Trims and extensions of quadratic APN functions

Christof Beierle[1] · **Gregor Leander**[1] · **Léo Perrin**[2]

Abstract
In this work, we study functions that can be obtained by restricting a vectorial Boolean function $F\colon \mathbb{F}_2^n \to \mathbb{F}_2^n$ to an affine hyperplane of dimension $n-1$ and then projecting the output to an $n-1$-dimensional space. We show that a multiset of $2 \cdot (2^n - 1)^2$ EA-equivalence classes of such restrictions defines an EA-invariant for vectorial Boolean functions on $\mathbb{F}_2^n$. Further, for all of the known quadratic APN functions in dimension $n < 10$, we determine the restrictions that are also APN. Moreover, we construct 6368 new quadratic APN functions in dimension eight up to EA-equivalence by extending a quadratic APN function in dimension seven. A special focus of this work is on quadratic APN functions with maximum linearity. In particular, we characterize a quadratic APN function $F\colon \mathbb{F}_2^n \to \mathbb{F}_2^n$ with linearity of 2^{n-1} by a property of the ortho-derivative of its restriction to a linear hyperplane. Using the fact that all quadratic APN functions in dimension seven are classified, we are able to obtain a classification of all quadratic 8-bit APN functions with linearity 2^7 up to EA-equivalence.

Keywords Almost perfect nonlinear · EA-equivalence · EA-invariant · Linearity · Restriction · Extension

Mathematics Subject Classification 06E30 · 94A60

1 Introduction

Let us be given two integers $n, m \in \mathbb{N}$ with $m < n$ and two vectorial Boolean functions $F\colon \mathbb{F}_2^n \to \mathbb{F}_2^n$ and $G\colon \mathbb{F}_2^m \to \mathbb{F}_2^m$. We say that F is an *extension* of G and that G is a

✉ Christof Beierle
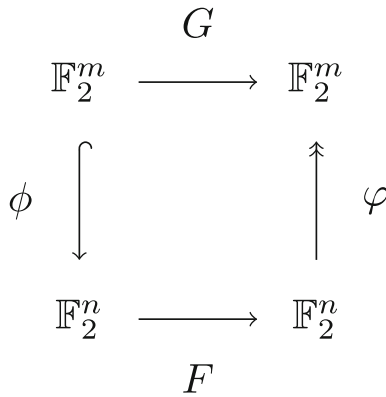   christof.beierle@rub.de

   Gregor Leander
   gregor.leander@rub.de

   Léo Perrin
   leo.perrin@inria.fr

1   Ruhr University Bochum, Bochum, Germany

2   Inria, Paris, France

restriction of F, denoted $G \prec F$, if there exists an affine injective mapping $\phi : \mathbb{F}_2^m \to \mathbb{F}_2^n$ and an affine surjection $\varphi : \mathbb{F}_2^n \to \mathbb{F}_2^m$ such that $G = \varphi \circ F \circ \phi$.

$$
\begin{array}{ccc}
 & G & \\
\mathbb{F}_2^m & \longrightarrow & \mathbb{F}_2^m \\
\phi \Big\downarrow & & \Big\uparrow \varphi \\
\mathbb{F}_2^n & \longrightarrow & \mathbb{F}_2^n \\
 & F &
\end{array}
$$

While the definition is sound for any vectorial Boolean functions F and G, we are mainly interested in the case where F and G are both APN functions.

In the remainder of this work, we concentrate on the case of $m = n - 1$, but let us recall first that there are well-known examples for APN restrictions, resp., APN extensions. Indeed, given an APN monomial function F on $\mathbb{F}_{2^n}$, then the restriction G of F to any proper subfield of $\mathbb{F}_{2^n}$ is APN.

The notion of restriction defines a strict partial ordering on the set of vectorial Boolean functions with the same dimension in the input and the output. Indeed the relation is irreflexive, as no function is its own extension simply as we exclude the case $n = m$ by requiring $m < n$. For the same reason, the relation is antisymmetric, i.e. no function can be both an extension and a restriction of any given function. Transitivity follows directly from the definition.

The notion of restriction for vectorial Boolean functions also defines a notion of restriction on EA-equivalence classes of vectorial Boolean functions. We say that the EA-equivalence class of F is the *extension* of the EA-equivalence class of G if there exist a function G' which is EA-equivalent to G such that $G' \prec F$. This is well-defined as, given two EA-equivalent functions F and F' and a function G that is the restriction of F, then there exists an EA-equivalent function G' to G such that G' is the restriction of F'.

As mentioned above, we only focus on the case $m = n - 1$, that is extensions and restrictions by adding or removing only a single dimension. One question is how to algorithmically check for a given APN function whether it is an extension or a restriction of another APN function and whether we can discover new APN functions as extensions or restrictions of known functions. In Sect. 3, we define an operation called *trimming*, which restricts a vectorial Boolean function F on $\mathbb{F}_2^n$ to a linear or affine hyperplane of dimension $n - 1$ and then projects the output to an $n - 1$-dimensional space by discarding one *component* function. Compared to the case in which only a *coordinate* is discarded, we show that this operation is sound in the sense that (1), any function on $\mathbb{F}_2^{n-1}$ that is a restriction of F is EA-equivalent to a trim of F and, (2), EA-equivalent functions yield EA-equivalent trims when considering all $2 \cdot (2^n - 1)^2$ possibilities to choose the affine hyperplanes and the component functions. This way, we obtain an EA-invariant, which we call *trim spectrum*. We then analyze how many of the known quadratic APN functions in dimensions $n < 10$ contain APN restrictions. The results are visualized in a so-called *trimming graph*, see Figs. 1 and 2.

For constructing new APN functions that have a given APN function as a restriction, the focus on EA-equivalence classes is helpful as, in a nutshell, extending a function by one

dimension boils down to constructing one additional coordinate function and deducing the values for the remaining input values. More precisely, an APN function G on $\mathbb{F}_2^n$ is a restriction of an APN function in dimension $n + 1$ if there exist Boolean functions $r_1, r_2 : \mathbb{F}_2^n \to \mathbb{F}_2$ and a vectorial Boolean function $G' : \mathbb{F}_2^n \to \mathbb{F}_2^n$ such that

$$
T : \begin{cases} \mathbb{F}_2^n \times \mathbb{F}_2 & \to \mathbb{F}_2^n \times \mathbb{F}_2 \\ \begin{pmatrix} x \\ y \end{pmatrix} & \mapsto \begin{pmatrix} G(x) \\ r_1(x) \end{pmatrix} \cdot (y + 1) + \begin{pmatrix} G'(x) \\ r_2(x) \end{pmatrix} \cdot y \end{cases} \tag{1}
$$

is APN. While for very small dimensions it is possible to check if a function G is an APN restriction of some function, this becomes prohibitively expensive as n increases. However, focusing on quadratic functions for T and G allows for much stronger results. As we will detail in Sect. 4, in the case where we want to determine if a given quadratic APN function G is a restriction of a quadratic APN function T, the function G' differs from G itself only by a linear mapping L and r_2 differs by a linear Boolean function ℓ from r_1. This, obviously, reduces the search space significantly. By using a recursive tree search with backtracking, we are able to construct 6,368 new quadratic APN functions in dimension $n = 8$ up to EA-equivalence. Those new functions are APN extensions of quadratic 7-bit APN functions by construction and it is worth remarking that the vast majority of the previously-known APN functions in dimension $n = 8$ are not, i.e., they do not have APN functions within their trim spectrum. As we found out that almost all of the quadratic APN functions in dimension $n = 7$ can be extended to quadratic APN functions in dimension $n = 8$, we conjecture that for each dimension n, there exist APN functions $F_i : \mathbb{F}_2^i \to \mathbb{F}_2^i, i = 2, \ldots, n$ such that $F_2 \prec F_3 \prec \cdots \prec F_{n-1} \prec F_n$, so called *recursive APN functions*.

For APN functions in the form of Eq. (1), the case where T is quadratic and r_1 is constant and equal to zero is of particular interest. Indeed, as it was already observed in [13, Remark 12], any quadratic APN function on $\mathbb{F}_2^n$ with linearity 2^{n-1}, i.e., the highest possible linearity of a quadratic APN function, is EA-equivalent to the extension T of a quadratic APN function G with choosing $r_1 = 0$ [as in the form of Eq. (1)]. Moreover, we show that for the ortho-derivative π_G of G, we have $\langle \pi_G(\alpha), L(\alpha) \rangle = 1$ for all $\alpha \in \mathbb{F}_2^n \setminus \{0\}$ with $\ell(\alpha) = 0$. This observation allows us in particular to classify all quadratic APN functions with maximum linearity in dimension eight, simply by using the recent classification of all quadratic 7-bit APN functions into EA-equivalence classes and by recovering L from the ortho-derivative of G using linear algebra.

In the last part of this paper, we provide some further observations on quadratic APN functions with maximum linearity. In particular, we provide a simple representation of those functions and study their Walsh spectra, as well as their ortho-derivatives. We conclude by listing several open problems for future work.

1.1 Related work

The effect on the differential uniformity and on the linearity of restricting a vectorial Boolean function to an affine subspace was first studied in [23]. Restrictions of APN functions that are obtained by discarding one output coordinate have also been studied before, see [18,19].

APN functions are completely classified up to $n \leq 5$, see [6]. For $n = 6, 7$, we know a complete classification of quadratic and cubic, and quadratic APN functions up to EA-equivalence, respectively [11,20,21]. For $n = 8$, at the time of submission of this manuscript in August 2021, we know 26,524 distinct quadratic APN functions up to EA-equivalence.

Those are the ones listed by Edel and Pott [17] in 2009, the 10 functions constructed in [28], the 8,157 functions found by the QAM approach in 2014 [31,32], the two functions coming from the Taniguchi family [27], the 12,921 functions found by the recursive tree search utilizing linear self-equivalences [2], and the 5,412 functions found by the QAM approach very recently [30]. The authors of [30] conjectured that there are more than 50,000 distinct quadratic APN functions in dimension $n = 8$ up to EA-equivalence.

One interesting result reported in [2] is the fact that, among the 12,921 found APN functions in dimension $n = 8$, four of them have a linearity of 2^{n-1}, which is the highest value that can possibly be achieved for quadratic APN functions. Note that for $n \leq 4$, every quadratic APN function admits a linearity of 2^{n-1} trivially.[1] In odd dimension $n \geq 5$, a quadratic APN function cannot have linearity 2^{n-1}, since every such function must be almost bent [15]. In dimension $n = 6$, there is exactly one quadratic APN function up to EA-equivalence which admits the highest possible linearity of 2^{n-1}. The existence of quadratic APN functions in dimension n having linearity 2^{n-1} is still unknown for $n > 8$. Preliminary observations on such functions have been remarked in [13].

In [20], the authors proposed a secondary approach to search for quadratic APN functions in dimension $n + 1$ by extending a quadratic APN function in dimension n. The approach was to guess the $(n + 1)$-th coordinate function and to utilize necessary properties of the algebraic normal form of the extended function. The search was then quite similar to the QAM approach [32]. However, no results were reported for $n \geq 7$.

2 Notation and preliminaries

By $\mathbb{N}$, we denote the set of natural numbers $\{1, 2, 3, \dots\}$ and by $\mathbb{F}_q$, we denote the finite field with q elements. In this work, we focus on functions between finite-dimensional $\mathbb{F}_2$-vector spaces, also called *vectorial Boolean functions*. For $n \in \mathbb{N}$, the set of invertible linear automorphisms from $\mathbb{F}_2^n$ to itself is denoted by $\mathrm{GL}(n, \mathbb{F}_2)$ and in our notation, we use matrices and their corresponding linear mappings interchangeably. In the following, let $\mathbb{V}, \mathbb{V}', \mathbb{W}, \mathbb{W}'$ be finite-dimensional (non-zero) vector spaces over $\mathbb{F}_2$. We denote the set of all linear mappings from $\mathbb{V}$ to $\mathbb{W}$ by $\mathcal{L}(\mathbb{V}, \mathbb{W})$. An *affine function* from $\mathbb{V}$ to $\mathbb{W}$ is a function of the form $x \mapsto L(x) + c$, where $L \in \mathcal{L}(\mathbb{V}, \mathbb{W})$ and $c \in \mathbb{W}$. Two vectorial Boolean functions $F \colon \mathbb{V} \to \mathbb{W}, G \colon \mathbb{V}' \to \mathbb{W}'$ are called *extended-affine equivalent* (*EA-equivalent* for short) if there exist affine bijections $A \colon \mathbb{V}' \to \mathbb{V}, B \colon \mathbb{W} \to \mathbb{W}'$ and an affine function $C \colon \mathbb{V}' \to \mathbb{W}'$ such that $G = B \circ F \circ A + C$. If $C = 0$, the functions F and G are called *affine-equivalent*, and if $C = 0$ and A and B are linear bijections, the two functions F and G are called *linear-equivalent*. We are interested in vectorial Boolean functions only up to EA-equivalence since the most important cryptographic properties are invariant under this equivalence relation, most importantly the algebraic degree, the differential uniformity, as well as the linearity. We recall the definition of those three notions in the following paragraphs. For a comprehensive textbook on the theory of Boolean functions and vectorial Boolean functions, we refer to [14].

Any Boolean function $f \colon \mathbb{F}_2^n \to \mathbb{F}_2$ can be uniquely expressed as a multivariate polynomial in $\mathbb{F}_2[X_1, \dots, X_n]/(X_1^2 + X_1, \dots, X_n^2 + X_n)$ via

$$f \colon \mathbb{F}_2^n \to \mathbb{F}_2, \quad x \mapsto \sum_{u \in \mathbb{F}_2^n} \left(a_u \prod_{i=1}^{n} x_i^{u_i} \right), \quad a_u \in \mathbb{F}_2.$$

---

[1] Since there exist linear APN functions in dimension $n \leq 2$, the linearity can be 2^n in those cases.

The *algebraic degree* of f is defined as $\max_{\{u \in \mathbb{F}_2^n | a_u \neq 0\}} \mathrm{wt}(u)$, where $\mathrm{wt}(u)$ denotes the Hamming weight of the binary vector u. Without loss of generality, a function from $\mathbb{V}$ to $\mathbb{W}$ with $\dim(\mathbb{V}) = n$, $\dim(\mathbb{W}) = m$ can be represented as a function $F \colon \mathbb{F}_2^n \to \mathbb{F}_2^m$ by applying a linear function in the input and in the output. In this representation, F can be given by its m *coordinate functions* $f_1, \dots, f_m \colon \mathbb{F}_2^n \to \mathbb{F}_2$ as $F(x_1, \dots, x_n) = (f_1(x_1, \dots, x_n), \dots, f_m(x_1, \dots, x_n))$. The *algebraic degree* of a vectorial Boolean function from $\mathbb{V}$ to $\mathbb{W}$ is defined as the maximum algebraic degree over all its coordinate functions when represented as a function from $\mathbb{F}_2^n$ to $\mathbb{F}_2^m$. Functions with algebraic degree equal to 2 are called *quadratic* and functions with algebraic degree at most 1 are called *affine*.

The *differential uniformity* [22] of a function $F \colon \mathbb{V} \to \mathbb{W}$ is defined as $\max_{\alpha \in \mathbb{V} \setminus \{0\}, \beta \in \mathbb{W}} |\{x \in \mathbb{V} \mid F(x) + F(x + \alpha) = \beta\}|$. It is straightforward to observe that the differential uniformity of a function $F \colon \mathbb{V} \to \mathbb{W}$ is an even integer larger than or equal to 2. For $\mathbb{F}_2$-vector spaces $\mathbb{V}$, $\mathbb{W}$ of the same finite dimension, a function $F \colon \mathbb{V} \to \mathbb{W}$ with the least possible differential uniformity of 2 is called *almost perfect nonlinear* (or *APN* for short) [24].

Let $\langle \cdot, \cdot \rangle_{\mathbb{V}} \colon \mathbb{V} \times \mathbb{V} \to \mathbb{F}_2$ and $\langle \cdot, \cdot \rangle_{\mathbb{W}} \colon \mathbb{W} \times \mathbb{W} \to \mathbb{F}_2$ be non-degenerate symmetric bilinear forms and let $F \colon \mathbb{V} \to \mathbb{W}$. A *component* of F is a function $\mathbb{V} \to \mathbb{F}_2, x \mapsto \langle b, F(x) \rangle_{\mathbb{W}}$, where $b \in \mathbb{W} \setminus \{0\}$. The *Walsh transform* of $F \colon \mathbb{V} \to \mathbb{W}$ at point $(\alpha, \beta) \in \mathbb{V} \times (\mathbb{W} \setminus \{0\})$ is defined as

$$\widehat{F}_\beta(\alpha) := \sum_{x \in \mathbb{V}} (-1)^{\langle \alpha, x \rangle_{\mathbb{V}} + \langle \beta, F(x) \rangle_{\mathbb{W}}}$$

and the *linearity* of F corresponds to the maximum absolute value of its Walsh transform, i.e., $\max_{\alpha \in \mathbb{V}, \beta \in \mathbb{W} \setminus \{0\}} |\widehat{F}_\beta(\alpha)|$. The linearity is a measure on how well a component can be approximated by an affine function. When $\mathbb{V} = \mathbb{F}_2^n$ for an integer $n \in \mathbb{N}$, we use $\langle x, y \rangle_{\mathbb{V}} = \langle x, y \rangle = \mathrm{wt}(\sum_{i=1}^n x_i y_i) \mod 2$, where $x = (x_1, x_2, \dots, x_n)$, $y = (y_1, y_2, \dots, y_n) \in \mathbb{F}_2^n$ and $\mathrm{wt}(k)$ denotes the Hamming weight of the binary expansion of $k \in \mathbb{N} \cup \{0\}$. In case of $\mathbb{V} = \mathbb{F}_{2^n}$ for an integer $n \in \mathbb{N}$, we use $\langle x, y \rangle_{\mathbb{V}} = \mathrm{Tr}(xy)$, where $x, y \in \mathbb{F}_{2^n}$ and Tr denotes the absolute trace function, defined as

$$\mathrm{Tr}(x) = x^{2^0} + x^{2^1} + x^{2^2} + \cdots + x^{2^{n-1}}.$$

It is well known that the Walsh transform of a quadratic Boolean function $f \colon \mathbb{F}_2^n \to \mathbb{F}_2$ only takes values in $\{0, \pm 2^{\frac{n+k}{2}}\}$, where k is the dimension of the vector space $\{a \in \mathbb{F}_2^n \mid x \mapsto f(x) + f(x + a) \text{ is constant}\}$, see [14, Prop. 55]. Therefore, the Walsh transform of a quadratic vectorial Boolean function $F \colon \mathbb{V} \to \mathbb{W}$ can only take 0 or powers of 2 as absolute values. In case that F is APN and $\dim(\mathbb{V}) = \dim(\mathbb{W}) = n > 2$, we know that the linearity of F cannot be equal to 2^n, see [14, Prop. 161]. Therefore, when F is APN and quadratic, the linearity of F can be at most 2^{n-1}, which motivates the following definition.

Definition 1 Let $n \in \mathbb{N}, n > 2$ and let $\mathbb{V}, \mathbb{W}$ be n-dimensional $\mathbb{F}_2$-vector spaces. We say that a quadratic APN function $F \colon \mathbb{V} \to \mathbb{W}$ has *maximum linearity* if it has linearity 2^{n-1}.

If $n \in \mathbb{N}$ is odd, every quadratic APN function is almost bent, i.e., its Walsh transform can only take values in $\{0, \pm, 2^{\frac{n+1}{2}}\}$, see [15]. Therefore, quadratic APN functions with maximum linearity can only exist in even dimensions n or for $n = 3$. Until recently, we only knew the existence of quadratic APN functions with maximum linearity up to $n = 6$, see [17] for an example in dimension 6. In [2], the authors found 4 EA-inequivalent instances in dimension $n = 8$. It is still an open problem whether quadratic APN functions with maximum linearity exist for $n \geq 10$.

In this work, we need the notion of the ortho-derivative of a quadratic APN function, which is defined as follows.

Definition 2 [12] Let $\mathbb{V}, \mathbb{W}$ be $\mathbb{F}_2$-vector spaces of the same finite dimension and let $\langle \cdot, \cdot \rangle_{\mathbb{W}} : \mathbb{W} \times \mathbb{W} \to \mathbb{F}_2$ be a non-degenerate symmetric bilinear form. Let $G : \mathbb{V} \to \mathbb{W}$ be a quadratic APN function. The *ortho-derivative* of G is defined as the unique function $\pi_G : \mathbb{V} \to \mathbb{W}$ with $\pi_G(0) = 0$ such that, for all $\alpha \in \mathbb{V} \setminus \{0\}$, we have $\pi_G(\alpha) \neq 0$ and

$$\forall x \in \mathbb{V} : \langle \pi_G(\alpha), B_\alpha(x) \rangle_{\mathbb{W}} = 0 \,,$$

where $B_\alpha : \mathbb{V} \to \mathbb{W}, x \mapsto G(x) + G(x + \alpha) + G(\alpha) + G(0)$.

The ortho-derivative π_G of a given quadratic APN function $G : \mathbb{F}_2^n \to \mathbb{F}_2^n$ is computed from the difference distribution table (DDT) of G by first identifying, for every $a \in \mathbb{F}_2^n$, the linear part of the affine space $\{b \in \mathbb{F}_2^n \mid \mathrm{DDT}_G[a, b] = 2\}$, and then finding the value $\pi_G(a)$ which is orthogonal to it.[2] Overall, the most computationally demanding step is the computation of the DDT, which takes time $\mathcal{O}(2^{2n})$.

The authors of [12] showed that for two EA-equivalent quadratic APN functions $G, G' : \mathbb{F}_2^n \to \mathbb{F}_2^n$, the ortho-derivatives π_G and $\pi_{G'}$ are linear-equivalent. Indeed, the linear-equivalence of the ortho-derivatives is a strongly discriminating EA-invariant for quadratic APN functions, which allows in many cases to efficiently detect the EA-inequivalence of two quadratic APN functions.

3 Function trimming

For a given function $F : \mathbb{F}_2^n \to \mathbb{F}_2^n$, we want to consider *all* the restrictions $G \prec F$ with $G : \mathbb{F}_2^{n-1} \to \mathbb{F}_2^{n-1}$. Since there are many choices for the affine injective mappings $\phi : \mathbb{F}_2^{n-1} \to \mathbb{F}_2^n$ and the affine surjections $\varphi : \mathbb{F}_2^n \to \mathbb{F}_2^{n-1}$, this would quickly become infeasible already for very small values of n. However, as we are only interested in vectorial Boolean functions up to EA-equivalence, the particular restrictions and projections that have to be taken into account can be significantly reduced, as we outline in the following. For an element $\alpha \in \mathbb{F}_2^n \setminus \{0\}$, we denote by $\alpha^\perp$ its orthogonal, i.e., $\alpha^\perp = \{x \in \mathbb{F}_2^n \mid \langle \alpha, x \rangle = 0\}$, which is an $n - 1$-dimensional linear hyperplane. We denote its complement set $\mathbb{F}_2^n \setminus \alpha^\perp$ by $\overline{\alpha^\perp}$.

For a non-zero element $\beta \in \mathbb{F}_2^n$ and an element $\gamma \in \mathbb{F}_2^n$ such that $\langle \beta, \gamma \rangle = 1$, we define $\rho_\beta^{(\gamma)}$ as the function

$$\rho_\beta^{(\gamma)} : \mathbb{F}_2^n \to \gamma^\perp, \quad x \mapsto x + \beta \cdot \langle \gamma, x \rangle \,.$$

If we represent $\mathbb{F}_2^n$ as the direct sum $\mathbb{F}_2^n = \gamma^\perp \oplus \{0, \beta\}$, for any vector $x = x_\beta \oplus x_\gamma \in \mathbb{F}_2^n$ with $x_\gamma \in \gamma^\perp, x_\beta \in \{0, \beta\}$, we have $\rho_\beta^{(\gamma)}(x) = x_\gamma$, i.e, $\rho_\beta^{(\gamma)}$ is a projection of $\mathbb{F}_2^n$ to $\gamma^\perp$. The following definition precisely captures the idea of restricting the input and projecting the output of a vectorial Boolean function.

Definition 3 (*Trim along* (H, β)) Let $n \in \mathbb{N}, n \geq 2, \beta \in \mathbb{F}_2^n$ be a non-zero element and let $H \subseteq \mathbb{F}_2^n$ be a hyperplane of dimension $n - 1$, so that $H = \alpha^\perp$ or $H = \overline{\alpha^\perp}$ for some non-zero $\alpha \in \mathbb{F}_2^n$. Let $\epsilon \in \mathbb{F}_2^n$ be zero if $H = \alpha^\perp$ and $\epsilon \notin \alpha^\perp$ otherwise, and let $\gamma \in \mathbb{F}_2^n \setminus \beta^\perp$. The *trim*

---

[2] We recall that $\mathrm{DDT}_G[a, b]$ is defined as $|\{x \in \mathbb{F}_2^n \mid G(x) + G(x + a) = b\}|$.

of a function F along (H, β) with respect to ϵ, γ is then defined as

$$\mathcal{T}^{\epsilon,\gamma}_{H \rightsquigarrow \beta} F \colon \alpha^\perp \to \gamma^\perp$$

$$x \mapsto \rho^{(\gamma)}_\beta \circ F(x + \epsilon) = \begin{cases} F(x + \epsilon) & \text{if } F(x + \epsilon) \in \gamma^\perp \\ F(x + \epsilon) + \beta & \text{otherwise} \end{cases}.$$

Note that, for a given $F \colon \mathbb{F}^n_2 \to \mathbb{F}^n_2$, we can convert every function $\mathcal{T}^{\epsilon,\gamma}_{H \rightsquigarrow \beta} F \colon \alpha^\perp \to \gamma^\perp$ to a function from $\mathbb{F}^{n-1}_2$ to $\mathbb{F}^{n-1}_2$ by applying linear bijections in the input and in the output. Moreover, if we are only interested in $\mathcal{T}^{\epsilon,\gamma}_{H \rightsquigarrow \beta} F$ up to affine-equivalence, the particular choice of ϵ and γ does not matter, as we show in the following proposition.

Proposition 1 *Let $n \in \mathbb{N}$, $n \geq 2$. For a fixed choice of (H, β) with $\beta \in \mathbb{F}^n_2$ being a non-zero element and $H \subseteq \mathbb{F}^n_2$ being a hyperplane of dimension $n - 1$, all trims of F along (H, β) with respect to some ϵ, γ are affine-equivalent.*

Proof We first consider the case of a fixed $\gamma \in \mathbb{F}^n_2 \setminus \beta^\perp$ and varying ϵ. If H is a linear hyperplane, i.e., $H = \alpha^\perp$ for some non-zero $\alpha \in \mathbb{F}^n_2$, there is only one valid choice of ϵ, i.e., $\epsilon = 0$. Let us therefore consider the case that $H = \overline{\alpha^\perp}$. Let $\epsilon, \epsilon' \in \mathbb{F}^n_2 \setminus \alpha^\perp$ and let $\epsilon_\alpha \in \alpha^\perp$ be such that $\epsilon' = \epsilon + \epsilon_\alpha$. We have

$$\mathcal{T}^{\epsilon',\gamma}_{H \rightsquigarrow \beta} F(x) = F((x + \epsilon_\alpha) + \epsilon) + \beta \langle \gamma, F((x + \epsilon_\alpha) + \epsilon) \rangle = \mathcal{T}^{\epsilon,\gamma}_{H \rightsquigarrow \beta} F(x + \epsilon_\alpha) \,,$$

so $\mathcal{T}^{\epsilon',\gamma}_{H \rightsquigarrow \beta} F$ is affine-equivalent to $\mathcal{T}^{\epsilon,\gamma}_{H \rightsquigarrow \beta} F$.

Let us now consider the case of a fixed ϵ and varying $\gamma \in \mathbb{F}^n_2 \setminus \beta^\perp$. Let $\gamma, \gamma' \in \mathbb{F}^n_2 \setminus \beta^\perp$ and let Q be the linear isomorphism $Q \colon \gamma^\perp \to \gamma'^\perp, x \mapsto x + \beta \langle \gamma', x \rangle$. We then have

$$Q \circ \mathcal{T}^{\epsilon,\gamma}_{H \rightsquigarrow \beta} F(x) = F(x + \epsilon) + \beta \langle \gamma, F(x + \epsilon) \rangle + \beta \langle \gamma', F(x + \epsilon) + \beta \langle \gamma, F(x + \epsilon) \rangle \rangle$$

$$= \begin{cases} F(x + \epsilon) + \beta \langle \gamma', F(x + \epsilon) \rangle & \text{if } \langle \gamma, F(x + \epsilon) \rangle = 0 \\ F(x + \epsilon) + \beta \langle \gamma', F(x + \epsilon) \rangle + \beta + \beta \langle \gamma', \beta \rangle & \text{if } \langle \gamma, F(x + \epsilon) \rangle = 1 \end{cases}$$

$$= F(x + \epsilon) + \beta \langle \gamma', F(x + \epsilon) \rangle = \mathcal{T}^{\epsilon,\gamma'}_{H \rightsquigarrow \beta} F(x) \,,$$

so $\mathcal{T}^{\epsilon,\gamma'}_{H \rightsquigarrow \beta} F$ is linear-equivalent to $\mathcal{T}^{\epsilon,\gamma}_{H \rightsquigarrow \beta} F$. □

Because of the above proposition, we say that the EA-equivalence class of $\mathcal{T}^{\epsilon,\gamma}_{H \rightsquigarrow \beta} F$ is *the trim of F along (H, β)*, denoted $\mathcal{T}_{H \rightsquigarrow \beta} F$.

Remark 1 To the best of our knowledge, the effect on the differential uniformity and on the linearity of restricting a vectorial Boolean function to an affine subspace was first studied in [23]. Moreover, the paper [23] also derived an upper bound and a lower bound on the differential uniformity of a vectorial Boolean function when composing it with an affine surjection from the output. There are some works that study subfunctions of APN functions obtained by discarding one output coordinate, e.g., [18,19]. We remark that the notion of a trim covers the case of restricting the input of F to an affine hyperplane and then discarding one output coordinate of F, but it is more general than that. Indeed, if $F \colon \mathbb{F}^n_2 \to \mathbb{F}^n_2$ is represented by its coordinate functions $F = (f_1, \dots, f_n)$ with $f_i \colon \mathbb{F}^n_2 \to \mathbb{F}_2, i \in \{1, \dots, n\}$, the function $F' \colon \mathbb{F}^n_2 \to \mathbb{F}^{n-1}_2, F' = (f_1, \dots, f_{j-1}, f_{j+1}, \dots, f_n)$ that is obtained by discarding the j-th coordinate of F is linear-equivalent to the function $\rho^{(e_j)}_{e_j} \circ F \colon \mathbb{F}^n_2 \to e^\perp_j$, where $e_j = (0, \dots, 0, 1, 0, \dots, 0)$ is the j-th unit vector in $\mathbb{F}^n_2$.

The following proposition states that every restriction of F in dimension $n - 1$ is EA-equivalent to a trim of F.

Proposition 2 *Let $n \in \mathbb{N}, n \geq 2$ and let $F \colon \mathbb{F}_2^n \to \mathbb{F}_2^n$ and $G \colon \mathbb{F}_2^{n-1} \to \mathbb{F}_2^{n-1}$ be given with $G \prec F$. Then, there exists a non-zero element $\beta \in \mathbb{F}_2^n$ and an affine hyperplane $H \subseteq \mathbb{F}_2^n$ of dimension $n - 1$ such that G is EA-equivalent to an (every) element in $\mathcal{T}_{H \rightsquigarrow \beta} F$.*

Proof By definition, there exists an affine injective mapping $\phi \colon \mathbb{F}_2^{n-1} \to \mathbb{F}_2^n$ and an affine surjection $\varphi \colon \mathbb{F}_2^n \to \mathbb{F}_2^{n-1}$ such that $G = \varphi \circ F \circ \phi$. Let $\tilde{\phi} \colon \mathbb{F}_2^{n-1} \to \mathcal{I}m(\tilde{\phi})$ denote the linear part of ϕ, such that $\phi = \tilde{\phi} + \epsilon$ for $\epsilon \in \mathbb{F}_2^n$ with $\epsilon = 0$ if ϕ is linear and $\epsilon \notin \mathcal{I}m(\tilde{\phi})$ otherwise. Note that $\tilde{\phi}$ is a bijection from $\mathbb{F}_2^{n-1}$ to $\mathcal{I}m(\tilde{\phi})$, where $\mathcal{I}m(\tilde{\phi}) = \alpha^\perp$ for a non-zero element $\alpha \in \mathbb{F}_2^n$. Further, let $\tilde{\varphi}$ denote the linear part of φ such that $\varphi = \tilde{\varphi} + b$ with $b \in \mathbb{F}_2^{n-1}$. We therefore have, for all $x \in \alpha^\perp$,

$$G \circ \tilde{\phi}^{-1}(x) = (\tilde{\varphi} \circ F(x + \epsilon)) + b \ .$$

Let M be the $(n - 1) \times n$ matrix over $\mathbb{F}_2$ such that $\tilde{\varphi}(x) = Mx$ for all $x \in \mathbb{F}_2^n$. Since $\tilde{\varphi}$ is surjective, the matrix M has rank $n - 1$, so there exist $n - 1$ linearly independent columns in M. Let P be an $n \times n$ permutation matrix such that P^{-1} permutes those linearly independent columns to the left side, i.e, we have

$$M P^{-1} = \begin{pmatrix} A^{-1} & \beta \end{pmatrix} \ ,$$

where A is an invertible $(n - 1) \times (n - 1)$ matrix and β is a column vector in $\mathbb{F}_2^{n-1}$. We then have $A M P^{-1} = \begin{pmatrix} I & A\beta \end{pmatrix}$, where I denotes the $(n - 1) \times (n - 1)$ identity matrix. Thus, for all $x \in \alpha^\perp$, we have

$$\begin{pmatrix} A(G \circ \tilde{\phi}^{-1}(x)) \\ 0 \end{pmatrix} = \begin{pmatrix} I & A\beta \\ 0 & 0 \end{pmatrix} P F(x + \epsilon) + \begin{pmatrix} Ab \\ 0 \end{pmatrix}$$

$$= P F(x + \epsilon) + \begin{pmatrix} A\beta \\ 1 \end{pmatrix} \langle e_n, P F(x + \epsilon) \rangle + \begin{pmatrix} Ab \\ 0 \end{pmatrix}$$

$$= P \left(F(x + \epsilon) + P^{-1} \begin{pmatrix} A\beta \\ 1 \end{pmatrix} \langle P^\top e_n, F(x + \epsilon) \rangle + P^{-1} \begin{pmatrix} A\beta \\ 0 \end{pmatrix} \right),$$

and finally

$$P^{-1} \begin{pmatrix} A(G \circ \tilde{\phi}^{-1}(x)) \\ 0 \end{pmatrix} + P^{-1} \begin{pmatrix} A\beta \\ 0 \end{pmatrix} = F(x + \epsilon) + P^{-1} \begin{pmatrix} A\beta \\ 1 \end{pmatrix} \langle P^\top e_n, F(x + \epsilon) \rangle.$$

$\square$

This proposition allows to reduce the number of restrictions we need to consider for a given function $F \colon \mathbb{F}_2^n \to \mathbb{F}_2^n$ to $2 \cdot (2^n - 1)^2$, i.e., we only need to consider all the trims $\mathcal{T}_{H \rightsquigarrow \beta} F$ of F, where (H, β) takes all possible values. In the following, we establish the fact that for EA-equivalent functions $F, G \colon \mathbb{F}_2^n \to \mathbb{F}_2^n$, the multiset of all possible trims of F is the same as the multiset of all possible trims of G.

Proposition 3 *Let $n \in \mathbb{N}, n \geq 2$ and let $F, G \colon \mathbb{F}_2^n \to \mathbb{F}_2^n$ be EA-equivalent via $G = B \circ F \circ (A + a) + b + C$ with $A, B \in \mathrm{GL}(n, \mathbb{F}_2)$, $a, b \in \mathbb{F}_2^n$ and C being an affine function in $\mathbb{F}_2^n$. Then, for each hyperplane $H \subseteq \mathbb{F}_2^n$ and each $\beta \in \mathbb{F}_2^n \setminus \{0\}$, we have that $\mathcal{T}_{H \rightsquigarrow \beta} G$ is EA-equivalent[3] to $\mathcal{T}_{H' \rightsquigarrow \beta'} F$, where $H' = A(H) + a$ and $\beta' = B^{-1}(\beta)$.*

---

[3] More precisely, since $\mathcal{T}_{H \rightsquigarrow \beta} G$ and $\mathcal{T}_{H' \rightsquigarrow \beta'} F$ are EA-equivalence classes, we have to say that that any representative in $\mathcal{T}_{H \rightsquigarrow \beta} G$ is EA-equivalent to any representative in $\mathcal{T}_{H' \rightsquigarrow \beta'} F$.

Proof Let us fix a non-zero element $\beta \in \mathbb{F}_2^n$ and an $n - 1$-dimensional hyperplane $H \subseteq \mathbb{F}_2^n$ such that $H = \alpha^\perp$ or $H = \overline{\alpha^\perp}$ for a non-zero $\alpha \in \mathbb{F}_2^n$. Further, let $\gamma \in \mathbb{F}_2^n \setminus \beta^\perp$ and $\epsilon \in \mathbb{F}_2^n$ with $\epsilon = 0$ if $H = \alpha^\perp$ and $\epsilon \notin \alpha^\perp$ if $H = \overline{\alpha^\perp}$. The proof is divided in three parts.

- Let first $G = F \circ (A + a)$, where $A \in \mathrm{GL}(n, \mathbb{F}_2)$ and $a \in \mathbb{F}_2^n$. Let $\alpha' \in \mathbb{F}_2^n$ be such that $A(\alpha^\perp) = \alpha'^\perp$. First, let us consider the case of $H = \alpha^\perp$. For any $x \in \alpha^\perp$, we then have

$$
\begin{aligned}
\mathcal{T}_{H \rightsquigarrow \beta}^{0,\gamma} G(x) = G(x) + \beta \langle \gamma, G(x) \rangle &= F(A(x) + a) + \beta \langle \gamma, F(A(x) + a) \rangle \\
&= \begin{cases} \mathcal{T}_{A(H)+a \rightsquigarrow \beta}^{0,\gamma} F(A(x) + a) & \text{if } a \in A(H) \\ \mathcal{T}_{A(H)+a \rightsquigarrow \beta}^{a,\gamma} F(A(x)) & \text{if } a \notin A(H) \end{cases} .
\end{aligned}
$$

Let us now consider the case of $H = \overline{\alpha^\perp}$. Then, $H = \alpha^\perp + \epsilon$ for $\epsilon \notin \alpha^\perp$. For any $x \in \alpha^\perp$, we then have

$$
\begin{aligned}
\mathcal{T}_{H \rightsquigarrow \beta}^{\epsilon,\gamma} G(x) &= G(x + \epsilon) + \beta \langle \gamma, G(x + \epsilon) \rangle \\
&= F(A(x + \epsilon) + a) + \beta \langle \gamma, F(A(x + \epsilon) + a) \rangle \\
&= F(A(x) + a + A(\epsilon)) + \beta \langle \gamma, F(A(x) + a + A(\epsilon)) \rangle \\
&= \begin{cases} \mathcal{T}_{A(H)+a \rightsquigarrow \beta}^{0,\gamma} F(A(x) + (a + A(\epsilon))) & \text{if } a + A(\epsilon) \in \alpha'^\perp \\ \mathcal{T}_{A(H)+a \rightsquigarrow \beta}^{a+A(\epsilon),\gamma} F(A(x)) & \text{if } a + A(\epsilon) \notin \alpha'^\perp \end{cases} .
\end{aligned}
$$

- Let now $G = B \circ F + b$, where $B \in \mathrm{GL}(n, \mathbb{F}_2)$, $b \in \mathbb{F}_2^n$. Let $\gamma' := B^\top(\gamma)$. For any $x \in \alpha^\perp$, we then have

$$
\begin{aligned}
\mathcal{T}_{H \rightsquigarrow \beta}^{\epsilon,\gamma} G(x) &= G(x + \epsilon) + \beta \langle \gamma, G(x + \epsilon) \rangle \\
&= B(F(x + \epsilon)) + \beta \langle \gamma, B(F(x + \epsilon)) \rangle + (b + \beta \langle \gamma, b \rangle) \\
&= B\big(F(x + \epsilon) + B^{-1}(\beta) \langle \gamma', F(x + \epsilon) \rangle \big) + (b + \beta \langle \gamma, b \rangle) \\
&= B \circ \mathcal{T}_{H \rightsquigarrow \beta'}^{\epsilon,\gamma'} F(x) + (b + \beta \langle \gamma, b \rangle) .
\end{aligned}
$$

- Finally, let $G = F + C$ with C being an affine function in $\mathbb{F}_2^n$. For any $x \in \alpha^\perp$, we then have

$$
\begin{aligned}
\mathcal{T}_{H \rightsquigarrow \beta}^{\epsilon,\gamma} G(x) &= G(x + \epsilon) + \beta \langle \gamma, G(x + \epsilon) \rangle \\
&= F(x + \epsilon) + \beta \langle \gamma, F(x + \epsilon) \rangle + C(x + \epsilon) + \beta \langle \gamma, C(x + \epsilon) \rangle \\
&= \mathcal{T}_{H \rightsquigarrow \beta}^{\epsilon,\gamma} F(x) + (C(x + \epsilon) + \beta \langle \gamma, C(x + \epsilon) \rangle) .
\end{aligned}
$$

$\square$

Proposition 3 motivates us to define the notion of the *trim spectrum* of a function $F \colon \mathbb{F}_2^n \to \mathbb{F}_2^n$, which is an EA-invariant. In the following, let $\mathcal{H}_n$ denote the set of all $n - 1$-dimensional hyperplanes of $\mathbb{F}_2^n$, i.e., $\mathcal{H}_n := \{\alpha^\perp \mid \alpha \in \mathbb{F}_2^n \setminus \{0\}\} \cup \{\overline{\alpha^\perp} \mid \alpha \in \mathbb{F}_2^n \setminus \{0\}\}$.

Definition 4 (*Trim Spectrum*) Let $n \in \mathbb{N}$, $n \geq 2$. The *trim spectrum* of a function $F \colon \mathbb{F}_2^n \to \mathbb{F}_2^n$ is the multiset of all trims of F along (H, β), where (H, β) takes all $2 \cdot (2^n - 1)^2$ possibilities, i.e., the multiset $\{\mathcal{T}_{H \rightsquigarrow \beta} F \mid H \in \mathcal{H}_n, \beta \in \mathbb{F}_2^n \setminus \{0\}\}$.

We recall that for an $n - 1$-dimensional hyperplane $H \subseteq \mathbb{F}_2^n$ and a non-zero element $\beta \in \mathbb{F}_2^n$, the trim $\mathcal{T}_{H \rightsquigarrow \beta} F$ refers to an EA-equivalence class, and not to a particular vectorial Boolean function.

Corollary 1 *The trim spectrum of a vectorial Boolean function is an EA-invariant. In other words, for $n \in \mathbb{N}$, $n \geq 2$, if F, $G \colon \mathbb{F}_2^n \to \mathbb{F}_2^n$ are EA-equivalent, the multisets $\{\mathcal{T}_{H \rightsquigarrow \beta} F \mid H \in \mathcal{H}_n, \beta \in \mathbb{F}_2^n \setminus \{0\}\}$ and $\{\mathcal{T}_{H \rightsquigarrow \beta} G \mid H \in \mathcal{H}_n, \beta \in \mathbb{F}_2^n \setminus \{0\}\}$ consist of the same EA-equivalence classes with the same multiplicities.*

Proof This follows directly from Proposition 3 and from the fact that the two functions $\mathcal{H}_n \to \mathcal{H}_n$, $H \mapsto H' = A(H) + a$ and $\mathbb{F}_2^n \setminus \{0\} \to \mathbb{F}_2^n \setminus \{0\}$, $\beta \mapsto \beta' = B^{-1}(\beta)$ are permutations for $A, B \in \mathrm{GL}(n, \mathbb{F}_2)$, $a \in \mathbb{F}_2^n$. □

Remark 2 We note that for a quadratic function $F \colon \mathbb{F}_2^n \to \mathbb{F}_2^n$, the trim spectrum can be simplified by only considering the *linear* hyperplanes H. In fact, for $\alpha, \beta \in \mathbb{F}_2^n \setminus \{0\}$ and $\epsilon \in \overline{\alpha^\perp}$, $\gamma \in \overline{\beta^\perp}$, $x \in \alpha^\perp$, we have

$$\mathcal{T}_{\alpha^\perp \rightsquigarrow \beta}^{\epsilon, \gamma} F(x) = F(x + \epsilon) + \beta \langle \gamma, F(x + \epsilon) \rangle$$

$$= A_\epsilon(x) + \beta \langle \gamma, A_\epsilon(x) \rangle + \mathcal{T}_{\alpha^\perp \rightsquigarrow \beta}^{0, \gamma} F(x) \, ,$$

where A_ϵ is the affine mapping such that, for all $x \in \mathbb{F}_2^n$, we have $F(x) + F(x + \epsilon) = A_\epsilon(x)$. Thus, the two trims $\mathcal{T}_{\alpha^\perp \rightsquigarrow \beta}^{\epsilon, \gamma} F$ and $\mathcal{T}_{\alpha^\perp \rightsquigarrow \beta}^{0, \gamma} F$ are EA-equivalent.

3.1 APN-trims of APN functions in small dimension

We could ask the following question: Among the APN functions that were known before our work, how many have APN functions as a restriction in one dimension lower?

To answer this question for the quadratic APN functions in small dimension, we proceeded as follows. For each quadratic APN function F in dimension $3 \leq n \leq 7$ up to EA-equivalence, we checked whether the trim spectrum of F contains an APN function. To illustrate this data, we plotted it in a *trimming graph* defined as follows. Each EA-equivalence class of a quadratic APN function corresponds to a node, and each node is at a height corresponding to the value of n ($n = 3$ at the lowest level, and then it is incremented going up each level). Then, there is a vertex from a node F at height n down to a node G at height $n - 1$ if the function G is in the trim spectrum of F. Functions that are neither the start nor the end of an edge are not represented. The result can be seen in the graph given in Fig. 1. This graph is complete in the sense that all EA-equivalence classes of quadratic APN functions in dimension up to $n = 7$ are known and we have taken into account all the relevant functions. More precisely, for $n \leq 4$, there is only the EA-equivalence class corresponding to the function $x \mapsto x^3$ over $\mathbb{F}_{2^n}$, for $n = 5$, there are the two EA-equivalence classes corresponding to the functions $x \mapsto x^3$ and $x \mapsto x^5$, for $n = 6$, there are the 13 quadratic EA-equivalence classes listed in [17, Table 5], and for $n = 7$, there are 488 EA-equivalence classes of quadratic APN functions [20].

As we can see, the trimming graph given in Fig. 1 has a complex structure where the following properties stand out.

- Two EA-equivalence classes of quadratic 6-bit APN functions are in the trim spectra of some 7-bit ones, but do not have any APN functions in their own trim spectra. Those functions correspond to Function no. 1.2 and Function no. 2.1 in [17, Table 5] and can be given in univariate representation as $x \mapsto x^3 + g^{11} x^6 + g x^9$ and $x \mapsto x^3 + g x^{24} + x^{10}$, respectively, where $g \in \mathbb{F}_{2^6}$ is an element with minimal polynomial $X^6 + X^4 + X^3 + X + 1$.
- Conversely, there is a 6-bit quadratic APN function that is not in the trim spectrum of any 7-bit one, but it has 5-bit APN functions in its trim spectrum. This is Function no.
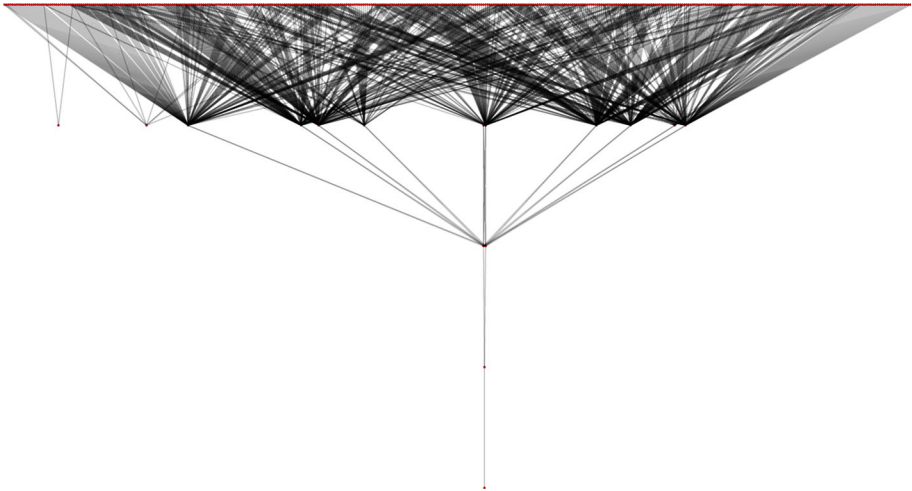
Fig. 1 The trimming graph of all quadratic APN functions for $n \leq 7$. Functions (i.e., nodes) that are neither the start nor the end of an edge are not represented

2.6 in [17, Table 5] (see also the representation we provide in Sect. 5.3). Note that this observation was already reported in [20, Sec. 3].

- Most of the EA-equivalence classes of quadratic 6-bit APN functions are in the trim spectra of multiple 7-bit ones, and most of the quadratic 7-bit APN functions that have APN functions in their trim spectra have multiple different EA-equivalence classes of APN functions in their trim spectra.
- Several of the quadratic 7-bit APN functions have a unique EA-equivalence class of 6-bit APN functions in their trim spectrum.
- For $n = 6$, one out of the 13 EA-inequivalent quadratic APN functions does not appear in the graph because it has no APN functions in its trim spectrum, and does not belong to the trim spectrum of any quadratic 7-bit APN function. That function is $x \mapsto x^3$. For $n = 7$, 50 functions out of the 488 EA-inequivalent quadratic APN functions do not appear because they do not have any APN functions in their trim spectra.

Moreover, for each of the known quadratic APN functions in dimension $n = 8$ up to EA-equivalence (except the new ones constructed in Sect. 4), we also checked whether it contains an APN function within its trim spectrum. The result is given in the graph depicted in Fig. 2. Unlike the previous one, this graph is *not* complete since quadratic APN functions in dimension eight are not classified yet, so we do not have a full list of all the quadratic 8-bit APN functions.

Looking at all of the 26,524 previously known quadratic 8-bit APN functions, we observe the following:

- Only 123 of those functions have an APN function within their trim spectrum.
- 15 have a unique EA-equivalence class of 7-bit APN functions in their trim spectrum that is also not in the trim spectrum of another of the 26,524 quadratic 8-bit APN functions.
- Three of the EA-equivalence classes quadratic 7-bit APN functions are in the trim spectrum of quadratic 8-bit APN functions, but do not have any APN functions in their own trim spectrum (meaning that these functions appear in Fig. 2 but not in Fig. 1).
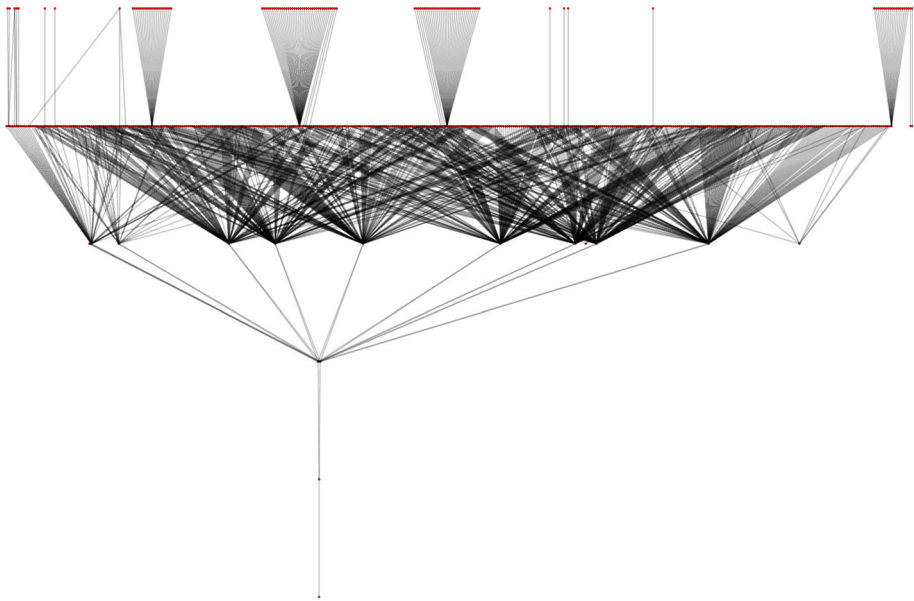
Fig. 2 The trimming graph of all quadratic APN functions in dimension n with $3 \leq n \leq 8$ that were known before our work. Functions (i.e., nodes) that are neither the start nor the end of an edge are not represented

To the best of our knowledge, there are 60 known quadratic APN functions in dimension 9 up to EA-equivalence. They either correspond to a polynomial with coefficients in $\mathbb{F}_2$ [29], to the (generalized) isotopic shift construction [7,8], to the infinite families given in [9,10], or to one of the 35 instances presented in [2]. None of those 60 instances contains an APN trim within their trim spectrum.

We further checked for some quadratic APN instances in dimension $n = 10$ that come from infinite families (i.e., the instances 10.1–10.2 and 10.5–10.17 from [5]) and for the 5 sporadic instances presented in [2] whether they contain an APN trim within their trim spectrum. This is not the case for any of those functions.

On the 6-bit APN function inequivalent to a quadratic function From [11], we know that the known 6-bit APN function CCZ-inequivalent to a quadratic function consist of 25 distinct EA-equivalence classes. For each of those EA-equivalence classes, we chose a representative and checked whether the trim spectrum contains APN functions. Indeed, this is the case for 21 out of the 25 classes. For one class, all the APN trims are quadratic, while for the 20 other classes, all the APN trims are cubic.

On the non-quadratic APN monomial functions We further checked for all of the non-quadratic APN monomial functions in dimension n with $5 \leq n \leq 10$ whether the trim spectrum contains an APN function. This is not the case.

In [4], we provide the source code for computing the trim spectrum of a given vectorial Boolean function, as well as the source code for computing the trimming graphs as given in Figs. 1 and 2.

3.2 Recursive APN functions

As one can observe from the trimming graph depicted in Fig. 2, there are quadratic APN functions in dimension $n = 8$ that contain an APN function in dimension $n = 7$ as a

restriction, which again contains an APN restriction in dimension $n = 6$, and so forth up to $n = 2$. This property is indicated by a path from the top level to the bottom level of the trimming graph (note that the trimming graph only depicts the nodes for $n \geq 3$). We call such functions *recursive* APN functions, formally defined in the following.

Definition 5 Let $n \in \mathbb{N}, n \geq 2$. An APN function $F_n : \mathbb{F}_2^n \to \mathbb{F}_2^n$ is called *recursive* if, for each $i \in \{2, \ldots, n-1\}$, there exists an APN function $F_i : \mathbb{F}_2^i \to \mathbb{F}_2^i$ such that $F_2 \prec F_3 \prec \cdots \prec F_{n-1} \prec F_n$.

In Appendix A, we give an example of a recursive APN function in dimension $n = 8$. Motivated by the new APN extensions we construct in Sect. 4 below, we raise the following conjecture.

Conjecture 1 *There exists a recursive APN function in every dimension $n \in \mathbb{N}, n \geq 2$.*

4 New APN extensions in dimension eight

In this section, up to EA-equivalence, we construct new quadratic APN functions in dimension eight as extensions of quadratic 7-bit APN functions. Note that a search for quadratic APN functions $F : \mathbb{F}_2^{n+1} \to \mathbb{F}_2^{n+1}$ which contain a quadratic APN function $G : \mathbb{F}_2^n \to \mathbb{F}_2^n$ as a restriction was already conducted in [20]. In this previous work, the search was based on necessary properties of the algebraic normal form of F and it was quite similar to the QAM approach [32]. However, no results were reported for $n \geq 7$.

The following proposition derives a simple form of such APN functions, which we utilize in our search.

Proposition 4 *Let $F : \mathbb{F}_2^{n+1} \to \mathbb{F}_2^{n+1}$ be a quadratic function. Then, there exists a function $G : \mathbb{F}_2^n \to \mathbb{F}_2^n$ of algebraic degree at most 2, a Boolean function $r : \mathbb{F}_2^n \to \mathbb{F}_2^n$ of algebraic degree at most 2, and two linear functions $L : \mathbb{F}_2^n \to \mathbb{F}_2^n, \ell : \mathbb{F}_2^n \to \mathbb{F}_2$ such that F is EA-equivalent to*

$$T : \mathbb{F}_2^n \times \mathbb{F}_2 \to \mathbb{F}_2^n \times \mathbb{F}_2$$
$$\begin{pmatrix} x \\ y \end{pmatrix} \mapsto \begin{pmatrix} G(x) \\ r(x) \end{pmatrix} + \begin{pmatrix} L(x) \\ \ell(x) \end{pmatrix} \cdot y .$$

Proof By applying an EA-transformation to F, we can obtain a function

$$T : \mathbb{F}_2^n \times \mathbb{F}_2 \to \mathbb{F}_2^n \times \mathbb{F}_2, \begin{pmatrix} x \\ y \end{pmatrix} \mapsto \begin{pmatrix} H(x, y) \\ h(x, y) \end{pmatrix} ,$$

where $H : \mathbb{F}_2^n \times \mathbb{F}_2 \to \mathbb{F}_2^n$ is of algebraic degree at most 2, $H(0, 0) = H(0, 1) = 0$ and $h : \mathbb{F}_2^n \times \mathbb{F}_2 \to \mathbb{F}_2$ is of algebraic degree at most 2 with $h(0, 0) = h(0, 1) = 0$. Then, by defining $G(x) = H(x, 0)$ and $r(x) = h(x, 0)$, we obtain

$$T \begin{pmatrix} x \\ y \end{pmatrix} = \begin{pmatrix} G(x) \\ r(x) \end{pmatrix} (y + 1) + \begin{pmatrix} H(x, 1) \\ h(x, 1) \end{pmatrix} y . \tag{2}$$

Note that since (G, r) is a restriction of (H, h) to a linear hyperplane, it is also of algebraic degree at most 2. Now, T is quadratic if and only if $x \mapsto (G(x) + H(x, 1), r(x) + h(x, 1))$ is of algebraic degree at most 1, which means that $H(x, 1) = G(x) + L(x)$ for an affine function L and $h(x, 1) = r(x) + \ell(x)$ for an affine function ℓ. Since we chose $(H(0, 1), h(0, 1)) = (H(0, 0), h(0, 0)) = (0, 0)$, we have $(L(0), \ell(0)) = (0, 0)$ and both L and ℓ must therefore be linear. □

Definition 6 Let $G\colon \mathbb{F}_2^n \to \mathbb{F}_2^n$ be a quadratic APN function and let $r\colon \mathbb{F}_2^n \to \mathbb{F}_2$ be a Boolean function of algebraic degree at most 2. The function G is called r-extendable if there exist two linear functions $L\colon \mathbb{F}_2^n \to \mathbb{F}_2^n, \ell\colon \mathbb{F}_2^n \to \mathbb{F}_2$ such that

$$T\colon \mathbb{F}_2^n \times \mathbb{F}_2 \to \mathbb{F}_2^n \times \mathbb{F}_2$$
$$\begin{pmatrix} x \\ y \end{pmatrix} \mapsto \begin{pmatrix} G(x) \\ r(x) \end{pmatrix} + \begin{pmatrix} L(x) \\ \ell(x) \end{pmatrix} \cdot y$$

is APN. If T is APN, we say that the tuple (G, r, L, ℓ) *yields an APN function T* and we say that T is an *APN extension of G in standard form*.

Remark 3 For any linear mappings $L\colon \mathbb{F}_2^n \to \mathbb{F}_2^n, \ell\colon \mathbb{F}_2^n \to \mathbb{F}_2$ and any Boolean function $r\colon \mathbb{F}_2^n \to \mathbb{F}_2$, we remark that if two functions $G, G'\colon \mathbb{F}_2^n \to \mathbb{F}_2^n$ are EA-equivalent, there exist linear mappings $L'\colon \mathbb{F}_2^n \to \mathbb{F}_2^n, \ell'\colon \mathbb{F}_2^n \to \mathbb{F}_2$ and a Boolean function $r'\colon \mathbb{F}_2^n \to \mathbb{F}_2$ EA-equivalent to r such that the two functions

$$\begin{pmatrix} x \\ y \end{pmatrix} \mapsto \begin{pmatrix} G(x) \\ r(x) \end{pmatrix} + \begin{pmatrix} L(x) \\ \ell(x) \end{pmatrix} \cdot y, \quad \begin{pmatrix} x \\ y \end{pmatrix} \mapsto \begin{pmatrix} G'(x) \\ r'(x) \end{pmatrix} + \begin{pmatrix} L'(x) \\ \ell'(x) \end{pmatrix} \cdot y$$

are EA-equivalent as well. Further, note that if T is given in the same form as in Proposition 4, the EA-equivalence class of G is contained within the trim spectrum of T by choosing $H = \mathbb{F}_2^n \times \{0\}$ and $\beta = e_{n+1}$.

Using a recursive tree search similar to the approach described in [1,2], we conducted a search for 8-bit quadratic APN functions that are an extension of a quadratic APN function in dimension seven. In particular, we applied the following search procedure:

1. Fix a representative $G\colon \mathbb{F}_2^7 \to \mathbb{F}_2^7$ of one of the 488 EA-equivalence classes of 7-bit quadratic APN functions.
2. Guess the Boolean function r of a possible APN extension T of G in standard form, i.e., randomly choose a function $r\colon \mathbb{F}_2^n \to \mathbb{F}_2$ of algebraic degree at most 2.
3. Recursively construct the linear function $(L, \ell)\colon \mathbb{F}_2^n \times \mathbb{F}_2 \to \mathbb{F}_2^n \times \mathbb{F}_2$ such that T is APN. In case there is a contradiction with the property of T being APN, the recursive algorithm backtracks. If a suitable function (L, ℓ) cannot be found after a predetermined number of iterations, we abort the search. Otherwise, we found an APN extension of G.

By repeatedly iterating the above algorithm, we found 6,368 new quadratic APN functions in dimension eight up to EA-equivalence. With our implementation, it takes about 2 CPU hours to find one APN extension in dimension eight. The new APN functions are available in the dataset [3] and our implementation is available at [4]. The check for EA-inequivalence to the previously-known APN functions was done using the method explained in [12]. In particular, we computed the extended Walsh spectra and the differential spectra of the ortho-derivatives of all the known and found quadratic 8-bit APN functions, which is a strongly discriminating EA-invariant.

As our new 8-bit APN functions are extensions of quadratic 7-bit APN functions by construction, they are all connected to some nodes at height 7 in the trimming graph. From the previously-known 8-bit APN functions (see Fig. 2), one might expect that there are only a few of the quadratic 7-bit APN functions that can be extended to quadratic 8-bit APN functions. However, it turns out that the vast majority of the quadratic APN functions in dimension $n = 7$ can be extended to a quadratic APN function in dimension $n = 8$. In fact, this observation is the reason we raised Conjecture 1.

Remark 4 It is possible to further restrict the definition of an "APN extension of G in standard form". Let $\mathcal{Q}_n$ be the set of quadratic homogeneous Boolean functions mapping n bits to 1, i.e. the set of n-bit quadratic Boolean functions with no linear or constant terms. Furthermore, let G be an n-bit quadratic APN function, and let (G, r, L, ℓ) yield an APN function T. Then we can impose for r to be in $\mathcal{Q}_n$, and for all coordinates G_i of G to be in $\mathcal{Q}_n$ as well: removing all affine terms is the same as adding an affine function to the output of T, which would not change its EA-equivalence class. This first restriction means that r can be searched for in a space of dimension $n(n-1)/2$. We can go further. In the procedure outlined above for extending a given function G, we first guess r and then find (L, ℓ). For a given r, setting $r' = r + \sum_i \epsilon_i G_i$ for some $\epsilon \in \mathbb{F}_2^n$ and then searching for all (L, ℓ) would yield the same EA-equivalence classes as starting from r. Indeed, we would simply find pairs (L, ℓ') where ℓ is replaced by $\ell' = \ell + \sum_i \epsilon_i L_i$. Thus, we can safely search for r in the complement of the span of the coordinates of G, i.e. in a space of dimension $n(n-1)/2 - n$. For $n = 7$, this quantity is only equal to 15. Unfortunately, for a given tuple $(G \colon \mathbb{F}_2^7 \to \mathbb{F}_2^7, r \colon \mathbb{F}_2^7 \to \mathbb{F}_2)$, exhausting all pairs (L, ℓ) using our implementation already takes several minutes, and exhausting all possible such pairs for each of the $488 \cdot 2^{15}$ choices of (G, r) is simply infeasible. Thus, while this reduction of the search space would work, it would be of no practical impact at this stage due to the cost of finding (L, ℓ). Still, should progress be made in this direction, it might become possible to exhaustively find all quadratic 8-bit APN extensions of quadratic APN functions in dimension $n = 7$.

The number of known instances of 8-bit APN functions The 6,368 APN functions constructed in this work together with the 23 APN functions listed in [17] (including one non-quadratic monomial function), the 8,157 APN functions constructed by the QAM method [31], the 10 APN functions presented in [28], the two APN functions from the Taniguchi family [27], the 12,921 APN functions from [2], and the 5,412 APN functions presented in [30], are all APN functions in dimension eight up to CCZ-equivalence known until January 2022 (32,893 in total).

5 Quadratic APN functions with maximum linearity

The following simple observation illustrates how a quadratic function in dimension $n + 1$ and having linearity 2^n can be obtained as an extension of a function on n bit. A similar argument (for APN functions) was already given in [13, Remark 12].

Proposition 5 *Let $F \colon \mathbb{F}_2^{n+1} \to \mathbb{F}_2^{n+1}$ be a quadratic function with linearity 2^n. Then, there exists a function $G \colon \mathbb{F}_2^n \to \mathbb{F}_2^n$ of algebraic degree at most 2 and two linear functions $L \colon \mathbb{F}_2^n \to \mathbb{F}_2^n, \ell \colon \mathbb{F}_2^n \to \mathbb{F}_2, \ell \neq 0$ such that F is EA-equivalent to*

$$T \colon \mathbb{F}_2^n \times \mathbb{F}_2 \to \mathbb{F}_2^n \times \mathbb{F}_2$$
$$\begin{pmatrix} x \\ y \end{pmatrix} \mapsto \begin{pmatrix} G(x) \\ 0 \end{pmatrix} + \begin{pmatrix} L(x) \\ \ell(x) \end{pmatrix} \cdot y \ .$$

Proof Since $F \colon \mathbb{F}_2^{n+1} \to \mathbb{F}_2^{n+1}$ is a quadratic function with linearity 2^n, it consists of a component which is EA-equivalent to $(x, y) \mapsto \ell(x)y$ for a linear function $\ell \colon \mathbb{F}_2^n \to \mathbb{F}_2, \ell \neq 0$, see [14, Thm.10 and p. 173]. Therefore, by applying an EA-transformation to F, we can obtain a function

$$T \colon \mathbb{F}_2^n \times \mathbb{F}_2 \to \mathbb{F}_2^n \times \mathbb{F}_2, \begin{pmatrix} x \\ y \end{pmatrix} \mapsto \begin{pmatrix} H(x, y) \\ \ell(x)y \end{pmatrix} \ ,$$

where $H : \mathbb{F}_2^n \times \mathbb{F}_2 \to \mathbb{F}_2^n$ is of algebraic degree at most 2, $H(0, 0) = H(0, 1) = 0$ and $\ell : \mathbb{F}_2^n \to \mathbb{F}_2, \ell \neq 0$ is linear. Then, by defining $G(x) = H(x, 0)$, we obtain

$$T \begin{pmatrix} x \\ y \end{pmatrix} = \begin{pmatrix} G(x) \\ 0 \end{pmatrix} (y + 1) + \begin{pmatrix} H(x, 1) \\ \ell(x) \end{pmatrix} y . \tag{3}$$

Note that since G is a restriction of H to a linear hyperplane, it is also of algebraic degree at most 2. Now, T is quadratic if and only if $x \mapsto G(x) + H(x, 1)$ is of algebraic degree at most 1, which means that $H(x, 1) = G(x) + L(x)$ for an affine function L. Since we chose $H(0, 1) = H(0, 0) = 0$, we have $L(0) = 0$ and L must therefore be linear.   □

Remark 5 For any linear mappings $L : \mathbb{F}_2^n \to \mathbb{F}_2^n, \ell : \mathbb{F}_2^n \to \mathbb{F}_2, \ell \neq 0$, we remark that if two functions $G, G' : \mathbb{F}_2^n \to \mathbb{F}_2^n$ are EA-equivalent, there exist linear mappings $L' : \mathbb{F}_2^n \to \mathbb{F}_2^n, \ell' : \mathbb{F}_2^n \to \mathbb{F}_2, \ell' \neq 0$ such that the two functions

$$\begin{pmatrix} x \\ y \end{pmatrix} \mapsto \begin{pmatrix} G(x) \\ 0 \end{pmatrix} + \begin{pmatrix} L(x) \\ \ell(x) \end{pmatrix} \cdot y, \quad \begin{pmatrix} x \\ y \end{pmatrix} \mapsto \begin{pmatrix} G'(x) \\ 0 \end{pmatrix} + \begin{pmatrix} L'(x) \\ \ell'(x) \end{pmatrix} \cdot y$$

are EA-equivalent as well. Thus, the function G as in Proposition 5 can be chosen up to EA-equivalence.

We now deduce when the functions T of the same form as given in Proposition 5 are APN.

Theorem 1 *Let $G : \mathbb{F}_2^n \to \mathbb{F}_2^n$ be a function of algebraic degree at most 2, $L : \mathbb{F}_2^n \to \mathbb{F}_2^n$ be linear and $\ell : \mathbb{F}_2^n \to \mathbb{F}_2, \ell \neq 0$ be linear. Then*

$$T : \mathbb{F}_2^n \times \mathbb{F}_2 \to \mathbb{F}_2^n \times \mathbb{F}_2$$
$$\begin{pmatrix} x \\ y \end{pmatrix} \mapsto \begin{pmatrix} G(x) \\ 0 \end{pmatrix} + \begin{pmatrix} L(x) \\ \ell(x) \end{pmatrix} \cdot y$$

is APN if and only if the following two assertions hold:

1. *G is APN.*
2. *$\langle \pi_G(\alpha), L(\alpha) \rangle = 1$ for all $\alpha \in \mathbb{F}_2^n \setminus \{0\}$ with $\ell(\alpha) = 0$.*

Proof By definition, the function T is APN if and only if, for all $\alpha, \gamma \in \mathbb{F}_2^n, \beta, \delta \in \mathbb{F}_2$ with $(\alpha, \beta) \neq (0, 0)$, the equation

$$T \begin{pmatrix} x \\ y \end{pmatrix} + T \begin{pmatrix} x + \alpha \\ y + \beta \end{pmatrix} = \begin{pmatrix} \gamma \\ \delta \end{pmatrix} \tag{4}$$

has at most two solutions $(x, y) \in \mathbb{F}_2^n \times \mathbb{F}_2$. By the definition of T, Eq. (4) is equivalent to

$$\begin{pmatrix} G(x) + G(x + \alpha) \\ 0 \end{pmatrix} + \begin{pmatrix} L(\alpha) \\ \ell(\alpha) \end{pmatrix} y + \begin{pmatrix} L(x) \\ \ell(x) \end{pmatrix} \beta + \begin{pmatrix} L(\alpha) \\ \ell(\alpha) \end{pmatrix} \beta = \begin{pmatrix} \gamma \\ \delta \end{pmatrix} . \tag{5}$$

For every $\alpha \in \mathbb{F}_2^n$, we recall that B_α is defined as $B_\alpha : \mathbb{F}_2^n \to \mathbb{F}_2^n, x \mapsto G(x) + G(x + \alpha) + G(\alpha) + G(0)$, which is a linear mapping if G is of algebraic degree at most 2. We now consider two cases.

Case $\beta = 0, \alpha \neq 0$ For $y = 0$, Eq. (5) simplifies to the system $(B_\alpha(x) = \gamma + G(\alpha) + G(0)) \wedge (\delta = 0)$, which directly yields that G being APN is a necessary condition for T being APN. Conversely, if G is APN, this system has at most 2 solutions $x \in \mathbb{F}_2^n$.

For $y = 1$, Eq. (5) simplifies to

$$\begin{pmatrix} B_\alpha(x) \\ \ell(\alpha) \end{pmatrix} = \begin{pmatrix} \gamma + G(\alpha) + G(0) + L(\alpha) \\ \delta \end{pmatrix} . \tag{6}$$

Similarly as above, Eq. (6) has no more than two solutions $x \in \mathbb{F}_2^n$ if G is APN. For T being APN, we also need to require that Eq. (6) has no solutions $x \in \mathbb{F}_2^n$ in the case where both $\ell(\alpha) = 0$ and $\gamma + G(\alpha) + G(0) \in \mathcal{I}m(B_\alpha)$. This is equivalent to the condition that $L(\alpha) \notin \mathcal{I}m(B_\alpha)$ whenever $\ell(\alpha) = 0$. Since $\mathcal{I}m(B_\alpha) = \{x \in \mathbb{F}_2^n \mid \langle \pi_G(\alpha), x \rangle = 0\}$ we obtain that $\langle \pi_G(\alpha), L(\alpha) \rangle = 1$ for all $\alpha \in \mathbb{F}_2^n \setminus \{0\}$ with $\ell(\alpha) = 0$.

To summarize, the two conditions 1 and 2 in the statement of the theorem are necessary and sufficient for Eq. (5) having at most 2 solutions $(x, y) \in \mathbb{F}_2^n \times \mathbb{F}_2$ for all $\alpha, \gamma \in \mathbb{F}_2^n$, $\beta, \delta \in \mathbb{F}_2$ with $\beta = 0, \alpha \neq 0$.

Case $\beta = 1$ We will show that Condition 2 of the statement is a sufficient condition for Eq. (5) having at most 2 solutions $(x, y) \in \mathbb{F}_2^n \times \mathbb{F}_2$.

For $y = 1$, Eq. (5) simplifies to

$$\begin{pmatrix} G(x) + G(x + \alpha) + L(x) \\ \ell(x) \end{pmatrix} = \begin{pmatrix} \gamma \\ \delta \end{pmatrix} \tag{7}$$

and for $y = 0$, Eq. (5) simplifies to

$$\begin{pmatrix} G(x) + G(x + \alpha) + L(x + \alpha) \\ \ell(x + \alpha) \end{pmatrix} = \begin{pmatrix} \gamma \\ \delta \end{pmatrix}. \tag{8}$$

An element $x \in \mathbb{F}_2^n$ is a solution of Eq. (7) if and only if $x + \alpha$ is a solution of Eq. (8). Therefore, for Eq. (5) having at most two solutions $(x, y) \in \mathbb{F}_2^n \times \mathbb{F}_2$, we need that Eq. (7) has at most 1 solution $x \in \mathbb{F}_2^n$. In other words, we need to show that the mapping

$$H_\alpha \colon \mathbb{F}_2^n \to \mathbb{F}_2^n \times \mathbb{F}_2, x \mapsto \begin{pmatrix} G(x) + G(x + \alpha) + L(x) \\ \ell(x) \end{pmatrix}$$

is injective. For this, let us choose an arbitrary element $x \in \mathbb{F}_2^n$ and a non-zero element $w \in \mathbb{F}_2^n$ and consider $H_\alpha(x) + H_\alpha(x + w)$, which is equal to

$$\begin{pmatrix} G(x) + G(x + \alpha) + G(x + w) + G(x + w + \alpha) + L(w) \\ \ell(w) \end{pmatrix}. \tag{9}$$

Since G is of algebraic degree at most 2, the mapping $x \mapsto G(x) + G(x + \alpha) + G(x + w) + G(x + w + \alpha)$ is constant. Thus,

$$H_\alpha(x) + H_\alpha(x + w) = H_\alpha(0) + H_\alpha(w) = \begin{pmatrix} B_w(\alpha) + L(w) \\ \ell(w) \end{pmatrix}.$$

The right-hand side can only be equal to 0 if $L(w) \in \mathcal{I}m(B_w)$ and $\ell(w) = 0$. Therefore, if $L(w) \notin \mathcal{I}m(B_w)$ for all $w \in \mathbb{F}_2^n \setminus \{0\}$ with $\ell(w) = 0$, the mapping H_α must be injective. □

Note that Condition 2 of Theorem 1 implies that the mapping

$$H_0 \colon \mathbb{F}_2^n \to \mathbb{F}_2^n \times \mathbb{F}_2$$
$$x \mapsto \begin{pmatrix} L(x) \\ \ell(x) \end{pmatrix}$$

has full rank equal to n. In particular, if T is APN, L can only be of rank n or $n - 1$. We further remark that, if $n > 2$ and T is APN, the APN function G must actually be quadratic (since affine functions in dimension $n > 2$ cannot be APN).

Corollary 2 *Let $G \colon \mathbb{F}_2^n \to \mathbb{F}_2^n$ be a quadratic APN function. G is 0-extendable if there exist linear functions $L \colon \mathbb{F}_2^n \to \mathbb{F}_2^n$ and $\ell \colon \mathbb{F}_2^n \to \mathbb{F}_2, \ell \neq 0$ such that $\langle \pi_G(x), L(x) \rangle = 1$ for all $x \in \mathbb{F}_2^n \setminus \{0\}$ with $\ell(x) = 0$.*

From Remark 5, it is obvious that the property of being 0-extendable is invariant under EA-equivalence. Moreover, since quadratic APN functions in odd dimension must be almost bent, 0-extendable APN functions can only exist in dimension $n = 2$ or in odd dimension n.

Let us now define the set

$$\Gamma_{G,\ell} := \{L \in \mathcal{L}(\mathbb{F}_2^n, \mathbb{F}_2^n) \mid \langle \pi_G(x), L(x) \rangle = 1 \text{ for all } x \in \mathbb{F}_2^n \setminus \{0\} \text{ with } \ell(x) = 0\},$$

which is either empty or an affine subspace of $\mathcal{L}(\mathbb{F}_2^n, \mathbb{F}_2^n)$. Given G and ℓ, the set $\Gamma_{G,\ell}$ can be recovered by first computing the ortho-derivative of G and by then solving a system of 2^{n-1} linear equations with n^2 unknowns. The following proposition yields a lower bound on $|\Gamma_{G,\ell}|$ in cases where $\Gamma_{G,\ell} \neq \emptyset$.

Proposition 6 *Let $n \in \mathbb{N}$, $n \geq 3$. Let $G : \mathbb{F}_2^n \to \mathbb{F}_2^n$ be a quadratic mapping, $L : \mathbb{F}_2^n \to \mathbb{F}_2^n$ be linear and $\ell : \mathbb{F}_2^n \to \mathbb{F}_2$, $\ell \neq 0$ be linear such that $(G, 0, L, \ell)$ yields an APN function T. For all $\mu, \nu \in \mathbb{F}_2^n$, the tuple $(G, 0, L + B_\mu + \ell\nu, \ell)$ yields an APN function EA-equivalent to T, where $B_\mu : \mathbb{F}_2^n \to \mathbb{F}_2^n$, $x \mapsto G(x) + G(x + \mu) + G(\mu) + G(0)$.*

The functions $L + B_\mu + \ell\nu$ are pairwise distinct for $\mu, \nu \in \mathbb{F}_2^n$. Moreover, for every $\mu \in \mathbb{F}_2^n$, we have

$$2^{n-1} = |\{\nu \in \mathbb{F}_2^n \mid \text{Rank}(L + B_\mu + \ell\nu) = n\}|$$
$$= |\{\nu \in \mathbb{F}_2^n \mid \text{Rank}(L + B_\mu + \ell\nu) = n - 1\}| .$$

Proof For an element $c \in \mathbb{F}_2^n$, let us consider the linear involution

$$M_c : \mathbb{F}_2^n \times \mathbb{F}_2 \to \mathbb{F}_2^n \times \mathbb{F}_2$$
$$\begin{pmatrix} x \\ y \end{pmatrix} \mapsto \begin{pmatrix} x + cy \\ y \end{pmatrix} .$$

For $\mu \in \mathbb{F}_2^n$, let us consider the function

$$T'_\mu : \mathbb{F}_2^n \times \mathbb{F}_2 \to \mathbb{F}_2^n \times \mathbb{F}_2$$
$$\begin{pmatrix} x \\ y \end{pmatrix} \mapsto T M_\mu \begin{pmatrix} x \\ y \end{pmatrix} + \begin{pmatrix} L(\mu) + G(\mu) + G(0) \\ \ell(\mu) \end{pmatrix} \cdot y .$$

By definition, T'_μ is EA-equivalent to T. Using the representation of T given in Eq. (3), we obtain

$$T'_\mu \begin{pmatrix} x \\ y \end{pmatrix} = \begin{pmatrix} G(x + \mu y) \\ 0 \end{pmatrix} (y + 1) + \begin{pmatrix} G(x + \mu y) + L(x + \mu y) \\ \ell(x + \mu y) \end{pmatrix} y$$
$$+ \begin{pmatrix} L(\mu) + G(\mu) + G(0) \\ \ell(\mu) \end{pmatrix} y$$
$$= \begin{pmatrix} G(x) \\ 0 \end{pmatrix} (y + 1) + \begin{pmatrix} G(x + \mu) + G(\mu) + G(0) + L(x) \\ \ell(x) \end{pmatrix} y$$
$$= \begin{pmatrix} G(x) \\ 0 \end{pmatrix} (y + 1) + \begin{pmatrix} G(x) + L(x) + B_\mu(x) \\ \ell(x) \end{pmatrix} y$$
$$= \begin{pmatrix} G(x) \\ 0 \end{pmatrix} + \begin{pmatrix} (L + B_\mu)(x) \\ \ell(x) \end{pmatrix} y ,$$

which is of the same form as in Theorem 1. Thus, $(G, 0, L + B_\mu, \ell)$ yields the APN function T'_μ.

For an element $v \in \mathbb{F}_2^n$, we obtain

$$M_v T \begin{pmatrix} x \\ y \end{pmatrix} = \begin{pmatrix} G(x) \\ 0 \end{pmatrix} + \begin{pmatrix} (L + \ell v)(x) \\ \ell(x) \end{pmatrix} y .$$

The function $M_v T$ is also EA-equivalent to T and of the same form as in Theorem 1. Thus, $(G, 0, L + \ell v, \ell)$ yields the APN function $M_v T$. Combining the above, we obtain that $(G, 0, L + B_\mu + v\ell, \ell)$ yields the APN function $M_v T'_\mu$, which is EA-equivalent to T.

To see that the functions $L + B_\mu + \ell v$ are pairwise distinct for all $\mu, v \in \mathbb{F}_2^n$, we need to show that the linear mapping

$$J : \mathbb{F}_2^n \times \mathbb{F}_2^n \to \mathcal{L}(\mathbb{F}_2^n, \mathbb{F}_2^n)$$
$$\begin{pmatrix} \mu \\ v \end{pmatrix} \mapsto B_\mu + \ell v$$

is injective. We show that the kernel of J is trivial. Suppose that, for all $x \in \mathbb{F}_2^n$, we have $B_\mu(x) + \ell(x)v = 0$. This implies $B_\mu(x) = v$ for all $x \in \mathbb{F}_2^n$ with $\ell(x) = 1$. Since ℓ is not the zero mapping and since B_μ is 2-to-1 for every non-zero μ, we have $\mu = 0$. From $\mu = 0$, we immediately deduce $v = 0$, so the kernel of J is trivial.

To prove the last statement, let us fix an element $\mu \in \mathbb{F}_2^n$. We consider $L' := L + B_\mu$. Suppose that $\mathrm{Rank}(L') \neq n$. We can choose an element $v \in \mathbb{F}_2^n$ such that $v \notin \mathcal{I}m(L')$. For such v, we have that $\mathrm{Rank}(L' + \ell v) = n$. This can be observed by looking at the kernel of $L' + \ell v$. For all $x \in \mathbb{F}_2^n$ with $\ell(x) = 0$, we have $L'(x) + \ell(x)v = L'(x) = 0$ if and only if $x = 0$, since $\mathrm{Rank}((L', \ell)) = n$. For all $x \in \mathbb{F}_2^n$ with $\ell(x) = 1$, we have $L'(x) + \ell(x)v = 0$ if and only if $L'(x) = v$, which is not possible since $v \notin \mathcal{I}m(L')$. Therefore, there exists an element $v \in \mathbb{F}_2^n$ such that $L'' := L + J(\mu, v)$ is invertible. By using a similar argument as above we obtain that, for all $v' \in \mathbb{F}_2^n$, the mapping $L'' + \ell v'$ is invertible if and only if $\ell(L''^{-1}(v')) = 0$. The statement follows since there are exactly 2^{n-1} elements $v' \in \mathbb{F}_2^n$ with $\ell(L''^{-1}(v')) = 0$. □

Let $G : \mathbb{F}_2^n \to \mathbb{F}_2^n$ be a quadratic APN function and $\ell : \mathbb{F}_2^n \to \mathbb{F}_2$, $\ell \neq 0$ be linear. The above proposition states that, if $\Gamma_{G,\ell} \neq \emptyset$, we have $|\Gamma_{G,\ell}| \geq 2^{2n}$. We say that two elements $L, L' \in \Gamma_{G,\ell}$ are Γ-*equivalent* if there exist $\mu, v \in \mathbb{F}_2^n$ such that $L' = L + B_\mu + \ell v$. As it was shown in Proposition 6, if $L, L' \in \Gamma_{G,\ell}$ are Γ-equivalent, the tuples $(G, 0, L, \ell)$ and $(G, 0, L', \ell)$ yield EA-equivalent APN functions.

5.1 A classification in dimension eight

Recently, Kalgin and Idrisova completely classified all quadratic 7-bit APN functions [20]. In total, there are 488 such functions up to EA-equivalence. By using this classification and by applying the results from Theorem 1 and Proposition 6, we can now classify *all* 8-bit quadratic APN functions with linearity 2^7.

Let $\mathcal{G} = \{G_1, G_2, \ldots, G_{488}\}$ be a set of 7-bit quadratic APN functions that contains one representative of each EA-equivalence class. Algorithm 1 describes how $\mathcal{G}$ can be used to obtain a classification of 8-bit quadratic APN functions with maximum linearity up to EA-equivalence.

A sage [26] implementation of Algorithm 1 is given in Appendix B. For each quadratic 7-bit APN function G, the running time of the ZEROEXTENSIONS procedure is less than one second on a PC. To execute this code, the library sboxU [25] is needed.

There are exactly four functions G in $\mathcal{G}$ for which there exists a $\gamma \in \mathbb{F}_2^7$ such that that $\Gamma_{G, x \mapsto \langle \gamma, x \rangle}$ is not empty. Moreover, for each of those four functions, there is exactly one

Algorithm 1 Classification of 8-bit quadratic APN functions with maximum linearity up to EA-equivalence

---

1: **function** ZeroExtensions(G)   ▷ $G \colon \mathbb{F}_2^n \to \mathbb{F}_2^n$ is a quadratic APN function
2:      sol $\leftarrow \emptyset$
3:      **for** $\gamma \in \mathbb{F}_2^n \setminus \{0\}$ **do**
4:          Compute $\Gamma_{G, x \mapsto \langle \gamma, x \rangle}$ by solving a linear system
5:          **for** $L \in \Gamma_{G, x \mapsto \langle \gamma, x \rangle}$ up to Γ-equivalence **do**
6:              sol $\leftarrow$ sol $\cup\, T$, where T is such that $(G, 0, L, x \mapsto \langle \gamma, x \rangle)$ yields T
7:          **end for**
8:      **end for**
9:      **return** sol
10: **end function**

11: sol $\leftarrow \emptyset$
12: **for** $G \in \mathcal{G}$ **do**
13:      sol $\leftarrow$ sol $\cup$ ZeroExtensions(G)
14: **end for**
15: **return** sol

---

such γ. The space $\Gamma_{G, x \mapsto \langle \gamma, x \rangle}$ is of size 2^{14} in all those cases, implying that there is only one element in $\Gamma_{G, x \mapsto \langle \gamma, x \rangle}$ up to Γ-equivalence. Thus, Algorithm 1 outputs four 8-bit quadratic APN functions with linearity 2^7. Those are pairwise inequivalent up to EA-equivalence. More precisely, they correspond to the four EA-equivalence classes reported in [2]. While in [2], the authors have shown that there are *at least* four pairwise EA-inequivalent quadratic APN functions in dimension eight with maximum linearity, by using Algorithm 1 we now deduced that there are *exactly* four such EA-equivalence classes.

Theorem 2 *In dimension eight, there are exactly four quadratic APN functions with linearity* 2^7 *up to EA-equivalence.*

We give representatives of those four EA-equivalence classes in Sect. 5.2 using a simpler representation.

Searching for 0-extensions of 9-bit and 11-bit quadratic APN functions For all of the 60 known instances of 9-bit quadratic APN functions, we checked whether there exists a $\gamma \in \mathbb{F}_2^9$ such that $\Gamma_{G, x \mapsto \langle \gamma, x \rangle}$ is non-empty. This is never the case. Thus, up to now, we do not know a quadratic 9-bit APN function that can be extended to a quadratic 10-bit APN function with linearity 2^9.

We also checked whether any of the known quadratic 11-bit APN functions coming from a known infinite family of APN functions (see the list in [5]) is 0-extendable. In particular, we checked the quadratic monomial functions and the function $\mathbb{F}_{2^{11}} \to \mathbb{F}_{2^{11}}, x \mapsto x^3 + \mathrm{Tr}\left(x^9\right)$ discovered in [10]. Also, none of those functions is 0-extendable.

5.2 A simpler representation

As a summary of previous results, we can assume without loss of generality that quadratic APN functions with maximum linearity are of the following form.

Theorem 3 *Let* $n \in \mathbb{N}, n \geq 3$ *and let* $\gamma \in \mathbb{F}_2^n \setminus \{0\}$ *be an arbitrary non-zero element. Let* $T \colon \mathbb{F}_2^n \times \mathbb{F}_2 \to \mathbb{F}_2^n \times \mathbb{F}_2$ *be a quadratic APN function with linearity* 2^n. *Then, there exist a quadratic APN function* $G \colon \mathbb{F}_2^n \to \mathbb{F}_2^n$ *such that* $\langle \pi_G(\alpha), \alpha \rangle = 1$ *for all* $\alpha \in \mathbb{F}_2^n \setminus \{0\}$ *with* $\langle \gamma, \alpha \rangle = 0$. *More precisely,* T *is EA-equivalent to*

$$\mathbb{F}_2^n \times \mathbb{F}_2 \to \mathbb{F}_2^n \times \mathbb{F}_2$$
$$\begin{pmatrix} x \\ y \end{pmatrix} \mapsto \begin{pmatrix} G(x) \\ 0 \end{pmatrix} + \begin{pmatrix} x \\ \langle \gamma, x \rangle \end{pmatrix} \cdot y .$$

Proof By Theorem 1, we know that there exist a quadratic APN function $Q : \mathbb{F}_2^n \to \mathbb{F}_2^n$, a linear mapping $L : \mathbb{F}_2^n \to \mathbb{F}_2^n$, and an element $\delta \in \mathbb{F}_2^n \setminus \{0\}$ such that $(Q, 0, L, x \mapsto \langle \delta, x \rangle)$ yields T. By Proposition 6, we can assume without loss of generality that L is invertible (then $(Q, 0, L, x \mapsto \langle \delta, x \rangle)$ does not necessarily yield T, but an APN function T' EA-equivalent to T). We then have

$$T' : \mathbb{F}_2^n \times \mathbb{F}_2 \to \mathbb{F}_2^n \times \mathbb{F}_2$$
$$\begin{pmatrix} x \\ y \end{pmatrix} \mapsto \begin{pmatrix} Q(x) \\ 0 \end{pmatrix} + \begin{pmatrix} L(x) \\ \langle \delta, x \rangle \end{pmatrix} \cdot y .$$

Let us choose an invertible linear mapping $L' : \mathbb{F}_2^n \to \mathbb{F}_2^n$ with $L'^\top(\delta) = \gamma$. It is straightforward to deduce that T' is EA-equivalent to

$$\mathbb{F}_2^n \times \mathbb{F}_2 \to \mathbb{F}_2^n \times \mathbb{F}_2$$
$$\begin{pmatrix} x \\ y \end{pmatrix} \mapsto \begin{pmatrix} L'^{-1} L^{-1} \circ Q \circ L'(x) \\ 0 \end{pmatrix} + \begin{pmatrix} x \\ \langle \gamma, x \rangle \end{pmatrix} \cdot y .$$

The result follows by defining $G := (LL')^{-1} \circ Q \circ L'$. $\qquad\square$

Remark 6 Let $g \in \mathbb{F}_{2^7}$ be an element with minimal polynomial $X^7 + X + 1$. We can represent the four pairwise EA-inequivalent quadratic APN functions in dimension eight with maximum linearity by the four functions $T_8^{(1)}, T_8^{(2)}, T_8^{(3)}, T_8^{(4)}$, where

$$T_8^{(i)} : \mathbb{F}_{2^7} \times \mathbb{F}_2 \to \mathbb{F}_{2^7} \times \mathbb{F}_2$$
$$\begin{pmatrix} x \\ y \end{pmatrix} \mapsto \begin{pmatrix} G_i(x) \\ 0 \end{pmatrix} + \begin{pmatrix} x \\ \mathrm{Tr}\,(x) \end{pmatrix} \cdot y$$

and where G_i are the four 7-bit quadratic APN functions defined in univariate representation by

$$G_1(x) = g^{92}x^{96} + g^{50}x^{80} + g^{27}x^{72} + g^{28}x^{68} + x^{66} + g^{97}x^{65} + g^{60}x^{48}$$
$$+ g^{88}x^{40} + g^{123}x^{36} + g^{43}x^{34} + g^{32}x^{33} + g^{26}x^{24} + g^{100}x^{20} + g^{115}x^{18}$$
$$+ g^{85}x^{17} + g^{111}x^{12} + g^{28}x^{10} + g^{93}x^9 + g^{113}x^6 + g^{53}x^5 + g^{10}x^3$$
$$G_2(x) = g^{68}x^{96} + g^3 x^{80} + g^{58}x^{72} + g^{39}x^{68} + g^{43}x^{66} + g^{96}x^{65} + g^{118}x^{48}$$
$$+ g^{102}x^{40} + g^{61}x^{36} + g^{69}x^{34} + g^{59}x^{33} + g^{110}x^{24} + g^{99}x^{20} + g^{53}x^{18}$$
$$+ g^{63}x^{17} + g^{55}x^{12} + g^{98}x^{10} + g^{31}x^9 + g^{57}x^6 + g^{69}x^5 + g^{87}x^3$$
$$G_3(x) = g^{71}x^{96} + g^{46}x^{80} + g^{15}x^{72} + g^{126}x^{68} + g^{44}x^{65} + g^{38}x^{48}$$
$$+ g^{104}x^{40} + x^{36} + g^{73}x^{34} + g^{83}x^{33} + g^{38}x^{24} + g^3 x^{20} + g^{120}x^{18}$$
$$+ g^{34}x^{17} + g^{78}x^{12} + g^{108}x^{10} + g^{28}x^9 + g^{113}x^6 + g^{100}x^5 + g^{70}x^3$$
$$G_4(x) = g^{71}x^{96} + g^{20}x^{80} + g^{125}x^{72} + g^{40}x^{68} + g^{71}x^{66} + g^{75}x^{65} + g^{113}x^{48}$$
$$+ g^{100}x^{40} + g^{29}x^{36} + g^{62}x^{34} + g^{40}x^{33} + g^{97}x^{24} + g^{22}x^{20} + g^{111}x^{18}$$
$$+ g^{106}x^{17} + g^{86}x^{12} + g^{29}x^{10} + gx^9 + g^{64}x^6 + g^{51}x^5 + g^{16}x^3 .$$

The Walsh transform of quadratic APN functions with maximum linearity To deduce the Walsh spectrum of a quadratic APN function with maximum linearity, we need the following well-known result on the sum of fourth powers of the Walsh coefficients of APN functions.

Lemma 1 *[16] Let $F : \mathbb{F}_2^n \to \mathbb{F}_2^n$. Then the following two statements are equivalent:*

1. *F is APN.*
2. *$\sum_{a,b\in\mathbb{F}_2^n, b\neq 0} \widehat{F}_b^4(a) = 2^{4n+1} - 2^{3n+1}$.*

Theorem 4 *Let $n \in \mathbb{N}$, $n \geq 3$ be odd and let $F : \mathbb{F}_2^{n+1} \to \mathbb{F}_2^{n+1}$ be a quadratic APN function with linearity 2^n. Then, F consists of 2^{n-1} components whose Walsh transform only take values in $\{0, \pm 2^{\frac{n+3}{2}}\}$ (i.e., semi-bent components), $2^{n+1} - 2 - 2^{n-1}$ components whose Walsh transform only take values in $\{\pm 2^{\frac{n+1}{2}}\}$ (i.e., bent components), and a single component with linearity 2^n.*

Proof Let $T : \mathbb{F}_2^n \times \mathbb{F}_2 \to \mathbb{F}_2^n \times \mathbb{F}_2$ be a function EA-equivalent to F and in the form as given in Theorem 3. For $a, b \in \mathbb{F}_2^n$ and $\bar{a}, \bar{b} \in \mathbb{F}_2$, it is straightforward to deduce that

$$\widehat{T}_{(b,\bar{b})}(a, \bar{a}) = \begin{cases} \widehat{G}_b(a) + (-1)^{\bar{a}} \widehat{G}_b(a+b) & \text{if } \bar{b} = 0 \\ \widehat{G}_b(a) + (-1)^{\bar{a}} \widehat{G}_b(a+b+\gamma) & \text{if } \bar{b} = 1 \end{cases}.$$

If $b = 0$, we only have one component $(b, \bar{b}) = (0, 1)$. In this case, we obtain $\widehat{T}_{(0,\bar{1})}(a, \bar{a}) = \widehat{G}_0(a) + (-1)^{\bar{a}} \widehat{G}_0(a+\gamma)$, which evaluates to 0 if and only if $(a, \bar{a}) \notin \{(0, 0), (0, 1), (\gamma, 0), (\gamma, 1)\}$. Otherwise, $\widehat{T}_{(0,\bar{1})}(a, \bar{a})$ evaluates to $\pm 2^n$.

Let us now consider the case $b \neq 0$. Since G is a quadratic APN function in odd dimension n, it must be almost bent. In other words, its component functions are all semi-bent, i.e., for all $a \in \mathbb{F}_2^n$, we have $\widehat{G}_b(a) \in \{0, \pm 2^{\frac{n+1}{2}}\}$. Therefore, each component function $(b, \bar{b})$ of T with $b \neq 0$ is either bent (i.e., $\forall(a, \bar{a}) \in \mathbb{F}_2^n \times \mathbb{F}_2 : \widehat{T}_{(b,\bar{b})}(a, \bar{a}) \in \{\pm 2^{\frac{n+1}{2}}\}$) or semi-bent (i.e., $\forall(a, \bar{a}) \in \mathbb{F}_2^n \times \mathbb{F}_2 : \widehat{T}_{(b,\bar{b})}(a, \bar{a}) \in \{0, \pm 2^{\frac{n+3}{2}}\}$).

Let k denote the number of semi-bent components of F and let the sets A, B, C be defined as follows:

$$A := \{(a, b) \in \mathbb{F}_2^{n+1} \times \mathbb{F}_2^{n+1} \setminus \{0\} \mid |\widehat{F}_b(a)| = 2^n\}$$
$$B := \{(a, b) \in \mathbb{F}_2^{n+1} \times \mathbb{F}_2^{n+1} \setminus \{0\} \mid |\widehat{F}_b(a)| = 2^{\frac{n+1}{2}}\}$$
$$C := \{(a, b) \in \mathbb{F}_2^{n+1} \times \mathbb{F}_2^{n+1} \setminus \{0\} \mid |\widehat{F}_b(a)| = 2^{\frac{n+3}{2}}\}.$$

From the previous observations, the number of bent components of F is equal to $2^{n+1} - 2 - k$ and we have $|A| = 4$, $|B| = (2^{n+1} - 2 - k)2^{n+1}$, and $|C| = k2^{n-1}$. The cardinalities of the sets $|B|$ and $|C|$ stated as above follow from Parseval's relation for the Walsh transform, i.e., for all $b \neq 0$, we have $\sum_{a\in\mathbb{F}_2^{n+1}} \widehat{F}_b^2(a) = 2^{2n+2}$ (see [14, p. 61]). We thus have

$$\sum_{a,b\in\mathbb{F}_2^{n+1}, b\neq 0} \widehat{F}_b^4(a) = |A|2^{4n} + |B|2^{2n+2} + |C|2^{2n+6}$$

$$= k(2^{3n+5} - 2^{3n+3}) + 2^{4n+2} + 2^{4n+4} - 2^{3n+4},$$

which must be equal to $2^{4n+5} - 2^{3n+4}$ according to Lemma 1. It follows that $k = 2^{n-1}$. □

On the ortho-derivative of APN functions with maximum linearity If $T : \mathbb{F}_2^n \times \mathbb{F}_2 \to \mathbb{F}_2^n \times \mathbb{F}_2$ is a quadratic APN function with linearity 2^n, then there exists an $(n-1)$-dimensional linear

space V such that the ortho-derivative π_T of T is constant on $V \setminus \{0\}$. Indeed, for any fixed non-zero $\gamma \in \mathbb{F}_2^n$, the APN function T is EA-equivalent to a function T' of the form as in Theorem 3, so for all $(x, y) \in \mathbb{F}_2^n \times \mathbb{F}_2$, we have that $\pi_{T'}(\alpha, \beta) \neq 0$ is orthogonal to

$$
\begin{pmatrix} G(x) + G(x + \alpha) + G(\alpha) + G(0) \\ 0 \end{pmatrix} + \beta \begin{pmatrix} x \\ \langle \gamma, x \rangle \end{pmatrix} + y \begin{pmatrix} \alpha \\ \langle \gamma, \alpha \rangle \end{pmatrix}
$$

as long as $(\alpha, \beta) \in (\mathbb{F}_2^n \times \mathbb{F}_2) \setminus \{0\}$. Setting $V':=\{(\alpha, \beta) \in \mathbb{F}_2^n \times \mathbb{F}_2 \mid \beta = 0 \text{ and } \langle \gamma, \alpha \rangle = 0\}$, we can observe that $\pi_{T'}(\alpha, \beta) = ((0, 0, \ldots, 0), 1)$ for all $(\alpha, \beta) \in V' \setminus \{0\}$. We recall that the ortho-derivatives of EA-equivalent functions are linear-equivalent [12, Prop. 39].

5.3 The case of Gold functions

It is worth highlighting that an EA-equivalent representation of the 6-bit quadratic APN function with linearity 2^5, i.e., Function no. 2.6 in [17, Table 5], can be given as

$$
T_6 \colon \mathbb{F}_{2^5} \times \mathbb{F}_2 \to \mathbb{F}_{2^5} \times \mathbb{F}_2
$$

$$
\begin{pmatrix} x \\ y \end{pmatrix} \mapsto \begin{pmatrix} x^3 \\ 0 \end{pmatrix} + \begin{pmatrix} x^{16} + x \\ \mathrm{Tr}\,(x) \end{pmatrix} \cdot y \,,
$$

i.e., it can be obtained as a 0-extension of the cube function over $\mathbb{F}_{2^5}$. Note that it was already observed in [20, Sec. 3] that both of the two quadratic EA-equivalence classes of 5-bit APN functions yield the EA-equivalence class of the 6-bit quadratic APN function with maximum linearity as a 0-extension. The following proposition gives us a necessary and sufficient condition on when a Gold APN function in odd dimension can be extended to a quadratic APN function with maximum linearity.

Proposition 7 *Let $n \in \mathbb{N}$ be an odd integer and let $i \in \mathbb{N}$ be an integer with $\gcd(i, n) = 1$. The APN function $G \colon \mathbb{F}_{2^n} \to \mathbb{F}_{2^n}, x \mapsto x^{2^i+1}$ is 0-extendable if and only if there exists a linear function (bijection) $L \colon \mathbb{F}_{2^n} \to \mathbb{F}_{2^n}$ such that, for all $x \in \mathbb{F}_{2^n} \setminus \{0\}$ with $\mathrm{Tr}\,(x) = 0$, we have $\mathrm{Tr}\left(x^{-(2^i+1)}L(x)\right) = 1$.*

Proof In the finite field $\mathbb{F}_{2^n}$, we use $\langle \alpha, x \rangle_{\mathbb{F}_{2^n}} = \mathrm{Tr}\,(\alpha x)$. Then, for the ortho-derivative of G, we have

$$
\pi_G \colon \mathbb{F}_{2^n} \to \mathbb{F}_{2^n}, x \mapsto \begin{cases} x^{-(2^i+1)} & \text{if } x \neq 0 \\ 0 & \text{if } x = 0 \end{cases} .
$$

Indeed, for all $\alpha, x \in \mathbb{F}_{2^n}$, we have $B_\alpha(x):=G(x)+G(x+\alpha)+G(\alpha)+G(0) = \alpha x^{2^i} + \alpha^{2^i} x$ and thus, $\mathrm{Tr}\left(x^{-(2^i+1)}B_\alpha(x)\right) = \mathrm{Tr}\left(\alpha x^{-1}\right) + \mathrm{Tr}\left(\alpha^{2^i} x^{-2^i}\right) = 0$.

Therefore, G is 0-extendable if and only if there exists a linear function $L' \colon \mathbb{F}_{2^n} \to \mathbb{F}_{2^n}$ and a non-zero $\beta \in \mathbb{F}_{2^n}$ such that, for all $x \in \mathbb{F}_{2^n} \setminus \{0\}$ with $\mathrm{Tr}\,(\beta x) = 0$, we have $\mathrm{Tr}\left(x^{-(2^i+1)}L'(x)\right) = 1$. If we substitute x by $\beta^{-1}x$, we obtain that, for all $x \in \mathbb{F}_{2^n} \setminus \{0\}$ with $\mathrm{Tr}\,(x) = 0$, we have $\mathrm{Tr}\left(x^{-(2^i+1)}\beta^{2^i+1}L'(\beta^{-1}x)\right) = 1$. The result follows by defining $L \colon \mathbb{F}_{2^n} \to \mathbb{F}_{2^n}, x \mapsto \beta^{2^i+1}L'(\beta^{-1}x)$.

Without loss of generality, we can assume L being a bijection because of Proposition 6. $\square$

We did not find any example of a 0-extendable Gold function in odd dimension n with $7 \leq n \leq 15$.

6 Open problems

Our work leaves several open problems, which we list in the following. We expect that a solution to any of those problems will provide further interesting insights within the theory of APN functions.

Open Problem 1 Study how restrictions of a function $F : \mathbb{F}_2^n \to \mathbb{F}_2^n$ are related to restrictions of a function F' CCZ-equivalent to F. Moreover, if we have two quadratic APN functions F and G such that $G \prec F$, determine whether it is possible to construct an APN function G' which is not CCZ-equivalent to a quadratic function such that $G' \prec F'$, where F' is CCZ-equivalent to F.

Open Problem 2 Find a recursive APN function in every dimension $n \geq 2$ (i.e., prove Conjecture 1).

Open Problem 3 Find an algorithmic way for finding valid pairs (L, ℓ) when building r-extendable APN functions that is more efficient than the method described in Sect. 4.

Open Problem 4 Construct an infinite family of quadratic APN functions with maximum linearity (or equivalently an infinite family of 0-extendable APN functions) or prove that such a family cannot exist.

Open Problem 5 Determine whether there exists a 0-extendable APN function in odd dimension $n > 5$ that comes from one of the known infinite families of APN functions.

Declarations

Conflict of interest All Authors declare that they have no competing interest.

Appendix A: An example of a recursive APN function in dimension eight

Below, we provide the look-up table of a quadratic recursive APN function $R : \mathbb{F}_2^8 \to \mathbb{F}_2^8$. The entries of the look-up table are denoted as hexadecimal values, omitting the `0x` prefix for presentation purposes.

$$R = [00, 79, b2, e1, 39, c7, 70, a4, 36, c0, 22, fe, 5e, 2f, b1, ea,$$
$$b9, f8, 1d, 76, 28, ee, 77, 9b, 0a, c4, 08, ec, ca, 83, 33, 50,$$
$$1e, 1d, 70, 59, b5, 31, 20, 8e, 58, d4, 90, 36, a2, a9, 91, b0,$$

```
8d, b6, f5, e4, 8e, 32, 0d, 9b, 4e, fa, 90, 0e, 1c, 2f, 39, 20,
8e, 26, 1f, 9d, ba, 95, d0, d5, a6, 81, 91, 9c, c3, 63, 0f, 85,
fc, 6c, 7b, c1, 60, 77, 1c, 21, 51, 4e, 70, 45, 9c, 04, 46, f4,
2f, fd, 62, 9a, 89, dc, 3f, 40, 77, 2a, 9c, eb, 80, 5a, 90, 60,
77, 9d, 2c, ec, 79, 14, d9, 9e, aa, cf, 57, 18, f5, 17, f3, 3b,
46, bf, d8, 0b, 0b, 75, 6e, 3a, 9c, ea, a4, f8, 80, 71, 43, 98,
eb, 2a, 63, 88, 0e, 48, 7d, 11, b4, fa, 9a, fe, 00, c9, d5, 36,
ef, 6c, ad, 04, 30, 34, 89, a7, 45, 49, a1, 87, cb, 40, d4, 75,
68, d3, 3c, ad, 1f, 23, b0, a6, 47, 73, b5, ab, 61, d2, 68, f1,
d1, f9, 6c, 6e, 91, 3e, d7, 52, 15, b2, 0e, 83, 04, 24, e4, ee,
b7, a7, 1c, 26, 5f, c8, 0f, b2, f6, 69, fb, 4e, 4f, 57, b9, 8b,
c7, 95, a6, de, 15, c0, 8f, 70, 73, ae, b4, 43, f0, aa, cc, bc,
8b, e1, fc, bc, f1, 1c, 7d, ba, ba, 5f, 6b, a4, 91, f3, bb, f3]
```

Let $g \in \mathbb{F}_{2^8}$ be an element with minimal polynomial $X^8 + X^4 + X^3 + X^2 + 1$. Then, R can also be given as a function over $\mathbb{F}_{2^8}$ by the univariate representation

$$
\begin{aligned}
R(x) = {} & g^{157}x + g^{237}x^2 + g^{169}x^3 + g^{56}x^4 + g^{43}x^5 + g^{11}x^6 + g^{154}x^8 + g^{89}x^9 \\
& + g^{155}x^{10} + g^{221}x^{12} + g^{157}x^{16} + g^5 x^{17} + g^{245}x^{18} + g^{32}x^{20} + g^{127}x^{24} \\
& + g^{49}x^{32} + g^{81}x^{33} + g^4 x^{34} + g^{146}x^{36} + g^{223}x^{40} + g^{44}x^{48} + g^{70}x^{64} \\
& + g^{127}x^{65} + g^{113}x^{66} + g^{52}x^{68} + g^{253}x^{72} + g^{209}x^{80} + g^{239}x^{96} + g^{43}x^{128} \\
& + g^4 x^{129} + g^{99}x^{130} + g^{89}x^{132} + g^{26}x^{136} + g^{47}x^{144} + g^{220}x^{160} + g^{253}x^{192}.
\end{aligned}
$$

The following sage code returns R and APN restrictions contained in R for $n = 7, \ldots, 2$.

```
n = 8 while (n>=2):
    mask = sum(int(1 << i) for i in xrange(0,n))
    R = [R[x] & mask for x in xrange(0, 2**n)]
    print(R)
    n = n−1
```

Appendix B: Sage implementation of Algorithm 1

```
from sboxU import *
load("sboxU/known_functions/sevenBitAPN.py")
n = 7

AllQuadG = all_quadratics()

def bit(a,i):
    return ((a>>i)

def inner_product(l,x):
    return Integer(l&x).bits().count(1)

# converts the matrix A to a look−up table
def matrix_to_sbox(A):
```

```
    T = []
    V = VectorSpace(GF(2),A.nrows())
    for v in V:
        T.append(ZZ(list(A*v),base=2))
    return T

def gen_system(G,ortho,l):
    M = []
    for a in range(2**n)[1::]:
        if (inner_product(l,a)==0):
            row = []
            for bit_pi in range(n):
                for bit_a in range(n):
                    row.append(bit(a,bit_a)*bit(ortho[a],bit_pi))
            M.append(row)
    return (matrix(GF(2),M))

def is_extendable(G,ortho,l):
    M = gen_system(G,ortho,l)
    v = vector(GF(2),[1]*(M.nrows()))
    try:
        mat = M.solve_right(v)
    except (ValueError):
        return []
    if (M.right_kernel().dimension()>(2*n)):
        print("There might be more solutions!\n")
    #otherwise there is only on L up to Gamma-equivalence
    L = matrix_to_sbox(matrix(GF(2),n,n,list(mat)))
    S = []
    for i in range(2**n):
        S.append(int(G[i]<<1))
    for i in range(2**n):
        S.append(int(((G[i]^^L[i])<<1)^^inner_product(l,i)))
    return S

# returns a list of APN extensions of G
def extensions(G):
    sol = []
    pi = ortho_derivative(G)
    for l in range(2**n):
        t = is_extendable(G,pi,l)
        if (not(t==[])):
            sol.append(t)
    return sol

sol = []
for i in range(len(AllQuadG)):
    print(i)
    t = extensions(AllQuadG[i])
    if (not(t==[])):
        sol.append(t)

print(sol)
```

References

1. Beierle C., Brinkmann M., Leander G.: Linearly self-equivalent APN permutations in small dimension. IEEE Trans. Inf. Theory **67**(7), 4863–4875 (2021).

2. Beierle C., Leander G.: New instances of quadratic APN functions. IEEE Trans. Inf. Theory **68**(1), 670–678 (2022).
3. Beierle C., Leander G., Perrin L.: Quadratic APN Extensions. https://doi.org/10.5281/zenodo.5821018. Dataset (Version 2.0)
4. Beierle C., Leander G., Perrin L.: Supplementary Code to Trims and Extensions of Quadratic APN Functions. https://doi.org/10.5281/zenodo.5871840. Software (Version v1)
5. Boolean Function Wiki: CCZ-inequivalent representatives from the known APN families for dimensions up to 11 (2021). https://boolean.h.uib.no/mediawiki/index.php/CCZ-inequivalent_representatives_from_the_known_APN_families_for_dimensions_up_to_11. Accessed 30 Aug 2021.
6. Brinkmann M., Leander G.: On the classification of APN functions up to dimension five. Des. Codes Cryptogr. **49**(1–3), 273–288 (2008).
7. Budaghyan L., Calderini M., Carlet C., Coulter R.S., Villa I.: Constructing APN functions through isotopic shifts. IEEE Trans. Inf. Theory **66**(8), 5299–5309 (2020).
8. Budaghyan L., Calderini M., Carlet C., Coulter R.S., Villa I.: Generalized isotopic shift construction for APN functions. Des. Codes Cryptogr. **89**(1), 19–32 (2021).
9. Budaghyan L., Carlet C., Leander G.: On a construction of quadratic APN functions. In: 2009 IEEE Information Theory Workshop, pp. 374–378 (2009). IEEE.
10. Budaghyan L., Carlet C., Leander G.: Constructing new APN functions from known ones. Finite Fields Their Appl. **15**(2), 150–159 (2009).
11. Calderini M.: On the EA-classes of known APN functions in small dimensions. Cryptogr. Commun. **12**(5), 821–840 (2020).
12. Canteaut A., Couvreur A., Perrin L.: Recovering or testing extended-affine equivalence (2021). arXiv:2103.00078.
13. Carlet C.: Characterizations of the differential uniformity of vectorial functions by the Walsh transform. IEEE Trans. Inf. Theory **64**(9), 6443–6453 (2018).
14. Carlet C.: Boolean Functions for Cryptography and Coding Theory. Cambridge University Press, Cambridge (2021).
15. Carlet C., Charpin P., Zinoviev V.A.: Codes, bent functions and permutations suitable for DES-like cryptosystems. Des. Codes Cryptogr. **15**(2), 125–156 (1998).
16. Chabaud F., Vaudenay S.: Links between differential and linear cryptanalysis. In: Santis A.D. (ed.) Advances in Cryptology—EUROCRYPT '94, Proceedings, vol. 950, pp. 356–365. LNCS. Springer, Berlin (1994).
17. Edel Y., Pott A.: A new almost perfect nonlinear function which is not quadratic. Adv. Math. Commun. **3**(1), 59–81 (2009).
18. Gorodilova A.A.: Characterization of almost perfect nonlinear functions in terms of subfunctions. Discret. Math. Appl. **26**(4), 193–202 (2016).
19. Idrisova V.: On an algorithm generating 2-to-1 APN functions and its applications to "the big APN problem". Cryptogr. Commun. **11**(1), 21–39 (2019).
20. Kalgin K., Idrisova V.: The classification of quadratic APN functions in 7 variables. IACR Cryptol. ePrint Arch. **2020**, 1515 (2020).
21. Langevin P.: Classification of APN cubics in dimension 6 over GF(2) (2012). http://langevin.univ-tln.fr/project/apn-6/apn-6.html. Accessed 30 Aug 2021.
22. Nyberg K.: Differentially uniform mappings for cryptography. In: Helleseth T. (ed.) Advances in Cryptology—EUROCRYPT '93, Proceedings, vol. 765, pp. 55–64. LNCS. Springer, Heidelberg (1993).
23. Nyberg K.: S-boxes and round functions with controllable linearity and differential uniformity. In: Preneel B. (ed.) Fast Software Encryption: Second International Workshop, Proceedings, vol. 1008, pp. 111–130. LNCS. Springer, Berlin (1994).
24. Nyberg K., Knudsen L.R.: Provable security against differential cryptanalysis. In: Brickell E.F. (ed.) Advances in Cryptology—CRYPTO '92, Proceedings, vol. 740, pp. 566–574. LNCS. Springer, Berlin (1992).
25. Perrin L.: sboxU. GitHub repository (2017). https://github.com/lpp-crypto/sboxU
26. Sage Developers: SageMath, the Sage Mathematics Software System (Version 9.3) (2021). https://www.sagemath.org
27. Taniguchi H.: On some quadratic APN functions. Des. Codes Cryptogr. **87**(9), 1973–1983 (2019).
28. Weng G., Tan Y., Gong G.: On quadratic almost perfect nonlinear functions and their related algebraic object. In: Workshop on Coding and Cryptography (WCC) (2013).
29. Yu Y., Kaleyski N., Budaghyan L., Li Y.: Classification of quadratic APN functions with coefficients in F2 for dimensions up to 9. Finite Fields and Their Applications **68**, 101733 (2020).
30. Yu Y., Perrin L.: Constructing more quadratic APN functions with the QAM method. IACR Cryptol. ePrint Arch. **2021**, 574 (2021).

31. Yu Y., Wang M., Li Y.: A matrix approach for constructing quadratic APN functions. IACR Cryptol. ePrint Arch. **2013**, 7 (2013).
32. Yu Y., Wang M., Li Y.: A matrix approach for constructing quadratic APN functions. Des. Codes Cryptogr. **73**(2), 587–600 (2014).