Quadratic-like balanced functions and 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 have this same property and we observe that the notion is affine invariant. We also study in each of these classes and in the class of quadratic-like APN permutations 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 also show that all the quadratic-like power permutations $F(x) = x^d$, $x \in \mathbb{F}_{2^n}$ must be quadratic, which generalizes a well-known similar result on power crooked functions. 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.

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.

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 substitution boxes (S-boxes) in those block ciphers having the structure of substitution permutation network (SPN) need to be permutations.

We know (see e.g. [7]) 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).

As we shall see, such a property is very useful for studying - or possibly 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 [14, 12]). 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 3, 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 3) 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 3).

We shall then study constructions of quadratic-like balanced functions, and focus on those that are neither quadratic, nor affine equivalent[2] to permutations having a Feistel form, nor crooked, nor even strongly plateaued. We shall characterize the notion by the Walsh transform.

[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).

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

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 $\mathbb{F}_2^n$, 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 $\mathbb{F}_2^n$: $a \cdot b = \sum_{i=1}^n a_i b_i \in \mathbb{F}_2$ 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 $tr(x) = \sum_{i=0}^{n-1} x^{2^i}$ 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 $D_a F(x) = F(x+a) + F(x)$. 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 $\deg(F) = \max_I \{|I|; a_I \neq 0\}$ 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 $F(0) = 0$. 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. [7, 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* [8] 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 any $a, b \in \mathbb{F}_2^n$, with $a \neq 0$, the equation $D_aF(x) = b$ admits at most 2 solutions.

The Walsh transform of an $(n,1)$-function f is $W_f(u) = \sum_{x\in\mathbb{F}_2^n}(-1)^{f(x)+u\cdot x}$, 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). 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 $\{0,a\}^\perp = \{x \in \mathbb{F}_2^n; a\cdot x = 0\}$, resp. in its complement, see [7, Proposition 29]. Recall that a balanced quadratic Boolean function always admits a 1-linear structure (see e.g. [7, 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 [7, Chapter 6, Subsection 5.1]. Crooked functions are (equivalently) APN strongly plateaued functions [6, 7].

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 $u, v \in \mathbb{F}_2^n$, $v \neq 0$. This implies that F is APN.

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, $v \neq 0$ 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 *if for any nonzero $v \in \mathbb{F}_2^m$, there exists $a \in \mathbb{F}_2^n$ such that $D_aF_v = v \cdot D_aF$ is constantly 1, that is, a is a 1-linear structure of F_v.*
In the case $m = n$, the function is called a quadratic-like permutation.
We shall call component-to-linear-structure map*, shortly* `cls` *map, any function mapping $v \in \mathbb{F}_2^m \setminus \{0\}$ 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 to 0.*

Notice that the property for the case of permutations can be characterized by means of the graph of the function.

Remark 1. *Given an (n,n)-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 a permutation if and only if Δ_F has no intersection with $(\mathbb{F}_2^n \setminus \{0\}) \times \{0\}$ and it is quadratic-like if, for every nonzero v, there exists a such that $(\{a\} \times \mathbb{F}_2^n) \cap \Delta_F \subset \{a\} \times (\{0,v\}^\perp)^c$ where $(\{0,v\}^\perp)^c$ is the complement of $\{0,v\}^\perp = \{y \in \mathbb{F}_2^n; v \cdot y = 0\}$.*

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 quadratic-like balanced.
If F is quadratic-like balanced, 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 [7, 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. [7, Proposition 55] and the few lines following this proposition). The second is a rephrasing of Lemma 1. □

The following example shows that this newly-introduced notion 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 quadratic-like permutation (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 quadratic-like balanced $(4,3)$-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.

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 $D_aF'(x) = F'(x+a) + F'(x) = L_1\big(F(A_2(x)+L_2(a)) + F(A_2(x))\big)$. Hence, $v \cdot D_aF'(x) = L_1^*(v) \cdot D_{L_2(a)}F(A_2(x))$, with L_1^* the adjoint linear operator of L_1, that is $v \cdot L_1(u) = L_1^*(v) \cdot u$ 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.*

Clearly, the notion 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 2. *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.*

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 *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, as quadratic-like balanced (n,m)-functions cannot exist when $m > n$, we have:

Proposition 3. (n,m)*-functions with* $m < n$ *do not satisfy the reversed quadratic-like property.*

Proof. Consider F an (n,m)-function. Set $\Delta(v) = \{a \in \mathbb{F}_2^n; v \cdot D_aF \equiv 1\}$ and $\Gamma(a) = \{v \in \mathbb{F}_2^m; v \cdot D_aF \equiv 1\}$. We have, by counting in two different ways the number of pairs (a,v) such that $v \cdot D_aF \equiv 1$, that $\sum_{v\neq 0} |\Delta(v)| = \sum_{a\neq 0} |\Gamma(a)|$. Assume that F satisfies the reversed quadratic-like property. Then for any $a \neq 0$, we have $|\Gamma(a)| \geq 1$. So $\sum_{v\neq 0} |\Delta(v)| = \sum_{a\neq 0} |\Gamma(a)| \geq (2^n - 1)$. On the other hand, the maximum value of $|\Delta(v)|$ is 2^{n-1}, since the set of those 1-linear structures of the Boolean function F_v is an affine space that is not a vector space. So, we have $2^n - 1 \leq \sum_{a\neq 0} |\Gamma(a)| = \sum_{v\neq 0} |\Delta(v)| \leq (2^m - 1)Max|\Delta(v)| \leq (2^m - 1)2^{n-1}$. Hence, $\frac{2^n-1}{2^{n-1}} \leq 2^m - 1$ and then $2^m - 1 \geq 2^{n-1} - 2^{-(n-1)}$, implying $2^m - 1 \geq 2^{n-1}$ (since it is the next closest integer), which in turn implies $2^m \geq 2^{n-1} + 1$, and therefore, $m \geq n$. □

Remark 3. *The reversed quadratic-like property does not imply balancedness. Indeed, balancedness is impossible for $m > n$, and functions satisfying the reversed quadratic-like property exist for every $m \geq n$. For instance, given an (n, m)-function F satisfying it, then we can construct an $(n, m+1)$-function $F' = [F||0]$ (where $||$ represents the concatenation), the last component being simply the zero function (or a constant function), such that F' satisfies the reversed quadratic-like property.*

Proposition 4. *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 reversed quadratic-like property. More generally, in the case of a quadratic-like balanced function, 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, there exists a* `cls` *map Γ and a nonzero $v \in \mathbb{F}_2^n$ such that $\Gamma(v) = a$.*

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

Remark 4. *If any derivative of an (n, n)-permutation F has for image set an affine space, then since this affine space does not include 0, it is included in the complement of a linear hyperplane and F satisfies then the reversed quadratic-like property.*

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 1. *For F a quadratic-like permutation, does F always satisfy the reversed quadratic-like property? What happens if F has degree 2?*

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

We consider now (n, n)-functions 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 equalities, for $a, v \neq 0$:

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

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

Proposition 5. *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 $tr_n(\lambda((x+1)^d + x^d))$ is constantly 1.*
3. *F satisfies the reversed quadratic-like property.*
4. *There exists a bijective `cls` map.*

Corollary 1. *All quadratic power permutations satisfy the reversed quadratic-like property with a bijective `cls` map.*

We further study this case, proving the following

Theorem 1. *The only power quadratic-like permutations are quadratic.*

Proof. We call 2-weight of an element of $\mathbb{Z}/(2^n-1)\mathbb{Z}$ the Hamming weight of the binary expansion of any of its representatives. Let x^d be a power permutation defined over $\mathbb{F}_{2^n}$ and assume it is quadratic-like. Recall that its algebraic degree equals the 2-weight of d. From Proposition 5, we have that there exists $\lambda \in \mathbb{F}_{2^n}$ such that $tr_n(\lambda((x+1)^d + x^d)) \equiv 1$. Let $I \subseteq \{0, \ldots, n-1\}$ be such that d has binary expansion $\sum_{i \in I} 2^i$ and let $\omega = |I|$ be the algebraic degree of $F(x) = x^d$. We assume that $\omega > 2$ (note that for $\omega = 2$, that is, when x^d is quadratic, we know that such (I, λ) exist and we know what they are; see e.g. [7]). In the following, we complete the proofs of Hertel-Pott [11] and Langevin-Veron [15], which addressed the case $\lambda = 1$, and so (for having $tr_n((x+1)^d + x^d) \equiv 1$) n odd, and they used it to characterize quadratic power functions (their result was then used by Kyureghyan [13] to show that power crooked functions are quadratic). We give all the necessary arguments and we generalize them to prove that this is never possible (i.e. we address the general case where λ is assumed to be any element and n has any parity).
For every $1 \leq k \leq \omega - 1$, the part of algebraic degree exactly k in $tr_n(\lambda((x+1)^d + x^d))$ equals the Boolean function $tr_n(\lambda \sum_{J \subset I; |J|=k} x^{\sum_{j \in J} 2^j})$. Denoting by R the (cyclotomic) equivalence relation "eRe' if there exists l such that $e' = 2^l e \pmod{2^n - 1}$", let us denote by $C_{i_1}, \ldots, C_{i_r}$ (where r is some positive integer and where $i_j \in C_{i_j}$) the corresponding equivalence classes in $\mathbb{Z}/(2^n-1)\mathbb{Z}$ (called cyclotomic classes of 2 modulo 2^n-1). Recall from e.g. [7] that there is existence and uniqueness of the representation of any n-variable Boolean function in the form $f(x) = \sum_{j=1}^{r} tr_{o(i_j)}(\beta_j x^{i_j}) + \beta_{2^n-1} x^{2^n-1}$, with $\begin{cases} \beta_j \in \mathbb{F}_{2^{o(i_j)}}, \\ \beta_{2^n-1} \in \mathbb{F}_2 \end{cases}$, where $o(i_j)$, the size of the cyclotomic class C_{i_j} containing i_j, divides n. We have

$\beta_j \in \mathbb{F}_{2^{o(i_j)}}$ because $\beta_j^{2^{o(i_j)}} = \beta_j$.
For every $k = 1, \ldots, \omega - 1$, we have then $tr_n(\lambda \sum_{J \subset I; |J|=k} x^{\sum_{j \in J} 2^j}) \equiv 0$, and for $k = 1$ we obtain that $tr_n(\lambda \sum_{j \in I} x^{2^j}) = tr_n((\sum_{j \in I} \lambda^{2^{-j}})x)$ is identically 0, which is equivalent to $\sum_{j \in I} \lambda^{2^{-j}} = 0$, and since $tr_n(\lambda) = 1$, this implies that $\omega = |I|$ is even.
For every $2 \leq k \leq \omega - 1$, let us denote by $C'_{k,i_1}, \ldots, C'_{k,i_r}$ the equivalence (sub)classes in the set $\{\sum_{j \in J} 2^j; J \subset I, |J| = k\}$ (note that all the elements in a class C_{i_j} have the same 2-weight, say, w_{i_j}, and all the C'_{k,i_j} with $k \neq w_{i_j}$ are empty). The (unique) univariate representation of $tr_n(\lambda(x^d + (x+1)^d))$ equals $\sum_{k=0}^{\omega-1} \sum_{j=1}^{r} tr_{o(i_j)}(tr^n_{o(i_j)}(\lambda \sum_{\alpha \in C'_{k,i_j}} x^\alpha))$.
Thanks to the property $tr^n_{o(i_j)}(u) = tr^n_{o(i_j)}(u^2)$, satisfied by all the functions $tr^n_{o(i_j)}$, each term $tr^n_{o(i_j)}(\lambda \sum_{\alpha \in C'_{k,i_j}} x^\alpha)$ in this sum can be written in the form $tr^n_{o(i_j)}((\sum_{\alpha \in C'_{k,i_j}} \lambda^{2^{\ell_\alpha}})x^{i_j})$ for some ℓ_α. By the uniqueness of the univariate representation, we have then $\sum_{\alpha \in C'_{k,i_j}} \lambda^{2^{\ell_\alpha}} = 0$ and since $tr_n(\lambda) = 1$, this implies $tr_n(\sum_{\alpha \in C'_{k,i_j}} \lambda^{2^{\ell_\alpha}}) = |C'_{k,i_j}| \pmod 2 = 0$, that is, C'_{k,i_j} has an even size.
Note that, by addition, for every $2 \leq k \leq \omega - 1$, $\sum_{j=1}^{r} |C'_{k,i_j}| = \binom{\omega}{k}$ is even, and since ω is also even, this is equivalent to the fact that $|I| = \omega$ is a power of 2, but we shall not use this.
- We first take $k = \omega - 1$. Consider an integer y such that $y \in C'_{\omega-1,i_j}$ for some j. Since $|C'_{\omega-1,i_j}|$ is even, then there exists a distinct $h \in C'_{\omega-1,i_j}$, $h \neq y$. Denote by Y and H the subsets of I (of size $\omega - 1$) such that $y = \sum_{j \in Y} 2^j$ and $h = \sum_{j \in H} 2^j$. Set t to be the smallest integer such that $y = 2^t h \pmod{2^n - 1}$. Hence it holds $Y = \{i \oplus t; i \in H\}$, where $\oplus$ is the sum in $\mathbb{Z}/n\mathbb{Z}$; we call $\tau : i \mapsto i \oplus t$ this translation, which is a 1-to-1 mapping from H to Y. The set $Z := H \cap Y$ has size $|Z| = \omega - 2$, and $H = Z \cup \{a\}$ and $Y = Z \cup \{b\}$ for some a, b. This implies that $I = Z \cup \{a, b\}$. Then we can construct a sequence $z_1 := a, z_2, \ldots, z_s := b$ such that $z_{i+1} := \tau(z_i) = z_i \oplus t$ for $1 \leq i \leq s - 1$. This is possible by hypothesis since $\tau(H) = \tau(Z \cup \{a\}) = Z \cup \{b\} = Y$. Indeed, taken any $c \in H$, either we construct a sequence $c_1, \ldots, c_\nu \in I$ with $c_1 := c$, $c_{i+1} := \tau(c_i)$ for $1 \leq i \leq \nu - 1$ and $c_\nu \notin H$, so $c_\nu = b$; or we construct an ultimately periodic sequence (the number of possible values in H being finite), that is, such that $c_\mu = \tau(c_\nu)$, for some $\mu < \nu$, and since τ is injective this implies $c_1 = \tau(c_{\nu-\mu+1})$, that is, the sequence is in fact periodic. Clearly, if we take $c = a$, we cannot be in the second case, since $a \notin Y$, so we can assume the existence of such a sequence $z_1, \ldots, z_s$ such that $z_1 = a, z_2, \ldots, z_s = b$. The only restriction on the integer s is $2 \leq s \leq \omega$. Notice that for $s = 2$ we have $b = \tau(a) = a \oplus t$, and for $s = \omega$ we have $I = \{z_1, \ldots, z_s\}$.

Set $J = I \setminus \{z_1, \ldots, z_s\}$, then

$$d = \sum_{i \in I} 2^i = \sum_{i=1}^{s} 2^{z_i} + \sum_{j \in J} 2^j = \sum_{i=0}^{s-1} 2^{a \oplus it} + \sum_{j \in J} 2^j.$$

We have:

$$\begin{aligned} H =& I \setminus \{b\} = \{z_1, \ldots, z_{s-1}\} \cup J, \\ \tau(H) =& \{\tau(z_1), \ldots, \tau(z_{s-1})\} \cup \tau(J) = \{z_2, \ldots, z_s\} \cup \tau(J), \\ =& Y = I \setminus \{a\} = \{z_2, \ldots, z_s\} \cup J; \end{aligned}$$

Hence, J is invariant under τ, that is $\tau(J) = J$. This implies $\sum_{j \in J} 2^j \equiv \sum_{j \in J} 2^{\tau(j)} \equiv 2^t \sum_{j \in J} 2^j \pmod{2^n - 1}$, so $(2^t - 1) \sum_{j \in J} 2^j \equiv 0 \pmod{2^n - 1}$. But since d is coprime with $2^n - 1$, we have that $(2^t - 1)d \not\equiv 0 \pmod{2^n - 1}$ and therefore $\tau(I) \neq I$, that is, $\tau(\{z_1, \ldots, z_s\}) \neq \{z_1, \ldots, z_s\}$; hence, $b \oplus t \neq a$ and then $t \neq n/2$.
- We now consider the case $k = 2$. Let j be such that $2^a + 2^{a+t} \in C'_{k,i_j}$. There are $s - 1$ shifts of the pair $\{a, a \oplus t\}$ (among which the pair itself) that are included in $\{z_1, \ldots, z_s\}$. And since $t \neq n/2$, we have that J contains $|J|$ other shifts of $\{a, a \oplus t\}$ (since each element c of J corresponds to a distinct pair $\{c, c + t\}$). Hence:

$$|C'_{k,i_j}| = s - 1 + |J| = \omega - 1.$$

We proved that ω is even, but also $|C'_{k,i_j}|$ is even for $2 \leq k \leq \omega - 1$. A contradiction. □

Note that Theorem 1 gives a more general result than the well-known one saying that the only crooked power permutations are quadratic (but on the other hand, it does not address crooked functions in a generalized sense, which are not balanced).

Remark 5. *Since for power permutations, quadratic-like bijectivity and reversed quadratic-like property are equivalent, we have the same negative result for power functions about 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.

4.1 Feistel permutations and generalizations

Proposition 6. *(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 quadratic-like permutation 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 $v_2 \neq 0$ and a_2 is any element satisfying $v_1 \cdot a_2 = 1$ if $v_1 \neq 0$, and where δ_0 is the Dirac (or Kronecker) symbol (whose value equals 1 at 0 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 quadratic-like permutations with their `cls` *maps defined similarly.*
(iii) Still more generally, let G be any quadratic-like balanced $(n - r, m - r)$-function, the function

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

is a quadratic-like balanced (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 $v = (v_1, v_2) \neq (0, 0)$ 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 $v_2 \neq 0$, then $a = (a_1, 0)$ such that $v_2 \cdot a_1 = 1$ satisfies $D_a(v \cdot F) \equiv 1$, and if $v_2 = 0$ then $v_1 \neq 0$ and we can take $a = (0, a_2)$ 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 $v_2 = 0$ and $v_1 \neq 0$. □

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

We still call Feistel the generalized form of permutations given in Proposition 6 (ii). We shall not call Feistel the functions in Proposition 6 (iii), because (iii) is a secondary construction of quadratic-like balanced 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.

When we shall give constructions of quadratic-like permutations, we will need to determine whether some of the constructed functions are outside the class of those permutations that are affine equivalent to Feistel permutations. This will be ensured when they do not satisfy the reversed quadratic-like property, thanks to the following proposition, which has its own interest.

Proposition 7. *A Feistel permutation satisfies the reversed quadratic-like property.*

Proof. Take a Feistel permutation $F(x, y) = (y, x + \phi(y))$, then the derivative in direction $a = (a_1, a_2)$ of the component $v = (v_1, v_2)$ 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 $a = (a_1, 0)$ does not pose any problem. Instead, if $a_2 \neq 0$, we can take $v_2 = 0$ and v_1 such that $v_1 \cdot a_2 = 1$. This proves the reversed quadratic-like property for the Feistel permutation. □

If all the functions we shall construct satisfy the reversed quadratic-like property, we shall need another way of ensuring that some of the constructed functions lie outside the class of those permutations that are affine equivalent to Feistel permutations. The following result provides such a way, and has additionally the interest of characterizing those permutations which are affine equivalent to the generalized Feistel permutations described in Proposition 6 (*iii*), and of showing that these are affine equivalent to those particular permutations described in this same Proposition 6 (*iii*) with $r = 1$:

Proposition 8. *A quadratic-like balanced map $F : \mathbb{F}_2^n \to \mathbb{F}_2^m$ is affine equivalent to a map as in Equation* (2) *if and only if there exists some nonzero direction a such that D_aF is constant and nonzero.*

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 (2), then $D_{(a_1,0)}F(x, y)$ equals $(0, a_1)$ 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 $L(b) = e_m$. For $G = L \circ F$ 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

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

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 quadratic-like balanced, G' is also quadratic-like balanced. Hence, G is as in Equation (2), 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 quadratic-like permutation 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 [10]: 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, since the notion has been later generalized, see e.g. [7]), 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 $\{0, \pi_F(a)\}^\perp$ where π_F (sometimes called the *orthoderivative* of F) is some function from $\mathbb{F}_2^n \setminus \{0\}$ to itself.
Note that the existence of non-quadratic crooked functions is an open problem.

Proposition 9. *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.*

Indeed, we know from [1] that both F and the orthoderivative are permutations, and we have that $v = \pi_F(a)$ is 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.

The converse of the above proposition is true in the class of APN functions. First we provide a result on quadratic-like APN permutations.

Proposition 10. *If F is an APN quadratic-like permutation, then it satisfies the reversed quadratic-like property. Moreover, there exists one and only one* `cls` *map for F, which is itself a permutation.*

Proof. First, recall that an APN permutation cannot have a derivative in a nonzero direction having a zero component (this result was used in [4] 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 $v \cdot D_aF(x) = 0$, 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 $\chi \in \mathbb{F}_2^n$ such that $D_aF(\chi) = 0_n$, 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 Γ can be injective (since it is not surjective). Hence, there must exist distinct nonzero directions v_1, v_2 such that $\Gamma(v_1) = \Gamma(v_2) = b$, for some nonzero $b \in \mathbb{F}_2^n$. So it holds $v_1 \cdot D_bF(x) = v_2 \cdot D_bF(x) \equiv 1$, implying $(v_1 + v_2) \cdot D_bF(x) = 0$, 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. □

The above proposition shows that every quadratic-like APN permutation is crooked. Indeed, for every nonzero a there exists v such that $v \cdot D_aF = 1$, so D_aF is valued in the complement of $\{0, v\}^\perp$, and then (since F is APN) its image set equals this complement. Hence the following result.

Proposition 11. *Given F an APN permutation, then F is quadratic-like if and only if F is crooked (in the strict sense of [1]).*

Remark 6. *The APN permutation in dimension 6 given in Ref. [3] is not quadratic-like. 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, 13].

4.3 Strongly plateaued balanced functions

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 [5]) 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 $W_{F_v}(0) = W_{f_v}(0)W_{\ell_v}(0)$ and since $W_{f_v}(0) \neq 0$, 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, combined with Remark 4 and [7, Proposition 107].

Proposition 12. *All strongly plateaued balanced functions are quadratic-like. Moreover, strongly plateaued permutations satisfy the reversed quadratic-like property.*

Remark 7. *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 single amplitude since they are AB) and not quadratic-like (since not crooked, and/or since non-quadratic power functions).*

5 Constructions

We are interested in constructing quadratic-like balanced functions of degree greater than 2 and being not Feistel nor strongly plateaued. Notice that Proposition 6 (*iii*) provides already an iterative construction method of quadratic-like balanced maps. For example, the permutation F_1 displayed in Example 1 can be obtained this way.

We continue with two trivial constructions, obtained by either shortening the output space, or enlarging the input space of a quadratic-like balanced map.

Remark 8. *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 9. *There is an obvious secondary construction of quadratic-like balanced functions:*
Let F be any quadratic-like balanced (n, m)-function, G any quadratic-like balanced (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 quadratic-like balanced $(n+r, m+s)$-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 $(v, w) \cdot D_{(a,b)}\mathcal{F}(x, y) = v \cdot D_a F(x) + w \cdot D_b G(y) + w \cdot D_a H(x)$. We assume $(v, w) \neq (0, 0)$. If $w = 0$ then $v \neq 0$ and we can take a such that $v \cdot D_a F \equiv 1$, If $w \neq 0$ we can take a=0 and b such that $w \cdot D_b G \equiv 1$.

Similarly, let F be any quadratic-like balanced (n, m)-function, G any quadratic-like balanced (r, s)-function 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 quadratic-like balanced $(n + r, m + s)$-function.

We present another method providing quadratic-like balanced maps. In the two constructions below (Propositions 13 and 14), 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 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 13. *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 $tr_m(c) = 1$. 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 $a_2 = 0$ 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 10. *There is some similarity between the function $(x, y) \mapsto x + \phi(y)$ involved in Feistel permutations (that is balanced and moreover quadratic-like balanced) and the function $(x, y) \mapsto x\phi(y)$ in Proposition 13. 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 quadratic-like balanced function.*

We can deduce a construction of quadratic-like permutations as follows.

Proposition 14. *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 $\mathbb{F}_2^{n-m}$ (or to $\mathbb{F}_{2^{n-m}}$ if the reader prefers) that is a quadratic-like permutation.*
Then the (n, n)-function $F : (x, y) \mapsto (x\phi(y), \varphi(y))$ is a quadratic-like permutation.

Proof. Consider a nonzero $(v_1, v_2) \in \mathbb{F}_{2^m} \times \mathbb{F}_{2^m}$. If $v_1 \neq 0$, we take $a_2 = 0$ and the derivative at direction $a = (a_1, 0)$ of $tr_m(v_1x\phi(y) + v_2\varphi(y))$ equals $tr_m(v_1a_1\phi(y))$ and we can finish as in the proof of Proposition 13. If $v_1 = 0$ (and $v_2 \neq 0$) then we take $a_1 = 0$ and the derivative at direction $a = (0, a_2)$ of $tr_m(v_1x\phi(y) + v_2\varphi(y))$ equals $tr_m(v_2D_{a_2}\varphi(y))$. By the hypothesis on φ, we know that there exists a_2 such that $tr_m(v'D_{a_2}\varphi(y)) \equiv 1$. □

Note that such quadratic-like permutations are non-quadratic when ψ is non-affine (or φ is non-quadratic). In a stronger way, the image sets of some derivatives $D_{(a_1,a_2)}F(x, y) = (xD_{a_2}\phi(y) + a_1\phi(y + a_2), D_{a_2}\varphi(y))$ may have maximum rank (i.e. rank n), assuming this is true for φ, and so, by induction.
The functions in Proposition 14 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 $(a_1, a_2) \neq (0, 0)$, when ϕ has no zero derivative in a nonzero direction, because if $a_2 \neq 0$, then $xD_{a_2}\phi(y) + a_1\phi(y + a_2)$ is non-constant whatever is a_1, and if $a_2 = 0$ (and $a_1 \neq 0$), $a_1\phi(y + a_2) = a_1\phi(y)$ is not constant since ϕ is not constant.
Note also that the functions in Proposition 14 may have the reversed quadratic-like property, for instance when ψ (and then ϕ) is constant and φ is quadratic, since we can take $v = (a_1^{-1}, 0)$ if $a_1 \neq 0$ and $v = (0, v_2)$ where v_2 is orthogonal to the direction of the image set of $D_{a_2}\phi$ if $a_1 = 0$; and it may not have the reversed quadratic-like property (for instance when ϕ is constant and the image set of some derivative of φ has maximum rank $n - m$).

5.1 A construction in ANF form

Starting from the quadratic-like permutation of Example 2, we provide a (iterative) construction of quadratic-like permutations not equivalent to Feistel permutation and of degree up to $n/2+1$.

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

$$F(x,y) = \begin{bmatrix} F_1(x,y) \\ F_2(x,y) \end{bmatrix} = \begin{bmatrix} (g(y)(A+B)+A) \star x \\ y \end{bmatrix}, \tag{3}$$

where we can write

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

Notice that the (cubic) quadratic-like permutation in Example 2 is such that $x = (x_1, x_2)$, $y = (x_3, x_4)$, $g(y) = x_3x_4$, $A = \begin{bmatrix} 1 & 0 \\ 1 & 1 \end{bmatrix}$ and $B = A^T$.

To study the quadratic-like permutation property for F as in (3), we take any nonzero $(v, w) \in \mathbb{F}_2^m \times \mathbb{F}_2^m$. If $v = 0$ then for $d \in \mathbb{F}_2^m$ such that $d \cdot w = 1$ we have $(v, w) \cdot D_{(0,d)}F = 1$. Assume now $v \neq 0$.

$$v \cdot F_1(x,y) = g(y) \sum_{i=1}^m v_i \sum_{k=1}^m (a_{ik}+b_{ik})x_k + \sum_{i=1}^m v_i \sum_{k=1}^m a_{ik}x_k$$

Then, for $(c, d) \in \mathbb{F}_2^m \times \mathbb{F}_2^m$ we have

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

Hence we want c such that $c \cdot (A^T \star v) = 1$ and $c \cdot (B^T \star v) = 1$. 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 there exists c such that $c \cdot u_1 = c \cdot u_2 = 1$. With such c we have $(v, w) \cdot D_{(c,0)}F = 1$. This proves that F is quadratic-like permutation.

To study the equivalence to a Feistel permutation, we need to verify whether there exists a direction (c, b) such that $D_{(c,b)}F$ is constant. The derivative for F_1 equals

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

and for being constant, we would need $a_{ik} + b_{ik} = 0$ for every i and for every k. Hence by taking A and B distinct, and g non-constant, we know that F can never have a constant derivative.

To study the reversed quadratic-like property, we consider the derivative in any nonzero direction (c, b). If $b \neq 0$ then by taking $(0, w)$ such that $w \cdot b = 1$, we have $(0, w) \cdot D_{(c,b)}F(x, y) = w \cdot b = 1$. Otherwise, if $b = 0$ then by taking v such that $v \cdot (A^T \star c) = v \cdot (B^T \star c) = 1$ we have $(v, 0) \cdot D_{(c,0)}F(x, y) = v \cdot D_{(c,0)}F_1(x, y) = 1$.

Notice that this construction can be generalized with $F_2(x, y) = H(y)$ quadratic-like permutation over $\mathbb{F}_2^m$. The generalized construction still satisfies the studied properties (quadratic-like permutation not equivalent to Feistel), and it satisfies the reversed quadratic-like property if H satisfies the reversed quadratic-like property.

This analysis is summarized in the following result.

Proposition 15. *For $n = 2m$ with $m > 2$, consider $g : \mathbb{F}_2^m \to \mathbb{F}_2$ any (non-constant) Boolean function and $H : \mathbb{F}_2^m \to \mathbb{F}_2^m$ a quadratic-like permutation. Take A, B any two distinct invertible $m \times m$ 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 $x, y \in \mathbb{F}_2^m$ is a quadratic-like permutation not equivalent to Feistel. With $\star$ we denote the product between matrices (of compatible dimensions). Moreover, F satisfies the reversed quadratic-like property if H satisfies the reversed quadratic-like property.

5.2 From Maiorana-McFarland bent maps

We recall a notion introduced in [9]:
An n-variable Boolean function f is *cubic-like bent* if for any nonzero $a \in \mathbb{F}_2^n$ there exists $b \in \mathbb{F}_2^n$ such that $D_a D_b f \equiv 1$. There is a strong connection between Maiorana-McFarland cubic-like bent functions and quadratic-like permutations:

Proposition 16. *Consider $f : \mathbb{F}_2^n \times \mathbb{F}_2^n \to \mathbb{F}_2$ a Maiorana-McFarland map $f(x, y) = x \cdot \pi(y) + g(y)$, with $x, y \in \mathbb{F}_2^n$, $\pi : \mathbb{F}_2^n \to \mathbb{F}_2^n$ and $g : \mathbb{F}_2^n \to \mathbb{F}_2$. If f is cubic-like bent, then π is a quadratic-like permutation. Moreover, if $g = 0$, then π satisfies also the reversed quadratic-like property.*

Proof. This follows from Proposition 14 and Proposition 9 of the work on cubic-like bent maps, [9]. □

Remark 11. *From the analysis presented in [9], we have that over $\mathbb{F}_2^4$ all the quadratic-like permutations satisfy also the reversed quadratic-like property.*

6 The Walsh transform 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. [7, Proposition 29]), there is a straightforward characterization of quadratic-like balanced functions by their Walsh transform. We give it in the next proposition. For our paper to be self-contained, we give a proof.

Proposition 17. *Consider any (n,m)-function $F:\mathbb{F}_2^n\to\mathbb{F}_2^m$, where n and m are two positive integers.*
F is quadratic-like balanced (resp., has the reversed quadratic-like property) if and only if, for every nonzero $v\in\mathbb{F}_2^n$, there exists $a_v\in\mathbb{F}_2^m$ (resp., for every nonzero $a\in\mathbb{F}_2^m$, there exists $v_a\in\mathbb{F}_2^n$) such that the function $u\mapsto W_F(u,v)$ vanishes on the linear hyperplane $\{0,a_v\}^\perp$ (resp., the function $u\mapsto W_F(u,v_a)$ vanishes on the linear hyperplane $\{0,a\}^\perp$).

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

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

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 $\{0,a\}^\perp$, 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 $D_aF_v(x)\equiv 1$, according to the Parseval relation. □

Remark 12. *This allows to show again that almost bent quadratic-like permutations are crooked (which is known by Proposition 11). Indeed, thanks to the Parseval relation, we know that for any almost bent (n,n)-function F and for every $v\neq 0$, 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 $\{0,a_v\}^\perp$. 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 $D_0F_v\equiv 0$ and $D_{a_v}F_v\equiv 1$, which we knew already, but also that for every $a\notin\{0,a_v\}$, the derivative D_aF_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.*

7 The ANF of a quadratic-like permutation

Consider $F : \mathbb{F}_2^n \to \mathbb{F}_2^n$ a quadratic-like permutation and $\phi : \mathbb{F}_2^n \to \mathbb{F}_2^n$ a `cls` map for F, with $\phi(0) = 0$.

For an integer k $(1 \leq k \leq n)$ we say that F satisfies the property (P_k) if ϕ sends a set of k linearly independent elements into linearly independent elements. Then, up to apply an affine transformation, we can assume $\phi(e_i) = e_i$ so $F_i(x) = e_i \cdot F(x) = f_i(x_1, \ldots, x_{i-1}, x_{i+1}, \ldots, x_n) + x_i$, for $i = 1, \ldots, k$.

Clearly, if F satisfies the property (P_k) for some positive $k > 1$ integers, then it also satisfies the property (P_{k-1}).

Remark 13. *Consider $F : \mathbb{F}_2^n \to \mathbb{F}_2^n$ a quadratic-like permutation. If there exists a linear bijection ϕ that is a `cls` map for F, then F satisfies the property (P_n). This implies that, up to affine equivalence, we can assume ϕ to be the identity, so that for any nonzero $v \in \mathbb{F}_2^n$ it holds $v \cdot D_v F(x) \equiv 1$. Notice that this function exists for $n \leq 3$. Indeed, up to affine transformation, for dimensions $n = 1, 2, 3$ we have*

$$F(x_1) = \begin{bmatrix} x_1 \end{bmatrix}, \; F(x_1, x_2) = \begin{bmatrix} x_1 \\ x_1 + x_2 \end{bmatrix}, \; F(x_1, x_2, x_3) = \begin{bmatrix} x_1 + x_2 x_3 \\ x_1 + x_2 + x_1 x_3 \\ x_1 + x_2 + x_3 + x_1 x_2 \end{bmatrix}.$$

Instead, for $n \geq 4$, no quadratic-like permutation admits such a linear ϕ. The proof of this last statement is quite techincal, so we leave it in the Appendix, see A.1.

Even without assuming the existence of such a linear `cls` map ϕ, we still have that a quadratic-like permutation F satisfies property (P_k) for some $k \geq 3$, see the following proposition. We leave the proof in the appendix, given its length and technicality, see A.2.

Proposition 18. *For $n \geq 3$ consider $F : \mathbb{F}_2^n \to \mathbb{F}_2^n$ a quadratic-like permutation, then F satisfies property (P_3). This means that, up to affine equivalence, the function has the following form*

$$F(x_1, \ldots, x_n) = \begin{bmatrix} f_1(x_2, \ldots, x_n) + x_1 \\ f_2(x_1, x_3, \ldots, x_n) + x_2 \\ f_3(x_1, x_2, x_4, \ldots, x_n) + x_3 \\ F_4(x_1, \ldots, x_n) \\ \vdots \\ F_n(x_1, \ldots, x_n) \end{bmatrix},$$

with $f_i : \mathbb{F}_2^{n-1} \to \mathbb{F}_2$.

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] M. Calderini, M. Sala, and I. Villa. A note on APN permutations in even dimension. Finite Field and their Applications, 2017.

[5] 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.

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

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

[8] 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.

[9] C. Carlet, I. Villa. On cubic-like bent Boolean functions. Cryptology ePrint Archive, Paper 2023/879, 2023.

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

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

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

[13] G. M. Kyureghyan, The only crooked power functions are $x2^k + 2^l$. European Journal of Combinatorics 28 (4), pp. 1345-1350, 2007.

[14] 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.

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

A Some proofs

A.1 Proof of Remark 13

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.

A.2 Proof of Proposition 18

To ease the reasoning, when we talk about valid directions for a component function F_v, we refer to those elements a such that $D_aF_v \equiv 1$. Moreover, to ease the notation, with g^i we denote a Boolean function in which the variable x_i does not play any role, and with $g^{i,j}$ we have that both variables x_i, x_j do not play a role.

The aim is to write the coordinates as $F_i(x) = f_i(x_1, \ldots, x_{i-1}, x_{i+1}, \ldots, x_n) + x_i$. Before starting, we recall how to apply a linear transformation in order to move from a valid direction a to a valid direction e_j, where e_j is the j-th element in the canonical base of $\mathbb{F}_2^n$. Consider $a = \sum_{i=1}^n \lambda_i e_i$ with $\lambda_j \neq 0$ for a j, and then consider the linear bijection L sending

$x_j \to x_j$ and $x_i \to x_i + \lambda_i x_j$ for $i = 1, \dots, n$, $i \neq j$. Notice that $L(e_j) = a$. Then consider the linear equivalent map $G = F \circ L$, it then holds $D_{e_j} G_v(x) = v \cdot (G(x + e_j) + G(x)) = v \cdot (F(L(x) + L(e_j)) + F(L(x))) = v \cdot D_a F(L(x)) \equiv 1$, as claimed. This implies that $G_v(x) = f_v^j(x) + x_j$. Moreover, notice that if F has already the first t coordinates as $f_i^i + x_i$ for $i = 1, \dots, t$, then if $j > t$, applying the above mentioned linear transformation will not change the form of the first t components.

The case $i = 1$ can be easily assumed valid, up to applying an affine transformation, and so $F_1(x) = f_1^1 + x_1$.

For $i = 2$, if there is a valid direction $a = \sum_{i=1}^n \lambda_i e_i$ with $\lambda_j \neq 0$ for a $j > 1$, then we apply the above mentioned linear transformation, we swap the variables x_2 and x_j, and we obtain F_2 as in the statement. Otherwise, assume that the only valid direction for F_2 is e_1, and so $F_2(x) = f_2^1 + x_1$. Then, for $F_1 + F_2 = f_1^1 + f_2^1$ we need a valid direction, which clearly is different from e_1. So, up to apply the mentioned linear transformation, we can assume that e_2 is a valid direction for $F_1 + F_2$ and we can replace $F_2 := F_1 + F_2$, leading to $F_2(x) = f_2^2 + x_2$.

Consider the case $i = 3$. If F_3 admits a valid direction $a = \sum_{i=1}^n \lambda_i e_i$ with $\lambda_j \neq 0$ for a $j > 2$, then we apply the above mentioned linear transformation, we swap the variables x_3 and x_j, and we obtain F_3 as in the statement. Moreover, if one among the components $F_1 + F_3$, $F_2 + F_3$, $F_1 + F_2 + F_3$ admits a valid direction $\sum_{i=1}^n \lambda_i e_i$ with $\lambda_j \neq 0$ for a $j \geq 3$, then we can perform the mentioned linear transformation and replace the coordinate F_3 with that component.

Hence we are left with the case that any component of the form $\eta F_1 + \nu F_2 + F_3$ has valid directions of the form $e_1, e_2, e_1 + e_2$.

- Assume e_1 is a valid direction for F_3, hence $F_3 = x_1 + f_3^1$. Consider $F_1 + F_3 = f_1^1 + f_3^1$. Clearly, e_2 must be a valid direction of $F_1 + F_3$, so $f_1^1 + f_3^1 = x_2 + h^{12}$. Then, for $F_1 + F_2 + F_3 = h^{12} + f_2^2$ it holds that e_1 is a valid direction, and so $f_2^2 = x_1 + f_2^{12}$. We proceed with $F_2 + F_3 = f_2^{12} + f_1^1 + h^{12}$ where e_2 is a valid direction, so $f_1^1 = x_2 + f_1^{12}$, but with this we have that $F_1 + F_2 = f_1^{12} + f_2^{12}$ admits a possible direction not in $\langle e_1, e_2 \rangle$, so with applying the mentioned linear transformation for $F_1 + F_2$ and with the final replacement, $F_1 := F_3$, $F_3 := F_1 + F_2$ we are done.
  The case e_2 is analogue to the previous one, so we do not need to analyse it.
- Assume $e_1 + e_2$ is a valid direction for F_3, but e_1, e_2 are not. Without loss of generality up to swapping the role of x_1 and x_2, we have $F_3 = x_1 + (x_1 + x_2)h^{12} + f_3^{12}$, with $h^{12} \neq 0, 1$. Let us write $F_1 = x_1 + x_2 g_1^{12} + f_1^{12}$ and $F_2 = x_2 + x_1 g_2^{12} + f_2^{12}$. Then, for $F_1 + F_3 = x_2 g_1^{12} + f_1^{12} + (x_1 + x_2)h^{12} + f_3^{12}$, the only possible valid direction are $e_2, e_1 + e_2$. For $F_2 + F_3 = x_1 g_2^{12} + f_2^{12} + (x_1 + x_2)(h^{12} + 1) + f_3^{12}$ the only possible valid directions are $e_1, e_1 + e_2$.
  - If a valid direction for $F_1 + F_3$ is e_2 and a valid direction for $F_2 + F_3$ is e_1, then $g_1^{12} + h^{12} \equiv 1$ and $g_2^{12} + h^{12} = 0$. In this case, $F_1 + F_2 + F_3 = f_1^{12} + f_2^{12} + f_3^{12}$
  - If a valid direction for $F_1 + F_3$ is e_2 and a valid direction for $F_2 + F_3$ is $e_1 + e_2$, then $g_1^{12} + h^{12} \equiv 1$ and $g_2^{12} \equiv 1$. In this case, $F_1 + F_2 + F_3 = f_1^{12} + x_1 + f_2^{12} + x_1 h^{12} + f_3^{12}$
  - If a valid direction for $F_1 + F_3$ is $e_1 + e_2$ and a valid direction for $F_2 + F_3$ is e_1, then $g_1^{12} \equiv 1$ and $g_2^{12} + h^{12} = 0$. In this case, $F_1 + F_2 + F_3 = f_1^{12} + f_2^{12} + x_2 h^{12} + f_3^{12}$
  - If a valid direction for $F_1 + F_3$ is $e_1 + e_2$ and a valid direction for $F_2 + F_3$ is $e_1 + e_2$, then $g_1^{12} \equiv 1$ and $g_2^{12} \equiv 1$. In this case, $F_1 + F_2 + F_3 = f_1^{12} + x_1 + f_2^{12} + (x_1 + x_2)h^{12} + f_3^{12}$

  For the first three cases, clearly $F_1 + F_2 + F_3$ has an admissible direction with $\lambda_j \neq 0$ for a $j \geq 3$. Also the last case works since $F_1 + F_2 = f_1^{12} + f_2^{12}$ and this situation has been already analysed in the previous item.

This concludes the proof since, up to a linear transformation, we have $F_3 = f_3^3 + x_3$.