Quadratic-like balanced functions and quadratic-like permutations

Claude Carlet and Irene Villa
Universities of Bergen, Norway, and Paris 8 (LAGA), France;
University of Trento, and University of Genoa, Italy.

E-mail: claude.carlet@gmail.com; irene1villa@gmail.com

Abstract

We study those (n, n)-permutations, and more generally those balanced (n, m)-functions, whose component functions all admit a derivative equal to constant function 1 (this property itself implies balancedness). We call these functions quadratic-like permutations (resp. quadratic-like balanced functions) since all quadratic balanced functions have this property. We show that all Feistel permutations, all crooked permutations and (more generally) all balanced strongly plateaued functions, and all permutations of the form $F(x) = x + \gamma f(x)$ where f is Boolean and more general permutations obtained by a generalized switching method that we introduce have this same property, and we observe that the notion is affine invariant. We show that for APN permutations, satisfying this property is equivalent to being crooked. We also study in each of these classes the "reversed" property that every derivative in a nonzero direction has a component function equal to constant function 1, and we show that this property can be satisfied only if $m \geq n$. We show that the "reversed" property implies injectivity and, for $m = n$, all the functions in the classes of quadratic-like permutations described above have the "reversed" property. We also observe that all the quadratic-like power permutations $F(x) = x^d$, $x \in \mathbb{F}_{2^n}$ must be quadratic. We give several constructions of quadratic-like permutations and balanced functions outside the three classes of quadratic balanced functions, permutations affine equivalent to Feistel permutations and crooked permutations. We characterize the property by the Walsh transform and the algebraic normal form.

Keywords: Vectorial Boolean functions, balanced functions, permutations

1 Introduction

Among the so-called (n, m)-functions $F : \mathbb{F}_2^n \to \mathbb{F}_2^m$, those that are balanced, that is, whose pre-images $F^{-1}(y) = \{x \in \mathbb{F}_2^n; F(x) = y\}$ all have the same

size (namely, the size 2^{n-m}, where necessarily $m \leq n$) present a particular interest in discrete mathematics, and in their applications such as cryptography. Indeed, using unbalanced substitution boxes (S-boxes) in a (Feistel) cipher needs in practice to complexify the cipher (see e.g. the block cipher PICARO [26]). Balanced S-boxes allow then a better speed and less complexity (if all the needed criteria can be satisfied by such a balanced function).

Among balanced functions, those such that $m = n$, that is, (n, n)-permutations, are of a still more specific interest, since permutation polynomials have always been the subject of a special attention in discrete mathematics, and S-boxes in those block ciphers having the structure of substitution permutation network (SPN) need to be permutations.

We know (see e.g. [10]) that an (n, m)-function is balanced if and only if its component functions, that is, the Boolean functions (from $\mathbb{F}_2^n$ to $\mathbb{F}_2$) of the form $v \cdot F$, where $v \in \mathbb{F}_2^m \setminus \{0\}$ and "$\cdot$" is some inner product in $\mathbb{F}_2^m$ (for instance the usual inner product $y \cdot y' = \sum_{i=1}^m y_i y'_i$), are all balanced (that is, have Hamming weight 2^{n-1}). We also know that quadratic Boolean functions $f : \mathbb{F}_2^n \to \mathbb{F}_2$, that is, Boolean functions whose algebraic degree (see definition in Section 2) is at most 2, are balanced if and only they admit at least one *derivative* (in some *direction* a) $D_a f(x) := f(x) + f(x + a)$ equal to constant function 1 (such an element a is called a *1-linear structure* of f).

Such a property may be useful for finding balanced functions (and in particular, permutations). But if all the component functions of F are quadratic, then the function F is itself quadratic. In cryptography, this is considered a weakness when F is used as an S-box, since it allows an attack on the cipher, called the higher order differential attack; see [23, 20]). However, the property that all component functions admit a 1-linear structure is not restricted to quadratic balanced functions. We shall see indeed that the (balanced) functions having this property constitute a strict super-class of the class of quadratic balanced functions, and is then particularly interesting to study, because the non-quadratic elements in this super-class have some advantages of quadratic functions without sharing their weaknesses. We shall call *quadratic-like balanced* the functions whose component functions all have a 1-linear structure.

The class of quadratic-like balanced functions contains, as we shall show in Section 4, several classic classes of vectorial balanced functions, and this gives a link between classes which apparently are quite different. It contains, for $m = n$ even, all the so-called *Feistel* permutations (which play an important role in the design of block ciphers)[1]. These permutations have the form $(x, y) \in (\mathbb{F}_2^{n/2})^2 \mapsto F(x, y) = (y, x + \phi(y))$, where $\phi : \mathbb{F}_2^{n/2} \to \mathbb{F}_2^{n/2}$ can be any function (whatever the choice of ϕ, function F is a permutation). The class of quadratic-like balanced functions also contains all crooked permutations (we shall recall in Section 2 what these functions are and prove this property in Section 4)

[1]To be honest, this inclusion has a limited impact on Feistel ciphers themselves, since in such ciphers, the Feistel permutations, which have a too simple structure from a cryptographic viewpoint, are composed to reach a sufficient complexity through the iteration of rounds, and the property of being a quadratic-like permutation (or balanced function) is not preserved by composition, similarly to quadraticity and contrary to bijectivity (and balancedness).

and more generally all balanced strongly plateaued functions (whose component functions all are partially-bent – see the definition in Section 2 and the proof in Section 4). Thus, we obtain that the notion of quadratic-like balanced function generalizes that of strongly plateaued function, which generalizes that of crooked permutations, suggesting a further motivation for studying this property. We shall see in Section 4 that for APN permutations (see the definition in Section 2) being quadratic-like balanced is equivalent to being crooked. We shall also show in Section 5 that all the permutations of the form $F(x) = x + \gamma f(x)$ where f is Boolean are quadratic-like[2]. We shall also introduce a generalization of the switching method and study how it can generate quadratic-like permutations.

We shall see in Section 3 that the notion is affine invariant. We shall also consider in Section 3 the possibility that every derivative in a nonzero direction has a component function equal to constant function 1, and call this the "reversed" property. This property can be satisfied only if $m \geq n$ since it implies injectivity (for $m = n$, it implies bijectivity) as we shall see, and for $m = n$ it can be seen as a natural generalization of the crookedness property. Another generalization that is in fact closely related was presented in [7], introduced in relation to an attack against a hash function, under the name of *weakly crooked of codimension 1* (for (n, n)-permutations, being weakly crooked of codimension 1 is more general than the reversed property). The work in [7] shows a cryptanalytic interest in the notion of the "reversed" property, and in Section 3 we provide results on the reversed property that slightly complete those on weakly crooked functions of some codimension $d \geq 1$. We shall study constructions of quadratic-like balanced functions in Section 5, and focus on those that are neither quadratic, nor affine equivalent[3] to permutations having a Feistel form, nor crooked, nor even strongly plateaued. We will prove that all the functions in these latter classes possess the "reversed" property. We shall characterize the notion of quadratic-like balancedness by the Walsh transform and by the algebraic normal form.

2 Preliminaries

For n a positive integer, we denote by $\mathbb{F}_2^n$ the n-dimensional vector space over $\mathbb{F}_2 = \{0, 1\}$, by e_i for $1 \leq i \leq n$ the i-th element of the canonical base of $\mathbb{F}_2^n$, by 0_n the vector of all zeros, and by $\mathbb{F}_{2^n}$ the finite field with 2^n elements. We shall denote by $+$ the addition in any of these two groups. The vector space $\mathbb{F}_2^n$ can be endowed with the structure of the field $\mathbb{F}_{2^n}$, by the very construction of the Galois extension $\mathbb{F}_{2^n}$ of $\mathbb{F}_2$, or given a basis $(\alpha_1, \ldots, \alpha_n)$ of $\mathbb{F}_{2^n}$ viewed as a vector space over $\mathbb{F}_2$, by mapping any $(x_1, \ldots, x_n) \in \mathbb{F}_2^n$ to $\sum_{i=1}^n x_i \alpha_i \in \mathbb{F}_{2^n}$. In the paper, we shall write $\mathbb{F}_2^n$ when we shall not use the structure of field and $\mathbb{F}_{2^n}$ when we shall use it. With "$\cdot$" we indicate any inner product over $\mathbb{F}_2^n$ or $\mathbb{F}_{2^n}$, for instance the usual inner product over $\mathbb{F}_2^n$: $a \cdot b = \sum_{i=1}^n a_i b_i \in \mathbb{F}_2$

[2]Recall that changing a permutation F into a permutation of the form $F(x) + \gamma f(x)$ where f is Boolean is called the switching method, see e.g. [10].

[3]The definition of this equivalence will be recalled in Section 2.

where $a = (a_1, \ldots, a_n)$ and $b = (b_1, \ldots, b_n)$, or the inner product over $\mathbb{F}_{2^n}$: for $a, b \in \mathbb{F}_{2^n}$, $a \cdot b = tr_n(ab) \in \mathbb{F}_2$, where $tr_n(x) = \sum_{i=0}^{n-1} x^{2^i}$ is the (absolute) trace function. We denote similarly inner products over $\mathbb{F}_2^n \times \mathbb{F}_2^m$ or over $\mathbb{F}_{2^n} \times \mathbb{F}_{2^m}$, defined as: $(a_1, a_2) \cdot (b_1, b_2) = a_1 \cdot b_1 + a_2 \cdot b_2$.

For positive integers n, m, we call (n, m)-functions (and n-variable Boolean functions when $m = 1$) the functions $F : \mathbb{F}_2^n \to \mathbb{F}_2^m$. If we do not specify n, m, we speak of vectorial Boolean functions if $m > 1$ and of Boolean functions if $m = 1$; in this latter case, we denote the functions by lower case letters $f : \mathbb{F}_2^n \to \mathbb{F}_2$. We can write an (n, m)-function F as $F = (f_1, \ldots, f_m)$, where the $(n, 1)$-functions f_i, for $i = 1, \ldots, m$, are called the *coordinates* of F. For $v \in \mathbb{F}_2^m$, the v-component of F is the $(n, 1)$-function $F_v : x \mapsto v \cdot F(x)$. For $a \in \mathbb{F}_2^n$, we call *derivative of F in the direction of a* the (n, m)-function $D_aF(x) = F(x+a)+F(x)$. A function F admits a unique representation as a multivariate polynomial in n variables $x_1, \ldots, x_n$:

$$F(x) = \sum_{I \subseteq \{1,\ldots,n\}} a_I \prod_{i \in I} x_i, \quad a_I \in \mathbb{F}_2^m; x = (x_1, \ldots, x_n).$$

The *algebraic degree*, or simply the *degree*, of F is then $\deg(F) = \max_I\{|I|; a_I \neq 0_m\}$ if the function is nonzero (and 0 if the function is zero). Notice that the algebraic degree of F equals the maximum degree of its component functions. Function F is *affine* if and only if $\deg(F) \leq 1$ and *linear* if additionally $F(0_n) = 0_m$. If $\deg(F) \leq 2$ then F is called *quadratic*, similarly we define *cubic* functions, and so on. An (n, m)-function F is called *balanced* if all its preimages, namely $F^{-1}(y) = \{u \in \mathbb{F}_2^n; F(u) = y\}$ for $y \in \mathbb{F}_2^m$, have the same size. We have that an (n, m)-function F is balanced if and only if all its component functions (that is, in the case of functions over the vector space $\mathbb{F}_2^n$, all the linear combinations of the coordinate functions with non-all zero coefficients) are balanced (see e.g. [10, Proposition 35]). For $m = n$, balanced functions are called *permutations*, since they induce a permutation over $\mathbb{F}_2^n$. Two (n, m)-functions F and G are: *affine equivalent* if $G = A_1 \circ F \circ A_2$ for A_1, A_2 affine bijections of $\mathbb{F}_2^m$ and $\mathbb{F}_2^n$ respectively; *extended affine (EA) equivalent* if $G = F' + A$ for F' affine equivalent to F and A an (n, m)-affine map; *CCZ-equivalent* [11] if $\mathcal{G}_G = \mathcal{A}(\mathcal{G}_F)$ for $\mathcal{A}$ affine bijection of $\mathbb{F}_2^{n+m}$ and $\mathcal{G}_F, \mathcal{G}_G$ the graph $\{(x, F(x)); x \in \mathbb{F}_2^n\}$ of F and G respectively. Affine equivalence is a particular case of EA-equivalence, which is itself a particular case of CCZ-equivalence. The balancedness property is generally preserved only by the affine equivalence, while the algebraic degree (when greater than 1) is also preserved by EA equivalence but in general not by CCZ equivalence.

An (n, n)-function is *crooked* (in the strict sense of [1]) if, for every nonzero $a \in \mathbb{F}_2^n$, the image set of D_aF is the complement of a linear hyperplane. More generally, an (n, n)-function is *almost perfect nonlinear (APN)* if, for every nonzero $a \in \mathbb{F}_2^n$, the image set of D_aF has size 2^{n-1}, that is, for any $b \in \mathbb{F}_2^n$, the equation $D_aF(x) = b$ admits at most 2 solutions.

The Walsh transform of an $(n, 1)$-function f (i.e. a Boolean function) is defined as $W_f(u) = \sum_{x \in \mathbb{F}_2^n} (-1)^{f(x)+u \cdot x}$, for $u \in \mathbb{F}_2^n$. The Parseval's relation

for Walsh transform writes $\sum_{u\in\mathbb{F}_2^n} W_f(u)^2 = 2^{2n}$ and the inverse Walsh transform formula writes $\sum_{u\in\mathbb{F}_2^n} W_f(u)(-1)^{u\cdot x} = 2^n(-1)^{f(x)}$. We also have the formula: $W_f^2(u) = \sum_{a\in\mathbb{F}_2^n}\Big(\sum_{x\in\mathbb{F}_2^n}(-1)^{f(x)+f(x+a)}\Big)(-1)^{u\cdot a}$ and its inverse formula $\sum_{x\in\mathbb{F}_2^n}(-1)^{f(x)+f(x+a)} = 2^{-n}\sum_{u\in\mathbb{F}_2^n}(-1)^{u\cdot a}W_f^2(u)$.
We say that $a\in\mathbb{F}_2^n$ is a *linear structure* of f if $D_af(x)$ is a constant function. Specifically, we say that a is a 0-linear structure (resp. 1-linear structure) if $f(x+a)+f(x)$ is the constant function 0 (resp. 1). Hence if f admits a 1-linear structure, then it is affine equivalent to a function of the form $x_1+g(x_2,\ldots,x_n)$, with g an $(n-1,1)$-function. The set E_0 of 0-linear structures of f is a vector space and, if the set of 1-linear structures of f is non-empty, this latter set is an affine space whose direction is E_0. We have that a is a 0-linear structure, resp. 1-linear structure, if and only if $supp(W_f) = \{u\in\mathbb{F}_2^n; W_f(u)\neq 0\}$ is included in $\{0_n,a\}^\perp = \{x\in\mathbb{F}_2^n; a\cdot x = 0\}$, resp. in its complement, see [10, Proposition 29]. Recall that a balanced quadratic Boolean function always admits a 1-linear structure (see e.g. [10, Proposition 55 and the lines following it]). We say that $f:\mathbb{F}_2^n\to\mathbb{F}_2$ is *bent* if its Walsh transform W_f takes the values $\pm 2^{\frac{n}{2}}$ only. We say that f is *partially-bent* if for any $a\in\mathbb{F}_2^n$ the derivative D_af is either balanced or constant. Hence, every quadratic functions is partially-bent. A vectorial Boolean function whose components are all partially-bent is called *strongly plateaued* (see [10, Chapter 6, Subsection 5.1]). Crooked functions are (equivalently) APN strongly plateaued functions [9, 10].
The Walsh transform of an (n,m)-function is defined as $W_F(u,v) = W_{F_v}(u)$. For $m=n$ odd, F is called *almost bent* (AB) if $W_F(u,v)\in\{0,\pm 2^{\frac{n+1}{2}}\}$ for every $u,v\in\mathbb{F}_2^n$, $v\neq 0_n$. This implies that F is APN.

Another important property that can be connected to the Walsh transform is the nonlinearity: for an (n,m)-function F the *nonlinearity* is defined as $nl(F) = \min_{v\neq 0_m} nl(F_v)$, where $nl(F_v)$ is the (Hamming) distance between F_v and the set of affine Boolean functions. It holds that $nl(F) = 2^{n-1} - \frac{1}{2}\max_{u\in\mathbb{F}_2^n, v\in\mathbb{F}_2^m\setminus\{0_m\}}|W_F(u,v)|$; and the maximum possible value for $nl(F)$ is $2^{n-1}-2^{n/2-1}$.

To conclude this part, we recall that when $m=n$, or more generally when m divides n, identifying $\mathbb{F}_2^n$ with $\mathbb{F}_{2^n}$ and $\mathbb{F}_2^m$ with its subfield of order 2^m, we can uniquely represent F as a univariate polynomial (of degree at most 2^n-1) over $\mathbb{F}_{2^n}$:

$$F(x) = \sum_{i=0}^{2^n-1} b_i x^i, \quad b_i\in\mathbb{F}_{2^n}.$$

Using this representation, the algebraic degree corresponds to the maximum 2-weight (i.e. Hamming weight of the binary expansion) of the exponents i such that $b_i\neq 0$. All the notions presented before find an equivalent definition in this setting. If not specified, it will be clear from the context whether we are considering the univariate or the multivariate representation of F.

3 Quadratic-like balanced functions

The idea of quadratic-like balancedness comes from the observation of the properties of balanced quadratic functions and the following lemma.

Lemma 1. *Consider any (n, m)-function $F : \mathbb{F}_2^n \to \mathbb{F}_2^m$, where n and m are two positive integers. If for any nonzero $v \in \mathbb{F}_2^m$, F_v admits a 1-linear structure, then F is balanced (which implies that $m \leq n$, and if $m = n$, then F is a permutation).*

Proof. As we recalled in Section 2, we know that any vectorial (n, m)-function F is balanced if and only if its component functions F_v, $v \neq 0_m$ are balanced. And we know that if a Boolean function has a derivative equal to constant 1, then it is balanced since it takes complementary values on two complementary affine hyperplanes. This completes the proof. □

We recalled in Section 2 that any balanced quadratic Boolean function $f : \mathbb{F}_2^n \to \mathbb{F}_2$ admits a 1-linear structure. Therefore, we introduce the following definition and terminology.

Definition 1. *A function $F : \mathbb{F}_2^n \to \mathbb{F}_2^m$ is called* quadratic-like balanced *(shortly, $\mathcal{QLB}$) if, for any nonzero $v \in \mathbb{F}_2^m$, there exists $a \in \mathbb{F}_2^n$ such that the derivative $D_aF_v = v \cdot D_aF$ of $F_v : x \mapsto v \cdot F(x)$ is constantly equal to 1, that is, a is a 1-linear structure of F_v. Equivalently, the image set of D_aF is disjoint from the hyperplane $\{0_m, v\}^\perp$.*
In the case $m = n$, the function is called a quadratic-like permutation *(shortly, $\mathcal{QLP}$).*
We shall call component-to-linear-structure map *(shortly, `cls` map) any function mapping $v \in \mathbb{F}_2^m \setminus \{0_m\}$ to one of such a (that is also nonzero) satisfying $D_aF_v \equiv 1$ (where " $\equiv$" means "constantly equal to"). We may extend the domain of such a map to $\mathbb{F}_2^m$ by mapping 0_m to 0_n.*

Notice that these functions appeared already in cryptographic frameworks. For example, Golić in [18, Theorem 2] has observed that if the filtering function of a filtered LFSR (with primitive polynomial) is *perfectly balanced*, that is of the form $g(x_1, \ldots, x_{n-1}) + x_n$ (up to some permutation of variables), then the property of uniformity is satisfied. Later, Canteaut [6] proved that this condition is also necessary. A function of that form is a basic example of a quadratic-like balanced Boolean function. Other known examples of quadratic-like balanced vectorial functions will appear below, in addition to balanced quadratic functions.

Remark 1. *An (n, m)-function is not $\mathcal{QLB}$ if and only if at least one of its component functions $f = v \cdot F$; $v \neq 0_m$, is such that, for every a, there exists an element x such that x belongs to the support (respectively, the co-support) of f and $x + a$ also belongs to the support (respectively, the co-support) of f, or equivalently:*

$$(f^{-1}(0) + f^{-1}(0)) \cup (f^{-1}(1) + f^{-1}(1)) = \mathbb{F}_2^n.$$

Hence, F is $\mathcal{QLB}$ if and only if any of its component functions f satisfies:

$$(f^{-1}(0)+f^{-1}(0)) \cup (f^{-1}(1)+f^{-1}(1)) \neq \mathbb{F}_2^n.$$

Moreover, for every $a \in \mathbb{F}_2^n \setminus \big((f^{-1}(0)+f^{-1}(0)) \cup (f^{-1}(1)+f^{-1}(1))\big)$, we have $D_a f \equiv 1$.
Notice that, if we know that f is balanced, then we have that $a \in f^{-1}(0)+f^{-1}(0)$ if and only if $a \in f^{-1}(1)+f^{-1}(1)$, because if for instance $a \notin f^{-1}(1)+f^{-1}(1)$, then for every x in $f^{-1}(1)$, we have $x+a \in f^{-1}(0)$, and all the 2^{n-1} elements x in the support of f are such that $f(x+a)=0$, that is, the translation by a maps the support of f to its co-support, and vice-versa. Hence, it cannot be that $a \in f^{-1}(0)+f^{-1}(0)$.
The conditions above reduce then to $f^{-1}(0)+f^{-1}(0)=\mathbb{F}_2^n$, respectively, $f^{-1}(0)+f^{-1}(0) \neq \mathbb{F}_2^n$.

The property can be characterized by means of the graph of the function.

Remark 2. *Given an (n,m)-function F, if we denote $\mathcal{G}_F := \{(x,F(x)); x \in \mathbb{F}_2^n\}$ and $\Delta_F := \mathcal{G}_F + \mathcal{G}_F$, then F is injective if and only if Δ_F has no intersection with $(\mathbb{F}_2^n \setminus \{0_n\}) \times \{0_m\}$ and it is quadratic-like if, for every nonzero $v \in \mathbb{F}_2^m$, there exists $a \in \mathbb{F}_2^n$ such that $(\{a\} \times \mathbb{F}_2^m) \cap \Delta_F \subset \{a\} \times (\{0_m, v\}^\perp)^c$ where $(\{0_m, v\}^\perp)^c$ is the complement of $\{0_m, v\}^\perp = \{y \in \mathbb{F}_2^m; v \cdot y = 0\}$.*

In the next proposition, we summarize in the terms of Definition 1 the observations made at the beginning of this section, and we recall the arguments for clarity:

Proposition 1. *Consider any (n,m)-function $F : \mathbb{F}_2^n \to \mathbb{F}_2^m$, where n and m are two positive integers.*
If F is balanced and quadratic, then it is $\mathcal{QLB}$.
If F is $\mathcal{QLB}$, then it is a balanced map (not necessarily quadratic); and then if $m=n$, F is a permutation.

Proof. The first assertion is a consequence of [10, Proposition 35] and the property that a quadratic Boolean function f is balanced if and only if it has a 1-linear structure (see e.g. [10, Proposition 55] and the few lines following this proposition). The second is a rephrasing of Lemma 1. □

Remark 3. *An apparently interesting subclass of $\mathcal{QLB}$ functions is that of maps $F : \mathbb{F}_2^n \to \mathbb{F}_2^m$ such that, for every nonzero $v \in \mathbb{F}_2^m$, there exists $b \in \mathbb{F}_2^m$ such that the set $\mathcal{E}_{F,b} = \{a \in \mathbb{F}_2^n; D_a F(x) \equiv b\}$ is non-empty and $v \cdot b = 1$. However, at least, for m large, this subclass is not that interesting. Indeed, while for $m=1$ the subclass coincides with the class of $\mathcal{QLB}$ functions, for $m \geq 2$, the functions in this subclass are (up to equivalence) the direct sums of a linear (m,m)-permutation and an $(n-m,m)$-function (and for $m=n$ they are then affine permutations), "direct" meaning that the functions have disjoint sets of input variables. Indeed, let us introduce the following sets:*

$$\mathcal{A} = \{a \in \mathbb{F}_2^n : D_a F \text{ is constant}\}; \quad \mathcal{B} = \{b \in \mathbb{F}_2^m : \mathcal{E}_{F,b} \neq \emptyset\}.$$

Then, when F belongs to the subclass, we have $|\mathcal{A}| \geq |\mathcal{B}|$. Notice that $\mathcal{B}$ is a linear space (as well as $\mathcal{A}$). Indeed, for $b_1, b_2 \in \mathcal{B}$, take $a_1 \in \mathcal{E}_{F,b_1}$ and $a_2 \in \mathcal{E}_{F,b_2}$. Now, $D_{a_1+a_2}F(x) = D_{a_1}F(x+a_2) + D_{a_2}F(x) = b_1 + b_2$, so $b_1 + b_2 \in \mathcal{B}$. Let $d \leq m$ be the dimension of $\mathcal{B}$. If $d < m$, then there exists a nonzero element $v \in \bigcap_{b\in\mathcal{B}}\{0_m, b\}^{\perp}$. Since F is a function in the subclass, there exists $b \in \mathcal{B}$ such that $v \cdot b = 1$, hence a contradiction. Therefore we have $d = m$.
Now, we show by induction on t, with $1 \leq t \leq m$, that for a function in the introduced subclass, up to affine transformation, the first t variables appear only in linear terms and the derivatives in the corresponding directions (that we can take without loss of generality equal to $e_1,\ldots,e_t$) are linearly independent.
First step, $t = 1$. There is a direction a such that $D_aF \equiv c_a$ is nonzero. Up to affine transformation, we have $a = e_1$ and define $D_{e_1}F \equiv c_1$. Therefore in F the variable x_1 appears only in linear terms.
Inductive step, $t < m$. Suppose that the first t variables of F appear only in linear terms and by setting $D_{e_i}F \equiv c_i$, for $i = 1,\ldots,t$, we have that $c_1,\ldots,c_t$ are linearly independent. Since $t < m$, there exists $v \in \bigcap_{i=1}^{t}\{0_m, c_i\}^{\perp}$ nonzero. Let a be the direction such that $D_aF \equiv c$ and $c \cdot v = 1$. Clearly, $c \notin \langle c_1,\ldots,c_t\rangle$ so a is linearly independent from $e_1,\ldots,e_t$ and up to an affine transformation we can assume $a = e_{t+1}$. So the induction step is proved.
Therefore, we proved that functions $F : \mathbb{F}_2^n \to \mathbb{F}_2^m$ belonging to this subclass are, up to affine equivalence, of the form $F(x_1,\ldots,x_n) = L(x_1,\ldots,x_m) + G(x_{m+1},\ldots,x_n)$, where $L : \mathbb{F}_2^m \to \mathbb{F}_2^m$ is a linear permutation, and $G : \mathbb{F}_2^{n-m} \to \mathbb{F}_2^m$ is any function.

The following example shows that the notion of quadratic-like balanced function is not trivial, in the sense that, in general, the set of quadratic balanced functions is a proper subset of the set of quadratic-like balanced functions, which is itself a proper subset of the set of balanced functions.

Example 1. *Over $\mathbb{F}_2^4$, consider the following two permutations*

$$F_1(x) = \begin{bmatrix} x_1x_2 + x_3 \\ x_1x_2 + x_1x_3 + x_2 \\ x_1x_2 + x_2x_3 + x_1 + x_2 \\ x_1x_2x_3 + x_4 \end{bmatrix}, \quad F_2(x) = \begin{bmatrix} x_1 \\ x_2 \\ x_1x_3 + x_4 \\ x_1x_2x_3 + x_2x_4 + x_3 \end{bmatrix}.$$

Then F_1 is an example of $\mathcal{QLP}$ (of degree 3), while F_2 is an example of permutation not quadratic-like. Notice that, by removing the first coordinate of F_1 and F_2, we have an example of $\mathcal{QLB}$ $(4,3)$-function (of degree 3) and an example of balanced $(4,3)$-function not quadratic-like. Another example of permutation not quadratic-like, is the inverse map considered in the univariate representation. Indeed, for $n = 4$, $2^n - 2 = 2 \cdot 7$, and for $v = 1$ there is no $a \in \mathbb{F}_{2^n}$ such that $tr_n(x^7 + (x+a)^7) = tr_n((a^{1/2} + a^4)x^3 + a^2x^5 + (a^{3/4} + a^{5/2} + a^6)x + a^7)$ is constantly 1.

These are just simple examples for illustration purposes. We shall see more general examples and counter-examples in the next subsections and sections.

3.1 Invariance under equivalence relations

When introducing a new property for vectorial Boolean functions, we are interested in knowing under which classical notion of equivalence (recalled in Section 2) the property is invariant. This allows to deduce a whole class of functions having the property from each function found which satisfies it, and to clarify what it means that some construction leads to new functions having the property.

Consider two affine equivalent (n, m)-functions F, F', with $F' = A_1 \circ F \circ A_2$, for A_1, A_2 affine bijections over $\mathbb{F}_2^m$ and $\mathbb{F}_2^n$ respectively. Let L_1, L_2 be the linear parts of A_1, A_2 resp., then for $a \in \mathbb{F}_2^n$, we have $D_a F'(x) = F'(x+a) + F'(x) = L_1\big(F(A_2(x)+L_2(a))+F(A_2(x))\big)$. Hence, $v \cdot D_a F'(x) = L_1^*(v) \cdot D_{L_2(a)} F(A_2(x))$, with L_1^* the adjoint linear operator of L_1, satisfying $v \cdot L_1(u) = L_1^*(v) \cdot u$ for any $u, v \in \mathbb{F}_2^m$. So we can state the following result.

Proposition 2. *The quadratic-like balancedness is invariant under affine equivalence.*

Of course, the notion is also preserved by the addition of a constant function, since this does not change the derivatives, but it is not preserved by EA-equivalence (and therefore by CCZ-equivalence), since the more general property of being balanced is not preserved. For example, consider F to be any affine permutation; F is a quadratic-like permutation but it is EA-equivalent to any constant function, which clearly cannot be a permutation.

Remark 4. *We investigated whether, restricted to permutations, the quadratic-like property is EA invariant. Consider the following $(5, 5)$-functions*

$$F(x) = \begin{bmatrix} x_1x_2x_3 + x_1x_2x_4 + x_1 + x_2x_3x_4 + x_2x_3 + x_5 \\ x_1x_2x_4 + x_1x_2 + x_1x_3x_4 + x_1x_3 + x_2 \\ x_1x_2x_3 + x_1x_2 + x_1x_3x_4 + x_1x_3 + x_2x_3x_4 + x_2x_3 + x_3 + x_5 \\ x_1x_2x_3 + x_1x_2x_4 + x_1x_3x_4 + x_1x_3 + x_4 \\ x_1 \end{bmatrix}, L(x) = \begin{bmatrix} x_5 \\ 0 \\ 0 \\ 0 \\ x_2 + x_3 \end{bmatrix},$$

then it can be verified that both F and $F+L$ are permutations, but F is quadratic-like and $F + L$ is not. Therefore we have that EA equivalence, restricted to permutations, in general does not preserve the quadratic-like property. The same holds for balanced (n, m)-functions, for $m < n$. This can be verified if we consider the $(5, 2)$-functions obtained by reducing F and L to their first two coordinates.
Moreover, when restricted to permutations, the quadratic-like property is not preserved by the application of the inverse transformation either. Indeed, consider the quadratic permutation, in univariate representation, $F(x) = x^3 \in \mathbb{F}_{2^5}[x]$ and its inverse $F^{-1}(x) = x^{21}$. Being quadratic, F is quadratic-like whereas we checked that F^{-1} is not. Hence, the quadratic-like property is in general not preserved by the application of the inverse transformation.

We verified that the property is invariant under affine transformation and addition of a constant function, hence to study to which extent the notion is

not preserved by EA-equivalence, we are left to study the behavior under the addition of a linear map. The conditions under which the quadratic-like property is obtained are displayed in the following proposition.

Proposition 3. *Consider an (n,m)-function F and a linear function $L:\mathbb{F}_2^n\to\mathbb{F}_2^m$. Then the map $F+L$ is $\mathcal{QLB}$ if and only if, for any nonzero $v\in\mathbb{F}_2^m$, we have $\{L(a);a\in A_v\}\cap\{0_m,v\}^\perp\neq\emptyset$ or $\{L(a);a\in B_v\}\cap\left(\{0_m,v\}^\perp\right)^c\neq\emptyset$, where A_v is the set of 1-linear structures of F_v and B_v is the set of 0-linear structures of F_v.*

Proof. The statement is a consequence of the fact that $D_aL(x)=L(a)$, hence $v\cdot D_a(F+L)=D_aF_v+v\cdot L(a)$. Then we have $v\cdot D_a(F+L)\equiv 1$ if and only if a is a 1-linear structure of F_v and $v\cdot L(a)=0$ or a is a 0-linear structure and $v\cdot L(a)=1$. □

Remark 5. *Notice that the above proposition does not imply that also F is quadratic-like balanced. Indeed, (using the same notation as in the proposition) there could be $v\in\mathbb{F}_2^m$ such that $A_v=\emptyset$ but such that there exists a nonzero $a\in B_v$ with $L(a)\cdot v=1$.*

Question 1. *Proposition 3 implies that a necessary condition for F to be EA-equivalent to a $\mathcal{QLB}$ function is that for every nonzero $v\in\mathbb{F}_2^m$, the set of linear structures of F_v is non-trivial. Can we find necessary and sufficient conditions on the function F such that there exists a linear map L satisfying that $F+L$ is quadratic-like balanced? This would provide necessary and sufficient conditions for F to be EA-equivalent to a $\mathcal{QLB}$ function.*
Note that such conditions are not known for general balancedness (even for bijectivity).

The above proposition can be generalized as follows.

Proposition 4. *Consider $F,G:\mathbb{F}_2^n\to\mathbb{F}_2^m$. Denoting $A_{v,F}=\{a\in\mathbb{F}_2^n;D_aF_v\equiv 1\}$ and $B_{v,F}=\{a\in\mathbb{F}_2^n;D_aF_v\equiv 0\}$, and $A_{v,G}$, $B_{v,G}$ similarly, we have that if, for every nonzero $v\in\mathbb{F}_2^m$, $(A_{v,F}\cap B_{v,G})\cup(B_{v,F}\cap A_{v,G})\neq\emptyset$, then $F+G$ is $\mathcal{QLB}$.*

3.2 The reversed quadratic-like property

An interesting question is to determine, for each quadratic-like balanced function F, whether for every nonzero a, there is v such that $D_aF_v\equiv 1$ (which is a kind of reverse of Definition 1; hence the name chosen below).

Definition 2. *We say that an (n,m)-function satisfies the* reversed quadratic-like property *(shortly, $\mathcal{RQL}$ property) if for every nonzero $a\in\mathbb{F}_2^n$, there exists $v\in\mathbb{F}_2^m$ such that D_aF_v is constantly 1.*

Note that the reversed quadratic-like property is also invariant under affine equivalence. Moreover, in the same way as quadratic-like balanced (n,m)-functions cannot exist when $m>n$, we have:

Proposition 5. *Every vectorial function satisfying the $\mathcal{RQ}\ell$ property is injective. In particular, (n,m)-functions with $m < n$ do not satisfy the $\mathcal{RQ}\ell$ property.*

Proof. Consider a non-injective (n,m)-function F. There exist $z_1, z_2 \in \mathbb{F}_2^n$ distinct such that $F(z_1) = F(z_2)$. Set then $a = z_1 + z_2 \neq 0_n$. No vector $v \in \mathbb{F}_2^m$ can exist such that $v \cdot D_a F \equiv 1$, since $D_a F(z_1) = F(z_1) + F(z_2) = 0_m$. Therefore F does not satisfy the $\mathcal{RQ}\ell$ property. □

Corollary 1. *Consider $F : \mathbb{F}_2^n \to \mathbb{F}_2^n$ satisfying the $\mathcal{RQ}\ell$ property, then F is a permutation.*

Remark 6. *Functions satisfying the $\mathcal{RQ}\ell$ property exist for every $m \geq n$, since we shall see that (n,n)-permutations satisfying the property exist for every n, and since, given an (n,m)-function F satisfying the $\mathcal{RQ}\ell$ property, we can construct an $(n,m+1)$-function $F' = [F, f]$ by concatenating F with any $(n,1)$-function f; function F' satisfies then automatically the $\mathcal{RQ}\ell$ property, since we can take $v' = (v, 0)$.*
The reversed quadratic-like property does not then imply balancedness in general, since for $m > n$, no balanced function exists.

Remark 7. *Not all injective functions satisfy the $\mathcal{RQ}\ell$ property. Indeed, for $m \geq n$, let F be any (n,n)-permutation that does not have the $\mathcal{RQ}\ell$ property (we shall see examples of such functions below, such as non-quadratic power permutations). Up to applying an affine transformation to the input variables, we can assume that for $a = e_1$, no v in $\mathbb{F}_2^n$ is such that $v \cdot D_a F \equiv 1$. Let G be any $(n-1, m-n)$-function, then the injective (n,m)-function $H = [F(x_1, \ldots, x_n), G(x_2, \ldots, x_n)]$ is such that for $a = e_1$, no w in $\mathbb{F}_2^m$ is s.t. $w \cdot D_a H \equiv 1$. Hence H is not $\mathcal{RQ}\ell$.*

Proposition 6. *Consider $F : \mathbb{F}_2^n \to \mathbb{F}_2^n$ a quadratic-like permutation. If F admits a `cls` map which is a permutation, then F satisfies the $\mathcal{RQ}\ell$ property. More generally, in the case of a $\mathcal{Q}\ell\mathcal{P}$, the reversed property corresponds to the fact that every nonzero a in $\mathbb{F}_2^n$ is in the image set of some `cls` map, so there exists a `cls` map ϕ and a nonzero $v \in \mathbb{F}_2^n$ such that $\phi(v) = a$.*

Proof. Consider $\phi : \mathbb{F}_2^n \to \mathbb{F}_2^n$ the permutation `cls` of F, and we denote by ϕ^{-1} its inverse. Then, for every nonzero $v \in \mathbb{F}_2^n$, we have $D_{\phi(v)} F_v = 1$, implying that for every nonzero $a \in \mathbb{F}_2^n$, we have $D_a F_{\phi^{-1}(a)} = 1$. From this it follows the $\mathcal{RQ}\ell$ property of F. A similar proof holds for the second part of the proposition. □

Remark 8. *If any derivative $D_a F$ of an injective (n,m)-function F has for image set an affine space, then since for any $a \neq 0_n$ this affine space does not include 0_m, it is included in the complement of a linear hyperplane and F satisfies then the reversed quadratic-like property.*

Remark 8 tells us that the reversed property can be seen as a generalization of the crookedness property, this will be clear in the dedicated pages, see Subsection 4.2. Recall a generalization of the crookedness property introduced in [7]: an

(n,n)-function F is said to be *weakly crooked of codimension* d, for some $d \geq 1$, if for any nonzero $a \in \mathbb{F}_2^n$, $Im(D_aF)$ is included in an affine subspace of codimension d. Hence, being weakly crooked of codimension 1 is equivalent to the fact that every nonzero vector a is a linear structure of some component. Therefore, all permutations satisfying the $\mathcal{RQ}\ell$ property are weakly crooked of codimension 1. Notice that, in the same way, we can state the $\mathcal{Q}\ell\mathcal{P}$ property as follows: for any affine subspace of codimension 1 there exists $a \in \mathbb{F}_2^n$ such that $Im(D_aF)$ is included in it.

Moreover, the hypothesis assumed in Remark 8 is in particular true for strongly plateaued functions (see [10, Proposition 107]). Notice also that the remark can be made more general: we do not need $Im(D_aF)$ to be an affine space for every a, we only need that the smallest affine space containing it (whose elements are the sums of odd numbers of elements of $Im(D_aF)$) does not contain 0_m.

We were not able to find examples of quadratic-like permutations not satisfying the reversed quadratic-like property. We leave then the following open question.

Question 2. *(a) For F a quadratic-like permutation, does F always satisfy the reversed quadratic-like property?*
(b) For F a permutation satisfying the reversed quadratic-like property, is F always a quadratic-like permutation?

The answer to these questions when we restrict ourselves to quadratic functions is yes:

Proposition 7. *Consider $F : \mathbb{F}_2^n \to \mathbb{F}_2^n$ of degree 2. Then F is a permutation (i.e. $\mathcal{Q}\ell\mathcal{P}$) if and only if it satisfies the $\mathcal{RQ}\ell$ property.*

This is a simple consequence of Remark 8 (since any derivative of a quadratic function being affine, its image set is an affine space) and of Corollary 1. This was already observed in [7].

More generally, we have according to Proposition 5 and Remark 8 that if F is any quadratic (n,m)-function, it is injective if and only if it satisfies the $\mathcal{RQ}\ell$ property.

3.3 Relation with cubic-like bent functions through the Maiorana-McFarland construction

We recall a notion introduced in [12]: an n-variable Boolean function f is called *cubic-like bent* if for any nonzero $a \in \mathbb{F}_2^n$ there exists $b \in \mathbb{F}_2^n$ such that $D_aD_bf \equiv 1$. There is a strong connection between the so-called Maiorana-McFarland cubic-like bent functions and $\mathcal{Q}\ell\mathcal{P}$ satisfying the $\mathcal{RQ}\ell$ property:

Proposition 8. *Consider a Maiorana-McFarland bent function of the form:*

$$(x,y) \in \mathbb{F}_2^n \times \mathbb{F}_2^n \to f(x,y) = x \cdot \pi(y) \in \mathbb{F}_2, \tag{1}$$

where $x, y \in \mathbb{F}_2^n$ and $\pi : \mathbb{F}_2^n \to \mathbb{F}_2^n$ is a permutation. Then f is cubic-like bent if and only if π is a quadratic-like permutation satisfying the reversed quadratic-like property. In such a case, any function

$$(x, y) \in \mathbb{F}_2^n \times \mathbb{F}_2^n \to f(x, y) = x \cdot \pi(y) + g(y) \in \mathbb{F}_2, \tag{2}$$

with $x, y \in \mathbb{F}_2^n$, $\pi : \mathbb{F}_2^n \to \mathbb{F}_2^n$ a permutation and $g : \mathbb{F}_2^n \to \mathbb{F}_2$ is cubic-like bent. Conversely, if such a function (2) is cubic-like bent for some g then π is a quadratic-like permutation.

Proof. The first assertion is equivalent to Proposition 9 in the work on cubic-like bent maps [12]. The rest is Proposition 14 in this same reference. □

Remark 9. *From the analysis presented in [12], we have that over $\mathbb{F}_2^4$ all the quadratic-like permutations satisfy also the reversed quadratic-like property.*

4 Some classic subclasses

We consider some known classes of balanced functions, and we study whether they are quadratic-like. The results obtained will illustrate the interest of the notion of quadratic-like balancedness. Indeed, we have three classic classes (Feistel permutations, crooked permutations and strongly plateaued balanced functions) which all three happen to be included in the class of quadratic-like balanced functions, providing some link between these three classes which were apparently completely unrelated. We conclude this section observing a non-existence result: there do not exist quadratic-like power permutations of degree larger than 2.

4.1 Feistel permutations and generalizations

Proposition 9. *(i) Every Feistel permutation*

$$(x, y) \in (\mathbb{F}_2^{n/2}) \times (\mathbb{F}_2^{n/2}) \mapsto F(x, y) = (y, x + \phi(y)),$$

where n is even and $\phi : \mathbb{F}_2^{n/2} \to \mathbb{F}_2^{n/2}$ is any function, is a $\mathcal{QLP}$ admitting as `cls` *map any function of the form $(v_1, v_2) \mapsto ((1 + \delta_0(v_2))a_1, \delta_0(v_2)a_2)$, where a_1 is any element satisfying $v_2 \cdot a_1 = 1$ if $v_2 \neq 0_{n/2}$ and a_2 is any element satisfying $v_1 \cdot a_2 = 1$ if $v_1 \neq 0_{n/2}$, and where δ_0 is the Dirac (or Kronecker) symbol (whose value equals 1 at $0_{n/2}$ and 0 everywhere else).*
(ii) More generally, all the (bijective) functions of the form $(x, y) \in \mathbb{F}_2^r \times \mathbb{F}_2^{n-r} \mapsto F(x, y) = (y, x + \phi(y))$, where n is any positive integer, r is some integer, $0 \leq r \leq n$ and $\phi : \mathbb{F}_2^{n-r} \to \mathbb{F}_2^r$ is any function, are $\mathcal{QLP}$ with their `cls` *maps defined similarly.*
(iii) Still more generally, let G be any $\mathcal{QLB}$ $(n-r, m-r)$-function, the function

$$(x, y) \in \mathbb{F}_2^r \times \mathbb{F}_2^{n-r} \mapsto F(x, y) = (G(y), x + \phi(y)) \tag{3}$$

is a $\mathcal{QLB}$ (n, m)-function.

Proof. (i) (ii) The component functions of such a function are $F_v(x,y) = v_1 \cdot y + v_2 \cdot (x + \phi(y))$ with $v = (v_1, v_2) \neq (0_{n-r}, 0_r)$ and have derivative in the direction $a = (a_1, a_2)$ equal to $D_a(F_v)(x,y) = v_1 \cdot a_2 + v_2 \cdot a_1 + v_2 \cdot D_{a_2}\phi(y)$. If $v_2 \neq 0_r$, then $a = (a_1, 0_{n-r})$ such that $v_2 \cdot a_1 = 1$ satisfies $D_a(v \cdot F) \equiv 1$, and if $v_2 = 0_r$ then $v_1 \neq 0_{n-r}$ and we can take $a = (0_r, a_2)$ such that $v_1 \cdot a_2 = 1$, to get $D_a(F_v) \equiv 1$. Hence, whatever the choice of ϕ, function F is a quadratic-like permutation.
(iii) This extends to the most general case by changing $v_1 \cdot a_2$ into $D_{a_2}G_{v_1}(y)$ in the expression of $D_a(F_v)(x,y)$, and by changing the condition $v_1 \cdot a_2 = 1$ into $D_{a_2}G_{v_1} \equiv 1$ when $v_2 = 0_r$ and $v_1 \neq 0_{m-r}$. □

Note that if ϕ is non-quadratic, then F is non-quadratic.

We still call *Feistel* the generalized form of permutations given in Proposition 9 (ii). We shall not call Feistel the functions in Proposition 9 (iii), because (iii) is a secondary construction of $\mathcal{Q}\ell\mathcal{B}$ functions (it uses such functions to build new ones), not a primary construction, and the set of the functions it allows to build is not clear. But for brevity, we shall sometimes call them *generalized Feistel*.

As a further illustration of the connection between the quadratic-like property and the $\mathcal{RQ}\ell$ property, we have the following result for Feistel permutations.

Proposition 10. *Any Feistel permutation (as in Proposition 9, Items (i) and (ii)) satisfies the $\mathcal{RQ}\ell$ property. Hence, any Feistel permutation is weakly crooked of codimension 1. Moreover, if we consider a more general permutation F as in Proposition 9, Item (iii) (see Equation (3)), then the $\mathcal{RQ}\ell$ property is inherited from G.*

Proof. Consider a Feistel permutation $F(x,y) = (y, x + \phi(y))$, then we have seen that the derivative in direction $a = (a_1, a_2) \in \mathbb{F}_2^r \times \mathbb{F}_2^{n-r}$ of the component F_v, where $v = (v_1, v_2) \in \mathbb{F}_2^{n-r} \times \mathbb{F}_2^r$, has the form $D_a(F_v)(x,y) = v_1 \cdot a_2 + v_2 \cdot a_1 + v_2 \cdot D_{a_2}\phi(y)$. The case $a = (a_1, 0_{n-r})$ does not pose any problem, and if $a_2 \neq 0_{n-r}$, we can take $v_2 = 0_r$ and v_1 such that $v_1 \cdot a_2 = 1$. This proves the reversed property for Feistel permutations.
Consider now the more general form as in Equation (3), $F(x,y) = (G(y), x + \phi(y))$, with $G : \mathbb{F}_2^{n-r} \to \mathbb{F}_2^{n-r}$ a quadratic-like permutation and assume that G satisfies the reversed property. We have then $D_a(F_v)(x,y) = v_1 \cdot D_{a_2}G(y) + v_2 \cdot a_1 + v_2 \cdot D_{a_2}\phi(y)$. Similarly as before, the case $a = (a_1, 0_{n-r})$ does not pose any problem, whereas if $a_2 \neq 0_{n-r}$ by taking $v = (v_1, 0_r)$ such that $v_1 \cdot D_{a_2}G(y) \equiv 1$, we have $D_a(F_v)(x,y) \equiv 1$. □

Remark 10. *Propositions 9 and 10 show that both $\mathcal{Q}\ell\mathcal{B}$ and $\mathcal{RQ}\ell$ properties of F are inherited from G.*
The converse in the case of $\mathcal{Q}\ell\mathcal{B}$ is true for every ϕ as well, since taking $v_2 = 0_r$ reduces the condition $D_{a_2}G_{v_1}(y) + v_2 \cdot a_1 + v_2 \cdot D_{a_2}\phi(y) \equiv 1$ to $D_{a_2}G_{v_1}(y) \equiv 1$. In the case of $\mathcal{RQ}\ell$, the converse may or may not be true[4] *and we leave it as an*

[4]If there exist two $(n-r, r)$-functions ϕ and G such that $G + \phi$ has the $\mathcal{RQ}\ell$ property (which is possible if we take $m = 2r \geq n$ since $r \geq n - r$) but G does not have it, and for

Open problem*: find examples of functions G that do not satisfy the $\mathcal{RQ}\ell$ and such that Function* (3) *satisfies it (or prove that such functions do not exist). Note that if we find such examples, then this will also provide examples of functions either satisfying the reversed property but not the quadratic-like property or the opposite. Indeed, if F satisfies $\mathcal{RQ}\ell$ property but G does not, then either:*
1) F does not satisfy the $\mathcal{Q}\ell\mathcal{B}$ property
or
2) F is $\mathcal{Q}\ell\mathcal{B}$, which implies that necessarily G is $\mathcal{Q}\ell\mathcal{B}$.
In the first case, F is $\mathcal{RQ}\ell$ but not $\mathcal{Q}\ell\mathcal{B}$, in the second case, G is not $\mathcal{RQ}\ell$ but it is $\mathcal{Q}\ell\mathcal{B}$.
Note also that if $F(x,y) = (G(y), x+\phi(y))$ satisfies the $\mathcal{RQ}\ell$ property, then G is injective, since if there exists $a_2 \neq 0_{n-r}$ and z such that $D_{a_2}G(z) = 0_{m-r}$, then denoting $a_1 = D_{a_2}\phi(z)$ and using that F has the $\mathcal{RQ}\ell$ property, we can see that there exist v_1, v_2 such that $v_1 \cdot 0_{m-r} + v_2 \cdot (a_1 + D_{a_2}\phi(z)) = 1$, a contradiction. This eliminates a possibility of proving negatively to the open problem above.

All the $\mathcal{Q}\ell\mathcal{B}$ functions we shall construct satisfy the $\mathcal{RQ}\ell$ property.

When we shall give constructions of quadratic-like permutations, we shall need a way to determine whether some of the constructed functions are outside the class of those permutations that are affine equivalent to Feistel permutations. The following result provides such a way, by characterizing those permutations which are affine equivalent to the generalized Feistel permutations described in Proposition 9 (*iii*), showing in particular that those such that $r = 1$ generate the whole class of functions (3), up to affine equivalence:

Proposition 11. *A quadratic-like balanced map $F : \mathbb{F}_2^n \to \mathbb{F}_2^m$ is affine equivalent to a map as in Equation* (3) *if and only if there exists some nonzero direction $a \in \mathbb{F}_2^n$ such that D_aF is constant and nonzero. It is then affine equivalent to a balanced (n,m)-function described in this same Proposition 9 (*iii*) with $r = 1$.*

Proof. First, recall that the property of having a nonzero direction admitting a constant derivative is invariant under affine equivalence.
If F is as in Equation (3), then $D_{(a_1,0_{n-r})}F(x,y)$ equals $(0_{m-r}, a_1)$ and is then constant.
Conversely, if $F : \mathbb{F}_2^n \to \mathbb{F}_2^m$ is quadratic-like balanced and there exists $a \in \mathbb{F}_2^n$ such that D_aF is constant and nonzero, then up to affine equivalence, we can assume $a = e_n$. For $b = D_aF \in \mathbb{F}_2^m$, consider a linear bijection L of $\mathbb{F}_2^m$ such that $L(b) = e_m$. By setting $G = L \circ F$, we have $D_aG(x) = L(F(x+a)+F(x)) = L(b) = e_m$. So, $D_{e_n}G(x) = e_m$, hence G has the following form

$$G(x) = \begin{bmatrix} G'(x_1, \ldots, x_{n-1}) \\ x_n + g(x_1, \ldots, x_{n-1}) \end{bmatrix},$$

every nonzero a_2 and every v_2, there exists v_1 such that $D_{a_2}G_{v_1}(y) + v_2 \cdot D_{a_2}\phi(y) \equiv 0$. If $a_1 = 0_r$ and $a_2 \neq 0_{n-r}$, then we take $v_1 = v_2$ such that $v_2 \cdot D_{a_2}(G+\phi) \equiv 1$; and if $a_1 \neq 0_r$, then we take v_2 such that $v_2 \cdot a_1 = 1$ and v_1 such that $D_{a_2}G_{v_1}(y) + v_2 \cdot D_{a_2}\phi(y) \equiv 0$. Then, F has the $\mathcal{RQ}\ell$ property but G does not. It is not clear however whether such functions G, ϕ can exist.

with $G' : \mathbb{F}_2^{n-1} \to \mathbb{F}_2^{m-1}$ and $g : \mathbb{F}_2^{n-1} \to \mathbb{F}_2$. Clearly, since G is $\mathcal{Q}\ell\mathcal{B}$, G' is also $\mathcal{Q}\ell\mathcal{B}$. Hence, G is as in Equation (3), with $r = 1$. □

Example 2. *Consider the following 4-bit permutations*

$$F_1(x) = \begin{bmatrix} x_1 + x_2x_3x_4 \\ x_1x_3x_4 + x_1 + x_2 \\ x_3 \\ x_4 \end{bmatrix}, \qquad F_2(x) = \begin{bmatrix} x_1 + x_2x_4 + x_2 + x_3 \\ x_1 + x_2 + x_3x_4 \\ x_1x_4 + x_1 + x_3 \\ x_4 \end{bmatrix}.$$

Then F_1 is an example of a $\mathcal{Q}\ell\mathcal{P}$ neither quadratic nor affine equivalent to a Feistel permutation; instead, F_2 is an example of a quadratic permutation not affine equivalent to a Feistel permutation. Notice that, up to affine equivalence, F_1 and F_2 are the only such examples (in dimension 4). This result is due to the complete classification (up to affine equivalence) of 4-bit permutations provided by De Canniere in [13]: among the list of 302 (inequivalent) permutations only 12 are quadratic-like, of which only 2 are not equivalent to Feistel, namely F_1 and F_2.

4.1.1 Composition of quadratic-like balanced maps

We know that for balanced functions, being quadratic, respectively, having the Feistel structure, is not preserved by composition. Let us check that the same happens with quadratic-like balancedness. Let us for instance consider the composition of the same Feistel permutation $(x, y) \mapsto (y, x+\phi(y))$ twice. We obtain the function $F(x, y) = (x+\phi(y), y+\phi(x+\phi(y)))$. Taking ϕ affine would not lead to a significantly different function. Let us then take ϕ of algebraic degree 2, and to make it simple, let us take the simplest possible one, the $(2, 2)$-function $\phi : (z_1, z_2) \in \mathbb{F}_2^2 \mapsto (z_1z_2, z_1) \in \mathbb{F}_2^2$. Then, for $x = (x_1, x_2)$ and $y = (y_1, y_2)$, we have $F(x, y) = \big(x_1 + y_1y_2,\ x_2 + y_1,\ y_1 + (x_1 + y_1y_2)(x_2 + y_1),\ y_2 + x_1 + y_1y_2\big)$, that is:

$$F(x, y) = \big(x_1 + y_1y_2,\ x_2 + y_1,\ y_1 + x_1x_2 + x_1y_1 + x_2y_1y_2 + y_1y_2,\ y_2 + x_1 + y_1y_2\big)$$

and, for $v = (v_1, \ldots, v_4)$, while for $v_3 = 0$ we can always find (a, b) such that $v \cdot D_{(a,b)}F(x, y) \equiv 1$, for $v_3 = 1$, this is never possible.

4.2 Crooked permutations

Recall that Reference [1] has introduced the notion of *crooked* (n, n)*-function* (sometimes called strict crooked function), such that, for every nonzero $a \in \mathbb{F}_2^n$, the image set of D_aF equals the complement of a linear hyperplane of $\mathbb{F}_2^n$, say the complement of $\{0_n, \pi_F(a)\}^\perp$ where π_F (sometimes called the *orthoderivative* of F) is some function from $\mathbb{F}_2^n \setminus \{0_n\}$ to itself. Such crooked functions are almost bent permutations. The notion has been later generalized (see e.g. [22, 10]). We call crooked the (n, n)-functions such that, for every nonzero $a \in \mathbb{F}_2^n$, the image set of D_aF equals an affine hyperplane of $\mathbb{F}_2^n$ (and hence equals

either $\{0_n, \pi_F(a)\}^\perp$ or its complement). Such APN functions can of course be permutations only if they are strict crooked.
Note that the existence of non-quadratic crooked functions is an open problem.

Proposition 12. *Let F be a crooked (n,n)-function in the strict sense of [1]. Then F is a quadratic-like permutation whose (unique) `cls` map equals the compositional inverse of the orthoderivative. Hence, F satisfies the reversed quadratic-like property.*

Proof. If F is crooked, we know from [1] that both F and the orthoderivative are permutations, and we have that $v = \pi_F(a)$ is by hypothesis such that $D_aF_v \equiv 1$, which makes that π_F^{-1} is a `cls` map for F. Its uniqueness as a component-to-linear-structure map is clear, since for any value $a \neq \pi_F^{-1}(v)$, we have that D_aF_v is in fact balanced. Notice that the fact that F satisfies the reverse quadratic-like property can be deduced also from [14, Theorem 8]. □

Notice that the $\mathcal{RQ}\ell$ property is a natural generalization of crookedness (still more than $\mathcal{Q}\ell\mathcal{P}$) since (strict) crooked means that any derivative in a nonzero direction has image set the complement of a linear hyperplane and $\mathcal{RQ}\ell$ means that any derivative in a nonzero direction has image set included in the complement of a linear hyperplane. As already mentioned, this generalization was already presented in [7] as *weakly crooked of codimension 1*.

The question of the converse of Proposition 12 arises: if an (n,n)-function is APN and is a quadratic-like permutation, is it necessarily crooked?

Proposition 13. *If F is an APN quadratic-like permutation, then it satisfies the reversed quadratic-like property and it is crooked. Moreover, there exists one and only one `cls` map for F, which is itself a permutation.*

Proof. We know that F being APN, the image set of D_aF has size 2^{n-1} for every nonzero a. Showing that it is crooked is then equivalent to showing that any nonzero a is such that $D_aF_v \equiv 1$ for some v (indeed, this is equivalent to saying that the image set of D_aF is included in the complement of a linear hyperplane $\{0_n, v\}^\perp$ and then that it is equal to it), that is, F has the $\mathcal{RQ}\ell$ property.
To proceed with the proof, first recall that an APN permutation cannot have a derivative in a nonzero direction having a zero component (this result was used in [5] to study APN permutations in even dimension). Let us recall why: if there exist nonzero $v \in \mathbb{F}_2^n, a \in \mathbb{F}_2^n$ such that $v \cdot D_aF \equiv 0$, then since F being APN, we have $|Im(D_aF)| = 2^{n-1}$, the image set of D_aF equals the whole linear hyperplane of equation $v \cdot x = 0$, and so there must exist an input $x \in \mathbb{F}_2^n$ such that $D_aF(x) = 0_n$, which contradicts the fact that F is a permutation.
Assume that there exists $\alpha \in \mathbb{F}_2^n$ such that, for every nonzero v, the component $v \cdot D_\alpha F(x)$ does not equal constant function 1. This implies that no `cls` map ϕ can be injective (since it is not surjective). Hence, there must exist distinct nonzero directions v_1, v_2 such that $\phi(v_1) = \phi(v_2) = b$, for some nonzero $b \in \mathbb{F}_2^n$. So it holds $v_1 \cdot D_bF = v_2 \cdot D_bF \equiv 1$, implying $(v_1 + v_2) \cdot D_bF \equiv 0$, contradicting the fact that F is an APN permutation.

This implies also that for any nonzero $v \in \mathbb{F}_2^n$, the only 0-linear structure of F_v is the zero element. The set of 1-linear structures of F_v being non-empty, it is an affine space whose direction is the vector space of 0-linear structures (see Section 2), which is here trivial, so it contains only one element. This implies that there exists one and only one `cls` map, which is a permutation since the reversed quadratic-like property is satisfied. □

Corollary 2. *Given F an APN permutation, then F is quadratic-like if and only if F is crooked (in the strict sense of [1]).*

Remark 11. *Since crooked maps, in the strict sense of [1], exist only over spaces of odd dimension, this implies that quadratic-like APN permutations defined over $\mathbb{F}_2^n$ do not exist if n is even.*
Notice that [5, Theorem 3.3] proved that an APN permutation in even dimension does not have any partially-bent component, extending a result by Nyberg [25] showing that it cannot have all partially-bent components.
Here we showed that an APN permutation in even dimension does not have all components quadratic-like balanced. However, we cannot extend this result as it was done for the case of partially-bent components. Indeed, the APN permutation in dimension 6 given in Ref. [3] is clearly not quadratic-like, but it has seven components that have 1-linear structures (these are exactly the 7 components of algebraic degree 3, all the rest of the components having algebraic degree 4 and not admitting any 1-linear structure).

So determining whether non-quadratic quadratic-like APN permutations exist exactly corresponds to the open problem on crooked functions (in the strict sense). We do know that they do not exist in monomial and binomial form, see [2, 21].

4.3 Strongly plateaued balanced functions

Crooked functions are a particular case of so-called strongly plateaued functions [9, 10]. Recall that an (n, m)-function is strongly plateaued if and only if all its component functions are partially bent. F_v being partially bent means (see [8]) that there exists a vector subspace E_v of $\mathbb{F}_2^n$, whose dimension is even, and a vector subspace E'_v of $\mathbb{F}_2^n$ whose sum with E_v is direct and equals $\mathbb{F}_2^n$, and an affine Boolean function ℓ_v on E'_v such that the restriction of F_v to E_v is bent and, for every $x \in E_v$ and every $y \in E'_v$, we have $F_v(x + y) = F_v(x) + \ell_v(y)$. Since denoting by f_v the bent function equal to the restriction of F_v to E_v, we have $W_{F_v}(0_n) = W_{f_v}(0_n)W_{\ell_v}(0_n)$ and since $W_{f_v}(0_n) \neq 0$, we have that F_v is balanced if and only if ℓ_v is balanced and this is equivalent to the existence of b such that $D_b\ell_v \equiv 1$. Then $D_{(0,b)}F_v \equiv 1$. Therefore, we have the following result, which is also a direct consequence of Remark 8 and [10, Proposition 107], and generalizes Proposition 12.

Proposition 14. *All strongly plateaued balanced functions are quadratic-like. Moreover, strongly plateaued permutations satisfy the $\mathcal{RQ}\ell$ property, that is, they are weakly crooked of codimension 1.*

Remark 12. *Of course the question whether all plateaued balanced functions (possibly with a single amplitude) are quadratic-like can be raised and the answer is no because we have the example of Kasami APN permutations that are plateaued (with a single amplitude since they are AB) and not quadratic-like (since not crooked, and/or since non-quadratic power functions).*

4.4 Non-existence of non-quadratic power quadratic-like permutations

We consider now (n,n)-permutations which are monomials when described in the univariate representation (over $\mathbb{F}_{2^n}$), which are called power functions and have the form $F(x) = x^d$ where d is a positive integer such that $\gcd(2^n - 1, d) = 1$. First, we notice that the quadratic-like property simplifies in this case. Indeed, we have the following well-known equalities, for $a, v \in \mathbb{F}_{2^n}^*$:

$$\begin{aligned} D_a F_v(ax) =& tr_n(v(ax+a)^d + v(ax)^d) = tr_n(va^d(x+1)^d + va^d(x)^d) \\ =& D_1 F_{va^d}(x). \end{aligned} \tag{4}$$

Hence, F is a quadratic-like permutation if and only if there exists $\lambda \in \mathbb{F}_{2^n}$ such that $D_1 F_\lambda \equiv 1$. Indeed, this condition is necessary according to (4), and it is sufficient thanks to the fact that $a \mapsto a^d$ is a permutation. Moreover, the reversed quadratic-like property is equivalent to the quadratic-like property: if ϕ is a `cls` map, then denoting $\lambda = \phi(1)$, we have, again thanks to (4), that $\phi(v) = \left(\frac{\lambda}{v}\right)^{1/d}$ for every nonzero v, where $1/d$ is the inverse of d modulo $2^n - 1$. Hence ϕ is bijective. We summarize this in the following proposition.

Proposition 15. *Consider $F(x) = x^d$ a power permutation. Then the following properties are equivalent.*

1. *F is a quadratic-like permutation.*
2. *There exists $\lambda \in \mathbb{F}_{2^n}$ such that $D_1 F_\lambda(x) = tr_n(\lambda((x+1)^d + x^d))$ is constantly 1.*
3. *F satisfies the reversed quadratic-like property.*

The `cls` map is then bijective.

Using known results, we have the following proposition (which, of course, had not been originally stated in terms of quadratic-like balancedness):

Proposition 16 ([16, 22])**.** *The only power quadratic-like permutations are quadratic.*

Proof. From Theorem 5 in [16], which is based on Lemma 2 in [22], we know that Boolean functions $Tr_n(\lambda x^d)$ of degree greater than 2 cannot have linear structures. Therefore we have that if x^d is a quadratic-like permutation defined over $\mathbb{F}_{2^n}$, then necessarily it is quadratic. □

Notice that the above proposition can be also deduced from [7, Proposition 4.7], which states that the only power $\mathcal{RQ}\ell$ (weakly crooked of codimension 1) permutations are quadratic, and Proposition 15, which tells us that the reversed property is equivalent to the $\mathcal{Q}\ell\mathcal{P}$ property for power maps.

5 Constructions

We are interested in constructing $\mathcal{Q}\ell\mathcal{B}$ functions of degree greater than 2 and being not Feistel nor strongly plateaued. For the constructions we present in this section, we also study whether the $\mathcal{RQ}\ell$ property is satisfied, clearly for the case $m = n$. Hence we also provide constructions of permutations satisfying the $\mathcal{RQ}\ell$ property, so being weakly crooked of codimension 1. Notice that in [7] no construction of such functions is given.

Firs, notice that Proposition 9 (*iii*) provides already an iterative construction method of $\mathcal{Q}\ell\mathcal{B}$ maps. For example, the permutation F_1 displayed in Example 1 can be obtained this way.

We continue with two trivial constructions, see the following two remarks, obtained by either shortening the output space, or enlarging the input space of a $\mathcal{Q}\ell\mathcal{B}$ map.

Remark 13. *Notice that from a quadratic-like balanced function $F : \mathbb{F}_2^n \to \mathbb{F}_2^m$ we can construct many quadratic-like balanced maps $F' : \mathbb{F}_2^n \to \mathbb{F}_2^t$ with $t < m$, since the notion is stable under the erasure of some coordinates of F.*

Remark 14. *Contrary to Boolean functions, vectorial functions do not allow many possibilities of providing secondary constructions. A classic secondary construction (much used in block ciphers) is concatenation: given r functions $F_i : \mathbb{F}_2^{n_i} \to \mathbb{F}_2^{m_i}$; $i = 1, \ldots, r$, we define $F(x_1, \ldots, x_r) = (F_1(x_1), \ldots, F_r(x_r))$, where $x_i \in \mathbb{F}_2^{n_i}$, which is a $(\sum_{i=1}^r n_i, \sum_{i=1}^r m_i)$-function. The component functions $v \cdot F$, $v \neq 0_{\sum_{i=1}^r m_i}$, of such F equal the direct sums of the functions $v_i \cdot F_i$. Since the direct sum of functions is balanced when at least one of these functions is balanced, we have that if all the F_i's are balanced, then F is balanced.*
This provides a secondary construction of $\mathcal{Q}\ell\mathcal{B}$ functions: if each F_i is $\mathcal{Q}\ell\mathcal{B}$, then F is $\mathcal{Q}\ell\mathcal{B}$, since $v \cdot D_a F(x) = \sum_{i=1}^r v_i \cdot D_{a_i} F_i(x_i)$ and to have $v \cdot D_a F(x) \equiv 1$, for $v \neq 0_{\sum_{i=1}^r m_i}$, we can choose i such that $v_i \neq 0_{m_i}$, then a_i such that $v_i \cdot D_{a_i} F_i \equiv 1$ and take $a = (0_{n_1}, \ldots, 0_{n_{i-1}}, a_i, 0_{n_{i+1}}, \ldots, 0_{n_r})$.
If all the F_i's have the $\mathcal{RQ}\ell$ property, then F has the $\mathcal{RQ}\ell$ property: given $a \neq 0_{\sum_{i=1}^r n_i}$, to have $v \cdot D_a F(x) \equiv 1$, we can choose i such that $a_i \neq 0_{n_i}$, then v_i such that $v_i \cdot D_{a_i} F_i \equiv 1$ and take $v = (0_{n_1}, \ldots, 0_{n_{i-1}}, v_i, 0_{n_{i+1}}, \ldots, 0_{n_r})$.
Now, the concatenation of two functions can be slightly complexified into a secondary construction which still preserves $\mathcal{Q}\ell\mathcal{B}$ functions:
Let F be any $\mathcal{Q}\ell\mathcal{B}$ (n, m)-function, G any $\mathcal{Q}\ell\mathcal{B}$ (r, s)-function and H any (n, s)-function, then $\mathcal{F} : (x, y) \in \mathbb{F}_2^n \times \mathbb{F}_2^r \mapsto (F(x), G(y) + H(x))$ is a $\mathcal{Q}\ell\mathcal{B}$ $(n+r, m+s)$-function. Indeed, for every $a \in \mathbb{F}_2^n$, $b \in \mathbb{F}_2^r$, $v \in \mathbb{F}_2^m$ and $w \in \mathbb{F}_2^s$, we have $(v, w) \cdot D_{(a,b)}\mathcal{F}(x, y) = v \cdot D_a F(x) + w \cdot D_b G(y) + w \cdot D_a H(x)$. Consider $(v, w) \neq (0_m, 0_s)$. If $w = 0_s$ then $v \neq 0_m$ and we can take a such that

$v \cdot D_a F \equiv 1$; and if $w \neq 0_s$ we can take $a = 0_n$ and b such that $w \cdot D_b G \equiv 1$. If F and G have the $\mathcal{RQ}\ell$ property, then $\mathcal{F}$ has the $\mathcal{RQ}\ell$ property: we assume $(a, b) \neq (0_n, 0_r)$; if $a = 0_n$ then $b \neq 0_r$ and we can take w such that $w \cdot D_b G \equiv 1$; and if $a \neq 0_n$ we can take $w = 0_s$ and v such that $v \cdot D_a F \equiv 1$.
Similarly, let F be any $\mathcal{Q}\ell\mathcal{B}$ (n, m)-function (resp, any (n, m)-function satisfying the $\mathcal{RQ}\ell$ property), G any $\mathcal{Q}\ell\mathcal{B}$ (r, s)-function (resp, any (r, s)-function satisfying the $\mathcal{RQ}\ell$ property) and K any (r, m)-function, then $\mathcal{F} : (x, y) \in \mathbb{F}_2^n \times \mathbb{F}_2^r \mapsto (F(x) + K(y), G(y))$ is a $\mathcal{Q}\ell\mathcal{B}$ $(n + r, m + s)$-function (resp, satisfies the $\mathcal{RQ}\ell$ property). Note that this construction generalizes that of (3) (after swapping the two parts of the output), since the identity is a $\mathcal{Q}\ell\mathcal{P}$.
These two latter secondary constructions can be iterated into a generalization of the concatenation which still preserves $\mathcal{Q}\ell\mathcal{B}$ and the $\mathcal{RQ}\ell$ property.

We present another method providing quadratic-like balanced maps. In the two constructions below (Propositions 17 and 18), we shall use vectorial functions ψ, ϕ from $\mathbb{F}_2^{n-m}$ to $\mathbb{F}_2^m$. But to define ψ, ϕ, we shall use an operation of multiplication between the elements of $\mathbb{F}_2^m$, for which 0_m is the only absorbent element. Hence, we shall need to work in the field $\mathbb{F}_{2^m}$. We consider then ψ, ϕ as being from the vector space $\mathbb{F}_2^{n-m}$ to the field $\mathbb{F}_{2^m}$.

Proposition 17. *Let $1 \leq m \leq n$. Consider any map $\psi : \mathbb{F}_2^{n-m} \to \mathbb{F}_{2^m}$ and set[5] $\phi(y) = \psi(y) + (\psi(y))^2 + c$, where $c \in \mathbb{F}_{2^m}$ is such that $tr_m(c) = 1$. Then the (n, m)-function $(x, y) \in \mathbb{F}_{2^m} \times \mathbb{F}_2^{n-m} \mapsto x\phi(y)$ is quadratic-like balanced.*

Proof. Take any nonzero $v \in \mathbb{F}_{2^m}$. The derivative at $a = (a_1, a_2) \in \mathbb{F}_{2^m} \times \mathbb{F}_2^{n-m}$ of $tr_m(vx\phi(y))$ equals $tr_m(vxD_{a_2}\phi(y) + va_1\phi(y + a_2))$. If we take $a_2 = 0_{n-m}$ to cancel $vxD_{a_2}\phi(y)$, we get then $tr_m(va_1\phi(y))$. Now, with $a_1 = v^{-1}$ we get $tr_m(\phi(y)) = tr_m(\psi(y) + (\psi(y))^2 + c) = tr_m(c) = 1$. □

Remark 15. *There is some similarity between the function $(x, y) \mapsto x + \phi(y)$ involved in Feistel permutations (that is balanced and moreover $\mathcal{Q}\ell\mathcal{B}$) and the function $(x, y) \mapsto x\phi(y)$ in Proposition 17. But in fact they are quite different, not only because addition and multiplication in $\mathbb{F}_{2^m}$ do not behave similarly nor have the same complexity, but also since there is no constraint on ϕ such that $x+\phi(y)$ is (quadratic-like) balanced, while for $x\phi(y)$, we need that $\phi(y)$ does not vanish for having a balanced function, and still more for having a $\mathcal{Q}\ell\mathcal{B}$ function.*

The function in Proposition 17 is an (n, m)-function with $m < n$ (unless it is the identity map multiplied by a constant), but we can deduce from this proposition a construction of quadratic-like permutations as follows.

Proposition 18. *Let $1 \leq m \leq n$. Consider any map $\psi : \mathbb{F}_2^{n-m} \to \mathbb{F}_{2^m}$ and set $\phi(y) = \psi(y) + (\psi(y))^2 + c$, where $c \in \mathbb{F}_{2^m}$ is such that $tr_m(c) = 1$. Moreover, consider a function φ from $\mathbb{F}_2^{n-m}$ to $\mathbb{F}_2^{n-m}$.*
Then the (n, n)-function $F : (x, y) \in \mathbb{F}_{2^m} \times \mathbb{F}_2^{n-m} \mapsto (x\phi(y), \varphi(y))$ is a $\mathcal{Q}\ell\mathcal{P}$ if and only if φ is a $\mathcal{Q}\ell\mathcal{P}$. Moreover, F satisfies the $\mathcal{RQ}\ell$ property if and only if φ satisfies the $\mathcal{RQ}\ell$ property.

[5] The idea of taking ϕ in such a form, for having $tr_m(\phi(y)) = 1$, is classic (see e.g. [14, Lemma 1]).

Proof. Consider a nonzero $v = (v_1, v_2) \in \mathbb{F}_{2^m} \times \mathbb{F}_2^{n-m}$. For a direction $a = (a_1, a_2) \in \mathbb{F}_{2^m} \times \mathbb{F}_2^{n-m}$, the derivative of $F_v(x, y) = tr_m(v_1 x\phi(y)) + v_2 \cdot \varphi(y)$ equals $tr_m(v_1(xD_{a_2}\phi(y) + a_1\phi(y + a_2)) + v_2 \cdot D_{a_2}\varphi(y)$. If $v_1 \neq 0$, we take $a_2 = 0_{n-m}$ and the derivative equals $tr_m(v_1 a_1 \phi(y))$ and taking $a_1 = v_1^{-1}$ as in the proof of Proposition 17, we get $tr_m(\phi(y)) = tr_m(c) = 1$. If $v_1 = 0 \in \mathbb{F}_{2^m}$ (and $v_2 \neq 0_{n-m}$) then we take $a_1 = 0$ and, by the hypothesis on φ, a proper a_2 such that the derivative equals $v_2 \cdot D_{a_2}\varphi(y) \equiv 1$. Hence F is a $\mathcal{Q}\ell\mathcal{P}$. The converse is obvious since if a function is $\mathcal{Q}\ell\mathcal{B}$, then any function obtained by removing some of its coordinate functions is $\mathcal{Q}\ell\mathcal{B}$.
We show now that F has the $\mathcal{RQ}\ell$ property if and only if φ has it too. Indeed, for $a = (0, a_2) \in \mathbb{F}_{2^m} \times \mathbb{F}_2^{n-m}$, we have $D_a F(x, y) = (xD_{a_2}\phi(y), D_{a_2}\varphi(y))$, so if F satisfies the reversed property, then the same holds for φ because, writing $v = (v_1, v_2)$, we have $D_a F_v(x, y) = tr_m(v_1 x D_{a_2}\phi(y)) + v_2 \cdot D_{a_2}\varphi(y)$ and when $D_a F_v(x, y) \equiv 1$ we must have $v_2 \cdot D_{a_2}\varphi(y) \equiv 1$ (and $tr_m(v_1 x D_{a_2}\phi(y)) \equiv 0$). The implication in the other direction is proved by considering that, for $a = (a_1, 0_{n-m})$, we have $D_a F(x) = (a_1\phi(y), 0)$, and therefore, with $v = (a_1^{-1}, 0)$, we have $D_a F_v \equiv 1$, and for any other possible element $a = (a_1, a_2)$, we have, for some choice of $v = (0, v_2)$, that $D_a F_v(x, y) = D_{a_2}\varphi_{v_2}(y) \equiv 1$. □

Note that such quadratic-like permutations are non-quadratic when ψ is non-affine (or φ is non-quadratic). The functions in Proposition 18 are not affine equivalent to Feistel, in general, since they do not have a constant derivative $D_{(a_1,a_2)}F(x, y)$ with nonzero (a_1, a_2). This is true either if ϕ has no zero derivative in a nonzero direction or if ϕ is non-constant and φ has no constant derivative in a nonzero direction. Indeed, recall that $D_{(a_1,a_2)}F(x, y) = (xD_{a_2}\phi(y) + a_1\phi(y+a_2), D_{a_2}\varphi(y))$. If $a_2 = 0_{n-m}$ (and $a_1 \neq 0_m$), $D_{(a_1,a_2)}F(x, y) = (a_1\phi(y), 0_{n-m})$ is non-constant. If $a_2 \neq 0_{n-m}$, then either $xD_{a_2}\phi(y) + a_1\phi(y + a_2)$ is non-constant, or $D_{a_2}\varphi(y)$ is non-constant.

5.1 A construction in ANF form

Starting (as we shall see) from the cubic quadratic-like permutation in Example 2, we provide a (iterative) construction of quadratic-like permutations not equivalent to Feistel permutation and of algebraic degree up to $n - 1$.

We take m and r two positive integers, $r \geq 2$, and set $n = m + r$. Consider $g : \mathbb{F}_2^m \to \mathbb{F}_2$ any Boolean function, and consider $A = [a_{ij}]$ and $B = [b_{ij}]$ distinct invertible $r \times r$ matrices over $\mathbb{F}_2$. For $x \in \mathbb{F}_2^r$ and $y \in \mathbb{F}_2^m$, by $A \star x$ we denote the multiplication between matrix A and (column) vector $x = (x_1, \ldots, x_r)$, outputting an element of $\mathbb{F}_2^r$. We study the $(r + m, r + m)$-function

$$F(x, y) = \begin{bmatrix} F_1(x, y) \\ F_2(x, y) \end{bmatrix} = \begin{bmatrix} \Big(g(y)(A + B) + A\Big) \star x \\ y \end{bmatrix}, \tag{5}$$

where we can write

$$F_1(x, y) = g(y) \left[\textstyle\sum_{k=1}^{r}(a_{ik} + b_{ik})x_k\right]_{1 \leq i \leq r} + \left[\textstyle\sum_{k=1}^{r} a_{ik}x_k\right]_{1 \leq i \leq r}.$$

The degree of F is equal to the degree of g plus 1, which can be then up to $m+1 = n-r+1$. Notice that the cubic $\mathcal{QLP}$ in Example 2 is such that $m = r = 2$, $x = (x_1, x_2)$, $y = (x_3, x_4)$, $g(y) = x_3 x_4$, $A = \begin{bmatrix} 1 & 0 \\ 1 & 1 \end{bmatrix}$ and $B = A^T$.

To study the $\mathcal{QLP}$ property for F defined by (5), we take any nonzero $(v, w) \in \mathbb{F}_2^r \times \mathbb{F}_2^m$. If $v = 0_r$, then for $(c, d) \in \mathbb{F}_2^r \times \mathbb{F}_2^m$, we have $(v, w) \cdot D_{(c,d)} F(x, y) \equiv w \cdot d$ and if $w \cdot d = 1$, we have $(v, w) \cdot D_{(0_r,d)} F \equiv 1$. Assume now $v \neq 0_r$. For $(c, d) \in \mathbb{F}_2^r \times \mathbb{F}_2^m$ we have

$$v \cdot D_{(c,d)} F_1(x, y) = D_d\, g(y)\, v \cdot ((A + B) \star x) + g(y + d) v \cdot ((A + B) \star c) + v \cdot (A \star c)$$

and

$$\begin{aligned}(v, w) \cdot D_{(c,0_m)} F(x, y) =& v \cdot D_{(c,0_m)} F_1(x, y) + w \cdot 0_m \\ =& g(y) \sum_{k=1}^{r} c_k \sum_{i=1}^{r} v_i (a_{ik} + b_{ik}) + \sum_{k=1}^{r} c_k \sum_{i=1}^{r} v_i a_{ik} \\ =& g(y)\, c \cdot \left((A^T + B^T) \star v\right) + c \cdot (A^T \star v)\end{aligned}$$

Hence it is sufficient that $c \cdot (A^T \star v) = 1$ and $c \cdot (B^T \star v) = 1$ for having $(v, w) \cdot D_{(c,0_m)} F \equiv 1$. Since A and B are invertible matrices, then $u_1 := A^T \star v$ and $u_2 := B^T \star v$ are both nonzero, and since $r \geq 2$, there exists c such that $c \cdot u_1 = c \cdot u_2 = 1$. With such c we have $(v, w) \cdot D_{(c,0_m)} F \equiv 1$. This proves that F is $\mathcal{QLP}$.

To show the $\mathcal{RQL}$ property, we consider the derivative in any nonzero direction (c, d). If $d \neq 0_m$ then by taking $(0_r, w)$ such that $w \cdot d = 1$, we have $(0_r, w) \cdot D_{(c,d)} F(x, y) \equiv w \cdot d = 1$. Otherwise, if $d = 0_m$ then by taking v such that $v \cdot (A^T \star c) = v \cdot (B^T \star c) = 1$ we have $(v, 0_m) \cdot D_{(c,0_m)} F(x, y) = v \cdot D_{(c,0_m)} F_1(x, y) \equiv 1$.

Finally, to study the equivalence to a Feistel permutation, we need, according to Proposition 11, to verify whether there exists a direction (c, d) such that $D_{(c,d)} F$ is constant and nonzero. The derivative for F_1 equals

$$\left[D_d g(y) \textstyle\sum_{k=1}^{r} (a_{ik} + b_{ik}) x_k + g(y + d) \sum_{k=1}^{r} (a_{ik} + b_{ik}) c_k + \sum_{k=1}^{r} a_{ik} c_k\right]_i,$$

which can be constant only if $a_{ik} + b_{ik} = 0$ for every i and for every k or if $D_d g$ is identically 0. Hence by taking A and B distinct, and g admitting no nonzero 0-linear structure ($d \neq 0_m$ such that $D_d g \equiv 0$), we know that F can never have a constant derivative.

Notice that this construction can be generalized with $F_2(x, y) = H(y)$ a $\mathcal{QLP}$ over $\mathbb{F}_2^m$. The generalized construction still satisfies the studied properties (quadratic-like permutation not equivalent to Feistel), and it satisfies the $\mathcal{RQL}$ property if and only if H satisfies the $\mathcal{RQL}$ property. Indeed it is easily seen from the previous calculations that if H satisfies the property, then F does it too. Conversely, if F satisfies the reverse property, then considering the derivative in the directions of the form $(0_r, d)$, there exist (v, w) such that $(v, w) \cdot D_{(0_r,d)} F(x, y) = D_d g(y) v \cdot ((A + B) \star x)) + w \cdot D_d H(y) \equiv 1$. Then it must be

that $D_d g(y)v \cdot ((A+B) \star x)) \equiv 0$ and $w \cdot D_d H(y) \equiv 1$, implying that also H satisfies the reverse property.

This analysis is summarized in the following result.

Proposition 19. *For $n = m + r$ with $r \geq 2$, consider $g : \mathbb{F}_2^m \to \mathbb{F}_2$ any Boolean function and $H : \mathbb{F}_2^m \to \mathbb{F}_2^m$ a quadratic-like permutation. Take A, B any two distinct invertible $r \times r$ matrices over $\mathbb{F}_2$. Then the (n, n)-function*

$$F(x, y) = \begin{bmatrix} (g(y)(A+B) + A) \star x \\ H(y) \end{bmatrix},$$

with $(x, y) \in \mathbb{F}_2^r \times \mathbb{F}_2^m$ is a quadratic-like permutation, and if g has no 0-linear structure, then F is not equivalent to a Feistel permutation (even a generalized one as in Proposition 9, (iii)). Moreover, F satisfies the reversed quadratic-like property if and only if H satisfies the reversed quadratic-like property.

Remark 16. *The secondary construction of Proposition 19 consists in applying, to each of the first r coordinate functions of F, the indirect sum construction (see [10, Proposition 83]) with $f_1(x)$ (resp. $f_2(x)$) being equal to the corresponding coordinate function of $A \star x$ (resp. $B \star x$), and with $g_1(y) = 0$ and $g_2(y) = g(y)$, and in taking for the last m coordinate functions the coordinate functions of the quadratic-like (m, m)-permutation H. Note that there is no condition on g in Proposition 19, but if g is constant, then $F(x, y)$ has the form $[C \star x, H(y)]$ trivially equivalent to a generalized Feistel permutation as in (3). Moreover, notice that with this construction, the obtained map F has degree $\max\{\deg(H), \deg(g) + 1\}$, where $\deg(H) \leq m - 1$ and $\deg(g) \leq m$. So we can construct $\mathcal{QLP}$s of degree up to $m + 1$ and, by taking $r = 2$, we can construct $\mathcal{QLP}$s of any degree up to $n - 1$.*

5.2 Using the switching method

For building new permutations over $\mathbb{F}_{2^n}$ from known ones, the principle of the switching method is to add a Boolean function f, or more generally a function valued in $\gamma\mathbb{F}_2$ for some $\gamma \in \mathbb{F}_{2^n}^*$, to a permutation F of $\mathbb{F}_{2^n}$ (the method can also be viewed as changing one of the coordinate functions of a permutation over $\mathbb{F}_2^n$, since we can choose a basis of $\mathbb{F}_{2^n}$ with γ as an element of the basis). The switching method has been initiated in [4] to construct almost perfect nonlinear functions (being not necessarily bijective) and the name and generalization of the idea is due to Dillon and has been developed in [17, 27]. The following proposition was given in [15] (before the name was introduced); we recall this simple result and we give a proof for our paper to be self-contained.

Proposition 20. *Let F be any permutation over $\mathbb{F}_{2^n}$ and f any Boolean function over $\mathbb{F}_{2^n}$. Let $G(x) = F(x) + \gamma f(x)$, for $\gamma \in \mathbb{F}_{2^n}^*$. Then G is a permutation if and only if the Boolean function $g = f \circ F^{-1}$ satisfies $D_\gamma g \equiv 0$.*

Proof. Since F is injective on $supp(f) = \{x \in \mathbb{F}_{2^n}; f(x) = 1\}$ and on its complement $supp(f)^c$, a necessary and sufficient condition for G to be a permutation is that there does not exist x in $supp(f)$ and x' in $supp(f)^c$, such that

$F(x) = F(x') + \gamma$. Equivalently, the set $F(supp(f)) + F(supp(f)^c)$ does not contain the element γ. Since $F(supp(f)^c) = (F(supp(f))^c$ because F is bijective, we have that $F + f$ is a permutation if and only if $\gamma \notin F(supp(f)) + (F(supp(f))^c$, that is, $F(supp(f))$ is stable under the translation by γ. This completes the proof, since $F(supp(f)) = \{y \in \mathbb{F}_{2^n}; F^{-1}(y) \in supp(f)\}$ equals the support of g and is then stable under the translation by γ if and only if $D_\gamma g \equiv 0$. □

Remark 17. *This characterization provides the same condition for the two functions $G = F + \gamma f$ and $G \circ F^{-1} = Id + \gamma g$ (where $Id(x) = x$); this is coherent with the fact that G is a permutation if and only if $G \circ F^{-1}$ is a permutation.*

Remark 18. *The differentially 4-uniform permutations found in [27] correspond to F being the multiplicative inverse function and to simple choices of g Boolean such that $D_1 g \equiv 0$ ($\gamma = 1$).*

Let us now take for F a quadratic-like permutation over $\mathbb{F}_{2^n}$, for f any Boolean function over $\mathbb{F}_{2^n}$ and let $\gamma \in \mathbb{F}_{2^n}^*$. Set $G = F + \gamma f$. We have $tr_n(vG) = tr_n(vF) + (tr_n(\gamma v))f$. For every nonzero $v \in \mathbb{F}_{2^n}$, there exists $a \in \mathbb{F}_{2^n}$ such that $D_a F_v \equiv 1$, hence $D_a G_v = D_a F_v + (tr_n(\gamma v)) D_a f = 1 + (tr_n(\gamma v)) D_a f$. For G to be a quadratic-like permutation, it suffices that f is such that, for every v with $tr_n(\gamma v) = 1$, at least one of those a such that $D_a F_v \equiv 1$ satisfies $D_a f \equiv 0$. Then $F + \gamma f$ will be a quadratic-like permutation (and then according to Proposition 20, we will have $D_\gamma g \equiv 0$ where $g = f \circ F^{-1}$).

Remark 19. *The quadratic-like bijectivity of G is not equivalent to that of $G \circ F^{-1} = Id + \gamma g$ (unless F is affine, as we shall see below), contrary to its bijectivity (see Remark 17).*

The simplest case to be studied is of course with $F(x) = x$ (which can be extended by affine equivalence to F being any affine permutation). We have then $D_a F_v \equiv 1$ when $tr_n(av) = 1$ and we want, for each v such that $tr_n(\gamma v) = 1$, to be able to choose one a such that $tr_n(av) = 1$ and $D_a f \equiv 0$. Any Boolean function f such that $D_\gamma f \equiv 0$ works since we can take $a = \gamma$.
Let us now consider the reversed property of such a function. For any nonzero $a \neq \gamma$, we can take v such that $tr_n(\gamma v) = 0$ and $tr_n(av) = 1$, which gives $tr_n(v D_a(F + \gamma f)) \equiv 1$ as desired. For $a = \gamma$, since $D_\gamma f \equiv 0$, we just need v such that $tr_n(\gamma v) = 1$. Hence:

Proposition 21. *For every positive integer n, all the permutations over $\mathbb{F}_{2^n}$ obtained by the switching method from $F(x) = x$ are quadratic-like and they satisfy the $\mathcal{RQ}\ell$ property, that is, they are weakly crooked of codimension 1.*

This extends of course to the permutations obtained from F an affine permutation. Note that Proposition 21 provides functions of any algebraic degree between 1 and $n-1$. All these constructed functions belong to the general Feistel class described in Equation (3). Indeed, for the permutation $G(x) = x + \gamma f(x)$ it holds that $D_\gamma G(x) \equiv \gamma$.

It seems difficult to design a more general case of application of the switching method, which would lead to quadratic-like permutations.

Remark 20. *Let us take F in the simplest class of quadratic permutations: that of Gold functions $F(x) = x^{2^j+1}$ with $\frac{n}{\gcd(j,n)}$ odd (this latter condition being for F to be a permutation). We know (see e.g. [10]) that the elements a such that $D_aF_v(x) \equiv 1$ are those such that $(va)^{2^{-j}} + va^{2^j} = 0$ and $tr_n(va^{2^j+1}) = 1$, that is, $a = \lambda v^{-\frac{1}{2^j+1}}$ where $\lambda \in \mathbb{F}_{2^{\gcd(j,n)}}$ (and therefore $\lambda^2 = \lambda^{2^j+1} = va^{2^j+1}$) and $tr_n(\lambda) = 1$. Choosing $\gamma = 1$, it is enough to choose f such that, for every v such that $tr_n(v) = 1$, at least one a exists which satisfies $D_aF_v(x) \equiv 1$ and $D_af \equiv 0$. We need to be able to ensure that f is not constant, since we would then get nothing new. Note that we can relax the condition by also allowing that $D_aF_v(x) \equiv 0$ (that is, $a = \lambda v^{-\frac{1}{2^j+1}}$ where $\lambda \in \mathbb{F}_{2^{\gcd(j,n)}}$ and $tr_n(\lambda) = 0$) and $D_af \equiv 1$.*

However, it is possible to generalize the switching method by replacing the Boolean function f by a vectorial function G (and the construction will work better for quadratic-like functions if the image set of G has low rank). We first need a simple lemma:

Lemma 2. *Let F be a permutation over $\mathbb{F}_2^n$. Then for every $a, b, x \in \mathbb{F}_2^n$, denoting $y = F(x)$, we have $D_aF(x) = b$ if and only if :*

$$D_bF^{-1}(y) = a. \tag{6}$$

Proof. Denoting $y = F(x)$, the relation $F(x) + F(x + a) = b$ is equivalent to $y + F(F^{-1}(y) + a) = b$, that is, $F^{-1}(y) + a = F^{-1}(y + b)$. Hence, we have $D_aF(x) = b$ if and only if $D_bF^{-1}(y) = a$. □

Proposition 22. *Let F be a permutation over $\mathbb{F}_2^n$ and $G : \mathbb{F}_2^n \to \mathbb{F}_2^n$ be a function. Then $F + G$ is a permutation if and only if, for every nonzero $b \in \mathbb{F}_2^n$, the image set of the derivative $D_b(G \circ F^{-1})$ does not contain b.*

Proof. We have that $F + G$ is a permutation if and only if there does not exist $a \neq 0_n$ and x in $\mathbb{F}_2^n$ such that $D_aF(x) = D_aG(x)$. Still denoting $y = F(x)$, we have $D_aF(x) = D_aG(x) = b$ for some b if and only if $G(F^{-1}(y)) + G(F^{-1}(y) + a) = y + F(F^{-1}(y) + a) = b$, that is (replacing $F^{-1}(y) + a$ by $F^{-1}(y + b)$ thanks to Relation (6)), $G \circ F^{-1}(y) + G \circ F^{-1}(y + b) = b$, that is $D_b(G \circ F^{-1})(y) = b$, and vice versa.
Then, $F + G$ is a permutation if and only if, for every $b \in \mathbb{F}_2^n$, the derivative $D_b(G \circ F^{-1})$ is valued in $\mathbb{F}_2^n \setminus \{b\}$. □

Note that, as in the case of the switching method, the pair $\{F, F + G\}$ is obtained by composing the elements of the pair $\{Id, Id + G \circ F^{-1}\}$ by F on the right, where Id is the identity function. And if we directly consider the case $F = Id$, the condition in Proposition 22 becomes that, for every nonzero b, D_bG does not take the value b.

Remark 21. *This generalizes what we recalled on the switching method, since if $G = \gamma f$ is valued in $\{0_n, \gamma\}$, then the image set of G and of any of its derivatives is included in $\{0_n, \gamma\}$ and $F + G$ is a permutation if and only if, for*

every nonzero $b \in \{0_n, \gamma\}$, that is, for $b = \gamma$, the derivative $D_b(G \circ F^{-1})$ equals 0_n. We obtain the condition $D_\gamma g \equiv 0$ of Proposition 20, where $g = f \circ F^{-1}$.

Note that, if G is valued in a $\mathbb{F}_2$-vector subspace E of $\mathbb{F}_2^n$, then a sufficient condition for being able to apply Proposition 22 with $F = Id$ is that for every $a \in E$, we have $D_a G(x) \equiv 0$.
In fact, this allows to have the quadratic-like property:

Proposition 23. *Let G be any (n, n)-function valued in a $\mathbb{F}_2$-vector subspace E of $\mathbb{F}_2^n$, and such that, for every $a \in E$, we have $D_a G(x) \equiv 0$. Then the function $Id + G$ is a quadratic-like permutation and satisfies the $\mathcal{RQL}$ property.*

Proof. For every $v \notin E^\perp$, let $a \in E$ be such that $tr(av) = 1$; we have $D_a G \equiv 0$ and $F = Id + G$ satisfies $D_a F_v \equiv 1$. For every nonzero $v \in E^\perp$, then $tr(vG)$ being identically 0, any of its derivatives equals 0, and taking $a \in \mathbb{F}_{2^n}$ such that $tr(va) = 1$, we have $D_a F_v \equiv 1$. For the reversed property, if $a \notin E$ then there exists $v \in E^\perp$ such that $v \cdot D_a(x + G(x)) = v \cdot a = 1$, and if $a \in E$ then there exists $v \in \mathbb{F}_{2^n}$ such that $v \cdot D_a(x + G(x)) = v \cdot a = 1$. □

Note that contrary to the case of the switching method, considering $F + \gamma G$ would not generalize further.

Remark 22. *The hypothesis "for every $a \in E$, we have $D_a G(x) \equiv 0$" can be weakened. It suffices that, for every $v \notin E^\perp$, at least one element $a \in E$ such that $v \cdot a = 1$ satisfies $D_a G_v \equiv 0$ or at least one element $a \in E$ such that $v \cdot a = 0$ satisfies $D_a G_v \equiv 1$. More generally, assume that F is a $\mathcal{QLP}$ and G is an (n, n)-function valued in a vector space E. If $v \notin E^\perp$, it suffices that at least one among those $a \in \mathbb{F}_{2^n}$ such that $D_a F_v \equiv \beta$ satisfies $D_a G_v \equiv 1 - \beta$, for a fixed $\beta \in \mathbb{F}_2$. And if $v \in E^\perp$ is nonzero, then since $G_v \equiv 0$ and there exists $a \in \mathbb{F}_{2^n}$ such that $D_a F_v \equiv 1$, we are all set.*

Remark 23. *The permutations constructed in Proposition 23 belong to the general Feistel class described in Equation (3). Indeed, setting $k = \dim(E)$, up to identifying E with the vector subspace having basis the first k elements in the canonical basis and writing the input in the form (x, y) with $x \in \mathbb{F}_2^k, y \in \mathbb{F}_2^{n-k}$, we have $G(x, y) = \phi(y)$ for some $\phi : \mathbb{F}_2^{n-k} \to \mathbb{F}_2^k \times \{0_{n-k}\}$, and these permutations are of the form $F(x, y) = [x + \phi(y), Id(y)]$. This means that Proposition 23, which has the advantage of having a simple statement, has a too strong hypothesis for allowing to provide new $\mathcal{QLP}$. Notice that the 4-bit $\mathcal{QLP}$ F_1 displayed in Example 2 belongs to the general switching method construction described in Remark 22 and it is not equivalent to a Feistel permutation. Indeed, $F_1(x) = Id(x) + G(x)$, where $G = [x_2x_3x_4,\ x_1 + x_1x_3x_4,\ 0,\ 0]$ satisfies the above conditions, and for every nonzero $a \in \mathbb{F}_2^4$ we have $D_a F(x) = a + D_a G(x)$ not constant.*

We tried to generalize the conditions in Proposition 23 as $D_{\lambda_i}(g_j + g_\ell) \equiv 0$ and $D_{\lambda_1 + \cdots + \lambda_k} g_j \equiv 0$, and we still get a $\mathcal{QLP}$ with $\mathcal{RQL}$ property but such function is still in the general Feistel class. We leave the question open to construct an infinite class of pairs (F, G) as in Remark 22 such that $F + G$ is $\mathcal{QLP}$ but it is not in the general Feistel class.

6 The Walsh transform and the nonlinearity of quadratic-like balanced functions

Since quadratic-like balanced functions are characterized by the fact that all their component functions have a 1-linear structure, and since there exists a characterization of linear structures by the Walsh transform (see e.g. [10, Proposition 29]), there is a straightforward characterization of $\mathcal{QLB}$ functions by their Walsh transform. We give it in the next proposition. For our paper to be self-contained, we provide a proof.

Proposition 24. *Consider any (n,m)-function $F:\mathbb{F}_2^n\to\mathbb{F}_2^m$.*
F is $\mathcal{QLB}$ (resp., has the $\mathcal{RQL}$ property) if and only if, for every nonzero $v\in\mathbb{F}_2^m$, there exists $a_v\in\mathbb{F}_2^n$ (resp., for every nonzero $a\in\mathbb{F}_2^n$, there exists $v_a\in\mathbb{F}_2^m$) such that the function $u\mapsto W_F(u,v)$ vanishes on the linear hyperplane $\{0_n,a_v\}^\perp$ (resp., the function $u\mapsto W_F(u,v_a)$ vanishes on the linear hyperplane $\{0_n,a\}^\perp$).

Proof. Assume that $D_aF_v(x)\equiv 1$, then we have:

$$\begin{aligned}W_F(u,v)&=\sum_{x\in\mathbb{F}_2^n}(-1)^{u\cdot x+F_v(x)}=\sum_{x\in\mathbb{F}_2^n}(-1)^{u\cdot x+F_v(x+a)+1}\\&=-\sum_{x\in\mathbb{F}_2^n}(-1)^{u\cdot(x+a)+F_v(x)}=-(-1)^{u\cdot a}W_F(u,v).\end{aligned}$$

Therefore, if $u\cdot a=0$, then $W_F(u,v)=0$.
Conversely, if the function $u\mapsto W_F(u,v)$ vanishes on the linear hyperplane $\{0_n,a\}^\perp$, then we have:

$$\begin{aligned}\sum_{x\in\mathbb{F}_2^n}(-1)^{v\cdot(F(x)+F(x+a))}&=2^{-n}\sum_{x,y,u\in\mathbb{F}_2^n}(-1)^{v\cdot(F(x)+F(y))+u\cdot(x+y+a)}\\&=2^{-n}\sum_{u\in\mathbb{F}_2^n}W_F^2(u,v)(-1)^{u\cdot a}=-2^{-n}\sum_{u\in\mathbb{F}_2^n}W_F^2(u,v)\end{aligned}$$

and therefore $\sum_{x\in\mathbb{F}_2^n}(-1)^{v\cdot D_aF(x)}=-2^n$, according to the Parseval relation, and then $D_aF_v(x)\equiv 1$. □

Remark 24. *We know that an (n,m)-function F is balanced if and only if, for every nonzero $v\in\mathbb{F}_2^m$, we have $W_F(0_n,v)=0$. For F to be $\mathcal{QLB}$, we need that, for every nonzero $v\in\mathbb{F}_2^m$, there is a whole linear hyperplane H_v in $\mathbb{F}_2^n$ such that: $\forall u\in H_v, W_F(u,v)=0$.*

Remark 25. *Proposition 24 allows to show again that almost bent quadratic-like permutations are crooked (which is known by Corollary 2). Indeed, thanks to the Parseval relation, we know that for any almost bent (n,n)-function F and for every $v\neq 0_n$, there exist 2^{n-1} elements u such that $W_F(u,v)=\pm 2^{\frac{n+1}{2}}$. These elements are then those of the complement of $\{0_n,a_v\}^\perp$. We have then $W_F^2(u,v)=$*

2^{n+1} *if* $a_v \cdot u = 1$ *and* $W_F^2(u,v) = 0$ *if* $a_v \cdot u = 0$*, which implies by the inverse formula seen in Section 2:* $\sum_{x \in \mathbb{F}_2^n} (-1)^{F_v(x)+F_v(x+a)} = 2^{-n} \sum_{u \in \mathbb{F}_2^n} (-1)^{u \cdot a} W_F^2(u,v) = 2 \sum_{\substack{u \in \mathbb{F}_2^n \\ a_v \cdot u = 1}} (-1)^{u \cdot a} = \sum_{u \in \mathbb{F}_2^n} (-1)^{u \cdot a} \Big(1 - (-1)^{a_v \cdot u}\Big) = 2^n \delta_0(a) - 2^n \delta_0(a + a_v)$*, which means that* $D_{0_n} F_v \equiv 0$ *and* $D_{a_v} F_v \equiv 1$*, which we knew already, but also that for every* $a \notin \{0_n, a_v\}$*, the derivative* $D_a F_v$ *is balanced. Hence, all the derivatives of* F_v *are constant or balanced, which means that* F_v *is partially-bent and then* F *is strongly plateaued and APN, that is, crooked.*

Remark 26. *Let us now consider the nonlinearity of quadratic-like balanced maps. Let* F *be a* $\mathcal{QLB}$ (n,m)*-function. For nonzero* $v \in \mathbb{F}_2^m$*, we have that if* $D_a(F_v) \equiv 1$ *then* F_v *is affine equivalent to a function of the form* $x_n + g(x_1, \ldots, x_{n-1})$*. Hence, we have* $nl(F) \leq 2nl(g) \leq 2(2^{n-2} - 2^{\frac{n-1}{2}-1})$*, that is:*

$$nl(F) \leq 2^{n-1} - 2^{\frac{n-1}{2}}. \tag{7}$$

Recall that for $m = n$*, the Sidelnikov-Chabaud-Vaudenay bound (see e.g. [10]) coincides with (7). This shows that the property of being quadratic-like does not a priori reduce the nonlinearity of an* (n,n)*-permutation, and indeed, for* n *odd, there are quadratic almost bent permutations.*
For $m < n$*, the Sidelnikov-Chabaud-Vaudenay bound states* $nl(F) \leq 2^{n-1} - \frac{1}{2}\sqrt{3 \times 2^n - 2 - 2\frac{(2^n-1)(2^{n-1}-1)}{2^m-1}}$*. The value at the right hand-side of this inequality is strictly smaller than* $2^{n-1} - 2^{\frac{n-1}{2}}$*. Hence, in that case, Relation (7) does not tell us anything interesting.*
If we consider an (n,n)*-permutation* F *with the* $\mathcal{RQL}$ *property, then Proposition 4.8 in [7] tells us that* $nl(F) \leq 2^{n-1} - 2^{\frac{n-1}{2}}$*. Indeed, by definition, at least one component function of* F *has a non-trivial linear structure. The same bound is of course valid for quadratic-like permutations and more general* $\mathcal{QLB}$ *functions.*

7 The ANF of a quadratic-like balanced function

Consider $F : \mathbb{F}_2^n \to \mathbb{F}_2^m$ a $\mathcal{QLB}$ function. To study the ANF of F, we introduce the following definition. For an integer k $(1 \leq k \leq m)$, we say that F satisfies the property (P_k) if there exists a `cls` map $\phi : \mathbb{F}_2^m \to \mathbb{F}_2^n$ for F, with $\phi(0_m) = 0_n$, which sends a set of k linearly independent elements into linearly independent elements. Clearly, if F satisfies the property (P_k) for some positive $k > 1$, then it also satisfies the property (P_{k-1}). Take $v_1, \ldots, v_k \in \mathbb{F}_2^m$ the linearly independent vectors such that $\phi(v_1), \ldots, \phi(v_k) \in \mathbb{F}_2^n$ are linearly independent. Denoting by $(e_1, \ldots, e_n)$ the canonical basis of $\mathbb{F}_2^n$ and by $(e'_1, \ldots, e'_m)$ the canonical basis of $\mathbb{F}_2^m$, we denote by L_1 a linear bijection of $\mathbb{F}_2^m$ such that $L_1(e'_i) = v_i$, for $i = 1, \ldots, k$, and by L_2 a linear bijection of $\mathbb{F}_2^n$ such that $L_2(e_i) = \phi(v_i)$, for

$i = 1, \ldots, k$. Then, we consider the map G affine equivalent to F, of the form $L_1^* \circ F \circ L_2$, where L_1^* is the adjoint linear operator of L_1. We have:

$$\begin{aligned} e_i' \cdot D_{e_i} G(x) =& e_i' \cdot L_1^*(F(L_2(x + e_i)) + F(L_2(x))) \\ =& L_1(e_i') \cdot (F(L_2(x) + L_2(e_i)) + F(L_2(x))) \\ =& v_i \cdot (F(L_2(x) + \phi(v_i)) + F(L_2(x))) = v_i \cdot D_{\phi(v_i)} F(L_2(x)) \equiv 1. \end{aligned}$$

Therefore, up to applying an affine transformation, we can assume $\phi(e_i') = e_i$ so, for $i = 1, \ldots, k$,

$$F_{e_i'}(x) = e_i' \cdot F(x) = g_i(x_1, \ldots, x_{i-1}, x_{i+1}, \ldots, x_n) + x_i. \tag{8}$$

Remark 27. *Consider $F : \mathbb{F}_2^n \to \mathbb{F}_2^m$ a $\mathcal{QLB}$ function, and recall that $n \geq m$. If there exists a linear map ϕ that is a* `cls` *map for F, then ϕ must be injective. Indeed, if there are distinct $v_1, v_2 \in \mathbb{F}_2^m$ such that $\phi(v_1) = \phi(v_2)$, then the contradiction is obtained from $\phi(v_1 + v_2) = 0_n$. This implies that, if such ϕ exists, then F satisfies the property (P_m), and, up to affine equivalence, we can assume that $\phi(e_i') = e_i$ for $i = 1, \ldots, m$, and complete the family $(e_1, \ldots e_m)$ into a basis of $\mathbb{F}_2^n$ whose $n-m$ last elements belong to the kernel of ϕ, and deduce that, for $v \in \mathbb{F}_2^m$, we have $\phi(v) = (v, 0_{n-m})$. Thus, we can consider the quadratic-like (m, m)-permutation G equal to the restriction of F to $\{x \in \mathbb{F}_2^n; x_{m+1} = \ldots = x_n = 0\}$, for which it holds $v \cdot D_v G(x) \equiv 1$ for any nonzero $v \in \mathbb{F}_2^m$. We checked that this works well for $m \leq 3$, with $G(x_1) = \begin{bmatrix} x_1 \end{bmatrix}$, $G(x_1, x_2) = \begin{bmatrix} x_1 \\ x_1 + x_2 \end{bmatrix}$, and $G(x_1, x_2, x_3) = \begin{bmatrix} x_1 + x_2 x_3 \\ x_1 + x_2 + x_1 x_3 \\ x_1 + x_2 + x_3 + x_1 x_2 \end{bmatrix}$. But unfortunately, no $\mathcal{QLP}$ admits a linear ϕ for $m \geq 4$. The proof of this last statement is quite technical, so we provide it as an appendix, see Appendix A.*

Even without assuming the existence of such a linear `cls` map ϕ, we still have that a quadratic-like balanced function F satisfies property (P_k) for some $k \geq \lfloor m/2 \rfloor + 2$, as the following proposition states.

Proposition 25. *For $3 \leq m \leq n$, consider $F : \mathbb{F}_2^n \to \mathbb{F}_2^m$ a $\mathcal{QLB}$ function, then F satisfies property (P_k) for any $k < (m + 5)/2$, that is, $k \leq \lfloor \frac{m}{2} \rfloor + 2$. This means that, up to affine equivalence, for $1 \leq j \leq \lfloor \frac{m}{2} \rfloor + 2$ we can assume*

$$F_{e_j'}(x) = e_j' \cdot F(x) = g_j(x_1, \ldots, x_{j-1}, x_{j+1}, \ldots, x_n) + x_j.$$

Proof. Consider $F : \mathbb{F}_2^n \to \mathbb{F}_2^m$ a $\mathcal{QLB}$ map. It is straightforward to see that F satisfies (P_2), for $n \geq m \geq 2$. Indeed, if for two distinct nonzero vectors $v, w \in \mathbb{F}_2^m$ there exists $a \in \mathbb{F}_2^n$ such that $v \cdot D_a F = w \cdot D_a F \equiv 1$, then for $v + w$ (which is nonzero) there is a different a' such that $(v + w) \cdot D_{a'} F \equiv 1$.

If F satisfies (P_m), and so (P_t) for any $1 \leq t \leq m$, the statement of the proposition is trivially satisfied (for $m \geq 3$, the condition $k < (m+5)/2$ implies $k \leq m$). Assume then that F satisfies (P_t) but does not satisfy (P_{t+1}), for some $1 < t < m$. So, we can assume without loss of generality that the first t

coordinates of F are as in (8), thus for brevity of the form $x_i + g_i$ for $1 \leq i \leq t$, while we denote the remaining $m-t$ coordinates as f_j for $t+1 \leq j \leq m$. Since (P_{t+1}) is not satisfied, then for every $v = (\eta, \lambda) \in \mathbb{F}_2^t \times \mathbb{F}_2^{m-t}$, with $\lambda \neq 0_{m-t}$, we have that $\{e'_1, \ldots, e'_t, v\}$ are linearly independent, so $\{\phi(e'_1), \ldots, \phi(e'_t), \phi(v)\}$ must be linearly dependent, for any `cls` map ϕ. Clearly, we can take ϕ such that $\phi(e'_i) = e_i$ for $1 \leq i \leq t$. Therefore, it holds the following:

$$\forall v \in \mathbb{F}_2^t \times (\mathbb{F}_2^{m-t} \setminus \{0_{m-t}\}) \ \{a \in \mathbb{F}_2^n; v \cdot D_a F \equiv 1\} \subseteq \langle e_1, \ldots, e_t \rangle. \tag{9}$$

In particular, for any $j = 1, \ldots, t$, the $(n, m-t+1)$-map $G = \begin{bmatrix} x_j + g_j \\ f_{t+1} \\ \vdots \\ f_m \end{bmatrix}$ is such that for any nonzero $w \in \mathbb{F}_2^{m-t+1}$ there exists $a = (a', 0_{n-t})$, $a' \in \mathbb{F}_2^t$, such that $w \cdot D_a G = D_a G_w \equiv 1$. So, by writing G_w as

$$G_w(x) = \sum_{I \subseteq \{t+1, \ldots, n\}} h_I^w(x_1, \ldots, x_t) \prod_{j \in I} x_j, \qquad h_I^w : \mathbb{F}_2^t \to \mathbb{F}_2,$$

it holds that $D_a G_w(x) = \sum_{I \subseteq \{t+1, \ldots, n\}} D_{a'} h_I^w(x_1, \ldots, x_t) \prod_{j \in I} x_j$, implying that $D_{a'} h_\emptyset^w \equiv 1$. Thus, by considering the restriction of G to $\{x \in \mathbb{F}_2^n; x_{t+1} = \cdots = x_n = 0\}$, we obtain a function from $\mathbb{F}_2^t$ to $\mathbb{F}_2^{m-t+1}$ which is $\mathcal{QLB}$, implying that $t \geq m - t + 1$, so $t \geq (m+1)/2$.
This implies that the minimum value k such that (P_k) is not satisfied is such that $k \geq (m+3)/2$ and so, for any $t < (m+3)/2$ property (P_t) is satisfied. In the following, we improve the result, showing that (P_t) is satisfied for any $t < (m+5)/2$.
Consider $\tilde{F}$ to be the restriction of F to $\{x \in \mathbb{F}_2^n; x_{t+1} = \cdots = x_n = 0\}$, thus $\tilde{F} : \mathbb{F}_2^t \to \mathbb{F}_2^m$. Since $t < m$, the quadratic-like property cannot be satisfied, so there exists a nonzero $\theta \in \mathbb{F}_2^m$ such that for any $a' \in \mathbb{F}_2^t$ we have $\theta \cdot D_{a'} \tilde{F} \not\equiv 1$. Since F is $\mathcal{QLB}$, there must exist $a \in \mathbb{F}_2^n$ such that $\theta \cdot D_a F \equiv 1$, so a is of the form $a = (a', \alpha) \in \mathbb{F}_2^t \times \mathbb{F}_2^{n-t}$ with $\alpha \neq 0_{n-t}$, thus $a \notin \langle e_1, \ldots, e_t \rangle$.

From Relation (9) we have that θ must be of the form $\theta = (\theta', 0_{m-t}) \in \mathbb{F}_2^t \times \mathbb{F}_2^{m-t}$. Without loss of generality, up to reordering the variables, we can assume $\theta = e'_1 + \cdots + e'_s$, for some $s \in \{2, \ldots, t\}$, where $s \neq 1$ since $\phi(e'_1) = e_1$. To characterize further the set of 1-linear structures displayed in Relation (9), we consider the following set of $t+1$ linearly independent elements $\{e'_1, \ldots, e'_{j-1}, e'_{j+1}, \ldots, e'_t, \theta, v\}$ with $1 \leq j \leq s$ and $v = (\eta, \lambda) \in \mathbb{F}_2^t \times \mathbb{F}_2^{m-t}$, $\lambda \neq 0_{m-t}$. We take a `cls` map ϕ such that $\phi(e'_i) = e_i$, for $1 \leq i \leq t$, and $\phi(\theta) = a$, then it must be that $\{e_1, \ldots, e_{j-1}, e_{j+1}, \ldots, e_t, a, \phi(v)\}$ are linearly dependent. Since $a \notin \langle e_1, \ldots, e_t \rangle$, together with Relation (9) this implies that $\phi(v) \in \langle e_1, \ldots, e_{j-1}, e_{j+1}, \ldots, e_t \rangle$. The vectors $e_1, \ldots, e_t$ being linearly independent, there is a unique linear combination which equals $\phi(v)$. According to what we just saw, the coefficient for e_j is zero. Since this can be done for any $1 \leq j \leq s$, for any $v = (\eta, \lambda) \in \mathbb{F}_2^t \times \mathbb{F}_2^{m-t}$, with $\lambda \neq 0_{m-t}$, we have $\{a \in \mathbb{F}_2^n; v \cdot D_a F \equiv 1\} \subseteq \langle e_{s+1}, \ldots, e_t \rangle$. Hence, taking any $j = s+1, \ldots, t$ and

noticing that $\phi(e'_j) = e_j$ for some `cls` map, the map $G = \begin{bmatrix} x_j + g_j \\ f_{t+1} \\ \vdots \\ f_m \end{bmatrix} : \mathbb{F}_2^n \to \mathbb{F}_2^{m-t+1}$ is such that for any nonzero $w \in \mathbb{F}_2^{m-t+1}$ there exists $a = (0_s, a', 0_{n-t})$, $a' \in \mathbb{F}_2^{t-s}$, such that $w \cdot D_a G \equiv 1$ (notice that we added only one coordinate of the form $x_j + g_j$ since we do not know, a priori, that the sum of two such functions $x_j + g_j + x_{j'} + g_{j'}$ has a 1-linear structure of the form of a). Similarly as before, we consider the restriction of G to $\{x \in \mathbb{F}_2^n; x_1 = \cdots = x_s = x_{t+1} = \cdots = x_n = 0\}$ and obtain a $\mathcal{QLB}$ function from $\mathbb{F}_2^{t-s}$ to $\mathbb{F}_2^{m-t+1}$, implying $t - s \geq m - t + 1$, so $2 \leq s \leq 2t - m - 1$. This also implies that $2t - m - 1 \geq 2$, so $t \geq (m+3)/2$. Therefore, the minimum value k such that a $\mathcal{QLB}$ (n, m)-function does not satisfy the property (P_k) is such that $k = t + 1 \geq (m + 5)/2$. In addition to what already stated, notice that, for $r = \lfloor m/2 \rfloor$, it holds $r + 2 < (m + 5)/2 < r + 3$, so the property (P_{r+2}) is satisfied. Thus, together with Equation (8), this concludes the proof of the proposition. □

Question 3. *Can we improve Proposition 25, by showing that, up to affine equivalence, any $\mathcal{QLP}$ has a still more specific ANF? For example, do quadratic-like permutations satisfy also property $(P_{\lfloor \frac{m}{2} \rfloor + 3})$?*

In the case of a $\mathcal{QLP}$ admitting an invertible `cls` map, such as crooked permutations, the above proposition can be improved.

Corollary 3. *For $n \geq 3$, consider $F : \mathbb{F}_2^n \to \mathbb{F}_2^n$ a quadratic-like permutation admitting a permutation $\phi : \mathbb{F}_2^n \to \mathbb{F}_2^n$ as `cls` map. Then, up to affine equivalence, we can assume for any $1 \leq j \leq n$*

$$F_{e_j}(x) = e_j \cdot F(x) = g_j(x_1, \ldots, x_{j-1}, x_{j+1}, \ldots, x_n) + x_j.$$

Proof. Following the proof of Proposition 25, if Relation (9) is satisfied for some $1 < t < n$, then for any $v = (\eta, \lambda) \in \mathbb{F}_2^t \times \mathbb{F}_2^{n-t}$, $\lambda \neq 0_{n-t}$, we have $\phi(v) \in \langle e_1, \ldots, e_t \rangle$. Moreover, being ϕ injective, $\phi(v) \neq \phi(e_i) = e_i$ for $1 \leq i \leq t$ and $\phi(v) \neq 0_n$. Thus it holds that $2^n - 2^t = |\{v = (\eta, \lambda) \in \mathbb{F}_2^t \times \mathbb{F}_2^{n-t};\ \lambda \neq 0_{n-t}\}| \leq |\langle e_1, \ldots, e_t \rangle \setminus \{0_n, e_1, \ldots, e_t\}| = 2^t - (t+1)$, implying $2^n \leq 2^{t+1} - t - 1 \leq 2^{t+1}$. This leads to a contradiction, since $t < n$, and concludes the proof. □

Conclusion

In this work we investigated a subclass of balanced functions, by introducing *quadratic-like balanced* functions, whose component functions all have by definition a 1-linear structure. These functions are all balanced. The notion of quadratic-like balanced function generalizes that of balanced quadratic function with the point of view of balancedness, in a similar way as plateaued functions generalize quadratic functions with the point of view of the Walsh transform. We also considered the reversed quadratic-like property, which for $n = m$ generalizes the (strict) crookedness. We studied quadratic-like balanced functions

via different tools, such as equivalence transformations, the Walsh transform and the algebraic normal form. We focused on some known classes of balanced maps, in particular of permutations, and we showed that many of them provide functions which are quadratic-like (while quadratic-like permutations do not represent a large part of all permutations). One notable case is the class of Feistel permutations, which play an important role in cryptography; indeed all Feistel permutations are quadratic-like. Moreover, we provided some primary and secondary constructions of quadratic-like balanced maps. It is interesting to notice that some of the problems posed by quadratic-like balanced functions are closely connected with other well know problems in this area of research, such as those related to crooked functions.
We have reported some open questions/open problems that we believe are of great interest to better understand the class of quadratic-like balanced functions. The main open question that we leave and which is probably very difficult, is to precisely determine, for every n, the class of quadratic-like permutations. Another open question is to determine whether quadratic-like permutations all have the reversed quadratic-like property, and vice versa. For the general class of balanced maps, we leave as an open problem the characterization of plateaued quadratic-like balanced functions.

Acknowledgements We thank P. Charpin and G. Kyureghyan for some useful comments on a previous version of this paper.
I. Villa is member of the INdAM Research Group GNSAGA.

Statements and Declarations

Competing Interests C. Carlet is an Editorial Board Member of Designs, Codes and Cryptography.

References

[1] T. Bending, and D. Fon-Der-Flaass. Crooked functions, bent functions and distance regular graphs. *Electron. J. Comb.* 5, Research paper 34 (electronic), 14 pages, 1998.

[2] J. Bierbrauer, and G. Kyureghyan. Crooked binomials. Designs Codes Cryptography 46(3), pp. 269-301, 2008.

[3] K. Browning, J. F. Dillon, M. McQuistan and A. J. Wolfe. An APN permutation in dimension 6. *Proceedings of Conference Finite Fields and Applications Fq9*, Contemporary Mathematics 518, pp. 33-42, 2010.

[4] L. Budaghyan, C. Carlet and G. Leander. Constructing new APN functions from known ones. *Finite Fields and Their Applications* 15, pp. 150-159, 2009.

[5] M. Calderini, M. Sala, and I. Villa. A note on APN permutations in even dimension. *Finite Field and their Applications* 46, pp. 1-16, 2017.

[6] A. Canteaut. Analysis and design of symmetric ciphers. Habilitation for Directing Theses, University of Paris 6, 2006.

[7] A. Canteaut, and M. Naya-Plasencia. Structural weaknesses of permutations with a low differential uniformity and generalized crooked functions. Finite Fields: Theory and Applications-FQ9-Contemporary Mathematics, AMS 518 (2010): 55-71.

[8] C. Carlet. Partially-bent functions. Designs Codes and Cryptography, 3, pp. 135- 145, 1993, and Proceedings of CRYPTO 1992, Lecture Notes in Computer Science 740, pp. 280-291, 1993.

[9] C. Carlet. Boolean and vectorial plateaued functions, and APN functions. *IEEE Transactions on Information Theory* 61 (11), pp. 6272-6289, 2015

[10] C. Carlet. *Boolean Functions for Cryptography and Coding Theory*. Cambridge University Press, 2021.

[11] C. Carlet, P. Charpin, and V. Zinoviev. Codes, bent functions and permutations suitable for DES-like cryptosystems. *Designs, Codes and Cryptography*, 15 (2), pp. 125-156, 1998.

[12] C. Carlet, I. Villa. On cubic-like bent Boolean functions. *Cryptology ePrint Archive*, Paper 2023/879, 2023. To appear in *Journal of Algebraic Combinatorics*.

[13] C. De Canniere. Analysis and Design of Symmetric Encryption Algorithms. PhD thesis (2007)

[14] P. Charpin. The crooked property. *Finite Fields and Their Applications* 81, 102032, 2022.

[15] P. Charpin and G. Kyureghyan. On a class of permutation polynomials over $\mathbb{F}_{2^n}$. In *International Conference on Sequences and Their Applications*, pp. 368-376. Berlin, Heidelberg: Springer Berlin Heidelberg, 2008.

[16] P. Charpin and G. Kyureghyan, Monomial functions with linear structure and permutation polynomials, in: *Finite Fields: Theory and Applications FQ9*, in: Contemp. Math., vol. 518, AMS, 2010, pp. 99-111.

[17] Y. Edel and A. Pott. A new almost perfect nonlinear function which is not quadratic. *Advances in Mathematics of Communications* 3 (1), pp. 59-81, 2009.

[18] J. D. Golić. On the security of nonlinear filter generators. In *International Workshop on Fast Software Encryption*, pp. 173-188 (1996).

[19] D. Hertel, and A. Pott. A characterization of a class of maximum nonlinear functions. *arXiv* preprint math/0508034 (2005).

[20] L. Knudsen. Truncated and higher order differentials. *Proceedings of Fast Software Encryption FSE 1995, Lecture Notes in Computer Science* 1008, pp. 196-211, 1995.

[21] G.M. Kyureghyan, The only crooked power functions are $x^{2^k+2^l}$. *European Journal of Combinatorics* 28 (4), pp. 1345-1350, 2007.

[22] G.M. Kyureghyan. Crooked maps in $\mathbb{F}_2^n$. *Finite Fields and their applications*, 13(3), 713-726, 2007.

[23] X. Lai. Higher order derivatives and differential cryptanalysis. *Proceedings of the "Symposium on Communication, Coding and Cryptography", in honor of J. L. Massey on the occasion of his 60'th birthday*, pp. 227-233, 1994.

[24] P. Langevin, and P. Véron. On the Non-linearity of Power Functions. *Designs, Codes and Cryptography*, 2005, 37, pp.31-43.

[25] K. Nyberg. S-boxes and round functions with controllable linearity and differential uniformity. *International Workshop on Fast Software Encryption, Lecture Notes in Computer Science*, vol.1008, pp.111-130, 1995.

[26] G. Piret, T. Roche and C. Carlet. PICARO – A Block Cipher Allowing Efficient Higher-Order Side-Channel Resistance. *Proceedings of ACNS 2012, Lecture Notes in Computer Science* 7341, pp. 311-328, 2012.

[27] L. Qu, Y. Tan, C. H. Tan and C. Li. Constructing Differentially 4-Uniform Permutations Over $\mathbb{F}_{2^{2k}}$ via the Switching Method. *IEEE Transactions on Information Theory* 59 (7), pp. 4675-4686, 2013.

A Proof of Remark 27

Assume that $F(x_1, \ldots, x_n)$ is a quadratic-like permutation admitting $\phi(x) = x$ the identity map. Consider $n \geq 4$, and name F_i the i-th coordinate of F. Then

$$\begin{aligned}
F_1(x) =& x_1 + x_2\ell_1 + x_2x_3t_1 + x_2x_4k_1 + x_2x_3x_4u_1 + x_3r_1 + x_3x_4s_1 + x_4v_1 + o_1\\
F_2(x) =& x_2 + x_1w_2 + x_1x_3g_2 + x_1x_4h_2 + x_1x_3x_4u_2 + x_3r_2 + x_3x_4s_2 + x_4v_2 + o_2\\
F_3(x) =& x_3 + x_1w_3 + x_1x_2f_3 + x_1x_4h_3 + x_1x_2x_4u_3 + x_2\ell_3 + x_2x_4k_3 + x_4v_3 + o_3\\
F_4(x) =& x_4 + x_1w_4 + x_1x_2f_4 + x_1x_3g_4 + x_1x_2x_3u_4 + x_2\ell_4 + x_2x_3t_4 + x_3r_4 + o_4,
\end{aligned}$$

with $\ell_i, t_i, k_i, r_i, s_i, v_i, o_i, w_i, g_i, h_i, f_i, u_i$ Boolean function in the variables $x_5, \ldots, x_n$. Notice that we already used the fact that $D_{e_i}F_i \equiv 1$ for $i = 1, \ldots, 4$. First, we consider that $D_{e_i+e_j}(F_i + F_j) \equiv 1$, for $1 \leq i < j \leq 4$.

- For $(i, j) = (1, 2)$, we have $1+\ell_1+x_3t_1+x_4k_1+x_3x_4u_1+1+w_2+x_3g_2+x_4h_2+x_3x_4u_2 \equiv 1$, so $u_2 = u_1$, $g_2 = t_1$, $h_2 = k_1$ and $w_2 = 1 + \ell_1$.
- For $(i, j) = (1, 3)$, we have $1+x_2t_1+x_2x_4u_1+r_1+x_4s_1+1+w_3+x_2f_3+x_4h_3+x_2x_4u_3 \equiv 1$, so $u_3 = u_1$, $f_3 = t_1$, $h_3 = s_1$ and $w_3 = r_1 + 1$.
- For $(i, j) = (1, 4)$, we have $1+x_2k_1+x_2x_3u_1+x_3s_1+v_1+1+w_4+x_2f_4+x_3g_4+u_4x_2x_3 \equiv 1$, so $u_4 = u_1$, $f_4 = k_1$, $g_4 = s_1$ and $w_4 = 1 + v_1$.

- For $(i,j) = (2,3)$, we have $1+x_1t_1+x_1x_4u_1+r_2+x_4s_2+1+x_1t_1+x_1x_4u_1+\ell_3+x_4k_3 \equiv 1$, so $k_3 = s_2$ and $\ell_3 = r_2 + 1$.
- For $(i,j) = (2,4)$, we have $1+x_1k_1+x_1x_3u_1+x_3s_2+v_2+1+x_1k_1+x_1x_3u_1+\ell_4+x_3t_4 \equiv 1$, so $t_4 = s_2$, $\ell_4 = v_2 + 1$.
- For $(i,j) = (3,4)$, we have $1+x_1s_1+x_1x_2u_1+x_2s_2+v_3+1+x_1s_1+x_1x_2u_1+x_2s_2+r_4 \equiv 1$, so $r_4 = v_3 + 1$.

Next step, $D_{e_i+e_j+e_l}(F_i + F_j + F_l) \equiv 1$.

- $(i,j,l) = (1,2,3)$, we have $1 + \ell_1 + (x_2 + x_3 + 1)t_1 + x_4k_1 + (x_2 + x_3 + 1)x_4u_1 + r_1 + x_4s_1 + \ell_1 + (x_1 + x_3 + 1)t_1 + x_4k_1 + (x_1 + x_3 + 1)x_4u_1 + r_2 + x_4s_2 + r_1 + (x_1 + x_2 + 1)t_1 + x_4s_1 + (x_1 + x_2 + 1)x_4u_1 + 1 + r_2 + x_4s_2 \equiv 1$, so $u_1 = 0$ and $t_1 = 1$.
- $(i,j,l) = (1,2,4)$, we have $1 + \ell_1 + x_3 + (x_2 + x_4 + 1)k_1 + x_3s_1 + v_1\ell_1 + x_3 + (x_1 + x_4 + 1)k_1 + x_3s_2 + v_2 + v_1 + (x_1 + x_2 + 1)k_1 + x_3s_1 + v_2 + 1 + x_3s_2 \equiv 1$, so $k_1 = 1$.
- $(i,j,l) = (1,3,4)$, we have $1 + x_2 + x_2 + r_1 + (x_3 + x_4 + 1)s_1 + v_1 + r_1 + x_2 + (x_1 + x_4 + 1)s_1 + x_2s_2 + v_3 + v_1 + x_2 + (x_1 + x_3 + 1)s_1 + x_2s_2 + v_3 + 1 \equiv 1$, so $s_1 = 1$.
- $(i,j,l) = (2,3,4)$, we have $1 + x_1 + x_1 + r_2 + (x_3 + x_4 + 1)s_2 + v_2 + 1 + x_1 + x_1 + r_2 + 1 + (x_2 + x_4 + 1)s_2 + v_3 + 1 + x_1 + x_1 + v_2 + 1 + (x_2 + x_3 + 1)s_2 + v_3 + 1 \equiv 1$, so $s_2 = 1$.

As last, from $D_{e_1+e_2+e_3+e_4}(F_1 + F_2 + F_3 + F_4) \equiv 1$ we have $1 + \ell_1 + (x_2 + x_3 + 1) + (x_2 + x_4 + 1) + +r_1 + (x_3 + x_4 + 1) + v_1 + 1 + w_2 + (x_1 + x_3 + 1) + (x_1 + x_4 + 1) + r_2 + (x_3 + x_4 + 1) + v_2 + r_1 + (x_1 + x_2 + 1) + (x_1 + x_4 + 1) + r_2 + 1 + (x_2 + x_4 + 1) + v_3 + v_1 + (x_1 + x_2 + 1) + (x_1 + x_3 + 1) + v_2 + 1 + (x_2 + 1x_3 + 1) + v_3 + 1 \equiv 1$ that gives us $0 = 1$. Hence a contradiction.