Characterization of basic 5-value spectrum functions through Walsh-Hadamard transform

Hodzic, Samir; Horak, Peter; Pasalic, Enes

Published in:
IEEE Transactions on Information Theory

Link to article, DOI:
10.1109/TIT.2020.3044059

Publication date:
2021

Document Version
Publisher's PDF, also known as Version of record

Citation (APA):
Hodzic, S., Horak, P., & Pasalic, E. (2021). Characterization of basic 5-value spectrum functions through Walsh-Hadamard transform. *IEEE Transactions on Information Theory*, *67*(2), 1038 - 1053.
https://doi.org/10.1109/TIT.2020.3044059

Characterization of basic 5-value spectrum functions through Walsh-Hadamard transform

Samir Hodžić, Peter Horak, Enes Pasalic

***Abstract*—The first and the third authors recently introduced a spectral construction of plateaued and of 5-value spectrum functions. In particular, the design of the latter class requires a specification of integers $\{W(u) : u \in \mathbb{F}_2^n\}$, where $W(u) \in \{0, \pm 2^{\frac{n+s_1}{2}}, \pm 2^{\frac{n+s_2}{2}}\}$, so that the sequence $\{W(u) : u \in \mathbb{F}_2^n\}$ is a valid spectrum of a Boolean function (recovered using the inverse Walsh transform). Technically, this is done by allocating a suitable Walsh support $S = S^{[1]} \cup S^{[2]} \subset \mathbb{F}_2^n$, where $S^{[i]}$ corresponds to those $u \in \mathbb{F}_2^n$ for which $W(u) = \pm 2^{\frac{n+s_i}{2}}$. In addition, two *dual* functions $g_{[i]} : S^{[i]} \to \mathbb{F}_2$ (with $\#S^{[i]} = 2^{\lambda_i}$) are employed to specify the signs through $W(u) = 2^{\frac{n+s_i}{2}}(-1)^{g_{[i]}(u)}$ for $u \in S^{[i]}$ whereas $W(u) = 0$ for $u \notin S$.**

In this work, two closely related problems are considered. Firstly, the specification of plateaued functions (duals) $g_{[i]}$, which additionally satisfy the so-called totally disjoint spectra property, is fully characterized (so that $W(u)$ is a spectrum of a Boolean function) when the Walsh support S is given as a union of two disjoint affine subspaces $S^{[i]}$. Especially, when plateaued dual functions $g_{[i]}$ themselves have affine Walsh supports, an efficient spectral design that utilizes arbitrary bent functions (as duals of $g_{[i]}$) on the corresponding ambient spaces is given. The problem of specifying affine inequivalent 5-value spectra functions is also addressed and an efficient construction method that ensures the inequivalence property is derived (sufficient condition being a selection of affine inequivalent duals). In the second part of this work, we investigate duals of plateaued functions with affine Walsh supports. For a given such plateaued function, we show that different orderings of its Walsh support which are employing the Sylvester-Hadamard recursion actually induce bent duals which are affine equivalent.

***Index Terms*—Bent functions, Plateaued functions, 5-value spectrum functions, Lexicographic ordering, Spectral construction methods**

I. Introduction

There are several classes of Boolean functions that are of special interest for cryptographic applications. Bent functions, introduced by Rothaus [20], have several nice combinatorial properties allowing for a wide range of their applications such as design theory, coding theory, sequences, cryptography. In terms of the Walsh-Hadamard transform (see relation (1) in Section II), the range of W_f of an n-variable bent function f is the set $\{\pm 2^{n/2}\}$. An exhaustive survey on bent functions related to their design and properties can be found in [7]. Another well-studied class of Boolean functions $f : \mathbb{F}_2^n \to \mathbb{F}_2$ having the range of their WHT equal to $\{0, \pm 2^r\}$ (for $r > \lceil n/2 \rceil$) is known as plateaued functions [29]. Their various design methods have been addressed in several papers [6], [8], [10], [17], [18], [26], [27]. Due to their simple characterization in the spectral domain an alternative design approach was proposed recently in [13], [14].

Similarly, the class of Boolean functions with Walsh-Hadamard spectral values in the set $\{0, \pm 2^{\lambda_1}, \pm 2^{\lambda_2}\}$ (where $\lceil \frac{n}{2} \rceil \le \lambda_1 < \lambda_2 < n$) deserves a special interest as well. For instance, the only known APN permutation over $GF(2)^6$ (up to equivalence), provided by Dillon [11], has a 5-value extended Walsh-Hadamard spectrum (the spectra of all component functions) with the values $\{0, \pm 2^{\frac{n}{2}}, \pm 2^{\frac{n+2}{2}}\}$, for $n = 6$. Traditional design methods of 5-value spectrum functions can be traced to the early work of Maitra and Sarkar [16] and some recent papers [3], [18], [25]. Whereas these methods commonly define 5-value spectrum functions in the algebraic normal form (ANF) domain, there is a possibility of specifying these functions directly in the spectral domain by using a suitable Walsh-Hadamard support (subset of $GF(2)^n$ for which the Walsh-Hadamard spectral values are nonzero) and determining the sign distribution. This approach has been recently taken in [15], for the first time transferring the design problem completely into the spectral domain. The main idea elaborated in [15] is to relate the spectral values $\pm 2^{\lambda_1}$ to one dual function, whereas the values $\pm 2^{\lambda_2}$ then specify another dual function. A suitable choice of these duals (specifying the signs of spectral values) then provides a valid 5-value spectrum of a Boolean function. Here, dual functions refer to functions defined on smaller variable spaces which regulate the signs of values 2^{λ_i}, $i = 1, 2$ (cf. Section III). The key concept relevant to this design is the notion of totally disjoint spectra functions introduced in [15], where also a construction of these functions (using two bent functions) was elaborated for even n.

In this article, we extend the analysis initiated in [15] towards a better understanding of the structure and design of 5-value spectrum functions. In the first part of this work (Sections III and IV), we will derive a characterization of *basic* 5-value spectrum functions (for these Walsh-Hadamard support is a union of two affine subspaces) whose duals are totally disjoint spectra functions (Theorems IV.2 and IV.3). This characterization, referring to Theorem IV.2, encompasses both so-called basic and non-basic plateaued duals. The term

S. Hodžić is with the Technical University of Denmark, DTU Compute, Denmark, e-mail: saho@dtu.dk

P. Horak is with the University of Washington, Tacoma, USA, e-mail: horak@uw.edu

E. Pasalic is with the University of Primorska, FAMNIT & IAM, Koper, Slovenia, e-mail: enes.pasalic6@gmail.com

Samir Hodžić is supported by a grant from the Independent Research Fund Denmark for Technology and Production, grant no. 8022-00348A. Enes Pasalic is partly supported by the Slovenian Research Agency (research program P1-0404 and research projects J1-9108, J1-1694), and the European Commission for funding the InnoRenew CoE project (Grant Agreement no. 739574) under the Horizon2020 Widespread-Teaming program and the Republic of Slovenia (Investment funding of the Republic of Slovenia and the European Union of the European regional Development Fund). All three authors are supported in part by Slovenian Research Agency, bilateral project between Slovenia and USA BI-US/18-20-025.

Communicated by A. Canteaut, Associate Editor for Cryptography.

basic here is used to distinguish the special case when Walsh-Hadamard supports of plateaued duals are strictly affine/linear subspaces, whereas other choices of these supports are called non-basic. We note that basic plateaued functions in [4] correspond to partially bent functions, while in [14] they are called trivial plateaued functions.

Moreover, considering the design of basic 5-value spectra functions, we provide an efficient and general construction method (Proposition IV.2) which utilizes the spectral construction method introduced in [13]. It is worth noticing that this method addresses any parity of n compared to the approach taken in [15] which only covers even n. For basic 5-value spectrum functions, we show that the two associated dual functions are necessarily plateaued.

To construct extended affine (EA) inequivalent basic 5-value spectra functions, we demonstrate that it is sufficient to employ affine inequivalent duals, which is addressed in Section IV-D. As we consider plateaued duals with affine Walsh supports, then using the results in [14] this inequivalence is achieved by simply employing inequivalent bent functions as duals of these plateaued functions. This relatively simple result has important consequences for the classification of these objects and most notably it relates the subclass of basic 5-value spectrum functions to affine equivalence classes of bent functions defined on smaller variable spaces.

In the second part of this work (Section V), we investigate the equivalence of duals which are obtained by imposing different orderings (in terms of Lemma III.1-(i)) on the affine/linear Walsh-Hadamard support (say) S_g of a given basic plateaued function g. Note that this has been left as an open problem in [13], [14]. It is shown that representing S_g differently either as $S_g = v_1 \oplus E = \{\tilde{\omega}_0, \ldots, \tilde{\omega}_{2^k-1}\}$ or as $S_g = v_2 \oplus E = \{\hat{\omega}_0, \ldots, \hat{\omega}_{2^k-1}\}$, with $v_1 \neq v_2$ ($v_1, v_2 \in S_g$) and a linear subspace E being ordered in terms of Lemma III.1-(i), results in affine equivalent duals of the same underlying plateaued function g (Theorem V.2).

The existence of 5-value spectrum functions whose sizes of supports, denoted by $S^{[i]}$ ($i = 1, 2$), are not a power of two, as well as those whose duals $g_{[i]}$ are not basic plateaued functions, remains to be answered. In the case when $\#S^{[i]}$ are not a power of two, it seems that there is no possibility to perform the analysis based on dual functions (considered as Boolean functions on smaller variables spaces). Furthermore, the question whether there are suitable cardinalities of $S^{[i]}$, satisfying the condition of Proposition III.3-(ii) and additionally fulfilling the design requirements imposed by the relationship in Proposition III.1, is of particular importance.

The rest of this paper is organized as follows. In Section II, we give some basic definitions related to Boolean functions and discuss the concept of dual of plateaued Boolean functions. The spectral design method for this class of functions is elaborated in Section III, where a general specification of the cardinalities of Walsh-Hadamard supports $S^{[i]}$ along with the value distribution of related exponential sums is given, cf. Proposition III.3. In Section IV, we give an efficient and general design method for basic 5-value spectrum functions. In addition, we analyse their mutual EA-equivalence and discuss briefly the notion of linear structures. A detailed study of different orderings imposed on the used affine subspaces in terms of [15, Lemma 3.1], is given in Section V. Concluding remarks are given in Section VI.

II. Preliminaries

By $\mathbb{F}_2^n$ we denote the vector space of all n-tuples $x = (x_1, \ldots, x_n)$, where $x_i \in \mathbb{F}_2$. For $x = (x_1, \ldots, x_n)$ and $y = (y_1, \ldots, y_n)$ in $\mathbb{F}_2^n$, the usual scalar (or dot) product over $\mathbb{F}_2$ is defined as $x \cdot y = x_1 y_1 \oplus \cdots \oplus x_n y_n$. By $\mathbf{0}_n$ we denote the all-zero vector with n coordinates, that is $(0, 0, \ldots, 0) \in \mathbb{F}_2^n$. By "$\sum$" we denote the integer sum (without modulo evaluation), whereas "$\bigoplus$" denotes the sum evaluated modulo two.

The set of all Boolean functions in n variables, which is the set of mappings from $\mathbb{F}_2^n$ to $\mathbb{F}_2$, is denoted by $\mathcal{B}_n$. The set of affine functions in n variables is given by $\mathcal{A}_n = \{a \cdot x \oplus b : a \in \mathbb{F}_2^n,\ b \in \{0, 1\}\}$, and similarly $\mathcal{L}_n = \{a \cdot x : a \in \mathbb{F}_2^n\} \subset \mathcal{A}_n$ denotes the set of linear functions. It is well-known that any $f : \mathbb{F}_2^n \to \mathbb{F}_2$ can be uniquely represented by its associated algebraic normal form (ANF) as follows:

$$f(x_1, \ldots, x_n) = \bigoplus_{u \in \mathbb{F}_2^n} \lambda_u \Big(\prod_{i=1}^{n} {x_i}^{u_i}\Big),$$

where $x_i, \lambda_u \in \mathbb{F}_2$ and $u = (u_1, \ldots, u_n) \in \mathbb{F}_2^n$. The corresponding (± 1)-*sequence of* $f : \mathbb{F}_2^n \to \mathbb{F}_2$ is defined as

$$\chi_f = ((-1)^{f(0,\ldots,0,0)}, (-1)^{f(0,\ldots,0,1)}, \ldots, (-1)^{f(1,\ldots,1,1)}).$$

The *Walsh-Hadamard transform* (WHT) of $f \in \mathcal{B}_n$, and its inverse WHT, at any point $u \in \mathbb{F}_2^n$ are defined by

$$\begin{cases} W_f(u) = \displaystyle\sum_{x \in \mathbb{F}_2^n} (-1)^{f(x) \oplus u \cdot x}, \\ (-1)^{f(x)} = 2^{-n} \displaystyle\sum_{u \in \mathbb{F}_2^n} W_f(u)(-1)^{u \cdot x}. \end{cases} \tag{1}$$

For the sake of simplicity, throughout the paper the function W_f will be briefly called Walsh function. For a given function $f \in \mathcal{B}_n$, its corresponding sequence $(W_f(u_0), \ldots, W_f(u_{2^n-1}))$ and support $S_f = \{\omega \in \mathbb{F}_2^n : W_f(\omega) \neq 0\}$, will be called *Walsh spectrum* and *Walsh support* respectively. We note that a given Boolean function uniquely corresponds to its Walsh spectrum, or equivalently, no two different Boolean functions may have the same Walsh spectrum.

A function $f \in \mathcal{B}_n$ is called bent if $|W_f(u)| = 2^{\frac{n}{2}}$ holds for all $u \in \mathbb{F}_2^n$. Rothaus [20] proved that a bent function exists only for n even. Clearly, for each bent function f there is a Boolean function $g \in \mathcal{B}_n$ such that $W_f(u) = 2^{\frac{n}{2}}(-1)^{g(u)}$. It can be shown that g is also bent, and $W_g(u) = 2^{\frac{n}{2}}(-1)^{f(u)}$ holds as well. Hence f and g are called mutually dual bent functions and g is denoted by f^*.

A function $f \in \mathcal{B}_n$ is called *s-plateaued* if the range of its Walsh function W_f is the set $\{0, \pm 2^{\frac{n+s}{2}}\}$. The value $2^{\frac{n+s}{2}}$ is called *amplitude*, where $s \geq 1$ if n is odd and $s \geq 2$ if n is even (clearly s and n always must have the same parity). For an s-plateaued function $f \in \mathcal{B}_n$, the cardinality of its Walsh support is $\#S_f = 2^{n-s}$ [1, Proposition 4].

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/TIT.2020.3044059, IEEE Transactions on Information Theory

Definition II.1. *A function $f \in \mathcal{B}_n$ is called 5-value spectrum function if the range of W_f equals $\{0, \pm 2^{\frac{n+s_1}{2}}, \pm 2^{\frac{n+s_2}{2}}\}$, where $s_2 > s_1 \geq 0$. Further, let $S_f^{[i]} = \{u \in \mathbb{F}_2^n : |W_f(u)| = 2^{\frac{n+s_i}{2}}\}$. Then f is called* basic *if both $S_f^{[1]}$ and $S_f^{[2]}$ are affine subspaces of $\mathbb{F}_2^n$.*

Clearly, $S_f^{[1]} \cup S_f^{[2]} \neq \mathbb{F}_2^n$ (equivalently: $2^{\lambda_1} + 2^{\lambda_2} < 2^n$), otherwise the range of W_f would not contain 0. Hence, in the spectral constructions of 5-value spectrum function this condition is always assumed.

For an arbitrary Boolean function $f \in \mathcal{B}_n$, the set of its values on $\mathbb{F}_2^n$ (*the truth table*) is defined as $T_f = (f(0,\ldots,0,0), f(0,\ldots,0,1),\ldots,f(1,\ldots,1,1))$. The *Sylvester-Hadamard* matrix of size $2^k \times 2^k$, is defined recursively as:

$$H_1 = (1),\ \ H_2 = \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix},\ H_{2^k} = \begin{pmatrix} H_{2^{k-1}} & H_{2^{k-1}} \\ H_{2^{k-1}} & -H_{2^{k-1}} \end{pmatrix}.$$

The i-th row of H_{2^k} we denote by $H_{2^k}^{(i)}$ ($i \in [0, 2^k - 1]$). Recall that $H_{2^k}^{(i)} = ((-1)^{u_i \cdot x_0}, \ldots, (-1)^{u_i \cdot x_{2^k-1}}) = \chi_\ell$ ($x_j \in \mathbb{F}_2^k$) is a (± 1)-sequence of a linear function $\ell : \mathbb{F}_2^k \to \mathbb{F}_2$, where $\ell(x) = u_i \cdot x$ ($u_i, x \in \mathbb{F}_2^k$).

Throughout the paper by $a < b$ ($a, b \in \mathbb{F}_2^n$) we denote the lexicographic ordering on $\mathbb{F}_2^n$. Also, $GL(n, \mathbb{F}_2)$ denotes the group of all invertible $\mathbb{F}_2$-linear transformations on $\mathbb{F}_2^n$. Two Boolean functions $h, f : \mathbb{F}_2^n \to \mathbb{F}_2$ are said to be EA-equivalent if there exists a matrix $M \in GL(n, \mathbb{F}_2)$, vectors $b, c \in \mathbb{F}_2^n$ and a constant $\varepsilon \in \{0,1\}$ such that $h(x) = f(xM \oplus b) \oplus c \cdot x \oplus \varepsilon$.

III. Spectral constructions of 5-value spectrum functions

In this section, we first recall the definition of the dual of 5-value spectrum Boolean functions which has been introduced recently in [15]. Essentially, it uses the same defining mechanism which has been established for plateaued functions in [13], [14]. Also, we recall the spectral construction method in [15] and then we derive new technical results which will be used in Section IV. We recall that when applying the spectral construction technique, we firstly construct a Walsh spectrum of a desired function, which is then obtained by applying the inverse Walsh transform. We will be mainly focusing on basic 5-value spectrum functions based on totally disjoint spectra plateaued functions [15], see Definition III.1.

Let $f : \mathbb{F}_2^n \to \mathbb{F}_2$ be a 5-value spectrum function whose Walsh spectrum contains values $0, \pm c_1, \pm c_2$ ($c_1 \neq c_2$), where $c_1, c_2 \in \mathbb{N}$. For $i = 1, 2$, by $S_f^{[i]} \subset \mathbb{F}_2^n$ we denote the set $S_f^{[i]} = \{u \in \mathbb{F}_2^n : |W_f(u)| = c_i\}$, and we define functions $f_{[i]}^* : S_f^{[i]} \to \mathbb{F}_2$ such that the following equality holds:

$$W_f(u) = \begin{cases} 0, & u \notin S_f^{[1]} \cup S_f^{[2]}, \\ c_i \cdot (-1)^{f_{[i]}^*(u)}, & u \in S_f^{[i]},\ \ i \in \{1,2\}. \end{cases} \tag{2}$$

Note that the function f uniquely defines the pairs $(S_f^{[1]}, f_{[1]}^*)$ and $(S_f^{[2]}, f_{[2]}^*)$. Throughout the paper, the functions $f_{[i]}^*$ (i=1,2) are called *duals* of f. In addition, we will consider functions f for which the sets $S_f^{[i]}$ are of the size power of 2, say 2^{λ_i}, with $2^{\lambda_1} + 2^{\lambda_2} < 2^n$ (except for Proposition III.3), since it allows us to consider the duals $f_{[i]}^*$ as functions in λ_i variables. Therefore, we first provide the description of $f_{[i]}^* : S_f^{[i]} \to \mathbb{F}_2$ as functions from $\mathbb{F}_2^{\lambda_i}$ to $\mathbb{F}_2$.

For $i = 1, 2$, let $v_i \in \mathbb{F}_2^n$ and $E_i = \{e_0^{(i)}, \ldots, e_{2^{\lambda_i}-1}^{(i)}\} \subset \mathbb{F}_2^n$ ($e_0^{(i)} = \mathbf{0}_n$) be lexicographically ordered subsets such that $S_f^{[i]} = \{\omega_0^{(i)}, \ldots, \omega_{2^{\lambda_i}-1}^{(i)}\} = v_i \oplus E_i$, where $\omega_j^{(i)} = v_i \oplus e_j^{(i)}$, for $j \in [0, 2^{\lambda_i} - 1]$. Clearly, the lexicographically ordered set E_i imposes an ordering on $S_f^{[i]}$ with respect to equality $\omega_j^{(i)} = v_i \oplus e_j^{(i)}$. Using the representation of $S_f^{[i]} = v_i \oplus E_i$, $i = 1, 2$, the function $f_{[i]}^*$ as a mapping from $\mathbb{F}_2^{\lambda_i}$ to $\mathbb{F}_2$ is defined by

$$\overline{f}_{[i]}^*(x_j) = f_{[i]}^*(v_i \oplus e_j^{(i)}) = f_{[i]}^*(\omega_j^{(i)}),\ \ j \in [0, 2^{\lambda_i} - 1], \tag{3}$$

where $\mathbb{F}_2^{\lambda_i} = \{x_0, \ldots, x_{2^{\lambda_i}-1}\}$ is ordered lexicographically.

Remark III.1. *Throughout this work, by affine subspace (say $S \subset \mathbb{F}_2^n$) we mean that S is equal to $v \oplus E$, for some linear subspace $E \subset \mathbb{F}_2^n$ and $v \in \mathbb{F}_2^n$. We do not require that $v \notin E$ in general, and thus whenever we say that S is an affine subspace, then it clearly includes the possibility for S to be a linear subspace (corresponding to the case when $v = \mathbf{0}_n$).*

The following lemma will be used more frequently, and it regards the ordering of E_i when E_i is a linear subspace.

Lemma III.1. *[13] Let $S = \{\omega_0, \ldots, \omega_{2^m-1}\} \subseteq \mathbb{F}_2^k$ be any affine subspace of dimension $m \geq 2$ such that $S = v \oplus E$, for some lexicographically ordered linear subspace $E = \{e_0, \ldots, e_{2^m-1}\} \subseteq \mathbb{F}_2^k$ and $v \in S$, where $\omega_i = v \oplus e_i$ for $i \in [0, 2^m - 1]$. Then:*

i) The lexicographic ordering of E implies that for any fixed $i \in \{0, \ldots, m-1\}$ it holds that $e_j = e_{2^i} \oplus e_{j-2^i}$ for all $2^i \leq j \leq 2^{i+1} - 1$.

ii) For an arbitrary vector $u \in \mathbb{F}_2^k$ it holds that

$$((-1)^{u\cdot\omega_0}, (-1)^{u\cdot\omega_1}, \ldots, (-1)^{u\cdot\omega_{2^m-1}}) = (-1)^{\varepsilon_u} H_{2^m}^{(r_u)}, \tag{4}$$

for some $0 \leq r_u \leq 2^m - 1$ and $\varepsilon_u \in \mathbb{F}_2$. In addition, $\{T_\ell : \ell \in \mathcal{L}_m\} \subseteq \{(u \cdot e_0, \ldots, u \cdot e_{2^m-1}) : u \in \mathbb{F}_2^k\}$, which means that $\mathcal{L}_m$ is contained in a multi-set of m-variable linear functions whose truth tables are $\{(u \cdot e_0, \ldots, u \cdot e_{2^m-1}) : u \in \mathbb{F}_2^k\}$.

Remark III.2. *In the rest of the paper, by $f_{[i]}^*$ we denote the duals of a 5-value spectrum function f whenever it is viewed as a function defined on $S_f^{[i]}$, and by $\overline{f}_{[i]}^*$ when we consider it as a function on $\mathbb{F}_2^{\lambda_i}$ (where $i = 1, 2$). The latter case implies that we must fix some ordering of $S_f^{[i]}$ in a suitable way. The orderings $E_i = \{e_0^{(i)}, \ldots, e_{2^{\lambda_i}-1}^{(i)}\}$ which will be considered are those for which $(u \cdot e_0^{(i)}, \ldots, u \cdot e_{2^{\lambda_i}-1}^{(i)})$, $e_j^{(i)} \in E_i \subset \mathbb{F}_2^n$ ($i = 1, 2$) corresponds to the truth table of some linear function in terms of Lemma III.1 (for all $u \in \mathbb{F}_2^n$).*

The so-called spectral construction of 5-value functions has been recently introduced in [15]. Now we slightly generalize [15, Proposition IV.1] (referring to the amplitude values s_1

and s_2) which describes the main design rationales behind the spectral construction of 5-value spectrum functions. The proof is given for self-completeness.

Proposition III.1. *For sets $S^{[i]} = \{u \in \mathbb{F}_2^n : |W(u)| = 2^{\frac{n+s_i}{2}}\}$ ($i = 1, 2$) with $s_1 > s_2 \geq 0$, we define the values of $W(u)$ by*

$$W(u) = \begin{cases} 0, & u \notin S^{[1]} \cup S^{[2]} \\ (-1)^{g_{[1]}(u)} \cdot 2^{\frac{n+s_1}{2}}, & u \in S^{[1]} \\ (-1)^{g_{[2]}(u)} \cdot 2^{\frac{n+s_2}{2}}, & u \in S^{[2]} \end{cases}, \quad (5)$$

where $g_{[i]} : S^{[i]} \to \mathbb{F}_2$ ($i = 1, 2$). Then, there exists a 5-value spectrum Boolean function $f : \mathbb{F}_2^n \to \mathbb{F}_2$ such that $W_f(u) = W(u)$ if and only if the equality

$$2^{\frac{s_1-s_2}{2}} X_1(u) + X_2(u) = (-1)^{\varepsilon_u} 2^{\frac{n-s_2}{2}}, \quad (6)$$

holds for all $u \in \mathbb{F}_2^n$ ($\varepsilon_u \in \{0, 1\}$), where $X_i(u) = \sum_{\omega \in S^{[i]}} (-1)^{g_{[i]}(\omega) \oplus u \cdot \omega}$, $i = 1, 2$. Hence, $f^*_{[i]} = g_{[i]}$ and $S_f^{[i]} = S^{[i]}$ for $i = 1, 2$.

Proof. Let $u \in \mathbb{F}_2^n$ be an arbitrary vector. By setting $W_f(u) = W(u)$, i.e. $f^*_{[i]} = g_{[i]}$ and $S_f^{[i]} = S^{[i]}$ ($i = 1, 2$), the inverse WHT formula (1) gives that

$$2^n (-1)^{f(u)} = \sum_{\omega \in \mathbb{F}_2^n} W_f(\omega)(-1)^{u \cdot \omega}$$
$$= 2^{\frac{n+s_1}{2}} \sum_{\omega \in S_f^{[1]}} (-1)^{f^*_{[1]}(\omega) \oplus u \cdot \omega} + 2^{\frac{n+s_2}{2}} \sum_{\omega \in S_f^{[2]}} (-1)^{f^*_{[2]}(\omega) \oplus u \cdot \omega},$$

which, after dividing both sides by $2^{\frac{n+s_2}{2}}$ ($s_2 < s_1$), is equivalent to (6). □

Remark III.3. *Note that if n is even, then the minimal amplitudes in (5) (providing the maximal nonlinearity of a 5-value spectrum function) are $2^{\frac{n}{2}}$ and $2^{\frac{n+2}{2}}$ (thus $s_1, s_2 \in \{0, 2\}$), and if n is odd, then the minimal amplitudes are given by $2^{\frac{n+1}{2}}$ and $2^{\frac{n+3}{2}}$ ($s_1, s_2 \in \{1, 3\}$). In what follows we will assume that the necessary condition that n and s_i are of the same parity is satisfied.*

The spectral constructions proposed in [15, Section IV] utilize the totally disjoint plateaued spectra functions whose definition is given as follows.

Definition III.1. *[15] Let $f : \mathbb{F}_2^n \to \mathbb{F}_2$ be a 5-value spectrum function with $S_f^{[i]} = \{u \in \mathbb{F}_2^n : |W_f(u)| = 2^{\frac{n+s_i}{2}}\}$, where $s_1 > s_2 \geq 0$ and $\#S_f^{[1]} + \#S_f^{[2]} < 2^n$ ($\#S_f^{[i]}$ not necessarily a power of 2). We say that the duals $f^*_{[i]} : S_f^{[i]} \to \mathbb{F}_2$ ($i = 1, 2$) of f are totally disjoint spectra functions if*

$$X_1(u) X_2(u) = 0 \quad \text{and} \quad |X_1(u)| + |X_2(u)| > 0, \quad \forall u \in \mathbb{F}_2^n, \quad (7)$$

where $X_i(u) = \sum_{\omega \in S_f^{[i]}} (-1)^{f^*_{[i]}(\omega) \oplus u \cdot \omega}$.

Remark III.4. *Note that in Definition III.1, in comparison to Definition IV.1 given in [15], we are not assuming that $\#S_f^{[i]}$ are powers of 2. As it will be shown later on in Proposition III.3-(ii), $\#S_f^{[i]}$ may take different values in general.*

Notice that the second condition in (7) means that $X_1(u)$ and $X_2(u)$ are never both equal to zero for any $u \in \mathbb{F}_2^n$. The following result (which we recall from [15]) gives necessary and sufficient conditions on the main design parameters of totally disjoint plateaued functions that provide 5-value spectrum functions by means of Proposition III.1. We also slightly adjust the notation in order to unify it with (5).

Proposition III.2. *[15] For sets $S^{[i]} = v_i \oplus E_i = \{u \in \mathbb{F}_2^n : |W(u)| = 2^{\frac{n+s_i}{2}}\}$ ($v_i \in \mathbb{F}_2^n$) with $s_1 > s_2 \geq 0$, we define the values $W(u)$ by (5) ($u \in \mathbb{F}_2^n$), where E_i are linear subspaces with $dim(E_i) = \lambda_i$ ($i = 1, 2$). Suppose that $g_{[i]} : \mathbb{F}_2^{\lambda_i} \to \mathbb{F}_2$ are totally disjoint spectra r_i-plateaued functions with $r_i \geq 1$. Then, $(W(u_0), \ldots, W(u_{2^n-1}))$ is a Walsh spectrum of a 5-value spectrum function $f : \mathbb{F}_2^n \to \mathbb{F}_2$ (i.e., $W_f(u) = W(u)$) if and only if $s_i + r_i + \lambda_i = n$ for $i = 1, 2$.*

We note that if for a fixed $i \in \{1, 2\}$ it holds that $r_i = 0$ with the corresponding λ_i being even (in which case $\overline{f}^*_{[i]}$ is bent), then $f^*_{[1]}$ and $f^*_{[2]}$ cannot be totally disjoint spectra functions. In this case the first condition in (7) can not be satisfied.

Remark III.5. *We note that an r_i-plateaued function $\overline{f}^*_{[i]}$ in λ_i variables having the Walsh support of cardinality $\#S_{\overline{f}^*_{[i]}} = 2^{\lambda_i - r_i} < 4$ can not exist except for the case when $\lambda_i = r_i = 1$, in which case $\overline{f}^*_{[i]}$ can be any function defined on $\mathbb{F}_2$ (i.e., it is a function in one variable only). In general, $\#S_{\overline{f}^*_{[i]}}$ is always a power of 2 with an even exponent, since λ_i and r_i are of the same parity. Additionally, if $\#E_i = 4$ (in Proposition III.2), then the dual function $\overline{f}^*_{[i]}$ can only be an affine or linear function (in the space of functions defined on $\mathbb{F}_2^2$, there exist only bent and affine/linear functions).*

In the following example, we present a 5-value spectrum function whose dual $f^*_{[1]} : S_f^{[1]} \to \mathbb{F}_2$ is a constant function with $\#S_f^{[1]} = 2$, and $f^*_{[2]} : S_f^{[2]} \to \mathbb{F}_2$ is a proper plateaued function with $\#S_f^{[2]} = 2^3$ (by proper we mean that it is not an affine/linear or bent function).

Example III.1. *Let us consider the 5-value spectrum function $f : \mathbb{F}_2^4 \to \mathbb{F}_2$ given as*

$$f(x_1, \ldots, x_4) = x_1x_2x_3 \oplus x_1x_3x_4 \oplus x_2x_3x_4 \oplus x_1x_4 \oplus x_2x_4 \oplus x_3.$$

The Walsh spectrum of f is given as

$$W_f = (0, 4, 8, 4, -4, 0, 4, 0, -4, 0, 4, 0, 8, -4, 0, -4).$$

Here, we precisely have that

$$S_f^{[1]} = \{(0,0,1,0), (1,1,0,0)\} = (0,0,1,0) \oplus \langle (1,1,0,0) \rangle = v_1 \oplus E_1,$$
$$S_f^{[2]} = (0,0,0,1) \oplus \langle (0,0,1,0), (0,1,0,1), (1,0,0,1) \rangle = v_2 \oplus E_2,$$

where v_i and E_i are clear from the context. Moreover, for the lexicographically ordered E_1 and E_2, one can define the functions $\overline{f}^*_{[1]} : \mathbb{F}_2 \to \mathbb{F}_2$ and $\overline{f}^*_{[2]} : \mathbb{F}_2^3 \to \mathbb{F}_2$ such that their truth tables are given as

$$T_{f^*_{[1]}} = (0, 0) \quad \text{and} \quad T_{f^*_{[2]}} = (0, 0, 1, 0, 1, 0, 1, 1),$$

which gives that their ANFs are $\overline{f}^*_{[1]}(x_1) = 1$ ($x_1 \in \mathbb{F}_2$) and $\overline{f}^*_{[2]}(x_1, x_2, x_3) = x_1 \oplus x_2 \oplus x_1x_2 \oplus x_1x_3 \oplus x_2x_3$, $(x_1, x_2, x_3) \in$

$\mathbb{F}_2^3$. *For these functions one can verify that* $(X_1(u), X_2(u)) \in \{(2,0),(0,\pm 4)\}$ *for all* $u \in \mathbb{F}_2^4$, *i.e.,* $f^*_{[1]}$ *and* $f^*_{[2]}$ *are totally disjoint spectra functions.*

The following result will enable us to prove that if a 5-value spectrum function $f : \mathbb{F}_2^n \to \mathbb{F}_2$ (with spectral values $0, \pm 2^{\frac{n+s_i}{2}}$, $s_1 \neq s_2$) is constructed using two totally disjoint spectra functions, then they are necessarily plateaued (see Corollary 1).

Proposition III.3. *Let* $f : \mathbb{F}_2^n \to \mathbb{F}_2$ *be a 5-value spectrum function constructed by (5) with totally disjoint spectra dual functions* $f^*_{[i]} : S_f^{[i]} \to \mathbb{F}_2$, $i = 1, 2$. *Then:*

- *i) The values of* $X_i(u)$ *are given as* $(X_1(u), X_2(u)) \in \{(\pm 2^{\frac{n-s_1}{2}}, 0), (0, \pm 2^{\frac{n-s_2}{2}})\}$, $\forall u \in \mathbb{F}_2^n$.
- *ii) The sizes* $\#S_f^{[i]}$ *are given as* $(\#S_f^{[1]}, \#S_f^{[2]}) = (t, 2^{n-s_2} - t \cdot 2^{s_1 - s_2})$, *for* $t \in \mathbb{N}$.

Proof. i) For arbitrary $u \in \mathbb{F}_2^n$, by Proposition III.1, we have that $2^{\frac{n+s_1}{2}} X_1(u) + 2^{\frac{n+s_2}{2}} X_2(u) = (-1)^{f(u)} 2^n$. By squaring both sides and using the fact that $X_1(u)X_2(u) = 0$ ($f^*_{[i]}$ are totally disjoint spectra functions), we have that

$$2^{n+s_1} X_1^2(u) + 2^{n+s_2} X_2^2(u) = 2^{2n}.$$

Since n and s_i (for all $i = 1, 2$) are of the same parity, then $n + s_i$ are even numbers. Denoting by $n + s_i = 2p_i$ for $p_i \in \mathbb{N}$ ($i = 1, 2$), we have that $(2^{p_1} X_1(u))^2 + (2^{p_2} X_2(u))^2 = 2^{2n}$. Since $X_i(u)$ are integers, then using the well-known Jacobi's two square theorem (see for instance [2, Lemma B.1]) we have that $(2^{p_1} X_1(u))^2 = 2^{2n}$ and $(2^{p_2} X_2(u))^2 = 0$, or vice versa (for all $u \in \mathbb{F}_2^n$). Thus, for all $u \in \mathbb{F}_2^n$ and $i = 1, 2$, we have that either $X_i(u) = \pm 2^{\frac{n-s_i}{2}}$ or $X_i(u) = 0$, which completes the first part.

ii) Using the Parseval's identity, i.e., $\sum_{u \in \mathbb{F}_2^n} W_f^2(u) = 2^{2n}$, and denoting by $p = \#S_f^{[1]}$ and $q = \#S_f^{[2]}$, we obtain the Diophantine equation given as

$$p \cdot 2^{n+s_1} + q \cdot 2^{n+s_2} = 2^{2n}.$$

The assumption $s_1 > s_2$ implies that $\gcd(2^{n+s_1}, 2^{n+s_2}) = 2^{n+s_2}$ and thus the set of all solutions (p, q) is given as $p = t$ and $q = 2^{n-s_2} - t \cdot 2^{s_1 - s_2}$, for $t \in \mathbb{N}$. □

Corollary 1. *Let* $f : \mathbb{F}_2^n \to \mathbb{F}_2$ *be a 5-value spectrum function constructed by (5) with totally disjoint spectra dual functions* $f^*_{[i]} : S_f^{[i]} \to \mathbb{F}_2$, $i = 1, 2$. *If* $\#S_f^{[i]} = 2^{\lambda_i}$ ($i = 1, 2$, $S_f^{[i]}$ *are not necessarily affine spaces), then* $\overline{f}^*_{[i]} : \mathbb{F}_2^{\lambda_i} \to \mathbb{F}_2$ *are* r_i*-plateaued functions, where* $r_i + s_i + \lambda_i = n$ ($i = 1, 2$).

Proof. If $\#S_f^{[i]} = 2^{\lambda_i}$ ($i = 1, 2$), then by Proposition III.3-(i) we have that $n - s_i = \lambda_i + r_i$ with $r_i \geq 1$ for $i = 1, 2$, and thus f is constructed out of two totally disjoint spectra r_i-plateaued functions $\overline{f}^*_{[i]}$ ($i = 1, 2$). □

Remark III.6. *By Proposition III.3-(ii),* $\#S_f^{[i]}$ *does not have to be a power of* 2. *In such a case a design of 5-value spectrum function appears to be difficult as it is not possible to employ dual functions defined on a subspace of* $\mathbb{F}_2^n$.

IV. Design method of basic 5-value spectrum functions

The main result of [15] given by Proposition III.2 concerns the construction of 5-value spectrum functions based on the use of totally disjoint spectra plateaued functions. Regarding the constructions, in [15, Section A] one can find a method of constructing totally disjoint spectra plateaued functions (only for even n) which can be utilized in Proposition III.2. In general, no other constructions of totally disjoint spectra plateaued functions are known. However, in the literature there does not exist any type of results which describes the structure of 5-value spectrum functions (whether it is basic or not). In this section, we will firstly provide a characterization of basic 5-value spectrum functions using totally disjoint spectra plateaued dual functions $f^*_{[i]}$ (Section IV-A) having affine Walsh supports $S_{f^*_{[i]}}$ ($\#S_f^{[i]}$ are powers of two). Then, in Section IV-B, we present new construction methods of 5-value spectrum functions based on totally disjoint spectra plateaued functions. Finally, in Section IV-C we briefly analyze the notion of linear structures in terms of the derived results, and in Section IV-D we analyse the equivalence of basic 5-value spectrum whose duals are basic plateaued functions (where we essentially apply results derived in [14]).

A. On characterization of basic 5-value spectrum functions

We start by recalling the spectral construction method which has been given in [13].

Theorem IV.1. *[13] Let* $S = v \oplus E = \{\omega_0, \ldots, \omega_{2^{k-r}-1}\} \subset \mathbb{F}_2^k$ *(*$k - r \geq 2$ *is even), where* $v \in \mathbb{F}_2^k$ *and* $E = \{e_0, e_1, \ldots, e_{2^{k-r}-1}\} \subset \mathbb{F}_2^k$ *is a linear subspace. For a function* $g : \mathbb{F}_2^{k-r} \to \mathbb{F}_2$ *with the Hamming weight* $wt(g) \in \{2^{k-r-1} - 2^{\frac{k-r}{2}-1}, 2^{k-r-1} + 2^{\frac{k-r}{2}-1}\}$, *we define the values* $W(u)$, *for* $u \in \mathbb{F}_2^k$, *by*

$$W(u) = \begin{cases} 2^{\frac{k+s}{2}} (-1)^{g(x_i)} & \text{for } u = v \oplus e_i \in S, \\ 0 & u \notin S. \end{cases} \tag{8}$$

Suppose that E *is ordered such that the equality*

$$((-1)^{u \cdot \omega_0}, (-1)^{u \cdot \omega_1}, \ldots, (-1)^{u \cdot \omega_{2^{k-r}-1}}) = (-1)^{\varepsilon_u} H^{(\mu_u)}_{2^{k-r}},$$

holds for some $0 \leq \mu_u \leq 2^{k-r} - 1$ *and* $\varepsilon_u \in \mathbb{F}_2$. *Then* $\{W(u) : u \in \mathbb{F}_2^k\}$ *is the spectrum of a Boolean* r*-plateaued function* $f : \mathbb{F}_2^k \to \mathbb{F}_2$ *(i.e.* $W_f(u) = W(u)$ *for all* $u \in \mathbb{F}_2^k$*) if and only if* g *is a bent function on* $\mathbb{F}_2^{k-r}$.

The following technical result will be essential in deriving properties of the sums $X_i(u)$ (from relation (6)) and their dependency on u in general. Note that in the next result, the set E_i is a linear subspace only in the statement ii).

Proposition IV.1. *Let a 5-valued spectrum function* $f : \mathbb{F}_2^n \to \mathbb{F}_2$ *be obtained by applying the inverse WHT to the spectrum* $\{W(u) : u \in \mathbb{F}_2^n\}$ *constructed by (5). Further, let* $E_i \subset \mathbb{F}_2^n$ *be a subset, and let* $\Delta_i \subset \mathbb{F}_2^n$ ($i = 1, 2$) *be a linear subspace such that* $\Delta_i \oplus E_i^\perp = \mathbb{F}_2^n$ *and* $\Delta_i \cap E_i^\perp = \{\boldsymbol{0}_n\}$. *Then:*

- *i) Assume that* $E_i = \{e_0^{(i)}, \ldots, e^{(i)}_{2^{\lambda_i}-1}\}$ *is a subset without any fixed ordering. The set* $\{(u \cdot e_0^{(i)}, \ldots, u \cdot e^{(i)}_{2^{\lambda_i}-1}) : u \in \Delta_i\}$ *contains mutually distinct sequences of length* 2^{λ_i}.

ii) For $i = 1, 2$ assume that $E_i = \{e_0^{(i)}, \ldots, e_{2^{\lambda_i}-1}^{(i)}\}$ is a linear subspace (ordered lexicographically, where $e_0^{(i)} = \boldsymbol{0}_n$), and let $\xi : \Delta_i \to \mathbb{F}_2^{\lambda_i}$ be defined by $\xi : \alpha \in \Delta_i \to \vartheta_\alpha \in \mathbb{F}_2^{\lambda_i}$ if

$$(\alpha \cdot e_0^{(i)}, \ldots, \alpha \cdot e_{2^{\lambda_i}-1}^{(i)}) = (\vartheta_\alpha \cdot z_0, \ldots, \vartheta_\alpha \cdot z_{2^{\lambda_i}-1})$$

holds, where $\mathbb{F}_2^{\lambda_i} = \{z_0, \ldots, z_{2^{\lambda_i}-1}\}$ is ordered lexicographically. Then ξ is an injective linear mapping.

Proof. i) For an arbitrary vector $u \in \Delta_i \oplus E_i^\perp$ given as $u = \alpha \oplus \gamma$ (where $\alpha \in \Delta_i$ and $\gamma \in E_i^\perp$), the equality $u \cdot e_j^{(i)} = (\alpha \oplus \gamma) \cdot e_j^{(i)} = \alpha \cdot e_j^{(i)}$ holds ($\forall e_j^{(i)} \in E_i$). Additionally, if we assume that for two distinct vectors $\alpha_1, \alpha_2 \in \Delta_i$ the equality $\alpha_1 \cdot e_j^{(i)} = \alpha_2 \cdot e_j^{(i)}$ holds for all $e_0^{(i)}, \ldots, e_{2^{\lambda_i}-1}^{(i)} \in E_i$, then $(\alpha_1 \oplus \alpha_2) \cdot e_j^{(i)} = 0$ ($\forall e_j^{(i)} \in E_i$) which implies $\alpha_1 \oplus \alpha_2 \in E_i^\perp$. However, the condition $\Delta_i \cap E_i^\perp = \{\boldsymbol{0}_n\}$ necessarily gives that $\alpha_1 = \alpha_2$. Consequently, we have that $(u \cdot e_0^{(i)}, \ldots, u \cdot e_{2^{\lambda_i}-1}^{(i)})$ are distinct in pairs only for $u = \alpha \in \Delta_i$.

ii) In the proof of i) we have shown that $\xi : \Delta_i \to \mathbb{F}_2^{\lambda_i}$ is an injective mapping. Due to the definition of ξ it is not difficult to see that $\xi(\alpha_1 \oplus \alpha_2) = \xi(\alpha_1) \oplus \xi(\alpha_2)$ holds for any two vectors $\alpha_1, \alpha_2 \in \Delta_i$, which means that ξ is an injective linear mapping. □

Remark IV.1. *It is important to emphasize that the statement Proposition IV.1-(i) does not depend on the structure, ordering and size of E_i. In Proposition IV.1-(ii) the equality $(\alpha \cdot e_0^{(i)}, \ldots, \alpha \cdot e_{2^{\lambda_i}-1}^{(i)}) = (\vartheta_\alpha \cdot z_0, \ldots, \vartheta_\alpha \cdot z_{2^{\lambda_i}-1})$ admits any ordering of E_i as long as it satisfies the recursion described in Lemma 3.1-(i). In this context, the definition of the mapping ξ depends on the ordering of E_i.*

Remark IV.2. *We also note that the equality $(\alpha \cdot e_0^{(i)}, \ldots, \alpha \cdot e_{2^{\lambda_i}-1}^{(i)}) = (\vartheta_\alpha \cdot z_0, \ldots, \vartheta_\alpha \cdot z_{2^{\lambda_i}-1})$ in Proposition IV.1 is possible by Lemma III.1, since for the lexicographically ordered linear subspace E_i the left side of the equality corresponds to the truth table of a linear function in λ_i variables ($e_0^{(i)} = \boldsymbol{0}_n$).*

In the following example, we illustrate the details of Proposition IV.1 where for simplicity we set that $E = E_1 = E_2$ is a linear subspace in $\mathbb{F}_2^5$.

Example IV.1. *Let $E = \langle (1,0,0,0,1), (0,0,1,1,0), (0,1,1,0,0) \rangle$ be a linear subspace of $\mathbb{F}_2^5$. Then $E^\perp = \langle (0,1,1,1,0), (1,0,0,0,1) \rangle$. If we set $\Delta = \langle (0,1,0,0,0), (0,0,0,1,0), (0,0,0,0,1) \rangle$, then $\Delta \oplus E^\perp = \mathbb{F}_2^5$ and $\Delta \cap E^\perp = \{\boldsymbol{0}_5\}$. As $(1,0,0,0,1)$ belongs to both E and $E^\perp$, we have that $E \oplus E^\perp \subsetneq \mathbb{F}_2^5$. This is due to the fact that the dot product "$\cdot$" (defined on $\mathbb{F}_2^5$) is not an inner product, since it fails to satisfy the positive semi-definiteness property.*

For simplicity, if we order the spaces $E = \{e_0, \ldots, e_7\}$ and $\Delta = \{\alpha_0, \ldots, \alpha_7\}$ lexicographically, we have that the set $\{(\alpha \cdot e_0, \ldots, \alpha \cdot e_7) : \alpha \in \Delta\}$ is given by

$$\begin{array}{c} \alpha_0 \to \\ \alpha_1 \to \\ \alpha_2 \to \\ \alpha_3 \to \\ \alpha_4 \to \\ \alpha_5 \to \\ \alpha_6 \to \\ \alpha_7 \to \end{array} \begin{pmatrix} 0&0&0&0&0&0&0&0 \\ 0&0&0&0&1&1&1&1 \\ 0&1&1&0&0&1&1&0 \\ 0&1&1&0&1&0&0&1 \\ 0&0&1&1&0&0&1&1 \\ 0&0&1&1&1&1&0&0 \\ 0&1&0&1&0&1&0&1 \\ 0&1&0&1&1&0&1&0 \end{pmatrix}. \tag{9}$$

For instance, the first row in the matrix (9) corresponds to the sequence $(\alpha_0 \cdot e_0, \ldots, \alpha_0 \cdot e_7)$, and so on. Also, we can see that no two rows are the same, which means that $\{(\alpha \cdot e_0, \ldots, \alpha \cdot e_7) : \alpha \in \Delta\}$ is not a multi-set (Proposition IV.1-(i)).

On the other hand, we define the injective linear mapping $\xi : \Delta \to \mathbb{F}_2^3$ such that $\xi(\alpha) = \vartheta_\alpha \in \mathbb{F}_2^3$ if $(\alpha \cdot e_0, \ldots, \alpha \cdot e_7) = (\vartheta_\alpha \cdot z_0, \ldots, \vartheta_\alpha \cdot z_7)$, where $\mathbb{F}_2^3 = \{z_0, \ldots, z_7\}$ is ordered lexicographically. Concretely, the values of $\xi(\alpha_i)$ ($\alpha_i \in \Delta$) are given as follows:

$$\begin{gathered} \xi : \quad \alpha_0 \to z_0 = \boldsymbol{0}_3, \quad \alpha_1 \to z_4 = (1,0,0), \\ \alpha_2 \to z_3 = (0,1,1), \quad \alpha_3 \to z_7 = (1,1,1), \\ \alpha_4 \to z_2 = (0,1,0), \quad \alpha_5 \to z_6 = (1,1,0), \\ \alpha_6 \to z_1 = (0,0,1), \quad \alpha_7 \to z_5 = (1,0,1). \end{gathered}$$

It is easy to check that ξ is an onto mapping, i.e. $\xi(\Delta) = \mathbb{F}_2^3$. In other words, we have that the rows in matrix in (9) (which are rows of linear functions on $\mathbb{F}_2^3$) are actually elements of the set $\{(\xi(\alpha_i) \cdot z_0, \ldots, \xi(\alpha_i) \cdot z_7) : \delta_i \in \Delta\}$, i.e., we have that

$$\begin{array}{c} z_0 \to \\ z_4 \to \\ z_3 \to \\ z_7 \to \\ z_2 \to \\ z_6 \to \\ z_1 \to \\ z_5 \to \end{array} \begin{pmatrix} 0&0&0&0&0&0&0&0 \\ 0&0&0&0&1&1&1&1 \\ 0&1&1&0&0&1&1&0 \\ 0&1&1&0&1&0&0&1 \\ 0&0&1&1&0&0&1&1 \\ 0&0&1&1&1&1&0&0 \\ 0&1&0&1&0&1&0&1 \\ 0&1&0&1&1&0&1&0 \end{pmatrix},$$

where for instance, the second row corresponds to the sequence $(\xi(\alpha_1) \cdot z_0, \ldots, \xi(\alpha_1) \cdot z_7) = (z_4 \cdot z_0, \ldots, z_4 \cdot z_7)$.

In order to proceed further with the analysis of basic 5-value spectrum functions $f : \mathbb{F}_2^n \to \mathbb{F}_2$, using Proposition IV.1 we have the following set of observations:

(I): In the equation

$$\begin{aligned} &2^{\frac{n+s_1}{2}}(-1)^{u \cdot v_1} \sum_{e^{(1)} \in E_1} (-1)^{f_{[1]}^*(v_1 \oplus e^{(1)}) \oplus u \cdot e^{(1)}} \\ &+ 2^{\frac{n+s_2}{2}}(-1)^{u \cdot v_2} \sum_{e^{(2)} \in E_2} (-1)^{f_{[2]}^*(v_2 \oplus e^{(2)}) \oplus u \cdot e^{(2)}} = 2^n(-1)^{f(u)} \end{aligned}$$

we have that the sums $\tilde{X}_i(u) = \sum_{e^{(i)} \in E_i} (-1)^{f_{[i]}^*(v_i \oplus e^{(i)}) \oplus u \cdot e^{(i)}}$ depend only on $u \in \Delta_i$, where $\Delta_i \oplus E_i^\perp = \mathbb{F}_2^n$ and $\Delta_i \cap E_i^\perp = \{\boldsymbol{0}_n\}$ (for both $i = 1, 2$). This is due to the fact that for any vector $\tilde{u} \in \mathbb{F}_2^n$ given as $\tilde{u} = u \oplus \kappa$, where $u \in \Delta_i$ and $\kappa \in E_i^\perp$, it holds that $\tilde{u}\cdot e = (u\oplus\kappa)\cdot e = u\cdot e$, and thus $\tilde{X}_i(\tilde{u}) = \tilde{X}_i(u)$.

(II): Let us now observe the duals $f^*_{[i]} : S_f^{[i]} \to \mathbb{F}_2$ and the terms $u \cdot e^{(i)}$ $(e^{(i)} \in E_i)$ in $\tilde{X}_i(u)$ $(i = 1,2)$. If $E_i = \{e_0^{(i)}, \ldots, e_{2^{\lambda_i}-1}^{(i)}\}$ satisfies the recursion of Lemma 3.1-(i), then it holds that $(u \cdot e_0^{(i)}, \ldots, u \cdot e_{2^{\lambda_i}-1}^{(i)})$ is the truth table of a linear function on $\mathbb{F}_2^{\lambda_i}$ $(i = 1,2)$. Thus, we can assume that for a fixed $u \in \mathbb{F}_2^n$ we have that

$$u\cdot e_j^{(1)} = \vartheta_u\cdot z_j \;\; (z_j \in \mathbb{F}_2^{\lambda_1}) \;\; \text{and} \;\; u\cdot e_j^{(2)} = \sigma_u\cdot y_j \;\; (y_j \in \mathbb{F}_2^{\lambda_2}),$$

for some vectors $\vartheta_u \in \mathbb{F}_2^{\lambda_1}$ and $\sigma_u \in \mathbb{F}_2^{\lambda_2}$ ($\mathbb{F}_2^{\lambda_i}$ ordered lexicographically). This consequently means that the equation $2^{\frac{n+s_1}{2}}(-1)^{u\cdot v_1}\tilde{X}_1(u) + 2^{\frac{n+s_2}{2}}(-1)^{u\cdot v_2}\tilde{X}_2(u) = 2^n(-1)^{f(u)}$ can be written as

$$2^{\frac{n+s_1}{2}}(-1)^{u\cdot v_1}W_{\overline{f}^*_{[1]}}(\vartheta_u)+2^{\frac{n+s_2}{2}}(-1)^{u\cdot v_2}W_{\overline{f}^*_{[2]}}(\sigma_u) = 2^n(-1)^{f(u)},$$

where we have defined $\overline{f}^*_{[i]} : \mathbb{F}_2^{\lambda_i} \to \mathbb{F}_2$ $(i = 1,2)$ so that

$$\overline{f}^*_{[1]}(z_j) = f^*_{[1]}(v_1 \oplus e_j^{(1)}) \; (z_j \in \mathbb{F}_2^{\lambda_1})$$

and

$$\overline{f}^*_{[2]}(y_j) = f^*_{[2]}(v_2 \oplus e_j^{(2)}) \; (y_j \in \mathbb{F}_2^{\lambda_2}).$$

(III): Inspired by the previous observation we will consider now $\xi_i : \Delta_i \to \mathbb{F}_2^{\lambda_i}$ $(i = 1,2)$ which will map the vector $u \in \mathbb{F}_2^n$ to $\mathbb{F}_2^{\lambda_i}$ such that $\xi_i(u) = \nu \in \mathbb{F}_2^{\lambda_i}$ if it holds that

$$(u \cdot e_0^{(i)}, \ldots, u \cdot e_{2^{\lambda_i}-1}^{(i)}) = (\nu \cdot z_0, \ldots, \nu \cdot z_{2^{\lambda_i}-1}), \tag{10}$$

where $z_j \in \mathbb{F}_2^{\lambda_i}$, $i = 1,2$. Clearly, the definition of ξ_i depends on the ordering of E_i, but it does not affect the analysis of the structure of f in general (since various orderings of E_i can be considered in the context of Lemma III.1). Hence, by Lemma III.1 the left side of (10) is the truth table of a linear function $\ell : \mathbb{F}_2^{\lambda_i} \to \mathbb{F}_2$ defined as $\ell(z) = \nu \cdot z$, $z \in \mathbb{F}_2^{\lambda_i}$. By Proposition IV.1 we have that ξ_i is injective and linear, and thus $\xi_i(\Delta_i) = \mathbb{F}_2^{\lambda_i}$.

(IV): Now, if we assume that $f^*_{[1]}$ and $f^*_{[2]}$ are totally disjoint spectra functions, then $\xi_i(\Delta_i) = \mathbb{F}_2^{\lambda_i}$ implies that the Walsh supports $S_{\overline{f}^*_{[i]}} \subset \mathbb{F}_2^{\lambda_i}$ have to be images of some subsets $U_i \subset \Delta_i$, i.e., it holds that $\xi_i(U_i) = S_{\overline{f}^*_{[i]}}$. Note that $U_i \neq \Delta_i$, since otherwise $U_i = \Delta_i$ (for some $i \in \{1,2\}$) implies that $S_{\overline{f}^*_{[i]}} = \xi_i(U_i) = \mathbb{F}_2^{\lambda_i}$, and this gives a contradiction to the assumption that $f^*_{[i]}$ are totally disjoint spectra functions (in this case (7) cannot be satisfied).

(V): Furthermore, since we have that $\xi_i(U_i) = \xi_i(U_i \oplus E_i^\perp)$ (due to observation **(I)**), then $f^*_{[i]}$ being totally disjoint spectra functions implies that it necessarily holds that $U_1 \oplus E_1^\perp$ and $U_2 \oplus E_2^\perp$ partition the space $\mathbb{F}_2^n$. This is due to the fact that for every $u \in \mathbb{F}_2^n$ we will always have that either $\xi_1(u) = \vartheta_u \in S_{\overline{f}^*_{[1]}}$ and $\xi_2(u) = \sigma_u \notin S_{\overline{f}^*_{[2]}}$, OR, $\xi_1(u) = \vartheta_u \notin S_{\overline{f}^*_{[1]}}$ and $\xi_2(u) = \sigma_u \in S_{\overline{f}^*_{[2]}}$.

(VI): In addition, we cannot say anything about the structure of U_i (its structure depends on $f^*_{[i]}$), except that $\#U_i = \#S_{\overline{f}^*_{[i]}} = 2^{\lambda_i - r_i}$ holds if $f^*_{[i]}$ are r_i-plateaued (even $\lambda_i - r_i = 0$ would be allowed, as indicated in Example III.1). However, one can deduce that $dim(\Delta_i) = dim(E_i) = \lambda_i$ together with $\Delta_i \oplus E_i^\perp = \mathbb{F}_2^n$ and $\Delta_i \cap E_i^\perp = \{\mathbf{0}_n\}$ (for both $i = 1,2$) imply that

$$\#(U_i \oplus E_i^\perp) = 2^{(\lambda_i - r_i)+(n-\lambda_i)} = 2^{n-r_i} = 2^{n-1},$$

since the equation $2^{n-r_1} + 2^{n-r_2} = 2^n$ has only one solution in r_i given by $r_1 = r_2 = 1$. This implies that λ_i have to be odd, since λ_i and r_i are of the same parity if $\overline{f}^*_{[i]}$ are r_i-plateaued functions.

The previous observations/conclusions describe necessary properties of totally disjoint spectra plateaued functions when employed for construction of 5-value spectrum functions (when $\#E_i = 2^{\lambda_i}$, Corollary 1). Before we formalize them (in form of a theorem whose proof is given in a more compact way), for convenience we introduce the following notation.

Notation $(\star)$**:** For a 5-value spectrum function $f : \mathbb{F}_2^n \to \mathbb{F}_2$ with $S_f = S_f^{[1]} \cup S_f^{[2]}$, assume that $S_f^{[i]}$ can be written in the form $S_f^{[i]} = v_i \oplus E_i = \{u \in \mathbb{F}_2^n : |W_f(u)| = 2^{\frac{n+s_i}{2}}\}$ $(s_1 > s_2 \geq 0)$, where E_i are linear subspaces with $dim(E_i) = \lambda_i$ and $v_i \in S_f^{[i]}$ $(i = 1,2)$. Additionally, let Δ_i be a linear subspace such that $\Delta_i \oplus E_i^\perp = \mathbb{F}_2^n$ and $\Delta_i \cap E_i^\perp = \{\mathbf{0}_n\}$, and let the function $\xi_i : \Delta_i \to \mathbb{F}_2^{\lambda_i}$ $(i = 1,2)$ be defined as in Proposition IV.1-(ii) where $E_i = \{e_0^{(i)}, \ldots, e_{2^{\lambda_i}-1}^{(i)}\}$ satisfy the recursion of Lemma III.1-(i) (Remark IV.2).

We recall that, by Corollary 1, the totally disjoint spectra duals $f^*_{[i]}$ are necessarily plateaued functions when $\#S_f^{[i]}$ are powers of 2.

Theorem IV.2. *Let **Notation** $(\star)$ hold. Then f is a basic 5-value spectrum function with totally disjoint spectra r_i-plateaued duals $\overline{f}^*_{[i]} : \mathbb{F}_2^{\lambda_i} \to \mathbb{F}_2$ (where $r_i + \lambda_i + s_i = n$, $r_i \geq 1$) if and only if the following holds:*

i) For some proper subsets $U_i \subset \Delta_i$ with $\#U_i = 2^{\lambda_i - r_i}$, it holds that $U_1 \oplus E_1^\perp$ and $U_2 \oplus E_2^\perp$ partition $\mathbb{F}_2^n$ and $S_{\overline{f}^*_{[i]}} = \xi_i(U_i)$ $(i = 1,2)$.

ii) $\#(U_i \oplus E_i^\perp) = 2^{n-1}$, or equivalently $r_1 = r_2 = 1$.

iii) λ_i are odd and $\lambda_1 \neq \lambda_2$.

Proof. $(\Rightarrow)$ $i)$ Let $u \in \mathbb{F}_2^n$ be an arbitrary vector. By observations **(III)** we have that $\xi_i(\Delta_i) = \mathbb{F}_2^{\lambda_i}$, and thus observation **(IV)** gives that for some subsets $U_i \subset \Delta_i$ (U_i are not necessarily affine subspaces) it necessarily holds that $S_{\overline{f}^*_{[1]}} = \xi_1(U_1)$ and $S_{\overline{f}^*_{[2]}} = \xi_2(U_2)$. Also note that $\#U_i = 2^{\lambda_i - r_i} = \#S_{\overline{f}^*_{[i]}} < \#\Delta_i$ ($f^*_{[i]}$ are r_i plateaued in λ_i variables) and $\xi_i(U_i \oplus E_i^\perp) = \xi_i(U_i) = S_{\overline{f}^*_{[i]}}$ holds for both $i = 1,2$ (observation **(V)**), i.e., the values of ξ_i are not affected by vectors from $E_i^\perp$.

Since $\overline{f}^*_{[i]}$ are totally disjoint spectra plateaued functions, that is $X_1(u)X_2(u) = 0$ and $|X_1(u)| + |X_2(u)| > 0$ hold for all $u \in \mathbb{F}_2^n$, the observation **(V)** is equivalent to the fact that the sets

$$S_{U_1} = \{u \in \mathbb{F}_2^n : X_1(u) \neq 0 \;\text{ and }\; X_2(u) = 0\},$$
$$S_{U_2} = \{u \in \mathbb{F}_2^n : X_1(u) = 0 \;\text{ and }\; X_2(u) \neq 0\},$$

have the property that $S_{U_1} \cup S_{U_2} = \mathbb{F}_2^n$ and $S_{U_1} \cap S_{U_2} = \emptyset$, i.e., S_{U_i} partition the space $\mathbb{F}_2^n$. This property clearly implies that $U_1 \cap U_2 = \emptyset$, since if there exists $u \in U_1 \cap U_2$, then $X_1(u) \neq 0$ and $X_2(u) \neq 0$ at the same time (due to $\xi_i(u) \in S_{\overline{f}^*_{[i]}}$ for both $i = 1, 2$), which contradicts to the previous conclusion.

We recall that $X_i(u) \neq 0$ (for fixed $i \in \{1, 2\}$) if and only if $u \in U_i \oplus E_i^{\perp}$, due to the fact that $S_{\overline{f}^*_{[i]}} = \xi_i(U_i \oplus E_i^{\perp}) = \xi_i(U_i)$ $(i = 1, 2)$. Since $\overline{f}^*_{[i]}$ are totally disjoint spectra, then $U_i \subseteq S_{U_i}$ $(i = 1, 2)$, and thus we further have that

$$\begin{aligned} S_{U_1} &= \{u \in \mathbb{F}_2^n : u \in (U_1 \oplus E_1^{\perp}) \cap ((\Delta_2 \setminus U_2) \oplus E_2^{\perp})\}, \\ S_{U_2} &= \{u \in \mathbb{F}_2^n : u \in (U_2 \oplus E_2^{\perp}) \cap ((\Delta_1 \setminus U_1) \oplus E_1^{\perp})\}. \end{aligned}$$

Clearly, we have that $S_{U_i} \subseteq U_i \oplus E_i^{\perp}$ $(i = 1, 2)$, and moreover, if we assume that for some $u \in \mathbb{F}_2^n$ it holds that $u \in (U_1 \oplus E_1^{\perp}) \cap (U_2 \oplus E_2^{\perp})$, then this contradicts the fact that $X_1(u)X_2(u) = 0$ (or $S_{U_1} \cap S_{U_2} = \emptyset$). Similarly, if there exists $u \in \mathbb{F}_2^n$ such that $u \notin (U_1 \oplus E_1^{\perp}) \cup (U_2 \oplus E_2^{\perp})$, then $X_1(u) = X_2(u) = 0$, which contradicts $|X_1(u)| + |X_2(u)| > 0$. Hence, we have that $U_i \oplus E_i^{\perp}$ partition the space $\mathbb{F}_2^n$.

The statement $ii)$ follows from observation **(VI)**, and $iii)$ follows from **(VI)** and the fact that $s_1 > s_2 \geq 0$ and $\lambda_i + s_i + 1 = n$ (Proposition III.2 with $r_i = 1$) imply that $\lambda_1 \neq \lambda_2$, and the proof is completed.

$(\Leftarrow)$ Let the conditions $(i) - (iii)$ hold. Then, condition (i) implies that for an arbitrary vector $u \in \mathbb{F}_2^n$ it holds that $X_1(u) \neq 0$ and $X_2(u) = 0$ when $u \in U_1 \oplus E_1^{\perp}$, or $X_1(u) = 0$ and $X_2(u) \neq 0$ when $u \in U_2 \oplus E_2^{\perp}$ (due to $S_{\overline{f}^*_{[i]}} = \xi_i(U_i)$). Thus, for all $u \in \mathbb{F}_2^n$ we have that $X_1(u)X_2(u) = 0$ and $|X_1(u)| + |X_2(u)| > 0$. This means that $\overline{f}^*_{[i]} : \mathbb{F}_2^{\lambda_i} \to \mathbb{F}_2$ are totally disjoint spectra functions, which are r_i-plateaued by Corollary 1 due to $dim(E_i) = \lambda_i$ and $dim(U_i) = \lambda_i - r_i$ $(i = 1, 2)$. □

Remark IV.3. *From the proof of Theorem IV.2 we clearly have that* $U_1 \cap U_2 = \xi_1^{-1}(S_{\overline{f}^*_{[1]}}) \cap \xi_2^{-1}(S_{\overline{f}^*_{[2]}}) = \emptyset$, *due to the fact that* $U_i \oplus E_i^{\perp}$ *(which contains* U_i*) partition the space* $\mathbb{F}_2^n$. *As mentioned in the proof, the sets* U_i *may not necessarily be affine subspaces, and their structure strictly depends on* $\overline{f}^*_{[i]}$.

Remark IV.4. *By [21], two functions, say* $f_1, f_2 : \mathbb{F}_2^{\lambda} \to \mathbb{F}_2$, *are said to satisfy the classical disjoint spectra property if* $W_{f_1}(u)W_{f_2}(u) = 0$ *holds for all* $u \in \mathbb{F}_2^{\lambda}$. *However, Theorem IV.2-*(iii) *implies that* $\overline{f}^*_{[1]}$ *and* $\overline{f}^*_{[2]}$ *cannot be classical disjoint spectra plateaued functions both defined on* $\mathbb{F}_2^{\lambda}$, *i.e. when* $\lambda = \lambda_1 = \lambda_2$. *In general, note that the totally disjoint spectra property allows that the functions* f_1, f_2 *are defined on domains of different dimensions.*

The following result provides a refinement of Theorem IV.2 in the case when $\overline{f}^*_{[i]}$ are basic plateaued functions.

Theorem IV.3. *Let* ***Notation*** $(\star)$ *hold. Then* $f : \mathbb{F}_2^n \to \mathbb{F}_2$ *is a basic 5-value spectrum function with totally disjoint spectra basic 1-plateaued duals* $\overline{f}^*_{[i]} : \mathbb{F}_2^{\lambda_i} \to \mathbb{F}_2$ $(1 + \lambda_i + s_i = n)$ *if and only if there exists a hyperplane* $A \subset \mathbb{F}_2^n$ *which can be represented as* $A = \overline{U}_i \oplus E_i^{\perp}$ *for* $i = 1, 2$, *where:*

i) The dimension of linear subspaces $E_i \subset \mathbb{F}_2^n$, *i.e.* $dim(E_i) = \lambda_i$ $(\lambda_1 \neq \lambda_2)$, *are odd integers.*

ii) $\overline{U}_i \subset \Delta_i$ $(dim(\overline{U}_i) = \lambda_i - 1)$ *are linear subspaces, where* $\Delta_i \oplus E_i^{\perp} = \mathbb{F}_2^n$ *and* $\Delta_i \cap E_i^{\perp} = \{\boldsymbol{0}_n\}$ $(i = 1, 2)$.

iii) There exists $\beta \in \mathbb{F}_2^n \setminus A$ *such that* $S_{\overline{f}^*_{[i]}} \subset \mathbb{F}_2^{\lambda_i}$ *are given by* $S_{\overline{f}^*_{[i]}} = \xi_i(U_i)$, *where* $U_1 = \overline{U}_1$, $U_2 = \beta \oplus \overline{U}_2$ *and* $\xi_i : U_i \to \mathbb{F}_2^{\lambda_i}$ $(i = 1, 2)$ *are defined as in Proposition IV.1-*(ii).

Proof. $(\Rightarrow)$ Recall that by Proposition IV.1-(ii) we have that $\xi_i : U_i \to \mathbb{F}_2^{\lambda_i}$ are linear injective mappings. Consequently, by Theorem IV.2-(i) we have that $S_{\overline{f}^*_{[i]}} = \xi_i(U_i)$ are affine spaces if and only if $U_i \subset \Delta_i$ are affine subspaces with $dim(U_i) = \lambda_i - 1$ $(r_i = 1)$. Here, λ_i are odd and different integers, due to Theorem IV.2-(iii).

By Theorem IV.2-$(i) - (ii)$ we have that $U_1 \oplus E_1^{\perp}$ and $U_2 \oplus E_2^{\perp}$ partition the space $\mathbb{F}_2^n$ and thus one of these sets is a hyperplane in $\mathbb{F}_2^n$, and other one is its coset. For instance, let $U_1 \oplus E_1^{\perp}$ be a hyperplane denoted by A, i.e. let $A = U_1 \oplus E_1^{\perp}$. Then by Theorem IV.2-$(i)$ we have that $\overline{U}_1 = U_1 \subset \Delta_1$ and $S_{\overline{f}^*_{[1]}} = \xi_1(\overline{U}_1)$.

On the other hand, since $U_2 \oplus E_2^{\perp}$ is a coset of A, it can be represented as $U_2 \oplus E_2^{\perp} = \beta \oplus A$, where $\beta \in \mathbb{F}_2^n \setminus A$. Since $E_2^{\perp}$ is strictly a linear subspace in $\mathbb{F}_2^n$, we have that $U_2 \subset \Delta_2$ is strictly an affine subspace. Clearly, since Δ_2 is a linear subspace, then U_2 can be represented as $U_2 = \beta \oplus \overline{U}_2$ for some linear subspace $\overline{U}_2$, and thus $A = (\beta \oplus U_2) \oplus E_2^{\perp} = \overline{U}_2 \oplus E_2^{\perp}$. Consequently, we have that $S_{\overline{f}^*_{[2]}} = \xi_2(\beta \oplus \overline{U}_2)$.

And finally, in order to prove that $\overline{U}_2$ is a linear subspace of Δ_2, we recall that $U_2 = \beta \oplus \overline{U}_2 \subset \Delta_2$. This implies that $\overline{U}_2 \subset \beta \oplus \Delta_2$, and if we assume that $\beta \notin \Delta_2$, then due to $\Delta_2 \cap E_2^{\perp} = \emptyset$ we have that $\beta \in E_2^{\perp}$. However, in this case we have that $A = \beta \oplus (U_2 \oplus E_2^{\perp}) = U_2 \oplus (\beta \oplus E_2^{\perp}) = U_2 \oplus E_2^{\perp}$. This contradicts to the fact that A is strictly a linear subspace and $U_2 \oplus E_2^{\perp}$ is strictly an affine subspace. Thus, it holds that $\beta \in \Delta_2$ and $\overline{U}_2 \subset \Delta_2$.

$(\Leftarrow)$ By Proposition IV.1 (and definition of ξ_i) we have that $S_{\overline{f}^*_{[1]}} = \xi_1(\overline{U}_1) = \xi_1(A)$ and $S_{\overline{f}^*_{[2]}} = \xi_2(\beta \oplus \overline{U}_2) = \xi_2(\beta \oplus A)$, and ξ_i (as injective linear functions) map the affine subspaces $\overline{U}_1$ and $\beta \oplus \overline{U}_2$ to $S_{\overline{f}^*_{[1]}} \subset \mathbb{F}_2^{\lambda_1}$ and $S_{\overline{f}^*_{[2]}} \subset \mathbb{F}_2^{\lambda_2}$ respectively. Thus, $S_{\overline{f}^*_{[i]}}$ are affine subspaces in $\mathbb{F}_2^{\lambda_i}$, which gives that $\overline{f}^*_{[i]}$ are basic plateaued functions. Now we prove that $\overline{f}^*_{[i]}$ are totally disjoint spectra functions.

Recall that $X_i(u) = \sum_{\omega \in S_f^{[i]}} (-1)^{f^*_{[i]}(\omega) \oplus u \cdot \omega}$, $i = 1, 2$. By given assumptions we have

$$\begin{cases} (-1)^{u \cdot v_1} X_1(u) = \sum\limits_{e \in E_1} (-1)^{f^*_{[1]}(v_1 \oplus e) \oplus u \cdot e} \neq 0 & \text{if and only if} \quad u \in A, \\ (-1)^{u \cdot v_2} X_2(u) = \sum\limits_{q \in E_2} (-1)^{f^*_{[2]}(v_2 \oplus q) \oplus u \cdot q} \neq 0 & \text{if and only if} \quad u \in \beta \oplus A. \end{cases}$$

Here, for $u \in A$ we have that the term $u \cdot e$ (for $e \in E_1$) corresponds to a term $\vartheta_u \cdot z$ $(z \in \mathbb{F}_2^{\lambda_1)})$ for which $\vartheta_u \in S_{\overline{f}^*_{[1]}} = \xi_1(\overline{U}_1) = \xi_1(A)$. Equivalently, by Proposition IV.1-(ii) we have that

$$\begin{cases} (-1)^{u \cdot v_1} X_1(u) = (-1)^{u \cdot v_1} X_1(\theta \oplus e') \neq 0 \text{ and } X_2(u) = 0 & \text{if and only if} \quad \theta \in U_1 \\ (-1)^{u \cdot v_2} X_2(u) = -1)^{u \cdot v_2} X_2(\rho \oplus e'') \neq 0 \text{ and } X_1(u) = 0 & \text{if and only if} \quad \rho \in U_2 \end{cases},$$

where $u = \theta \oplus e' \in A$ $(e' \in E_1^{\perp})$, or $u = \rho \oplus e'' \in \beta \oplus A$ $(e'' \in E_2^{\perp})$. Since we have that $\xi_1(\theta) = \vartheta_\theta \in S_{\overline{f}^*_{[1]}}$ and

$\xi_2(\rho) = \vartheta_\rho \in S_{\overline{f}^*_{[2]}}$, then the r_i-plateaued functions $\overline{f}^*_{[i]}$ are totally disjoint spectra functions. □

Hence, Theorems IV.2 and IV.3 provide a structural relation between the Walsh supports $S_{\overline{f}^*_{[i]}}$ and linear spaces E_i. It is important to emphasize that Theorem IV.2 also encompasses basic 5-value spectrum functions with non-basic plateaued dual functions $\overline{f}^*_{[i]}$.

We note that Theorem IV.3 can be utilized as a generic construction method for 5-value spectrum functions. In order to show how its conditions can be satisfied efficiently (which is further elaborated in Section IV-B), we provide a formal description of a spectral construction of 5-value spectrum functions which combines Theorems IV.3 and IV.1.

Theorem IV.4. *Let $A \subset \mathbb{F}_2^n$ $(i = 1, 2)$ be an arbitrary hyperplane with representations $A = \overline{U}_i \oplus E_i^\perp$, where $E_i \subset \mathbb{F}_2^n$ $(dim(E_i) = \lambda_i$, λ_i is odd) and $\overline{U}_i \subset \Delta_i$ $(dim(\overline{U}_i) = \lambda_i - 1)$ are linear subspaces such that $\Delta_i \oplus E_i^\perp = \mathbb{F}_2^n$, $\Delta_i \cap E_i^\perp = \{\mathbf{0}_n\}$ $(i = 1, 2)$. In addition:*

i) Let $\beta \notin A$ (thus $A \cup (\beta \oplus A) = \mathbb{F}_2^n$), and let λ_i be odd $(i = 1, 2)$.

ii) Let the affine Walsh supports $S_{\overline{f}^*_{[i]}} \subset \mathbb{F}_2^{\lambda_i}$ be given as

$$S_{\overline{f}^*_{[1]}} = \xi_1(\overline{U}_1) \ \ \textit{and} \ \ S_{\overline{f}^*_{[2]}} = \xi_2(\beta \oplus \overline{U}_2),$$

with $\#S_{\overline{f}^*_{[i]}} = \#\overline{U}_i = 2^{\lambda_i - 1}$ and $\xi_i : \overline{U}_i \to \mathbb{F}_2^{\lambda_i}$ $(i = 1, 2)$ being defined as in Proposition IV.1-(ii).

Then basic 1-plateaued functions $\overline{f}^*_{[i]}$ constructed by Theorem IV.1, with Walsh supports $S_{\overline{f}^*_{[i]}}$ and arbitrary bent duals $g_i : \mathbb{F}_2^{\lambda_i - r_i} \to \mathbb{F}_2$, are totally disjoint spectra functions which correspond to a 5-value spectrum function $f : \mathbb{F}_2^n \to \mathbb{F}_2$ with $S_f^{[i]} = v_i \oplus E_i$ and duals $f^*_{[i]}$.

Remark IV.5. *Theorem IV.4 emphasizes that by having affine Walsh supports $S_{\overline{f}^*_{[i]}}$ one can always (by Theorem IV.1) utilize arbitrary bent duals g_i in order to construct plateaued dual functions $f^*_{[i]}$ $(i = 1, 2)$.*

Hence, Theorems IV.2 and IV.3 provide a characterization of basic 5-value spectrum functions, where $f^*_{[i]}$ are totally disjoint spectra plateaued functions. The functions $f^*_{[i]}$ are basic plateaued functions when U_i are affine subspaces (Theorem IV.2), or equivalently when $\overline{U}_i$ are linear subspaces (in Theorems IV.3 and IV.4). As an interesting open problem we leave the constructions of 5-value spectrum functions using Theorem IV.2 with non-basic plateaued duals $\overline{f}^*_{[i]}$.

B. Satisfying the conditions of Theorem IV.3

In this section we present a construction method of 5-value spectrum functions based on totally disjoint property. The main idea is to choose a hyperplane A and $\beta \in \mathbb{F}_2^n$ such that $A \cup (\beta \oplus A) = \mathbb{F}_2^n$ (clearly $\beta \notin A$). Then we find two suitable representation of A as $A = \overline{U}_i \oplus \Theta_i$ (which one can always do), where we simply have that $E_i^\perp = \Theta_i$ (E_i are linear spaces). In this process we follow and satisfy the conditions of Theorems IV.2, IV.3 and IV.4.

Proposition IV.2. *Let $A \subset \mathbb{F}_2^n$ be a hyperplane and $\beta \in \mathbb{F}_2^n$, such that $\beta \notin A$. Let the linear subspaces $\overline{U}_i, \Theta_i \subset A$ $(i = 1, 2)$ be chosen such that*

$$\begin{cases} A = \overline{U}_i \oplus \Theta_i, \quad \overline{U}_i \cap \Theta_i = \{\mathbf{0}_n\} \\ \#\Theta_i^\perp = 2^{\lambda_i}, \ \textit{where} \ \ \lambda_i \geq 1 \ \ \textit{are odd.} \end{cases} \tag{11}$$

Then, the linear subspaces $\overline{U}_i$ and $E_i = \Theta_i^\perp$ satisfy the properties of Theorem IV.3.

Proof. Since the Walsh support $S_{\overline{f}^*_{[i]}} \subset \mathbb{F}_2^{\lambda_i}$ of a 1-plateaued function $\overline{f}^*_{[i]} : \mathbb{F}_2^{\lambda_i} \to \mathbb{F}_2$ is of the size $\#S_{\overline{f}^*_{[i]}} = 2^{\lambda_i - 1}$ and λ_i are odd, then $\lambda_i - 1$ are even $(\lambda_i - 1 \geq 0)$, and by (11) the subspaces $\overline{U}_i$ can be used as preimages of functions ξ_i, i.e., $\overline{U}_i$ are suitable for defining Walsh supports $S_{\overline{f}^*_{[1]}} = \xi_1(\overline{U}_1)$ and $S_{\overline{f}^*_{[2]}} = \xi_2(\beta \oplus \overline{U}_2)$. Also, by (11) it is clear that $\overline{U}_i \subset \Delta_i$, where the linear subspace Δ_i satisfies the property $\Delta_i \oplus \Theta_i = \mathbb{F}_2^n$ and $\Delta_i \cap \Theta_i = \{\mathbf{0}_n\}$ $(i = 1, 2)$. □

Remark IV.6. *We note that the role of vectors $v_i \in \mathbb{F}_2^n$, where $S_f^{[i]} = v_i \oplus E_i$, is to provide the disjoint property of sets E_i obtained in Proposition IV.2.*

In what follows, we provide a construction of a 5-value spectrum function on $n = 5$ variables with amplitudes $2^{\frac{5+1}{2}} = 8$ and $2^{\frac{5+3}{2}} = 16$. Deliberately, we will consider the extremal case when $\#E_1 = 2$ which does not give many possibilities for such a 5-value Walsh spectra. Clearly, for larger n, $dim(E_i)$ could be chosen larger. Then the same procedure provides much bigger variety of constructions thanks to the availability of many more bent duals $g_i : \mathbb{F}_2^{\lambda_i - r_i} \to \mathbb{F}_2$ of $\overline{f}^*_{[i]}$ (Theorem IV.3) and space decompositions.

Example IV.2. *Let us construct the spectrum W_f by relation (5) which will in turn give a 5-value spectrum function f : $\mathbb{F}_2^5 \to \mathbb{F}_2$ $(n = 5)$. By $b_1, \ldots, b_5 \in \mathbb{F}_2^5$ we denote the canonical basis of $\mathbb{F}_2^5$, where the only non-zero coordinate of b_i is at i-th position, $i \in [1, 5]$.*

For simplicity, let $A = \{z \in \mathbb{F}_2^5 : z \cdot b_5 = 0\}$ be a hyperplane $(dim(A) = 4)$, and by $\beta = b_5$ we have that $A \cap (\beta \oplus A) = \emptyset$. In addition, since by Proposition IV.2 we have to choose $E_i = \Theta_i^\perp \subset \mathbb{F}_2^5$ such that $\#E_i$ is an odd power of 2 (Theorem IV.2), we may choose the values

$$\lambda_1 = 1 \ \ \textit{and} \ \ \lambda_2 = 3,$$

for which it holds that $\#E_1 + \#E_2 = 2^{\lambda_1} + 2^{\lambda_2} = 2^1 + 2^3 < 2^5$. This immediately gives that the dimensions of $\overline{U}_i$ and $\Theta_i = E_i^\perp$ in the decomposition $A = \overline{U}_i \oplus \Theta_i$ are given as

$$dim(\overline{U}_1) = 0, \quad dim(\Theta_1) = 5 - \lambda_1 = 4,$$

$$dim(\overline{U}_2) = 2, \quad dim(\Theta_2) = 5 - \lambda_2 = 2,$$

since we have that $dim(\overline{U}_i) + dim(\Theta_i) = n - 1 = 4 = dim(A)$. We necessarily have that $\overline{U}_1 = \{\mathbf{0}_5\}$ and $\Theta_1 = A$, which implies that

$$E_1 = \Theta_1^\perp = A^\perp = \{\mathbf{0}_5, b_5\}.$$

Furthermore, we can choose $\overline{U}_2$ and Θ_2 as

$$\overline{U}_2 = \langle (0, 1, 0, 1, 0), (0, 1, 1, 0, 0) \rangle,$$

$$\Theta_2 = \langle (1,0,0,0,0), (1,0,0,1,0) \rangle.$$

One can verify that $\overline{U}_2 \oplus \Theta_2 = A$ *and* $\overline{U}_2 \cap \Theta_2 = \{\boldsymbol{0}_5\}$*. Thus, we have that* E_2 *is given as*

$$E_2 = \Theta_2^{\perp} = \langle b_2, b_3, b_5 \rangle.$$

Now we proceed with construction of suitable 1*-plateaued functions* $\overline{f}^*_{[i]} : \mathbb{F}_2^{\lambda_i} \to \mathbb{F}_2$ $(i = 1, 2)$*. Firstly, the fact that* $\#E_1 = 2$ *implies that* $\overline{f}^*_{[1]}$ *can be any function defined on* $\mathbb{F}_2$ *(Remark III.5). Thus, we may set that* $\overline{f}^*_{[1]}(x_1) = 0$ *for* $x_1 \in \mathbb{F}_2$*. This actually gives that* $S_{\overline{f}^*_{[1]}} = \{0\} \subset \mathbb{F}_2$*.*

On the other hand, by setting that E_2 *is ordered lexicographically, we compute* $\xi_2(\beta \oplus \overline{U}_2) = S_{\overline{f}^*_{[2]}} \subset \mathbb{F}_2^3$ *(where* ξ_2 *is defined as in Proposition IV.1 and* $\beta = b_5$*), and we get*

$$S_{\overline{f}^*_{[2]}} = \xi_2(\beta \oplus \overline{U}_2) = \{(0,0,1), (1,1,1), (1,0,1), (0,1,1)\}.$$

With respect to this ordering of $S_{\overline{f}^*_{[2]}}$ *(being in a basic way compatible with Lemma III.1), we can choose the dual* $g : \mathbb{F}_2^2 \to \mathbb{F}_2$ *of* $\overline{f}^*_{[2]}$ *to be defined as* $g_1(x_1, x_2) = x_1 x_2$ $(T_g = (0,0,0,1))$*, i.e., we take that*

$$\overline{f}^*_{[2]}(0,0,1) = g(0,0) = 0, \quad \overline{f}^*_{[2]}(1,1,1) = g(0,1) = 0,$$
$$\overline{f}^*_{[2]}(1,0,1) = g(1,0) = 0, \quad \overline{f}^*_{[2]}(0,1,1) = g(1,1) = 1.$$

Consequently, by relation (5) we obtain the function $\overline{f}^*_{[2]}(x_1, x_2, x_3) = x_1 \oplus x_1 x_2 \oplus x_3$*.*

At the end, we have to choose $v_1, v_2 \in \mathbb{F}_2^5$ *such that* $(v_1 \oplus E_1) \cap (v_2 \oplus E_2) = \emptyset$ *(Remark IV.6). For instance, one can choose* $v_1 = \boldsymbol{0}_6$ *and* $v_2 = (0,0,1,1,0)$*, and thus by defining* $S_f^{[1]} = E_1$ *and* $S_f^{[2]} = v_2 \oplus E_2$ *and relation (5) (for lexicographically ordered* E_i*) the spectrum* $W_f = (W_f(u_0), \ldots, W_f(u_{2^5-1}))$ *is given as*

$$W_f = (16, 16, 8, -8, 0, 0, 8, -8, 0, 0, 8, -8, 0, 0, -8, 8, 0, \ldots, 0).$$

Note that the higher amplitude 16 *is associated with the set* $S_f^{[1]}$ *and lower amplitude* 8 *with* $S_f^{[2]}$*. Inverting the spectrum* W_f *we obtain a 5-value spectrum function* $f : \mathbb{F}_2^5 \to \mathbb{F}_2$ *given as*

$$f(x_1, \ldots, x_5) = x_2 x_3 x_5 \oplus x_4 x_5.$$

We note that basic 5-value spectrum functions constructed by Theorem IV.4 and Proposition IV.2 possess a lot of diversity, since one can choose arbitrary bent functions in lower number of variables (as duals of $\overline{f}^*_{[i]}$) and consider various decompositions of the hyperplane A. In this context, these two results represent a generic construction of totally disjoint plateaued functions which can be utilized for construction of basic 5-value spectrum functions. In the next subsection we briefly analyse the notion of linear structures of 5-value spectrum functions, with respect to the spectral design approach.

C. On linear structures of 5-value spectrum functions

First we recall the definition of a linear structure of a Boolean function.

Definition IV.1. *A function* $f : \mathbb{F}_2^n \to \mathbb{F}_2$ *is said to possess a linear structure* $\alpha \in \mathbb{F}_2^n$ *if* $f(\alpha \oplus x) \oplus f(x) = c$ *holds for all* $x \in \mathbb{F}_2^n$*, for some* $c \in \mathbb{F}_2$*. The vector* α *is called an invariant linear structure if* $c = 0$*, and a complementary linear structure when* $c = 1$*.*

We note that the function $f(x_1, \ldots, x_5) = x_2 x_3 x_5 \oplus x_4 x_5$ constructed in Example IV.2 does have a single invariant non-zero linear structure $(1,0,0,0,0)$. This is visible from the fact that x_1 is not present in the ANF of f. The main question in this context is whether one can construct 5-value spectrum functions without non-zero linear structures using the spectral approach.

To address this question most efficiently, in terms of the spectral approach, we recall the following result.

Theorem IV.5. *[12] A function* $f : \mathbb{F}_2^n \to \mathbb{F}_2$ *admits at least one (non-zero) linear structure if and only if the smallest affine subspace which contains* S_f *is different from* $\mathbb{F}_2^n$*.*

Since the largest affine subspace different from $\mathbb{F}_2^n$ is of cardinality 2^{n-1}, by Theorem IV.5 we have that a 5-value spectrum function does not have non-zero linear structures if it holds that

$$\#S_f = \#S_f^{[1]} + \#S_f^{[2]} > 2^{n-1}.$$

The case $\#S_f = 2^{n-1}$ is possible if and only if S_f is not affine subspace in $\mathbb{F}_2^n$. Regarding 5-value spectrum functions with totally disjoint spectra duals, by Theorem IV.2 we have that $\#S_f = 2^{\lambda_1} + 2^{\lambda_2}$ $(\#S_f^{[i]} = 2^{\lambda_i}$, $i = 1, 2)$, where λ_1 and λ_2 are odd and different. However, by [2, Lemma B.1] it is not difficult to see that the equality $2^{\lambda_1} + 2^{\lambda_2} = 2^{n-1}$ can not be satisfied when n is even.

As the condition $\#S_f = \#S_f^{[1]} + \#S_f^{[2]} > 2^{n-1}$ can be easily satisfied in terms of the spectral approach in general, the question is whether it can be satisfied in Theorem IV.4 and Proposition IV.2. The following example indicates that for certain values of n the necessary requirements are indeed fulfilled.

Example IV.3. *Let us consider the 5-value spectrum function* $d : \mathbb{F}_2^6 \to \mathbb{F}_2$ *given as*

$$d(x_1, \ldots, x_6) = x_4 x_5 \oplus x_1 x_6 \oplus x_2 x_3 x_6 \oplus x_4 x_6.$$

One can verify that the function d *is a 5-value spectrum functions with totally disjoint spectra functions, whose structure satisfies Theorem IV.4 and Proposition IV.2. In the context of Theorem IV.5, one can check that* d *does not have non-zero linear structures, since* $\#S_d = 40 > 2^{6-1} = 32$*.*

Remark IV.7. *It can be readily verified that the only possibilities for* λ_1 *and* λ_2 *in Example IV.2 are* 1 *and* 3*. Therefore, the cardinality of the Walsh support of* $f(x_1, \ldots, x_5) = x_2 x_3 x_5 \oplus x_4 x_5$ *is smaller than* $2^{n-1} = 16$*, and thus* f *admits non-zero linear structures.*

In the next subsection we further analyse the equivalence of 5-value functions constructed by Theorem IV.4 and Proposition IV.2.

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/TIT.2020.3044059, IEEE Transactions on Information Theory

D. On equivalence of basic 5-value spectrum functions

Let $f,h : \mathbb{F}_2^n \to \mathbb{F}_2$ be two affine equivalent 5-value spectrum functions, that is $h(x) = f(xA \oplus b) \oplus c \cdot x \oplus \varepsilon$, for some matrix $A \in GL(n,\mathbb{F}_2)$, vectors $b, c \in \mathbb{F}_2^n$ and $\varepsilon \in \{0,1\}$. For any $u \in \mathbb{F}_2^n$, we have that

$$\begin{aligned} W_h(u) &= \sum_{x\in\mathbb{F}_2^n} (-1)^{f(xA\oplus b)\oplus c\cdot x\oplus\varepsilon\oplus u\cdot x} \\ &= \sum_{y\in\mathbb{F}_2^n} (-1)^{f(y)\oplus(u\oplus c)A^{-T}\cdot y\oplus(u\oplus c)\cdot bA^{-1}\oplus\varepsilon} \\ &= \begin{cases} 2^{\frac{n+s_i}{2}}(-1)^{f^*_{[i]}((u\oplus c)A^{-T})\oplus(u\oplus c)\cdot bA^{-1}\oplus\varepsilon}, & (u\oplus c)A^{-T} \in S_f^{[i]} \\ 0, & (u\oplus c)A^{-T} \notin S_f \end{cases} \\ &= \begin{cases} 2^{\frac{n+s_i}{2}}(-1)^{h^*_{[i]}(u)}, & (u\oplus c)A^{-T} \in S_f^{[i]} \\ 0, & (u\oplus c)A^{-T} \notin S_f \end{cases} \end{aligned} \quad (12)$$

where $S_f = S_f^{[1]} \cup S_f^{[2]}$, and $S_f^{[i]} = \{z \in \mathbb{F}_2^n : |W_f(z)| = 2^{\frac{n+s_i}{2}}\}$, $s_1 > s_2 \geq 0$. From (12), we have that $S_h^{[i]} = c \oplus S_f^{[i]} A^T$ $(i = 1,2)$ and consequently

$$h^*_{[i]}(u) = f^*_{[i]}((u\oplus c)A^{-T}) \oplus (u \oplus c)\cdot bA^{-1} \oplus \varepsilon.$$

Using the ideas given in [14, Theorem 3.2], one can deduce the following results that describe the equivalence of basic 5-value spectrum functions whose duals are basic plateaued functions. We note that the arguments and computations used in the proof of [14, Theorem 3.2] do not depend on the property of the duals $\overline{f}^*_{[i]}$ and $\overline{h}^*_{[i]}$, i.e., whether they are plateaued or not.

Theorem IV.6. *Let $f,h : \mathbb{F}_2^n \to \mathbb{F}_2$ be two basic 5-value spectrum functions whose Walsh supports $S_f = S_f^{[1]} \cup S_f^{[2]}$ and $S_h = S_h^{[1]} \cup S_h^{[2]}$ are related as $S_h^{[i]} = c \oplus S_f^{[i]} M$ $(i = 1,2)$, for some matrix $M \in GL(n,\mathbb{F}_2)$ and $c \in \mathbb{F}_2^n$. Representing $S_f^{[i]} = v_i \oplus E_i = \{\omega_i = v_i \oplus e_j^{(i)} : e_j \in E_i\}$ for a lexicographically ordered linear space $E = \{e_0^{(i)}, \ldots, e_{2^{\lambda_i}-1}^{(i)}\}$, let $\overline{f}^*_{[i]}$ and $\overline{h}^*_{[i]}$ be two functions defined as*

$$\overline{f}^*_{[i]}(x_j) = f^*_{[i]}(\omega_j) \ \ and \ \ \overline{h}^*_{[i]}(x_j) = h^*_{[i]}(z_j), \quad (i \in [0, 2^{\lambda_i} - 1]), \quad (13)$$

where $z_j = c \oplus \omega_j M \in S_h^{[i]}$. Then f and h are EA-equivalent if and only if the duals of $\overline{f}^*_{[i]}, \overline{h}^*_{[i]} : \mathbb{F}_2^{\lambda_i} \to \mathbb{F}_2$ are EA-equivalent functions.

We note that Theorem IV.6 does not impose any conditions on the duals $\overline{f}^*_{[i]}$ and $\overline{h}^*_{[i]}$. Thus we have the following consequence related to plateaued dual functions.

Corollary 2. *Let the notation of Theorem IV.6 hold. If $\overline{f}^*_{[i]}, \overline{h}^*_{[i]} : \mathbb{F}_2^{\lambda_i} \to \mathbb{F}_2$ are r_i-plateaued functions, then f and h are EA-equivalent if and only if the duals of $\overline{f}^*_{[i]}, \overline{h}^*_{[i]}$ are EA-equivalent bent functions on $\mathbb{F}_2^{\lambda_i - r_i}$.*

Following [14, Theorem 3.1-(i)], we have that f and h (being 5-value spectrum functions, basic or not) are not equivalent if S_h and S_f cannot be related in an affine manner as $S_h = c \oplus S_f M$, for some $M \in GL(n,\mathbb{F}_2)$ and $c \in \mathbb{F}_2^n$. Also, one easily obtains the following result which is a direct consequence of (12) and the fact that $\#S_h^{[i]} = \#(c \oplus S_f^{[i]} M)$, for any $M \in GL(n,\mathbb{F}_2)$ and $c \in \mathbb{F}_2^n$.

Corollary 3. *Let $f,h : \mathbb{F}_2^n \to \mathbb{F}_2$ be two 5-value spectrum function with Walsh supports $S_f = S_f^{[1]} \cup S_f^{[2]}$ and $S_h = S_h^{[1]} \cup S_h^{[2]}$. Then:*

i) If for at least one $i \in \{1,2\}$ it holds that $\#S_h^{[i]} \neq \#S_f^{[i]}$, then f and h are inequivalent functions.

ii) If for at least one $i \in \{1,2\}$ the sets $S_h^{[i]}$ and $S_f^{[i]}$ cannot be related in an affine manner, then f and h are inequivalent functions.

Remark IV.8. *Note that the spectral construction method of 5-value spectrum functions presented in Sections IV-A and IV-B allows the construction of many inequivalent 5-value spectrum functions (via Corollary 3), just with setting that $\#S_h^{[i]} \neq \#S_f^{[i]}$ (for at least one $i = 1,2$). Regarding Corollary-(ii) we can see that if for instance $S_h^{[i]}$ is an affine space and $S_f^{[i]}$ is not an affine space (for at least one $i \in \{1,2\}$), then f and h are affine inequivalent.*

In the context of Proposition IV.2, one can notice that different decompositions of a hyperplane A as $A = U_i \oplus E_i^{\perp}$ may imply inequivalent 5-value spectrum functions, as described below.

Proposition IV.3. *Let $f,h : \mathbb{F}_2^n \to \mathbb{F}_2$ be two 5-value spectrum functions constructed by Proposition IV.2, by choosing the same hyperplane $A \subset \mathbb{F}_2^n$. Assume that A has two different (decomposition) representations given by $A = U_i \oplus E_i^{\perp}$ and $A = \tilde{U}_i \oplus \tilde{E}_i^{\perp}$, with conditions in (11) being satisfied. Assume that $\#E_i = 2^{\lambda_i}$ and $\#\tilde{E}_i = 2^{m_i}$ (λ_i, m_i are odd, $i = 1,2$). Then:*

i) If $(2^{\lambda_1}, 2^{\lambda_2}) \notin \{(2^{m_1}, 2^{m_2}), (2^{m_2}, 2^{m_1})\}$, then f and h are EA-inequivalent.

ii) Let $(2^{\lambda_1}, 2^{\lambda_2}) = (2^{m_1}, 2^{m_2})$. Then, f and h are EA-equivalent if and only if $\overline{f}^*_{[i]}$ and $\overline{h}^*_{[i]}$ are EA-equivalent plateaued functions for both $i = 1,2$.

Proof. Suppose that the hyperplane A has two decompositions $A = U_i \oplus E_i^{\perp}$ and $A = \tilde{U}_i \oplus \tilde{E}_i^{\perp}$. By Proposition III.2, we always have that $\lambda_i + s_i + r_i = n$ $(r_i = 1)$ and $m_i + s_i + \tilde{r}_i = n$ $(\tilde{r}_i = 1)$, where we assume that the duals of f are r_i-plateaued functions, and the duals of h are $\tilde{r}_i$-plateaued functions. These conditions imply that λ_i and m_i are related to parameters s_i (which determine the amplitudes of f and h), i.e., we have that the dimension of $dim(E_i) = \lambda_i$ and $dim(\tilde{E}_i) = m_i$ affect the values of s_i. In this context, using (12), we always have that the Walsh supports $S_h^{[i]}$ and $S_f^{[i]}$ are related in an affine way via the same amplitude $2^{\frac{n+s_i}{2}}$. However, if f and h are EA-equivalent, then $\lambda_i + s_i + r_i = n$ $(r_i = 1)$ and $m_i + s_i + \tilde{r}_i = n$ mean that $(2^{\lambda_1}, 2^{\lambda_2})$ has to be equal to either $(2^{m_1}, 2^{m_2})$ or, to $(2^{m_2}, 2^{m_1})$. Thus, if $(2^{\lambda_1}, 2^{\lambda_2}) \notin \{(2^{m_1}, 2^{m_2}), (2^{m_2}, 2^{m_1})\}$, then by Corollary 3-$(i)$ we have that f and h are EA-inequivalent. The second statement uses the same arguments and Corollary 2. □

On the other hand, it is very important to emphasize the relation between Theorem IV.6 and the results presented in Section V. Namely, one can notice that the relation between S_h and S_f is affine (in Theorem IV.6), and with respect to this relation we have defined in (13) the functions $f^*_{[i]}$ and $h^*_{[i]}$ on $\mathbb{F}_2^{\lambda_i}$. It is clear that any two affine subspaces $S_h^{[i]}$ and $S_f^{[i]}$ can be related in an affine manner, but in that case the equivalence between f and h will then depend on their duals $f^*_{[i]}$ and $h^*_{[i]}$.

Now, Theorem V.2 derived later on in Section V-B actually clarifies the following important property, that is, whatever is the definition of $f^*_{[i]}$ and $h^*_{[i]}$ on $\mathbb{F}_2^{\lambda_i}$ with respect to $S_f^{[i]} = v_i \oplus E_i$ and $S_h^{[i]} = \tilde{v}_i \oplus \tilde{E}_i$, as long as E_i and $\tilde{E}_i$ satisfy the recursion of Lemma III.1 (as mentioned in Remark IV.1), the duals $\overline{f}^*_{[i]}$ and $\overline{h}^*_{[i]}$ will be EA-equivalent plateaued functions. This simply means that inequivalent bent dual functions of $\overline{f}^*_{[i]}$ and $\overline{h}^*_{[i]}$ can be utilized in the spectral construction approach in order to get inequivalent 5-value spectrum functions (for any ordering of E_i and $\tilde{E}_i$ in terms of Lemma III.1). In fact, already the inequivalence of one dual, e.g. $\overline{f}^*_{[1]}$ is inequivalent to $\overline{h}^*_{[1]}$, is sufficient to imply the inequivalence between f and h.

The relation between different duals defined through different orderings of an underlying set in terms of Lemma III.1 (whether we are considering duals of basic 5-value functions, or duals of plateaued functions) has not been studied in [13], [14]. This relation will be investigated in detail in the following section.

V. On different duals of plateaued functions

In order to describe the structure and the main objectives of this section, we firstly provide necessary settings.

Let $A = \{a_0, a_1, ..., a_{2^t-1}\}$ be a set. By saying that A is ordered with respect to a linear ordering $\prec$, or simply A is ordered by $\prec$, we mean that $a_i \prec a_j$ if $i < j$. We recall that the notion of the lexicographic order is used in the standard sense. Let $E = \{e_0, e_1, \dots, e_{2^k-1}\}$ be a set ordered by $\prec$ and $v \in \mathbb{F}_2^n$. If not stated otherwise, then the ordering $\ll$ of the set $T = v \oplus E = \{\omega_0, \dots, \omega_{2^k-1}\}$, where $\omega_i = v \oplus e_i$, will be induced by the ordering $\preceq$ of E, i.e., $\omega_i \ll \omega_j$ if $e_i \prec e_j$.

Let $f : \mathbb{F}_2^n \to \mathbb{F}_2$ be an s-plateaued function with dual $f^* : S_f \to \mathbb{F}_2$ and an affine subspace $S_f \subset \mathbb{F}_2^n$. In order to represent S_f as $S_f = v \oplus E$ as described in [13, Section 2.1] (with a linear subspace E), we first choose an arbitrary vector $v \in S_f$. Then, for the fixed vector $v \in S_f$, we obtain the set E by computing $E = v \oplus S_f$. If the linear space $E = \{e_0, e_1, \dots, e_{2^k-1}\}$ (where $k = n - s$) is ordered lexicographically, then the ordering $\ll$ induced on $S_f = \{\omega_0, \dots, \omega_{2^k-1}\}$ implies that $\omega_i = v \oplus e_i \ll \omega_j = v \oplus e_j$ if $e_i < e_j$ ($i \in [0, 2^k - 1]$), i.e., we have that S_f is ordered as

$$S_f = \{\omega_0, \dots, \omega_{2^k-1}\} = \{v \oplus e_0, v \oplus e_1, \dots, v \oplus e_{2^k-1}\}.$$

Additionally, we note that the induced ordering $\ll$ of S_f is not in general a lexicographic order although the ordering on E is.

With respect to the fixed representation $S_f = v \oplus E$, we define the dual f^* as a function on the lexicographically ordered space $\mathbb{F}_2^k = \{x_0, \dots, x_{2^k-1}\}$ such that $\overline{f}^*(x_i) = f^*(v \oplus e_i) = f^*(\omega_i)$, where $x_i \in \mathbb{F}_2^k$ (see [13, Section 2.1]).

As stated above, for the affine space S_f there exists a unique linear subspace E such that $S_f = v \oplus E$. It is very well known that S_f can be represented as $S_f = w \oplus E$ for any element $w \in S_f$. However, we point out that for $v_1 \neq v_2 \in S_f$, the orderings of $S_f = v_1 \oplus E$ and $S_f = v_2 \oplus E$ induced by the ordering of E are different orderings of S_f. So, each representation of S_f in the form $S_f = v \oplus E$, $v \in S_f$ leads to a different ordering of S_f.

Obviously, these different orderings of S_f induce two different duals $\overline{f}^*_1$ and $\overline{f}^*_2$ defined on $\mathbb{F}_2^k$. By Lemma 3.1 and Theorem IV.1 one can easily verify that both duals are bent functions on $\mathbb{F}_2^k$. The main objective of this section is to answer the following questions:

Q1: What is the importance and role of the lexicographic ordering in defining a dual f^* (of a plateaued function) as a function $\overline{f}^* : \mathbb{F}_2^k \to \mathbb{F}_2$ in comparison to other possible orderings which satisfy the recursion given in Lemma III.1 (these orderings necessarily imply bentness of $\overline{f}^*$, when E is a linear subspace)?

Q2: Let $\overline{f}^*_1$ and $\overline{f}^*_2$ be duals of an s-plateaued function $f : \mathbb{F}_2^n \to \mathbb{F}_2$ obtained by two different orderings of S_f induced by representations $S_f = v_1 \oplus E$ and $S_f = v_2 \oplus E$, respectively (that is $\overline{f}^*_i(x_j) = f^*(v_i \oplus e_j)$, $x_j \in \mathbb{F}_2^k$, $e_j \in E$, $n - s = k$). Are then the duals $\overline{f}^*_1$ and $\overline{f}^*_2$ affine equivalent? In other words, does there exists $A_{k\times k} \in GL(k, \mathbb{F}_2)$ and $c \in \mathbb{F}_2^k$ such that $\overline{f}^*_1(xA_{k\times k} \oplus c) = \overline{f}^*_2(x)$ ($x \in \mathbb{F}_2^k$)?

In the rest of this section the questions **Q1** and **Q2** will be answered by a thorough analysis of the properties of dual functions. Note that at the end of Subsection IV-D the main consequences of **Q1** and **Q2** have been discussed for 5-value spectrum functions.

A. Answering *Q1*

We start by recalling some of the main parts of the proof of [13, Theorem 3.1]. Let f be an s-plateaued function with $S_f = v \oplus E$, where $v \in S_f$ and $\#E = 2^{n-s}$. For any $u \in \mathbb{F}_2^n$, by the inverse WHT (1) we have that

$$\sum_{e\in E}(-1)^{f^*(v\oplus e)\oplus u\cdot e} = 2^{\frac{n-s}{2}}(-1)^{f(u)}.$$

If we want to define f^* as a function on $\mathbb{F}_2^{n-s}$, then one has to impose an ordering on E. If we take that E has "some" ordering (not necessarily lexicographic) given as $E = \{e_0, \dots, e_{2^k-1}\}$ ($k = n - s$), then the previous equation (by setting $f^*(v \oplus e_i) = \overline{f}^*(x_i)$, $x_i \in \mathbb{F}_2^k$) is given as

$$\sum_{i=0}^{2^k-1}(-1)^{\overline{f}^*(x_i)\oplus u\cdot e_i} = 2^{\frac{k}{2}}(-1)^{f(u)}.$$

Clearly, $\overline{f}^*$ is bent on $\mathbb{F}_2^k$ if and only if $\Omega_f = \{(u \cdot e_0, \dots, u \cdot e_{2^k-1}) : u \in \mathbb{F}_2^n\}$ contains truth tables of all linear functions in k variables, i.e., $\Lambda_k = \{T_\ell : \ell \in \mathcal{L}_k\} \subset \Omega_f$. In general, Ω_f may contain truth tables of non-linear functions, and this depends on the structure and ordering of the set E.

However, if we consider $(u \cdot e_0, \dots, u \cdot e_{2^k-1})$, then by Lemma III.1 and the assumption that E is a linear space, we have that $\Lambda_k \subset \Omega_f$ if the ordering of the space E satisfies the recursion $e_j = e_{j-2^i} \oplus e_{2^i}$, for all $2^i \leq j \leq 2^{i+1} - 1$ and $i \in \{0, \dots, k-1\}$. On the other hand, among many orderings that one can impose on E, we have that the lexicographic ordering is an example of ordering which satisfies this recursion (and lexicographic ordering has been used in several works [13]–[15]). For instance, if we take that $E = \{e_0, \dots, e_{2^k-1}\}$ is ordered lexicographically, then for an arbitrary matrix $D \in GL(n, \mathbb{F}_2)$ we have that $ED = \{e_0 D, \dots, e_{2^k-1} D\}$ also satisfies the above recursion due to the simple fact that D is a linear mapping (see also [14, Proposition 3.1]).

To answer the question **Q1**, in what follows we derive several results which actually describe the role of lexicographic ordering in relation to $\Lambda_k \subset \Omega_f$ (for a given linear space E). More precisely, we first show that any linear space which satisfies the recursion of Lemma III.1-(i) is actually an image of some linear space ordered lexicographically. Towards the end of this subsection, we discuss the fact that the *lexicographically ordered* space $\mathbb{F}_2^k$ is always embedded in a *lexicographically ordered linear subspace* $E \subset \mathbb{F}_2^n$ with $dim(E) = k$.

Proposition V.1. *Let* $\overline{E} = \{\overline{e}_0, \dots, \overline{e}_{2^k-1}\} \subseteq \mathbb{F}_2^n$ *be a linear subspace. Then, the recursion* $\overline{e}_j = \overline{e}_{j-2^i} \oplus \overline{e}_{2^i}$ *holds (for all* $2^i \leq j \leq 2^{i+1} - 1$ *and* $i \in \{0, \dots, k-1\}$*) if and only if for an arbitrary (fixed) lexicographically ordered linear subspace* $E = \{e_0, \dots, e_{2^k-1}\} \subset \mathbb{F}_2^n$ *there exists* $M_{n\times n} \in GL(n, \mathbb{F}_2)$ *such that* $\overline{E} = EM_{n\times n}$ *and* $\overline{e}_i = e_i M$ *for* $i \in [0, 2^k - 1]$.

Proof. A lengthy technical proof of this result is given in Appendix - Section VII-A. □

Using the same idea to construct the matrix $M_{n\times n}$ as in the proof of Proposition V.1 (see (15) in Appendix), one can easily prove the following result.

Proposition V.2. *Let* $\overline{E} = \{\overline{e}_0, \dots, \overline{e}_{2^k-1}\} \subseteq \mathbb{F}_2^n$ *be a linear subspace such that* $\overline{e}_j = \overline{e}_{j-2^i} \oplus \overline{e}_{2^i}$ *holds (for all* $2^i \leq j \leq 2^{i+1} - 1$ *and* $i \in \{0, \dots, k-1\}$*). Then:*

i) There exists $M_{n\times n} \in GL(n, \mathbb{F}_2)$ *such that* $\overline{e}_i = e_i M_{n\times n}$*, where* $\overline{E} = \{e_0, \dots, e_{2^k-1}\}$ *is ordered lexicographically.*

ii) Moreover, for any two orderings $\overline{E} = \{e_0^{(1)}, \dots, e_{2^k-1}^{(1)}\}$ *and* $\overline{E} = \{e_0^{(2)}, \dots, e_{2^k-1}^{(2)}\}$ *such that* $e_j^{(t)} = e_{j-2^i}^{(t)} \oplus e_{2^i}^{(t)}$ *holds (for all* $2^i \leq j \leq 2^{i+1} - 1$ *and* $i \in \{0, \dots, k-1\}$, $t = 1, 2$*), there exists* $M_{n\times n} \in GL(n, \mathbb{F}_2)$ *such that* $e_i^{(1)} = e_i^{(2)} M_{n\times n}$ *(*$i \in [0, 2^k - 1]$*).*

Another interesting property, related to lexicographically ordered linear spaces, one can find in the proof of [13, Lemma 3.1-(i)]. Namely, if we consider a lexicographically ordered linear subspace $E = \{e_0, \dots, e_{2^k-1}\} \subset \mathbb{F}_2^n$ as a matrix of the size $2^k \times n$, then its reduced row-echelon form reveals which columns of E constitute the lexicographically ordered space $\mathbb{F}_2^k$. These columns are the ones in which the pivots are placed. The following proposition formalizes the previous observation.

Proposition V.3. *Let* $E = \{e_0, \dots, e_{2^k-1}\} \subseteq \mathbb{F}_2^n$ *be a lexicographically ordered linear subspace where* $e_i = (e_1^{(i)}, \dots, e_n^{(i)})$ *(*$i \in [0, 2^k - 1]$*). Then there exist coordinates* $i_1, \dots, i_k \in [1, n]$ *such that* $1 \leq i_1 < i_2 < \dots < i_k \leq n$ *and*

$$(e_{i_1}^{(i)}, \dots, e_{i_k}^{(i)}) = z_i \in \mathbb{F}_2^k, \quad i \in [0, 2^k - 1],$$

where $\mathbb{F}_2^k = \{z_0, \dots, z_{2^k-1}\}$ *is ordered lexicographically (*$z_0 = \boldsymbol{0}_k$*).*

Remark V.1. *We note that Proposition V.3 can also be proved inductively, using only the definition of lexicographic ordering, but we omit it here since it is more complex than the proof of [13, Lemma 3.1-(i)] (based on the row-echelon form).*

The previous two results clearly exhibit that the lexicographic ordering of a linear subspace can be seen as a *natural ordering* that one can impose on it, and this is the main conclusion related to **Q1**. This is mainly due to Proposition V.3 and the fact that the lexicographically ordered space $\mathbb{F}_2^k$ is embedded in a lexicographically ordered linear subspace $E \subset \mathbb{F}_2^n$, with $dim(E) = k \leq n$.

In the context of spectral construction methods of plateaued functions, it is usually very convenient to endow an affine Walsh support S_f with the lexicographic order instead of using the ordering of S_f induced by E through the representation $S_f = v \oplus E$ ($v \in S_f$). For this purpose, we provide the following result.

Proposition V.4. *Let* $S_f = \{\omega_0, \dots, \omega_{2^k-1}\} \subseteq \mathbb{F}_2^n$ *be a lexicographically ordered affine subspace (thus* $\omega_0 \neq \boldsymbol{0}_n$*). Then the linear space* $E = \omega_0 \oplus S_f = \{\boldsymbol{0}_n, e_1, e_2, \dots, e_{2^k-1}\}$ *is ordered lexicographically, where* $e_i = \omega_0 \oplus \omega_i$*, for* $i \in [0, 2^k - 1]$.

Proof. We need to prove that $\mathbf{0}_n = \omega_0 \oplus \omega_0 < \omega_0 \oplus \omega_1 < \dots < \omega_0 \oplus \omega_{2^k-1}$. Equivalently, for the lexicographically ordered linear subspace $E = \{e_0, \dots, e_{2^k-1}\}$, we have to prove that for $e_i < e_j$ it holds that $e_i \oplus \omega_0 < e_j \oplus \omega_0$ for all $i < j$, where ω_0 is the minimal vector of a coset of E (denote the coset by C_{ω_0}) which contains it. Thus, for $e_i = (\alpha_1, \dots, \alpha_{t-1}, 0, \eta_{t+1}, \dots, \eta_n) < e_j = (\alpha_1, \dots, \alpha_{t-1}, 1, \mu_{t+1}, \dots, \mu_n)$, let us assume that $e_i \oplus \omega_0 > e_j \oplus \omega_0$ for some $i < j$. This is possible only if the t-th coordinate of ω_0 is equal to 1, i.e., $\omega_0 = (\nu_1, \dots, \nu_{t-1}, 1, \nu_{t+1}, \dots, \nu_n)$, in which case we have that

$$\begin{aligned} e_i \oplus e_j \oplus \omega_0 &= (\mathbf{0}_{t-1}, 1, \eta_{t+1} \oplus \mu_{t+1}, \dots, \eta_n \oplus \mu_n) \oplus \omega_0 \\ &= (\nu_1, \dots, \nu_{t-1}, 0, \theta_{t+1}, \dots, \theta_n) \in C_{\omega_0}, \end{aligned}$$

since $\omega_0 \in C_{\omega_0}$ implies that $\omega_0 \oplus e \in C_{\omega_0}$, for any $e \in E$ (recall that C_{ω_0} is a coset of E). However, this contradicts the fact that ω_0 is the minimal element of C_{ω_0}. □

Remark V.2. *Proposition V.4 can be used in Theorem IV.1 if we want to construct an* n*-variable plateaued function with an affine Walsh support* $S_f \subset \mathbb{F}_2^n$*. It is sufficient to order* $S_f = \{\omega_0, \dots, \omega_{2^k-1}\}$ *lexicographically (i.e.,* $\omega_i < \omega_j$*, for* $i < j$*), and then the dual* $\overline{f}^*(x_i) = f^*(\omega_i)$ *(*$x_i \in \mathbb{F}_2^k$*) is a bent function on* $\mathbb{F}_2^k$*.*

B. Answering *Q2*

In this section, we show that if S_f is endowed by two induced ordering stemming from two different representations of $S_f = v_i \oplus E_i$, where E_1 and E_2 are different orderings of a linear subspace E satisfying the recursion of Lemma III.1-(i), then the duals $\overline{f}_1^*$ and $\overline{f}_2^*$ are equivalent functions. We start with the following example which illustrates how two different choices of $v_1, v_2 \in S_f$ actually provide different orderings of S_f.

Example V.1. *Let us consider the Walsh support $S_f \subset \mathbb{F}_2^4$ given as*

$$S_f = v \oplus E = (1,0,0,1) \oplus \langle (0,1,1,0),(1,0,1,0),(1,0,1,1) \rangle.$$

Furthermore, let us consider two representations of S_f (E ordered lexicographically) given as

$$S_f = (1,1,1,0) \oplus E = \begin{pmatrix} 1 & 1 & 1 & 0 \\ 1 & 1 & 1 & 1 \\ 1 & 0 & 0 & 0 \\ 1 & 0 & 0 & 1 \\ 0 & 1 & 0 & 0 \\ 0 & 1 & 0 & 1 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 1 & 1 \end{pmatrix},$$

and

$$S_f = (0,1,0,1) \oplus E = \begin{pmatrix} 0 & 1 & 0 & 1 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 1 \\ 0 & 0 & 1 & 0 \\ 1 & 1 & 1 & 1 \\ 1 & 1 & 1 & 0 \\ 1 & 0 & 0 & 1 \\ 1 & 0 & 0 & 0 \end{pmatrix}.$$

Here, we have that the first representation gives the ordering $S_f = \{\tilde{\omega}_0, \ldots, \tilde{\omega}_{2^k-1}\}$ with $\tilde{\omega}_i = (1,1,1,0) \oplus e_i$, and the second $S_f = \{\hat{\omega}_0, \ldots, \hat{\omega}_{2^k-1}\}$ with $\hat{\omega}_i = (0,1,0,1) \oplus e_i$, where $E = \{e_0, \ldots, e_{2^k-1}\} = \langle (0,1,1,0),(1,0,1,0),(1,0,1,1) \rangle$ is ordered lexicographically.

Note that the duals $\overline{f}_1^*$ and $\overline{f}_2^*$ defined as $\overline{f}_1^*(x_i) = f^*(v_1 \oplus e_i)$ and $\overline{f}_2^*(x_i) = f^*(v_2 \oplus e_i)$ are not the same mappings since $v_1 \oplus e_i = \tilde{\omega}_i$ and $v_2 \oplus e_i = \hat{\omega}_i$, and thus $\overline{f}_1^*(x_i) = f^*(\tilde{\omega}_i)$ and $\overline{f}_2^*(x_i) = f^*(\hat{\omega}_i)$.

Hence, with the following result we show that the relation between the variables of $\overline{f}_1^*$ and $\overline{f}_2^*$ is actually affine, where in $S_f = v_i \oplus E_i$ we assume that $E_1 = E_2 = E$ is lexicographically ordered.

Theorem V.1. *Let $f : \mathbb{F}_2^n \to \mathbb{F}_2$ be an s-plateaued function with an affine Walsh support $S_f \subset \mathbb{F}_2^n$ ($k = n - s$). Assume that $S_f = v_1 \oplus E = \{\tilde{\omega}_0, \ldots, \tilde{\omega}_{2^k-1}\}$ and $S_f = v_2 \oplus E = \{\hat{\omega}_0, \ldots, \hat{\omega}_{2^k-1}\}$ are two orderings of S_f ($v_1, v_2 \in S_f$ two arbitrary vectors), where $E = \{e_0, \ldots, e_{2^k-1}\} \subset \mathbb{F}_2^n$ is a linear subspace ordered lexicographically. If the duals $\overline{f}_1^*, \overline{f}_2^* : \mathbb{F}_2^k \to \mathbb{F}_2$ are defined as $\overline{f}_i^*(x_j) = f^*(v_i \oplus e_j)$ ($i = 1,2$, $j \in [0, 2^k-1]$), then $\overline{f}_i^*$ are equivalent functions on $\mathbb{F}_2^k$, i.e., there exists an invertible matrix $A_{k \times k} \in GL(k, \mathbb{F}_2)$ and $c \in \mathbb{F}_2^k$ such that $\overline{f}_1^*(xA_{k\times k} \oplus c) = \overline{f}_2^*(x)$, for $x \in \mathbb{F}_2^k$.*

Proof. An affine relation between $v_1 \oplus E$ and $v_2 \oplus E$, where E is ordered lexicographically, is established using the mapping $L : v_1 \oplus E \to v_2 \oplus E$ defined as $L(z) = b \oplus zM_{n\times n}$, where $M_{n\times n} = I_{n \times n}$ and $b = v_2 \oplus v_1$. Then, we have $L(v_1 \oplus e_i) = b \oplus (v_1 \oplus e_i)M_{n\times n} = v_2 \oplus e_i$. Furthermore, we have that $L(v_1 \oplus e_i) = v_2 \oplus e_i \in S_f$ is actually equal to some $v_1 \oplus e_j$ (for some $e_j \in E$), i.e., we have that $L(v_1 \oplus e_i) = v_2 \oplus e_i = v_1 \oplus e_j$. In what follows, we show that the relation between e_i and e_j in the previous equality is not arbitrary, and in fact they are related in an affine manner in terms of vectors $x_i, x_j \in \mathbb{F}_2^k$.

By Proposition V.3 there exists a matrix $K_{n\times k}$ such that $e_j K_{n\times k} = x_j$ (for every $j \in [0, 2^k - 1]$), and thus for $\overline{v}_2 = v_2 K_{n\times k}$ and $\overline{v}_1 = v_1 K_{n \times k}$ we have that

$$\overline{v}_2 \oplus e_i K_{n\times k} = \overline{v}_1 \oplus x_j, \quad \overline{v}_1, \overline{v}_2 \in \mathbb{F}_2^k.$$

Furthermore, using the relation (9) given in [14], we have that $e_i \in E$ can be written as

$$e_i = x_i \begin{pmatrix} e_{2^{k-1}} \\ \vdots \\ e_2 \\ e_1 \end{pmatrix} = x_i R_{k\times n}, \quad x_i \in \mathbb{F}_2^k, \tag{14}$$

where $\{e_{2^t} : t = 0, 1, \ldots, k-1\}$ is a basis of the lexicographically ordered set E (where clearly $e_{2^{k-1}} > \ldots > e_2 > e_1$). Using this representation we have that

$$\overline{v}_2 \oplus e_i K_{n\times k} = \overline{v}_2 \oplus x_i R_{k\times n} K_{n\times k} = \overline{v}_1 \oplus x_j,$$

and consequently, we have that $x_i A_{k\times k} \oplus (\overline{v}_1 \oplus \overline{v}_2) = x_j$, where $A_{k \times k} = R_{k\times n}K_{n\times k}$. Since the mapping L is injective on S_f, then the mapping $A_{k\times k}$ has to be invertible. Denoting by $c = \overline{v}_1 \oplus \overline{v}_2 \in \mathbb{F}_2^k$ we finally have that

$$\begin{aligned} \overline{f}_2^*(x_i) &= f^*(v_2 \oplus e_i) = f^*(v_1 \oplus e_j) = \overline{f}_1^*(x_j) \\ &= \overline{f}_1^*(x_i A_{k\times k} \oplus c), \quad x_i \in \mathbb{F}_2^k, \end{aligned}$$

which completes the proof. □

Note that in the proof of Theorem V.1, there exist different matrices $K_{n\times k}$ for which $e_j K_{n \times k} = x_j \in \mathbb{F}_2^k$ holds, i.e., $\{e_j K_{n\times k} : e_j \in E\} = \mathbb{F}_2^k$. One particular choice, with respect to the matrix $R_{k\times n}$ given in (14), may result that $A_{k\times k}$ is actually the identity matrix $I_{k\times k}$.

More precisely, for the lexicographically ordered linear space $E = \{e_0, \ldots, e_{2^k-1}\}$ with $e_i = (e_1^{(i)}, \ldots, e_n^{(i)})$, let $i_1, \ldots, i_k \in [1, n]$ be indices such that $1 \le i_1 < i_2 < \ldots < i_k \le n$ and $(e_{i_1}^{(i)}, \ldots, e_{i_k}^{(i)}) = z_i \in \mathbb{F}_2^k$, $i \in [0, 2^k - 1]$, where $\mathbb{F}_2^k = \{z_0, \ldots, z_{2^k-1}\}$ is ordered lexicographically ($z_0 = \mathbf{0}_k$). The existence of the set of indices $i_1, \ldots, i_k$ is due to Proposition V.3.

If we define $K_{k\times n} = (J_1, \ldots, J_k)$, where $J_j = (J_{1j}, \ldots, J_{nj})^T$ are column vectors such that $J_{tj} = 1$ only for $t = i_j$ ($J_{tj} = 0$ for $t \neq i_j$), where $i_j \in \{i_1, \ldots, i_k\}$, then it is not difficult to see that the product $R_{k\times n}K_{n\times k}$ will always be an identity matrix ($R_{k\times n}$ given as in (14)), i.e., we will have that $A_{k\times k} = I_{k \times k}$.

Even more generally, in the following result we show that the equivalence of the duals $\overline{f}_1^*$ and $\overline{f}_2^*$ is still valid, if their definitions corresponds to two different orderings of E which satisfy the recursion of Lemma III.1-(i). In fact, the following result answers to **Q2**.

Theorem V.2. *Let $f : \mathbb{F}_2^n \to \mathbb{F}_2$ be an s-plateaued function with an affine Walsh support $S_f \subset \mathbb{F}_2^n$ ($k = n - s$), given in two representations $S_f = v_t \oplus E_t$, where $E_t = \{e_0^{(t)}, \ldots, e_{2^k-1}^{(t)}\}$ is a linear subspace and $e_j^{(t)} = e_{j-2^i}^{(t)} \oplus e_{2^i}^{(t)}$ holds (for all $2^i \le j \le 2^{i+1} - 1$ and $i \in \{0, \ldots, k-1\}$, $t = 1, 2$). If the duals $\overline{f}_t^* : \mathbb{F}_2^k \to \mathbb{F}_2$ are defined as $\overline{f}_t^*(x_j) = f^*(v_t \oplus e_j^{(t)})$ ($t = 1, 2$, $j \in [0, 2^k - 1]$), then $\overline{f}_1^*$ and $\overline{f}_2^*$ are equivalent functions on $\mathbb{F}_2^k$.*

Proof. By Proposition V.2-(ii) there exists an affine mapping $L : v_1 \oplus E_1 \rightarrow v_2 \oplus E_2$ which preserves the ordering structure from E_1 to E_2. Then, using the same computational steps and arguments as in the proof of Theorem V.1, one proves that $\overline{f}_1^*$ and $\overline{f}_2^*$ are equivalent functions on $\mathbb{F}_2^k$. □

To summarize this section, we conclude that regardless of orderings that Walsh support $S_f = v \oplus E$ is endowed with, where ordering of E satisfies the recursion of Lemma III.1-(i)), then duals $\overline{f}^* : \mathbb{F}_2^k \rightarrow \mathbb{F}_2$ corresponding to these orderings will be equivalent functions on $\mathbb{F}_2^k$. In other words, Theorem V.2 shows that the mapping P mentioned in Remark 2.1 in [13], [14] is actually an affine transformation.

VI. Conclusions

This article gives a detailed analysis of the so-called basic 5-value spectrum Boolean functions in terms of their design (based on totally disjoint plateaued functions) and their classification with respect to EA-equivalence. The main challenge that remains to be addressed are efficient design methods of non-basic classes (using Walsh supports which are not affine subspaces though of cardinality 2^{λ_i}) of these objects, which would give EA-inequivalent functions to basic ones (Corollary 3). A hard problem of specifying such functions for arbitrary cardinalities of the corresponding Walsh supports, though governed by Proposition III.3, remains to be answered and especially the existence of such function needs to be established in the first place.

References

[1] A. Canteaut and P. Charpin, “Decomposing bent functions,” IEEE Trans. Inf. Theory, vol. 49, no. 8, pp. 2004–2019, 2003.

[2] A. Canteaut, C. Carlet, P. Charpin and C. Fontaine, “On cryptographic properties of the cosets of $R(1, m)$,” IEEE Trans. Inf. Theory, vol. 47, no. 4, pp. 1494–1513, 2001.

[3] X. Cao and L. Hu, “Two Boolean functions with five-valued Walsh spectra and high nonlinearity,” International Journal of Foundations of Computer Science, vol. 26, no. 5, pp. 537–556, 2015.

[4] C. Carlet, “Partially-bent functions,” Designs, Codes and Cryptography, vol. 3, pp. 135–145, 1993.

[5] C. Carlet, “Vectorial Boolean functions for cryptography,” in Boolean models and methods in mathematics, computer science, and engineering, Cambridge, U.K.: Cambridge University Press, pp. 398 – 469, 2010.

[6] C. Carlet. “Boolean and vectorial plateaued functions and APN functions,” IEEE Trans. Inf. Theory, vol. 61, no. 11, pp. 6272–6289, 2015.

[7] C. Carlet and S. Mesnager, “Four decades of research on bent functions,” Designs, Codes and Cryptogr., vol. 78, no. 1, pp. 5–50, 2016.

[8] C. Carlet and E. Prouff, “On plateaued functions and their constructions,” Fast Software Encryption–FSE 2003, Berlin, Germany: Springer-Verlag, LNCS vol. 2887, pp. 54–73, 2003.

[9] N. Cepak, E. Pasalic, and A. Muratović-Ribić, “Frobenius linear translators giving rise to new infinite classes of permutations and bent functions,” Cryptography and Communications, vol 11, no. 6, pp. 1275–1295, 2019.

[10] T. W. Cusick, “Highly nonlinear plateaued functions,” IET Information Security, vol. 11, no. 2, pp. 78–81, 2016.

[11] J. F. Dillon, “APN polynomials: An update,” invited talk at Finite Fields: Theory and Applications–FQ9, Dublin, Ireland, 2009.

[12] S. Dubuc. “Linear structures of Boolean functions,” IEEE International Symposium on Information Theory 1998 (16-21 Aug), DOI: 10.1109/ISIT.1998.709045, 1998.

[13] S. Hodžić, E. Pasalic, and Y. Wei, “A general framework for secondary constructions of bent and plateaued functions,” Designs, Codes and Cryptogr., vol. 88, pp. 2007–2035, 2020.

[14] S. Hodžić, E. Pasalic, Y. Wei, and F. Zhang, “Designing plateaued Boolean functions in spectral domain and their classification,” IEEE Trans. Inf. Theory, vol. 65, no. 9, pp. 5865–5879, 2019.

[15] S. Hodžić, E. Pasalic, and W.-G. Zhang, “Generic Constructions of Five-Valued Spectra Boolean Functions,” IEEE Trans. Inf. Theory, vol. 65, no. 11, pp. 7554 – 7565, 2019.

[16] S. Maitra and P. Sarkar, “Cryptographically significant Boolean functions with five valued Walsh spectra,” Theoretical Computer Science, vol. 276, no. 1-2, pp. 133–146, 2002.

[17] S. Mesnager, “On semi-bent functions and related plateaued functions over the Galois field $\mathbb{F}_{2^n}$,” in Open Problems in Mathematics and Computational Science, Springer, pp. 243–273, 2014.

[18] S. Mesnager and F. Zhang, “On constructions of bent, semi-bent and five valued spectrum functions from old bent functions,” Advances in Mathematics of Communications, vol. 11, no. 2, pp. 339–345, 2017.

[19] B. Preneel, W. V. Leekwijck, L. V. Linden, R. Govaerts, and J. Vandewalle, “Propagation characteristics of Boolean functions,” Advances in Cryptology–EUROCRYPT’90, Berlin, Germany: Springer-Verlag, LNCS vol. 473, pp. 161–173, 1991.

[20] O. S. Rothaus, “On ‘bent’ functions,” Journal of Combinatorial Theory, Series A, vol. 20, no. 3, pp. 300–305, 1976.

[21] P. Sarkar, and S. Maitra, “ Cross-correlation analysis of cryptographically useful Boolean functions and S-boxes,” Theory of Computing Systems, vol. 35, no. 1, pp. 39–57, 2002.

[22] N. Tokareva, “On the number of bent functions from iterative constructions: lower bounds and hypotheses,” Advances in Mathematics of Communications, vol. 5, no. 4, pp. 609–621, 2011.

[23] Y. Wei, E. Pasalic, F. Zhang, W. Wu, and C.-X. Wang, “New constructions of resilient functions with strictly almost optimal nonlinearity via non-overlap spectra functions,” Information Sciences, vol. 415–416, pp. 377–396, 2017.

[24] G.-Z. Xiao and J. L. Massey, “A spectral characterization of correlation-immune combining functions,” IEEE Trans. Inf. Theory, vol. 34, no. 3, pp. 569–571, 1988.

[25] G. Xu, X. Cao, and S. Xu, Several classes of Boolean functions with few Walsh transform values,” Applicable Algebra in Engineering, Communication and Computing, vol. 28, no. 2, pp. 155–176, 2017.

[26] F. Zhang, C. Carlet, Y. Hu, and T. J. Cao, “Secondary constructions of highly nonlinear Boolean functions and disjoint spectra plateaued functions. Information Sciences, vol. 283, pp. 94–106, 2014.

[27] F. Zhang, Y. Wei, E. Pasalic, and S. Xia, “Large sets of disjoint spectra plateaued functions inequivalent to partially linear functions,” IEEE Trans. Inf. Theory, vol. 64, no. 4, pp. 2987–2999, 2018.

[28] W.-G. Zhang and E. Pasalic. “Generalized Maiorana-McFarland construction of resilient Boolean functions with high nonlinearity and good algebraic properties,” IEEE Trans. Inf. Theory, vol. 60, no. 10, pp. 6681–6695, 2014.

[29] Y. Zheng and X. M. Zhang. “On plateaued functions,” IEEE Trans. Inf. Theory, vol. 47, no. 3, pp. 1215–1223, 2001.

VII. Appendix

A. *Proof of Proposition V.1*

($\Leftarrow$) Suppose that $\overline{E} = \{\overline{e}_0, \ldots, \overline{e}_{2^k-1}\}$ is an image of some lexicographically ordered linear subspace $E = \{e_0, \ldots, e_{2^k-1}\}$ under an invertible linear mapping $M_{n\times n} \in GL(n, \mathbb{F}_2)$, i.e., let $\overline{e}_i = e_i M_{n\times n}$ ($i \in [0, 2^k - 1]$). Then by Lemma III.1-(i) we have that $e_j = e_{j-2^i} \oplus e_{2^i}$ holds for all $2^i \leq j \leq 2^{i+1} - 1$ and $i \in \{0, \ldots, k-1\}$. By multiplying the equality $e_j = e_{j-2^i} \oplus e_{2^i}$ by $M_{n\times n}$ we have that $\overline{e}_j = e_j M_{n\times n} = e_{j-2^i} M_{n\times n} \oplus e_{2^i} M_{n\times n} = \overline{e}_{j-2^i} \oplus \overline{e}_{2^i}$, for all j in the interval $2^i \leq j \leq 2^{i+1} - 1$ and $i \in \{0, \ldots, k-1\}$, i.e., $\overline{E}$ satisfies the recursion.

($\Rightarrow$) Assume now that $\overline{E} = \{\overline{e}_0, \ldots, \overline{e}_{2^k-1}\}$ satisfies the recursion $\overline{e}_j = \overline{e}_{j-2^i} \oplus \overline{e}_{2^i}$ for all $2^i \leq j \leq 2^{i+1} - 1$ and $i \in \{0, \ldots, k-1\}$. Since by Lemma III.1-(ii) we have that $\{T_\ell : \ell \in \mathcal{L}_k\} \subset \{(u \cdot \overline{e}_0, \ldots, u \cdot \overline{e}_{2^k-1}) : u \in \mathbb{F}_2^n\}$, then if we view $\overline{E} = [T_{\ell_1}, \ldots, T_{\ell_n}]$ as a matrix of size $2^k \times n$, its columns T_{ℓ_i} correspond to some linear functions $\ell_i : \mathbb{F}_2^k \rightarrow \mathbb{F}_2$.

Without loss of generality, let us assume that the first k columns $T_{\ell_1}, \ldots, T_{\ell_k}$ are linearly independent linear functions (these exist due to $dim(\overline{E}) = k$). Hence, we have that $\overline{E} = [T_{\ell_1}, \dots, T_{\ell_k}, T_{\ell_{k+1}}, \dots, T_{\ell_n}]$, where $T_{\ell_{k+1}}, \dots, T_{\ell_n}$ are columns which can be obtained as linear combinations of the first k columns $T_{\ell_1}, \dots, T_{\ell_k}$. On the other hand, assume that an arbitrary (fixed) lexicographically ordered linear subspace $E \subset \mathbb{F}_2^n$ can be written as a matrix of the size $2^k \times n$ as well, i.e., $E = [T_{\lambda_1}, \dots, T_{\lambda_n}]$ with λ_i being linear functions defined on $\mathbb{F}_2^k$. For the matrix E, we also assume that the first k columns are linearly independent. Now, let us consider the matrix equality $\overline{E}M_{n\times n} = E$ with a block matrix $M_{n\times n}$ as

$$\begin{aligned}&[T_{\ell_1}, \dots, T_{\ell_k}, T_{\ell_{k+1}}, \dots, T_{\ell_n}] \begin{pmatrix} A_{k\times k} & C_{k\times(n-k)} \\ \mathbf{0}_{(n-k)\times k} & B_{(n-k)\times(n-k)} \end{pmatrix} \\ &= [T_{\lambda_1}, \dots, T_{\lambda_k}, T_{\lambda_{k+1}}, \dots, T_{\lambda_n}], \end{aligned} \tag{15}$$

where $\mathbf{0}_{(n-k)\times k}$ is a zero matrix. In what follows we show that there exists submatrices $A_{k\times k}$, $B_{(n-k)\times(n-k)}$ and $C_{k\times(n-k)}$ for which $M_{n\times n}$ is invertible, and satisfies (15).

Firstly, in the multiplication $\overline{E}M_{n\times n}$, the matrix $A_{k\times k}$ selects linear combinations of the first k columns of the matrix $\overline{E}$, and it affects the first k columns of E (which are linearly independent functions). Due to the fact $\{\ell_i : i = 1, \dots, k\}$ and $\{d_i : i = 1, \dots, k\}$ are both sets of linearly independent functions, it is clear that there always exists an invertible matrix $A_{k\times k}$ which induces the necessary transformation from columns $T_{\ell_1}, \dots, T_{\ell_k}$ to $T_{d_1}, \dots, T_{d_k}$. And finally, it is clear that for an arbitrary matrix $B_{(n-k)\times(n-k)}$ one can always find a matrix $C_{k\times(n-k)}$ such that the equality

$$[T_{\ell_1}, \dots, T_{\ell_k}]C_{k\times(n-k)} \oplus [T_{\ell_{k+1}}, \dots, T_{\ell_n}]B_{(n-k)\times(n-k)} = [T_{d_{k+1}}, \dots, T_{d_n}]$$

holds. Thus, an invertible matrix $B_{(n-k)\times(n-k)}$ (along with invertibility of $A_{k\times k}$) provides the invertibility of $M_{n\times n}$.

Note that we required that the first k columns of $\overline{E}$ and E are linearly independent (which is not necessary in general). Without this setting we would only have that the entries of the matrices $A_{k\times k}$, $B_{(n-k)\times(n-k)}$ and $C_{k\times(n-k)}$ are placed differently in the matrix $M_{n\times n}$, where the arguments for invertibility and existence still hold. □

Samir Hodžić received his Ph.D. degree in cryptology from University of Primorska, FAMNIT, Koper, Slovenia, in 2017. His research area is mainly symmetric-key cryptographic primitives and in particular the design of cryptographic Boolean functions. He is currently with Technical University of Denmark, DTU Compute, Denmark.

Peter Horak has received his Ph.D. (1979) and D.Sc. (1995) degrees in mathematics from Comenius University in Bratislava, Slovakia. His research interests include graph theory, combinatorics, coding theory, cryptography, and theoretical computer science. He also has a paper on the number theory and another one on topology. These two papers have been published in American Mathematical Monthly. Peter Horak has held a permanent or visiting positions at several universities in (Czecho)Slovakia, USA, Canada, and Kuwait. Since2003 he is a professor of mathematics at University of Washington, Tacoma. He solved (with coauthors) four problems of Paul Erdős and a problem of Donald Knuth. His Erdos number is 1.

Enes Pasalic received the Ph.D. degree in cryptology from Lund University, Lund, Sweden, in 2003. His main research interest is in cryptology and in particular the design and analysis of symmetric encryption schemes. Since May 2003, he has been doing a postdoctoral research at INRIA (Versaille, France) crypto group, and later in 2005 at the Technical University of Denmark, Lyngby. He is currently with University of Primorska, FAMNIT and IAM, Koper, Slovenia.