Changing almost perfect nonlinear functions on affine subspaces of small codimensions

Hiroaki Taniguchi[a]

Alexandr Polujan[b]

Alexander Pott[b]

Razi Arshad[c]

Abstract

A function $F\colon \mathbb{F}_2^n \to \mathbb{F}_2^m$ with $m \geqslant n$ is called almost perfect nonlinear (APN) if, for every nonzero $a \in \mathbb{F}_2^n$ and every $b \in \mathbb{F}_2^m$, the equation $F(x+a) + F(x) = b$ has at most two solutions $x \in \mathbb{F}_2^n$. One of the central problems in the research on APN functions lies in discovering new constructions of these mappings. In this paper, we introduce secondary construction methods for APN functions by modifying given ones on affine subspaces of small codimensions. We provide explicit criteria for determining when such modifications preserve the APN property and show that some of the newly constructed functions are inequivalent to the original ones.

Mathematics Subject Classifications: 06E30, 11T06, 94A60

1 Introduction

Let $\mathbb{F}_2^n$ be the n-dimensional vector space over the finite field with two elements $\mathbb{F}_2$. A mapping $F\colon \mathbb{F}_2^n \to \mathbb{F}_2^m$ is called an (n, m)-function. Almost perfect nonlinear (APN) functions are (n, m)-functions F with optimal differential properties. Formally, it means that the cardinality of the set $\{x \in \mathbb{F}_2^n\colon F(x+a) + F(x) = b\}$, which is always even due to the parity of solutions x and $x+a$, is less than or equal to 2, for any nonzero $a \in \mathbb{F}_2^n$ and for any $b \in \mathbb{F}_2^m$. Originally introduced in the (n, n)-case, APN functions are valuable primitives in cryptographic applications, especially in the design of S-Boxes [11]. Due to their correspondence to certain optimal codes with minimum distance five [10] and the possibility of constructing from them difference sets [14, 15] and large Sidon sets [13], they play a significant role in coding theory and, in general, discrete mathematics and

[a]Yamato University, Department of Education, Suita, Japan (`taniguchi.hiroaki.math@gmail.com`).

[b]Otto von Guericke University Magdeburg, 39106 Magdeburg, Germany
(`alexandr.polujan@gmail.com`, `alexander.pott@ovgu.de`).

[c]Kingston University, School of Computer Science and Mathematics, London, UK
(`r.arshad@kingston.ac.uk`).

combinatorics [17]. Recently, there has been an increasing interest in studying (n, m)-APN functions for the case $m > n$; for the recent works on the topic, we refer to [1, 22].

A central challenge in APN function research is discovering new construction methods of such functions, which can be classified into primary and secondary. Primary constructions aim to provide new infinite families of APN functions "from scratch" (for the summary of the known infinite families, we refer to the recent article [19]), while secondary constructions aim to construct new functions from the known ones. Some of the well-known secondary construction methods of APN functions (we briefly explain them further) include the switching construction (and its various generalizations), modifications by applying functions of a special shape, and isotopic shift construction, to name a few.

For a given (n, n)-APN function F, represented as a vector of coordinate single-output functions $F(x) = (f_1(x), f_2(x), \ldots, f_n(x))$, the switching construction aims at constructing a new APN function of the form $F'(x) = (f_1(x), f_2(x), \ldots, f_n'(x))$, i.e., by modifying a single coordinate function of a given APN function (w.l.o.g, the last one). An advantage of this approach is that it preserves much of the information from the original function F, allowing room to demonstrate the APN property of a new function F'; see, e.g., [8, 16]. Note that switching [16] and several related methods [26, 18], which can be viewed as its generalizations, can be used both for generating numerous new examples through computer searches in fixed dimensions and constructing new infinite families of APN functions [8]. In the latter case, one obtains APN functions of the form $G(x) = F(x) + Tr(H(x))$ defined on the finite field $\mathbb{F}_{2^n}$, which gives the motivation to study further generalization in polynomial form. For example, in [9, 24], the authors studied the APN-ness of mappings $\mathbb{F}_{2^n} \ni x \mapsto L_1(x^3) + L_2(x^9)$ where L_1 and L_2 are linear. In [12], the authors investigated APN-ness of mappings of the form $G(x) = F(x) + \mathrm{Tr}(x)L(x)$, which corresponds to modifications by linear functions on hyperplanes. The studies [7, 6] provide an analysis of the APN property of mappings defined as $G(x) = xL_1^{2^i}(x) + x^{2^i}L_2(x)$ on $\mathbb{F}_{2^n}$. This approach to constructing APN functions is called the (generalized) isotopic shift method.

While the previously discussed constructions focus on modifying a single APN function, another possible approach is to combine several given APN functions to build a new one. For example, the idea of constructing an APN function in $n + 1$ variables from two APN functions in n variables has been studied in [18] and later extended in [3, 4]. These results, in turn, stimulate further investigations of various algebraic decompositions of APN functions. For example, the connection between different APN functions was shown useful, when certain decompositions of (n, n)-APN functions helped to characterize the structure of quadratic APN functions with the maximum linearity [4].

These findings motivate our further investigation of variations of the known secondary constructions of APN functions, their algebraic decompositions, and, in particular, modifications of APN functions on affine subspaces with small codimensions. This approach preserves much of the structure of the original APN function enabling the verification of the APN property for a modified function and, in many cases, allowing for an explicit characterization of this property.

Our contribution and the structure of the paper The paper is organized as follows. In Subsection 1.1 we give a necessary background on APN functions. In Section 2, we consider construction methods of (n, m)-APN functions. In Subsection 2.1, we consider the switching construction for (n, m)-APN functions, and in Section 2.2, we investigate the question of constructing an (n, m)-APN function F from two $(n-1, m)$-APN functions f and g defined on complementary hyperplanes of $\mathbb{F}_2^n$. Notably, we uncover structural connections between such mappings and present a necessary and sufficient condition on the functions f and g to ensure that F is APN (Theorem 2.10), along with a simplified condition for the case when both f and g are quadratic (Proposition 2.11). In the remaining sections, we concentrate solely on the construction methods of (n, n)-APN functions. In Section 3, we investigate how to construct a new quadratic APN function G from a given quadratic APN function F on $\mathbb{F}_2^n$ by adding to it a linear function defined on a hyperplane. Identifying $\mathbb{F}_2^n$ with the finite field $\mathbb{F}_{2^n}$, this question can be interpreted as finding APN functions on $\mathbb{F}_{2^n}$ of the form $G(x) = F(x) + \text{Tr}(x)L(x)$, where F is a quadratic APN function and L is a linear mapping on $\mathbb{F}_{2^n}$. In Subsection 3.1, we provide a complete characterization of the APN property of such modifications (Theorem 3.2) and call such APN functions G and F "hyperplane-equivalent" or H-equivalent, for short (Definition 3.4). Remarkably, we indicate that all extended-affine equivalence classes of quadratic APN functions on $\mathbb{F}_{2^6}$ have a representative of the form $G(x) = x^3 + \text{Tr}(x)L(x)$, which is H-equivalent to $F(x) = x^3$ (Theorem 3.5). Thus, we provide a new unifying approach to describe quadratic APN functions on $\mathbb{F}_{2^6}$. Motivated by these observations, in Subsection 3.2, we further investigate the APN property for quadratic APN functions that are H-equivalent to x^3. Particularly, we provide a necessary and sufficient condition for the APN-ness of mappings $\mathbb{F}_{2^n} \ni x \mapsto x^3 + \text{Tr}(x)L(x)$ using certain exponential sums (Theorem 3.7). Finally, in Section 4, we present a necessary and sufficient condition (Theorem 4.1) for constructing new APN functions from a given one by adding constant functions defined on complementary affine subspaces of codimension two. We indicate in Example 4.2 that the proposed construction method yields extended-affine inequivalent functions. The paper is concluded in Section 5.

1.1 Preliminaries

Let $\mathbb{F}_{2^n}$ be the finite field of 2^n elements. We sometimes identify $\mathbb{F}_{2^n}$ with $\mathbb{F}_2^n$ as an $\mathbb{F}_2$-vector space. We denote the sets $\mathbb{F}_{2^n} \backslash \{0\}$ by $\mathbb{F}_{2^n}^\times$ and $\mathbb{F}_2^n \backslash \{0\}$ by $(\mathbb{F}_2^n)^\times$. For the finite fields $K \supset F$ of characteristic 2, we denote the *trace function* from K to F by Tr_F^K. We denote $\text{Tr}_{\mathbb{F}_2}^K$ by Tr and call it the *absolute trace* of K. The mappings $\mathbb{F}_{2^n} \ni x \mapsto \sum_{i=0}^{n-1} a_i x^{2^i}$, where all $a_i \in \mathbb{F}_{2^n}$, are called *linearized polynomials*; these are linear mappings defined on the finite field $\mathbb{F}_{2^n}$.

A function $F \colon \mathbb{F}_2^n \to \mathbb{F}_2^m$ is called an *almost perfect nonlinear (APN)* (n, m)-function if the cardinality of the set $\{x \in \mathbb{F}_2^n \colon F(x+a) + F(x) = b\}$ is less than or equal to 2 for any nonzero $a \in \mathbb{F}_2^n$ and for any $b \in \mathbb{F}_2^m$. Sometimes we omit the specification of n and m, when they are clear from the context. A function $F \colon \mathbb{F}_2^n \to \mathbb{F}_2^m$ is called *quadratic* if the mapping $\mathbb{F}_2^m \times \mathbb{F}_2^m \ni (x, y) \mapsto F(x+y) + F(x) + F(y) + F(0)$ is $\mathbb{F}_2$-bilinear.

On the set of all (n, m)-functions we introduce the following equivalence relations that preserve the APN property. The functions F_1 and F_2 from $\mathbb{F}_2^n$ to $\mathbb{F}_2^m$ are called *Carlet-Charpin-Zinoviev equivalent* (*CCZ-equivalent*, for short) if the graphs $G_{F_1} := \{(x, F_1(x)) \colon x \in \mathbb{F}_2^n\}$ and $G_{F_2} := \{(x, F_2(x)) \colon x \in \mathbb{F}_2^n\}$ in $\mathbb{F}_2^n \oplus \mathbb{F}_2^m$ are affine equivalent [10], that is, if there exists an $\mathbb{F}_2$-linear isomorphism $l \in GL_2(\mathbb{F}_2^n \oplus \mathbb{F}_2^m)$ and an element $v \in \mathbb{F}_2^n \oplus \mathbb{F}_2^m$ such that $l(G_{F_1}) + v = G_{F_2}$. We say that (n, m)-functions F and F' are *extended-affine equivalent (EA-equivalent)*, if there exist two affine permutations $A_1 \colon \mathbb{F}_2^m \to \mathbb{F}_2^m, A_2 \colon \mathbb{F}_2^n \to \mathbb{F}_2^n$ and an affine function $A_3 \colon \mathbb{F}_2^n \to \mathbb{F}_2^m$ such that $A_1 \circ F \circ A_2 + A_3 = F'$. We note that in general, CCZ-equivalence is coarser than EA-equivalence, and that EA-equivalent functions are also CCZ-equivalent. However, in the case of quadratic APN functions, they coincide, as shown in [25].

Finally, we define the following invariant that will be used later to distinguish inequivalent functions. The Γ-*rank* of a function $F \colon \mathbb{F}_2^n \to \mathbb{F}_2^m$ is the rank of the incidence matrix over $\mathbb{F}_2$ of the incidence structure $\{\mathcal{P}, \mathcal{B}, I\}$, where $\mathcal{P} = \mathbb{F}_2^n \oplus \mathbb{F}_2^m$, $\mathcal{B} = \mathbb{F}_2^n \oplus \mathbb{F}_2^m$ and $(a, b)I(u, v)$ for $(a, b) \in \mathcal{P}$ and $(u, v) \in \mathcal{B}$ if and only if $F(a + u) = b + v$. It is well-known that if two functions F_1 and F_2 from $\mathbb{F}_2^n$ to $\mathbb{F}_2^m$ are CCZ-equivalent, then they have the same Γ-rank, see [16].

2 Constructing (n, m)-APN functions

In this section, we study construction methods of (n, m)-APN functions using two different approaches. The first one is based on the well-known switching construction introduced for the case of (n, n)-APN functions, and the second one is based on the concatenation of two $(n - 1, m)$-APN functions defined on complementary hyperplanes in $\mathbb{F}_2^n$.

2.1 Revisiting the switching construction for (n, m)-APN functions

For a function $f \colon \mathbb{F}_2^n \to \mathbb{F}_2^m$, we define the mapping $B_f(x, t) := f(x + t) + f(x) + f(t) + f(0)$, for $x, t \in \mathbb{F}_2^n$. Recall the following definition and lemmas in [22].

Definition 2.1 (Definition 1 of [22])**.** For a function $f \colon \mathbb{F}_2^n \to \mathbb{F}_2^m$, let us define the subsets $D_f(\mathbb{F}_2^n)$ and $D_f^*(\mathbb{F}_2^n)$ of $\mathbb{F}_2^m$ as

$$D_f(\mathbb{F}_2^n) := \{B_f(x, t) + B_f(y, t) \mid x, y, t \in \mathbb{F}_2^n\} \text{ and,}$$
$$D_f^*(\mathbb{F}_2^n) := \{B_f(x, t) + B_f(y, t) \mid x, y, t \in \mathbb{F}_2^n \text{ with } x \neq y, t \neq 0 \text{ and } x \neq y + t\}$$

We denote by $\pi \circ f$ the composition mapping defined by $(\pi \circ f)(x) := \pi(f(x))$.

Lemma 2.2 (Lemma 2 of [22])**.** *Let $f \colon \mathbb{F}_2^n \to \mathbb{F}_2^m$ be an APN function. Let $l < m$ be a positive integer and let $\pi \colon \mathbb{F}_2^m \to \mathbb{F}_2^l$ be an $\mathbb{F}_2$-linear surjection. Then, $\pi \circ f$ is an APN function if and only if $D_f^*(\mathbb{F}_2^n) \cap \ker(\pi) = \emptyset$.*

Recall that a function $f \colon \mathbb{F}_2^n \to \mathbb{F}_2^m$ is called a *differentially 4-uniform* function if $|\{x \in \mathbb{F}_2^n \colon f(x + a) + f(x) = b\}| \leqslant 4$ for any nonzero $a \in \mathbb{F}_2^n$ and for any $b \in \mathbb{F}_2^m$.

Lemma 2.3 (Lemma 3 of [22]). *Let $f \colon \mathbb{F}_2^n \to \mathbb{F}_2^m$ be an APN function. Let $\pi \colon \mathbb{F}_2^m \to \mathbb{F}_2^{m-1}$ be an $\mathbb{F}_2$-linear surjection such that $D_f^*(\mathbb{F}_2^n) \cap \ker(\pi) \neq \emptyset$. Then, $\pi \circ f \colon \mathbb{F}_2^n \to \mathbb{F}_2^{m-1}$ is a differentially 4-uniform function.*

The following proposition is a slight generalization of the switching construction (Theorem 3 of [16]).

Proposition 2.4. *Let $f \colon \mathbb{F}_2^n \to \mathbb{F}_2^m$ be a function and $g \colon \mathbb{F}_2^n \to \mathbb{F}_2$ a Boolean function such that $F \colon \mathbb{F}_2^n \ni x \mapsto (f(x), g(x)) \in \mathbb{F}_2^m \oplus \mathbb{F}_2$ is an APN $(n, m+1)$-function. Let u be a nonzero element of $\mathbb{F}_2^m$. Then, $f(x) + ug(x)$ is an APN (n, m)-function if and only if $f(x+t) + f(x) + f(y+t) + f(y) = u$ implies $g(x+t) + g(x) + g(y+t) + g(y) = 0$.*

Proof. Let $\pi \colon \mathbb{F}_2^m \oplus \mathbb{F}_2 \ni (x, y) \mapsto x + uy \in \mathbb{F}_2^m$ be an $\mathbb{F}_2$-linear surjection with $\ker(\pi) = \langle (u, 1) \rangle$. Then, $(\pi \circ F)(x) = f(x) + ug(x)$. By Lemma 2.2, $\pi \circ F$ is an APN function if and only if $(u, 1) \notin D_F^*(\mathbb{F}_2^n)$, which is equivalent to the condition "$B_f(x, t) + B_f(y, t) = f(x+t) + f(x) + f(y+t) + f(y) = u$ implies $B_g(x, t) + B_g(y, t) = g(x+t) + g(x) + g(y+t) + g(y) = 0$", because $B_F(x, t) + B_F(y, t) = (B_f(x, t) + B_f(y, t), B_g(x, t) + B_g(y, t))$. $\square$

Remark 2.5. If f in Proposition 2.4 is not an APN function, then f is a differentially 4-uniform function by Lemma 2.3. Let f be a differentially 4-uniform function. Thus, $F \colon \mathbb{F}_2^n \ni x \mapsto (f(x), g(x)) \in \mathbb{F}_2^m \oplus \mathbb{F}_2$ is an APN $(n, m+1)$-function if and only if the following conditions are satisfied: for $x \neq y, x \neq y + t$ and $t \neq 0$, $f(x+t) + f(x) + f(y+t) + f(y) = 0$ implies $g(x+t) + g(x) + g(y+t) + g(y) = 1$.

Lemma 2.6 (See [20]). *Let $n = 2k$ be an even integer with $k > 1$. Then, for any $a \in \mathbb{F}_{2^n}^\times$ and $b \in \mathbb{F}_{2^n}$, the following statements hold.*

1. *$x^{-1} + (x+a)^{-1} = b$ has no root in $\mathbb{F}_{2^n}$ if and only if $\mathrm{Tr}(\frac{1}{ab}) = 1$.*

2. *$x^{-1} + (x+a)^{-1} = b$ has 2 root in $\mathbb{F}_{2^n}$ if and only if $ab \neq 1$ and $\mathrm{Tr}(\frac{1}{ab}) = 0$.*

3. *$x^{-1} + (x+a)^{-1} = b$ has 4 root in $\mathbb{F}_{2^n}$ if and only if $b = a^{-1}$. Furthermore, when $b = a^{-1}$ the 4 root of the above equation in $\mathbb{F}_{2^n}$ are $\{0, a, \omega a, \omega^2 a\}$, where $\omega \in \mathbb{F}_{2^2} \backslash \mathbb{F}_2$.*

Now, we give an example of a differentially 4-uniform function f on $\mathbb{F}_{2^n}$ and a Boolean function $g \colon \mathbb{F}_{2^n} \to \mathbb{F}_2$ such that $F(x) = (f(x), g(x))$ is an $(n, n+1)$-APN function.

Example 2.7. Let $n = 2k$ be an even integer with $k > 1$. Then, the inverse function $f(x) = x^{2^n - 2}$ is a differentially 4-uniform function on $\mathbb{F}_{2^n}$. By Lemma 2.6, we see that $f(x+a) + f(x) + f(y+a) + f(y) = 0$ with $x \neq y$, $x \neq y + a$ and $a \neq 0$ implies $\{x, x+a, y, y+a\} = \{0, a, \omega a, \omega^2 a\}$. Hence, for a Boolean function $g \colon \mathbb{F}_{2^n} \to \mathbb{F}_2$, we see that $F \colon \mathbb{F}_{2^n} \ni x \to (f(x), g(x)) \in \mathbb{F}_{2^n} \oplus \mathbb{F}_2$ is an $(n, n+1)$-APN function if and only if $g(0) + g(a) + g(\omega a) + g(\omega^2 a) = 1$ for any $a \in \mathbb{F}_{2^n}^\times$.

Let $A := \{x^3 \mid x \in \mathbb{F}_{2^n}^\times\}$. Then, $\mathbb{F}_{2^n}^\times = A \cup \omega A \cup \omega^2 A$, where $\omega A = \{\omega a \mid a \in A\}$ and $\omega^2 A = \{\omega^2 a \mid a \in A\}$. Let us define g by $\{g(a), g(\omega a), g(\omega^2 a)\} = \{0, 0, 1\}$ or $\{1, 1, 1\}$ for $a \in A$, and $g(0) = 0$. Then, we see that $g(0) + g(a) + g(\omega a) + g(\omega^2 a) = 1$ for any $a \in \mathbb{F}_{2^n}^\times$ by definition. Hence, $F \colon \mathbb{F}_{2^n} \ni x \to (f(x), g(x)) \in \mathbb{F}_{2^n} \oplus \mathbb{F}_2$ is an $(n, n+1)$-APN function.

In the following proposition, we show that every APN function on $\mathbb{F}_{2^n}$ can be obtained from a differentially 4-uniform function using the switching construction in Proposition 2.4. While most of the secondary constructions of new APN functions are based on constructing them from the known APN functions, this result provides a strategy for finding new APN functions from suitably chosen differentially 4-uniform functions. The proof of this statement is not difficult to see, nevertheless, we give it for the reader's convenience.

Proposition 2.8. *Let f be an APN function on $\mathbb{F}_{2^n}$. Then, there exist a differentially 4-uniform function f_1 on $\mathbb{F}_{2^n}$, a Boolean function $g\colon \mathbb{F}_{2^n} \to \mathbb{F}_2$ and an element $u \in \mathbb{F}_{2^n}^{\times}$, such that $f(x) = f_1(x) + ug(x)$ holds for all $x \in \mathbb{F}_{2^n}$.*

Proof. Let f be any APN function on $\mathbb{F}_{2^n}$ and $g\colon \mathbb{F}_{2^n} \to \mathbb{F}_2$ be a Boolean function. Then, $F(x) := (f(x), g(x))$ is an APN $(n, n+1)$-function. Moreover, we assume that g satisfies, for some $x, y, t \in \mathbb{F}_{2^n}$, $B_g(x,t) + B_g(y,t) = g(x) + g(x+t) + g(y) + g(y+t) = 1$. (Obviously, we have that $x \neq y, t \neq 0$ and $x \neq y + t$ for this x, y, t.) We note that $D_f^*(\mathbb{F}_2^n) = \mathbb{F}_{2^n}^{\times}$ since f is an (n,n)-APN function. (It is the "Dillon's observation"; see p. 381 of [11]). Since $D_F^*(\mathbb{F}_{2^n}) = \{(B_f(x,t) + B_f(y,t), B_g(x,t) + B_g(y,t)) \mid x, y, t \in \mathbb{F}_2^n$ with $x \neq y, t \neq 0$ and $x \neq y + t\}$, there exists $(u, 1) \in D_F^*(\mathbb{F}_{2^n})$ for some $u \in \mathbb{F}_{2^n}^{\times}$. Let $\pi\colon \mathbb{F}_{2^n} \oplus \mathbb{F}_2 \ni (x, y) \mapsto x + uy \in \mathbb{F}_{2^n}$ be a surjective linear mapping with the kernel $\langle (u, 1) \rangle$. Then, $f_1(x) := \pi(F(x)) = f(x) + ug(x)$ is a differentially 4-uniform function on $\mathbb{F}_{2^n}$ by Lemma 2.3. Thus, the APN function f can be expressed as $f(x) = f_1(x) + ug(x)$ using a differentially 4-uniform function f_1, a Boolean function g and an element $u \in \mathbb{F}_{2^n}^{\times}$. $\qed$

Remark 2.9. The discussion in [11, p. 407] explains that for an APN function f_1, a Boolean function g and an element $u \in \mathbb{F}_{2^n}^{\times}$, the function $f := f_1 + ug$ is differentially 4-uniform in general, and APN in rare cases. Note that this reasoning can also be extended to the case where f_1 is differentially δ-uniform. Proposition 2.8, on the other hand, states that for any APN function f, there exists a differentially 4-uniform function f_1, a Boolean function g and an element $u \in \mathbb{F}_{2^n}^{\times}$, such that f can be expressed as $f := f_1 + ug$. This latter expression, although trivial, expresses our point of view: we want to *firstly* construct a differentially 4 uniform function and then *secondly* modify this to transform it into an APN function.

2.2 Constructing (n, m)-APN functions from $(n-1, m)$-APN functions

Let $n \geqslant 3$ and $m \geqslant n$. Let F be an APN function from $\mathbb{F}_2^n$ to $\mathbb{F}_2^m$. We identify $\mathbb{F}_2^{n-1}$ as an $(n-1)$-dimensional subspace (a hyperplane) of $\mathbb{F}_2^n$. Let $e_0 \in \mathbb{F}_2^n$ with $e_0 \notin \mathbb{F}_2^{n-1}$. Then, the complement of $\mathbb{F}_2^{n-1}$ can be expressed as $\mathbb{F}_2^{n-1} + e_0 := \{x + e_0 \colon x \in \mathbb{F}_2^{n-1}\}$. Moreover, we have $\mathbb{F}_2^n = \mathbb{F}_2^{n-1} \cup (\mathbb{F}_2^{n-1} + e_0)$. Let us define $f(x) := F(x)$ for $x \in \mathbb{F}_2^{n-1}$, and $g(x) := F(x + e_0)$ for $x \in \mathbb{F}_2^{n-1}$. Then, the functions f, g from $\mathbb{F}_2^{n-1}$ to $\mathbb{F}_2^m$ are APN. In this section, we investigate under which conditions one can "concatenate" two APN functions f, g from $\mathbb{F}_2^{n-1}$ to $\mathbb{F}_2^m$ in order to get an APN mapping F from $\mathbb{F}_2^n = \mathbb{F}_2^{n-1} \cup (\mathbb{F}_2^{n-1} + e_0)$ to $\mathbb{F}_2^m$ defined by $F(x) = f(x)$ and $F(x + e_0) = g(x)$, for $x \in \mathbb{F}_2^{n-1}$. In the following theorem,

we provide a necessary and sufficient condition for $F\colon \mathbb{F}_2^n \to \mathbb{F}_2^m$ to be APN under this construction.

Theorem 2.10. *Let f, g be functions from $\mathbb{F}_2^{n-1}$ to $\mathbb{F}_2^m$. Let $e_0 \in \mathbb{F}_2^n \backslash \mathbb{F}_2^{n-1}$. Let us define F from $\mathbb{F}_2^n$ to $\mathbb{F}_2^m$ by $F(x) := f(x)$ and $F(x + e_0) := g(x)$ for $x \in \mathbb{F}_2^n$. Then, F is an APN function if and only if the following conditions hold:*

(1) *f and g are APN functions from $\mathbb{F}_2^{n-1}$ to $\mathbb{F}_2^m$,*

(2) *$f(x + a) + f(x) + g(y + a) + g(y) \neq 0$ holds for any $x, y \in \mathbb{F}_2^{n-1}$ and for any nonzero $a \in \mathbb{F}_2^{n-1}$.*

Proof. Recall that F is an APN function if and only if, for any nonzero $A \in \mathbb{F}_2^n$ and for $X, Y \in \mathbb{F}_2^n$, $F(X + A) + F(X) = F(Y + A) + F(Y)$ implies $X = Y$ or $X = Y + A$. Note that condition (2) means: If $f(x) + f(y) + g(u) + g(v) \neq 0$ if u, v, x, y are four different elements in $\mathbb{F}_2^{n-1}$ with $u + v + x + y = 0$.

Firstly, assume that F is an APN function. We will show that f and g must satisfy the conditions (1) and (2).

Let $A = a \in (\mathbb{F}_2^{n-1})^{\times}$. For any $Y = y \in \mathbb{F}_2^{n-1}$, we must have $X = y \in \mathbb{F}_2^{n-1}$ or $X = y + a \in \mathbb{F}_2^{n-1}$ from $F(X + a) + F(X) = F(y + a) + F(y)$. Since $X \in \mathbb{F}_2^{n-1}$, we have $f(X + a) + f(X) = f(y + a) + f(y)$ from $F(X + a) + F(X) = F(y + a) + F(y)$. Thus, f must be an APN function. Next, for any $Y = y + e_0$ with $y \in \mathbb{F}_2^{n-1}$ we must have $X = y + e_0$ or $X = y + a + e_0$ from $F(X + a) + F(X) = F(y + e_0 + a) + F(y + e_0)$. Since $X = x + e_0$ for some $x \in \mathbb{F}_2^{n-1}$, we have $g(x + a) + g(x) = g(y + a) + g(y)$ from $F(X + a) + F(X) = F(y + e_0 + a) + F(y + e_0)$. Hence, g must be an APN function. Thus, the condition (1) must be satisfied.

Let $A = a \in (\mathbb{F}_2^{n-1})^{\times}$. For any $Y = y \in \mathbb{F}_2^{n-1}$, since $X = y$ or $X = y + a$, $F(X + a) + F(X) = F(y + a) + F(y)$ does not have a solution $X = x + e_0$ for $x \in \mathbb{F}_2^{n-1}$. Thus, $F(x + e_0 + a) + F(x + e_0) \neq F(y + a) + F(y)$ holds for any $x, y \in \mathbb{F}_2^{n-1}$, therefore we must have $g(x + a) + g(x) \neq f(y + a) + f(y)$ for any $x, y \in \mathbb{F}_2^{n-1}$. Thus, the condition (2) must be satisfied.

Conversely, let us assume that the conditions (1) and (2) hold. Assume $F(X + A) + F(X) = F(Y + A) + F(Y)$ with $A \neq 0$. We will prove that $X = Y$ or $X = Y + A$. We divide this into the following four cases:

(i) $A = a \in (\mathbb{F}_2^{n-1})^{\times}$ and $Y = y \in \mathbb{F}_2^{n-1}$,

(ii) $A = a \in (\mathbb{F}_2^{n-1})^{\times}$ and $Y = y + e_0$ with $y \in \mathbb{F}_2^{n-1}$,

(iii) $A = a + e_0$ with $a \in \mathbb{F}_2^{n-1}$ and $Y = y$ with $y \in \mathbb{F}_2^{n-1}$,

(iv) $A = a + e_0$ with $a \in \mathbb{F}_2^{n-1}$ and $Y = y + e_0$ with $y \in \mathbb{F}_2^{n-1}$.

Firstly, let us consider the case (i). If $X = x \in \mathbb{F}_2^{n-1}$, then we have $f(x + a) + f(x) = f(y + a) + f(y)$, hence $x = y$ or $x = y + a$ by (1). Let $X = x + e_0$ with $x \in \mathbb{F}_2^{n-1}$, then we have $g(x + a) + g(x) = f(y + a) + f(y)$ which has no solution by (2). Therefore, $X = Y$ or $X = Y + A$ in case (i).

Next, we consider the case (ii). Assume $X = x \in \mathbb{F}_2^{n-1}$. Then, we have $f(x+a)+f(x) = g(y+a)+g(y)$ which has no solution by (2). If $X = x+e_0$ with $x \in \mathbb{F}_2^{n-1}$, then we have $g(x+a)+g(x) = g(y+a)+g(y)$, hence $x+e_0 = y+e_0$ or $x+e_0 = y+e_0+a$ by (1). Thus, we have $X = Y$ or $X = Y+A$ in case (ii).

Let us consider the case (iii). If $X = x \in \mathbb{F}_2^{n-1}$, then we have $g(x+a)+f(x)+g(y+a)+f(y) = 0$, hence $x = y$. If $X = x+e_0$ with $x \in \mathbb{F}_2^{n-1}$, then we have, again, $f(x+a)+g(x)+g(y+a)+f(y) = 0$. For the same reason as above, we have $x+e_0 = y+(a+e_0)$. Therefore we have $x = y$ or $x+e_0 = y+(a+e_0)$. Thus, we have $X = Y$ or $X = Y+A$ in case (iii).

Lastly, we consider the case (iv). If $X = x \in \mathbb{F}_2^{n-1}$, then we have $g(x+a)+f(x)+f(y+a)+g(y) = 0$, hence $x = (y+e_0)+(a+e_0)$. If $X = x+e_0$ with $x \in \mathbb{F}_2^{n-1}$, then we have $f(x+a)+g(x)+f(y+a)+g(y) = 0$. For the same reason as above, we have $x+e_0 = y+e_0$. Thus, we also have $X = Y$ or $X = Y+A$ in case (iv).

Hence, F must be an APN function under the conditions (1) and (2). $\square$

Now, let F be a *quadratic* APN function from $\mathbb{F}_2^n$ to $\mathbb{F}_2^m$. As before, for an element $e_0 \notin \mathbb{F}_2^{n-1}$, we define $f(x) := F(x)$ for $x \in \mathbb{F}_2^{n-1}$, and $g(x) := F(x+e_0)$ for $x \in \mathbb{F}_2^{n-1}$. In this case, we get two quadratic APN functions f, g from $\mathbb{F}_2^{n-1}$ to $\mathbb{F}_2^m$, where $g(x) = f(x)+L(x)+c$ for an element $c := F(e_0)+F(0)$ and a linear mapping $L(x) := B_F(x, e_0)$ with $B_F(x, e_0) := F(x+e_0)+F(x)+F(e_0)+F(0)$. In the following statement, we provide a necessary and sufficient condition that characterizes the APN-ness of the quadratic function F defined by $F(x) := f(x)$ and $F(x+e_0) := g(x)$, for $x \in \mathbb{F}_2^{n-1}$.

Proposition 2.11. *Let f be a quadratic APN function from $\mathbb{F}_2^{n-1}$ to $\mathbb{F}_2^m$, L be an $\mathbb{F}_2$-linear mapping from $\mathbb{F}_2^{n-1}$ to $\mathbb{F}_2^m$, and $c \in \mathbb{F}_2^m$. Define a function $F\colon \mathbb{F}_2^n \to \mathbb{F}_2^m$ by*

$$F(x) := f(x) \quad and \quad F(x+e_0) := f(x)+L(x)+c,$$

for some fixed $e_0 \in \mathbb{F}_2^n \setminus \mathbb{F}_2^{n-1}$ and all $x \in \mathbb{F}_2^{n-1}$. Then, F is a quadratic APN function if and only if

$$\mathbb{F}_2^{n-1} \ni x \mapsto L(x)+B_f(x, A) \in \mathbb{F}_2^m \tag{2.1}$$

are one-to-one mappings for every $A \in \mathbb{F}_2^{n-1}$.

Proof. Define $g := f+L+c$. We verify the conditions (1) and (2) in Theorem 2.10.

Since f and g are APN functions, condition (1) is satisfied.

Condition (2) is equivalent to $f(x+a)+f(x) \neq g(y+a)+g(y) = f(y+a)+f(y)+L(a)$ for any $x, y \in \mathbb{F}_2^{n-1}$ if $a \neq 0$, that is, $L(a)+(f(x+a)+f(x))+(f(y+a)+f(y)) \neq 0$ for any $x, y \in \mathbb{F}_2^{n-1}$ if $a \neq 0$, which means $L(a)+B_f(a, x+y) \neq 0$ if $a \neq 0$, $a \in \mathbb{F}_2^{n-1}$. Note that $f(x+a)+f(x)+f(y+a)+f(y) = B_f(a, x)+B_f(a, y) = B_f(a, x+y)$, where the second equality holds since f is quadratic. We put $A := x+y$ and think of a as the variable x in the linear equation defined by Eq. (2.1). Using the fact that Eq. (2.1) describes a linear function, we see that $L(a)+B_f(a, x+y) \neq 0$ if $a \neq 0$ is exactly the condition in Eq. (2.1). $\square$

3 Modifying quadratic APN functions on hyperplanes

In the previous section, we considered a method for constructing APN functions by concatenating *two* APN functions defined on complementary hyperplanes. An alternative approach to constructing new APN functions involves modifying a *single* given APN function on a hyperplane. In this case, the APN property is characterized as follows:

Corollary 3.1. *[12, Corollary 1] Let $T_0 = \{x\colon \mathrm{Tr}(x) = 0\}$ and $G\colon \mathbb{F}_{2^n} \to \mathbb{F}_{2^n}$ be defined by*

$$G(x) = F(x) + \mathrm{Tr}(x)L(x),$$

where F and L are arbitrary mappings on $\mathbb{F}_{2^n}$ (where L is not necessarily linear). Then, for every $a \in T_0$ we have

$$D_a G(x) = (F(x) + F(x + a)) + \mathrm{Tr}(x)(L(x) + L(x + a)).$$

Suppose that the mappings $F(x)$ and $F'(x) := F(x) + L(x)$ are APN. Set $I_a = \mathrm{Im}\,(D_a F) \cap \mathrm{Im}\,(D_a F')$. Then, G is APN if and only if for any nonzero $a \in T_0$ and every $b \in I_a$ there is $x \in \mathbb{F}_{2^n}$ with

$$D_a F(x) = b \text{ and } \mathrm{Tr}(x) = 1, \text{ or } D_a F'(x) = b \text{ and } \mathrm{Tr}(x) = 0.$$

In this section, we consider in detail a particular case when F is *quadratic APN* and L is *linear*.

3.1 A characterization for the quadratic case and the notion of H-equivalence

First, we derive a necessary and sufficient condition for the APN-ness of the functions $F(x) + \mathrm{Tr}(x)L(x)$ on $\mathbb{F}_{2^n}$, where F is a quadratic APN function and L is a linear mapping on $\mathbb{F}_{2^n}$.

Theorem 3.2. *Let F be a quadratic APN function on $\mathbb{F}_{2^n}$ and L an $\mathbb{F}_2$-linear mapping on $\mathbb{F}_{2^n}$. Let $e_0 \in \mathbb{F}_{2^n}$ with $\mathrm{Tr}(e_0) = 1$. Then, the mapping*

$$G(x) = F(x) + \mathrm{Tr}(x)L(x), \quad for \quad x \in \mathbb{F}_{2^n},$$

is a quadratic APN function on $\mathbb{F}_{2^n}$ if and only if $L_a\colon T_0 \ni x \mapsto L(x) + B_F(x, a + e_0) \in \mathbb{F}_{2^n}$ are one-to-one mappings from T_0 to $\mathbb{F}_{2^n}$ for any $a \in T_0$. (Hence, $G(x) = F(x) + \mathrm{Tr}(x)L(x)$ is a quadratic APN function on $\mathbb{F}_{2^n}$ if, and only if, $L_a(x) = 0$ implies $x = 0$ for any $a \in T_0$).

Proof. Let $f := F|_{T_0}$ be the restriction of F to T_0; f is a quadratic APN function from T_0 to $\mathbb{F}_{2^n}$. For $x \in T_0$, we have $F(x) + \mathrm{Tr}(x)L(x) = f(x)$ and $F(x + e_0) + \mathrm{Tr}(x + e_0)L(x + e_0) = f(x) + L(x) + B_F(x, e_0) + L(e_0) + F(e_0) + F(0)$. Let G' be a function on $\mathbb{F}_{2^n}$ defined by $G'(x) := f(x)$ and $G'(x + e_0) := f(x) + L(x) + B_F(e_0, x)$ for $x \in T_0$, then $G'(x) = F(x) + \mathrm{Tr}(x)(L(x) + L(e_0) + F(e_0) + F(0))$ for $x \in \mathbb{F}_{2^n}$, which is EA-equivalent to $G(x) = F(x) + \mathrm{Tr}(x)L(x)$. By Proposition 2.11, G' is an APN function if

and only if $T_0 \ni x \mapsto L(x) + B_F(x, e_0) + B_F(x, a) \in \mathbb{F}_{2^n}$ are one-to-one mappings for any $a \in T_0$. Thus, $G(x) = F(x) + \text{Tr}(x)L(x)$ is a quadratic APN function on $\mathbb{F}_{2^n}$ if and only if $L_a \colon T_0 \ni x \mapsto L(x) + B_F(x, a + e_0) \in \mathbb{F}_{2^n}$ are one-to-one mappings from T_0 to $\mathbb{F}_{2^n}$ for any $a \in T_0$. $\qquad\square$

Example 3.3. Let e_0 be a fixed element of $\mathbb{F}_{2^n}$ such that $\text{Tr}(e_0) = 1$. For the quadratic function $F(x) = x^3$ on $\mathbb{F}_2^n$, we consider (for different values of n) linear mappings L on $\mathbb{F}_{2^n}$ with $L(e_0) = 0$ satisfying the conditions of Theorem 3.2. For $F(x) = x^3$ on $\mathbb{F}_{2^4}$, there are 448 such mappings L; for $F(x) = x^3$ on $\mathbb{F}_{2^5}$, there are $4\,608$ such mappings L; and for $F(x) = x^3$ on $\mathbb{F}_{2^6}$, we found about $40\,000$ such mappings L.

As the previous example indicates, it is possible to obtain many APN functions by modifying the values of a given APN function on a hyperplane using an affine function. This observation essentially leads to the following notion of equivalence.

Definition 3.4. Let H be a hyperplane of $\mathbb{F}_2^n$. Let F and G be APN functions on $\mathbb{F}_2^n$. We say that functions F and G are H-*equivalent* if there exists an affine function $L \colon \mathbb{F}_2^n \to \mathbb{F}_2^n$ s.t. for all $x \in \mathbb{F}_{2^n}$ it holds that $G(x) = F(x)$ if $x \in H$, and $G(x) = F(x) + L(x)$ if $x \notin H$.

The following result demonstrates that H-equivalence can be used to derive not only numerous APN functions from a single one but also many that are EA-inequivalent.

Theorem 3.5. *Up to EA-equivalence, every quadratic APN function on $\mathbb{F}_{2^6}$ has the form $\mathbb{F}_{2^6} \ni x \mapsto x^3 + \text{Tr}(x)L(x)$, where L is a linearized polynomial on $\mathbb{F}_{2^6}$.*

Proof. First, we observe H-equivalence can be studied in the representatives of EA-equivalence classes. Let G be an APN function on $\mathbb{F}_{2^n}$ defined by $G(x) = F(x) + 1_H(x)L(x)$, for $x \in \mathbb{F}_2^n$, where H is a hyperplane given by $H = \{x \in \mathbb{F}_2^n \colon a \cdot x = \beta\}$, for some $a \in \mathbb{F}_2^n$ and $\beta \in \mathbb{F}_2$. Consider the function $G' = A \circ G \circ B + C$ which is EA-equivalent to G, i.e., $A, B \colon \mathbb{F}_2^n \to \mathbb{F}_2^n$ are affine invertible mappings and $C \colon \mathbb{F}_2^n \to \mathbb{F}_2^n$ is affine. Denote by $1_H \colon \mathbb{F}_2^n \to \mathbb{F}_2$ the indicator function of $H \subset \mathbb{F}_2^n$, i.e., $1_H(x) = 1$ if $x \in H$ and $1_H(x) = 0$ if $x \notin H$. By definition of G', we have

$$
\begin{aligned}
G'(x) &= A\big(F(B(x)) + C(x) + A(1_H(B(x))L(B(x)))\big) \\
&= F'(x) + 1_H(B(x))L'(x) \\
&= F'(x) + 1_{H'}(x)L'(x),
\end{aligned}
$$

where $F' = A \circ F \circ B + C$, $L' = A \circ L \circ B$ and the hyperplane H' is defined by $H' = \{x \in \mathbb{F}_2^n \colon a \cdot B(x) = \beta\}$. In this way, it is enough to show that a representative of every EA-equivalence class of quadratic APN functions on $\mathbb{F}_2^6$ can be obtained from $\mathbb{F}_{2^6} \ni x \mapsto x^3$ using H-equivalence.

Let the multiplicative group of $\mathbb{F}_{2^6}$ be defined by $(\mathbb{F}_{2^6})^* = \langle a \rangle$, where $\alpha^6 + \alpha^4 + \alpha^3 + \alpha + 1 = 0$. In Table 3.1, we give the linearized polynomials $L_i \colon \mathbb{F}_{2^6} \to \mathbb{F}_{2^6}$ that define quadratic APN functions $G_i(x) = F(x) + \text{Tr}(x)L_i(x)$. We also indicate, which of these functions are EA-equivalent to the k-th Dillon APN function, whose univariate representations can be found in [21, Table 4]. The EA-equivalence was verified using Magma [5]. $\qquad\square$

Table 3.1: APN functions $G_i(x) = x^3 + \text{Tr}(x)L_i(x)$ on $\mathbb{F}_{2^6}$ and their EA-equivalence to Dillon's quadratic APN functions $D_k(x)$.

G_i	$L_i(x)$	D_k
G_1	$L_1(x) = 0$	D_1
G_2	$L_2(x) = \alpha^{42}x + \alpha^3 x^2 + \alpha^{34}x^{2^2} + \alpha^{59}x^{2^3} + \alpha^{59}x^{2^4} + \alpha^{12}x^{2^5}$	D_{10}
G_3	$L_3(x) = \alpha^{18}x + \alpha^{60}x^2 + \alpha^{17}x^{2^2} + \alpha^4 x^{2^3} + \alpha^{17}x^{2^4} + \alpha^4 x^{2^5}$	D_2
G_4	$L_4(x) = \alpha^{18}x + \alpha^{60}x^2 + \alpha^{57}x^{2^2} + \alpha^7 x^{2^3} + \alpha^{32}x^{2^4} + \alpha^{62}x^{2^5}$	D_3
G_5	$L_5(x) = \alpha^{42}x + \alpha x^2 + \alpha^{29}x^{2^2} + \alpha^{55}x^{2^3} + \alpha^9 x^{2^4} + \alpha^{56}x^{2^5}$	D_5
G_6	$L_6(x) = \alpha^{42}x + \alpha^{21}x^2 + \alpha^4 x^{2^3} + \alpha^{48}x^{2^4} + \alpha^{16}x^{2^5}$	D_6
G_7	$L_7(x) = \alpha^{42}x + \alpha^{19}x^2 + \alpha^{51}x^{2^2} + \alpha^{59}x^{2^3} + \alpha^{26}x^{2^4} + \alpha^{38}x^{2^5}$	D_7
G_8	$L_8(x) = \alpha^{42}x + \alpha^{19}x^2 + \alpha^{60}x^{2^2} + \alpha^{11}x^{2^3} + \alpha^{25}x^{2^4} + \alpha^{13}x^{2^5}$	D_{12}
G_9	$L_9(x) = \alpha^{42}x + \alpha^{21}x^2 + \alpha^{22}x^{2^2} + \alpha^{31}x^{2^3} + \alpha^{15}x^{2^4} + \alpha^{61}x^{2^5}$	D_{13}
G_{10}	$L_{10}(x) = \alpha^{42}x + \alpha^{47}x^2 + \alpha^{35}x^{2^2} + \alpha^{54}x^{2^3} + \alpha^{23}x^{2^4} + \alpha^{27}x^{2^5}$	D_8
G_{11}	$L_{11}(x) = \alpha^{42}x + \alpha^{21}x^2 + \alpha^{23}x^{2^2} + \alpha^{32}x^{2^3} + \alpha^{14}x^{2^4} + \alpha^{51}x^{2^5}$	D_{11}
G_{12}	$L_{12}(x) = \alpha^{42}x + \alpha^{21}x^2 + \alpha^4 x^{2^2} + \alpha^{56}x^{2^3} + \alpha^{17}x^{2^4} + \alpha^{20}x^{2^5}$	D_4
G_{13}	$L_{13}(x) = \alpha^{42}x + \alpha^{21}x^2 + \alpha^{27}x^{2^3} + \alpha^{34}x^{2^4} + \alpha^{52}x^{2^5}$	D_9

Remark 3.6. 1. In [16], it was shown that switching cannot be used to obtain representatives of all EA-equivalence classes of quadratic APN functions starting from a single class. However, this can be achieved using H-equivalence with the hyperplane $H = \{x \in \mathbb{F}_{2^n} \colon \text{Tr}(x) = 0\}$. Indeed, by Theorem 3.2, two EA-inequivalent quadratic APN functions on $\mathbb{F}_{2^6}$ have the form $F(x) = x^3 + \text{Tr}(x)L(x)$ and $F'(x) = x^3 + \text{Tr}(x)L'(x)$, from what follows that $F'(x) = F(x) + \text{Tr}(x)L''(x)$, where $L'' := L + L'$ is a linear mapping on $\mathbb{F}_{2^6}$. We believe that it is an interesting research direction to investigate what proportion of the known quadratic APN functions in higher dimensions can be written in this form.

2. For an (n,n)-function F, the mapping $W_F \colon \mathbb{F}_{2^n} \times \mathbb{F}_{2^n} \to \mathbb{Z}$ defined by $W_F(a,b) = \sum_{x \in \mathbb{F}_{2^n}} (-1)^{\text{Tr}(bF(x)+ax)}$, where $a, b \in \mathbb{F}_{2^n}, b \in \mathbb{F}_{2^n}^\times$, is called the *Walsh transform* of F. The multiset $\mathcal{W}_F = \{* \, W_F(a,b) \colon a \in \mathbb{F}_{2^n}, b \in \mathbb{F}_{2^n}^\times \, *\}$ is called the *Walsh spectrum* of F. If n is even, an APN function F on $\mathbb{F}_{2^n}$ is said to have the *the classical Walsh spectrum* if

$$\mathcal{W}_F = \left\{ * \, 0 \left[2^{n-2} \cdot (2^n - 1)\right], \pm 2^{\frac{n+2}{2}} \left[\frac{1}{3}(2^n - 1) \cdot \left(2^{n-3} \pm 2^{\frac{n-4}{2}}\right)\right], \right.$$
$$\left. \pm 2^{\frac{n}{2}} \left[\frac{2}{3}(2^n - 1) \cdot \left(2^{n-1} \pm 2^{\frac{n}{2}-1}\right)\right] \, * \right\}.$$

Otherwise, F is said to have a *non-classical Walsh spectrum*; see [21]. Note that most of the known examples and constructions of quadratic APN functions on $\mathbb{F}_{2^n}$ have the classical Walsh spectrum and only a few sporadic examples with a non-classical spectrum are known; for the recent advances in such functions, we refer to [4]. Note that, up to EA-equivalence, the function G_7 in Table 3.1 is the only quadratic APN function on $\mathbb{F}_{2^6}$ with a non-classical Walsh spectrum since its Walsh transform takes the values in the set

$\{0, \pm 8, \pm 16, \pm 32\}$. Remarkably, this function can be constructed via H-equivalence from the Gold APN function $\mathbb{F}_{2^6} \ni x \mapsto x^3$ with the classical Walsh spectrum.

3.2 A necessary and sufficient condition for the APN-ness of $G(x) = x^3 + \text{Tr}(x)L(x)$

In the previous subsection, we showed that one can obtain many EA-inequivalent APN functions by modifying the mapping $x \in \mathbb{F}_{2^n} \mapsto x^3$ on the "trace-one" hyperplane. In this regard, it is natural to ask: When does the mapping $G(x) = x^3 + Tr(x)L(x)$ define an APN function G on $\mathbb{F}_{2^n}$? In the following theorem, we provide an answer to this question using certain exponential sums.

Theorem 3.7. *Let G be a function from $\mathbb{F}_{2^n}$ to $\mathbb{F}_{2^n}$ defined as*

$$G(x) = x^3 + \text{Tr}(x)L(x).$$

Then, G is APN if and only if

$$\sum_{x \in \mathbb{F}_{2^n} \setminus \{0,1\}} (-1)^{\text{Tr}\left(\frac{x^2 L(x^2+x)}{(x^2+x)^3}\right)} - \frac{1}{2} \sum_{x \in \mathbb{F}_{2^n} \setminus \{0,1\}} (-1)^{\text{Tr}\left(\frac{L(x^2+x)}{(x^2+x)^3}\right)} = 2^{n-1} - 1. \tag{3.1}$$

Proof. Assume that for every $a, b \in \mathbb{F}_{2^n}$ with $a \neq 0$, the equation $G(x+a) + G(x) = b$ has at most two solutions. Since $G(x)$ is a quadratic function, we just count the number of solutions of the equation $G(x+a) + G(x) + G(a) = 0$. This gives

$$G(x+a) + G(x) + G(a) = (x+a)^3 + \text{Tr}(x+a)L(x+a)$$
$$+ x^3 + \text{Tr}(x)L(x) + a^3 + \text{Tr}(a)L(a) = 0.$$

After simplification, we have

$$x^2 a + a^2 x + \text{Tr}(x)L(a) + \text{Tr}(a)L(x) = 0. \tag{3.2}$$

We have to show that this equation has only two solutions for $a \neq 0$. Note that we can see immediately two solutions, namely $x = 0$ and $x = a$.

I. Consider the case $\text{Tr}(a) = 0$. Then, Eq. (3.2) becomes

$$x^2 a + a^2 x + \text{Tr}(x)L(a) = 0. \tag{3.3}$$

We show that this equation has exactly two solutions if and only if the condition in Eq. (3.1) holds. Assume that $\text{Tr}(x) = 0$. Then, Eq. (3.3) becomes

$$x^2 a + a^2 x = 0.$$

The above equation has exactly two solutions $x \in \{0, a\}$. Now, we show that the case $\text{Tr}(x) = 1$ gives no solutions if and only if Eq. (3.1) holds. Assume that $\text{Tr}(x) = 1$. Then, Eq. (3.3) becomes

$$x^2 a + a^2 x + L(a) = 0. \tag{3.4}$$

Let $H = \{x \in \mathbb{F}_{2^n} \colon \operatorname{Tr}(x) = 0\}, \hat{H} = \mathbb{F}_{2^n} \backslash H$ and $H^\times = H \backslash \{0\}$. Let

$$t_0 = \#\{x \in H, a \in H^\times \colon x^2 a + a^2 x + L(a) = 0\}, \text{ and}$$
$$t_1 = \#\{x \in \hat{H}, a \in H^\times \colon x^2 a + a^2 x + L(a) = 0\}.$$

Then, we define

$$s_0 = \sum_{\beta \in \mathbb{F}_{2^n}, a \in H^\times, x \in H} (-1)^{\operatorname{Tr}(\beta(x^2 a + a^2 x + L(a)))} = 2^n t_0,$$

$$s_1 = \sum_{\beta \in \mathbb{F}_{2^n}, a \in H^\times, x \in \mathbb{F}_{2^n}} (-1)^{\operatorname{Tr}(\beta(x^2 a + a^2 x + L(a)))} = 2^n (t_0 + t_1).$$

In this way, the value of t_1 is given by

$$t_1 = \frac{s_1 - s_0}{2^n}.$$

First, we consider the expressions of s_1 and s_0:

$$
\begin{aligned}
s_1 &= \sum_{\beta \in \mathbb{F}_{2^n}, a \in H^\times} (-1)^{\operatorname{Tr}(\beta L(a))} \sum_{x \in \mathbb{F}_{2^n}} (-1)^{\operatorname{Tr}(\beta(x^2 a + a^2 x))} \\
&= \sum_{\beta \in \mathbb{F}_{2^n}, a \in H^\times} (-1)^{\operatorname{Tr}(\beta L(a))} \sum_{x \in \mathbb{F}_{2^n}} (-1)^{\operatorname{Tr}(\beta a^3((\frac{x}{a})^2 + (\frac{x}{a})))},
\end{aligned}
\tag{3.5}
$$

and similarly

$$
\begin{aligned}
s_0 &= \sum_{\beta \in \mathbb{F}_{2^n}, a \in H^\times} (-1)^{\operatorname{Tr}(\beta L(a))} \sum_{x \in H} (-1)^{\operatorname{Tr}(\beta(x^2 a + a^2 x))} \\
&= \sum_{\beta \in \mathbb{F}_{2^n}, a \in H^\times} (-1)^{\operatorname{Tr}(\beta L(a))} \sum_{x \in H} (-1)^{\operatorname{Tr}(\beta a^3((\frac{x}{a})^2 + (\frac{x}{a})))}.
\end{aligned}
\tag{3.6}
$$

Since both expressions depend on the evaluation of $\operatorname{Tr}(\beta a^3((\frac{x}{a})^2 + (\frac{x}{a})))$, let us consider the solutions of the equation $\operatorname{Tr}(\beta a^3((\frac{x}{a})^2 + (\frac{x}{a}))) = 0$. Note that for $\beta \in \mathbb{F}_{2^n}$ and a fixed $a \in \mathbb{F}_{2^n}$ with $\operatorname{Tr}(a) = 0$ we have that

$$\operatorname{Tr}\left(\beta a^3 \left(\left(\frac{x}{a}\right)^2 + \left(\frac{x}{a}\right)\right)\right) = 0$$

holds for all $x \in H$ if and only if

$$\operatorname{Tr}\left(x^2 \left(\frac{\beta a^3}{a^2} + \frac{\beta^2 a^6}{a^2}\right)\right) = 0 \iff \frac{\beta a^3}{a^2} + \frac{\beta^2 a^6}{a^2} = 0 \text{ or } 1.$$

First, we consider $\frac{\beta a^3}{a^2} + \frac{\beta^2 a^6}{a^2} = 0$, which gives the following cases:

(1) $\beta = 0$,

(2) $\beta a^3 + \beta^2 a^6 = 0$ if and only if $\beta = \frac{1}{a^3}$ (provided $\beta \neq 0$).

On the other hand, the condition $\frac{\beta a^3}{a^2} + \frac{\beta^2 a^6}{a^2} = 1$ is equivalent to

(3) $\beta a^3 + \beta^2 a^6 = a^2$.

We note that in the latter case, $\text{Tr}(\beta a^3 ((\frac{x}{a})^2 + (\frac{x}{a}))) = 0$ holds for all $x \in H$, but not for all $x \in \mathbb{F}_{2^n}$, hence this case occurs just in Eq. (3.6), but not in Eq. (3.5).

Considering these three cases, we can now compute the values of s_1 and s_0. With the first two cases, Eq. (3.5) becomes

$$
\begin{aligned}
s_1 &= \sum_{\beta \in \mathbb{F}_{2^n}, a \in H^\times} (-1)^{\text{Tr}(\beta L(a))} \sum_{x \in \mathbb{F}_{2^n}} (-1)^{\text{Tr}(\beta a^3 ((\frac{x}{a})^2 + (\frac{x}{a})))} \\
&= 2^n (2^{n-1} - 1) + 2^n \left(\sum_{a \in H^\times} (-1)^{\text{Tr}\left(\frac{L(a)}{a^3}\right)} \right),
\end{aligned}
\tag{3.7}
$$

where the first term corresponds to case (1) $\beta = 0$, while the second term corresponds to case (2) $\beta a^3 = 1$. Consider now Eq. (3.6). Let $\gamma = \beta a^3$. Then, we have $\beta = \frac{\gamma}{a^3}$. From case (3), we have that $\gamma + \gamma^2 = a^2$. Therefore, we obtain

$$
\begin{aligned}
s_0 =& 2^{n-1}(2^{n-1} - 1) + 2^{n-1} \sum_{a \in H^\times} (-1)^{\text{Tr}\left(\frac{L(a)}{a^3}\right)} \\
&+ 2^{n-1} \left(\sum_{\substack{a \in H^\times \, s.t. \, a^2 = \gamma + \gamma^2 \\ for \, \gamma \in \mathbb{F}_{2^n} \setminus \{0,1\}}} (-1)^{\text{Tr}\left(\gamma \frac{L(a)}{a^3}\right)} \right),
\end{aligned}
$$

where the first two terms are again obtained as in Eq. (3.7). Now, substitute $a = \sqrt{\gamma + \gamma^2}$, the above equation becomes

$$
\begin{aligned}
s_0 =& 2^{n-1}(2^{n-1} - 1) + 2^{n-1} \sum_{a \in H^\times} (-1)^{\text{Tr}\left(\frac{L(a)}{a^3}\right)} \\
&+ 2^{n-1} \left(\sum_{\gamma \in \mathbb{F}_{2^n} \setminus \{0,1\}} (-1)^{\text{Tr}\left(\frac{\gamma L(\sqrt{\gamma + \gamma^2})}{(\sqrt{\gamma + \gamma^2})^3}\right)} \right) \\
=& \frac{s_1}{2} + 2^{n-1} \left(\sum_{\gamma \in \mathbb{F}_{2^n} \setminus \{0,1\}} (-1)^{\text{Tr}\left(\frac{\gamma L(\sqrt{\gamma + \gamma^2})}{(\sqrt{\gamma + \gamma^2})^3}\right)} \right).
\end{aligned}
\tag{3.8}
$$

Eq. (3.3) has exactly two solutions for $a \neq 0$ with $\text{Tr}(a) = 0$ if and only if $t_1 = s_1 - s_0 = 0$, hence $s_0 = s_1$. Substituting $s_0 = s_1$ in Eq. (3.8) and replacing γ with x^2, we get

$$
s_1 = 2^n \sum_{x \in \mathbb{F}_{2^n} \setminus \{0,1\}} (-1)^{\text{Tr}\left(\frac{x^2 L(x^2 + x)}{(x^2 + x)^3}\right)}.
\tag{3.9}
$$

Substituting the obtained above value of s_1 in Eq. (3.7), we get

$$\sum_{x \in \mathbb{F}_{2^n} \setminus \{0,1\}} (-1)^{\mathrm{Tr}\left(\frac{x^2 L(x^2+x)}{(x^2+x)^3} \right)} - \sum_{a \in H^\times} (-1)^{\mathrm{Tr}\left(\frac{L(a)}{a^3} \right)} = 2^{n-1} - 1,$$

which is equivalent to the original condition given in Eq. (3.1) since

$$\sum_{a \in H^\times} (-1)^{\mathrm{Tr}\left(\frac{L(a)}{a^3} \right)} = \frac{1}{2} \sum_{x \in \mathbb{F}_{2^n} \setminus \{0,1\}} (-1)^{\mathrm{Tr}\left(\frac{L(x^2+x)}{(x^2+x)^3} \right)},$$

because $x^2 + x$ runs through all the elements in $H^\times$ twice if $x \in \mathbb{F}_{2^n} \setminus \{0,1\}$. This completes the proof of the first case $\mathrm{Tr}(a) = 0$.

II. Consider the case $\mathrm{Tr}(a) = 1$. Then, Eq. (3.2) becomes

$$x^2 a + a^2 x + \mathrm{Tr}(x) L(a) + L(x) = 0. \tag{3.10}$$

Assume that $\mathrm{Tr}(x) = 0$. Then, Eq. (3.10) becomes

$$x^2 a + a^2 x + L(x) = 0,$$

which is symmetric to Eq. (3.4) w.r.t. a change of the variables. Assuming that there is a solution $x \neq 0$ with $\mathrm{Tr}(x) = 0$, one can find $a \in \mathbb{F}_{2^n}$ s.t. it satisfies Eq. (3.4). Case **I** shows that $\mathrm{Tr}(a) = 0$, a contradiction.

Assume now that $\mathrm{Tr}(x) = 1$. In this case,

$$x^2 a + a^2 x + L(a) + L(x) = 0$$

or, putting $y = x + a$,

$$y^2 a + a^2 y + L(y) = 0. \tag{3.11}$$

One solution is $y = 0$, hence $x = a$. But for a given $y \neq 0$ with $\mathrm{Tr}(y) = 0$, there is no a with $\mathrm{Tr}(a) = 1$ which satisfies Eq. (3.11), as in case **I**, hence also for $\mathrm{Tr}(a) = 1$ we have the only two solutions $x \in \{0, a\}$ for Eq. (3.2).

In this way, we conclude that G is APN if and only if the condition in Eq. (3.1) holds. $\qquad \square$

Remark 3.8. In comparison with Theorem 3.2, Theorem 3.7 provides a more practical criterion for verifying the APN property. Specifically, Theorem 3.2 requires checking the injectivity of the mappings $L_a \colon T_0 \to \mathbb{F}_{2^n}$ for every $a \in T_0$, which becomes computationally expensive for large n. In contrast, Theorem 3.7 reduces this task to verifying the single condition given in Eq. (3.1). Using this criterion, one can check with a computer algebra system that linearized polynomials in Table 3.1 indeed satisfy the APN condition given in Theorem 3.7.

4 Modifying APN functions on affine subspaces of codimension two

In the previous section, we showed that it is possible to construct a new APN function from a given one by adding a linear function defined on a hyperplane. In this section, we show that new APN functions can be obtained by adding carefully selected constant functions on disjoint affine subspaces of codimension two. The following theorem provides a complete characterization of the APN property for such modifications.

Theorem 4.1. *Let F be an APN function from $\mathbb{F}_2^n$ to $\mathbb{F}_2^n$. Let U be an $(n-2)$-dimensional subspace of $\mathbb{F}_2^n$ and let $U_1 = U + u_1$, $U_2 = U + u_2$, $U_3 = U + u_3$ and $U_4 = U + u_4$ be the four cosets of U such that $\mathbb{F}_2^n = U_1 \cup U_2 \cup U_3 \cup U_4$, where $u_1 = 0$ and u_2, u_3, $u_4 \in \mathbb{F}_2^n$. Define the function $G \colon \mathbb{F}_2^n \to \mathbb{F}_2^n$ as follows*

$$G(x) = \begin{cases} F(x) + a_1, & \text{for } x \in U_1, \\ F(x) + a_2, & \text{for } x \in U_2, \\ F(x) + a_3, & \text{for } x \in U_3, \\ F(x) + a_4, & \text{for } x \in U_4, \end{cases} \qquad (4.1)$$

where $a_1, a_2, a_3, a_4 \in \mathbb{F}_2^n$. Then, the function G is APN if and only if the condition

$$F(x_1) + F(x_2) + F(x_3) + F(x_4) \neq a_1 + a_2 + a_3 + a_4$$

holds for all 2-dimensional affine subspaces $\{x_1, x_2, x_3, x_4\}$ of $\mathbb{F}_2^n$ with $|\{x_1, x_2, x_3, x_4\} \cap U_i| = 1$, for all $i = 1, 2, 3, 4$.

Proof. Let U be an $(n-2)$-dimensional linear subspace of $\mathbb{F}_2^n$. We decompose $\mathbb{F}_2^n$ into four cosets of U such that $\mathbb{F}_2^n = U_1 \cup U_2 \cup U_3 \cup U_4$, where $U_1 = U + u_1 = U$, $U_2 = U + u_2$, $U_3 = U + u_3$ and $U_4 = U + u_4$, where $u_1 = 0$ and $u_2, u_3, u_4 \in \mathbb{F}_2^n$. Since F is an APN function, we have that the condition

$$F(x_1) + F(x_2) + F(x_3) + F(x_4) \neq 0$$

holds for all 2-dimensional affine subspaces $\{x_1, x_2, x_3, x_4\}$ of $\mathbb{F}_2^n$. Now, we consider the distribution of affine 2-dimensional subspaces $\{x_1, x_2, x_3, x_4\}$ in the subspaces U_1, U_2, U_3, U_4.

Recall that the set $\{x_1, x_2, x_3, x_4\}$ is an affine 2-dimensional subspace of $\mathbb{F}_2^n$ if all x_1, x_2, x_3, x_4 are pairwise different and $x_1 + x_2 + x_3 + x_4 = 0$. Assume that $x_1, x_2 \in U_i$, $x_3 \in U_j$ and $x_4 \in U_k$, where i, j, k are pairwise different. Then, $x_1 + x_2 \in U_1$ and $x_3 + x_4 \notin U_1$. Therefore, $x_1 + x_2 + x_3 + x_4 = 0 \in U_1$ is not possible. The only possible distributions of x_1, x_2, x_3, x_4 between U_i are either:

1) $x_1, x_2, x_3, x_4 \in U_i$, for some i,

2) $x_1, x_2 \in U_i$ and $x_3, x_4 \in U_j$, for some $i \neq j$,

3) $x_1 \in U_i, x_2 \in U_j, x_3 \in U_k, x_4 \in U_l$, for $i \neq j \neq k \neq l$ (equivalently, the condition $|\{x_1, x_2, x_3, x_4\} \cap U_i| = 1$ holds for all $i = 1, 2, 3, 4$).

In order to derive a necessary and sufficient condition for the APN-ness of the function G defined in Eq. (4.1), we need to verify that $G(x_1) + G(x_2) + G(x_3) + G(x_4) \neq 0$ holds for all 2-dimensional flats $\{x_1, x_2, x_3, x_4\}$. To do so, we consider three possible distributions of the elements x_i between the subspaces U_j.

In the first case, we have that $x_1, x_2, x_3, x_4 \in U_i$, for some i. Then,

$$G(x_1) + G(x_2) + G(x_3) + G(x_4)$$
$$= (F(x_1) + a_i) + (F(x_2) + a_i) + (F(x_3) + a_i) + (F(x_4) + a_i) \neq 0$$

due to the APN property of F.

In the second case, we have that $x_1, x_2 \in U_i$ and $x_3, x_4 \in U_j$, for some $i \neq j$. Consequently,

$$G(x_1) + G(x_2) + G(x_3) + G(x_4)$$
$$= (F(x_1) + a_i) + (F(x_2) + a_i) + (F(x_3) + a_j) + (F(x_4) + a_j) \neq 0$$

again due to the APN property of F.

In the third case, we have that the condition $|\{x_1, x_2, x_3, x_4\} \cap U_i| = 1$ holds for all $i = 1, 2, 3, 4$. W.l.o.g, we assume that $x_i \in U_i$. Then, we have

$$G(x_1) + G(x_2) + G(x_3) + G(x_4)$$
$$= (F(x_1) + a_1) + (F(x_2) + a_2) + (F(x_3) + a_3) + (F(x_4) + a_4)$$
$$= F(x_1) + F(x_2) + F(x_3) + F(x_4) + (a_1 + a_2 + a_3 + a_4).$$

In this way, the function G is APN if and only if the condition

$$F(x_1) + F(x_2) + F(x_3) + F(x_4) \neq a_1 + a_2 + a_3 + a_4$$

holds for all 2-dimensional affine subspaces $\{x_1, x_2, x_3, x_4\}$ of $\mathbb{F}_2^n$ with the property

$$|\{x_1, x_2, x_3, x_4\} \cap U_i| = 1$$

for all $i = 1, 2, 3, 4$. $\qquad\square$

In the following example, we indicate that using Theorem 4.1 one construct an APN function, that is EA-inequivalent to a given one.

Example 4.2. Let F be an APN function from $\mathbb{F}_{2^8}$ to $\mathbb{F}_{2^8}$ defined as $F(x) = x^3$. Let the multiplicative group of $\mathbb{F}_{2^8}$ be defined by $(\mathbb{F}_{2^8})^* = \langle a \rangle$, where $\alpha^8 + \alpha^4 + \alpha^3 + \alpha^2 + 1 = 0$. First, we decompose $\mathbb{F}_{2^8}$ into four cosets U_1, U_2, U_3, U_4 defined by

$$U_1 = \{x \in \mathbb{F}_{2^8} : \mathrm{Tr}_2^8(x) = 0\},$$
$$U_2 = \{x \in \mathbb{F}_{2^8} : \mathrm{Tr}_2^8(x) = 1\},$$
$$U_3 = \{x \in \mathbb{F}_{2^8} : \mathrm{Tr}_2^8(x) = \beta\},$$
$$U_4 = \{x \in \mathbb{F}_{2^8} : \mathrm{Tr}_2^8(x) = \beta^2\},$$

where β is a root of $x^2 + x + 1$; in the defined above field $\mathbb{F}_{2^8}$, we have that $\beta \in \{\alpha^{85}, \alpha^{170}\}$. Compute the set

$$A = \mathbb{F}_{2^8} \setminus \left\{ \sum_{i=1}^{4} F(x_i) \colon \sum_{i=1}^{4} x_i = 0 \text{ and } x_i \in U_i, \text{ for } i = 1, 2, 3, 4 \right\}$$
$$= \{0, 1, \alpha^{85}, \alpha^{170}\}.$$

We can choose $a_1, a_2, a_3, a_4 \in \mathbb{F}_{2^8}$ such that $a_1 + a_2 + a_3 + a_4 \in A$. Setting $a_1 = a_2 = 0, a_3 = \alpha^{85}\beta, a_4 = \alpha^{85}\beta^2$, we have that $a_1 + a_2 + a_3 + a_4 = \alpha^{85} \in A$. Define the function $G \colon \mathbb{F}_{2^8} \to \mathbb{F}_{2^8}$ as in Eq. (4.1), that is

$$G(x) = \begin{cases} F(x) + a_1, & \text{for } x \in U_1, \\ F(x) + a_2, & \text{for } x \in U_2, \\ F(x) + a_3, & \text{for } x \in U_3, \\ F(x) + a_4, & \text{for } x \in U_4, \end{cases} = \begin{cases} F(x), & \text{if } \mathrm{Tr}_2^8(x) = 0, \\ F(x), & \text{if } \mathrm{Tr}_2^8(x) = 1, \\ F(x) + \alpha^{85}\beta, & \text{if } \mathrm{Tr}_2^8(x) = \beta, \\ F(x) + \alpha^{85}\beta^2, & \text{if } \mathrm{Tr}_2^8(x) = \beta^2. \end{cases}$$

Then, the function G is APN by Theorem 4.1. For the constructed function G, we give a "simplified" finite filed representation. To do so, we recall that the polynomial representation of the trace function from $\mathbb{F}_{2^n}$ to its subfield $\mathbb{F}_{2^m}$ is given by $\mathrm{Tr}_m^n(x) = \sum_{i=0}^{\frac{n}{m}-1} x^{2^{i \cdot m}}$. First, we observe that $\mathrm{Tr}_1^8(x) = \mathrm{Tr}_1^2(\mathrm{Tr}_2^8(x)) = \mathrm{Tr}_2^8(x) + (\mathrm{Tr}_2^8(x))^2$. In this way, we have that if $\mathrm{Tr}_2^8(x) \in \{0, 1\}$ then $\mathrm{Tr}_1^8(x) = 0$. On the other hand, if $\mathrm{Tr}_2^8(x) \in \{\beta, \beta^2\}$ then $\mathrm{Tr}_1^8(x) = 1$. In this way, the APN function $G \colon \mathbb{F}_{2^8} \to \mathbb{F}_{2^8}$ can be written as

$$G(x) = x^3 + \alpha^{85} \mathrm{Tr}_1^8(x) \mathrm{Tr}_2^8(x).$$

Finally, we notice that G is EA-inequivalent to $F(x) = x^3$ on $\mathbb{F}_{2^8}$, since $\Gamma\text{-rank}(G) = 13\,842 \neq \Gamma\text{-rank}(F) = 11\,818$.

5 Conclusion and open problems

In this paper, we consider further secondary constructions of APN functions. The following questions related to the computational results obtained in Section 3 deserve further theoretical investigations:

1. As we show in Remark 3.5, every quadratic APN function in dimension 6 can be written (up to EA-equivalence) as a univariate polynomial $G_i(x) = x^3 + \mathrm{Tr}(x)L_i(x)$, for $x \in \mathbb{F}_{2^6}$, where $L_i \colon \mathbb{F}_{2^6} \to \mathbb{F}_{2^6}$ is a suitable linear mapping. Alternatively, as shown in [7], each quadratic APN function in dimension 6 can also be characterized (up to EA-equivalence) through the isotopic shift construction. We believe it would be valuable to explore these two approaches further and gain a deeper understanding of their connections.

2. As we indicate in Remark 3.5, it is possible to construct APN functions with the non-classical spectrum from those with the classical one by modifying them on hyperplanes using suitable linear functions. Find more such examples in higher dimensions and analyze whether infinite families of APN functions with the non-classical Walsh spectrum of the form $\mathbb{F}_{2^n} \ni x \mapsto x^3 + \mathrm{Tr}(x)L(x)$ exist.

3. More general, find linearized polynomials satisfying the APN condition given in Eq. (3.1), which inevitably lead to quadratic APN functions of the form $\mathbb{F}_{2^n} \ni x \mapsto x^3 + \mathrm{Tr}(x)L(x)$. Is it possible to obtain APN functions of the form $\mathbb{F}_{2^n} \ni x \mapsto x^3 + \mathrm{Tr}(x)Q(x)$, where Q is quadratic, or more general, nonlinear?

Acknowledgments

References

[1] M. Abbondati, M. Calderini, and I. Villa, "On Dillon's property of (n, m)-functions," *Cryptography and Communications*, vol. 16, no. 6, pp. 1449–1473, 2024. doi:10.1007/s12095-024-00730-1

[2] R. Arshad, "Contributions to the theory of almost perfect nonlinear functions," Ph.D. dissertation, Otto-von-Guericke-Universität Magdeburg, Fakultät für Mathematik, 2018. doi:10.25673/13406

[3] C. Beierle and C. Carlet, "Gold functions and switched cube functions are not 0-extendable in dimension $n > 5$," *Des. Codes Cryptogr.*, vol. 91, no. 2, pp. 433–449, 2023. doi:10.1007/S10623-022-01111-6

[4] C. Beierle, G. Leander, and L. Perrin, "Trims and extensions of quadratic APN functions," *Des. Codes Cryptogr.*, vol. 90, no. 4, pp. 1009–1036, 2022. doi:10.1007/S10623-022-01024-4

[5] W. Bosma, J. Cannon, and C. Playoust, "The Magma algebra system. I. The user language," *Journal of Symbolic Computation*, vol. 24, no. 3-4, pp. 235–265, 1997. doi:10.1006/jsco.1996.0125

[6] L. Budaghyan, M. Calderini, C. Carlet, R. Coulter, and I. Villa, "Generalized isotopic shift construction for APN functions," *Designs, Codes and Cryptography*, vol. 89, no. 1, pp. 19–32, 2021. `doi:10.1007/s10623-020-00803-1`

[7] L. Budaghyan, M. Calderini, C. Carlet, R. S. Coulter, and I. Villa, "Constructing APN functions through isotopic shifts," *IEEE Transactions on Information Theory*, vol. 66, no. 8, pp. 5299–5309, 2020. `doi:10.1109/TIT.2020.2974471`

[8] L. Budaghyan, C. Carlet, and G. Leander, "Constructing new APN functions from known ones," *Finite Fields and Their Applications*, vol. 15, no. 2, pp. 150–159, 2009. `doi:10.1016/j.ffa.2008.10.001`

[9] L. Budaghyan, C. Carlet, and G. Leander, "On a construction of quadratic APN functions," in *2009 IEEE Information Theory Workshop*, 2009, pp. 374–378. `doi:10.1109/ITW.2009.5351383`

[10] C. Carlet, P. Charpin, and V. Zinoviev, "Codes, bent functions and permutations suitable for DES-like cryptosystems," *Design Codes Cryptography*, vol. 15, no. 2, pp. 125–156, 1998. `doi:10.1023/A:1008344232130`

[11] C. Carlet, *Boolean Functions for Cryptography and Coding Theory*. Cambridge University Press, 2021. `doi:10.1017/9781108606806`

[12] P. Charpin and G. M. Kyureghyan, "On sets determining the differential spectrum of mappings," *Int. J. Inf. Coding Theory*, vol. 4, no. 2/3, pp. 170–184, 2017. `doi:10.1504/IJICOT.2017.10004710`

[13] I. Czerwinski and A. Pott, "On large Sidon sets," 2024. `arXiv:2411.12911`

[14] J. F. Dillon, "Multiplicative difference sets via additive characters," *Designs, Codes and Cryptography*, vol. 17, no. 1, pp. 225–235, 1999. `doi:10.1023/A:1026435428030`

[15] J. F. Dillon and H. Dobbertin, "New cyclic difference sets with Singer parameters," *Finite Fields and Their Applications*, vol. 10, no. 3, pp. 342–389, 2004. `doi:10.1016/j.ffa.2003.09.003`

[16] Y. Edel and A. Pott, "A new almost perfect nonlinear function which is not quadratic," *Advances in Mathematics of Communications*, vol. 3, no. 1, pp. 59–81, 2009. `doi:10.3934/amc.2009.3.59`

[17] F. Gölöğlu, "Projective polynomials over finite fields and their applications in cryptography and combinatorics," *Habilitation Thesis*, 2023. `https://chres.is.cuni.cz/media/documents/2023/03/27/FG_short.pdf`

[18] K. Kalgin and V. Idrisova, "The classification of quadratic APN functions in 7 variables and combinatorial approaches to search for APN functions," *Cryptography and Communications*, vol. 15, no. 2, pp. 239–256, 2023. `doi:10.1007/s12095-022-00588-1`

[19] K. Li and N. Kaleyski, "Two new infinite families of APN functions in trivariate form," *IEEE Transactions on Information Theory*, vol. 70, no. 2, pp. 1436–1452, 2024. `doi:10.1109/TIT.2023.3313148`

[20] K. Nyberg, "Differentially uniform mappings for cryptography," in *Advances in Cryptology — EUROCRYPT '93*, T. Helleseth, Ed. Berlin, Heidelberg: Springer Berlin Heidelberg, 1994, pp. 55–64. `doi:10.1007/3-540-48285-7_6`

[21] A. Pott, "Almost perfect and planar functions," *Designs, Codes and Cryptography*, vol. 78, no. 1, pp. 141–195, 2016. `doi:10.1007/s10623-015-0151-x`

[22] H. Taniguchi, "D-property for APN functions from $\mathbb{F}_2^n$ to $\mathbb{F}_2^{n+1}$," *Cryptography and Communications*, vol. 15, no. 3, pp. 627–647, 2023. `doi:10.1007/s12095-023-00627-5`

[23] H. Taniguchi, "On quadratic APN functions $F(x) + Tr(x)L(x)$," in *The 8th International Workshop on Boolean Functions and their Applications*, 2023, pp. 123–127. `http://boolean.w.uib.no/files/2023/09/book_of_abstracts.pdf`

[24] I. Villa, "On APN functions $L_1(x^3) + L_2(x^9)$ with linear L_1 and L_2," *Cryptography and Communications*, vol. 11, no. 1, pp. 3–20, 2019. `doi:10.1007/s12095-018-0283-8`

[25] S. Yoshiara, "Equivalences of quadratic APN functions," *Journal of Algebraic Combinatorics*, vol. 35, no. 3, pp. 461–475, 2012. `doi:10.1007/s10801-011-0309-1`

[26] Y. Yu, M. Wang, and Y. Li, "A matrix approach for constructing quadratic APN functions," *Designs, Codes and Cryptography*, vol. 73, no. 2, pp. 587–600, 2014. `doi:10.1007/s10623-014-9955-3`