Determining those Boolean functions whose restrictions to affine spaces are plateaued

Claude Carlet[1], Darrion Thornburgh[2]

[1]Universities of Paris 8, France and Bergen, Norway.
claude.carlet@gmail.com
[2]Department of Mathematics, Vanderbilt University, USA.
darrion.thornburgh@vanderbilt.edu

Abstract

Quadratic Boolean functions (that is, Boolean functions of algebraic degree at most 2), bent Boolean functions (i.e. maximally nonlinear Boolean functions in even numbers of variables) and, as we observe in this paper, partially-bent Boolean functions (i.e. affine extensions of bent functions to linear super-spaces), share a strong property: all their restrictions to affine hyperplanes are plateaued (i.e. have a Walsh transform valued in a set of the form $\{0, \pm\lambda\}$, where λ is a positive integer called the amplitude). In this paper we determine for any n and $k < n$ the class C_k^n of those n-variable Boolean functions whose restrictions to all k-dimensional affine subspaces of $\mathbb{F}_2^n$ are plateaued (of any amplitude). We show that, for any $n \geq 4$, C_{n-1}^n equals the class of partially-bent functions, and for $3 \leq k \leq n-2$, C_k^n equals the class of quadratic functions (while for $0 \leq k \leq 2$, it equals of course the class of all Boolean functions).This provides a new characterization (after almost 20 years) of partially-bent functions and a hierarchy among n-variable Boolean functions by six nested classes, each of which happens to be, for any $n \geq 5$, strictly included in the next one: quadratic functions, partially-bent functions, the restrictions of $(n+1)$-variable partially-bent functions to $\mathbb{F}_2^n$, plateaued functions, the restrictions of $(n+1)$-variable plateaued functions to $\mathbb{F}_2^n$, and all Boolean functions. We leave open the two problems of determining exactly what are the third and fifth of these classes, but we begin the study of the first of these two classes by characterizing the situation where a plateaued function g has a restriction f to an affine hyperplane H that is plateaued. We also characterize when g is partially-bent. Our characterization of partially-bent (resp., quadratic) functions extends to strongly plateaued vectorial functions. We state an open question on vectorial functions that happens to be related to an important one on crooked functions.

Keywords: Boolean function, plateaued function, partially-bent function.

1 Introduction

Boolean functions, that is, functions from the $\mathbb{F}_2$-vector space $\mathbb{F}_2^n$ (or the finite field $\mathbb{F}_{2^n}$) for some positive integer n, to $\mathbb{F}_2$, and vectorial functions, that is, functions from $\mathbb{F}_2^n$ to $\mathbb{F}_2^m$, whose study is a domain of research of its own, have many applications in mathematics and computer science.

In particular, cryptography uses them as nonlinear components in symmetric ciphers that are essential to their robustness (see e.g. [11]), coding theory uses them to build error correcting codes (see e.g. [30]), some of which offer optimal combinations of parameters (see e.g. [13, 24]), and some combinatorics notions (such as difference sets in elementary Abelian 2-groups, see [20, 34]) are closely related to Boolean or vectorial functions.

Some general classes of Boolean functions have been studied in the literature. The first one, historically, is that of quadratic functions (whose derivatives are affine). It is the simplest class after that of affine functions (which are unsuitable for cryptography). The parameters of quadratic functions are much simpler to determine and to study than those of general functions (see e.g. [11, Section 5.2]). But quadratic functions are peculiar and their algebraic degree is too low from a general cryptographic viewpoint. Moreover, the class of quadratic functions is very small. After the introduction of bent functions in [34], partially-bent functions have been introduced in [8] (one of their equivalent definitions is that the restriction of the function to some vector subspace of $\mathbb{F}_2^n$ is bent and this bent function is affinely extended to the whole space to obtain the partially-bent function). Their class includes all quadratic functions. Partially-bent functions share many of the nice properties of quadratic functions. Their general structure is still quite simple (but in a less global way than for quadratic functions, since the structure of the bent functions, on which they are built, is essentially unknown). They are also peculiar (for instance, non-bent partially-bent functions have so-called linear structures and this is a cryptographic weakness) and they are not that numerous, since bent functions are rare. Later have been introduced plateaued functions in [38], which are defined by a property of their Walsh transform. Plateaued functions are considered to constitute the most important class of functions, offering a suitable compromise between the robustness of their properties (suitable for applications) and the size and generality of the class. The specificity of their Walsh spectrum presents much interest from a cryptographic viewpoint (either that it represents a weakness, see e.g. [7], or a strength thanks to its regularity), and also from a coding theoretic viewpoint since the Walsh spectrum of Boolean functions is related to important parameters of the codes they generate, such as their weight distribution. The class of plateaued functions has a much less simple structure than that of partially-bent functions (we know still less how generating general plateaued functions than partially-bent functions), but nice properties and characterizations are known [10]. This class, which is in some cases a good corpus where to find Boolean functions for applications, is also small compared to the space of all Boolean functions, see [31], but it is (until now) the widest known on which we still have nice properties (see e.g. [37]) and characterizations. In [33], plateaued Boolean functions are characterized by means of their Cayley graphs with, in the nontrivial cases, their Cayley graphs being strongly 3-walk-regular (a natural generalization of strongly regular graphs introduced in [36]; these latter graphs, for their part, being linked to bent functions [2]).

We have (before the present paper) a hierarchy among n-variable Boolean functions by four nested classes, each of which is strictly included in the next one: quadratic functions, partially-bent functions, plateaued functions, and all Boolean functions.

The restrictions of Boolean functions and vectorial functions to affine subspaces have been the subject of several studies (see e.g. [5, 6, 9, 12, 14, 15, 19, 21, 23, 26, 27, 28, 29, 39]). Such restrictions are directly related to the coefficients in the algebraic normal forms of Boolean functions and to their algebraic degrees, and the Poisson and second-order Poisson formulas (see e.g. [11]) deal also with them. Studying them also presents some interest for cryptography because of the existence of guess-and-determine attacks, consisting in making assumptions resulting in the fact that the input to a function (implemented in the cipher) would be restricted to a particular affine

space[1]. In coding theory, some codes (such as Reed-Muller codes and codes whose parity-check or generator matrices are built from vectorial functions or are obtained from the similar matrices of classic codes by removing their columns which do not belong to the support of a Boolean function) are inherently defined in terms of Boolean functions, and restricting the domain of the involved Boolean functions is a natural operation on such codes. In the general study of Boolean functions, studying the restrictions to affine spaces, which has been initiated for bent functions in [5, 6], poses questions that are often difficult to answer. The general behavior of the classes of partially-bent and plateaued functions with respect to the restriction of Boolean functions to affine subspaces has never been studied.

In this paper, we address the question of determining those n-variable Boolean functions whose restrictions to all affine spaces of a given dimension $k \leq n$ are partially-bent (respectively, plateaued, with possibly diverse amplitudes). Some papers in the literature have been interested in this kind of question. It is proved in [6] (where plateaued functions were called "three valued") that all bent functions have the property that all their restrictions to affine hyperplanes are plateaued. We shall see that this extends to partially-bent functions and that the plateauedness of the restrictions is characteristic of partial bentness. This provides in a way a converse to the result of [6]. This same latter reference also studies the restrictions to affine spaces of codimension 2, but focuses on those bent functions whose restrictions to at least one such affine space and to its three other cosets are all bent (leading to what the authors call a bent 4-decomposition). A characterization of bent functions is also given in [5, Theorem V.3] by means of their plateaued restrictions to complementary affine hyperplanes and a similar result is given for those functions in odd numbers of variables whose derivatives $D_a f(x) = f(x+a) + f(x)$ in nonzero directions a belonging to a linear hyperplane are balanced. But no study of Boolean functions whose restrictions to all k-dimensional affine spaces are partially-bent (resp., plateaued) has been made. We encountered this question while working on Gorodilova's conjecture regarding quadratic almost perfect nonlinear (APN) functions, see [16]. Characterizing such Boolean functions and their restrictions is useful concretely for proving that any quadratic APN function in an even number $n \geq 4$ of variables has at least 5 semi-bent components. Incidentally, our results also show that a hypothesis formulated in [1] for characterizing that a strongly plateaued function F has the so-called D-property on any hyperplane amounts to assuming that F is quadratic (when one assumes the same condition on every hyperplane), see the text after Proposition 4.17 in [16].

In this paper we mathematically prove that, for $3 \leq k \leq n-2$ (resp. $k = n-1 \geq 4$), only quadratic (resp. partially-bent) functions have all their restrictions to k-dimensional affine spaces plateaued. This provides a new characterization of partially-bent functions. The last known one dates back to 2008, see [40, 17]. We also address the case where the restrictions are partially-bent. This shows a nice distinction between the properties of quadratic functions and those of non-quadratic partially-bent functions, and between the properties of partially-bent functions and those of non-partially-bent plateaued functions (and more general Boolean functions). We observe that, for $n \geq 5$, we have six nested classes of Boolean functions: those containing respectively quadratic functions, partially-bent functions, the restrictions of $(n+1)$-variable partially-bent functions to $\mathbb{F}_2^n$, plateaued functions, the restrictions of $(n+1)$-variable plateaued functions to $\mathbb{F}_2^n$, and all Boolean functions; these classes are distinct. For $n \leq 4$, plateaued is equivalent to quadratic and the first four classes coincide.

[1]The success probability of the attack equals then the product of the probability that the input to the function belongs indeed to such a particular affine space, and of the probability that the attack concretely implemented by the attacker works in such a particular framework. The same happens with the complexity of the attack.

Our paper is organized as follows:
- our main result is Theorem 1, stated at the beginning of Section 3;
- we decompose its proof in Section 3 into four lemmas;
- in Section 4, we begin the study of those plateaued functions that are the restrictions of partially-bent (respectively, plateaued) functions to affine hyperplanes, and we give a characterization: a function g having a plateaued restriction f to an affine hyperplane H is plateaued if and only if the restriction f' of g to the complement of H is plateaued as well, with the same amplitude, and has a Walsh support that is either equal or disjoint from that of f; the characterization of when g is moreover partially-bent is a little more complex; in the case the Walsh supports of f and f' are equal, these functions must be partially-bent (with an additional condition) but when the supports are disjoint, they can be only plateaued (with the additional condition that the union of the supports is an affine space);
- in Section 5, we extend our main result to vectorial functions, which is rather straightforward, but our Corollary 4 represents in itself an interesting characterization of strongly plateaued functions;
- in our conclusion, we state the two open problems consisting in the determination of all restrictions of partially-bent functions and all restrictions of plateaued functions to affine hyperplanes. We also mention an open question on vectorial functions, which happens to be equivalent to a well-known and long-standing open question on crooked functions (are they all quadratic?).

2 Preliminaries

Let n be a positive integer. We denote by $\mathbb{F}_2^n$ the $\mathbb{F}_2$-vector space of all binary vectors of length n. For every non-negative integer $k \leq n$, its *k-dimensional affine subspaces* are the cosets of k-dimensional linear subspaces. We shall denote by $\mathcal{B}_n$ the vector space of all *n-variable Boolean functions* $f : \mathbb{F}_2^n \to \mathbb{F}_2$. A Boolean function is called *quadratic* if all its derivatives $D_a f(x) = f(x+a) + f(x)$ (sum calculated in $\mathbb{F}_2$) are affine Boolean functions[2] (i.e. sums of linear forms and constants in $\mathbb{F}_2$). Equivalently, all its second-order derivatives $D_a D_b f(x) = f(x+a+b) + f(x+a) + f(x+b) + f(x)$ are constant, and still equivalently, all its third-order derivatives $D_a D_b D_c f(x) = \sum_{y \in x + \langle a,b,c \rangle} f(y)$ are identically 0. Two n-variable Boolean functions f, g will be called *affine equivalent* if there exists an affine permutation $x \mapsto x \times M + a$ (where M is an invertible $n \times n$ matrix) such that $g = f \circ A$. They are called *EA equivalent* if g is affine equivalent to the sum of f and an affine Boolean function. A notion (or a parameter) on $\mathcal{B}_n$ will be called an *affine invariant* if it is preserved by affine equivalence. More on Boolean functions and equivalences can be found in [11] (as almost all that we shall recall in this section).

The inner product[3] in $\mathbb{F}_2^n$ we will consider in this paper is the usual dot product, defined for every $x = (x_1, \ldots, x_n), y = (y_1, \ldots, y_n) \in \mathbb{F}_2^n$ as $x \cdot y = \sum_{i=1}^n x_i y_i$ where this sum is calculated in $\mathbb{F}_2$; however, our results would hold (and be equivalent) for any symmetric non-degenerate bilinear form. The vector space of functions $x \in \mathbb{F}_2^n \mapsto u \cdot x$ equals that of all linear functionals from $\mathbb{F}_2^n$ to $\mathbb{F}_2$. Given a linear mapping $L : \mathbb{F}_2^n \to \mathbb{F}_2^n$, we call the *adjoint operator* of L the unique linear function L^* such that, for every $x, y \in \mathbb{F}_2^n$, we have $x \cdot L(y) = L^*(x) \cdot y$.

[2] This is equivalent to saying that the algebraic degree is at most 2, see [11].

[3] We do not require positive definiteness in the definition of an inner product, since we are in a nonzero characteristic; this condition is replaced by non-singularity.

For any n-variable Boolean function $f : \mathbb{F}_2^n \to \mathbb{F}_2$, we define the Walsh transform of f:

$$W_f(u) = \sum_{x \in \mathbb{F}_2^n} (-1)^{f(x)+u\cdot x}; u \in \mathbb{F}_2^n,$$

where the sum is calculated in $\mathbb{Z}$. We have the so-called Parseval relation $\sum_{u\in\mathbb{F}_2^n} W_f^2(u) = 2^{2n}$, which implies $\max_{u\in\mathbb{F}_2^n} W_f^2(u) \geq 2^n$. An n-variable Boolean function is called *bent* if it achieves this bound with equality, that is, its Walsh transform takes values $\pm 2^{n/2}$ only (where n is necessarily even). Equivalently, the minimum Hamming distance between f and affine Boolean functions (called the nonlinearity of f) takes the maximum value $2^{n-1} - 2^{n/2-1}$. There exists then a Boolean function $\widetilde{f}$ such that $W_f(u) = 2^{n/2}(-1)^{\widetilde{f}(u)}$. This (also bent) function $\widetilde{f}$ is called the *dual* of f. For any $n \geq 4$, the $(n/2+1)$th order derivative of any bent function vanishes (we say that f has an algebraic degree at most $n/2$). For $n = 2$, f is bent if and only if it is not affine. A function f is affine if and only if its Walsh support $\mathrm{supp}(W_f) = \{u \in \mathbb{F}_2^n; W_f(u) \neq 0\}$ is a singleton. Finally, a Boolean function is bent if and only if all its derivatives $D_a f$, where $a \neq 0$, are balanced.

Partially-bent functions were first introduced by the first author in [8] while studying a conjecture of [32], which led to a class of functions generalizing quadratic functions and bent functions. The simplest way to define them is as follows: an n-variable Boolean function is partially-bent if it is EA equivalent to a function of the form $f(x_1, \ldots, x_n) = g(x_1, \ldots, x_r)$, where g is a bent r-variable Boolean function, that is, f is EA equivalent to an extension of a bent function with the possibility of free variables. More precisely, there exist two linear subspaces E (of an even dimension) and E' of $\mathbb{F}_2^n$, whose direct sum equals $\mathbb{F}_2^n$, and Boolean functions g, bent on E, and h, affine on E', such that $f(x + x') = g(x) + h(x')$ for all $(x, x') \in E \times E'$. Equivalently, a partially-bent function is a Boolean function whose derivatives are constant or balanced. All quadratic Boolean functions and all bent Boolean functions are partially-bent. Note that since for $r \geq 4$, g has an algebraic degree of at most $r/2$ and for $r = 2$, it is quadratic, then f has an algebraic degree of at most $n/2$ or is quadratic. In particular, for $n \leq 4$, f is quadratic.

A plateaued Boolean function $f\colon \mathbb{F}_2^n \to \mathbb{F}_2$ is a function whose Walsh transform $W_f(u) = \sum_{x\in\mathbb{F}_2^n}(-1)^{f(x)+u\cdot x}$ only takes values $\{0, \pm\lambda\}$ for some non-negative integer λ (which is, because of the Parseval's relation, a power of 2 whose exponent is at least $\frac{n}{2}$, and is called the amplitude of f). The notion of plateauedness is affine invariant.

Partially-bent functions are those plateaued functions whose Walsh support $\mathrm{supp}(W_f)$ is an affine space (see [11, Subsection 6.2.2]).

Since we are interested in the plateauedness of the restrictions of Boolean functions to affine subspaces of $\mathbb{F}_2^n$, we need to define it properly. All affine invariant notions can be defined for functions over affine spaces. This fact is often used in papers but rarely explained explicitly, which we do now. Let N be an affine invariant notion on Boolean functions (such as plateauedness) and P be an affine invariant parameter of Boolean functions (such as algebraic degree, nonlinearity, algebraic immunity, etc., see [11]). Then N and P can be defined for any function $f : A \to \mathbb{F}_2$ (or more generally for every vectorial Boolean function $F : A \to \mathbb{F}_2^m$) where A is an affine subspace of $\mathbb{F}_2^n$. More precisely, suppose $A = a + \langle e_1, \ldots, e_k\rangle$ where $\{e_1, \ldots, e_k\}$ is a linearly independent family generating the underlying vector space of A. We define $N(f)$ (resp. $P(f)$) as equal to $N(g)$ (resp. $P(g)$), where g is the k-variable Boolean function defined by $g(x_1, \ldots, x_k) = f(a+x_1e_1+\cdots+x_ke_k)$, that is, $g = f \circ \phi$, where $\phi : \mathbb{F}_2^k \to A$ is an affine isomorphism. Indeed, $N(g)$ and $P(g)$ do not depend on the choice of a nor of that of the basis $(e_1, \ldots, e_k)$, thanks to affine invariance, because changing a or $e_1, \ldots, e_k$ changes g into an affine equivalent function.

In particular, we say that f is plateaued on A if there is an affine isomorphism $\phi : \mathbb{F}_2^k \to A$ such that $f \circ \phi$ is plateaued. This is equivalent to saying that, for every $u \in \mathbb{F}_2^n$, we have that $W_{f|_A}(u) = \sum_{x\in A}(-1)^{f(x)+u\cdot x}$ equals 0 or $\pm\lambda$, where λ is some integer (equal to a power of 2 whose exponent is at least $k/2$, according to Parseval's relation). Indeed, the set of Walsh transform absolute values of a function over an affine space A is the set of correlation absolute values between the function and the affine Boolean functions over A, and it is then equal to the set of values $|\sum_{x\in A}(-1)^{f(x)+u\cdot x}|$ where u ranges over $\mathbb{F}_2^n$ (but the absolute values of the Walsh transform are repeated several times when considering $|\sum_{x\in A}(-1)^{f(x)+u\cdot x}|$ for all $u \in \mathbb{F}_2^n$).

Remark 1. *The Walsh transform of a restriction, when defined as equal to W_g, where there is an affine isomorphism $\phi : \mathbb{F}_2^k \to A$ such that $g = f \circ \phi$, depends not only on the choice of the inner product "$\cdot$" but also on the choice of ϕ. Write $\phi(u) = a + \psi(u)$, where $\psi\colon \mathbb{F}_2^k \to V$ is an invertible linear mapping with $A = a + V$ for $a \in \mathbb{F}_2^n$. To avoid ambiguity, we denote by $\langle\cdot,\cdot\rangle_k$ and $\langle\cdot,\cdot\rangle_n$ the dot product on $\mathbb{F}_2^k$ and $\mathbb{F}_2^n$, respectively. We then have for $u \in \mathbb{F}_2^k$, $W_g(u) = \sum_{x\in A}(-1)^{f(x)+\langle u,\psi^{-1}(x+a)\rangle_k}$. For a fixed $u \in \mathbb{F}_2^k$, the function $v \mapsto \langle u, \psi^{-1}(v)\rangle_k$ is a linear functional on V, and so it is in V^* (that is, the dual of V), and moreover, there is a unique coset $w + V^\perp$ such that $\langle u, \psi^{-1}(v)\rangle_k = \langle w + v', v\rangle_n = \langle w, v\rangle_n$ for all $v \in V$ and $v' \in V^\perp$, implying (after replacing v by $x + a$): $W_g(u) = (-1)^{\langle w,a\rangle_n}\sum_{x\in A}(-1)^{f(x)+\langle w,x\rangle_n}$. So, as w ranges over some k-dimensional subspace $W \subseteq \mathbb{F}_2^n$ such that $W \oplus V^\perp = \mathbb{F}_2^n$, the values that $W_{f|_A}(w) = \sum_{x\in A}(-1)^{f(x)+\langle w,x\rangle_n}$ takes are equal to the Walsh spectrum of g, up to taking absolute values. Also, when w ranges over $\mathbb{F}_2^n$, the values that $W_{f|_A}(w)$ takes are equal to the Walsh spectrum of $f|_A$ repeated 2^{n-k} times.*

We now recall the following elementary group-theoretic fact that we will require in the proof of Lemma 4. If $S \subseteq G$ is a non-empty subset of an additive group G such that $g + S = \{g + s : s \in S\}$ is either equal to S or disjoint from S for all $g \in G$, then S is a right-coset of a subgroup of G. We provide a short proof for the sake of self-containment. Let $H = \mathrm{Stab}(S) = \{g \in G : g + S = S\}$. Let $s_0 \in S$. Since $h + S = S$ for all $h \in H$, we have $H + s_0 \subseteq S$. Let us show $S \subseteq H + s_0$. If $s \in S$, then $((s - s_0) + S) \cap S \neq \emptyset$, implying $(s - s_0) + S = S$ by our hypothesis. Hence, $s \in H + s_0$ for all $s \in S$, i.e. $S \subseteq H + s_0$. Thus, $S = H + s_0$.

3 Study of the class of n-variable Boolean functions whose restrictions to k-dimensional spaces are plateaued

Since plateaued functions play an important role nowadays in the study of Boolean functions for cryptography, and since studying the restrictions of Boolean functions to affine subspaces is also becoming increasingly relevant, it seems natural to study the class of those n-variable Boolean functions whose restrictions to all affine subspaces of $\mathbb{F}_2^n$ of some dimension are plateaued.

Definition 1. *Let n, k be any positive integers satisfying $0 \leq k \leq n$. We denote by C_k^n the class of n-variable Boolean functions whose restrictions to all k-dimensional affine spaces are plateaued.*

The set C_n^n is by definition the set of plateaued n-variable functions. Of course, every quadratic function (of algebraic degree at most 2) belongs to C_k^n for every k, since the restriction of a quadratic function is quadratic and then plateaued (it is quadratic because its third-order derivatives being identically zero, the restrictions of these derivatives are also identically zero). The sets C_0^n, C_1^n and

C_2^n equal the whole space $\mathcal{B}_n$ of n-variable Boolean functions for every n, since the restrictions of f that we consider being then in at most 2 variables, they have an algebraic degree of at most 2. We need to determine what are the sets C_k^n for $3 \leq k \leq n-1$. We are also interested in determining those Boolean functions whose restrictions are partially-bent. Our main result will be the following.

Theorem 1. *Let n be any positive integer such that $n \geq 4$. Let f be any n-variable Boolean function. Then f is partially-bent if and only if $f \in C_{n-1}^n$. Moreover, for all $3 \leq k \leq n-2$, C_k^n is equal to the set of quadratic Boolean functions in n variables (whose restrictions are quadratic and hence partially-bent). Consequently, for all $3 \leq k \leq n-1$, the class of n-variable Boolean functions whose restrictions to all k-dimensional affine spaces are partially-bent is equal to the set of quadratic Boolean functions in n variables.*

We shall need a series of lemmas for proving it. Notice that an n-variable Boolean function f belongs to C_k^n, if and only if, for any $(n-k)$-dimensional linear subspace[4] L and any coset A of $L^\perp$, there exists λ_A such that, for all $u \in \mathbb{F}_2^n$, we have $\sum_{x\in A}(-1)^{f(x)+u\cdot x} \in \{0, \pm\lambda_A\}$. As we noticed in Remark 1, we can reduce the range of u to a vector space whose direct sum with L equals $\mathbb{F}_2^n$. But we can also have u ranging over $\mathbb{F}_2^n$, the only effect of this being that we visit several times each value of the Walsh transform of the restriction of f to A. Note that the value λ_A does not depend only on L in this definition.

Using the Poisson summation formula (see [11, Relation 2.41]), the condition is equivalent to

$$\forall a, u \in \mathbb{F}_2^n, \frac{1}{|L|}\sum_{v\in u+L}(-1)^{a\cdot v}W_f(v) \in \{0, \pm\lambda_{a+L^\perp}\}. \tag{1}$$

The sum of an affine function and of a function in C_k^n belongs to C_k^n, since the restriction of the affine function is affine and the sum of an affine function and a plateaued function is plateaued. Since plateauedness is also affine invariant, the set C_k^n is then preserved by EA equivalence.

Given $k < l < n$, an n-variable Boolean function belongs to C_k^n if and only if all its restrictions to l-dimensional affine spaces belong to C_k^l. Hence, one might have the impression that the larger k is, the weaker the condition for belonging to C_k^n and the larger C_k^n is. But we shall see that this is not quite true. We will have that, when $n \geq 5$ and $3 \leq k \leq n-2$, C_k^n is a strict subset of C_{n-1}^n and all these sets C_k^n will be equal to each other, which does not contradict the impression above. But we shall see that C_2^n is a strict superset of C_3^n, which does contradict it.

We now recall from [6] that, for every n even, any bent n-variable function belongs to C_{n-1}^n. We include a proof for our paper to be self-contained. More results on the restrictions of bent functions to 1-codimensional and 2-codimensional affine subspaces can be found in [6] (where plateaued functions are called "three valued"). We show also that the only bent functions in C_{n-2}^n are quadratic, which is a new result.

Lemma 1. *Assume that n is even and that $f\colon \mathbb{F}_2^n \to \mathbb{F}_2$ is a bent function. Then $f \in C_{n-1}^n$. Moreover, $f \in C_{n-2}^n$ if and only if f is quadratic.*

Proof. For every Boolean function f, linear hyperplane $H = \{0, e\}^\perp$, and vector $a \in \mathbb{F}_2^n$, we have:

$$W_{f_{|H}}(a) = \frac{W_f(a) + W_f(a+e)}{2} \quad \text{and} \quad W_{f_{|H^c}}(a) = \frac{W_f(a) - W_f(a+e)}{2},$$

[4] It will slightly simplify our presentation to introduce a symbol for the orthogonal of the linear space underlying the affine space A rather than for the linear space itself; in practice we will deal more with those L having a small dimension.

where $H^c = \mathbb{F}_2^n \setminus H$. In both cases, since f is bent, we obtain a value of the form $\pm 2^{n/2-1} \pm 2^{n/2-1}$ (where the two consecutive $\pm$ do not necessarily represent the same sign) belonging then to $\{0, \pm 2^{n/2}\}$. Both functions $f_{|H}$ and $f_{|H^c}$ are then plateaued (with the same amplitude $2^{n/2}$), and f belongs then to C_{n-1}^n.
For the second part, we first observe that $n-2$ is non-negative as it should be. Given L of dimension 2, relation (1) is equivalent to

$$\frac{1}{4} \sum_{v \in u+L} (-1)^{a \cdot v} W_f(v) \in \{0, \pm \lambda_{a+L^\perp}\},$$

that is,

$$\sum_{v \in u+L} (-1)^{\widetilde{f}(v)+a \cdot v} \in \{0, \pm c_{L,a}\},$$

for some $c_{L,a} \in \{2, 4\}$ and every $u \in \mathbb{F}_2^n$, where $\widetilde{f}$ is the dual of f. Two cases happen according to whether $c_{L,a} = 2$ or $c_{L,a} = 4$: (1) for all u, the function $\widetilde{f}(v) + a \cdot v$ is either balanced on $u + L$ or it has an odd weight on $u + L$, (2) for all u, the function $\widetilde{f}(v) + a \cdot v$ is constant or balanced on $u + L$, or equivalently, denoting $L = \langle e_1, e_2 \rangle$, the second-order derivative $D_{e_1} D_{e_2} \widetilde{f}$ is identically 0. Now, assume that $f \in C_{n-2}^n$. The dual of a quadratic bent Boolean function is also quadratic (see e.g. [11]), and so it suffices to show that $D_{e_1} D_{e_2} \widetilde{f}$ is constant for any linearly independent $e_1, e_2 \in \mathbb{F}_2^n$. Still denoting $L = \langle e_1, e_2 \rangle$, if there exists $a \in \mathbb{F}_2^n$ such that $c_{L,a} = 4$, then as we saw above, $D_{e_1} D_{e_2} \widetilde{f}$ is identically zero. So, assume that $c_{L,a} = 2$ for all $a \in \mathbb{F}_2^n$, and moreover, assume for the sake of a contradiction that there exists $x_0 \in \mathbb{F}_2^n$ such that $D_{e_1} D_{e_2} \widetilde{f}(x_0) = 0$. Then, $\widetilde{f}|_{x_0+L}$ is affine because it has an even weight and any even weight Boolean function over $\mathbb{F}_2^2$ is affine. There exists a linear function $\ell \colon \mathbb{F}_2^n \to \mathbb{F}_2$ such that $\widetilde{f}|_{x_0+L} + \ell|_{x_0+L}$ is constant. Since there exists $a \in \mathbb{F}_2^n$ such that $\ell(v) = a \cdot v$ for all $v \in \mathbb{F}_2^n$, we have that $\widetilde{f}(v) + a \cdot v$ is constant as v ranges across $x_0 + L$, implying $c_{L,a} = 4$, a contradiction. Thus, $D_{e_1} D_{e_2} \widetilde{f}$ is identically 1. From the above two cases, all second-order derivatives of $\widetilde{f}$ are constant, and so f is quadratic. □

As previously mentioned, it seems natural that the chain of inclusions $C_3^n \subseteq C_4^n \subseteq \cdots \subseteq C_{n-1}^n \subseteq C_n^n$ holds. However, in the proof of following lemma, we will see that this result is slightly more involved than expected and that the additional condition $n \geq 4$ is required.

Lemma 2. *Let n and k be positive integers satisfying $3 \leq k < n$. Then $C_k^n \subseteq C_{k+1}^n$.*

Proof. Let us first address the case $k = n - 1$, that is, prove that, for $n \geq 4$, all the elements in C_{n-1}^n are plateaued functions. Let $f \in C_{n-1}^n$ with $n \geq 4$. For every nonzero vector $e \in \mathbb{F}_2^n$, there exist integers i_e, j_e such that, for every vector a, we have $W_f(a) + W_f(a+e) \in \{0, \pm 2^{i_e}\}$ and $W_f(a) - W_f(a+e) \in \{0, \pm 2^{j_e}\}$. That is, for distinct $a, b \in \mathbb{F}_2^n$, we have $W_f(a) + W_f(b) \in \{0, \pm 2^{i_{a+b}}\}$ and $W_f(a) - W_f(b) \in \{0, \pm 2^{j_{a+b}}\}$.
Multiplying and denoting $k_e = i_e + j_e$, if $W_f^2(a), W_f^2(b), W_f^2(c)$ are distinct and sorted such that $W_f^2(a) > W_f^2(b) > W_f^2(c)$, then we have $W_f^2(a) - W_f^2(b) = 2^{k_{a+b}}$ and $W_f^2(b) - W_f^2(c) = 2^{k_{b+c}}$, and $W_f^2(a) - W_f^2(c)$ equals $2^{k_{a+c}} = 2^{k_{a+b}} + 2^{k_{b+c}}$, and therefore, $k_{a+b} = k_{b+c}$ (and $k_{a+c} = k_{a+b} + 1$), that is, given three vectors a, b, c such that $W_f^2(a), W_f^2(b), W_f^2(c)$ are distinct, there is an order on $W_f^2(a), W_f^2(b), W_f^2(c)$ which puts them in an arithmetic progression. This excludes that the image set of W_f^2 has size more than 3.

The image set of W_f^2 cannot have size 3 either, because the only triplets of squares in an arithmetic progression have common differences that are not powers of 2. Indeed, suppose that we have three squares $A^2, B^2 = A^2 + 2^k$ and $C^2 = A^2 + 2^{k+1}$, then $(B-A)(B+A) = (C-B)(C+B) = 2^k$ and $(C-A)(C+A) = 2^{k+1}$ and then $B - A = 2^r, B + A = 2^{k-r}, C - B = 2^s, C + B = 2^{k-s}$ and $C - A = 2^t = 2^r + 2^s$, so $s = r$. But we arrive to a contradiction since $C + B \neq B + A$. We have then proved that the image set of W_f^2 has size 1 (and we know that f is then bent, because of Parseval's relation) or has size 2. Let us now prove that in this latter case, f is necessarily plateaued.
Assume that the image of W_f^2 is equal to $\{A^2, B^2\}$ with $0 \leq B < A$ and that A^2 is matched at least twice by W_f^2. Let $a, b \in \mathbb{F}_2^n$ be then distinct such that $A^2 = W_f^2(a) = W_f^2(b)$. Then $W_f(a)+W_f(b) \in \{0, \pm 2A\}$ and $W_f(a) - W_f(b) \in \{0, \pm 2A\}$, and exactly one of $W_f(a) + W_f(b)$ or $W_f(a) - W_f(b)$ has absolute value $2A \neq 0$. By our assumption above, we have $\pm 2A$ is equal to one of $\pm 2^{i_{a+b}}$ or $\pm 2^{j_{a+b}}$, and so A is a power of 2. Taking now x and $e \neq 0$ such that $W_f^2(x) = A^2$ and $W_f^2(x+e) = B^2$, we have $W_f^2(x) - W_f^2(x+e) \in \{0, \pm 2^{k_e}\}$. Since $A^2 > B^2$, we have $W_f^2(x) - W_f^2(x+e) = 2^{k_e}$. Then $(A-B)(A+B) = 2^{k_e}$, and so there exists $r \geq 0$ such that $A - B = 2^r$ and $A + B = 2^{k_e - r}$, and so $2A = 2^r + 2^{k_e - r}$. Since we already have that A is a power of 2, it follows that $r = k_e - r$, and so $A = 2^r$. Thus $2^r - B = A - B = 2^r$ implies $B = 0$. So, W_f^2 has image $\{0, A^2\}$ and f is plateaued.
The remaining case is when $|\{u \in \mathbb{F}_2^n : W_f^2(u) = A^2\}| = 1$ (and therefore, $|W_f(x)| = B$ for every $x \neq a$, where a is the unique element such that $|W_f(a)| = A$). Let us prove that it can happen only if f is affine. If $B = 0$, then f is affine, so we assume now $0 < B < A$. Since $2^n - 1 \geq 3$, there exist $b, e \in \mathbb{F}_2^n$ with $e \neq 0$ such that $|W_f(b)| = |W_f(b+e)| = B$ and one of $W_f(b) + W_f(b+e)$ or $W_f(b) - W_f(b+e)$ must be equal to a power of 2, implying $2B$ is a power of 2, and so B is too. Moreover, $A \neq B$ and $|W_f(a+e)| = B$ imply that $W_f(a) + W_f(a+e) = \pm 2^{i_e}$ and $W_f(a) - W_f(a+e) = \pm 2^{j_e}$, and both the difference and sum of A and B is a power of 2. So let us write $A + B = 2^r$ and $A - B = 2^s$. Then $2B = 2^r - 2^s = 2^s(2^{r-s} - 1)$, implying $2^{r-s} - 1 = 1$, so $r = s + 1$. Hence, $A = 3B$ and $A = 3 \cdot 2^{s-1}$ and $B = 2^{s-1}$. Parseval's relation then provides $2^{2n} = (2^n - 1)B^2 + A^2 = (2^n - 1)B^2 + 9B^2 = (2^n + 8)B^2$. However, $2^n + 8$ is not a power of 2 since $n \geq 4$. We arrive then to a contradiction and f is then plateaued. This concludes the proof that $C_{n-1}^n \subset C_n^n$ for all $n \geq 4$.
Note that this implies that, for every $k \geq 3$ and $n > k$, we have $C_k^n \subseteq C_{k+1}^n$ (recall that C_n^n is the class of n-variable plateaued functions). Indeed, if $f \in C_k^n$, then considering a restriction of f onto a $(k+1)$-dimensional affine subspace and call it g, we have $g \in C_k^{k+1}$ as $k + 1 \geq 4$, so $g \in C_{k+1}^{k+1}$ by the previous part of this proof, and then $f \in C_{k+1}^n$. □

Let us show now that not only bent functions belong to C_{n-1}^n, but more generally, so do all partially-bent functions, and let us also characterize the membership of such functions to C_{n-2}^n.

Lemma 3. *Let $f : \mathbb{F}_2^n \to \mathbb{F}_2$ be a partially-bent function. Then $f \in C_{n-1}^n$. Moreover, if $n \geq 2$, then $f \in C_{n-2}^n$ if and only if f is quadratic.*

Proof. Up to affine equivalence and the addition of an affine function, which both preserve C_{n-1}^n, we can take $f(x, y) = g(x)$ where $x \in \mathbb{F}_2^r$, with r even, and $y \in \mathbb{F}_2^{n-r}$ and g is bent. Let H be an affine hyperplane of $\mathbb{F}_2^n$. Then H is defined by one of the following two manners:
- H has an equation of the form $x_i = \ell(\widehat{x}, y)$, where $\widehat{x}$ is x deprived of its ith coordinate and ℓ is an $(n-1)$-variable affine function in $(\widehat{x}, y)$,
- H has an equation of the form $y_i = \ell(x, \widehat{y})$, where $\widehat{y}$ is y deprived of its ith coordinate and ℓ is an $(n-1)$-variable affine function in $(x, \widehat{y})$.
In the latter case, $f_{|H}$ has the same form as f and is then plateaued. Indeed, up to affine equivalence,

$W_f(a,b)$ equals $W_{f_{|H}}(a,\widehat{b})$ if $b_i=0$ and $W_f(a,b)$ equals 0 otherwise.
In the former case, we have $f_{|H}(\widehat{x},y)=g(x_1,\ldots,x_{i-1},\ell(\widehat{x},y),x_{i+1},\ldots,x_r)$. If $\ell(\widehat{x},y)$ does not depend on y, then since $g\in C^r_{r-1}$ (as g is bent) and $g(x_1,\ldots,x_{i-1},\ell(\widehat{x},y),x_{i+1},\ldots,x_r)$ is its restriction to a hyperplane, we know that $\widehat{x}\mapsto g(x_1,\ldots,x_{i-1},\ell(\widehat{x},y),x_{i+1},\ldots,x_r)$ is plateaued, and in particular, this implies $f_{|H}$ is also plateaued. If $\ell(\widehat{x},y)$ does depend on y, say on y_1, then we know that $f_{|H}$ is affine equivalent to the function

$$(x_1,\ldots,x_r,y_2,\ldots,y_{n-r})\mapsto g(x_1,\ldots,x_r),$$

(by renaming y_1 as x_i) which is plateaued. We note that we have proved in fact that if, given any positive integer $r\leq n$, for every $x\in\mathbb{F}_2^r$ and $y\in\mathbb{F}_2^{n-r}$, we have $f(x,y)=g(x)$ where g is any r-variable plateaued function, then f belongs to C^n_{n-1} if and only if g belongs to C^r_{r-1}.
If $f\in C^n_{n-2}$, then if $n\leq 4$, we know that f is quadratic, and if $n\geq 5$, then according to Lemma 2, it is plateaued and belongs to C^n_{n-1} and then, according to the observation above, g belongs to C^r_{r-1} (if $r\leq 3$, we know this is true for every r-variable Boolean function) and to C^r_{r-2} (the restrictions of g to affine hyperplanes being in C^{r-1}_{r-2}; if $r\leq 4$, we know this is true for every r-variable Boolean function). Since we proved that any bent function f belongs to C^n_{n-2} (that is, to $\bigcap_{i=n-2}^n C^n_i$) if and only if it is quadratic, this generalizes to partially-bent functions. □

Remark 2. *We provide an alternative (and simpler) proof that partially-bent functions are in C^n_{n-1} as we believe both proofs are useful for understanding the situation, and this second proof will be useful in Theorem 2 below. We know that partially-bent functions are those plateaued functions whose Walsh support $S=\mathrm{supp}(W_f)$ is an affine space, as recalled in Section 2. We have $W_f(a)=\pm\lambda$ if $a\in S$ and $W_f(a)=0$ otherwise. Since S is an affine space, then for every nonzero $e\in\mathbb{F}_2^n$, we have $e+S=S$ if e belongs to the underlying vector space of S (which we will see in Section 4.1 is equal to the orthogonal of the linear kernel of f), and $S\cap(e+S)=\emptyset$ otherwise. Then, denoting again $H=\{0,e\}^\perp$, we have that $W_{f_{|H}}(a)=\frac{W_f(a)+W_f(a+e)}{2}$ and $W_{f_{|H^c}}(a)=\frac{W_f(a)-W_f(a+e)}{2}$ both belong to $\{0,\pm\lambda\}$ for every vector $a\in\mathbb{F}_2^n$ in the first case, and to $\{0,\pm\frac{\lambda}{2}\}$ in the second case.*

To prove Theorem 1, it suffices now to show that any function in C^n_{n-1} is indeed partially-bent.

Lemma 4. *Let $n\geq 4$. Then $f\in C^n_{n-1}$ if and only if f is partially-bent.*

Proof. We have already seen by Lemma 3 that if f is partially-bent, then f is in C^n_{n-1}, so it remains to prove the converse. Let $f\in C^n_{n-1}$. By Lemma 2, f is plateaued, and let us denote its amplitude by A. As we already mentioned, partially-bent functions are equivalently defined as plateaued functions with affine Walsh supports, so it suffices to show that the Walsh support of f is an affine space.
Since $f\in C^n_{n-1}$, for any nonzero $e\in\mathbb{F}_2^n$, we know that either $W_f(a)\neq 0$ if and only if $W_f(a+e)\neq 0$ for all $a\in\mathbb{F}_2^n$, or $W_f(a)\neq 0$ implies $W_f(a+e)=0$ for all $a\in\mathbb{F}_2^n$, as otherwise the restriction of f to an affine hyperplane with underlying vector space $\{0,e\}^\perp$ would not be plateaued. Note that if $e\in\mathbb{F}_2^n\setminus\{0\}$ satisfies the first case, then $\mathrm{supp}(W_f)=\mathrm{supp}(W_f)+e$, where $\mathrm{supp}(W_f)$ is the Walsh support of f, and if $e\in\mathbb{F}_2^n$ is in the second case, then $\mathrm{supp}(W_f)$ and $\mathrm{supp}(W_f)+e$ are disjoint.
Taking $G=\mathbb{F}_2^n$ and $S=\mathrm{supp}(W_f)$, we see that S is a non-empty subset of an additive group such that its translations (i.e. the sets $g+S$ for any $g\in G$) are equal to S or disjoint from S, implying S is a right-coset of a subgroup of G (see the preliminaries section). That is, S is an affine subspace and f is therefore partially-bent. □

Theorem 1 immediately follows. Indeed, Lemma 4 characterizes partially-bent functions as those functions in C^n_{n-1}, and if $3 \leq k \leq n-2$ and $f \in C^n_k$, then f is a partially-bent function in C^n_{n-2} by Lemma 2, implying it is quadratic by Lemma 3. The last sentence of Theorem 1 comes from the fact that if all the restrictions of f to all k-dimensional affine spaces are partially-bent then f belongs to C^n_{k-1}. This completes the proof if $k \geq 4$. If $k = 3$, the restrictions to 3-dimensional affine spaces are quadratic since they are partially-bent, and this completes the proof.

Remark 3. *The restrictions of non-quadratic partially-bent functions to affine hyperplanes provide numerous examples of plateaued non-partially-bent functions. Indeed, we observed in computer investigations that most restrictions of such functions to affine hyperplanes are not partially-bent. In the case that f is a so-called Maiorana-McFarland bent function [20], this can be checked mathematically: the input to f is written in the form (x, y) where $x, y \in \mathbb{F}_2^m$ and $m = n/2$; we define $f(x, y) = x \cdot \pi(y) + g(y)$, where π is a permutation of $\mathbb{F}_2^m$ and g is a Boolean function on $\mathbb{F}_2^m$ (and $+$ is the addition in $\mathbb{F}_2$). The derivatives of f have the form $D_{(a,b)}f(x, y) = x \cdot D_b\pi(y) + a \cdot \pi(y + b) + D_b g(y)$ (and it is well-known that if $b \neq 0$ then since $D_b\pi(y) \neq 0$ for every y, we have that $D_{(a,b)}f$ is balanced, and if $b = 0$ and $a \neq 0$ then $D_{(a,b)}f(x, y) = a \cdot \pi(y)$ is also balanced). However, the derivatives of the restriction of f to a hyperplane H of equation $u \cdot x + v \cdot y = \epsilon$ (where $(u, v) \in (\mathbb{F}_2^m)^2 \setminus \{(0, 0)\}$, $\epsilon \in \mathbb{F}_2$) are in general neither constant nor balanced (this is because either $u \neq 0$ and the equation of H can then be written in the form $x_i = \widehat{u} \cdot \widehat{x} + v \cdot y + \epsilon$, or $v \neq 0$ and the equation becomes $y_i = u \cdot x + \widehat{v} \cdot \widehat{y} + \epsilon$, and in both cases, the restriction of $D_{(a,b)}f(x, y)$ (where $u \cdot a + v \cdot b = 0$) does not have the same properties as $D_{(a,b)}f$ itself, which made it balanced).*
The fact that a majority of the restrictions of a non-quadratic bent function to hyperplanes are not partially-bent is proved theoretically in the next proposition, as the consequence of an interesting property of bent functions.

Proposition 1. *Let f be a bent n-variable Boolean function. Let H be an affine hyperplane with underlying vector space $\{0, e\}^\perp$. Then $f|_H$ is partially-bent if and only if the Boolean function $D_e\widetilde{f}$ is affine. The set E of those $e \in \mathbb{F}_2^n$ such that f is partially-bent on $\{0, e\}^\perp$ (equivalently, on its complement if $e \neq 0$) is then a subspace. This implies that, if f is non-quadratic, a majority of the restrictions of f to hyperplanes are not partially-bent.*

Proof. We know that $f|_H$ is plateaued, and by the relation $W_{f|_H}(u) = \frac{1}{2}\big(W_f(u) + (-1)^\epsilon W_f(u+e)\big) = 2^{n/2-1}\Big((-1)^{\widetilde{f}(u)} + (-1)^\epsilon (-1)^{\widetilde{f}(u+e)}\Big)$, where $e \cdot x = \epsilon$ for all $x \in H$, we know that $supp(W_{f|_H}) = \{u \in \mathbb{F}_2^n : D_e\widetilde{f}(u) = \epsilon\}$. We have that $f|_H$ is partially-bent if and only if the set $\{u \in \mathbb{F}_2^n : D_e\widetilde{f}(u) = \epsilon\}$ is an affine space[5], but $\widetilde{f}$ is bent and so its nonzero derivatives are balanced, and therefore this is the same as saying $D_e\widetilde{f}$ is affine. The set $E = \{e \in \mathbb{F}_2^n \setminus \{0\} : D_e\widetilde{f} \text{ is affine}\}$ is such that $E \cup \{0\}$ is a subspace. If f is non-quadratic, then $\widetilde{f}$ is non-quadratic, so the subspace $E = \{e \in \mathbb{F}_2^n : D_e\widetilde{f} \text{ is affine}\}$ is not equal to $\mathbb{F}_2^n$ and has then size at most 2^{n-1}. This implies there can be at most $2(2^{n-1} - 1) = 2^n - 2$ affine hyperplanes of which a non-quadratic bent function is partially-bent on, and this is strictly less than half of the total number $2(2^n - 1) = 2^{n+1} - 2$ of affine hyperplanes. □

[5]We know that $f|_H$ is partially-bent if and only if the function $f \circ \phi$ is partially-bent, where $\phi : \mathbb{F}_2^{n-1} \to H$ is an affine isomorphism. We have then that $f|_H$ is partially-bent if and only if the support of $W_{f\circ\phi}$ is an affine space, and we can check that this is equivalent to the fact that the set $supp(W_{f|_H})$ is an affine space, since assuming without loss of generality that $H = \langle e_1, \ldots, e_{n-1}\rangle$ where $(e_1, \ldots, e_n)$ is the standard basis, and ϕ is linear such that $\phi(e_i) = e_i$ for $i = 1, \ldots, n-1$, we have $supp(W_{f|_H}) = supp(W_{f\circ\phi}) \times \{0\}$.

Remark 4. *Of course, the question whether we can generalize this result to partially-bent functions arises. That is, if f is non-quadratic partially-bent, are less than half of its restrictions to hyperplanes partially-bent?*
Up to EA equivalence, considering a partially-bent function consists in taking an r-variable bent function $f(x_1, \ldots, x_r)$ and adding fictitious variables $x_{r+1}, \ldots, x_n$. The hyperplane has equation $\sum_{j=1}^{n} a_j x_j = \epsilon$ for some nonzero $(a_1, \ldots, a_n) \in \mathbb{F}_2^n$ and some $\epsilon \in \mathbb{F}_2$. Two cases occur: $a_{r+1} = \cdots = a_n = 0$ or there exists $i \in \{r+1, \ldots, n\}$ such that $a_i = 1$. In the latter case the restriction is just f with $n-r-1$ fictitious variables (because replacing x_i by its value given by the equation does not change the expression of the function) and it is partially-bent. In the former case, the restriction is EA equivalent to a restriction of a bent function with $n-r$ fictitious variables (because we restrict within the r first variables). Clearly, it is no more true that less than half of the restrictions to hyperplanes are partially-bent. In fact, the latter case makes that if $n-r-1 \geq 0$, more than half of the restrictions are partially-bent.

4 Study of the class of n-variable plateaued Boolean functions that are restrictions of $(n+1)$-variable partially-bent functions

Since the restrictions of non-quadratic partially-bent functions are plateaued but are not all partially-bent, a natural problem is to determine all those plateaued functions which are the restrictions of partially-bent functions in one more variable. Note that there exists a partially-bent function $g : \mathbb{F}_2^{n+1} \to \mathbb{F}_2$ whose restriction to an affine hyperplane is affine equivalent to a given n-variable function f if and only if (by composing g by an appropriate affine automorphism of $\mathbb{F}_2^{n+1}$) there exists an $(n+1)$-variable partially-bent function g' whose restriction to $\mathbb{F}_2^n \times \{0\}$ coincides with f. Clearly, all partially-bent functions have this property, since any n-variable partially-bent function f is the restriction of the $(n+1)$-variable function $g(x_1, \ldots, x_{n+1}) = f(x_1, \ldots, x_n)$. Determining all the other functions having the property, in general, seems challenging.

The sub-problem of determining (for n odd) the restrictions of $(n+1)$-variable bent functions g to hyperplanes is itself difficult. We have seen that they are n-variable plateaued functions of amplitude $2^{\frac{n+1}{2}}$ (i.e. n-variable near bent functions), and as observed in [28, Theorem 2], it is equivalent to determining those n-variable near bent functions f such that there exists another near bent function whose Walsh support is complementary of the Walsh support of f. Indeed, we have seen that, given an $(n+1)$-variable bent function g and a nonzero vector e, denoting the restriction of g to the linear hyperplane $\{0, e\}^\perp$ by f and its restriction to the complement of this linear hyperplane by h, and extending the Walsh transforms of f and h to the whole space $\mathbb{F}_2^{n+1}$ as we explained in Section 2, we have $W_f(u) = \frac{W_g(u)+W_g(u+e)}{2}$ and $W_h(u) = \frac{W_g(u)-W_g(u+e)}{2}$. Since $W_g(u) = 2^{n/2}(-1)^{\widetilde{g}(u)}$, we have then that the support of W_f (resp. W_h) equals the co-support of $D_e\widetilde{g}$ (resp. the support of $D_e\widetilde{g}$).
It is not known how to simply characterize when a near bent function f admits the existence of another near bent function h whose Walsh support is the complement of the Walsh support of f. However, there is an interesting simple case considered in [28, Theorem 3]: for any near bent n-variable function f (n odd) and any nonzero $c \in \mathbb{F}_2^n$, it is equivalent to say that the function[6]

[6]Here we take a different - but affine equivalent - expression for g, in comparison with [28], so that f coincides with the restriction of g to $\mathbb{F}_2^n \times \{0\}$.

$g(x, x_{n+1}) = (x_{n+1}+1)f(x)+x_{n+1}(f(x)+c\cdot x)$; $x \in \mathbb{F}_2^n, x_{n+1} \in \mathbb{F}_2$, is bent and that c is a 1-valued linear structure of the indicator function φ of the Walsh support of f (that is, $D_c\varphi$ equals constant function 1, or more simply, denoting the Walsh support of f by S, that $S + c = S^c$). Note that this condition does not imply that the Walsh support of f is an affine space and it then does not imply that f is partially-bent. In [28, Theorem 4] is observed that when f is quadratic, such c always exists, because φ is then affine, which is not that interesting in our case. However, if φ is quadratic (which again does not imply that its support is an affine space), we have the same since a balanced quadratic function always has a 1-linear structure, according to [11, Proposition 55].

Proposition 2. *Let n be any positive odd integer and f any n-variable near bent function. If the indicator function of the Walsh support of f is quadratic (e.g. if f itself is quadratic), then f coincides with the restriction of an $(n+1)$-variable bent function to $\mathbb{F}_2^n \times \{0\}$.*

We wish now to extend these results to plateaued functions. Let us extend the observations of Remark 2. If g is an $(n+1)$-variable plateaued function with amplitude μ, then for every nonzero $e \in \mathbb{F}_2^n$ and for $H = \{0, e\}^\perp$, we have that denoting by $\mathbf{S}$ the Walsh support of g (which is an affine space if and only if g is partially-bent), then if $\mathbf{S} + e = \mathbf{S}$, then both $W_{g_{|H}}(a) = \frac{W_g(a)+W_g(a+e)}{2}$ and $W_{g_{|H^c}}(a) = \frac{W_g(a)-W_g(a+e)}{2}$ belong to $\{0, \pm\mu\}$, for every vector $a \in \mathbb{F}_2^n$, and if $\mathbf{S} \cap (\mathbf{S} + e) = \emptyset$, they both belong to $\{0, \pm\frac{\mu}{2}\}$, for every vector $a \in \mathbb{F}_2^n$. In the former case, all we can say about the Walsh support of $g_{|H}$ is that it is included in $\mathbf{S} \cap \mathbb{F}_2^n$, while in the latter case, the Walsh support of $g_{|H}$ equals $(\mathbf{S} \cup (\mathbf{S} + e)) \cap \mathbb{F}_2^n$. A last case, which does not happen if $\mathbf{S}$ is an affine space but can happen otherwise, is when $\mathbf{S} \cap (\mathbf{S}+e)$ neither equals $\mathbf{S}$ nor $\emptyset$. Then, there exist $a_1 \in \mathbf{S} \cap (\mathbf{S}+e)$, for which we have $W_{g_{|H}}(a_1), W_{g_{|H^c}}(a_1) \in \{0, \pm\mu\}$ and $a_2 \in (\mathbf{S} \setminus (\mathbf{S} + e)) \cup ((\mathbf{S} + e) \setminus \mathbf{S})$, for which we have $W_{g_{|H}}(a_2), W_{g_{|H^c}}(a_2) \in \{\pm\frac{\mu}{2}\}$. Then, it is only possible for $g_{|H}$ (resp. $g_{|H^c}$) to be plateaued if any $a_1 \in (\mathbf{S} \cap (\mathbf{S} + e)) \cap \mathbb{F}_2^n$ satisfies $W_{g_{|H}}(a_1) = 0$ (resp. $W_{g_{|H^c}}(a_1) = 0$). This seems a condition difficult to study and ensure in general. We shall be able to address it in the next theorem under the condition that one of the two restrictions of g to H and its complement is plateaued.

As we observed at the beginning of this section, since the notions of partial bentness and plateauedness are EA-invariant, we can assume without loss of generality (by applying an affine transformation to g) that $e = (0, \ldots, 0, 1)$ and $H = \mathbb{F}_2^n \times \{0\}$. This leads us to a well-known construction: for two n-variable functions f and f', we consider the $(n+1)$-variable function by $g(x, x_{n+1}) = (x_{n+1}+1)f(x)+x_{n+1}f'(x)$. This construction (which is in fact a representation of all $(n+1)$-variable Boolean functions by means of pairs of n-variable Boolean functions) is known as the Siegenthaler (secondary) construction (see e.g. [11, Section 7.1.9]) and is used in a particular case in [28]. For any g given by the (general) Siegenthaler construction, we have

$$W_g(a, \epsilon) = \sum_{x \in \mathbb{F}_2^n, \eta \in \mathbb{F}_2} (-1)^{(\eta+1)f(x)+\eta f'(x)+x\cdot a+\epsilon\eta} = W_f(a) + (-1)^\epsilon W_{f'}(a).$$

Let us prove that, given two plateaued n-variable Boolean functions f, f', the function g is plateaued if and only if f and f' have the same amplitude and either their Walsh supports are equal or they are disjoint.

Theorem 2. *Let f and f' be n-variable Boolean functions with n any non-negative integer, such that f is plateaued, and let $g(x, x_{n+1}) = (x_{n+1}+1)f(x)+x_{n+1}f'(x)$ be defined by the Siegenthaler construction. Then g is plateaued if and only if f' is plateaued, f and f' have the same amplitude,*

and their Walsh supports S and S', respectively, are either equal or disjoint.
If g is plateaued of amplitude μ, then f and f' have amplitude $\frac{\mu}{2}$ when their Walsh supports are equal and μ when they are disjoint.
Moreover, g is partially-bent if and only if either:

1. *f and f' are partially-bent with the same Walsh support $S = S'$ and the function $a \mapsto \epsilon_a$ on S defined by $W_g(a, \epsilon_a) \neq 0$ is affine;*
2. *f' is plateaued and $S \cap S' = \emptyset$ and $S \cup S'$ is an affine space.*

Proof. Suppose that g is plateaued with amplitude μ. For any $a \in \mathbb{F}_2^n$, we have that $W_g(a, 0) = W_f(a) + W_{f'}(a)$ and $W_g(a, 1) = W_f(a) - W_{f'}(a)$ are both valued in $\{0, \pm\mu\}$. Moreover, we then know that $W_f(a) = \frac{W_g(a,0)+W_g(a,1)}{2}$ belongs to $\{0, \pm\lambda\}$ and $W_{f'}(a) = \frac{W_g(a,0)-W_g(a,1)}{2}$ belongs to $\{0, \pm\frac{\mu}{2}, \pm\mu\}$ for all $a \in \mathbb{F}_2^n$.
If $S = S'$, then for any $a \in S$, there exists $\epsilon \in \mathbb{F}_2$ such that $W_f(a)$ and $(-1)^\epsilon W_{f'}(a)$ have the same sign and we have then $\mu = |W_g(a, \epsilon)| = |W_f(a)| + |W_{f'}(a)| = \lambda + |W_{f'}(a)|$, implying $|W_{f'}(a)| = \lambda$ since $\lambda, \mu/2$ and μ are powers of 2. If $S \cap S' = \emptyset$, then for any $a \in S'$ and $\epsilon \in \mathbb{F}_2$, we have $|W_g(a, \epsilon)| = |W_{f'}(a)| \neq 0$, implying $|W_{f'}(a)| = \mu$, which is also equal to λ by applying the same argument to f. In both cases, we see that f' is plateaued with the same amplitude as f.
By way of contradiction, assume that S and S' are not equal nor disjoint. There exists $a_0 \in S \cap S'$, and so one of $W_g(a_0, 0)$ or $W_g(a_0, 1)$ is nonzero since, as above, we can always choose the sign of $(-1)^\epsilon$ in the expression of $W_g(a, \epsilon)$ such that $W_f(a)$ and $W_{f'}$ have the same sign. In particular, $W_g(a_0, 0)$ or $W_g(a_0, 1)$ has absolute value $\mu = \lambda + |W_{f'}(a_0)|$ as g and f are plateaued. Note that this implies $\mu - \lambda = |W_{f'}(a_0)| > 0$, implying that $|W_{f'}(a_0)| = \frac{\mu}{2}$ (since we know that $W_{f'}(a_0) \in \{0, \pm\frac{\mu}{2}, \pm\mu\}$). Hence, $\mu = 2\lambda$. We know then that $|W_{f'}|$ is valued as $\frac{\mu}{2}$ on $S \cap S'$. Moreover, for any $a \in S' \setminus S$, we have $W_{f'}(a) = \pm\mu$. We have $S \subseteq S'$ because if there did exist $a \in S \setminus S'$, then for any $\epsilon \in \mathbb{F}_2$, it would follow that $|W_g(a, \epsilon)| = |W_f(a)| \neq 0$, implying $\lambda = \mu$, a contradiction. Now, applying Parseval's relation to f', we have that

$$2^{2n} = \sum_{a \in S} W_{f'}^2(a) + \sum_{a \in S' \setminus S} W_{f'}^2(a) = |S|\frac{\mu^2}{4} + (|S'| - |S|)\mu^2,$$

and upon the substitution of $|S| = 2^{2n}\lambda^{-2} = 2^{2(n+1)\mu^{-2}}$, this gives $2^{2n} = 2^{2n} + |S'|\mu^2 - 2^{2(n+1)}$, and then $|S'| = \frac{2^{2(n+1)}}{\mu^2} = \frac{2^{2n}}{\lambda^2} = |S|$, a contradiction. The converse is obvious.
Let us now prove the second part of the theorem. First, assume that $S = S'$, f and f' are partially-bent (i.e. S is an affine space), and the function $a \mapsto \epsilon_a$ defined on S by $W_g(a, \epsilon_a) \neq 0$ is affine. By the first part of the present theorem, we know that g is plateaued. Let us note that $a \mapsto \epsilon_a$ defined on S by $W_g(a, \epsilon_a) \neq 0$ is well-defined because if $a \in S$, then our assumption $S = S'$ tells us that exactly one of $W_g(a, 0)$ or $W_g(a, 1)$ is nonzero. For any $a \notin S$, it is immediate that $W_g(a, \epsilon) = 0$ for any $\epsilon \in \mathbb{F}_2$. Hence, the Walsh support of g, say $\mathbf{S}$, is equal to the graph $\{(a, \epsilon_a) : a \in S\}$. The graph of an affine function on an affine space is an affine space, and thus g is partially-bent.
Now, assume f' is plateaued and $S \cap S' = \emptyset$ and that $S \cup S'$ is an affine space. Note that we do not include in this hypothesis that f' has the same amplitude as f, while we need it to be true, so we first need to prove it. If it were the case that f' did not have the same amplitude as f, then S and S' would be two subsets of $\mathbb{F}_2^n$ whose sizes are distinct powers of 2 that sum to another power of two, an impossibility. Then, by the first part of this theorem, g is plateaued. For every $a \in S$, we have $W_f(a) \in \{\pm\lambda\}$, and $W_{f'}(a) = 0$ and therefore $W_g(a, \epsilon) \in \{\pm\lambda\}$, where λ is the amplitude

of f. Also, for every $a \in S'$, we have $W_f(a) = 0$ and $W_{f'}(a) \in \{\pm\lambda\}$. For every $a \notin S \cup S'$, we have $W_g(a, \epsilon) = 0$. So, the Walsh support of g is $\mathbf{S} = (S \cup S') \times \mathbb{F}_2$, which is by our hypothesis an affine space. Hence, g is partially-bent.
Conversely assume that g is partially-bent. Then, the Walsh support $\mathbf{S}$ of g is an affine space. Also, according to the first part of the present theorem, f' is plateaued[7], f and f' have the same amplitude, and their Walsh supports S and S', respectively, are either equal or disjoint.
If $S = S'$, then the Walsh support of g is equal to the set of those pairs $(a, \epsilon) \in \mathbb{F}_2^n \times \mathbb{F}_2$ such that $a \in S$ and $W_f(a) + (-1)^\epsilon W_{f'}(a) \neq 0$. In particular, for any $a \in S$, there exists a unique $\epsilon_a \in \mathbb{F}_2$ such that $W_g(a, \epsilon_a) = \pm 2\lambda$ and $W_g(a, \epsilon_a + 1) = 0$, and so, the Walsh support of g is equal to $\{(a, \epsilon_a) : a \in S\}$. Then, S is an affine subspace because it is equal to the projection on $\mathbb{F}_2^n$ of the affine space $\mathbf{S}$ (and then, it is the image by a linear homomorphism of an affine space). Hence, f and f' are partially-bent, and moreover, we know that $a \mapsto \epsilon_a$ defined on S is an affine function since its graph is an affine space.
Now, consider the case that $S \cap S' = \emptyset$. It is immediately obvious that $\mathbf{S} = (S \cup S') \times \mathbb{F}_2$. Since $\mathbf{S}$ is an affine space, we then have that $S \cup S'$ is too, as desired. □

Remark 5. *1. We are somewhat surprised by the first part of Theorem 2 since we initially thought that f and g could be plateaued while f' would not be plateaued. The situation in this part of the theorem is nicely simple. However, it does not provide a characterization of those n-variable functions which are the restrictions of $(n+1)$-variable plateaued functions, because it assumes that f is plateaued, while we know that the restriction of a plateaued function to an affine hyperplane can be non-plateaued.*
2. The second part of Theorem 2 provides a characterization of those n-variable functions which are the restrictions of $(n+1)$-variable partially-bent functions, since, as we already observed, the Siegenthaler construction covers all possible $(n+1)$-variable Boolean functions when f and f' are any n-variable functions. Theorem 1 tells us that when f is the restriction of a partially-bent function, f is plateaued. Conversely, partially-bent n-variable functions are such restrictions, as well as the non-partially-bent n-variable functions satisfying Condition 2 in Theorem 2. This is a characterization since we make no assumption on f'.
3. To complete the determination of the set of restrictions of partially-bent functions to affine hyperplanes, we would need to see what are the plateaued functions f such that there exists a plateaued function f' satisfying Condition 2, that is, whose Walsh support equals the complement of that of f in an affine space (say, A). Note that the size of A is necessarily $2|S|$, because of Parseval's relation (or because of the result of Theorem 2), since f and f' have the same amplitude. We deduce from $|A| = 2|S|$ that the restrictions of partially-bent functions to affine hyperplanes constitute a strict subset of that of all plateaued functions. Indeed, take for f a plateaued function whose Walsh support S is such that the smallest affine space containing S has a size strictly larger than $2|S|$, then f cannot be (affine equivalent to) the restriction of a partially-bent function to an affine hyperplane. Such a function can be built, for instance, as a Maiorana-McFarland function $f(x, y) = x \cdot \phi(y) + h(y)$ with $x \in \mathbb{F}_2^r, y \in \mathbb{F}_2^{n-r}$, choosing $r \geq n/2$ and $\phi : \mathbb{F}_2^{n-r} \to \mathbb{F}_2^r$ injective. Indeed, we have then $S = Im(\phi) \times \mathbb{F}_2^{n-r}$ (see below in Corollary 1), and we can take $Im(\phi)$ containing 0 and of rank k such that $2^k > 2|Im(\phi)| = 2^{n-r+1}$ (which is possible if, for instance, the nonzero elements of $Im(\phi)$ are linearly independent elements and $k = |Im(\phi)| - 1 = 2^{n-r} - 1 > n - r + 1$). Then any affine space A containing S is such that $|A| > 2|S|$, a contradiction.
4. It is not immediately clear how to best interpret condition (1) of Theorem 2 in a constructive

[7] We could also invoke Theorem 1 for this.

way. We leave it as an open question.

Remark 6. *A straightforward yet useful consequence of Theorem 2 is that for any n-variable plateaued Boolean function f and affine hyperplane $H \subseteq \mathbb{F}_2^n$, the restriction $f|_H$ is plateaued if and only if $f|_{H^c}$ is plateaued, and if so, then they both have the same amplitude. Assume that n and k are positive integers with $1 \leq k < n$ such that f is plateaued on all k-dimensional and all $(k+1)$-dimensional linear subspaces (without assuming the same for their cosets). Then, for a k-dimensional linear subspace L and any $u \notin L$, we know that f is plateaued on the $(k+1)$-dimensional subspace $L \cup (u+L)$. By considering $f|_{L\cup(u+L)}$ as a plateaued $(k+1)$-variable Boolean function, we see that, according to Theorem 2, its restriction to $u+L$ (which is an affine hyperplane of $L \cup (u+L)$) is plateaued with amplitude equal to the amplitude of $f|_L$. Since L and $u \notin L$ were arbitrary, we have $f \in C_k^n$, and all the restrictions of f to the cosets of a k-dimensional vector space L have the same amplitude.*

We can see that the only possibility of having g partially-bent and f not partially-bent arises with Condition 2 in Theorem 2. Let us provide a construction.

Corollary 1. *Let f and f' be Maiorana-McFarland functions: $f(x,y) = x \cdot \phi(y) + h(y)$ and $f'(x,y) = x \cdot \phi'(y) + h'(y)$, with $x \in \mathbb{F}_2^r, y \in \mathbb{F}_2^{n-r}$, and where $r \geq n/2$ and $\phi : \mathbb{F}_2^{n-r} \to \mathbb{F}_2^r$, $\phi' : \mathbb{F}_2^{n-r} \to \mathbb{F}_2^r$ are injective. Then for $a \in \mathbb{F}_2^r$ and $b \in \mathbb{F}_2^{n-r}$, we have $W_f(a,b) = 2^r \sum_{y\in\phi^{-1}(a)} (-1)^{h(y)+b\cdot y}$ and $W_{f'}(a,b) = 2^r \sum_{y\in\phi'^{-1}(a)} (-1)^{h'(y)+b\cdot y}$ and then $S = Im(\phi) \times \mathbb{F}_2^{n-r}$, $S' = (Im(\phi') + c) \times \mathbb{F}_2^{n-r}$. Both f and f' are plateaued, and if $Im(\phi)$ and $(Im(\phi')+c)$ are such that $Im(\phi) \cap (Im(\phi')+c) = \emptyset$ and $Im(\phi) \cup (Im(\phi')+c)$ is an affine space, then $g(x,y,x_{r+1}) = (x_{r+1}+1)f(x,y) + x_{r+1}f'(x,y)$, with $x \in \mathbb{F}_2^r, y \in \mathbb{F}_2^{n-r}$, $x_{r+1} \in \mathbb{F}_2$, is partially-bent while, if $Im(\phi)$ (resp., $(Im(\phi')+c)$) is not an affine space, then f (resp., f') is not partially-bent.*

Given a plateaued n-variable function f, if we want to use Theorem 2 to build a plateaued $(n+1)$-variable function g whose restriction to $\mathbb{F}_2^n \times \{0\}$ coincides with f (if possible a partially-bent one), we need to find another n-variable plateaued function f' satisfying the proper conditions from our result. Of course, it is more convenient and automatic if f' can be defined by an expression involving f. Since f' must be plateaued with the same amplitude as f, a natural way is to take f' EA-equivalent to f (this is what Leander and McGuire do in [28], but in a doubly particular way, restricting themselves to g bent and f near bent, and taking f' equal to the sum of f and a linear Boolean function). We consider then $f'(x) = f(L(x)+a) + c \cdot x + \epsilon$, where L is a linear automorphism of $\mathbb{F}_2^n$, a, c are two vectors in $\mathbb{F}_2^n$, and $\epsilon \in \mathbb{F}_2$. We first note that, without loss of generality about f, we can take $a = 0$ and $\epsilon = 0$, since denoting $f''(x) = f'(x+a) + \epsilon$, we have $W_{f''}(u) = (-1)^{a\cdot u+\epsilon} W_{f'}(u)$, and f'' has the same Walsh support as f'.

Proposition 3. *Let n be any positive integer and f be any n-variable function that is plateaued. Let c be an element of $\mathbb{F}_2^n$ and L a linear automorphism of $\mathbb{F}_2^n$. Then, denoting by L^{-1} the inverse of L and by T the adjoint operator of L^{-1} (satisfying $a \cdot L^{-1}(x) = T(a) \cdot x$ for every $a, x \in \mathbb{F}_2^n$), the $(n+1)$-variable function $g(x, x_{n+1}) = (x_{n+1}+1)f(x) + x_{n+1}(f \circ L(x) + c \cdot x)$ is plateaued if and only if the Walsh support S of f is such that $S = c + T^{-1}(S)$ or $S \cap (c + T^{-1}(S)) = \emptyset$. Moreover, g is partially-bent if and only if either:*

1. *f is partially-bent, its Walsh support S satisfies $S = c + T^{-1}(S)$, and the function $a \mapsto \epsilon_a$ on S defined by $W_g(a, \epsilon_a) \neq 0$ is affine;*
2. *$S \cap (c + T^{-1}(S)) = \emptyset$ and $S \cup (c + T^{-1}(S))$ is an affine space.*

In particular, if $L = Id$ and S is contained in an affine space of size $2|S|$ and the restriction of the indicator of S to this affine space is quadratic, then such c exists.

Proof. Denoting $f'(x) = f \circ L(x) + c \cdot x$, we have:

$$W_{f'}(a) = \sum_{x \in \mathbb{F}_2^n} (-1)^{f \circ L(x) + (c+a) \cdot x} = \sum_{x \in \mathbb{F}_2^n} (-1)^{f(x) + (c+a) \cdot L^{-1}(x)}$$

$$= \sum_{x \in \mathbb{F}_2^n} (-1)^{f(x) + T(c+a) \cdot x} = W_f(T(c+a)),$$

and the Walsh support of f' equals then $c + T^{-1}(S)$. The proof is then an obvious consequence of Theorem 2.
The last claim follows by the same reasoning from the beginning of this section. □

Corollary 2. *Let f be a Maiorana-McFarland function: $f(x,y) = x \cdot \phi(y) + h(y)$, with $x \in \mathbb{F}_2^r, y \in \mathbb{F}_2^{n-r}$, and where $r \geq n/2$ and $\phi : \mathbb{F}_2^{n-r} \to \mathbb{F}_2^r$ is injective. Let A be an affine automorphism of $\mathbb{F}_2^n$ such that there exist $A_1 \colon \mathbb{F}_2^r \to \mathbb{F}_2^r$ and $A_2 \colon \mathbb{F}_2^{n-r} \to \mathbb{F}_2^{n-r}$ (affine automorphisms) satisfying $A(x,y) = (A_1(x), A_2(y))$. Let f' be the n-variable Boolean function $f'(x,y) = f \circ A(x,y) + c \cdot x + k(y)$, where $c \in \mathbb{F}_2^r$ and k is any $(n-r)$-variable function. Let $A_1(x) = L_1(x) + c_1$ for a linear automorphism L_1 of $\mathbb{F}_2^r$ and $c_1 \in \mathbb{F}_2^r$, and let L_1^* be the adjoint operator of L_1. Let $\phi' = L_1^* \circ \phi \circ A_2$. Then the Walsh supports of f and f' are respectively $S = Im(\phi) \times \mathbb{F}_2^{n-r}$ and $S' = (Im(\phi') + c) \times \mathbb{F}_2^{n-r} = (L_1^*(Im(\phi)) + c) \times \mathbb{F}_2^{n-r}$. Both f and f' are plateaued, and if $Im(\phi)$ and L_1^* and c are such that $Im(\phi) \cap (L_1^*(Im(\phi)) + c) = \emptyset$ and $Im(\phi) \cup (L_1^*(Im(\phi)) + c)$ is an affine space, then $g(x,y,x_{r+1}) = (x_{r+1}+1)f(x,y) + x_{r+1}f'(x,y)$, with $x \in \mathbb{F}_2^r, y \in \mathbb{F}_2^{n-r}$, $x_{r+1} \in \mathbb{F}_2$ is partially-bent while, if $Im(\phi)$ is not an affine space, then f and f' are not partially-bent.*

Indeed, f' is also Maiorana-McFarland since $f'(x,y) = x \cdot (\phi'(y) + c) + h'(y)$ for all $(x,y) \in \mathbb{F}_2^r \times \mathbb{F}_2^{n-r}$, where $h' = h \circ A_2 + c_1 \cdot (\phi \circ A_2) + k$, and the proof is a direct consequence of Corollary 1.

Remark 7. *Let us consider using secondary constructions other than the Siegenthaler construction. Using the direct sum, the function we could add to f would be 1-variable, since we want g to be in $n+1$ variables. It would then be affine, and this would result in a similar situation as above. Using the indirect sum (see [11, Theorem 21]), we would have $g(x, x_{n+1}) = f(x) + l_1(x_{n+1}) + (f + f')(x)\,(l_1 + l_2)(x_{n+1})$; $x \in \mathbb{F}_2^n, x_{n+1} \in \mathbb{F}_2$, where f' is another n-variable function and l_1, l_2 are 1-variable functions, and where $l_1(0) = l_2(0) = 0$ (so that f coincides with the restriction of g to $\mathbb{F}_2^n \times \{0\}$). But $l_1(1) = l_2(1)$ would correspond to a direct sum and $l_1(1) = 0$, $l_2(1) = 1$ would give $g(x, x_{n+1}) = f(x) + x_{n+1}(f + f')(x))$, and correspond to Siegenthaler's construction.*

4.1 Plateaued Boolean functions with non-trivial linear structures

As we have seen, it is a natural problem to determine the plateauedness of the restrictions of plateaued functions, and in this subsection, we show that examples of plateaued restrictions can be found from plateaued Boolean functions with non-trivial linear structures.

For $\epsilon \in \mathbb{F}_2$, an *$\epsilon$-valued linear structure* of a Boolean function $f \colon \mathbb{F}_2^n \to \mathbb{F}_2$ is a point $a \in \mathbb{F}_2^n$ such that $D_a f(x) = f(x) + f(x+a)$ is identically equal to ϵ. The *linear kernel* of a Boolean function $f \colon \mathbb{F}_2^n \to \mathbb{F}_2$ is the linear subspace $\mathcal{E}_f$ equal to the set of all linear structures of f, or equivalently,

$$\mathcal{E}_f = \{a \in \mathbb{F}_2^n : D_a f \text{ is constant}\}.$$

There is a close relation between the Walsh support of a Boolean function and the orthogonal of its linear kernel. The following proposition is not properly speaking new (see [22]), but it presents a known property in a more precise and useful way.

Proposition 4. *Let $f\colon \mathbb{F}_2^n \to \mathbb{F}_2$ be a Boolean function. The smallest affine subspace (with respect to inclusion) containing* $\mathrm{supp}(W_f)$ *is a coset of $\mathcal{E}_f^\perp$.*

Proof. Suppose $a_0 \in \mathbb{F}_2^n$ is an ϵ-valued linear structure of f, where $\epsilon \in \mathbb{F}_2$. It is well known that for for any $u \in \mathbb{F}_2^n$, we have $W_f(u) = (-1)^{a_0 \cdot u + \epsilon} W_f(u)$, implying $\mathrm{supp}(W_f) \subseteq \{u \in \mathbb{F}_2^n : a_0 \cdot u = \epsilon\}$ (cf. [11, Proposition 29]). So, $\mathrm{supp}(W_f)$ is contained in the intersection $\bigcap_{a \in \mathcal{E}_f} \{u \in \mathbb{F}_2^n : a \cdot u = \epsilon_a\}$, where for $a \in \mathcal{E}_f$, we denote by $\epsilon_a \in \mathbb{F}_2$ the constant value of $D_a f$. That is, $\mathrm{supp}(W_f)$ is contained in some coset $w_0 + \mathcal{E}_f^\perp$ of $\mathcal{E}_f^\perp$.

Now, let $V \subseteq \mathbb{F}_2^n$ be the unique linear subspace with the property that there exists $u_0 \in \mathbb{F}_2^n$ such that $u_0 + V$ is the smallest affine subspace containing $\mathrm{supp}(W_f)$. Clearly, we have $V \subseteq \mathcal{E}_f^\perp$, and so $\mathcal{E}_f \subseteq V^\perp$. For any $a \in V^\perp$, the value of $a \cdot u$ is invariant of the choice of $u \in u_0 + V$, and let us call this constant value $\epsilon_a \in \mathbb{F}_2$. For any $x \in \mathbb{F}_2^n$ and $a \in V^\perp$, the inverse Walsh transform formula gives $(-1)^{f(x+a)} = 2^{-n} \sum_{u \in \mathrm{supp}(W_f)} (-1)^{u \cdot (x+a)} W_f(u) = 2^{-n} (-1)^{\epsilon_a} \sum_{u \in \mathrm{supp}(W_f)} (-1)^{u \cdot x} W_f(u) = (-1)^{\epsilon_a} (-1)^{f(x)}$, implying $a \in \mathcal{E}_f$. Therefore $V^\perp = \mathcal{E}_f$, and so $V = \mathcal{E}_f^\perp$. □

The characterization of the linear kernel provided in Proposition 4 also provides as a corollary the (more or less) well-known fact that a plateaued Boolean function $f\colon \mathbb{F}_2^n \to \mathbb{F}_2$ has its Walsh support equal to a coset of $\mathcal{E}_f^\perp$ if and only if f is partially-bent (as we have previously recalled that partially-bent functions are those plateaued Boolean functions whose Walsh supports are affine spaces). By only using the fact that the Walsh support of f is contained in a coset of $\mathcal{E}_f^\perp$, we can construct plateaued restrictions on affine spaces from plateaued Boolean functions with linear structures.

Proposition 5. *Let $f\colon \mathbb{F}_2^n \to \mathbb{F}_2$ be a Boolean function, and let $S = \mathrm{supp}(W_f)$. Then f is plateaued with amplitude λ if and only if for any linear subspace $L \subseteq \mathbb{F}_2^n$ satisfying $L \cap (S + S) = \{0\}$, we have f is plateaued on any coset of $L^\perp$ with amplitude $\lambda |L|^{-1}$.*

Proof. Consider a subspace $L \subseteq \mathbb{F}_2^n$ such that $L \cap (S + S) = \{0\}$. Then any coset of L intersects S at most once. Therefore, by relation (1), for any $u \in \mathbb{F}_2^n$, we have that any Walsh coefficient of $f|_{u+L^\perp}$ has absolute value 0 or $\lambda |L|^{-1}$, and the statement follows. The converse is obvious by taking $L = \{0\}$. □

Note that the same statement of Proposition 5 holds if we replace $S + S$ by $\mathcal{E}_f^\perp$. Indeed, for a Boolean function $f\colon \mathbb{F}_2^n \to \mathbb{F}_2$ and a linear subspace $L \subseteq \mathbb{F}_2^n$ such that $L \cap \mathcal{E}_f^\perp = \{0\}$, we have that $L \cap (S + S) = \{0\}$ because S is contained in a coset of $\mathcal{E}_f^\perp$ by Lemma 4.

Let f be any n-variable Boolean function and F any subspace such that $F \oplus \mathcal{E}_f = \mathbb{F}_2^n$. Then it is well-known that, for any $(x, y) \in F \times \mathcal{E}_f$, we can write $f(x + y) = g(x) + \ell(y)$ for some Boolean function g on F and an affine function ℓ on $\mathcal{E}_f$ (which can be taken linear). Hence, f is plateaued on $\mathbb{F}_2^n$ if and only if g is plateaued on F. Assuming that f is plateaued, we see that for any affine subspace $A \subseteq \mathbb{F}_2^n$ whose underlying vector space contains F, the restriction $f|_A$ is plateaued (while the converse is not necessarily true). In fact, if the underlying vector space V of A satisfies $V + \mathcal{E}_f = \mathbb{F}_2^n$, then $f|_A$ is plateaued on A since V contains some F_V such that $F_V \oplus \mathcal{E}_f = \mathbb{F}_2^n$. Since $\{0, e\}^\perp + \mathcal{E}_f = \mathbb{F}_2^n$ if and only if $e \notin \mathcal{E}_f^\perp$, we then know that f is plateaued on $\{0, e\}^\perp$ and its complement for all $e \notin \mathcal{E}_f^\perp$. This is also an immediate consequence of Proposition 5.

Corollary 3. *Let $f\colon \mathbb{F}_2^n \to \mathbb{F}_2$ be a plateaued Boolean function with a non-trivial linear structure. Then f is plateaued on $\{0,e\}^\perp$ and its complement for any $e \notin \mathcal{E}_f^\perp$.*

Proof. The statement is immediate upon applying Proposition 5 with $L = \{0,e\}$ with $e \notin \mathcal{E}_f^\perp$. □

It is easy to see that not all plateaued restrictions on affine hyperplanes of plateaued Boolean functions arise in the same way as described in Corollary 3. Let $n \geq 4$, and let $f\colon \mathbb{F}_2^n \to \mathbb{F}_2$ be a non-affine partially-bent function. Then $\mathcal{E}_f^\perp$ is not equal to $\{0\}$. By Theorem 1, f is plateaued on every affine hyperplane, implying f is plateaued on $\{0,e\}^\perp$ for all $e \in \mathcal{E}_f^\perp \setminus \{0\}$, but $\{0,e\} \cap \mathcal{E}_f^\perp \neq \{0\}$ by definition. Thus, non-partially-bent plateaued functions that have many linear structures provide examples of Boolean functions that are plateaued on a large number of affine hyperplanes.

5 Vectorial functions

Given two positive integers n, m, a vectorial function $F : \mathbb{F}_2^n \to \mathbb{F}_2^m$ (called an (n,m)-function) is quadratic if and only if all its *component functions* $x \in \mathbb{F}_2^n \mapsto v\cdot F(x)$; $v \in \mathbb{F}_2^m \setminus \{0\}$ are quadratic. An (n,m)-function F is called plateaued if all its component functions are plateaued Boolean functions. A vectorial function whose component functions are all partially-bent is called *strongly plateaued* (see [10, Proposition 4] and [11, Section 6.5]).

Definition 2. *Let n, m, k be any positive integers satisfying $0 \leq k \leq n$. We denote by $\mathcal{C}_k^{n,m}$ the class of (n,m)-functions whose restrictions to all k-dimensional affine spaces are plateaued.*

We deduce directly from Theorem 1:

Corollary 4. *Let n, m be any positive integers such that $n \geq 4$. Let F be any (n,m)-function. Then F is strongly plateaued if and only if $F \in \mathcal{C}_{n-1}^{n,m}$. Moreover, for all $3 \leq k \leq n-2$, $\mathcal{C}_k^{n,m}$ is equal to the set of quadratic vectorial functions in n variables. Hence, if all the restrictions to affine hyperplanes of an (n,m)-function are strongly plateaued, this function is necessarily quadratic.*

Corollary 4 and Theorem 2 imply that if F is strongly plateaued but not quadratic, then there exists $v \neq 0$ and an affine hyperplane H such that $v \cdot f_{|H}$ and $v \cdot F_{|H^c}$ are neither partially-bent but have disjoint Walsh supports S and S' such that $S \cup S' = A$ for some affine space A.

Conclusion

We have seen in this paper that having all restrictions to affine hyperplanes plateaued is very restrictive for a Boolean function (resp., a vectorial function), since it is equivalent to being partially-bent (resp., strongly plateaued).
Having all restrictions to affine hyperplanes partially-bent (resp., strongly plateaued), which is then equivalent to having all restrictions to affine spaces of codimension 2 plateaued, is still more restrictive since it is equivalent to being quadratic.
We found rather surprising these two results when we obtained them, since even the necessary plateauedness of any function whose restrictions to all affine subspaces of dimension k for $3 \leq k < n$ are plateaued seemed initially not obvious to us.
From what we have seen in this paper, the following six classes of Boolean functions form a nested sequence: quadratic functions, partially-bent functions, the restrictions of partially-bent functions

to affine hyperplanes, plateaued functions, the restrictions of plateaued functions to affine hyperplanes, and all Boolean functions. All these classes are distinct for $n \geq 5$.
We have begun the study of the natural problem of determining the third class (equivalently, the class of all those plateaued Boolean functions which are the restrictions of partially-bent functions in one more variable). We have observed that all partially-bent functions belong to this class. We provided a characterization of its elements, although fully determining them from our characterization seems challenging.
Another natural problem is to determine the fifth class (equivalently, the class of all those Boolean functions which are the restrictions of plateaued functions in one more variable), since the restrictions of plateaued Boolean functions are not all plateaued. Here also, all plateaued functions have this property, and determining those other Boolean functions which have it seems difficult.
The same problems with vectorial functions (replacing "partially-bent" with "strongly plateaued") seem even more difficult to solve. And there is also an open question on vectorial functions which seems natural, but which happens to be equivalent to a know open question. Recall that an APN strongly plateaued function is called a crooked function. The restrictions to affine hyperplanes of strongly plateaued functions are not necessarily strongly plateaued, but is it still true when we additionally assume that the functions are APN (that is, are crooked)? According to our corollary on the restrictions of strongly plateaued functions, this question is equivalent to asking whether crooked functions can be non-quadratic, which is a classic open question. This sheds new light on this long-standing question. Indeed, we can try to prove that any crooked function is quadratic (if this is true) by showing that the restrictions of the component functions of a crooked function to a hyperplane are all partially-bent (equivalently, their Walsh supports are affine spaces).
We leave these general problems open.

Acknowledgment We thank Philippe Langevin for his useful information on the classifications of Boolean functions.

References

[1] M. Abbondati, M. Calderini, and I. Villa. On Dillon's property of (n, m)-functions. *Cryptography and Communications*, 16(6), pp.1449-1473, 2024.

[2] A. Bernasconi, B. Codenotti and J.M. Vanderkam. A characterization of bent functions in terms of strongly regular graphs. *IEEE Transactions on Computers* 50 (9), pp. 984-985, 2001.

[3] K. Browning, J. F. Dillon, M. McQuistan and A. J. Wolfe. An APN permutation in dimension 6. *Proceedings of Conference Finite Fields and Applications Fq9*, Contemporary Mathematics 518, pp. 33-42, 2010.

[4] M. Calderini, M. Sala and I. Villa. A note on APN permutations in even dimension. *Finite Fields and Their Applications* 46, pp. 1-16, 2017.

[5] A. Canteaut, C. Carlet, P. Charpin and C. Fontaine. On cryptographic properties of the cosets of $R(1, m)$. *IEEE Transactions on Information Theory* 47 (4), pp. 1494-1513, 2001.

[6] A. Canteaut and P. Charpin. Decomposing bent functions. *IEEE Transactions on Information Theory* 49, pp. 2004-2019, 2003.

[7] A. Canteaut and M. Videau. Degree of composition of highly nonlinear functions and applications to higher order differential cryptanalysis. *Proceedings of EUROCRYPT 2002, Lecture Notes in Computer Science* 2332, pp. 518-533, 2002.

[8] C. Carlet. Partially-bent functions. *Designs, Codes and Cryptography*, vol. 3, no. 2, pp. 135–145, 1993. https://doi.org/10.1007/BF01388412

[9] C. Carlet. On known and new differentially uniform functions. *Proceedings of the 16th Australasian Conference on Information Security and Privacy ACISP 2011, Lecture Notes in Computer Science* 6812, pp. 1-15, 2011.

[10] C. Carlet. Boolean and vectorial plateaued functions, and APN functions. *IEEE Transactions on Information Theory* 61 (11), pp. 6272-6289, 2015.

[11] C. Carlet. Boolean Functions for Cryptography and Coding Theory. Monograph in *Cambridge University Press*, 562 pages, 2021.

[12] C. Carlet. Two Generalizations of Almost Perfect Nonlinearity. *J. Cryptol.* 38(2): 20, 2025.

[13] C. Carlet, P. Charpin, and V. Zinoviev. Codes, bent functions and permutations suitable for DES-like cryptosystems. *Designs, Codes and Cryptography*, 15 (2), pp. 125-156, 1998.

[14] C. Carlet, S. Feukoua and A. Sălăgean. The stability of the algebraic degree of Boolean functions when restricted to affine spaces. *Designs, Codes and Cryptography*, 93(11), pp.4799-4832, 2025.

[15] C. Carlet and E. Piccione. On vectorial functions mapping strict affine subspaces of their domain into strict affine subspaces of their co-domain, and the strong D-property. *Adv. Math. Commun.* 19(3): 793-828, 2025.

[16] C. Carlet and D. Thornburgh. Resolving a conjecture on quadratic APN functions and a new quadratic (n,n)-function associated to crooked functions. *arXiv:2608.23888* https://arxiv.org/abs/2608.23888.

[17] A. Çeşmelioglu, W. Meidl and A. Topuzoğlu. Partially bent functions and their properties. *Applied Algebra and Number Theory*, Cambridge Univ Press, pp. 22-38, 2014.

[18] C. Carlet and I. Villa. On cubic-like bent Boolean functions. *Journal of Algebraic Combinatorics*, 61(4), p.50, 2025.

[19] P. Charpin. Normal Boolean functions. *Journal of Complexity*, 20(2-3), pp.245-265, 2004.

[20] J. F. Dillon. Elementary Hadamard Difference sets. *Ph. D. Thesis, Univ. of Maryland*, 1974.

[21] J. F. Dillon and G. McGuire. Near bent functions on a hyperplane. *Finite Fields and Their Applications* 14 (3), pp. 715-720, 2008.

[22] S. Dubuc. Characterization of linear structures. *Designs, Codes and Cryptography* 22, pp. 33-45, 2001.

[23] F. Göloglu and A. Pott. Results on the crosscorrelation and autocorrelation of sequences. *Proceedings of International Conference on Sequences and Their Applications SETA 2008, Lecture Notes in Computer Science* 5203, pp. 95-105, 2008.

[24] A. M. Kerdock. A class of low-rate non linear codes. *Information and Control* 20, pp. 182-187, 1972.

[25] Gohar M. Kyureghyan. Crooked maps in $\mathbb{F}_{2^n}$. *Finite Fields and Their Applications* 13 (3), pp. 713-726, 2007.

[26] J. Lahtonen, G. McGuire and H. Ward. Gold and Kasami-Welch functions, quadratic forms and bent functions. *Advances in Mathematics of Communications* 1, pp. 243-250, 2007.

[27] G. Leander and G. McGuire. Spectra of functions, subspaces of matrices, and going up versus going down. *Proceedings of AAECC-17 Conference, Lecture Notes in Computer Science* 4851, pp. 51-66, 2007.

[28] G. Leander and G. McGuire. Construction of bent functions from near bent functions. *Journal of Combinatorial Theory, Series A* 116, pp. 960-970, 2009.

[29] Y. Li and M. Wang. Constructing differentially 4-uniform permutations over $GF(2^{2m})$ from quadratic APN permutations over $GF(2^{2m+1})$. *Designs, Codes and Cryptography* 72 (2), pp. 249-264, 2014.

[30] S. Mesnager. Linear codes from functions. In *Concise Encyclopedia of Coding Theory*, pp. 463-526. Chapman and Hall/CRC, 2021.

[31] V. Potapov. Upper bounds on the numbers of binary plateaued and bent functions. *Cryptography and Communications* 16.6, pp. 1347-1356, 2024.

[32] B. Preneel, R. Govaerts, and J. Vandewalle. Boolean functions satisfying higher order propagation criteria. *Advances in Cryptology — EUROCRYPT '91*, Lecture Notes in Computer Science, vol. 547, Springer, Berlin, Heidelberg, 1991, pp. 141–152.

[33] C. Riera, P. Solé, P. Stănică. A Complete Characterization of Plateaued Boolean Functions in Terms of Their Cayley Graphs. *Progress in Cryptology – AFRICACRYPT 2018*, 2018.

[34] O. S. Rothaus. On "bent" functions. *Journal of Combinatorial Theory, Series A* 20, pp. 300-305, 1976.

[35] F. J. MacWilliams and N. J. Sloane. The theory of error-correcting codes, *North Holland*. 1977.

[36] E.R. van Dam and G.R. Omidi. Strongly walk-regular graphs. *Journal of Combinatorial Theory, Series A* 120, pp. 803-810, 2013.

[37] S. Yoshiara. Equivalences among plateaued APN functions. *Designs, Codes and Cryptography* 85(2), pp. 205-217, 2017.

[38] Y. Zheng and X. M. Zhang. Plateaued functions. *Proceedings of ICICS 1999, Lecture Notes in Computer Science* 1726, pp. 284-300, 1999.

[39] Y. Zheng, X.-M. Zhang, and H. Imai. Restriction, terms and nonlinearity of Boolean functions. *Theoretical Computer Science*, 226(1-2), pp. 207-223, 1999.

[40] Y. Zheng and X.-M. Zhang. On Balanced Nonlinear Boolean Functions. *NATO Science for Peace and Security Series - D: Information and Communication Security*, Vol 18: Boolean Functions in Cryptology and Information Security, IOS Press, pp. 243-282, 2008.