathbb{F}_p$ are bent functions.*

Proof. Suppose that $f : \mathbb{V}_n^{(p)} \to \mathbb{F}_p$ and $g : \mathbb{V}_m^{(p)} \to \mathbb{F}_p$ are bent functions. Then the

Walsh transform of h at any $(u,v) \in \mathbb{V}_n^{(p)} \times \mathbb{V}_m^{(p)}$ is

$$\begin{aligned}
W_h(u,v) &= \sum_{x\in\mathbb{V}_n^{(p)},\, y\in\mathbb{V}_m^{(p)}} \zeta_p^{h(x,y)-\langle u,x\rangle_n-\langle v,y\rangle_m} \\
&= \sum_{x\in\mathbb{V}_n^{(p)},\, y\in\mathbb{V}_m^{(p)}} \zeta_p^{f(x)+g(y)-\langle u,x\rangle_n-\langle v,y\rangle_m} \\
&= \sum_{x\in\mathbb{V}_n^{(p)}} \zeta_p^{f(x)-\langle u,x\rangle_n} \sum_{y\in\mathbb{V}_m^{(p)}} \zeta_p^{g(y)-\langle v,y\rangle_m} \\
&= W_f(u)W_g(v) \\
&= (\varepsilon_{f,u} p^{n/2} \zeta_p^{f^*(u)})(\varepsilon_{g,v} p^{m/2} \zeta_p^{g^*(v)}) \\
&= \varepsilon_{f,u}\varepsilon_{g,v} p^{(n+m)/2} \zeta_p^{f^*(u)+g^*(v)},
\end{aligned}$$

where $\varepsilon_{f,u}, \varepsilon_{g,v} \in \{\pm 1, \pm i\}$. Hence, h is a bent function.

Conversely, let $h(x,y) = f(x) + g(y)$ be a bent function for some p-ary (or Boolean) functions $f : \mathbb{V}_n^{(p)} \to \mathbb{F}_p$ and $g : \mathbb{V}_m^{(p)} \to \mathbb{F}_p$. Since $h : \mathbb{V}_n^{(p)} \times \mathbb{V}_m^{(p)} \to \mathbb{F}_p$ is bent, for all $(u,v) \in \mathbb{V}_n^{(p)} \times \mathbb{V}_m^{(p)}$, we have $|W_h(u,v)| = p^{(n+m)/2}$. To obtain a contradiction, we suppose that $f : \mathbb{V}_n^{(p)} \to \mathbb{F}_p$ is not bent. By Parseval's identity, we know $\sum_{x\in\mathbb{V}_n^{(p)}} |W_f(x)|^2 = p^{2n}$. Hence, we may assume that $|W_f(u_1)| < p^{n/2}$ for some $u_1 \in \mathbb{V}_n^{(p)}$. If $g : \mathbb{V}_m^{(p)} \to \mathbb{F}_p$ is bent, then by the first part of the proof for any $v \in \mathbb{V}_m^{(p)}$ we have

$$|W_h(u_1,v)| = |W_f(u_1)W_g(v)| = |W_f(u_1)||W_g(v)| < p^{n/2}p^{m/2} = p^{(n+m)/2},$$

which is not possible as h is bent. In the case that, $g : \mathbb{V}_m^{(p)} \to \mathbb{F}_p$ is not bent, using again Parseval's identity, we get $|W_g(v_1)| < p^{m/2}$ for some $v_1 \in \mathbb{V}_m^{(p)}$. Thus,

$$|W_h(u_1,v_1)| = |W_f(u_1)W_g(v_1)| = |W_f(u_1)||W_g(v_1)| < p^{n/2}p^{m/2} = p^{(n+m)/2},$$

which contradicts again h being bent. Therefore, f is bent. Similarly, g is also bent. □

Remark 2. *As one can see (from the proof of Proposition 2), the direct sum of a weakly regular and a non-weakly regular bent function is non-weakly regular, and the direct sum of two weakly regular bent functions is again a weakly regular bent function.*

For vectorial bent functions $F : \mathbb{V}_n^{(p)} \to \mathbb{V}_k^{(p)}$ and $G : \mathbb{V}_m^{(p)} \to \mathbb{V}_k^{(p)}$ the same construction is valid since the function $H(x,y) = F(x) + G(y)$ is bent whenever F and G are bent.

1.5.2. Rothaus's construction

Another construction of bent functions is given by Rothaus as follows. If f_1, f_2 and f_3 are three Boolean bent functions on $\mathbb{F}_2^n$ with $f_1+f_2+f_3$ also bent, then the function f defined by

$$\begin{aligned} f(x,x_1,x_2) = {} & f_1(x)f_2(x)+f_1(x)f_3(x)+f_2(x)f_3(x) \\ & +(f_1(x)+f_2(x))x_1+(f_1(x)+f_3(x))x_2+x_1x_2 \end{aligned}$$

is a bent function from $\mathbb{F}_2^n \times \mathbb{F}_2 \times \mathbb{F}_2$ to $\mathbb{F}_2$.

A generalization of Rothaus's construction is presented by Meidl in (Meidl, 2016).

Theorem 4. *(Meidl, 2016) Let g_1, g_2 and g_3 be three linearly independent component functions of a vectorial bent function $G : \mathbb{V}_n^{(p)} \to \mathbb{V}_m^{(p)}$, $m \geq 3$. Then for some elements a, b, c of $\mathbb{F}_p$, the function $g : \mathbb{F}_p^n \times \mathbb{F}_p \times \mathbb{F}_p \to \mathbb{F}_p$ given by*

$$\begin{aligned} g(x,x_1,x_2) = {} & g_1^2(x)-g_1(x)g_2(x)+g_2(x)g_3(x)-g_1(x)g_3(x)+ag_1(x)+bg_2(x) \\ & +cg_3(x)+(g_2(x)-g_1(x))x_1+(g_3(x)-g_1(x))x_2+x_1x_2 \end{aligned}$$

is bent if and only if $a+b+c \neq 0$.

Trivially, for $p=2$ the function g given in Theorem 4 is bent if and only if $a+b+c=1$. Taking $a=1$ and $b=c=0$, we obtain the construction of Rothaus for Boolean functions.

1.5.3. Some other constructions

In (Leander & McGuire, 2009), a construction of Boolean bent functions from near-bent functions was presented. If $f : \mathbb{V}_n^{(2)} \to \mathbb{F}_2$ is a function that is near-bent, then for any $a \in \mathbb{V}_n^{(2)}$, the absolute value of the Walsh transform $\mathcal{W}_f(a)$ is 0 or $2^{\frac{n+1}{2}}$. Hence, using Parseval's identity, one can easily show that the support of $\mathcal{W}_f$ contains exactly 2^{n-1} elements. In (Leander & McGuire, 2009), using such functions, the following secondary construction of Boolean bent functions is shown.

Theorem 5. *Let $g, h : \mathbb{V}_n^{(2)} \to \mathbb{F}_2$ be two near-bent functions with the property that*

supp$(\mathcal{W}_g) \cap$ *supp*$(\mathcal{W}_h) = \emptyset$. *Then the function* $f : \mathbb{V}_n^{(2)} \times \mathbb{F}_2 \to \mathbb{F}_2$ *given by*

$$f(x,y) = yg(x) + (y+1)h(x)$$

is bent.

The most well-known examples of Boolean near-bent functions are the functions $f(x) = \mathrm{Tr}_1^n(x^{2^k+1})$, where k is relatively prime to n and n is odd. Such quadratic functions are called Gold functions. Gold showed $\mathcal{W}_f(x) = 0$ if and only if $\mathrm{Tr}_1^n(x) = 0$, see (Gold, 1968).

Example 3. *(Leander & McGuire, 2009, Corollary 5) Let* n *be an odd integer with* $n > 7$, *and* g_1, g_2 *be two Boolean functions on the finite field* $\mathbb{F}_{2^n}$, *given by* $g_1(x) = \mathrm{Tr}_1^n(x^9)$ *and* $g_2(x) = \mathrm{Tr}_1^n(x^5)$. *Then* g_1 *and* g_2 *are Gold functions and the support of their Walsh transform is*

$$H = \{x \in \mathbb{F}_{2^n} : \mathrm{Tr}_1^n(x) \neq 0\}.$$

Let $h : \mathbb{F}_{2^n} \to \mathbb{F}_2$ *be a Boolean function defined by* $h(x) = \mathrm{Tr}_1^n(x^5 + x)$. *Then for* $a \in \mathbb{F}_{2^n}$ *the Walsh transform of* h *at* a *is*

$$\begin{aligned}\mathcal{W}_h(a) &= \sum_{x \in \mathbb{F}_{2^n}} (-1)^{\mathrm{Tr}_1^n(x^5+x)+\mathrm{Tr}_1^n(ax)} \\ &= \sum_{x \in \mathbb{F}_{2^n}} (-1)^{\mathrm{Tr}_1^n(x^5)+\mathrm{Tr}_1^n((a+1)x)} \\ &= \mathcal{W}_{g_2}(a+1).\end{aligned}$$

Since n *is odd, we have* $\mathrm{Tr}_1^n(a) = 0$ *if and only if* $\mathrm{Tr}_1^n(a+1) = 1$ *for any* $a \in \mathbb{F}_{2^n}$. *Hence,* h *is a near-bent function whose support consists of elements (in* $\mathbb{F}_{2^n}$*) with zero trace. Then using Theorem 5, we can conclude that the function given by* $f(x,y) = y\mathrm{Tr}_1^n(x^9) + (y+1)\mathrm{Tr}_1^n(x^5+x)$ *is a Boolean bent function on* $\mathbb{F}_{2^n} \times \mathbb{F}_2$ *with degree* 3.

A p-ary version of Theorem 5 was proven in (Çeşmelioğlu et al., 2013b).

Theorem 6. *Let* p *be an odd prime and* $f_i : \mathbb{V}_n^{(p)} \to \mathbb{F}_p$, $0 \leq i \leq p-1$ *be* p *near-bent functions such that* *supp*$(\mathcal{W}_i) \cap$ *supp*$(\mathcal{W}_j) = \emptyset$ *for* $i \neq j$. *Then the function* $F : \mathbb{V}_n^{(p)} \times \mathbb{F}_p \to \mathbb{F}_p$ *given by*

$$F(x,y) = f_y(x)$$

is bent.

Unlike the Boolean case, there is no quadratic near-bent function $f(x) = \mathrm{Tr}_1^n(cx^{p^k+1})$, $c \in \mathbb{F}_{p^n}$, for odd p. However, two classes of quadratic binomial near-bent functions were found, see (Çeşmelioğlu, McGuire & Meidl, 2012, Theorem 4).

Finally, using any p bent functions on a vector space $\mathbb{V}_n^{(p)}$ of dimension n, a construction of bent function on an $n+2$ dimensional domain was presented in (Çeşmelioğlu et al., 2013b), which can be seen as a special case of Theorem 6.

Theorem 7. *Let $g_0, g_1, \ldots, g_{p-1}$ be arbitrary bent functions from $\mathbb{V}_n^{(p)}$ to $\mathbb{F}_p$. Then the function $G : \mathbb{V}_n^{(p)} \times \mathbb{F}_p^2 \to \mathbb{F}_p$ given by*

$$G(x, x_{n+1}, y) = g_y(x) + x_{n+1}y$$

is a bent function with the dual $G^*(x, x_{n+1}, y) = g_{x_{n+1}}(x) - x_{n+1}y$. If the dual functions g_i^* of g_i, $0 \le i \le p-1$, are all bent, then G^* is also bent.

1.6 Normality of Bent Functions

The notion of normality of Boolean functions was introduced by Dobbertin in (Dobbertin, 1994), then it was also generalized to p-ary functions.

Definition 7. *A function f from a vector space $\mathbb{V}_n^{(p)}$ of dimension $n = 2m$ to the finite field $\mathbb{F}_p$, where p is an arbitrary prime, is called normal if it is constant on an affine subspace of dimension $m = n/2$.*

It is shown in (Charpin, 2004) and (Meidl & Pirsic, 2018) that for $p = 2$ and p is odd, respectively, that if a function $f : \mathbb{V}_n^{(p)} \to \mathbb{F}_p$ is constant on an affine subspace of dimension k, then we have $p^k \le max_{b \in \mathbb{V}_n^{(p)}} |\mathcal{W}_f(b)|$. Hence, normal bent functions attain the maximal bound. In fact, many of the classical constructions of bent functions are normal.

- The Maiorana-McFarland bent function given in Theorem 2 is constant on the affine subspace $\mathbb{F}_{p^m} \times \pi^{-1}(0)$ because it takes the value $G(\pi^{-1}(0))$ on $\mathbb{F}_{p^m} \times \pi^{-1}(0)$. Hence, it is normal.
- PS^+ bent functions $F : \mathbb{V}_n^{(p)} \to \mathbb{F}_p$, which is a special case of the partial spread bent functions defined in Theorem 3(ii), are normal by definition. The sit-

uation is not the same for the PS^- bent functions. PS_{ap} bent functions as a subclass of the PS^- bent functions are normal. However, there exist PS^- bent functions which are not normal, since the functions given in Theorem 3(i), by construction, are not constant on any subspace U_i. As an example of such functions, we refer to (Polujan, Mariot & Picek, 2025).

- Quadratic bent functions $f_1 : \mathbb{F}_2^4 \to \mathbb{F}_2$ with $f_1(x_1, x_2, x_3, x_4) = x_1x_2 + x_3x_4$ and $f_2 : \mathbb{F}_5^4 \to \mathbb{F}_5$ with $f_2(x_1, x_2, x_3, x_4) = x_1^2 + x_2^2 + x_3^2 + x_4^2$ are normal as f_1 is zero on $\mathbb{F}_2 \times \{0\} \times \mathbb{F}_2 \times \{0\}$ and f_2 is zero on the subspace $\{(x_1, 2x_1, x_3, 2x_3) : x_1, x_3 \in \mathbb{F}_5\}$.

The dual of a normal bent function $f : \mathbb{V}_n^{(p)} \to \mathbb{F}_p$ which is constant on an $(n/2)$-dimensional subspace behaves similarly regarding to normality.

Lemma 3. *Let n be even and p be an arbitrary prime. If a function $f : \mathbb{V}_n^{(p)} \to \mathbb{F}_p$ is a bent function that is constant on a subspace $U \subset \mathbb{V}_n^{(p)}$ of dimension $n/2$, then the dual $f^* : \mathbb{V}_n^{(p)} \to \mathbb{F}_p$ of f is constant on $U^\perp$, where $U^\perp$ is the orthogonal complement of U.*

Proof. Suppose that $f(x) = c$ on U for some $c \in \mathbb{F}_p$, and consider the sum

$$\begin{aligned} \sum_{v \in U^\perp} \mathcal{W}_f(v) &= \sum_{v \in U^\perp} \sum_{x \in \mathbb{V}_n^{(p)}} \zeta_p^{f(x) - \langle v, x \rangle_n} \\ &= \sum_{x \in \mathbb{V}_n^{(p)}} \zeta_p^{f(x)} \sum_{v \in U^\perp} \zeta_p^{-\langle v, x \rangle_n} = |U^\perp| \sum_{x \in U} \zeta_p^{f(x)} = p^{n/2} \sum_{x \in U} \zeta_p^c = p^n \zeta_p^c. \end{aligned} \tag{1.11}$$

Since n is even, the Walsh transform of f at any $v \in \mathbb{V}_n^{(p)}$ is $\mathcal{W}_f(v) = \varepsilon_v p^{n/2} \zeta_p^{f^*(v)}$ with $\varepsilon_v = \pm 1$. As $|U^\perp| = p^{n/2}$, we get $\sum_{v \in U^\perp} \mathcal{W}_f(v) = p^n \sum_{v \in U^\perp} \varepsilon_v \zeta_p^{f^*(v)}$. Then using Equation (1.11), we can conclude $\varepsilon_v = 1$ and $f^*(v) = c$ for all $v \in U^\perp$, which completes the proof. □

More generally, it is shown in (Çeşmelioğlu, Meidl & Pott, 2013c, Theorem 1) that if $f : \mathbb{V}_n^{(p)} \to \mathbb{F}_p$, $n = 2m$, is a bent function that is constant on an affine subspace $a + U$, then the dual f^* of f is affine on $U^\perp$ and the sign of the Walsh transform is positive on $U^\perp$. Hence, a weakly regular but not regular bent function cannot be normal. For example, the Walsh transform of the quadratic bent function $f : \mathbb{F}_5^4 \to \mathbb{F}_5$ with $f(x_1, x_2, x_3, x_4) = x_1^2 + x_2^2 + x_3^2 + 3x_4^2$ has a negative sign for any element in $\mathbb{F}_5^4$, which implies that f is not normal. This argument is not valid for $p = 2$ as all Boolean bent functions are regular. Actually, the existence of nonnormal Boolean bent functions has been an open question for years. In (Canteaut, Daum, Dobbertin & Leander,

2006), an algorithm for testing the normality of Boolean functions is presented, and the first examples of nonnormal Boolean bent functions are given; see (Canteaut et al., 2006).

1.7 Bent Partitions

As we have already examined, the partial spread construction is the most effective construction of bent functions. A large number of bent functions from an even-dimensional vector space $\mathbb{V}_n^{(p)}$ to $\mathbb{F}_p$, which are constant on the subspaces of a (partial) spread, can be obtained. In addition, one can generate bent functions from the vector space $\mathbb{V}_n^{(p)}$ to an arbitrary abelian group G of order p^k, $k \leq n/2$. In (Meidl & Pirsic, 2021), it is shown that spreads are not the only partitions of $\mathbb{V}_n^{(2)}$ that can be used to obtain bent functions from $\mathbb{V}_n^{(2)}$ to various abelian groups of order 2^k with $k \leq \frac{n}{2}$. The first aim in (Meidl & Pirsic, 2021) was to find examples of bent functions from $\mathbb{V}_n^{(2)}$ to the cyclic group $\mathbb{Z}_{2^k}$ that are not constructed from partial spreads. More precisely, the following examples of bent functions from $\mathbb{F}_{2^m} \times \mathbb{F}_{2^m}$ to $\mathbb{Z}_{2^k}$ are obtained, where $m = n/2$.

Theorem 8. *For two positive integers m and j satisfying $\gcd(2^m-1, 2^j+1) = 1$ and $\gcd(2^m-1, 2^j-1) = 2^k-1$, let $e = 2^m - 2^j - 2$ and d be the multiplicative inverse of e modulo 2^m-1. Then the functions f_1 and f_2 given by*

$$f_1(x) = \sum_{i=0}^{k-1} \mathrm{Tr}_1^m(\alpha_i x y^d) 2^i, \qquad f_2(x) = \sum_{i=0}^{k-1} \mathrm{Tr}_1^m(\alpha_i^{-e} x^e y) 2^i, \tag{1.12}$$

where $\{\alpha_0, \alpha_1, \ldots, \alpha_{k-1}\}$ is a basis of $\mathbb{F}_{2^k}$ over $\mathbb{F}_2$, are bent functions from $\mathbb{F}_{2^m} \times \mathbb{F}_{2^m}$ to $\mathbb{Z}_{2^k}$.

Using an argument related to the algebraic degree of $\mathrm{Tr}_1^m(\alpha_i^{-e} x^e y)$ (and similarly of $\mathrm{Tr}_1^m(\alpha_i x y^d)$) it was shown in (Meidl & Pirsic, 2021) that f_1 and f_2 do not come from the partial spread construction if $j > 0$. It was also shown that the sets of preimages of these functions have similar properties as (partial) spreads concerning the construction of bent functions.

Let k be a positive divisor of m with $\gcd(2^m-1, 2^k+1) = 1$, and let $e = 2^m - 2^k - 2$.

In fact, we take $j = k$ in Theorem 8. For $s \in \mathbb{F}_{2^m}$, we define

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

Then the sets U and U_s, $s \in \mathbb{F}_{2^m}$, pairwise intersect trivially, and for any $(u, v) \in \mathbb{F}_{2^m} \times \mathbb{F}_{2^m}$ either $u = 0$ in which case $(u, v) = (0, v) \in U$, or $(u, v) \in U_s$ with $s = vu^e$. Hence, the sets U and U_s, $s \in \mathbb{F}_{2^m}$, form a partition of $\mathbb{F}_{2^m} \times \mathbb{F}_{2^m}$.

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

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

where d is the multiplicative inverse of e modulo $2^m - 1$.

For an element $\gamma \in \mathbb{F}_{2^k}$, 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 settings, it was shown in (Meidl & Pirsic, 2021, Lemma 4) that

$$\Gamma_1 = \{\mathcal{A}(0) \cup U, \mathcal{A}(\gamma) : \gamma \in \mathbb{F}_{2^k}^*\},$$
$$\Gamma_2 = \{\mathcal{B}(0) \cup V, \mathcal{B}(\gamma) : \gamma \in \mathbb{F}_{2^k}^*\}$$

are the sets of preimages of f_2 and f_1, respectively, where f_1, f_2 are given as in Theorem 8. Here we can observe that $\mathcal{A}(0) \cup U$ is the preimage of zero under f_2, and similarly preimage of zero under f_1 is $\mathcal{B}(0) \cup V$. Moreover, the following theorem is proven in (Meidl & Pirsic, 2021), which gives motivation to introduce the concept of bent partitions.

Theorem 9. *Let m and k be two positive integers such that k divides m, and suppose that $\gcd(2^m - 1, 2^k + 1) = 1$ and that the sets U, V, $\mathcal{A}(\gamma)$ and $\mathcal{B}(\gamma)$, where γ is an element of $\mathbb{F}_{2^k}$, are defined as above. Then we have the following.*

(i) Every Boolean function whose support is the union of exactly 2^{k-1} of the sets $\mathcal{A}(\gamma)$ is bent. Similarly, Boolean functions that have the union of 2^{k-1} of the subsets $\mathcal{A}(\gamma)$ together with U as their support are bent.

(ii) Every Boolean function whose support is the union of exactly 2^{k-1} of the sets $\mathcal{B}(\gamma)$ is a bent function. In the same way, Boolean functions that have the union of 2^{k-1} of the subsets $\mathcal{B}(\gamma)$ together with the subspace V as their support

are bent.

Remark 3. *In the special case $k = m$, for any element $s \in \mathbb{F}_{2^m}$, we have $U_s = \{(x, sx^2) : x \in \mathbb{F}_{2^m}\}$. Then U_s is a subspace of $\mathbb{F}_{2^m} \times \mathbb{F}_{2^m}$, which comes from the fact that $(a+b)^2 = a^2 + b^2$ for all $a, b \in \mathbb{F}_{2^m}$. Hence, the partition $\{U, \mathcal{A}(\gamma) : \gamma \in \mathbb{F}_{2^k}\} = \{U, U_s^* : s \in \mathbb{F}_{2^k}\}$ reduces to a spread partition of $\mathbb{F}_{2^m} \times \mathbb{F}_{2^m}$. The same is true for $\{V, \mathcal{B}(\gamma) : \gamma \in \mathbb{F}_{2^k}\}$.*

Motivated by the construction given above, the concept of a bent partition is introduced in (Anbar & Meidl, 2022).

Definition 8. *Let K be a positive integer divisible by p, and let $\Gamma = \{A_1, \ldots, A_K\}$ be a partition of $\mathbb{V}_n^{(p)}$ with the property that every function f from $\mathbb{V}_n^{(p)}$ to $\mathbb{F}_p$ for which every $c \in \mathbb{F}_p$ has exactly the elements of $\frac{K}{p}$ of the sets A_i in its preimage is bent. Then Γ is called a bent partition of $\mathbb{V}_n^{(p)}$ of depth K.*

The standard example of a bent partition is obtained from a spread of $\mathbb{V}_n^{(p)}$, where $n = 2m$. More explicitly, let U_0, U_1, ..., U_{p^m} be subspaces of a spread of $\mathbb{V}_n^{(p)}$. Then the set $\{U_0 \cup U_1, U_2^*, \ldots, U_{p^m}^*\}$, with $U_i^* = U_i \setminus \{0\}$, is a bent partition of $\mathbb{V}_n^{(p)}$ of depth p^m. Note that we can replace $U_0 \cup U_1$ with the union of any other two subspaces, and together with the nonzero elements of other subspaces, we obtain another bent partition of $\mathbb{V}_n^{(p)}$. Likewise, one can construct bent partitions from partial spreads; see (Anbar & Meidl, 2022).

In characteristic 2, some significant examples of bent partitions (of the vector space $\mathbb{F}_{2^m} \times \mathbb{F}_{2^m}$) are obtained using Theorem 9.

Example 4. *For a positive divisor k of m with $\gcd(2^m - 1, 2^k + 1) = 1$, the partition $\Gamma_1 = \{\mathcal{A}(0) \cup U, \mathcal{A}(\gamma) : \gamma \in \mathbb{F}_{2^k}^*\}$ is a bent partition by the first part of Theorem 9. We can replace $\mathcal{A}(0)$ with any $\mathcal{A}(\gamma)$ with $\gamma \in \mathbb{F}_{2^k}^*$ to obtain another bent partition of $\mathbb{F}_{2^m} \times \mathbb{F}_{2^m}$. By the last part of Theorem 9, the partition $\Gamma_2 = \{\mathcal{B}(0) \cup V, \mathcal{B}(\gamma) : \gamma \in \mathbb{F}_{2^k}^*\}$ is also a bent partition.*

In (Nyberg, 1991a), the value distribution of a bent function is given in various cases by Nyberg. We recall the results from (Anbar & Meidl, 2022).

Lemma 4. *Let p be a prime and $f : \mathbb{V}_n^{(p)} \to \mathbb{F}_p$ be a bent function. For $t \in \mathbb{F}_p$, let b_t be the cardinality of the preimage set $f^{-1}(t)$.*

(i) If n is even, then $b_c = p^{n-1} \pm (p-1)p^{\frac{n}{2}-1}$ for some unique $c \in \mathbb{F}_p$ and $b_t =$

$p^{n-1} \mp p^{\frac{n}{2}-1}$ *for all* $t \in \mathbb{F}_p \setminus \{c\}$, *where* $\pm$ *signs are taken correspondingly. Moreover, if* f *is regular, then* f *has upper signs.*

(ii) Let n *and* p *be odd. Then* $b_0 = p^{n-1}$, *and either* $b_t = p^{n-1} + \left(\frac{t}{p}\right) p^{\frac{n}{2}-1}$ *for all* $t \in \mathbb{F}_p \setminus \{0\}$ *or* $b_t = p^{n-1} - \left(\frac{t}{p}\right) p^{\frac{n}{2}-1}$ *for all* $t \in \mathbb{F}_p \setminus \{0\}$, *where* $\left(\frac{*}{*}\right)$ *is the Legendre symbol.*

Remark 4. *If* $\Gamma = \{A_1, \ldots, A_K\}$ *is a bent partition of* $\mathbb{V}_n^{(p)}$, *then clearly* n *must be even for* $p = 2$. *This is also the case for odd* p, *except for the case* $p = K = 3$, *as if* n *and* p *are odd, then by Lemma 4(ii) the cardinality* b_t *changes depending on* t. *However, by definition of a bent partition once we fix a preimage partition of a bent function we can arbitrarily choose which set will be mapped to which value. Hence,* n *is not odd.*

In (Anbar & Meidl, 2022), using Lemma 4, the possible cardinalities of the sets in a bent partition are presented.

Theorem 10. *Let* $\Gamma = \{A_1, \ldots, A_K\}$ *be a bent partition of* $\mathbb{V}_n^{(p)}$. *Then except one set, say* A_1, *every set* A_j *has the same cardinality, namely*

$$|A_j| = \frac{p^{n/2}(p^{n/2} \mp 1)}{K}, \ 2 \le j \le K, \ \textit{and}$$
$$|A_1| = \frac{p^{n/2}(p^{n/2} \mp 1)}{K} \pm p^{n/2}.$$

Remark 5. *Note that for all known examples of bent partitions we have* $|A_1| > |A_j|$, $2 \le j \le K$, *and* K *is a power of* p, *except the case* $p = K = 3$. *For* $p = K = 3$, *we have* $|A_1| < |A_2| < |A_3|$.

In Example 4, the union of the subspace U with $\mathcal{A}(0)$ forms the larger set in the bent partition Γ_1. Similarly, the subspace V together with $\mathcal{B}(0)$ gives the larger set in Γ_2. Considering also the construction of bent partitions from (partial) spreads, the definition of a bent partition refined as follows.

Definition 9. *Let* K *be an integer divisible by* p, *and let* $\Gamma = \{U, A_1, \ldots, A_K\}$ *be a partition of* $\mathbb{V}_n^{(p)}$. *It is called a normal bent partition of* $\mathbb{V}_n^{(p)}$ *of depth* K, *if every function* f *from* $\mathbb{V}_n^{(p)}$ *to* $\mathbb{F}_p$ *with the following properties is bent:*

- *Every* $c \in \mathbb{F}_p$ *has exactly* K/p *of the sets* $A_1, \ldots, A_K$ *in its preimage, and*
- f *is also constant on* U.

The possible cardinalities of the sets in a normal bent partition are also known.

Theorem 11. *(Anbar & Meidl, 2022, Theorem 4(i)) Let $\Gamma = \{U, A_1, \ldots, A_K\}$ be a normal bent partition of $\mathbb{V}_n^{(p)}$. Then we have*

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

Proof. Without loss of generality we may assume

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

Suppose first that $p = 2$. To get a contradiction, assume that the cardinalities of the sets A_j are not all the same. Then we get $\sum_{j=1}^{K/2} |A_j| < \sum_{j=K/2+1}^{K} |A_j|$. Any union of $K/2$ of sets A_j, $1 \le j \le K$, is the support of a bent function obtained from Γ. Hence, by Lemma 4(i), we have

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

By the definition of a normal bent partition, the union $U \cup \bigcup_{j=K/2+1}^{K} A_j$ is also the support of a bent function f. Then we have $|supp(f)| = |f^{-1}(1)| > 2^{n-1} + 2^{n/2-1}$, which is not possible by Lemma 4(i). Hence, we get $|A_1| = |A_2| = \cdots = |A_{K-1}| = |A_K|$. As $U \cup \bigcup_{j=K/2+1}^{K} A_j$ and $\bigcup_{j=K/2+1}^{K} A_j$ are both supports of some bent functions, their cardinalities are $2^{n-1} + 2^{n/2-1}$ and $2^{n-1} - 2^{n/2-1}$, respectively. Therefore, $|U| = 2^{n/2}$ and $|A_j| = \frac{2^{n/2}(2^{n/2}-1)}{K},\ 1 \le j \le K$.

Now, let p be an odd prime. Suppose again that the cardinalities of the sets A_j are not all the same. Then we have $\sum_{j=1}^{\frac{K}{p}} |A_j| < \sum_{j=(p-1)\frac{K}{p}+1}^{K} |A_j|$. Since any union K/p of sets A_j can be the preimage of an element in $\mathbb{F}_p$, using Lemma 4(i) (and taking upper signs without loss of generality), we obtain

$$\sum_{j=1}^{\frac{K}{p}} |A_j| = p^{n-1} - p^{n/2-1} \quad \text{and} \quad \sum_{j=(p-1)\frac{K}{p}+1}^{K} |A_j| = p^{n-1} + (p-1)p^{n/2-1}.$$

Similar to the case $p = 2$, also $U \cup \bigcup_{j=(p-1)\frac{K}{p}+1}^{K} A_j$ is the preimage of an element $t \in \mathbb{F}_p$ under a bent function obtained from Γ. Then we conclude $|f^{-1}(t)| > p^{n-1} + (p-1)p^{n/2-1}$, contradicting Lemma 4$(i)$. Therefore, $|A_i| = |A_j|$ for all $i, j \in \{1, 2, \ldots, K\}$. As both sets $U \cup \bigcup_{j=(p-1)\frac{K}{p}+1}^{K} A_j$ and $\bigcup_{j=(p-1)\frac{K}{p}+1}^{K} A_j$ are the preim-

ages of some bent functions, we have $|U \cup \bigcup_{j=(p-1)\frac{K}{p}+1}^{K} A_j| = p^{n-1} + (p-1)p^{n/2-1}$ and $|\bigcup_{j=(p-1)\frac{K}{p}+1}^{K} A_j| = p^{n-1} - p^{n/2-1}$. Thus, we obtain the desired cardinalities. □

It was shown in (Anbar & Meidl, 2022) that the set U in the definition of a normal bent partition is an affine subspace of $\mathbb{V}_n^{(p)}$ (of dimension $n/2$). Therefore, every bent function obtained from a normal bent partition is normal. By Theorem 10, if $\Gamma = \{A_1, \ldots, A_K\}$ is a bent partition of $\mathbb{V}_n^{(p)}$, then two situations can occur:

$$\begin{aligned} &\text{Type I. } |A_2| = |A_3| = \cdots = |A_K|, \text{ and } |A_1| = |A_2| + p^{n/2}, \text{ or} \\ &\text{Type II. } |A_2| = |A_3| = \cdots = |A_K|, \text{ and } |A_1| = |A_2| - p^{n/2}. \end{aligned} \tag{1.13}$$

In the case $|A_1| = |A_2| + p^{n/2}$, it can be turned into a normal bent partition if and only if A_1 contains an affine subspace U of dimension $n/2$, see (Anbar & Meidl, 2022, Corollary 2). We will call a bent partition $\Gamma = \{A_1, \ldots, A_K\}$ nonnormal if it is of Type I with A_1 not containing an $(n/2)$-dimensional affine subspace, or it is of Type II.

Similar to spreads, we can obtain vectorial bent functions using (normal) bent partitions.

Theorem 12. *(Anbar & Meidl, 2022, Theorem 5) Let $\Gamma = \{U, A_1, \ldots, A_{p^k}\}$ be a normal bent partition of $\mathbb{V}_n^{(p)}$ of depth p^k, and let $F : \mathbb{V}_n^{(p)} \to \mathbb{V}_k^{(p)}$ be a function such that every $c \in \mathbb{V}_k^{(p)}$ has the elements of exactly one A_j in its preimage, and the elements of U are mapped to some fixed $c_0 \in \mathbb{V}_k^{(p)}$. Then F is a vectorial bent function.*

Proof. We need to prove that for any nonzero element $\beta \in \mathbb{V}_k^{(p)}$, the component function $F_\beta(x) = \langle \beta, F(x) \rangle_k$ is a bent function. $F_\beta(x)$ is constant on U as $F_\beta(x) = \langle \beta, c_0 \rangle_k$ for all $x \in U$. Then by the definition of normal bent partition it is enough to show that every element in $\mathbb{F}_p$ has the elements of exactly p^{k-1} of the sets A_j in its preimage. If A_j is mapped to $c_j \in \mathbb{V}_k^{(p)}$, then $F_\beta(x) = \langle \beta, c_j \rangle_k$ on A_j, $j = 1, \ldots, p^k$. As $\beta \neq 0$, we also see that the function $L(x) := \langle \beta, x \rangle_k$ is balanced on $\mathbb{V}_k^{(p)}$, which implies the desired result. Hence, F_β is a bent function. □

Note that we can get vectorial bent functions $F : \mathbb{V}_n^{(p)} \to \mathbb{V}_t^{(p)}$ for $t < k$, in the same manner. Moreover, using the normal bent partition given in the above theorem, one can obtain bent functions from $\mathbb{V}_n^{(p)}$ to the cyclic group $\mathbb{Z}_{p^k}$, see (Anbar & Meidl, 2022).

As can be easily observed, we can extend the bent partitions obtained from (partial) spreads to normal bent partitions. In particular, if $\{U_0, U_1, \ldots, U_{p^m}\}$ is a spread of $\mathbb{V}_n^{(p)}$, $n = 2m$, then the set $\{U_0, U_1^*, \ldots, U_{p^m}^*\}$, where $U_i^* = U_i \setminus \{0\}$, forms a normal bent partition of $\mathbb{V}_n^{(p)}$ (of depth p^m). Similarly, the bent partitions Γ_1 and Γ_2 of $\mathbb{F}_{2^m} \times \mathbb{F}_{2^m}$ given in Example 4 can be extended to normal partitions $\{U, \mathcal{A}(\gamma) : \gamma \in \mathbb{F}_{2^k}\}$ and $\{V, \mathcal{B}(\gamma) : \gamma \in \mathbb{F}_{2^k}\}$, respectively. We will denote these partitions by Γ_1 and Γ_2 from now on. In (Anbar & Meidl, 2022), the normal bent partitions Γ_1 and Γ_2 are generalized for odd primes p, which is not straightforward.

Let m and k be two positive integers such that k divides m, and suppose that $\gcd(p^m - 1, p^k + p - 1) = 1$. Let $e = p^k + p - 1$, and let d be an integer with $de \equiv 1 \bmod (p^m - 1)$. For any $s \in \mathbb{F}_{p^m}$, we define

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

Then the sets U, and U_s^*, $s \in \mathbb{F}_{p^m}$, give rise to a partition of $\mathbb{F}_{p^m} \times \mathbb{F}_{p^m}$.

Likewise, for any $s \in \mathbb{F}_{p^m}$ we define

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

For an element $\gamma \in \mathbb{F}_{p^k}$, let

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

With these settings, the following two partitions of $\mathbb{F}_{p^m} \times \mathbb{F}_{p^m}$

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

are obtained. Note that in characteristic 2 above, we have $e = 2^m - 2^k - 2$. Then $-e \equiv 2^k + 1$ modulo $2^m - 1$. Hence, for $p = 2$, these partitions coincide with the ones we defined previously. In (Anbar & Meidl, 2022), it was shown that the partitions Γ_1 and Γ_2 are normal bent partitions.

Theorem 13. *Let m and k be two positive integers such that k divides m, and let $\gcd(p^m - 1, p^k + p - 1) = 1$, and that the sets U, V, $\mathcal{A}(\gamma)$ and $\mathcal{B}(\gamma)$, where γ is an element of $\mathbb{F}_{p^k}$, are defined as above. Suppose that $f : \mathbb{F}_{p^m} \times \mathbb{F}_{p^m} \to \mathbb{F}_p$ is a p-ary*

function with the following properties:

(i) 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.

(ii) f is constant c_0 on U (respectively V) for some $c_0 \in \mathbb{F}_p$.

Then f is a regular bent function.

For the proof, we refer to (Anbar & Meidl, 2022, Theorem 7). The proof is obtained by using character sums. More precisely, the Walsh transform of f is computed at any $(u,v) \in \mathbb{F}_{p^m} \times \mathbb{F}_{p^m}$. Using the proof, it was also concluded in (Anbar & Meidl, 2022) that if f is a bent function coming from Γ_1, then its dual f^* is a bent function obtained by Γ_2, and vice versa.

Remark 6. *Similar to the case $p = 2$, if $k = m$, then we have $U_s = \{(x, sx^p) : x \in \mathbb{F}_{p^m}\}$ for any $s \in \mathbb{F}_{p^m}$. Hence, U_s is a subspace of $\mathbb{F}_{p^m} \times \mathbb{F}_{p^m}$ (over $\mathbb{F}_p$). Therefore, the partition $\{U, \mathcal{A}(\gamma) : \gamma \in \mathbb{F}_{p^k}\} = \{U, U_s^* : s \in \mathbb{F}_{p^k}\}$ reduces to a partition equivalent to the Desarguesian spread partition of $\mathbb{F}_{p^m} \times \mathbb{F}_{p^m}$. The same holds for $\{V, \mathcal{B}(\gamma) : \gamma \in \mathbb{F}_{p^k}\}$. Therefore, these partitions are called generalized Desarguesian spreads.*

Some examples of bent functions obtained from the normal bent partitions Γ_1 and Γ_2 are as follows.

Example 5. *Let p be an arbitrary prime, and let the integers m, k, and e be as above. Let $f : \mathbb{F}_{p^m} \times \mathbb{F}_{p^m} \to \mathbb{F}_p$ be a function defined by $f(x,y) = \mathrm{Tr}_1^m(x^{-e}y)$. Clearly, f is zero on $U = \{(0,y) : y \in \mathbb{F}_{p^m}\}$. f is also constant on any $\mathcal{A}(\gamma)$, $\gamma \in \mathbb{F}_{p^k}$. To see this, let (u,v) be an element in $\mathcal{A}(\gamma)$. Then $(u,v) \in U_s = \{(x, sx^e) : x \in \mathbb{F}_{p^m}\}$ for some $U_s \subseteq \mathcal{A}(\gamma)$. Thus, we have*

$$f(u,v) = \mathrm{Tr}_1^m(u^{-e}v) = \mathrm{Tr}_1^m(u^{-e}su^e) = \mathrm{Tr}_1^m(s) = \mathrm{Tr}_1^k(\mathrm{Tr}_k^m(s)) = \mathrm{Tr}_1^k(\gamma) = l.$$

As γ runs over $\mathbb{F}_{p^k}$, we get exactly p^{k-1} of the sets $\mathcal{A}(\gamma)$ are mapped to l. Hence, f is a bent function constructed from Γ_1. Similarly, one can show that the function $g : \mathbb{F}_{p^m} \times \mathbb{F}_{p^m} \to \mathbb{F}_p$ given by $g(x,y) = \mathrm{Tr}_1^m(xy^{-d})$ is a bent function obtained by Γ_2.

More generally, let $B : \mathbb{F}_{p^k} \to \mathbb{F}_p$ be a balanced function with $B(0) = 0$. Then the function $f : \mathbb{F}_{p^m} \times \mathbb{F}_{p^m} \to \mathbb{F}_p$ defined by $f(x,y) = B(\mathrm{Tr}_k^m(x^{-e}y))$ is a bent function obtained from Γ_1. We can construct bent functions from the partition Γ_2 in the same manner. Such functions are called generalized PS_{ap} bent functions.

1.8 LP-packings

As we have already observed, the partitions Γ_1 and Γ_2 given above can be considered as a generalization of the Desarguesian spread. In addition to being normal bent partitions, Γ_1 and Γ_2 share another common property with spreads; which is giving an LP-packing. The concept of LP-packings (Latin square type partial difference set packings) is introduced very recently in (Jedwab & Li, 2021), by Jedwab and Li. In order to define an LP-packing, we first need to give the definition of a partial difference set.

Definition 10. *Let G be a group of order v. A subset D of G with $\varkappa$ elements is called a $(v,\varkappa,\lambda,\mu)$ partial difference set (PDS) of G, if every nonzero element of D can be written as d_1-d_2, where d_1, $d_2\in D$, exactly in λ ways, and every nonzero element of $G\setminus D$ exactly in μ ways. In addition, if $-D=D$ and $0\notin D$, then D is called a regular partial difference set.*

A PDS is called of (n,s) Latin square type if its parameters are of the form $(n^2,s(n-1),n+s^2-3s,s^2-s)$, and of (n,s) negative Latin square type if the parameters are $(n^2,s(n+1),-n+s^2+3s,s^2+s)$ for some integers $n\geq 1, s\geq 0$.

If G is a finite group, then $\emptyset$, $\{0\}$, $G\setminus\{0\}$ and G are PDSs. For nontrivial examples of PDSs, see (Ma, 1994).

Definition 11. *(Jedwab & Li, 2021, Definition 3.1) Let $t>1$ and $c>0$ be integers, G be an abelian group of order t^2c^2, and let U be a subgroup of G of order tc. A (c,t) LP-packing in G relative to U is a collection $\{P_1,\ldots,P_t\}$ of t pairwise disjoint regular (tc,c) Latin square type PDSs in G for which $\bigcup_{i=1}^{t}P_i=G\setminus U$.*

The canonical example of an LP-packing is obtained from a spread of $\mathbb{V}_n^{(p)}$, where $n=2m$. More precisely, let U_0, U_1, ... , U_{p^m} be the subspaces of a spread of $\mathbb{V}_n^{(p)}$. Then for each i, the set $U_i\setminus\{0\}$ is a $(p^{2m},p^m-1,p^m-2,0)$ regular PDS of G. Hence, $\{U_1^*,\ldots,U_{p^m}^*\}$, $U_i^*=U_i\setminus\{0\}$, is a $(1,p^m)$ LP-packing in $\mathbb{V}_{2m}^{(p)}$ relative to U_0.

A characterization of partial difference sets by means of characters is given in (Ma, 1994). It is used in (Anbar, Kalaycı & Meidl, 2022) as a main tool to show that the sets $\mathcal{A}(\gamma)$ in Γ_1 are PDSs.

Lemma 5. *Let G be an abelian group of order v. Suppose that D is a subset of G with $\varkappa$ elements satisfying the conditions $-D=D$ and $0\notin D$. Then D is a*

$(v, \varkappa, \lambda, \mu)$ PDS if and only if for every nontrivial character χ of G, we have

$$\chi(D) = \frac{\beta \pm \sqrt{\Delta}}{2}, \tag{1.14}$$

where $\beta = \lambda - \mu$, $\delta = \varkappa - \mu$ and $\Delta = \beta^2 + 4\delta$.

For $u, v \in \mathbb{F}_{p^m}$, let $\chi_{u,v}$ denote the character on $\mathbb{F}_{p^m} \times \mathbb{F}_{p^m}$ given by $\chi_{u,v}(x,y) = \zeta_p^{\mathrm{Tr}_1^m(ux+vy)}$. It is shown in (Anbar et al., 2022) that

$$\chi_{u,v}(\mathcal{A}(\gamma)) = \begin{cases} p^m - p^{m-k} & , \text{ if } \gamma = -\mathrm{Tr}_k^m(uv^{-d})^p, v \neq 0 \\ -p^{m-k} & , \text{ otherwise,} \end{cases} \tag{1.15}$$

where $(u,v) \neq (0,0)$ and $\gamma \in \mathbb{F}_{p^k}$. Then using Lemma 5 and the above equation, we find that each $\mathcal{A}(\gamma)$ is a partial difference set with parameters

$$(p^{2m}, p^{m-k}(p^m - 1), p^m + p^{m-k}(p^{m-k} - 3), p^{m-k}(p^{m-k} - 1)),$$

i.e., the sets $\mathcal{A}(\gamma)$, $\gamma \in \mathbb{F}_{p^k}$, are of Latin square type with $n = p^m$ and $s = p^{m-k}$. Similarly, each $\mathcal{B}(\gamma)$ is a (p^m, p^{m-k}) Latin square type PDS. By construction, any of $\mathcal{A}(\gamma)$ in Γ_1 is regular. The same holds for each $\mathcal{B}(\gamma)$ in Γ_2. Therefore, we can conclude $\{\mathcal{A}(\gamma) : \gamma \in \mathbb{F}_{p^k}\}$ is a (p^{m-k}, p^k) LP-packing in $\mathbb{F}_{p^m} \times \mathbb{F}_{p^m}$ relative to the subgroup U. Likewise, $\{\mathcal{B}(\gamma) : \gamma \in \mathbb{F}_{p^k}\}$ is a (p^{m-k}, p^k) LP-packing in $\mathbb{F}_{p^m} \times \mathbb{F}_{p^m}$ relative to the subgroup V.

In (Jedwab & Li, 2021, Section 7), the relation between LP-packings and bent functions is studied. We summarize some result of that section in the following proposition.

Proposition 3. *Let G, H be finite abelian groups, and let $f : G \to H$ be a surjective function satisfying $f(0_G) = 0_H$ (without loss of generality). If for every $h \neq 0_H$ the preimage set $f^{-1}(h)$ is a regular $\left(\sqrt{|G|}, \frac{\sqrt{|G|}}{|H|}\right)$ Latin square type PDS, and $f^{-1}(0_H) \setminus \{0_G\}$ is a regular $\left(\sqrt{|G|}, \frac{\sqrt{|G|}}{|H|} + 1\right)$ Latin square type PDS, then f is a bent function.*

In particular, for an LP-packing $\{P_1, \ldots, P_t\}$ in G relative to the subgroup U, a function $f : G \to H$ satisfying properties (i), (ii) below, is bent:

(i) Every $h \in H$ has precisely $t/|H|$ of the PDSs P_i in its preimage set,

(ii) $f(x) = 0_H$, w.l.o.g., for all $x \in U$.

Proof. The first part is stated in Section 7 of (Jedwab & Li, 2021). The second part then follows with the fact that combining the subsets of an LP-packing into collections of equal size gives an LP-packing with fewer subsets, see (Jedwab & Li, 2021, Lemma 3.11). □

Proposition 3 has an immediate consequence for elementary abelian groups.

Corollary 1. *Let $\{P_1, \ldots, P_t\}$ be an LP-packing in $\mathbb{V}_n^{(p)}$ relative to the subgroup U (of order $p^{n/2}$). Then $\{U, P_1, \ldots, P_t\}$ is a normal bent partition of $\mathbb{V}_n^{(p)}$ of depth t.*

In characteristic 2, the converse is also true for some special case. The following is (Anbar et al., 2022, Theorem 3), which in terms of LP-packings can be stated as below.

Theorem 14. *Let n, m, and k be positive integers with $n = 2m$, $k \leq m$, and let $\{U, A_1, \ldots, A_{2^k}\}$ be a normal bent partition of $\mathbb{V}_n^{(2)}$. If one of the sets A_i, $1 \leq i \leq 2^k$, is a PDS, then all the sets A_i are regular $(2^m, 2^{m-k})$ Latin square type PDSs, and $\{A_1, \ldots, A_{2^k}\}$ is a $(2^{m-k}, 2^k)$ LP-packing in $\mathbb{V}_n^{(2)}$ relative to U.*

2. BENT PARTITIONS FROM TERNARY BENT FUNCTIONS

Let f be a ternary bent function, that is, a bent function from $\mathbb{V}_n^{(3)}$ to $\mathbb{F}_3$ for some even integer $n = 2m$. As n is even, we have $\mathcal{W}_f(b) = \pm\zeta_3^{f^*(b)}3^{n/2}$ for any $b \in \mathbb{V}_n^{(3)}$. In particular, $\mathcal{W}_f(0) = \pm\zeta_3^{f^*(0)}3^{n/2}$. We may assume $f^*(0) = 0$, which we can always arrange by adding a constant to the bent function. Then we have

$$\begin{aligned}
\pm 3^m = \mathcal{W}_f(0) &= \sum_{x \in \mathbb{V}_n^{(3)}} \zeta_p^{f(x)-\langle 0,x\rangle_n} \\
&= |f^{-1}(0)|\zeta_3^0 + |f^{-1}(1)|\zeta_3^1 + |f^{-1}(2)|\zeta_3^2 \\
&= |f^{-1}(0)| + |f^{-1}(1)|\zeta_3 + |f^{-1}(2)|(-1-\zeta_3) \\
&= (|f^{-1}(0)| - |f^{-1}(2)|) + (|f^{-1}(1)| - |f^{-1}(2)|)\zeta_3,
\end{aligned}$$

which implies $|f^{-1}(1)| = |f^{-1}(2)|$. More precisely, the following two possibilities can occur.

(i) If $\mathcal{W}_f(0) = 3^m$, then $|f^{-1}(0)| = 3^{m-1}(3^m+2)$,
$|f^{-1}(1)| = |f^{-1}(2)| = 3^{m-1}(3^m-1)$, or

(ii) if $\mathcal{W}_f(0) = -3^m$, then $|f^{-1}(0)| = 3^{m-1}(3^m-2)$,
$|f^{-1}(1)| = |f^{-1}(2)| = 3^{m-1}(3^m+1)$.

Note that if f is regular, then case (i) applies, and if f is weakly regular but not regular, then we have case (ii).

We next show that for every ternary bent function, the collection of the preimage sets forms a bent partition.

Theorem 15. *Let n be any positive integer, and let $f : \mathbb{V}_n^{(3)} \to \mathbb{F}_3$ be a bent function. Then $\mathcal{P} = \{f^{-1}(0), f^{-1}(1), f^{-1}(2)\}$ is a bent partition of $\mathbb{V}_n^{(3)}$. Moreover, one of the following situations can occur.*

(i) If n is odd, then $\mathcal{P} = \{A_1, A_2, A_3\}$ with $|A_1| > |A_2| > |A_3|$.

(ii) If n is even, then possible situations are as below.

(a) $\mathcal{P}=\{A_1,A_2,A_3\}$ *with* $|A_1|>|A_2|=|A_3|$ *and* A_1 *contains a subspace* U *of dimension* $n/2$. *Then* $\bar{\mathcal{P}}=\{U,A_1\setminus U,A_2,A_3\}$ *is a normal bent partition.*

(b) $\mathcal{P}=\{A_1,A_2,A_3\}$ *is a nonnormal bent partition with* $|A_1|>|A_2|=|A_3|$, *if* A_1 *does not contain an* $(n/2)$*-dimensional subspace.*

(c) $\mathcal{P}=\{A_1,A_2,A_3\}$ *is a nonnormal bent partition with* $|A_1|<|A_2|=|A_3|$.

For every normal ternary bent function, case (a) applies.

Proof. It can be observed that any of the six permutations of the preimage sets of f yields a preimage set distribution of one of the six ternary bent functions $af(x)+c$, where $a\in\mathbb{F}_3^*$, $c\in\mathbb{F}_3$. Hence, $\mathcal{P}$ is a bent partition.

(i) If n is odd, then by Lemma 4(ii) a ternary bent function $f:\mathbb{V}_n^{(3)}\to\mathbb{F}_3$ yields a bent partition $\{A_1,A_2,A_3\}$ with $|A_1|=3^{n-1}+3^{(n-1)/2}$, $|A_2|=|f^{-1}(0)|=3^{n-1}$ and $|A_3|=3^{n-1}-3^{(n-1)/2}$, which gives the desired assertion.

(ii) Let n be even, and $|A_1|>|A_2|=|A_3|$. Suppose that A_1 contains an $(n/2)$-dimensional subspace U, thus f is constant c on U, for some $c\in\mathbb{F}_3$. Changing the value of f on U to the constant $c_1\in\mathbb{F}_3$, results in another bent function; see (Carlet, 1994), (Potapov, 2016). This implies that $\bar{\mathcal{P}}$ is a normal bent partition, giving the case (a). If A_1 does not contain an $(n/2)$-dimensional subspace, then $\mathcal{P}$ cannot be altered to a normal bent partition, hence $\mathcal{P}$ is a nonnormal bent partition of Type I, describing the case (b). Otherwise, $|A_1|<|A_2|=|A_3|$ and $\mathcal{P}$ is a nonnormal bent partition of Type II, which gives the case (c), see Equation (1.13).

In order to show the last statement, let f be a normal ternary bent function. By definition, f is constant on an $(n/2)$-dimensional subspace U. Then U is a subset of A_i for some $i\in\{1,2,3\}$, say A_1. With the same argument as above, $\{U,A_1\setminus U,A_2,A_3\}$ is a normal bent partition, which also implies $|A_1\setminus U|=|A_2|=|A_3|$.

It should be noted that if f is a regular normal bent function, then case (a) applies, and for a regular nonnormal bent function we have case (b). If f is weakly regular but not regular, then case (c) applies.

Remark 7. *Bent partitions in Theorem 15(i), n odd, form an exception. Because bent partitions of* $\mathbb{V}_n^{(p)}$, *for odd n, do not exist except for the case that* $p=3$ *and* $K=3$, *see Remark 4.*

In (Tan, Pott & Feng, 2010), a characterization of weakly regular ternary bent functions through partial difference sets is presented. The main result is as follows.

Proposition 4. *(Tan et al., 2010, Theorem 1) Let $m \geq 2$ and $f : \mathbb{F}_{3^{2m}} \to \mathbb{F}_3$ be a ternary bent function satisfying $f(-x) = f(x)$ and $f(0) = 0$. If we define*

$$D_i := \{x \in \mathbb{F}_{3^{2m}} \mid f(x) = i\} = f^{-1}(i)$$

for each $0 \leq i \leq 2$, then the following statements hold.

(i) f is weakly regular if and only if D_1 and D_2 are both $(3^{2m}, 3^{2m-1} + \varepsilon 3^{m-1}, 3^{2m-2}, 3^{2m-2} + \varepsilon 3^{m-1})$ PDSs, where $\varepsilon = \pm 1$ (the choice of ε for D_1 and D_2 should be the same).

(ii) The set $D_0 \setminus \{0\}$ is a $(3^{2m}, 3^{2m-1} - 1 - 2\varepsilon 3^{m-1}, 3^{2m-2} - 2\varepsilon 3^{m-1} - 2, 3^{2m-2} - \varepsilon 3^{m-1})$ PDS, where ε is the same as in the first part of the theorem.

In Proposition 4, we have $\varepsilon = -1$ if f is regular, and $\varepsilon = 1$ if f is weakly regular but not regular, which can be observed from the possible cardinalities of preimage sets of ternary bent functions. Note that for $\varepsilon = -1$, D_1 and D_2 are of $(3^m, 3^{m-1})$ Latin square type, and $D_0 \setminus \{0\}$ is of $(3^m, 3^{m-1} + 1)$ Latin square type. If $\varepsilon = 1$, then D_1 and D_2 are of $(3^m, 3^{m-1})$ negative Latin square type, and $D_0 \setminus \{0\}$ is of $(3^m, 3^{m-1} - 1)$ negative Latin square type.

Theorem 15 and Proposition 4 together imply that ternary bent functions yield bent partitions; some of these bent partitions result in LP-packings, some do not. For weakly regular bent functions $f : \mathbb{V}_{2m}^{(3)} \to \mathbb{F}_3$, we have the following cases. We again use the notation $D_i = f^{-1}(i)$, and we suppose that $f(0) = 0$.

- f is regular, normal with subspace U, and $f(x) = f(-x)$ for all $x \in \mathbb{V}_{2m}^{(3)}$. Then $\mathcal{P} = \{D_0 \setminus U, D_1, D_2\}$ is an LP-packing in $\mathbb{V}_{2m}^{(3)}$ relative to U. Hence, $\{U, D_0 \setminus U, D_1, D_2\}$ is a normal bent partition of $\mathbb{V}_{2m}^{(3)}$.

  Regular quadratic bent functions and Maiorana-McFarland bent functions $x \cdot \pi(y)$ with permutation π satisfying $\pi(-y) = -\pi(y)$ (like for power permutations) are examples of such functions.

- f is regular, normal with subspace U, and $f(x) \neq f(-x)$ for some $x \in \mathbb{V}_{2m}^{(3)}$. Then $\mathcal{P} = \{U, D_0 \setminus U, D_1, D_2\}$ is a normal bent partition of $\mathbb{V}_{2m}^{(3)}$, not yielding an LP-packing. Note that condition $f(x) = f(-x)$ is necessary for $-D_i = D_i$ for all i.

Maiorana-McFarland bent functions $x \cdot \pi(y)$ with permutation π, for which $\pi(-y) \neq -\pi(y)$ for some y are such functions.

- f is regular, not normal. Then $\mathcal{P} = \{D_0, D_1, D_2\}$ is a nonnormal bent partition of $\mathbb{V}_{2m}^{(3)}$ of Type I. Clearly, $\mathcal{P}$ is not an LP-packing, however, if $f(x) = f(-x)$ for all $x \in \mathbb{V}_{2m}^{(3)}$, then $\mathcal{P}$ is a partition of $\mathbb{V}_{2m}^{(3)}$ into three PDSs of Latin square type, otherwise not. We do not know an example of this case.

- f is weakly regular, but not regular, which implies that f is not normal. Then $\mathcal{P} = \{D_0, D_1, D_2\}$ is a nonnormal bent partition of $\mathbb{V}_{2m}^{(3)}$ of Type II, see Equation (1.13).

  Weakly regular but not regular quadratic bent or weakly regular but not regular Coulter-Matthews bent functions are examples of such functions satisfying the condition $f(x) = f(-x)$. We refer to (Coulter & Matthews, 1997) for Coulter-Matthews bent functions.

  Examples not satisfying $f(x) = f(-x)$ for all x can be found as follows. If $f_0, f_1, f_2 : \mathbb{V}_{2m}^{(3)} \to \mathbb{F}_3$ are weakly regular but not regular bent functions, then the function $f : \mathbb{V}_{2m}^{(3)} \times \mathbb{F}_3 \times \mathbb{F}_3 \to \mathbb{F}_3$ given by $f(x, y, z) = f_y(x) - yz$ is weakly regular but not regular, see (Çeşmelioğlu, Meidl & Pott, 2013a), and the condition $f(-x, -y - z) = f(x, y, z)$ does not hold in general.

If f is a non-weakly regular ternary bent function, then by Proposition 4, D_0, D_1, D_2 are not PDSs, but we can obtain bent partitions of all three kinds, as the following examples (confirmed with MAGMA) show.

Example 6. *Let $f : \mathbb{F}_{3^4} \to \mathbb{F}_3$ be given by $f(x) = \mathrm{Tr}_1^4(\alpha^{10}x^{22} + x^4)$, where α is a root of the irreducible polynomial $x^4 + x + 2 \in \mathbb{F}_3[x]$. Then f is a non-weakly regular bent function, see (Helleseth & Kholosha, 2010), which is normal, see (Çeşmelioğlu et al., 2013a). In fact, f vanishes on a 2-dimensional subspace U and $\mathcal{P} = \{U, D_0 \setminus U, D_1, D_2\}$ is a normal bent partition.*

The function $f : \mathbb{F}_{3^6} \to \mathbb{F}_3$ given by $f(x) = \mathrm{Tr}_1^6(\alpha^7 x^{98})$, where α is a primitive element of $\mathbb{F}_{3^6}$, is a not normal non-weakly regular bent function, see (Helleseth & Kholosha, 2006) and (Meidl & Pirsic, 2018). We observe that $|D_0| < |D_1| = |D_2|$, so $\mathcal{P} = \{D_0, D_1, D_2\}$ is a nonnormal bent partition of Type II.

Finally, if $f(x, y) = g(x) + h(y)$ is the direct sum of the non-weakly regular bent function $g : \mathbb{F}_{3^6} \to \mathbb{F}_3$, where $g(x) = \mathrm{Tr}_1^6(\alpha^7 x^{98})$ is as in the previous example, and the weakly regular but not regular quadratic bent function $h : \mathbb{F}_{3^2} \to \mathbb{F}_3$ given by

$h(x) = \mathrm{Tr}_1^2(x^4)$, then $f : \mathbb{F}_{3^6} \times \mathbb{F}_{3^2} \to \mathbb{F}_3$ is non-weakly regular. Using MAGMA, we observe that f is not normal, $|D_0| > |D_1| = |D_2|$. Consequently, $\mathcal{P} = \{D_0, D_1, D_2\}$ is a nonnormal bent partition of Type I.

3. LP-PACKINGS FROM GENERALIZED DESARGUESIAN SPREADS

A main objective in (Jedwab & Li, 2021) is to show that LP-packings exists in a large variety of finite abelian groups. With this aim, a procedure for lifting LP-packings in an abelian group G' to LP-packings in certain larger abelian groups G is presented. More precisely, a recursive method to produce LP-packings in the group $G = \mathbb{Z}_{p^a}^{2s}$, where a and s are positive integers is shown. This method uses spreads in the elementary abelian group $\mathbb{Z}_p^{2s}$ as the base case. In this part, we show that generalized Desarguesian spreads can also be applied in a lifting procedure. On the one hand, we can obtain potentially new LP-packings, hence bent partitions, in elementary abelian groups. On the other hand, LP-packings in nonelementary abelian groups can be obtained from a base case, which is different from a spread.

The concept of LP-partition is essential in the lifting procedure given in (Jedwab & Li, 2021). Hence, first we recall the definition of an LP-partition and some related results obtained in (Jedwab & Li, 2021). For a subgroup H of G, we denote by $H^\perp$ the set of characters which are principal (i.e., trivial) on H.

Definition 12. *(Jedwab & Li, 2021, Definition 4.1) Let $t > 1$ and $c > 0$ be integers. Let G be an abelian group of order t^2c^2, let V be a subgroup of G of order tc^2, and let $H \leqslant V$.*

A (c,t) LP-partition in $G \setminus V$ relative to H is a collection $\{R_1, \ldots, R_t\}$ of t disjoint $(t-1)c^2$-subsets of G whose union is $G \setminus V$ and for which the multiset equality

$$\{\chi(R_1), \ldots, \chi(R_t)\} = \begin{cases} \{-c^2, \ldots, -c^2\} & \text{if } \chi \in V^\perp, \\ \{0, \ldots, 0\} & \text{if } \chi \in H^\perp \setminus V^\perp, \\ \{(t-1)c, -c, \ldots, -c\} & \text{if } \chi \notin H^\perp \end{cases}$$

holds for all non-principal characters χ of G.

Example 7. *(Jedwab & Li, 2021, Example 4.3) Using (Jedwab & Li, 2021, Lemma*

3.3), which gives the character sums over elements of an LP-packing, it is concluded in (Jedwab & Li, 2021) that a $(1,t)$ LP-packing in G relative to a subgroup U is identical to a $(1,t)$ LP-partition in $G \setminus U$ relative to U. Hence, given a spread $\{U_0, U_1, \ldots, U_{p^m}\}$ of $\mathbb{V}_n$, $n = 2m$, the collection $\{U_1^*, \ldots, U_{p^m}^*\}$, where $U_i^* = U_i \setminus \{0\}$, is a $(1,p^m)$ LP-partition of $\mathbb{V}_n \setminus U_0$ relative to the subspace U_0.

In (Jedwab & Li, 2021, Theorem 4.6) a method is presented to construct an LP-partition (in a certain group) from a collection of LP-partitions in some factor groups.

Proposition 5. *(Jedwab & Li, 2021, Theorem 4.6) Let $t = p^k$ for a prime p and a positive integer k. Let*

- *G be an abelian group of order t^4c^2,*
- *$Q \le G' \le G$ be subgroups of G, where $Q \cong \mathbb{Z}_p^{2k}$ and $G/G' \cong \mathbb{Z}_p^{2k}$,*
- *$H_0, \ldots, H_t$ be subgroups of G forming a spread when viewed as subgroups of Q,*
- *$V_0, \ldots, V_t$ be subgroups of G for which $\{V_0/G', \ldots, V_t/G'\}$ is a spread of G/G', and $H_i \le V_i$ for each $i = 1, \ldots, t$.*

Suppose that for each $i = 1, \ldots, t$ there exists a (c,t) LP-partition in $V_i/H_i \setminus G'/H_i$ relative to Q/H_i. Then there exists a (tc,t) LP-partition in $G \setminus V_0$ relative to H_0.

Via combining the subsets of an LP-partition with the subsets obtained by lifting an LP-packing, the following is also shown in (Jedwab & Li, 2021).

Proposition 6. *(Jedwab & Li, 2021, Theorem 4.4) Let $t = p^k$ for a prime p and a positive integer k. Let*

- *G be an abelian group of order t^4c^2, containing subgroups*
- *$H \le U \le V \le G$ of orders t, t^2c, t^3c^2, respectively.*

Suppose that there exists a (tc,t) LP-partition in $G \setminus V$ relative to H, and a (c,t) LP-packing in V/H relative to U/H. Then there exists a (tc,t) LP-packing in G relative to U.

The proofs for Proposition 5 and Proposition 6 are constructive proofs. We refer the reader to (Jedwab & Li, 2021, Section 4).

LP-partitions from spreads are employed in Proposition 5 to construct an LP-partition in G. With spreads in elementary abelian groups, LP-packings can then

be obtained also in nonelementary abelian groups.

To show that certain generalized Desarguesian spreads can also be employed in the lifting procedure, as a first step, we obtain some LP-partitions from the generalized Desarguesian spreads.

3.1 LP-partitions from Generalized Desarguesian Spreads

In this subsection, we generate LP-partitions from generalized Desarguesian spreads for the case where p is odd and $k = m/2$, and for the case that $p = 2$ and $k = m/3$. We note that our required condition $\gcd(2^m - 1, 2^k + 1) = 1$ is satisfied for every m divisible by 3 and $k = m/3$. We will use the following two lemmas, the first one for odd characteristic, the second for characteristic 2.

Lemma 6. *Let $m = 2k$, p be an odd prime such that for $e = p^k + p - 1$ we have $\gcd(p^m - 1, e) = 1$, and define $\mathcal{Z} = \{\omega \in \mathbb{F}_{p^m} : \mathrm{Tr}_k^m(\omega) = 0\}$. Then the following statements hold.*

i) Let $v \in \mathcal{Z} \setminus \{0\}$, $y \in \mathbb{F}_{p^k}$, and let x be the (unique) element in $\mathbb{F}_{p^m}$ such that $vx^e = y$. Then $x \in \mathcal{Z}$.

ii) If $vx^e = y \in \mathbb{F}_{p^k}^*$ for some $v \in \mathbb{F}_{p^m}^*$ and $x \in \mathcal{Z}$, then $v \in \mathcal{Z}$.

Proof. We first show that x^e permutes the set (subspace) $\mathcal{Z}$, i.e., $x \in \mathcal{Z}$ implies $x^e \in \mathcal{Z}$. Then we show that for a product $vx = y \in \mathbb{F}_{p^k} \setminus \{0\}$, if one of the factors is in $\mathcal{Z}$, say $v \in \mathcal{Z}$, then also $x \in \mathcal{Z}$. This simultaneously proves (i) and (ii).

Suppose that $x \in \mathcal{Z}$, then $x + x^{p^k} = 0$, i.e., $x = -x^{p^k}$. This implies that

$$x^e = x^{p^k+p-1} = x^{p^k} x^{p-1} = -xx^{p-1} = -x^p.$$

Note that $x \in \mathcal{Z}$ implies $-x^p \in \mathcal{Z}$, as $x + x^{p^k} = 0$ implies $-(x + x^{p^k})^p = 0$. Hence, $x^e \in \mathcal{Z}$, that is, x^e is a permutation of $\mathcal{Z}$.

For some $y \in \mathbb{F}_{p^k}$ and $v \in \mathcal{Z} \setminus \{0\}$, let $x \in \mathbb{F}_{p^m}$ be such that $vx = y$. Then for $x = \frac{y}{v}$ we have

$$\mathrm{Tr}_k^m(x) = x + x^{p^k} = \frac{y}{v} + \frac{y^{p^k}}{v^{p^k}} = \frac{y}{v} - \frac{y}{v} = 0,$$

where in the last equality we used that $y^{p^k} = y$ as $y \in \mathbb{F}_{p^k}$, and $v^{p^k} = -v$ as $v \in \mathcal{Z}$. Consequently, $x \in \mathcal{Z}$. □

Lemma 7. *Let $m = 3k$, $\mathcal{Z} = \{\omega \in \mathbb{F}_{2^m} : \mathrm{Tr}_k^m(\omega) = 0\}$ and $e = 2^k + 1$. Then the following statements hold.*

i) Let $v \in \mathcal{Z} \setminus \{0\}$, $y \in \mathbb{F}_{2^k}$, and let x be the (unique) element in $\mathbb{F}_{2^m}$ such that $vx^e = y$. Then $x \in \mathcal{Z}$.

ii) If $vx^e = y \in \mathbb{F}_{2^k}^*$ for some $v \in \mathbb{F}_{2^m}^*$ and $x \in \mathcal{Z}$, then $v \in \mathcal{Z}$.

Proof. i) Let $v \in \mathcal{Z} \setminus \{0\}$ be fixed. Then we have $v^{2^{2k}+2^k+1} \in \mathbb{F}_{2^k}$, since $2^m - 1 = (2^k - 1)(2^{2k} + 2^k + 1)$. As $\gcd(2^m - 1, e) = \gcd(2^k - 1, e) = 1$, for any $y \in \mathbb{F}_{2^k}$, there exists a unique $z \in \mathbb{F}_{2^k}$ such that $z^e = z^{2^k+1} = \frac{y}{v^{2^{2k}+2^k+1}}$. Now, observe that $x = zv^{2^k}$, since $vx^e = vz^{2^k+1}(v^{2^k})^{2^k+1} = z^{2^k+1}v^{2^{2k}+2^k+1} = y$. We also have $x \in \mathcal{Z}$, since $z \in \mathbb{F}_{2^k}$ and $v \in \mathcal{Z}$ implies

$$\mathrm{Tr}_k^m(x) = \mathrm{Tr}_k^m(zv^{2^k}) = z\mathrm{Tr}_k^m(v^{2^k}) = z\mathrm{Tr}_k^m(v) = 0.$$

ii) If the element $y = vx^e$ is in $\mathbb{F}_{2^k}^*$, then $y = y^{2^{2k}}$. Note that we have

$$\begin{aligned} y^{2^{2k}} &= (vx^e)^{2^{2k}} = v^{2^{2k}}(x^{2^k+1})^{2^{2k}} = v^{2^{2k}}x^{2^{3k}+2^{2k}} \\ &= v^{2^{2k}}x^{2^{2k}+1}, \end{aligned}$$

as $m = 3k$. Then, $y = y^{2^{2k}}$ implies that $vx^{2^k+1} = v^{2^{2k}}x^{2^{2k}+1}$, and hence $v = v^{2^{2k}}x^{2^{2k}-2^k}$, as $x \neq 0$. That is, $v^{2^k} = v^{2^{3k}}x^{2^{3k}-2^{2k}} = vx^{2^{3k}-2^{2k}}$. Since $v \neq 0$, we have $v^{2^k-1} = x^{2^{2k}(2^k-1)}$, which implies that $v = zx^{2^{2k}}$ for some $z \in \mathbb{F}_{2^k}$. Then

$$\mathrm{Tr}_k^m(v) = \mathrm{Tr}_k^m(zx^{2^{2k}}) = z\mathrm{Tr}_k^m(x^{2^{2k}}) = z\mathrm{Tr}_k^m(x) = 0,$$

since $z \in \mathbb{F}_{p^k}$ and $x \in \mathcal{Z}$. Hence, $v \in \mathcal{Z}$.

□

With Lemma 6, we obtain an LP-partition for odd characteristic.

Proposition 7. *Let $m = 2k$, p be an odd prime such that $\gcd(p^m - 1, p^k + p - 1) = 1$. Suppose that*

- *$G = \mathbb{F}_{p^m} \times \mathbb{F}_{p^m}$, $\mathcal{Z} = \{\omega \in \mathbb{F}_{p^m} : \mathrm{Tr}_k^m(\omega) = 0\}$,*

- $V = \{(x,y) : y \in \mathbb{F}_{p^m}, x \in \mathcal{Z}\}$, $H = \{(0,y) : y \in \mathbb{F}_{p^k}\}$, *and*

- *for* $\gamma \in \mathbb{F}_{p^k}$, $\mathcal{R}(\gamma) = \bigcup_{s \in \mathbb{F}_{p^m} : \mathrm{Tr}_k^m(s) = \gamma} \{(x, sx^e) : x \in \mathbb{F}_{p^m}, x \notin \mathcal{Z}\}$.

Then $\{R(\gamma) : \gamma \in \mathbb{F}_{p^k}\}$ *is a* (p^k, p^k) *LP-partition in* $G \setminus V$ *relative to* H.

Proof. Clearly $t = c = p^k$, $H \leq V \leq G$, and $|V| = tc^2 = p^{3k}$. We also have

$$|R(\gamma)| = p^{m-k}(p^m - p^{m-k}) = p^{2k}(p^k - 1) = (t-1)c^2$$

for all $\gamma \in \mathbb{F}_{p^k}$, $R(\gamma_1) \cap R(\gamma_2) = \emptyset$ if $\gamma_1 \neq \gamma_2$ and $\bigcup_{\gamma \in \mathbb{F}_{p^k}} R(\gamma) = G \setminus V$.

Now we show that the multiset equality in Definition 12 holds for all non-principal characters of $\mathbb{F}_{p^m} \times \mathbb{F}_{p^m}$. That is, we show that

$$\{\chi(R_\gamma) \ : \ \gamma \in \mathbb{F}_{p^k}\} \ = \begin{cases} \{-p^{2k}, \ldots, -p^{2k}\} & , \text{ if } \chi \in V^\perp, \\ \{0, \ldots, 0\} & , \text{ if } \chi \in H^\perp \setminus V^\perp, \\ \{(p^k-1)p^k, -p^k, \ldots, -p^k\} & , \text{ if } \chi \notin H^\perp \end{cases}$$

holds for all non-principal characters of $\mathbb{F}_{p^m} \times \mathbb{F}_{p^m}$.

Let $S_\gamma = \{s \in \mathbb{F}_{p^m} \ : \ \mathrm{Tr}_k^m(s) = \gamma\}$. If we fix $s_\gamma \in S_\gamma$, then $S_\gamma = s_\gamma + \mathcal{Z}$. Note that $\mathcal{Z}^\perp = \{u \in \mathbb{F}_{p^m} \ : \ \mathrm{Tr}_1^m(ux) = 0 \text{ for all } x \in \mathcal{Z}\} = \mathbb{F}_{p^k}$. We again denote the characters of $\mathbb{F}_{p^m} \times \mathbb{F}_{p^m}$ by $\chi_{u,v}(x,y) = \zeta_p^{\mathrm{Tr}_1^m(ux+vy)}$ for $u, v \in \mathbb{F}_{p^m}$ and a primitive p-th root of unity by ζ_p. We have the following cases.

Case 1: $\chi_{u,v} \in V^\perp$.

Since $|V| = p^{3k}$, we have $|V^\perp| = p^k$. As the characters $\chi_{u,0}$ of $\mathbb{F}_{p^m} \times \mathbb{F}_{p^m}$ with $u \in \mathbb{F}_{p^k}$ are principal on V, we have $V^\perp = \{\chi_{u,v} : u \in \mathbb{F}_{p^k}, v = 0\}$. Let $\chi_{u,0}$ be a non-principal character in $V^\perp$, i.e., $u \neq 0$. Recall that $\sum_{x \in \mathbb{F}_{p^m}} \zeta_p^{\mathrm{Tr}_1^m(ux)} = 0$ as $u \neq 0$. Now, we show that $\chi_{u,0}(R_\gamma) = -p^{2k}$ for any $\gamma \in \mathbb{F}_{p^k}$.

$$\begin{aligned} \chi_{u,0}(R_\gamma) &= \sum_{s \in S_\gamma} \sum_{x \in \mathbb{F}_{p^m}} \zeta_p^{\mathrm{Tr}_1^m(ux)} - \sum_{s \in S_\gamma} \sum_{x \in \mathcal{Z}} \zeta_p^{\mathrm{Tr}_1^m(ux)} \\ &= - \sum_{s \in S_\gamma} \sum_{x \in \mathcal{Z}} \zeta_p^{\mathrm{Tr}_1^m(ux)} \\ &= - \sum_{s \in S_\gamma} p^{m-k} = -p^{m-k} p^{m-k} = -p^{2k}, \end{aligned} \tag{3.1}$$

where we used $u \in \mathbb{F}_{p^k} = \mathcal{Z}^\perp$ in the third equality.

Case 2: $\chi_{u,v} \in H^\perp \setminus V^\perp$.

Since $|H| = p^k$, we have $|H^\perp| = p^{2m-k} = p^{3k}$. As the characters $\chi_{u,v}$ of $\mathbb{F}_{p^m} \times \mathbb{F}_{p^m}$

with $u \in \mathbb{F}_{p^m}$ and $v \in \mathcal{Z}$ are principal on H, we have $H^\perp = \{\chi_{u,v} : u \in \mathbb{F}_{p^m}, v \in \mathcal{Z}\}$. Let $\chi_{u,v}$ be a non-principal character in

$$H^\perp \setminus V^\perp = \{\chi_{u,v} : v = 0 \text{ and } u \in \mathbb{F}_{p^m} \setminus \mathbb{F}_{p^k}, \text{ or } v \in \mathcal{Z} \setminus \{0\} \text{ and } u \in \mathbb{F}_{p^m}\}.$$

First suppose that $v = 0$ and $u \in \mathbb{F}_{p^m} \setminus \mathbb{F}_{p^k}$. Note that $\sum_{x \in \mathcal{Z}} \zeta_p^{\mathrm{Tr}_1^m(ux)} = 0$ since $u \notin \mathbb{F}_{p^k}$. Then as in Equation (3.1), we have $\chi_{u,0}(R_\gamma) = -\sum_{s \in S_\gamma} \sum_{x \in \mathcal{Z}} \zeta_p^{\mathrm{Tr}_1^m(ux)} = 0$.

Now suppose that $v \in \mathcal{Z} \setminus \{0\}$ and $u \in \mathbb{F}_{p^m}$. Then by using $S_\gamma = s_\gamma + \mathcal{Z}$, we obtain the following equalities.

$$\begin{aligned}
\chi_{u,v}(R_\gamma) &= \sum_{s \in S_\gamma} \sum_{x \in \mathbb{F}_{p^m}} \zeta_p^{\mathrm{Tr}_1^m(ux+vsx^e)} - \sum_{s \in S_\gamma} \sum_{x \in \mathcal{Z}} \zeta_p^{\mathrm{Tr}_1^m(ux+vsx^e)} \\
&= \sum_{s \in \mathcal{Z}} \sum_{x \in \mathbb{F}_{p^m}} \zeta_p^{\mathrm{Tr}_1^m(ux+v(s_\gamma+s)x^e)} - \sum_{s \in \mathcal{Z}} \sum_{x \in \mathcal{Z}} \zeta_p^{\mathrm{Tr}_1^m(ux+v(s_\gamma+s)x^e)} \\
&= \sum_{x \in \mathbb{F}_{p^m}} \zeta_p^{\mathrm{Tr}_1^m(ux+vx^e s_\gamma)} \sum_{s \in \mathcal{Z}} \zeta_p^{\mathrm{Tr}_1^m(vx^e s)} - \sum_{x \in \mathcal{Z}} \zeta_p^{\mathrm{Tr}_1^m(ux+vx^e s_\gamma)} \sum_{s \in \mathcal{Z}} \zeta_p^{\mathrm{Tr}_1^m(vx^e s)}.
\end{aligned}$$

Recall that

$$\sum_{s \in \mathcal{Z}} \zeta_p^{\mathrm{Tr}_1^m(vx^e s)} = \begin{cases} p^{m-k} & , \text{ if } vx^e \in \mathbb{F}_{p^k}, \\ 0 & , \text{ otherwise.} \end{cases}$$

Hence, we can write $\chi_{u,v}(R_\gamma)$ as

$$\chi_{u,v}(R_\gamma) = p^{m-k} \sum_{\substack{x \in \mathbb{F}_{p^m} \\ vx^e \in \mathbb{F}_{p^k}}} \zeta_p^{\mathrm{Tr}_1^m(ux+vx^e s_\gamma)} - p^{m-k} \sum_{\substack{x \in \mathcal{Z} \\ vx^e \in \mathbb{F}_{p^k}}} \zeta_p^{\mathrm{Tr}_1^m(ux+vx^e s_\gamma)}. \tag{3.2}$$

Since $v \in \mathcal{Z} \setminus \{0\}$, by Lemma 6(i), $vx^e \in \mathbb{F}_{p^k}$ implies that $x \in \mathcal{Z}$. That is, $\sum_{\substack{x \in \mathbb{F}_{p^m} \\ vx^e \in \mathbb{F}_{p^k}}} \zeta_p^{\mathrm{Tr}_1^m(ux+vx^e s_\gamma)} = \sum_{\substack{x \in \mathcal{Z} \\ vx^e \in \mathbb{F}_{p^k}}} \zeta_p^{\mathrm{Tr}_1^m(ux+vx^e s_\gamma)}$, and hence $\chi_{u,v}(R_\gamma) = 0$.

Case 3: $\chi_{u,v} \notin H^\perp$.
Since $\chi_{u,v} \notin H^\perp$, we have $\chi_{u,v}(x,y) = \zeta_p^{\mathrm{Tr}_1^m(ux+vy)}$ for some $u \in \mathbb{F}_{p^m}$ and $v \in \mathbb{F}_{p^m} \setminus \mathcal{Z}$. We can write $\chi_{u,v}(R_\gamma)$ as in Equation (3.2). Since $v \notin \mathcal{Z}$, by Lemma 6(ii), the conditions $x \in \mathcal{Z}$ and $vx^e \in \mathbb{F}_{p^k}$ hold only if $x = 0$. Hence, Equation (3.2) can be written as follows.

$$\chi_{u,v}(R_\gamma) = p^{m-k} \sum_{\substack{x \in \mathbb{F}_{p^m} \\ vx^e \in \mathbb{F}_{p^k}}} \zeta_p^{\mathrm{Tr}_1^m(ux+vx^e s_\gamma)} - p^{m-k}.$$

Set $y = vx^e$. Then we have $x = v^{-d}y^d$ as $de \equiv 1 \bmod (p^m-1)$. Set $\tilde{u} = \mathrm{Tr}_k^m(uv^{-d})$. By using $y \in \mathbb{F}_{p^k}$ and $\mathrm{Tr}_k^m(s_\gamma) = \gamma$, we have the following equalities.

$$\begin{aligned} \mathrm{Tr}_1^m(ux + vx^e s_\gamma) &= \mathrm{Tr}_1^m(uv^{-d}y^d + s_\gamma y) \\ &= \mathrm{Tr}_1^k(\mathrm{Tr}_k^m(uv^{-d})y^d + \mathrm{Tr}_k^m(s_\gamma)y) \\ &= \mathrm{Tr}_1^k(\tilde{u}y^d + \gamma y) = \mathrm{Tr}_1^k(\tilde{u}^p y^{dp} + \gamma y). \end{aligned} \tag{3.3}$$

Since $e = p^k + p - 1$, we have $e \equiv p \bmod (p^k-1)$. Together with $ed \equiv 1 \bmod (p^m-1)$, we obtain that $ed \equiv pd \equiv 1 \bmod (p^k-1)$. That is, $\mathrm{Tr}_1^m(ux + vs_\gamma x^e) = \mathrm{Tr}_1^k((\tilde{u}^p + \gamma)y)$ by Equation (3.3). Then

$$\begin{aligned} \chi_{u,v}(R_\gamma) &= p^{m-k} \sum_{y \in \mathbb{F}_{p^k}} \zeta_p^{\mathrm{Tr}_1^k((\tilde{u}^p+\gamma)y)} - p^{m-k} \\ &= \begin{cases} p^m - p^{m-k} = p^k(p^k-1) & , \text{ if } \gamma = -\tilde{u}^p, \\ -p^{m-k} = -p^k & , \text{ otherwise.} \end{cases} \end{aligned}$$

As there exists a unique $\gamma \in \mathbb{F}_{p^k}$ satisfying $\gamma = -\tilde{u}^p$, we get the desired conclusion. □

With Lemma 7, we similarly obtain an LP-partition in characteristic 2.

Proposition 8. *Let $m = 3k$. Let*

- $G = \mathbb{F}_{2^m} \times \mathbb{F}_{2^m}$, $\mathcal{Z} = \{\omega \in \mathbb{F}_{2^m} : \mathrm{Tr}_k^m(\omega) = 0\}$,
- $V = \{(x,y) : y \in \mathbb{F}_{2^m}, x \in \mathcal{Z}\}$, $H = \{(0,y) : y \in \mathbb{F}_{2^k}\}$, *and*
- *for* $\gamma \in \mathbb{F}_{2^k}$, $\mathcal{R}(\gamma) = \bigcup_{s \in \mathbb{F}_{2^m} : \mathrm{Tr}_k^m(s) = \gamma} \{(x, sx^e) \ : \ x \in \mathbb{F}_{2^m}, x \notin \mathcal{Z}\}$.

Then $\{R(\gamma) \ : \ \gamma \in \mathbb{F}_{2^k}\}$ is a $(2^{2k}, 2^k)$ LP-partition in $G \setminus V$ relative to H.

With Propositions 7 and 8, we obtain LP-partitions from generalized Desarguesian spreads for the two situations, p odd, $k = m/2$, and $p = 2$, $k = m/3$. A natural question is, if the partitions in Proposition 7 and Proposition 8 are LP-partitions also for other divisors k of m satisfying $\gcd(p^m - 1, p^k + p - 1) = 1$.

It is easy to confirm with counterexamples that Lemma 6 does not hold for some odd primes p and $k = m/3$, $k = m/4$ for some integers m. With MAGMA, for $p = 3$, $m = 3$ and $k = m/3 = 1$ and $p = 7$, $m = 4$ and $k = m/4 = 1$, we confirmed that the character value distribution for $\chi \in V^\perp$, $\chi \in H^\perp \setminus V^\perp$ and $\chi \notin H^\perp$, where V, H are defined as in Proposition 7, is in fact not as required in Definition 12.

Consequently, generally Lemma 6 and the analog Lemma 7 are required so that the partitions in Propositions 7 and 8 are LP-partitions. In the following, we will show that Lemma 6(i) respectively Lemma 7(i) never holds if $k < m/4$. This shows that in general, we can not expect to obtain LP-partitions as in Propositions 7 and 8 for other divisors k of m. (Observe that for $p = 2$, $k = m/2$ and $k = m/4$ do not satisfy $\gcd(2^m - 1, 2^k + 1) = 1$.)

In our next proofs, we will employ some basic facts from the theory of function fields over finite fields, which we summarize in the following. For details, we refer to (Stichtenoth, 2009). Let F be a function field of genus $g(F)$ over the constant field $\mathbb{F}_{p^m}$. We say that $\mathbb{F}_{p^m}$ is the full constant field of F if $\mathbb{F}_{p^m}$ is algebraically closed in F. We denote by $\mathbb{P}_F$ the set of all places of F. For $P \in \mathbb{P}_F$, we denote by $\mathcal{O}_P$ the corresponding valuation ring and by v_P the corresponding valuation of P. The quotient ring $\mathcal{O}_P/P$ is a field containing $\mathbb{F}_{p^m}$. The extension degree $[\mathcal{O}_P/P : \mathbb{F}_{p^m}]$ of $\mathcal{O}_P/P$ over $\mathbb{F}_{p^m}$ is finite, and it is called the degree of P, denoted by $\deg(P)$. If $\deg(P) = 1$, that is, $\mathcal{O}_P/P = \mathbb{F}_{p^m}$, then P is called rational. If $F = \mathbb{F}_{p^m}(u)$, i.e., F is a rational function field, then we denote by $(u = \alpha)$ and $(u = \infty)$ the places of F corresponding to the zero and the pole of $u - \alpha$, respectively.

Let F/E be a Galois extension of function fields of degree n. A place P of F is said to lie over the place R of E, denoted by $P|R$, if $R \subseteq P$. For any element $\alpha \in E$, we have $v_P(\alpha) = e(P|R)v_R(\alpha)$ for a fixed positive integer $e(P|R)$, which is called the ramification index of P over R. Moreover, $\mathcal{O}_R/R$ is a subfield of $\mathcal{O}_P/P$, and the extension degree $[\mathcal{O}_P/P : \mathcal{O}_R/R]$ is called the relative degree of P over R, denoted by $f(P|R)$. For any place R of E, there are finitely many places of F lying over R. By the Fundamental Equality (Stichtenoth, 2009, Theorem 3.1.11), we have $\sum_{P|R} e(P|R)f(P|R) = [F : E] = n$, where the sum runs over the places of F lying over R. If $e(P|R) = n$, then we say that R is totally ramified in F. If this holds, then P is the unique place lying over R. If there are n places of F lying over R, then we say that R splits completely in F. In both cases, the degree of a place over R and the degree of R are the same.

For a Galois extension F/E, let P be a place of F lying over the place R of E. We denote by $G_i(P|R)$ the i-th ramification group of P over R for $i \geq -1$. The different exponent $d(P|R)$ of P over R can be given by $d(P|R) = \sum_{i=0}^{\infty} |G_i(P|R)|$. Then, by the Hurwitz genus formula (Stichtenoth, 2009, Theorem 3.4.13), we can give the genus $g(F)$ via the following formula if F and E have the same full constant field.

$$2g(F) - 2 = [F : E](2g(E) - 2) + \sum_{P|R} \sum_{R \in \mathbb{P}_E} d(P|R)\deg(P).$$

We are mainly interested in Galois extensions of Artin-Schreier type. For details, we refer to (Stichtenoth, 2009, Proposition 3.7.8).

Lemma 8. *Let $F_1 = \mathbb{F}_{p^m}(u, \beta)$ and $F_2 = \mathbb{F}_{p^m}(u, \gamma)$ be the function fields defined by $\beta^{p^k} - \beta = u$ and $\gamma^{p^k} - \gamma = u^{-e}$, respectively. Consider the compositum F of F_1 and F_2 over $\mathbb{F}_{p^m}(u)$. Then the following statements hold.*

(i) $\mathbb{F}_{p^m}$ *is the full constant field of* F.

(ii) The extension degree $[F : \mathbb{F}_{p^m}(u)]$ *is* p^{2k}.

(iii) $g(F) = \frac{1}{2}\left(p^k(e+1)(p^k-1) - 2(p^k-1)\right)$.

(iv) $(u = 0)$ *and* $(u = \infty)$ *are the only places of* $\mathbb{F}_{p^m}(u)$ *ramified in* F. *Their ramification indices are* p^k, *and there are* p^k *rational places lying over each of them.*

(v) If P *is a rational place of* F *lying over* $(u = \alpha)$ *for some* $\alpha \in \mathbb{F}_{p^m}^*$, *then there are* p^{2k} *rational places lying over* $(u = \alpha)$.

Proof. The extensions $F_1/\mathbb{F}_{p^m}(u)$ and $F_2/\mathbb{F}_{p^m}(u)$ are Galois extensions of degree p^k, namely Artin-Schreier extensions. The pole $(u = \infty)$ of u is the only place of $\mathbb{F}_{p^m}(u)$ which is ramified in F_1. It is totally ramified with the different exponent $2(p^k - 1)$. Therefore, $\mathbb{F}_{p^m}$ is the full constant field of F_1, and by the Hurwitz genus formula, $g(F_1) = 0$. Moreover, $(u = 0)$ is the only place of $\mathbb{F}_{p^m}(u)$ which is ramified in F_2. It is totally ramified with different exponent $(e+1)(p^k - 1)$. The field $\mathbb{F}_{p^m}$ is also the full constant field of F_2. By the Hurwitz genus formula, we have

$$2g(F_2) - 2 = -2p^k + (e+1)(p^k - 1).$$

Since $(u = \infty)$ is not ramified in F_2, any place R of F_2 lying over $(u = \infty)$ is ramified in F with the ramification index p^k, i.e., it is totally ramified. This implies that $\mathbb{F}_{p^m}$ is the full constant field of F and that F/F_2 is an Artin-Schreier extension of degree p^k, which proves (i) and (ii).

Since $(u = \infty)$ is the only ramified place in F_1, a place R of F_2 is ramified in F if and only if R lies over $(u = \infty)$, see Abhyankar's lemma (Stichtenoth, 2009, Theorem 3.9.1). As $(u = \infty)$ splits completely in F_2, there are p^k rational places of F_2 lying over $(u = \infty)$ totally ramified in F with different exponents $2(p^k - 1)$.

Then considering the extension F/F_2, by the Hurwitz genus formula, we obtain

$$\begin{aligned} 2g(F) &= p^k(-2p^k + (e+1)(p^k-1)) + 2p^k(p^k-1) + 2 \\ &= p^k(e+1)(p^k-1) - 2(p^k-1), \end{aligned}$$

which proves (iii).

Similarly, $(u=0)$ is the only place of $\mathbb{F}_{p^m}(u)$ ramified in F_2, which splits completely in F_1. Hence, the only ramified places of F_1 in F are the rational ones lying over $(u=0)$, which proves (iv) together with the above arguments.

Let P be a rational place of F lying over $(u=\alpha)$ for $\alpha \in \mathbb{F}_{p^m}^*$. As P is rational, the places $P \cap F_1$ and $P \cap F_2$ of F_1 and F_2, respectively, are rational. As $F_1/\mathbb{F}_{p^m}(u)$ and $F_2/\mathbb{F}_{p^m}(u)$ are Galois extensions, this implies that $(u=\alpha)$ splits completely in F_1 and F_2. Therefore, $(u=\alpha)$ splits completely in F, see (Stichtenoth, 2009, Proposition 3.9.6). As $[F : \mathbb{F}_{p^m}(u)] = p^{2k}$, there are p^{2k} rational places lying over $(u=\alpha)$, which proves (v). □

For a function field F of genus $g(F)$ with the full constant field $\mathbb{F}_{p^m}$, the Hasse-Weil bound ((Stichtenoth, 2009, Theorem 5.2.3)) states that the number $N(F)$ of rational places of F satisfies the following equality:

$$|N(F) - (p^m+1)| \leq 2p^{m/2} g(F)$$

Therefore, by Lemma 8 (i) and (iii), we obtain the following result.

Corollary 2. *Let F be the function field defined as in Lemma 8. Then the number $N(F)$ of rational places of F satisfies*

$$N(F) \leq p^m + 1 + p^{m/2}\left(p^k(e+1)(p^k-1) - 2(p^k-1)\right). \tag{3.4}$$

Proposition 9. *Let $k < m/4$. Then for any given $v \in \mathcal{Z}$, there exists $x \in \mathbb{F}_{p^m} \setminus \mathcal{Z}$ such that $vx^e \in \mathbb{F}_{p^k}$.*

Proof. For $v \in \mathcal{Z}$ and $y \in \mathbb{F}_{p^k}$, suppose that there exists $x \in \mathcal{Z}$ such that $y = vx^e$, i.e., $v = yx^{-e}$. This holds if and only if $v^{-d} = (yx^{-e})^{-d} = y^{-d}x$, as $ed \equiv 1 \bmod (p^m-1)$. Then we have

$$\mathrm{Tr}_k^m(v^{-d}) = \mathrm{Tr}_k^m(y^{-d}x) = y^{-d}\mathrm{Tr}_k^m(x) = 0,$$

i.e., we have $\mathrm{Tr}_k^m(v) = \mathrm{Tr}_k^m(v^{-d}) = 0$. In particular, for any given $v \in \mathcal{Z}$ and $y \in \mathbb{F}_{p^k}$,

there exists $x \in \mathcal{Z}$ satisfying $y = vx^e$ if and only if the map $v \mapsto v^{-d}$ is a bijection on $\mathcal{Z}$. Hence, we conclude that $\mathrm{Tr}_k^m(v) = 0$ if and only if $\mathrm{Tr}_k^m(v^{-d}) = 0$. Setting $u = v^{-d}$, this is equivalent to the following property:
P: $\mathrm{Tr}_k^m(u) = 0$ if and only if $\mathrm{Tr}_k^m(u^{-e}) = 0$.
Therefore, it suffices to show that the number N_u of elements $u \in \mathbb{F}_{p^m}$ satisfying **P** is less than p^{m-k} if $k < m/4$.

Suppose that $\mathrm{Tr}_k^m(u) = \mathrm{Tr}_k^m(u^{-e}) = 0$, then there exist $\beta, \gamma \in \mathbb{F}_{p^m}$ such that $u = \beta^{p^k} - \beta$ and $u^{-e} = \gamma^{p^k} - \gamma$. Consequently, (β, γ) is an $(\mathbb{F}_{p^m}$-)rational point of the curve $\mathcal{X}$ over $\mathbb{F}_{p^m}$ defined by $f(Y, Z) = (Y^{p^k} - Y)^e (Z^{p^k} - Z) - 1$. Then F, given as in Lemma 8, is the function field of $\mathcal{X}$.

An affine point (β_0, γ_0) of $\mathcal{X}$ is singular if and only if $(\partial f/\partial Y)(\beta_0, \gamma_0) = (\partial f/\partial Z)(\beta_0, \gamma_0) = f(\beta_0, \gamma_0) = 0$, where $\partial f/\partial Y$ and $\partial f/\partial Z$ denote the partial derivatives of f with respect to Y and Z, respectively. Since $\partial f/\partial Y = (Y^{p^k} - Y)^{e-1}(Z^{p^k} - Z)$ and $\partial f/\partial Z = -(Y^{p^k} - Y)^e$, the curve $\mathcal{X}$ has no affine singular points. A point $(\beta_0 : \gamma_0 : 0)$ is a point of $\mathcal{X}$ at infinity if and only if $\beta_0 = 0$ or $\gamma_0 = 0$. More precisely, $P_1 = (0 : 1 : 0)$ and $P_2 = (1 : 0 : 0)$ are the only points of $\mathcal{X}$ at infinity with multiplicities $m_{P_1} = p^k e$ and $m_{P_2} = p^k$, respectively.

It is a well-known fact that each non-singular rational point of $\mathcal{X}$ corresponds to a unique rational place of its function field. Since P_1 and P_2 are the points corresponding to places of F lying over $(u = 0)$ and $(u = \infty)$, respectively, there is a one to one correspondence between the set of affine rational points of $\mathcal{X}$ and the set of rational places of F not lying over $(u = 0)$ and $(u = \infty)$. Recall that there are $2p^k$ rational places lying over $(u = 0)$ and $(u = \infty)$. Also, we know that if there is a rational place lying over $(u = \alpha)$ with $\alpha \in \mathbb{F}_{p^m}^*$, then there are p^{2k} rational places lying over $(u = \alpha)$ by Lemma 8. Therefore, we have

$$N_u = \frac{N_{aff}(\mathcal{X})}{p^{2k}} + 1 = \frac{N(F) - 2p^k}{p^{2k}} + 1, \tag{3.5}$$

where $N_{aff}(\mathcal{X})$ is the number of affine rational points of $\mathcal{X}$ (and $+1$ corresponds to $u = 0$). Then we obtain the desired result $N_u < p^{m-k}$ by Equations (3.4) and (3.5). □

3.2 Lifting of Generalized Desarguesian Spreads

In (Jedwab & Li, 2021, Section 5), a recursive construction of LP-packings in nonelementary abelian groups is presented, which uses spreads in elementary abelian groups as initial ingredient. We apply the results in (Jedwab & Li, 2021), which we recall in Propositions 5 and 6, with the LP-partitions we derived from generalized Desarguesian spreads in Section 3.1. The resulting recursive procedure in Theorem 16 below applies for odd characteristic.

Theorem 16. *Let p be odd and $m = 2k$. Then for all $\ell \geq -1$, there exists a $(p^{m+\ell k}, p^k)$ LP-packing*

(i) in the (nonelementary abelian) group $G \cong \mathbb{Z}_{p^{\ell+2}}^{2k} \times \mathbb{V}_{2m-2k}^{(p)}$ relative to $U \cong \mathbb{Z}_{p^{\ell+2}}^{k} \times \mathbb{V}_{m-k}^{(p)}$, and

(ii) in the elementary abelian group $G \cong \mathbb{V}_{2m+2(\ell+1)k}^{(p)}$ relative to $U \cong \mathbb{V}_{m+(\ell+1)k}^{(p)}$.

Proof. The proof is by induction on ℓ. Again, let $\mathcal{Z} = \{x \in \mathbb{F}_{p^m} : \mathrm{Tr}_k^m(x) = 0\}$. Using that p does not divide m/k, one can easily confirm that $\mathbb{Z}_p^k \times \mathcal{Z} \cong \mathbb{F}_{p^k} \times \mathcal{Z} \cong \mathbb{F}_{p^m}$. In the nonelementary abelian case, we identify the group $G \cong \mathbb{Z}_{p^{\ell+2}}^{2k} \times \mathbb{V}_{2m-2k}^{(p)}$ with $G = \mathbb{Z}_{p^{\ell+2}}^{k} \times \mathcal{Z} \times \mathbb{Z}_{p^{\ell+2}}^{k} \times \mathcal{Z}$. The elementary abelian group $G \cong \mathbb{V}_{2m+2(\ell+1)k}^{(p)}$ will be identified with $G = \mathbb{F}_{p^k} \times \mathcal{Z} \times \mathbb{F}_{p^k} \times \mathcal{Z} \times \mathbb{F}_{p^k}^{\ell+1} \times \mathbb{F}_{p^k}^{\ell+1}$. Note that for $\ell = -1$, we have the elementary abelian group of order p^{2m} in both cases.

(i) In the case of the nonelementary abelian group, we have the following induction hypothesis.
We suppose that for $-1 \leq t < \ell$ there exist a (p^{m+tk}, p^k) LP-partition in $\mathbb{Z}_{p^{t+2}}^{k} \times \mathcal{Z} \times \mathbb{Z}_{p^{t+2}}^{k} \times \mathcal{Z} \setminus \mathbb{Z}_{p^{t+1}}^{k} \times \mathcal{Z} \times \mathbb{Z}_{p^{t+2}}^{k} \times \mathcal{Z}$ relative to $\{0\} \times \{0\} \times \mathbb{Z}_p^k \times \{0\}$ and a (p^{m+tk}, p^k) LP-packing in $\mathbb{Z}_{p^{t+2}}^{k} \times \mathcal{Z} \times \mathbb{Z}_{p^{t+2}}^{k} \times \mathcal{Z}$ relative to $\{0\} \times \{0\} \times \mathbb{Z}_{p^{t+2}}^{k} \times \mathcal{Z}$.

Note that, for $t = -1$, the existence of an LP-partition holds by Proposition 7 and the second argument holds by the LP-packing obtained with a spread in an elementary abelian p-group.

For $t = \ell$, we define the following subgroups of the nonelementary abelian

group $G = \mathbb{Z}_{p^{\ell+2}}^k \times \mathcal{Z} \times \mathbb{Z}_{p^{\ell+2}}^k \times \mathcal{Z}$.

$$
\begin{aligned}
G' &= (p\mathbb{Z}_{p^{\ell+2}})^k \times \mathcal{Z} \times (p\mathbb{Z}_{p^{\ell+2}})^k \times \mathcal{Z},\\
V = V_0 &= (p\mathbb{Z}_{p^{\ell+2}})^k \times \mathcal{Z} \times \mathbb{Z}_{p^{\ell+2}}^k \times \mathcal{Z},\\
U &= \{0\} \times \{0\} \times \mathbb{Z}_{p^{\ell+2}}^k \times \mathcal{Z},\\
Q &= (p^{\ell+1}\mathbb{Z}_{p^{\ell+2}})^k \times \{0\} \times (p^{\ell+1}\mathbb{Z}_{p^{\ell+2}})^k \times \{0\}, \text{ and}\\
H = H_0 &= \{0\} \times \{0\} \times (p^{\ell+1}\mathbb{Z}_{p^{\ell+2}})^k \times \{0\}.
\end{aligned}
$$

Note that we have $G/G' \cong Q \cong \mathbb{Z}_p^k \times \mathbb{Z}_p^k$. Consider the group homomorphism $\varphi : G \to Q$ defined by $(a,b,c,d) \mapsto (p^{\ell+1}a, 0, p^{\ell+1}c, 0)$. The map φ is onto and its kernel $\mathrm{Ker}(\varphi)$ is G'. Consequently, $\bar{\varphi} : G/G' \to Q$ defined by $(a,b,c,d) + G' \mapsto \varphi(a,b,c,d)$ is an isomorphism.

Let $\{H_i : i = 0, \ldots, p^k\}$ be a spread of Q. Set $V_i = \varphi^{-1}(H_i)$ for $i = 0, \ldots, p^k$. Then $\{V_i/G' : i = 0, \ldots, p^k\}$ is a spread of G/G'. Note that

$$H_i \leq Q \leq G' \leq V_i \leq G,$$

and $(a,b,c,d) \in V_i$ if and only if $(p^{\ell+1}a, 0, p^{\ell+1}c, 0) \in H_i$. Hence, we observe that for any $(a,b,c,d) + H_i \in V_i/H_i$, we have $p^{\ell+1}((a,b,c,d) + H_i) = (p^{\ell+1}a, 0, p^{\ell+1}c, 0) + H_i = H_i$. Therefore, an element of V_i/H_i has order at most $p^{\ell+1}$. Since the order of V_i/H_i is $p^{2(m+\ell k)}$, we conclude that

$$V_i/H_i \cong \mathbb{Z}_{p^{\ell+1}}^k \times \mathcal{Z} \times \mathbb{Z}_{p^{\ell+1}}^k \times \mathcal{Z}.$$

By induction hypothesis (for $t = \ell - 1$), we know that there exists a $(p^{m+(\ell-1)k}, p^k)$ LP-partition in $V_i/H_i \setminus G'/H_i$ relative to Q/H_i. Hence, by Proposition 5 we conclude that there exists a $(p^{m+\ell k}, p^k)$ LP-partition in $G \setminus V$ relative to H. Moreover, by induction hypothesis there exists a $(p^{m+(\ell-1)k}, p^k)$ LP-packing in $V/H \cong \mathbb{Z}_{p^{\ell+1}}^k \times \mathcal{Z} \times \mathbb{Z}_{p^{\ell+1}}^k \times \mathcal{Z}$ relative to $U/H \cong \{0\} \times \{0\} \times \mathbb{Z}_{p^{\ell+1}}^k \times \mathcal{Z}$. Hence, by Proposition 6, there is a $(p^{m+\ell k}, p^k)$ LP-packing in G relative to U.

(ii) In the case of the elementary abelian group, we have the following induction hypothesis.
We suppose that for $-1 \leq t < \ell$ there exist a (p^{m+tk}, p^k) LP-partition in $\mathbb{F}_{p^k} \times \mathcal{Z} \times \mathbb{F}_{p^k} \times \mathcal{Z} \times \mathbb{F}_{p^k}^{t+1} \times \mathbb{F}_{p^k}^{t+1} \setminus \{0\} \times \mathcal{Z} \times \mathbb{F}_{p^k} \times \mathcal{Z} \times \mathbb{F}_{p^k}^{t+1} \times \mathbb{F}_{p^k}^{t+1}$ relative to $\{0\} \times \{0\} \times \mathbb{F}_{p^k} \times \{0\} \times \{0\}^{t+1} \times \{0\}^{t+1}$, and a (p^{m+tk}, p^k) LP-packing in $\mathbb{F}_{p^k} \times \mathcal{Z} \times \{0\} \times \mathcal{Z} \times \mathbb{F}_{p^k}^{t+1} \times \mathbb{F}_{p^k}^{t+1} \times \{0\} \times \mathbb{F}_{p^k}$ relative to $\{0\} \times \{0\} \times \{0\} \times \mathcal{Z} \times \{0\}^{t+1} \times$

$\mathbb{F}_{p^k}^{t+1} \times \{0\} \times \mathbb{F}_{p^k}$.

Note that, for $t = -1$, the existence of the LP-partition and the LP-packing follows from the previous argument.

For $t = \ell$, we similarly define the following subgroups of the elementary abelian group $G = \mathbb{F}_{p^k} \times \mathcal{Z} \times \mathbb{F}_{p^k} \times \mathcal{Z} \times \mathbb{F}_{p^k}^{\ell+1} \times \mathbb{F}_{p^k}^{\ell+1}$.

$$\begin{aligned}
G' &= \mathbb{F}_{p^k} \times \mathcal{Z} \times \mathbb{F}_{p^k} \times \mathcal{Z} \times \mathbb{F}_{p^k}^{\ell} \times \mathbb{F}_{p^k}^{\ell} \times \{0\} \times \{0\},\\
V &= V_0 = \mathbb{F}_{p^k} \times \mathcal{Z} \times \mathbb{F}_{p^k} \times \mathcal{Z} \times \mathbb{F}_{p^k}^{\ell} \times \mathbb{F}_{p^k}^{\ell} \times \{0\} \times \mathbb{F}_{p^k},\\
U &= \{0\} \times \{0\} \times \mathbb{F}_{p^k} \times \mathcal{Z} \times \{0\}^{\ell} \times \mathbb{F}_{p^k}^{\ell} \times \{0\} \times \mathbb{F}_{p^k},\\
Q &= \mathbb{F}_{p^k} \times \{0\} \times \mathbb{F}_{p^k} \times \{0\} \times \{0\}^{\ell+1} \times \{0\}^{\ell+1}, \text{ and}\\
H &= H_0 = \{0\} \times \{0\} \times \mathbb{F}_{p^k} \times \{0\} \times \{0\}^{\ell+1} \times \{0\}^{\ell+1}.
\end{aligned}$$

Then, for $s \in \mathbb{F}_{p^k}$, we define

$$\begin{aligned}
H_s &= \{(x, 0, sx, 0) : x \in \mathbb{F}_{p^k}\} \times \{0\}^{\ell+1} \times \{0\}^{\ell+1}, \text{ and}\\
V_s &= \mathbb{F}_{p^k} \times \mathcal{Z} \times \mathbb{F}_{p^k} \times \mathcal{Z} \times \mathbb{F}_{p^k}^{\ell} \times \mathbb{F}_{p^k}^{\ell} \times \{(z, sz) : z \in \mathbb{F}_{p^k}\}.
\end{aligned}$$

Observe that $\{H, H_s : s \in \mathbb{F}_{p^k}\}$ forms a spread of Q. Moreover, we have $H \leq G' \leq V$, $H_s \leq G' \leq V_s$, and $\{V/G', V_s/G' : s \in \mathbb{F}_{p^k}\}$ forms a spread of G/G'. For a fixed $s \in \mathbb{F}_{p^k}$, we consider $\varphi_s : V_s \to \mathbb{F}_{p^k} \times \mathcal{Z} \times \mathbb{F}_{p^k} \times \mathcal{Z} \times \mathbb{F}_{p^k}^{\ell} \times \mathbb{F}_{p^k}^{\ell}$ given by $(x, u, y, w, \alpha, \beta, z, sz) \mapsto (z, u, y - sx, w, \alpha, \beta)$. Then $\varphi_s(x, u, y, w, \alpha, \beta, z, sz) = (0, 0, 0, 0, 0, 0)$ if and only if $z = u = w = \alpha = \beta = 0$ and $y = sx$. Equivalently, $(x, u, y, w, \alpha, \beta, z, sz) \in H_s$. Since φ_s is onto, $\bar{\varphi} : V_s/H_s \to \mathbb{F}_{p^k} \times \mathcal{Z} \times \mathbb{F}_{p^k} \times \mathcal{Z} \times \mathbb{F}_{p^k}^{\ell} \times \mathbb{F}_{p^k}^{\ell}$ defined by $(x, u, y, w, \alpha, \beta, z, sz) + H_s \mapsto \varphi_s(x, u, y, w, \alpha, \beta, z, sz)$ is an isomorphism. We also have

$$\begin{aligned}
\bar{\varphi}_s(G'/H_s) &= \{0\} \times \mathcal{Z} \times \mathbb{F}_{p^k} \times \mathcal{Z} \times \mathbb{F}_{p^k}^{\ell} \times \mathbb{F}_{p^k}^{\ell}, \text{ and}\\
\bar{\varphi}_s(Q/H_s) &= \{0\} \times \{0\} \times \mathbb{F}_{p^k} \times \{0\} \times \{0\}^{\ell} \times \{0\}^{\ell}.
\end{aligned}$$

By induction hypothesis, there exists a $(p^{m+(\ell-1)k}, p^k)$ LP-partition in $V_s/H_s \setminus G'/H_s$ relative to Q/H_s. Then by Proposition 5, there exists a $(p^{m+\ell k}, p^k)$ LP-partition in $G \setminus V$ relative to H. Moreover, by induction hypothesis $V/H = \mathbb{F}_{p^k} \times \mathcal{Z} \times \{0\} \times \mathcal{Z} \times \mathbb{F}_{p^k}^{\ell} \times \mathbb{F}_{p^k}^{\ell} \times \{0\} \times \mathbb{F}_{p^k}$ has a $(p^{m+(\ell-1)k}, p^k)$ LP-packing relative to $U/H = \{0\} \times \{0\} \times \{0\} \times \mathcal{Z} \times \{0\}^{\ell} \times \mathbb{F}_{p^k}^{\ell} \times \{0\} \times \mathbb{F}_{p^k}$. Hence, by Proposition 6 there is a $(p^{m+\ell k}, p^k)$ LP-packing in G relative to U.

We note that with a proper isomorphism of G, we obtain the induction hy-

pothesis for $t = \ell$. More precisely, by identifying $G = \mathbb{F}_{p^k} \times \mathcal{Z} \times \mathbb{F}_{p^k} \times \mathcal{Z} \times \mathbb{F}_{p^k}^{\ell} \times \mathbb{F}_{p^k}^{\ell} \times \mathbb{F}_{p^k} \times \mathbb{F}_{p^k}$, the isomorphism ψ of G defined by

$$\psi(x, u, y, w, \alpha, \beta, z, s) = (z, u, x, w, \alpha, \beta, y, s)$$

gives the arguments in the induction hypothesis.

□

4. SOME SECONDARY CONSTRUCTIONS

Let $\Gamma = \{A_1, A_2, \ldots, A_{p^k}\}$ be a bent partition of $\mathbb{V}_n^{(p)}$ of depth p^k. By definition, every p-ary function of which every $c \in \mathbb{F}_p$ has exactly p^{k-1} of the sets A_j in its preimage set is a bent function. Then by Theorem 12, every function from $\mathbb{V}_n^{(p)}$ to $\mathbb{V}_k^{(p)}$, which maps to every $\gamma \in \mathbb{V}_k^{(p)}$ exactly one of the sets A_j, is a vectorial bent function. In (Wang et al., 2023), where connections between bent partitions and induced vectorial bent functions are investigated, the following class of vectorial dual-bent functions, respectively, of bent partitions are defined.

Definition 13. *Let n, k be two positive integers with n being even and $k \leq n/2$.*

(i) A vectorial dual-bent function $F : \mathbb{V}_n^{(p)} \to \mathbb{V}_k^{(p)}$ is said to satisfy Condition $\mathcal{A}$ if

- *every component function $F_c = \langle c, F\rangle_k$, $c \in \mathbb{V}_k^{(p)} \setminus \{0\}$, of F is regular or every component function F_c is weakly regular but not regular, and*
- *there exists a vectorial dual F^* of F such that for every nonzero $c \in \mathbb{V}_k^{(p)}$ we have $(F_c)^* = F_c^*$ (i.e., σ in Remark 1 is the identity permutation).*

(ii) Let $\Gamma = \{A_c : c \in \mathbb{V}_k^{(p)}\}$ be a bent partition of $\mathbb{V}_n^{(p)}$ of depth p^k. We say that Γ satisfies Condition $\mathcal{C}$ if

- *$\mathbb{F}_p^* A_c = A_c$ for all $c \in \mathbb{V}_k^{(p)}$, and*
- *every bent function which is obtained from Γ is regular, or every bent function which is obtained from Γ is weakly regular but not regular.*

Remark 8. *Let $\Gamma = \{A_c : c \in \mathbb{V}_k^{(p)}\}$, with p being odd, be a bent partition satisfying Condition $\mathcal{C}$, and let $f : \mathbb{V}_n^{(p)} \to \mathbb{F}_p$ be a bent function obtained from Γ. If Γ is of Type I, then from the cardinalities given in Equation 1.13 we get $\mathcal{W}_f(0) = \sum_{t\in\mathbb{F}_p} |f^{-1}(t)|\zeta_p^t = p^{n/2}\zeta_p^c$, if A_1 is mapped to c. Hence, f is regular. In the case where Γ is of Type II, in the same way we get $\mathcal{W}_f(0) = -p^{n/2}\zeta_p^c$, which implies that f is weakly regular but not regular. The second case can only occur if $p = 3$ (see Proposition 3 in (Wang, Fu & Wei, 2024)).*

Proposition 10. *(Wang et al., 2023, Theorems 1, 2) Let $F : \mathbb{V}_n^{(p)} \to \mathbb{V}_k^{(p)}$ be a vectorial dual-bent function satisfying Condition $\mathcal{A}$, and let $D_F^c = \{x \in \mathbb{V}_n^{(p)} : F(x) = c\}$ be the preimage set of $c \in \mathbb{V}_k^{(p)}$. Then $\{D_F^c : c \in \mathbb{V}_k^{(p)}\}$ is a bent partition of $\mathbb{V}_n^{(p)}$ of depth p^k satisfying Condition $\mathcal{C}$.*
Conversely, if p is odd and $\Gamma = \{A_c : c \in \mathbb{V}_k^{(p)}\}$ is a bent partition of $\mathbb{V}_n^{(p)}$ satisfying Condition $\mathcal{C}$, then with $F(x) = c$ if $x \in A_c$, we obtain a vectorial dual-bent function $F : \mathbb{V}_n^{(p)} \to \mathbb{V}_k^{(p)}$, which satisfies Condition $\mathcal{A}$.

It follows from Proposition 10 that vectorial dual-bent functions with Condition $\mathcal{A}$ and bent partitions with Condition $\mathcal{C}$ are equivalent concepts for odd primes p.

Using Remark 8, we say that a vectorial dual-bent function F satisfying Condition $\mathcal{A}$ is of Type I if its components are regular; otherwise F is of Type II. The equivalences in Proposition 10 can be extended via partial difference sets, see (Wang et al., 2023, Section IV), (Wang et al., 2024).

Proposition 11. *For an even integer n, an integer $k \leq n/2$, and an odd prime p with $p^k > 3$, let F be a function from $\mathbb{V}_n^{(p)}$ to $\mathbb{V}_k^{(p)}$, and for every $c \in \mathbb{V}_k^{(p)}$, let D_F^c be the preimage set of c. Then the following is equivalent.*

(i) F is a vectorial dual-bent function satisfying Condition $\mathcal{A}$.

(ii) $\Gamma = \{D_F^c : c \in \mathbb{V}_k^{(p)}\}$ is a bent partition of $\mathbb{V}_n^{(p)}$ of depth p^k satisfying Condition $\mathcal{C}$.

(iii) All sets D_F^c are $(p^{n/2}, p^{n/2-k})$ Latin square type PDS, respectively, negative Latin square type PDS, except for one set $D_F^{c_0}$ which contains the element 0, and for which $D_F^{c_0} \setminus \{0\}$ is a $(p^{n/2}, p^{n/2-k}+1)$ Latin square type PDS, respectively, a $(p^{n/2}, p^{n/2-k}-1)$ negative Latin square type PDS. The negative Latin square type case corresponds to the case that Γ is of Type II (this case can only occur if $p = 3$).

Remark 9. *The situation is slightly different for the case $p = 2$, for which every bent partition trivially satisfies Condition $\mathcal{C}$. The preimage set partition of a vectorial dual-bent function $F : \mathbb{V}_n^{(2)} \to \mathbb{V}_k^{(2)}$ satisfying Condition $\mathcal{A}$ is a bent partition of which the sets are Latin square type PDSs, and a vectorial bent function derived from a bent partition of $\mathbb{V}_n^{(2)}$ of which all sets are Latin square type PDSs, is a vectorial dual-bent function satisfying Condition $\mathcal{A}$. However, there may exist bent partitions of $\mathbb{V}_n^{(2)}$, of which not all sets are PDSs, and for which a corresponding vectorial bent*

function is not a vectorial dual-bent function satisfying Condition $\mathcal{A}$. By Theorem 14, for a normal bent partition $\{U, A_1, \ldots, A_{2^k}\}$ of $\mathbb{V}_n^{(2)}$, either all sets A_i are Latin square type PDSs, or none of them is a PDS.

For odd characteristic, we can extend the equivalences in Proposition 11 to normal bent partitions.

Proposition 12. *For an odd prime p, an even integer n and an integer $k \leq n/2$ with $p^k > 3$, let F be a function from $\mathbb{V}_n^{(p)}$ to $\mathbb{V}_k^{(p)}$, and for every $c \in \mathbb{V}_k^{(p)}$, let D_F^c be the preimage set of c. Then the following is equivalent.*

(i) F is a vectorial dual-bent function satisfying Condition $\mathcal{A}$, which is constant c_0 on an $(n/2)$-dimensional subspace U.

(ii) $\Gamma = \{U, D_F^{c_0} \setminus U, D_F^c : c \in \mathbb{V}_k^{(p)}, c \neq c_0\}$ is a normal bent partition with $\mathbb{F}_p^* D_F^c = D_F^c$, $c \in \mathbb{V}_k^{(p)}$, and $\mathbb{F}_p^*(D_F^{c_0} \setminus U) = D_F^{c_0} \setminus U$.

(iii) $\{D_F^{c_0} \setminus U, D_F^c : c \in \mathbb{V}_k^{(p)}, c \neq c_0\}$ is a $(p^{n/2}, p^{n/2-k})$ LP-packing in $\mathbb{V}_n^{(p)}$ relative to U with $\mathbb{F}_p^* D_F^c = D_F^c$, $c \in \mathbb{V}_k^{(p)}$, and $\mathbb{F}_p^*(D_F^{c_0} \setminus U) = D_F^{c_0} \setminus U$.

Proof. We first show the equivalence of (i) and (ii). By Proposition 10, the preimage set partition of F is a bent partition satisfying Condition $\mathcal{C}$. With $\mathbb{F}_p^* D_F^{c_0} = D_F^{c_0}$ and $\mathbb{F}_p^* U = U$, as U is a subspace, we also have $\mathbb{F}_p^*(D_F^{c_0} \setminus U) = D_F^{c_0} \setminus U$. With the assumption that F is constant on U, Γ given as in (ii) is a normal bent partition. The converse is immediate.

We now show that (i) implies (iii). By Proposition 11, for all $c \neq c_0$, D_F^c is a $(p^{n/2}, p^{n/2-k})$ Latin square type PDS, except for $D_F^{c_0}$, for which $D_F^{c_0} \setminus \{0\}$ is a $(p^{n/2}, p^{n/2-k}+1)$ Latin square type PDS. It remains to show that then $D_F^{c_0} \setminus U$ is a $(p^{n/2}, p^{n/2-k})$ Latin square type PDS. By Equation (1.14), for any non-trivial character χ of $\mathbb{V}_n^{(p)}$ and $c \in \mathbb{V}_k^{(p)}$, we have

$$\chi(D_F^c) = \{p^{n/2} - p^{n/2-k}, -p^{n/2-k}\}.$$

Recall that for any non-trivial character of χ of $\mathbb{V}_n^{(p)}$, we have $\sum_{c \in \mathbb{V}_k^{(p)}} \chi(D_F^c) = 0$. Hence, there exists a unique $\tilde{c} \in \mathbb{V}_k^{(p)}$ such that $\chi(D_F^{\tilde{c}}) = p^{n/2} - p^{n/2-k}$, and $\chi(D_F^c) = -p^{n/2-k}$ for all $c \in \mathbb{V}_k^{(p)} \setminus \{\tilde{c}\}$.

Let χ be a non-trivial character of $\mathbb{V}_n^{(p)}$ corresponding to $\alpha \in \mathbb{V}_n^{(p)}$, i.e., $\chi(x) = \zeta_p^{\langle \alpha, x \rangle_n}$. As U is a subspace of $\mathbb{V}_n^{(p)}$ of order $p^{n/2}$, we have $\chi(U) = 0$ or $\chi(U) = p^{n/2}$. Suppose that $\chi(U) = 0$. Then we have $\chi(D_F^{c_0} \setminus U) = \chi(D_F^{c_0}) - \chi(U) = \chi(D_F^{c_0})$, i.e.,

$\chi(D_F^{c_0} \setminus U) = p^{n/2} - p^{n/2-k}$ or $\chi(D_F^{c_0} \setminus U) = -p^{n/2-k}$.

We now suppose that $\chi(U) = p^{n/2}$. If $\chi(D_F^{c_0}) = p^{n/2} - p^{n/2-k}$, then similarly, $\chi(D_F^{c_0} \setminus U) = -p^{n/2-k}$. Hence, we need to observe that if $\chi(U) = p^{n/2}$ then $\chi(D_F^{c_0}) \neq -p^{n/2-k}$. Suppose that $\chi(U) = p^{n/2}$ and $\chi(D_F^{c_0}) = -p^{n/2-k}$, i.e., $\chi(D_F^{c_0} \setminus U) = -p^{n/2} - p^{n/2-k}$. Let $\tilde{c} \in \mathbb{V}_k^{(p)}$ be the unique element such that $\chi(D_F^{\tilde{c}}) = p^{n/2} - p^{n/2-k}$. With the ordering of $\mathbb{V}_k^{(p)} = \{c_0, c_1, \ldots, c_{p^k-1} = \tilde{c}\}$, we set $A_i = D_F^{c_i}$ for $i = 1, \ldots, p^k - 1$ and $A_0 = D_F^{c_0} \setminus U$. Then we consider the following partition of $\mathbb{V}_n^{(p)}$.

$$\mathcal{P} = \{\mathcal{A}_i, U : i = 0, \ldots, p-1\},$$

where $\mathcal{A}_i = \cup_{j=0}^{p^{k-1}-1} A_{j+ip^{k-1}}$. Note that we have

$$\begin{aligned} \chi(\mathcal{A}_0) &= -p^{n/2} - p^{n/2-1}, \\ \chi(\mathcal{A}_i) &= -p^{n/2-1} \text{ for } i = 1, \ldots, p-2, \\ \chi(\mathcal{A}_{p-1}) &= p^{n/2} - p^{n/2-1}. \end{aligned}$$

As $\Gamma = \{U, D_F^{c_0} \setminus U, D_F^c : c \in \mathbb{V}_k^{(p)}, c \neq c_0\}$ is a normal bent partition, we consider the bent function $f : \mathbb{V}_n^{(p)} \to \mathbb{F}_p$ defined by $f(x) = a_i$ for all $x \in \mathcal{A}_i$, where $\{a_i : i = 0, \ldots, p-1\} = \mathbb{F}_p$, and $f(x) = a$ for a fixed $a \in \mathbb{F}_p$ for all $x \in U$. Then

$$\begin{aligned} \mathcal{W}_f(\alpha) &= \sum_{i=0}^{p-1} \chi(\mathcal{A}_i)\zeta_p^{a_i} + p^{n/2}\zeta_p^a \\ &= -p^{n/2}\zeta_p^{a_0} + p^{n/2}\zeta_p^{a_{p-1}} + p^{n/2}\zeta_p^a \\ &= p^{n/2}(-\zeta_p^{a_0} + \zeta_p^{a_{p-1}} + \zeta_p^a), \end{aligned}$$

where $\zeta_p = e^{2\pi\iota/p} = \cos(2\pi/p) + \iota\sin(2\pi/p)$. Choosing $a_{p-1} = a = 0$ and $a_0 = 1$, we obtain $\mathcal{W}_f(\alpha) = p^{n/2}(2 - \zeta_p) = p^{n/2}(2 - \cos(2\pi/p) - \iota\sin(2\pi/p))$. Since $p > 2$, we have $|\cos(2\pi/p)| < 1$. That is, the real part $2 - \cos(2\pi/p) > 1$, implying that $|\mathcal{W}_f(\alpha)| > p^{n/2}$, which contradicts Γ being a bent partition. Then the fact that (iii) implies (ii) by Corollary 1 finishes the proof. □

For characteristic 2, which by Remark 9 is different, we have the following proposition.

Proposition 13. *For an even integer n and an integer $2 \leq k \leq n/2$, let F be a function from $\mathbb{V}_n^{(2)}$ to $\mathbb{V}_k^{(2)}$, and for every $c \in \mathbb{V}_k^{(2)}$, let D_F^c be the preimage set of c. Then the following is equivalent.*

(i) *F is a vectorial dual-bent function satisfying Condition $\mathcal{A}$, which is constant c_0 on an $(n/2)$-dimensional subspace U.*

(ii) *$\{D_F^{c_0} \setminus U, D_F^c : c \in \mathbb{V}_k^{(2)}, c \neq c_0\}$ is a $(2^{n/2}, 2^{n/2-k})$ LP-packing in $\mathbb{V}_n^{(2)}$ relative to U, i.e., $\Gamma = \{U, D_F^{c_0} \setminus U, D_F^c : c \in \mathbb{V}_k^{(2)}, c \neq c_0\}$ is a normal bent partition for which all sets are Latin square type PDSs.*

Proof. (i) $\Rightarrow$ (ii): By Proposition 10 and Remark 9, the preimage set partition of F is a bent partition $\{D_F^c : c \in \mathbb{V}_k^{(2)}\}$ of which all sets are Latin square type PDSs. Since F is constant on U, $\{U, D_F^{c_0} \setminus U, D_F^c : c \in \mathbb{V}_k^{(2)}, c \neq c_0\}$ is a normal bent partition. With D_F^c, $c \neq c_0$, also $D_F^{c_0} \setminus U$ is a Latin square type PDS, see Remark 9. Hence $\{D_F^{c_0} \setminus U, D_F^c : c \in \mathbb{V}_k^{(2)}, c \neq c_0\}$ is an LP-packing relative to U.
(ii) $\Rightarrow$ (i): If $\{U, D_F^{c_0} \setminus U, D_F^c : c \in \mathbb{V}_k^{(2)}, c \neq c_0\}$ is a normal bent partition of which all sets are Latin square type PDSs, then the union of U with any of the sets in the partition is a Latin square type PDS, see e.g. (Anbar et al., 2022, Theorem 4). In particular, also $D_F^{c_0}$ is a Latin square type PDS, hence F is a vectorial dual-bent function satisfying Condition $\mathcal{A}$, see Remark 9. □

4.1 Direct Sum Constructions

In this subsection, we analyze the generation of bent partitions, LP-packings, vectorial dual-bent functions with the direct sum construction. In (Jedwab & Li, 2021, Section 3), a construction of a new LP-packing from two given LP-packings is presented.

Proposition 14. *(Jedwab & Li, 2021, Theorem 3.15) For two even integers n and m, let $\mathcal{P}_1 = \{A_1, \ldots, A_{p^k}\}$ be a $(p^{n/2-k}, p^k)$ LP-packing in $\mathbb{V}_n^{(p)}$ relative to U_1, and $\mathcal{P}_2 = \{B_1, \ldots, B_{p^k}\}$ be a $(p^{m/2-k}, p^k)$ LP-packing in $\mathbb{V}_m^{(p)}$ relative to U_2. Then $\{K_1, \ldots, K_{p^k}\}$ with*

$$K_\ell = (A_\ell \times U_2) \cup (U_1 \times B_\ell) \cup \bigcup_{i=1}^{p^k} (A_i \times B_{i+\ell}) \tag{4.1}$$

for $\ell = 1, \ldots, p^k$, where the subscript $i + \ell$ is reduced modulo p^k, is a $(p^{\frac{m+n}{2}-k}, p^k)$ LP-packing in $\mathbb{V}_n^{(p)} \times \mathbb{V}_m^{(p)}$ relative to $U_1 \times U_2$.

As also indicated in (Jedwab & Li, 2021), Equation (4.1) gives one way of combining the sets A_i and B_j from $\mathcal{P}_1$ and $\mathcal{P}_2$ (note that the ordering of the sets in $\mathcal{P}_1$ and $\mathcal{P}_2$ is also arbitrary).

By Corollary 1, the LP-packing construction in Proposition 14 has an interpretation of a normal bent partition construction $\Gamma_1 \times \Gamma_2 = \{U_1 \times U_2, K_1, \ldots, K_{p^k}\}$ of $\mathbb{V}_n^{(p)} \times \mathbb{V}_m^{(p)}$ from normal bent partitions $\Gamma_1 = \{U_1, A_1, \ldots, A_{p^k}\}$ of $\mathbb{V}_n^{(p)}$ and $\Gamma_2 = \{U_2, B_1, \ldots, B_{p^k}\}$ of $\mathbb{V}_m^{(p)}$.

From a (normal) bent partition, we can construct vectorial bent functions by Theorem 12. Conversely, with Proposition 10, the preimage set partition of a vectorial dual-bent function satisfying Condition $\mathcal{A}$ is a bent partition (satisfying Condition $\mathcal{C}$).

Considering the above argument, we can relate the LP-packing construction in Proposition 14 with a construction of vectorial dual-bent functions. In this interpretation, the construction in (Jedwab & Li, 2021) corresponds to the well-known direct sum construction of a vectorial bent function $H(x,y) = F(x) + G(y)$ from two vectorial bent functions $F : \mathbb{V}_n^{(p)} \to \mathbb{V}_k^{(p)}$ and $G : \mathbb{V}_m^{(p)} \to \mathbb{V}_k^{(p)}$. As by Proposition 10, vectorial dual-bent functions induce bent partitions if they satisfy Condition $\mathcal{A}$. In the subsequent theorem, we assume that the involved vectorial bent functions are vectorial dual-bent satisfying Condition $\mathcal{A}$. The bent partitions then satisfy Condition $\mathcal{C}$. We state this version of the direct sum construction for both, bent partitions (which can be of Type I or of Type II) and normal bent partitions (or LP-packings). To simplify the notation, without loss of generality, the vectorial functions in this section map into the finite field $\mathbb{F}_{p^k}$.

Theorem 17. *Let n, m and k be positive integers with $k \le n/2$ and $k \le m/2$, and let p be a prime.*

(i) Let $F : \mathbb{V}_n^{(p)} \to \mathbb{F}_{p^k}$ and $G : \mathbb{V}_m^{(p)} \to \mathbb{F}_{p^k}$ be vectorial dual-bent functions satisfying Condition $\mathcal{A}$, and let $\Gamma_1 = \{A_i : i \in \mathbb{F}_{p^k}\}$ and $\Gamma_2 = \{B_i : i \in \mathbb{F}_{p^k}\}$ be the bent partitions of $\mathbb{V}_n^{(p)}$ and $\mathbb{V}_m^{(p)}$ satisfying Condition $\mathcal{C}$, obtained from F and G, that is, $F(x) = i$ if and only if $x \in A_i$, and $G(x) = i$ if and only if $x \in B_i$.

The preimage set partition $\{C_j : j \in \mathbb{F}_{p^k}\}$ with $C_j = \{(x,y) \in \mathbb{V}_n^{(p)} \times \mathbb{V}_m^{(p)} : H(x,y) = j\}$ of the vectorial bent function $H(x,y) = F(x) + G(y)$ is a bent partition satisfying Condition $\mathcal{C}$, and

$$C_j = H^{-1}(j) = \bigcup_{i \in \mathbb{F}_{p^k}} (A_i \times B_{j-i}), \tag{4.2}$$

where the indices are determined in $\mathbb{F}_{p^k}$.

(ii) Let $F : \mathbb{V}_n^{(p)} \to \mathbb{F}_{p^k}$ *and* $G : \mathbb{V}_m^{(p)} \to \mathbb{F}_{p^k}$ *be vectorial dual-bent functions satisfying Condition* $\mathcal{A}$*, and suppose that* $F(x) = \beta$ *if* $x \in U_1$ *and* $G(x) = \gamma$ *if* $x \in U_2$ *for an* $(n/2)$*-dimensional subspace of* $\mathbb{V}_n^{(p)}$ *and an* $(m/2)$*-dimensional subspace of* $\mathbb{V}_m^{(p)}$*. Let* $\Gamma_1 = \{U_1, A_i : i \in \mathbb{F}_{p^k}\}$ *and* $\Gamma_2 = \{U_2, B_i : i \in \mathbb{F}_{p^k}\}$ *be normal bent partitions of* $\mathbb{V}_n^{(p)}$ *and* $\mathbb{V}_m^{(p)}$ *obtained from* F *and* G*. Let* $H(x, y) = F(x) + G(y)$*. Then* H *is a vectorial dual-bent function satisfying Condition* $\mathcal{A}$*. Moreover, the partition* $\{U_1 \times U_2, C_j : j \in \mathbb{F}_{p^k}\}$*, with*

$$C_j = H^{-1}(j) = (A_{j-\gamma} \times U_2) \cup (U_1 \times B_{j-\beta}) \cup \bigcup_{i \in \mathbb{F}_{p^k}} (A_i \times B_{j-i}), \tag{4.3}$$

where the indices are determined in $\mathbb{F}_{p^k}$*, is a normal bent partition of* $\mathbb{V}_n^{(p)} \times \mathbb{V}_m^{(p)}$ *(satisfying Condition* $\mathcal{C}$*).*

Proof. (i) Since F and G are vectorial dual-bent functions satisfying Condition $\mathcal{A}$, for some vectorial duals F^* and G^* of F and G, and a nonzero $\gamma \in \mathbb{F}_{p^k}$, we have

$$\begin{aligned} \mathrm{Tr}_1^k(\gamma F(x))^* &= \mathrm{Tr}_1^k(\gamma F^*(x)), \quad \text{and} \\ \mathrm{Tr}_1^k(\gamma G(x))^* &= \mathrm{Tr}_1^k(\gamma G^*(x)). \end{aligned}$$

For nonzero $\gamma \in \mathbb{F}_{p^k}$, consider the component

$$\mathrm{Tr}_1^k(\gamma(F(x) + G(y))) = \mathrm{Tr}_1^k(\gamma F(x)) + \mathrm{Tr}_1^k(\gamma G(y)).$$

By the fact that $\mathcal{W}_{(F+G)_\gamma}(u, v) = \mathcal{W}_{F_\gamma}(u)\mathcal{W}_{G_\gamma}(v)$, we have

$$\begin{aligned} \mathrm{Tr}_1^k(\gamma(F(x) + G(y)))^* &= \mathrm{Tr}_1^k(\gamma F(x))^* + \mathrm{Tr}_1^k(\gamma G(y))^* \\ &= \mathrm{Tr}_1^k(\gamma F^*(x)) + \mathrm{Tr}_1^k(\gamma G^*(y)) \\ &= \mathrm{Tr}_1^k(\gamma(F^*(x) + G^*(y))). \end{aligned}$$

This shows that $F(x) + G(y)$ is vectorial dual-bent with vectorial dual $F^*(x) + G^*(y)$ and $((F(x) + G(y))_\gamma)^* = ((F(x) + G(y))^*)_\gamma$. Note that all components of $F(x) + G(y)$ are regular if all components of F and G are regular or all components of F and G are weakly regular but not regular. If all components of one of F and G are regular, and for the other function all components are weakly regular but not regular, then all components of $F(x) + G(y)$ are weakly regular but not regular. The function $F(x) + G(y)$ therefore satisfies Condition $\mathcal{A}$, and the preimage set partition of $F(x) + G(y)$

is a bent partition of $\mathbb{V}_n^{(p)} \times \mathbb{V}_m^{(p)}$ satisfying Condition $\mathcal{C}$.

The correctness of the sets in the preimage set partition of $F(x)+G(y)$ in (4.2) is confirmed straightforwardly.

(ii) With the same arguments as for (i) (using Proposition 10), we see that the preimage set partition of $F(x)+G(y)$ is a bent partition. Moreover, $F(x)+G(y)$ is constant on the $(\frac{n+m}{2})$-dimensional subspace $U_1 \times U_2$, by which a normal bent partition is provided. The sets in (4.3) are again obtained straightforwardly. □

Once given the bent partitions Γ_1 and Γ_2, with another choice of vectorial bent functions F and G from Γ_1 and Γ_2, in general, $F(x)+G(y)$ gives rise to another different bent partition of $\mathbb{V}_n^{(p)} \times \mathbb{V}_m^{(p)}$. In the following theorem we observe that for any p-ary bent functions f from the bent partition Γ_1 and g from Γ_2, there exist vectorial bent functions $\bar{F} : \mathbb{V}_n^{(p)} \to \mathbb{F}_{p^k}$ and $\bar{G} : \mathbb{V}_m^{(p)} \to \mathbb{F}_{p^k}$ obtained from Γ_1, respectively Γ_2, such that the direct sum $f(x)+g(y)$ is in the bent partition corresponding to $\bar{F}(x)+\bar{G}(y)$. On the other hand, quite remarkably, the bent partition derived from $F(x)+G(y)$ inherits (vectorial) bent functions which cannot be obtained as a direct sum of a bent function $\tilde{F}$ from Γ_1 and a bent function $\tilde{G}$ from Γ_2.

Theorem 18. *Let n, m and k be as above, and let $F : \mathbb{V}_n^{(p)} \to \mathbb{F}_{p^k}$, $G : \mathbb{V}_m^{(p)} \to \mathbb{F}_{p^k}$ be vectorial dual-bent functions satisfying Condition $\mathcal{A}$. Let Γ_1, Γ_2 be the corresponding (normal) bent partitions of $\mathbb{V}_n^{(p)}$ respectively of $\mathbb{V}_m^{(p)}$ of depth $p^k > 3$, and let Γ_H be the bent partition of $\mathbb{V}_n^{(p)} \times \mathbb{V}_m^{(p)}$ corresponding to the preimage set partition of $H(x,y) = F(x)+G(y)$. Then we have the following:*

(i) For any p-ary bent functions f respectively g from Γ_1 respectively Γ_2, there exist vectorial bent functions $\bar{F}$ and $\bar{G}$ from Γ_1 respectively Γ_2, such that $f(x)+g(y)$ is obtained from the bent partition of $\bar{F}(x)+\bar{G}(y)$.

(ii) With the bent partition Γ_H, one can generate vectorial bent functions, which cannot be obtained as the direct sum of a vectorial bent function from Γ_1 and a vectorial bent function from Γ_2.

(iii) With the bent partition Γ_H, one can generate p-ary bent functions, which cannot be obtained as the direct sum of a p-ary bent function from Γ_1 and a p-ary bent function from Γ_2.

Proof. (i) Let $\Gamma_1 = \{A_1, \ldots, A_{p^k}\}$, for $c \in \mathbb{F}_p$, let $f^{-1}(c) = A_{1,c} \cup \cdots \cup A_{p^{k-1},c}$, and let $\{\alpha \in \mathbb{F}_{p^k} : \mathrm{Tr}_1^k(\alpha) = c\} = \{\alpha_{1,c}, \ldots, \alpha_{p^{k-1},c}\} \subseteq \mathbb{F}_{p^k}$. We define $\bar{F} : \mathbb{V}_n^{(p)} \to \mathbb{F}_{p^k}$ by

$\bar{F}(x) = \alpha_{i,c}$ for all $x \in A_{i,c}$, $c \in \mathbb{F}_p$ and $i = 1, \ldots, p^{k-1}$. Then $\Gamma_1 = \Gamma_{\bar{F}} = \{\bar{F}^{-1}(\alpha) : \alpha \in \mathbb{F}_{p^k}\}$, and for $x \in A_{i,c}$, we have

$$\mathrm{Tr}_1^k(\bar{F}(x)) = \mathrm{Tr}_1^k(\alpha_{i,c}) = c,$$

i.e., $\mathrm{Tr}_1^k(\bar{F}(x)) = f(x)$ for all $x \in \mathbb{V}_n^{(p)}$. Similarly, we define $\bar{G} : \mathbb{V}_m^{(p)} \to \mathbb{F}_{p^k}$ such that $\Gamma_2 = \Gamma_{\bar{G}}$ and $\mathrm{Tr}_1^k(\bar{G}(x)) = g(x)$. Then $f(x)+g(y)$ is obtained from the bent partition of $\bar{F}(x)+\bar{G}(y)$.

(ii) Let $\Gamma_1 = \{A_i : i \in \mathbb{F}_{p^k}\}$ and $\Gamma_2 = \{B_i : i \in \mathbb{F}_{p^k}\}$ be such that $F^{-1}(i) = A_i$ and $G^{-1}(i) = B_i$ for all $i \in \mathbb{F}_{p^k}$, and let $H(x,y) = F(x)+G(y)$. Without loss of generality, we can suppose that $H(0,0) = 0$ as for any $c \in \mathbb{F}_{p^k}$, we have $\Gamma_H = \Gamma_{H+c}$. Set $H_i = H^{-1}(i)$, i.e.,

$$H_i = \bigcup_{j \in \mathbb{F}_{p^k}} A_j \times B_{i-j}, \tag{4.4}$$

where the indices are determined in $\mathbb{F}_{p^k}$. Let $\tilde{H}$ be a bent function from $\mathbb{V}_n^{(p)} \times \mathbb{V}_m^{(p)}$ to $\mathbb{F}_{p^k}$ obtained from Γ_H. Then we have $\tilde{H}(x,y) = \tau(i)$ for all $(x,y) \in H_i$ for a permutation τ of $\mathbb{F}_{p^k}$. Note that $\tilde{H}$ is obtained from Γ_H if and only if $\tilde{H}+c$ is obtained from Γ_H for any $c \in \mathbb{F}_{p^k}$. Moreover, $\tilde{H}$ can be obtained as a direct sum of functions derived from Γ_1 and Γ_2 if and only if for any $c \in \mathbb{F}_{p^k}$, $\tilde{H}+c$ can be obtained as a direct sum of functions derived from Γ_1 and Γ_2. Therefore, we can also assume that $\tau(0) = 0$.

Now suppose that $\tilde{H}(x,y) = \tilde{F}(x)+\tilde{G}(y)$ for some functions $\tilde{F}$, $\tilde{G}$ derived from Γ_1 and Γ_2, respectively. Let τ_1, τ_2 be the permutations of $\mathbb{F}_{p^k}$ for which

- $\tilde{F}$ is $\tau_1(i)$ on A_i and
- $\tilde{G}$ is $\tau_2(i)$ on B_i.

By Equation (4.4), for each $i \in \mathbb{F}_{p^k}$, we then have

$$\tau(i) = \tau_1(j)+\tau_2(i-j) \text{ for all } j \in \mathbb{F}_{p^k}. \tag{4.5}$$

In particular, for $j = 0$ and $i = j$,

$$\tau(i) = \tau_1(0)+\tau_2(i), \text{ and } \tau(i) = \tau_1(i)+\tau_2(0) \text{ for all } i \in \mathbb{F}_{p^k}.$$

Equivalently,

$$\tau_1(i) = \tau(i) - \tau_2(0), \text{ and } \tau_2(i) = \tau(i) - \tau_1(0) \text{ for all } i \in \mathbb{F}_{p^k}.$$

Hence by Equation (4.5), for all $i, j \in \mathbb{F}_{p^k}$, we have

$$\tau(i-j) = \tau(i) - \tau(j) + \tau_1(0) + \tau_2(0).$$

Considering $i = j = 0$, the assumption $\tau(0) = 0$ implies that $\tau_1(0) + \tau_2(0) = 0$. Therefore, for all $i, j \in \mathbb{F}_{p^k}$, we have

$$\tau(i-j) = \tau(i) - \tau(j). \tag{4.6}$$

Consequently, if $\tilde{H}$ is obtained as a direct sum of functions obtained from Γ_1 and Γ_2, then the permutation τ of $\mathbb{F}_{p^k}$ has to satisfy the linearity condition in Equation (4.6). For $p^k > 3$, we can find a permutation τ which does not satisfy Equation (4.6), and the desired assertion follows.

(iii) The proof is by contradiction. Suppose that any p-ary bent function h from Γ_H can be written as a direct sum of p-ary bent functions f and g from Γ_1 and Γ_2, respectively. Let $\tilde{H} : \mathbb{V}_n^{(p)} \times \mathbb{V}_m^{(p)} \to \mathbb{F}_{p^k}$ be a vectorial bent function from Γ_H. By (ii), we can assume that $\tilde{H}$ is not a direct sum $F(x) + G(y)$ for vectorial bent functions F and G from Γ_1 and Γ_2, respectively. Let $h_1(x,y), \ldots, h_k(x,y)$ be a basis of $\tilde{H}$. Then any nontrivial linear combination of $h_1(x,y), \ldots, h_k(x,y)$ is a bent function from $\mathbb{V}_n^{(p)} \times \mathbb{V}_m^{(p)}$ to $\mathbb{F}_p$. Note that h_i is a p-ary bent function obtained from Γ_H for all $i = 1, \ldots, k$. Then by our assumption, h_i can be written as $h_i(x,y) = f_i(x) + g_i(y)$ for some f_i from Γ_1 and g_i from Γ_2 for all $i = 1, \ldots, k$.

If $f_1(x), \ldots, f_k(x)$ are linearly dependent then we have $c_1 f_1(x) + \cdots + c_k f_k(x) = 0$ for some $c_i \in \mathbb{F}_p$ not all of them zero. In this case, we have

$$\begin{aligned} \tilde{h}(x,y) &= c_1 h_1(x,y) + \cdots + c_k h_k(x,y) \\ &= c_1 g_1(y) + \cdots + c_k g_k(y) \\ &= \tilde{g}(y), \end{aligned}$$

and for a nonzero $u \in \mathbb{V}_n^{(p)}$ and $v \in \mathbb{V}_m^{(p)}$, we have

$$\begin{aligned}\mathcal{W}_{\tilde{h}}(u,v) &= \sum_{(x,y)\in\mathbb{V}_n^{(p)}\times\mathbb{V}_m^{(p)}} \zeta_p^{\tilde{g}(y)-\langle u,x\rangle_n-\langle v,y\rangle_m} \\ &= \sum_{y\in\mathbb{V}_m^{(p)}} \zeta_p^{\tilde{g}(y)-\langle v,y\rangle_m} \sum_{x\in\mathbb{V}_n^{(p)}} \zeta_p^{-\langle u,x\rangle_n} \\ &= 0.\end{aligned}$$

Hence, $\tilde{h}$ is not a bent function from $\mathbb{V}_n^{(p)} \times \mathbb{V}_m^{(p)}$ to $\mathbb{F}_p$, which is a contradiction. We conclude that $f_1(x), \ldots, f_k(x)$ are linearly independent. Similarly, we observe that $g_1(x), \ldots, g_k(x)$ are linearly independent. This proves that f_i respectively g_i are the basis of a vectorial bent function F from Γ_1 respectively G from Γ_2. Observe that then $\tilde{H}$ is a direct sum of a vectorial bent function F from Γ_1 and a vectorial bent function G from Γ_2, which contradicts our assumption on $\tilde{H}$. □

Remark 10. *The permutations τ of $\mathbb{F}_{p^k}$ satisfying* (4.6) *are exactly the linear permutations. Under the assumption that $\tau(0) = 0$, with $i = 0$ we see that $\tau(-j) = -\tau(j)$. Then*

$$\tau(i+j) = \tau(i-(-j)) = \tau(i) - \tau(-j) = \tau(i) + \tau(j).$$

Corollary 3. *Let $F : \mathbb{V}_n^{(p)} \to \mathbb{F}_{p^k}$, $G : \mathbb{V}_m^{(p)} \to \mathbb{F}_{p^k}$ be vectorial dual-bent functions satisfying Condition A, and let Γ_1, Γ_2 be the corresponding bent partitions of $\mathbb{V}_n^{(p)}$ respectively $\mathbb{V}_m^{(p)}$ of depth $p^k > 3$. Further, let $H(x,y) = F(x) + G(y)$, and let Γ_H be the preimage set partition of H, which is a bent partition of $\mathbb{V}_n^{(p)} \times \mathbb{V}_m^{(p)}$ of depth p^k. A vectorial bent function $\tilde{H} : \mathbb{V}_n^{(p)} \times \mathbb{V}_m^{(p)} \to \mathbb{F}_{p^k}$ obtained from Γ_H can be written as a direct sum of some vectorial bent functions $\tilde{F}$, $\tilde{G}$ obtained from Γ_1 and Γ_2 respectively, if and only if $\tilde{H}(x,y) = \tau(H(x,y) - H(0,0))$ for an affine permutation τ of $\mathbb{F}_{p^k}$. In this case, H and $\tilde{H}$ are affine equivalent.*

Proof. Recall that $\Gamma_H = \Gamma_{H+c}$ for any $c \in \mathbb{F}_{p^k}$. Hence, by the proof of Theorem 18(ii), if $\tilde{H}$ is a bent function obtained from $\Gamma_{H+H(0,0)}$, then $\tilde{H}(x,y) = \tau(H(x,y) - H(0,0))$ for a permutation τ of $\mathbb{F}_{p^k}$ for which $\tau(x) - \tau(0)$ is linear, see Remark 10, i.e., τ is an affine permutation of $\mathbb{F}_{p^k}$.

Conversely, suppose that $\tilde{H}(x,y) = \tau(H(x,y) - H(0,0))$ for an affine permutation τ

of $\mathbb{F}_{p^k}$. Write $\tau(x) = \sigma(x) + \tau(0)$, that is, $\sigma(x)$ is the linear part of $\tau(x)$. Then

$$\begin{aligned}\tilde{H}(x,y) &= \tau(H(x,y) - H(0,0)) \\ &= \sigma(F(x)) - \sigma(F(0)) + \sigma(G(y)) - \sigma(G(0)) + \tau(0).\end{aligned}$$

Set $\tilde{F}(x) = \sigma(i) - \sigma(F(0))$ on A_i and $\tilde{G}(y) = \sigma(i) - \sigma(G(0)) + \tau(0)$ on B_i, i.e., $\tilde{F}$, $\tilde{G}$ are bent functions obtained from Γ_1 and Γ_2 respectively. Then $\tilde{H}(x,y) = \tilde{F}(x) + \tilde{G}(y)$ gives the desired conclusion. □

All so far known bent partitions are of Type I (except for the preimage set partitions of ternary bent functions). However, theoretically the direct sum construction can be applied to any pair of bent partitions related to vectorial dual-bent functions satisfying Condition $\mathcal{A}$. For two single weakly regular bent functions $f : \mathbb{V}_n^{(p)} \to \mathbb{F}_p$, $g : \mathbb{V}_m^{(p)} \to \mathbb{F}_p$, the direct sum $f(x) + g(y)$ is regular if both f, g are regular, or both f, g are weakly regular but not regular. Otherwise, $f(x) + g(y)$ is weakly regular but not regular. As it is easy to confirm, accordingly, Γ_H in Theorem 18 is of Type I if both Γ_1, Γ_2 are of Type I or both are of Type II. Otherwise, Γ_H is of Type II.

4.2 Generalizations of the Construction in (Wang et al., 2023)

PS_{ap} bent functions have the following vectorial version. For an s-dimensional vector space $\mathbb{V}_s^{(p)}$ (over $\mathbb{F}_p$) with $s \leq m$, let $B : \mathbb{F}_{p^m} \to \mathbb{V}_s^{(p)}$ be a balanced function with $B(0) = 0$. Then the function $F : \mathbb{F}_{p^m} \times \mathbb{F}_{p^m} \to \mathbb{V}_s^{(p)}$ given by $F(x,y) = B(xy^{p^m-2})$ is a vectorial PS_{ap} bent function. In (Wang et al., 2023), using the PS_{ap} bent functions, a secondary construction of vectorial bent functions is presented from a collection of vectorial bent functions satisfying Condition $\mathcal{A}$.

Proposition 15. *(Wang et al., 2023, Theorem 4) Let n, m and k be positive integers with n being even and $k \leq n/2$, and let $s < m$ be a positive divisor of m. For every $i \in \mathbb{F}_{p^s}$, let $F(i;x)$ be a vectorial dual-bent function from $\mathbb{V}_n^{(p)}$ to $\mathbb{F}_{p^s}$ satisfying Condition $\mathcal{A}$ and also the property that for any $c \in \mathbb{V}_k^{(p)} \backslash \{0\}$, the constant $\varepsilon_{F_{(i;x)_c}} \in \{-1, 1\}$ is the same independent of i, c.*

Suppose that $\alpha, \beta \in \mathbb{F}_{p^m}$ are linearly independent over $\mathbb{F}_{p^s}$. Let R be a permutation of $\mathbb{F}_{p^m}$ with $R(0) = 0$, and let $T : \mathbb{F}_{p^s} \to \mathbb{F}_{p^s}$ be an arbitrary function. Then the

function $H : \mathbb{V}_n^{(p)} \times \mathbb{F}_{p^m} \times \mathbb{F}_{p^m} \to \mathbb{F}_{p^s}$ *given by*

$$H(x,y,z) = F(\mathrm{Tr}_s^m(\alpha R(yz^{p^m-2})); x) + \mathrm{Tr}_s^m(\beta R(yz^{p^m-2})) + T(\mathrm{Tr}_s^m(\alpha R(yz^{p^m-2})))$$

is a vectorial dual-bent function satisfying Condition $\mathcal{A}$*.*

Observe that $\mathrm{Tr}_s^m(\gamma R(yz^{p^m-2}))$, $\gamma \in \mathbb{F}_{p^m}^*$, is a vectorial PS_{ap} bent function, hence it is itself a vectorial dual-bent function satisfying Condition $\mathcal{A}$. This motivates a generalization of the function H in Proposition 15 by replacing $\mathrm{Tr}_s^m(\alpha R(yz^{p^m-2}))$ and $\mathrm{Tr}_s^m(\beta R(yz^{p^m-2}))$ by appropriately chosen vectorial dual-bent functions satisfying Condition $\mathcal{A}$ corresponding to other bent partitions satisfying Condition $\mathcal{C}$.

Let $e(y) : \mathbb{V}_{2m}^{(p)} \to \mathbb{F}_{p^k}$ be a vectorial dual-bent function satisfying Condition $\mathcal{A}$, and hence its preimage set partition $\Gamma = \{A_1, \ldots, A_{p^k}\}$ is a bent partition of $\mathbb{V}_{2m}^{(p)}$ of depth p^k satisfying Condition $\mathcal{C}$. We denote by ε_Γ the sign of bent functions obtained from Γ, i.e., $\varepsilon_\Gamma = 1$ if every bent function obtained from Γ is regular (Type I), and $\varepsilon_\Gamma = -1$ if every bent function obtained from Γ is weakly regular but not regular (Type II). Let $s < k$ be a divisor of k, and let α, β be two elements of $\mathbb{F}_{p^k}$ that are linearly independent over $\mathbb{F}_{p^s}$. We set

$$\ell(y) = \mathrm{Tr}_s^k(\alpha e(y)) \text{ and } \ t(y) = \mathrm{Tr}_s^k(\beta e(y)).$$

Note that as $\alpha, \beta \in \mathbb{F}_{p^k}$ are linearly independent over $\mathbb{F}_{p^s}$, we have $\beta - j\alpha \neq 0$ for all $j \in \mathbb{F}_{p^s}$.

Lemma 9. *For any* $j \in \mathbb{F}_{p^s}$*, the function* $t(y) - j\ell(y)$ *is a bent function from* $\mathbb{V}_{2m}^{(p)}$ *to* $\mathbb{F}_{p^s}$ *obtained from* Γ *such that for* $b \in \mathbb{V}_{2m}^{(p)}$ *and nonzero* $c \in \mathbb{F}_{p^s}$*,*

$$\mathcal{W}_{(t-j\ell)_c}(b) = \varepsilon_\Gamma p^m \zeta_p^{e^*_{c(\beta-j\alpha)}(b)}, \tag{4.7}$$

where $e^*(y)$ *is the vectorial-dual of* $e(y)$ *satisfying Condition* $\mathcal{A}$*, i.e.,* $e_c^*(y) = (e_c)^*(y)$ *for all nonzero* $c \in \mathbb{F}_{p^k}$*.*

Proof. Note that $t(y) - j\ell(y) = \mathrm{Tr}_s^k((\beta - j\alpha)e(y))$. As $\beta - j\alpha \neq 0$, the function $t(y) - j\ell(y)$ is a bent function from $\mathbb{V}_{2m}^{(p)}$ to $\mathbb{F}_{p^s}$ obtained from Γ. For $b \in \mathbb{V}_{2m}^{(p)}$ and $c \in \mathbb{F}_{p^s}^*$,

we have the following equalities:

$$\begin{aligned}\mathcal{W}_{(t-j\ell)_c}(b) &= \sum_{y\in\mathbb{V}_{2m}^{(p)}} \zeta_p^{\mathrm{Tr}_1^s(c(t(y)-j\ell(y)))-<b,y>_{2m}} \\ &= \sum_{y\in\mathbb{V}_{2m}^{(p)}} \zeta_p^{\mathrm{Tr}_1^s(c\mathrm{Tr}_s^k((\beta-j\alpha)e(y)))-<b,y>_{2m}} \\ &= \sum_{y\in\mathbb{V}_{2m}^{(p)}} \zeta_p^{\mathrm{Tr}_1^k(c(\beta-j\alpha)e(y))-<b,y>_{2m}} \\ &= \mathcal{W}_{e_{c(\beta-j\alpha)}}(b).\end{aligned}$$

Then the result follows from the fact that $\beta - j\alpha \neq 0$ and that $e(y)$ is a vectorial dual-bent function satisfying Condition $\mathcal{A}$. □

We now define our function $H : \mathbb{V}_n^{(p)} \times \mathbb{V}_{2m}^{(p)} \to \mathbb{F}_{p^s}$ which generalizes the vectorial dual-bent function in Proposition 15.

Let n be an even integer, m, k be integers with $k \leq m \leq n/2$, and let s be a non-trivial divisor of k. As above, let $e : \mathbb{V}_{2m}^{(p)} \to \mathbb{F}_{p^k}$ be a vectorial dual-bent function satisfying Condition $\mathcal{A}$, and let $\alpha, \beta \in \mathbb{F}_{p^k}$ be linearly independent over $\mathbb{F}_{p^s}$. For vectorial dual-bent functions $F(i;x)$ from $\mathbb{V}_n^{(p)}$ to $\mathbb{F}_{p^s}$, $i \in \mathbb{F}_{p^s}$, and an arbitrary function $T : \mathbb{F}_{p^s} \to \mathbb{F}_{p^s}$, let

$$H(x,y) = F(\mathrm{Tr}_s^k(\alpha e(y)); x) + \mathrm{Tr}_s^k(\beta e(y)) + T(\mathrm{Tr}_s^k(\alpha e(y))). \tag{4.8}$$

Theorem 19. *For every $i \in \mathbb{F}_{p^s}$, let $F(i;x)$ be a vectorial dual-bent function from $\mathbb{V}_n^{(p)}$ to $\mathbb{F}_{p^s}$ satisfying Condition $\mathcal{A}$ and also the property that for any $c \in \mathbb{V}_k^{(p)} \backslash \{0\}$, the constant $\varepsilon_{F_{(i;x)_c}} \in \{-1, 1\}$ is the same independent of i, c. Then the function H defined by Equation 4.8 is a vectorial dual-bent function satisfying Condition $\mathcal{A}$.*

Proof. For any nonzero $c \in \mathbb{F}_{p^s}$ the corresponding component function is $H_c(x,y) =$

$\mathrm{Tr}_1^s(cH(x,y))$, so the Walsh transform of H_c at $(a,b) \in \mathbb{V}_n^{(p)} \times \mathbb{V}_{2m}^{(p)}$ is

$$\begin{aligned}
\mathcal{W}_{H_c}(a,b) &= \sum_{x\in\mathbb{V}_n^{(p)}, y\in\mathbb{V}_{2m}^{(p)}} \zeta_p^{\mathrm{Tr}_1^s(c(F(\ell(y);x)+t(y)+T(\ell(y))))-\langle a,x\rangle_n-\langle b,y\rangle_{2m}} \\
&= \sum_{i\in\mathbb{F}_{p^s}} \sum_{x\in\mathbb{V}_n^{(p)}} \sum_{y\in\mathbb{V}_{2m}^{(p)}:\ell(y)=i} \zeta_p^{\mathrm{Tr}_1^s(cF(i;x))+\mathrm{Tr}_1^s(ct(y))+\mathrm{Tr}_1^s(cT(i))-\langle a,x\rangle_n-\langle b,y\rangle_{2m}} \\
&= \sum_{i\in\mathbb{F}_{p^s}} \zeta_p^{\mathrm{Tr}_1^s(cT(i))} \sum_{x\in\mathbb{V}_n^{(p)}} \zeta_p^{\mathrm{Tr}_1^s(cF(i;x))-\langle a,x\rangle_n} \sum_{y\in\mathbb{V}_{2m}^{(p)}:\ell(y)=i} \zeta_p^{\mathrm{Tr}_1^s(ct(y))-\langle b,y\rangle_{2m}} \\
&= p^{-s} \sum_{i\in\mathbb{F}_{p^s}} \zeta_p^{\mathrm{Tr}_1^s(cT(i))} \mathcal{W}_{F(i;x)_c}(a) \sum_{y\in\mathbb{V}_{2m}^{(p)}} \zeta_p^{\mathrm{Tr}_1^s(ct(y))-\langle b,y\rangle_{2m}} \sum_{j\in\mathbb{F}_{p^s}} \zeta_p^{\mathrm{Tr}_1^s(cj(i-\ell(y)))} \\
&= p^{-s} \sum_{i\in\mathbb{F}_{p^s}} \zeta_p^{\mathrm{Tr}_1^s(cT(i))} \mathcal{W}_{F(i;x)_c}(a) \sum_{j\in\mathbb{F}_{p^s}} \zeta_p^{\mathrm{Tr}_1^s(cij)} \sum_{y\in\mathbb{V}_{2m}^{(p)}} \zeta_p^{\mathrm{Tr}_1^s(c(t(y)-j\ell(y)))-\langle b,y\rangle_{2m}} \\
&= p^{-s} \sum_{i\in\mathbb{F}_{p^s}} \zeta_p^{\mathrm{Tr}_1^s(cT(i))} \mathcal{W}_{F(i;x)_c}(a) \sum_{j\in\mathbb{F}_{p^s}} \zeta_p^{\mathrm{Tr}_1^s(cij)} \mathcal{W}_{(t-j\ell)_c}(b).
\end{aligned}$$

Then using Equation 4.7, we obtain the following equalities.

$$\begin{aligned}
\mathcal{W}_{H_c}(a,b) &= \varepsilon_\Gamma p^{m-s} \sum_{i\in\mathbb{F}_{p^s}} \zeta_p^{\mathrm{Tr}_1^s(cT(i))} \mathcal{W}_{F(i;x)_c}(a) \sum_{j\in\mathbb{F}_{p^s}} \zeta_p^{\mathrm{Tr}_1^s(cij)} \zeta_p^{e^*_{c(\beta-j\alpha)}(b)} \\
&= \varepsilon_\Gamma p^{m-s} \sum_{i\in\mathbb{F}_{p^s}} \zeta_p^{\mathrm{Tr}_1^s(cT(i))} \mathcal{W}_{F(i;x)_c}(a) \sum_{j\in\mathbb{F}_{p^s}} \zeta_p^{\mathrm{Tr}_1^s(cij)} \zeta_p^{\mathrm{Tr}_1^k(c(\beta-j\alpha)e^*(b))} \\
&= \varepsilon_\Gamma p^{m-s} \sum_{i\in\mathbb{F}_{p^s}} \zeta_p^{\mathrm{Tr}_1^s(cT(i))} \mathcal{W}_{F(i;x)_c}(a) \sum_{j\in\mathbb{F}_{p^s}} \zeta_p^{\mathrm{Tr}_1^s(cij)} \zeta_p^{\mathrm{Tr}_1^s(c\mathrm{Tr}_s^k((\beta-j\alpha)e^*(b)))} \\
&= \varepsilon_\Gamma p^{m-s} \zeta_p^{\mathrm{Tr}_1^s(c\mathrm{Tr}_s^k(\beta e^*(b)))} \sum_{i\in\mathbb{F}_{p^s}} \zeta_p^{\mathrm{Tr}_1^s(cT(i))} \mathcal{W}_{F(i;x)_c}(a) \sum_{j\in\mathbb{F}_{p^s}} \zeta_p^{\mathrm{Tr}_1^s(cj(i-\mathrm{Tr}_s^k(\alpha e^*(b))))} \\
&= \varepsilon_\Gamma p^{m} \zeta_p^{\mathrm{Tr}_1^s(c\mathrm{Tr}_s^k(\beta e^*(b)))} \zeta_p^{\mathrm{Tr}_1^s(cT(\mathrm{Tr}_s^k(\alpha e^*(b))))} \mathcal{W}_{F(\mathrm{Tr}_s^k(\alpha e^*(b));x)_c}(a) \\
&= \varepsilon\varepsilon_\Gamma p^{m+\frac{n}{2}} \zeta_p^{\mathrm{Tr}_1^s(c\mathrm{Tr}_s^k(\beta e^*(b)))} \zeta_p^{\mathrm{Tr}_1^s(cT(\mathrm{Tr}_s^k(\alpha e^*(b))))} \zeta_p^{(F(\mathrm{Tr}_s^k(\alpha e^*(b));x)_c)^*(a)} \\
&= \varepsilon\varepsilon_\Gamma p^{m+\frac{n}{2}} \zeta_p^{\mathrm{Tr}_1^s(c\mathrm{Tr}_s^k(\beta e^*(b)))} \zeta_p^{\mathrm{Tr}_1^s(cT(\mathrm{Tr}_s^k(\alpha e^*(b))))} \zeta_p^{F^*(\mathrm{Tr}_s^k(\alpha e^*(b));x)_c(a)} \\
&= \varepsilon\varepsilon_\Gamma p^{m+\frac{n}{2}} \zeta_p^{\mathrm{Tr}_1^s(c(F^*(\mathrm{Tr}_s^k(\alpha e^*(b));x)(a)+\mathrm{Tr}_s^k(\beta e^*(b))+T(\mathrm{Tr}_s^k(\alpha e^*(b)))))},
\end{aligned}$$

where ε is the sign of $F(i;x)$ for all $i \in \mathbb{F}_{p^s}$. Note that we used the property that $(F(\mathrm{Tr}_s^k(\alpha e^*(b));x)_c)^* = F^*(\mathrm{Tr}_s^k(\alpha e^*(b));x)_c$ in the second last equality. Therefore, $H(x,y)$ is a vectorial dual-bent function for which all components have the sign $\varepsilon\varepsilon_\Gamma$, and such that

$$H^*(x,y) = F^*(\mathrm{Tr}_s^k(\alpha e^*(y));x) + \mathrm{Tr}_s^k(\beta e^*(y)) + T(\mathrm{Tr}_s^k(\alpha e^*(y)))$$

and $H_c^* = (H_c)^*$. □

Corollary 4. *Let $H : \mathbb{V}_n^{(p)} \times \mathbb{V}_{2m}^{(p)} \to \mathbb{F}_{p^s}$ be the function in Equation* (4.8)*, for $\gamma \in \mathbb{F}_{p^s}$, let $D_H^\gamma = \{(x,y) \in \mathbb{V}_n^{(p)} \times \mathbb{V}_{2m}^{(p)} : H(x,y) = \gamma\}$, and let $\Gamma_H = \{D_H^\gamma : \gamma \in \mathbb{F}_{p^s}\}$ be the preimage set partition of H.*

(i) Γ_H is a bent partition satisfying Condition $\mathcal{C}$.

(ii) Let $e : \mathbb{V}_{2m}^{(p)} \to \mathbb{F}_{p^k}$ in Equation (4.8) *be obtained from a normal bent partition, i.e., e is constant $\tilde{i}$ on an m-dimensional subspace W of $\mathbb{V}_{2m}^{(p)}$. If $F(\mathrm{Tr}_s^k(\alpha\tilde{i}); x)$ is a vectorial dual-bent function from a normal bent partition of $\mathbb{V}_n^{(p)}$, then Γ_H provides a normal bent partition, respectively a $(p^{n/2+m}, p^{n/2+m-s})$ LP-packing in $\mathbb{V}_n^{(p)} \times \mathbb{V}_{2m}^{(p)}$.*

Proof. (i) Follows immediately from Theorem 19 and Proposition 10.

(ii) By assumption, $e(y) = \tilde{i}$ if $y \in W$ and $F(\mathrm{Tr}_s^k(\alpha\tilde{i}); x) = \gamma_1$ for all x in some $(n/2)$-dimensional subspace V of $\mathbb{V}_n^{(p)}$. Then for $(x,y) \in V \times W$, we have

$$H(x,y) = F(\mathrm{Tr}_s^k(\alpha\tilde{i}); x) + \mathrm{Tr}_s^k(\beta\tilde{i}) + T(\mathrm{Tr}_s^k(\alpha\tilde{i})) = \gamma_1 + \mathrm{Tr}_s^k(\beta\tilde{i}) + T(\mathrm{Tr}_s^k(\alpha\tilde{i})) = \tilde{\gamma}.$$

Then by Proposition 12(ii), $\tilde{\Gamma}_H = \{V \times W, D_H^{\tilde{\gamma}} \setminus \{V \times W\}, D_H^\gamma : \gamma \neq \tilde{\gamma}\}$ is a normal bent partition of $\mathbb{V}_n^{(p)} \times \mathbb{V}_{2m}^{(p)}$. By Proposition 12(iii), $\tilde{\Gamma}_H$ induces a $(p^{n/2+m-s}, p^s)$ LP-packing in $\mathbb{V}_n^{(p)} \times \mathbb{V}_{2m}^{(p)}$ relative to $V \times W$.

Example 8. *Using for $e : \mathbb{F}_{p^m} \times \mathbb{F}_{p^m} \to \mathbb{F}_{p^k}$ the generalized PS_{ap} functions given in Example* 5*, we obtain vectorial dual-bent functions H_1, H_2 of the form*

$$\begin{aligned} H_1(x, y_1, y_2) = {} & F(\mathrm{Tr}_s^k(\alpha R(\mathrm{Tr}_k^m(y_2 y_1^{-e}))); x) \\ & + \mathrm{Tr}_s^k(\beta R(\mathrm{Tr}_k^m(y_2 y_1^{-e}))) + T(\mathrm{Tr}_s^k(\alpha R(\mathrm{Tr}_k^m(y_2 y_1^{-e})))) \end{aligned}$$

and

$$\begin{aligned} H_2(x, y_1, y_2) = {} & F(\mathrm{Tr}_s^k(\alpha R(\mathrm{Tr}_k^m(y_1 y_2^{-d}))); x) \\ & + \mathrm{Tr}_s^k(\beta R(\mathrm{Tr}_k^m(y_1 y_2^{-d}))) + T(\mathrm{Tr}_s^k(\alpha R(\mathrm{Tr}_k^m(y_1 y_2^{-d})))). \end{aligned}$$

We remark that determining the vectorial dual H_1^* of H_1, for which $(H_{1c})^* = (H_1^*)_c$,

one obtains

$$H_1^*(x,y_1,y_2) = F^*(\mathrm{Tr}_s^k(\alpha R(-\mathrm{Tr}_k^m(y_1 y_2^{-d})^p)); x) + \mathrm{Tr}_s^k(\beta R(-\mathrm{Tr}_k^m(y_1 y_2^{-d})^p)) \\ + T(\mathrm{Tr}_s^k(\alpha R(-\mathrm{Tr}_k^m(y_1 y_2^{-d})^p))).$$

BIBLIOGRAPHY

Anbar, N., Kalaycı, T., & Meidl, W. (2022). Bent partitions and partial difference sets. *IEEE Trans. Inform. Theory*, *68*(10), 6894–6903.

Anbar, N., Kalaycı, T., & Meidl, W. (2023). Generalized semified spreads. *Designs, Codes and Cryptography*, *91*, 545–562.

Anbar, N. & Meidl, W. (2022). Bent partitions. *Designs, Codes and Cryptography*, *90*(4), 1081–1101.

Canteaut, A., Daum, M., Dobbertin, H., & Leander, G. (2006). Finding nonnormal bent functions. *Discrete Applied Mathematics*, *154*(2), 202–218.

Carlet, C. (1994). Two new classes of bent functions. *Advances in Cryptology - EUROCRYPT 93*, *765*, 77–101.

Çeşmelioğlu, A., McGuire, G., & Meidl, W. (2012). A construction of weakly and non-weakly regular bent functions. *J. Combin. Theory, Ser. A*, *119*(2), 420–429.

Çeşmelioğlu, A. & Meidl, W. (2013). A construction of bent functions from plateaued functions. *Designs, Codes and Cryptography*, *66*, 231–242.

Çeşmelioğlu, A., Meidl, W., & Pott, A. (2013a). Generalized maiorana-mcfarland class and normality of p-ary bent functions. *Finite Fields Appl.*, *24*, 105–117.

Çeşmelioğlu, A., Meidl, W., & Pott, A. (2013b). On the dual of (non)-weakly regular bent functions and self-dual bent functions. *Advances in Mathematics of Communications*, *7*(4), 425–440.

Çeşmelioğlu, A., Meidl, W., & Pott, A. (2013c). On the normality of p-ary bent functions. *Pre-proceedings of the International Workshop on Coding and Cryptography*.

Çeşmelioğlu, A., Meidl, W., & Pott, A. (2018). Vectorial bent functions and their duals. *Linear Algebra Appl.*, *548*, 305–320.

Charpin, P. (2004). Normal boolean functions. *Journal of Complexity*, *20*(2-3), 245–265.

Coulter, R. & Matthews, R. (1997). Planar functions and planes of lenz-barlotti class ii. *Designs, Codes and Cryptography*, *10*, 167–184.

Dobbertin, H. (1994). Construction of bent functions and balanced boolean functions with high nonlinearity. *Fast Software Encryption, Lecture Notes in Computer Science*, *1008*, 61–74.

Gold, R. (1968). Maximal recursive sequences with 3-valued recursive cross-correlation functions. *IEEE Trans. Inform. Theory*, *14*(1), 154–156.

Helleseth, T. & Kholosha, A. (2006). Monomial and quadratic bent functions over the finite fields of odd characteristic. *IEEE Trans. Inform. Theory*, *52*(5), 2018–2032.

Helleseth, T. & Kholosha, A. (2010). New binomial bent functions over the finite fields of odd characteristic. *IEEE Trans. Inform. Theory*, *56*(9), 4646–4652.

Jedwab, J. & Li, S. (2021). Packings of partial difference sets. *Comb. Theory*, *1*(18).

Kumar, P., Scholtz, R., & Welch, L. (1985). Generalized bent functions and their properties. *J. Combin. Theory Ser. A*, *40*(1), 90–107.

Leander, G. & McGuire, G. (2009). Construction of bent functions from near-bent functions. *J. Combin. Theory Ser. A*, *116*(4), 960–970.

Lidl, R. & Niederreiter, H. (1997). *Finite Fields, 2nd edn.* Cambridge: Cambridge University Press.

Ma, S. (1994). A survey of partial difference sets. *Designs, Codes and Cryptography*, *4*, 221–261.

Meidl, W. (2016). Generalized rothaus construction and non-weakly regular bent functions. *J. Combin. Theory Ser. A*, *141*, 78–89.

Meidl, W. & Pirsic, I. (2018). On the normality of p-ary bent functions. *Cryptography and Communications*, *10*, 1037–1049.

Meidl, W. & Pirsic, I. (2021). Bent and $_{2^k}$-bent functions from spread-like partitions. *Designs, Codes and Cryptography*, *89*, 75–89.

Nyberg, K. (1991a). Construction of bent functions and difference sets. *Advances in cryptology–EUROCRYPT'90*, *473*, 151–160.

Nyberg, K. (1991b). Perfect nonlinear s-boxes. *Advances in cryptology–EUROCRYPT'91*, *547*, 378–386.

Polujan, A., Mariot, L., & Picek, S. (2025). On two open problems on the normality of bent functions. *Discrete Applied Mathematics*, *360*, 115–118.

Potapov, V. (2016). On minimal distance between q-ary bent functions. *Problems of redundancy in information and control systems, IEEE*, 115–116.

Rothaus, O. (1976). On "bent" functions. *J. Combin. Theory Ser. A*, *20*, 300–305.

Serre, J. (1973). *A course in arithmetic.* Springer-Verlag.

Stichtenoth, H. (2009). *Algebraic Function Fields and Codes.* Berlin, Germany: Springer-Verlag.

Tan, Y., Pott, A., & Feng, T. (2010). Strongly regular graphs associated with ternary bent functions. *J. Combin. Theory Ser. A*, *117*(6), 668–682.

Wang, J., Fu, F., & Wei, Y. (2023). Bent partitions, vectorial dual-bent functions and partial difference sets. *IEEE Trans. Inf. Theory*, *69*(11).

Wang, J., Fu, F., & Wei, Y. (2024). A further study of vectorial dual-bent functions. *IEEE Trans. Inf. Theory*, *70*(10), 7472–7483.