On Some Properties of Quadratic APN Functions of a Special Form

Irene Villa
Department of Informatics
University of Bergen
Bergen, Norway
Irene.Villa@uib.no

Abstract—In a recent paper [1], it is shown that functions of the form $L_1(x^n)+L_2(x^{n+1})$, where $L_1$ and $L_2$ are linear, are a good source for construction of new infinite families of APN functions. In the present work we study necessary and sufficient conditions for such functions to be APN.

I. INTRODUCTION

For given positive integers $n$ and $m$, a function $F$ from the finite field with $2^n$ elements to the finite field with $2^m$ elements is called a vectorial Boolean function or an $(n, m)$-function, and in the case when $m=1$ it is simply called a Boolean function. Boolean functions are among the most fundamental objects investigated in pure and applied mathematics and computer science. Boolean function theory is an important tool for solving problems of analysis and synthesis of discrete devices which transform and process information. The primary motivation for studying Boolean functions comes from cryptography. In modern society, exchange and storage of information in an efficient, reliable and secure manner is of fundamental importance. Cryptographic primitives are used to protect information against eavesdropping, unauthorized changes and other misuse. In the case of symmetric cryptography ciphers are designed by appropriate composition of nonlinear Boolean functions. For example, the security of block ciphers depends on S-boxes which are $(n, m)$-functions. For most of cryptographic attacks on block ciphers there are certain properties of functions which measure the resistance of the S-box to these attacks. The differential attack introduced by Biham and Shamir is one of the most efficient cryptanalysis tools for block ciphers. It is based on the study of how differences in an input can affect the resulting difference at the output. When $n = m$ the functions that contribute an optimal resistance against differential attack are called Almost Perfect Nonlinear (APN). Such APN function $F(x)$ are characterized by having at most two solutions for every equation $F(x+a) - F(x) = b$, where $a$ and $b$ are general elements of the field and $a$ is not null. The role of APN functions is not just related to cryptography. In coding theory APN functions define binary error correcting codes optimal in a certain sense. In projective geometry quadratic APN functions define dual hyperovals. Recent advances in APN functions have made a prominent impact on the theory of commutative semifields. For these reasons many works were focused on the studying and the construction of such optimal functions.

Let $n$ be a positive integer and $\mathbb{F}_{2^n}$ the finite field with $2^n$ elements. If $n$ is an even number, then we have that $3|(2^n - 1)$ and we denote with $k$ the integer value $2^n/3$.

A function $F$ from $\mathbb{F}_{2^n}$ to $\mathbb{F}_{2^m}$ admits a unique representation, called Univariate Polynomial Representation, over $\mathbb{F}_{2^m}$ of degree at most $2^m - 1$:

$$F(x) = \sum_{j=0}^{2^m-1} \delta_j x^j, \text{ with } \delta_j \in \mathbb{F}_{2^n}. $$

For every integer $j$ consider its binary expansion $\sum_{k=0}^{n-1} j_k 2^k$ and denote with $w_2(j)$ the number of nonzero coefficients (i.e. $\sum_{k=0}^{n-1} j_k$). The algebraic degree of the function $F$ is the max$_j w_2(j)$. Functions of algebraic degree 1 are called affine and of degree 2 quadratic. Linear functions are affine functions without the constant term and they can be represented as $L(x) = \sum_{j=0}^{n-1} j_k x^j$. A known example of a linear function defined over any dimension $n$ is the trace function $Tr(x) = Tr_2(x) = \sum_{j=0}^{n-1} x^{2^j}$. In particular the trace is a Boolean function, i.e. $Tr : \mathbb{F}_{2^n} \rightarrow \mathbb{F}_2$. For $m$ positive divisor of $n$ we use the notation $Tr^m(x) = \sum_{i=0}^{n/m-1} x^{2^{im}}$.

Given a function $F$ we define its $\lambda$-component as the Boolean function $f_\lambda : \mathbb{F}_{2^n} \rightarrow \mathbb{F}_2$ with $f_\lambda(x) = Tr(\lambda \cdot F(x))$, for $\lambda \in \mathbb{F}_{2^n}$. For a Boolean function $f$ we define the Walsh transformation as

$$\hat{f}_\lambda(u) = \sum_{x \in \mathbb{F}_{2^n}} (-1)^{f(x) + \lambda u(x)} $$

with $u \in \mathbb{F}_{2^n}$. With Walsh Spectrum we refer to the set of all possible values of the Walsh transformation. With the symbol $\mathcal{F}(f)$ we indicate the Walsh transformation valued in 0,

$$\mathcal{F}(f) = \sum_{x \in \mathbb{F}_{2^n}} (-1)^{f(x)} = 2^n - 2 \cdot \text{wt}(f),$$

where wt($f$) is the Hamming weight of $f$ (i.e. the cardinality of the set $\{x \in \mathbb{F}_{2^n} : f(x) = 1\}$). Therefore we have that a Boolean function $f$ is balanced (wt($f$) = $2^{n-1}$) if and only if $\mathcal{F}(f) = 0$. A Boolean function $f$ is called bent if its Walsh spectrum corresponds to the set $\{\pm 2^{n/2}\}$. Therefore such function can exist only for even values of $n$. Moreover, we have that $f$ is bent if and only if, for every $a \in \mathbb{F}_{2^n}$, the function $D_a f(x) = f(x+a) + f(x)$ is balanced.

For every nonzero element $a \in \mathbb{F}_{2^n}$ the derivative of $F$ in the direction of $a$ is the function $D_a F(x) = F(x+a) + F(x)$. The function $F$ is called almost perfect nonlinear (APN) if for every $a \neq 0$ and every $b$ in $\mathbb{F}_{2^n}$, the equation $D_a F(x) = b$ admits at most 2 solutions. Used as S-Boxes in block ciphers,
APN functions are useful since they oppose an optimal resistance against differential cryptanalysis.

The APN property is invariant under the action of some transformations of functions.

- Given $A_1, A_2$ affine permutations and $A$ an affine function, if $F$ is APN then also $G = A_1 \circ F \circ A_2 + A$ is APN; in this case the functions are called extended affine equivalent (EA-equivalent).

- Two functions $F$ and $G$ are CCZ-equivalent if there exists an affine permutation $L$ of $\mathbb{F}_2^n$, such that $L(G) = G$, where $G$ is the graph of the function $F$, with $(x, F(x)) : x \in \mathbb{F}_2^n$. Also CCZ-equivalence preserve the APN property. Moreover, we have that EA-equivalence is a particular case of CCZ-equivalence.

Many different works have been focused on finding and constructing new families of APN functions. Table I gives us all known values for exponents $d$ such that the function $x^d$, defined over $\mathbb{F}_2^n$, is APN.

Since EA-equivalence preserves the algebraic degree of a function and, in general, the functions listed in Table I have different algebraic degrees, it is easy to verify that these APN functions are EA-inequivalent. Instead the algebraic degree is not an invariant for CCZ-equivalence. But also for this case it was possible to prove some inequalities. In [10] it is shown that two different Gold functions $x^{2^i+1}$ and $x^{2^j+1}$, where $1 \leq i < j \leq n/2$, are CCZ-invariant and that in general the Gold functions are CCZ-invariant to the Welch and to any Kasami functions. Moreover, the inverse and Dobbertin functions are not CCZ-equivalent to each other and to all other known APN power functions, [10]. For all the other cases the problem is still open.

Before the work in [11] the only known APN functions were EA-equivalent to power functions and it was supposed that all APN functions are EA-equivalent to power functions. In [11] it is showed the existence of classes of APN mappings EA-inequivalent to power functions. Such functions were constructed by applying CCZ-equivalence to the Gold APN mappings. In [12] we can find the first examples of APN function CCZ-invariant to power functions. The first infinite families of such APN polynomial can be found in [11]. In Table II these functions are listed. They are all quadratic functions.

In this work we focus on functions of the form

$$F'(x) = F(x^3) = L_1(x^3) + L_2(x^9),$$

where $L_1$ and $L_2$ are linear functions. From now on, we will refer to $L_1$ and $L_2$ as to the linear functions

$$L_1(x) = \sum_{i=0}^{n-1} b_ix^{2^i} \quad \text{and} \quad L_2(x) = \sum_{i=0}^{n-1} c_ix^{2^i},$$

with $b_i, c_i \in \mathbb{F}_2^n$. In particular we want to study conditions on $L_1$ and $L_2$ such that $F'$ is APN.

Some results are already been given in different papers. In [15] the function $x^3 + Tr(x^9)$ is proved to be APN for any dimension $n$. Moreover, for $n \geq 7$ it is proved to be CCZ-invariant to the Gold functions, to the inverse and Dobbertin functions and EA-invariant to power functions. For a quadratic APN function $F : \mathbb{F}_2^n \to \mathbb{F}_2^n$ and a quadratic boolean function $f : \mathbb{F}_2^n \to \mathbb{F}_2^n$, under some conditions it is proved that the function $F(x) + f(x)$ is APN. In particular these conditions are that for every nonzero $a \in \mathbb{F}_2^n$ there must exist a linear Boolean function $l_a$ satisfying:

1. $\varphi_F(x, a) = l_a(\varphi_F(x, a))$,
2. if $\varphi_F(x, a) = 1$ for some $x \in \mathbb{F}_2^n$, then $l_a(1) = 0$,

where $\varphi_F(x, a) = \chi_F(x) + \chi(x + a) + \chi(a) + \chi(0)$. A similar theorem is proved when $f : \mathbb{F}_2^n \to \mathbb{F}_2^n$, where $m$ is a divisor of $n$. Due to this result the following functions, defined over $\mathbb{F}_2^{2m}$ where $m$ is an even positive integer, are APN:

- $x^3 + Tr_{n/m}(x^{m^2+2}) = x^3 + x^{2m^2+2} + x^{m^2+1}$,
- $x^3 + (Tr_{n/m}(x^{m^2+2}))^3$.

When $F$ is a Gold function, all possible APN mappings $F(x) + f(x)$, where $f$ is a Boolean function, are computed until dimension 15. The only possibilities, different from $x^3 + Tr(x^3)$, are for $n = 5$ the function $x^3 + Tr(x^3)$ (CCZ-equivalent to Gold functions) and for $n = 8$ the function $x^3 + Tr(x^3)$ (CCZ-invariant to power functions and to $x^3 + Tr(x^9)$).

In [1] the function $x^3 + Tr(x^9)$ has been generalized to form (1). It has been proved that for $n$ even a sufficient condition is $L_1(x) + L_2(x^3)$ being a permutation over $\mathbb{F}_2^n$. In the odd dimension a weaker conditions lead to an APN mapping. Moreover from the fact that by applying a linear function $l(x) = ax + b$, with $a \in \mathbb{F}_2^n$ and $b \in \mathbb{F}_2^n$, to a permutation we obtain another one, a simply but useful statement has been proved. In particular it is stated that for $n$ even, $L$ a linear function over $\mathbb{F}_2^n$, $a \in \mathbb{F}_2^n$, and $b \in \mathbb{F}_2^n$ if $x + L(x^3)$ is a permutation over $\mathbb{F}_2^n$, then the function

$$ax^3 + L(a^9x^9 + a^{i^2}b^0 + ab^2x^4)$$

is APN over $\mathbb{F}_2^n$.

The statement just mentioned gives new examples of APN functions in even dimensions. The following infinite families of function are proved to be APN also in odd dimensions:

1. $x^3 + a^{-1}Tr_a(x^{a^3})$, with $a \in \mathbb{F}_2^n$ and any positive $n$,
2. $x^3 + a^{-1}Tr_3(a^{i^2}x^{i^2} + a^{12}x^{16})$, with $a \in \mathbb{F}_2^n$ and $n$ divisible by 3,
3. $x^3 + a^{-1}Tr_3(a^{2}x^{9} + a^{6}x^{18})$, with $a \in \mathbb{F}_2^n$ and $n$ divisible by 3.

| Functions | Exponents $d$ | Conditions | Degree | Proven |
|-----------|--------------|------------|--------|--------|
| Golden    | $2^i + 1$   | gcd(i, n)/4 | 2      | [2], [3] |
| Kasami    | $2^{2i} - 2^i + 1$ | gcd(i, n)/4 | $i+1$  | [4], [5] |
| Welch     | $2^{2i} + 3$ | $n = 2^i + 1$ | 3      | [6]    |
| Niho      | $2^i + 2^{i+1}/2 - 1$, $t$ even | $n = 2^i + 1$ | $(t + 2)/2$ | $t+1$ | [7] |
| Reverse   | $2^{2i - 1}$ | $n = 2^i + 1$ | $n - 1$ | [8], [9] |
| Dobbertin | $2^{2i} + 2^{2i}/2 - 2i - 1$ | $n = 5i$ | $i + 3$ | [9] |
In [1] some conditions for constructing permutations, and consequently for constructing APN functions, are given.

- For a general positive \( n \) and a linear function \( L \) over \( \mathbb{F}_{2^n} \) if for every \( u \in \mathbb{F}_{2^n} \) such that \( L(u) \neq 0 \), the condition
  \[
  Tr_n \left( \frac{a}{(L(u))^3} \right) = \begin{cases} 
  0 & \text{if } n \text{ is odd} \\
  1 & \text{if } n \text{ is even}
  \end{cases}
  \]
  is satisfied, then the function \( x + L(x^3) \) is a permutation.

- For \( n \) even integer and \( L \) a linear function over \( \mathbb{F}_{2^n} \) the function \( x + L(x^3) \) is a permutation of \( \mathbb{F}_{2^n} \) if and only if for every \( b \in \mathbb{F}_{2^n} \), such that \( L^*(b) \neq 0 \) there exists an element \( \gamma \in \mathbb{F}_{2^n} \) such that \( L^*(b) = \gamma^3 \) and \( Tr_n(\gamma^{-1}b) \neq 0 \), where \( L^* \) denotes the adjoint linear mapping of \( L \).

- For \( n \) odd integer and \( L \) a linear function over \( \mathbb{F}_{2^n} \) the function \( x + L(x^3) \) is a permutation of \( \mathbb{F}_{2^n} \) if and only if for every \( b \in \mathbb{F}_{2^n} \), either \( L^*(b) = 0 \) or \( Tr_n(\gamma^{-1}b) = 0 \), where \( L^* \) denotes the adjoint linear mapping of \( L \).

The above mentioned function \( x^9 + Tr(x^3) \), for \( n = 8 \), is a clear example of the fact that there are other possible conditions for function of the form (1) to be APN. Therefore with this work we try to find new conditions and new relations for the APN property.

II. APN CONDITIONS

A. Necessary and sufficient conditions

Let \( F(x) = L_1(x) + L_2(x^3) \), with \( L_1 \) and \( L_2 \) as in (2), be a function defined over \( \mathbb{F}_{2^n} \) for a positive integer \( n \) and \( F'(x) = F(x^3) = L_1(x^3) + L_2(x^9) \).

Just analysing the APN property for a quadratic function we can state the following lemma.

Lemma 1. For any positive integer \( n \) and any linear functions \( L_1 \) and \( L_2 \) of \( \mathbb{F}_{2^n} \), a function \( F' \) defined by (1) is APN if and only if for every \( a \in \mathbb{F}_{2^n} \) one of the following conditions is satisfied:

1) \( x \neq 0, 1 \)
   \[
   L_1(a^3(x^2 + x)) + L_2(a^9(x^8 + x)) \neq 0;
   \]

2) \( y \neq 0 \) and \( Tr(y) = 0 \)
   \[
   L_1(a^3y) + L_2(a^9(y^4 + y^2 + y)) \neq 0.
   \]

Proof: Since \( F' \) is a quadratic function satisfying \( F'(0) = 0 \), APN condition can be reformulated as the following: for any \( a \in \mathbb{F}_{2^n} \)

\[
F'(ax + a) + F'(ax) + F'(a) = 0
\]
if and only if \( x \in \{0, 1\} \).

The equation above is equivalent to \( L_1(a^3(x^2 + x)) + L_2(a^9(x^8 + x)) = 0 \), therefore we have that

\[
L_1(a^3(x^2 + x)) + L_2(a^9(x^8 + x)) \neq 0
\]
if and only if \( x \neq 0, 1 \). Lets denote now \( y = x^2 + x \). Since \( x \neq 0, 1 \) we have that
\( y \neq 0 \) and \( Tr(y) = 0 \). The second condition follows easily.

Proposition 1. Let \( F' \) be APN and, referring to (2), construct the linear function \( L_3(x) = \sum_{i=0}^{n-1} d_i x^i \) with coefficients

\[
d_0 = b_0 + b_{n-1} + c_0 + c_{n-3} \\
d_1 = b_1 + b_0 + c_1 + c_{n-2} \\
d_2 = b_2 + b_1 + c_2 + c_{n-1} \\
d_i = b_i + b_{i-1} + c_i + c_{n-3}, \text{ for } 3 \leq i \leq n - 1.
\]

Then \( L_3 \) is a 2-to-1 map satisfying \( L_3(x) = 0 \) if and only if \( x = 0, 1 \).
Using equation (4) with \( a = 1 \), consider the following map: \( L_1(x^2 + x) + L_2(x^6 + x) \). Analysing the two linear functions we have: 
\[
L_1(x^2 + x) = (b_0 + b_{n-1})x + \sum_{i=0}^{n-1} (b_i + b_{i-1})x^i,
\]
\[
L_2(x^6 + x) = (c_0 + c_{n-3})x + (c_1 + c_{n-2})x^2 + (c_2 + c_{n-1})x^3 + \sum_{i=3}^{n-3} (c_i + c_{i-3})x^i.
\]
Therefore \( L_1(x^2 + x) + L_2(x^6 + x) \) corresponds to the linear function \( L_3(x) \) described above. From Lemma 1 we have that \( L_3(x) = 0 \) if and only if \( x = 0, 1 \).

The following lemma gives a quite fast way to verify if a function \( F' \) can be APN, since you have to evaluate it over a third of the elements of the space.

**Lemma 2.** For \( n \) even assume \( F' \) is APN. Let \( a \in \mathbb{F}_2^n \) be a primitive element and \( k = 2^{n-1} \). Then \( F'(a) \neq 0 \) for any \( a \neq 0 \) or equivalently \( F(a^3) = F'(a) \neq 0 \) for \( 0 \leq j \leq k - 1 \).

**Proof:** For \( n \) even we have \( Tr(t) = 0 \). Therefore using equation (5) with \( y = 1 \) we get for any \( a \neq 0 \)
\[
L_1(a^3) + L_2(a^9) = F(a^3) = F'(a) \neq 0.
\]
For \( a 
eq 0 \) we have that \( a = a^j \) with \( 0 \leq j \leq 2^n - 2 \). Since we consider just cubic power of \( a \), we can restrict the possibilities to \( 0 \leq j \leq k - 1 \). This concludes the proof.

**Remark 1.** If we consider \( j = 0 \) in Lemma 2 then
\[
L_1(1) + L_2(1) = \sum_{i=0}^{n-1} b_i + \sum_{i=0}^{n-1} c_i = \sum_{i=0}^{n-1} (b_i + c_i) \neq 0.
\]
Moreover, if we just consider linear functions defined over \( \mathbb{F}_2 \) (i.e. \( b_i, c_i \in \mathbb{F}_2 \)) then a fast way to check if \( F' \) is not APN is by verifying that \( L_1 \) and \( L_2 \) have the same parity number of monomials.

**Lemma 3.** Let \( n \) be an even number multiple of 3 and \( F' \) be APN. Then for any \( a \neq 0 \) \( L_1(a^3 \beta) \neq 0 \), with \( \beta \in \mathbb{F}_2^3 \) such that \( Tr_3(\beta) = 0 \).

**Proof:** Consider such an element \( \beta \) and call \( m \) the integer \( \frac{n}{3} \). We have that \( Tr_3(\beta) \) is equal to \( \sum_{j=0}^{m-1} \sum_{i=0}^{2^2} \beta = \sum_{j=0}^{m-1} Tr_3(\beta) = 0 \). Therefore we can apply (5) with \( y = \beta \) and obtain
\[
L_1(a^3 \beta) + L_2(a^9 (\beta^3 + \beta^2 + \beta)) = L_1(a^3 \beta) \neq 0 \forall a \neq 0.
\]

**Lemma 4.** Consider a function \( F' \) from \( \mathbb{F}_{2^n} \) to itself defined as in (1). \( F' \) is APN if and only if it satisfies the following condition:
\[
\text{for every } a, y \neq 0 \text{ with } Tr(y) = 0 \text{ if an element } t \in \mathbb{F}_{2^n} \text{ satisfies } Tr(t) = 0 \text{ and}
\]
\[
L_1(a^3 y) = L_2(a^9 y^3 t)
\]
\[
\text{then } L_2(a^9 (y^4 + ty^3 + y^2 + y)) \neq 0.
\]

**Proof:** By Lemma 1 we have that APN property for \( F' \) is equivalent to
\[
\text{for any } a, y \in \mathbb{F}_{2^n}, Tr(y) = 0 \ L_1(a^3 y) + L_2(a^9 (y^4 + y^2 + y)) \neq 0.
\]
Assuming that there exists an element \( t \) that satisfies the conditions in the statement. Let us re-write the formula above as
\[
0 \neq L_1(a^3 y) + L_2(a^9 (y^4 + y^2 + y))) = L_1(a^3 y) + L_2(a^9 (y^4 + t y^3 + y^2 + y)) = L_2(a^9 (y^4 + t y^3 + y^2 + y)).
\]
Therefore the APN condition is equivalent to
\[
L_2(a^9 (y^4 + t y^3 + y^2 + y)) \neq 0.
\]

On the other hand assume that for any \( t \) of null trace we have \( L_1(a^3 y) \neq L_2(a^9 y^3 t) \).

Let us consider the second term of the formula,
\[
L_2(a^9 (y^4 + y^2 + y)) = L_2(a^9 (y + 1/y + 1/y^2)).
\]
Since \( Tr(y + 1/y + 1/y^2) = 0 \), the term belongs to the set \( \Omega \). Therefore the relation is again respected.

**Corollary 1.** For general \( a \neq 0 \) and \( y \neq 0 \) with \( Tr(y) = 0 \), if the equation
\[
L_1(a^3 y) = L_2(a^9 y^3 t)
\]
is satisfied only for \( t \) with \( Tr(t) = 1 \), then the function \( F'(x) = F(x^3) = L_1(x^3) + L_2(x^9) \) is APN.

**Proof:** In this case the hypothesis of the previous lemma is always satisfied, since there is no element \( t \) such that \( L_1(a^3 y) = L_2(a^9 y^3 t) \) and \( Tr(t) = 0 \). Therefore the function \( F' \) is APN.

**B. On APN functions of the form \( x^9 + L(x^3) \)**

From [15] we know that in \( \mathbb{F}_{2^n} \) the function \( F'(x) = x^9 + Tr(x^3) \) is APN.

**Lemma 5.** If \( 3 | n \) then the function \( x^9 + Tr(x^3) \) is not APN over \( \mathbb{F}_{2^n} \).

**Proof:** From Lemma 1 we have that \( x^9 + Tr(x^3) \) is APN if and only if for any \( a \neq 0 \) and any \( x \neq 1 \)
\[
Tr(a^3 (x^2 + x)) + a^9 (x^8 + x) \neq 0.
\]
If we now consider \( n \) multiple of 3, \( x \in \mathbb{F}_{2^n} \setminus \mathbb{F}_2 \) and \( a = 1 \) we obtain
\[
Tr(a^3 (x^2 + x)) + a^9 (x^8 + x) = 0.
\]

Using Lemma 4 it was possible to implement, using the software MAGMA, a fast algorithm that checks if \( x^9 + Tr(x^3) \) is APN over \( \mathbb{F}_{2^n} \). Running the code for \( n \) up to 200 the only APN functions are for dimensions 4, 5 and 8.

Let us consider now a more general form for \( F' \), \( G(x) = x^a + L(x^3) \) with \( L \) linear function in \( \mathbb{F}_{2^n} [x] \).

With some computational work, done with MAGMA, we tried to find more APN functions of this form in other dimensions. In Table III we summarize the results we obtained. With \( \alpha \) we indicate a primitive element of \( \mathbb{F}_{2^n} \). We searched for APN functions in \( \mathbb{F}_{2^n} \), up to \( n = 10 \), of the form \( x^9 + L(x^3) \). We studied their CCZ-equivalence relation and obtained the representatives for each dimension. Obviously for every \( n \) not
TABLE III. APN functions of the form $x^9 + L(x^3)$ over $\mathbb{F}_{2^n}$

| $n$ | CCZ-eq | Representatives |
|-----|--------|-----------------|
| 4   | 1      | $L = 0$         |
| 5   | 2      | $L = 0, L = \text{Tr}$ |
| 6   | 2      | $L = \alpha^{23}x + \alpha x^2$, $L = \alpha^{37}x + x^2$ |
| 7   | 1      | $L = 0$         |
| 8   | 4      | $L = 0, L = x^2 + x^2$ , $L = x^{23} + x^{27}, L = \text{Tr}$ |
| 9   | 0      | $L = 0$         |
| 10  | 2      | $L = \alpha^{1022}x + \alpha^{1022}x^2 + \alpha x^2$ |

multiple of 3, the Gold function $x^9$ (corresponding to the case $L(x) = 0$) is APN.

For greater dimensions we just checked the possible APN function of the form $x^9 + L(x^3)$ with $L \in \mathbb{F}_2[x]$, up to CCZ-equivalence.

- for $n = 11$ there are no APN except $F(x) = x^9$;
- for $n = 12$ there are no APN;
- for $n = 13$ there are no APN except $F(x) = x^9$;
- for $n = 14$ there are no APN except $F(x) = x^9$;
- for $n = 15$ there are no APN;
- for $n = 16$ there are no APN except $F(x) = x^9$.

For $n = 4$ the function $x^9 + \text{Tr}(x^3)$ is CCZ-equivalent to the Gold function $x^9$.

For $n = 6$ the found APN functions are not CCZ-equivalent to functions $x^9 + L(x^3)$ defined over $\mathbb{F}_2$. Moreover we get:

- for $L(x) = \alpha^{33}x + \alpha x^2$ the function $x^9 + L(x^3)$ is CCZ-equivalent to $x^3 + x^9 + \text{Tr}(x^3)$;
- for $L(x) = \alpha^{23}x + x^2$ the function $x^9 + L(x^3)$ is CCZ-equivalent to $x^3 + \alpha^{-1} \text{Tr}(\alpha^3x^9)$.

Both of these functions belong to the class of APN functions studied in [1]

For $n = 8$ we compared the found APN mappings with the list of known APN function in dimension 8 in [18]. We get the following:

- for $L(x) = x^2 + x^4$ the function $x^9 + L(x^3)$ is CCZ-equivalent to $x^3 + \text{Tr}(x^9)$;
- for $L(x) = x^2 + x^4$ the function $x^9 + L(x^3)$ is CCZ-equivalent to $x^3$;
- for $L(x) = x^2 + \alpha^{85}x^3 + x^2$ the function $x^9 + L(x^3)$ is not CCZ-equivalent to any function of the form $x^3 + a^{-1} \text{Tr}(\alpha x^3)$ but is CCZ-equivalent to function $\alpha^{35}x^{144} + \alpha^{120}x^{66} + \alpha^{60}x^{18} + x^3$, no. 6 in the list of APN mapping of $\mathbb{F}_{2^9}$ in [18].

C. On the number of bent components

From [19] we get the following theorem.

**Theorem 1.** Let $F$ be a function from $\mathbb{F}_{2^n}$ to $\mathbb{F}_{2^n}$. Then for any non-zero $a \in \mathbb{F}_{2^n}$

$$
\sum_{\lambda \in \mathbb{F}_{2^n}} F^2(D_a f_\lambda) \geq 2^{2n+1}.
$$

Moreover, $F$ is APN if and only if for every non-zero $a \in \mathbb{F}_{2^n}$

$$
\sum_{\lambda \in \mathbb{F}_{2^n}} F^2(D_a f_\lambda) = 2^{2n+1}.
$$

**Lemma 6.** $F_1(x) = L_1(x^3) + L_2(x^9)$ is an APN function if and only if for any $a \in \mathbb{F}_{2^n}$ there exists one and only one $\lambda \in \mathbb{F}_{2^n}$, such that $\text{Tr}(\lambda L_1(\lambda x^3 + \alpha^3x) + \lambda L_2(\lambda x^8 + \alpha^8x))$ is constantly 0.

**Proof:** Since $F_1$ is a quadratic function, every component has at most algebraic degree 2 and, consequently, the Boolean function $D_a f_1(\lambda)$ can be either affine or constant. If $D_a f_1(\lambda)$ is affine then $F(D_a f_1(\lambda)) = 0$. In the other case we have $F(D_a f_1(\lambda)) = \pm 2^n$ and $F^2(D_a f_1(\lambda)) = 2^{2n}$. Let consider the set

$$
\Delta_a = \{ \lambda \in \mathbb{F}_{2^n} : D_a f_1(\lambda) \text{ is constant} \},
$$

then

$$
\sum_{\lambda \in \mathbb{F}_{2^n}} F^2(D_a f_1(\lambda)) = 2^{2n} \cdot |\Delta_a|,
$$

From the previous theorem we have that $F_1$ is APN if and only if the sum is equal to $2^{2n+1}$, hence if and only if $|\Delta_a| = 2$. Since $f_0$, and consequently $D_a f_1$, is the constantly null function, we have that $0$ belongs to the set $\Delta_a$ for every $a \neq 0$. Therefore, $F_1$ is APN if and only if $|\Delta_a| = 1$, with

$$
\Delta_a = \Delta_a \setminus \{0\}.
$$

This is true for every generic quadratic APN function $F(x)$.

In our specific case we have

$$
D_a f_1(x) = \text{Tr}(\lambda (F'(x) + F' (x + a))) = \text{Tr}(\lambda [L_1(ax^3 + a^2x + a^3) + L_2(ax^8 + a^8x)] + \text{Tr}(\lambda L_1(\lambda x^3 + \alpha x^2) + L_2(ax^8 + a^8x)] + \text{Tr}(\lambda L_1(ax^3 + a^2x) + L_2(ax^8 + a^8x))).
$$

In order to study its constant conditions it is sufficient to study the function $g(x) = \text{Tr}(\lambda L_1(ax^3 + a^2x + a^3x) + L_2(ax^8 + a^8x))$. Since $g(0) = 0$, we have that if $g$ is constant then it is the constant zero function and this concludes the proof.

**Remark 2.** Equivalently, we can study the conditions for $\text{Tr}(\lambda L_1(ax^3 + a^2x) + L_2(ax^8 + a^8x))$ to be the constant null function. Due to the property of the Trace function we can study the conditions for $\lambda L_1(ax^3 + a^2x) + L_2(ax^8 + a^8x))$ to be equal to $\eta + \eta^2$, with $\eta = \eta(a, \lambda, x)$.

Recalling the notation used in the proof we defined:

$$
\Delta_\lambda \text{ as in (6) and } \Delta_\lambda^* \text{ as in (7)};
$$

$$
V_\lambda = \{ a \in \mathbb{F}_{2^n} : D_a f_1(\lambda) \text{ is constant} \};
$$

$$
V_\lambda^* = V_\lambda \setminus \{0\}.
$$

From Proposition 1 in [20] we get that the dimension of the kernel of $f_3$ and $n$ have the same parity, where the kernel
of a quadratic form \( f \) is the subspace of \( \mathbb{F}_{2^n} \)
\( \{ u \in \mathbb{F}_{2^n} : f(u + v) + f(u) + f(v) = 0 \text{ for any } v \in \mathbb{F}_{2^n} \} \).
From Lemma 1 in [20] we get that, since \( f_\lambda \) is a quadratic
Boolean function, its kernel corresponds to the subspace \( V_\lambda \).
Therefore we have \( \dim_{\mathbb{F}_2}(V_\lambda) \equiv n \mod 2 \).

Moreover let’s consider the set
\( \Gamma_i = \{ \lambda \neq 0 : \dim(V_\lambda) = i \} \).
If \( \Gamma_i \) not empty then \( i \) has the same parity as \( n \). It can be
easily proved by considering a not null element \( \lambda \) in the set, i.e.
such that \( \dim V_\lambda = i \). Since the dimension of \( V_\lambda \) has the
same parity as \( n \), the same can be state on \( i \).
The set \( \Gamma_i \) correspond to the set of all bent components.

**Corollary 2.** From Lemma 6 it is straightforward to prove
that APN property for a quadratic function is equivalent to the
following statement: for any \( \lambda_1 \neq \lambda_2 \in \mathbb{F}_{2^n}^* 
V_{\lambda_1} \cap V_{\lambda_2} = \emptyset \) and \( \sum_{\lambda \neq 0} |V_\lambda| = 2^n - 1 \).

1) **Computational Results:** Using the software MAGMA
we tried to verify for functions \( F' \) of form (1) defined over
small dimensions the relation between the APN property and
the number of bent components. From the results obtained
taking random linear functions \( L_1, L_2 \) and constructing \( F' \)
for \( n \in \{4, 6, 8 \} \) the relation seems the following one:

**Conjecture 1.** For an even \( n \), a function \( F' \) of the form (1) is
APN if and only if it has exactly \( \frac{1}{2}(2^n - 1) \) bent components.

We know that this is not true for general quadratic functions.
Indeed consider the quadratic APN function presented by
Dillon in 2006 [21]
\[
F(x) = x^3 + u^{11}x^5 + u^{13}x^9 + x^{17} + u^{11}x^{13} + x^{48} ;
\]
defined over \( \mathbb{F}_{2^9} \) where \( u \) is a primitive element, root of the
polynomial \( x^9 + x^4 + x^3 + x + 1 \). This function has 46 bent
components and 46 > \( \frac{1}{2}(2^6 - 1) = 42 \).

**III. CONCLUSION**

In this work we continued the study of quadratic functions of
the form \( L_1(x^2) + L_2(x^3) \) and related APN conditions. New
necessary and sufficient conditions are presented in this paper.
Such conditions allow us to compute a faster algorithm that
checks the existence of other APN functions of such form.
New results are given considering functions of the form \( x^9 + L(x^3) \).
Up to CCZ-equivalence new APN functions are found in
different low dimensions.

**REFERENCES**

[1] L. Budaghyan, C. Carlet, and G. Leander, “On a construction of
quadratic APN functions”, Proceedings of IEEE Information Theory
workshop ITW’09, Oct. 2009, pp. 374-378.

[2] R. Gold, “Maximal recursive sequences with 3-valued recursive
correlation functions”, IEEE Trans. Inform. Theory, 14, 1968, pp. 154-
156.

[3] K. Nyberg, “Differentially uniform mappings for cryptography”,
Advances in Cryptography, EUROCRYPT’93, Lecture Notes in Computer
Science 765, 1994, pp. 55-64.

[4] H. Janwa, and R. Wilson, “Hyperplane sections of Fermat varieties in
\( P^3 \) in char. 2 and some applications to code codes”, Proceedings of
AAECC-10, LNCS, vol. 673, Berlin, Springer-Verlag, 1993, pp. 180-
194.

[5] T. Kasami , “The weight enumerators for several classes of subcodes
of the second order binary Reed-Muller codes”, Inform. and Control,
18, 1971, pp. 369-394.

[6] H. Dobbertin, “Almost perfect nonlinear power functions over \( GF(2^n) \): the
Welch case”, IEEE Trans. Inform. Theory, 45, 1999, pp. 1271-1275.

[7] H. Dobbertin, “Almost perfect nonlinear power functions over \( GF(2^n) \):
the Niho case”, Inform. and Comput., 151, 1999, pp. 57-72.

[8] T. Beth, and C. Ding, “On almost perfect nonlinear permutations”,
Advances in Cryptology-EUROCRYPT’93, Lecture Notes in Computer
Science, 765, Springer-Verlag, New York, 1993, pp. 65-76.

[9] H. Dobbertin, “Almost perfect nonlinear power functions over \( GF(2^n) \):
a new case for \( n \) divisible by 5”, Proceedings of Finite Fields and
Applications FQ5, 2000, pp. 113-121.

[10] L. Budaghyan, C. Carlet, and G. Leander, “On inequivalence between
known power APN functions”, Proceedings of the International Work-
shop on Boolean Functions: Cryptography and Applications, BFCA
2008, Copenhagen, Denmark, May 2008.

[11] L. Budaghyan, Carlet, and A. Pott, “New Classes of Almost Bent
and Almost Perfect Nonlinear Functions”, IEEE Trans. Inform. Theory,
vol.52, no. 3, Mar. 2006, pp. 1141-1152.

[12] Y. Edel, G. Kyureghyan, and A. Pott, “A new APN function which is
not equivalent to a power mapping”, IEEE Trans. Inform. Theory, vol.
52, no. 2, Feb. 2006, pp. 744-747.

[13] L. Budaghyan, Carlet, and G. Leander, “Two classes of quadratic
APN binomials inequivalent to power functions”, IEEE Trans. Inform.
Theory, 54(9), 2008, pp. 4218-4229.

[14] L. Budaghyan, and C. Carlet, “Classes of Quadratic APN Trinomials
and Hexanomials and Related Structures”, IEEE Trans. Inform. Theory,
vol.54, no. 5, May 2008, pp. 2354-2357.

[15] L. Budaghyan, C. Carlet, and G. Leander, “Constructing new APN
functions from known ones”, Finite Fields and Their Applications,
vol.15, issue 2, Apr. 2009, pp. 150-159.

[16] C. Bracken, E. Byrne, N. Markin, and G. McGuire, “New families of
quadratic almost perfect nonlinear trinomials and multinomials”, Finite
Fields and Their Applications, 14(3), 2008, pp. 703-714.

[17] C. Bracken, E. Byrne, N. Markin, and G. McGuire, “A Few More
Quadratic APN Functions”, Cryptography and Communications, 3(1),
2011, pp. 43-53.

[18] Y. Edel, and A. Pott, “A new almost perfect nonlinear function which
is not quadratic”, IACR Cryptology ePrint Archive 2008, 2008, pp. 313.

[19] T.P. Berger, A. Canteau, P. Charpin, and Y. Lang-Chapuy, “On Almost
Perfect Nonlinear Functions Over \( F_{2^n} \) “, IEEE Trans. Inform. Theory,
Vol. 52, N. 9, Sep. 2006, pp. 4160-4170.

[20] A. Canteau, P. Charpin, and G. M. Kyureghyan, “A new class of
monomial bent functions”, Finite Fields and Their Applications, vol.14,
issue 1, Jan. 2008, pp. 221-241.

[21] J. F. Dillon, “APN Polynomials and Related Codes”, Polynomials over
Finite Fields and Applications, Banff International Research Station, Nov.
2006.