Restricting vectorial functions to affine spaces and deducing infinite families of 4-uniform permutations, in relation to 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

June 14, 2023

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 $\mathbb{F}_2^N$ to a subset of an affine subspace of dimension n, or at least of a dimension less than M. 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 that if it is zero, there automatically exists a strict affine subspace of its domain that is mapped by $\mathcal{F}$ into a subset of 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 $\mathcal{F}$ 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. We will build upon the follow fact: the restriction of $\mathcal{G}$ over 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 $\mathcal{F}(x) = \psi(\mathcal{G}(x))$ over 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. The fact of not satisfying this nice property is also positive in a way since it allows to construct a number of APN $(N-1, N-1)$-functions from $\mathcal{G}$. We give a characterization of the strong D-property for crooked 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. Completing a result from Taniguchi for $N \geq 6$ even, we can prove that the strong D-property of the Gold APN function in dimension N 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.

We then move our focus to infinite families of $(N-1,N-1)$-permutations constructed as the restriction 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 but with the extra hypothesis that $\mathcal{G}$ is an APN permutation. There are in the literature two families of differentially 4-uniform permutations corresponding to this framework, but no proof was given that they are not APN. We investigate these constructions deeply and prove that they do not produce APN permutations in dimension $n=N-1$ even. We present our own construction and we show a relation between infinite families of APN (N,N)-permutations and infinite families of 4-uniform $(N-1,N-1)$-permutations. This gives a deeper understanding on the problem of constructing infinite families of APN permutations in even dimension (for trying to solve the so-called big APN problem) with the method explored in this paper. This problem is also related to the strong D-property and we conjecture that some classes of APN power permutations have such property in dimension large enough. We show that only few APN permutations do not have the strong D-property (and this happens only for small dimension). Our construction gives many families of 4-uniform $(N-1,N-1)$-permutations with high nonlinearity that are additionally, under some conditions, complete permutations.

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 (whatever it is) are not numerous. One has been much studied: identify $\mathbb{F}_q^n$ with the field $\mathbb{F}_{q^n}$ (thanks to the choice of a basis of the vector space $\mathbb{F}_{q^n}$ over $\mathbb{F}_q$) and search for infinite classes of permutation polynomials. The representation of each permutation is then very simple (we just need a 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 [1, 2]), 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 even functions from $\mathbb{F}_{q^N}$ to itself, such that there exists an n-dimensional affine subspace A of the vector space $\mathbb{F}_{q^N}$ over $\mathbb{F}_q$, that is mapped by $\mathcal{F}$ onto an affine subspace A' of $\mathbb{F}_{q^N}$ of the same dimension; 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 $\mathbb{F}_{q^n}$ - completed into a basis of $\mathbb{F}_{q^N}$ over $\mathbb{F}_q$, and the polynomial representation 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 when the (n,n)-function is not 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 [4] the D-property as a generalization for APN (N, M)-functions of a property proved by Dillon on APN (N, N)-functions. A consequence of the work by Taniguchi in [4] is that the restriction of an APN (N, N)-function $\mathcal{G}$ over 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 $\mathcal{F}(x) = \psi(\mathcal{G}(x))$ over 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 $\mathcal{G}$ over 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 presented as a positive result for some classes of functions (namely power and quadratics); 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 by the restriction of functions with zero nonlinearity was the one constructed by the first author in 2011 [5] by using the 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 [6] 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 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 [5] for the case N even because, in that dimension, the 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 give many families of 4-uniform permutations in $\mathbb{F}_{2^n}$ where $n = N-1$ with high nonlinearity and that are, under some conditions, complete permutation polynomials. 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 inverse function in odd dimension and the inverse of the Gold APN function. Because the importance of showing such nonexistence results, we believe that this is a good argument to conjecture that those two APN power permutations have the strong D-property in dimension N large enough. We leave the difficult proof of these conjectures for future work.

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 (N, M)-function providing an (n, m)-function. The differential uniformity of the restriction is bounded above by the differential uniformity of the starting function. We give an explicit form of the Walsh transform and 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 with affine components that is a sufficient condition for the existence of a strict affine subspace of its domain that is mapped into a subset of 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. 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 use this to conjecture such property. In Section 6, we study the infinite families introduced in [5, 6] and prove that they can never produce APN permutations in even dimension. We give two conjectures on the strong D-property of some power APN permutations and we define many families of 4-uniform permutations with high nonlinearity that are, under some conditions, complete permutation polynomials when represented in $\mathbb{F}_{2^n}$ where $n = N - 1$.

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 [2]. 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 $c_i \neq 0$.

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 $x \cdot y = \mathrm{Tr}_N(\alpha xy)$ 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 [7]) 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 [2]. 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 [2]. 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 [2] (after Corollary 5). The integer 2^k is called the amplitude of f. Function f is called *bent* if $k = N/2$, *near-bent* if $k = (N+1)/2$, and semi-bent if $k = N/2 + 1$. 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 [2, 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 [2] (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 [8].

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 ([7]). *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 $\mathcal{F}$ to a subset of 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 $\mathcal{F}$ to a subset of a strict affine space of the co-domain of $\mathcal{F}$, we shall of course be interested in the cryptographic properties for $\mathcal{F}_A$. 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 $\mathcal{F}$ to a subset of 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 [9, 10]). We shall recall a useful characterization of the APN property.

Proposition 3.2 ([2]). *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 [11, 7], but without that a precise expression of the Walsh transform be exhibited. The results that we shall revisit were obtained in [11] in a complex way and in [7] 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

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

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

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

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 $\ker \psi^* = (\operatorname{Im} \psi)^\perp = (\mathbb{F}_2^m)^\perp = \{0\}$ and $(\phi^{-1})^*$ is also injective because $\ker(\phi^{-1})^* = (\operatorname{Im} \phi^{-1})^\perp = (\mathbb{F}_2^n)^\perp = \{0\}$. 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 $v' \in \operatorname{Im} \psi^* \setminus \{0\}$. By using Lemma 3.4, we have that $v' \in \mathbb{F}_2^M \setminus (E')^\perp$ and we can set $E_2 = \operatorname{Im} \psi^*$. 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 [11, 7]. Observe that by using relation (4), we have that a sufficient condition for $\mathrm{nl}(\mathcal{F}_A) \neq 0$ 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 to a subset of 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. According to Theorem 1, $\mathrm{nl}(\mathcal{F}_A) = 0$ if and only if there exist $b \in \mathbb{F}_2^N$ and $v \in \mathbb{F}_2^M \setminus (E')^\perp$ such that $\left|\sum_{x \in b+E^\perp} (-1)^{x \cdot a} W_\mathcal{F}(x, v)\right| = 2^N$. Using the Poisson summation formula (1), we have then $|\sum_{x\in A}(-1)^{v\cdot\mathcal{F}(x)+b\cdot x}| = 2^n$ and therefore $v \cdot \mathcal{F}(x) + b \cdot x$ is constant on A. Let $f = v \cdot \mathcal{F}(x) + b \cdot x$, then f is a n-normal 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

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. 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 $M = N \geq 3$. We will show that this technique allows to construct more functions than the ones provided by $\mathcal{G}$ since we can drop the nonlinearity to 0 and not be 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 $f_M^{-1}(0)$ to a subset of 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 $A = \{x \in \mathbb{F}_2^N \mid \forall v \in V,\ v \cdot \mathcal{F}(x) = \ell(v)\}$. If $A \neq \emptyset$, then A is an affine space mapped by $\mathcal{F}$ to a subset of 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 to a subset of 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. Being non-empty, it is then 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 (more or less) 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 $v \in \mathrm{Im}\,\psi^*$. 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 $\mathrm{nl}\,(\mathcal{F}_B) = 0$.

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 take 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 $\mathbb{F}_2^M$, that is the one composed by vectors of Hamming weight 1 and "$\cdot$" 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 $V = \langle e_1, \ldots, e_{M-m} \rangle$. Then $V^\perp$ is the vector space of all vectors in $\mathbb{F}_2^M$ that have the firsts $M-m$ coordinates equal to zero 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 $v \in \mathbb{F}_2^N$ 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 so by choosing appropriate $g_1, \ldots, g_{N-m}$ we have that $\mathcal{G} = (g_1, \ldots, g_N)$ has nonzero nonlinearity. Let $N - m < i \leq N$ and let $\bar{g}_i$ be the Boolean function obtained by g_i removing all the terms of degree less or equal than 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 we can always find $\bar{g}_1, \ldots, \bar{g}_{N-m} \in \mathbb{V}$ such that $\bar{g}_1, \ldots, \bar{g}_N \in \mathbb{V}$ are linearly independent. Since any linear combinations using elements of $\mathbb{V}$ can only result in either the zero function or a Boolean function with algebraic degree at least 2, we can conclude the proof by setting $g_i = \bar{g}_i$ for $i \leq N - m$.

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 $i \leq N - m$. Let

$\mathcal{L}(x) = \mathcal{A}(x)+x$, then we have that $\mathcal{F}(x) = \psi(\mathcal{G}(x))+\mathcal{A}(x) = \psi(\mathcal{G}'(x))+x$ where $\mathcal{G}' = \mathcal{G}+\mathcal{L}$ because $\psi\circ\mathcal{L} = \mathcal{L}$. 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, 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.*

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 with image of 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

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

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 follows directly. □

The following proposition groups together two known results that have been rediscovered several times (for instance, in [6, 4]). 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 [2, Proposition 161]. Conversely if $\delta_{\mathcal{F}} = 4$, then $\mathcal{G}$ is differentialy 4-uniform again by Theorem 2.

Let us prove 2. Let $n = N - 1$. Using 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 are no bent (n, n)-functions for $n \geq 3$, then $\mathrm{nl}(\mathcal{F}_A) = 2^{n-1} - 2^{\frac{n}{2}}$. □

In the setting of Proposition 4.6, we can conclude that to construct APN $(N-1, N-1)$-functions we can assume that $\mathcal{G}$ is differentialy 4-uniform and has nonzero nonlinearty by Proposition 4.3.

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 [4]. This will motivate the introduction of the notion of strong D-property. We will investigate this property for crooked functions and for their inverse when they exists. 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 use this to 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 to study the differential uniformity of restrictions (see Theorem 2), while this information could be overlooked by using their notion. 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 $v_0 \in \mathbb{F}_2^N \setminus \operatorname{Im} \psi^*$.

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 $\mathcal{F}_A$ is APN if and only if for any $a \in E \setminus \{0\}$ we have that $\delta_{\mathcal{G}_A}(a, b)$ is nonzero (that equals 2 because $\mathcal{G}_A$ is APN) for some $b \in \mathbb{F}_2^N$ implies $\delta_{\mathcal{G}_A}(a, b+c) = 0$. 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 [2] (after Proposition 161). Using that as a motivation, Taniguchi in [4] 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 APN (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 $\mathcal{G}_A$ over 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 [4, 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 $\mathbb{F}_2^N$.

If $\mathcal{G}$ is APN, 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 integral attacks (see [12]). 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 a good thing too 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 a number of 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 not CCZ invariant, which is less intuitive, 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 [4] studies the D-property of $(N-1, N)$-functions constructed as the restrictions of APN (N, N)-functions over 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 [4] 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 it is enough to verify the strong D-property on only one linear hyperplane 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 $\pi' = \{vx : x \in \pi\}$ 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. It follows from Lemma 5.1 and the fact that since $\mathcal{G}$ is quadratic, we have for all $a, b, x \in \mathbb{F}_2^N$ that $D_a D_b \mathcal{G}(x) = D_a D_b \mathcal{G}(0) = \varphi_{\mathcal{G}}(a, b)$ where $\varphi_{\mathcal{G}}(a, b) = \mathcal{G}(a+b) + \mathcal{G}(a) + \mathcal{G}(b) + \mathcal{G}(0)$.

Proposition 5.4. *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 5.4 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 [2, Corollary 18], 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 5.12 below that such extension exists, but it will require a more complicated argument.

Remark 5.5. *By combining Remark 5.3 and Proposition 5.4, it is enough for the Gold APN function to verify the strong D-property on the linear hyperplane $\{x \in \mathbb{F}_{2^N} \mid \mathrm{Tr}(x) = 0\}$ (and it is the only function, up to EA equivalence, for which we can do this).*

Regarding the strong D-property of quadratic APN (N, N)-function, we can say something more for the case N even depending on the amplitude of its components. We cannot say much for the case N odd since, in that case, all quadratic APN functions are automatically AB.

Proposition 5.6. *Let $\mathcal{G}$ be a quadratic APN function in even dimension N. Then we have the following:*

1. *If there are at least two linearly independent components of $\mathcal{G}$ that are not bent and not semi-bent, then $\mathcal{G}$ has the strong D-property.*

2. *If $\mathcal{G}$ has the strong D-property, then $\mathrm{nl}(\mathcal{G}) > 2^{N-2}$.*

Proof. We recall that for any quadratic function in odd dimension the APN property is equivalent to the AB property.

Let us prove 1. Suppose that $\mathcal{G}$ does not have the strong D-property. Then there exist an affine hyperplane A and $c \in \mathbb{F}_2^N \setminus \{0\}$ such that $\mathcal{G}(x)+\mathcal{G}(y)+\mathcal{G}(z)+\mathcal{G}(x+y+z) \neq c$ for all $x, y, z \in A$. By Lemma 5.1, we have that for any linear function ψ with $\ker \psi = \langle c \rangle$ the function $\mathcal{F}_A$ is an APN $(N-1, N-1)$-function where $\mathcal{F}(x) = \psi(\mathcal{G}(x))$. So $\mathcal{F}_A$ is AB because it is a quadratic APN function in dimension $N-1$ odd. Let $v_1, v_2 \in \mathbb{F}_2^N$ be linearly independent and such that $v_1 \cdot \mathcal{G}$ and $v_2 \cdot \mathcal{G}$ have amplitude respectively λ_1 and λ_2 strictly greater than $2^{N/2+1}$. Since $\operatorname{Im} \psi^{\perp}$ has dimension 1, we can suppose that $v_1 \in \mathbb{F}_2^N \setminus \operatorname{Im} \psi^{\perp}$. Therefore, there exists $u \in \mathbb{F}_2^N$ such that $\frac{1}{2} \left| \sum_{z \in E^{\perp}} (-1)^{a \cdot z} W_{\mathcal{G}}(u+z, v_1) \right| \geq \lambda_1/2$ where $A = a + E$. By Theorem 1 and Theorem 2, we have $\mathrm{nl}(\mathcal{F}_A) \leq 2^{N-2} - \lambda_1/4 < 2^{N-2} - 2^{N/2-1}$ that is a contradiction because $\mathcal{F}_A$ is AB.

Let us prove 2. If $\mathrm{nl}(\mathcal{G}) \leq 2^{N-2}$, then we that $\mathrm{nl}(\mathcal{G}) = 2^{N-2}$ because it is the minimum nonlinearity that a quadratic APN function can achieve. It is proven in [9, 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 a subset of 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 5.7. *Using Proposition 5.6, we have that the extended Walsh spectrum of a quadratic APN function $\mathcal{G}$ in even dimension N can give additional information on the strong D-property. We recall that the number of nonzero Walsh values in a plateaued function over $\mathbb{F}_2^N$ of amplitude 2^k is 2^{2N-2k} (according to Parseval's relation). As a consequence, we have that many of the quadratic APN function in dimension 8 discovered in [10] have the strong D-property. Namely the ones that have the value $2^6 = 64$ appearing $2 \cdot 2^{16-12} = 32$ times in the extended Walsh spectrum. Regarding quadratic APN functions with nonlinearity 2^{N-2}, we know that they exist in dimension 6 [13] and 8 [10]. Moreover, we can conclude that they have only one component of amplitude 2^{N-1} and the rest are either bent or semi-bent because otherwise such functions have the strong D-property and we know they do not have it. The situation is unclear for quadratic APN functions that either have Gold-like spectrum (all components bent or semi-bent) or have one and only one component with amplitude 2^k where $N/2+1 < k < N-1$ and all the other components are bent or semi-bent. Functions of the first kind are very common among the known APN functions [2], while examples of functions of the second kind can be found in dimension 8 [10] where $k = 6$ but there is no clear indication of how common they are in higher dimension.*

5.2 The strong D-property of crooked functions

We are going to study the strong D-property of crooked functions. Abbondati et al. in [14] proved a characterization of the D-property of strongly plateaued APN $(N-1, N)$-functions obtained as the restriction of strongly plateaued APN (N, N)-functions (that are crooked; see e.g. [2] after Definition 68) where N is odd. The characterization we are going to present is similar, but with some important differences. It is valid for any N, fast to verify, and practical for proving that some classes of functions have the strong D-property for N large enough. As a consequence, we will present a characterization of the strong D-property for APN permutations with quadratic inverse.

Remark 5.8. *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. [2] (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).*

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 $\pi_{\mathcal{G}}$. In the following proposition, we give an expression for such Walsh transform.

Proposition 5.9. *Let $\mathcal{G}$ be a crooked (N, N)-function with $N \geq 3$. Let $\pi_{\mathcal{G}}$ be the ortho-derivative of $\mathcal{G}$. 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 $w \in \mathbb{F}_2^N$. Then 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. Let $u, v \in \mathbb{F}_2^N$ and set

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

We have that

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

since we know that $\sum_{w \in \mathbb{F}_2^N} (-1)^{w \cdot y} = 2^N \delta_0(y)$. 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 have that

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

□

Remark 5.10. *Let $\mathcal{G}$ be a crooked (N,N)-function with $N \geq 3$. We give some preliminary observations on the cardinality of sets $\Lambda_c = \{(a,b) \in (\mathbb{F}_2^N)^2 \mid \varphi_{\mathcal{G}}(a,b) = c\}$ where $c \in \mathbb{F}_2^N$. Observe that since $\mathcal{G}$ is strongly plateaued, then $|\Lambda_c| = |\{(a,b) \in (\mathbb{F}_2^N)^2 \mid D_aD_b\mathcal{G}(u) = c\}|$ for any $u \in \mathbb{F}_2^N$ [2, Corollary 18]. Therefore, $|\Lambda_c| \neq 0$ because $\mathcal{G}$ has the D-property. If $c = 0$, we have that $|\Lambda_0| = 3 \cdot 2^N - 2$ [2, Proposition 172]. Otherwise, $|\Lambda_c|$ is divisible by 6. 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). To conclude, let us prove that for any $(a,b),(a',b') \in \Lambda_c$ the two sets $S = \{a,b,a+b\}$ and $S' = \{a',b',a'+b'\}$ are either equal or disjoint. If $S \cap S'$ is not empty, then let $x \in S \cap S'$. Take $y \in \mathbb{F}_2^N$ such that $(x,y) \in \Lambda_c$ then because $\mathcal{G}$ is APN, y is also in $S \cap S'$. Hence, $\{x,y,x+y\}$ is contained in $S \cap S'$ and so $\{x,y,x+y\} = S \cap S'$ because $S \cap S'$ has cardinality at most 3. Therefore, the sets S, S' are both equal to $\{x,y,x+y\}$.*

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 $\lambda^{\min} = 2^N - 2 = \lambda^{\max}$ [2, 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).

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

Lemma 5.11. *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*

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

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

Proof. Let $c, v \in \mathbb{F}_2^N \setminus \{0\}$. We claim that $|\Gamma_{v,c}^{(1)}| < \frac{|\Lambda_c|}{3}$ if and only if, for all $u \in \mathbb{F}_2^N$, there exist $a, b \in \mathbb{F}_2^N$ such that $\mathcal{G}(a+b+u)+\mathcal{G}(a+u)+\mathcal{G}(b+u)+\mathcal{G}(u) = c$ and $v \cdot a = v \cdot b = 0$. To prove that, we show in a first step that $|\Gamma_{v,c}^{(1)}| < \frac{|\Lambda_c|}{3}$ if and only if there exists $(a,b) \in \Lambda_c$ with $v \cdot a = v \cdot b = 0$. As a second step, we will show that if there exists $u \in \mathbb{F}_2^N$ such that $\mathcal{G}(a+b+u)+\mathcal{G}(a+u)+\mathcal{G}(b+u)+\mathcal{G}(u) = c$ 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 $\mathcal{G}(a+b+u)+\mathcal{G}(a+u)+\mathcal{G}(b+u)+\mathcal{G}(u) = c$ and $v \cdot a = v \cdot b = 0$ (this implication is then an equivalence, since the converse is of course true). With these two steps proven, we can conclude the proof. Suppose that $|\Gamma_{v,c}^{(1)}| < \frac{|\Lambda_c|}{3}$ 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 $c \in \mathbb{F}_2^N \setminus \{0\}$. Since $|\Gamma_{v,c}^{(1)}| < \frac{|\Lambda_c|}{3}$, then there exist $a, b \in \mathbb{F}_2^N$ such that $\mathcal{G}(a+b+u)+\mathcal{G}(a+u)+\mathcal{G}(b+u)+\mathcal{G}(u) = c$ and $v \cdot a = v \cdot b = 0$. So 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. 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 exists $x, y, z \in \mathbb{F}_2^N$ 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, for all all $u \in \mathbb{F}_2^N$, there exist $a, b \in \mathbb{F}_2^N$ such that $\mathcal{G}(a + b + u) + \mathcal{G}(a + u) + \mathcal{G}(b + u) + \mathcal{G}(u) = c$ and $v \cdot a = v \cdot b = 0$. So we have that $|\Gamma_{v,c}^{(1)}| < \frac{|\Lambda_c|}{3}$.

We prove now the first step. 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 $|\Gamma_c| = |\Lambda_c|/2$ because if $a \in \Gamma_c$ then $\{b \in \mathbb{F}_2^N \mid (a, b) \in \Lambda_c\}$ contains two elements exactly, since $\mathcal{G}$ is APN (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 $(a, b) \in \Lambda_c$ (see Remark 5.10) and 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 $|\Gamma_{v,c}^{(1)}| \leq (2/3)|\Gamma_c| = |\Lambda_c|/3$ 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 $|\Gamma_{v,c}^{(1)}| < |\Lambda_c|/3$ 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 $v \cdot a = v \cdot b = 0$.

Let us prove now the second step. Let us fix $u \in \mathbb{F}_2^N$ and observe that $\mathcal{G}_u(x) = \mathcal{G}(x + u)$ is also crooked. Set $\Lambda_c(u) = \{(a, b) \in (\mathbb{F}_2^N)^2 \mid \varphi_{\mathcal{G}_u}(a, b) = c\}$ and $\Gamma_{v,c}^{(1)}(u) = \{a \in \mathbb{F}_2^N \mid c \cdot \pi_{\mathcal{G}_u}(a) = 0,\ v \cdot a = 1\}$. Using what we have proven in the previous paragraph, we have that $|\Gamma_{v,c}^{(1)}(u)| < |\Lambda_c(u)|/3$ if and only if there exist $a, b \in \mathbb{F}_2^N$ such that $\varphi_{\mathcal{G}_u}(a, b) = \mathcal{G}(a+b+u)+\mathcal{G}(a+u)+\mathcal{G}(b+u)+\mathcal{G}(u) = c$ 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 $|\Gamma_{v,c}^{(1)}(u_1)| < |\Lambda_c(u_1)|/3$ if and only if $|\Gamma_{v,c}^{(1)}(u_2)| < |\Lambda_c(u_2)|/3$. It follows from the fact that $|\Lambda_c(u_1)| = |\Lambda_c(u_2)|$ because $\mathcal{G}$ is strongly plateaued [2, Corollary 18] and that $\Gamma_{v,c}^{(1)}(u_1) = \Gamma_{v,c}^{(1)}(u_2)$ because $\pi_{\mathcal{G}_{u_1}} = \pi_{\mathcal{G}_{u_2}}$. □

In the following proposition, we show (as announced after Proposition 5.4) that Proposition 5.4 holds even if we assume that $\mathcal{G}$ is crooked instead of quadratic APN. 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 5.12. *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 that $\varphi_{\mathcal{G}}(a, b) \neq c$.*

Proof. Let $E = \langle v \rangle^\perp$ for some $v \in \mathbb{F}_2^N \setminus \{0\}$. Using the second step of the proof of Lemma 5.11, we have that if there exist $a, b \in \mathbb{F}_2^N$ such that $\varphi_{\mathcal{G}}(a, b) = c$ and $v \cdot a = v \cdot b = 0$, then for all $u \in \mathbb{F}_2^N$ there exists $a, b \in \mathbb{F}_2^N$ such that $\mathcal{G}(a+b+u)+\mathcal{G}(a+u)+\mathcal{G}(b+u)+\mathcal{G}(u) = c$ and $v \cdot a = v \cdot b = 0$. This is enough to conclude the proof by Lemma 5.1 because $A = u + E$ for some $u \in \mathbb{F}_2^N$. □

Remark 5.13. *Thanks to Proposition 5.9, the condition in Lemma 5.11, 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* $c, v \in \mathbb{F}_2^N \setminus \{0\}$ *and set* $\Gamma_{v,c}^{(0)} = \{a \in \Gamma_c \mid v \cdot a = 0\}$*. Since*

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

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* $|\Gamma_{c,v}^{(1)}| = \frac{|\Lambda_c| + 2 - W_{\pi_{\mathcal{G}}}(v,c)}{4}$*. So one can check by means of the Walsh transform the strong D-property by using Lemma 5.11. This way of checking the strong D-property is fast because it reduces to the computation of the Walsh transform of a function.*

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 such that* $\mathrm{nl}(\pi_{\mathcal{G}}) = 2^{N-1} - (\omega/2)$*. If* $\omega < (\lambda^{\min}/3) - 2$*, then* $\mathcal{G}$ *has the strong D-property.*

Proof. Let $c, v \in \mathbb{F}_2^N \setminus \{0\}$. We have that $W_{\pi_{\mathcal{G}}}(v,c) = |\Lambda_c| - 4|\Gamma_{c,v}^{(1)}| + 2$ by (8). If we prove that $|\Gamma_{c,v}^{(1)}| < |\Lambda_c|/3$, then by Lemma 5.11 we can conclude that $\mathcal{G}$ has the strong D-property. The hypothesis $\omega < \frac{\lambda^{\min}}{3} - 2$ implies:

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

□

We shall now present in Theorem 4, in the case where $\mathcal{G}$ is a quadratic permutation, a sufficient condition for $\mathcal{G}$ and $\mathcal{G}^{-1}$ to have both the strong D-property, which only depends on the nonlinearity of $\pi_{\mathcal{G}}$, but this time, the second-order nonlinearity. We shall need the next lemma that uses a similar idea to Lemma 5.11. We recall that since $\mathcal{G}$ is an (N,N)-permutation, N must be odd (and therefore $\mathcal{G}$ is AB).

Lemma 5.14. *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* $\varphi_{\mathcal{G}^{-1}}(a,b) = c$ *and* $v \cdot a = v \cdot b = 0$*.*

Proof. Let $(a,b) \in (\mathbb{F}_2^N)^2$ be such that $\varphi_{\mathcal{G}^{-1}}(a,b) = c$ and $v \cdot a = v \cdot b = 0$. Mapping (a,b) into $(\mathcal{G}(a), \mathcal{G}(b))$ we have that $\varphi_{\mathcal{G}^{-1}}(\mathcal{G}(a), \mathcal{G}(b)) + c = 0$ is equivalent to $\mathcal{G}^{-1}(\mathcal{G}(a)+\mathcal{G}(b))+a+b+\mathcal{G}^{-1}(0)+c=0$ and to $\mathcal{G}(a+b+c_0)+\mathcal{G}(a)+\mathcal{G}(b)=0$ and we are led 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 $a\in\mathbb{F}_2^N$ such that $\mathcal{G}(a+b+c_0)+\mathcal{G}(a)+\mathcal{G}(b)=0$ for some $b\in\mathbb{F}_2^N$, then $\Omega_{c,v}^{(1)}$ is the set of all $a\in\Omega_c$ with $v\cdot\mathcal{G}(a)=1$. Note that c_0 is nonzero, since we know that $\mathcal{G}(x)=0$ if and only if $x=\mathcal{G}^{-1}(0)$ and $c_0=c+\mathcal{G}^{-1}(0)$ with $c\neq x$ then implies $c_0\neq 0$. Observe that since $\mathcal{G}(a+b+c_0)+\mathcal{G}(a)+\mathcal{G}(b)=0$ is equivalent to $D_{a+c_0}\mathcal{G}(b)+D_{a+c_0}\mathcal{G}(c_0)=\mathcal{G}(c_0)$, there exists b satisfying this equality if and only if $\mathcal{G}(c_0)$ belongs to the direction of the hyperplane $D_{a+c_0}\mathcal{G}$, and we have then $\Omega_c=\{a\in\mathbb{F}_2^N\setminus\{c_0\}\mid \pi(a+c_0)\cdot\mathcal{G}(c_0)=0\}$. Since $\mathcal{G}$ is AB, then $|\Omega_c|=\frac{2^N-2}{2}$. Moreover, if $(a,b)\in\mathbb{F}_2^N$ is such that $\mathcal{G}(a+b+c_0)+\mathcal{G}(a)+\mathcal{G}(b)=0$, then the number of elements among $\mathcal{G}(a)$, $\mathcal{G}(b)$, and $\mathcal{G}(a+b+c_0)$ that are non-orthogonal to v is necessarily even. Similarly as the proof of Lemma 5.11, we have that $|\Omega_{c,v}^{(1)}|<(2/3)|\Omega_c|=\frac{2^N-2}{3}$ if and only if there exists (a,b) 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. To 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 $f(a)=g(a)+h(a)$ where $g(a)=\mathcal{G}(c_0)\cdot\pi_\mathcal{G}(a+c_0)$ and $h(a)=v\cdot\mathcal{G}(a)$. Let $\gamma_{i,j}=|\{a\in a\in\mathbb{F}_2^N\setminus\{c_0\}\mid g(a)=i,\ h(a)=j\}|$. 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 5.14. Then we will show 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 $\mathcal{G}^{-1}$. Let us 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 $\pi_\mathcal{G}(0)=0$. Then 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 we have that

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

and that

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

Observe that since $-\sum_{a\in\mathbb{F}_2^N}(-1)^{f(a)} \leq \left|\sum_{a\in\mathbb{F}_2^N}(-1)^{f(a)}\right| \leq \omega_2$, then

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

By Lemma 5.14, we have that there exists $a, b \in \mathbb{F}_2^N$ such that $\varphi_{\mathcal{G}^{-1}}(a, b) = c$ and $v \cdot a = v \cdot b = 0$. Let us 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 $u \in \mathbb{F}_2^N$ and 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 $\mathcal{G}(x) = x^{2^i+1}$ be the Gold APN function over $\mathbb{F}_{2^N}$ where $\gcd(i, N) = 1$. 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 5.5). Therefore, we can use some of the results by Taniguchi in [4]. We have that $\mathcal{G}$ has the strong D-property for $N \geq 6$ even [4, Example 6]. By using Theorem 3, we are going to address the case N odd. With this result, all the cases will be covered. To apply Theorem 3, we will prove that the (first-order) nonlinearity of the ortho-derivative of the Gold APN function is greater or equal than the second-order nonlinearity of the inverse function x^{-1}. Then we conclude by using a lower bound proven in [15].

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 $N < 10$ can be verified computationally and the case $N \geq 10$ even follows from [4, Example 6] and Remark 5.5. 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 [16] 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 5.8). 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 [15, 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

$$\sqrt{(2^N-1)2^{N/2+2} + 3\cdot 2^N} < \frac{2^N-2}{3} - 2 \tag{10}$$

holds and conclude by using Theorem 3. Observe that the expression on the left side of (10) is equal to $\sqrt{2^{(3N+4)/2} + 2^{N+1} + 2^N - 2^{(N+4)/2}}$ that is less or 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 (10) holds for $N \geq 11$. □

We observe that for the Gold APN function in even dimension, the values of $\lambda^{\max}$ and $\lambda^{\min}$ defined in Remark 5.10 are known [2] (Example 2 after Theorem 18), so we could have proven similarly that for some positive integer N_0 the Gold APN function has the strong D-property for $N \geq N_0$ even. We didn't do that because the even case was already proven by Taniguchi [4, Example 6].

The ortho-derivatives of other classes of quadratic APN functions can be derived from the work done in the paper [16], 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 [4, Example 16], Taniguchi proved a result on the D-property of the restriction of the Dobbertin APN power function in even dimension over the linear hyperplane $E = \{x \in \mathbb{F}_{2^N} \mid \mathrm{Tr}(x) = 0\}$. We are going to use the same idea in odd dimension, that is to apply [4, Theorem 25] and [4, Theorem 26]. The two theorems together cover all cases of power APN functions x^d since they are all such that $\gcd(d, 2^N-1) = 1$ if N is odd and $\gcd(d, 2^N-1) = 3$ otherwise (this is an observation by Dobbertin stated in [2, Proposition 165]). We group the two theorems in the following lemma.

Lemma 5.15 ([4]). *Let $\mathcal{G}(x) = x^d$ be an APN power function over $\mathbb{F}_{2^N}$ with $N \geq 3$. Let $E_k = \{x \in \mathbb{F}_{2^k} \mid \mathrm{Tr}_k(x) = 0\}$ for any k. Let $t > 2$ be a positive integer such that t divides N and such that t is even if N is even. 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.*

Proposition 5.16. *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. We will use the notation $E_k = \{x \in \mathbb{F}_{2^k} \mid \mathrm{Tr}_k(x) = 0\}$ for any k. 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 5.15. 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 $2^{4t} = 2^{3t} = 2^{2t} = 2^t = 1 \mod 2^t - 1$. The function x^3 over $\mathbb{F}_{2^t}$ has the strong D-property by Theorem 5, so the restriction of x^3 over E_t has the D-property. To prove the case $t = 7$, we use again Lemma 5.15 but this time we consider the restriction over $\mathbb{F}_{2^5}$. 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 $t \geq 2$, 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.*

Unfortunately, all the results obtained by Taniguchi in [4] are only for the case of restrictions over the hyperplane $E = \{x \in \mathbb{F}_{2^N} \mid \mathrm{Tr}(x) = 0\}$ and not its complement A. According to Remark 5.3, proving that for $t \geq 2$ the restriction of the Dobbertin APN function over A has the D-property is the last piece to prove Conjecture 1.

6 On the non-APNness of infinite families of $(N-1, N-1)$-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 $\psi(\mathcal{G}(x)) + x$ or to to $\psi(\mathcal{G}(x))$ where $\mathcal{G}$ has nonzero nonlinearity and ψ is a linear function with kernel of dimension 1. This follows from Proposition 4.3 because either the affine component of $\mathcal{F}$ is constant or it is not. In this section, we will be interested in the case where $\mathcal{G}$ is an APN permutation and we 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 to ours. 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 begin with two examples of differentially 4-uniform permutations in literature which enter in our framework, up to the addition of a linear function, and in which 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 family [5]

We shall discuss the family constructed by the first author in [5] (for a more completed version see [2] Subsection 11.6.4, sixth point) for N odd (which is more interesting since the inverse function, on which the construction is based, is then APN). We are going to prove the family does not contain any APN permutation (in even dimension).

The permutation in even dimension $N-1$ is obtained as the restriction of the (N,N)-function $\mathcal{F}(x) = \frac{1}{x^2+1} + \frac{1}{x+1} + x$ over 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 [5] 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 exists $x, y, z \in \mathbb{F}_{2^N}$ 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

$$\begin{cases} x^{2^N-2} + y^{2^N-2} + (x+y+1)^{2^N-2} = 0 \\ \mathrm{Tr}(x) = \mathrm{Tr}(y) = 1 \end{cases} \tag{11}$$

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 [17, 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 a projective plane 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 $N \geq 7$, system (11) has a solution.*
2. *If $N \geq 5$, 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 (11) 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 (11) 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 (11) has solution if and only if $G(X, Y) = F(X^2+X+1, Y^2+Y+1)$ has a root (X, Y). 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 [18] (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 (11) 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 verify that the restriction* *of $\psi(x^{-1})$ over 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 $(x, y) \in (\mathbb{F}_{2^N})^2$:*

$$\begin{cases} x^{2^N-2} + y^{2^N-2} + (x + y + \epsilon)^{2^N-2} + \epsilon + c = 0 \\ \mathrm{Tr}(x) = \mathrm{Tr}(y) = \epsilon \end{cases} . \qquad (12)$$

According to Remark 5.3, proving that there exists a solution $(x, y) \in (\mathbb{F}_{2^N})^2$ of system (12) 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 the system (12) 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 equal to left side of the first equation of system (12). However, having c and ϵ as parameters of the curve (while above we had only one value for c and one for ϵ) increase 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 19.

6.2 On the non-APNness of Li-Wang families

Li and Wang in [6] 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 kernel of dimension 1, $E = \mathrm{Im}\,\psi$, 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 $\gcd(i, N) = 1$ is the inverse of the Gold APN function [6, 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 $s = i \mod 3$ [6, Theorem 6]. We will show that both families never produce APN permutations (in even dimension $N-1$). Using that 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.

Lemma 6.2. *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 $\mathrm{nl}(x^{-1}) \geq 2^{N-1} - 2^{N/2}$ [2]. 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 $\mathcal{G}(x) = x^{\frac{1}{d}} + \operatorname{Tr}_3^N(x + x^{2^{2s}})$.*

Proof. Observe that $\operatorname{Im}\psi_c = \{x \in \mathbb{F}_{2^N} \mid \operatorname{Tr}(\pi(c)x) = 0\}$ 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. Let $c \in \mathbb{F}_{2^N} \setminus \{0\}$. Using Lemma 5.1, we have that if there exists $a, b \in \mathbb{F}_{2^N}$ such that $\varphi_{\mathcal{G}}(a, b) = c$ and $\operatorname{Tr}(\pi(c)a) = \operatorname{Tr}(\pi(c)b) = 0$, then $\mathcal{F}_E$ is not APN. To prove the existence of such a and b, we are going to use Lemma 5.14. Let $c_0 = c + \mathcal{G}(0)$ and $\Omega^{(1)}_{c,\pi(c)} = \{a \in \mathbb{F}_2^N \setminus \{c_0\} \mid \operatorname{Tr}(\pi(a + c_0)\mathcal{G}^{-1}(c_0)) = 0,\ \operatorname{Tr}(\pi(c)\mathcal{G}^{-1}(a)) = 1\}$. Using Lemma 5.14, we have that if $|\Omega^{(1)}_{c,\pi(c)}| < \frac{2^N-2}{3}$, then there exists $a, b \in \mathbb{F}_{2^N}$ such that $\varphi_{\mathcal{G}}(a, b) = c$ and $\operatorname{Tr}(\pi(c)a) = \operatorname{Tr}(\pi(c)b) = 0$. Since $\pi(x) = x^{-d}$, $\mathcal{G}^{-1}(x) = x^d$, and $\mathcal{G}(0) = 0$ then $\Omega^{(1)}_{c,\pi(c)} = \{a \in \mathbb{F}_2^N \setminus \{c\} \mid \operatorname{Tr}((a + c)^{-d}c^d) = 0,\ \operatorname{Tr}(c^{-d}a^d) = 1\}$. Notice that

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

where in the first equality we use the substitution $a := a + c$, in the second we use the fact that $\operatorname{Tr}(c^{-d}(a + c)^d) = \operatorname{Tr}(c^{-d}a^d) + 1$, and in the third we use the substitution $a := a^{-d}c^d$. So we have that $|\Omega^{(1)}_{c,\pi(c)}| + |\{a \in \mathbb{F}_{2^N} \mid \operatorname{Tr}(a) = 1,\ \operatorname{Tr}(a^{-1}) = 0\}| = |\{a \in \mathbb{F}_{2^N} \setminus \{0\} \mid \operatorname{Tr}(a^{-1}) = 0\}| = 2^{N-1} - 1$ and $|\Omega^{(1)}_{c,\pi(c)}| \leq 2^{N-1} - 1 - 2^{N-2} + 2^{N/2-1} = 2^{N-2} + 2^{N/2-1} - 1$ by Lemma 6.2. We conclude by observing that $2^{N-2} + 2^{N/2-1} - 1 < \frac{2^N-2}{3}$ 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 $\mathcal{F}(x) = \psi_1(\mathcal{G}(x)) = \psi_1(x^{\frac{1}{d}}) + \psi_1(\operatorname{Tr}_3^N(x + x^{2^{2s}}))$ (see Remark 4.4). $\square$

With the previous theorem, 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 19.

6.3 On a general construction for families of permutations

We will build upon the results by Li and Wang in [6] to investigate completely the problem of constructing an $(N-1, N-1)$-permutation from an (N, N)-function $\mathcal{F}(x) = \psi(\mathcal{G}(x))$ where ψ is a linear function with kernel of dimension 1 and $\mathcal{G}$ is a permutation. Then we discuss the case where $\mathcal{F}(x)$ is equal to $\psi(\mathcal{G}(x)) + x$ instead. In this way, we provide many families of permutations with good cryptographic properties.

We will present the *Li-Wang construction* with our notation.

Construction 1 (Li-Wang construction [6])**.** *Let $\mathcal{G}$ be an APN permutation over $\mathbb{F}_{2^N}$ with quadratic compositional inverse $\mathcal{G}^{-1}$ and such that $\mathcal{G}(0) = 0$. So N is odd because quadratic APN permutations exist only in odd dimension [2, Subsection 11.3.4]. For any $c \in \mathbb{F}_{2^N} \setminus \{0\}$ the function $\psi_c(y) = \mathcal{G}^{-1}(y) + \mathcal{G}^{-1}(y + c) + \mathcal{G}^{-1}(c)$ is linear with kernel of dimension 1. Li and Wang proved that by taking $\mathcal{F}(x) = \psi_c(\mathcal{G}(x))$, the restriction $\mathcal{F}_E$ where $E = \operatorname{Im}\psi_c$ is a permutation with differential uniformity 4 [6, Theorem 2] and optimal known nonlinearity in even dimension [6, Theorem 3], that is $2^{n-1} - 2^{\frac{n}{2}}$ where $n = N - 1$. We will prove that if A is the complement of E, then also $\mathcal{F}_A$ is a permutation and it is CCZ equivalent to $\mathcal{F}_E$. Even if Li and Wang in [6] did not discuss the function $\mathcal{F}_A$, we will still say that it is a product of the Li-Wang construction.*

With the following Lemma (heavily inspired by the first part of [6, Theorem 2]) we are going to exhibit some necessary and sufficient conditions such that the restriction over an affine hyperplane of a function of the form $\psi(\mathcal{G}(x))$ is a permutation when $\mathcal{G}$ is a permutation and ψ is linear with kernel of dimension 1.

Lemma 6.3. *Let $\mathcal{G}$ be a permutation over $\mathbb{F}_{2^N}$, let $v, c \in \mathbb{F}_{2^N} \setminus \{0\}$, let $E = \{x \in \mathbb{F}_{2^N} \mid \operatorname{Tr}(vx) = 0\}$, let A be the complement of E, and let ψ be any linear function over $\mathbb{F}_{2^N}$ with $\ker\psi = \langle c \rangle$. Let $\mathcal{F}(x) = \psi(\mathcal{G}(x))$ and let $\mathcal{B}(x) = \mathcal{G}^{-1}(\mathcal{G}(x) + c)$. Then the following are equivalent:*

1. *$\mathcal{F}_E$ is a permutation.*
2. *$\mathcal{B}(E) = A$.*
3. *$\mathcal{F}_A$ is a permutation.*
4. *$\operatorname{Tr}(v\mathcal{B}(x)) = \operatorname{Tr}(vx) + 1$ for all $x \in \mathbb{F}_{2^N}$.*
5. *$\operatorname{Tr}(vD_c\mathcal{G}^{-1}(x)) = 1$ for all $x \in \mathbb{F}_{2^N}$.*

Proof. We observe that for $x, y \in \mathbb{F}_{2^N}$ with $x \neq y$, we have that $\mathcal{F}(x) = \mathcal{F}(y)$ if and only if $\mathcal{G}(x) + \mathcal{G}(y) \in \ker\psi$. Since $\mathcal{G}$ is a permutation, this happens only if $\mathcal{G}(x) + \mathcal{G}(y) = c$. Observe that the latter equation is equivalent to the equation $y = \mathcal{G}^{-1}(\mathcal{G}(x) + c) = \mathcal{B}(x)$.

Let us prove that 1 implies 2. Suppose that there exists $x \in E$ such that $y = \mathcal{B}(x) = \mathcal{G}^{-1}(\mathcal{G}(x) + c)$ is in E. Then $\mathcal{G}(x) + \mathcal{G}(y) = c$ and this is a contradiction since $\mathcal{F}_E$ is a permutation. So $\mathcal{B}(E) \subseteq A$ and therefore $\mathcal{B}(E) = A$ because $\mathcal{B}$ is a permutation.

Let us prove that 2 implies 1. Suppose that there exists $x, y \in E$ with $x \neq y$ and $\mathcal{G}(x) + \mathcal{G}(y) = c$. Then $y = \mathcal{B}(x)$, but this is not possible because $\mathcal{B}(E) = A$.

To prove that 2 and 3 are equivalent, the argument is similar to the proof that 2 and 1 are equivalent. Indeed, we have that 2 is equivalent to $\mathcal{B}(A) = E$ because $\mathcal{B}$ is a permutation.

We have that 2 and 4 are equivalent since $\mathcal{B}(E) = A$ (resp. $\mathcal{B}(A) = E$) is equivalent to having that, for any $x \in \mathbb{F}_{2^N}$ such that $\mathrm{Tr}(vx) = 0$ (resp. $\mathrm{Tr}(vx) = 1$), we have that $\mathrm{Tr}(v\mathcal{B}(x)) = 1$ (resp. $\mathrm{Tr}(v\mathcal{B}(x)) = 0$).

We have that 4 and 5 are equivalent since $\mathcal{B}(x) + x = \mathcal{G}^{-1}(\mathcal{G}(x) + c) + x = \mathcal{G}^{-1}(\mathcal{G}(x) + c) + \mathcal{G}^{-1}(\mathcal{G}(x)) = D_c\mathcal{G}^{-1}(y)$ for $y = \mathcal{G}(x)$. □

As a consequence of Lemma 6.3, we have that the Li-Wang construction (Construction 1) produces two permutations that are $\mathcal{F}_E$ and $\mathcal{F}_A$.

We observe that Condition 5 on $\mathcal{G}^{-1}$ in Lemma 6.3 is met by any crooked permutation because the image of every derivative (with nonzero direction) is an affine hyperplane that is not linear [2] (see after Definition 68). So the Li-Wang construction (Construction 1) is in this framework because quadratic APN functions are crooked. The simplest example is the Gold APN function in odd dimension. However, $\mathcal{G}^{-1}$ can be not crooked and satisfy condition 5 of Lemma 6.3. As an example, Li and Wang constructed in [6, Theorem 6] a family of permutations where $\mathcal{G}^{-1}$ is not crooked. They showed that for $\mathcal{G}(x) = x^{\frac{1}{2^i+1}} + \mathrm{Tr}_3^N(x + x^{2^{2s}})$ with N odd divisible by 3, $\gcd(i, N) = 1$, and $s = i \mod 3$, we have that $\mathrm{Tr}(D_1\mathcal{G}^{-1}(x)) = 1$ for all $x \in \mathbb{F}_{2^N}$ [6, Lemma 5] and that the restriction of $\mathcal{F}(x) = \mathcal{G}(x)^{2^i} + \mathcal{G}(x)$ over $E = \{x \in \mathbb{F}_{2^N} \mid \mathrm{Tr}(x) = 0\}$ is a permutation. But their result is less exciting after observing that $\mathcal{F}_E$ is EA equivalent to family [6, Theorem 4], that is the restriction of $x^{\frac{2^i}{2^i+1}} + x^{\frac{1}{2^i+1}}$ over E because the two functions in dimension N are EA equivalent (see Remark 4.4). So it still remains unclear if it is possible to use Lemma 6.3 to construct a permutation in dimension $N-1$ using an APN permutation $\mathcal{G}$ which is EA inequivalent to any permutation with quadratic inverse.

Using Lemma 6.3, we are now going to define our construction.

Construction 2. *Let $N \geq 4$ be a positive integer, let $\mathcal{G}$ be a permutation over $\mathbb{F}_{2^N}$, and let $v, c \in \mathbb{F}_{2^N} \setminus \{0\}$ be such that $\mathrm{Tr}(vD_c\mathcal{G}^{-1}) = 1$. Let $E = \{x \in \mathbb{F}_{2^N} \mid \mathrm{Tr}(vx) = 0\}$, let A be the complement of E, and let ψ be any linear function over $\mathbb{F}_{2^N}$ with $\ker\psi = \langle c\rangle$. By Lemma 6.3, we have that $\mathcal{F}_E$ and $\mathcal{F}_A$ are permutations where $\mathcal{F}(x) = \psi(\mathcal{G}(x))$. By Theorem 2, both functions have nonlinearity greater or equal than $\mathrm{nl}(\mathcal{G}) - 2^{N-2}$ and they are 2δ-uniform if $\mathcal{G}$ is δ-uniform (in particular, they are 4-uniform if $\mathcal{G}$ is APN).*

Proposition 6.4. *The Li-Wang construction (Construction 1), the family defined in [6, Theorem 4], and the one defined in [6, Theorem 6] are a particular case of Construction 2.*

Proof. The framework of Construction 2 is exactly the one given in Lemma 6.3 and we have already shown that the Li-Wang construction and those families are in such framework. □

In the following lemma, we give a description of $(\mathcal{F}_E)^{-1}$ (resp. $(\mathcal{F}_A)^{-1}$) by following a similar idea to [6, Proposition 2]. This gives a sufficient condition to have that $\mathcal{F}_E$ and $\mathcal{F}_A$ are CCZ equivalent.

Lemma 6.5. *In the setting of Construction 2, the following holds on $\mathcal{F}(x) = \psi(\mathcal{G}(x))$:*

1. *Defining the two functions over* $\mathbb{F}_{2^N}$*:*

$$\mathcal{H}(x) = \mathcal{G}^{-1}(x) + \mathrm{Tr}\left(v\mathcal{G}^{-1}(x)\right) D_c\mathcal{G}^{-1}(x)$$

   and $\mathcal{H}'(x) = \mathcal{H}(x) + D_c\mathcal{G}^{-1}(x)$*, we have that for every linear hyperplane* E_0 *in* $\mathbb{F}_{2^N}$ *such that* $c \notin E_0$*, function* $(\mathcal{F}_E)^{-1}$ *is affine equivalent to* $\mathcal{H}_{E_0}$ *and function* $(\mathcal{F}_A)^{-1}$ *is affine equivalent to* $\mathcal{H}'_{E_0}$*.*

2. *If the function* $D_c\mathcal{G}^{-1}(x)$ *is affine, then* $\mathcal{F}_E$ *is CCZ equivalent to* $\mathcal{F}_A$*.*

Proof. Let us prove 1. Let $a \in \mathbb{F}_{2^N}$. Observe that the restriction of ψ over E_0 is bijective with codomain $\mathrm{Im}\,\psi$ because $E_0 \cap \ker\psi = \{0\}$ and E_0 has the same cardinality as $\mathrm{Im}\,\psi$. We claim that $\mathcal{H}_{E_0} = (\mathcal{F}_E)^{-1} \circ \psi_{E_0}$ and $\mathcal{H}'_{E_0} = (\mathcal{F}_A)^{-1} \circ \psi_{E_0}$. To prove it, we show that for any linear function ψ' such that $\psi'_{\mathrm{Im}\,\psi} = (\psi_{E_0})^{-1}$ we have that $\mathcal{H}_{E_0} = (\psi'_{\mathrm{Im}\,\psi} \circ \mathcal{F}_E)^{-1}$ and $\mathcal{H}'_{E_0} = (\psi'_{\mathrm{Im}\,\psi} \circ \mathcal{F}_A)^{-1}$. Let $x \in a+E$ and $y = \psi'(\mathcal{F}(x))$. We claim that $x = \mathcal{H}(y)$ if $a \in E$ and $x = \mathcal{H}'(y)$ otherwise and this will conclude the proof. Observe that $y = \mathcal{G}(x)$ if $\mathcal{G}(x) \in E_0$ and $y = \mathcal{G}(x) + c$ otherwise. This implies that $y = \mathcal{G}(x)$ if $\mathrm{Tr}\left(v\mathcal{G}^{-1}(y)\right) = \mathrm{Tr}\,(vx) = \mathrm{Tr}(va)$ and that $y = \mathcal{G}(x)+c$ if $\mathrm{Tr}\left(v\mathcal{G}^{-1}(y)\right) = \mathrm{Tr}\left(v\mathcal{G}^{-1}(y+c)\right)+1 = \mathrm{Tr}\,(vx)+1 = \mathrm{Tr}(va)+1$. Let $g(y) = \mathrm{Tr}\left(v\mathcal{G}^{-1}(y)\right) + \mathrm{Tr}(va)$, then

$$x = \begin{cases} \mathcal{G}^{-1}(y) & \text{if } g(y) = 0, \\ \mathcal{G}^{-1}(y+c) & \text{otherwise.} \end{cases}$$

Since we have that

$$\begin{aligned} x =& (g(y)+1)\mathcal{G}^{-1}(y) + g(y)\mathcal{G}^{-1}(y+c) \\ =& \mathcal{G}^{-1}(y) + g(y)D_c\mathcal{G}^{-1}(y), \end{aligned}$$

then $x = \mathcal{H}(y)$ if $a \in E$ and $x = \mathcal{H}'(y)$ otherwise.

Let us prove 2. Let E_0 be a linear hyperplane such that $c \notin E_0$. Using 1, we have that $(\mathcal{F}_E)^{-1}$ is affine equivalent to $\mathcal{H}_{E_0}$ and $(\mathcal{F}_A)^{-1}$ is affine equivalent to $\mathcal{H}'_{E_0}$. Since the function $D_c\mathcal{G}^{-1}(x)$ is affine and $\mathcal{H}'(x) = \mathcal{H}(x)+D_c\mathcal{G}^{-1}(x)$, then $\mathcal{H}_{E_0}$ and $\mathcal{H}'_{E_0}$ are EA equivalent (see Remark 4.4). Therefore, function $(\mathcal{F}_E)^{-1}$ is EA equivalent to function $(\mathcal{F}_A)^{-1}$ and so function $\mathcal{F}_E$ is CCZ equivalent to function $\mathcal{F}_A$. ☐

In the proof of Lemma 6.5, we showed the existence of a sequence of inversions, EA transformations, and affine transformations which transforms $\mathcal{F}_E$ into $\mathcal{F}_A$ and we deduced that these two functions are CCZ equivalent by the transitivity of the CCZ equivalence relation. This is possible because we have imposed that $D_c\mathcal{G}^{-1}$ is an affine function, so the equivalence may not be true in the general setting of Construction 2. Regarding EA equivalence, we verified computationally that there are some examples where $\mathcal{F}_E$ and $\mathcal{F}_A$ are CCZ equivalent but not EA inequivalent. We did our investigation for the case of the function $\mathcal{G}(x) = x^{\frac{1}{2^i+1}}$ with $\gcd(i, N) = 1$ for $N \in \{7, 9\}$ (see Construction 2). Observe that the choice of ψ does not matter as long as the kernel is equal to $\langle c\rangle$, because changing ψ (with the same kernel) result in affine equivalent functions. We have that $\mathcal{F}_E$ and $\mathcal{F}_A$ are CCZ equivalent by Lemma 6.5 because $D_c\mathcal{G}^{-1}(x) = cx^{2^i} + c^{2^i}x + c^{2^i+1}$ is linear. We verified computationally that for $c = 1$ (so v must be 1) we have that $\mathcal{F}_E$ and $\mathcal{F}_A$ are not EA equivalent. For

$c \notin \mathbb{F}_2$ we have that, in some cases (but not all of them), $\mathcal{F}_E$ and $\mathcal{F}_A$ are EA equivalent. This shows that, in some cases, we are able to construct a new function more than the ones constructed by Li and Wang in [6].

In [6, Theorem 5], Li and Wang observed that the family constructed in [6, Theorem 4] using the inverse of the Gold APN function, can be twisted to increase the algebraic degree of the compositional inverse. They show that $\mathcal{F}'_E$ is a permutation where $\mathcal{F}'(x) = \mathcal{F}(x) + x$ and that $(\mathcal{F}'_E)^{-1}$ has algebraic degree $(N+1)/2$. We will show that the same twist can be applied to a particular case of Construction 2, that is when $\psi_c(x) = D_c\mathcal{G}^{-1}(x) + D_c\mathcal{G}^{-1}(0)$ is a linear function with kernel of dimension 1 and $\psi = \psi_c$. This setting includes the Li-Wang construction because $\mathcal{G}^{-1}$ is a quadratic APN function and so ψ_c has the property we want. For $\mathcal{F}'(x) = \mathcal{F}(x) + x$, we construct two functions $\mathcal{F}'_E$ and $\mathcal{F}'_A$ that are EA equivalent respectively to $\mathcal{F}_E$ and $\mathcal{F}_A$ (see Remark 4.3). To prove that $\mathcal{F}'_E$ and $\mathcal{F}'_A$ are permutations, we will prove that $\mathcal{F}'$ is a permutation. We will study two properties that requires a specific representation over $\mathbb{F}_{2^{N-1}}$ and that are not affine invariant. The first one is that the two functions are complete permutations (i.e. are permutations $\mathcal{P}(x)$ such that $\mathcal{P}(x) + x$ is also a permutation) and the second is that $(\mathcal{F}'_E)^{-1} = \mathcal{F}'_A$. There is no mention of these property in [6] because we believe that the authors where more focused on affine invariant properties and they did not focus on representations of restrictions.

Proposition 6.6. *Suppose to be in the setting of Construction 2 with the additional hypothesis that $\psi_c(x) = D_c\mathcal{G}^{-1}(x) + D_c\mathcal{G}^{-1}(0)$ is a linear function with kernel of dimension 1 and that $\psi = \psi_c$. Let $\mathcal{F}'(x) = \psi_c(\mathcal{G}(x)) + x$, let $a = D_c\mathcal{G}^{-1}(0)$, and let ϕ be a linear bijective function from $\mathbb{F}_{2^{N-1}}$ to E. Then we have the following:*

1. *We have that $a \in A$ and that function $\mathcal{F}'(x)$ is equal to $\mathcal{G}^{-1}(\mathcal{G}(x) + c) + a$.*
2. *Up to affine equivalence, we can write $\mathcal{F}_E(y) = \phi^{-1}(\mathcal{F}(\phi(y)))$, $\mathcal{F}_A(y) = \phi^{-1}(\mathcal{F}(\phi(y) + a))$, $\mathcal{F}'_E(y) = \phi^{-1}(\mathcal{F}'(\phi(y)))$, and $\mathcal{F}'_A(y) = \phi^{-1}(\mathcal{F}'(\phi(y) + a) + a)$.*
3. *Using the representations in 2, we have that $\mathcal{F}_E$, $\mathcal{F}_A$, $\mathcal{F}'_E$, and $\mathcal{F}'_A$ are complete permutations and that $\mathcal{F}'_A = (\mathcal{F}'_E)^{-1}$.*

Proof. Let us prove 1. We have that $a \in A$ because $\mathrm{Tr}(vD_c\mathcal{G}^{-1}) = 1$. Function $\mathcal{F}'(x)$ is equal to $\mathcal{G}^{-1}(\mathcal{G}(x) + c) + a$ because $\psi_c(\mathcal{G}(x)) = \mathcal{G}^{-1}(\mathcal{G}(x) + c) + \mathcal{G}^{-1}(\mathcal{G}(x)) + D_c\mathcal{G}^{-1}(0) = \mathcal{G}^{-1}(\mathcal{G}(x) + c) + x + a$.

Let us prove 2. Let ζ be a linear surjective function from $\mathbb{F}_{2^N}$ to $\mathbb{F}_{2^{N-1}}$ such that $\zeta(x) = \phi^{-1}(x)$ for all $x \in E$. We have that $(\phi, 0, \zeta, 0)$ is a representation of $\mathcal{F}_E$ and of $\mathcal{F}'_E$, $(\phi, a, \zeta, 0)$ is a representation of $\mathcal{F}_A$, and (ϕ, a, ζ, a) is a representation of $\mathcal{F}'_A$ (see Definition 3.1). Since $\zeta(x) = \phi^{-1}(x)$ for all $x \in E$, the representations we mentioned are exactly those we want to prove.

Let us prove 3. Since $\mathcal{F}'(x) = \mathcal{G}^{-1}(\mathcal{G}(x)+c)+a$, then $\mathcal{F}'$ is a permutation and the two functions $\mathcal{F}'_E$ and ${\mathcal{F}'}_A$ are permutations. We claim that $\mathcal{F}_E(y)+\mathcal{F}'_E(y) = y$ and that $\mathcal{F}_A(y) + \mathcal{F}'_A(y) = y$. Since $\mathcal{F}(x) + \mathcal{F}'(x) = x$, we have that $\mathcal{F}_E(y) + \mathcal{F}'_E(y) = \phi^{-1}\left(\mathcal{F}(\phi(y)) + \mathcal{F}'(\phi(y))\right) = \phi^{-1}\left(\phi(y)\right) = y$ and that $\mathcal{F}_A(y)+\mathcal{F}'_A(y) = \phi^{-1}\left(\mathcal{F}(\phi(y) + a) + \mathcal{F}'(\phi(y) + a) + a\right) = \phi^{-1}\left(\phi(y) + a + a\right) = y$. We claim that $\mathcal{F}'_A = (\mathcal{F}'_E)^{-1}$. Observe that since $\mathcal{F}'(x) + D_c\mathcal{G}^{-1}(0) = \mathcal{G}^{-1}(\mathcal{G}(x) + c)$, we have that $\mathcal{F}'(\mathcal{F}'(x) + a) + a = x$ and that $(\mathcal{F}')^{-1}(x) = \mathcal{F}'(x + a) + a$. We conclude by showing that $(\mathcal{F}'_E)^{-1}(y) = \phi^{-1}((\mathcal{F}')^{-1}(\phi(y))) = \phi^{-1}(\mathcal{F}'(\phi(y)+a)+a) = \mathcal{F}'_A(y)$. □

Using Proposition 6.6, we define the following construction.

Construction 3. *Suppose to be in the setting of Construction 2 with the additional hypothesis that* $\psi_c(x) = D_c\mathcal{G}^{-1}(x) + D_c\mathcal{G}^{-1}(0)$ *is a linear function with kernel of dimension* 1 *and that* $\psi = \psi_c$. *Let* $\mathcal{F}'(x) = \psi_c(\mathcal{G}(x)) + x$. *Using the representations in* 2 *of Proposition 6.6, we have that* $\mathcal{F}_E$, $\mathcal{F}_A$, $\mathcal{F}'_E$, *and* $\mathcal{F}'_A$ *are complete permutations and that* $\mathcal{F}'_A = (\mathcal{F}'_E)^{-1}$ *by using the representations. Functions* $\mathcal{F}'_E$ *and* $\mathcal{F}'_A$ *are EA equivalent respectively to* $\mathcal{F}_E$ *and* $\mathcal{F}_A$ *(see Remark 4.4), so the differential uniformity and the nonlinearity are the same as in Construction 2.*

Using the representations in 2 *and the results in* 3 *of Proposition 6.6, we can describe precisely the linear function that maps the graph of* $\mathcal{F}_E$ *to the graph of* $\mathcal{F}_A$. *We claim that such function is* $(y,z) \mapsto (y+z,z)$ *over* $(\mathbb{F}_{2^{N-1}})^2$. *Since* $(y,\mathcal{F}_E(y)) \mapsto (y+\mathcal{F}_E(y),\mathcal{F}_E(y)) = (\mathcal{F}'_E(y),\mathcal{F}_E(y))$, *we have to show that* $\mathcal{F}_E(w) = \mathcal{F}_A(y)$ *where* $w = (\mathcal{F}'_E)^{-1}(y)$. *Indeed, we have that* $\mathcal{F}_E(w) = \mathcal{F}_E(w)+w+w = \mathcal{F}'_E(w)+w = y+\mathcal{F}'_A(y) = \mathcal{F}_A(y)$ *because* $w = \mathcal{F}'_A(y)$.

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

References

[1] 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.

[2] C. Carlet, "Boolean functions for cryptography and coding theory," 2021. See pages 2, 4, 6, 8, 15, 16, 17, 18, 19, 20, 21, 25, 26, 28, 30, and 31.

[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 3, 15, 16, and 26.

[4] 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 3, 14, 15, 16, 17, 24, 25, and 26.

[5] C. Carlet, "On known and new differentially uniform functions," in *Australasian Conference on Information Security and Privacy*. Springer, 2011, pp. 1–15. See pages 3, 4, 26, and 27.

[6] 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, 14, 28, 30, 31, and 33.

[7] 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, 7, 8, and 10.

[8] J. Bierbrauer and G. M. Kyureghyan, "Crooked binomials," *Designs, Codes and Cryptography*, vol. 46, no. 3, pp. 269–301, 2008. See page 7.

[9] C. Carlet, "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 8 and 18.

[10] 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 8 and 18.

[11] 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 10.

[12] 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 16.

[13] K. Browning, "APN polynomials and related codes," *Special volume of Journal of Combinatorics, Information and System Sciences*, vol. 34, pp. 135–159, 2009. See page 18.

[14] M. Abbondati, M. Calderini, and I. Villa, "On dillon's property of (n, m)-functions," *arXiv preprint arXiv:2302.13922*, 2023. See page 19.

[15] C. Carlet, "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 24 and 25.

[16] 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 24 and 25.

[17] X.-d. Hou, *Lectures on finite fields*. American Mathematical Soc., 2018, vol. 190. See page 27.

[18] 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 27 and 37.

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 [18] 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();
```