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

Claude Carlet\textsuperscript{1,2} and Enrico Piccione\textsuperscript{1}

\textsuperscript{1}University of Bergen, Bergen, Norway
\textsuperscript{2}University of Paris 8, Saint-Denis, France

Abstract

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

We then focus on the case of an \((N, N)\)-function \( F \) of the form \( \psi(G(x)) \) where \( G \) is almost perfect nonlinear (APN) and \( \psi \) is a linear function with a kernel of dimension 1. We observe that the restriction of \( G \) to an affine hyperplane \( A \) has the D-property (introduced by Taniguchi after a result from Dillon) as an \((N - 1, N)\)-function, if and only if, for every such \( \psi \), the restriction of \( F(x) = \psi(G(x)) \) to \( A \) is not an APN \((N - 1, N - 1)\)-function. If this holds for all affine hyperplanes \( A \), we say that \( G \) has the strong D-property. We note that not satisfying this cryptographically interesting property also has a positive aspect, since it allows constructing APN \((N - 1, N - 1)\)-functions from \( G \). We give a characterization of the strong D-property for crooked functions (a particular case of APN functions) and their compositional inverse (if it exists) by means of their ortho-derivatives, and we prove that the Gold APN function and its inverse in dimension \( N \) odd big enough both have the strong D-property. We also prove in simpler a way than Taniguchi in 2023 that the strong D-property of the Gold APN function holds for \( N \geq 6 \) even. In conclusion, we have that the Gold APN function has the strong D-property if and only if \( N = 6 \) or \( N \geq 8 \) and that the inverse of the Gold APN function has the strong D-property if and only if \( N \geq 7 \) is odd. Then we give a partial result on the Dobbertin APN power function, and on the basis of this result, we conjecture that it has the strong D-property as well.
We then move our focus to two known infinite families of differentially
4-uniform \((N-1, N-1)\)-permutations constructed as the restrictions of
\((N,N)\)-functions \(F(x) = \psi(G(x))\) or \(F(x) = \psi(G(x)) + x\) where \(\psi\) is linear
with a kernel of dimension 1 and \(G\) is an APN permutation. After a deeper
investigation on these classes, we provide proofs (which were missing) that
they are not APN in dimension \(n = N-1\) even. Then we present our
own construction by relaxing some hypothesis on \(\psi\) and \(G\).

1 Introduction

Given a power \(q\) of a prime, the known methods for designing infinite classes of
permutations over the space \(\mathbb{F}_{q^n}\) that admit a simple representation (of any form)
are not numerous. One has been much studied: identifying \(\mathbb{F}_{q^n}\) with the field \(\mathbb{F}_{q^n}\)
(thanks to the choice of a basis of the vector space \(\mathbb{F}_{q^n}\) over \(\mathbb{F}_q\)). Permutation
polynomials over \(\mathbb{F}_{q^n}\) provide such bijections having a simple representation
(given by the chosen basis of the vector space \(\mathbb{F}_{q^n}\) and the polynomial expression
of the permutation). But permutation polynomials having good properties for
applications such as cryptography and coding theory (the two most important
properties being a large nonlinearity and a low differential uniformity) are not
that numerous and this classical method has provided only a few interesting
classes (see [19, 15]), that can be used in such applications. Another method
which has been little investigated (see [18]), surprisingly, is to find permutation
polynomials \(F\) over \(\mathbb{F}_{q^n}\) with \(N > n\), or functions from \(\mathbb{F}_{q^n}\) to itself, such that
there exists an \(n\)-dimensional affine subspace \(A\) of the domain, that is mapped by
\(F\) onto an affine subspace \(A'\) of the same dimension in the co-domain; we identify
then \(A\) and \(A'\) with \(\mathbb{F}_{q^n}\) through choices of bases, and we obtain a permutation
over \(\mathbb{F}_{q^n}\) with a simple representation over \(\mathbb{F}_{q^n}\). This representation consists
again in a basis, but this time, of the affine subspace, which is in \(\mathbb{F}_{q^n}\) and not
in \(\mathbb{F}_{q^n}\), and the polynomial expression of the permutation over \(\mathbb{F}_{q^n}\), which is
now a polynomial over \(\mathbb{F}_{q^n}\) and not over \(\mathbb{F}_{q^n}\) and a basis of the affine space
containing the image set. 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. If we consider an infinite family of functions \(F\) such that
we can choose an affine space \(A\) as above, then this provides a second infinite
family. Moreover, we will see that we can estimate the nonlinearity and the
differential uniformity of the restriction. Of course, a particular case of this is
when we know (for instance thanks to a Lagrange interpolation) a polynomial
representation of an \((n,n)\)-function, and we consider, for \(N\) a multiple of \(n\),
the \((N,N)\)-function which admits the same polynomial representation. Then
automatically, this \((N,N)\)-function maps the vector subspace \(\mathbb{F}_{q^n}\) to itself. Such
situation has been studied in the literature. Recall for instance that exceptional
polynomials are those polynomials over finite fields whose associate \((N,N)\)-
functions are bijective for infinitely many values of \(N\). Almost no results seem
known that would relate the nonlinearities of the \((n,n)\)-function and the \((N,N)\)-
function, and apart from an obvious bound, the same happens with differential
uniformity. The same can be said if we do the reverse operation, that is taking an
\((n,n)\)-function, extend it to an \((N,N)\)-function where \(n\) divides \(N\) and relate the
cryptographic properties of the second function with respect to the first. In
this paper, we wish to find new ways of generating functions with potentially

2
good cryptographic parameters, without restricting ourselves to when $n$ is a divisor of $N$. We study the case $q = 2$ and we are also more generally interested in cases where the $(n, n)$-function is not necessarily bijective.

A particular setting which is surprisingly difficult to study is when the $(N, N)$-function $F$ is equal to $\psi(\mathcal{G}(x))$ where $\mathcal{G}$ is almost perfect nonlinear (APN) and $\psi$ 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 [26] the D-property as a generalization for APN $(N, M)$-functions of a property proved by Dillon on APN $(N, N)$-functions and being that $(\mathcal{F}(x) + \mathcal{F}(y) + \mathcal{F}(z) + \mathcal{F}(x + y + z): x, y, z \in \mathbb{F}_q^N) = \mathbb{F}_q^M$. Further studies of such property have been done by Abbondati et al. in [1].

A consequence of the work by Taniguchi in [26] is that the restriction of an APN $(N, N)$-function $\mathcal{G}$ to an affine hyperplane $A$ has the D-property as an $(N - 1, N)$-function if and only if for every linear surjective $(N, N - 2)$-function $\psi$, the restriction of $\mathcal{F}(x) = \psi(\mathcal{G}(x))$ to $A$ is not an APN $(N - 1, N - 1)$-function. We use this as a motivation for the introduction of the notion of the strong D-property of an $(N, N)$-function $\mathcal{G}$, meaning that the restriction of $\mathcal{G}$ to $A$ has the D-property as an $(N - 1, N)$-function for all affine hyperplanes $A$. Such setting was partially investigated by the same Taniguchi and viewed as a positive result for some classes of functions (namely, power and quadratic functions; see also the introduction of Subsection 5.1 where we explain one of its interests); in our paper, we build upon the fact that its negation is also a rather positive property since it allows constructing a number of APN $(N - 1, N - 1)$-functions from $\mathcal{G}$. Therefore, it is important to study the strong D-property of all classes of functions because if they have it, they are stronger cryptographically than other APN functions, and if they do not, we can construct new APN functions in dimension $N - 1$ and this is also important.

The first infinite family defined as the restriction of functions with zero nonlinearity to affine hyperplanes was constructed by the first author in 2011 [12] by using the multiplicative inverse function. It is composed of 4-uniform $(n, n)$-permutations with optimal algebraic degree $n - 1$, and nonlinearity at least $2^n - 2^{\frac{n}{2} + 1}$ (that is not optimal) for $n$ even and at least $2^n - 2^{\frac{n}{2} + 1} - 1$ for $n$ odd. Three years after, in 2014, Li and Wang [23] constructed many families of 4-uniform $(n, n)$-permutations where $n$ is even with optimal known nonlinearity $2^n - 2^\frac{n}{2}$ and algebraic degree $2^\frac{n}{2}$, using the compositional inverse of the Gold APN function. We investigate these constructions deeply and prove that they do not produce APN permutations in dimension $n = N - 1$ even, which had not been done in [12, 23]. We will not study the family from [12] for the case $N$ even because, in that dimension, the multiplicative inverse function is not APN and this setting is out of the scope of this paper. The theory we develop for such proofs helps to understand the problem of constructing APN permutations in even dimension (for trying to solve the so-called big APN problem) with this method. We observe that if the $(N, N)$-permutations used for constructing these $(N - 1, N - 1)$-permutations have the strong D-property, then any restriction of the $(N, N)$-permutation to an affine hyperplane is non-APN. The converse of this implication is not true in general, and we show evidence that proving the non-APNness of such classes of permutations can be easier than proving the strong D-property of the APN permutation $\mathcal{G}$. In practice, proving the strong D-property is a matter of showing that many systems of equations have at least one solution, while we solve only those systems that are relevant
for the construction of permutations in dimension $N - 1$. We do this for the multiplicative inverse function in odd dimension and the compositional inverse of the Gold APN function.

The paper is organized as follows: In Section 2, we give some preliminaries on vectorial Boolean functions. In Section 3, we discuss more generally the cryptographic properties of the restriction of any (so-called initial) $(N, M)$-function providing an $(n, m)$-function. The differential uniformity of the restriction is bounded above by the differential uniformity of the initial function. We give an explicit form of the Walsh transform and of the nonlinearity of the restriction. Then we discuss a sufficient condition such that the nonlinearity of the restriction is nonzero. In Section 4, we discuss the special case of $(N, M)$-functions having some affine components that is a sufficient condition for the existence of a strict affine subspace of its domain that is mapped into a strict affine subspace of its co-domain. We prove that, up to EA equivalence, we can write these functions in the form $F(x) = \psi(G(x))$ where $\psi$ is linear, and we can assume that $G$ 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. Then we discuss a sufficient condition such that the nonlinearity of the restriction is nonzero. In Section 4, we discuss the special case of $(N, M)$-functions having some affine components that is a sufficient condition for the existence of a strict affine subspace of its domain that is mapped into a strict affine subspace of its co-domain. We prove that, up to EA equivalence, we can write these functions in the form $F(x) = \psi(G(x))$ where $\psi$ is linear, and we can assume that $G$ 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. Then we discuss a sufficient condition such that the nonlinearity of the restriction is nonzero. In Section 4, we discuss the special case of $(N, M)$-functions having some affine components that is a sufficient condition for the existence of a strict affine subspace of its domain that is mapped into a strict affine subspace of its co-domain. We prove that, up to EA equivalence, we can write these functions in the form $F(x) = \psi(G(x))$ where $\psi$ is linear, and we can assume that $G$ 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. Then we discuss a sufficient condition such that the nonlinearity of the restriction is nonzero. In Section 4, we discuss the special case of $(N, M)$-functions having some affine components that is a sufficient condition for the existence of a strict affine subspace of its domain that is mapped into a strict affine subspace of its co-domain. We prove that, up to EA equivalence, we can write these functions in the form $F(x) = \psi(G(x))$ where $\psi$ is linear, and we can assume that $G$ 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. Then we discuss a sufficient condition such that the nonlinearity of the restriction is nonzero.
represented as a univariate polynomial, \( F(x) = \sum_{i=0}^{2^N-1} c_i x^i \) where \( c_i \in \mathbb{F}_{2^N} \), called the univariate representation. The algebraic degree of \( F \) is equal to the maximum Hamming weight of the binary expansion of the exponents \( i \) of the terms of the polynomial \( F(x) \) such that \( c_i \neq 0 \). The monomial functions \( x^i \) are also called power functions to avoid any confusion with the monomial functions involved in the ANF.

Two \((N,M)\)-functions \( F \) and \( F' \) are called affine equivalent if one equals the other composed on the right by an affine permutation of \( \mathbb{F}_{2^M}^\ast \) and on the left by an affine permutation over \( \mathbb{F}_{2^M}^\ast \). More generally, they are called extended affine (EA) equivalent if one is affine equivalent to the sum of the other and of an affine permutation over \( \mathbb{F}_{2^M}^\ast \). They are affine equivalent (as \((N,M)\)-functions) if and only if their graphs \( \{(x,F(x)) : x \in \mathbb{F}_{2^N}^\ast \} \) and \( \{(x,F'(x)) : x \in \mathbb{F}_{2^N}^\ast \} \) 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 \( \mathbb{F}_{2^N}^\ast \) and an inner product in \( \mathbb{F}_{2^M}^\ast \) (there will be no ambiguity). For any \( a \in \mathbb{F}_{2^N}^\ast \setminus \{0\} \), we can define the inner product \( x \cdot y = \text{Tr}_N(axb) \) over \( \mathbb{F}_{2^N}^\ast \), where \( \text{Tr}_N(x) = \sum_{i=0}^{2^N-1} x^i \) is the absolute trace function from \( \mathbb{F}_{2^N} \) to \( \mathbb{F}_2 \). If it is clear from the context, then we write \( \text{Tr} = \text{Tr}_N \). For \( k,N \) such that \( k|N \) we denote by \( \text{Tr}^N_k(x) \) the relative trace function from \( \mathbb{F}_{2^N} \) to \( \mathbb{F}_2 \), equal to \( x + x^{2^k} + x^{2^{2k}} + \ldots + x^{2^{k(N-1)}} \).

We define the adjoint operator in the context of vector spaces over \( \mathbb{F}_2 \). Let \( \psi : \mathbb{F}_{2^N}^\ast \rightarrow \mathbb{F}_{2^M}^\ast \) be a linear function. The adjoint operator is the linear mapping \( \psi^* : \mathbb{F}_2^M \rightarrow \mathbb{F}_2^N \) such that for all \( a \in \mathbb{F}_{2^N}^\ast \), \( b \in \mathbb{F}_{2^M}^\ast \), \( \psi(a) \cdot b = a \cdot \psi^*(b) \). Since every linear form over a field \( \mathbb{F} \) can be written in a unique way as \( \lambda \rightarrow a \cdot \lambda \), we have indeed that \( \psi^*(b) \) is defined as equal to the unique element \( c \) corresponding to the linear form \( a \rightarrow \psi(a) \cdot b \). In this way, if we have chosen an inner product, then \( \psi^* \) is uniquely defined. Let \( E \) be a vector subspace of \( \mathbb{F}_{2^N}^\ast \). We denote by \( E^\perp \) the orthogonal of \( E \) with respect to the inner product "\( \cdot \)", equal to the vector space of all those \( v \in \mathbb{F}_{2^N}^\ast \) such that \( v \cdot e = 0 \) for every \( e \in E \). Let \( u_1, \ldots, u_n \in \mathbb{F}_{2^N}^\ast \). We define \( E = \langle u_1, \ldots, u_n \rangle \) as the vector space spanned by \( u_1, \ldots, u_n \). We say that \( A \subseteq \mathbb{F}_{2^N}^\ast \) 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 \( u,v \in \mathbb{F}_{2^N}^\ast \) and \( v \in \mathbb{F}_{2^M}^\ast \) we denote by \( W_\mathcal{F}(u,v) \) the value at \((u,v)\) of the Walsh transform of \( \mathcal{F} \):

\[
W_\mathcal{F}(u,v) = \sum_{x \in \mathbb{F}_{2^N}^\ast} (-1)^{v \cdot \mathcal{F}(x)} u \cdot x.
\]

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 [11]) satisfied by the Walsh transform related to affine subspaces. Let \( v \in \mathbb{F}_{2^M}^\ast \), \( a, b \in \mathbb{F}_{2^N}^\ast \), and \( E,E_0 \) be two vector subspaces of \( \mathbb{F}_{2^N}^\ast \) such that \( E \oplus E_0 = \mathbb{F}_{2^N}^\ast \). The Walsh transform satisfies the Poisson summation formula:

\[
\sum_{u \in a + E} (-1)^{a \cdot u} W_\mathcal{F}(u,v) = |E_\perp| (-1)^{a \cdot b} \sum_{x \in a + E} (-1)^{v \cdot \mathcal{F}(x) + b \cdot x}. \tag{1}
\]
The Walsh transform satisfies the second-order Poisson summation formula:

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

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

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

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

The nonlinearity should be large (as close to the maximum $2^{n-1} - 2^{\frac{n-1}{2}}$ as possible) for allowing the vectorial function to contribute to the resistance of the block cipher using it as a substitution box to the linear attack [15]. As a generalization of the nonlinearity, we have the $d$-th order nonlinearity of a vectorial Boolean function $F$ denoted as $\text{nl}_d(F)$ that is equal to the minimum Hamming distance between the nonzero components of $F$ and the set $B_{N,d}$ 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 $\text{nl}_d(F) = 2^{N-1} - \frac{\omega_d}{2}$ where

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

The differential uniformity of $F$ is the (positive and even) integer $\delta_F$ defined as:

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

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

A Boolean function $f$ over $\mathbb{F}_2^N$ is called plateaued if its extended Walsh spectrum assumes only two values that are 0 and a positive number, which happens to be equal to $2^k$ for some $k \geq \frac{N}{2}$, because of the Parseval’s relation [15] (after Corollary 5). Quadratic functions are plateaued. The integer $2^k$ is called the amplitude of $f$. The function $f$ is called bent if $k = \frac{N}{2}$, near-bent if $k = \frac{N+1}{2}$, and semi-bent if $k = \frac{N}{2} + 1$. A generalization of bent functions is partially-bent functions that are characterized by the property of having all their derivatives either constant or balanced. Partially-bent functions are also plateaued. A vectorial Boolean function is called respectively plateaued, strongly plateaued, and bent if all its components are respectively plateaued, partially-bent, and bent. An almost bent (AB) function $F$ is an $(N, N)$-function that
reaches the SCV bound [15, Theorem 6], that is such that \( \text{nl}(F) = 2^{N-1} - 2^{N-1} \). 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 \( a \in F_N^2 \setminus \{0\} \), the image set of \( D_a F \) is an affine hyperplane; equivalently, they are APN and strongly plateaued [15] (after Definition 68). Crooked functions share almost all the nice properties of quadratic APN functions, and it is conjectured that the two notions coincide.

Let \( f \) be a Boolean function over \( F_{2^N} \), 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** ([11]). Let \( f \) be a Boolean function over \( F_{2^N} \). If \( f \) is \( n \)-weakly-normal, then \( \text{nl}(f) \leq 2^{N-1} - 2^{n-1} \).

### 3 Cryptographic properties of restrictions of vectorial functions to affine spaces

Let \( \mathcal{F} \) be an \((N, M)\)-function such that there exists an affine space \( A \) of dimension \( n \), that is mapped by \( \mathcal{F} \) into an affine space \( A' \) of dimension \( m \). We identify then \( A \) with \( F_{2^n} \) and \( A' \) with \( F_{2^m} \) through the choice of bases, and we obtain an \((n, m)\)-function. We shall denote by \( \mathcal{F}_A \) one of the functions obtained this way. When we shall find such case of an affine space mapped by a function \( \mathcal{F} \) into a strict affine space of the co-domain of \( \mathcal{F} \), we shall of course be interested in the cryptographic properties of \( \mathcal{F}_A \). But there are several possibilities of defining the affine space in which \( \mathcal{F}(A) \) is included (hence, to choose the dimension \( m \) of the co-domain of \( \mathcal{F}_A \)). And if this affine space is taken too large, then the nonlinearity of \( \mathcal{F}_A \) will be automatically zero, because when we see an \((n, m)\)-function as an \((n, m')\)-function with \( m' > m \) by adding virtual coordinate functions (which equal the zero function if we identify \( F_{2^m} \) with \( F_{2^m} \times \{0\} \subset F_{2^{m'}} \)), this drops the nonlinearity to zero. So, if it is not specified otherwise, we shall assume that \( A' \) is the intersection of all the affine spaces that contain \( \mathcal{F}(A) \).

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

\[
\mathcal{F}_A(x) = \psi(\phi(x) + a) + a'
\]

where \( \phi \) is a linear bijective function from \( F_{2^n} \) to \( E \), and \( \psi \) is a linear surjective \((M, m)\)-function such that \( \psi(E') = F_{2^m} \).

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

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

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

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

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

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

3.2 The Walsh transform and nonlinearity of restrictions

Concerning the nonlinearity, the situation is also apparently simple: the nonlinearity of \(\mathcal{F}_A\) equals the minimum Hamming distance between the components of \(\mathcal{F}_A\) and the affine Boolean functions over \(A\). But we need to define what is a component function of \(\mathcal{F}_A\) and the situation is then a little more delicate. We also need a way to effectively calculate the nonlinearity. In practice, we can first try to relate the Walsh transform of the restriction to the Walsh transform of \(\mathcal{F}\). The nonlinearity of the restriction of a Boolean function to an affine space has been studied in [24, 27, 11], but without that a precise expression of the Walsh transform be exhibited. The results that we shall revisit were obtained in [27] in a complex way and in [11] 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 \(\zeta\) be any linear function and let \(\zeta^*\) be the adjoint operator of \(\zeta\) with respect to an inner product. We recall that \(\text{Im}\zeta^* = (\ker\zeta)^\perp\) and \(\ker\zeta^* = (\text{Im}\zeta)^\perp\).

**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 \((\phi, a, \psi, a')\) of \(\mathcal{F}_A\), we have \(\text{Im}\psi^* \oplus (E')^\perp = \mathbb{F}_2^M\). Moreover, for every \(\psi' \in \mathbb{F}_2^M \setminus (E')^\perp\) there exists a representation \((\phi, a, \psi, a')\) of \(\mathcal{F}_A\) such that \(\psi' \in \text{Im}\psi^*\).

**Proof.** Let us prove that \(\text{Im}\psi^* \oplus (E')^\perp = \mathbb{F}_2^M\) for any representation \((\phi, a, \psi, a')\) of \(\mathcal{F}_A\). Let \(w' \in \text{Im}\psi^* \cap (E')^\perp\) and \(w \in \mathbb{F}_2^n\) 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 \(\psi(E') = \mathbb{F}_2^n\), we have that \(w = 0\) and that \(w' = 0\). This
is a contradiction. So $\text{Im} \, \psi^* \cap (E')^\perp = \{0\}$. Since $\text{Im} \, \psi^*$ (resp. $(E')^\perp$) has dimension $m$ (resp. $M - m$), we have that $\text{Im} \, \psi^* \oplus (E')^\perp = \mathbb{F}_2^M$.

Let us prove the second part. Let $v' \in \mathbb{F}_2^M \setminus (E')^\perp$ and let $(\phi, a, \psi, a')$ be a representation of $\mathcal{F}_A$. If $v' \in \text{Im} \, \psi^*$, there is nothing to prove. Otherwise, we will prove that there exists a linear function $\nu$ such that $v' \in \text{Im} \, \nu^*$ and $(\phi, a, \nu, a')$ 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 $\zeta$ be a linear function from $\mathbb{F}_2^n$ to $\mathbb{F}_2^m$ such that $\text{Im} \, \zeta = E_0$ and consider $\nu = \zeta^*$. We claim that $\nu$ is such that $v' \in \text{Im} \, \nu^*$ and that $(\phi, a, \nu, a')$ is a representation of $\mathcal{F}_A$. Since $\text{Im} \, \nu^* = \text{Im} \, \zeta = E_0$, then $v' \in \text{Im} \, \nu^*$. To prove that $(\phi, a, \nu, a')$ is a representation of $\mathcal{F}_A$ we must prove that $\nu(E') = \mathbb{F}_2^n$. Since $\ker \nu = (\text{Im} \, \nu^*)^\perp = E_0^\perp$ 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 $\nu(E') = \mathbb{F}_2^n$.

\textbf{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 $(\phi, a, \psi, a')$ be a representation of $\mathcal{F}_A$. Then for all $u \in \mathbb{F}_2^n$, $v \in \mathbb{F}_2^m$

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

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

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

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

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

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

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

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

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 $\psi^*$ is injective.
So \( v' \in \text{Im} \psi^* \setminus \{0\} \). By using Lemma 3.4, we have that \( v' \in \mathbb{F}_2^M \setminus (E')^\perp \) and we can set \( E_2 = \text{Im} \psi^* \). 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: \[ |\sum_{z \in E^\perp} (-1)^{z \cdot a} W_{F}(u' + z, v')| = |\sum_{z \in E^\perp} (-1)^{z \cdot a} W_{F}(u_1 + z, v')| \] . So we can assume \( u' \in E_1 \). The rest is clear.

\[ \square \]

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

The case \( \text{nl}(\mathcal{F}) = 0 \) 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

\[ \text{nl}(\mathcal{F}_A) \geq \text{nl}(\mathcal{F}) - (2^{N-1} - 2^{n-1}) \]  \hfill (4)

that is already known from [27, 11]. Observe that by using relation (4), we have that a sufficient condition for having \( \text{nl}(\mathcal{F}_A) \neq 0 \) is that \( \text{nl}(\mathcal{F}) > 2^{N-1} - 2^{n-1} \). But this property is impossible to satisfy with \( m < M \) since if \( \mathcal{F} \) maps \( A \) into an affine hyperplane, of equation, say, \( v \cdot x + \epsilon = 0 \), then the Boolean function \( v \cdot \mathcal{F}(x) \) being constant over \( A \), it is \( n \)-normal and Proposition 2.1 shows that this is impossible. This observation proves the following proposition.

**Proposition 3.5.** Let \( N, M, n \) be positive integers such that \( N \geq n \). Let \( \mathcal{F} \) be an \((N, M)\)-function. If \( \text{nl}(\mathcal{F}) > 2^{N-1} - 2^{n-1} \), 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 \( \text{nl}(\mathcal{F}_A) \neq 0 \) 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 \( \text{nl}(\mathcal{F}_A) = 0 \), then there exist \( v \in \mathbb{F}_2^M \setminus (E')^\perp \) and \( u \in \mathbb{F}_2^N \) such that \( |W_{\mathcal{F}}(u, v)| \geq 2^n \).

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

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

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

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

Constructing an \((N, M)\)-function \(F\) with no affine component that maps an affine space of dimension \(n < N\) into an affine space of dimension \(m < M\) is not that difficult. Let \(F\) be an \((n, m)\)-function and \(G\) be an \((n', m')\)-function both without affine components, then the \((n + n', m + m')\)-function \(F\) defined as \((x, y) \mapsto (F(x), G(y))\) does not have affine components and maps the affine space \(A = F_2^n \times \{0\}^{n'}\) (resp. \(A = \{0\}^n \times F_2^{n'}\)) of dimension \(n\) (resp. \(n'\)) into the affine space \(A' = F_2^n \times \{0\}^{m'}\) (resp. \(A' = \{0\}^m \times F_2^{m'}\)) of dimension \(m\) (resp. \(m'\)). However, this procedure does not produce really new functions since \(F\) and \(G\) are known. It is challenging to find examples of “interesting” \((N, M)\)-functions \(F\) (having good cryptographic properties) with no affine components that map an affine space of dimension \(n < N\) into an affine space of dimension \(m < M\) and such that \(F_A\) has good cryptographic properties. Of course, as we saw in the introduction, if we take an \((N, N)\)-function \(F\) that can be represented as a polynomial with coefficients in \(F_{2^n}\) with \(n\) a strict divisor of \(N\), then \(F\) maps \(F_{2^n}\) onto itself. But then, \(n\) is necessarily a divisor of \(N\). We wish here to study another way of generating functions from known ones (and studying their cryptographic parameters).

In this section, we will study the case where function \(F\) has affine components (that is when \(\text{nl}(F) = 0\)) because we can find automatically a strict affine subspace of its domain mapped to a strict affine subspace of its co-domain. Also, it seems interesting to us that, from a function that is bad, cryptographically, because it has zero nonlinearity, we can construct potentially a good function by restricting its domain. This renews the cryptographic interest of the known infinite classes of permutation polynomials having zero nonlinearity. We will prove that, up to EA equivalence, we can write \(F(x) = \psi(G(x))\) where \(\psi\) is linear, and we can assume that \(G\) has nonzero nonlinearity for the case \(M = N \geq 3\).

For any \((N, M)\)-function \(G\), we will see that instead of studying restrictions of \(G\), we can study restrictions of functions of the form \(F(x) = \psi(G(x))\) where \(\psi\) is linear. Moreover, we will be able to construct more functions, because if \(\psi\) is not surjective, then \(\text{nl}(F) = 0\) (because the image set of \(F\) being then included in an affine hyperplane, a component function of \(F\) is then constant) and we are not constrained by the necessary condition of Proposition 3.5 as explained in Remark 3.7.

4.1 Functions mapping affine spaces to subsets of proper affine subspaces

The next proposition is a generalization of the simple following observation: assume that \(F\) has an affine component; for instance, assume that its last coordinate function \(f_m\) is affine, then \(F\) maps (without loss of generality up to affine equivalence) the affine space equal to the pre-image \(f_m^{-1}(0)\) into the affine space \(\{y \in F_2^M; y_M = 0\}\).

**Proposition 4.1.** Let \(F\) be an \((N, M)\)-function. Let \(V\) be any subset of \(F_2^M\) such that \(v \cdot F\) is affine for every \(v \in V\). Let \(\ell : F_2^M \rightarrow F_2\) be any linear form and \(A = \{x \in F_2^N \mid \forall v \in V, v \cdot F(x) = \ell(v)\}\). Then we have \(A \neq \emptyset\) for some \(\ell\), and for any such \(\ell\), \(A\) is an affine space mapped by \(F\) into the affine space
\[ A' = \{ y \in \mathbb{F}_2^M \mid \forall v \in V, v \cdot y = \ell(v) \} \text{ with direction } (V)^\perp. \text{ Any translate } a + A \text{ for } a \in \mathbb{F}_2^N \text{ is also mapped into an affine space of direction } (V)^\perp. \]

Proof. By definition, \( A \) equals the intersection of the affine spaces \( \{ x \in \mathbb{F}_2^N \mid v \cdot \mathcal{F}(x) = \ell(v) \} \), where \( v \) ranges over \( V \). Such \( A \) is non-empty for any \( \ell \) defined over \( V \) by \( \ell(v) = v \cdot \mathcal{F}(x) \), where \( x \) is some fixed element in \( \mathbb{F}_2^N \), and completed into a linear function over \( \mathbb{F}_2^M \). Then \( A \) is an affine space. The image of \( A \) by \( \mathcal{F} \) is clearly a subset of the affine space \( \{ y \in \mathbb{F}_2^M \mid \forall v \in V, v \cdot y = \ell(v) \} \), whose direction equals its homogeneous version, that is, \( (V)^\perp \). 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 \( (V)^\perp \).

Note that taking \( \ell \) 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 \( v \in (V) \). Hence, we can then always assume that \( V \) is a vector space.

Remark 4.2. As we already evoked it at the beginning of Section 3, we need to reduce the dimension of the co-domain of the restriction of a function to an affine space in such a way that we erase all its affine components, if we want the restriction to have a chance of having nonzero nonlinearity. More precisely, let \( V = \{ v \in \mathbb{F}_2^M \mid v \cdot \mathcal{F} \text{ is affine} \} \) (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 \( \text{nl} (\mathcal{F}_B) = 0 \), 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 \( (\phi, b, \psi, b') \) of \( \mathcal{F}_B \) such that \( v \in \text{Im } \psi^* \). Since \( v \cdot \mathcal{F} \) is affine, then also \( v \cdot \mathcal{F}(\phi(x) + b) \) is affine and

\[
\begin{align*}
v \cdot \mathcal{F}(\phi(x) + b) &= v' \cdot \psi(\mathcal{F}(\phi(x) + b)) = v' \cdot \psi(b') + v' \cdot \mathcal{F}_B(x) \\
\end{align*}
\]

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

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 \( \psi \) be any linear \((M, M)\)-function with \( \text{Im } \psi = V^\perp \), then there exists an \((N, M)\)-function \( \mathcal{G} \), and an affine \((N, M)\)-function \( A \) such that:

\[
\mathcal{F}(x) = \psi(\mathcal{G}(x)) + A(x).
\]


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

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

2. **Assuming that $v \cdot \mathcal{F}$ is constant for all $v \in V$, we can take $\mathcal{A} = 0$.**

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

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

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

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 $\{x \in \mathbb{F}_2^N \mid \forall v \in \text{Im } \psi^\perp, v \cdot A(x) = \ell(v)\}$ and their images by $\mathcal{F}$ and by $\psi \circ \mathcal{G}$ have $\text{Im } \psi$ 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 \{ $x \in \mathbb{F}^N_2$ \mid \forall v \in \text{Im} \psi^{-1}, v : \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 $\text{Im} \psi$.

**Remark 4.5.** Let $\mathcal{G}$ be an $(N, N)$-function. Suppose there exists an affine $n$-dimensional subspace $A$ of $\mathbb{F}^N_2$ such that $\mathcal{G}(A) \subseteq A'$ where $A'$ is an $m$-dimensional subspace of $\mathbb{F}^M_2$. Without loss of generality, assume that $A' = E'$ is a vector space. For any linear $(M, M)$-function $\psi$ such that $\psi(E') = \text{Im} \psi$ has dimension $m$, we have that, by choosing the appropriate representations (see Definition 3.1), the two $(n, m)$-functions $\mathcal{G}_A$ and $\mathcal{F}_A$ are affine equivalent where $\mathcal{F}(x) = \psi(G(x))$. In fact, we can assume that $\mathcal{F}_A = \psi_{E'} \circ \mathcal{G}_A$ where $\psi_{E'}$ is a linear $(m, m)$-permutation because $E'$ and $\text{Im} \psi$ have the same dimension.

As a consequence of the previous remarks, studying the cryptographic properties of restrictions of functions of the form $\mathcal{F}(x) = \psi(G(x))$ 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 $\text{Im} \psi$ (that can also be the whole space if $\psi$ is a permutation).

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

1. For every $u \in \mathbb{F}^N_2$ and $v \in \mathbb{F}^M_2$, we have that $W_\mathcal{F}(u, v) = W_\mathcal{G}(u, \psi^*(v))$ and that $\text{nl}(\mathcal{F}_A) \geq \text{nl}(\mathcal{G}) - (2^{N-1} - 2^{n-1})$.

2. Let $a \in \mathbb{F}^N_2$ and $b \in \mathbb{F}^M_2$. If $b \notin \text{Im} \psi$, then $\delta_\mathcal{F}(a, b) = \delta_\mathcal{F}_A(a, b) = 0$. If $b \in \text{Im} \psi$, then for any $b' \in \mathbb{F}^M_2$ 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 $\mathbb{F}^M_2$. 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 $\text{Im} \psi$, 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 $\text{Im} \psi$.

Let us prove 1. Given $u \in \mathbb{F}^N_2$ and $v \in \mathbb{F}^M_2$, we have that $W_\mathcal{F}(u, v) = W_\mathcal{G}(u, \psi^*(v))$ because $v \cdot \psi(G) = \psi^*(v) \cdot \mathcal{F}$. Because of Theorem 1 and the fact that the direction of $\mathcal{F}(A)$ is included $\text{Im} \psi$, the nonlinearity of $\mathcal{F}_A$ is

$$2^{n-1} - \frac{1}{2^{N-n+1}} \max_{u \in \mathbb{F}^N_2, v \in \mathbb{F}^M_2} \left( |\sum_{z \in E^+} (-1)^{a \cdot W_\mathcal{F}(u + z, v)}| \right).$$

14
where $A = a + E$. Let $u \in \mathbb{F}_2^N$, $v \in \mathbb{F}_2^M \setminus \text{Im } \psi^\perp$, then we have that

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

Since $v \not\in \text{Im } \psi^\perp = \ker \psi^*$, then $\psi^*(v) \neq 0$. So we can conclude that $\text{nl}(\mathcal{F}_A) \geq \text{nl}(\mathcal{G}) - (2^{N-1} - 2^{n-1})$.

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:

$$\mathcal{F}(x) + \mathcal{F}(x + a) = \psi(\mathcal{G}(x) + \mathcal{G}(x + a)) = b,$$ (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:

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

The first equation $\psi(z) = b$ has solutions if and only if $b \in \text{Im } \psi$, 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 $b \in \text{Im } \psi$, we can obtain $\delta_{\mathcal{F}_A}(a, b)$ similarly.

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 $b \in \text{Im } \psi$, the set of solutions of the first equation of Equation (6) equals $b' + \ker \psi$ for some $b' \in \mathbb{F}_2^M$ such that $\psi(b') = b$. For every $c \in \ker \psi$, the number of solution to the equation $\mathcal{G}(x) + \mathcal{G}(x + a) = b' + c$ is exactly $\delta_{\mathcal{G}_A}(a, b' + c)$ where $\mathcal{G}_A$ is the restriction of $\mathcal{G}$ to $A$ with co-domain $\mathbb{F}_2^M$. Consequently, we have that $\delta_{\mathcal{F}_A}(a, b) = \sum_{c \in \ker \psi} \delta_{\mathcal{G}_A}(a, b' + c)$. The two bounds follow directly. $\square$

**Remark 4.6.** Consider the setting of Theorem 2 with $M = N$ and $m = n$. Assuming that $\mathcal{G}$ belongs to an infinite family of $(N, N)$-functions, then computing $\delta_{\mathcal{G}}$ could be hard, and therefore the bound $\delta_{\mathcal{G}} \leq \delta_{\mathcal{F}} \leq 2^{N-n} \delta_{\mathcal{G}}$ is not useful. However, if $\mathcal{G}$ belongs to an infinite family of APN $(N, N)$-functions, then we have that $\delta_{G_A}$ is $2$ and that $2 \leq \delta_{\mathcal{F}_A} \leq 2^{N-n+1}$. So it is reasonable to study the case $n = N - 1$ because then $\mathcal{F}_A$ is at most 4-uniform.

The following proposition groups together two results that are known for a long time (at least in the folklore) and have been rediscovered several times (for instance, in [23, 26]). In our case, they will follow from Theorem 2.

**Proposition 4.7.** Let $N \geq 4$, let $\mathcal{G}$ be an $(N, N)$-function, let $\psi$ be a linear $(N, N)$-function where $n = N - 1$ is the dimension of $\text{Im } \psi$, 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 differentially 4-uniform.

15
2. If $G$ is AB, then $F_A$ is differentially 4-uniform and has nonlinearity $2^{n-1} - 2^\frac{n}{2}$.

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

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

Let $F(x) = \psi(G(x))$ be as in Proposition 4.7 and let $A$ be an affine hyperplane. By Proposition 4.3, we can assume that $G$ has nonzero nonlinearity. Moreover, to have that $F_A$ is an APN $(N-1,N-1)$-function, it is necessary that $G$ is at least differentially 4-uniform. In the next section, we will investigate the case where $G$ is APN, and we will study sufficient conditions to conclude that $F_A$ is APN.

Remark 4.8. There exist examples of infinite families of differentially 4-uniform $(N,N)$-functions $F$ and hyperplanes $A$ of $\mathbb{F}_2^N$ mapped to subsets of hyperplanes of $\mathbb{F}_2^N$ and such that $F_A$ is APN. Indeed, take an APN $(n,n)$-function $F$ and define, for instance $F(x,x_{n+1}) = \left(F(x) + x_{n+1}L(x), x_{n+1}\ell(x)\right)$, with $x \in \mathbb{F}_2^n, x_{n+1} \in \mathbb{F}_2$, where $(L,\ell)$ is a linear $(n,n+1)$-function whose kernel has dimension at most 2 (this is not very different from the construction in [3] but we shall apply it here to reach differential 4-uniformity). Then the image of $A = \mathbb{F}_2^n \times \{0\}$ is included in $A$, and the equation $D_{(a,n+1)}F(x,x_{n+1}) = (b,n+1)$ is equivalent to the system of equations

$$
\begin{cases}
D_aF(x) + x_{n+1}L(a) + a_{n+1}L(x) = b + a_{n+1}L(a) \\
x_{n+1}\ell(a) + a_{n+1}\ell(x) = b_{n+1} + a_{n+1}\ell(a)
\end{cases}
$$

For $a = 0$ and $a_{n+1} = 1$, this system writes $\begin{cases} L(x) = b \\ \ell(x) = b_{n+1} \end{cases}$ and has at most 4 solutions. For $a \neq 0$, it writes $\begin{cases} D_aF(x) + a_{n+1}L(x) = b + a_{n+1}L(a) \\ a_{n+1}\ell(x) = b_{n+1} + a_{n+1}\ell(a) \end{cases}$ if $x_{n+1} = 0$ and $\begin{cases} D_aF(x) + a_{n+1}L(x) = b + a_{n+1}L(a) + L(a) \\ a_{n+1}\ell(x) = b_{n+1} + (a_{n+1} + 1)\ell(a) \end{cases}$ if $x_{n+1} = 1$. So it is enough that the first equation in each of the two latter systems has at most two solutions. This is obtained for instance if $F(x) = x^3$ with $x \in \mathbb{F}_2^n$ and $L(x) = x$ (whatever is $\ell$) since these equations have then degree 2. Other examples can be given.

There even exist examples of quadratic APN $(N,N)$-functions $F$ having this property (see [2, 6]) but these are sporadic.

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

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

**Open Question 2.** Do there exist (possibly sporadic) non-quadratic APN functions mapping a hyperplane $A$ into a hyperplane, and whose restriction $F_A$ is also APN?
5 APN \((N-1, N-1)\)-functions as restrictions of \((N, N)\)-functions with an affine component, and the D-property

In this section, we will discuss the problem of constructing APN \((N-1, N-1)\)-functions as restrictions of \((N, N)\)-functions with an affine component. We recall that according to Remark 4.6 this is not a restrictive setting. We will show that this problem is closely related to the D-property of \((N-1, N)\)-functions discussed by Taniguchi in [26]. This will motivate the introduction of the notion of strong D-property. We will investigate this property for crooked functions and for their compositional inverses (when they are bijective). Then we will prove that the Gold APN function and its inverse have the strong D-property for \(N\) large enough. As a consequence, we will present a partial result on the Dobbertin APN function, and we conjecture that it has the strong D-property.

To the best of our knowledge, the paper by Beierle, 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 \(\eta\) is an injective affine \((n, N)\)-function and \(\zeta\) is a surjective affine \((M, m)\)-function. The only difference (up to affine equivalence) with our notion of restriction is that we impose that \(\zeta\) is injective on \(\mathcal{G}(\text{Im } \eta)\) (see Definition 3.1). So restrictions in our sense, can be seen as a special case of restrictions in their sense. Conversely, it is fairly simple to show that the work by Beierle et al. on trims fits our framework. Observe that we can write without loss of generality \(\zeta = \zeta' \circ \psi\) where \(\psi\) is a linear \((M, M)\)-function with \(\text{Im } \psi\) of dimension \(m\) and \(\zeta'\) is an affine \((M, m)\)-function injective on \(\text{Im } \psi\). 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 \(\psi\) is very relevant for the study of the differential uniformity of restrictions (see Theorem 2), while this information could be overlooked when dealing with specific constructions. Moreover, to construct permutations as restrictions of functions we need to impose anyway that \(\zeta\) 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 constructing \((N-1, N-1)\)-restrictions in their sense. Let \(\mathcal{F}_A\) be a restriction (in our sense) of an \((N, N)\)-function \(\mathcal{F}(x) = \psi(G(x))\) where \(A\) is an affine hyperplane, and \(\psi\) is a linear \((N, N)\)-function with a kernel of dimension 1. Such \((N-1, N-1)\)-function \(\mathcal{F}_A\) is a trim of \(\mathcal{G}\) by the Beierle 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 \(v_0 \in \mathbb{F}_2^N \setminus \text{Im } \psi^*\).

These observations show the relationship between [3] and our present work. But there is in fact little intersection between [3] and our paper (even in the present section), since in [3], the authors study specific constructions of quadratic APN functions (and we can see the difficulty of obtaining them), while we study
general sufficient conditions allowing \( F_A \) to be APN. Our results are then complementary of those of [3].

A useful characterization for \( F_A \) to be APN when \( G \) is APN is that \( G(x) + G(y) + G(z) + G(x + y + z) \neq c \) for all \( x, y, z \in A \) where \( c \in \mathbb{F}_2^N \setminus \{0\} \) and \( \ker \psi = \langle c \rangle \). Indeed, \( F_A \) is APN if and only if \( G(x) + G(y) + G(z) + G(x + y + z) \not\in \{0, c\} \) for distinct \( x, y, z \in A \) and since \( G \) is assumed APN, \( G(x) + G(y) + G(z) + G(x + y + z) \) cannot be zero. It is also a direct consequence of Theorem 2 because, \( G_A \) being APN, \( F_A \) is APN if and only if, for any \( a \in E \setminus \{0\} \), we have \( \delta_{G_A}(a, b) \neq 0 \) for some \( b \in F_2^N \) only when \( \delta_{G_A}(a, b + c) = 0 \). This is equivalent to saying that for any \( a \in E \) and \( x, y \in A \) we have that \( D_a G(x) + D_a G(y) \neq c \).

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

### 5.1 The strong D-property

It is known that for any APN \((N, N)\)-function \( G \) and any \( c \in \mathbb{F}_2^N \setminus \{0\} \) there exist \( x, y, z \in \mathbb{F}_2^N \) such that \( G(x) + G(y) + G(z) + G(x + y + z) = c \). This was proven by J. Dillon in a private communication reported in [15] (after Proposition 161). Using this as a motivation, Taniguchi in [26] called \( D \)-property of an \((n, m)\)-function \( G \), the fact that \( \{G(x) + G(y) + G(z) + G(x + y + z) : x, y, z \in \mathbb{F}_2^n\} = \mathbb{F}_2^m \). If \( n \neq m \), it is not true that all differentially 2-uniform \((n, m)\)-functions have the D-property. When \( m = n + 1 \), the property is very relevant to our setting. Consider an APN \((N, N)\)-function \( G \) and its restriction \( G_A \) to an affine hyperplane \( A \). Observe that, according to Lemma 5.1, if \( G_A \) has the D-property as an \((N - 1, N)\)-function, then any projection of \( G_A \) onto a hyperplane is not an APN \((N - 1, N - 1)\)-function. Moreover, if every projection of \( G_A \) over a hyperplane is not an APN \((N - 1, N - 1)\)-function then \( G_A \) has the D-property. The two observations above can be also seen as a consequence of [26, Lemma 3] because \( G_A \) 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 \( G \) has the strong D-property if we have that

\[ \{G(x) + G(y) + G(z) + G(x + y + z) : x, y, z \in A\} = \mathbb{F}_2^N, \]

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

We observe that the strong D-property does not imply APNness. An example is the multiplicative inverse function over \( \mathbb{F}_2^n \) that is 4-uniform and has the strong D-property.

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

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

Examples of APN functions that do not have the strong D-property are some sporadic examples such as \( x^3 \) in dimensions 3 and 5, and all the quadratic APN functions with nonlinearity \( 2^{N-2} \) in \( N \) variables (see Proposition 5.7 below); some sporadic ones being known.
Open Problem 1. Find an infinite class of APN functions that do not have the strong D-property.

If $\mathcal{G}$ is APN, then satisfying this property can be seen as a nice feature because the sums of the values of $\mathcal{G}$ taken over hyperplanes present then some uniformity in their distribution and this kind of random behaviour may help ciphers using $\mathcal{G}$ as an S-box to resist some attacks (e.g. integral attacks; see [21]). Moreover, such property is stronger than the D-property of an APN $(N,N)$-function (and is then possibly not satisfied by a given APN $(N,N)$-function). In the same time, not satisfying it may be seen as positive as well because it allows to construct at least one $(N − 1, N − 1)$-function from $\mathcal{G}$ (see Lemma 5.1). So either $\mathcal{G}$ has a good cryptographic property or we can construct APN functions in dimension $N − 1$. In both cases, we learn something new about $\mathcal{G}$.

We observe that the strong D-property is EA invariant, which is straightforward, and it is not CCZ invariant, which is a little less intuitive; an example (that can be verified computationally) is the Gold APN function $x^3$ over $\mathbb{F}_2^n$ that does not have the strong D-property, but $x^3$ has it over $\mathbb{F}_2^5$.

Taniguchi in [26] studies the D-property of $(N − 1, N)$-functions constructed as the restrictions of APN $(N, N)$-functions to the linear hyperplane $\{x ∈ \mathbb{F}_{2N} | \text{Tr}(x) = 0\}$ (where we identify $\mathbb{F}_{2^N}^2$ and $\mathbb{F}_{2^N}$). The results obtained in [26] indicate that the strong D-property could be very common among quadratic functions and power functions.

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

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

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

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

The following proposition follows from Remark 5.4 and Lemma 5.1.

Proposition 5.5. Let $N ≥ 3$, let $\mathcal{G}$ be a quadratic APN $(N, N)$-function, let $\psi$ be a linear $(N, N)$-function where $\ker(\psi) = \{c\}$ for $c ∈ \mathbb{F}_N^N \setminus \{0\}$, 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 $a, b ∈ E$ we have that $\varphi_\mathcal{G}(a,b) ≠ c$.

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

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

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

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

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

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

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

We have shown that every quadratic APN $(N, N)$-functions with nonlinearity $2^{N-2}$ does not have the strong D-property. If such functions exist for every even $N \geq 10$ this could suggest that the strong D-property could be less common than expected. While we have a strong feeling that for large enough $N$ all APN power functions have the strong D-property, we cannot say the same for quadratic APN functions. Indeed, the data collected in [3] could suggest otherwise (we recall that the trimming operation is identical to our construction) because we have that for $3 \leq N \leq 8$, several quadratic APN $(N, N)$-functions with a nonlinearity strictly larger than $2^{N-2}$ do not have the strong D-property. Another hypothesis could be that for some $N_0 \in \mathbb{N}$, all APN $(N, N)$-functions with $N \geq N_0$ have the strong D-property, but we have no way to verify this for large $N$. Indeed, $N_0$ should be at least 9 and we do not know enough quadratic APN functions in this dimension. In conclusion, answering these questions appears to be very difficult and out of reach for now.
5.2 The strong D-property of crooked functions

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

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

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

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

\[
W_{\pi_G}(u, v) = \sum_{a \in \mathbb{F}_2^N} (-1)^{u \cdot a} |\Lambda_{v,a}| + 2 - 2^N (\delta_0(u) + \delta_0(v))
\]

where \( \Lambda_{v,a} = \{ b \in \mathbb{F}_2^N | \varphi_G(a, b) = v \} \).

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

\[
\mu_{u,v} = \sum_{a,b,w \in \mathbb{F}_2^N} (-1)^{w \cdot (\varphi_G(a,b) + u) + u \cdot a}.
\]

We have that:

\[
\mu_{u,v} = \sum_{a \in \mathbb{F}_2^N} (-1)^{u \cdot a} \sum_{w \in \mathbb{F}_2^N} (-1)^{w \cdot (\varphi_G(a,b) + v)} = 2^N \sum_{a \in \mathbb{F}_2^N} (-1)^{u \cdot a} |\Lambda_{v,a}|
\]

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

For any \( a \in \mathbb{F}_2^N \setminus \{0\} \), we have that \( \sum_{b \in \mathbb{F}_2^N} (-1)^{w \cdot \varphi_G(a,b)} \) equals \( 2^N \) if \( w \in \langle \pi_G(a) \rangle \) and 0 otherwise. By separating the cases (1) \( a = 0 \), (2) \( a \neq 0 \) and \( w = 0 \), (3) \( a = 0 \) and \( w \neq \pi_G(a) \), (4) \( a \neq 0 \) and \( w \not\in \langle \pi_G(a) \rangle \), we then have:

\[
\mu_{u,v} = 2^N \sum_{w \in \mathbb{F}_2^N \setminus \{0\}} (-1)^{w \cdot v} + 2^N \sum_{a \in \mathbb{F}_2^N \setminus \{0\}} (-1)^{w \cdot a} + 2^N \sum_{a \in \mathbb{F}_2^N \setminus \{0\}} (-1)^{v \cdot \pi_G(a) + u \cdot a}
\]

\[
= 2^N \delta_0(v) + 2^N \delta_0(u) - 2^N + 2^N W_{\pi_G}(u, v) - 2^N.
\]

Remark 5.11. Let \( G \) be a crooked \((N, N)\)-function with \( N \geq 3 \). The next lemma will characterize the strong D-property by means of the ortho-derivative and the size of the sets \( \Lambda_c = \bigcup_{a \in \mathbb{F}_2^N} \{a\} \times \Lambda_{c,a} \) where \( \Lambda_{c,a} \) is defined as in Proposition 5.10. We give then here some preliminary observations on the cardinality of these sets \( \Lambda_c = \{(a, b) \in (\mathbb{F}_2^N)^2 | \varphi_G(a, b) = c\} \) where \( c \in \mathbb{F}_2^N \). We observe that, since \( G \) is plateaued, then \( |\Lambda_c| = |\{(a, b) \in (\mathbb{F}_2^N)^2 | D_a D_b G(u) = c\}| \) for any
Let $\lambda^\text{min}$ and $\lambda^\text{max}$ 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 $\lambda^\text{min} \leq 2^N - 2 \leq \lambda^\text{max}$. A characterization of $G$ being AB is that $\lambda^\text{min} = 2^N - 2 = \lambda^\text{max}$ [15, Corollary 27]. If $N$ is even, then $\lambda^\text{min} < 2^N - 2 < \lambda^\text{max}$ since $G$ cannot be AB (note also that $2^N - 2$ is not divisible by 6 because $2^{N-1} - 1$ is divisible by 3 only if $N$ is odd).

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

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

1. We have that $|\Gamma^{(1)}_{v,c}| < \frac{|\Lambda_c|}{4}$ holds if and only if there exists $(a, b) \in \Lambda_c$ with $v \cdot a = v \cdot b = 0$.

2. If there exists $u \in \mathbb{F}_2^N$ such that $D_a D_b G(u) = c$ and $v \cdot a = v \cdot b = 0$, then for all $u \in \mathbb{F}_2^N$ there exist $a, b \in \mathbb{F}_2^N$ such that $D_a D_b G(u) = c$ and $v \cdot a = v \cdot b = 0$.

**Proof.** 1. Let $\Gamma_c$ be the set of all $a \in \mathbb{F}_2^N$ such that $(a, b) \in \Lambda_c$ for some $b \in \mathbb{F}_2^N$, then we have that $|\Gamma_c| = \frac{|\Lambda_c|}{2}$ because if $a \in \Gamma_c$ then $\{b \in \mathbb{F}_2^N \mid (a, b) \in \Lambda_c\}$ contains two elements exactly, since $\varphi_G(a, b) = \varphi_G(a, b')$ implies $D_a D_b G(0) + D_a D_{b'} G(0) = D_a D_{b+a} G(b) = 0$ and, since $G$ is APN, can happen only if $b' = b$ or $b' = b + a$ (note that since $c$ is nonzero, $a$ is nonzero). Then $\Gamma^{(1)}_{v,c} = \{a \in \Gamma_c \mid v \cdot a = 1\}$ because if $v \cdot a = 1$ then $a \neq 0$ and so we have that $\varphi_G(a, b) = c$ for some $b \in \mathbb{F}_2^N$ if and only if $c \cdot \pi_G(a) = 0$. Observe that $\Gamma_c$ can be partitioned in sets of the form $\{a, b, a + b\}$ such that $(a, b) \in \Lambda_c$. Indeed, this follows from the APN property because if we take $(a, b), (a', b') \in \Lambda_c$ and for instance $a = a'$ (resp. $a = b'$ or $a = a' + b'$) then we have that $\{a, b, a + b\} = \{a', b', a' + b'\}$. Observe that for any $(a, b) \in \Lambda_c$, we have that the cardinality $|\{a, b, a + b\} \cap \Gamma^{(1)}_{v,c}|$ is equal either to 0 or to 2 (indeed, the number of elements among $a, b, a + b$ that are non-orthogonal to $v$ is necessarily even). Then $|\Gamma^{(1)}_{v,c}| \leq \frac{|\Lambda_c|}{4}$ with equality only if for all $\{a, b, a + b\} \subseteq \Gamma_c$ with $(a, b) \in \Lambda_c$ we have that $|\{a, b, a + b\} \cap \Gamma^{(1)}_{v,c}| = 2$. So $|\Gamma^{(1)}_{v,c}| < \frac{|\Lambda_c|}{4}$ if and only if there exists $(a, b) \in \Lambda_c$ with $|\{a, b, a + b\} \cap \Gamma^{(1)}_{v,c}| = 0$ that is such that $v \cdot a = v \cdot b = 0$.

2. Let $u \in \mathbb{F}_2^N$, then $G_a(x) = G(x + u)$ is also crooked. Set $\Lambda_c(u) = \{(a, b) \in (\mathbb{F}_2^N)^2 \mid \varphi_G(a, b) = c\}$ and $\Gamma^{(1)}_{v,c}(u) = \{a \in \mathbb{F}_2^N \mid c \cdot \pi_G(a) = 0, v \cdot a = 1\}$. By
using 1, we have that $|\Gamma^{(1)}_{v,c}(u)| < \frac{|\Lambda_c|}{3}$ if and only if there exist $a, b \in \mathbb{F}_2^N$ such that $\varphi_{\mathcal{G}}(a, b) = D_x D_y \mathcal{G}(u) = c$ 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 $|\Gamma^{(1)}_{v,c}(u_1)| < \frac{|\Lambda_c(u_2)|}{3}$ if and only if $|\Gamma^{(1)}_{v,c}(u_2)| < \frac{|\Lambda_c(u_2)|}{3}$. It follows from the fact that $|\Lambda_c(u_1)| = |\Lambda_c(u_2)|$ and that $\Gamma^{(1)}_{v,c}(u_1) = \Gamma^{(1)}_{v,c}(u_2)$. The first equality holds by [15, Theorem 18] because $\mathcal{G}$ is plateaued and $\varphi_{\mathcal{G}_{v,c}}(a, b) = D_x D_y \mathcal{G}(u_1)$ for any $a, b \in \mathbb{F}_2^N$ and $i = 1, 2$. The second equality holds because $\pi_{\mathcal{G}_{v,c}} = \pi_{\mathcal{G}_{v,c}}$ since $\mathcal{G}_{u_i}(x) = \mathcal{G}_{u_2}(x + u_1 + u_2)$.  

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

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

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

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

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

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

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

(8)

and $W_{\pi_\mathcal{G}}(0, c) = |\Lambda_c| - 2^N + 2$, we have that $|\Lambda_c| = W_{\pi_\mathcal{G}}(0, c) + 2^N - 2$ and $|\Gamma^{(1)}_{c,v}| = \frac{|\Lambda_c| + 2^N - W_{\pi_\mathcal{G}}(0, c)}{2}$. So one can check by means of the Walsh transform the strong D-property by using Lemma 5.13.
In the following theorem, we give a sufficient condition for the strong D-property of a crooked function by means of the (first-order) nonlinearity of its ortho-derivative and of the parameter $\lambda^{\min}$ that we introduced above. Note that if $G$ 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 $G$ 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 $G$ be a crooked $(N, N)$-function with $N \geq 3$. Let $\pi_G$ be the ortho-derivative of $G$. Let $\lambda^{\min} = \min_{c, v \in F_2^N \setminus \{0\}} |\Lambda_c|$ where $\Lambda_c = \{(a, b) \in (F_2^N)^2 \mid \varphi_G(a, b) = c\}$ and $\omega$ be the so-called linearity of $\pi_G$, that is, let:

\[ \text{nl}(\pi_G) = 2^{N-1} \cdot \frac{\omega}{2}. \]

If $\omega < \frac{\lambda^{\min}}{3} - 2$, then $G$ has the strong D-property.

More generally, let $\omega' = -\min_{c, v \in F_2^N \setminus \{0\}} (W_{\pi_G}(v, c))$. If $\omega' < \frac{\lambda^{\min}}{3} - 2$, then $G$ has the strong D-property. Moreover, if $N$ is odd, then $\omega' < \frac{2^{N-2}}{3} - 2$ if and only if $G$ has the strong D-property.

**Proof.** Let $c, v \in F_2^N \setminus \{0\}$. We have that $W_{\pi_G}(v, c) = |\Lambda_c| - 4|\Gamma^{(1)}_{c,v}| + 2$ by (8). If we prove that $|\Gamma^{(1)}_{c,v}| < \frac{|\Lambda_c|}{3}$, then by Lemma 5.13 we can conclude that $G$ has the strong D-property. The hypothesis $\omega' < \frac{\lambda^{\min}}{3} - 2$ implies:

\[ |\Gamma^{(1)}_{c,v}| = \frac{|\Lambda_c| + 2 - W_{\pi_G}(v, c)}{4} < \frac{|\Lambda_c| + 2 + \omega'}{4} < \frac{|\Lambda_c| + 2 + \left|\frac{|\Lambda_c|}{3} - 2\right|}{4} = \frac{|\Lambda_c|}{3}, \]

and using Relation (3) with $F = \pi_G$, we have $\omega' \leq \omega$.

For $N$ odd, we have $\lambda^{\min} = 2^N - 2$ by [15, Corollary 27]. So if $\omega' < \frac{2^{N-2}}{3} - 2$, then $G$ has the strong D-property. Conversely, let $c, v \in F_2^N \setminus \{0\}$. If $G$ has the strong D-property, then $|\Gamma^{(1)}_{c,v}| < \frac{|\Lambda_c|}{3}$ by Lemma 5.13 and $W_{\pi_G}(v, c) < \frac{|\Lambda_c|}{3} - 2$ by using the equation $|\Gamma^{(1)}_{c,v}| = \frac{|\Lambda_c| + 2 - W_{\pi_G}(v, c)}{4}$. Since $|\Lambda_c| = 2^N - 2$ by [15, Corollary 27], we have that $\omega' < \frac{2^{N-2}}{3} - 2$. \qed

**Remark 5.15.** Let $\beta = \frac{\lambda^{\min}}{3} - 2$ and let $u$ be the primitive element of the field $F_{2^N}$ over $F_2$ chosen by MAGMA. There are examples of quadratic APN functions where the condition $\omega < \beta$ is not satisfied and $\omega' < \beta$ is satisfied. Some examples are the function $x^3$ over $F_{2^5}$ with $(\omega', \omega, \beta) = (8, 16, 16)$ and the function $ux^{24} + x^{10} + x^4$ over $F_{2^6}$ with $(\omega', \omega, \beta) = (8, 24, 16)$. Moreover, for the case $N$ even, we have that $\omega' < \beta$ is only sufficient and not necessary. Indeed, the following functions have the strong D-property but $\omega' \geq \beta$: the function $ux^9 + u^1x^6 + x^3$ over $F_{2^9}$ with $(\omega', \omega, \beta) = (16, 24, 16)$ and the function $u^{29}x^{48} + u^{15}x^{34} + u^{35}x^{33} + u^{62}x^{20} + u^{10}x^6 + u^{40}x^5$ over $F_{2^9}$ with $(\omega', \omega, \beta) = (24, 32, 8)$. There are also cases where $\omega' = \omega$, for instance in the case of the Gold APN function in dimension $N = 5$, whose ortho-derivative $x^{(2^4 + 1)}$ is plateaued and is a permutation. As we have seen previously, this is not true for the Gold APN function in even dimension.
In the following proposition, we show that Proposition 5.5 holds even if we assume that \( \mathcal{G} \) is crooked instead of quadratic APN (as we announced it after stating that proposition). It is indeed important, each time we have a result on APN quadratic functions, to check whether it extends to crooked functions: if it does, then this argues in favor of the conjecture that all crooked functions are quadratic, and if not, this makes this conjecture more questionable.

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

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

We shall now present in Theorem 4, in the case where \( \mathcal{G} \) is a quadratic APN permutation, a sufficient condition for \( \mathcal{G} \) and \( \mathcal{G}^{-1} \) to have both the strong D-property, which only depends on the second-order nonlinearity of \( \pi_\mathcal{G} \). We shall need the next lemma that uses a similar idea to Lemma 5.13. We recall that since \( \mathcal{G} \) is an \((N,N)\)-permutation, \( N \) must be odd (and therefore \( \mathcal{G} \) is AB), see e.g. [22].

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

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

\[
\begin{align*}
\mathcal{G}(a' + b' + c_0) + \mathcal{G}(a') + \mathcal{G}(b') = 0 \\
v \cdot \mathcal{G}(a') = v \cdot \mathcal{G}(b') = 0.
\end{align*}
\]

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

Theorem 4. Let $G$ be a quadratic APN $(N, N)$-permutation. Let $\pi_G$ be the ortho-derivative of $G$. Let $\omega_2$ be such that $\mu_2(\pi_G) = 2N-1 - (\omega_2/2)$. If $\omega < \frac{2^N-2}{3}$, then $G$ and $G^{-1}$ have the strong D-property.

Proof. Since $\mu_2(\pi_G) \geq \mu_2(\pi_G)$, then $\omega \leq \omega_2$ where $\mu_2(\pi_G) = 2N-1 - (\omega_2/2)$. Since $\lambda_{\min} = 2N - 2$, then $G$ has the strong D-property by Theorem 3. Let us prove that $G^{-1}$ has the strong D-property. Let $c, v \in \mathbb{F}_2^N \setminus \{0\}$ and $c_0 = c + G^{-1}(0)$. Let $g(a) = G(c_0) \cdot \pi_G(a + c_0)$ and $h(a) = v \cdot G(a)$. Let $\gamma_{ij} = |\{a \in \mathbb{F}_2^N \setminus \{c_0\} \mid g(a) = i, h(a) = j\}|$.

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 $\pi_{G^{-1}}(a, b) = c$ and $v \cdot a = v \cdot b = 0$ by Lemma 5.17.

We also claim that, for all $u \in \mathbb{F}_2^N$ there exists $a, b \in \mathbb{F}_2^N$ such that $G^{-1}(a + b + u) + G^{-1}(a + u) + G^{-1}(b + u) + G^{-1}(u) = c$ and $v \cdot a = v \cdot b = 0$. This will imply the strong D-property of $G^{-1}$.

We first prove the first claim. Observe that $g$ and $h$ are balanced because $\pi_G$ and $G$ are permutations and $G(c_0) \neq 0$. Moreover, $g(c_0) = 0$ because $\pi_0(0) = 0$.

Before proceeding with the proof, we show three relations that we will need later.

We have that $\gamma_{0,1} + \gamma_{0,0} = |g^{-1}(0) \setminus \{c_0\}| = 2N-1 - 1$, $\gamma_{0,1} + \gamma_{1,1} = |h^{-1}(1) \setminus \{c_0\}| = 2N-1 + 2\delta_0(h(c_0))$, and $\gamma_{0,0} + \gamma_{0,0} = |h^{-1}(0) \setminus \{c_0\}| = 2N-1 - \delta_0(h(c_0))$.

So, denoting $f = g + h$, we have that:

$$\sum_{a \in \mathbb{F}_2^N \setminus \{c_0\}} (-1)^{f(a)} = \gamma_{1,0} + \gamma_{0,0} - \gamma_{1,0} - \gamma_{0,1},$$

$$= 2\gamma_{0,0} - 2\gamma_{0,1} + (\gamma_{0,1} + \gamma_{1,1}) - (\gamma_{1,0} + \gamma_{0,0}) =$$

$$= -4\gamma_{0,1} + 2(\gamma_{1,0} + \gamma_{0,0}) - 1 - 2\delta_0(h(c_0))$$

$$= -4\gamma_{0,1} + 2N - 3 - 2\delta_0(h(c_0)),$$

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

$$\sum_{a \in \mathbb{F}_2^N \setminus \{c_0\}} (-1)^{f(a)} = 2\delta_0(h(c_0)) - 1 + \sum_{a \in \mathbb{F}_2^N \setminus \{c_0\}} (-1)^{f(a)}$$

$$= 2N - 4\gamma_{0,1} - 4 + 4\delta_0(h(c_0)).$$

(10)

Observe that $-\sum_{a \in \mathbb{F}_2^N} (-1)^{f(a)} \leq \sum_{a \in \mathbb{F}_2^N} (-1)^{f(a)} \leq \omega_2$ because $h$ is quadratic.

So we can conclude, using (10), that

$$\gamma_{0,1} = \frac{1}{4} \left( 2N - \sum_{a \in \mathbb{F}_2^N} (-1)^{f(a)} - 1 + \delta_0(h(c_0)) \right) \leq \frac{2N + \omega_2}{4} < \frac{2N - 2}{3}.$$
We now prove the second claim. We have proven that, for any crooked function $\mathcal{G}$, if $n_{\mathcal{G}}(\pi_{\mathcal{G}}) > 2^{N-1} - \frac{2^{N-2} + 1}{2}$, then there exists $a, b \in \mathbb{F}_2^N$ such that $\varphi_{\mathcal{G}^{-1}}(a, b) = c$ and $v \cdot a = v \cdot b = 0$. Let $u \in \mathbb{F}_2^N$; we observe that $\pi_{\mathcal{G}} = \pi_{\mathcal{G}^N}$ where $\mathcal{G}^n(x) = \mathcal{G}(x) + u$ and $(\mathcal{G}^n)^{-1}(x) = \mathcal{G}^{-1}(x + u)$. Since $n_{\mathcal{G}}(\pi_{\mathcal{G}^N}) = n_{\mathcal{G}}(\pi_{\mathcal{G}}) > 2^{N-1} - \frac{2^{N-2} + 1}{2}$, there exists $a, b \in \mathbb{F}_2^N$ such that $\varphi_{(\mathcal{G}^n)^{-1}}(a, b) = \mathcal{G}^{-1}(a + b + u) + \mathcal{G}^{-1}(a + u) + \mathcal{G}^{-1}(b + u) + \mathcal{G}^{-1}(u) = c$ and $v \cdot a = v \cdot b = 0$.

\[ \Box \]

5.3 The strong D-property of the Gold APN function and its compositional inverse

In this subsection, the ortho-derivative of a crooked function over $\mathbb{F}_{2^N}$ is defined by using the inner product $a \cdot b = \text{Tr}(ab)$ for any $a, b \in \mathbb{F}_{2^N}$. Let $\mathcal{G}(x) = x^{2^{n+1}}$ where $\gcd(i, N) = 1$ be the Gold APN function over $\mathbb{F}_{2^N}$. To prove the strong D-property of $\mathcal{G}$, it is enough to verify the D-property of the $(N-1, N)$-function $\mathcal{G}_E$ where $E = \{ x \in \mathbb{F}_{2^N} \mid \text{Tr}(x) = 0 \}$ (see Remark 5.6). Therefore, we can use some of the results by Taniguchi in \[26\]. We have that $\mathcal{G}$ has the strong D-property for $N \geq 6$ even \[26\, \text{Example 6}\] . In this subsection, we are going to address the case $N$ odd. With this result, all cases will be covered for Gold functions\footnote{Taniguchi could not address in \[26\] the case of odd dimension $N$, except for the cube function $F(x) = x^3$ when the dimension is a multiple of $9, 11, 13$ or $15$.}.

Moreover, we are going to prove that the strong D-property holds also for its compositional inverse $\mathcal{G}^{-1}$ which is defined only for $N$ odd. We will do that by showing a lower bound of the second-order non-linearity of $\pi_{\mathcal{G}}(x) = x^{-(2^{n+1})}$ and then we will apply Theorem 4. We will need to use the upper bound proved in \[25\] on the value of the extended Kloosterman sum.

Lemma 5.18 \[25\]. Let $\mathcal{F}(x), \mathcal{G}(x)$ be non-degenerate non-zero polynomials with coefficients in $\mathbb{F}_{2^N}$ (non-degenerate meaning that each non-zero term has an odd univariate degree). Then

\[
\sum_{x \in \mathbb{F}_{2^N}} (-1)^{\text{Tr}((\mathcal{F}^{-1})+\mathcal{G}(x))} \leq (\text{d}(\mathcal{F}) + \text{d}(\mathcal{G})) 2^{N/2} + 1
\]

where $\text{d}(\mathcal{F})$ and $\text{d}(\mathcal{G})$ are respectively the algebraic degree of $\mathcal{F}$ and $\mathcal{G}$.

Corollary 5.19. Let $\mathcal{F}, \mathcal{G}$ be functions over $\mathbb{F}_{2^N}$ such that $\text{Tr}(\mathcal{F})$ and $\text{Tr}(\mathcal{G})$ are not constant functions. Then

\[
\sum_{x \in \mathbb{F}_{2^N}} (-1)^{\text{Tr}((\mathcal{F}^{-1})+\mathcal{G}(x))} \leq (\text{d}(\mathcal{F}) + \text{d}(\mathcal{G})) 2^{N/2} + 1
\]

where $\text{d}(\mathcal{F})$ and $\text{d}(\mathcal{G})$ are respectively the algebraic degree of $\mathcal{F}$ and $\mathcal{G}$.

Proof. Let $\Sigma = \sum_{x \in \mathbb{F}_{2^N}} (-1)^{\text{Tr}((\mathcal{F}^{-1})+\mathcal{G}(x))}$. Consider the univariate representations of $\mathcal{F}(x), \mathcal{G}(x)$ (which are polynomials with coefficients in $\mathbb{F}_{2^N}$ and univariate degree at most $2^N - 1$). Suppose that $\mathcal{G}(x)$ is degenerate. Therefore,
\( G(x) \) has a non-zero term \( cx^e \) with even univariate degree. If \( e = 0 \), then \( \Sigma \) is equal to

\[
\left| (1 - \text{Tr}(c) \sum_{x \in \mathbb{F}_{2^N}} (-1)\text{Tr}(\mathcal{F}(x^{-1}) + G(x) + c)) \right|
\]

If \( e \neq 0 \), there exist a positive odd integer \( e' \) and a positive integer \( k \) such that \( e' = 2^k e \mod 2^N - 1 \) and we have that \( \text{Tr}(G(x)) = \text{Tr}(G(x) + cx^e + c^2x^{e'}) \). We can do similarly for \( \mathcal{F} \). So there exist \( \mathcal{F}'(x), G'(x) \) non-degenerate non-zero polynomials with coefficients in \( \mathbb{F}_{2^N} \) such that \( \Sigma = \sum_{x \in \mathbb{F}_{2^N}} (-1)\text{Tr}(\mathcal{F}'(x^{-1}) + G'(x)) \) and \( d(\mathcal{F}') = d(\mathcal{F}), d(G') = d(G) \). We conclude by using Lemma 5.18.

**Theorem 5.** Let \( N \geq 3 \) and \( i \) be such that \( \gcd(i, N) = 1 \). Then the Gold APN function \( x^{2^{N-1}+1} \) over \( \mathbb{F}_{2^N} \) has the strong D-property if and only if \( N = 6 \) or \( N \geq 8 \). If \( N \) is odd, the compositional inverse of the Gold APN function \( x^{2^{N-1}+1} \) has the strong D-property if and only if \( N \geq 7 \).

*Proof.* Let \( d = 2^i + 1 \). As we have discussed previously, the case \( N < 8 \) has been verified computationally and the case \( N = 8 \) follows from [26, Example 6] (which shows that the restrictions to the hyperplane \( \{x \in \mathbb{F}_{2^N} \mid \text{Tr}(x) = 0\} \) of Gold APN functions in even dimension have the D-property) and Remark 5.6. By using Theorem 4, we will prove the case \( N \geq 9 \) odd for both \( x^d \) and \( x^i \). Let \( G(x) = x^d \), then we have that \( \pi_G(x) = x^{-d} \) [8]. Let \( \mathcal{H} \) be a function over \( \mathbb{F}_{2^N} \) with algebraic degree at most \( 2 \). Let \( v \in \mathbb{F}_{2^N} \setminus \{0\} \) and let \( \Sigma = \sum_{x \in \mathbb{F}_{2^N}} (-1)\text{Tr}(vx^{-d} + \mathcal{H}(x)) \). If \( \text{Tr}(\mathcal{H}) \) is constant, then \( \Sigma = \sum_{x \in \mathbb{F}_{2^N}} (-1)\text{Tr}(vx^i) \) = 0 since \( N \) is odd. If \( \text{Tr}(\mathcal{H}) \) is not a constant function, then we can apply Corollary 5.19 and we have that \( \Sigma \leq 2^{N/2+2} + 1 \). So we have that \( \|\pi_G\| \geq 2^{N-1} - (2^{N/2+2} + 1)/2 \). Since \( 2^{N/2+2} + 1 < 2^{N-2}/3 - 2 \) if \( N \geq 9 \), we can conclude the proof by Theorem 4.

**Remark 5.20.** We observe that for the Gold APN function in even dimension \( N \), all the values of \( |A_c| \) defined in Remark 5.11 are known from [13, Example 2], so we can prove similarly that for some positive integer \( N_0 \) the Gold APN function has the strong D-property for \( N \geq N_0 \) even. We obtain this way a simpler proof than in [26, Example 6]. Let \( N \) be even, \( c \in \mathbb{F}_{2^N} \setminus \{0\} \), and \( G \) be a Gold APN function over \( \mathbb{F}_{2^N} \). We have that either \( |A_c| \in \{2^N - 2^{N/2-1} - 2, 2^N + 2^{N/2} - 2\} \) or \( |A_c| \in \{2^N + 2^{N/2+1} - 2, 2^N - 2^{N/2} - 2\} \). Therefore, we have that \( 2^N - 2^{N/2} - 2 \leq \lambda \). Now we can use a similar argument to the proof of Theorem 5. If \( \mathcal{H}(x) = ux \) for some \( u \in \mathbb{F}_{2^N} \), then \( \Sigma = |W_{\pi_G}(u, v)| \). Assume that \( u \neq 0 \). Observe that \( |W_{\pi_G}(0, v)| = \sum_{x \in \mathbb{F}_{2^N}} (-1)^{\text{Tr}(vx^i)} \leq 2^{N/2+1} \) and if \( u \neq 0 \), then \( |W_{\pi_G}(u, v)| \leq 3 \cdot 2^{N/2} + 1 \) by Corollary 5.19. Since \( 3 \cdot 2^{N/2} + 1 < (2^N - 2^{N/2} - 2)/3 - 2 \leq \lambda \) if \( N \geq 8 \), we can conclude by Theorem 3.

The ortho-derivatives of other classes of quadratic APN functions can be derived from the work done in the paper [8], but they do not have an easy-to-handle representation like the Gold APN function.

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

**Lemma 5.21** ([26]). Let $G(x) = x^d$ be an APN power function over $\mathbb{F}_{2^N}$ with $N \geq 3$. Let $t > 2$ be a positive integer such that $t$ divides $N$ and such that $t$ is even if $N$ is even. Let us denote $E_t = \{ x \in \mathbb{F}_{2^t} \mid \text{Tr}_t(x) = 0 \}$ and $E_N = \{ x \in \mathbb{F}_{2^N} \mid \text{Tr}_N(x) = 0 \}$. If the $(t - 1, t)$-function $G_{E_t}$ has the D-property, then the $(N - 1, N)$-function $G_{E_N}$ has the D-property.

We deduce:

**Proposition 5.22.** Let $t$ be a positive integer, let $G(x) = x^d$ where $d = 2^{4t} + 2^{2t} + 2^t - 1$ be the Dobbertin APN function over $\mathbb{F}_{2^{4t}}$, and let $E = \{ x \in \mathbb{F}_{2^{4t}} \mid \text{Tr}_{5t}(x) = 0 \}$. Then the $(5t - 1, 5t)$-function $G_E$ has the D-property if and only if $t \geq 2$.

**Proof.** Let $E_k = \{ x \in \mathbb{F}_{2^k} \mid \text{Tr}_k(x) = 0 \}$ be defined for any positive integer $k$. 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 5.21. So it is enough to prove that the $(t - 1, t)$-function $G_{E_t}$ has the D-property. Observe that $G$ restricted to $\mathbb{F}_{2^t}$ is equal to the cube function $x^3$ because $2^{4t} \equiv 2^{3t} \equiv 2^{2t} \equiv 2^t \equiv 1 \pmod{2^t - 1}$. The function $x^3$ over $\mathbb{F}_{2^t}$ has the strong D-property by Theorem 5 since $t \neq 7$, so the restriction of $x^3$ to $E_t$ has the D-property. To prove the case $t = 7$, we use again Lemma 5.21 but this time we consider the restriction to $\mathbb{F}_{2^{5t}}$. It can be verified computationally that the $(4, 5)$-function $G_{E_t}$ has the D-property.

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

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

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

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

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

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

The permutation in even dimension $N - 1$ is obtained as the restriction of the $(N, N)$-function $F(x) = \frac{x}{x + 1} + \frac{y}{y + 1} + x$ to the linear hyperplane $E = \{x \in \mathbb{F}_{2N} \mid \text{Tr}(x) = 0\}$. The fact that $F_E$ is a permutation is proved in [12] thanks to observations involving the Dickson permutation polynomials. Using Lemma 5.1 and changing $x$ into $x + 1$, $F_E$ is not APN if and only if there exist $x, y, z \in \mathbb{F}_{2N}$ such that $\text{Tr}(x) = \text{Tr}(y) = \text{Tr}(z) = 1$ and $x^{2N-2} + y^{2N-2} + z^{2N-2} + (x + y + z)^{2N-2} = 1$ (because $\text{Tr}(a + 1) = \text{Tr}(a) + 1$). We shall prove more: there is a solution $(x, y, z)$ such that $z = 1$, that is, the system
\[
\begin{align*}
\{ & \quad x^{2N-2} + y^{2N-2} + (x + y + 1)^{2N-2} = 0 \\
\text{Tr}(x) = \text{Tr}(y) = 1
\end{align*}
\]
has a solution in $\mathbb{F}_{2N}$ for $N > 7$ odd. We will prove it by using the well known Hasse-Weil bound [20, 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 $\mathbb{F}_{2N}$. Then a curve in the projective plane $\mathbb{P}^2(\mathbb{F}_{2N})$ is defined as $V^2(\mathbb{F}_{2N})(H) = \{(X : Y : Z) \in \mathbb{P}^2(\mathbb{F}_{2N}) \mid H(X, Y, Z) = 0\}$ where $\mathbb{P}^2(\mathbb{F}_{2N}) = \{(X : Y : Z) : (X, Y, Z) \in (\mathbb{F}_{2N})^3 \setminus \{(0, 0, 0)\}\}$ and $(X : Y : Z) = \{(aX, aY, aZ) \in \mathbb{F}_{2N}^3 \mid a \in \mathbb{F}_{2N} \setminus \{0\}\}$. The curve is called absolutely irreducible if and only if the multivariate polynomial $H$ is irreducible in every extension field of $\mathbb{F}_{2N}$. 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 $\partial$ indicates the partial formal derivative) has no solution in every field extension of $\mathbb{F}_{2N}$ 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

\[ ||V_{F_{E}}(E)\rangle - (2^N + 1) \leq 2g \cdot 2^{N/2} \]

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

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

1. If \( N \geq 7 \), then System (11) has a solution.
2. If \( N \geq 5 \), then the \((N-1, N-1)\)-permutation \( F_E \) is not APN where \( F(x) = \frac{1}{x+1} + \frac{1}{x+1} + x \) and \( E = \{ x \in \mathbb{F}_{2^N} | \text{Tr}(x) = 0 \} \).

**Proof.** Note that since \( \text{Tr}(x) = \text{Tr}(y) = 1 \), 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 a solution if and only if \( G(X, Y) = F(X^2 + X + 1, Y^2 + Y + 1) \) has a root \((X, Y)\) (since \( X \mapsto X^2 + X + 1 \) is onto \( E + 1 \)). Let \( D \) be the degree of \( G(X, Y) \) and let \( H(X, Y, Z) = Z^D \cdot G(\frac{X}{Z}, \frac{Y}{Z}) \) be the homogenization of \( G(X, Y) \). We verified by using MAGMA [5] (can be done easily since the curve has coefficients in \( \mathbb{F}_2 \)) that \( V_{F_{E}(E)}(H) \) 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

\[ |V_{F_{E}(E)}(H)| \geq 2^N + 1 - 2 \cdot 3 \cdot 2^{N/2} \].

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 \( F_E \) is not APN. Since the case \( N = 5 \) can be verified computationally, this concludes the proof.

\[ \square \]

**Remark 6.1.** When considering the strong D-property of the inverse function, the problem is more complex since it corresponds to verifying that the restriction of \( \psi(x^{-1}) \) to \( A \) is not APN whatever is the affine hyperplane \( A \) and whatever is the kernel of \( \psi \) (while above, we verified this for the hyperplane of equation \( \text{Tr}(x) = 1 \) and for \( \ker \psi = \{1\} \) 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 \((x, y) \in (\mathbb{F}_{2^N})^2:\)

\[
\begin{cases}
  x^{2^N-2} + y^{2^N-2} + (x + y + \epsilon)^{2^N-2} + \epsilon + c = 0 \\
  \text{Tr}(x) = \text{Tr}(y) = \epsilon
\end{cases}
\]

(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 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 \( G_{c, \epsilon}(X, Y, Z) = F_{c, \epsilon}(X^2 + X + \epsilon, Y^2 + Y + \epsilon) \) where \( F_{c, \epsilon}(x, y) \) is a polynomial whose zeros are the solutions of the first equation of System (12). However, having \( c \) and \( \epsilon \) as parameters of the curve (while above we had only one value for \( c \) and one for \( \epsilon \)) increases the difficulty of the problem noticeably because we cannot use MAGMA to prove properties of the curve (notice that the coefficients of the curve do not belong to a fixed subfield as for the case \( c = 1 \)).

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

31
Conjecture 2 is verified computationally for every odd \(N\) between 5 and 25.

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

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

### 6.2 On the non-APNness of the Li-Wang families

Li and Wang in [23] define explicitly two families of permutations in dimension \(N - 1\) even, of the form \(F_E\) where \(F(x) = \psi(G(x))\), \(\psi\) is a linear function with a kernel of dimension 1, \(E = \text{Im} \psi\), and \(G\) is an APN permutation. The first one is such that \(\psi(x) = cx^2 + c^2 x\) for any \(c \in \mathbb{F}_{2^n} \setminus \{0\}\) and \(G(x) = x^{\frac{1}{1 \pm} N}\) with \(\gcd(i, N) = 1\) \((G\) is the inverse of the Gold APN function) [23, Theorem 4].

The second one is such that \(\psi(x) = x^s + x\) and \(G(x) = x^{\frac{1}{1 \pm} N} + \text{Tr}_1^N(x + x^{2^i})\) with \(N\) divisible by 3, \(\gcd(i, N) = 1\), and \(s = i \mod 3\) [23, Theorem 6]. For \(N \leq 9\), it has been verified computationally in [23] that both families do not produce APN permutation in even dimension \(N - 1\). Since \(x^{\frac{1}{1 \pm} N}\) has the strong D-property for \(N \geq 7\) (see Theorem 5) and such property is EA invariant, both families never produce APN permutations (see Lemma 5.1).

### 7 Constructions of permutations with the Li-Wang method

We show that the construction of Li and Wang in [23] can be generalized by investigating the problem of constructing an \((N - 1, N - 1)\)-permutation from an \((N, N)\)-function \(F(x) = \psi(G(x))\) where \(\psi\) is a linear function with a kernel of dimension 1 and \(G\) is a permutation. Then we discuss the case where \(F(x)\) is equal to \(\psi(G(x)) + x\) instead. In this way, we provide many families of complete permutations with good cryptographic properties.

We present now the Li-Wang construction with our notation.

**Construction 1** (Li-Wang construction [23]). Let \(G\) be an APN permutation over \(\mathbb{F}_{2^n}\) with a quadratic compositional inverse \(G^{-1}\) and such that \(G(0) = 0\). So \(N\) is odd because quadratic APN permutations exist only in odd dimension, since any plateaued APN \((n, n)\)-function has always some bent components when \(n\) is even [15, Subsection 11.3.4]. For any \(c \in \mathbb{F}_{2^n} \setminus \{0\}\), the function
Lemma 7.1. \( \psi_c(y) = G^{-1}(y) + G^{-1}(y+c) + G^{-1}(c) \) is linear with a kernel of dimension 1 since \( G^{-1} \) is a quadratic APN function. Li and Wang proved that by taking \( F(x) = \psi_c(G(x)) \), the restriction \( F_E \), where \( E = \text{Im} \psi_c \), is a permutation with differential uniformity 4 \cite[Theorem 2]{23} and optimal known nonlinearity in even dimension \cite[Theorem 3]{23}, that is \( 2^{n-1} - 2^2 \) where \( n = N - 1 \). We will prove that if \( A \) is the complement of \( E \), then also \( F_A \) is a permutation and it is CCZ equivalent to \( F_E \). Even if Li and Wang in \cite[Theorem 3]{23} did not discuss the function \( \psi \), we will still consider it a product of the Li-Wang construction.

With the following Lemma (heavily inspired by the first part of \cite[Theorem 2]{23} but providing an original result) we are going to exhibit some necessary and sufficient conditions such that the restriction to an affine hyperplane of a function of the form \( \psi(G(x)) \) is a permutation when \( G \) is a permutation and \( \psi \) is linear with a kernel of dimension 1. This will generalize the Li-Wang construction.

Lemma 7.1. Let \( G \) be a permutation over \( \mathbb{F}_{2^n} \). Let \( v, c \in \mathbb{F}_{2^n} \setminus \{0\} \) and let \( E = \{ x \in \mathbb{F}_{2^n} \mid \text{Tr}(vx) = 0 \} \). Let \( A \) be the complement of \( E \), and let \( \psi \) be any linear function over \( \mathbb{F}_{2^n} \) with ker \( \psi = \{c\} \). Let \( F(x) = \psi(G(x)) \) and let \( B(x) = G^{-1}(G(x) + c) \). Then the following are equivalent:

1. \( F_E \) is a permutation.
2. \( B(E) = A \).
3. \( F_A \) is a permutation.
4. \( \text{Tr}(vB(x)) = \text{Tr}(vx) + 1 \) for all \( x \in \mathbb{F}_{2^n} \).
5. \( \text{Tr}(vD_cG^{-1}(x)) = 1 \) 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 \( F(x) = F(y) \) if and only if \( G(x) + G(y) \in \ker \psi \). Since \( G \) is a permutation, this happens only if \( G(x) + G(y) = c \). Observe that the latter equation is equivalent to the equation \( y = G^{-1}(G(x) + c) = B(x) \).

Let us prove that 1 implies 2. Suppose that there exists \( x \in E \) such that \( y = B(x) = G^{-1}(G(x) + c) \) is in \( E \). Then \( G(x) + G(y) = c \) and this is a contradiction since \( F_E \) is a permutation and \( x \neq y \) (because \( c \neq 0 \)). So \( B(E) \subseteq A \) and therefore \( B(E) = A \) because \( B \) is a permutation.

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

To prove that 2 and 3 are equivalent, we first prove similarly that \( F_A \) is a permutation if and only if \( B(A) = E \), and we can see this is equivalent to 2 because \( B \) is a permutation.

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

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

As a consequence of Lemma 7.1, we have that the Li-Wang construction (Construction 1) produces two permutations that are \( F_E \) and \( F_A \), because Condition 5 on \( G^{-1} \) in Lemma 7.1 is met for any \( c \in \mathbb{F}_{2^n} \setminus \{0\} \) and with \( v = \pi_{G^{-1}}(c) \),
since $\mathcal{G}^{-1}$ is a crooked permutation. Indeed, since $\mathcal{G}^{-1}$ is crooked, the image of every derivative $D_s \mathcal{G}^{-1}$ is the affine hyperplane $A = D_s \mathcal{G}^{-1}(0) + (\pi_{\mathcal{G}^{-1}}(e))^{-1}$ and $A$ is not a linear hyperplane because $D_s \mathcal{G}^{-1}(x) \neq 0$ for all $x \in \mathbb{F}_{2^N}$, since $\mathcal{G}^{-1}$ is a permutation. So (the Li-Wang) Construction 1 is in this framework because quadratic APN functions are crooked. The simplest example is when $\mathcal{G}^{-1}$ is a Gold APN function in odd dimension. However, $\mathcal{G}^{-1}$ can be not crooked and however satisfy condition 5 of Lemma 7.1. As an example, Li and Wang constructed in their [23, Theorem 6] a family of permutations where $\mathcal{G}^{-1}$ is not crooked. They showed that for $\mathcal{G}(x) = x^{\frac{2^N-1}{3}} + \text{Tr}^{N}_1(x + x^{3^i})$ with $N$ odd divisible by 3, gcd$(i,N) = 1$, and $s = i \mod 3$, we have that $\text{Tr}(D_1 \mathcal{G}^{-1}(x)) = 1$ for all $x \in \mathbb{F}_{2^N}$ [23, Lemma 5] and that the restriction of $\mathcal{F}(x) = \mathcal{G}(x)^2 + \mathcal{G}(x)$ to $E = \{x \in \mathbb{F}_{2^N} \mid \text{Tr}(x) = 0\}$ is a permutation. Since the authors did not know about Lemma 7.1, they prove those results specifically for that function. But their result is less exciting after observing that $\mathcal{F}_E$ is EA equivalent to their own family [23, Theorem 4], that is the restriction of $x^{\frac{2^N-1}{3}} + x^{\frac{1}{3^i}}$ to $E$ because the two functions in dimension $N$ are EA equivalent (see Remark 4.4). So in [23], it remained unclear if it is possible to construct a permutation in dimension $N - 1$, using an APN permutation $\mathcal{G}$ which is EA inequivalent to any permutation with quadratic inverse. We show that it is possible by applying directly Lemma 7.1.

Take $\mathcal{G}^{-1}$ to be the APN permutation over $\mathbb{F}_{2^N}$ given in [10, subsection 5.1] named $F_2$. It is straightforward to verify that $\text{Tr}(D_1 \mathcal{G}^{-1}) = 1$ where $c = \zeta^{4i}$ and $\zeta$ is defined as in [10] to be the primitive element of $\mathbb{F}_{2^N}$ over $\mathbb{F}_2$ chosen by MAGMA. It can also be verified that the permutations over $\mathbb{F}_{2^N}$ obtained in this way are not APN.

Using Lemma 7.1, 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 $\text{Tr}(vD_i \mathcal{G}^{-1}(x)) = 1$ for all $x \in \mathbb{F}_{2^N}$. Let $E = \{x \in \mathbb{F}_{2^N} \mid \text{Tr}(vx) = 0\}$, let $A$ be the complement of $E$, and let $\psi$ be any linear function over $\mathbb{F}_{2^N}$ with ker $\psi = \langle c \rangle$. By Lemma 7.1, 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 larger than or equal to nil($\mathcal{G}$) $- 2^{N-2}$ and they are $2\delta$-uniform if $\mathcal{G}$ is $\delta$-uniform (in particular, they are 4-uniform if $\mathcal{G}$ is APN).

**Proposition 7.2.** The Li-Wang construction (Construction 1), the family defined in [23, Theorem 4], and the one defined in [23, Theorem 6] are particular cases of Construction 2.

**Proof.** The framework of Construction 2 is exactly the one given in Lemma 7.1 and we have already shown that the Li-Wang construction and those families are in such framework.

Once a permutation has been obtained, it is important to give the expression of its inverse, if this is at all possible. This was not provided in [23]. Moreover, since we have seen that the Li-Wang construction provides two functions and not only one, it is interesting to look whether these two functions are equivalent or not. In the following lemma, we give a description of $(\mathcal{F}_E)^{-1}$ (resp. $(\mathcal{F}_A)^{-1}$) by following a similar idea to [23, Proposition 2]. This gives a sufficient condition to have that $\mathcal{F}_E$ and $\mathcal{F}_A$ are CCZ equivalent.
Lemma 7.3. In the setting of Construction 2, the following holds for \( F(x) = ψ(G(x))\):

1. Let \( H(x) = G^{-1}(x) + \text{Tr} (vG^{-1}(x)) D_{c} G^{-1}(x) \) and \( H'(x) = H(x) + D_{c} G^{-1}(x) \). Let \( U \) be any linear hyperplane of \( \mathbb{F}_{2}^{N} \) such that \( c \not\in U \), then function \( (F_{E})^{-1} \) is affine equivalent to \( H_{U} \) and function \( (F_{A})^{-1} \) is affine equivalent to \( H'_{U} \).

2. If the function \( D_{c} G^{-1}(x) \) is affine, then \( F_{E} \) is CCZ equivalent to \( F_{A} \).

Proof. Let us prove 1. Observe that the restriction of \( ψ \) to \( U \) is bijective with codomain \( \text{Im} \psi \) because \( U \cap \text{ker} \psi = \{0\} \), thanks to the hypothesis \( c \not\in U \), and since \( U \) has the same cardinality as \( \text{Im} \psi \). We claim that \( H_{U} = (F_{E})^{-1} \circ ψ_{U} \) (where \( ψ_{U} \) is the restriction of \( ψ \) to \( U \)), and \( H'_{U} = (F_{A})^{-1} \circ ψ_{U} \). To prove it, we show that for any linear function \( ψ' \) such that \( \psi'_{\text{Im} \psi} = (ψ_{U})^{-1} \) we have that \( H_{U} = (ψ'_{\text{Im} \psi} \circ F_{E})^{-1} \) and \( H'_{U} = (ψ'_{\text{Im} \psi} \circ F_{A})^{-1} \). Let \( x \in a + E \) where \( a \) is some element of \( \mathbb{F}_{2}^{N} \) and \( y = ψ'(F(x)) \). We claim that \( x = H(y) \) if \( a \in E \) and \( x = H'(y) \) otherwise and this will conclude the proof. Observe that \( y = G(x) \) if \( G(x) \in U \) and \( y = G(x) + c \) otherwise. This implies that \( y = G(x) \) if \( \text{Tr}(vG^{-1}(y)) = \text{Tr}(vx) = \text{Tr}(va) \) and that \( y = G(x) + c \) if \( \text{Tr}(vG^{-1}(y)) = \text{Tr}(vG^{-1}(y + c)) + 1 = \text{Tr}(vx) + 1 = \text{Tr}(va) + 1 \). Let \( g(y) = \text{Tr}(vG^{-1}(y)) + \text{Tr}(va) \), then \( x = G^{-1}(y) \) if \( g(y) = 0 \) and \( x = G^{-1}(y + c) \) otherwise. Since we have that

\[
x = (g(y) + 1)G^{-1}(y) + g(y)G^{-1}(y + c) = G^{-1}(y) + g(y)D_{c} G^{-1}(y),
\]

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

Let us prove 2. Let \( U \) be a linear hyperplane such that \( c \not\in U \). Using 1, we have that \( (F_{E})^{-1} \) is affine equivalent to \( H_{U} \) and \( (F_{A})^{-1} \) is affine equivalent to \( H'_{U} \). Since the function \( D_{c} G^{-1}(x) \) is affine and \( H'(x) = H(x) + D_{c} G^{-1}(x) \), then \( H_{U} \) and \( H'_{U} \) are EA equivalent (see Remark 4.4). Therefore, function \( (F_{E})^{-1} \) is EA equivalent to function \( (F_{A})^{-1} \) and so function \( F_{E} \) is CCZ equivalent to function \( F_{A} \).

In the proof of Lemma 7.3, we showed the existence of a sequence of inversions, EA transformations, and affine transformations which transforms \( F_{E} \) into \( F_{A} \) 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 \( D_{c} G^{-1} \) is an affine function, so the equivalence may not be true in the general setting of Construction 2.

In [23, Theorem 5], Li and Wang observed that the family constructed in [23, 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 \( F_{E}' \) is a permutation where \( F'(x) = F(x) + x \) and that \( (F_{E}')^{-1} \) 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 \( ψ_{c}(x) = D_{c} G^{-1}(x) + D_{c} G^{-1}(0) \) is a linear function with a kernel of dimension 1 and \( ψ = ψ_{c} \) (which is the case in [23]). This setting includes the Li-Wang construction because \( G^{-1} \) is a quadratic APN function and so \( ψ_{c} \) has the property we want. For \( F'(x) = F(x) + x \), we construct two functions \( F_{E}' \) and \( F_{A}' \) that are EA equivalent respectively to \( F_{E} \) and \( F_{A} \).
ψ in Construction 2 with the additional hypothesis that representations of restrictions.

There is no mention of this property in [23] because we believe that the authors were more focused on affine invariant properties, and they did not focus on representations of restrictions.

**Proposition 7.4.** Let $G$ be a permutation and $F$, $E$, and $A$ be defined as in Construction 2 with the additional hypothesis that $\psi_c(x) = D_0 G^{-1}(x) + D_0 G^{-1}(0)$ is a linear function with a kernel of dimension 1 and that $\psi = \psi_c$. Let $F'(x) = \psi_c(G(x)) + x$, let $a = D_0 G^{-1}(0)$, and let $\phi$ be a linear bijective function from $\mathbb{F}_{2^N}$ to $E$. Then we have the following:

1. $a$ belongs to $A$ and function $F'(x)$ is equal to $G^{-1}(G(x) + c) + a$.

2. Up to affine equivalence, we can write $F_E(y) = \phi^{-1}(F(\phi(y)))$, $F_A(y) = \phi^{-1}(F(\phi(y) + a))$, $F'_E(y) = \phi^{-1}(F'(\phi(y)))$, and $F'_A(y) = \phi^{-1}(F'(\phi(y) + a) + a)$.

3. Using the representations in 2, we have that $F_E$, $F_A$, $F'_E$, and $F'_A$ are complete permutations and that $F'_A = (F'_E)^{-1}$.

**Proof.** Let us prove 1. We have that $a \in A$ because $\text{Tr}(\psi D_0 G^{-1}) = 1$. Function $F'(x)$ is equal to $G^{-1}(G(x) + c) + a$ because $\psi_c(G(x)) = G^{-1}(G(x) + c) + G^{-1}(G(x) + c) = \psi_c(G(x) + c) + a$.

Let us prove 2. Let $\zeta$ be a linear bijective function from $\mathbb{F}_{2^N}$ to $\mathbb{F}_{2^N}$ such that $\zeta(x) = \phi^{-1}(x)$ for all $x \in E$. We have that $(\phi,0,\zeta,0)$ is a representation of $F_E$ and of $F'_E$, $(\phi,a,\zeta,a)$ is a representation of $F_A$, and $(\phi,a,\zeta,a)$ is a representation of $F'_A$ (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 $F'(x) = G^{-1}(G(x) + c) + a$, then $F'$ is a permutation and the two functions $F_E$ and $F'_A$ are permutations. We claim that $F_E(y) + F'_E(y) = y$ and that $F_A(y) + F'_A(y) = y$. Since $F(x) + F'(x) = x$, we have that $F_E(y) + F'_E(y) = \phi^{-1}(F(\phi(y))) + \phi^{-1}(\phi(y)) = y$ and that $F_A(y) + F'_A(y) = \phi^{-1}(F(\phi(y) + a) + F'(\phi(y) + a) + a) = \phi^{-1}(\phi(y) + a + a) = y$. We claim that $F'_A = (F'_E)^{-1}$. Observe that since $F'(x) + D_0 G^{-1}(0) = G^{-1}(G(x) + c)$, we have that $F'(F'(x) + a) + a = x$ and that $F'(x + a) + a = x$. We conclude by showing that $(F'_E)^{-1}(y) = \phi^{-1}((F')^{-1}(\phi(y))) = \phi^{-1}(F'(\phi(y) + a) + a) = F'_A(y)$.

Using Proposition 7.4, we define the following construction.

**Construction 3.** In the setting of Construction 2 with the additional hypothesis that $\psi_c(x) = D_0 G^{-1}(x) + D_0 G^{-1}(0)$ is a linear function with a kernel of dimension 1 and that $\psi = \psi_c$, let $F'(x) = \psi_c(G(x) + x)$. Using the representations in Proposition 7.4, item 2, we have that $F_E$, $F_A$, $F'_E$, and $F'_A$ are complete permutations and that $F'_A = (F'_E)^{-1}$. Functions $F'_E$ and $F'_A$ are EA equivalent respectively to $F_E$ and $F_A$ (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 7.4, we can describe precisely the linear function that maps the graph of $F_E$ to the
graph of $F_A$. We claim that such function is $(y, z) \mapsto (y + z, z)$ over $(\mathbb{F}_{2^n}-1)^2$.

Since $(y, F_E(y)) \mapsto (y + F_E(y), F_E(y)) = (F'_E(y), F_E(y))$, we have to show that $F_E(w) = F_A(y)$ where $w = (F'_E)^{-1}(y)$. Indeed, we have that $F_E(w) = F_E(w) + w = F'_E(w) + w = y + F'_A(y) = F_A(y)$ because $w = F'_A(y)$.

Conclusion

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

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

References


