A notion on S-boxes for a partial resistance to some integral attacks

Claude Carlet,

University of Bergen, Department of Informatics, 5005 Bergen, Norway University of Paris 8, Department of Mathematics, 93526 Saint-Denis, France. *E-mail:* claude.carlet@gmail.com, Orcid: 0002-6118-7927

Abstract

In two recent papers, we introduced and studied the notion of kthorder sum-freedom of a vectorial function $F: \mathbb{F}_2^n \to \mathbb{F}_2^m$. This notion generalizes that of almost perfect nonlinearity (which corresponds to k = 2) and has some relation with the resistance to integral attacks of those block ciphers using F as a substitution box (S-box), by preventing the propagation of the division property of k-dimensional affine spaces. In the present paper, we show that this notion, which is rarely satisfied by vectorial functions, can be weakened while retaining the property that the S-boxes do not propagate the division property of k-dimensional affine spaces. This leads us to the property that we name kth-order t-degree-sum-freedom, whose strength decreases when t increases, and which coincides with kthorder sum-freedom when t = 1. The condition for kth-order t-degreesum-freedom is that, for every k-dimensional affine space A, there exists a non-negative integer j of 2-weight at most t such that $\sum_{x \in A} (F(x))^j \neq 0$. We show, for a general kth-order t-degree-sum-free function F, that t can always be taken smaller than or equal to $\min(k, m)$ under some reasonable condition on F, and that it is larger than or equal to $\frac{k}{\deg(F)}$, where $\deg(F)$ is the algebraic degree of F. We also show two other lower bounds: one, that is often tighter, by means of the algebraic degree of the compositional inverse of F when F is a permutation, and another (valid for every vectorial function) by means of the algebraic degree of the indicator of the graph of the function. We study examples for k = 2 (case in which t = 1corresponds to APNness) showing that finding j of 2-weight 2 can be challenging, and we begin the study of power functions, for which we prove upper bounds. We study in particular the multiplicative inverse function (used as an S-box in the AES), for which we characterize the kth-order t-degree-sum-freedom by the coefficients of the subspace polynomials of k-dimensional vector subspaces (deducing the exact value of t when k divides n) and we extend to kth-order t-degree-sum-freedom the result that it is kth-order sum-free if and only if it is (n-k)th-order sum-free.

^{*}The research of the author is partly supported by the Norwegian Research Council

Keywords: vectorial function, S-box, almost perfect nonlinear, *k*th-order sumfree, integral attack, division property.

1 Introduction

A (vectorial) (n, m)-function $F : \mathbb{F}_2^n \to \mathbb{F}_2^m$ is called kth-order sum-free [8] if, for every k-dimensional affine space A in \mathbb{F}_2^n , we have $\sum_{x \in A} F(x) \neq 0$. This is equivalent to saying that the kth-order derivatives $D_{a_1} \dots D_{a_k} F(x)$ (where the first order derivative is defined as $D_a F(x) = F(x) + F(x+a)$ and the kth-order derivative is its iteration) never vanish when a_1, \dots, a_k are linearly independent over \mathbb{F}_2 .

There is a relation between this notion and integral attacks [13]. Todo [18] has introduced, in the framework of these cryptanalyses, the notion of division property of a set, and Boura-Canteaut [4] have translated it into the language of Reed-Muller codes (see a survey in [12]). A set $X \subseteq \mathbb{F}_2^n$ is said to have the division property at an order l if its indicator has an algebraic degree of at most n-l. Integral attacks practically lead to studying the propagation of the division property through rounds, which needs to study it through substitution boxes (S-boxes, which are the nonlinear components in rounds). It is shown in [8] that kth-order sum-freedom makes it impossible the propagation of the division property of k-dimensional affine spaces through the S-box. Since the division property is often (but not always) investigated by cryptanalysts by focussing on affine spaces, the study of kth-order sum-freedom is useful for designers, helping them to protect ciphers against such kind of integral attacks, and for cryptanalysts, letting them know which affine spaces can be considered in integral attacks. However, the functions satisfying kth-order sum-freedom for a given k are rare, and even if a function satisfies it for some value of k, it may not satisfy it for other values. Fortunately, we show in the present paper that this criterion can be generalized into a version depending on some parameter t > 1, that is satisfied for every k by any vectorial function for a large enough value of t (kth-order sum-freedom corresponding to t = 1). This latter notion is practically more useful and easier to satisfy (but it is still more difficult to study).

In the present paper, we begin the study of this new notion, called kth-order t-degree-sum-freedom. The condition for such a property to be satisfied by F is that, for every k-dimensional affine space A, there exists a non-negative integer j of 2-weight at most t such that $\sum_{x \in A} (F(x))^j \neq 0$, where the 2-weight of a non-negative integer equals the Hamming weight of its binary expansion. For general k, we show that we can take $t \leq \min(k,m)$ under a reasonable assumption on F, and that we necessarily have $t \geq \frac{k}{\deg(F)}$, where $\deg(F)$ is the algebraic degree of F. This generalizes the fact that a function of algebraic degree d cannot be kth-order sum-free for k > d. We improve this bound with two other lower bounds: one that is valid when F is a permutation, by means of the algebraic degree of the compositional inverse of F, and another, that is valid for every vectorial function and can be still tighter, by means of the algebraic

degree of the indicator of the graph of the function. We study a little more in detail the case of k = 2 (where t = 1 corresponds to APNness) and see that the determination of the values of j can be challenging even when determining t is easy. We focus then on power functions, for which we prove upper bounds on the minimum value of t, given k. We study specifically the multiplicative inverse function (used as an S-box in the AES), and characterize the minimum value of t by means of the coefficients of the subspace polynomials of k-dimensional vector spaces in \mathbb{F}_{2^n} (which allows us to completely clarify the situation when k divides n). We show that this function is kth-order t-degree-sum-free if and only if it is (n - k)th-order t-degree-sum-free, which allows to strengthen the upper bounds found.

2 Preliminaries

Given two positive integers n, m, we call (n, m)-function (vectorial function if we do not wish to specify n, m) any function $F : \mathbb{F}_2^n \to \mathbb{F}_2^m$. If m = 1, we speak of an *n*-variable Boolean function and we denote it by a lowercase symbol f. We can endow the domain or the co-domain of such function (or both) with the structure of a finite field, since any finite field \mathbb{F}_{2^n} of characteristic 2 is an *n*-dimensional vector space over \mathbb{F}_2 , and given a basis $(\alpha_1, \ldots, \alpha_n)$, we have the correspondence $(x_1, \ldots, x_n) \mapsto \sum_{i=1}^n x_i \alpha_i$.

Two (n, m)-functions F, G are called affine equivalent if $G = A \circ F \circ A'$ where A (resp. A') is an affine automorphism of \mathbb{F}_2^m (resp. \mathbb{F}_2^n), and they are more generally called CCZ equivalent if the graph of F, that is, $\{(x, F(x)); x \in \mathbb{F}_3^n\}$ can be mapped to the graph of G by an affine automorphism \mathcal{A} of $\mathbb{F}_2^n \times \mathbb{F}_2^m$. Denoting $\mathcal{A} = (\mathcal{A}_1, \mathcal{A}_2)$, the mapping $F_1 : x \in \mathbb{F}_2^n \mapsto \mathcal{A}_1(x, F(x))$ is then a permutation of \mathbb{F}_2^n , and denoting $F_2(x) = \mathcal{A}_2(x, F(x))$, we have $G = F_2 \circ F_1^{-1}$ (see e.g. [7]).

We call F a *kth-order sum-free function* if, for every *k*-dimensional affine subspace A of \mathbb{F}_2^n (or of \mathbb{F}_{2^n}), we have $\sum_{x \in A} F(x) \neq 0$ [8]. The (n, n)-functions that are second-order sum-free are also called *almost perfect nonlinear* (APN). When viewing a vectorial function as defined over \mathbb{F}_2^n , we can represent it by its (unique) algebraic normal form $F(x) = \sum_{I \subseteq \{1,...,n\}} a_I \prod_{i \in I} x_i$ with $a_I \in \mathbb{F}_2^m$ (or $a_I \in \mathbb{F}_{2^m}$). This allows to define its algebraic degree $\max\{|I|; a_I \neq 0\}$ where $|\ldots|$ denotes the size.

When viewing a vectorial function as defined over \mathbb{F}_{2^n} and valued in this same field (which includes the possibility it is valued in a sub-field of \mathbb{F}_{2^n} and allows then to consider not only (n, n)-functions but also (n, m)-functions, where mdivides n), we can represent it by its (unique) univariate representation F(x) = $\sum_{i=0}^{2^n-1} \delta_i x^i, \, \delta_i \in \mathbb{F}_{2^n}$. The algebraic degree of F equals then $\max\{w_2(i); \delta_i \neq 0\}$, where $w_2(i)$ is the 2-weight of i (i.e., the Hamming weight of its binary expansion). Function F is called a *power function* if $F(x) = x^d$, for some exponent $d \in \mathbb{Z}/(2^n - 1)\mathbb{Z}$.

A subset X of \mathbb{F}_2^n or \mathbb{F}_{2^n} satisfies the *division property at the order* l if the *n*-variable Boolean function equal to its indicator (taking value 1 on X and 0)

elsewhere) has algebraic degree at most n - l (see [4]).

3 A weakening of the sum-freedom notion

To show why sum-freedom can be weakened, let us briefly recall why the kthorder sum-freedom of an S-box avoids the propagation of the division property of k-dimensional affine spaces through it. We first need to say what is the image of a set that must be considered as the result of the processing of a set X (supposed to have the division property) through the S-box: if the S-box F is a permutation, or is more generally injective, then the image of X by F to be considered is the classic one $F(X) = \{F(x); x \in X\} = \{y \in \mathbb{F}_2^m; X \cap F^{-1}(y) \neq \emptyset\}$. If not, then the image to be considered is (see [12]):

$$F((X)) := \{ y \in \mathbb{F}_2^m; X \cap F^{-1}(y) \text{ has an odd size} \}$$

(we use a specific notation to avoid any confusion between F(X) and F((X)) when F is not injective). What is shown in [8] is that if $\sum_{x \in X} F(x) \neq 0$, then F((X)) does not have the division property at the order 2.

Let us recall why this is true and show that this nicely simple notion of sumfreedom is in fact too demanding in most cases, as a property implying the non-propagation of the division property. Let X have an even size (so that it has at least the division property at the order 1). Then F((X)) has an even size as well, and we have $\sum_{x \in X} F(x) = \sum_{y \in F((X))} y$. The fact that the sum $\sum_{y \in F((X))} y$ is nonzero is equivalent to the property that the indicator of F((X))has at least algebraic degree n - 1 (this is a particular case of [7, Corollary 2]; see more details in [8, Subsection 3.2]). Then no propagation of the division property is possible for k-dimensional affine spaces when F is kth-order sumfree, since F((X)) only satisfies the division property at the order 1. But we do not need the division property to drop to order 1 for the integral attack to be made impossible, we only need that the division property falls to a small enough level.

The propagation of the division property has been studied in [4, 12] through a representation of the S-box by its algebraic normal form, that is, viewing it as defined over the vector space \mathbb{F}_2^n . This leads to the notion of parity set introduced in [4]. The division property fails to be propagated at the order t + 1 if there exists a vector $v \in \mathbb{F}_2^m$ of Hamming weight at most t such that $\sum_{x \in X} F^v(x) = 1$, where $F^v(x)$ equals the composition of F on its left by the (multivariate) monomial Boolean function $\prod_{i \in supp(v)} x_i$. We will not develop here this approach. We shall identify the vector space \mathbb{F}_2^m with the field \mathbb{F}_{2^m} (see Section 2)). We do so because:

• it is often simpler to address the propagation of the division property in fields than in vector spaces, because it translates into the nullity of some power sums, that are simpler to handle than sums taken by the functions F^v ,

- in many block ciphers such as the AES, S-boxes are naturally defined over fields and valued in them,
- most of the important (infinite classes of) vectorial functions for cryptography are defined over fields and valued in them,
- in particular, many important functions for cryptography are power functions over finite fields, and no infinite class of (for instance) APN functions is known by its algebraic normal form.

3.1 Preliminaries on Reed-Muller codes

We know (see [15, 7]) that, for every $1 \leq d \leq m$, the dual of the Reed-Muller code RM(d-1,m), of order d-1 and length 2^m , equals the Reed-Muller code RM(m-d,m), of order m-d and of the same length, that is, any *m*-variable Boolean function f has algebraic degree strictly less than d if and only if, for every Boolean function g of algebraic degree at most m-d, we have $\sum_{y \in \mathbb{F}_{2^m}} f(y)g(y) = 0$, or more generally, for every (m, r)-function G (with $r \geq 1$), of algebraic degree at most m-d, we have $\sum_{y \in \mathbb{F}_{2^m}} f(y)G(y) = 0$. Hence:

Lemma 1 Let m be any positive integer, and let $0 \leq d \leq m$. Any nonzero m-variable Boolean function f has algebraic degree at least d if and only if there exists a Boolean function g of algebraic degree at most m - d, such that $\sum_{y \in \mathbb{F}_{2^m}} f(y)g(y) \neq 0$, or equivalently there exists, for some $r \geq 1$, an (m, r)-function G of algebraic degree at most m - d, such that $\sum_{y \in \mathbb{F}_{2^m}} f(y)G(y) \neq 0$.

In particular, for every nonzero *m*-variable Boolean function f, there exists an *m*-variable Boolean function g (which has of course an algebraic degree of at most m), such that $\sum_{y \in \mathbb{F}_{2m}} f(y)g(y) \neq 0$ (taking d = 0 in Lemma 1, or directly choosing for Boolean function g the indicator of a singleton $\{a\}$, where f(a) = 1).

Moreover, when the domain of the Boolean function is endowed with the structure of the field \mathbb{F}_{2^m} , we can specify Lemma 1 in a way that will be convenient in our framework. We recall that the 2-weight of j is the Hamming weight of the binary expansion of j.

Lemma 2 [7, Corollary 2] Let m be any positive integer, and let $0 \le d \le m$. Any nonzero m-variable Boolean function f has algebraic degree at least d if and only if there exists a non-negative integer j whose 2-weight satisfies $w_2(j) \le m - d$, and such that $\sum_{y \in \mathbb{F}_{2m}} y^j f(y) \ne 0$.

For making the paper self-contained, let us give a proof of this fact (a different proof from that of [7]):

• the functions in the Reed-Muller code of order m-d are the Boolean functions whose univariate representation has the form (see e.g. [7, Relation

(2.16)]):

u

$$\sum_{\substack{j \in \Gamma(m)\\ j_2(j) \le m-d}} tr_{m_j}(\beta_j y^j), \text{ with } \forall j \in \Gamma(m), \beta_j \in \mathbb{F}_{2^{m_j}},$$

where $\Gamma(m)$ is a set of representatives of the cyclotomic classes of 2 modulo $2^m - 1$, the integer m_j is the size of the cyclotomic class containing j, and $tr_{m_j}(y) = \sum_{i=0}^{m_j-1} y^{2^i}$ is the absolute trace function from $\mathbb{F}_{2^{m_j}}$ to \mathbb{F}_2 ,

• for every $y \in \mathbb{F}_{2^m}$, we have $y^j \in \mathbb{F}_{2^{m_j}}$, and we deduce $\sum_{y \in \mathbb{F}_{2^m}} y^j f(y) \neq 0$ for some j of 2-weight at most m - d if and only if there exists β_j in $\mathbb{F}_{2^{m_j}}$ such that $\sum_{y \in \mathbb{F}_{2^m}} tr_{m_j}(\beta_j y^j) f(y) = 1$, that is, f is not orthogonal to the Reed-Muller code of order m - d, that is, does not belong to the Reed-Muller code of order d - 1.

3.2 Weakening the notion of sum-freedom

From the results recalled above, we deduce the following proposition, by taking d = m - t (that is, m - d = t), and observing that if f is the indicator of F((X)) in \mathbb{F}_{2^m} , where F is an (n, m)-function, then for every (m, r)-function G, we have $\sum_{y \in \mathbb{F}_{2^m}} G(y) f(y) = \sum_{x \in X} (G \circ F)(x)$, and in particular, $\sum_{y \in \mathbb{F}_{2^m}} y^j f(y) = \sum_{x \in X} (F(x))^j$.

Proposition 1 For any positive integers n, m, t, let $F : \mathbb{F}_2^n \to \mathbb{F}_{2^m}$ be any (n,m)-function (where \mathbb{F}_2^n can be identified with \mathbb{F}_{2^n} or not) and X any set in \mathbb{F}_2^n . The set F((X)) fails to have the division property of order t + 1 (i.e. the *m*-variable Boolean function equal to the indicator of F((X)) has an algebraic degree at least m - t) if and only if some non-negative integer j exists such that $w_2(j) \leq t$ and $\sum_{x \in X} (F(x))^j \neq 0$, which is equivalent to: some (m, r)-function G (with $r \geq 1$) of algebraic degree at most t exists such that $\sum_{x \in X} (G \circ F)(x) \neq 0$.

Note that a k-dimensional affine space A, with $k \ge 1$, having an even size, the set F((A)) has also an even size, and $\sum_{x \in A} (F(x))^0$ then equals 0. This leads to the definition:

Definition 1 Let $F : \mathbb{F}_2^n \to \mathbb{F}_{2^m}$ be an (n,m)-function. Let $1 \leq k \leq n$ and $1 \leq t \leq m$. Then F is called kth-order t-degree-sum-free if, for every k-dimensional affine space A, there exists a positive integer j whose 2-weight is at most t and such that $\sum_{x \in A} (F(x))^j \neq 0$.

According to what we observed above, this is equivalent to the fact that, for some $r \geq 1$, there exists a vectorial (m, r)-function G of algebraic degree at most t such that $\sum_{x \in X} (G \circ F)(x) \neq 0$.

Remark. For any new property of (n, m)-functions F, we need to determine whether the composition of F by any affine permutation L of \mathbb{F}_2^n on

the right and/or by any affine permutation L' of \mathbb{F}_2^m on the left, and/or the addition of any affine (n, m)-function preserve(s) the property, and more generally whether, when an affine permutation Σ of $\mathbb{F}_2^n \times \mathbb{F}_2^m$ maps the graph $\mathcal{G}_F = \{(x, F(x)); x \in \mathbb{F}_2^n\}$ of F to the graph of an (n, m)-function G, and Fsatisfies the property, then G satisfies the property. Two functions F and G are called affine equivalent if $G = L' \circ F \circ L$ where L, L' are affine permutations, they are called EA equivalent if G is affine equivalent to the sum of F and an affine function, and they are called CCZ equivalent if $\mathcal{G}_G = \Sigma(\mathcal{G}_F)$ for some affine permutation Σ (see e.g. [7]). We need to see whether the property is preserved by affine (resp. EA, CCZ) equivalence; if it is the case, then we say that the property is affine (resp. EA, CCZ) invariant.

For every $k \geq 2$ and $t \geq 1$, the property of being kth-order t-degree-sum-free for an (n, m)-function is preserved by the composition on the right by any affine automorphism L of \mathbb{F}_2^n (since $\sum_{x \in A} (F \circ L(x))^j = \sum_{x \in L(A)} (F(x))^j$ and L(A)is a k-dimensional affine space if and only if A is a k-dimensional affine space), and by the composition on the left by any affine automorphism L' of \mathbb{F}_{2^m} , since the sum of the images by L' of an even number of elements equals 0 if and only if the sum of these elements equals 0, so the property is affine invariant. It is EA invariant, since any affine (n, m)-function sums to 0 over every affine space of dimension at least 2. But it is not CCZ invariant, since if F is a (non-affine) permutation, it can be kth-order t-degree-sum-free while its compositional inverse is not. \diamond

Remark. In the conclusion of [8] is evoked the possibility of studying the following property: given $2 \leq l \leq k \leq n$ and any k-dimensional affine space A, the restriction of F to A has algebraic degree at least l (kth-order sum-freedom corresponds then to l = k). Let us compare this property with kth-order t-degree-sum-freedom. For this, let us endow A with the structure of the finite field \mathbb{F}_{2^k} . According to [7, Corollary 2], we know that the (k, m)-function $F_{|A|}$ (the restriction of F to A) has algebraic degree at least l if and only if there exists a non-negative integer r of 2-weight at most n-l, such that $\sum_{x \in A} x^r F(x) \neq 0$. This is different from kth-order t-degree-sum-freedom, whatever is t, even when m = n. For instance, taking for F the multiplicative inverse function, the sums involved in this property are $\sum_{x \in A} x^{r-1}$ while those involved in kth-order t-degree-sum-freedom are $\sum_{x \in A} x^{2^n-1-j}$, and the minimum 2-weight of r such that $\sum_{x \in A} x^{r-1} \neq 0$ is very different from the minimum 2-weight of j such that $\sum_{x \in A} x^{2^n-1-j} \neq 0$. The property mentioned in the conclusion of [8], even if it may be interesting to study for its own sake, has probably a weaker relation with integral attacks than kth-order t-degree-sum-freedom.

Proposition 2 If an (n, m)-function F is kth-order t-degree-sum-free, then the propagation through the S-box of the division property of order t + 1 of any k-dimensional affine space fails.

Indeed, for every k-dimensional affine space A, the algebraic degree of the indicator of F((A)) is at least m - t.

Remark. The notion could be extended to non-affine sets X, but then it would become quite complex to study, and it seems then reasonable to start studying this notion by restricting vectorial functions to affine spaces.

The larger t, the weaker the notion of kth-order t-degree-sum-freedom (if a function is kth-order t-degree-sum-free, then it is kth-order t'-degree-sum-free for every $t' \ge t$). The classic kth-order sum-freedom corresponds to t = 1. Indeed, the only possibility for F to be kth-order 1-degree sum-free is that $\sum_{x \in A} (F(x))^{2^i} = (\sum_{x \in A} F(x))^{2^i} \neq 0$ for some i, that is, $\sum_{x \in A} F(x) \neq 0$.

Remark. For k = 1, the property in Definition 1 is equivalent to saying that the function $(F(x))^j$ is injective. If F is injective, then we can take t = 1, and if it is not, then t does not exist.

For k = n, the question in Definition 1 is the (minimum) 2-weight of those j such that the function $(F(x))^j$ has algebraic degree n. Unlike the case k = 1, this question is not trivial for general functions, even if it is simpler than for general k. Note that there are functions for which it is still simpler, such as power functions $x \in \mathbb{F}_{2^n} \mapsto x^d$, for which the condition on j is $w_2(dj) = n$, that is, $j \in \frac{2^n - 1}{\gcd(d, 2^n - 1)}\mathbb{Z}/(2^n - 1)\mathbb{Z}$.

For k = n - 1, we have the same question to address, with the functions $F(x)(tr_n(ax) + \epsilon)$ where $a \in \mathbb{F}_{2^n}^*$ and $\epsilon \in \mathbb{F}_2$.

Let us see now that any (n, m)-function satisfying some reasonable condition is kth-order t-degree-sum-free for some t smaller than or equal to m.

Lemma 3 Every (n,m)-function such that, for any k-dimensional affine space A, the set F((A)) is non-empty (in particular, every injective (n,m)-function) is kth-order m-degree-sum-free.

Indeed, we recalled after Lemma 1 the existence, for every nonzero *m*-variable function f, of an *m*-variable Boolean function g of algebraic degree at most m such that $\sum_{y \in \mathbb{F}_{2^m}} f(y)g(y) \neq 0$. Taking for f the indicator of F((A)), this proves the existence of a non-negative integer j of 2-weight at most m such that $\sum_{y \in \mathbb{F}_{2^m}} y^j f(y) = \sum_{x \in A} (F(x))^j \neq 0$. The value t = m satisfies then the condition of Definition 1. This allows to give the following:

Definition 2 Let n, m be two positive integers and let $2 \le k \le n$. Let F be any (n, m)-function such that, for any k-dimensional affine space A, the set F((A)) is non-empty (for instance, let F be injective). We call kth-order sumfree min-degree of F the smallest value of $t \le m$ such that F is kth-order t-degree-sum-free.

According to the EA invariance of kth-order t-degree-sum-freedom, the kthorder sum-free min-degree of the functions having the property requested in Definition 2 (i.e. for any k-dimensional affine space A, the set F((A)) is nonempty) is an affine invariant parameter, that is, if L and L' are two affine permutations, then the kth-order sum-free min-degree of F equals the kth-order sum-free min-degree of $L \circ F \circ L'$. This can also be seen by the fact that the composition by affine automorphisms preserves the algebraic degree (see e.g. [7])

Remark. The condition on F in Definition 2 is necessary, since if it is not satisfied for some A, the kth-order sum-free min-degree cannot exist. Take for instance $F(x) = G(x + x^2)$, then for every j, the sum of the values of $(F(x))^j$ over an affine space stable under translation by 1 equals 0.

It would be nice to characterize precisely, for every n, m and k such that $2 \leq k$ k < n, what is the set of all the (n, m)-functions satisfying this condition. For k = 1, it is clearly the set of injective functions. For k = 2, it is the set of those functions F such that, for every nonzero $a \in \mathbb{F}_2^n$, $D_a F$ takes zero value for at most two inputs (among which we have all APN functions). For k = n, it is the set of those functions whose image multiset has some points having an odd multiplicity. For $k \in \{3, \ldots, n-1\}$, we leave this question open, but we give an example of an infinite class of non-bijective (m, m)-functions satisfying it for every even k. We take for F any power (m, m)-function $F(x) = x^d$ such that $gcd(d, 2^m - 1) = 3$ (as are all APN power functions over \mathbb{F}_{2^m} for m even, see [7, Proposition 165]). Let A be a k-dimensional vector subspace of \mathbb{F}_{2^m} and suppose that $F((A)) = \emptyset$. Let us denote by w a primitive element of \mathbb{F}_4 . The pre-images by F are the singleton $\{0\}$ and the 3-sets $u\mathbb{F}_4^*$, where $u \neq 0$. Since $F((A)) = \emptyset$, then A must not contain 0, and for every $a \in A$, we must have either $aw \in A$ (and $aw^2 \notin A$ which is in fact automatically implied by $0 \notin A$ since $a + aw + aw^2 = 0$ or $aw^2 \in A$ (and $aw \notin A$). Since if $b = aw^2$ then a = bw, we have then that A is the disjoint union of a set S of size 2^{k-1} and of the set $wS = \{wx; x \in S\}$. The elements of S are the elements x of A such that $wx \in A$. Hence, $S = A \cap w^2 A$ is an affine space. Since $A = S \cup wS$ is an affine space and S is an affine hyperplane of A, the \mathbb{F}_2 -vector space E underlying S is then stable under the multiplication by w. Then E is a vector space over \mathbb{F}_4 and its dimension k-1, as an \mathbb{F}_2 -vector space, is then even. This proves that if we take k even, then F satisfies the condition of Definition 2.

Note that, since for m odd, all APN power (m, m)-functions are bijective, all APN power functions satisfy the condition in Definition 2 for any k if m is odd and for any even k if m is even.

3.3 An upper bound on the *k*th-order sum-free min-degree

We shall prove that every (n, m)-function satisfying the condition of Definition 2 is kth-order k-degree-sum-free, that is, has kth-order sum-free min-degree at most k. This is clearly true if F((A)) is an affine space, but it is not immediately clear in general.

Remark. Note that F((A)) having an even size, it cannot be reduced to $\{0\}$. There exists then b in $F((A)) \setminus \{0\}$. Denoting by 1_b the indicator of the singleton $\{b\}$ in \mathbb{F}_{2^m} , we have $\sum_{x \in A} (1_b \circ F)(x) = 1$, but 1_b has algebraic degree m and the question is: can we replace it (or another function having the same property) by a function of algebraic degree at most k? Without loss of generality, up to affine equivalence, we can assume that b is the all-1 vector. Then $1_b(y) = \prod_{i=1}^m y_i$ and denoting the coordinate functions of F by f_1, \ldots, f_m , we have $(1_b \circ F)(x) = \prod_{i=1}^m f_i(x)$. By Jordan's reduction, there exist, up to a permutation of the input variables (which we can apply without loss of generality), n-k affine Boolean functions l_{k+1}, \ldots, l_n , such that, for every $x = (x_1, \ldots, x_n)$ in A, we have $x_{k+1} = l_{k+1}(x_1, \ldots, x_k), \ldots, x_n = l_n(x_1, \ldots, x_k)$. For every $x \in A$, we can substitute in $\prod_{i=1}^m f_i(x)$ every $x_{k+l}, l = 1, \ldots, n-k$, with $l_{k+l}(x_1, \ldots, x_k)$. Then f_1, \ldots, f_m become functions in k variables, but it is not clear whether we can express $1_b \circ F$ or any other function g such that $\sum_{x \in A} (g \circ F)(x) = 1$ in the form $g' \circ F$ where g' has algebraic degree at most k.

The question whether the indicator f of F((A)) has its algebraic degree larger than m - k (equivalent to the question whether there exists a Boolean function g of algebraic degree at most k over \mathbb{F}_2^m such that fg has algebraic degree m) needs then to be approached in a different way. This is what we do below. \diamond

Proposition 3 Let n, m be two positive integers and let $2 \le k \le n$. Let F be any (n, m)-function such that $F((A)) \ne \emptyset$ for every k-dimensional affine space A. Then F has kth-order sum-free min-degree at most $\min(k, m)$, with equality if and only if there exists a k-dimensional affine space A on which F is injective (with $k \le m$) and whose image is an affine space, or F((A)) equals \mathbb{F}_{2^m} (with $k \ge m$).

Proof. Since we know that we can take $t \leq m$, we just have to show, for proving the upper bound, that we can take $t \leq k$. For every k-dimensional affine space A, the set F((A)) has size at most 2^k and its indicator f has then an algebraic degree at least m-k (indeed, we know, see [15, 7], that any nonzero m-variable Boolean function of algebraic degree at most d has Hamming weight at least 2^{m-d}). There exists then, according to Lemma 2, an integer j of 2-weight at most k such that $\sum_{y \in \mathbb{F}_{2^m}} y^j f(y) = \sum_{x \in A} (F(x))^j \neq 0$. This proves the bound. Let us now determine when this bound is an equality.

If $m \geq k$, then the *k*th-order sum-free min-degree of F equals k if and only if there exists a k-dimensional affine space A such that, for every non-negative integer j such that $w_2(j) < k$, we have $\sum_{y \in \mathbb{F}_{2^m}} y^j f(y) = \sum_{x \in A} (F(x))^j = 0$, that is, the algebraic degree of the indicator function of F((A)) is at most m - k, that is, given the size of F((A)), equals m - k, which is equivalent to the fact that F((A)) is a k-dimensional affine space (see [15, 7]).

If $m \leq k$, then the *k*th-order sum-free min-degree of *F* equals *m* if and only if F((A)) equals \mathbb{F}_{2^m} , since otherwise, the algebraic degree of the indicator of F((A)) is at least 1 and the *k*th-order sum-free min-degree of *F* is then at most m-1.

We shall see that the bound of Proposition 3 is tight, at least for m = n.

3.4 Lower bounds on the *k*th-order sum-free min-degree

After the upper bound on the value of t in the previous subsection, we show in the present subsection a lower bound. Denoting by deg (F(x)) the algebraic degree of function F(x), we have, for every non-negative integer j:

 $\deg\left((F(x))^j\right) \le w_2(j)\,\deg(F),$

since the algebraic degree of the function $G : x \in \mathbb{F}_{2^m} \mapsto x^j$ equals $w_2(j)$ and we have, for every (n, m)-function F, and any (m, m)-function G: $\deg(G \circ F) \leq \deg(G) \deg(F)$. Let A be any k-dimensional affine space. If $\deg((F(x))^j) < k$, then we have $\sum_{x \in A} (F(x))^j = 0$. We deduce:

Proposition 4 Let F be any (n,m)-function that is kth-order t-degree sumfree. We have:

$$t \ge \left\lceil \frac{k}{\deg(F)} \right\rceil. \tag{1}$$

Indeed, if $t < \frac{k}{\deg(F)}$ then, for every j such that $w_2(j) \le t$, we have deg $((F(x))^j) \le \deg(F) w_2(j) < k$.

Note that Proposition 4 generalizes the property that F cannot be kth-order sum-free when $\deg(F) < k$, and it provides an information only when $\deg(F) < k$, since we know that $t \ge 1$.

3.4.1 Alternate lower bounds

Other upper bounds exist on the algebraic degree of the composition of functions, which are often better than the so-called naive bound $\deg(G \circ F) \leq \deg(G) \deg(F)$, and we shall directly deduce lower bounds on t which will be often better.

The first bound, proved in [5], on the algebraic degree of composed functions, is valid under a very strong hypothesis¹: the Walsh transform $W_F(u, v) = \sum_{x \in \mathbb{F}_2^n} (-1)^{v \cdot F(x) + u \cdot x}$ (where \cdot denotes by abuse of notation an inner product in \mathbb{F}_2^n and an inner product in \mathbb{F}_{2^m}) has all its values divisible by 2^l , for a large enough value of l. Then we have deg $(G \circ F) \leq n - l + \text{deg}(G)$, and therefore:

$$t \ge k - n + l.$$

Indeed, if t < k - n + l then, for every j such that $w_2(j) \leq t$, we have $deg((F(x))^j) \leq n - l + t < k$.

The second upper bound, proved in [3], on the algebraic degree of composed functions, does not apply to all functions either, but its assumption, which is that F is a permutation (with m = n, then), is always satisfied when dealing

 $^{^1{\}rm This}$ bound is then essentially useful for identifying a feature that should be avoided when choosing an S-box; we give it for being complete on the state of the art.

with the model of block ciphers called Substitution-Permutation networks. This bound is:

$$\deg(G \circ F) \le n - 1 - \left\lfloor \frac{n - 1 - \deg(G)}{\deg(F^{-1})} \right\rfloor.$$
(2)

It is always less that n (when G itself has an algebraic degree less than n), which is an important advantage over the naive bound, and it outperforms the latter in many cases where this one is less than n.

Note that if we apply this bound twice, we obtain $\deg(G) = \deg(G \circ F^{-1} \circ F) \leq n - 1 - \left\lfloor \frac{n - 1 - \deg(G \circ F^{-1})}{\deg(F^{-1})} \right\rfloor \leq n - 1 - \left\lfloor \frac{\left\lfloor \frac{n - 1 - \deg(G)}{\deg(F)} \right\rfloor}{\deg(F^{-1})} \right\rfloor$, and it would be nice to find a bound which performs better under the same hypothesis when we apply it twice this way.

Remark. Taking for F and G power functions over \mathbb{F}_{2^n} , say, $F(x) = x^r$ and $G(x) = x^s$, we have $G \circ F(x) = x^{rs}$ and we have then:

$$w_2(rs) \le n - 1 - \left\lfloor \frac{n - 1 - w_2(s)}{w_2(r')} \right\rfloor,$$
 (3)

where $w_2(rs)$ is the 2-weight of the representative of rs modulo $2^n - 1$ that lies in $\{0, \ldots, 2^n - 2\}$, and r' is the inverse of r in $\mathbb{Z}/(2^n - 1)\mathbb{Z}$.

Note that $w_2(r')$ needs to be small for allowing a significant bound. For instance, when r is a Gold APN exponent, $r = 2^i + 1$, gcd(i, n) = 1, and n is odd (so that r is invertible mod $2^n - 1$), this gives, according to [17, 16]: $w_2(rs) \leq n - 1 - \left\lfloor \frac{2(n-1-w_2(s))}{n+1} \right\rfloor$, which gives $w_2(rs) \leq n-2$ or $w_2(rs) \leq n-1$. But there are values of r for which the bound is interesting, for instance when r is the inverse of a Gold exponent. And the naive bound, which says that $w_2(rs) \leq w_2(r)w_2(s)$, often gives no information at all.

Bound (2) implies:

Proposition 5 Let F be any (n, n)-permutation and let $\deg(F^{-1})$ be the algebraic degree of the compositional inverse of F. Then, if F is kth-order t-degree sum-free, we have:

$$t \ge n - 1 - (n - 1 - k) \deg(F^{-1}), \tag{4}$$

i.e., the kth-order sum-free min-degree of F is at least this number.

Indeed, according to (2), if $t < n - 1 - (n - 1 - k) \deg(F^{-1})$ then, for every j such that $w_2(j) \le t$, we have $\deg\left((F(x))^j\right) < n - 1 - \left\lfloor \frac{(n-1-k)\deg(F^{-1})}{\deg(F^{-1})} \right\rfloor = k$. Note that Proposition 5 provides an information only if $n - 1 - (n - 1 - k) \deg(F^{-1}) > 1$, that is, $\deg(F^{-1}) < \frac{n-2}{n-1-k}$, since we know that $t \ge 1$. The condition $\deg(F^{-1}) < \frac{n-2}{n-1-k}$ is always satisfied when $n < \frac{n-2}{n-1-k}$ (since $\deg(F^{-1}) \le n$), that is, when $k > n + \frac{2}{n} - 2$, but this corresponds to $k \in \{n-1, n\}$ and then for most values of k it needs to be satisfied. **Remark.** We have $n - 1 - (n - 1 - k) \deg(F^{-1}) \leq k$ since $k \leq n - 1$ and $\deg(F^{-1}) \geq 1$, and this is coherent with Proposition 3, since F is a permutation.

Proposition 5 can be applied to show that some permutations cannot be kth-order sum-free (that is, kth-order t-degree sum-free with t = 1). We have $n - 1 - (n - 1 - k) \deg(F^{-1}) \ge 2$ if and only if $\deg(F^{-1}) \le \frac{n-3}{n-1-k}$. We deduce:

Corollary 1 Let n and k be positive integers such that $2 \le k \le n-2$ and F an (n,n)-permutation. If $\deg(F^{-1}) \le \frac{n-3}{n-1-k}$, then F is not kth-order sum-free.

Indeed, (4) implies $t \ge 2$, a contradiction with t = 1.

Of course this corollary does not allow to prove that the multiplicative inverse function is not kth-order sum-free for some $k \in \{3, \ldots, n-3\}$, since this function is involutive and has an algebraic degree that is maximum for a permutation (this generalizes to any permutation of algebraic degree n-1, since we know from [4] that its inverse has then the same algebraic degree).

A third bound, proved in [6], is (with the naive bound) the only known upper bound valid for all (n, m)-functions:

$$\deg(G \circ F) \le \deg(1_{\mathcal{G}_F}) + \deg(G) - m, \tag{5}$$

where $\deg(1_{\mathcal{G}_F})$ is the algebraic degree of the (n+m)-variable Boolean function equal to the indicator of the graph $\mathcal{G}_F = \{(x, F(x)); x \in \mathbb{F}_2^n\}$. This bound is in general tighter than the naive bound, and it can be tighter than (2), as seen in [6]. Of course, the algebraic degree of the indicator of the graph may be more difficult to evaluate than the algebraic degree of the inverse.

Remark. When *F* and *G* are power functions, say $F(x) = x^r$, $G(x) = x^s$, using that $1_{\mathcal{G}_F}(x, y) = 1$ if and only if $y = x^r$, we have $1_{\mathcal{G}_F}(x, y) = (y + x^r)^{2^n - 1} + 1 = 1 + \sum_{i=0}^{2^n - 1} x^{ri} y^{2^n - 1 - i}$ (the latter equality being obtained by a binomial expansion, using for instance Lucas's theorem to show that $\binom{2^n - 1}{i}$ (mod 2) equals 1 for every $i \in \{0, \ldots, 2^n - 1\}$). We have then $\deg(1_{\mathcal{G}_F}) = \max\{w_2(ri) + w_2(2^n - 1 - i) = w_2(ri) + n - w_2(i); i \in \mathbb{Z}/(2^n - 1)\mathbb{Z}\}$ (where the elements of $\mathbb{Z}/(2^n - 1)\mathbb{Z}$ are identified with their representatives in $\{0, \ldots, 2^n - 2\}$; note that by writing $i \in \mathbb{Z}/(2^n - 1)\mathbb{Z}$, we lose the case $i = 2^n - 1$, but this case provides the value $w_2(ri) + n - w_2(i) = n$, which cannot be larger than the maximum, since for i = 0 we get also $w_2(ri) + n - w_2(i) = n$). Bound (5) becomes

$$w_2(rs) \le \max\{w_2(ri) + w_2(s) - w_2(i); i \in \mathbb{Z}/(2^n - 1)\mathbb{Z}\}$$
(6)

where the 2-weights of rs and ri are those of the representatives of these numbers in $\{0, \ldots, 2^n - 2\}$ (i.e. the coset-leaders). Hence, in the case of power functions, Bound (5) doesn't give any interesting information since $w_2(rs)$ is one of the elements $w_2(ri) + w_2(s) - w_2(i)$ (for i = s).

Bound (5) implies:

Proposition 6 Let F be any (n, m)-function and let $\deg(1_{\mathcal{G}_F})$ be the algebraic degree of the indicator of the graph $\mathcal{G}_F = \{(x, F(x)); x \in \mathbb{F}_2^n\}$ of F. Then, if F is kth-order t-degree sum-free, we have:

$$t \ge m + k - \deg(1_{\mathcal{G}_F}),\tag{7}$$

i.e., the kth-order sum-free min-degree of F is at least this number.

Indeed, according to Relation (5), if $t < m + k - \deg(1_{\mathcal{G}_F})$ then, for every j such that $w_2(j) \leq t$, we have $\deg((F(x))^j) < k$.

Note that there is in [6] an exact expression of $\deg(G \circ F)$, but this expression of the degree is complex.

Remark. We have $m + k - \deg(1_{\mathcal{G}_F}) \leq k$ since $\deg(1_{\mathcal{G}_F}) \geq m$, and this is coherent with Proposition 3, when F satisfies the condition in Definition 2.

Here also, Proposition 6 can be applied to show that some functions cannot be kth-order sum-free (that is, kth-order t-degree sum-free with t = 1). We have $m + k - \deg(1_{\mathcal{G}_F}) \geq 2$ if and only if $\deg(1_{\mathcal{G}_F}) \leq m + k - 2$. Proposition 6 implies then:

Corollary 2 Let n, m and k be positive integers such that $2 \le k \le n-1$ and F an (n,m)-function. If $\deg(1_{\mathcal{G}_F}) \le m+k-2$, then F is not kth-order sum-free.

Indeed, Relation (7) implies $t \ge 2$, a contradiction with t = 1.

This corollary does not allow to prove that the multiplicative inverse function is not kth-order sum-free for some $k \in \{3, \ldots, n-3\}$ either, since we have for this function that $\deg(1_{\mathcal{G}_{F_{inv}}}) = 2n$ is strictly larger than n + k - 2 for every $2 \leq k \leq n$. The fact that $\deg(1_{\mathcal{G}_{F_{inv}}}) = 2n$ comes from the relation $1_{\mathcal{G}_{F_{inv}}}(x,y) = (y + x^{2^n - 2} + 1)^{2^n - 1} = \sum_{i=0}^{2^n - 1} (x(y+1))^i = (x(y+1) + 1)^{2^n - 1}$.

4 A few examples in the particular case of k = 2

In this section we visit some examples of (infinite classes of) non-APN functions satisfying the condition of Definition 2, and we look whether it is difficult to determine the values of those j of minimum 2-weight such that $(F(x))^j$ sums to nonzero values over affine planes. Since F satisfies the condition in Definition 2, Proposition 3 tells us that there is always a value of j that has 2-weight at most 2. We shall see that, even for this particular value of k, which is the simplest to consider when $k \leq n-2$, and even when F is a power function, which also simplifies the study, determining for each k-dimensional affine space

 \diamond

A the actual values of j of 2-weight at most k such that $\sum_{x \in A} (F(x))^j \neq 0$, can be challenging.

A non-APN (n, n)-function has what [14] calls vanishing flats (which are in fact vanishing planes, since they are the affine planes $\{x, y, z, x + y + z\}$, with x, y, z distinct, over which F sums to 0, but we shall respect the published terminology)². For a non-vanishing flat, the smallest value of the 2-weight of j for which $(F(x))^j$ sums to a nonzero value equals 1, and we need then to only consider the planes that are vanishing flats, when investigating such values of j. Note that the vanishing flats of a vectorial (n, m)-function F are by definition the projections over \mathbb{F}_2^n , parallel to \mathbb{F}_2^m , of the affine planes included in the graph of F. The next lemma is straightforward.

Lemma 4 Let F be an (n,m)-function satisfying the condition in Definition 2 and $P = \{x, y, z, x + y + z\}$ a vanishing flat of F. Then we have that $F(P) = \{F(x), F(y), F(z), F(x + y + z)\}$ is an affine plane and, given an integer j, we have $\sum_{x \in P} (F(x))^j \neq 0$ if and only if F(P) is not a vanishing flat of the power function $G(x) = x^j$ over \mathbb{F}_{2^m} .

In the first example below, determining the vanishing flats P is easy, and determining the values of j such that $\sum_{x \in P} (F(x))^j \neq 0$ for each of them seems difficult (it is easy for some of them, but not for all). In the second example, determining the vanishing flats P is easy, and determining the values of j such that $\sum_{x \in P} (F(x))^j \neq 0$ for each of them is easy as well. In the last example, even determining the vanishing flats is non-trivial, except for those including the zero element. We keep the study of the inverse function for the next Section.

4.1 Quadratic power functions

It is easy to determine the vanishing flats of quadratic power functions (as done in [14] among other results). Without loss of generality, we take $F(x) = x^d$ where $d = 2^i + 1$. Before recalling what these vanishing flats are, we first need to determine when F satisfies the condition of Definition 2 for k = 2, so that it can be second-order t-degree-sum-free for some value of t.

Lemma 5 Let $F(x) = x^d$ where $d = 2^i + 1$. Then F satisfies the condition of Definition 2 if and only if n is odd or gcd(i, n) = 1.

Proof. If gcd(i, n) = 1, then F is APN and we have seen in the remark after Definition 2 that any power APN function satisfies the condition of Definition 2 for k = 2. We assume now that gcd(i, n) > 1. Let P be an affine plane. We have $F((P)) = \emptyset$ if and only if we can write $P = \{x, y, z, x + y + z\}$ with F(x) = F(z) and F(y) = F(x + y + z). Denoting a = x + z, we have $P = \{x, x + a, y, y + a\}$ with $a \neq 0$ and x, y distinct modulo a, such that $ax^{2^i} + ax^{2^i} + ax^{2^i}$

 $^{^2 \}mathrm{More}$ generally, when the dimension of the affine space equals k instead of 2, we speak of vanishing k-flats.

 $a^{2^{i}}x + a^{2^{i}+1} = ay^{2^{i}} + a^{2^{i}}y + a^{2^{i}+1} = 0, \text{ that is, } \begin{cases} ax^{2^{i}} + a^{2^{i}}x = a^{2^{i}+1} \\ a(x+y)^{2^{i}} + a^{2^{i}}(x+y) = 0 \end{cases},$

that is, $\begin{cases} \left(\frac{x}{a}\right)^{2^{i}} + \frac{x}{a} = 1\\ x + y \in a \mathbb{F}_{2^{\text{gcd}(i,n)}} \end{cases}$. If *n* is odd, the first equation has no solution *x*

since $tr_n\left(\left(\frac{x}{a}\right)^{2^i} + \frac{x}{a}\right) = 0$ and $tr_n(1) = 1$, and F satisfies then the condition of Definition 2. If n is even, then choosing any solution x of the first equation and any $y \in x + a\left(\mathbb{F}_{2gcd(i,n)} \setminus \mathbb{F}_2\right)$ provides an affine plane P such that $F((P)) = \emptyset$, and the condition of Definition 2 is not satisfied by F. \Box

4.1.1 Vanishing flats

Lemma 6 [14] Let n, i be positive integers. Let $F(x) = x^{2^i+1}$. The vanishing flats of F are the planes $\{x, y, z, x+y+z\}$ with x, y, z distinct, such that y+z = w(x+z) where $w \in \mathbb{F}_{2^l} \setminus \mathbb{F}_2$ with $l = \gcd(i, n)$. Equivalently, they are the planes $\{x, y, z, x+y+z\}$ with x, y distinct and z = wx + (w+1)y, where $w \in \mathbb{F}_{2^l} \setminus \mathbb{F}_2$ (and such vanishing flats exist then if and only if this latter set is not empty, that is, $\gcd(i, n) > 1$, which is indeed equivalent to the fact that F is non-APN).

Let us give an original proof of this known result, for self-completeness. A plane $\{x, y, z, x + y + z\}$ with x, y, z distinct, is a vanishing flat of F if and only if $x^{2^i+1}+y^{2^i+1}+z^{2^i+1}+(x+y+z)^{2^i+1}=0$, that is, $(x+z)(y+z)^{2^i}+(x+z)^{2^i}(y+z)=0$, or equivalently, $(y+z)^{2^i-1}=(x+z)^{2^i-1}$, that is, y+z=w(x+z) where w is any (2^i-1) th root of unity different from 1 in \mathbb{F}_{2^n} , which is equivalent to $w \in \mathbb{F}_{2^l} \setminus \mathbb{F}_2$ with $l = \gcd(i, n)$. And y+z=w(x+z) being equivalent to $z=\frac{wx+y}{1+w}$, we obtain the stated expression by changing w into $(w+1)^{-1}+1$ (which belongs to $\mathbb{F}_{2^l} \setminus \mathbb{F}_2$ if and only if w belongs to $\mathbb{F}_{2^l} \setminus \mathbb{F}_2$). The fact that x, y are distinct is sufficient for having x, y, z distinct. Note that this characterization of vanishing flats is coherent with the fact that F is APN if and only if $l = \gcd(i, n)$ equals 1 (since l = 1 if and only if $\mathbb{F}_{2^l} \setminus \mathbb{F}_2$ is empty).

4.1.2 On the values of j such that $\sum_{x \in P} (F(x))^j \neq 0$

For gcd(i, n) = 1, that is, for F APN, we know that F is second-order 1-degreesum-free. For gcd(i, n) > 1, assuming that the condition of Definition 2 is satisfied (that is, n is odd, according to Lemma 5) for each vanishing flat P, the determination of those integers j of 2-weight 2 such that $\sum_{x \in P} (F(x))^j \neq 0$ can be reduced without loss of generality to the case where $j = 2^r + 1$ (and we can impose $r \leq \frac{n-1}{2}$). We have by hypothesis that $x^{2^i+1} + y^{2^i+1} + z^{2^i+1} + (x + y +$ $z)^{2^i+1} = 0$. We have then that $(F(x))^j + (F(y))^j + (F(z))^j + (F(x + y + z))^j$ equals $x^{(2^i+1)(2^r+1)} + y^{(2^i+1)(2^r+1)} + z^{(2^i+1)(2^r+1)} + (x^{2^i+1} + y^{2^i+1} + z^{2^i+1})^{2^r+1} =$ $(xy^{2^r})^{2^i+1} + (yx^{2^r})^{2^i+1} + (xz^{2^r})^{2^i+1} + (zx^{2^r})^{2^i+1} + (yz^{2^r})^{2^i+1} + (zy^{2^r})^{2^i+1}$. We can assume that y = 1, since y is nonzero and dividing x, y, z by a same nonzero constant preserves the property of being a vanishing flat (note that it does not change the relation z = wx + (w + 1)y either). The condition becomes $x^{2^{i}+1} + (x^{2^{r}})^{2^{i}+1} + (xz^{2^{r}})^{2^{i}+1} + (zx^{2^{r}})^{2^{i}+1} + (z^{2^{r}})^{2^{i}+1} + z^{2^{i}+1} \neq 0$ and replacing z by its value z = wx + w + 1, where $w \in \mathbb{F}_{2^{\text{gcd}(i,n)}} \setminus \mathbb{F}_2$, this gives:

$$x^{2^{i}+1} + (x^{2^{r}})^{2^{i}+1} + (x(wx+w+1)^{2^{r}})^{2^{i}+1} + ((wx+w+1)x^{2^{r}})^{2^{i}+1} + ((wx+w+1)^{2^{r}})^{2^{i}+1} + (wx+w+1)^{2^{i}+1} \neq 0, \forall x \in \mathbb{F}_{2^{n}}.$$

The fact that $w^{2^i} = w$ does not simplify much the value of $(wx + w + 1)^{2^i+1} = (wx^{2^i} + w + 1)(wx + w + 1) = w^2x^{2^i+1} + (w^2 + w)(x^{2^i} + x) + w^2 + 1$. Determining all values of r satisfying this condition needs to solve the equation

$$\begin{split} (w^{2^{r}} + w)^{2} & (x^{(2^{r}+1)(2^{i}+1)} + x^{2^{i}+1} + x^{2^{r}(2^{i}+1)} + 1) + \\ & (w^{2} + w)^{2^{r}} & (x^{2^{i+r}+2^{i}+1} + x^{2^{r}+2^{i}+1} + x^{2^{i+r}} + x^{2^{r}}) + \\ & (w^{2} + w) & (x^{2^{r+i}+2^{r}+2^{i}} + x^{2^{r+i}+2^{r}+1} + x^{2^{i}} + x) = 0, \end{split}$$

which does not seem easy to solve.

Lemma 4 slightly simplifies the work. Let $P = \{x, y, z, x + y + z\}$ be a vanishing flat of F, then $F(P) = \{x^{2^{i}+1}, y^{2^{i}+1}, z^{2^{i}+1}, (x + y + z)^{2^{i}+1}\}$ is an affine plane and we have $\sum_{x \in P} (F(x))^{2^{r}+1} \neq 0$ if and only if F(P) is not a vanishing flat of the Gold function $G(x) = x^{2^{r}+1}$. According to Lemma 6, this is equivalent to $\frac{y^{2^{i}+1}+z^{2^{i}+1}}{x^{2^{i}+1}+z^{2^{i}+1}} \notin \mathbb{F}_{2^{\text{gcd}(r,n)}}$. - If gcd(r,n) = 1, then clearly F(P) is a non-vanishing flat; hence, all the values

- If gcd(r, n) = 1, then clearly F(P) is a non-vanishing flat; hence, all the values of j of the form $(2^r + 1)2^l$ where gcd(r, n) = 1 are such that $\sum_{x \in P} (F(x))^j \neq 0$. - If gcd(r, n) > 1, then after taking, without loss of generality, y = 1 and z = wx + w + 1, where $w \in \mathbb{F}_{2^{gcd(i,n)}} \setminus \mathbb{F}_2$, we are led to considering the equation

$$(1 + (wx + w + 1)^{2^{i}+1})^{2^{r}-1} = (x^{2^{i}+1} + (wx + w + 1)^{2^{i}+1})^{2^{r}-1},$$

that is (after multiplying both members by $(1 + (wx + w + 1)^{2^i+1})(x^{2^i+1} + (wx + w + 1)^{2^i+1}))$ the same equation as above. The work is simplified if, while keeping y = 1 and z = wx + w + 1, we rather express that $\frac{z^{2^i+1}+y^{2^i+1}}{x^{2^i+1}+y^{2^i+1}} \notin \mathbb{F}_{2^{\text{gcd}(r,n)}}$, that is, $\frac{(wx+w+1)^{2^i+1}+1}{x^{2^i+1}+1} \notin \mathbb{F}_{2^{\text{gcd}(r,n)}}$. For each $w' \in \mathbb{F}_{2^{\text{gcd}(r,n)}} \setminus \mathbb{F}_2$, we need to consider the equation $(wx + w + 1)^{2^i+1} + 1 = w'(x^{2^i+1} + 1)$, that is:

$$(w^{2} + w')(x^{2^{i}+1} + 1) + (w^{2} + w)(x^{2^{i}} + x) = 0.$$
(8)

The equations of the form $ax^{2^{i+1}} + bx + c = 0$ are addressed in [11] and the references therein (the resolution is not that simple); but as far as the author knows, the equations of the form $ax^{2^{i+1}} + b(x^{2^{i}} + x) + c = 0$ have been less studied.

4.2 Inverses of quadratic power permutations

Determining the vanishing flats of non-quadratic functions is in most cases difficult. A case where it is simplified is when the function is a permutation whose compositional inverse is quadratic (and if it is also a power function, it is simpler), or more generally when the function is CCZ equivalent to a quadratic (power) function. It is indeed shown in [14] that if two functions are CCZ-equivalent, then their vanishing flats correspond to each others in a simple way. We rephrase below this result and we give a short argument, for self-completeness.

Lemma 7 [14] Let F be any (n, m)-function and let G be CCZ equivalent to F. Let $\mathcal{A} = (\mathcal{A}_1, \mathcal{A}_2)$ be an affine automorphism which maps the graph of F to the graph of G and let $F_1(x)$ be the permutation equal to $\mathcal{A}_1(x, F(x))$. Then the vanishing flats of G are the images by F_1 of the vanishing flats of F.

In particular, if F is an (n, n)-permutation, then the vanishing flats of F^{-1} are the images by F of the vanishing flats of F. They are the affine planes of the form $\{F(x), F(y), F(z), F(x+y+z) = F(x) + F(y) + F(z)\}$.

A plane $P = \{x, y, z, x + y + z\}$ is then a vanishing flat of F^{-1} if and only if $\{F^{-1}(x), F^{-1}(y), F^{-1}(z), F^{-1}(x) + F^{-1}(y) + F^{-1}(z)\}$ is a vanishing flat of F.

Proof. We know that the vanishing flats of G are the projections over \mathbb{F}_2^n parallel to \mathbb{F}_2^m of the affine planes included in the graph of G. For every subset S of $\mathbb{F}_2^n \times \mathbb{F}_2^m$, $\mathcal{A}(S)$ is an affine plane if and only if S is an affine plane. The affine planes P' included in the graph of G are then the images by \mathcal{A} of the affine planes P included in the graph of F. The projection over \mathbb{F}_2^n parallel to \mathbb{F}_2^m of P' equals the image by F_1 of P. This completes the proof in the general case. In the case where $G = F^{-1}$, we have $\mathcal{A}(x, y) = (y, x)$ and then $F_1(x) = F(x)$. \Box

Let us study the case where $F(x) = x^d$ is a quadratic power permutation. Without loss of generality, we take $d = 2^i + 1$, where $gcd(d, 2^n - 1) = \frac{gcd(2^{2i}-1,2^n-1)}{gcd(2^{i}-1,2^n-1)} = \frac{2^{gcd(2i,n)}-1}{2^{gcd(i,n)}-1} = 1$ (that is, where gcd(2i,n) equals gcd(i,n), that we assume different from 1 so that F is not APN).

For instance, with $F(x) = x^5$ and $n \equiv 2 \pmod{4}$, we have i = 2, $\gcd(2i, n) = \gcd(i, n) = 2$ and $F^{-1}(x) = x^{\frac{3\cdot 2^n - 2}{5}}$ (with $3 \cdot 2^n - 2$ divisible by 5), since $5\frac{3\cdot 2^n - 2}{5} \equiv 1 \pmod{2^n - 1}$. We have that $G(x) = F^{-1}(x)$ is not second-order sum-free, that is, not APN, since its inverse x^5 is not APN, because $\gcd(2, n) = 2 \neq 1$.

Coming back to the general case of $F(x) = x^d$, the vanishing flats of F^{-1} are, according to Lemma 7, the planes $\{x^d, y^d, z^d, x^d + y^d + z^d = (x + y + z)^d\}$. According to Lemma 6, the vanishing flats of F(x) when $d = 2^i + 1$ are the planes $\{x, y, z, x + y + z\}$ with x, y, z distinct, such that z = wx + (w + 1)y, where w ranges over $\mathbb{F}_{2gcd(i,n)} \setminus \mathbb{F}_2$ (and the condition $x \neq y$ is sufficient for having x, y, z distinct). We deduce: **Lemma 8** The vanishing flats of the function $x^{\frac{1}{d}}$, where $d = 2^i + 1$, gcd(2i, n) = gcd(i, n), are the planes of the form:

$$P = \{x^d, y^d, (wx + (w+1)y)^d, ((w+1)x + wy)^d\},\$$

where $x \neq y \in \mathbb{F}_{2^n}$ and $w \in \mathbb{F}_{2^{\operatorname{gcd}(i,n)}} \setminus \mathbb{F}_2$.

In particular, for $n \equiv 2 \pmod{4}$, the vanishing flats of the permutation $x^{\frac{3 \cdot 2^n - 2}{5}}$ are the affine planes of the form:

$${x^5, y^5, (wx + w^2y)^5, (w^2x + wy)^5}$$

where $x \neq y \in \mathbb{F}_{2^n}$ and w is a primitive element of \mathbb{F}_4 . Let us now see what gives $\sum_{x \in P} (x^{\frac{1}{d}})^j$ when P is a vanishing flat of $x^{\frac{1}{d}}$ (that we assume non-APN; hence we take $\gcd(i, n) > 1$) and j is a positive integer of 2-weight 2. Without loss of generality, we take $j = 1 + 2^r$, and we have to calculate $(x^d)^{\frac{j}{d}} + (y^d)^{\frac{j}{d}} + ((wx + (w + 1)y)^d)^{\frac{j}{d}} + ((w + 1)x + wy)^d)^{\frac{j}{d}} = x^{1+2^r} + y^{1+2^r} + (wx + (w + 1)y)^{1+2^r} + ((w + 1)x + wy)^{1+2^r} = (1 + w^{1+2^r} + (w + 1)^{1+2^r})(x^{1+2^r} + y^{1+2^r}) + (w(w + 1)^{2^r} + w^{2^r}(w + 1))(xy^{2^r} + x^{2^r}y) = (w^{2^r} + w)(x^{1+2^r} + y^{1+2^r} + xy^{2^r} + x^{2^r}y) = (w^{2^r} + w)(x + y)^{1+2^r}$, which equals 0 if and only if $w^{2^r} + w = 0$, that is, $w \in \mathbb{F}_{2^r} \cap (\mathbb{F}_{2^{\gcd(i,n)}} \setminus \mathbb{F}_2) = \mathbb{F}_{2^{\gcd(r,i,n)}} \setminus \mathbb{F}_2$. We deduce:

Proposition 7 Let $F(x) = x^d$, where $d = 2^i + 1$, with gcd(2i, n) = gcd(i, n) > 1. Given any vanishing flat P of F^{-1} and a corresponding value w given by Lemma 8, the set of those integers j of 2-weight 2 such that $\sum_{x \in P} (x^{\frac{1}{d}})^j \neq 0$ equals the set of those integers $(2^r + 1)2^j$, where l is any integer and r is such that $w \in \mathbb{F}_{2gcd(i,n)} \setminus \mathbb{F}_{2gcd(r,i,n)}$.

We knew that, for any vanishing set P, there exists an integer j of 2-weight 2 such that $\sum_{x \in P} (x^{\frac{1}{d}})^j \neq 0$. We can check it here, since for any $w \in \mathbb{F}_{2^{\gcd(i,n)}} \setminus \mathbb{F}_2$, the set of those integers r such that $w \in \mathbb{F}_{2^{\gcd(i,n)}} \setminus \mathbb{F}_{2^{\gcd(r,i,n)}}$ is non-empty. We see that the case of $x^{\frac{1}{d}}$ when d is a quadratic exponent is simpler than the case of x^d itself.

4.3 Some other power functions

As we wrote, we shall study apart in Subsection 6 the case of the multiplicative inverse function $x^{2^{n-2}}$ (equivalently, of the function $x^{2^{n-1}-1}$). Let us study, for 2 < k < n-1, the second-order sum-free min-degree of the power functions $P_k(x) = x^{2^{k-1}}$ (which are shown in [8] to be kth-order sum-free). Note that if $gcd(k,n) \ge 3$, then the restriction of $P_k(x)$ to $\mathbb{F}_{2gcd(k,n)}$ equals $1 + \delta_0(x)$, where δ_0 is the Dirac (or Kronecker) function, taking value 1 at 0 and 0 elsewhere, and P_k does not satisfy the condition of Definition 2, since for every affine plane P in $\mathbb{F}_{2gcd(k,n)}$ not containing 0, we have $P_k((P)) = \emptyset$. We shall then assume that $gcd(k,n) \le 2$. Note that x^{2^k-1} equals identity for k = 1 and is APN for k = 2. We assume then $k \ge 3$. The vanishing flats of P_k are not investigated in [14] nor in the references therein (only their number is studied, for a few values of k). However, the differential spectrum of the functions $x^{2^{k}-1}$ has been studied in [2] and the following has some (very partial) intersection with this paper. The condition that the function $x^{2^{k}-1}$ sums to a nonzero value over an affine plane $\{x, y, z, x + y + z\}$ (with $x, y, z \in \mathbb{F}_{2^n}$ distinct) is $x^{2^{k}-1} + y^{2^k-1} + z^{2^k-1} + (x + y + z)^{2^{k}-1} \neq 0$ and we can reduce ourselves to z = 1. We obtain $x^{2^k-1} + y^{2^k-1} + 1 + (x + y + 1)^{2^k-1} \neq 0$. Hence, if the equation $x^{2^k-1} + y^{2^k-1} + 1 + (x + y + 1)^{2^k-1} = 0$ admits solutions (x, y) such that x and y are distinct and different from 1, we shall have to consider integers j of 2-weight 2 for the corresponding affine planes $\{x, y, z, x + y + z\}$.

• If the affine plane P includes 0 (i.e. is a linear plane), then without loss of generality, we can take x + y + 1 = 0 (x and y being then nonzero and distinct), then the equation above becomes $x^{2^k-1} + (x+1)^{2^k-1} + 1 = 0$. Multiplying by x(x+1) (which is nonzero), we obtain $x^{2^k}(x+1) + x(x^{2^k} + 1) + x(x+1) = 0$, that is, $x^{2^k} + x^2 = 0$, or equivalently $x^{2^{k-1}-1} = 1$, since x cannot be zero because y would then equal 1. We have $gcd(2^{k-1} - 1, 2^n - 1) = 2^l - 1$, where

$$l = \gcd(k - 1, n).$$

If l = 1, then any plane of the form $\{x, x + 1, 1, 0\}$, or more generally of the form $P = z \cdot \{x, x + 1, 1, 0\}$, where $x \in \mathbb{F}_{2^n} \setminus \mathbb{F}_2$, is non-vanishing, and if l > 1, then P is a vanishing flat (that we need to consider when we take j of 2-weight 2) if and only if $x \in \mathbb{F}_{2^l} \setminus \mathbb{F}_2$ (that is, if P is a linear plane in \mathbb{F}_{2^l}). For $j = 2^i + 1$, we have $(zx)^{(2^k-1)j} + (z(x+1))^{(2^k-1)j} + z^{(2^k-1)j} =$ $z^{(2^k-1)j}((x^{2^k-1})^{2^i+1} + ((x+1)^{2^k-1})^{2^i+1} + 1)$. Since $x \in \mathbb{F}_{2^l} \setminus \mathbb{F}_2$, we have $x^{2^k-1} = x$, and $(x+1)^{2^k-1} = x+1$, and $(x^{2^k-1})^{2^i+1} + ((x+1)^{2^k-1})^{2^i+1} +$ $1 = x^{2^i+1} + (x+1)^{2^i+1} + 1 = x^{2^i} + x$. Hence, $\sum_{x \in P_k((P))} x^{2^i+1}$ is nonzero if and only if $x \in \mathbb{F}_{2^l} \setminus \mathbb{F}_{2^{\text{gcd}(i,l)}}$. Hence, given a linear vanishing flat $P = \{0, 1, x, x + 1\}$ of P_k (included in \mathbb{F}_{2^l}), the integers j of 2-weight 2 such that $\sum_{x \in P_k((P))} x^j \neq 0$ are the integers of the form $2^r(2^i+1)$ such that $x \in \mathbb{F}_{2^l} \setminus \mathbb{F}_{2^{\text{gcd}(i,l)}}$ (and we have, as we knew in advance, that there exist such j, since we can take for instance i co-prime with l).

• If P does not include 0, then we have $x, y, x + y + 1 \neq 0$. Multiplying the equation $x^{2^k-1} + y^{2^k-1} + 1 + (x + y + 1)^{2^k-1} = 0$ by x + y + 1 gives $x^{2^k-1}y + x^{2^k-1} + xy^{2^k-1} + y^{2^k-1} + x + y = 0$, that is, $\frac{x^{2^k-1}+1}{x+1} = \frac{y^{2^k-1}+1}{y+1}$. Hence, an affine plane $z \cdot \{x, y, 1, x + y + 1\}$ with x, y nonzero, x, y, 1 distinct and $x + y + 1 \neq 0$, is a vanishing flat of x^{2^k-1} if and only if x, y belong to the same pre-image by the function $x \in \mathbb{F}_{2^n} \setminus \{1\} \mapsto \frac{x^{2^k-1}+1}{x+1}$, and we need to determine what are the pre-images (which are vector spaces containing 1, deprived of 0 and 1) that contain at least two elements x, y that are distinct and such that $x + y + 1 \neq 0$ (note that $\frac{x^{2^k-1}+1}{x+1} = \frac{x^{2^k}+x}{x^2+x}$ has its value

unchanged when we replace x by x + 1, so we need pre-images of size at least 4, which are then vector spaces (since the equation $x^{2^k} + x = \lambda(x^2 + x)$ is linear homogeneous) of dimension at least 3, deprived of 0 and 1). For instance, the pre-image of 0 equals $\mathbb{F}_{2^r} \setminus \mathbb{F}_2$ where $r = \gcd(k, n) = 1$, which leads to a vanishing flat if $r \ge 3$. The pre-image of 1 equals $\mathbb{F}_{2^r} \setminus \{1\}$ where $r = \gcd(k - 1, n) = 1$, which leads to a vanishing flat if $r \ge 3$. Note that, since 0 belongs to this pre-image, then up to a permutation among the elements of the plane, this case and the case x + y + 1 = 0 have an intersection.

We leave open the determination of all the vanishing flats P of $x^{2^{k}-1}$ and, for each of them, of the values of j whose 2-weight is minimum such that $x^{j(2^{k}-1)}$ sums to a nonzero value over P. Some particular values of k, such as those studied in [2], may be simpler to study than others.

5 Some general results on power functions

An (n, n)-function $F(x) = x^d$, where $x \in \mathbb{F}_{2^n}$ and $d \in \mathbb{Z}/(2^n - 1)\mathbb{Z}$, is kth-order tdegree-sum-free if and only if, for every k-dimensional affine space A, there exists a non-negative integer j of 2-weight at most t, such that $\sum_{x \in A} x^{dj} \neq 0$. We shall see that the study of the kth-order sum-free min-degree of power functions x^l , where l is a multiple of d, gives an information on that of x^d . This is quite positive, but a determination of the kth-order sum-free min-degree of all power functions seems elusive, even for k = 2 (for which this determination includes as a very partial sub-problem the determination of all APN power functions, which is currently only in the state of a conjecture). Note also that Lemma 4 does not generalize to vanishing k-flats for k > 2.

5.1 The influence of the *k*th-order sum-free min-degree of "multiples"

Proposition 8 Let $d \in \mathbb{Z}/(2^n - 1)\mathbb{Z}$ and let l be a nonzero multiple of d in $\mathbb{Z}/(2^n - 1)\mathbb{Z}$:

$$0 \not\equiv l \equiv dr \pmod{2^n - 1}$$

If the power function x^l is kth-order t-degree-sum-free for some k and t (i.e. if the kth-order sum-free min-degree of x^l is at most t), then $F(x) = x^d$ is kth-order $(w_2(r)t)$ -degree-sum-free (i.e. its kth-order sum-free min-degree is at most $w_2(r)t$).

Moreover, if r is invertible in $\mathbb{Z}/(2^n - 1)\mathbb{Z}$ and r' is its inverse, then F(x) is kth-order $\left(n - 1 - \left\lfloor \frac{n-1-t}{w_2(r')} \right\rfloor\right)$ -degree-sum-free.

Proof. Let A be any k-dimensional vector subspace of \mathbb{F}_{2^n} and j a non-negative integer of 2-weight at most t such that $\sum_{x \in A} x^{lj} \neq 0$. Then we have $\sum_{x \in A} x^{drj} \neq 0$ and since we have $w_2(rj) \leq w_2(r) w_2(j)$, this proves the first assertion. When r is invertible, Bound (3) says that $w_2(rj) \leq n-1 - \lfloor \frac{n-1-w_2(j)}{w_2(r')} \rfloor$. This proves

the second assertion.

Remark. Proposition 8 allows to reach a min-degree of 1 (i.e. to have a *t*thorder sum-free function) only when x^r is linear and x^l is *t*th-order sum-free (i.e. t = 1): if we take t > 1, then both bounds in the proposition have values larger than 1, and if t = 1, we have as only possible choice of $w_2(r)$ (for the first bound) the value 1 and this is also the case for the value of $w_2(r')$ (for the second bound).

Remark. This result extends of course to any (n, m)-function F such that, for some positive integer r, the function $(F(x))^r$ is kth-order t-degree-sum-free for some k and t.

5.2 An upper bound on the *k*th-order sum-free min-degree of any power permutation

We deduce now from Proposition 8 an improvement for power permutations (in some cases) of the upper bound $\min(k, m)$ on the kth-order sum-free min-degree.

Proposition 9 Let n, k be positive integers such that $k \leq n-1$. Let $F(x) = x^d$ be any power permutation over \mathbb{F}_{2^n} . Let d' be the inverse of d modulo $2^n - 1$, $r = d'(2^k - 1) \pmod{2^n - 1}$. Let r' equal the inverse of r in $\mathbb{Z}/(2^n - 1)\mathbb{Z}$ if gcd(k, n) = 1, and equal to $2^n - 1$ otherwise. Then F is kth-order w-degree-sum-free (i.e. its kth-order sum-free min-degree is at most w) where:

$$w = \min\left(w_2(r), n-1 - \left\lfloor \frac{n-2}{w_2(r')} \right\rfloor\right).$$

Proof. We know from [8] that the power function x^{2^k-1} is kth-order sumfree, that is, kth-order 1-degree sum-free and we have: $d(d'(2^k-1)) \equiv 2^k - 1$ (mod $2^n - 1$). Proposition 8 with $l = 2^k - 1$ and t = 1 completes the proof. \Box

There are many cases where w < k. For instance, when gcd(k, n) = 1 and $d' = \frac{l}{2^k - 1}$ (i.e. $d = \frac{2^k - 1}{l}$), where l is co-prime with n and has 2-weight strictly smaller than k, we have $w_2(d'(2^k - 1)) < k$.

5.3 A generalization

The existence of any class of kth-order sum-free power functions, other than x^{2^k-1} , would give another upper bound similar to that of Proposition 9. The only change (up to a multiplication by a power of 2) on the exponent $2^k - 1 = \sum_{i=0}^{k-1} 2^i$ which seems to preserve the kth-order sum-freedom of the power function x^{2^k-1} is replacing its exponent by $\sum_{i=0}^{k-1} 2^{ij} = \frac{2^{kj}-1}{2^j-1}$ for some j co-prime with n. This corresponds to changing the Frobenius $x \mapsto x^2$ into another generator of the Galois group, its power $x \mapsto x^{2^j}$. The kth-order sum-freedom of the

resulting power function comes from the fact recalled in [8] that, if L_0, \ldots, L_{k-1} are linear, then for every a_1, \ldots, a_k in \mathbb{F}_{2^n} , we have $D_{a_1} \ldots D_{a_k} \left(\prod_{i=0}^{k-1} L_i \right) (x) = \sum_{\sigma \in G_k} \prod_{i=1}^k L_{\sigma(i)}(a_i)$, where G_k is the set of bijections from $\{1, \ldots, k\}$ to $\{0, \ldots, k-1\}$, and we obtain another so-called Moore exponent set (see [1, Bottom of page 2]). Applying Proposition 8 with $l = \frac{2^{kj}-1}{2^{j}-1}$, we have $r = d'(\sum_{i=0}^{k-1} 2^{ij})$, which may have another 2-weight than $d'(2^k - 1)$. The next proposition generalizes Proposition 9.

Proposition 10 Let n, k be positive integers such that $k \leq n-1$. Let $F(x) = x^d$ be any power permutation over \mathbb{F}_{2^n} . Let j be any positive integer co-prime with n. Let d' be the inverse of d modulo $2^n - 1$, $r = d'(\sum_{i=0}^{k-1} 2^{ij}) \pmod{2^n - 1}$ and if $gcd(\sum_{i=0}^{k-1} 2^{ij}, 2^n - 1) = 1$, let r' the inverse of r in $\mathbb{Z}/(2^n - 1)\mathbb{Z}$, and otherwise $r' = 2^n - 1$. Then F is kth-order w-degree-sum-free where:

$$w = \min\left(w_2(r), n-1 - \left\lfloor \frac{n-2}{w_2(r')} \right\rfloor\right).$$

Remark. Note that for n odd, we can also apply Proposition 8 with l = -1 when k = 2 (because the multiplicative inverse function is second-order 1-degree-sum-free, since it is APN) or k = n - 2 (because the multiplicative inverse function is (n - 2)th-order 1-degree-sum-free, being (n - 2)th-order sum-free, see [9]). This gives that any power permutation $F(x) = x^d$ in odd dimension n is second-order t-degree-sum-free and (n - 2)th-order t-degree-sum-free, where t equals the 2-weight of $r = -d' \in \mathbb{Z}/(2^n - 1)\mathbb{Z}$.

For $3 \le k \le n-3$, there does not seem to exist other infinite classes of kth-order sum-free power functions (to be used in conjunction with Proposition 8) than those used in Proposition 10, see [1, Theorem 1.1].

6 The case of multiplicative inverse function

The multiplicative inverse function

$$F_{inv}(x) = x^{2^n - 2}, \quad x \in \mathbb{F}_{2^n},$$

is, as we recalled above, second-order 1-degree-sum-free (i.e. APN) if and only if $n \ge 3$ is odd. Let us address the case of n even.

Proposition 11 Let n be an even integer such that $n \ge 4$. The multiplicative inverse function $F_{inv}(x) = x^{2^n-2}, x \in \mathbb{F}_{2^n}$, is 2nd-order 2-sum-free.

Proof. We know from [8] that for every affine space A that is not a vector space (i.e. which does not include the zero vector), we have $\sum_{x \in A} F(x) \neq 0$. In the case of a 2-dimensional vector space, that is, $A = \{0, a, b, a + b\}$ with a and b linearly independent over \mathbb{F}_2 , we have $\frac{1}{a} + \frac{1}{b} + \frac{1}{a+b} = \frac{a^2+b^2+ab}{ab(a+b)} = \frac{a\left((\frac{b}{a})^2 + \frac{b}{a} + 1\right)}{b(a+b)}$. As already observed in [14], the only affine planes over which the inverse function sums to 0 are then the vector spaces of the form $a \mathbb{F}_4$, since the equation

 $1 + x^2 + x = 0$ has for solutions the two primitive elements of \mathbb{F}_4 . Over such plane, the cube function x^3 sums to a nonzero value, and since the cube function is quadratic, F_{inv} is 2nd-order 2-sum-free.

On the basis of computer investigations, we conjecture in [9] that, for every $k \in \{3, \ldots, n-3\}$ and every $n \ge 6$, the inverse function is not kth-order 2-degree-sum-free (see also [10]). It is then useful to study the values of t for which it is kth-order t-degree-sum-free.

We saw that Corollaries 1 and 2 do not allow to prove this conjecture, even partially.

6.1 A general upper bound on the *k*th-order sum-free mindegree for $k \ge 2$

Since F_{inv} has an algebraic degree of n - 1, Relation (1) does not give any information, but we have:

Proposition 12 For every $2 \le k \le n$, the multiplicative inverse (n, n)-function is kth-order t-degree-sum-free with $t = \min\left(n-k, n-1-\left\lfloor\frac{n-2}{n-k'}\right\rfloor\right)$, where k' equals the inverse of k modulo n if gcd(k, n) = 1 and equals 0 otherwise.

Proof. We apply Proposition 9 with $d' = 2^n - 2$ and $r = (2^n - 2)(2^k - 1) \pmod{2^n - 1} = 2^n - 2^k \pmod{2^n - 1}$. We have:

- $w_2(r) = n k$,
- if gcd(k,n) = 1, then let k' be the inverse of k modulo n, the inverse of $2^k 1$ modulo $2^n 1$ equals $2^{k(k'-1)} + 2^{k(k'-2)} + \dots + 2^k + 1$, since $(2^k 1)(2^{k(k'-1)} + 2^{k(k'-2)} + \dots + 2^k + 1) = 2^{kk'} 1 \equiv 1 \pmod{2^n 1}$. The inverse r' of the opposite $2^n 2^k$ of $2^k 1$ modulo $2^n 1$ equals then $(2^n 1) (2^{k(k'-1)} + 2^{k(k'-2)} + \dots + 2^k + 1)$ and has 2-weight n k'. Then, $n 1 \lfloor \frac{n-2}{w_2(r')} \rfloor$ equals $n 1 \lfloor \frac{n-2}{n-k'} \rfloor$.

This completes the proof.

The bound $t \leq n-k$ in Proposition 12 gives an information when n-k < k, that is, $k > \frac{n}{2}$. For $k < \frac{n}{2}$, we will have a result thanks to Corollary 2 below. We have $n-1 - \left\lfloor \frac{n-2}{n-k'} \right\rfloor < n-k$ when $\left\lfloor \frac{n-2}{n-k'} \right\rfloor \geq k$, that is, $n-2 \geq k(n-k')$ (which can happen, when k is not too large and k' is not too small).

Note that for k = n - 2, we obtain t = 2 (since $n - 2 \ge k(n - k')$ is impossible), which is the correct value if we do not distinguish the parity of n, since we have, thanks to Corollary 4 below and Proposition 11 above, that F_{inv} is (n - 2)thorder 2-degree sum-free for n even and (n - 2)th-order 1-degree sum-free for nodd.

6.2 Relation with subspace polynomials and consequences

Subspace polynomials (see below) play an important role with respect to the kth-order (regular) sum-freedom of the inverse function (see [8, 9]). In the present subsection, we use a different approach for revisiting this role, and we deduce that the property that the kth-order sum-freedom of the multiplicative inverse function is equivalent to its (n - k)th-order sum-freedom extends to the kth-order sum-free min-degree.

We also deduce another similarity between the sum-freedom of the inverse function and its sum-free min-degree: when we studied its sum-freedom, we observed a difference between the sums $\sum_{x \in A} F_{inv}(x)$ when A is a vector subspace of \mathbb{F}_2^n , and when it is another affine subspace. We will see this is also the case for the sums $\sum_{x \in A} (F_{inv}(x))^j$ when considering the kth-order sum-free min-degree.

Subspace polynomials Let E_k be a k-dimensional vector space and let $L_{E_k}(x) = \prod_{u \in E_k} (x+u)$. Such a polynomial is called a subspace polynomial. It is a linearized polynomial and we write then $L_{E_k}(x) = \sum_{i=0}^k b_{k,i} x^{2^i}$ ($b_{k,0} \neq 0$, $b_{k,k} = 1$); see more in [9].

Consequence on the sums $\sum_{x \in E_k \setminus \{0\}} x^{-j}$: Since for every $x \in E_k$, we have $x = \frac{1}{b_{k,0}} \sum_{i=1}^k b_{k,i} x^{2^i}$, we have for every nonzero $x \in E_k$ and every non-negative integer j, by dividing this equality by x^{j+1} , that $x^{-j} = \frac{1}{b_{k,0}} \sum_{i=1}^k b_{k,i} x^{2^i - 1 - j}$. We deduce that:

$$\sum_{x \in E_k \setminus \{0\}} x^{-j} = \frac{1}{b_{k,0}} \sum_{i=1}^{\kappa} b_{k,i} \Big(\sum_{x \in E_k \setminus \{0\}} x^{2^i - 1 - j} \Big).$$

з

Hence, since for every (n, n)-function F of algebraic degree less than k, we have $\sum_{x \in E_k} F(x) = 0$ and we also have $\sum_{x \in E_k \setminus \{0\}} x^0 = 1$, we deduce:

Lemma 9 Let n and k be any positive integers such that $k \leq n$ and let E_k be any k-dimensional vector space and $L_{E_k}(x) = \prod_{u \in E_k} (x+u) = \sum_{i=0}^k b_{k,i} x^{2^i}$. Let

 $r = \min\{i; 1 \le i \le k \text{ and } b_{k,i} \ne 0\}.$

Then $\sum_{x \in E_k \setminus \{0\}} x^{-j}$ equals 0 for every $1 \leq j < 2^r - 1$ and is nonzero for $j = 2^r - 1$.

This result extends results from [8, 9] (which say, taking j = 1, that $\sum_{x \in E_k \setminus \{0\}} x^{-1}$ equals 0 if r > 1 and is nonzero if r = 1.).

Consequence on the sums $\sum_{x \in E_k \setminus \{0\}} (x+a)^{-j}$; $a \notin E_k$: Let $A_k = a + E_k$ be a k-dimensional affine space not containing 0. Since we know from [8] that $\sum_{x \in A_k} x^{-1} \neq 0$, we have that j = 1 is such that $\sum_{x \in A_k} x^{-j} \neq 0$ and we do not need to consider larger values of j. By curiosity, let us however show how the method used above for vector spaces can be adapted to find again this result.

We have $A_k = L_{E_k}^{-1}(b)$ for some nonzero $b = L_{E_k}(a)$. Then, for every $x \in A_k$, we have $b = \sum_{i=0}^{k} b_{k,i} x^{2^i}$ and then $\sum_{x \in A_k} x^{-j} = \frac{1}{b} \sum_{i=0}^{k} \left(b_{k,i} \sum_{x \in A_k} x^{2^{i-j}} \right)$. We find for j = 1 that since $\sum_{x \in A_k} x^{2^{i-1}}$ equals 0 for i < k (since $x^{2^{i-1}}$ has an algebraic degree of i) and is nonzero for i = k (since $\sum_{x \in A_k} x^{2^{k-1}}$ equals the value at x of a kth-order derivative of the function $x^{2^{k-1}}$ and we know from [8] that this constant derivative is nonzero). This provides a different way of proving the known result from [8].

We deduce from the observations above (and from the fact that $j = 2^r - 1$ has a 2-weight of r):

Proposition 13 Let n and k be positive integers such that $k \leq n$. The kthorder sum-free min-degree of the multiplicative inverse function F_{inv} over \mathbb{F}_{2^n} equals the minimum positive integer such that, for every k-dimensional vector subspace E_k of \mathbb{F}_{2^n} , denoting $L_{E_k}(x) = \prod_{u \in E_k} (x+u) = \sum_{i=0}^k b_{k,i} x^{2^i}$, we have $t \geq \min\{i; 1 \leq i \leq k \text{ and } b_{k,i} \neq 0\}.$

A case where we know that F_{inv} is not kth-order sum-free is when k divides n, since $\sum_{x \in \mathbb{F}_{2^k}} x^{-1}$ equals 0, and the next step is determining the kth-order sum-free min-degree of F_{inv} in such a case.

Corollary 3 If k divides n, then the kth-order sum-free min-degree of the multiplicative inverse function F_{inv} over \mathbb{F}_{2^n} equals k.

Indeed, for $E_k = \mathbb{F}_{2^k}$, we have $L_{E_k}(x) = x^{2^k} + x$. Hence, according to Proposition 13, the *k*th-order sum-free min-degree is at least *k*, and according to Proposition 3, it equals then *k*.

We can see that the bound of Proposition 3 is tight, at least for m = n.

A more general case where we know that F_{inv} is not kth-order sum-free is when $\gcd(k,n) > 1$, see [9]. In such a case, we have $L_{\mathbb{F}_{2gcd}(k,n)}(x) = x^{2^{gcd}(k,n)} + x$, and according to Lemma 9, we have then that $\sum_{x \in \mathbb{F}_{2gcd}(k,n)} x^{-j}$ equals 0 when $j < 2^{gcd(k,n)} - 1$ and is nonzero when $j = 2^{gcd(k,n)} - 1$. If E_k is a $\frac{k}{gcd(k,n)}$ dimensional vector subspace of \mathbb{F}_{2^n} over $\mathbb{F}_{2gcd(k,n)}$, then E_k equals the disjoint union of multiplicative cosets $w\mathbb{F}_{2gcd(k,n)}^*$ where w ranges over a basis S of E_k over $\mathbb{F}_{2gcd(k,n)}$, and we have then that $\sum_{x \in E_k} x^{-j} = (\sum_{w \in S} w^{-j})(\sum_{x \in \mathbb{F}_{2gcd(k,n)}^*} x^{-j})$ equals 0 if and only if $\sum_{w \in S} w^{-j} = 0$ or $\sum_{x \in \mathbb{F}_{2gcd(k,n)}^*} x^{-j} = 0$. Hence the kthorder sum-free min-degree of F_{inv} is larger than or equal to $\gcd(k, n)$. It seems difficult to determine in which cases it equals $\gcd(k, n)$ and in which cases it is larger.

The next corollary generalizes to the sum-free min-degree the equality, proved in [9], between the kth-order sum-freedom of the inverse function and its (n - k)th-order sum-freedom.

Corollary 4 For any $n \ge 2$ and any $k \in \{2, ..., n-2\}$, the kth-order sum-free min-degree of the multiplicative inverse (n, n)-function equals its (n-k)th-order sum-free min-degree.

Proof. It is recalled in [9] that if E_k is any k-dimensional vector subspace of \mathbb{F}_{2^n} and $E_{n-k} = L_{E_k}(\mathbb{F}_{2^n})$ then E_{n-k} has dimension n-k and we have the following relation in $\mathbb{F}_{2^n}[x]$:

$$L_{E_{n-k}} \circ L_{E_k}(x) = L_{E_k} \circ L_{E_{n-k}}(x) = x^{2^n} + x.$$

Writing $L_{E_k}(x) = \sum_{i=0}^{k} b_{k,i} x^{2^i}$ and $L_{E_{n-k}}(x) = \sum_{i=0}^{n-k} b_{n-k,i} x^{2^i}$, we have $L_{E_{n-k}} \circ L_{E_k}(x) = \sum_{i=0}^{n-k} \sum_{j=0}^{k} b_{n-k,i} (b_{k,j})^{2^i} x^{2^{i+j}}$. We have then, by considering the coefficient of x^{2^r} :

$$\forall r \in \{1, \dots, n-1\}, \quad \sum_{i=0}^{r} b_{n-k,i} (b_{k,r-i})^{2^{i}} = 0.$$
 (9)

We know from Proposition 13 that, if t is the kth-order sum-free min-degree of the inverse function, then $b_{k,0}$ and $b_{k,t}$ are nonzero and $b_{k,1} = \cdots = b_{k,t-1} = 0$. The relations corresponding to Relation (9) for $r = 1, \ldots, t-1$ imply $b_{n-k,1} = \cdots = b_{n-k,t-1} = 0$ and the tth relation implies $b_{n-k,t} \neq 0$. Proposition 13 completes the proof.

Corollary 4 and Proposition 12 give:

Corollary 5 For every $2 \le k \le n$, the multiplicative inverse (n, n)-function is kth-order t-degree-sum-free with $t = \min\left(k, n-k, n-1-\lfloor \frac{n-2}{n-k'} \rfloor, n-1-\lfloor \frac{n-2}{k'} \rfloor\right)$, where k' equals the inverse of k modulo n (and n - k' is the inverse of n - k modulo n) if gcd(k, n) = 1 and equals 0 (resp. n) otherwise.

Remark. The kth-order sum-free min-degree of F_{inv} is then at most $t = \min\left(k, n-k, n-1 - \lfloor \frac{n-2}{n-k'} \rfloor, n-1 - \lfloor \frac{n-2}{k'} \rfloor\right)$. For $k \leq \frac{n}{2}$, we have often t = k and we do not get then more information than with Proposition 3. But for $k > \frac{n}{2}$, the bound of Corollary 5 is strictly better than that of Proposition 3. We do not know whether the kth-order sum-free min-degree of F_{inv} is always strictly larger than 1 for $k \in [3, n-3]$, but we conjecture it. Determining the exact kth-order sum-free min-degree of F_{inv} seems challenging.

Conclusion

We have introduced a notion on vectorial functions extending that of sumfreedom (which itself extended the notion of almost perfect nonlinearity).

This has led to the parameter that we called kth-order sum-free min-degree, which quantifies to which extent an S-box F prevents from the propagation of the division property of k-dimensional affine spaces, in the framework of an integral attack. We proved that all the vectorial (n, m)-functions such that, for every k-dimensional affine space A, the set $F((A)) = \{y \in \mathbb{F}_2^m; A \cap F^{-1}(y) \text{ has an odd size}\}$ is non-empty (in particular, all injective vectorial functions), have a kth-order sum-free min-degree smaller than or equal to $\min(k, m)$. We could also prove several lower bounds on the kth-order sum-free min-degree of vectorial functions.

We leave open the determination, for every $k \in \{3, \ldots, n-1\}$, of the vectorial functions having the property that F((A)) is non-empty for every k-dimensional affine space A. We identified an infinite class of (non-necessarily-bijective) (m, m)-functions satisfying this property for every even k, which includes all APN power functions.

A vectorial function is kth-order sum-free if and only if its kth-order sum-free min-degree equals 1. Functions being kth-order sum-free seem rare, and the weakening of this notion, by considering the functions whose kth-order sum-free min-degree can equal a larger value (not too large, in order to preserve the non-propagation of the division property of k-dimensional vector spaces), nicely extends the corpus to be studied. But determining the kth-order sum-free min-degree of vectorial functions seems quite difficult.

We could prove several upper bounds specific to the case of power functions.

We leave open the determination of the kth-order sum-free min-degree t of the multiplicative inverse function for $k \in \{3, ..., n-3\}$, and more generally of all the functions x^{2^r-1} for $k \in \{2, ..., n-2\} \setminus \{r\}$, and of all other cryptographically interesting functions.

The precise determination, for a given non-APN function F, of those positive integers j of 2-weight 2, such that $(F(x))^j$ sums to a non-zero value over a generic non-vanishing flat is also left open, even for the (seemingly simpler) cases of quadratic power functions and of functions of the form x^{2^k-1} . We could determine them for the compositional inverses of quadratic power permutations.

Finally, we could show, thanks to a simple and general characterization by subspace polynomials of the kth-order sum-free min-degree of the multiplicative inverse function, that it equals k when k divides n and that, in general, it equals its (n - k)th-order sum-free min-degree, thus extending a result on its kth-order sum-freedom.

Acknowledgement We thank Stjepan Picek for his kind help with a computer investigation.

References

- D. Bartoli and Y. Zhou. Asymptotics of Moore exponent sets. Journal of Combinatorial Theory, Series A 175, p.105281, 2020.
- [2] C. Blondeau, A. Canteaut and P. Charpin. Differential Properties of $x \mapsto x^{2^t-1}$. *IEEE Transactions on Information Theory* 57 (12), pp. 8127-8137, 2011.

- [3] C. Boura and A. Canteaut. On the Influence of the Algebraic Degree of F^{-1} on the Algebraic Degree of $G \circ F$. *IEEE Transactions on Information Theory* 59 (1), pp. 691-702, 2013.
- [4] C. Boura and A. Canteaut. Another view of the division property. Proceedings of CRYPTO 2016, Part I. Lecture Notes in Computer Science 9814 pp. 654-682, 2016.
- [5] 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. See also https://hal.inria.fr/inria-00072221/document
- [6] C. Carlet. Graph indicators of vectorial functions and bounds on the algebraic degree of composite functions. *IEEE Transactions on Information Theory* 66 (12), pp. 7702-7716, 2020.
- [7] C. Carlet. Boolean Functions for Cryptography and Coding Theory. Monograph in *Cambridge University Press*, 562 pages, 2021.
- [8] C. Carlet. Two generalizations of almost perfect nonlinearity. To appear in the *Journal of Cryptology* (Topical Collection on Advances in Boolean Functions with Applications in Cryptography). Available at Cryptology ePrint Archive 2024/841
- [9] C. Carlet. On the vector subspaces of \mathbb{F}_{2^n} over which the multiplicative inverse function sums to zero. To appear in *Designs, Codes and Cryptography*, special issue in memory of Kai-Uwe Schmidt. Available at Cryptology ePrint Archive 2024/1007.
- [10] C. Carlet and X.-D. Hou. More on the sum-freedom of the multiplicative inverse function. Preprint, 2024.
- [11] K.H Kim, J.H. Choe, and S. Mesnager. Complete solution over \mathbb{F}_{p^n} of the equation $X^{p^k+1} + X + a = 0$. Finite Fields and Their Applications, 76, p.101902.
- [12] P. Hebborn, G. Leander, and A. Udovenko. Mathematical aspects of division property. *Cryptography and Communications* 15, no. 4, pp. 731-774, 2023.
- [13] L. Knudsen and D. Wagner. Integral cryptanalysis. Proceedings of Fast Software Encryption FSE 2002, Lecture Notes in Computer Science vol. 2365, pp. 112127, 2002.
- [14] S. Li, W. Meidl, A. Polujan, A. Pott, C. Riera, and P. Stănică. Vanishing flats: A combinatorial viewpoint on the planarity of functions and their application. *IEEE Transactions on Information Theory* 66 (11), pp.7101-7112, 2020.

- [15] F. J. MacWilliams and N. J. Sloane. The theory of error-correcting codes, North Holland. 1977.
- [16] G. Kyureghyan and V. Suder. On inversion in \mathbb{Z}_{2^n-1} . Finite Fields and Their Applications 25, pp. 234-254, 2014.
- [17] K. Nyberg. Differentially uniform mappings for cryptography. Proceedings of EUROCRYPT 1993, Lecture Notes in Computer Science 765, pp. 55-64, 1994.
- [18] Y. Todo. Structural evaluation by generalized integral property. Proceedings of EUROCRYPT 2015, Lecture Notes in Computer Science 9056, pp. 287-314, 2015.