On vectorial functions mapping strict affine subspaces of their domain into strict affine subspaces of their co-domain, and the strong D-property

Claude Carlet[1,2] and Enrico Piccione[1]

[1]University of Bergen, Bergen, Norway
[2]University of Paris 8, Saint-Denis, France

Abstract

Given three positive integers $n < N$ and M, we study those functions $\mathcal{F}$ from the vector space $\mathbb{F}_2^N$ (possibly endowed with the field structure) to $\mathbb{F}_2^M$, which map at least one n-dimensional affine subspace of $\mathbb{F}_2^N$ into an affine subspace whose dimension is less than M, possibly equal to n. This provides functions from $\mathbb{F}_2^n$ to $\mathbb{F}_2^m$ for some m (and in some cases, permutations) that have a simple representation over $\mathbb{F}_2^N$ or over $\mathbb{F}_{2^N}$. We show that the nonlinearity of $\mathcal{F}$ must not be too large for allowing this and we observe that if it is zero, there automatically exists a strict affine subspace of its domain that is mapped by $\mathcal{F}$ into a strict affine subspace of its co-domain. In this case, we show that the nonlinearity of the restriction may be large. We study the other cryptographic properties of such restriction, viewed as an (n, m)-function (resp. an (n, n)-permutation).

We then focus on the case of an (N, N)-function $\mathcal{F}$ of the form $\psi(\mathcal{G}(x))$ where $\mathcal{G}$ is almost perfect nonlinear (APN) and ψ is a linear function with a kernel of dimension 1. We observe that the restriction of $\mathcal{G}$ to an affine hyperplane A has the D-property (introduced by Taniguchi after a result from Dillon) as an $(N-1, N)$-function, if and only if, for every such ψ, the restriction of $\mathcal{F}(x) = \psi(\mathcal{G}(x))$ to A is not an APN $(N-1, N-1)$-function. If this holds for all affine hyperplanes A, we say that $\mathcal{G}$ has the strong D-property. We note that not satisfying this cryptographically interesting property also has a positive aspect, since it allows to construct APN $(N-1, N-1)$-functions from $\mathcal{G}$. We give a characterization of the strong D-property for crooked functions (a particular case of APN functions) by means of their ortho-derivatives and we prove that the Gold APN function in dimension $N \geq 9$ odd does have the strong D-property (we also give a simpler proof that the strong D-property of the Gold APN function in even dimension $N \geq 6$ holds if and only if $N = 6$ or $N \geq 8$). Then we give a partial result on the Dobbertin APN power function, and on this basis, we conjecture that it has the strong D-property as well.

We then move our focus to two known infinite families of differentially 4-uniform $(N-1, N-1)$-permutations constructed as the restrictions of (N, N)-functions $\mathcal{F}(x) = \psi(\mathcal{G}(x))$ or $\mathcal{F}(x) = \psi(\mathcal{G}(x)) + x$ where ψ and $\mathcal{G}$ are as before, with the extra hypothesis that $\mathcal{G}$ is an APN permutation.

After a deeper investigation on these classes, we provide proofs (which were missing) that they are not APN in dimension $n = N - 1$ even.

1 Introduction

Given a power q of a prime, the known methods for designing infinite classes of permutations over the space $\mathbb{F}_q^n$ that admit a simple representation (of any form) are not numerous. One has been much studied: identifying $\mathbb{F}_q^n$ with the field $\mathbb{F}_{q^n}$ (thanks to the choice of a basis of the vector space $\mathbb{F}_{q^n}$ over $\mathbb{F}_q$), permutation polynomials over $\mathbb{F}_{q^n}$ provide such bijections having a simple representation (given by the chosen basis of the vector space $\mathbb{F}_{q^n}$ and the polynomial expression of the permutation). But permutation polynomials having good properties for applications such as cryptography and coding theory (the two most important properties being a large nonlinearity and a low differential uniformity) are not that numerous and this classical method has provided only a few interesting classes (see [18, 15]), that can be used in such applications. Another method which has been little investigated, surprisingly, is to find permutation polynomials $\mathcal{F}$ over $\mathbb{F}_{q^N}$ with $N > n$, or functions from $\mathbb{F}_{q^N}$ to itself, such that there exists an n-dimensional affine subspace A of the domain, that is mapped by $\mathcal{F}$ onto an affine subspace A' of the same dimension in the co-domain; we identify then A and A' with $\mathbb{F}_q^n$ through choices of bases and we obtain a permutation over $\mathbb{F}_q^n$ with a simple representation over $\mathbb{F}_{q^N}$. This representation consists again in a basis, but this time, of the affine subspace, which is in $\mathbb{F}_{q^N}$ and not in $\mathbb{F}_{q^n}$, and the polynomial expression of the permutation over $\mathbb{F}_{q^N}$, which is now a polynomial over $\mathbb{F}_{q^N}$ and not over $\mathbb{F}_{q^n}$. This representation is a little less simple than in the classical case, but it is still quite simple compared to a look-up table; it is also more informative. In this paper, we study the case $q = 2$ and we are also more generally interested in cases where the (n, n)-function is not necessarily bijective.

A setting that could seem restrictive but which is surprisingly difficult to study is when the (N, N)-function $\mathcal{F}$ (that is a function from $\mathbb{F}_2^N$ to itself) is equal to $\psi(\mathcal{G}(x))$ where $\mathcal{G}$ is almost perfect nonlinear (APN) and ψ is a linear function with a kernel of dimension 1. This setting was also explored by Beierle et al. in 2022 [3] to find new quadratic APN functions. One year later, Taniguchi introduced in [23] the D-property as a generalization for APN (N, M)-functions of a property proved by Dillon on APN (N, N)-functions and being that $\{\mathcal{F}(x) + \mathcal{F}(y) + \mathcal{F}(z) + \mathcal{F}(x + y + z) \colon x, y, z \in \mathbb{F}_2^N\} = \mathbb{F}_2^M$. Further studies of such property have been done by Abbondati et al. in [1]. A consequence of the work by Taniguchi in [23] is that the restriction of an APN (N, N)-function $\mathcal{G}$ to an affine hyperplane A has the D-property as an $(N - 1, N)$-function if and only if for every linear surjective $(N, N - 1)$-function ψ, the restriction of $\mathcal{F}(x) = \psi(\mathcal{G}(x))$ to A is not an APN $(N - 1, N - 1)$-function. We use this as a motivation for the introduction of the notion of the *strong D-property* of an (N, N)-function $\mathcal{G}$, meaning that the restriction of $\mathcal{G}$ to A has the D-property as an $(N - 1, N)$-function for all affine hyperplanes A. Such setting was partially investigated by the same Taniguchi and viewed as a positive result for some classes of functions (namely, power and quadratic functions; see also the introduction of Subsection 5.1 where we explain one of its interests); in our paper, we build upon the fact that its negation is also a rather positive property since it allows to construct a number of APN $(N-1, N-1)$-functions from $\mathcal{G}$. Therefore, it is important to study the strong D-property of all classes of functions because if they have it, they are stronger cryptographically than other APN functions, and if they do not, we can construct new APN functions in dimension $N-1$ and this is also important.

The first infinite family defined as the restriction of functions with zero nonlinearity to affine hyperplanes was constructed by the first author in 2011 [12] by using the multiplicative inverse function. It is composed of 4-uniform (n, n)-permutations with optimal algebraic degree $n-1$, and nonlinearity at least $2^{n-1}-2^{\frac{n}{2}+1}$ (that is not optimal) for n even and at least $2^{n-1}-\lfloor 2^{\frac{n}{2}+1}\rfloor-1$ for n odd. Three years after, in 2014, Li and Wang [22] constructed many families of 4-uniform (n, n)-permutations where n is even with optimal known nonlinearity $2^{n-1}-2^{\frac{n}{2}}$ and algebraic degree $\frac{n+2}{2}$, using the compositional inverse of the Gold APN function. We investigate these constructions deeply and prove that they do not produce APN permutations in dimension $n=N-1$ even. We will not study the family [12] for the case N even because, in that dimension, the multiplicative inverse function is not APN and this setting is out of the scope of this paper. The theory we develop for such proofs helps understanding the problem of constructing APN permutations in even dimension (for trying to solve the so-called big APN problem) with this method. We observe that if the (N, N)-permutations used for constructing these $(N-1, N-1)$-permutations have the strong D-property, then any restriction of the (N, N)-permutation to an affine hyperplane is non-APN. The converse of this implication is not true in general and we show evidence that proving the non-APNness of such classes of permutations can be easier than proving the strong D-property of the APN permutation $\mathcal{G}$. In practice, proving the strong D-property is a matter of showing that many systems of equations have at least one solution while we solve only those systems that are relevant for the construction of permutations in dimension $N-1$. We do this for the multiplicative inverse function in odd dimension and the compositional inverse of the Gold APN function. Given the importance of showing such nonexistence results, we believe that this is a good argument to conjecture that the inverse and Gold power permutations have the strong D-property in dimension N large enough. We leave the difficult proof of these conjectures for future work.

The paper is organized as follows: In Section 2, we give some preliminaries on vectorial Boolean functions. In Section 3, we discuss more generally the cryptographic properties of the restriction of any (so-called initial) (N, M)-function providing an (n, m)-function. The differential uniformity of the restriction is bounded above by the differential uniformity of the initial function. We give an explicit form of the Walsh transform and of the nonlinearity of the restriction. Then we discuss a sufficient condition such that the nonlinearity of the restriction is nonzero. In Section 4, we discuss the special case of (N, M)-functions having some affine components that is a sufficient condition for the existence of a strict affine subspace of its domain that is mapped into a strict affine subspace of its co-domain. We prove that, up to EA equivalence, we can write these functions in the form $\mathcal{F}(x)=\psi(\mathcal{G}(x))$ where ψ is linear and we can assume that $\mathcal{G}$ has nonzero nonlinearity for the case $M=N \geq 3$. With this easier-to-handle form, we determine some bounds on the cryptographic property of the restriction. This section has some intersection with [3], but a small one. In Section 5, we introduce the strong D-property of APN (N, N)-functions. We give a characterization for crooked functions and prove that the Gold APN function has the strong D-property for $N \geq 9$ odd (and thanks to Taniguchi's result for N even, we can address all cases). As a Corollary, we give a partial result on the strong D-property of the Dobbertin APN power function and we conjecture the strong D-property of this function. In Section 6, we study the infinite families introduced in [12, 22] and prove that they can never produce APN permutations in even dimension.

2 Preliminaries

Let $N, M \in \mathbb{N}$. We say that $\mathcal{F}$ is an (N, M)-function if $\mathcal{F}$ is a function from $\mathbb{F}_2^N$ (which can be identified with $\mathbb{F}_{2^N}$) to $\mathbb{F}_2^M$ (which can be identified with $\mathbb{F}_{2^M}$). When we do not wish to specify the values of N and M, we speak of a vectorial function. We say that $\mathcal{F}$ is a permutation over $\mathbb{F}_2^N$ if $\mathcal{F}$ is a bijective (N, N)-function. We say that f is a Boolean function over $\mathbb{F}_2^N$ if f is a $(N, 1)$-function.

A Boolean function f over $\mathbb{F}_2^N$ has a unique representation as a multivariate polynomial with coefficients in $\mathbb{F}_2$ and of degree at most N called the *algebraic normal form (ANF)*. The degree of the ANF of f is called the *algebraic degree* of f [15]. We can write an (N, M)-function as $\mathcal{F} = (f_1, f_2, \ldots, f_M)$, where the Boolean functions $f_1, f_2, \ldots, f_M$ are called the *coordinate functions* of $\mathcal{F}$. A *component function* (briefly, a component) of $\mathcal{F}$ is any nonzero linear combination of its coordinate functions. The algebraic degree of $\mathcal{F}$ is equal to the maximum algebraic degree among its coordinate functions (and then also, among its component functions). A vectorial Boolean function $\mathcal{F}$ is *affine*, *quadratic*, or *cubic* if its algebraic degree is respectively less than or equal to 1, 2, or 3. Moreover, $\mathcal{F}$ is *linear* if it is affine and $\mathcal{F}(0) = 0$. If we identify $\mathbb{F}_2^N$ with the finite field $\mathbb{F}_{2^N}$, then any function $\mathcal{F}$ over $\mathbb{F}_{2^N}$ is also uniquely represented as a univariate polynomial, $\mathcal{F}(x) = \sum_{i=0}^{2^N-1} c_i x^i$ where $c_i \in \mathbb{F}_{2^N}$, called the *univariate representation*. The algebraic degree of $\mathcal{F}$ is equal to the maximum Hamming weight of the binary expansion of the exponents i of the terms of the polynomial $\mathcal{F}(x)$ such that $c_i \neq 0$. The *monomial functions* x^i are also called *power functions* to avoid any confusion with the monomial functions involved in the ANF.

Two (N, M)-functions $\mathcal{F}$ and $\mathcal{F}'$ are called affine equivalent if one equals the other composed on the right by an affine permutation of $\mathbb{F}_2^N$ and on the left by an affine permutation over $\mathbb{F}_2^M$. More generally, they are called extended affine (EA) equivalent if one is affine equivalent to the sum of the other and of an affine (N, M)-function. Still more generally, they are called CCZ equivalent if the indicators of their graphs $\{(x, \mathcal{F}(x)) \colon x \in \mathbb{F}_2^N\}$ and $\{(x, \mathcal{F}'(x)) \colon x \in \mathbb{F}_2^N\}$ are affine equivalent (as $(N+M)$-variable Boolean functions). A particular case of CCZ equivalence is between any (N, N)-permutation and its compositional inverse. If a notion is preserved by affine (respectively, EA, CCZ) equivalence, we shall say that it is affine (respectively EA, CCZ) invariant.

We denote by the same symbol "$\cdot$" an inner product in $\mathbb{F}_2^N$ and an inner product in $\mathbb{F}_2^M$ (there will be no ambiguity). For any $\alpha \in \mathbb{F}_{2^N} \setminus \{0\}$, we can define the inner product $x \cdot y = \mathrm{Tr}_N(\alpha x y)$ over $\mathbb{F}_{2^N}$, where $\mathrm{Tr}_N(x) = \sum_{i=0}^{N-1} x^{2^i}$ is the absolute trace function from $\mathbb{F}_{2^N}$ to $\mathbb{F}_2$. If it is clear from the context, then we write $\mathrm{Tr} = \mathrm{Tr}_N$. For k, N such that $k|N$ we denote by $\mathrm{Tr}_k^N(x)$ the relative trace function from $\mathbb{F}_{2^N}$ to $\mathbb{F}_{2^k}$, equal to $x + x^k + x^{2k} \cdots + x^{N-k}$.

We define the adjoint operator in the context of vector spaces over $\mathbb{F}_2$. Let $\psi\colon \mathbb{F}_2^N \to \mathbb{F}_2^M$ be a linear function. The adjoint operator is the linear mapping $\psi^*\colon \mathbb{F}_2^M \to \mathbb{F}_2^N$ such that for all $a \in \mathbb{F}_2^N, b \in \mathbb{F}_2^M$, $\psi(a) \cdot b = a \cdot \psi^*(b)$. Since every linear form over a field $\mathbb{F}$ can be written in a unique way as $a \to a \cdot c$, we have indeed that $\psi^*(b)$ is defined as equal to the unique element c corresponding to the linear form $a \to \psi(a) \cdot b$. In this way, if we have chosen an inner product, then ψ^* is uniquely defined. Let E be a vector subspace of $\mathbb{F}_2^N$. We denote by $E^\perp$ the orthogonal of E with respect to the inner product "$\cdot$", equal to the vector space of all those $v \in \mathbb{F}_2^N$ such that $v \cdot e = 0$ for every $e \in E$. Let $u_1, \dots, u_n \in \mathbb{F}_2^N$. We define $E = \langle u_1, \dots, u_n \rangle$ as the vector space spanned by $u_1, \dots, u_n$. We say that $A \subseteq \mathbb{F}_2^N$ is respectively an affine line, or an affine plane, or an affine hyperplane if A is an affine space of dimension 1, or 2, or $N-1$.

Let $\mathcal{F}$ be an (N, M)-function. For any $u \in \mathbb{F}_2^N$ and $v \in \mathbb{F}_2^M$ we denote by $W_\mathcal{F}(u, v)$ the value at (u, v) of the Walsh transform of $\mathcal{F}$:

$$W_\mathcal{F}(u, v) = \sum_{x \in \mathbb{F}_2^N} (-1)^{v \cdot \mathcal{F}(x) + u \cdot x}.$$

The extended Walsh spectrum of $\mathcal{F}$ is the multiset of all the absolute values that the Walsh function assumes.

We shall recall two equalities (first discovered in [10]) satisfied by the Walsh transform related to affine subspaces. Let $v \in \mathbb{F}_2^M$, $a, b \in \mathbb{F}_2^N$, and E, E_0 be two vector subspaces of $\mathbb{F}_2^N$ such that $E \oplus E_0 = \mathbb{F}_2^N$. The Walsh transform satisfies the *Poisson summation formula*:

$$\sum_{u \in b + E^\perp} (-1)^{a \cdot u} W_\mathcal{F}(u, v) = |E^\perp| (-1)^{a \cdot b} \sum_{x \in a + E} (-1)^{v \cdot \mathcal{F}(x) + b \cdot x}. \tag{1}$$

The Walsh transform satisfies the *second-order Poisson summation formula*:

$$\sum_{u \in E^\perp} W_\mathcal{F}(u, v)^2 = |E^\perp| \sum_{a \in E_0} \left(\sum_{x \in a + E} (-1)^{v \cdot \mathcal{F}(x)} \right)^2. \tag{2}$$

The two main cryptographic parameters of a vectorial function are its nonlinearity and its differential uniformity, which both are CCZ invariants.

The nonlinearity of $\mathcal{F}$ equals by definition the minimum Hamming distance between the component functions $v \cdot \mathcal{F}$, $v \neq 0$, of $\mathcal{F}$ and the affine Boolean functions $u \cdot x + \epsilon$, $\epsilon \in \mathbb{F}_2$ over $\mathbb{F}_2^N$. It equals:

$$\mathrm{nl}(\mathcal{F}) = 2^{N-1} - \frac{1}{2} \max_{u \in \mathbb{F}_2^N, v \in \mathbb{F}_2^M \setminus \{0\}} |W_\mathcal{F}(u, v)|. \tag{3}$$

The nonlinearity should be large (as close to the maximum $2^{n-1} - 2^{\frac{n}{2}-1}$ as possible) for allowing the vectorial function to contribute to the resistance of the block cipher using it as a substitution box to the linear attack [15]. As a generalization of the nonlinearity, we have the d-th order nonlinearity of a vectorial Boolean function $\mathcal{F}$ denoted as $\mathrm{nl}_d(\mathcal{F})$ that is equal to the minimum Hamming distance between the nonzero components of $\mathcal{F}$ and the set $\mathbb{B}_{N,d}$ of Boolean functions over $\mathbb{F}_2^N$ with algebraic degree at most d (for $d = 1$ it is the same notion as nonlinearity). Moreover, we have that $\mathrm{nl}_d(\mathcal{F}) = 2^{N-1} - \frac{\omega_d}{2}$

where

$$\omega_d = \max_{g\in\mathbb{B}_{N,d}, v\in\mathbb{F}_2^M\setminus\{0\}} \left| \sum_{x\in\mathbb{F}_2^N} (-1)^{v\cdot\mathcal{F}(x)+g(x)} \right|.$$

The differential uniformity of $\mathcal{F}$ is the (positive and even) integer $\delta_\mathcal{F}$ defined as:

$$\delta_\mathcal{F} = \max_{a\in\mathbb{F}_2^N\setminus\{0\}, b\in\mathbb{F}_2^M} \delta_\mathcal{F}(a,b),$$

where $\delta_\mathcal{F}(a,b) = \left|\{x\in\mathbb{F}_2^N \mid D_a\mathcal{F}(x) = b\}\right|$ and $D_a\mathcal{F}(x) = \mathcal{F}(x+a)+\mathcal{F}(x)$ is the derivative of $\mathcal{F}$ through the direction $a\in\mathbb{F}_2^N\setminus\{0\}$. An (N,M)-function is called differentially δ-uniform if its differential uniformity is at most δ. The differential uniformity should be low (as close to the minimum 2 as possible) for allowing the vectorial function to contribute to the resistance of block cipher using it as a substitution box (in SPN, ”function” should be ”permutation”, and in a Feistel cipher, “(N,N)” can be “(N,M)”) to the differential attack [15]. If $\delta = 2$, we call $\mathcal{F}$ *almost perfect nonlinear (APN).*

A Boolean function f over $\mathbb{F}_2^N$ is called plateaued if its extended Walsh spectrum assumes only two values that are 0 and a positive number, which happens to be equal to 2^k for some $k \geq \frac{N}{2}$, because of the Parseval's relation [15] (after Corollary 5). Quadratic functions are plateaued. The integer 2^k is called the amplitude of f. Function f is called *bent* if $k=\frac{N}{2}$, *near-bent* if $k=\frac{N+1}{2}$, and semi-bent if $k=\frac{N}{2}+1$. A generalization of bent functions is *partially-bent* functions that are characterized by the property of having all their derivatives either constant or balanced. Partially-bent functions are also plateaued. A vectorial Boolean function is called respectively *plateaued*, *strongly plateaued*, and *bent* if all its components are respectively *plateaued*, *partially-bent*, and *bent*. An *almost bent (AB)* function $\mathcal{F}$ is an (N,N)-function that reaches the SCV bound [15, Theorem 6], that is such that $\mathrm{nl}(\mathcal{F}) = 2^{N-1} - 2^{\frac{N-1}{2}}$. AB functions have many interesting properties such as being APN and having all near-bent components; they can only exist in odd dimension N. *Crooked* functions are (N,N)-functions such that for any $a\in\mathbb{F}_2^N\setminus\{0\}$, the image set of $D_a\mathcal{F}$ is an affine hyperplane; equivalently, they are APN and strongly plateaued [15] (after Definition 68). Crooked functions share almost all the nice properties of quadratic APN functions and it is conjectured that the two notions coincide. It has been proven that there is no bijective crooked function in even dimension and that the only crooked monomials and binomials are quadratic [21, 4].

Let f be a Boolean function over $\mathbb{F}_2^N$, then f is said to be *n-normal* (resp. *n-weakly-normal*), if there exists an n-dimensional affine space A such that f is constant (resp. affine) on A.

Proposition 2.1 ([10])**.** *Let f be a Boolean function over $\mathbb{F}_2^N$. If f is n-weakly-normal, then* $\mathrm{nl}(f) \leq 2^{N-1} - 2^{n-1}$.

3 Cryptographic properties of restrictions of vectorial functions to affine spaces

Let $\mathcal{F}$ be an (N,M)-function such that there exists an affine space A of dimension n, that is mapped by $\mathcal{F}$ into an affine space A' of dimension m. We identify then A with $\mathbb{F}_2^n$ and A' with $\mathbb{F}_2^m$ through the choice of bases and we obtain an (n,m)-function. We shall denote by $\mathcal{F}_A$ one of the functions obtained this way. When we shall find such case of an affine space mapped by a function $\mathcal{F}$ into a strict affine space of the co-domain of $\mathcal{F}$, we shall of course be interested in the cryptographic properties of $\mathcal{F}_A$. But there are several possibilities of defining the affine space in which $\mathcal{F}(A)$ is included (hence, to choose the dimension m of the co-domain of $\mathcal{F}_A$). And if this affine space is taken too large, then the nonlinearity of $\mathcal{F}_A$ will be automatically zero, because when we see an (n,m)-function as an (n,m')-function with $m' > m$ by adding virtual coordinate functions (which equal the zero function if we identify $\mathbb{F}_2^m$ with $\mathbb{F}_2^m \times \{0\} \subset \mathbb{F}_2^{m'}$), this drops the nonlinearity to zero. So, if it is not specified otherwise, we shall assume that A' is the intersection of all the affine spaces that contain $\mathcal{F}(A)$.

Definition 3.1. *Let $\mathcal{F}$ be an (N,M)-function such that there exists an affine space $A = a + E$ (where E is a vector space) of dimension n, that is mapped by $\mathcal{F}$ into an affine space $A' = a' + E'$ (where E' is a vector space) of dimension m. We call then $\mathcal{F}$ an $(E,a,E',a')_{n,m}$ affine-to-affine mapping. We say that the tuple (ϕ, a, ψ, a') is a* representation *of $\mathcal{F}_A$ if*

$$\mathcal{F}_A(x) = \psi\left(\mathcal{F}(\phi(x) + a) + a'\right)$$

where ϕ is a linear bijective function from $\mathbb{F}_2^n$ to E, and ψ is a linear surjective (M,m)-function such that $\psi(E') = \mathbb{F}_2^m$.

Note that all the representations defined in Definition 3.1 are affine equivalent and if a function $\mathcal{F}'$ is affine equivalent to $\mathcal{F}$, then the resulting restriction of $\mathcal{F}'$ is affine equivalent to a restriction of $\mathcal{F}$ (if both are represented as (n,m)-functions).

3.1 Differential uniformity of restrictions

Concerning the differential uniformity, the situation is rather simple. Let $\mathcal{F}$ be an (N,M)-function that is an $(E,a,E',a')_{n,m}$ affine-to-affine mapping. It is clear that the differential uniformity of $\mathcal{F}_A$ where $A = a + E$ is given by

$$\delta_{\mathcal{F}_A} = \max_{\alpha \in E \setminus \{0\},\, \beta \in E'} \left| \{x \in A \,|\, \mathcal{F}(x+\alpha) + \mathcal{F}(x) = \beta\} \right|.$$

Observe that if $\mathcal{F}$ is differentially δ-uniform for some δ, then the restriction $\mathcal{F}_A$ is also differentially δ-uniform, since for every nonzero $\alpha \in E \setminus \{0\}$, $\beta \in E'$, we have

$$\#\{x \in A \,|\, \mathcal{F}(x+a) + \mathcal{F}(x) = b\} \leq \#\{x \in \mathbb{F}_2^N \,|\, \mathcal{F}(x+a) + \mathcal{F}(x) = b\}.$$

In particular, the restriction of an almost perfect nonlinear (APN) function is still APN (examples of such APN functions have been discussed in [14, 2]). We shall recall a useful characterization of the APN property.

Proposition 3.2 ([15])**.** *Let $\mathcal{F}$ be an (N,M)-function with $M \geq N \geq 3$. Then $\mathcal{F}$ is APN if and only if for all distinct $x,y,z \in \mathbb{F}_2^N$, we have $\mathcal{F}(x) + \mathcal{F}(y) + \mathcal{F}(z) \neq \mathcal{F}(x+y+z)$.*

3.2 The Walsh transform and nonlinearity of restrictions

Concerning the nonlinearity, the situation is also apparently simple: the nonlinearity of $\mathcal{F}_A$ equals the minimum Hamming distance between the components of $\mathcal{F}_A$ and the affine Boolean functions over A. But we need to define what is a component function of $\mathcal{F}_A$ and the situation is then a little more delicate. We also need a way to effectively calculate the nonlinearity. In practice, we can first try to relate the Walsh transform of the restriction to the Walsh transform of $\mathcal{F}$. The nonlinearity of the restriction of a Boolean function to an affine space has been studied in [24, 10], but without that a precise expression of the Walsh transform be exhibited. The results that we shall revisit were obtained in [24] in a complex way and in [10] by using the Poisson summation formula (1) and the second-order Poisson summation formula (2), which led to bounds and to the study of their cases of equality without needing a precise expression of the Walsh transform. Let us provide such a precise expression in the framework which is ours here, that is, for vectorial functions.

Remark 3.3. *Let ζ be any linear function and let ζ^* be the adjoint operator of ζ with respect to an inner product. We recall that $\operatorname{Im}\zeta^* = (\ker\zeta)^\perp$ and $\ker\zeta^* = (\operatorname{Im}\zeta)^\perp$.*

Lemma 3.4. *Let $\mathcal{F}$ be an (N, M)-function that is an $(E, a, E', a')_{n,m}$ affine-to-affine mapping and let $A = a + E$. Then for every representation (ϕ, a, ψ, a') of $\mathcal{F}_A$, we have $\operatorname{Im}\psi^* \oplus (E')^\perp = \mathbb{F}_2^M$. Moreover, for every $v' \in \mathbb{F}_2^M \setminus (E')^\perp$ there exists a representation (ϕ, a, ψ, a') of $\mathcal{F}_A$ such that $v' \in \operatorname{Im}\psi^*$.*

Proof. Let us prove that $\operatorname{Im}\psi^* \oplus (E')^\perp = \mathbb{F}_2^M$ for any representation (ϕ, a, ψ, a') of $\mathcal{F}_A$. Let $w' \in \operatorname{Im}\psi^* \cap (E')^\perp$ and $w \in \mathbb{F}_2^m$ be such that $\psi^*(w) = w'$. Suppose that $w' \neq 0$. Let $e' \in E'$, then $w \cdot \psi(e') = \psi^*(w) \cdot e' = w' \cdot e' = 0$ because $w' \in (E')^\perp$. Since $\psi(E') = \mathbb{F}_2^m$, we have that $w = 0$ and that $w' = 0$. This is a contradiction. So $\operatorname{Im}\psi^* \cap (E')^\perp = \{0\}$. Since $\operatorname{Im}\psi^*$ (resp. $(E')^\perp$) has dimension m (resp. $M - m$), we have that $\operatorname{Im}\psi^* \oplus (E')^\perp = \mathbb{F}_2^M$.

Let us prove the second part. Let $v' \in \mathbb{F}_2^M \setminus (E')^\perp$ and let (ϕ, a, ψ, a') be a representation of $\mathcal{F}_A$. If $v' \in \operatorname{Im}\psi^*$, there is nothing to prove. Otherwise, we will prove that there exists a linear function ν such that $v' \in \operatorname{Im}\nu^*$ and (ϕ, a, ν, a') is a representation of $\mathcal{F}_A$. Let E_0 be a vector space over $\mathbb{F}_2$ such that $v' \in E_0$ and $E_0 \oplus (E')^\perp = \mathbb{F}_2^M$. Then E_0 has dimension m. Let ζ be a linear function from $\mathbb{F}_2^m$ to $\mathbb{F}_2^M$ such that $\operatorname{Im}\zeta = E_0$ and consider $\nu = \zeta^*$. We claim that ν is such that $v' \in \operatorname{Im}\nu^*$ and that (ϕ, a, ν, a') is a representation of $\mathcal{F}_A$. Since $\operatorname{Im}\nu^* = \operatorname{Im}\zeta = E_0$, then $v' \in \operatorname{Im}\nu^*$. To prove that (ϕ, a, ν, a') is a representation of $\mathcal{F}_A$ we must prove that $\nu(E') = \mathbb{F}_2^m$. Since $\ker\nu = (\operatorname{Im}\nu^*)^\perp = E_0^\perp$ and $E_0^\perp \cap E' = (E_0 + (E')^\perp)^\perp = \{0\}$, then $\nu(E')$ has dimension m and this is enough to prove that $\nu(E') = \mathbb{F}_2^m$. □

Theorem 1. *Let $\mathcal{F}$ be an (N, M)-function that is an $(E, a, E', a')_{n,m}$ affine-to-affine mapping, let $A = a + E$, and let (ϕ, a, ψ, a') be a representation of $\mathcal{F}_A$. Then for all $u \in \mathbb{F}_2^n$, $v \in \mathbb{F}_2^m$*

$$W_{\mathcal{F}_A}(u, v) = \frac{(-1)^\epsilon}{2^{N-n}} \sum_{z \in E^\perp} (-1)^{z \cdot a} W_{\mathcal{F}}((\phi^{-1})^*(u) + z, \psi^*(v))$$

where $\epsilon = \psi^*(v) \cdot a' + a \cdot (\phi^{-1})^*(u)$ *and*

$$\mathrm{nl}(\mathcal{F}_A) = 2^{n-1} - \frac{1}{2^{N-n+1}} \max_{u' \in E_1,\, v' \in (E_2 \setminus \{0\})} \left| \sum_{z \in E^\perp} (-1)^{z \cdot a} W_{\mathcal{F}}(u'+z, v') \right|,$$

where $E^\perp \oplus E_1 = \mathbb{F}_2^N$ *and* $(E')^\perp \oplus E_2 = \mathbb{F}_2^M$. *Moreover, we can write the nonlinearity of* $\mathcal{F}_A$ *as*

$$\mathrm{nl}(\mathcal{F}_A) = 2^{n-1} - \frac{1}{2^{N-n+1}} \max_{u' \in \mathbb{F}_{2N},\, v' \in \mathbb{F}_2^M \setminus (E')^\perp} \left| \sum_{z \in E^\perp} (-1)^{z \cdot a} W_{\mathcal{F}}(u'+z, v') \right|.$$

Proof. Let $\mathcal{F}'(x) = \mathcal{F}(x+a) + a'$ and $\mathcal{F}_A = \psi \circ \mathcal{F}' \circ \phi$. First notice that ψ^* is injective because $\ker \psi^* = (\mathrm{Im}\, \psi)^\perp = (\mathbb{F}_2^m)^\perp = \{0\}$ and $(\phi^{-1})^*$ is also injective because $\ker(\phi^{-1})^* = (\mathrm{Im}\, \phi^{-1})^\perp = (\mathbb{F}_2^n)^\perp = \{0\}$. Let $u \in \mathbb{F}_2^n$, $v \in \mathbb{F}_2^m$ and set $u' = (\phi^{-1})^*(u), v' = \psi^*(v)$. We have:

$$W_{\mathcal{F}_A}(u,v) = \sum_{x \in \mathbb{F}_2^n} (-1)^{v' \cdot \mathcal{F}'(\phi(x)) + u \cdot x} = \sum_{y \in E} (-1)^{v' \cdot \mathcal{F}'(y) + u' \cdot y}.$$

By using the Poisson summation formula (1) we have that

$$W_{\mathcal{F}_A}(u,v) = \frac{1}{2^{N-n}} \sum_{z \in E^\perp} W_{\mathcal{F}'}(z+u', v').$$

We continue by writing the Walsh transform of $\mathcal{F}'$ in term of the Walsh transform of $\mathcal{F}$, that is $W_{\mathcal{F}'}(z+u',v') = (-1)^{a' \cdot v' + a \cdot u'}(-1)^{a \cdot z} W_{\mathcal{F}}(z+u',v')$.

Notice that we can exclude the case $v' = 0$ when we compute the nonlinearity of $\mathcal{F}_A$, since by definition we must take $v \neq 0$ and we saw that ψ^* is injective. So $v' \in \mathrm{Im}\, \psi^* \setminus \{0\}$. By using Lemma 3.4, we have that $v' \in \mathbb{F}_2^M \setminus (E')^\perp$ and we can set $E_2 = \mathrm{Im}\, \psi^*$. Let $E_1 \subseteq \mathbb{F}_2^N$ be a vector space such that $E^\perp \oplus E_1 = \mathbb{F}_2^N$. We can write u' as $u' = u_1 + u_2$, where $u_1 \in E_1$ and $u_2 \in E^\perp$, and consequently: $\left|\sum_{z \in E^\perp} (-1)^{z \cdot a} W_{\mathcal{F}}(u'+z,v')\right| = \left|\sum_{z \in E^\perp} (-1)^{z \cdot a} W_{\mathcal{F}}(u_1+z,v')\right|$. So we can assume $u' \in E_1$. The rest is clear. □

3.3 A sufficient condition to have $\mathrm{nl}(\mathcal{F}_A) \neq 0$

The case $\mathrm{nl}(\mathcal{F}) = 0$ is interesting (and we shall study it apart in Section 4): we shall see that $\mathcal{F}_A$ can have good nonlinearity, even when starting from a function $\mathcal{F}$ with zero nonlinearity. A direct consequence of Theorem 1 is the following relation

$$\mathrm{nl}(\mathcal{F}_A) \geq \mathrm{nl}(\mathcal{F}) - (2^{N-1} - 2^{n-1}) \tag{4}$$

that is already known from [24, 10]. Observe that by using relation (4), we have that a sufficient condition for having $\mathrm{nl}(\mathcal{F}_A) \neq 0$ is that $\mathrm{nl}(\mathcal{F}) > 2^{N-1} - 2^{n-1}$. But this property is impossible to satisfy with $m < M$ since if $\mathcal{F}$ maps A into an affine hyperplane, of equation, say, $v \cdot x + \epsilon = 0$, then the Boolean function $v \cdot \mathcal{F}(x)$ being constant over A, it is n-normal and Proposition 2.1 shows that this is impossible. This observation proves the following proposition.

Proposition 3.5. *Let N, M, n be positive integers such that $N \geq n$. Let $\mathcal{F}$ be an (N, M)-function. If $\mathrm{nl}(\mathcal{F}) > 2^{N-1} - 2^{n-1}$, then for every affine space $A \subseteq \mathbb{F}_2^N$ of dimension n we have that $\mathcal{F}(A)$ is not included in any affine space of dimension $m < M$.*

We are going to prove a sufficient condition for having $\mathrm{nl}(\mathcal{F}_A) \neq 0$ which will be weaker and then more useful.

Proposition 3.6. *Let $\mathcal{F}$ be an (N, M)-function that is an $(E, a, E', a')_{n,m}$ affine-to-affine mapping and let $A = a + E$. If $\mathrm{nl}(\mathcal{F}_A) = 0$, then there exist $v \in \mathbb{F}_2^M \setminus (E')^\perp$ and $u \in \mathbb{F}_2^N$ such that $|W_\mathcal{F}(u, v)| \geq 2^n$.*

Proof. We have $\mathrm{nl}(\mathcal{F}_A) = 0$ if and only if there exist $b \in \mathbb{F}_2^N$ and $v \in \mathbb{F}_2^M \setminus (E')^\perp$ such that $v \cdot \mathcal{F}(x) + b \cdot x$ is constant on A (this is by definition, and it can also be seen by using Theorem 1 and the Poisson summation formula (1), which shows that $\left|\sum_{x \in b+E^\perp} (-1)^{x \cdot a} W_\mathcal{F}(x, v)\right| = 2^N$ if and only if $|\sum_{x \in A} (-1)^{v \cdot \mathcal{F}(x) + b \cdot x}| = 2^n$). Let $f = v \cdot \mathcal{F}(x) + b \cdot x$, then f is an n-normal N-variable function, and therefore $\mathrm{nl}(f) \leq 2^{N-1} - 2^{n-1}$, by Proposition 2.1. So we can conclude that there exists $u \in \mathbb{F}_2^N$ such that $|W_\mathcal{F}(u, v)| \geq 2^n$. □

Remark 3.7. *By using Proposition 3.6, we have immediately a sufficient condition for $\mathrm{nl}(\mathcal{F}_A) \neq 0$ that is*

$$\max_{u \in \mathbb{F}_2^N,\, v \in \mathbb{F}_2^M \setminus (E')^\perp} |W_\mathcal{F}(u, v)| < 2^n.$$

This observation justifies the setting of the next section where we will assume that only some components have zero nonlinearity while the others can have any value for their nonlinearity.

4 Functions with affine components

Constructing an (N, M)-function $\mathcal{F}$ with no affine components that maps an affine space of dimension $n < N$ into an affine space of dimension $m < M$ is not that difficult. Let F be an (n, m)-function and G be an (n', m')-function both without affine components, then the $(n+n', m+m')$-function $\mathcal{F}$ defined as $(x, y) \mapsto (F(x), G(y))$ does not have affine components and maps an affine space $A = \mathbb{F}_2^n \times \{0\}^{n'}$ (resp. $A = \{0\}^n \times \mathbb{F}_2^{n'}$) of dimension n (resp. n') into an affine space $A' = \mathbb{F}_2^m \times \{0\}^{m'}$ (resp. $A' = \{0\}^m \times \mathbb{F}_2^{m'}$) of dimension m (resp. m'). However, this procedure does not produce really new functions since F and G are known. It is challenging to find examples of "interesting" (N, M)-functions $\mathcal{F}$ (having good cryptographic properties) with no affine components that map an affine space of dimension $n < N$ into an affine space of dimension $m < M$ and such that $\mathcal{F}_A$ has good cryptographic properties.

In this section, we will study the case where function $\mathcal{F}$ has affine components (that is when $\mathrm{nl}(\mathcal{F}) = 0$) because we can find automatically a strict affine subspace of its domain mapped to a strict affine subspace of its co-domain. Also, it seems interesting to us that, from a function that is bad, cryptographically, because it has zero nonlinearity, we can construct potentially a good function by restricting its domain. This renews the cryptographic interest of the known infinite classes of permutation polynomials having zero nonlinearity. We will prove that, up to EA equivalence, we can write $\mathcal{F}(x) = \psi(\mathcal{G}(x))$ where ψ is linear and we can assume that $\mathcal{G}$ has nonzero nonlinearity for the case $M = N \geq 3$. For any (N, M)-function $\mathcal{G}$, we will see that instead of studying restrictions of $\mathcal{G}$, we can study restrictions of functions of the form $\mathcal{F}(x) = \psi(\mathcal{G}(x))$ where ψ is linear. Moreover, we will be able to construct more functions, because if ψ is not surjective, then $\mathrm{nl}(\mathcal{F}) = 0$ (because the image set of $\mathcal{F}$ being then included in an affine hyperplane, a component function of $\mathcal{F}$ is then constant) and we are not constrained by the necessary condition of Proposition 3.5 as explained in Remark 3.7.

4.1 Functions mapping affine spaces to subsets of proper affine subspaces

The next proposition is a generalization of the simple following observation: assume that $\mathcal{F}$ has an affine component; for instance, assume that its last coordinate function f_M is affine, then $\mathcal{F}$ maps (without loss of generality up to affine equivalence) the affine space equal to the pre-image $f_M^{-1}(0)$ into the affine space $\{y \in \mathbb{F}_2^M; y_M = 0\}$.

Proposition 4.1. *Let $\mathcal{F}$ be an (N, M)-function. Let V be any subset of $\mathbb{F}_2^M$ such that $v \cdot \mathcal{F}$ is affine for every $v \in V$. Let $\ell\colon \mathbb{F}_2^M \to \mathbb{F}_2$ be any linear form and $A = \{x \in \mathbb{F}_2^N \mid \forall v \in V, v \cdot \mathcal{F}(x) = \ell(v)\}$. Then we have $A \neq \emptyset$ for some ℓ, and for any such ℓ, A is an affine space mapped by $\mathcal{F}$ into the affine space $A' = \{y \in \mathbb{F}_2^M \mid \forall v \in V, v \cdot y = \ell(v)\}$ with direction $\langle V\rangle^\perp$. Any translate $a + A$ for $a \in \mathbb{F}_2^N$ is also mapped into an affine space of direction $\langle V\rangle^\perp$.*

Proof. By definition, A equals the intersection of the affine spaces $\{x \in \mathbb{F}_2^N \mid v \cdot \mathcal{F}(x) = \ell(v)\}$, where v ranges over V. Such A is non-empty for any ℓ defined over V by $\ell(v) = v \cdot \mathcal{F}(x)$, where x is some fixed element in $\mathbb{F}_2^N$, and completed into a linear function over $\mathbb{F}_2^M$. Then A is an affine space. The image of A by $\mathcal{F}$ is clearly a subset of the affine space $\{y \in \mathbb{F}_2^M \mid \forall v \in V, v \cdot y = \ell(v)\}$, whose direction equals its homogeneous version, that is, $\langle V\rangle^\perp$. And any translate $a+A$ of A has the same form, by changing $\ell(v)$ into $\ell(v) + v \cdot (\mathcal{F}(a) + \mathcal{F}(0))$. Indeed, since $v \cdot \mathcal{F}$ is affine, we have $v \cdot \mathcal{F}(x + a) = v \cdot \mathcal{F}(x) + v \cdot \mathcal{F}(a) + v \cdot \mathcal{F}(0)$. Then, $\mathcal{F}(a + A)$ and $\mathcal{F}(A)$ are subsets of affine spaces with the same direction $\langle V\rangle^\perp$. □

Note that taking ℓ linear does not reduce the generality since it is necessary for allowing A to be non-empty. Moreover, observe that if $v \cdot \mathcal{F}$ is affine for every $v \in V$, then $v \cdot \mathcal{F}$ is affine for every $v \in \langle V\rangle$. Hence, we can then always assume that V is a vector space.

Remark 4.2. *As we already evoked it at the beginning of Section 3, we need to reduce the dimension of the co-domain of the restriction of a function to an affine space in such a way that we erase all its affine components, if we want the restriction to have a chance of having nonzero nonlinearity. More precisely, let $V = \{v \in \mathbb{F}_2^M \mid v \cdot \mathcal{F}$ is affine$\}$ (that is, let V be maximal); let W be a strict subspace of V, $\alpha \in \mathbb{F}_2^N$, and $B = \{x \in \mathbb{F}_2^N \mid \forall w \in W, w \cdot \mathcal{F}(x) = w \cdot \mathcal{F}(\alpha)\}$. Then $\mathrm{nl}(\mathcal{F}_B) = 0$, where the co-domain of $\mathcal{F}_B$ is an affine space with direction $W^\perp$. Indeed, let $v \in V \setminus W$. By using Lemma 3.4, we can choose a* *representation (ϕ, b, ψ, b') of $\mathcal{F}_B$ such that $v \in \operatorname{Im} \psi^*$. Since $v \cdot \mathcal{F}$ is affine, then also $v \cdot \mathcal{F}(\phi(x) + b)$ is affine and*

$$v \cdot \mathcal{F}(\phi(x) + b) = v' \cdot \psi\left(\mathcal{F}(\phi(x) + b)\right) = v' \cdot \psi(b') + v' \cdot \mathcal{F}_B(x)$$

where $v = \psi^*(v')$. Consequently $v' \cdot \mathcal{F}_B$ is affine and, since $v' \neq 0$ because $v \neq 0$, we conclude that $\operatorname{nl}(\mathcal{F}_B) = 0$.

Note that $\mathcal{F}_A$ can still have zero nonlinearity even if V is maximal, since a component function $f = v \cdot \mathcal{F}$ of $\mathcal{F}$ for $v \notin V$ can be non-affine, and its restriction f_A be affine.

4.2 Cryptographic properties of restrictions of functions with affine components

Before studying the cryptographic properties of restrictions of (N, M)-functions with affine components, let us put them in a form easing their study, and make a first observation.

Proposition 4.3. *Let $\mathcal{F}$ be an (N, M)-function. Let $V \subseteq \mathbb{F}_2^M$ be a vector space such that, for every $v \in V$, we have that $v \cdot \mathcal{F}$ is affine. Let ψ be any linear (M, M)-function with $\operatorname{Im} \psi = V^\perp$, then there exists an (N, M)-function $\mathcal{G}$, and an affine (N, M)-function $\mathcal{A}$ such that:*

$$\mathcal{F}(x) = \psi\left(\mathcal{G}(x)\right) + \mathcal{A}(x).$$

Suppose that $M = N \geq 3$ and V is the whole vector space of those $v \in \mathbb{F}_2^N$ such that $v \cdot \mathcal{F}$ is affine, then $\mathcal{G}$ can be taken such that $\operatorname{nl}(\mathcal{G}) \neq 0$ and additionally we have the following:

1. *Assuming that $v \cdot \mathcal{F}$ is non-constant for all $v \in V \setminus \{0\}$, we can take $\mathcal{A}(x) = x$.*
2. *Assuming that $v \cdot \mathcal{F}$ is constant for all $v \in V$, we can take $\mathcal{A} = 0$.*

Proof. Let $e_1, \ldots, e_M$ be the canonical basis of $\mathbb{F}_2^M$, composed by vectors of Hamming weight 1 and let "$\cdot$" be the inner product of $\mathbb{F}_2^M$ defined as $v \cdot w = v_1 w_1 + \cdots v_M w_M$ where $v = (v_1, \ldots, v_M), w = (w_1, \ldots, w_M) \in \mathbb{F}_2^M$. Let m be the dimension of the vector space $V^\perp$. Up to affine equivalence, we can assume that $V = \langle e_1, \ldots, e_{M-m} \rangle = \mathbb{F}_2^{M-m} \times \{(0, \ldots, 0)\}$. Then $V^\perp = \langle e_{M-m+1}, \ldots, e_M \rangle = \{(0, \ldots, 0)\} \times \mathbb{F}_2^m$ and $\mathcal{F} = (f_1, \ldots, f_M)$ is such that its firsts $M - m$ coordinates are affine functions. Let $\mathcal{A} = (a_1, \ldots, a_M)$ be the affine (N, M)-function such that $a_i = f_i$ if $i \leq M - m$ and $a_i = 0$ otherwise. Then the image of the function $\mathcal{F} + \mathcal{A}$ is contained in $V^\perp$ and there exists an (N, M)-function $\mathcal{G} = (g_1, \ldots, g_M)$ such that $\mathcal{F}(x) = \psi\left(\mathcal{G}(x)\right) + \mathcal{A}(x)$ where the i-th coordinate of $\psi(x)$ is x_i if $i > M - m$ and 0 otherwise. Therefore, $f_i = g_i$ for $i > M - m$. We are going to use this setting for the rest of the proof.

Let us prove that if $M = N \geq 3$ and V is the vector space of all $v \in \mathbb{F}_2^M$ such that $v \cdot \mathcal{F}$ is affine, then we can choose $\mathcal{G}$ such that $\operatorname{nl}(\mathcal{G}) \neq 0$. By construction $f_i = a_i$ if $i \leq N - m$ and $f_i = g_i$ otherwise, so the coordinate functions $g_1, \ldots, g_{N-m}$ can be chosen arbitrarily. By hypothesis, any nonzero linear combination of $g_{N-m+1}, \ldots, g_N$ is not affine. Let us show that by choosing appropriate $g_1, \ldots, g_{N-m}$, we can extend this to all $g_1, \ldots, g_N$ and we will have then that $\mathcal{G} = (g_1, \dots, g_N)$ has nonzero nonlinearity. Let $N - m < i \leq N$ and let $\bar{g}_i$ be the Boolean function obtained from g_i by removing all the terms of degree at most 1 in the algebraic normal form (ANF). Considering now the vector space $\mathbb{V}$ of all the Boolean functions that are either 0 or have only terms of degree strictly greater than 1 in their ANF, we have that $\mathbb{V}$ has dimension $\sum_{d=2}^{N} \binom{N}{d} = 2^N - N - 1$. Since $N \geq 3$, we have that $2^N - N - 1 > N$ and by completing the free family $\bar{g}_{N-m+1}, \dots, \bar{g}_N$, we can always find $\bar{g}_1, \dots, \bar{g}_{N-m} \in \mathbb{V}$ such that $\bar{g}_1, \dots, \bar{g}_N \in \mathbb{V}$ are linearly independent. This concludes the proof that $\mathcal{G}$ can have nonzero nonlinearity.

Let us prove 1. Since $v \cdot \mathcal{F} = v \cdot \mathcal{A}$ is non-constant for all $v \in V \setminus \{0\}$, then we can assume up to affine equivalence that $a_i = x_i$ for $i \leq N - m$ and that $a_i = 0$ for $i > N - m$. Let $\mathcal{L}(x) = \mathcal{A}(x) + x$. Then $\mathcal{L}$ vanishes over V and therefore $\psi \circ \mathcal{L} = \mathcal{L}$ because the i-th coordinate of $\psi(x)$ is x_i if $i > N - m$ and 0 otherwise. Therefore, we have that $\mathcal{F}(x) = \psi(\mathcal{G}(x)) + \mathcal{A}(x) = \psi(\mathcal{G}'(x)) + x$ where $\mathcal{G}' = \mathcal{G} + \mathcal{L}$. We conclude by observing that $\mathrm{nl}(\mathcal{G}') = \mathrm{nl}(\mathcal{G}) \neq 0$.

Let us prove 2. Since $v \cdot \mathcal{F} = v \cdot \mathcal{A}$ is constant for all $v \in V \setminus \{0\}$, then we can assume up to affine equivalence that $a_i = 0$ for $i \leq N - m$. So we have that $\mathcal{A} = 0$. □

Note that, in the framework of Proposition 4.3, the affine spaces A of Proposition 4.1 are all the affine spaces of the form $\{x \in \mathbb{F}_2^N \mid \forall v \in \operatorname{Im} \psi^{\perp},\ v \cdot \mathcal{A}(x) = \ell(v)\}$ and their images by $\mathcal{F}$ and by $\psi \circ \mathcal{G}$ have $\operatorname{Im} \psi$ for direction.

Remark 4.4. *Referring again to Proposition 4.3, consider the two functions $\mathcal{F}(x) = \psi(\mathcal{G}(x))$ and $\mathcal{F}'(x) = \psi(\mathcal{G}(x)) + \mathcal{A}(x)$. It is clear that the two are EA equivalent. Let A be equal to $\{x \in \mathbb{F}_2^N \mid \forall v \in \operatorname{Im} \psi^{\perp},\ v \cdot \mathcal{A}(x) = \ell(v)\}$ as in Proposition 4.1, then the two restrictions $\mathcal{F}_A$ and $\mathcal{F}'_A$ are EA equivalent if we consider the restriction of the codomain over an affine space with direction $\operatorname{Im} \psi$.*

Remark 4.5. *Let $\mathcal{G}$ be an (N, N)-function. Suppose there exists an affine n-dimensional subspace A of $\mathbb{F}_2^N$ such that $\mathcal{G}(A) \subseteq A'$ where A' is an m-dimensional subspace of $\mathbb{F}_2^M$. Without loss of generality, assume that $A' = E'$ is a vector space. For any linear (M, M)-function ψ such that $\psi(E') = \operatorname{Im} \psi$ has dimension m, we have that, by choosing the appropriate representations (see Definition 3.1), the two (n, m)-functions $\mathcal{G}_A$ and $\mathcal{F}_A$ are affine equivalent where $\mathcal{F}(x) = \psi(\mathcal{G}(x))$. In fact, we can assume that $\mathcal{F}_A = \psi_{E'} \circ \mathcal{G}_A$ where $\psi_{E'}$ is a linear (m, m)-permutation because E' and $\operatorname{Im} \psi$ have the same dimension.*

As a consequence of the previous remarks, studying the cryptographic properties of restrictions of functions of the form $\mathcal{F}(x) = \psi(\mathcal{G}(x))$ is not restrictive in our setting. In the general hypothesis of the next theorem we do not assume that there is an affine space mapped to the subset of a strict subspace of dimension $m < M$, but we let m to be equal to the dimension of $\operatorname{Im} \psi$ (that can also be the whole space if ψ is a permutation).

Theorem 2. *Let $\mathcal{G}$ be an (N, M)-function and ψ a linear (M, M)-function whose image has dimension m. Let A be any affine space with dimension n and direction E. Then the (N, M)-function $\mathcal{F}(x) = \psi(\mathcal{G}(x))$ and the (n, m)-function $\mathcal{F}_A$ have the following cryptographic properties:*

1. *For every $u \in \mathbb{F}_2^N$ and $v \in \mathbb{F}_2^M$, we have that $W_{\mathcal{F}}(u, v) = W_{\mathcal{G}}(u, \psi^*(v))$ and that $\mathrm{nl}(\mathcal{F}_A) \geq \mathrm{nl}(\mathcal{G}) - (2^{N-1} - 2^{n-1})$.*

2. *Let $a \in \mathbb{F}_2^N$ and $b \in \mathbb{F}_2^M$. If $b \notin \operatorname{Im}\psi$, then $\delta_{\mathcal{F}}(a,b) = \delta_{\mathcal{F}_A}(a,b) = 0$. If $b \in \operatorname{Im}\psi$, then for any $b' \in \mathbb{F}_2^M$ such that $\psi(b') = b$ we have that:*

$$\delta_{\mathcal{F}}(a,b) = \sum_{c \in \ker\psi} \delta_{\mathcal{G}}(a, b'+c),$$

and if $a \in E$, we have that

$$\delta_{\mathcal{F}_A}(a,b) = \sum_{c \in \ker\psi} \delta_{\mathcal{G}_A}(a, b'+c),$$

where $\mathcal{G}_A$ is the restriction of $\mathcal{G}$ to A with co-domain $\mathbb{F}_2^M$. Moreover, we have that $\delta_{\mathcal{G}} \leq \delta_{\mathcal{F}} \leq 2^{M-m}\delta_{\mathcal{G}}$ and $\delta_{\mathcal{G}_A} \leq \delta_{\mathcal{F}_A} \leq 2^{M-m}\delta_{\mathcal{G}_A}$.

Proof. Observe that the image of $\mathcal{F}$ is included in $\operatorname{Im}\psi$, so $\mathcal{F}_A$ can be represented as an (n,m)-function since n is the dimension of A and m is the dimension of $\operatorname{Im}\psi$.

Let us prove 1. Given $u \in \mathbb{F}_2^N$ and $v \in \mathbb{F}_2^M$, we have that $W_{\mathcal{F}}(u,v) = W_{\mathcal{G}}(u, \psi^*(v))$ because $v \cdot \psi(\mathcal{G}) = \psi^*(v) \cdot \mathcal{F}$. Because of Theorem 1 and the fact that the direction of $\mathcal{F}(A)$ is included $\operatorname{Im}\psi$, the nonlinearity of $\mathcal{F}_A$ is

$$2^{n-1} - \frac{1}{2^{N-n+1}} \max_{u \in \mathbb{F}_2^N,\, v \in \mathbb{F}_2^M \setminus (\operatorname{Im}\psi)^{\perp}} \left| \sum_{z \in E^{\perp}} (-1)^{z \cdot a} W_{\mathcal{F}}(u+z, v) \right|,$$

where $A = a + E$. Let $u \in \mathbb{F}_2^N$, $v \in \mathbb{F}_2^M \setminus (\operatorname{Im}\psi)^{\perp}$, then we have that

$$\begin{aligned} \left| \sum_{z \in E^{\perp}} (-1)^{z \cdot a} W_{\mathcal{F}}(u+z, v) \right| &= \left| \sum_{z \in E^{\perp}} (-1)^{z \cdot a} W_{\mathcal{G}}(u+z, \psi^*(v)) \right| \\ &\leq 2^{N-n} \max_{z \in E^{\perp}} \left| W_{\mathcal{G}}(u+z, \psi^*(v)) \right|. \end{aligned}$$

Since $v \notin (\operatorname{Im}\psi)^{\perp} = \ker\psi^*$, then $\psi^*(v) \neq 0$. So we can conclude that $\operatorname{nl}(\mathcal{F}_A) \geq \operatorname{nl}(\mathcal{G}) - (2^{N-1} - 2^{n-1})$.

Let us prove 2. Let $a \in \mathbb{F}_2^N$ and $b \in \mathbb{F}_2^M$, then the integer $\delta_{\mathcal{F}}(a,b)$ is the number of solutions $x \in \mathbb{F}_2^N$ of the equation:

$$\mathcal{F}(x) + \mathcal{F}(x+a) = \psi\left(\mathcal{G}(x) + \mathcal{G}(x+a)\right) = b, \tag{5}$$

which equals, by denoting $z = \mathcal{G}(x) + \mathcal{G}(x+a)$, the number of solutions $(x,z) \in \mathbb{F}_2^N \times \mathbb{F}_2^M$ of the system:

$$\begin{cases} \psi(z) = b \\ \mathcal{G}(x) + \mathcal{G}(x+a) = z \end{cases} \tag{6}$$

The first equation $\psi(z) = b$ has solutions if and only if $b \in \operatorname{Im}\psi$, and in that case, the set of solutions equals the affine space $b' + \ker\psi$ for some $b' \in \mathbb{F}_2^M$ such that $\psi(b') = b$. For every $c \in \ker\psi$, the number of solution to the equation $\mathcal{G}(x) + \mathcal{G}(x+a) = b' + c$ is $\delta_{\mathcal{G}}(a, b'+c)$, and consequently we have that $\delta_{\mathcal{F}}(a,b) = \sum_{c \in \ker\psi} \delta_{\mathcal{G}}(a, b'+c)$. Consider now the restriction $\mathcal{F}_A$ where A is an affine space with direction E. If $a \in E$ and $b \in \operatorname{Im}\psi$, we can obtain $\delta_{\mathcal{F}_A}(a,b)$ in a similar way. We still have that Equation (5) with unknown in A has the same number of solutions as System (6) with unknown in $A \times \mathbb{F}_2^M$. Since $b \in \operatorname{Im}\psi$, the set of solutions of the first equation of Equation (6) equals $b' + \ker\psi$ for some $b' \in \mathbb{F}_2^M$ such that $\psi(b') = b$. For every $c \in \ker\psi$, the number of solution to the equation $\mathcal{G}(x) + \mathcal{G}(x+a) = b' + c$ is exactly $\delta_{\mathcal{G}_A}(a, b' + c)$ where $\mathcal{G}_A$ is the restriction of $\mathcal{G}$ to A with co-domain $\mathbb{F}_2^M$. Consequently we have that $\delta_{\mathcal{F}_A}(a,b) = \sum_{c\in\ker\psi} \delta_{\mathcal{G}_A}(a, b'+c)$. The two bounds follow directly. □

The following proposition groups together two results that are known since a long time (at least in the folklore) and have been rediscovered several times (for instance, in [22, 23]). In our case, they will follow from Theorem 2.

Proposition 4.6. *Let $N \geq 4$, let $\mathcal{G}$ be an (N,N)-function, let ψ be a linear (N,N)-function where $n = N-1$ is the dimension of $\operatorname{Im}\psi$, and let $\mathcal{F}(x) = \psi(\mathcal{G}(x))$. For any affine hyperplane A of $\mathbb{F}_2^N$, the following hold:*

1. *If $\mathcal{G}$ is APN, then $\delta_{\mathcal{F}} = 4$. Conversely, if $\delta_{\mathcal{F}} = 4$, then $\mathcal{G}$ is differentialy 4-uniform.*

2. *If $\mathcal{G}$ is AB, then $\mathcal{F}_A$ is differentialy 4-uniform and has nonlinearity $2^{n-1} - 2^{\frac{n}{2}}$.*

Proof. Let us prove 1. If $\mathcal{G}$ is APN, then $\delta_{\mathcal{F}} \leq 4$ by Theorem 2. Since $\mathcal{F}$ has zero nonlinearity, then it cannot be APN [15, Proposition 161]. Conversely if $\delta_{\mathcal{F}} = 4$, then $\mathcal{G}$ is differentialy 4-uniform again by Theorem 2.

Let us prove 2. Using Theorem 1 and Theorem 2, each of the nonzero Walsh values of $\mathcal{F}_A$ is either $\pm 2^{\frac{n}{2}}$ or $\pm 2^{\frac{n}{2}+1}$. Since there is no bent (n,n)-function for $n \geq 3$, then $\mathrm{nl}(\mathcal{F}_A) = 2^{n-1} - 2^{\frac{n}{2}}$. □

Let $\mathcal{F}(x) = \psi(\mathcal{G}(x))$ be as in Proposition 4.6 and let A be an affine hyperplane. By Proposition 4.3, we can assume that $\mathcal{G}$ has nonzero nonlinearity. Moreover, to have that $\mathcal{F}_A$ is an APN $(N-1, N-1)$-function, it is necessary that $\mathcal{G}$ is at least differentialy 4-uniform. In the next section, we will investigate the case where $\mathcal{G}$ is APN and we will study sufficient conditions to conclude that $\mathcal{F}_A$ is APN.

Remark 4.7. *There exist examples of infinite families of differentially 4-uniform (N,N)-functions $\mathcal{F}$ and hyperplanes A of $\mathbb{F}_2^N$ mapped to subsets of hyperplanes of $\mathbb{F}_2^N$ and such that $\mathcal{F}_A$ is APN. Indeed, take an APN (n,n)-function F and define for instance $\mathcal{F}(x, x_{n+1}) = \Big(F(x) + x_{n+1}L(x), x_{n+1}\ell(x)\Big)$, with $x \in \mathbb{F}_2^n, x_{n+1} \in \mathbb{F}_2$, where (L, ℓ) is a linear $(n, n+1)$-function whose kernel has dimension at most 2 (this is not very different from the construction in [3] but we shall apply it here to reach differential 4-uniformity). Then the image of $A = \mathbb{F}_2^n \times \{0\}$ is included in A, and the equation $D_{(a,a_{n+1})}\mathcal{F}(x, x_{n+1}) = (b, b_{n+1})$ is equivalent to the system of equations* $\begin{cases} D_aF(x) + x_{n+1}L(a) + a_{n+1}L(x) = b + a_{n+1}L(a) \\ x_{n+1}\ell(a) + a_{n+1}\ell(x) = b_{n+1} + a_{n+1}\ell(a) \end{cases}$. *For $a = 0$ and $a_{n+1} = 1$, this system writes* $\begin{cases} L(x) = b \\ \ell(x) = b_{n+1} \end{cases}$ *and has at most 4 solutions. For $a \neq 0$, it writes* $\begin{cases} D_aF(x) + a_{n+1}L(x) = b + a_{n+1}L(a) \\ a_{n+1}\ell(x) = b_{n+1} + a_{n+1}\ell(a) \end{cases}$ *if $x_{n+1} = 0$ and* $\begin{cases} D_aF(x) + a_{n+1}L(x) = b + a_{n+1}L(a) + L(a) \\ a_{n+1}\ell(x) = b_{n+1} + (a_{n+1}+1)\ell(a) \end{cases}$ *if $x_{n+1} = 1$. So*

it is enough that the first equation in each of the two latter systems has at most two solutions. This is obtained for instance if $F(x) = x^3$ with $x \in \mathbb{F}_{2^n}$ and $L(x) = x$ (whatever is ℓ) since these equations have then degree 2. Other examples can be given.
There even exist examples of quadratic APN (N, N)-functions $\mathcal{F}$ having this property (see [2, 6]) but these are sporadic.

The following open questions have been already more or less considered in [3] (see Open Problems 4 and 5):

Open Question 1. *Does there exist any example of an infinite class of APN functions $\mathcal{F}$ mapping a hyperplane A into a hyperplane, and whose restriction $\mathcal{F}_A$ is also APN?*

Open Question 2. *Does there exist (possibly sporadic) non-quadratic APN functions mapping a hyperplane A into a hyperplane, and whose restriction $\mathcal{F}_A$ is also APN?*

5 APN $(N-1, N-1)$-functions as restrictions of (N, N)-functions with an affine component, and the D-property

In this section, we will discuss the problem of constructing APN $(N-1, N-1)$-functions as restrictions of (N, N)-functions with an affine component. We will show that this problem is closely related to the D-property of $(N-1, N)$-functions discussed by Taniguchi in [23]. This will motivate the introduction of the notion of strong D-property. We will investigate this property for crooked functions and for their compositional inverses (when they are bijective). Then we will prove that the Gold APN function has the strong D-property for N large enough. As a consequence, we will present a partial result on the Dobbertin APN function and we conjecture that it has the strong D-property.

To the best of our knowledge, the paper by Berierle, Leander, and Perrin [3] is the first that investigates the problem of constructing APN $(N-1, N-1)$-functions from APN (N, N)-functions. We shall emphasize some differences between their approach and ours. They use the term "restriction" of an (N, M)-function $\mathcal{G}$ to indicate any (n, m)-function of the form $\zeta \circ \mathcal{G} \circ \eta$ where η is an injective affine (n, N)-function and ζ is a surjective affine (M, m)-function. The only difference (up to affine equivalence) with our notion of restriction is that we impose that ζ is injective on $\mathcal{G}(\operatorname{Im}\eta)$ (see Definition 3.1). So restrictions in our sense, can be seen as a special case of restrictions in their sense. On the other hand, it is fairly simple to study restrictions in their sense using our terminology. Observe that we can write without loss of generality $\zeta = \zeta' \circ \psi$ where ψ is a linear (M, M)-function with $\operatorname{Im}\psi$ of dimension m and ζ' is an affine (M, m)-function injective on $\operatorname{Im}\psi$. Then $\zeta \circ \mathcal{G} \circ \eta = \zeta' \circ (\psi \circ \mathcal{G}) \circ \eta$ is a restriction of $\psi \circ \mathcal{G}$ in our sense. In our setting, specifying the kernel of ψ is very relevant for the study of the differential uniformity of restrictions (see Theorem 2), while this information could be overlooked when dealing with specific constructions. Moreover, to construct permutations as restrictions of functions we need to impose anyway that ζ is injective on the image of the chosen affine space through the function we are restricting.

In [3], they focus on the case $N = M$ and $n = m = N - 1$ and define the *trimming* operation on $\mathcal{G}$ to constructing an $(N-1, N-1)$-function, that can be described as choosing an affine hyperplane A, taking the restriction (also in our sense) $\mathcal{G}_A$ as an $(N-1, N)$-function and then discard one component of $\mathcal{G}_A$. They prove that this operation is EA equivalent to construct $(N-1, N-1)$-restrictions in their sense. Let $\mathcal{F}_A$ be a restriction (in our sense) of an (N, N)-function $\mathcal{F}(x) = \psi(\mathcal{G}(x))$ where A is an affine hyperplane, and ψ is a linear (N, N)-function with kernel of dimension 1. Such $(N-1, N-1)$-function $\mathcal{F}_A$ is a trim of $\mathcal{G}$ by the Berierle et al. [3] terminology. Indeed, any component $v' \cdot \mathcal{F}_A$ for some $v' \in \mathbb{F}_2^{N-1} \setminus \{0\}$ is equal (up to affine equivalence) to $\psi^*(v) \cdot \mathcal{G}_A$ for some $v \in \mathbb{F}_2^N \setminus \{0\}$, so we can obtain $\mathcal{F}_A$ by discarding a component $v_0 \cdot \mathcal{G}_A$ from $\mathcal{G}_A$ for some $v_0 \in \mathbb{F}_2^N \setminus \operatorname{Im} \psi^*$.
These observations show the relationship between [3] and our present work. But there is in fact little intersection between [3] and our paper (even in the present section), since in [3], the authors study specific constructions of quadratic APN functions (and we can see the difficulty of obtaining them), while we study general sufficient conditions allowing $\mathcal{F}_A$ to be APN. Our results are then complementary of those of [3].

A useful characterization for $\mathcal{F}_A$ to be APN when $\mathcal{G}$ is APN is that $\mathcal{G}(x) + \mathcal{G}(y) + \mathcal{G}(z) + \mathcal{G}(x + y + z) \neq c$ for all $x, y, z \in A$ where $c \in \mathbb{F}_2^N \setminus \{0\}$ and $\ker \psi = \langle c \rangle$. Indeed, it is a direct consequence of Theorem 2 because, $\mathcal{G}_A$ being APN, $\mathcal{F}_A$ is APN if and only if, for any $a \in E \setminus \{0\}$, we have $\delta_{\mathcal{G}_A}(a, b) = 0$ for some $b \in \mathbb{F}_2^N$ only when $\delta_{\mathcal{G}_A}(a, b + c) = 0$. This is equivalent to saying that for any $a \in E$ and $x, y \in A$ we have that $D_a\mathcal{G}(x) + D_a\mathcal{G}(y) \neq c$.

Lemma 5.1. *Let $\mathcal{G}$ be an APN (N, N)-function with $N \geq 3$, let ψ be a linear (N, N)-function where $\ker \psi = \langle c \rangle$ for $c \in \mathbb{F}_2^N \setminus \{0\}$, let $\mathcal{F}(x) = \psi(\mathcal{G}(x))$, and let A be an affine hyperplane. Then $\mathcal{F}_A$ is APN if and only if we have that $\mathcal{G}(x) + \mathcal{G}(y) + \mathcal{G}(z) + \mathcal{G}(x + y + z) \neq c$ for all $x, y, z \in A$.*

5.1 The strong D-property

It is known that for any APN (N, N)-function $\mathcal{G}$ and any $c \in \mathbb{F}_2^N \setminus \{0\}$ there exist $x, y, z \in \mathbb{F}_2^N$ such that $\mathcal{G}(x) + \mathcal{G}(y) + \mathcal{G}(z) + \mathcal{G}(x + y + z) = c$. This was proven by J. Dillon in a private communication reported in [15] (after Proposition 161). Using this as a motivation, Taniguchi in [23] called *D-property* of an (N, M)-function $\mathcal{G}$, the fact that $\{\mathcal{G}(x) + \mathcal{G}(y) + \mathcal{G}(z) + \mathcal{G}(x + y + z) \colon x, y, z \in \mathbb{F}_2^N\} = \mathbb{F}_2^M$. If $N \neq M$, it is not true that all differentially 2-uniform (N, M)-functions have the D-property. When $M = N + 1$, the property is very relevant to our setting. Consider an APN (N, N)-function $\mathcal{G}$ and its restriction $\mathcal{G}_A$ to an affine hyperplane A. Observe that according to Lemma 5.1 if $\mathcal{G}_A$ has the D-property as an $(N-1, N)$-function, then we cannot construct an APN $(N-1, N-1)$-function. This observation can be also seen as a consequence of [23, Lemma 3] because $\mathcal{G}_A$ is APN. This discussion motivates the following definition of *strong D-property*.

Definition 5.2 (strong D-property)**.** *We say that an (N, N)-function $\mathcal{G}$ has the strong D-property if we have that*

$$\{\mathcal{G}(x) + \mathcal{G}(y) + \mathcal{G}(z) + \mathcal{G}(x + y + z) \colon x, y, z \in A\} = \mathbb{F}_2^N,$$

for all affine hyperplanes A of $\mathbb{F}_2^N$.

We checked that all APN power functions in dimension N between 8 and 25 have the strong D-property.

Open Question 3. *Do all APN power functions have the strong D-property?*

Examples of APN functions that do not have the strong D-property are some sporadic examples such as x^3 in dimensions 3 and 5, and all the quadratic APN functions with nonlinearity 2^{N-2} in N variables (see Proposition 5.7 below); some sporadic ones being known.

Open Problem 1. *Find an infinite class of APN functions that do not have the strong D-property.*

If $\mathcal{G}$ is APN, then satisfying this property can be seen as a nice feature because the sums of the values of $\mathcal{G}$ taken over hyperplanes present then some uniformity in their distribution and this kind of random behavior may help ciphers using $\mathcal{G}$ as an S-box to resist some attacks (e.g. integral attacks; see [20]). Moreover, such property is stronger than the D-property of an APN (N, N)-function (and is then possibly not satisfied by a given APN (N, N)-function). In the same time, not satisfying it may be seen as positive as well because it allows to construct at least one $(N-1, N-1)$-function from $\mathcal{G}$ (see Lemma 5.1). So either $\mathcal{G}$ has a good cryptographic property or we can construct APN functions in dimension $N-1$. In both cases, we learn something new about $\mathcal{G}$.

We observe that the strong D-property is EA invariant, which is straightforward, and it is not CCZ invariant, which is a little less intuitive; an example (that can be verified computationally) is the Gold APN function x^3 over $\mathbb{F}_{2^5}$ that does not have the strong D-property, but $x^{\frac{1}{3}}$ has it over $\mathbb{F}_{2^5}$.

Taniguchi in [23] studies the D-property of $(N-1, N)$-functions constructed as the restrictions of APN (N, N)-functions to the linear hyperplane $\{x \in \mathbb{F}_{2^N} \mid \mathrm{Tr}(x) = 0\}$ (where we identify $\mathbb{F}_2^N$ and $\mathbb{F}_{2^N}$). The results obtained in [23] indicate that the strong D-property could be very common among quadratic functions and power functions.

Regarding power functions, we have the following remark that states that it is enough to verify the strong D-property on only one linear hyperplane (that we choose to be the space of elements with zero trace) and its complement.

Remark 5.3. *Let $A = \{x \in \mathbb{F}_{2^N} \mid \mathrm{Tr}(vx) = \epsilon\}$ where $\epsilon \in \mathbb{F}_2$ and $v \in \mathbb{F}_{2^N} \setminus \{0\}$. Let d be a positive integer, then for any affine plane $\pi \subseteq A$ we have that $\sum_{x\in\pi} x^d = v^{-d} \sum_{x\in\pi'} x^d$ where $\pi' = \{vx\colon x \in \pi\}$ is a plane contained in $A' = \{x \in \mathbb{F}_{2^N} \mid \mathrm{Tr}(x) = \epsilon\}$. So if $\{x^d+y^d+z^d+(x+y+z)^d \mid x, y, z \in A'\} = \mathbb{F}_{2^N}$, then $\{x^d + y^d + z^d + (x + y + z)^d \mid x, y, z \in A\} = v^d \cdot \mathbb{F}_{2^N} = \mathbb{F}_{2^N}$.*

For quadratic APN functions, we have the following proposition that allows us to verify the strong D-property on linear hyperplanes instead of on all hyperplanes.

Remark 5.4. *Let $E = \{x \in \mathbb{F}_{2^N} \mid \mathrm{Tr}(vx) = 0\}$ where $v \in \mathbb{F}_{2^N} \setminus \{0\}$ and let A be an affine hyperplane with direction E. Let $\mathcal{G}$ be a quadratic (N, N)-function and let $x, y, z \in A$. Set $a = x+y$ and $b = x+z$, then $\mathcal{G}(x)+\mathcal{G}(y)+\mathcal{G}(z)+\mathcal{G}(x+y+z) = D_aD_b\mathcal{G}(x) = \varphi_{\mathcal{G}}(a, b)$ where $\varphi_{\mathcal{G}}(a, b) = D_aD_b\mathcal{G}(0) = \mathcal{G}(a+b)+\mathcal{G}(a)+\mathcal{G}(b)+\mathcal{G}(0)$, since $D_aD_b\mathcal{G}$ is constant. Moreover, $a, b \in E$. So we have that $\{\mathcal{G}(x) + \mathcal{G}(y) + \mathcal{G}(z) + \mathcal{G}(x + y + z)\colon x, y, z \in A\} = \{\varphi_{\mathcal{G}}(a, b)\colon a, b \in E\}$.*

The following proposition follows from Remark 5.4 and Lemma 5.1.

Proposition 5.5. *Let $N \geq 3$, let $\mathcal{G}$ be a quadratic APN (N,N)-function, let ψ be a linear (N,N)-function where $\ker\psi = \langle c \rangle$ for $c \in \mathbb{F}_2^N \setminus \{0\}$, let $\mathcal{F}(x) = \psi(\mathcal{G}(x))$, and let A be an affine hyperplane with direction E. Then $\mathcal{F}_A$ is APN if and only if for all $a,b \in E$ we have that $\varphi_{\mathcal{G}}(a,b) \neq c$.*

The argument that we used for the proof of Proposition 5.5 cannot be extended for crooked functions since the fact that every second-order derivative is constant is a characterization of quadratic functions. If we try to apply the same approach to a crooked function $\mathcal{G}$, we are led to using [15, Corollary 18] (characterizing strongly plateaued functions by their second-order derivatives), but we cannot because x, y and z live in an affine space and the restriction of a plateaued function to an affine space is not necessarily plateaued. We will show however in Proposition 5.16 below that such extension exists, but it will require a more complicated argument.

Remark 5.6. *By combining Remark 5.3 and Remark 5.4, it is enough for Gold functions to verify the strong D-property on the linear hyperplane $\{x \in \mathbb{F}_{2^N} \mid \mathrm{Tr}(x) = 0\}$ (and they are the only functions, up to EA equivalence, for which we can do this).*

Regarding quadratic APN (N,N)-functions that have the strong D-property, we can give a lower bound on their nonlinearity. However, this is useful only for the case N even because in the odd case, all quadratic APN functions are AB.

Proposition 5.7. *Let $\mathcal{G}$ be a quadratic APN function in even dimension N. If $\mathcal{G}$ has the strong D-property, then $\mathrm{nl}(\mathcal{G}) > 2^{N-2}$.*

Proof. If $\mathrm{nl}(\mathcal{G}) \leq 2^{N-2}$, then we have that $\mathrm{nl}(\mathcal{G}) = 2^{N-2}$ because it is the minimum nonlinearity that a quadratic APN function can achieve since it is plateaued and has nonzero nonlinearity [15, Proposition 161]. It is proven in [14, Remark 12] that if a quadratic APN (N,N)-function $\mathcal{G}$ is such that $\mathrm{nl}(\mathcal{G}) = 2^{N-2}$, then there exists an EA equivalent function $\mathcal{G}'$ to $\mathcal{G}$ such that $\mathcal{G}'$ maps some affine hyperplane A into an affine hyperplane. So $\mathcal{G}'_A$ is an APN $(N-1,N-1)$-function and clearly it does not have the D-property if represented as an $(N-1,N)$-function. So $\mathcal{G}'$ does not have the strong D-property and the same holds for $\mathcal{G}$. □

Remark 5.8. *A big open problem on APN functions is whether they can have very low nonlinearity (we know they cannot have nonlinearity zero). The minimum known is 2^{N-2} for an N-variable APN function, achieved by some quadratic APN functions in dimension 6 [6] and 8 [2]. However, there is no clear indication of how common they are in higher dimension.*

Open Problem 2. *Find non-quadratic APN functions with nonlinearity 2^{N-2}, or less, if possible an infinite class.*

5.2 The strong D-property of crooked functions

We are going to study the strong D-property of crooked functions. We will see that the strong D-property of a crooked function $\mathcal{G}$ can be characterized by the Walsh transform of its ortho-derivative. From this characterization, we derive a sufficient condition for the strong D-property of a crooked function. In the end, we will present a sufficient condition for the strong D-property of an APN permutations with quadratic inverse.

Remark 5.9. *Let $\mathcal{G}$ be a crooked (N,N)-function with $N \geq 3$. Let $\pi_{\mathcal{G}}$ be the ortho-derivative of $\mathcal{G}$, that is the unique function such that $\pi_{\mathcal{G}}(0)=0$ and $\pi_{\mathcal{G}}(a) \cdot \varphi_{\mathcal{G}}(a,b)=0$ for all $a,b \in \mathbb{F}_2^N$ where $\varphi_{\mathcal{G}}(a,b)=\mathcal{G}(a+b)+\mathcal{G}(a)+\mathcal{G}(b)+\mathcal{G}(0)$. As discussed in e.g. [15] (after Definition 68), we have that $\mathcal{G}$ is strongly plateaued and if N is odd, then $\pi_{\mathcal{G}}$ is a permutation and $\mathcal{G}$ is almost bent (AB).*

In the following proposition, we give an expression for such Walsh transform.

Proposition 5.10. *Let $\mathcal{G}$ be a crooked (N,N)-function with $N \geq 3$. Let $\pi_{\mathcal{G}}$ be the ortho-derivative of $\mathcal{G}$. For any $u,v \in \mathbb{F}_2^N$ we have that:*

$$W_{\pi_{\mathcal{G}}}(u,v)=\sum_{a \in \mathbb{F}_2^N}(-1)^{u \cdot a}|\Lambda_{v,a}|+2-2^N(\delta_0(u)+\delta_0(v))$$

where $\Lambda_{v,a}=\{b \in \mathbb{F}_2^N \mid \varphi_{\mathcal{G}}(a,b)=v\}$.

Proof. Let $u,v \in \mathbb{F}_2^N$ and set:

$$\mu_{u,v}=\sum_{a,b,w \in \mathbb{F}_2^N}(-1)^{w \cdot(\varphi_{\mathcal{G}}(a,b)+v)+u \cdot a}.$$

We have that

$$\mu_{u,v}=\sum_{a \in \mathbb{F}_2^N}(-1)^{u \cdot a}\sum_{w \in \mathbb{F}_2^N}\sum_{b \in \mathbb{F}_2^N}(-1)^{w \cdot(\varphi_{\mathcal{G}}(a,b)+v)}=2^N\sum_{a \in \mathbb{F}_2^N}(-1)^{u \cdot a}|\Lambda_{v,a}|$$

since we know that $\sum_{w \in \mathbb{F}_2^N}(-1)^{w \cdot y}=2^N\delta_0(y)$.
For any $a \in \mathbb{F}_2^N \setminus \{0\}$, we have that $\sum_{b \in \mathbb{F}_2^N}(-1)^{w \cdot \varphi_{\mathcal{G}}(a,b)}$ equals 2^N if $w \in \langle \pi_{\mathcal{G}}(a) \rangle$ and 0 otherwise. By separating the cases (1) $a=0$, (2) $a \neq 0$ and $w=0$, (3) $a \neq 0$ and $w=\pi_{\mathcal{G}}(a)$, (4) $a \neq 0$ and $w \notin \langle \pi_{\mathcal{G}}(a) \rangle$, we then have:

$$\begin{aligned}\mu_{u,v}=&2^N\sum_{w \in \mathbb{F}_2^N}(-1)^{w \cdot v}+2^N\sum_{a \in \mathbb{F}_2^N \setminus \{0\}}(-1)^{u \cdot a}+2^N\sum_{a \in \mathbb{F}_2^N \setminus \{0\}}(-1)^{v \cdot \pi_{\mathcal{G}}(a)+u \cdot a}\\ =&2^{2N}\delta_0(v)+2^{2N}\delta_0(u)-2^N+2^N W_{\pi_{\mathcal{G}}}(u,v)-2^N.\end{aligned}$$

□

Remark 5.11. *Let $\mathcal{G}$ be a crooked (N,N)-function with $N \geq 3$. The next lemma will characterize the strong D-property by means of the ortho-derivative and the size of the sets $\Lambda_c=\bigcup_{a \in \mathbb{F}_2^N}\{a\} \times \Lambda_{c,a}$ where $\Lambda_{c,a}$ is defined as in Proposition 5.10. We give then here some preliminary observations on the cardinality of these sets $\Lambda_c=\{(a,b) \in (\mathbb{F}_2^N)^2 \mid \varphi_{\mathcal{G}}(a,b)=c\}$ where $c \in \mathbb{F}_2^N$. We observe that, since $\mathcal{G}$ is plateaued, then $|\Lambda_c|=|\{(a,b) \in (\mathbb{F}_2^N)^2 \mid D_aD_b\mathcal{G}(u)=c\}|$ for any $u \in \mathbb{F}_2^N$ [15, Theorem 18]. Therefore, $|\Lambda_c| \neq 0$ because $\mathcal{G}$ has the D-property. If $c=0$, we have that $|\Lambda_0|=3 \cdot 2^N-2$ [15, Proposition 172]. Otherwise, $|\Lambda_c|$ is divisible by 6 (which is true even if $\mathcal{G}$ is not APN). Indeed, if $(a,b) \in \Lambda_c$ then a,b are linearly independent and $(x,y) \in \Lambda_c$ for any distinct $x,y \in \{a,b,a+b\}$, so we have exactly 6 choices of ordered pairs (x,y) in each affine plane (deprived* *of 0)* $\{a, b, a+b\}$*, and the sets of pairs associated to distinct affine planes are disjoint.*

Let $\lambda^{\min}$ *and* $\lambda^{\max}$ *be respectively the minimum and the maximum among the cardinalities* $|\Lambda_c|$ *for* $c \in \mathbb{F}_2^N \setminus \{0\}$*. Since*

$$\sum_{c \in \mathbb{F}_2^N \setminus \{0\}} |\Lambda_c| = 2^{2N} - |\Lambda_0| = 2^{2N} - 3 \cdot 2^N + 2 = (2^N - 2)(2^N - 1),$$

then $\lambda^{\min} \leq 2^N - 2 \leq \lambda^{\max}$*. A characterization of* $\mathcal{G}$ *being AB is that* $\lambda^{\min} = 2^N - 2 = \lambda^{\max}$ *[15, Corollary 27]. If* N *is even, then* $\lambda^{\min} < 2^N - 2 < \lambda^{\max}$ *since* $\mathcal{G}$ *cannot be AB (note also that* $2^N - 2$ *is not divisible by* 6 *because* $2^{N-1} - 1$ *is divisible by* 3 *only if* N *is odd).*

Before addressing the characterization of the strong D-property of a crooked function, we need the following preliminary lemma.

Lemma 5.12. *Let* $\mathcal{G}$ *be a crooked* (N, N)*-function with* $N \geq 3$*. Let* $\pi_{\mathcal{G}}$ *be the ortho-derivative of* $\mathcal{G}$*. Let* $c, v \in \mathbb{F}_2^N \setminus \{0\}$*,* $\Gamma_{v,c}^{(1)} = \{a \in \mathbb{F}_2^N \mid c \cdot \pi_{\mathcal{G}}(a) = 0,\ v \cdot a = 1\}$*, and* $\Lambda_c = \{(a, b) \in (\mathbb{F}_2^N)^2 \mid \varphi_{\mathcal{G}}(a, b) = c\}$*. Then the following holds:*

1. *We have that* $|\Gamma_{v,c}^{(1)}| < \frac{|\Lambda_c|}{3}$ *holds if and only if there exists* $(a, b) \in \Lambda_c$ *with* $v \cdot a = v \cdot b = 0$*.*
2. *If there exists* $u \in \mathbb{F}_2^N$ *such that* $D_a D_b \mathcal{G}(u) = c$ *and* $v \cdot a = v \cdot b = 0$*, then for all* $u \in \mathbb{F}_2^N$ *there exist* $a, b \in \mathbb{F}_2^N$ *such that* $D_a D_b \mathcal{G}(u) = c$ *and* $v \cdot a = v \cdot b = 0$

Proof. 1. Let Γ_c be the set of all $a \in \mathbb{F}_2^N$ such that $(a, b) \in \Lambda_c$ for some $b \in \mathbb{F}_2^N$, then we have that $|\Gamma_c| = \frac{|\Lambda_c|}{2}$ because if $a \in \Gamma_c$ then $\{b \in \mathbb{F}_2^N \mid (a, b) \in \Lambda_c\}$ contains two elements exactly, since $\varphi_{\mathcal{G}}(a, b) = \varphi_{\mathcal{G}}(a, b')$ implies $D_a D_b \mathcal{G}(0) + D_a D_{b'} \mathcal{G}(0) = D_a D_{b+b'} \mathcal{G}(b) = 0$ and, since $\mathcal{G}$ is APN, can happen only if $b' = b$ or $b' = b + a$ (note that since c is nonzero, a is nonzero). Then $\Gamma_{v,c}^{(1)} = \{a \in \Gamma_c \mid v \cdot a = 1\}$ because if $v \cdot a = 1$ then $a \neq 0$ and so we have that $\varphi_{\mathcal{G}}(a, b) = c$ for some $b \in \mathbb{F}_2^N$ if and only if $c \cdot \pi_{\mathcal{G}}(a) = 0$. Observe that Γ_c can be partitioned in sets of the form $\{a, b, a+b\}$ such that $(a, b) \in \Lambda_c$. Indeed, this follows from the APN property because if we take $(a, b), (a', b') \in \Lambda_c$ and for instance $a = a'$ (resp. $a = b'$ or $a = a' + b'$) then we have that $\{a, b, a+b\} = \{a', b', a'+b'\}$. Observe that for any $(a, b) \in \Lambda_c$, we have that the cardinality $|\{a, b, a+b\} \cap \Gamma_{v,c}^{(1)}|$ is equal either to 0 or to 2 (indeed, the number of elements among a, b, and $a+b$ that are non-orthogonal to v is necessarily even). Then $|\Gamma_{v,c}^{(1)}| \leq \frac{2}{3} |\Gamma_c| = \frac{|\Lambda_c|}{3}$ with equality only if for all $\{a, b, a+b\} \subseteq \Gamma_c$ with $(a, b) \in \Lambda_c$ we have that $|\{a, b, a+b\} \cap \Gamma_{v,c}^{(1)}| = 2$. So $|\Gamma_{v,c}^{(1)}| < \frac{|\Lambda_c|}{3}$ if and only if there exists $(a, b) \in \Lambda_c$ with $|\{a, b, a+b\} \cap \Gamma_{v,c}^{(1)}| = 0$ that is such that $v \cdot a = v \cdot b = 0$.

2. Let $u \in \mathbb{F}_2^N$, then $\mathcal{G}_u(x) = \mathcal{G}(x+u)$ is also crooked. Set $\Lambda_c(u) = \{(a, b) \in (\mathbb{F}_2^N)^2 \mid \varphi_{\mathcal{G}_u}(a, b) = c\}$ and $\Gamma_{v,c}^{(1)}(u) = \{a \in \mathbb{F}_2^N \mid c \cdot \pi_{\mathcal{G}_u}(a) = 0,\ v \cdot a = 1\}$. By using 1, we have that $|\Gamma_{v,c}^{(1)}(u)| < \frac{|\Lambda_c(u)|}{3}$ if and only if there exist $a, b \in \mathbb{F}_2^N$ such that $\varphi_{\mathcal{G}_u}(a, b) = D_a D_b \mathcal{G}(u) = c$ and $v \cdot a = v \cdot b = 0$. To conclude the proof, we must show that, for any $u_1, u_2 \in \mathbb{F}_2^N$, we have that $|\Gamma_{v,c}^{(1)}(u_1)| < \frac{|\Lambda_c(u_1)|}{3}$ if and only if $|\Gamma_{v,c}^{(1)}(u_2)| < \frac{|\Lambda_c(u_2)|}{3}$. It follows from the fact that $|\Lambda_c(u_1)| = |\Lambda_c(u_2)|$ and

that $\Gamma^{(1)}_{v,c}(u_1) = \Gamma^{(1)}_{v,c}(u_2)$. The first equality holds by [15, Theorem 18] because $\mathcal{G}$ is plateaued and $\varphi_{\mathcal{G}_{u_i}}(a,b) = D_aD_b\mathcal{G}(u_i)$ for any $a,b \in \mathbb{F}_2^N$ and $i = 1,2$. The second equality holds because $\pi_{\mathcal{G}_{u_1}} = \pi_{\mathcal{G}_{u_2}}$ since $\mathcal{G}_{u_1}(x) = \mathcal{G}_{u_2}(x+u_1+u_2)$. □

With the following lemma, we give a characterization of the strong D-property for crooked functions that depends on their ortho-derivative.

Lemma 5.13. *Let $\mathcal{G}$ be a crooked (N,N)-function with $N \geq 3$. Let $\pi_{\mathcal{G}}$ be the ortho-derivative of $\mathcal{G}$. Then $\mathcal{G}$ has the strong D-property if and only if, for all $c, v \in \mathbb{F}_2^N \setminus \{0\}$, we have that the following strict inequality*

$$|\Gamma^{(1)}_{v,c}| < \frac{|\Lambda_c|}{3} \tag{7}$$

holds where $\Gamma^{(1)}_{v,c} = \{a \in \mathbb{F}_2^N \mid c \cdot \pi_{\mathcal{G}}(a) = 0,\ v \cdot a = 1\}$ and $\Lambda_c = \{(a,b) \in (\mathbb{F}_2^N)^2 \mid \varphi_{\mathcal{G}}(a,b) = c\}$.

Proof. Suppose that $|\Gamma^{(1)}_{v,c}| < \frac{|\Lambda_c|}{3}$ for all $c, v \in \mathbb{F}_2^N \setminus \{0\}$. Let A be an affine hyperplane, then there exists $v \in \mathbb{F}_2^N \setminus \{0\}$ and $u \in \mathbb{F}_2^N$ such that $A = \{x \in \mathbb{F}_2^N \mid v \cdot (x+u) = 0\}$; let $c \in \mathbb{F}_2^N \setminus \{0\}$, then since $|\Gamma^{(1)}_{v,c}| < \frac{|\Lambda_c|}{3}$ and by applying 1 of Lemma 5.12, we have that there exist $a, b \in \mathbb{F}_2^N$ such that $D_aD_b\mathcal{G}(u) = c$ and $v \cdot a = v \cdot b = 0$. So (changing u into x and taking $y = x+a$, $z = x+b$) we have that $\{\mathcal{G}(x) + \mathcal{G}(y) + \mathcal{G}(z) + \mathcal{G}(x+y+z) \colon x,y,z \in A\} = \mathbb{F}_2^N$ (to get zero, it is enough to set $x = y = z$). So $\mathcal{G}$ has the strong D-property.
Conversely, suppose that $\mathcal{G}$ has the strong D-property. Let $c, v \in \mathbb{F}_2^N \setminus \{0\}$. Since $\{\mathcal{G}(x) + \mathcal{G}(y) + \mathcal{G}(z) + \mathcal{G}(x+y+z) \colon x,y,z \in E\} = \mathbb{F}_2^N$ where $E = \langle v \rangle^{\perp}$, then there exist $x, y, z \in \mathbb{F}_2^N$ such that $\mathcal{G}(x) + \mathcal{G}(y) + \mathcal{G}(z) + \mathcal{G}(x+y+z) = c$ and $v \cdot x = v \cdot y = v \cdot z = 0$. Therefore, according to 2 of Lemma 5.12, for all $u \in \mathbb{F}_2^N$, there exist $a, b \in \mathbb{F}_2^N$ such that $D_aD_b\mathcal{G}(u) = c$ and $v \cdot a = v \cdot b = 0$. So by taking $u = 0$, we have that $|\Gamma^{(1)}_{v,c}| < \frac{|\Lambda_c|}{3}$ according to 1 of Lemma 5.12. □

Remark 5.14. *Thanks to Proposition 5.10, the condition in Lemma 5.13, for the strong D-property of a crooked (N,N)-function $\mathcal{G}$ can be expressed by means of the Walsh transform of $\pi_{\mathcal{G}}$. Indeed, let $c, v \in \mathbb{F}_2^N \setminus \{0\}$, $\Lambda_c = \{(a,b) \in (\mathbb{F}_2^N)^2 \mid \varphi_{\mathcal{G}}(a,b) = c\}$, $\Gamma_c = \{a \in \mathbb{F}_2^N \mid (a,b) \in \Lambda_c$ for some $b \in \mathbb{F}_2^N\}$, $\Gamma^{(\epsilon)}_{v,c} = \{a \in \Gamma_c \mid v \cdot a = \epsilon\}$ where $\epsilon \in \mathbb{F}_2$. Since*

$$\begin{aligned} W_{\pi_{\mathcal{G}}}(v,c) = &\sum_{a \in \mathbb{F}_2^N} (-1)^{v \cdot a} |\Lambda_{c,a}| + 2 = 2|\Gamma^{(0)}_{c,v}| - 2|\Gamma^{(1)}_{c,v}| + 2 \\ =&2|\Gamma_c| - 4|\Gamma^{(1)}_{c,v}| + 2 = |\Lambda_c| - 4|\Gamma^{(1)}_{c,v}| + 2 \end{aligned} \tag{8}$$

and $W_{\pi_{\mathcal{G}}}(0,c) = |\Lambda_c| - 2^N + 2$, we have that $|\Lambda_c| = W_{\pi_{\mathcal{G}}}(0,c) + 2^N - 2$ and $|\Gamma^{(1)}_{c,v}| = \frac{|\Lambda_c| + 2 - W_{\pi_{\mathcal{G}}}(v,c)}{4}$. So one can check by means of the Walsh transform the strong D-property by using Lemma 5.13.

In the following theorem, we give a sufficient condition for the strong D-property of a crooked function by means of the (first-order) nonlinearity of its ortho-derivative and of the parameter $\lambda^{\min}$ that we introduced above. Note that if $\mathcal{G}$ is AB (N odd) then $\lambda^{\min}$ equals $2^N - 2$ and the condition is nicely simple since it depends only on the nonlinearity. If $\mathcal{G}$ is not AB, then $\lambda^{\min}$ needs to be determined, or at least bounded from below, and this may represent much work.

Theorem 3. *Let $\mathcal{G}$ be a crooked (N,N)-function with $N \geq 3$. Let $\pi_{\mathcal{G}}$ be the ortho-derivative of $\mathcal{G}$. Let $\lambda^{\min} = \min_{c\in\mathbb{F}_2^N\setminus\{0\}} |\Lambda_c|$ where $\Lambda_c = \{(a,b) \in (\mathbb{F}_2^N)^2 \mid \varphi_{\mathcal{G}}(a,b) = c\}$ and ω be the so-called* linearity *of $\pi_{\mathcal{G}}$, that is, let:*

$$\mathrm{nl}(\pi_{\mathcal{G}}) = 2^{N-1} - \frac{\omega}{2}.$$

If $\omega < \frac{\lambda^{\min}}{3} - 2$, then $\mathcal{G}$ has the strong D-property.
More generally, let $\omega' = -\min_{c,v\in\mathbb{F}_2^N\setminus\{0\}}(W_{\pi_{\mathcal{G}}}(v,c))$. If $\omega' < \frac{\lambda^{\min}}{3} - 2$, then $\mathcal{G}$ has the strong D-property. Moreover, if N is odd, then $\omega' < \frac{2^N-2}{3} - 2$ if and only if $\mathcal{G}$ has the strong D-property.

Proof. Let $c,v \in \mathbb{F}_2^N \setminus \{0\}$. We have that $W_{\pi_{\mathcal{G}}}(v,c) = |\Lambda_c| - 4|\Gamma^{(1)}_{c,v}| + 2$ by (8). If we prove that $|\Gamma^{(1)}_{c,v}| < \frac{|\Lambda_c|}{3}$, then by Lemma 5.13 we can conclude that $\mathcal{G}$ has the strong D-property. The hypothesis $\omega' < \frac{\lambda^{\min}}{3} - 2$ implies:

$$|\Gamma^{(1)}_{c,v}| = \frac{|\Lambda_c| + 2 - W_{\pi_{\mathcal{G}}}(v,c)}{4} \leq \frac{|\Lambda_c| + 2 + \omega'}{4} < \frac{|\Lambda_c| + 2 + \frac{|\Lambda_c|}{3} - 2}{4} = \frac{|\Lambda_c|}{3},$$

and using Relation (3) with $\mathcal{F} = \pi_{\mathcal{G}}$, we have $\omega' \leq \omega$.
For N odd, we have $\lambda^{\min} = 2^N - 2$ by [15, Corollary 27]. So if $\omega' < \frac{2^N-2}{3} - 2$, then $\mathcal{G}$ has the strong D-property. Conversely, let $c,v \in \mathbb{F}_2^N \setminus \{0\}$. If $\mathcal{G}$ has the strong D-property, then $|\Gamma^{(1)}_{c,v}| < \frac{|\Lambda_c|}{3}$ by Lemma 5.13 and $-W_{\pi_{\mathcal{G}}}(v,c) < \frac{|\Lambda_c|}{3} - 2$ by using the equation $|\Gamma^{(1)}_{c,v}| = \frac{|\Lambda_c|+2-W_{\pi_{\mathcal{G}}}(v,c)}{4}$. Since $|\Lambda_c| = 2^N - 2$ by [15, Corollary 27], we have that $\omega' < \frac{2^N-2}{3} - 2$. □

Remark 5.15. *Let $\beta = \frac{\lambda^{\min}}{3} - 2$ and let u be the primitive element of the field $\mathbb{F}_{2^n}$ over $\mathbb{F}_2$ chosen by MAGMA. There are examples of quadratic APN functions where the condition $\omega < \beta$ is not satisfied and $\omega' < \beta$ is satisfied. Some examples are the function x^3 over $\mathbb{F}_{2^6}$ with $(\omega',\omega,\beta) = (8,16,16)$ and the function $ux^{24} + x^{10} + x^3$ over $\mathbb{F}_{2^6}$ with $(\omega',\omega,\beta) = (8,24,16)$. Moreover, for the case N even, we have that $\omega' < \beta$ is only sufficient and not necessary. Indeed, the following functions have the strong D-property but $\omega' \geq \beta$: the function $ux^9 + u^{11}x^6 + x^3$ over $\mathbb{F}_{2^6}$ with $(\omega',\omega,\beta) = (16,24,16)$ and the function*

$$u^{29}x^{48} + u^{15}x^{34} + u^{35}x^{33} + u^{62}x^{20} + u^{10}x^6 + u^{40}x^5$$

over $\mathbb{F}_{2^6}$ with $(\omega',\omega,\beta) = (24,32,8)$. There are also cases where $\omega' = \omega$, for instance in the case of the Gold APN function in dimension $N = 5$, whose ortho-derivative $x^{-(2^i+1)}$ is plateaued and is a permutation. As we have seen previously, this is not true for the Gold APN function in even dimension.

In the following proposition, we show that Proposition 5.5 holds even if we assume that $\mathcal{G}$ is crooked instead of quadratic APN (as we announced it after stating that proposition). It is indeed important, each time we have a result on APN quadratic functions, to check whether it extends to crooked functions: if it does, then this argues in favor of the conjecture that all crooked functions are quadratic, and if not, this makes this conjecture more questionable.

Proposition 5.16. *Let $N \geq 3$, let $\mathcal{G}$ be a crooked (N,N)-function, let ψ be a linear (N,N)-function where $\ker\psi = \langle c\rangle$ for $c \in \mathbb{F}_2^N \setminus \{0\}$, let $\mathcal{F}(x) = \psi(\mathcal{G}(x))$, and let A be an affine hyperplane with direction E. Then $\mathcal{F}_A$ is APN if and only if, for all $a, b \in E$, we have $\varphi_{\mathcal{G}}(a,b) \neq c$.*

Proof. Let $E = \langle v\rangle^{\perp}$ for some $v \in \mathbb{F}_2^N \setminus \{0\}$. Let $u \in \mathbb{F}_2^N$ be such that $A = u + E$. By using Lemma 5.1, it is enough to prove that $D_aD_b\mathcal{G}(u) \neq c$ for all $a, b \in \mathbb{F}_2^N$ with $v \cdot a = v \cdot b = 0$ if and only if $D_aD_b\mathcal{G}(0) \neq c$ for all $a, b \in \mathbb{F}_2^N$ with $v \cdot a = v \cdot b = 0$, and proving both implications follows dircetly from Lemma 5.12, item 2. □

We shall now present in Theorem 4, in the case where $\mathcal{G}$ is a quadratic APN permutation, a sufficient condition for $\mathcal{G}$ and $\mathcal{G}^{-1}$ to have both the strong D-property, which only depends on the second-order nonlinearity of $\pi_{\mathcal{G}}$. We shall need the next lemma that uses a similar idea to Lemma 5.13. We recall that since $\mathcal{G}$ is an (N,N)-permutation, N must be odd (and therefore $\mathcal{G}$ is AB), see e.g. [21].

Lemma 5.17. *Let $\mathcal{G}$ be a crooked (N,N)-permutation. Let $c, v \in \mathbb{F}_2^N \setminus \{0\}$ and $c_0 = c + \mathcal{G}^{-1}(0)$. Let $\Omega_{c,v}^{(1)} = \{a \in \mathbb{F}_2^N \setminus \{c_0\} \mid \mathcal{G}(c_0) \cdot \pi_{\mathcal{G}}(a + c_0) = 0,\ v \cdot \mathcal{G}(a) = 1\}$. Then $|\Omega_{c,v}^{(1)}| < \frac{2^N-2}{3}$ if and only if there exists $a, b \in \mathbb{F}_2^N$ such that $\varphi_{\mathcal{G}^{-1}}(a,b) = c$ (where we still denote $\varphi_{\mathcal{G}^{-1}}(a,b) = \mathcal{G}^{-1}(a+b) + \mathcal{G}^{-1}(a) + \mathcal{G}^{-1}(b) + \mathcal{G}^{-1}(0)$ but here for a possibly non-crooked function $\mathcal{G}^{-1}$) and $v \cdot a = v \cdot b = 0$.*

Proof. The condition $\varphi_{\mathcal{G}^{-1}}(a,b) = c$ is equivalent, denoting $a' = \mathcal{G}^{-1}(a)$ and $b' = \mathcal{G}^{-1}(b)$), to $\varphi_{\mathcal{G}^{-1}}(\mathcal{G}(a'), \mathcal{G}(b')) + c = 0$, that is, to $\mathcal{G}^{-1}(\mathcal{G}(a') + \mathcal{G}(b')) + a' + b' + \mathcal{G}^{-1}(0) + c = 0$, or equivalently to $\mathcal{G}(a' + b' + c_0) + \mathcal{G}(a') + \mathcal{G}(b') = 0$. Then, the condition $\varphi_{\mathcal{G}^{-1}}(a,b) = c$ and $v \cdot a = v \cdot b = 0$ is equivalent to the system

$$\begin{cases} \mathcal{G}(a' + b' + c_0) + \mathcal{G}(a') + \mathcal{G}(b') = 0 \\ v \cdot \mathcal{G}(a') = v \cdot \mathcal{G}(b') = 0. \end{cases} \tag{9}$$

Let Ω_c be the set of those elements $a \in \mathbb{F}_2^N$ such that, for some $b \in \mathbb{F}_2^N$, we have $\mathcal{G}(a + b + c_0) + \mathcal{G}(a) + \mathcal{G}(b) = 0$. Note that $\mathcal{G}(c_0)$ is nonzero, because otherwise $c_0 = \mathcal{G}^{-1}(0)$ and $c = 0$. Hence, c_0 does not belong to Ω_c. Since $\mathcal{G}(a+b+c_0)+\mathcal{G}(a)+\mathcal{G}(b) = 0$ is equivalent to $D_{a+c_0}\mathcal{G}(b) + D_{a+c_0}\mathcal{G}(c_0) = \mathcal{G}(c_0)$, then $\Omega_c = \{a \in \mathbb{F}_2^N \setminus \{c_0\} \mid \pi(a + c_0) \cdot \mathcal{G}(c_0) = 0\}$, and $\Omega_{c,v}^{(1)}$ is the set of all $a \in \Omega_c$ with $v \cdot \mathcal{G}(a) = 1$. We claim that $|\Omega_{c,v}^{(1)}| < (2/3)|\Omega_c|$ and since $\mathcal{G}$ is AB, then $|\Omega_c| = \frac{2^N-2}{2}$ and $|\Omega_{c,v}^{(1)}| < (2/3)|\Omega_c| = \frac{2^N-2}{3}$. Indeed, similarly as for Γ_c in the proof of Lemma 5.12, item 1, Ω_c can be partitioned in sets of the form $\{a, b, a+b+c_0\}$ where $\mathcal{G}(a+b+c_0)+\mathcal{G}(a)+\mathcal{G}(b) = 0$ (it is a partition because if we have for instance $\mathcal{G}(a+b+c_0)+\mathcal{G}(a)+\mathcal{G}(b) = 0$ and $\mathcal{G}(a+b'+c_0)+\mathcal{G}(a)+\mathcal{G}(b') = 0$ for two distinct b, b', then we have $\mathcal{G}(a+b+c_0)+\mathcal{G}(a+b'+c_0)+\mathcal{G}(b)+\mathcal{G}(b') = 0$, a contradiction with the APN property. Moreover, if $(a,b) \in (\mathbb{F}_2^N)^2$ is such that $\mathcal{G}(a+b+c_0)+\mathcal{G}(a)+\mathcal{G}(b) = 0$, then the number of elements among $\mathcal{G}(a+b+c_0)$, $\mathcal{G}(a)$, and $\mathcal{G}(b)$ that are non-orthogonal to v is necessarily even. Similarly as for $|\Gamma_{c,v}^{(1)}|$ in the proof of 1 in Lemma 5.12, we have that $|\Omega_{c,v}^{(1)}| < (2/3)|\Omega_c| = \frac{2^N-2}{3}$ if and only if there exists $(a,b) \in (\mathbb{F}_2^N)^2$ solution of System (9). □

Theorem 4. *Let $\mathcal{G}$ be a quadratic APN (N,N)-permutation. Let $\pi_{\mathcal{G}}$ be the ortho-derivative of $\mathcal{G}$. Let ω_2 be such that $\mathrm{nl}_2(\pi_{\mathcal{G}}) = 2^{N-1} - (\omega_2/2)$. If $\omega_2 < \frac{2^N-2}{3} - 2$, then $\mathcal{G}$ and $\mathcal{G}^{-1}$ have the strong D-property.*

Proof. Since $\mathrm{nl}(\pi_{\mathcal{G}}) \geq \mathrm{nl}_2(\pi_{\mathcal{G}})$, then $\omega \leq \omega_2$ where $\mathrm{nl}(\pi_{\mathcal{G}}) = 2^{N-1} - (\omega/2)$. Since $\lambda^{\min} = 2^N - 2$, then $\mathcal{G}$ has the strong D-property by Theorem 3. Let us prove that $\mathcal{G}^{-1}$ has the strong D-property. Let $c, v \in \mathbb{F}_2^N \setminus \{0\}$ and $c_0 = c + \mathcal{G}^{-1}(0)$. Let $g(a) = \mathcal{G}(c_0) \cdot \pi_{\mathcal{G}}(a + c_0)$ and $h(a) = v \cdot \mathcal{G}(a)$. Let $\gamma_{i,j} = |\{a \in \mathbb{F}_2^N \setminus \{c_0\} \mid g(a) = i,\, h(a) = j\}|$.
We claim that $\gamma_{0,1} < \frac{2^N-2}{3}$ and this will prove that there exists $a, b \in \mathbb{F}_2^N$ such that $\varphi_{\mathcal{G}^{-1}}(a,b) = c$ and $v \cdot a = v \cdot b = 0$ by Lemma 5.17.
We also claim that, for all $u \in \mathbb{F}_2^N$ there exists $a, b \in \mathbb{F}_2^N$ such that $\mathcal{G}^{-1}(a+b+u) + \mathcal{G}^{-1}(a+u) + \mathcal{G}^{-1}(b+u) + \mathcal{G}^{-1}(u) = c$ and $v \cdot a = v \cdot b = 0$. This will imply the strong D-property of $\mathcal{G}^{-1}$.
We fisrt prove the first claim. Observe that g and h are balanced because $\pi_{\mathcal{G}}$ and $\mathcal{G}$ are permutations and $\mathcal{G}(c_0) \neq 0$. Moreover, $g(c_0) = 0$ because $\pi_{\mathcal{G}}(0) = 0$. Before proceeding with the proof, we show three relations that we will need later. We have that $\gamma_{0,1} + \gamma_{0,0} = |g^{-1}(0) \setminus \{c_0\}| = 2^{N-1} - 1$, $\gamma_{0,1} + \gamma_{1,1} = |h^{-1}(1) \setminus \{c_0\}| = 2^{N-1} - 1 + \delta_0(h(c_0))$, and $\gamma_{1,0} + \gamma_{0,0} = |h^{-1}(0) \setminus \{c_0\}| = 2^{N-1} - \delta_0(h(c_0))$. So, denoting $f = g + h$, we have that:

$$\begin{aligned}\sum_{a \in \mathbb{F}_2^N \setminus \{c_0\}} (-1)^{f(a)} &= \gamma_{1,1} + \gamma_{0,0} - \gamma_{1,0} - \gamma_{0,1} \\ &= 2\gamma_{0,0} - 2\gamma_{0,1} + (\gamma_{0,1} + \gamma_{1,1}) - (\gamma_{1,0} + \gamma_{0,0}) = \\ &= -4\gamma_{0,1} + 2(\gamma_{0,1} + \gamma_{0,0}) - 1 + 2\delta_0(h(c_0)) = \\ &= -4\gamma_{0,1} + 2^N - 3 + 2\delta_0(h(c_0)),\end{aligned}$$

the second equality above coming from $(\gamma_{0,1} + \gamma_{1,1}) - (\gamma_{1,0} + \gamma_{0,0}) = (2^{N-1} - 1 + \delta_0(h(c_0))) - (2^{N-1} - \delta_0(h(c_0))) = 2\delta_0(h(c_0)) - 1$. We deduce, since $g(c_0) = 0$:

$$\begin{aligned}\sum_{a \in \mathbb{F}_2^N} (-1)^{f(a)} &= 2\delta_0(h(c_0)) - 1 + \sum_{a \in \mathbb{F}_2^N \setminus \{c_0\}} (-1)^{f(a)} \\ &= 2^N - 4\gamma_{0,1} - 4 + 4\delta_0(h(c_0)). \qquad (10)\end{aligned}$$

Observe that $-\sum_{a \in \mathbb{F}_2^N} (-1)^{f(a)} \leq \left|\sum_{a \in \mathbb{F}_2^N} (-1)^{f(a)}\right| \leq \omega_2$ because h is quadratic. So we can conclude, using (10), that

$$\begin{aligned}\gamma_{0,1} &= \frac{1}{4}\left(2^N - \sum_{a \in \mathbb{F}_2^N} (-1)^{f(a)}\right) - 1 + \delta_0(h(c_0)) \\ &\leq \frac{2^N + \omega_2}{4} < \frac{2^N - 2}{3}.\end{aligned}$$

We now prove the second claim. We have proven that, for any crooked function $\mathcal{G}$, if $\mathrm{nl}_2(\pi_{\mathcal{G}}) > 2^{N-1} - \frac{2^N-2}{6} + 1$, then there exists $a, b \in \mathbb{F}_2^N$ such that $\varphi_{\mathcal{G}^{-1}}(a,b) = c$ and $v \cdot a = v \cdot b = 0$. Let $u \in \mathbb{F}_2^N$; we observe that $\pi_{\mathcal{G}} = \pi_{\mathcal{G}^u}$ where $\mathcal{G}^u(x) = \mathcal{G}(x) + u$ and $(\mathcal{G}^u)^{-1}(x) = \mathcal{G}^{-1}(x+u)$. Since $\mathrm{nl}_2(\pi_{\mathcal{G}^u}) = \mathrm{nl}_2(\pi_{\mathcal{G}}) > 2^{N-1} - \frac{2^N-2}{6} + 1$, there exists $a, b \in \mathbb{F}_2^N$ such that $\varphi_{(\mathcal{G}^u)^{-1}}(a,b) = \mathcal{G}^{-1}(a+b+u) + \mathcal{G}^{-1}(a+u) + \mathcal{G}^{-1}(b+u) + \mathcal{G}^{-1}(u) = c$ and $v \cdot a = v \cdot b = 0$. □

5.3 The strong D-property of the Gold APN function

Let $\mathcal{G}(x) = x^{2^i+1}$ where $\gcd(i,N) = 1$ be the Gold APN function over $\mathbb{F}_{2^N}$. To prove the strong D-property of $\mathcal{G}$, it is enough to verify the D-property of the $(N-1,N)$-function $\mathcal{G}_E$ where $E = \{x \in \mathbb{F}_{2^N} \mid \mathrm{Tr}(x) = 0\}$ (see Remark 5.6). Therefore, we can use some of the results by Taniguchi in [23]. We have that $\mathcal{G}$ has the strong D-property for $N \geq 6$ even [23, Example 6]. By using Theorem 3, we are going to address the case N odd. With this result, all cases will be covered for Gold functions[1]. To apply Theorem 3, we will prove that the (first-order) nonlinearity of the ortho-derivative of the Gold APN function is larger than the second-order nonlinearity of the inverse function x^{-1}, or equal. Then we conclude by using a lower bound proven in [11].

For the rest of the section, the ortho-derivative of a crooked function over $\mathbb{F}_{2^N}$ is defined by using the inner product $a \cdot b = \mathrm{Tr}(ab)$ for any $a, b \in \mathbb{F}_{2^N}$.

Theorem 5. *Let $N \geq 3$ and i be such that $\gcd(i,N) = 1$. Then the Gold APN function x^{2^i+1} over $\mathbb{F}_{2^N}$ has the strong D-property if and only if $N = 6$ or $N \geq 8$.*

Proof. As we have discussed previously, the cases $N < 10$ have been verified computationally and the case N even follows from [23, Example 6] (which shows that the restrictions to the hyperplane $\{x \in \mathbb{F}_{2^N} \mid \mathrm{Tr}(x) = 0\}$ of Gold APN functions in even dimension have the D-property) and Remark 5.6. By using Theorem 3, we will prove the case $N \geq 11$ odd. We have that $\pi_{\mathcal{G}}(x) = x^{-(2^i+1)}$ as shown in [8] where $\mathcal{G}(x) = x^{2^i+1}$. Let $u, v \in \mathbb{F}_{2^N}$. Since N is odd, then $\pi_{\mathcal{G}}$ is a permutation (see Remark 5.9). So the nonlinearity of $\pi_{\mathcal{G}}$ depends on the values of $W_{\pi_{\mathcal{G}}}(u,v)$ with $u \neq 0$ and $v \neq 0$. Observe that since

$$W_{\pi_{\mathcal{G}}}(u,v) = \sum_{x \in \mathbb{F}_{2^N}} (-1)^{\mathrm{Tr}(v \cdot \pi_{\mathcal{G}}(x) + ux)} = \sum_{x \in \mathbb{F}_{2^N}} (-1)^{\mathrm{Tr}(v \cdot \pi_{\mathcal{G}}(x^{-1}) + ux^{-1})},$$

and $\pi_{\mathcal{G}}(x^{-1}) = x^{2^i+1}$ is quadratic, we have that

$$\mathrm{nl}(\pi_{\mathcal{G}}) = 2^{N-1} - \frac{1}{2} \max_{u,v \in \mathbb{F}_{2^N} \setminus \{0\}} |W_{\pi_{\mathcal{G}}}(u,v)| \geq \mathrm{nl}_2(x^{-1}).$$

By [11, Proposition 5], we have that

$$\mathrm{nl}_2(x^{-1}) \geq 2^{N-1} - \frac{1}{2}\sqrt{(2^N-1)2^{N/2+2} + 3 \cdot 2^N}$$

and therefore

$$|W_{\pi_{\mathcal{G}}}(u,v)| \leq \sqrt{(2^N-1)2^{N/2+2} + 3 \cdot 2^N}$$

for any $u, v \in \mathbb{F}_{2^N} \setminus \{0\}$. We claim that for $N \geq 11$ we have that the inequality

$$\sqrt{(2^N-1)2^{N/2+2} + 3 \cdot 2^N} < \frac{2^N-2}{3} - 2 \tag{11}$$

holds and conclude by using Theorem 3. Observe that the expression on the left side of (11) is equal to $\sqrt{2^{(3N+4)/2} + 2^{N+1} + 2^N - 2^{(N+4)/2}}$ that is less or

[1] Taniguchi could not address in [23] the case of odd dimension N, except for the cube function $F(x) = x^3$ when the dimension is a multiple of 9,11,13 or 15.

equal than $\sqrt{2 \cdot 2^{(3N+4)/2}} = 2^{(3N+6)/4}$. The inequality $2^{(3N+6)/4} < \frac{2^N-2}{3} - 2$ is equivalent to the inequality $2^{(3N+10)/4} + 2^{(3N+6)/4} + 8 < 2^N$ that is true if and only if $N > 10$. So (11) holds for $N \geq 11$. □

Remark 5.18. *We observe that for the Gold APN function in even dimension N, all the values of $|\Lambda_c|$ defined in Remark 5.11 are known from[13, Example 2], so we can prove similarly that for some positive integer N_0 the Gold APN function has the strong D-property for $N \geq N_0$ even. We obtain this way a simpler proof than in [23, Example 6]. Let N be even, $c \in \mathbb{F}_{2^N} \setminus \{0\}$, and $\mathcal{G}$ be a Gold APN function over $\mathbb{F}_{2^N}$. We have that either $|\Lambda_c| \in \{2^N - 2^{N/2+1} - 2, 2^N + 2^{N/2} - 2\}$ or $|\Lambda_c| \in \{2^N + 2^{N/2+1} - 2, 2^N - 2^{N/2} - 2\}$. In the case N even, we have that $|W_{\pi_\mathcal{G}}(0,c)| \in \{2^{N/2+1}, 2^{N/2}\}$ that is strictly less than $(2^N - 2^{N/2} - 2)/3 \leq \lambda^{\min}/3 - 2 = (2^N - 2)/3$ for $N \geq 6$. Now we can use a similar argument to the proof of Theorem 5 by considering only the values $W_{\pi_\mathcal{G}}(u,v)$ for $u, v \in \mathbb{F}_{2^N} \setminus \{0\}$. For any $u, v \in \mathbb{F}_{2^N} \setminus \{0\}$, we have that*

$$|W_{\pi_\mathcal{G}}(u,v)| = \left| \sum_{x \in \mathbb{F}_{2^N}} (-1)^{\mathrm{Tr}(v \cdot \pi_\mathcal{G}(x^{-1}) + ux^{-1})} \right| \leq 2^N - 2\,\mathrm{nl}_2(x^{-1})$$

for any $u, v \in \mathbb{F}_{2^N} \setminus \{0\}$ and so

$$|W_{\pi_\mathcal{G}}(u,v)| \leq \sqrt{(2^N - 1)2^{N/2+2} + 3 \cdot 2^N}$$

by [11, Proposition 5]. We claim that

$$\sqrt{(2^N - 1)2^{N/2+2} + 3 \cdot 2^N} < \frac{\lambda^{\min}}{3} - 2$$

for $N \geq 12$ and this will conclude the proof as in Theorem 5. Using similar steps, we get $2^{(3N+6)/4} < \frac{\lambda^{\min}}{3} - 2$ and $\lambda^{\min} > 2^{(3N+10)/4} + 2^{(3N+6)/4} + 6$. Since $\lambda^{\min} \leq 2^N - 2^{N/2+1} - 2$, we need to show that $2^N > 2^{(3N+10)/4} + 2^{(3N+6)/4} + 2^{N/2+1} + 8$ and this is true for $N \geq 12$.

The ortho-derivatives of other classes of quadratic APN functions can be derived from the work done in the paper [8], but they do not have an easy-to-handle representation like the Gold APN function. In Theorem 3, we have used the fact that the function $\pi_\mathcal{G}(x^{-1})$ is quadratic and this is a relevant case for the Gold APN function.

In [23, Example 16], Taniguchi proved the D-property of the restriction of the Dobbertin APN power function in even dimension to the linear hyperplane $E = \{x \in \mathbb{F}_{2^N} \mid \mathrm{Tr}(x) = 0\}$. For that, he used his [23, Theorem 26], which applies to any power APN function x^d such that $\gcd(d, 2^N - 1) = 3$. We shall show that the same method can be applied to the case of N odd, by using his [23, Theorem 25], which applies to any power APN function x^d such that $\gcd(d, 2^N - 1) = 1$. Note that these two theorems together cover all cases of power APN functions, thanks to the result of Dobbertin reported in [15, Proposition 165]). We group the two theorems in the following lemma.

Lemma 5.19 ([23])**.** *Let $\mathcal{G}(x) = x^d$ be an APN power function over $\mathbb{F}_{2^N}$ with $N \geq 3$. Let $t > 2$ be a positive integer such that t divides N and such that*

t is even if N is even. Let us denote $E_t = \{x \in \mathbb{F}_{2^t} \mid \mathrm{Tr}_t(x) = 0\}$ and $E_N = \{x \in \mathbb{F}_{2^N} \mid \mathrm{Tr}_N(x) = 0\}$. If the $(t-1,t)$-function $\mathcal{G}_{E_t}$ has the D-property, then the $(N-1,N)$-function $\mathcal{G}_{E_N}$ has the D-property.

We deduce:

Proposition 5.20. *Let t be a positive integer, let $\mathcal{G}(x) = x^d$ where $d = 2^{4t} + 2^{3t} + 2^{2t} + 2^t - 1$ be the Dobbertin APN function over $\mathbb{F}_{2^{5t}}$, and let $E = \{x \in \mathbb{F}_{2^{5t}} \mid \mathrm{Tr}_{5t}(x) = 0\}$. Then the $(5t-1,5t)$-function $\mathcal{G}_E$ has the D-property if and only if $t \geq 2$.*

Proof. The cases $t \leq 5$ can be verified computationally. Assume $t > 5$. Let us prove the case $t \neq 7$. Since t is even if $5t$ is even, we can use Lemma 5.19. So it is enough to prove that the $(t-1,t)$-function $\mathcal{G}_{E_t}$ has the D-property. Observe that $\mathcal{G}$ restricted to $\mathbb{F}_{2^t}$ is equal to the cube function x^3 because $2^{4t} \equiv 2^{3t} \equiv 2^{2t} \equiv 2^t \equiv 1 \pmod{2^t - 1}$. The function x^3 over $\mathbb{F}_{2^t}$ has the strong D-property by Theorem 5 since $t \neq 7$, so the restriction of x^3 to E_t has the D-property. To prove the case $t = 7$, we use again Lemma 5.19 but this time we consider the restriction to $\mathbb{F}_{2^5}$. It can be verified computationally that the $(4,5)$-function $\mathcal{G}_{E_5}$ has the D-property. □

The previous proposition does not imply the strong D-property of the Dobbertin APN function for $t \geq 2$, since according to Remark 5.3, we would have to also consider the restriction to the complement of E, but it is enough as a strong argument to conjecture that it holds.

Conjecture 1. *For $t \geq 2$, the Dobbertin APN function in dimension $N = 5t$ has the strong D-property.*

6 Revisiting two infinite families of differentially 4-uniform $(N-1,N-1)$-permutations

When constructing an infinite family of $(N-1,N-1)$-permutations $\mathcal{F}_A$ by restricting to an affine hyperplane a family of (N,N)-functions $\mathcal{F}$ with one affine component, we have only two cases to consider up to equivalence: either $\mathcal{F}$ is equal to $\psi(\mathcal{G}(x))$ or it is equal to $\psi(\mathcal{G}(x)) + x$ where $\mathcal{G}$ has nonzero nonlinearity and ψ is a linear function with a kernel of dimension 1. This follows from Proposition 4.3 by affine equivalence with possible addition of a constant (which both preserve bijectivity), the two cases $\psi(\mathcal{G}(x))$ and $\psi(\mathcal{G}(x))+x$ happening when the affine component of $\mathcal{F}$ is constant, respectively is not. In this section, we will be interested in the case where $\mathcal{G}$ is an APN permutation and study whether $\mathcal{F}_A$ can be APN. As we have mentioned at the beginning of Section 5, Berierle et al. in [3] investigated a similar setting. However, they did not impose the permutation property on $\mathcal{G}$ and neither they were aiming to construct specifically permutations as the restriction of $\mathcal{G}$ (in their sense of the term) because they used an approach up to EA equivalence. We revisit the classes of differentially 4-uniform permutations that are known in the literature and which are obtained as the restrictions of APN permutations, up to the addition of a linear function. The permutation $\mathcal{G}$ is the multiplicative inverse function in the first example, and the compositional inverse of a Gold permutation in the second example.

6.1 On the non-APNness of the family from [12]

We shall discuss the family constructed by the first author in [12] (a completed version can be found in [15, Subsection 11.6.4, sixth point]). We study it for N odd (and the permutation will then be in even dimension $N-1$), which is more interesting since differentially 4-uniform permutations are the best we can hope as long as an infinite class of APN permutations is not found in even dimension, while in an odd dimension, we know a series of infinite classes of APN permutations. We wish to prove that the family does not contain any APN permutation (in even dimension), which has always been assumed (since we consider that the APN permutation from [7] is the only one known in even dimension up to CCZ equivalence) but never been proved.

The permutation in even dimension $N-1$ is obtained as the restriction of the (N,N)-function $\mathcal{F}(x) = \frac{1}{x^2+1} + \frac{1}{x+1} + x$ to the linear hyperplane $E = \{x \in \mathbb{F}_{2^N} \mid \mathrm{Tr}(x) = 0\}$. The fact that $\mathcal{F}_E$ is a permutation is proved in [12] thanks to observations involving the Dickson permutation polynomials. Using Lemma 5.1 and changing x into $x+1$, $\mathcal{F}_E$ is not APN if and only if there exist $x, y, z \in \mathbb{F}_{2^N}$ such that $\mathrm{Tr}(x) = \mathrm{Tr}(y) = \mathrm{Tr}(z) = 1$ and $x^{2^N-2} + y^{2^N-2} + z^{2^N-2} + (x+y+z)^{2^N-2} = 1$ (because $\mathrm{Tr}(a+1) = \mathrm{Tr}(a)+1$). We shall prove more: there is a solution (x,y,z) such that $z = 1$, that is, the system

$$\begin{cases} x^{2^N-2} + y^{2^N-2} + (x+y+1)^{2^N-2} = 0 \\ \mathrm{Tr}(x) = \mathrm{Tr}(y) = 1 \end{cases} \tag{12}$$

has a solution in $\mathbb{F}_{2^N}$ for $N \geq 7$ odd. We will prove it by using the well known Hasse-Weil bound [19, Chapter 5] for algebraic curves over finite fields, while for $N = 5$, the strong D-property itself can be verified computationally.

The Hasse-Weil bound works in the following setting. Let $H(X,Y,Z)$ be an homogeneous multivariate polynomial with coefficients in $\mathbb{F}_{2^N}$. Then a curve in the projective plane $\mathbb{P}^2(\mathbb{F}_{2^N})$ is defined as $V_{\mathbb{P}^2(\mathbb{F}_{2^N})}(H) = \{(X:Y:Z) \in \mathbb{P}^2(\mathbb{F}_{2^N}) \mid H(X,Y,Z) = 0\}$ where $\mathbb{P}^2(\mathbb{F}_{2^N}) = \{(X:Y:Z) \colon (X,Y,Z) \in (\mathbb{F}_{2^N})^3 \setminus \{(0,0,0)\}\}$ and $(X:Y:Z) = \{(aX,aY,aZ) \in \mathbb{F}_{2^N}^3 \mid a \in \mathbb{F}_{2^N} \setminus \{0\}\}$. The curve is called absolutely irreducible if and only if the multivariate polynomial H is irreducible in every extension field of $\mathbb{F}_{2^N}$. The curve is called non-singular if the system given by the equations $\partial_X H(X,Y,Z) = 0$, $\partial_Y H(X,Y,Z) = 0$, $\partial_Z H(X,Y,Z) = 0$ (where ∂ indicates the partial formal derivative) has no solution in every field extension of $\mathbb{F}_{2^N}$ such that $(X,Y,Z) \neq (0,0,0)$. The Hasse-Weil bound states that if a curve is both absolutely irreducible and non-singular, then

$$||V_{\mathbb{P}^2(\mathbb{F}_{2^N})}(H)| - (2^N+1)| \leq 2g \cdot 2^{N/2}$$

where $g = \frac{(D-1)(D-2)}{2}$ is the genus of the curve and D is the degree of H.

Theorem 6. *Let N be odd. Then we have that:*

1. *If $N \geq 7$, then System (12) has a solution.*
2. *If $N \geq 5$, then the $(N-1, N-1)$-permutation $\mathcal{F}_E$ is not APN where $\mathcal{F}(x) = \frac{1}{x^2+1} + \frac{1}{x+1} + x$ and $E = \{x \in \mathbb{F}_{2^N} \mid \mathrm{Tr}(x) = 0\}$.*

Proof. Note that since $\mathrm{Tr}(x) = \mathrm{Tr}(y) = 1$, any solutions (x,y) of (12) are nonzero and such that $x+y+1$ is also nonzero. Then we can rewrite equation

$x^{2^N-2}+y^{2^N-2}+(x+y+1)^{2^N-2}=0$ of System (12) into $y(x+y+1)+x(x+y+1)+xy=0$. Set $F(x,y)=y(x+y+1)+x(x+y+1)+xy$. Therefore, System (12) has a solution if and only if $G(X,Y)=F(X^2+X+1,Y^2+Y+1)$ has a root (X,Y) (since $X\mapsto X^2+X+1$ is onto $E+1$). Let D be the degree of $G(X,Y)$ and let $H(X,Y,Z)=Z^D\cdot G(\frac{X}{Z},\frac{Y}{Z})$ be the homogenization of $G(X,Y)$. We verified by using MAGMA [5] (see Appendix A) that $V_{\mathbb{P}^2(\mathbb{F}_{2^N})}(H)$ does not contain points at infinity (that are points with $Z=0$), it is absolutely irreducible, it is non-singular, and it has genus 3. So we can apply the Hasse-Weil bound and we have that $|V_{\mathbb{P}^2(\mathbb{F}_{2^N})}(H)|\geq 2^N+1-2\cdot 3\cdot 2^{N/2}$. Since $2^N+1-6\cdot 2^{N/2}>0$ for $N\geq 7$, we have proved the first part. By using Lemma 5.1, if System (12) has a solution, then $\mathcal{F}_E$ is not APN. Since the case $N=5$ can be verified computationally, this concludes the proof. □

Remark 6.1. *When considering the strong D-property of the inverse function, the problem is more complex since it corresponds to verifying that the restriction of $\psi(x^{-1})$ to A is not APN whatever is the affine hyperplane A and whatever is the kernel of ψ (while above, we verified this for the hyperplane of equation $\mathrm{Tr}(x)=1$ and for $\ker\psi=\langle 1\rangle$ only). However, using a similar reduction as in the proof of Theorem 6, we can define for any $c\in\mathbb{F}_{2^N}\setminus\{0\}$ and any $\epsilon\in\mathbb{F}_2$ the following system in $(x,y)\in(\mathbb{F}_{2^N})^2$:*

$$\begin{cases} x^{2^N-2}+y^{2^N-2}+(x+y+\epsilon)^{2^N-2}+\epsilon+c=0 \\ \mathrm{Tr}(x)=\mathrm{Tr}(y)=\epsilon \end{cases}. \tag{13}$$

According to Remark 5.3, proving that there exists a solution $(x,y)\in(\mathbb{F}_{2^N})^2$ of System (13) for all $c\in\mathbb{F}_{2^N}\setminus\{0\}$ and all $\epsilon\in\mathbb{F}_2$ implies that the inverse function in dimension N has the strong D-property. To prove that System (13) has a solution, we can define an algebraic curve by using the polynomial $H_{c,\epsilon}(X,Y,Z)$ that is the homogenization of $G_{c,\epsilon}(X,Y)=F_{c,\epsilon}(X^2+X+\epsilon,Y^2+Y+\epsilon)$ where $F_{c,\epsilon}(x,y)$ is a polynomial whose zeros are the solutions of the first equation of System (13). However, having c and ϵ as parameters of the curve (while above we had only one value for c and one for ϵ) increases the difficulty of the problem noticeably because we cannot use MAGMA to prove properties of the curve (notice that the coefficients of the curve do not belong to a fixed subfield as for the case $c=1$).

Conjecture 2. *For any $N\geq 5$ odd, the inverse function in dimension N has the strong D-property.*

Conjecture 2 is verified computationally for every odd N between 5 and 25.

Remark 6.2. *It is conjectured in [9, 16] that, for $n\geq 3$, no APN (n,n)-function has algebraic degree n, or in other words, that every APN (n,n)-function F satisfies $\sum_{x\in\mathbb{F}_{2^n}}F(x)=0$. If this conjecture is true, then by affine equivalence, every (N,N)-function $\mathcal{F}$ such that, for some affine subspace A of $\mathbb{F}_2^N$ of dimension at least 3, the image $\mathcal{F}(A)$ of A by $\mathcal{F}$ is included in an affine space of the same dimension and the corresponding restriction $\mathcal{F}_A$ is APN satisfies $\sum_{x\in A}\mathcal{F}(x)=0$. It is proved in [17] that the inverse function sums to a nonzero value over any affine space that is not a vector space (i.e., excluding 0). Hence, if the conjecture is true, then denoting by $\mathcal{G}$ the inverse function over $\mathbb{F}_{2^N}$ and given a hyperplane A and a linear (N,N)-function ψ of kernel $\ker\psi=\langle c\rangle$, the* *only possibility for the restriction of $\mathcal{F}(x) = \psi(\mathcal{G}(x))$ to A to be APN is that $\sum_{x\in A}\mathcal{G}(x) = c$, because $\sum_{x\in A}\mathcal{F}(x) = \psi(\sum_{x\in A}\mathcal{G}(x))$. If this condition is not satisfied, then $\mathcal{F}_A$ has algebraic degree $N-1$ (its number of variables) and differential uniformity 4.*

In the case where A is a vector space, the situation is more complex and not completely clarified in [17].

6.2 On the non-APNness of Li-Wang families

Li and Wang in [22] define explicitly two families of permutations in dimension $N-1$ even, of the form $\mathcal{F}_E$ where $\mathcal{F}(x) = \psi(\mathcal{G}(x))$, ψ is a linear function with a kernel of dimension 1, $E = \operatorname{Im}\psi$, and $\mathcal{G}$ is an APN permutation. The first one is such that $\psi(x) = cx^{2^i} + c^{2^i}x$ for any $c \in \mathbb{F}_{2^N}\setminus\{0\}$ and $\mathcal{G}(x) = x^{\frac{1}{2^i+1}}$ with $\gcd(i,N) = 1$ ($\mathcal{G}$ is the inverse of the Gold APN function) [22, Theorem 4]. The second one is such that $\psi(x) = x^{2^i} + x$ and $\mathcal{G}(x) = x^{\frac{1}{2^i+1}} + \mathrm{Tr}_3^N(x + x^{2^{2s}})$ with N divisible by 3, $\gcd(i,N) = 1$, and $s = i \mod 3$ [22, Theorem 6]. We will show that both families never produce APN permutations (in even dimension $N-1$). Using this as a motivation, we conjecture that the inverse of the Gold APN function has the strong D-property in dimension $N \geq 5$ odd. We first need a lemma (that we do not claim to be new; we give a proof for self-completeness).

Lemma 6.3. *Let $N \geq 3$ be odd. Then $|\{x \in \mathbb{F}_{2^N} \mid \mathrm{Tr}(x) = 1,\ \mathrm{Tr}(x^{-1}) = 0\}| \geq 2^{N-2} - 2^{N/2-1}$.*

Proof. Let $\gamma_{i,j} = |\{x \in \mathbb{F}_{2^N} \mid \mathrm{Tr}(x) = i,\ \mathrm{Tr}(x^{-1}) = j\}|$. Since $\gamma_{1,0} = \gamma_{0,1}$ and $\gamma_{1,1} + \gamma_{1,0} = \gamma_{0,0} + \gamma_{1,0} = 2^{N-1}$, we have that

$$\begin{aligned}\sum_{x\in\mathbb{F}_{2^N}} (-1)^{\mathrm{Tr}(x^{-1}+x)} &= \gamma_{1,1} + \gamma_{0,0} - 2\gamma_{1,0}\\ &= (\gamma_{1,1} + \gamma_{1,0}) + (\gamma_{0,0} + \gamma_{1,0}) - 4\gamma_{1,0}\\ &= 2^N - 4\gamma_{1,0}.\end{aligned}$$

We conclude by observing that $\sum_{x\in\mathbb{F}_{2^N}} (-1)^{\mathrm{Tr}(x^{-1}+x)} \leq 2^{N/2+1}$ because $\mathrm{nl}(x^{-1}) \geq 2^{N-1} - 2^{N/2}$ [15]. This concludes the proof. □

Theorem 7. *Let N, i be positive integers such that $N \geq 5$ is odd and $\gcd(i,N) = 1$. Let $d = 2^i + 1$. For any $c \in \mathbb{F}_{2^N}\setminus\{0\}$, set $\psi_c(x) = cx^{2^i} + c^{2^i}x$. Then we have the following:*

1. *For any $c \in \mathbb{F}_{2^N}\setminus\{0\}$, function $\mathcal{F}_E$ is not APN where $E = \operatorname{Im}\psi_c$, $\mathcal{F}(x) = \psi_c(\mathcal{G}(x))$, and $\mathcal{G}(x) = x^{\frac{1}{d}}$.*
2. *Let $s = i \mod 3$ and let N be divisible by 3. Then $\mathcal{F}_E$ is not APN where $E = \operatorname{Im}\psi_1$, $\mathcal{F}(x) = \psi_1(\mathcal{G}(x))$, and $\mathcal{G}(x) = x^{\frac{1}{d}} + \mathrm{Tr}_3^N(x + x^{2^{2s}})$.*

Proof. Observe that $\operatorname{Im}\psi_c = \{x \in \mathbb{F}_{2^N} \mid \mathrm{Tr}(\pi(c)x) = 0\}$ where $\pi(x) = x^{-d}$ is the ortho-derivative of $\mathcal{G}^{-1}(x) = x^d$ because $\psi_c(x) = \varphi_{\mathcal{G}^{-1}}(c,x)$.

Let us prove 1. Using the reverse direction in the equivalence stated by Lemma 5.1 and specifying $x = 0, y = a, z = b$, we have that if there exists $a, b \in \mathbb{F}_{2^N}$ such that $\varphi_{\mathcal{G}}(a,b) = c$ and $\mathrm{Tr}(\pi(c)a) = \mathrm{Tr}(\pi(c)b) = 0$, then $\mathcal{F}_E$ is not APN. To prove the existence of such a and b, we are going to use Lemma 5.17. Let $c_0 = c+\mathcal{G}(0)$ and $\Omega^{(1)}_{c,\pi(c)} = \{a \in \mathbb{F}_2^N \setminus \{c_0\} \mid \mathrm{Tr}(\pi(a+c_0)\mathcal{G}^{-1}(c_0)) = 0,\ \mathrm{Tr}(\pi(c)\mathcal{G}^{-1}(a)) = 1\}$. Using Lemma 5.17, we have that if $|\Omega^{(1)}_{c,\pi(c)}| < (2^N-2)/3$, then there exists $a, b \in \mathbb{F}_{2^N}$ such that $\varphi_{\mathcal{G}}(a,b) = c$ and $\mathrm{Tr}(\pi(c)a) = \mathrm{Tr}(\pi(c)b) = 0$. Since $\pi(x) = x^{-d}$, $\mathcal{G}^{-1}(x) = x^d$, and $\mathcal{G}(0) = 0$ then $\Omega^{(1)}_{c,\pi(c)} = \{a \in \mathbb{F}_2^N \setminus \{c\} \mid \mathrm{Tr}((a+c)^{-d}c^d) = 0,\ \mathrm{Tr}(c^{-d}a^d) = 1\}$. Then, substituting a with $a + c_0 = a + c$ and using that $\mathrm{Tr}(c^{-d}(a+c)^d) = \mathrm{Tr}(c^{-d}a^d + c^{-2^i}a^{2^i} + c^{-1}a + 1) = \mathrm{Tr}(c^{-d}a^d) + 1$, we have:

$$\begin{aligned}
|\Omega^{(1)}_{c,\pi(c)}| &= |\{a \in \mathbb{F}_{2^N} \setminus \{0\} \mid \mathrm{Tr}(a^{-d}c^d) = 0,\ \mathrm{Tr}(c^{-d}(a+c)^d) = 1\}| \\
&= |\{a \in \mathbb{F}_{2^N} \setminus \{0\} \mid \mathrm{Tr}(a^{-d}c^d) = 0,\ \mathrm{Tr}(c^{-d}a^d) = 0\}| \\
&= |\{a \in \mathbb{F}_{2^N} \setminus \{0\} \mid \mathrm{Tr}(a) = 0,\ \mathrm{Tr}(a^{-1}) = 0\}|,
\end{aligned}$$

where the latter equality is obtained by substituting $a^{-d}c^d$ with a, which is possible since N is odd. Notice that we have that $|\Omega^{(1)}_{c,\pi(c)}| + |\{a \in \mathbb{F}_{2^N} \mid \mathrm{Tr}(a) = 1,\ \mathrm{Tr}(a^{-1}) = 0\}| = |\{a \in \mathbb{F}_{2^N} \setminus \{0\} \mid \mathrm{Tr}(a^{-1}) = 0\}| = 2^{N-1} - 1$ and then $|\Omega^{(1)}_{c,\pi(c)}| \leq 2^{N-1} - 1 - 2^{N-2} + 2^{N/2-1} = 2^{N-2} + 2^{N/2-1} - 1$ by Lemma 6.3. We conclude by observing that $2^{N-2} + 2^{N/2-1} - 1 < (2^N-2)/3$ if and only if $2^{N-1} + 2^{N-2} + 2^{N/2} + 2^{N/2-1} < 2^N + 1$ that is true for $N \geq 5$.
Let us prove 2. It follows from the fact that the $(N-1, N-1)$-function defined in *1* for $c = 1$ is EA equivalent to $\mathcal{F}_E$ because $\mathcal{F}(x) = \psi_1(\mathcal{G}(x)) = \psi_1(x^{\frac{1}{d}}) + \psi_1(\mathrm{Tr}_3^N(x + x^{2^{2s}}))$ (see Remark 4.4). □

With Theorem 7, we have a partial result on the strong D-property of the inverse of the Gold APN permutation. So, as for the inverse function, we believe this is a good argument to conjecture the strong D-property of the inverse of the Gold APN function in dimension $N \geq 5$ odd (it can be verified computationally that the property does not hold for $N = 3$).

Conjecture 3. *For $N \geq 5$ odd, the inverse of the Gold APN function in dimension N has the strong D-property.*

Conjecture 3 is verified computationally for every odd N between 5 and 25.

Conclusion

In this paper, we have made a general study of the restrictions of functions $\mathcal{F} : \mathbb{F}_2^N \mapsto \mathbb{F}_2^M$ to affine subspaces of $\mathbb{F}_2^N$, which map these affine spaces into strict affine subspaces of $\mathbb{F}_2^M$, providing then potentially new (n,m)-functions F, for some $n < N$ and $m < M$. After studying the main cryptographic properties of these (n,m)-functions F when they exist, we have observed that when $\mathcal{F}$ has affine components, they always exist. When $n = m = N-1 = M-1$ and $\mathcal{F}$ has affine components, $\mathcal{F}$ has the form $\psi \circ \mathcal{G}$ where $\mathcal{G}$ is an (N,N)-function and ψ is a linear (N,N)-function whose kernel has dimension 1. We have related the question of the APNness of the restriction F of such $\mathcal{F}$ when $\mathcal{G}$ is APN to the D-property introduced by Taniguchi. The existence of an APN restriction of this kind is equivalent to the fact that $\mathcal{G}$ does not have what we called the strong D-property. This showed that any APN function $\mathcal{G}$, either has the advantage of possessing the strong D-property, or has that of admitting an APN restriction F to an affine hyperplane mapped into an affine hyperplane. We showed the strong D-property of all Gold APN functions (this completed Taniguchi's work, one result of whom is equivalent to showing this strong D-property in even dimension N while he was stuck with the odd dimension) and we also completed Taniguchi's work on the Dobbertin function, but only partially. We proved that the two known infinite classes of differentially 4-uniform permutations in even dimension do not contain APN functions. Much work, probably difficult, remains to be done, in particular for studying the strong D-property of other known infinite classes of APN functions than Gold, and for investigating restrictions of (possibly APN) functions to affine subspaces of codimension larger than 1, which could provide new infinite classes of functions having good cryptographic properties and a simple representation, with potential to find new APN functions, possibly bijective.

Acknowledgements We thank Xiang-dong Hou, Cunsheng Ding, Gary McGuire, Sihem Mesnager and Daniel Panario for useful information.

References

[1] M. Abbondati, M. Calderini, and I. Villa, "On dillon's property of (n, m)-functions," *arXiv preprint arXiv:2302.13922*, 2023. See page 2.

[2] C. Beierle and G. Leander, "New instances of quadratic APN functions," *IEEE Transactions on Information Theory*, vol. 68, no. 1, pp. 670–678, 2021. See pages 7, 16, and 19.

[3] C. Beierle, G. Leander, and L. Perrin, "Trims and extensions of quadratic APN functions," *Designs, Codes and Cryptography*, vol. 90, no. 4, pp. 1009–1036, 2022. See pages 2, 3, 15, 16, 17, and 28.

[4] J. Bierbrauer and G. M. Kyureghyan, "Crooked binomials," *Designs, Codes and Cryptography*, vol. 46, no. 3, pp. 269–301, 2008. See page 6.

[5] W. Bosma, J. Cannon, and C. Playoust, "The magma algebra system I: The user language," *Journal of Symbolic Computation*, vol. 24, no. 3-4, pp. 235–265, 1997. See pages 30 and 36.

[6] K. Browning, J. Dillon, R. Kibler, and M. McQuistan, "APN polynomials and related codes," *Special volume of Journal of Combinatorics, Information and System Sciences*, vol. 34, pp. 135–159, 2009. See pages 16 and 19.

[7] K. Browning, J. Dillon, M. McQuistan, and A. Wolfe, "An apn permutation in dimension six," *Finite Fields: theory and applications*, vol. 518, pp. 33–42, 2010. See page 29.

[8] L. Budaghyan, C. Carlet, and T. Helleseth, "On bent functions associated to AB functions," in *2011 IEEE Information Theory Workshop*. IEEE, 2011, pp. 150–154. See pages 26 and 27.

[9] L. Budaghyan, C. Carlet, T. Helleseth, N. Li, and B. Sun, "On upper bounds for algebraic degrees of APN functions," *IEEE Transactions on Information Theory*, vol. 64, no. 6, pp. 4399–4411, 2017. See page 30.

[10] C. Carlet, "On the degree, nonlinearity, algebraic thickness, and nonnormality of Boolean functions, with developments on symmetric functions," *IEEE Transactions on Information Theory*, vol. 50, no. 9, pp. 2178–2185, 2004. See pages 5, 6, 8, and 9.

[11] ——, "Recursive lower bounds on the nonlinearity profile of Boolean functions and their applications," *IEEE Transactions on Information Theory*, vol. 54, no. 3, pp. 1262–1272, 2008. See pages 26 and 27.

[12] ——, "On known and new differentially uniform functions," in *Australasian Conference on Information Security and Privacy*. Springer, 2011, pp. 1–15. See pages 3, 4, and 29.

[13] ——, "Boolean and vectorial plateaued functions and APN functions," *IEEE Transactions on Information Theory*, vol. 61, no. 11, pp. 6272–6289, 2015. See page 27.

[14] ——, “Characterizations of the differential uniformity of vectorial functions by the Walsh transform,” *IEEE transactions on information theory*, vol. 64, no. 9, pp. 6443–6453, 2017. See pages 7 and 19.

[15] ——, “Boolean functions for cryptography and coding theory,” 2021. See pages 2, 4, 5, 6, 7, 15, 17, 19, 20, 21, 22, 23, 27, 29, and 31.

[16] ——, “On APN functions whose graphs are maximal Sidon sets,” in *LATIN 2022: Theoretical Informatics: 15th Latin American Symposium, Guanajuato, Mexico, November 7–11, 2022, Proceedings*. Springer, 2022, pp. 243–254. See page 30.

[17] ——, “On the affine subspaces of F_{2^n} over which the multiplicative inverse function sums to zero,” *Preprint*, 2023. See pages 30 and 31.

[18] X.-d. Hou, “Permutation polynomials over finite fields—a survey of recent advances,” *Finite Fields and Their Applications*, vol. 32, pp. 82–119, 2015. See page 2.

[19] ——, *Lectures on finite fields*. American Mathematical Soc., 2018, vol. 190. See page 29.

[20] L. Knudsen and D. Wagner, “Integral cryptanalysis,” in *Fast Software Encryption: 9th International Workshop, FSE 2002 Leuven, Belgium, February 4–6, 2002 Revised Papers 9*. Springer, 2002, pp. 112–127. See page 18.

[21] G. M. Kyureghyan, “Crooked maps in $\mathbb{F}_2^n$,” *Finite Fields and their applications*, vol. 13, no. 3, pp. 713–726, 2007. See pages 6 and 24.

[22] Y. Li and M. Wang, “Constructing differentially 4-uniform permutations over GF(2^{2m}) from quadratic APN permutations over GF(2^{2m+1}),” *Designs, codes and cryptography*, vol. 72, no. 2, pp. 249–264, 2014. See pages 3, 4, 15, and 31.

[23] H. Taniguchi, “D-property for APN functions from $\mathbb{F}_2^n$ to $\mathbb{F}_2^{n+1}$,” *Cryptography and Communications*, pp. 1–21, 2023. See pages 2, 15, 16, 17, 18, 26, and 27.

[24] Y. Zheng, X.-M. Zhang, and H. Imai, “Restriction, terms and nonlinearity of boolean functions,” *Theoretical Computer Science*, vol. 226, no. 1-2, pp. 207–223, 1999. See pages 8 and 9.

A Second part of the proof of Theorem 6

The curve $V_{\mathbb{P}^2(\mathbb{F}_{2^N})}(H)$ has coefficients in $\mathbb{F}_2$, so to prove that for any N odd it is absolutely irreducible, non-singular, and of genus 3 it is enough to study those invariants for $V_{\mathbb{P}^2(\mathbb{F}_2)}(H)$. The following code in MAGMA [5] proves our claims.

```
propertiesCurve:=procedure()
    R<x,y,z>:=ProjectiveSpace(GF(2),2);
    F:=y*(x+y+1)+x*(x+y+1)+x*y;
    G:=Evaluate(F,[x^2+x+1,y^2+y+1,z]);
    H:=Zero(GF(2));
    D:=Degree(G);
    for m in Terms(G) do
      H+:=m*z^(D-Degree(m));
    end for;
    C:=Curve(R,H);
    printf "\n\n";
    printf "F=%o\n",F;
    printf "Set G(x,y)=F(x^2+x+1,y^2+y+1)\n";
    printf "G=%o\n",G;
    printf "The curve has degree %o\n",D;
    printf "Define H as the homogenization of G\n";
    printf "H=%o\n",H;
    printf "C: H=0\n";
    printf "The curve C is absolutely irreducible = %o\n",
    IsAbsolutelyIrreducible(C);
    printf "The curve C is not singular = %o\n",IsNonsingular(C);
    printf "The curve C has genus %o\n",Genus(C);
    printf "\n";
    printf "The curve C does not have points at infinity\n";
    printf "H(x,y,0)=%o\n",Evaluate(H,[x,y,0]);
    printf "By setting y=1, the equation %o=0",
    Evaluate(H,[x,1,0]);
    printf " does not have solution for N odd\n";
end procedure;

propertiesCurve();
```