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 kth-order 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 kth-order sum-freedom when $t = 1$. The condition for kth-order t-degree-sum-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 study examples for $k = 2$ (case in which $t = 1$ corresponds to APNness) showing that finding j of 2-weight 2 can be challenging, and we begin the study of power functions, and in particular, of the multiplicative inverse function (used as S-box in the AES), for which 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. We begin the study of the cases of $k \in \{2, 3, n - 3, n - 2, n - 1, n\}$.

Keywords: vectorial function, S-box, almost perfect nonlinear, kth-order sum-free, integral attack, division property.

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

1 Introduction

A (vectorial) (n,m)-function $F : \mathbb{F}_2^n \to \mathbb{F}_2^m$ is called kth-order sum-free [4] 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 $D_{a_1} \dots D_{a_k} F(x)$ 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 [8]. Todo [11] has introduced, in the framework of these cryptanalyses, the notion of division property of a set, and Boura-Canteaut [2] have translated it into the language of Reed-Muller codes (see a survey in [7]). A set $X \subseteq \mathbb{F}_2^n$ is said to have the *division property* at an order t if its indicator has an algebraic degree at most $n-t$. Integral attacks practically lead to studying the propagation of the division property through rounds, which needs to study it through S-boxes. It is shown in [4] 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 $t \geq 1$, 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 notion is then 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 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 study a little more in detail the case of $k = 2$ (corresponding to APNness) and the case for general k of power functions, and we focus specifically on the multiplicative inverse function (used as S-box in the AES), by showing that it is is kth-order t-degree-sum-free if and only if it is $(n-k)$th-order t-degree-sum-free and by studying the cases of $k \in \{2, 3, n-3, n-2, n-1, n\}$.

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 for instance the finite field $\mathbb{F}_{2^n}$ is an n-dimensional vector space over $\mathbb{F}_2$, and given a basis $(\alpha_1, \ldots, \alpha_n)$, we have the correspondence $(x_1, \ldots, x_n) \mapsto \sum_{i=1}^n x_i \alpha_i$.
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 $\sum_{x \in A} F(x) \neq 0$ [4].
When viewing a vectorial function as defined over $\mathbb{F}_2^n$, we can represent it by its (unique) *algebraic normal form* $F(x) = \sum_{I \subseteq \{1,\ldots,n\}} a_I \prod_{i \in I} x_i$ 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 m divides 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.
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 [2]).

3 A weakening of the sum-freedom notion

To show why sum-freedom can be weakened, let us briefly recall why kth-order sum-freedom avoids the propagation of the division property of k-dimensional affine spaces through the S-box. We first need to say what is the image of a set that needs to 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 [7]):

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

(we use a specific notation to avoid any confusion between $F(X)$ and $F((X))$ when F is not injective). What is shown in [4] 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 now show that this nicely simple notion of sum-freedom is 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 $n-1$ (see more details in [4, Subsection 3.2]). Then no propagation of the division property is possible for k-dimensional affine spaces when F is kth-order sum-free, 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 [2, 7] 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 [2]. 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 $\mathbb{F}_{2^m}$ (by choosing a basis $(\alpha_1, \ldots, \alpha_m)$ of this m-dimensional vector space over $\mathbb{F}_2$, and identifying any vector $(x_1, \ldots, x_m) \in \mathbb{F}_2^m$ with the element $\sum_{i=1}^m x_i \alpha_i$ of the field). We believe this has an interest, since:

- it is in some cases simpler to address the propagation of the division property in fields than in vector spaces,
- in many block ciphers such as the AES, S-boxes are naturally defined and valued in fields,
- most of the important (infinite classes of) vectorial functions for cryptography are defined and valued in fields,
- 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 [10, 3]) that, for every $1 \leq d \leq m$, the dual of the Reed-Muller code of order $d-1$ equals the Reed-Muller code of order $m-d$, 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 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 (taking $d = 0$), for every nonzero m-variable Boolean function f, there exists an m-variable Boolean function g of algebraic degree at most m, such that $\sum_{y\in\mathbb{F}_{2^m}} f(y)g(y) \neq 0$ (note that we can take for g the indicator of a singleton $\{a\}$, where $f(a) = 1$).
Moreover, when the domain of the Boolean function equals $\mathbb{F}_{2^m}$, 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 *[3, Corollary 2] 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 if there exists a non-negative integer j whose 2-weight satisfies $w_2(j) \leq m - d$, and such that $\sum_{y\in\mathbb{F}_{2^m}} y^j f(y) \neq 0$.*

For making the paper self-contained, let us give a proof of this fact (a different proof from that of [3]):

- the functions in the Reed-Muller code of order $m-d$ are the Boolean functions whose univariate representation has the form (see e.g. [3, Relation (2.16)]):

$$\sum_{\substack{j\in\Gamma(m)\\ w_2(j)\leq m-d}} tr_{m_j}(\beta_j y^j), \text{ with } \forall j \in \Gamma(m), \beta_j \in \mathbb{F}_{2^{m_j}},$$

  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 $\mathbb{F}_2$,

- since for every $y \in \mathbb{F}_{2^m}$, we have $y^j \in \mathbb{F}_{2^{m_j}}$, we have $\sum_{y\in\mathbb{F}_{2^m}} y^j f(y) \neq 0$ 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 by taking $d = m-t$ (that is, $m-d = t$) the following proposition, after observing that if f is the indicator of $F((X))$ in $\mathbb{F}_{2^m}$, then we have $\sum_{y\in\mathbb{F}_{2^m}} G(y)f(y) = \sum_{x\in X} G\circ F(x)$ and $\sum_{y\in\mathbb{F}_{2^m}} y^j f(y) = \sum_{x\in X} \big(F(x)\big)^j$:

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 $t+1$ if and only if some non-negative integer j exists such that $w_2(j) \leq t$ and $\sum_{x\in X} \big(F(x)\big)^j \neq 0$, which is equivalent to: some (m, r)-function G (with $r \geq 1$) of algebraic degree at most t exists such that $\sum_{x\in X}(G \circ F)(x) \neq 0$.*

Indeed, $F((X))$ fails to satisfy the division property at the order $l = t + 1$ if its indicator has algebraic degree at least $m - l + 1 = m - t$. 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 non-negative integer j whose 2-weight is at most t and such that $\sum_{x \in A} \big(F(x)\big)^j \neq 0$.*

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 $\sum_{x \in X}(G \circ F)(x) \neq 0$.

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.*

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. $\diamond$

The larger t, the weaker the notion of kth-order t-degree-sum-freedom. The classic kth-order sum-freedom corresponds to $t = 1$. Indeed, a k-dimensional affine space A, with $k \geq 1$, having an even size, the set $F((A))$ has also an even size, and the only possibility for F to be kth-order 1-degree sum-free is then that $\sum_{x \in A}(F(x))^{2^i} = (\sum_{x \in A} F(x))^{2^i} \neq 0$ for some i, that is, $\sum_{x \in A} F(x) \neq 0$.

Of course, if a function is kth-order t-degree-sum-free, then it is kth-order t'-degree-sum-free for every $t' \geq t$.

Let us see now that any (n, m)-function satisfying some some reasonable condition is kth-order t-degree-sum-free for some t, and more precisely, that the value of t can be taken 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 above 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 $\sum_{y \in \mathbb{F}_{2^m}} y^j f(y) = \sum_{x \in A} \big(F(x)\big)^j \neq 0$. The value $t = m$ satisfies then the condition of Definition 1 (note that even if $F((A))$ equals $\{0\}$, in which case we have $\sum_{x \in A}(F(x))^j = 0$ for every positive integer j, we can take $j = 0$ to have $\sum_{x \in A}(F(x))^j \neq 0$; we can more generally do so when $F((A))$ is any singleton). This leads to the following:

Definition 2 *Let n, m be two positive integers and let $2 \leq k \leq n$. 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 degree-sum-free-limit *of F the smallest value of $t \leq m$ such that F is kth-order t-degree-sum-free.*

According to the observations above, the kth-order degree-sum-free-limit of the functions ensuring, for any k-dimensional affine space A, that the set $F((A))$ is non-empty, is an affine invariant parameter, that is, if L and L' are two affine permutations, then the kth-order degree-sum-free-limit of F equals the kth-order degree-sum-free-limit of $L \circ F \circ L'$.

Remark. The condition on F in Definition 2 is necessary, since if it is not satisfied for some A, the kth-order degree-sum-free-limit cannot exist. Take for instance $F(x) = x + x^2$, 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 what are all the functions satisfying this condition.
We leave this as an open problem, but we give an example of an infinite class of non-bijective (m, m)-functions satisfying it: for every positive even integers m and k such that $k \leq m$, we take for F any power (m, m)-functions $F(x) = x^d$ such that $\gcd(d, 2^m - 1) = 3$ (as are all APN power functions over $\mathbb{F}_{2^m}$, see [3, 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 $u \neq 0$. Then if $F((A)) = \emptyset$, 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 vector space E over $\mathbb{F}_2$ underlying S is then stable under the multiplication by w. It is then a vector space over $\mathbb{F}_4$ and its dimension as an $\mathbb{F}_2$-vector space is then even. This proves that if $k - 1$ is odd, then F satisfies the condition of Definition 2.
Note that, since for n odd, all APN power functions are bijective, all APN power functions satisfy the condition in Definition 2. ◇

3.3 An upper bound on the kth-order degree-sum-free-limit

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 degree-sum-free-limit at most k. This is clearly true if $F((A))$ is an affine space, but it is not immediately clear whether it is true in general.

Remark. If $F((A)) = \{0\}$ then we can take $j = 0$ and otherwise, there exists 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? Let us consider F valued in $\mathbb{F}_2^m$; this will simplify our presentation and we know that the two representations of F over $\mathbb{F}_2^m$ and $\mathbb{F}_{2^m}$ are equivalent. Without loss of generality we can then 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. In fact, the question is: the indicator of $F((A))$ has it algebraic degree larger than $m - k$? This is indeed equivalent to the question whether there exists a Boolean function g over $\mathbb{F}_2^m$ such that fg has algebraic degree m. The next proposition clarifies this. ◇

Proposition 3 *Let n, m be two positive integers and let $2 \leq k \leq n$. Let F be any (n, m)-function such that $F((A)) \neq \emptyset$ for every k-dimensional affine space A. Then F has kth-order degree-sum-free-limit at most* $\min(k, m)$.

Proof. Since we know that we can take $t \leq m$, we just have to show that we can take $t \leq k$. For every k-dimensional affine space A, $F((A))$ has size at most 2^k and its indicator f has then algebraic degree at least $m - k$ (indeed, we know, see [10, 3]) 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 (the opposite of) Lemma 2, an integer j of 2-weight at most k such that $\sum_{y\in\mathbb{F}_{2^m}} y^j f(y) = \sum_{x\in A}(F(x))^j \neq 0$. □

3.4 A lower bound on kth-order degree-sum-free-limit

Let us show a lower bound on the value of t. Denoting by $\deg\big(F(x)\big)$ the algebraic degree of function $F(x)$, we have, for every non-negative integer j:

$$\deg\big((F(x))^j\big) \leq w_2(j)\ \deg(F),$$

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 $\deg\big((F(x))^j\big) < k$, 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 sum-free. We have:*

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

Indeed, if $t < \frac{k}{\deg(F)}$ then, for every j such that $w_2(j) \leq t$, we have $\deg\left((F(x))^j\right) \leq \deg(F)\, w_2(j) < k$.
Note that Proposition 4 generalizes the obvious fact that a function of algebraic degree d cannot be kth-order sum-free for $k > d$.

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

In this section, we visit a few examples of (infinite classes of) non-APN permutations, illustrating the upper bound on the kth-order degree-sum-free-limit of Proposition 3.
A non-APN (n,n)-function has what [9] calls *vanishing flats* (which would better be called 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); we shall respect this terminology. To evaluate the second-order degree-sum-free-limit of a given permutation, we need to determine its vanishing flats, and for each of them, visit by increasing 2-weight the integers j until we find one such that $(F(x))^j$ sums to a nonzero value over this vanishing flat. Proposition 3 tells us that this will always happen with 2-weight 2.
The examples below show that determining the vanishing flats of a function F may be easy (then, determining the values of j such that $\sum_{x\in P}(F(x))^j \neq 0$ may be easy or hard), or it may be hard. In the first example, determining the vanishing flats P is easy, and determining the values of j is hard; in the second example, both determinations are rather easy; in the last example, determining the vanishing flats is hard.

4.1 Quadratic power functions

It is easy to determine the vanishing flats of quadratic power functions $F(x)$ (but it is more complex to evaluate the sum of the values taken by $(F(x))^j$ over them).

Lemma 4 *Let n, i be positive integers. Let $F(x) = x^{1+2^i}$. 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 $l = \gcd(i, n)$.*

Proof. The vanishing flats of F are the planes $\{x, y, z, x+y+z\}$ with x, y, z distinct, such that $x^{1+2^i} + y^{1+2^i} + z^{1+2^i} + (x+y+z)^{1+2^i} = 0$, 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 (satisfying then $w^{2^i} = w$) different from 1 in $\mathbb{F}_{2^n}$, which is equivalent to $w \in \mathbb{F}_{2^l} \setminus \mathbb{F}_2$ with

$l = \gcd(i, n)$. □

Let us now see if it is difficult for each such vanishing flat P to determine j such that $\sum_{x \in P} (F(x))^j \neq 0$. Without loss of generality, we take $F(x) = x^d$ where $d = 1 + 2^i$. According to Lemma 4, 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 $l = \gcd(i, n)$. Note that $y+z = w(x+z)$ is equivalent to $z = \frac{wx+y}{w+1}$, and we have then $z^d = \left(\frac{wx+y}{w+1}\right)^{1+2^i} = \frac{(wx+y)(w^{2^i}x^{2^i}+y^{2^i})}{(w+1)(w+1)^{2^i}} = \frac{(wx+y)(wx^{2^i}+y^{2^i})}{w^2+1} = \frac{w^2x^d+wxy^{2^i}+wx^{2^i}y+y^d}{w^2+1}$ and $(x + y + z)^d = \frac{\left((w+1)(x+y)+wx+y\right)^d}{w^2+1} = \frac{(x+wy)^d}{w^2+1} = \frac{x^d+wxy^{2^i}+wx^{2^i}y+w^2y^d}{w^2+1}$. Let us now consider a positive integer j of 2-weight 2. Without loss of generality, we take $j = 1 + 2^r$. We want to evaluate:

$$x^{dj} + y^{dj} + \left(\frac{w^2x^d + wxy^{2^i} + wx^{2^i}y + y^d}{w^2 + 1}\right)^j + \left(\frac{x^d + wxy^{2^i} + wx^{2^i}y + w^2y^d}{w^2 + 1}\right)^j =$$

$$x^{dj} + y^{dj} + \frac{A}{(w^2 + 1)^j},$$

where $A = (w^2x^d+wxy^{2^i}+wx^{2^i}y+y^d)(w^{2^{r+1}}x^{d2^r}+w^{2^r}x^{2^r}y^{2^{i+r}}+w^{2^r}x^{2^{i+r}}y^{2^r}+y^{d2^r})+(x^d+wxy^{2^i}+wx^{2^i}y+w^2y^d)(x^{d2^r}+w^{2^r}x^{2^r}y^{2^{i+r}}+w^{2^r}x^{2^{i+r}}y^{2^r}+w^{2^{r+1}}y^{d2^r})$, that is, $A = w^{2^{r+1}+2}x^{dj} + w^{2^r+2}x^{d+2^r}y^{2^{i+r}} + w^{2^r+2}x^{d+2^{i+r}}y^{2^r} + w^2x^dy^{d2^r} + w^{2^{r+1}+1}x^{d2^r+1}y^{2^i} + w^{2^r+1}x^{2^r+1}y^{2^{i+r}+2^i} + w^{2^r+1}x^{2^{i+r}+1}y^{2^r+2^i} + wxy^{d2^r+2^i} + w^{2^{r+1}+1}x^{d2^r+2^i}y + w^{2^r+1}x^{2^r+2^i}y^{2^{i+r}+1} + w^{2^r+1}x^{2^{i+r}+2^i}y^{2^r+1} + wx^{2^i}y^{d2^r+1} + w^{2^{r+1}}x^{d2^r}y^d + w^{2^r}x^{2^r}y^{2^{i+r}+d} + w^{2^r}x^{2^{i+r}}y^{2^r+d} + y^{dj} + x^{dj} + w^{2^r}x^{2^r+d}y^{2^{i+r}} + w^{2^r}x^{2^{i+r}+d}y^{2^r} + w^{2^{r+1}}x^dy^{d2^r} + wx^{d2^r+1}y^{2^i} + w^{2^r+1}x^{2^r+1}y^{2^{i+r}+2^i} + w^{2^r+1}x^{2^{i+r}+1}y^{2^r+2^i} + w^{2^{r+1}+1}xy^{d2^r} + wx^{d2^r+2^i}y + w^{2^r+1}x^{2^r+2^i}y^{2^{i+r}+1} + w^{2^r+1}x^{2^{i+r}+2^i}y^{2^r+1} + w^{2^{r+1}+1}x^{2^i}y^{d2^r} + w^2x^{d2^r}y^d + w^{2^r+2}x^{2^r}y^{2^{i+r}+d} + w^{2^r+2}x^{2^{i+r}}y^{2^r+d} + w^{2^{r+1}+2}y^{dj} =$
$(w^{2j} + 1)x^{dj} + (w^{j+1} + w^{j-1})x^{d+2^r}y^{2^{i+r}} + (w^{j+1} + w^{j-1})x^{d+2^{i+r}}y^{2^r} + (w^2 + w^{2j-2})x^dy^{d2^r} + (w^{2j-1} + w)x^{d2^r+1}y^{2^i} + (w^j + w^{2j-1})x^jy^{2^ij} + wxy^{2^i+d2^r} + (w^{2j-1} + w)x^{2^i+d2^r}y + (w^j + w^{2j-1})x^{2^i+2^r}y^{2^{i+r}+1} + wx^{2^i}y^{d2^r+1} + (w^{2j-1} + w^2)x^{d2^r}y^d + (w^{j-1}+w^{j+1})x^{2^r}y^{d+2^{i+r}} + (w^{j-1}+w^{j+1})x^{2^{i+r}}y^{d+2^r} + y^{dj} + w^{2j-1}xy^{d2^r} + w^{2^{r+1}+1}x^{2^i}y^{d2^r} + w^{2j}y^{dj}$.
According to Proposition 3, we know that j of 2-weight 2 exists such that this expression is nonzero, but determining such j seems hard.

4.2 Inverses of quadratic power permutations: an example

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. It is indeed shown in [9] that if two functions are CCZ-equivalent, then their vanishing flats correspond to each others. Let us detail what happens with a permutation F and its compositional inverse F^{-1}, since we will need such details below. Let $\{x, y, z, x + y + z\}$ be a vanishing flat

of F. We have by hypothesis $F(x)+F(y)+F(z)+F(x+y+z)=0$. This equality can be written in the form $x+y+z=F^{-1}\big(F(x)+F(y)+F(z)\big)$, that is, $F^{-1}(F(x))+F^{-1}(F(y))+F^{-1}(F(z))+F^{-1}\big(F(x)+F(y)+F(z)\big)=0$. Hence if $\{x,y,z,x+y+z\}$ is a vanishing flat of F, then $\{F(x),F(y),F(z),F(x)+F(y)+F(z)\}$ is a vanishing flat of F^{-1}, and the converse is also true by exchanging the roles of F and F^{-1}. We summarize this in the following lemma, that is not really a new result, but which clarifies the situation:

Lemma 5 *Let $P=\{x,y,z,x+y+z\}$ be any affine plane of $\mathbb{F}_{2^n}$ and let F be any permutation of $\mathbb{F}_{2^n}$. Then P is a vanishing flat of F if and only if $\{F(x),F(y),F(z),F(x)+F(y)+F(z)\}$ is a vanishing flat of F^{-1}.*

Let us study the case of the power function $F(x)=x^d$ with $d=\frac{3\cdot 2^n-2}{5}$ with $n\equiv 2 \pmod 4$, which is the compositional inverse of the power permutation x^5, since we have $5d\equiv 1 \pmod{2^n-1}$, and with $k=2$, we have that x^d is not second-order sum-free, that is, not APN, since it inverse x^5 is not APN, because $\gcd(2,n)=2\neq 1$. According to Lemma 5 applied to F^{-1} instead of F, the vanishing flats of F are the planes $\{x^5,y^5,z^5,x^5+y^5+z^5\}$ where $\{x,y,z,x+y+z\}$ are the vanishing flats of the power permutation x^5. According to Lemma 4, the vanishing flats of x^5 are the planes $\{x,y,z,x+y+z\}$ with x,y,z distinct, such that $y+z=w(x+z)$ or $y+z=w^2(x+z)$, where w and $w^2=w+1$ are the two primitive elements of $\mathbb{F}_4$, that is $z=w^2x+wy$ or $z=wx+w^2y$ (and in both cases, the condition $x\neq y$ is enough to ensure that x,y,z are distinct). We deduce:

Lemma 6 *The vanishing flats of the function $F(x)=x^d$, where $d=\frac{3\cdot 2^n-2}{5}$ and $n\equiv 2 \pmod 4$, are the planes:*

$$\{x^5,y^5,(w^2x+wy)^5,x^5+y^5+(w^2x+wy)^5=$$

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

and

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

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

where in both cases $x\neq y$.

We can check, since d is the inverse of 5, that F sums to 0 over each of these planes. Let us now see what gives $\sum_{x\in P}(F(x))^j$ when j is a positive integer of 2-weight 2 and P is any of these planes. Without loss of generality, we take $j=1+2^i$. We obtain in both cases $x^{1+2^i}+y^{1+2^i}+(w^2x+wy)^{1+2^i}+(wx+w^2y)^{1+2^i}=x^{1+2^i}+y^{1+2^i}+(w^2x+wy)(w^{2^{i+1}}x^{2^i}+w^{2^i}y^{2^i})+(wx+w^2y)(w^{2^i}x^{2^i}+w^{2^{i+1}}y^{2^i})$.

1. If $i\equiv 0 \pmod 3$, then we obtain $x^{1+2^i}+y^{1+2^i}+(w^2x+wy)(w^2x^{2^i}+wy^{2^i})+(wx+w^2y)(wx^{2^i}+w^2y^{2^i})=0$.

2. If $i\equiv 1 \pmod 3$, then we obtain $x^{1+2^i}+y^{1+2^i}+(w^2x+wy)(wx^{2^i}+w^2y^{2^i})+(wx+w^2y)(w^2x^{2^i}+wy^{2^i})=x^{1+2^i}+y^{1+2^i}+xy^{2^i}+x^{2^i}y=(x+y)^{1+2^i}\neq 0$.

3. If $i \equiv 2 \pmod 3$, then we obtain $x^{1+2^i} + y^{1+2^i} + (w^2x + wy)(w^2x^{2^i} + wy^{2^i}) + (wx + w^2y)(wx^{2^i} + w^2y^{2^i}) = 0$.

Determining j is this case is then easy.

4.3 Some other power functions

We shall study apart the case of the multiplicative inverse function in Subsection 5.2. Let us study the case of the power functions $P_k(x) = x^{2^k-1}$ (which are shown in [4] to be kth-order sum-free). For $k \leq 2$, there is nothing special to say about them, since they equal identity for $k = 1$ and are APN for $k = 2$. We assume then $k \geq 3$. The vanishing flats of P_k are not investigated in [9], so we need to address the case of j having a 2-weight equal to 1. Without loss of generality we can take $j = 1$. 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 again 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 larger than 1 for the corresponding affine planes $\{x, y, z, x+y+z\}$.

- If $x + y + 1 = 0$ (with x and y nonzero and distinct), then the equation 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 $x^{2^{k-1}-1} = 1$. We have $\gcd(2^{k-1}-1, 2^n-1) = 2^{\gcd(k-1,n)} - 1$. Hence, if $k - 1$ is co-prime with n, then the function sums to a nonzero value over $\{x, y, z, x+y+z\} = \{x, x+1, 1, 0\}$, and if $k - 1$ is not co-prime with n, then $\{x, x+1, 1, 0\}$ is a vanishing flat (that we need to consider when we move to j of a 2-weight larger than 2). Note that for $k = n - 1$ and n even, this gives what we know on the vanishing flats of the inverse function (see below): $x^{2^{k-1}-1} = 1$ becomes $x^{2^{n-2}-1} = 1$, that is, $x \in \mathbb{F}_4^*$ and (taking rid of the restriction that $z = 1$) the vanishing flats are the planes $z \cdot \mathbb{F}_4$ where $z \in \mathbb{F}_{2^n}^*$. But for $k = n - 2$, $x^{2^{k-1}-1} = 1$ becomes $x^{2^{n-3}-1} = 1$, that is, $x \in \mathbb{F}_8^*$, and we get vanishing flats of the form $z \cdot \{0, 1, x, x + 1\}$, where $x \in \mathbb{F}_8 \setminus \mathbb{F}_2$ and $z \in \mathbb{F}_{2^n}^*$. For $j = 1 + 2^i$, we have $z^{(2^k-1)j} + (zx)^{(2^k-1)j} + (z(x+1))^{(2^k-1)j} = z^{(2^k-1)j}(1 + (x^{1+2^i})^{2^k-1} + (x^{2^i+1} + x^{2^i} + x + 1)^{2^k-1})$.

- If $x+y+1 \neq 0$, then multiplying the equation by it gives $x^{2^k-1}y+x^{2^k-1}+xy^{2^k-1} + y^{2^k-1} + x + y = 0$, that is, $\frac{x^{2^k-1}+1}{x+1} = \frac{y^{2^k-1}+1}{y+1}$.
  We are then brought to considering those pre-images by the function $x \in \mathbb{F}_{2^n} \setminus \{1\} \mapsto \frac{x^{2^k-1}+1}{x+1}$ that contain at least two distinct elements x, y such that $x + y + 1 \neq 0$. For instance, the pre-image of 0 equals $\mathbb{F}_{2^r} \setminus \{1\}$ where $s = \gcd(k, n) = 1$, which leads to a vanishing flat if $s \geq 3$, and 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 $r \geq 3$.

We do not see how the known results on this function [1] can allow to determine all vanishing sets, for general k.

5 Power functions

An (n, n)-function $F(x) = x^d, x \in \mathbb{F}_{2^n}$ (where d is better viewed in $\mathbb{Z}/(2^n-1)\mathbb{Z}$, note that the 2-weight is coherent with this structure), is kth-order t-degree-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 $\sum_{x \in A} x^{dj} \neq 0$. Addressing the kth-order t-degree-sum-freedom of a power function x^d includes then addressing it for the functions x^l where l is a multiple of d, and we have:

Proposition 5 *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, then $F(x) = x^d$ is kth-order $(w_2(r)t)$-degree-sum-free.

Proof. Let A be any k-dimensional vector space 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 $w_2(rj) \leq w_2(r)w_2(j) \leq w_2(r)t$. □

5.1 A general upper bound on t for permutations

We give now an upper bound on the kth-order degree-sum-free-limit of power functions which, in some cases, is tighter than the bound $\min(k, m)$.

Proposition 6 *Let $F(x) = x^d$ be any power permutation and let d' be the inverse of d modulo $2^n - 1$. Then F is kth-order t-degree-sum-free where t equals the 2-weight of $r = d'(2^k - 1) \in \mathbb{Z}/(2^n-1)\mathbb{Z}$.*

Proof. We know from [4] that the power function x^{2^k-1} is kth-order sum-free, that is, kth-order 1-degree sum-free and we have: $d(d'(2^k-1)) \equiv 2^k - 1 \pmod{2^n - 1}$. Proposition 5 with $t = 1$ completes the proof. □

Of course, this gives an information only if $w_2(d'(2^k-1)) < w_2(2^k-1) = k$.

5.2 The multiplicative inverse function

The multiplicative inverse function

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

being APN for n odd, that is, second-order sum-free, it is second-order 1-degree-sum-free.
We know that F_{inv} is not 2nd-order sum-free over $\mathbb{F}_{2^n}$ when n is even, since it is not APN. Hence the multiplicative inverse function is not 2nd-order 1-sum-free. The next proposition shows that it is however kth-order t-degree-sum-free for the value of t coming immediately after 1.

Proposition 7 *Let n be an even integer such that $n \geq 4$. 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 [4] that for every affine space A that is not a vector space (i.e. which does not include the 0 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 $\frac{1}{a} + \frac{1}{b} + \frac{1}{a+b} = \frac{a^2+b^2+ab}{ab(a+b)} = \frac{a\left(1+(\frac{b}{a})^2+\frac{b}{a}\right)}{b(a+b)}$. 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 that, for every $k \in \{3, \ldots, n-3\}$ and every $n \geq 6$, the inverse function is not kth-order 2-degree-sum-free (see [5], see also [6]). It is then useful to study the values of t for which it is kth-order t-degree-sum-free.

5.2.1 A general upper bound on t

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

Proposition 8 *For every $2 \leq k \leq n$, the multiplicative inverse (n,n)-function is kth-order t-degree-sum-free with $t = n - k$.*

This is a direct consequence of Proposition 6 with $d' = 2^n - 2$ and $r = (2^n - 2)(2^k - 1) = 2^n - 2^k \in \mathbb{Z}/(2^n - 1)\mathbb{Z}$.
This result gives an information only for $n - k < k$, that is, $k > \frac{n}{2}$.
An interesting question would be to see whether $t = n - k$ can be lowered.

5.2.2 Relation with subspace polynomials and consequences

Case of vector spaces: Let E_k be a k-dimensional vector space and let $L_{E_k}(x) = \prod_{u \in E_k}(x + u) = \sum_{i=0}^{k} b_{k,i} x^{2^i}$ (see [4] and recall that $b_{k,0} \neq 0$ and $b_{k,k} = 1$). Such a (linearized) polynomial is sometimes called a subspace polynomial.
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 nonzero $x \in E_k$ and every non-negative integer j, by dividing 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:

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

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

Lemma 7 *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*

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

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

This result extends results from [4, 5].

Case of affine spaces not being vector spaces, i.e. not including 0: Let A_k be a k-dimensional affine space not containing 0. Since we know from [4] that $\sum_{x\in A_k} x^{-1}\neq 0$, we can take $j=1$ and do not have to look for larger values of j. By curiosity, let us show however how the method used above for vector spaces can be adapted to find again this result. Let E_k be the direction of A_k (that is, $E_k=A_k+A_k$). We have $A_k=L_{E_k}^{-1}(b)$ for some nonzero b. Then, for every $x\in A_k$, we have $b=\sum_{i=0}^{k} b_{k,i}x^{2^i}$ and then $\sum_{x\in A_k} x^{-j}=\frac{1}{b}\sum_{i=0}^{k}\Big(b_{k,i}\sum_{x\in A_k} x^{2^i-j}\Big)$. We find for $j=1$ that since $\sum_{x\in A_k} x^{2^i-1}$ is 0 for $i<k$ and nonzero for $i=k$, then $\sum_{x\in A_k} x^{-1}\neq 0$. This provides a different way of proving the known result from [4]. For $j\geq 2$, then we have that $\sum_{x\in A_k} x^{-j}=\frac{1}{b}\sum_{i=0}^{k}\Big(b_{k,i}\sum_{x\in A_k} x^{2^i-1-(j-1)}\Big)$ equals 0 for every j such that $j-1<2^k-1$ and is (of course) nonzero for $j=2^k$.

We deduce from the observations above:

Proposition 9 *The multiplicative inverse function F_{inv} is kth-order t-degree-sum-free, where t is 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 $t\geq\min\{i; 1\leq i\leq k \text{ and } b_{k,i}\neq 0\}$.*

Corollary 1 *If k divides n, then we have $t=k$.*

Proof. This is a direct consequence of the fact that, for $E_k=\mathbb{F}_{2^k}$, we have $L_{E_k}(x)=x^{2^k}+x$. □

The next corollary generalizes to the degree-sum-free-limit the equality, proved in [5], between the kth-order sum-freedom of the inverse function and its $(n-k)$th-order sum-freedom.

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

Proof. It is recalled in [5] 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 $L_{E_{n-k}} \circ L_{E_k}(x) = \sum_{i=0}^{n-k} \sum_{j=0}^{k} (b_{k,j})^{2^i} b_{n-k,i} x^{2^{i+j}}$. We have then:

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

We know from Proposition 9 that, if t is the kth-order degree-sum-free-limit 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 $t-1$ first relations in (2) imply $b_{n-k,1} = \cdots = b_{n-k,t-1} = 0$ and the tth relation implies $b_{n-k,t} \neq 0$. □

5.2.3 The case of $k = 3$

The result [4, Proposition 8] gives a necessary and sufficient condition on two elements a, b such that a, b and 1 are linearly independent over $\mathbb{F}_2$ and F_{inv} sums to 0 over the 3-dimensional vector space E spanned by $a, b, 1$ (and this is straightforwardly generalized to the 3-dimensional vector space spanned by three linearly independent elements a, b, c by replacing a by $\frac{a}{c}$, b by $\frac{b}{c}$ and multiplying all the elements in the vector space by c, which does not change the fact that the sum of the function x^{-j} over the vector space sums to 0 or to a nonzero value). The condition is $ab^4 + a^4b + ab^8 + a^8b + a^4b^8 + a^8b^4 = 0$. Dividing by ab and factorizing gives $(a^7+1)(b^3+1) = (a^3+1)(b^7+1)$. Note that if $a \in \mathbb{F}_4$ (that is, $a \in \mathbb{F}_4 \setminus \mathbb{F}_2$), then the condition becomes $(a+1)(b^3+1) = 0$, that is, $b \in \mathbb{F}_4 \setminus \mathbb{F}_2$, but then $a, b, 1$ are not linearly independent. The condition can then be written:

$$a, b \notin \mathbb{F}_4, \quad a, b, 1 \text{ linearly independent, and } \quad \frac{a^7+1}{a^3+1} = \frac{b^7+1}{b^3+1}. \tag{3}$$

To determine the kth-order degree-sum-free-limit of the multiplicative inverse function, we need then, for every a, b satisfying (3), to find the minimum 2-weight (necessarily at least 2) of non-negative integers j such that:

$$a^{-j} + b^{-j} + 1 + (a+b)^{-j} + (a+1)^{-j} + (b+1)^{-j} + (a+b+1)^{-j} \neq 0.$$

We leave this question open for the moment.

5.2.4 The case of $k \geq n-4$

If $k = n$, then Corollary 1 shows that $t = n$.
If $k = n-1$, then we know from [5] that the inverse function is kth-order sum-free and then $t = 1$.
If $k = n-2$, then we can apply Corollary 2 and we have that F_{inv} is $(n-2)$th-order 1-degree-sum-free over $\mathbb{F}_{2^n}$ when n is odd, and it is only kth-order 2-degree-sum-free when n is even. By curiosity, let us prove it also directly. We know from [5], for general k, that $\sum_{u \in E_k \setminus \{0\}} \frac{1}{u}$ equals the coefficient of x in the univariate representation of the indicator function $1_{E_k}(x)$ and it is deduced that if $(u_1, \ldots, u_{n-k})$ is a basis of $E^\perp = \{y \in \mathbb{F}_{2^n}; tr_n(x\,y) = 0, \forall x \in E\}$, since we have $1_E(x) = \prod_{i=1}^{n-k}(1 + tr_n(u_i\,x))$, the coefficient of x equals then:

$$\sum_{\substack{b \in \{-\infty, 0, \ldots, n-1\}^{n-k}; \\ \sum_{i=1}^{n-k} 2^{b_i} \equiv 1 \pmod{2^n-1}}} \left(\prod_{i=1}^{n-k} u_i^{2^{b_i}} \right).$$

For $k = n-2$, we obtain $u_1 + u_2 + \left(u_1 u_2\right)^{\frac{1}{2}}$ and the $(n-2)$-dimensional spaces over which the inverse function sums to 0 are of the form $(a\,\mathbb{F}_4)^\perp$, $a \in \mathbb{F}_{2^n}^*$, that is, of the form $a\,\mathbb{F}_4^\perp$, $a \in \mathbb{F}_{2^n}^*$. We can use Proposition 9: $\mathbb{F}_4^\perp$ equals $\{x \in \mathbb{F}_{2^n}; tr_n(x) = tr_n(wx) = 0\}$, where w is a primitive element of $\mathbb{F}_4$ and its subspace polynomial equals then the gcd of $tr_n(x)$ and $tr_n(wx)$. We have $\gcd\left(tr_n(x), tr_n(wx)\right) = \gcd\left(tr_n(x), wtr_n(x) + tr_n(wx)\right) = \gcd\left(x + x^4 + \cdots + x^{2^{n-2}}, tr_n(x)\right) = x + x^4 + \cdots + x^{2^{n-2}}$. We deduce:

Proposition 10 *Let $n \geq 4$ be any even integer. Then the multiplicative inverse function is $(n-2)$th-order 2-degree-sum-free.*

If $k = n-3, n-4$, then it can be proved (see [5]) that F_{inv} is not $(n-3)$th-order sum-free over $\mathbb{F}_{2^n}$ We leave the study of the kth-order degree-sum-free-limit open for the moment.

References

[1] 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.

[2] 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.

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

[4] C. Carlet. Two generalizations of almost perfect nonlinearity. Cryptology ePrint Archive 2024/841

[5] C. Carlet. On the vector subspaces of $\mathbb{F}_{2^n}$ over which the multiplicative inverse function sums to zero. Cryptology ePrint Archive 2024/1007

[6] C. Carlet and X.-D. Hou. More on the sum-freedom of the multiplicative inverse function. Preprint, 2024.

[7] P. Hebborn, G. Leander, and A. Udovenko. Mathematical aspects of division property. *Cryptography and Communications* 15, no. 4, pp. 731-774, 2023.

[8] L. Knudsen and D. Wagner. Integral cryptanalysis. *Proceedings of Fast Software Encryption FSE 2002, Lecture Notes in Computer Science* vol. 2365, pp. 112127, 2002.

[9] 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.

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

[11] Y. Todo. Structural evaluation by generalized integral property. *Proceedings of EUROCRYPT 2015, Lecture Notes in Computer Science* 9056, pp. 287-314, 2015.