Zeros of special polynomials and their impact on a class of APN functions

Daniele Bartoli   Marco Calderini   Giuseppe Marino   Francesco Pavese

Abstract

In 2021, Calderini et al. introduced a construction for APN functions on $\mathbb{F}_{2^{2m}}$ in bivariate form

$$f(x, y) = \left(xy,\ x^{2^r+1} + x^{2^{r+m/2}} y^{2^{m/2}} + bxy^{2^r} + cy^{2^r+1}\right) \qquad r < m/2, \gcd(r, m) = 1.$$

They showed that this family exists provided the existence of a polynomial

$$P_{c,b}(X) = (cX^{2^r+1} + bX^{2^r} + 1)^{2^{m/2}+1} + X^{2^{m/2}+1},$$

with no zeros in $\mathbb{F}_{2^{2m}}$. For $m \leq 6$ it was shown that we can have APN functions belonging to this family. However, up to now, no construction of such polynomials is known for $m \geq 8$. In this work we provide a non-existence result of such functions whenever $r < m/8 - 1$, by application of techniques from algebraic varieties over finite fields. In particular, for $r = 1$ we have that the construction of Calderini et al. cannot provide an APN function for $m \geq 8$.

Keywords: APN functions, Bivariate construction, Zeros of polynomials

1   Introduction

Let $\mathbb{F}_{2^n}$ be the finite field with 2^n elements. A function f from $\mathbb{F}_{2^n}$ into itself is called almost perfect nonlinear (APN) if for any non zero $a \in \mathbb{F}_{2^n}$ and any $b \in \mathbb{F}_{2^n}$, the equation

$$f(x + a) + f(x) = b$$

admits at most two solutions.

APN functions play a central role in modern cryptography since they provide optimal resistance against differential cryptanalysis ([3]) when used as substitution boxes in block ciphers.

D. Bartoli: Department of Mathematics and Informatics, University of Perugia, Perugia, Italy; *e-mail*: daniele.bartoli@unipg.it

M. Calderini: Department of Mathematics, University of Trento, Trento, Italy; *e-mail*: marco.calderini@unitn.it

G. Marino: Department of Mathematics and Applications "R. Caccioppoli", University of Naples "Federico II", Naples, Italy; *e-mail*: giuseppe.marino@unina.it

F. Pavese: Department of Mechanics, Mathematics and Management, Polytechnic University of Bari, Bari, Italy; *e-mail*: francesco.pavese@poliba.it

Beyond cryptography, they also appear as optimal objects in coding theory, combinatorics, and projective geometry [13, 14, 15].

Despite their importance, only a few infinite families of APN functions are currently known, and their classification up to CCZ- or EA-equivalence remains an open problem (see [23] for a list of known APN families and for the definition of these equivalence relations).

Several of the known families that can be defined in even dimension have been obtained using the so called bivariate construction introduced by Carlet in [11]. In particular, let $n = 2m$, we can decompose $\mathbb{F}_{2^n}$ as $\mathbb{F}_{2^m} \times \mathbb{F}_{2^m}$, and a function from $\mathbb{F}_{2^m} \times \mathbb{F}_{2^m}$ into itself can be represented using bivariate polynomials, that is, $f(x, y) = (f_1(x, y), f_2(x, y))$ with $f_1, f_2 \in \mathbb{F}_{2^m}[x, y]$.

In [11], the author considered functions $f(x, y)$ where $f_1(x, y)$ was given by the Maiorana-McFarland function xy, and provided some necessary and sufficient conditions for the APN property of $f(x, y)$. He also introduced a class of APN function in bivariate form which was later proved (see [9]) to be equivalent to the hexanomial family constructed in [8]. The bivariate construction was later used for obtaining other classes of APN functions ([9, 26, 27]). Recently, in [18], Göloğlu proposed a generalization of the bivariate construction based on the so-called biprojective polynomials. Bi-projective polynomials has been used for constructing several classes of APN functions lately [10, 19, 24].

Within specific families, the APN property is intrinsically connected to the existence of polynomials with well-defined structural properties. Accordingly, a fundamental problem is to determine whether APN functions derived from these constructions exist in infinitely many dimensions or whether they are restricted to finitely many instances [2, 5, 7, 17].

In particular, the existence of several classes of bivariate APN families constructed to date relies on the fact that a certain projective polynomial, that is a polynomial of type $x^{2^r+1} + x + a$, admits no roots over $\mathbb{F}_{2^m}$ [10, 11, 26].

Projective polynomials and their roots have been studied in several works, such as [4, 7, 20, 21]. So, applying Bluher's results ([4]), one obtains that these constructions yield an APN function in every dimension in which they are defined.

For the case of the APN class introduced in [9], the existence of instances coming from this construction is related to the roots of a certain polynomial, which is not projective.

In particular, the APN class given in [9] is the following:

Theorem 1.1. *[9, Theorem 6.2] Let $n = 2m$ with m even, and let $r < m/2$ be such that $\gcd(r, m) = 1$. Consider $b, c \in \mathbb{F}_{2^m}$ Then*

$$f_{b,c,r}(x, y) = \left(xy, \ x^{2^r+1} + x^{2^{r+m/2}} y^{2^{m/2}} + bxy^{2^r} + cy^{2^r+1}\right)$$

is APN if and only if

$$P_{c,b}(X) = \left(cX^{2^r+1} + bX^{2^r} + 1\right)^{2^{m/2}+1} + X^{2^{m/2}+1}$$

has no zero in $\mathbb{F}_{2^m}$.

The authors showed that for $n \leq 12$ (so $m \leq 6$) it was possible to produce new APN functions (up to CCZ-equivalence). However, if such functions exist also for higher dimensions is an open problem.

The aim of this work is to investigate such an open question. In particular, we prove that for each $r < m/8 - 1$ there are no instances of $b, c \in \mathbb{F}_{2^m}$ for which $f_{b,c,r}(x, y)$ is APN.

The main tool is given by application of techniques from algebraic varieties over finite fields.

Denote $q = 2^{m/2}$. First observe that $P_{c,b}(X)$ has a zero in $\mathbb{F}_{q^2}$ if and only if there exists $x \in \mathbb{F}_{q^2}^*$ such that

$$\frac{cx^{2^r+1} + bx^{2^r} + 1}{x} \tag{1.1}$$

is a $(q + 1)$-root of unity. This is equivalent to ask that

$$\frac{cx^{2^r+1} + bx^{2^r} + 1}{x} = \frac{x^q}{c^q x^{(2^r+1)q} + b^q x^{2^r q} + 1}.$$

Let $x = x_0 + \xi x_1$, where $\{1, \xi\}$ is an $\mathbb{F}_q$ basis of $\mathbb{F}_{q^2}$ and $x_0, x_1 \in \mathbb{F}_q$. The previous condition (since $x \neq 0$) can be equivalently rewritten as

$$\left(c(x_0 + \xi x_1)^{2^r+1} + b(x_0 + \xi x_1)^{2^r} + 1\right)\left(c^q(x_0 + \xi^q x_1)^{2^r+1} + b^q(x_0 + \xi^q x_1)^{2^r} + 1\right) + (x_0 + \xi x_1)(x_0 + \xi^q x_1) = 0.$$

In order to prove that for each $b, c \in \mathbb{F}_{q^2}$ there is at least a solution $(\overline{x_0}, \overline{x_1}) \in \mathbb{F}_q^2$ to the above equation, we consider the algebraic curve $\mathcal{D}_{b,c,r}$ defined by

$$\left(c(X + \xi Y)^{2^r+1} + b(X + \xi Y)^{2^r} + 1\right)\left(c^q(X + \xi^q Y)^{2^r+1} + b^q(X + \xi^q Y)^{2^r} + 1\right) + (X + \xi Y)(X + \xi^q Y) = 0.$$

Via the change of variables $(X + \xi Y, X + \xi^q Y) \mapsto (X, Y)$, $\mathcal{D}_{b,c,r}$ is affinely equivalent to the plane curve $\mathcal{C}_{b,c,r}$ defined by

$$\left(cX^{2^r+1} + bX^{2^r} + 1\right)\left(c^q Y^{2^r+1} + b^q Y^{2^r} + 1\right) + XY = 0.$$

Our strategy consists in proving that $\mathcal{C}_{b,c,r}$, $b, c \in \mathbb{F}_{q^2}$, $c \neq 0$, $r \geq 1$, is absolutely irreducible and so is $\mathcal{D}_{b,c,r}$. Hence, by the Hasse-Weil bound we obtain the existence of at least one point $(\overline{x_0}, \overline{x_1}) \in \mathbb{F}_q^2$ in $\mathcal{D}_{b,c,r}$. The case $c = 0$ is treated separataly. Therefore, by Theorem 1.1 the function $f_{b,c,r}(x, y)$ is not APN.

2 Preliminary results

We now recall some basic facts on curves/surfaces over (finite) fields. For more details, we refer to [16, 22], or the reader's favorite algebraic geometry book. As customary, for a field $\mathbb{F}$, we denote by $\overline{\mathbb{F}}$ its algebraic closure, and by $\mathbb{P}^m(\mathbb{F})$ (respectively, $\mathbb{A}^m(\mathbb{F})$) the m-dimensional projective (respectively, affine) space over the field $\mathbb{F}$. Solutions of one or more polynomial equations form what we call algebraic hypersurfaces or varieties. An algebraic hypersurface defined over a field $\mathbb{F}$ is called absolutely irreducible if the associated polynomial is irreducible over every algebraic extension of $\mathbb{F}$. An absolutely irreducible $\mathbb{F}$-rational component of a hypersurface defined by a polynomial F is an absolutely irreducible hypersurface, associated to a factor of F defined over $\overline{\mathbb{F}}$.

In two dimensions, C is an affine curve over a field $\mathbb{F}$ if it is the zero set of a polynomial $F(X, Y) \in \mathbb{F}[X, Y]$. A projective curve C over a field $\mathbb{F}$ is the zero set of a homogeneous polynomial $F(X, Y, Z) \in \mathbb{F}[X, Y, Z]$. The polynomial F is the defining polynomial of C.

Finally, we will make use of the following version of the celebrated Hasse-Weil theorem.

Theorem 2.1 (Aubry-Perret bound [1, Corollary 2.5]). *Let $C \subset \mathbb{P}^n(\mathbb{F}_q)$ be an absolutely irreducible curve which is a complete intersection of $(n-1)$ hypersurfaces of degrees $d_1, \ldots, d_{n-1}$ and set $d = \prod_{i=1}^{n-1} d_i$. Then the number $C(\mathbb{F}_q)$ of $\mathbb{F}_q$-rational points of C in $\mathbb{P}^n(\mathbb{F}_q)$ satisfies*

$$q + 1 - (d-1)(d-2)\sqrt{q} \leq \#C(\mathbb{F}_q) \leq q + 1 + (d-1)(d-2)\sqrt{q}. \tag{2.1}$$

3   The case $c = 0$

In this section we will consider the case $c = 0$ and prove that for any $b \in \mathbb{F}_{q^2}^*$ the polynomial $P_{0,b}(X) = \left(bX^{2^r} + 1\right)^{q+1} + X^{q+1}$ has a zero in $\mathbb{F}_{q^2}$, and thus, we cannot have an APN function of the form $f_{b,0,r}$, where $f_{b,c,r}$ is as in Theorem 1.1.

For this purpose let us denote $\mu_{q+1} := \{x^{q-1} : x \in \mathbb{F}_{q^2}^*\}$ the set of $(q+1)$th root of unity in $\mathbb{F}_{q^2}$. Any element b of $\mathbb{F}_{q^2}^*$ can be uniquely represented as $b = ut$ for some $t \in \mathbb{F}_q^*$ and $u \in \mu_{q+1}$.

Let us recall the following well-known result, which comes from the Hilbert's Theorem 90.

Lemma 3.1. *Let $\alpha \in \mathbb{F}_{2^m}$ and let j be such that $\gcd(j, m) = 1$. Then, $Tr_2^{2^m}(\alpha) = 0$ if and only if there exists $\beta \in \mathbb{F}_{2^m}$ such that $\alpha = \beta^{2^j} - \beta$. Here $Tr_2^{2^m}$ is the trace map from $\mathbb{F}_{2^m}$ onto $\mathbb{F}_2$.*

Lemma 3.2. *Let $b \in \mathbb{F}_{q^2}^*$, and r be such that $\gcd(r, m) = 1$. Then, the polynomial $\left(bX^{2^r} + 1\right)^{q+1} + X^{q+1}$ has a zero in $\mathbb{F}_{q^2}$.*

Proof. We note that $\left(bX^{2^r} + 1\right)^{q+1} + X^{q+1}$ has a zero in $\mathbb{F}_{q^2}$ if and only if there exist $x \in \mathbb{F}_{q^2}$ and $u \in \mu_{q+1}$ such that

$$bx^{2^r} + ux + 1 = 0. \tag{3.1}$$

Now, $b = u't$ for some $t \in \mathbb{F}_q^*$ and $u' \in \mu_{q+1}$. Therefore, performing the substitution $x \mapsto b^{-2^{-r}}x$ and considering $u = u'^{2^{-r}} \in \mu_{q+1}$, Equation (3.1) becomes

$$x^{2^r} + t'x + 1 = 0, \tag{3.2}$$

where $t' = t^{-2^{-r}}$.

Let us note that $\gcd(2^r - 1, q - 1) = 1$, so there exists $\bar{t} \in \mathbb{F}_q^*$ such that $\bar{t}^{2^r - 1} = t'$. Therefore, substituting $x \mapsto \bar{t}x$ in Equation (3.2) and dividing by $\bar{t}^{2^r}$ we obtain

$$x^{2^r} + x = \bar{t}^{-2^r}.$$

Now, since $\bar{t}^{-2^r}$ is an element of $\mathbb{F}_q$ we have that $Tr_2^{q^2}\left(\bar{t}^{-2^r}\right) = 0$. Hence, being $\gcd(r, m) = 1$, from Lemma 3.1 we have that there exists an element in $\mathbb{F}_{q^2}$ such that $x^{2^r} + x = \bar{t}^{-2^r}$. $\square$

As a consequences we get the following:

Theorem 3.3. *Let $n = 2m$ with m even, and let $r < m/2$ be such that $\gcd(r, m) = 1$. Then, for any $b \in \mathbb{F}_{2^m}^*$, the function $f_{b,0,r}(x, y)$ defined as in Theorem 1.1 is not APN.*

4 On the irriducibility of $C_{b,c,r}$

Theorem 4.1. *The curve $C_{b,c,r} : F_{b,c,r}(X,Y) = 0$, where*

$$F_{b,c,r}(X,Y) = \left(cX^{2^r+1} + bX^{2^r} + 1\right)\left(c^q Y^{2^r+1} + b^q Y^{2^r} + 1\right) - XY,$$

$b, c \in \mathbb{F}_{q^2}, c \neq 0, r \geq 1$, is absolutely irreducible for any $b, c \in \mathbb{F}_{q^2}$.

Proof. First observe that there is no non-constant factor $G(X,Y) \in \overline{\mathbb{F}_q}[X,Y]$ of $F_{b,c,r}$ of degree 0 in X or Y. By way of contradiction suppose that $G(X) \mid F_{b,c,r}(X,Y)$: then $G(X) \mid GCD((cX^{2^r+1} + bX^{2^r} + 1), X) = 1$, a contradiction to G being non-trivial.

Consider $F_{b,c,r}(X,Y) = G(X,Y)H(X,Y)$, $G, H \in \overline{\mathbb{F}_q}[X,Y]$. To be more explicit,

$$\begin{aligned}
G(X,Y) &:= g_0(X)Y^s + g_1(X)Y^{s-1} + \cdots + g_s(X); \\
H(X,Y) &:= h_0(X)Y^{2^r+1-s} + h_1(X)Y^{2^r+1-s-1} + \cdots + h_{2^r+1-s}(X),
\end{aligned}$$

where each g_i and h_i are polynomials in X. Without loss of generality, we can suppose that $1 \leq s \leq 2^{r-1}$. Also

$$g_0(X)h_0(X) = c^q(cX^{2^r+1} + bX^{2^r} + 1)$$

and thus, since $c \neq 0$, $GCD(g_0(X), h_0(X)) = 1$. Comparing the coefficient of Y^{2^r} in $G(X,Y)H(X,Y)$ and in $F_{b,c,r}(X,Y)$ we deduce

$$g_0(X)h_1(X) + g_1(X)h_0(X) = b^q(cX^{2^r+1} + bX^{2^r} + 1).$$

1. In the case where $\deg(g_0(X)) > 0$, from the equations above we deduce that $g_0(X) \mid g_1(X)h_0(X)$ and thus $g_0(X) \mid g_1(X)$ since g_0 and h_0 are coprime.

   Consider now the coefficient of $Y^{2^r+1-\ell}$, $\ell \in [2\ldots s]$, in $G(X,Y)H(X,Y)$ and in $F_{b,c,r}(X,Y)$. Since they must coincide and $2^r + 1 - s \geq 2^r + 1 - 2^{r-1} = 2^{r-1} + 1 > 1$, we have that

   $$\sum_{i=0}^{\ell} g_i(X)h_{\ell-i}(Y) = 0.$$

   Thus, using induction, $g_0(X) \mid g_\ell(X)$, $\ell = 2, \ldots, s$. Therefore $g_0(X) \mid G(X,Y)$ and we find a non-costant factor of $F_{b,c,r}$ of degree 0 in Y, a contradiction.

2. In the case where $\deg(g_0(X)) = 0$, then $h_0(X) = \lambda(cX^{2^r+1} + bX^{2^r} + 1)$ for some $\lambda \in \overline{\mathbb{F}_q}^*$.

   If $s = 1$, then $G(X,Y) = g_0Y + g_1(X)$. This means that $F_{b,c,r}(X, \widetilde{g}(X)) \equiv 0$ for some $\widetilde{g}(X) \in \overline{\mathbb{F}_q}[X]$. Let $\alpha \geq 0$ be the degree of $\widetilde{g}(X)$. From $F_{b,c,r}(X, \widetilde{g}(X)) \equiv 0$ we deduce that

   $$2^r + 1 + \alpha(2^r + 1) = \alpha + 1,$$

   a contradiction to $\alpha \geq 0$.

Thus $s \geq 2$. Arguing as above, we consider the coefficient of $Y^{2^r+1-\ell}$, $\ell \in [2\ldots s]$, in $G(X,Y)H(X,Y)$ and in $F_{b,c,r}(X,Y)$. Using induction, $h_0(X) \mid h_\ell(X)$, $\ell = 2,\ldots,s$. Also, the coefficient of $Y^{2^r+1-s-\ell}$, $\ell \in [1\ldots 2^r+1-2s]$, in $G(X,Y)H(X,Y)$ is

$$g_0(X)h_{s+\ell}(X) + g_1(X)h_{s+\ell-1}(X) + \cdots + g_s(X)h_\ell(X).$$

Since it vanishes, we obtain, again by induction, $h_0(X) \mid h_{s+\ell}(X)$, for $\ell \leq 2^r+1-2s$. Thus $h_0(X) \mid H(X,Y)$ and again we find a non-costant factor of $F_{b,c,r}$ of degree 0 in Y, a contradiction.

$\square$

Therefore, we get the following non-existence result.

Theorem 4.2. *Let $m \geq 2$ be an even integer. Then,*

1. *for any $b \in \mathbb{F}_{2^m}$, $c \in \mathbb{F}_{2^m}^*$ and $r < m/8 - 1$ the function $f_{b,c,r}$ is not APN;*

2. *for any $b \in \mathbb{F}_{2^m}^*$ and $r < m/2$ the function $f_{b,0,r}$ is not APN;*

Proof. Let $q = 2^{m/2}$. From Theorem 4.1 we get that the curve $\mathcal{D}_{b,c,r}$, defined over $\mathbb{F}_q$, is absolutely irreducible of order $d = 2^{r+1} + 2$. Now, applying the Hasse-Weil bound (Theorem 2.1), noting that the curve has two points at the infinity, we get that the number of $\mathbb{F}_q$-rational (affine) points of $\mathcal{D}_{b,c,r}$ are at least $q + 1 - (d-1)(d-2)\sqrt{q} - 2$. It is easy to see that if $r < \frac{m}{8} - 1$ we have $q + 1 - (d-1)(d-2)\sqrt{q} - 2 > 0$.

The second case comes from Theorem 3.3. $\square$

Remark 4.3. For the case $r = 1$, Theorem 4.2 implies that for $m \geq 18$ the function $f_{b,c,1}$ cannot be APN for any choice of $b,c \in \mathbb{F}_{2^m}$.

In [9], the authors show that for $m \leq 6$, we have instance of APN functions coming from Theorem 1.1 for $r = 1$. To check that $f_{b,c,1}$ cannot be APN for $8 \leq m \leq 16$ we need the following proposition which allows us to reduce the number of pairs (b,c).

Proposition 4.4. *Let $k \geq 0$ be an integer, and $u \in \mu_{q+1}$. Then, for any $b,c \in \mathbb{F}_{q^2}$ the equation*

$$\left(cx^{2^r+1} + bx^{2^r} + 1\right)^{q+1} + x^{q+1} = 0 \tag{4.1}$$

admits a solution over $\mathbb{F}_{q^2}$ if and only if

$$\left(c^{2^k}u^{2^k(2^r+1)}x^{2^r+1} + b^{2^k}u^{2^{k+r}}x^{2^r} + 1\right)^{q+1} + x^{q+1} = 0 \tag{4.2}$$

has a solution.

Proof. If we perform the change of variable $x \mapsto ux^{2^{-k}}$, then (4.1) becomes

$$\left(cu^{(2^r+1)}x^{2^{-k}(2^r+1)} + bu^{2^r}x^{2^{r-k}} + 1\right)^{q+1} + x^{2^{-k}(q+1)} = 0.$$

Now, raising it to the power of 2^k we get (4.2). $\square$

6

Remark 4.5. Proposition 4.4 permits to reduce the number of pairs $(b, c) \in \mathbb{F}_{q^2} \times \mathbb{F}_{q^2}^*$, and thus of polynomials $P_{c,b}(X)$, for checking the existence of an APN function as in Theorem 1.1. Indeed, let $b \in \mathbb{F}_{q^2}$, and let $B_b := \{b^{2^k} \cdot u^{2^{r+k}} : u \in \mu_{q+1}, 0 \leq k \leq m\}$. Then, Proposition 4.4 implies that if for any $c \in \mathbb{F}_{q^2}^*$ the polynomial $P_{c,b}(X)$ admits always a solution in $\mathbb{F}_{q^2}$, then for any $b' \in B_b$ we have that $P_{c,b'}(X)$ admits always a solution in $\mathbb{F}_{q^2}$ for any $c \in \mathbb{F}_{q^2}^*$.

Therefore, we can partition $\mathbb{F}_{q^2}$ in sets of type B_b and restrict the analysis to one representative for each set. For example, let $m = 16$, using Proposition 4.4 we reduce the analysis to $36 \cdot (2^{16} - 1)$ pairs instead of $2^{16} \cdot (2^{16} - 1)$.

By (1.1), the existence of a root of the polynomial

$$P_{c,b}(X) = \left(cX^{2^r+1} + bX^{2^r} + 1\right)^{q+1} + X^{q+1}$$

is equivalent to the existence of an element $u \in \mu_{q+1}$ such that the equation

$$cx^{2^r+1} + bx^{2^r} + ux + 1 = 0$$

admits a root in $\mathbb{F}_{q^2}$. This equation can be transformed into

$$x^{2^r+1} + x + A = 0, \tag{4.3}$$

where

$$A = \frac{(ub + c)c^{2^r-1}}{\left(uc^{2^r-1} + b^{2^r}\right)^{2^{-r}+1}},$$

under the assumption that $uc^{2^r-1} + b^{2^r} \neq 0$, see for instance [4]. In [7, Theorem 2.1] it has been proved that equation (4.3) admits no solution over $\mathbb{F}_{q^2}$ if and only if

$$A = \frac{a(a+1)^{2^r+2^{-r}}}{(a + a^{2^{-r}})^{2^r+1}}, \tag{4.4}$$

for some non-cube a. For the case $r = 1$, the previous request is equivalent to ask that

$$A = a + \frac{1}{a},$$

for some non-cube a. So, for $r = 1$, using MAGMA [6] it is possible to check that one can always find some $u \in \mu_{q+1}$ such that $uc + b^2 \neq 0$ and the associated value of A does *not* belong to the set

$$\left\{ a + \frac{1}{a} : a \text{ not a cube} \right\},$$

for any choice of $b, c \in \mathbb{F}_{2^m}$ and $8 \leq m \leq 16$. Therefore, the function $f_{b,c,1}$ cannot be APN. So, we get the following result.

Corollary 4.6. *Let $m \geq 8$ be an even integer. Then, for any choice $b, c \in \mathbb{F}_{2^m}$ the function $f_{b,c,1}$ as in Theorem 1.1 is not APN.*

Moreover, by a computer check we could verify that $f_{b,c,r}$ cannot be APN also for $8 \leq m \leq 22$, and $r < m/2$ with $\gcd(r, m) = 1$. In particular, for any $r < m/2$ and any choice of b, c, there exists $u \in \mu_{q+1}$ such that $uc^{2^r-1} + b^{2^r} \neq 0$ and (4.4) is *not* satisfied for any non-cube a. Therefore, we conjecture the following:

Conjecture 4.7. *Let $m \geq 8$ be an even integer. Then, for any choice $b, c \in \mathbb{F}_{2^m}$ and $r \leq m/2$, $\gcd(r, m) = 1$, the function $f_{b,c,r}$ as in Theorem 1.1 is not APN.*

5 Concluding remarks

In this work, using algebraic-geometric tools we proved that the bivariate construction of APN functions introduced in [9] cannot yield APN functions whenever $r < \frac{m}{8} - 1$. In particular, for the case $r = 1$, this implies that the function cannot be APN for $m \geq 18$. Moreover, by performing computations in MAGMA we established that for $m \geq 8$ there are no APN functions from this class when $r = 1$. These results naturally lead to the following conjecture:

$$\text{For } m \geq 8 \text{ and } r < \frac{m}{2}, \text{ no APN function arises from Theorem 1.1.}$$

Computationally this conjecture holds for $8 \leq m \leq 22$.

If true, this conjecture implies that the Calderini et al. construction does not generate an infinite family of APN functions, but only sporadic examples for $m \leq 6$, where APN functions of this type indeed exist, as shown in [9].

A possible way to investigate this conjecture could be trying to show that for any choice of parameters b, c, one can always find some $u \in \mu_{q+1}$ such that the associated value of A, as in (4.3), does *not* belong to the set

$$\left\{ \frac{a(a+1)^{2^r+2^{-r}}}{(a + a^{2^{-r}})^{2^r+1}} : a \text{ not a cube} \right\}.$$

An equivalent approach could be that of studying the permutation property of certain linearized polynomials. Indeed, projective polynomials are related to linearized polynomials. In particular, noting that x^{2^r-1} permutes $\mathbb{F}_{2^m}$ when $\gcd(r, m) = 1$, the polynomial $P_A(X) = X^{2^r+1} + X + A$ has no roots over $\mathbb{F}_{2^m}$ if and only if $L_A(X) = X^{2^{2r}} + X^{2^r} + AX$ is a permutation polynomial, since $P_A(X^{2^r-1})X = L_A(X)$.

Linearized polynomials of this form and their zeros have been studied in several works (see for instance [12, 21, 25]).

References

[1] Y. Aubry, G. McGuire and F. Rodier, A few more functions that are not APN infinitely often, finite fields theory and applications, *Contemporary Math.*, **518** (2010), 23–31.

[2] D. Bartoli, M. Calderini, O. Polverino and F. Zullo, On the infiniteness of a family of APN functions, *J. Algebra*, **598** (2022), 68–84.

[3] E. Biham and A. Shamir, Differential cryptanalysis of DES-like cryptosystems, *J. Cryptology*, **4** (1991), no. 1, 3–72.

[4] A. W. Bluher, On $x^{q+1} + ax + b$, *Finite Fields Appl.*, **10** (2004), no. 3, 285–305.

[5] A. W. Bluher, On existence of Budaghyan-Carlet APN hexanomials, *Finite Fields Appl.*, **24** (2013), 118–123.

[6] W. Bosma, J. Cannon, C. Playoust, The Magma algebra system. I. The user language. Computational algebra and number theory, *J. Symbolic Comput.*, **24** (1997), no. 3-4, 235–265.

[7] C. Bracken, C. H. Tan and Y. Tan, On a class of quadratic polynomials with no zeros and its application to APN functions, *Finite Fields Appl.*, **25** (2014), 26–36.

[8] L. Budaghyan and C. Carlet, Classes of quadratic APN trinomials and hexanomials and related structures, *IEEE Trans. Inform. Theory*, **54** (2008), no. 5, 2354–2357.

[9] M. Calderini, L. Budaghyan and C. Carlet, On known constructions of APN and AB functions and their relation to each other, *Rad Hrvat. Akad. Znan. Umjet. Mat. Znan.*, **25(546)** (2021), 79–105.

[10] M. Calderini, K. Li and I. Villa, Extending two families of bivariate APN functions, *Finite Fields Appl.*, **88** (2023), Paper No. 102190, 20 pp.

[11] C. Carlet, Relating three nonlinearity parameters of vectorial functions and building APN functions from bent functions, *Des. Codes Cryptogr.*, **59** (2011), no. 1-3, 89–109.

[12] J. H. Choe, On the solutions of $X^{q^2} + aX^q + bX = c$ over $\mathbb{F}_{2^n}$, *Cryptogr. Commun.*, **17** (2025), no. 4, 1125–1147.

[13] R. S. Coulter and M. Henderson, A class of functions and their application in constructing semi-biplanes and association schemes, *Discrete Math.*, **202** (1999), no. 1-3, 21–31.

[14] P. Dembowski and T. G. Ostrom, Planes of order n with collineation groups of order n^2, *Math. Z.*, **103** (1968), 239–258.

[15] U. Dempwolff and Y. Edel, Dimensional dual hyperovals and APN functions with translation groups, *J. Algebraic Combin.*, **39** (2014), no. 2, 457–496.

[16] W. Fulton, *Algebraic curves*, Advanced Book Classics, Addison-Wesley Publishing Company Advanced Book Program, Redwood City, CA, 1989.

[17] F. Göloğlu, Almost perfect nonlinear trinomials and hexanomials, *Finite Fields Appl.*, **33** (2015), 258–282.

[18] F. Göloğlu, Biprojective almost perfect nonlinear functions, *IEEE Trans. Inform. Theory*, **68** (2022), no. 7, 4750–4760.

[19] F. Göloğlu and L. Kölsch, Equivalences of biprojective almost perfect nonlinear functions, *Combinatorial Theory*, **5** (2025), no. 3.

[20] T. Helleseth and A. Kholosha, On the equation $x^{2^l+1} + x + a = 0$ over GF(2^k), *Finite Fields Appl.*, **14** (2008), no. 1, 159–176.

[21] T. Helleseth and A. Kholosha, $x^{2^l+1} + x + a$ and related affine polynomials over GF(2^k), *Cryptogr. Commun.*, **2** (2010), no. 1, 85–109.

[22] J. W. P. Hirschfeld, G. Korchmáros and F. Torres, *Algebraic Curves over a Finite Field*. Princeton Series in Applied Mathematics, Princeton. 2008.

[23] K. Li and N. S. Kaleyski, Two new infinite families of APN functions in trivariate form, *IEEE Trans. Inform. Theory*, **70** (2024), no. 2, 1436–1452.

[24] K. Li, Y. Zhou, C. Li and L. Qu, Two new families of quadratic APN functions, *IEEE Trans. Inform. Theory*, **68** (2022), no. 7, 4761–4769.

[25] G. M. McGuire and J. Sheekey, A characterization of the number of roots of linearized and projective polynomials in the field of coefficients, *Finite Fields Appl.*, **57** (2019), 68–91.

[26] H. Taniguchi, On some quadratic APN functions, *Des. Codes Cryptogr.*, **87** (2019), no. 9, 1973–1983.

[27] Y. Zhou and A. Pott, A new family of semifields with 2 parameters, *Adv. Math.*, **234** (2013), 43–60.