Two generalizations of almost perfect nonlinearity

Claude Carlet,

E-mail: claude.carlet@gmail.com

Universities of Bergen, Norway and Paris 8, France.

Abstract. Almost perfect nonlinear (in brief, APN) functions are (so-called vectorial) functions $F : \mathbb{F}_2^n \to \mathbb{F}_2^n$ playing roles in several domains of information protection, at the intersection of computer science and mathematics. Their definition comes from cryptography and is also related to coding theory. The cryptographic motivation for studying APN functions is that, when they are used as substitution boxes (S-boxes), ensuring nonlinearity in block ciphers, they contribute optimally to the resistance against differential attacks. Their study has been very active since the 90's, and has posed interesting and difficult mathematical questions, that are still unanswered.
Since the introduction of differential attacks, more recent types of cryptanalyses have been designed, such as integral attacks. No notion about S-boxes has been identified which would play a similar role with respect to integral attacks. In this paper, we introduce and study two generalizations of almost perfect nonlinearity, that directly extend classical characterizations of APN functions, and are also related to the integral attack. The two resulting notions are significantly different (and behave differently) from differential uniformity, which is a well-known generalization of APNness; they also behave differently from each other, despite the apparent similarity between their definitions. We study the different ways to define them, and on the example of Kasami functions, how difficult they are to achieve. We prove their satisfiability, their monotonicity, their invariance under classical equivalence relations and we characterize them by the Walsh transform.
We begin a study of the multiplicative inverse function (used as a substitution box in the Advanced Encryption Standard and other block ciphers) from the viewpoint of these two notions. In particular, we find a simple expression of the sum of the values taken by this function over affine subspaces of $\mathbb{F}_{2^n}$ that are not vector subspaces. This formula shows that, in such case, the sum never vanishes (which is a remarkable property of the inverse function).

Keywords: Vectorial function, Substitution box, Almost perfect nonlinearity

1 Introduction

One of the main attacks on block ciphers, in symmetric cryptography, is the differential attack [5]. Almost perfect nonlinear (APN) (n, n)-functions $F : \mathbb{F}_2^n \to \mathbb{F}_2^n$, introduced in [37, 36], are those (vectorial Boolean) functions which contribute to an optimal resistance, against this attack, of the block ciphers using F as a substitution box (S-box); see also [34] and [6, 12, 14]. Such S-boxes are essential for including nonlinearity and ensuring what C. Shannon called confusion. Almost perfect nonlinearity can be characterized in at least three equivalent ways (the first of which is the original definition):
(i) for every nonzero $a \in \mathbb{F}_2^n$, the derivative[1] $D_aF(x) = F(x)+F(x+a)$ is 2-to-1 (that is, every element of the co-domain has either two pre-images or none by D_aF);
(ii) the restriction of F to any affine plane $\{x, y, z, x + y + z\}$ of $\mathbb{F}_2^n$ (with $x, y, z, x + y + z$ distinct, that is, with x, y, z distinct) is not an affine function;
(iii) the sum of the values taken by $F(x)$ when x ranges over any affine plane is nonzero (that is, $F(x)+F(y)+F(z)+F(x+y+z)$ is nonzero for every distinct x, y, z).
There is also a characterization in terms of coding theory [14] that we shall not use in this paper.

The notion of APN function is mathematically important since its definition is very simple and it poses difficult questions, that have remained open for more than thirty years now, despite an active related research activity in all domains of discrete mathematics. It is also important cryptographically, of course. For instance, the choice of the substitution boxes in the most important block cipher for civil use, the Advanced Encryption Standard (AES) [19], is directly related to the work of Kaisa Nyberg in [36] about APN functions. Much still needs to be understood on the structure and the properties of APN functions. For instance, finding an APN permutation in an even number of variables larger than 6 would be an important theoretical and practical advance, as well as determining whether APN functions necessarily have non-weak nonlinearity for every n (that is, whether the nonzero linear combinations of their coordinate functions are always at reasonably large Hamming distance from all affine Boolean functions $x \mapsto a \cdot x + \epsilon$, $a \in \mathbb{F}_2^n$, $\epsilon \in \mathbb{F}_2$). This latter question is settled only for $n \leq 6$ (see [3] and [2]; see also [13] where a lower bound is found for a subclass). The nonlinearity is a parameter of vectorial functions related to the resistance against linear attacks (another very important class of attacks).

A way to progress on a notion is to introduce and study generalizations making sense from both theoretical and practical points of view. A well-known generalization of APNness, also related to the differential attack, is differential uniformity [34, 35], which extends the first of the three definitions of APNness above: given three positive integers n, m and δ, an (n, m)-function $F : \mathbb{F}_2^n \to \mathbb{F}_2^m$

[1] To distinguish this derivative from the classical derivative of a polynomial, we could specify "discrete derivative".

is differentially δ-uniform if, for every $a \neq 0$ in $\mathbb{F}_2^n$ and every b in $\mathbb{F}_2^m$, the equation $D_aF(x) = b$ has at most δ solutions. The value $\delta = 2$ is the smallest possible, since for every function F, the number of these solutions is even, because $D_aF(x) = D_aF(x + a)$ (the situation is different in odd characteristic), and cannot be always zero. APNness is equivalent to differential 2-uniformity and the term is reserved for (n, n)-functions.

Other generalizations of APNness have been introduced in the literature. An (n, m)-function F is called weakly APN in [1] if its nonzero derivatives all have image set size larger than 2^{n-2}, and it is called partially APN in [8] if, for some $c \in \mathbb{F}_2^n$, the sum of the values $F(x)$ when x ranges over any affine plane containing c is nonzero. One more generalization, called almost perfect c-nonlinearity (APcN), was introduced recently in [22], whose definition is similar to APNness and is related to the c-differential uniformity of vectorial functions, defined for a function F as the maximal number of solutions $(a, b) \in \mathbb{F}_{2^n}^{\star} \times \mathbb{F}_{2^n}$ of the equation $F(x) + cF(x+a) = b$. These ad hoc generalizations are not directly related to efficient attacks and will not play a role in the present paper.

Another kind of attacks has drawn the attention of the cryptographic community and provides one of the most efficient cryptanalytic tools for block ciphers: integral attacks [26, 41], which are generalizations of higher order differential attacks [28, 25] and of the square attack [21]. Given a block cipher, those attacks are based on the propagation of sums of values, called *integrals*, through the encryption algorithm. They exploit the existence of a subset of plaintexts such that summing (with a possible ponderation by field elements, see [38]) the corresponding ciphertexts results in a value that is predictable in some way (ideally, independent of the key), after some number of rounds of encryption (for instance, the sum evaluates to zero in some positions). This yields in some cases a distinguisher, which can be turned into a key recovery attack, as for the differential attack. Integral cryptanalysis applies to some ciphers which are not vulnerable to the differential and linear cryptanalyses, and the 128-bit AES limited to six rounds (instead of ten), while it resists these latter attacks, is vulnerable to integral attacks.
It is well-known that providing arguments that a given cipher is resistant against integral attacks is difficult, because the sums can a priori be made over any set, and the behavior of integrals is difficult to analyse. Studying each S-box independently of the rest of the algorithm, as done by Nyberg and Knudsen for the differential attack [36, 37], does not work so well and there is no equivalent to APNness for such attacks. Of course, we know that even for the regular APN concept, there is no 100% correspondence between strong S-boxes and strong ciphers, but the situation with integral attacks is worse.
Integral attacks have been refined in [40] thanks to the so-called division property, and in [4] is initiated a theory to describe integral and divisional cryptanalyses in a way similar to linear cryptanalysis and (quasi-)differential cryptanalysis, where the Linear Approximation Table (correlation matrix) and the Difference Distribution Table are replaced by an Algebraic Transition Matrix, which has the nice property that the algebraic transition matrix of a composition of func-

tions is the product of their corresponding algebraic transition matrices, and there is a simple similar result for concatenation. In addition to the theoretical advance that this notion represents and the computational improvements that it allows (through algorithms computing division properties and efficiently searching for [extended] integral properties), it induces progress in the direction which interests us in the present paper: highlighting the features of vectorial functions allowing them to contribute to the resistance of block ciphers using them as an S-box against integral attacks. But it does not give yet a specific and simple criterion on S-boxes for their contribution to the resistance against these attacks.
Further improvements could lead to such criteria in the future, but it seems useful already to try helping the designers to make choices between S-boxes, in order to improve the resistance of block ciphers against integral attacks. Defining such features seems easier if we restrict ourselves to those attacks where the set over which are considered the integrals is taken as an affine subspace (and actually, this is the case in most attacks, see e.g. [24]; often, but not always, see e.g. [29], this affine space corresponds to fixing some bits in the plaintext). In a similar way as the existence probability of differentials for a block cipher depends on the existence of sufficiently non-uniform derivatives for the involved S-boxes, it seems natural that the condition of the unpredictability of the propagation of integrals is more difficult to achieve if, for some S-boxes used in the cipher, there exist affine spaces A over which they sum to zero. This is illustrated for instance in [40] (where the notion of division property is introduced). Recall that a division property consists of an affine subspace that after evaluation leads to a zero sum for the ith bit of the output. It seems clear that if the situation thus described happens at the level of an S-box, for all bits of the output, the risk for the designer that an integral attack can be found thanks to a distinguisher is greater. And actually, [40] considers explicitly the possibility that the sum of the values taken by an S-box over an affine space of inputs is zero (this scenario is denoted by $\mathcal{B}$ in [40, End of Section 2 and Section 3]). Of course, the non-existence of such affine spaces A of inputs to the S-boxes in a block cipher (property that we shall call informally *sum freedom*) does not ensure that no attack can be found, but the existence of such A of a small enough dimension seems a feature that would better be avoided, if possible.
Sum freedom with affine spaces of a given (small enough) dimension seems then an interesting property to be studied for S-boxes: if every other of the crucial properties is identical between two possible choices of S-boxes, it makes sense to go (taking also into account implementation criteria) for the S-box that does not sum to zero for small dimensions (larger than or equal to two) and if it does so for larger dimensions, then it should be the least possible. Note that for dimension one, the condition of not summing to zero over affine spaces corresponds for (n, n)-functions to bijectivity, and for dimension two, it corresponds to APNness.

There is some relation between sum freedom and invariant subspace attacks, that have been studied in a larger generality in [31]. An invariant subspace is an affine subspace A whose image (by some permutation F, which can be an S-box, or more interestingly, the part of a round that is preceding the addition of the round key) is a coset of A, so that there exist round keys that are such that the image after the addition of the key equals A. If this happens, then F sums to 0 over A (indeed, the sum of the elements of any affine space of a dimension at least 2 equals 0). Hence, sum freedom protects against the existence of invariant subspaces (and is much more demanding than avoiding invariant subspaces).

There is also some relation between sum freedom and the older notion of normality proposed by Dobbertin in [20] for Boolean functions and later generalized (e.g. in [33]): given $k \leq n$, an n-variable (vectorial) Boolean function F is called k-normal (resp. k-weakly-normal) if there exists a k-dimensional flat on which F is constant (resp. affine). Such functions are considered peculiar when k is large enough (but almost all known bent Boolean functions are $\frac{n}{2}$-normal, see *e.g.*[12]). It is shown in [10] that almost all[2] n-variable Boolean functions are non-k_n-weakly-normal when the sequence k_n satisfies $k_n \geq c \log_2 n$ for some $c > 1$ and every n. The notion of kth-order sum-freedom corresponds (for $k \geq 2$) to a strengthening (a considerable one if k is large enough) of the notion of non-k-weak-normality extended to vectorial functions into: the restriction of F to any k-dimensional flat has (optimal) algebraic degree k.

In the present paper, we study the notions which generalize in a natural way the two characterizations (ii) and (iii) above of APNness (replacing "affine plane" by "k-dimensional affine space", with $k \geq 2$). We call them kth-order-non-affineness and kth-order-sum-freedom. The latter is related to the integral attack, according to the observations above, and the former seems interesting to study as well, at least for comparison with the latter. We shall see that studying these two notions gives some view on the almost perfect nonlinearity property itself. We show that each of the two notions is significantly different from differential uniformity, and that there are big differences between them too as well.

The paper is organized as follows. After preliminaries in Section 2, we define the two notions in Section 3, we study the different ways of expressing them, and we study the APN Kasami functions as an example; we verify the existence of functions satisfying each notion. We study in Section 4 the properties of the two notions, which show important differences between them and in some cases with APNness. After studying in Subsection 4.1 the constraints on the algebraic degree implied by these notions and in Subsection 4.2 their (non-)monotonicity, we generalize in Subsection 4.3 the Chabaud-Vaudenay characterization of APNness by the Walsh transform to kth-order-non-affineness and to kth-order-sum-freedom (both characterizations happen to be more difficult to obtain than for APNness, and their expressions are more complex). We study in Subsection 4.4 the invariance under the classical equivalences of both notions. In Section 5, we begin a study, with respect to these two notions, of the multiplicative inverse function $x \in \mathbb{F}_{2^n} \mapsto x^{2^n-2}$ (which is clearly, since Nyberg's works and the invention of the AES, the most important infinite class of vectorial functions to be studied from a cryptographic point of view). We show in particular that this

[2] In the sense of probability.

function sums to nonzero values over all affine subspaces of $\mathbb{F}_{2^n}$ that are not linear subspaces, whatever is their dimension.

2 Preliminaries

Given two positive integers n and m, the functions from $\mathbb{F}_2^n$ to $\mathbb{F}_2^m$ are called (n,m)-functions. When n and/or m are not specified, these functions are called vectorial functions. In the particular case of $m=1$, they are called n-variable Boolean functions, or Boolean functions in dimension n. The vector space of n-variable Boolean functions is denoted by $\mathcal{B}_n$. Every (n,m)-function F admits a unique algebraic normal form, that is, a representation as a multivariate polynomial of the form $F(x)=\sum_{I\subseteq\{1,\dots,n\}} a_I \prod_{i\in I} x_i = \sum_{I\subseteq\{1,\dots,n\}} a_I\, x^I$; $x=(x_1,\dots,x_n)\in\mathbb{F}_2^n, a_I\in\mathbb{F}_2^m$. The degree $\max\{|I|; a_I\neq 0\}$ of this multivariate polynomial is called the algebraic degree of F and denoted by $d_{alg}(F)$. Any function F is affine, that is, satisfies $F(x)+F(y)+F(z)+F(x+y+z)=0$ for every $x,y,z\in\mathbb{F}_2^n$ if, and only if, its algebraic degree is at most 1. We shall say that a function is *quadratic* if it has algebraic degree at most 2 (hence, affine functions are particular quadratic functions in this terminology, which is nowadays widely accepted since defining quadratic functions as having algebraic degree exactly 2 would make many statements more complex). Function F has algebraic degree at most $r<n$ if, and only if, it sums to zero over every affine space of dimension $k>r$. An (n,m)-function has algebraic degree n (the maximum) if, and only if, it sums to a nonzero value over $\mathbb{F}_2^n$.

If $\mathbb{F}_2^n$ is endowed with the structure of the field $\mathbb{F}_{2^n}$ (which is always possible since we know that $\mathbb{F}_{2^n}$ is an n-dimensional vector space over $\mathbb{F}_2$), then every (n,n)-function (and thus, every (n,m)-function where m divides n) can be uniquely represented by its univariate representation:

$$F(x)=\sum_{i=0}^{2^n-1}\delta_i x^i\in\mathbb{F}_{2^n}[x]/(x^{2^n}+x);\ \delta_i\in\mathbb{F}_{2^n} \tag{1}$$

(we call power functions the functions of univariate representation $F(x)=x^i$). The algebraic degree of function F in (1) equals the largest Hamming weight of the binary expansion of those exponents i whose coefficients δ_i are nonzero. The Hamming weight of the binary expansion of an integer i is called its 2-weight and is denoted by $w_2(i)$. Note that any Boolean function f over $\mathbb{F}_{2^n}$ is also an (n,n)-function because its co-domain $\mathbb{F}_2$ is a subfield of $\mathbb{F}_{2^n}$. For such a function, we have $\delta_0,\delta_{2^n-1}\in\mathbb{F}_2$ and $\delta_{2i}=\delta_i^2$ for every $i\in\{1,\dots,2^n-2\}$ (where the index $2i$ is taken modulo 2^n-1). Denoting by tr_n the absolute trace function over $\mathbb{F}_{2^n}$: $tr_n(x)=\sum_{i=0}^{n-1}x^{2^i}$ (which satisfies $tr_n(x^2)=tr_n(x)$ and is valued in $\mathbb{F}_2$), we can then write the univariate representation of f in the form $\delta_0+tr_n(\sum_{i=0}^{2^n-1}b_i x^i)$ (but there is no more uniqueness of the b_i; the representation with uniqueness is more complex, see e.g. [12])).

The *Walsh transform* of a Boolean function f is the function from $\mathbb{F}_2^n$ to $\mathbb{Z}$ defined as follows:

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

where "$\cdot$" is some inner product in $\mathbb{F}_2^n$. The Walsh transform satisfies the so-called *inverse Walsh transform relation*:

$$\sum_{u \in \mathbb{F}_2^n} W_f(u)(-1)^{u\cdot v} = 2^n(-1)^{f(v)}, \forall v \in \mathbb{F}_2^n, \tag{2}$$

The Walsh transform of an (n, m)-function F takes value $W_{v\cdot F}(u)$ at input $(u, v) \in \mathbb{F}_2^n \times \mathbb{F}_2^m$:

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

where "$\cdot$" denotes, by abuse of notation, two inner products, one in $\mathbb{F}_2^n$ and one in $\mathbb{F}_2^m$.

Two (n, m)-functions F and G are called affine equivalent if there exist two affine permutations L over $\mathbb{F}_2^m$ and L' over $\mathbb{F}_2^n$ such that $G = L \circ F \circ L'$. In the case of Boolean functions, L is taken equal to identity. More generally, F and G are called extended-affine (EA) equivalent if there exists an affine function L from $\mathbb{F}_2^n$ to $\mathbb{F}_2^m$ such that F and $G+L$ are affine equivalent. Still more generally, they are called CCZ equivalent if their graphs $\mathcal{G}_F = \{(x, F(x));\, x \in \mathbb{F}_2^n\}$ and $\mathcal{G}_G = \{(x, G(x));\, x \in \mathbb{F}_2^n\}$ are affine equivalent (that is, one is the image of the other by an affine permutation over $\mathbb{F}_2^{n+m}$). Writing the affine automorphism mapping $\mathcal{G}_F$ to $\mathcal{G}_G$ as $(x, y) \mapsto (L_1(x, y), L_2(x, y))$ where $L_1 : \mathbb{F}_2^{n+m} \to \mathbb{F}_2^n$ and $L_2 : \mathbb{F}_2^{n+m} \to \mathbb{F}_2^m$ are affine functions, then defining $F_1(x) = L_1(x, F(x))$ and $F_2(x) = L_2(x, F(x))$, we have that F_1 is a permutation of $\mathbb{F}_2^n$ and $G = F_2 \circ F_1^{-1}$, see e.g. [12]. A particular case of CCZ equivalence is between any (n, n)-permutation and its inverse, since the two graphs are the swaps of each other. In the case of Boolean functions, CCZ equivalence reduces to EA equivalence (see e.g. [12]).

We shall say that a notion is affine invariant (respectively, EA invariant, CCZ invariant) if it is preserved by affine equivalence (respectively, EA equivalence, CCZ equivalence). For theoretical and practical reasons, it is important to determine the most general equivalence preserving each notion introduced.

We have seen in the introduction that an (n, m)-function is called differentially δ-uniform if $|\{x \in \mathbb{F}_2^n; F(x) + F(x + a) = b\}| \leq \delta$ for every nonzero $a \in \mathbb{F}_2^n$ and every $b \in \mathbb{F}_2^m$. As observed initially by Nyberg, we have $\delta \geq 2^{n-m}$, with equality if, and only if, F is bent, that is, the minimum Hamming distance between the nonzero linear combinations of the coordinate functions of F and the affine Boolean functions achieves the maximum $2^{n-1} - 2^{\frac{n}{2}-1}$; such functions exist if, and only if, n is even and $m \leq \frac{n}{2}$, as proved in [34]. We shall speak of almost perfect nonlinear function when $\delta = 2$ and $m = n$. When $m = n-1$ such functions do not exist since they would be bent and we know that this is not possible unless $n = 2$. When $m \geq n+1$ we keep the term of differential 2-uniformity. Chabaud and Vaudenay have characterized in [17] the APNness of (n,n)-functions by the Walsh transform: F is APN if, and only if, $\sum_{u\in\mathbb{F}_2^n}\sum_{v\in\mathbb{F}_2^n} W_F^4(u,v) = 3\cdot 2^{4n} - 2^{3n+1}$ (and this characterization has been generalized to the characterization of differentially uniform functions in [11] in diverse ways).

3 Two new generalizations of APNness

In this section, we introduce the two extensions of the notion of APN function and we detail the equivalent ways to define them; we study an example to see how difficult they are to satisfy (and to check), and we study their satisfiability.

Definition 1. *Let $2 \leq k \leq n$ and m be positive integers. An (n,m)-function F is called kth-order-non-affine (resp. kth-order-sum-free) if, for every k-dimensional affine subspace (i.e. k-flat) A of $\mathbb{F}_2^n$, the restriction of F to A is not an affine function (resp. the sum $\sum_{x\in A} F(x)$ is nonzero).*

Clearly, kth-order-sum-freedom implies kth-order-non-affineness, since the sum of the values taken by an affine function over an affine space of dimension at least 2 equals 0. We shall see that kth-order-sum-freedom is a strong property and kth-order-non-affineness is a much weaker one.
By the definition of affineness, F is kth-order-non-affine if, and only if, every k-dimensional affine space in $\mathbb{F}_2^n$ contains an affine plane (a 2-dimensional affine space) on which F does not sum to 0. Consequently, if a function is kth-order-non-affine, then it is lth-order-non-affine for every $l \geq k$ (see more in Subsection 4.2). In particular, every APN function is kth-order-non-affine for every $k \geq 2$. Of course, for every $k \leq l \leq n$, F is kth-order-non-affine (resp. kth-order-sum-free) if, and only if, its restriction to any l-dimensional affine space of $\mathbb{F}_2^n$ is kth-order-non-affine (resp. kth-order-sum-free).

Note that F is kth-order-sum-free if, and only if, for every $(k-1)$-dimensional affine subspace A of $\mathbb{F}_2^n$ and every coset $a+A \neq A$, we have $\sum_{x\in A} F(x) \neq \sum_{x\in A} F(x+a)$, that is, $\sum_{x\in A} D_aF(x) \neq 0$ (note that this does not mean that D_aF is $(k-1)$th-rder-sum-free, despite the similarity, since a must not belong to the underlying linear space of A, for ensuring $a+A \neq A$). Equivalently, for every $(k-1)$-dimensional vector subspace E of $\mathbb{F}_2^n$, the mapping $\phi_E : a \in \mathbb{F}_2^n/E \to \sum_{x\in a+A} F(x)$ is injective. There is then a connection between 3rd-order-sum-freedom and the so-called D-property (saying that the union of the image sets of all such mappings ϕ_E, when E ranges over the set of all affine planes, covers $\mathbb{F}_2^m \setminus \{0\}$). D-property is so named in [39] because Dillon was the first to consider it, by showing that it is satisfied by every APN (n,n)-function (see his result reported in [12] after Proposition 161).
An (n,m)-function F is third-order-sum-free if and only if, for every $a \neq 0$, the system of equations

$$\begin{cases} x+y+z+t=0 \\ D_aF(x)+D_aF(y)+D_aF(z)+D_aF(t)=0 \end{cases}$$

has no solution (x, y, z, t) with x, y, z, t distinct such that $a \notin \langle x+y, x+z \rangle = \{0, x+y, x+z, x+t\}$ (where we denote by $< S >$ the vector space spanned by a set S in a vector space). Equivalently, for every nonzero $u \in \mathbb{F}_2^n$ and every $v \in \mathbb{F}_2^m$, the system

$$\begin{cases} x+y=u \\ D_aF(x)+D_aF(y)=v \end{cases}$$

has at most one solution as an unordered pair $\{x, y\}$ in a linear hyperplane H such that $u \in H$ and $a \notin H$.
This is a convenient characterization when the derivative of F is simple enough. But when D_aF is complex (we shall see the example of Kasami functions below), it may be better, as we shall see in the next subsection, to state the condition by means of F rather than its derivative: for every $v \in \mathbb{F}_2^m$, the system

$$\begin{cases} x+y+z+t=0 \\ F(x)+F(y)+F(z)+F(t)=v \end{cases} \tag{3}$$

does not have two solutions $\{x, y, z, t\}$ and $\{x', y', z', t'\}$ with x, y, z, t distinct in $\mathbb{F}_2^n$ and such that $x+x'=y+y'=z+z'=t+t' \neq 0$. Note that if F is APN, then we can without loss of generality assume that $v \neq 0$. Note also that the APNness of F is not mandatory, since for APNness we need that (3) is never satisfied with $v=0$ and x, y, z, t distinct while here we can accept one solution.

3.1 Example of the Kasami almost bent functions

Of course, the so-called Gold power functions over $\mathbb{F}_{2^n}$, equal to $G_i(x) = x^{2^i+1}$ with $i < n/2$ and $\gcd(i, n) = 1$, which are the simplest APN (hence, k-th-order-non-affine for every $k \geq 2$ and second-order-sum-free) functions, are not kth-order-sum-free for $k \geq 3$ since they have algebraic degree 2 and sum then to 0 over every k-dimensional affine space with $k \geq 3$.
The Kasami functions are the power functions over $\mathbb{F}_{2^n}$ equal to $K_i(x) = x^{2^{2i}-2^i+1}$, with $i < n/2$ and $\gcd(i, n) = 1$; they have algebraic degree $i+1$. For any n, K_i is APN. It is then kth-order-non-affine for every $k \geq 2$. If additionally, n is odd, K_i also contributes to an optimal resistance against the linear attack (it is what we call an almost bent function). See more details in [12] and the references therein. The Kasami function is used as an S-box (with n odd) in the Misty and Kasumi block ciphers.
For n odd, we have $K_i = G_{3i} \circ G_i^{-1}$ where G_i^{-1} is the compositional inverse of G_i (which is a permutation). Denoting $x = G_i(\mathtt{x})$, $y = G_i(\mathtt{y})$, $z = G_i(\mathtt{z})$, and $t = G_i(\mathtt{t})$, System (3) writes:

$$\begin{cases} G_i(\mathtt{x})+G_i(\mathtt{y})+G_i(\mathtt{z})+G_i(\mathtt{t})=0 \\ G_{3i}(\mathtt{x})+G_{3i}(\mathtt{y})+G_{3i}(\mathtt{z})+G_{3i}(\mathtt{t})=v \end{cases},$$

with $\mathtt{x}, \mathtt{y}, \mathtt{z}, \mathtt{t}$ distinct, and denoting $\mathtt{x}+\mathtt{y}$ by α and $\mathtt{z}+\mathtt{t}$ by β, we have then to solve the system

$$\begin{cases} D_\alpha G_i(\mathtt{x})+D_\beta G_i(\mathtt{z})=0 \\ D_\alpha G_{3i}(\mathtt{x})+D_\beta G_{3i}(\mathtt{z})=v \end{cases}.$$

This is equivalent to

$$\begin{cases} \alpha\mathtt{x}^{2^i}+\alpha^{2^i}\mathtt{x}+\alpha^{2^i+1}+\beta\mathtt{z}^{2^i}+\beta^{2^i}\mathtt{z}+\beta^{2^i+1}=0 \\ \alpha\mathtt{x}^{2^{3i}}+\alpha^{2^{3i}}\mathtt{x}+\alpha^{2^{3i}+1}+\beta\mathtt{z}^{2^{3i}}+\beta^{2^{3i}}\mathtt{z}+\beta^{2^{3i}+1}=v \end{cases}.$$

Note that since $G_i(\mathtt{x})$ and $G_i(\mathtt{y})$ are distinct as well as $G_i(\mathtt{z})$ and $G_i(\mathtt{t})$, we have that α,β cannot be zero. The system writes then

$$\begin{cases} \alpha^{2^i+1}\left(\left(\frac{\mathtt{x}}{\alpha}\right)^{2^i}+\frac{\mathtt{x}}{\alpha}+1\right)+\beta^{2^i+1}\left(\left(\frac{\mathtt{z}}{\beta}\right)^{2^i}+\frac{\mathtt{z}}{\beta}+1\right)=0 \\ \alpha^{2^{3i}+1}\left(\left(\frac{\mathtt{x}}{\alpha}\right)^{2^{3i}}+\frac{\mathtt{x}}{\alpha}+1\right)+\beta^{2^{3i}+1}\left(\left(\frac{\mathtt{z}}{\beta}\right)^{2^{3i}}+\frac{\mathtt{z}}{\beta}+1\right)=v \end{cases},$$

which is equivalent by using the relation $\left(\left(\frac{\mathtt{x}}{\alpha}\right)^{2^i}+\frac{\mathtt{x}}{\alpha}+1\right)+\left(\left(\frac{\mathtt{x}}{\alpha}\right)^{2^i}+\frac{\mathtt{x}}{\alpha}+1\right)^{2^i}+\left(\left(\frac{\mathtt{x}}{\alpha}\right)^{2^i}+\frac{\mathtt{x}}{\alpha}+1\right)^{2^{2i}}=\left(\frac{\mathtt{x}}{\alpha}\right)^{2^{3i}}+\frac{\mathtt{x}}{\alpha}+1$ to:

$$\begin{cases} \left(\frac{\mathtt{x}}{\alpha}\right)^{2^i}+\frac{\mathtt{x}}{\alpha}+1=\left(\frac{\beta}{\alpha}\right)^{2^i+1}\left(\left(\frac{\mathtt{z}}{\beta}\right)^{2^i}+\frac{\mathtt{z}}{\beta}+1\right) \\ L\left(\left(\frac{\beta}{\alpha}\right)^{2^i+1}\left(\left(\frac{\mathtt{z}}{\beta}\right)^{2^i}+\frac{\mathtt{z}}{\beta}+1\right)\right)+\left(\frac{\beta}{\alpha}\right)^{2^{3i}+1}\left(\left(\frac{\mathtt{z}}{\beta}\right)^{2^{3i}}+\frac{\mathtt{z}}{\beta}+1\right)=\frac{v}{\alpha^{2^{3i}+1}}. \end{cases} \tag{4}$$

where $L(x)=x+x^{2^i}+x^{2^{2i}}$.

Function F is 3rd-order-sum-free if and only if System (4) does not admit two different solutions $(\alpha,\mathtt{x},\beta,\mathtt{z})$ and $(\alpha',\mathtt{x}',\beta',\mathtt{z}')$ in $\mathbb{F}_{2^n}^*\times\mathbb{F}_{2^n}\times\mathbb{F}_{2^n}^*\times\mathbb{F}_{2^n}$ with $\mathtt{x},\mathtt{x}+\alpha,\mathtt{z},\mathtt{z}+\beta$ distinct and $G_i(\mathtt{x})+G_i(\mathtt{x}')=G_i(\mathtt{x}+\alpha)+G_i(\mathtt{x}'+\alpha')=G_i(\mathtt{z})+G_i(\mathtt{z}')=G_i(\mathtt{z}+\beta)+G_i(\mathtt{z}'+\beta')\neq 0$.

Note that, given a solution $(\alpha,\beta,\mathtt{z})$ to the second equation in System (4), there exists $\mathtt{x}$ satisfying the first equation if and only if $\left(\frac{\beta}{\alpha}\right)^{2^i+1}\left(\left(\frac{\mathtt{z}}{\beta}\right)^{2^i}+\frac{\mathtt{z}}{\beta}+1\right)$ has trace 1 (which is a rather light condition). The difficultly is to handle the condition $G_i(\mathtt{x})+G_i(\mathtt{x}')=G_i(\mathtt{x}+\alpha)+G_i(\mathtt{x}'+\alpha')=G_i(\mathtt{z})+G_i(\mathtt{z}')=G_i(\mathtt{z}+\beta)+G_i(\mathtt{z}'+\beta')\neq 0$ when studying the existence of two solutions of the system, but it is plausible that, for every n and every $i<n/2$ such that $\gcd(i,n)=1$, K_i is not 3rd-order-sum-free, except maybe when n is too small for allowing pairs of solutions satisfying the conditions.

We leave this general question open. We checked by a computer investigation that $K_2(x)=x^{13}$ is 3rd-order-sum-free over $\mathbb{F}_{2^5}$, but is not over $\mathbb{F}_{2^7}$ nor over $\mathbb{F}_{2^9}$. Similarly, $K_3(x)=x^{57}$ is not 3rd-order-sum-free over $\mathbb{F}_{2^7}$ nor over $\mathbb{F}_{2^9}$, and $K_4(x)=x^{241}$ is not 3rd-order-sum-free over $\mathbb{F}_{2^9}$.

This example shows that kth-order-sum-freedom is a very strong criterion for $k\geq 3$, much more demanding (but not stronger in a mathematical sense) than for $k=2$, that is, than APNness, which can be proved for the Kasami function rather easily when n is odd, as shown in [16].

A big difference between kth-order-non-affineness and kth-order-sum-freedom is then that the former is weaker when k increases (note that for $k=n$, it just means that F is not an affine function) while the latter is more and more demanding when k increases from 2 to $\lfloor n/2 \rfloor$ (but lth-order-sum-freedom does not imply kth-order-sum-freedom when $k < l$). We shall say a little more in Subsection 4.2.

3.2 Relation of sum freedom with higher-order derivatives

Any k-dimensional affine subspace A of $\mathbb{F}_2^n$ has the form $a+ < a_1, \dots, a_k >$ where $a \in \mathbb{F}_2^n$ and $a_1, \dots, a_k$ are linearly independent in $\mathbb{F}_2^n$ over $\mathbb{F}_2$, and $\sum_{x \in A} F(x)$ equals then the value $D_{a_1} D_{a_2} \dots D_{a_k} F(a)$ of the so-called kth-order (discrete) derivative $D_{a_1} D_{a_2} \dots D_{a_k} F$, which is the iteration of the first-order derivative $D_a F(x) = F(x) + F(x+a)$. This is well-known. Hence, F is kth-order-sum-free if, and only if, every kth-order derivative $D_{a_1} \dots D_{a_k} F$ with $a_1, \dots, a_k$ $\mathbb{F}_2$-linearly independent never takes the zero value. This illustrates again the difficulty of proving that a given (n, n)-function is kth-order sum-free: if we for instance represent it as a polynomial over $\mathbb{F}_{2^n}$, we have to prove that some polynomial functions (the derivatives $D_{a_1} \dots D_{a_k} F$) do not vanish, which is in general quite hard. And indeed, for $k = 2$ already, the proofs by Dobbertin and his co-authors of the APNness of the known APN polynomial functions are quite difficult, and we have seen with the Kasami functions that, even when these proofs could be simplified, checking 3rd-order-sum-freedom may still be quite tough.
Another related method consists of showing that the restriction of F to any k-dimensional affine space A, viewed as a (k, m)-function through the choice of a basis of the vector space equal to the direction of A (all such (k, m)-functions are affine equivalent), has algebraic degree k, exactly, but this method seems hard to implement, except when k is close to n.

Remark 1. The work made in [23] about the Kasami Boolean bent functions $f_\lambda(x) = tr_n(\lambda K_i(x))$ (where λ is not a cube in $\mathbb{F}_{2^n}$) has some similarity with the kth-order-sum-freedom of the Kasami functions K_i that we studied above for $k = 3$; but it is in fact much simpler: it proves that the derivatives of orders $i-1$ and $i-2$ of $f_\lambda(x)$ do not completely vanish under some conditions on n. To prove this, the author had to calculate $D_{a_1} D_{a_2} \dots D_{a_k} f_\lambda$ and to prove that for any such λ, there exists x in $\mathbb{F}_{2^n}$ such that $D_{a_1} D_{a_2} \dots D_{a_k} f_\lambda(x) \neq 0$. For this, it is enough to show that at least one monomial (that the author could choose) in the univariate representation of this latter Boolean function has a nonzero coefficient, while showing kth-order sum-freedom by calculating the kth-order derivative leads to showing that the value of $D_{a_1} D_{a_2} \dots D_{a_k} F(x)$ is nonzero *for every* $x \in \mathbb{F}_{2^n}$, which needs to take into account all the monomials with their coefficients, and to make a work with them which seems very hard.

3.3 Existence of kth-order-non-affine functions and of kth-order-sum-free functions

The existence of kth-order-non-affine (n, n)-functions for every $k \geq 2$ is clear for every $n \geq k$, since all APN functions are kth-order-non-affine for every $2 \leq$

$k \leq n$. Moreover, given a kth-order-non-affine (n, m)-function F, any $(n, m+1)$-function obtained by adding any coordinate function to F is kth-order-non-affine; we deduce then the existence of kth-order-non-affine (n, m)-functions for every $m \geq n \geq k \geq 2$.

We know that differentially 2-uniform (n, m)-functions (that is, second-order-non-affine (n, m)-functions) do not exist for $m < n$ when $n > 2$. But for $k > 2$, the set of those triples (n, m, k) for which kth-order-non-affine (n, m)-functions exist is not clear in general. We leave open the determination of this region. Note that for some particular values of k, the situation is simple. For instance, when $k = n$, the existence of such functions is obvious whatever is m, and when n is even, $m \leq \frac{n}{2}$ and $k > \frac{n}{2}$, it is too since we know that bent Boolean functions cannot be affine on an affine space of dimension strictly larger than $\frac{n}{2}$, as shown in a theorem from [9] reported in [12, Theorem 14]; all bent functions are then kth-order-non-affine.

We shall see that kth-order-sum-freedom has a more complex behavior than kth-order-non-affineness, and even the question of the existence of functions satisfying it is not straighforward. We need then to address it first, for avoiding studying an empty class for $k > 2$. Let us show that the cube function (which is APN and then second-order-sum-free) is the first element of an infinite sequence of kth-order-sum-free (n, n)-functions.

Proposition 1. *Let $2 \leq k \leq n$ be integers. Let $P_k(x)$ be the power function x^{2^k-1} over $\mathbb{F}_{2^n}$. Denoting by G_k the set of bijections from $\{1, \ldots, k\}$ to $\{0, \ldots, k-1\}$, we have:*

$$D_{a_1} \ldots D_{a_k} P_k(x) = \sum_{\sigma \in G_k} \prod_{i=1}^{k} a_i^{2^{\sigma(i)}} = \prod_{l \in \mathbb{F}_2^k, l \neq 0} \left(\sum_{i=1}^{k} l_i a_i \right), \tag{5}$$

and P_k is kth-order-sum-free.

Proof. We have $2^k - 1 = \sum_{i=1}^{k} 2^{i-1}$, hence $P_k(x) = \prod_{i=1}^{k} L_i(x)$, where $L_i(x) = x^{2^{i-1}}$. It is well-known and easily shown by induction on k that, if $L_0, \ldots, L_{k-1}$ are linear functions, then for every $a_1, \ldots, a_k$ in $\mathbb{F}_{2^n}$, $D_{a_1} \ldots D_{a_k}(\prod_{i=0}^{k-1} L_i)(x) = \sum_{\sigma \in G_k} \prod_{i=1}^{k} L_{\sigma(i)}(a_i)$. We have then:

$$D_{a_1} \ldots D_{a_k} P_k(x) = \sum_{\sigma \in G_k} \prod_{i=1}^{k} a_i^{2^{\sigma(i)}}.$$

Each of the factors of $\prod_{l \in \mathbb{F}_2^k, l \neq 0} \left(\sum_{i=1}^{k} l_i a_i \right)$ (which are pairwise co-prime multivariate polynomials in $a_1, \ldots, a_k$) divides $D_{a_1} \ldots D_{a_k} P_k(x)$, since it is easily seen that $\sum_{\sigma \in G_k} \prod_{i=1}^{k} a_i^{2^{\sigma(i)}} = 0$ when $a_1 \ldots, a_k$ are not $\mathbb{F}_2$-linearly independent. The set of multivariate polynomials over $\mathbb{F}_{2^n}$ is an integral domain and a unique factorization domain, see e.g. [30]. Hence, $\prod_{l \in \mathbb{F}_2^k, l \neq 0} \left(\sum_{i=1}^{k} l_i a_i \right)$ divides $D_{a_1} \ldots D_{a_k} P_k(x)$. Since the two polynomials are monic and have the same degree $2^k - 1$, they are then equal. This proves (5) and completes the proof since this product is nonzero, the a_i's being linearly independent. □

As in the case of kth-order-non-affineness, given a kth-order-sum-free (n, m)-function F, any $(n, m+1)$-function obtained by adding any coordinate function to F is kth-order-sum-free. We deduce then from Proposition 1 the existence of kth-order-sum-free (n, m)-functions for every $m \geq n \geq k \geq 2$. Here also, for $m < n$, no second-order-sum-free function exists for $n > 2$, but for $k > 2$, the condition on n, m, k such that some (n, m)-functions can be kth-order-sum-free is not clear (however, when $k = n$, the existence is obvious whatever is m, and when $k = n-1$, it is easily seen that m needs to be at least 2, since if a Boolean function f has odd Hamming weight restrictions to the hyperplanes of equations $x_n = 0, x_n = 1, x_{n-1} = 0$ and $x_{n-1} = 1$, it cannot have odd Hamming weight restrictions to the hyperplanes of equations $x_n + x_{n-1} = 0$, and $x_n + x_{n-1} = 1$).

4 Properties of the two notions

Let us go into more details with the properties of the two notions that we briefly saw after introducing their definition.
We first state explicitly what we observed immediately after Definition 1 and study the converse:

Proposition 2. *For every $2 \leq k \leq n$ and m, if an (n, m)-function is kth-order-sum-free, then it is kth-order-non-affine.*

About the converse of this implication:
- for $k = 2$, it is of course valid, since the two notions coincide (with APNness),
- for $k \geq 3$, the converse of Proposition 2 is not true; there exist indeed, for every $n \geq k$ and every $m \geq 1$, kth-order-non-affine (n, m)-functions which are not kth-order-sum-free, because there are non-affine Boolean functions, even quadratic ones, which sum to zero, that is, which have an even Hamming weight. An interesting particular case in this regard is when k is a divisor of n and F is a polynomial function over $\mathbb{F}_{2^n}$ whose coefficients all belong to $\mathbb{F}_{2^k}$ (in other words, $F(x^{2^k})$ equals $(F(x))^{2^k}$ for every $x \in \mathbb{F}_{2^n}$; when $k = 1$, such F is called an idempotent). Then F maps the subfield $\mathbb{F}_{2^k}$ (which is a k-dimensional vector space) into itself, and if it maps $\mathbb{F}_{2^k}$ onto itself, that is, if it is a permutation of $\mathbb{F}_{2^k}$, then $\sum_{x \in \mathbb{F}_{2^k}} F(x) = 0$ and F is then not kth-order-sum-free while F can be kth-order-non-affine. For instance, an APN power (n, n)-function F cannot be kth-order-sum-free for k an odd divisor of n (we know from Dobbertin, as reported in [12], that F is then a permutation of $\mathbb{F}_{2^k}$). Of course, if k is even and such that F is a permutation of $\mathbb{F}_{2^k}$ (for instance, when F itself is a permutation), we have the same situation.

4.1 Algebraic degree

Recall that any (n, m)-function has an algebraic degree bounded above by some integer $d < n$ if, and only if, it sums to zero over every affine space whose dimension is strictly larger than d (this is well-known for Boolean functions, see e.g. [12], and it directly generalizes to (n,m)-functions). We have then, more generally than we observed above about Gold functions:

Proposition 3. *For every $2 \leq k \leq n$ and every m, all kth-order-sum-free (n,m)-functions have necessarily algebraic degree at least k (and this latter necessary condition is also sufficient if $k=n$).*

This makes a difference with kth-order-non-affineness, since all APN functions, among which are quadratic ones, are kth-order-non-affine for every $k \geq 2$.
In fact, an (n,m)-function F is kth-order-sum-free if, and only if, the restriction of F to any k-dimensional affine space, viewed as a k-variable function through the choice of a basis of the vector space equal to the direction of this affine space (i.e. such that the affine space is a coset - a translate - of the linear space), has algebraic degree k.

Remark. Since the algebraic degree of the indicator 1_A of any k-dimensional affine subspace A of $\mathbb{F}_2^n$ equals $n-k$ and the algebraic degree of the product of a Boolean function and a vectorial function is bounded above by the sum of their algebraic degrees, F cannot be kth-order-sum-free when $n-k+d_{alg}(F) < n$, since the algebraic degree of $1_A F$ is then smaller than n and $\sum_{x\in A} F(x) = \sum_{x\in\mathbb{F}_2^n} 1_A(x)F(x)$ equals then 0. This gives again that if F is kth-order-sum-free, then $d_{alg}(F) \geq k$, as in Proposition 3. It provides additionally that if $d_{alg}(F) = k$, then F is kth-order-sum-free if, and only if, $d_{alg}(1_A F) = d_{alg}(1_A) + d_{alg}(F)$, for every k-dimensional affine space A. We say then that F has no degree-drop k-dimensional affine space (see [15] where the case of Boolean functions is studied). $\diamond$

4.2 Monotonicity/non-monotonicity

Monotonicity of non-affineness We have seen in Section 3 that if a function is kth-order-non-affine then it is lth-order-non-affine for every $l \geq k$ (a slightly different way of seeing this is by observing that the restriction of every affine function to every affine subspace of its domain is affine). The notion is then monotonic. In particular, kth-order-non-affineness for $k \geq 3$ is a generalization (and a weakening) of APNness, as is differential uniformity, but differently.
The monotonicity of the notion is strict. For instance, there are third-order-non-affine functions which are not APN: given an APN (n,n)-function F and a point $a \in \mathbb{F}_2^n$, let $G(x) = \begin{cases} F(x) \text{ if } x \neq a \\ b \text{ if } x = a \end{cases}$, where b is chosen so that G is not APN (it is easy to find b; it is not even clear whether any APN function F and any points a and b can exist such that G is APN, see [7]). Function G is third-order-non-affine because, for every 3-dimensional affine space A, there exists an affine plane included in $A \setminus \{a\}$ and since G coincides with F on this affine plane, it is not affine on it; hence G is not affine on A.
We shall see in Subsection 5.1 that the multiplicative inverse function is also an example of a 3rd-order-non-affine function that is not APN, when n is even.

Non-monotonicity of sum freedom Propositions 1 and 3 imply the existence of functions that are kth-order-sum-free and not lth-order-sum-free for some $l \geq k$. Note also that kth-order-sum-freedom is not decreasing monotonic either (that is, preserved when we decrease k). For instance, take a non-APN (n,n)-function of algebraic degree n; then F is nth-order-sum-free and it is not second-order-sum-free.
We see that the behavior of kth-order-sum-freedom is pretty complex, while it is better adapted to withstand integral attacks (and in particular, higher order differential attacks) than kth-order-non-affineness.
However, there is some monotonicity of the notion: if for some n, a function F is kth-order-sum-free over $\mathbb{F}_2^n$, then for every $k \leq m \leq n$, the restriction of F to any m-dimensional affine space of $\mathbb{F}_2^n$ whose image set is an m-dimensional affine space of $\mathbb{F}_2^n$ is kth-order-sum-free. This implies for instance the monotonicity with respect to the divisibility partial order over n, of the notion restricted to polynomial functions with coefficients in a subfield $\mathbb{F}_{2^m}$.

4.3 Characterization by the Walsh transform

It is usual, when a notion is studied, to try to characterize it by the Walsh transform. Many important cryptographic properties of Boolean and vectorial functions can be translated in terms of the Walsh transform. For instance, when Chabaud and Vaudenay studied in [17] the notions of almost perfect nonlinearity and almost bentness, they characterized them by the Walsh transform (and after that, it took 24 years before a characterization could be found for differentially uniform functions in [11]). We give now characterizations of the two notions by the Walsh transform. They are rather complex; this was expected since both are more complex than APNness, and even a slight increase in the complexity of a notion implies a more important increase for its characterization.

***k*th-order-non-affineness** Given a k-dimensional affine subspace A (over $\mathbb{F}_2$) of $\mathbb{F}_2^n$, the restriction of $F : \mathbb{F}_2^n \to \mathbb{F}_2^m$ to A is affine if and only if, for every $v \in \mathbb{F}_2^m$, the Boolean function $v \cdot F$, where "$\cdot$" is some inner product in $\mathbb{F}_2^m$, is affine on A. According to the Parseval relation (which, for a k-variable Boolean function, writes $\sum_{u\in\mathbb{F}_2^k} W_f^2(u) = 2^{2k}$, see e.g. [12]) and to the inverse Walsh transform relation, this is equivalent to $\sum_{x\in A}(-1)^{v\cdot F(x)+u\cdot x} \in \{0, \pm 2^k\}$ for all $u \in \mathbb{F}_2^n$, where (by an abuse of notation), we also denote by "$\cdot$" some inner product in $\mathbb{F}_2^n$. Hence, the restriction of F to A is affine if and only if, for every $u \in \mathbb{F}_2^n$ and $v \in \mathbb{F}_2^m$, we have:

$$\Big(\sum_{x\in A}(-1)^{v\cdot F(x)+u\cdot x}\Big)^2\Big(2^{2k} - \Big(\sum_{x\in A}(-1)^{v\cdot F(x)+u\cdot x}\Big)^2\Big) = 0.$$

Note that this latter expression is always non-negative. Therefore, the restriction of F to A is affine if and only if:

$$\sum_{u\in\mathbb{F}_2^n, v\in\mathbb{F}_2^m}\Big(\sum_{x\in A}(-1)^{v\cdot F(x)+u\cdot x}\Big)^2\Big(2^{2k} - \Big(\sum_{x\in A}(-1)^{v\cdot F(x)+u\cdot x}\Big)^2\Big) = 0.$$

For every $v \in \mathbb{F}_2^m$, we have:

$$\sum_{u\in\mathbb{F}_2^n}\Big(\sum_{x\in A}(-1)^{v\cdot F(x)+u\cdot x}\Big)^2=\sum_{x,y\in A}(-1)^{v\cdot(F(x)+F(y))}\sum_{u\in\mathbb{F}_2^n}(-1)^{u\cdot(x+y)}=2^{n+k}.$$

Writing $A=a+E$, where $a\in\mathbb{F}_2^n$ and E is a k-dimensional vector space, the Poisson summation formula (see *e.g.* [12, Relation (2.41)]) writes $\sum_{x\in A}(-1)^{v\cdot F(x)+u\cdot x}=\pm 2^{k-n}\sum_{w\in u+E^\perp}(-1)^{a\cdot w}W_F(w,v)$, where $E^\perp=\{w\in\mathbb{F}_2^n;\forall x\in E, w\cdot x=0\}$, and therefore, we have:

$$\sum_{u\in\mathbb{F}_2^n,v\in\mathbb{F}_2^m}\Big(\sum_{x\in A}(-1)^{v\cdot F(x)+u\cdot x}\Big)^4=$$

$$2^{4k-4n}\sum_{u\in\mathbb{F}_2^n,v\in\mathbb{F}_2^m}\Big(\sum_{w\in u+E^\perp}(-1)^{a\cdot w}W_F(w,v)\Big)^4=$$

$$2^{4k-4n}\sum_{\substack{u\in\mathbb{F}_2^n,v\in\mathbb{F}_2^m\\(T_1,T_2,T_3,T_4)\in(E^\perp)^4}}(-1)^{a\cdot\sum_{i=1}^4 T_i}\prod_{i=1}^4 W_F(u+T_i,v).$$

We deduce:

Proposition 4. *For every $2\le k\le n$ and m, any (n,m)-function is kth-order-non-affine if and only if, for every $a\in\mathbb{F}_2^n$ and every k-dimensional vector subspace E of $\mathbb{F}_2^n$, we have:*

$$2^{n+m+3k}-2^{4k-4n}\sum_{\substack{u\in\mathbb{F}_2^n,v\in\mathbb{F}_2^m\\(T_1,T_2,T_3,T_4)\in(E^\perp)^4}}(-1)^{a\cdot\sum_{i=1}^4 T_i}\prod_{i=1}^4 W_F(u+T_i,v)>0.$$

***k*th-order-sum-freedom** Still taking $A=a+E$, where E is a k-dimensional $\mathbb{F}_2$-vector subspace of $\mathbb{F}_2^n$, we have $\sum_{x\in A}F(x)\neq 0$ if and only if we have: $\sum_{v\in\mathbb{F}_2^m}(-1)^{v\cdot\left(\sum_{x\in A}F(x)\right)}=0$. Hence, fixing E and letting a range over $\mathbb{F}_2^n$, we have $\sum_{x\in a+E}F(x)\neq 0$ for every $a\in\mathbb{F}_2^n$ if and only if:

$$\sum_{a\in\mathbb{F}_2^n}\left(\sum_{v\in\mathbb{F}_2^m}(-1)^{v\cdot\sum_{x\in a+E}F(x)}\right)^2=\sum_{\substack{a\in\mathbb{F}_2^n\\v,v'\in\mathbb{F}_2^m}}(-1)^{(v+v')\cdot\sum_{x\in E}F(a+x)}\tag{6}$$

equals 0, that is, according to the inverse Walsh transform formula, and denoting by $U=(u_x)_{x\in E}$ the elements of $(\mathbb{F}_2^n)^E$:

$$\sum_{\substack{a\in\mathbb{F}_2^n\\v,v'\in\mathbb{F}_2^m}}\sum_{U\in(\mathbb{F}_2^n)^E}\left(\prod_{x\in E}W_F(u_x,v+v')(-1)^{\sum_{x\in E}(a+x)\cdot u_x}\right)=\tag{7}$$

$$\sum_{U\in(\mathbb{F}_2^n)^E}\ \sum_{v,v'\in\mathbb{F}_2^m}\left(\prod_{x\in E} W_F(u_x,v+v')\right)\left(\sum_{a\in\mathbb{F}_2^n}(-1)^{\sum_{x\in E}(a+x)\cdot u_x}\right)=0,$$

that is:

$$\sum_{\substack{U\in(\mathbb{F}_2^n)^E\\ \sum_{x\in E}u_x=0}}\ \sum_{v,v'\in\mathbb{F}_2^m}\left(\prod_{x\in E} W_F(u_x,v+v')\right)(-1)^{\sum_{x\in E}x\cdot u_x}=0, \tag{8}$$

since $\sum_{a\in\mathbb{F}_2^n}(-1)^{\sum_{x\in E}(a+x)\cdot u_x}$ equals 0 if $\sum_{x\in E}u_x\neq 0$.

Let us now write $E=< a_1,\ldots,a_k >$. Then writing $\sum_{i=1}^k x_i a_i$ (where $x=(x_1,\ldots,x_k)\in\mathbb{F}_2^k$) instead of $x\in E$, Relation (8) becomes:

$$\sum_{\substack{U\in(\mathbb{F}_2^n)^{\mathbb{F}_2^k}\\ \sum_{x\in\mathbb{F}_2^k}u_x=0}}\ \sum_{v,v'\in\mathbb{F}_2^m}\left(\prod_{x\in\mathbb{F}_2^k} W_F\left(u_x,v+v'\right)\right)(-1)^{\sum_{x\in\mathbb{F}_2^k}(\sum_{i=1}^k x_i a_i)\cdot u_x} \tag{9}$$

$$=0.$$

When $a_1,\ldots,a_k$ are not $\mathbb{F}_2$-linearly independent, we have $\sum_{x\in E}F(a+x)=D_{a_1}\ldots D_{a_k}F(a)=0$ for every a and then the value corresponding to (6) equals 2^{n+2m} and Expression (7) equals $(2^n)^{2^k}$ times more, that is, has value $2^{(1+2^k)n+2m}$. The number of k-tuples $(a_1,\ldots,a_k)$ of linearly dependent elements equals $2^{kn}-(2^n-1)(2^n-2)\cdots(2^n-2^{k-1})$. Hence, F is kth-order-sum-free if, and only if, the sum for $(a_1,\ldots,a_k)$ ranging over $(\mathbb{F}_2^n)^k$ of Expression (9) is equal to $2^{(1+2^k)n+2m}\left(2^{kn}-(2^n-1)(2^n-2)\cdots(2^n-2^{k-1})\right)$. This sum equals:

$$\sum_{\substack{U\in(\mathbb{F}_2^n)^{\mathbb{F}_2^k}\\ \sum_{x\in\mathbb{F}_2^k}u_x=0}}\ \sum_{v,v'\in\mathbb{F}_2^m}\left(\prod_{x\in\mathbb{F}_2^k} W_F\left(u_x,v+v'\right)\right)\sum_{(a_1,\ldots,a_k)\in(\mathbb{F}_2^n)^k}(-1)^{\sum_{x\in\mathbb{F}_2^k}(\sum_{i=1}^k x_i a_i)\cdot u_x}=$$

$$\sum_{\substack{U\in(\mathbb{F}_2^n)^{\mathbb{F}_2^k}\\ \sum_{x\in\mathbb{F}_2^k}u_x=0}}\ \sum_{v,v'\in\mathbb{F}_2^m}\left(\prod_{x\in\mathbb{F}_2^k} W_F\left(u_x,v+v'\right)\right)\sum_{(a_1,\ldots,a_k)\in(\mathbb{F}_2^n)^k}\prod_{i=1}^k(-1)^{a_i\cdot(\sum_{x\in\mathbb{F}_2^k}x_i u_x)}=$$

$$\sum_{\substack{U\in(\mathbb{F}_2^n)^{\mathbb{F}_2^k}\\ \sum_{x\in\mathbb{F}_2^k}u_x=0}}\ \sum_{v,v'\in\mathbb{F}_2^m}\left(\prod_{x\in\mathbb{F}_2^k} W_F\left(u_x,v+v'\right)\right)\prod_{i=1}^k\left(\sum_{a\in\mathbb{F}_2^n}(-1)^{a\cdot(\sum_{x\in\mathbb{F}_2^k}x_i u_x)}\right)=$$

$$2^{nk}\sum_{\substack{U\in(\mathbb{F}_2^n)^{\mathbb{F}_2^k};\forall i=1,\ldots,k,\\ \sum_{x\in\mathbb{F}_2^k}x_i u_x=\sum_{x\in\mathbb{F}_2^k}u_x=0}}\ \sum_{v,v'\in\mathbb{F}_2^m}\left(\prod_{x\in\mathbb{F}_2^k} W_F\left(u_x,v+v'\right)\right).$$

Note that U may be identified with the (k,n)-function $x \mapsto U(x) = u_x$ and the condition $\forall i = 1, \dots, k; \sum_{x \in \mathbb{F}_2^k} x_i u_x = \sum_{x \in \mathbb{F}_2^k} u_x = 0$, is that each of its n coordinate functions is orthogonal to the k-variable constant function 1 and to all k-variable Boolean functions $x_1, \dots, x_k$, that is, belongs to the dual of the first-order Reed-Muller code $RM(1,k)$, that is, belongs to $RM(k-2,k)$. The characterization of kth-order-sum-freedom writes then (using that $v + v'$ ranges 2^m times over $\mathbb{F}_2^m$):

Proposition 5. *For every $2 \leq k \leq n$ and m, any (n,m)-function is kth-order-sum-free if and only if:*

$$\sum_{U \in [RM(k-2,k)]^n} \sum_{v \in \mathbb{F}_2^m} \left(\prod_{x \in \mathbb{F}_2^k} W_F\left(U(x), v\right) \right) =$$

$$2^{n(1+2^k-k)+m} \left(2^{kn} - (2^n-1)(2^n-2)\cdots(2^n-2^{k-1})\right).$$

Note that for $m = n$ and $k = 2$, Proposition 5 gives a characterization of APN (n,n)-functions, and since $RM(k-2,k)$ equals $\{(0,0,0,0),(1,1,1,1)\}$, the condition in this characterization writes:

$$\sum_{u \in \mathbb{F}_2^n} \sum_{v \in \mathbb{F}_2^n} W_F^4(u,v) = 2^{3n}\left(2^{2n} - (2^n-1)(2^n-2)\right) = 3 \cdot 2^{4n} - 2^{3n+1};$$

this is exactly the Chabaud-Vaudenay characterization [17].

Remark. Paradoxically (since the properties of kth-order-non-affineness are in general easier to show than those of kth-order-sum-freedom), it seems difficult to characterize kth-order-non-affineness by a single formula involving the Walsh transform, as we did for kth-order-sum-freedom. ◇

4.4 Invariance under equivalence

In Boolean function theory, when we study a property of (n,m)-functions, an important point is to determine the groups of permutations σ of $\mathbb{F}_2^n$ and τ of $\mathbb{F}_2^m$ such that, if F satisfies the property, then $\tau \circ F \circ \sigma$ does too, and more generally the groups of permutations Σ of $\mathbb{F}_2^n \times \mathbb{F}_2^m$ such that, if F satisfies the property and if Σ maps the graph of F to the graph of an (n,m)-function G, then G satisfies the property. We say that the composition by σ (resp. τ, Σ) preserves the property and this leads to a notion of equivalence between (n,m)-functions preserving the property. Let us determine the equivalences preserving kth-order-non-affineness and kth-order-sum-freedom (and being a priori the most general as such); this will show one more difference between the two introduced notions. We assume that σ, τ are affine functions since otherwise the affineness of an affine space A is not preserved when applying σ to A and the affineness/non-affineness of the restriction of F (resp. the fact that its sum of values equals zero or is nonzero) is not preserved when composing with τ. Also, we assume that Σ is an affine function.

Proposition 6. *For every $k \geq 2$, every $n \geq k$ and every m, the property of being kth-order-non-affine, for an (n,m)-function, is CCZ invariant.*

Proof. Let L be an affine automorphism of $\mathbb{F}_2^n \times \mathbb{F}_2^m$ and let F and G be two (n,m)-functions such that the graph $\{(x, G(x)); x \in \mathbb{F}_2^n\}$ of G equals the image by L of the graph $\{(x, F(x)); x \in \mathbb{F}_2^n\}$ of F. Let F_1 and F_2 be defined as recalled in Section 2: $F_1(x) = L_1(x, F(x))$ and $F_2(x) = L_2(x, F(x))$, where $L = (L_1, L_2)$. Recall that we have $G = F_2 \circ F_1^{-1}$. If F is not kth-order-non-affine, then let A be a k-dimensional affine subspace of $\mathbb{F}_2^n$ over which F is affine. Then F_1 is affine over A. Moreover, the image A' of A by F_1 is a k-dimensional affine subspace of $\mathbb{F}_2^n$, and F_1^{-1} is affine over A'. Besides, F_2 is affine over A. Then G is affine over A'. Hence CCZ equivalence preserves the fact of not being kth-order-non-affineness. This completes the proof, by contraposition. □

Proposition 7. *For every $k \geq 3$, the property of being kth-order-sum-free for an (n,m)-function is only EA invariant in general, and for $k = 2$, it is CCZ invariant.*

Proof. The notion is clearly EA invariant for every $k \geq 2$, $n \geq k$ and m, by contraposition again, since the fact that a function sums to zero over at least one k-dimensional affine space is preserved by affine equivalence and by the addition of affine functions. The notion is CCZ invariant for $k = 2$ since APNness is, see for instance [12, Subsection 3.4.1]). For $k \geq 3$, it is easy to find examples of kth-order-sum-free (n,n)-permutations whose compositional inverses are not kth-order-sum-free. For instance, in $\mathbb{F}_{2^5}$, the power function x^7 is third-order-sum-free as we saw with Proposition 1, while its inverse equals x^9 (indeed $9 \times 7 = 63 \equiv 1 \pmod{31}$) and is then not third-order-sum-free, since it is quadratic. □

5 The case of the multiplicative inverse function

The multiplicative inverse function is the function from the field $\mathbb{F}_{2^n}$ to itself whose univariate representation (see Section 2) equals x^{2^n-2}, also denoted by x^{-1} since the exponents live in $\mathbb{Z}/(2^n-1)\mathbb{Z}$, that is, the power function coinciding with the inverse function $x \mapsto \frac{1}{x}$ over $\mathbb{F}_{2^n}^*$ and which maps 0 to 0. Its algebraic degree equals $n-1$. It is used (with n even for computational reasons) in the S-boxes of many of the most important block ciphers such as AES. It contributes optimally to the resistance of ciphers using it as an S-box when n is odd (it is APN) and sub-optimally when n is even (it is differentially 4-uniform).

5.1 The kth-order-non-affineness of multiplicative inverse function

For n odd, since the inverse function is APN [36], it is kth-order-non-affine for every $k \geq 2$.

For n even, it is only differentially 4-uniform [36] and we need to study whether it is third-order-non-affine. Let a, b be any $\mathbb{F}_2$-linearly independent elements of $\mathbb{F}_{2^n}$. If x is $\mathbb{F}_2$-linearly independent of a, b, then $x^{-1} + (x+a)^{-1} + (x+b)^{-1} +$

$(x+a+b)^{-1} = \frac{ab(a+b)}{x(x+a)(x+b)(x+a+b)}$ does not vanish. If $x \in \mathbb{F}_{2^n}$ is $\mathbb{F}_2$-linearly dependent of a, b, we have that $x^{-1} + (x+a)^{-1} + (x+b)^{-1} + (x+a+b)^{-1} = \frac{1}{a} + \frac{1}{b} + \frac{1}{a+b} = \frac{b}{a(a+b)} \left(\left(\frac{a}{b}\right)^2 + \frac{a}{b} + 1 \right)$ equals 0 if, and only if, $a \in \{wb, w^2b\}$ where w is a primitive element of $\mathbb{F}_4$. Let A be any 3-dimensional affine space, then there exist $\mathbb{F}_2$-linearly independent elements a, b in the direction of A which are not such that $a \in \{wb, w^2b\}$ (indeed, b being chosen, the set $\{0, b, wb, w^2b\}$ is a vector space of dimension 2 only) and then the restriction of F to A is not affine. We deduce that F is third-order-non-affine, that is, kth-order-non-affine for every $k \geq 3$.

5.2 Sums of the values taken by the multiplicative inverse function over affine spaces not containing 0

In this section, we obtain an explicit expression of the sum of the values of the multiplicative inverse function taken over affine subspaces of $\mathbb{F}_{2^n}$ that are not vector subspaces. This allows us to prove that such sum is always nonzero.

Let E_k be any k-dimensional vector subspace of $\mathbb{F}_{2^n}$. It is well-known that the polynomial $L_{E_k}(x) = \prod_{u \in E_k}(x+u)$ is a linearized polynomial. Let us write then:

$$L_{E_k}(x) = \sum_{i=0}^{k} b_{k,i} x^{2^i}, \tag{10}$$

where $b_{k,k} = 1$ and $b_{k,0} = \prod_{u \in E_k, u \neq 0} u \neq 0$.

Since we are in characteristic 2, the (polynomial) derivative of $L_{E_k}(x)$ equals $L'_{E_k}(x) = b_{k,0}$, while according to the classical formula on the derivative of a product, we have: $L'_{E_k}(x) = \sum_{u \in E_k} \prod_{v \in E_k, v \neq u}(x+v)$. For $x \in E_k$, this does not give any information (indeed, it gives $b_{k,0} = \prod_{v \in E_k, v \neq x}(x+v)$), but for $x \notin E_k$, this gives $b_{k,0} = \left(\sum_{u \in E_k} \frac{1}{x+u}\right) L_{E_k}(x)$. We have then:

Theorem 1. *For every $0 \leq k \leq n$, let E_k be any k-dimensional $\mathbb{F}_2$-subspace of $\mathbb{F}_{2^n}$ and let $F(x) = x^{2^n-2} = x^{-1}$ be the multiplicative inverse function over $\mathbb{F}_{2^n}$. We have:*

$$\forall x \notin E_k, \ \sum_{u \in E_k} F(x+u) = \sum_{u \in E_k} \frac{1}{x+u} = \frac{\prod_{u \in E_k, u \neq 0} u}{\prod_{u \in E_k}(x+u)} = \frac{b_{k,0}}{L_{E_k}(x)} \neq 0, \tag{11}$$

where $L_{E_k}(x) = \prod_{u \in E_k}(x+u)$ and $b_{k,0}$ is its coefficient of x.

Remark. For every $0 \leq k \leq n$, the restriction of the multiplicative inverse function to any k-dimensional affine subspace of $\mathbb{F}_{2^n}$ that is not a vector space has then maximal algebraic degree k, when viewed as a (k, n)-function. This property seems rare among all permutations over $\mathbb{F}_2^n$. Summing the values taken over affine spaces is probably a good way of distinguishing the multiplicative inverse function from random (n, n)-functions or permutations. This may allow to guess that a secret S-box used in a block cipher is equivalent to the inverse function. And if we know that an S-box used in a cipher is the multiplicative inverse function, it may allow to build a distinguisher. $\diamond$

Remark. In [27] is shown that the only affine spaces that are mapped by the inverse function to affine spaces are the multiplicative cosets of the subfields of $\mathbb{F}_{2^n}$ (0 included). The result of [27, Theorem 1], stating that the affine spaces that are not vector spaces cannot be mapped by the inverse function to affine spaces, is a direct consequence of Theorem 1 in the present paper. Indeed, the sum of the values in an affine space of dimension at least 2 equals 0. $\diamond$

5.3 Sums of the values taken by the multiplicative inverse function over linear subspaces

The case of subspaces containing 0 (that is, linear subspaces) is much more complex. Computer investigations made for $6 \leq n \leq 12$ show that the inverse function is not kth-order sum-free, whatever is $k \in \{3, \ldots, n-3\}$ (but we could see that for $n = 5$, it is 3rd-order-sum-free). Proving this for every n will probably need much work (we could not find a general result allowing to prove this; only partial results could be found).

Conclusion

We have introduced and studied two natural generalizations of almost perfect nonlinearity (APN), called kth-order-non-affineness and kth-order-sum-freedom. These notions are related to the resistance of block ciphers to integral attacks, and in weaker ways, to invariant subspace attacks and to Dobbertin's notion of normality. While, at the smallest possible order 2, these two generalizations both coincide with APNness, they behave for larger orders quite differently from each other (in particular, the latter is much stronger than the former) and from APNness. We have seen that their study poses interesting questions. We have stated the following open problems:

- Determine for $k > 2$, the set of those triples (n, m, k) for which kth-order-non-affine (n, m)-functions exist. Determine these functions.
- Determine for $k > 2$, the set of those triples (n, m, k) for which kth-order-sum-free (n, m)-functions exist. Determine these functions.
- Characterize the kth-order-non-affineness of vectorial functions by a single formula involving their Walsh transform.
- Prove that the Kasami APN functions are not 3rd-order-sum-free for $n \geq 6$.
- Study the kth-order-non-affineness and kth-order-sum-freedom. of the known infinite classes of APN functions.
- Prove that the multiplicative inverse function is not kth-order-sum-free for $k \in \{3, \ldots, n-3\}$ $(n \geq 6)$.

The (partial) study of the behavior of the multiplicative inverse function over $\mathbb{F}_{2^n}$ with respect to kth-order-sum-freedom, led to an interesting property of this particular but cryptographically important infinite class of functions: it sums to non-zero values over all affine subspaces of teir domain that are not linear subspaces. This property distinguishes it from random functions.

Acknowledgement. The author is grateful to Vincent Rijmen for his useful indications on the cryptographic relevance of the two notions studied in this paper, and to Stjepan Picek for his kind help with computations.

References

1. R. Aragona, M. Calderini, D. Maccauro and M. Sala. On some differential properties of Boolean functions. *Applicable Algebra in Engineering, Communication and Computing* 27 (5), pp. 359-372, 2016.
2. C. Beierle and C. Carlet. Gold functions and switched cube functions are not 0-extendable in dimension $n > 5$. *Designs, Codes and Cryptography* 91(2), pp. 433-449, 2023.
3. C. Beierle, G. Leander, and L. Perrin. Trims and extensions of quadratic APN functions. *Designs, Codes and Cryptography*, 90(4):10091036, 2022.
4. T. Beyne and M. Verbauwhede. Integral Cryptanalysis Using Algebraic Transition Matrices. *IACR Transactions on Symmetric Cryptology*, 2023 (4), pp. 244-269. See also *Cryptology ePrint Archive*, 2023.
5. E. Biham and A. Shamir. Differential Cryptanalysis of DES-like Cryptosystems. *Journal of Cryptology*, Vol 4, no.1, pp. 3-72, 1991.
6. C. Blondeau and K. Nyberg. Perfect nonlinear functions and cryptography. *Finite Fields and Their Applications* 32, pp. 120-147, 2015.
7. L. Budaghyan, C. Carlet, T. Helleseth and N. Kaleyski. On the Distance Between APN Functions. *IEEE Transactions on Information Theory* 66 (9), pp. 5742-5753, 2020. See also: Changing Points in APN Functions. *IACR Cryptology ePrint Archive* (http://eprint.iacr.org/) 2018/1217.
8. L. Budaghyan, N. Kaleyski, S. Kwon, C. Riera and P. Stănică. Partially APN Boolean functions and classes of functions that are not APN infinitely often. *Special Issue on Boolean Functions and Their Applications 2018, Cryptography and Communications* 12 (3), pp. 527-545.
9. C. Carlet. Two new classes of bent functions. *Proceedings of EUROCRYPT 1993, Lecture Notes in Computer Science* 765, pp. 77-101, 1994.
10. C. Carlet, On Cryptographic Complexity of Boolean Functions. *Finite Fields with Applications to Coding Theory, Cryptography and Related Areas* (Proceedings of the Conference Fq6), Springer-Verlag, Berlin, pp. 53-69, 2002.
11. C. Carlet. Characterizations of the differential uniformity of vectorial functions by the Walsh transform, *IEEE Transactions on Information Theory* 64 (9), pp. 6443-6453, 2018. (preliminary version available in *IACR Cryptology ePrint Archive* http://eprint.iacr.org/ 2017/516, 2017).
12. C. Carlet. Boolean Functions for Cryptography and Coding Theory. Monograph in *Cambridge University Press*, 562 pages, 2021.
13. C. Carlet. On the properties of the Boolean functions associated to the differential spectrum of general APN functions and their consequences. *IEEE Transactions on Information Theory* 67(10), pp.6926-6939, 2021.

14. C. Carlet, P. Charpin, and V. Zinoviev. Codes, bent functions and permutations suitable for DES-like cryptosystems. *Designs, Codes and Cryptography*, 15 (2), pp. 125-156, 1998.
15. C. Carlet, S. Feukoua, and A. Sălăgean. On the algebraic degree stability of Boolean functions when restricted to affine spaces. To appear in the proceedings of the *Thirteenth International Workshop on Coding and Cryptography* WCC 2024.
16. C. Carlet, K. H. Kim, and S. Mesnager. A direct proof of APN-ness of the Kasami functions. *Designs, Codes and Cryptography*, vol. 89, p. 441-446, 2021.
17. F. Chabaud and S. Vaudenay. Links between Differential and Linear Cryptanalysis. *Proceedings of EUROCRYPT 1994, Lecture Notes in Computer Science* 950, pp. 356-365, 1995.
18. W.E. Clark, X.D. Hou and A. Mihailovs. The affinity of a permutation of a finite vector space. *Finite Fields and Their Applications* 13(1), pp. 80-112, 2007.
19. J. Daemen and V. Rijmen, *The Design of Rijndael: AES - The Advanced Encryption Standard.* Springer, 2002.
20. H. Dobbertin. Construction of bent functions and balanced Boolean functions with high nonlinearity. *Proceedings of Fast Software Encryption FSE 1994, Lecture Notes in Computer Science* 1008, pp. 61-74, 1995.
21. J. Daemen, L. Knudsen and V. Rijmen. The block cipher square. *Proceedings of Fast Software Encryption FSE 1997, Lecture Notes in Computer Science*, vol. 1267, pp. 149165, 1997.
22. P. Ellingsen, P. Felke, C. Riera, P. Stănică and A. Tkachenko. C-differentials, multiplicative uniformity, and (almost) perfect c-nonlinearity. *IEEE Transactions on Information Theory* 66(9), pp.5781-5789, 2020.
23. A.A. Frolova. The essential dependence of Kasami bent functions on the products of variables. *Journal of Applied and Industrial Mathematics* 7, pp.166-176, 2013.
24. P. Hebborn, B. Lambin, G. Leander and Y. Todo. Lower bounds on the degree of block ciphers. *Proceedings of ASIACRYPT 2020, Part I, Lecture Notes in Computer Science*, vol. 12491, pp. 537566, 2020.
25. L. Knudsen. Truncated and higher order differentials. *Proceedings of Fast Software Encryption FSE 1995, Lecture Notes in Computer Science* 1008, pp. 196-211, 1995.
26. L. Knudsen and D. Wagner. Integral cryptanalysis. *Proceedings of Fast Software Encryption FSE 2002, Lecture Notes in Computer Science* vol. 2365, pp. 112127, 2002.
27. N. Kolomeec and D. Bykov. On the image of an affine subspace under the inverse function within a finite field. To appear in *Designs, Codes and Cryptograhy.*
28. X. Lai. Higher order derivatives and differential cryptanalysis. *Proceedings of the "Symposium on Communication, Coding and Cryptography", in honor of J. L. Massey on the occasion of his 60'th birthday*, pp. 227-233, 1994.
29. B. Lambin, P. Derbez and P. Fouque. Linearly equivalent s-boxes and the division property. *Designs, Codes and Cryptography* 88 (10), pp. 22072231, 2020.
30. S. Lang. Algebra, Graduate Texts in Mathematics, 211 (Revised third ed.), New York: Springer-Verlag, 2002.
31. G. Leander, B. Minaud and S. Rønjom. A generic approach to invariant subspace attacks: Cryptanalysis of Robin, iSCREAM and Zorro. In *Annual International Conference on the Theory and Applications of Cryptographic Techniques*, pp. 254-283, 2015. Berlin, Heidelberg: Springer Berlin Heidelberg.
32. F. J. MacWilliams and N. J. Sloane. *The theory of error-correcting codes*, North Holland. 1977.

33. M. J. Mihaljevic, S. Gangopadhyay, G. Paul, H. Imai. Generic cryptographic weakness of k-normal Boolean functions in certain stream ciphers and cryptanalysis of grain-128. *Period. Math. Hung.* 65(2): 205-227, 2012.
34. K. Nyberg. Perfect non-linear S-boxes. *Proceedings of EUROCRYPT' 91, Lecture Notes in Computer Science* 547, pp. 378-386, 1992.
35. K. Nyberg. On the construction of highly nonlinear permutations. *Proceedings of EUROCRYPT' 92, Lecture Notes in Computer Science* 658, pp. 92-98, 1993.
36. K. Nyberg. Differentially uniform mappings for cryptography. *Proceedings of EUROCRYPT' 93, Lecture Notes in Computer Science* 765, pp. 55-64, 1994.
37. K. Nyberg and L. R. Knudsen. Provable security against differential cryptanalysis. *Proceedings of CRYPT0' 92, Lecture Notes in Computer Science* 740, pp. 566-574, 1993.
38. B. Sun, L. Qu and C. Li. New cryptanalysis of block ciphers with low algebraic degree. *Proceedings of FSE 2009, Lecture Notes in Computer Science* 5665, pp. 180-192, 2009.
39. H. Taniguchi. D-property for APN functions from $\mathbb{F}_2^n$ to $\mathbb{F}_2^{n+1}$. *Cryptography and Communications* 15, no. 3 , pp. 121, 2023.
40. Y. Todo. Structural evaluation by generalized integral property. *Proceedings of EUROCRYPT 2015, Lecture Notes in Computer Science* 9056, pp. 287-314, 2015.
41. M.R. Zaba, H. Raddum, M. Henricksen and E. Dawson. Bit-Pattern Based Integral Attack. *Proceedings of FSE 2008, Lecture Notes in Computer Science* 5086, pp. 363-381, 2008.