Cubic Maiorana-McFarland bent functions with no affine derivative

Bimal Mandal[1], Sugata Gangopadhyay[2] and Pantelimon Stănică[3]
[1]Department of Mathematics
[2]Department of Computer Science and Engineering
Indian Institute of Technology Roorkee, Roorkee 247667 INDIA
[3]Department of Applied Mathematics
Naval Postgraduate School, Monterey, CA 93943–5216, USA
{bimalmandal90, gsugata}@gmail.com, pstanica@nps.edu

January 21, 2017

Abstract

A class of cubic Maiorana-McFarland ($\mathcal{M}$) bent functions having no affine derivative was constructed by Canteaut and Charpin [2], thereby solving an open problem posed by Hou [12]. The goal of the paper is two-fold: we construct two classes of cubic $\mathcal{M}$ bent functions with no affine derivative and show their mutual affine inequivalence.

1 Introduction

Let $\mathbb{Z}$ be the ring of integers, $\mathbb{F}_{2^n}$ be the extension field of degree n over $\mathbb{F}_2$, the prime field of characteristic 2, $\mathbb{F}_{2^n}^* = \mathbb{F}_{2^n} \setminus \{0\}$, and for $m, t \in \mathbb{Z}^+$ (positive integers), let $\mathbb{F}_{2^t}^m = \{(x_1, x_2, \ldots, x_m) : x_i \in \mathbb{F}_{2^t}, 1 \leq i \leq m\}$ be the vector space of dimension m over $\mathbb{F}_{2^t}$. It is customary for the extension field $\mathbb{F}_{2^{mt}}$ to be identified with $\mathbb{F}_{2^t}^m$ as $\mathbb{F}_{2^t}$-vector spaces and used, interchangeably, where the context allows it. A function from $\mathbb{F}_{2^n}$ to $\mathbb{F}_2$ is said to be a *Boolean function* in n variables. The set of all Boolean functions in n variables is denoted by $\mathcal{B}_n$. The univariate representation of any function $f \in \mathcal{B}_n$ is

$$f(x) = \sum_{j \in \Gamma(n)} \mathrm{Tr}_1^{n_j}(\alpha_j x^j) + \varepsilon(1 + x^{2^n-1}), \tag{1}$$

where $\Gamma(n)$ is the set of cyclotomic coset leaders modulo $2^n - 1$, n_j is the size of the cyclotomic class containing j, $\alpha_j \in \mathbb{F}_{2^{n_j}}$, $\varepsilon = \sum_{x \in \mathbb{F}_{2^n}} f(x) \pmod 2$, and $\mathrm{Tr}_1^k(x) = x + x^2 + x^{2^2} + \cdots + x^{2^{k-1}}$, $k \in \mathbb{Z}^+$, is the trace function. For every $j \in \mathbb{Z}/(2^n - 1)\mathbb{Z}$, we can write $j = \sum_{s \in E} 2^s$ where $E \subseteq \{0, 1 \ldots, n-1\}$. The cardinality of E, denoted by $|E|$, is referred to as the 2-weight of j and written as $w_2(j)$. The support of $f \in \mathcal{B}_n$ is $supp(f) = \{x \in \mathbb{F}_{2^n} : f(x) \neq 0\}$, whose cardinality $wt(f) = |supp(f)|$ is the (Hamming) *weight* of f. The (Hamming) *distance* between any two Boolean functions $f, g \in \mathcal{B}_n$, denoted by $d(f, g)$, is the number of input values at which the outputs of f and g disagree, i.e., the cardinality of $\{x : f(x) \neq g(x), x \in \mathbb{F}_{2^n}\}$.

The *algebraic degree* of f is defined by $\deg(f) = \max_{j\in\Gamma(n)}\{w_2(j) : \alpha_j \neq 0\}$. Boolean functions with algebraic degree at most 1 are said to be *affine functions*. Precisely, an affine function $\varphi_{a,\varepsilon} : \mathbb{F}_{2^n} \to \mathbb{F}_2$ is of the form

$$\varphi_{a,\varepsilon}(x) = \mathrm{Tr}_1^n(ax) + \varepsilon, \text{ for all } x \in \mathbb{F}_{2^n},$$

where $a \in \mathbb{F}_{2^n}$, $\varepsilon \in \mathbb{F}_2$ (if $\varepsilon = 0$, then $\varphi_{a,0}$ is a *linear* function). Suppose $n = mt$, where $m, t \in \mathbb{Z}^+$, and $f : \mathbb{F}_{2^t}^m \to \mathbb{F}_2$. Then the *m-variate representation* of f is

$$f(x_1, \ldots, x_m) = \mathrm{Tr}_1^t(g(x_1, \ldots, x_m)), \text{ for all } (x_1, \ldots, x_m) \in \mathbb{F}_{2^t}^m, \tag{2}$$

where $g(x_1, \ldots, x_m) \in \mathbb{F}_{2^t}[x_1, \ldots, x_m]$. In this paper we will mostly use bivariate representations of Boolean functions.

The *nonlinearity* of $f \in \mathcal{B}_n$ is $nl(f) = \min\{d(f, \varphi_{a,\varepsilon}) : a \in \mathbb{F}_{2^n}, \varepsilon \in \mathbb{F}_2\}$. The *Walsh-Hadamard transform* of f at $a \in \mathbb{F}_{2^n}$ is defined by

$$W_f(a) = \sum_{x\in\mathbb{F}_{2^n}} (-1)^{f(x)+\mathrm{Tr}_1^n(ax)}. \tag{3}$$

The multiset $[W_f(a) : a \in \mathbb{F}_{2^n}]$ is said to be the *Walsh-Hadamard spectrum* of f. In the bivariate case, where $f : \mathbb{F}_{2^t}^2 \to \mathbb{F}_2$, instead of (3) we have

$$W_f(a, b) = \sum_{(x,y)\in\mathbb{F}_{2^t}^2} (-1)^{f(x,y)+\mathrm{Tr}_1^t(ax)+\mathrm{Tr}_1^t(by)}, \tag{4}$$

for all $(a, b) \in \mathbb{F}_{2^t}^2$. It is known that the nonlinearity of $f \in \mathcal{B}_n$ can be expressed in terms of the Walsh-Hadamard coefficients as

$$nl(f) = 2^{n-1} - \frac{1}{2}\max_{a\in\mathbb{F}_{2^n}} |W_f(a)| \leq 2^{n-1} - 2^{\frac{n}{2}-1}, n \geq 1, \tag{5}$$

(the upper bound is a direct consequence of Parseval's identity $\sum_{a\in\mathbb{F}_{2^n}} W_f^2(a) = 2^{2n}$). It is known [8] that the upper bound is tight if $n \in \mathbb{Z}^+$ is even, and achieved by *bent functions* (first studied by Rothaus [15] and Dillon [9]), which are functions f for which $nl(f) = 2^{n-1} - 2^{\frac{n}{2}-1}$. Also, f is bent if and only if $W_f(x) = \pm 2^{\frac{n}{2}}$, for all $x \in \mathbb{F}_{2^n}$, if and only if $\sum_{x\in\mathbb{F}_{2^n}} (-1)^{f(x)+f(x+a)} = 0$, for all $a \in \mathbb{F}_{2^n}^*$.

1.1 Maiorana-McFarland bent functions

Suppose $n = 2t$ where $t \in \mathbb{Z}^+$. Any permutation $\pi : \mathbb{F}_{2^t} \to \mathbb{F}_{2^t}$ can be represented by a polynomial $\pi(x) = \sum_{j=0}^{2^t-1} \alpha_j x^j$ where $\alpha_j \in \mathbb{F}_{2^t}$, for all $0 \leq j \leq 2^t - 1$. The algebraic degree of π is $\deg(\pi) := \max\{w_2(j) : \alpha_j \neq 0\}$. Rothaus [15] proved that any function of the form

$$\begin{aligned} &f : \mathbb{F}_{2^t} \times \mathbb{F}_{2^t} \to \mathbb{F}_2 \\ &f(x, y) = \mathrm{Tr}_1^t(x\pi(y)) + g(y), \text{ for all } (x, y) \in \mathbb{F}_{2^t} \times \mathbb{F}_{2^t}, \end{aligned} \tag{6}$$

where $g \in \mathcal{B}_t$, is bent. These bent functions are said to be Maiorana-McFarland bent functions and their set is denoted by $\mathcal{M}$. In this paper we assume g to be identically zero. For $f \in \mathcal{M}$ with $g = 0$ the algebraic degree is $\deg(f) = \deg(\pi) + 1$. Maiorana-McFarland construction provides a natural connection between permutations over finite

fields and functions in $\mathcal{M}$. Permutations having algebraic degree 1 are said to be linearized permutations. Each linearized permutation on $\mathbb{F}_{2^t}$ generates a quadratic function in $\mathcal{M}$.

Suppose that $\gcd(t,i)=e$, with $\frac{t}{e}$ an odd positive integer, and $\alpha \in \mathbb{F}_{2^t}$ such that $\alpha \neq \zeta^{m(2^e-1)}$ for any $m \in \mathbb{Z}$ and any primitive element ζ of $\mathbb{F}_{2^t}$. Blokhuis et al. [1] mention that σ_j, $j \in \{1,2,3\}$, listed below are linearized permutations on $\mathbb{F}_{2^t}$.

$$\begin{aligned} \sigma_1(x) &= x^{2^i} + \alpha x, \\ \sigma_2(x) &= x^{2^{2i}} + \alpha^{2^i} x, \\ \sigma_3(x) &= x^{2^i} + \alpha^{2^i} x. \end{aligned} \tag{7}$$

Some other linearized polynomials over $\mathbb{F}_{2^t}$ which will be used in the paper are as follows:

$$\begin{aligned} \sigma_4(y) &= y^{2^{2i}} + \alpha^{2^{2i}} y, \\ \sigma_5(y) &= y^{2^{2i}} + \alpha y, \\ \sigma_6(y) &= y + \alpha^{2^i} y^{2^i}, \\ \sigma_7(y) &= y + \alpha^{2^{2i}} y^{2^{2i}}, \\ \sigma_8(y) &= y + \alpha^{2^{2i}} y^{2^i}. \end{aligned} \tag{8}$$

Observe that the linearized function $\sigma_4(y)=0$ if and only if $y=0$ or $y^{2^{2i}-1} = \alpha^{2^{2i}}$. If $y^{2^{2i}-1} = \alpha^{2^{2i}}$, then $\left(\alpha^{\frac{2^t-1}{2^e-1}}\right)^{2^{2i}} = 1$, since $e \,|\, i$, which implies $\alpha^{\frac{2^t-1}{2^e-1}} = 1$. This is a contradiction, since $\alpha^{\frac{2^t-1}{2^e-1}} \neq 1$. Thus, σ_4 is a linearized permutation. Similarly, it can be proved that σ_j, $j = 5,6,7,8$ are linearized permutations.

Each function $f(x,y) = \mathrm{Tr}_1^t(x\sigma_j(y))$, $1 \leq j \leq 8$, is a quadratic bent in $\mathcal{M}$. Moreover, the following two quadratic permutations were constructed by Blockhuis et al. [1]:

$$\begin{aligned} \pi_1(y) &= y^{2^i+1} + \alpha y^{2^{t-i}+1}, \\ \pi_2(y) &= y(\mathrm{Tr}_\ell^t(y) + \alpha y), \end{aligned} \tag{9}$$

where $t = k\ell$, k is an odd integer and $\ell > 1$ is any positive integer (discussed later in details in Section 2.1) on the parameter α. In this paper, we use the functions of the form $f_j(x,y) = \mathrm{Tr}_1^t(x\pi_j(y))$, $1 \leq j \leq 2$ as a source of cubic bent functions and consider their differential properties.

1.2 Preliminary results

Recall the following well known facts from elementary number theory, which we use frequently in this paper. Suppose that $ax \equiv b \pmod{n}$ where $a,b,n \in \mathbb{Z}$ and $d = \gcd(a,n)$. Then

1. if d does not divide b, the congruence has no solution;
2. if d divide b then all solutions of the congruence are $x_0 + k\frac{n}{d}$, $0 \leq k < d$, where x_0 is the unique solution to $(\frac{a}{d})x \equiv (\frac{b}{d}) \pmod{\frac{n}{d}}$.

Let t be a positive integer and $\gcd(t,i)=e$. Then [7, p. 2]

$$\gcd(2^{2i}-1,2^t-1)=2^{\gcd(2i,t)}-1=\begin{cases}2^e-1, & \text{if } \frac{t}{e} \text{ is odd;}\\ 2^{2e}-1, & \text{if } \frac{t}{e} \text{ is even.}\end{cases}$$

Theorem 1 ([7, Theorem 3.1])**.** *Let ζ be a primitive element of $\mathbb{F}_{2^t}$ and $\gcd(t,i)=e$. For any $a\in\mathbb{F}_{2^t}^*$, consider the equation $a^{2^i}x^{2^{2i}}+ax=0$ over $\mathbb{F}_{2^t}$. Then:*

1. *If $\frac{t}{e}$ is odd then there are 2^e solutions to this equation for any choice of $a\in\mathbb{F}_{2^t}^*$.*
2. *If $\frac{t}{e}$ is even then there are two possible cases:*
   (a) *if $a=\zeta^{s(2^e+1)}$ for some s, then there are 2^{2e} solutions to the equation.*
   (b) *if $a\neq\zeta^{s(2^e+1)}$ for any s, then there exists one solution only, namely $x=0$.*

1.3 Affine equivalence

The general linear group of degree n over $\mathbb{F}_2$, denoted by $GL(n,\mathbb{F}_2)$, is the group of invertible linear transformations acting on $\mathbb{F}_{2^n}$. For any $A\in GL(n,\mathbb{F}_2)$ and $x\in\mathbb{F}_{2^n}$ we denote the action of A on x by $x\mapsto xA$. The affine general linear group, $AGL(n,\mathbb{F}_2)$, is the set of all transformations of the form $x\mapsto xA+b$ where $b\in\mathbb{F}_{2^n}$. This group can be thought of as the semidirect product $GL(n,\mathbb{F}_2)\ltimes\mathbb{F}_{2^n}$, but we will not need that here.

Definition 2. *Two Boolean functions $f,g\in\mathcal{B}_n$ are said to be affine equivalent if there exists $(A,b)\in AGL(n,\mathbb{F}_2)$ such that $g(x)=f(xA+b)$, for all $x\in\mathbb{F}_{2^n}$.*

For Boolean functions used as cryptographic primitives the notion of equivalence is further generalized as follows.

Definition 3. *Two Boolean functions $f,g\in\mathcal{B}_n$ are said to be extended affine equivalent (EA-equivalent) if there exist $(A,b)\in AGL(n,\mathbb{F}_2)$, $a\in\mathbb{F}_{2^n}$ and $\varepsilon\in\mathbb{F}_2$ such that $g(x)=f(xA+b)+\varphi_{a,\varepsilon}(x)$, for all $x\in\mathbb{F}_{2^n}$ where $\varphi_{a,\varepsilon}(x)=\mathrm{Tr}_1^n(ax)+\varepsilon$.*

If two Boolean functions $f,g\in\mathcal{B}_n$ have different algebraic degrees then they are EA-inequivalent. Therefore, the algebraic degree serves as an EA-invariant. The multiset consisting of absolute values of Walsh-Hadamard transforms of a function f is said to be its *absolute Walsh-Hadamard spectrum*. If the absolute Walsh-Hadamard spectra of two Boolean functions are different, which is possible even if their algebraic degrees are the same, then we know that they are EA-inequivalent. Thus, the absolute Walsh-Hadamard spectrum serves as a more sophisticated EA-invariant. In fact, the autocorrelation spectrum which is another invariant is also connected to the Walsh-Hadamard spectrum. For bent functions the absolute Walsh-Hadamard spectrum is unique and flat, set to $2^{\frac{n}{2}}$ where n is the number of variables. For this reason the invariants dependent on Walsh-Hadamard spectra are unable to decide EA-inequivalence of bent functions. In this paper, we use a second-derivative based invariant to distinguish between the classes of cubic bent functions in $\mathcal{M}$ which have no affine derivative.

1.4 Derivatives and affine inequivalence

The problem of deciding EA-inequivalence is completely solved for Boolean functions having algebraic degrees at most 2, that is, for affine and quadratic Boolean functions. We refer to MacWilliams and Sloane [14, Chapter 15] for detailed discussion on quadratic Boolean functions including their affine inequivalence. In the absence of a general theory for functions having algebraic degree three and above we address the problem by considering derivatives of these functions.

Definition 4. *The derivative of $f \in \mathcal{B}_n$ with respect to an m-dimensional $\mathbb{F}_2$-subspace V of $\mathbb{F}_{2^n}$, or the mth-(order) derivative, is the function $D_V f : \mathbb{F}_{2^n} \to \mathbb{F}_2$ defined by*

$$D_V f(x) = \sum_{a \in V} f(x+a), \text{ for all } x \in \mathbb{F}_{2^n}. \tag{10}$$

The algebraic degree to $D_V f$ is at most $\deg(f) - m$. If V is one-dimensional then $D_V f(x) = f(x+a) + f(x)$ where $a \in V \setminus \{0\}$, which is usually denoted by $D_a f(x)$. If V is a 2-dimensional subspace of $\mathbb{F}_{2^n}$ we choose any pair of distinct elements $a, b \in V \setminus \{0\}$ and write

$$D_V f(x) = D_{a,b} f(x) = f(x) + f(x+a) + f(x+b) + f(x+a+b),$$

for all $x \in \mathbb{F}_{2^n}$. Obviously the choice of (a, b) does not change the function $D_V f$.

Dillon [9] proposed proving inequivalence of Boolean functions by considering their mth-order derivatives over all distinct m-dimensional subspaces of $\mathbb{F}_{2^n}$.

Theorem 5 ([9, Theorem 2.1])**.** *For any function $f \in \mathcal{B}_n$ let $\mathcal{D}_k(f)$ denote the multiset of all k-dimensional derivatives of f. If $f, g \in \mathcal{B}_n$ are affinely equivalent, then so are $\mathcal{D}_k(f)$ and $\mathcal{D}_k(g)$. If the nonsingular affine transformation A (operating on $\mathcal{B}_n$) maps f onto g, then it also maps $\mathcal{D}_k(f)$ onto $\mathcal{D}_k(g)$.*

Dillon proved the following corollary to Theorem 5.

Corollary 6. *If $\mathcal{P}$ is any affine invariant for $\mathcal{B}_n$, then $f \longrightarrow \mathcal{P}\{\mathcal{D}_n(f)\}$ is also an affine invariant for $\mathcal{B}_n$.*

Derivatives have been used for this purpose by Carlet [4] and, Canteaut and Charpin [2]. Second derivatives have been used by Gangopadhyay [11] extensively to demonstrate affine inequivalence between cubic bent function in $\mathcal{M}$ which are in many ways similar to each other. The technique can be summarized as follows:

1. For $f \in \mathcal{B}_n$, construct the set

   $$S_f = \{wt(D_V f) : V \text{ varies over all distinct two dimensional subspaces of } \mathbb{F}_2^n\}.$$

2. Construct the frequency distribution of the weights in S_f. We refer to S_f as the second-derivative weight distribution of f.

3. For any two $f, g \in \mathcal{B}_n$, if the second-derivative weight distributions of f and g are different then f and g are affine inequivalent.

1.5 A problem proposed by Hou

Hou [12] proposed the problem of finding values of n for which there exist n-variable cubic bent functions having no affine derivative. Canteaut and Charpin [2, Lemma 1] considered the cubic bent functions of the form $f(x,y) = \mathrm{Tr}_1^t(xy^{2^i+1})$ and proved that they have no affine derivative. Using this result they constructed an infinite family of cubic bent functions. Gangopadhyay [11] identified subclasses of inequivalent bent functions within this class, by using an invariant proposed by Dillon [9].

Theorem 7 ([11], Theorem 4)**.** *Let $n = 2t$. If $f_i(x,y) = \mathrm{Tr}_1^t(xy^{2^i+1})$ where $x, y \in \mathbb{F}_{2^t}$, $n \geq 6$, $i \in \mathbb{Z}$ such that $1 \leq i < t$ and $\gcd(2^i+1, 2^t-1) = 1$, then the number of constant functions among $D_V f_i$ is*

$$\frac{(2^t-1)(2^{t+e-1}(2^e+1)-(2^t+1))}{3}$$

where $\gcd(t,i) = e$.

Using this result, Gangopadhyay [11, Corollary 5] proved that if $\gcd(t,i) \neq \gcd(t,j)$ then f_i and f_j are not affine equivalent. In this paper our goal is not only to identify some more classes of cubic bent functions in $\mathcal{M}$ having no affine derivative but also to prove affine inequivalence between the classes of functions so obtained. We use Theorem 7 almost exclusively for that purpose.

1.6 Motivation

Boolean functions are used in many cryptosystems. For example, in some LFSR based stream ciphers, a Boolean function is used to combine the outputs of several LFSRs. To design a secure cryptosystem, it is required that the output of the Boolean function should not be correlated with a subset of input variables, and thus, to resist correlation attacks [16], the concept of resiliency of a Boolean function was invented. In [3, Proposition 4.2], Camion et al. constructed a resilient function which is quite similar to the Maiorana–McFarland bent functions. Further, in a block cipher, linear structures have been investigated for their cryptanalytic significance. In [6], Charpin et al. derived a relation between polynomial with linear structure and a Maiorana–McFarland function with an affine derivative.

In the recent past some new cryptographic properties have been proposed which are relevant particularly when functions depending on a small number of variables are used as cryptographic primitives. One such property is the second-order nonlinearity of a Boolean function [5], that is, the Hamming distance of the function from the set of quadratic Boolean functions. The experimental evidences [10, Section 3] suggest that cubic bent functions having no affine derivative might be possessing higher second-order derivatives than the rest.

Thus, Boolean functions that do or do not posses affine derivative are important from a cryptographic perspective. In this paper we show that the functions of the form $f_j(x,y) = \mathrm{Tr}_1^t(x\pi_j(y))$, $1 \leq j \leq 2$, where π_j's are defined by (9), do not have affine derivative and they are mutually affine inequivalent.

Our analysis shows that there exist quite a few affine inequivalent classes of cubic bent function in $\mathcal{M}$ having no affine derivative. Primary research direction ought to be towards finding out such bent functions outside $\mathcal{M}$ and evaluating the significance of those functions in cryptography and coding theory.

2 Cubic bent functions in $\mathcal{M}$

Two subclasses of cubic bent functions in $\mathcal{M}$ are constructed by using the permutations in (9). We show that the functions in each of these classes have no affine derivative. We prove that the functions in the different subclasses are affine inequivalent by considering their second-derivative weight distributions. Thus we extend the number of known cubic bent functions in $\mathcal{M}$ with no affine derivative.

2.1 Subclass associated to $\pi_1(y) = y^{2^i+1} + \alpha y^{2^{t-i}+1}$

Let $n = 2t$, $t \geq 3$ and ζ be a primitive element of $\mathbb{F}_{2^t}$. Blokhuis et al. [1] proved that the function $\pi_1 : \mathbb{F}_{2^t} \to \mathbb{F}_{2^t}$ defined by

$$\pi_1(y) = y^{2^i+1} + \alpha y^{2^{t-i}+1},$$

for all $y \in \mathbb{F}_{2^t}$, where $i \in \mathbb{Z}$ such that $1 \leq i < t$ is a permutation if the following conditions are satisfied:

1. $\gcd(i,t) = e$ and $\frac{t}{e}$ is odd;
2. $\alpha \neq \zeta^{s(2^e-1)}$, for any $s \in \mathbb{Z}$.

Lemma 8. *Under the above conditions, the cubic Maiorana-McFarland bent function $f_i : \mathbb{F}_{2^t} \times \mathbb{F}_{2^t} \longrightarrow \mathbb{F}_2$ defined by*

$$f_i(x,y) = \mathrm{Tr}_1^t(xy^{2^i+1} + \alpha x y^{2^{t-i}+1}), \text{ for all } (x,y) \in \mathbb{F}_{2^t} \times \mathbb{F}_{2^t}, \tag{11}$$

does not possess any affine derivative.

Proof. Let $a, b \in \mathbb{F}_{2^t}$. Then the first derivative of f_i at $(a,b) \in \mathbb{F}_{2^t} \times \mathbb{F}_{2^t}$ is

$$\begin{aligned} D_{(a,b)}f_i(x,y) &= \mathrm{Tr}_1^t\left(a\pi_1(y) + (x+a)D_b\pi_1(y)\right) \\ &= \mathrm{Tr}_1^t\Big(a\left(y^{2^i+1} + \alpha y^{2^{t-i}+1}\right) \\ &\qquad + (x+a)\left(y^{2^i}b + yb^{2^i} + b^{2^i+1} + \alpha y^{2^{t-i}}b + \alpha y b^{2^{t-i}} + \alpha b^{2^{t-i}+1}\right)\Big), \end{aligned}$$

for all $(x,y) \in \mathbb{F}_{2^t} \times \mathbb{F}_{2^t}$. If $a \neq 0$, then $D_{(a,b)}f_i(x,y)$ is a quadratic function. If $a = 0$ and $b \neq 0$, then

$$D_{(0,b)}f_i(x,y) = \mathrm{Tr}_1^t\left(x\left(y^{2^i}b + yb^{2^i} + \alpha y^{2^{t-i}}b + \alpha y b^{2^{t-i}}) + x(b^{2^i+1} + \alpha b^{2^{t-i}+1}\right)\right)$$

is an affine function if and only if $p(y) = y^{2^i}b + yb^{2^i} + \alpha y^{2^{t-i}}b + \alpha y b^{2^{t-i}}$ is constant for all $y \in \mathbb{F}_{2^t}$. Since $p(0) = 0$, then (simplifying by y above) $y^{2^i-1} + b^{2^i-1} + \alpha y^{2^{t-i}-1} + \alpha b^{2^{t-i}-1} = 0$, for all $y \in \mathbb{F}_{2^t}^*$. For $y = 1$, we get $b^{2^i-1} + \alpha b^{2^{t-i}-1} = 1 + \alpha$, which renders

$$y^{2^i-1} + \alpha y^{2^{t-i}-1} + 1 + \alpha = 0. \tag{12}$$

If $\alpha = 0$, then the solution space of (12) is $\mathbb{F}_{2^e}$. If $\alpha \neq 0$, we know that for $y \in \mathbb{F}_{2^e}$, then $y^{2^i-1} = 1 = y^{2^{t-i}-1}$, since $e = \gcd(i,t)$. Therefore (12) is identically zero. Otherwise, substituting $y = c \in \mathbb{F}_{2^t} \setminus \mathbb{F}_{2^e}$ in (12) $c^{2^i-1} + \alpha c^{2^{t-i}-1} + 1 + \alpha = 0$, so $\alpha = \frac{c+c^{2^i}}{c+c^{2^{t-i}}}$

and then, $\alpha^{2^i} = \frac{(c+c^{2^i})^{2^i}}{(c+c^{2^{t-i}})^{2^i}} = (c+c^{2^i})^{2^i-1}$, that is, $\left(\alpha^{\frac{2^t-1}{2^e-1}}\right)^{2^i} = 1$, since $e \mid i$, which implies $\alpha^{\frac{2^t-1}{2^e-1}} = 1$. This is a contradiction, since $\alpha^{\frac{2^t-1}{2^e-1}} \neq 1$ (otherwise, the condition $\alpha \neq \zeta^{s(2^e-1)}$ would be violated). Thus equation (12) does not hold for all $y \in \mathbb{F}_{2^t}$. Therefore, $D_{(0,b)}f_i$ is not an affine function, and our lemma is shown. □

Theorem 9. *The number of distinct* 2*-dimensional subspaces corresponding to constant second-derivatives of* f_i *is*

$$\frac{(2^t-1)\left(2^{t+e-1}(2^e+1)-(2^t+1)\right)}{3}.$$

Proof. Let $V = \langle (a,b),(c,d)\rangle$ be any 2-dimensional subspace of $\mathbb{F}_{2^t} \times \mathbb{F}_{2^t}$. The second order derivative of f_i is

$$\begin{aligned} D_V f_i(x,y) &= \mathrm{Tr}_1^t((ad+bc)y^{2^i} + (ad^{2^i} + cb^{2^i})y + \alpha(ad+cb)y^{2^{t-i}} \\ &+ \alpha(ad^{2^{t-i}} + cb^{2^{t-i}})y + \gamma x + (ad^{2^i+1} + cb^{2^i+1}) + \alpha(ad^{2^{t-i}+1} + cb^{2^{t-i}+1}) \\ &+ (a+c)\gamma) \end{aligned}$$

where $\gamma = (bd^{2^i} + b^{2^i}d) + \alpha(bd^{2^{t-i}} + b^{2^{t-i}}d)$.
Case 1: We first assume $b = 0$, $d = 0$. Then $D_V f_i(x,y) = 0$ for all $(x,y) \in \mathbb{F}_{2^t} \times \mathbb{F}_{2^t}$. Thus, with respect to any 2-dimensional subspace of $\mathbb{F}_{2^t} \times \{0\}$ the second order derivative of f_i is 0. Therefore the number of 2-dimensional subspaces such that $D_V f_i$ is constant, is equal to $\frac{(2^t-1)(2^{t-1}-1)}{3}$.
Case 2: Let $b = 0$ but $d \neq 0$. Then

$$\begin{aligned} D_V f_i(x,y) &= \mathrm{Tr}_1^t\left((ad)y^{2^i} + (ad^{2^i})y + \alpha(ad)y^{2^{t-i}} + \alpha(ad^{2^{t-i}})y + (ad^{2^i+1}) + \alpha(ad^{2^{t-i}+1})\right) \\ &= \mathrm{Tr}_1^t\left(((ad)^{2^{t-i}} + ad^{2^i} + (\alpha ad)^{2^i} + \alpha ad^{2^{t-i}})y\right) + \mathrm{Tr}_1^t\left(ad^{2^i+1} + \alpha ad^{2^{t-i}+1}\right). \end{aligned}$$

Thus, $D_V f_i(x,y)$ is constant if and only if $(ad)^{2^{t-i}} + ad^{2^i} + (\alpha ad)^{2^i} + \alpha ad^{2^{t-i}} = 0$, and so,

$$\begin{aligned} 0 &= ad + a^{2^i}d^{2^{2i}} + (\alpha ad)^{2^{2i}} + (\alpha a)^{2^i}d \\ &= (a^{2^i} + (\alpha a)^{2^{2i}})d^{2^{2i}} + (a + (\alpha a)^{2^i})d, \end{aligned}$$

which can be writen as $h^{2^i}d^{2^{2i}} + hd = 0$, where $h = a + (\alpha a)^{2^i}$. Thus, $h \neq 0$ as $a \neq 0$. Then, by Theorem 1, the above equation has $2^e - 1$ nonzero solutions for d in $\mathbb{F}_{2^t}$. Therefore, for any nonzero $a \in \mathbb{F}_{2^t}$, it is possible to choose d in $2^e - 1$ ways, a can be chosen in $2^t - 1$ ways and c in 2^t ways, since the subspace generated by $\{(a,0),(c,d)\}$ is equal to the subspace generated by $\{(a,0),(a+c,d)\}$. Therefore the total number of 2-dimensional subspaces such that the second derivative of f_i is constant, is equal to $(2^t-1)2^{t-1}(2^e-1)$.
Case 3: Let $b \neq 0$ and $d \neq 0$.
Subcase (i): Let $b = d$. Then the subspace generated by $\{(a,b),(c,d)\}$ is equal to the subspace generated by $\{(a+c,b+d),(c,d)\} = \{(a+c,0),(c,d)\}$, which is the same as in the previous case.

Subcase (ii): Let $b \neq d$. Then, $D_V f_i(x,y)$ is constant if and only if

$$\mathrm{Tr}_1^t\left((ad+bc)y^{2^i}+(ad^{2^i}+cb^{2^i})y+\alpha(ad+cb)y^{2^{t-i}}+\alpha(ad^{2^{t-i}}+cb^{2^{t-i}})y\right)=0 \quad (13)$$

and

$$\gamma = 0. \quad (14)$$

From (14), we have $b^{2^i-1}+\alpha b^{2^{t-i}-1}=d^{2^i-1}+\alpha d^{2^{t-i}-1}$, since $b\neq 0$ and $d\neq 0$. Again, from (14),

$$0=\gamma=\gamma^{2^i}=b^{2^i}d^{2^{2i}}+b^{2^{2i}}d^{2^i}+\alpha^{2^i}(b^{2^i}d+bd^{2^i})=(bd^{2^i}+b^{2^i}d)^{2^i}+\alpha^{2^i}(b^{2^i}d+bd^{2^i}).$$

Let $z=bd^{2^i}+b^{2^i}d$. Then the above equation can be written as $z^{2^i}+\alpha^{2^i}z=0$, which has the only solution $z=0$, that is,

$$\begin{aligned} &b^{2^i}d+bd^{2^i}=0, \Longleftrightarrow \left(\frac{d}{b}\right)^{2^i-1}=1, \text{ as } b\neq 0 \text{ and } d\neq 0,\\ &\text{and so, } \frac{d}{b}\in \mathbb{F}_{2^e}^*, \text{ as } \gcd(t,i)=e. \end{aligned} \quad (15)$$

Since $b\neq d$, for any nonzero b, there exist a nonzero $\lambda\in\mathbb{F}_{2^e}$ with $\lambda\neq 1$ such that $d=\lambda b$. Thus, d can be chosen in 2^e-2 ways and b in 2^t-1 ways.

Further, from equation (13), we have

$$\begin{aligned} &\mathrm{Tr}_1^t\left((ad+bc)y^{2^i}+\alpha(ad+cb)y^{2^{t-i}}+y\left((ad^{2^i}+cb^{2^i})+\alpha(ad^{2^{t-i}}+cb^{2^{t-i}})\right)\right)=0,\\ \Leftrightarrow &\mathrm{Tr}_1^t\left((ad+bc)y^{2^i}+\alpha(ad+cb)y^{2^{t-i}}+y(ad+bc)(b^{2^i-1}+\alpha b^{2^{t-i}-1})\right)=0,\\ \Leftrightarrow &\mathrm{Tr}_1^t\left(\left((ad+bc)^{2^{t-i}}+(\alpha(ad+cb))^{2^i}+(ad+bc)(b^{2^i-1}+\alpha b^{2^{t-i}-1})\right)y\right)=0, \end{aligned}$$

for all $y\in\mathbb{F}_{2^t}$ if and only if the following (equivalent) statements hold

$$\begin{aligned} &(ad+bc)^{2^{t-i}}+(\alpha(ad+cb))^{2^i}+(ad+bc)(b^{2^i-1}+\alpha b^{2^{t-i}-1})=0,\\ \Leftrightarrow &b^{2^{t-i}}(a\lambda+c)^{2^{t-i}}+b^{2^i}(\alpha(a\lambda+c))^{2^i}+(a\lambda+c)(b^{2^i}+\alpha b^{2^{t-i}})=0,\\ \Leftrightarrow &b^{2^{t-i}}w^{2^{t-i}}+b^{2^i}(\alpha w)^{2^i}+w(b^{2^i}+\alpha b^{2^{t-i}})=0, \text{ where } w=a\lambda+c,\\ \Leftrightarrow &bw+(\alpha b)^{2^{2i}}w^{2^{2i}}+(b^{2^{2i}}+\alpha^{2^i}b)w^{2^i}=0,\\ \Leftrightarrow &w((\alpha b)^{2^{2i}}w^{2^{2i}-1}+(b^{2^{2i}}+\alpha^{2^i}b)w^{2^i-1}+b)=0. \end{aligned}$$

Therefore, we infer that either $w=0$ or $(\alpha b)^{2^{2i}}w^{2^{2i}-1}+(b^{2^{2i}}+\alpha^{2^i}b)w^{2^i-1}+b=0$,

which can be transformed into

$$
\begin{aligned}
&(\alpha b)^{2^{2i}} w^{(2^i-1)(2^i+1)} + (b^{2^{2i}} + \alpha^{2^i} b) w^{2^i-1} + b = 0, \\
\Leftrightarrow &\alpha^{2^{2i}} b^{2^{2i}} \mu^{2^i+1} + b^{2^{2i}} \mu + \alpha^{2^i} b\mu + b = 0, \text{ where } w^{2^i-1} = \mu, \\
\Leftrightarrow &(\alpha^{2^i}\mu + 1)^{2^i} b^{2^{2i}} \mu + (\alpha^{2^i}\mu + 1) b = 0, \\
\Leftrightarrow &b(\alpha^{2^i}\mu + 1)(b^{2^{2i}-1}\mu(\alpha^{2^i}\mu + 1)^{2^i-1} + 1) = 0, \\
&\alpha^{2^i}\mu + 1 \neq 0, \text{ since the only solution of } \alpha^{2^i} w^{2^i} + w = 0 \text{ is } w = 0 \text{ due to } \sigma_6(y), \\
\Leftrightarrow &b^{2^{2i}-1}\mu(\alpha^{2^i}\mu + 1)^{2^i-1} + 1 = 0, \text{ as } b \neq 0 \text{ and } \alpha^{2^i}\mu + 1 \neq 0, \\
\Leftrightarrow &b^{(2^i+1)(2^i-1)} w^{2^i-1}(\alpha^{2^i} w^{2^i-1} + 1)^{2^i-1} + 1 = 0, \\
\Leftrightarrow &(b^{2^i+1}(\alpha^{2^i} w^{2^i} + w))^{2^i-1} = 1, \\
\Leftrightarrow &b^{2^i+1}(\alpha^{2^i} w^{2^i} + w) \in \mathbb{F}_{2^i}^*, \\
\Leftrightarrow &b^{2^i+1}(\alpha^{2^i} w^{2^i} + w) \in \mathbb{F}_{2^e}^*, \text{ as } \gcd(i,t) = e,
\end{aligned}
$$

and thus

$$\alpha^{2^i} w^{2^i} + w = \frac{\lambda'}{b^{2^i+1}}, \text{ as } b \neq 0 \text{ and } \lambda' \in \mathbb{F}_{2^e}. \tag{16}$$

Since the homogeneous part of the above equation is a linear equation which has a unique solution $w = 0$, then the equation (16) has a unique solution in $\mathbb{F}_{2^t}$ for each $\lambda' \in \mathbb{F}_{2^e}$. Thus w can be chosen in 2^e ways (including $w = 0$). For fixed a and b, c can be chosen in 2^e ways. Therefore, a can be chosen in 2^t ways, b in $2^t - 1$ ways, d in $2^e - 2$ ways and c in 2^e ways. Each 2-dimensional subspace generated by a pair of vectors (a, b) and (c, d) satisfying the above conditions, contains altogether 6 distinct bases satisfying these conditions. Therefore, the total number of distinct two dimensional subspaces with bases of this type is $\frac{2^{t+e}(2^t-1)(2^e-2)}{6}$. Adding the counts from the above three cases we obtain the total count $\frac{(2^t-1)(2^{t+e-1}(2^e+1)-(2^t+1))}{3}$, and the theorem is shown. □

Remark 10. *If $\alpha = 0$, then the cubic Maiorana–McFarland bent function, defined as in equation (11) is $f_i(x, y) = Tr_1^t(xy^{2^i+1})$, for all $(x, y) \in \mathbb{F}_{2^t} \times \mathbb{F}_{2^t}$. From Theorem 7, we have the number of constant functions among the second order derivative of f_i is $\frac{(2^t-1)(2^{t+e-1}(2^e+1)-(2^t+1))}{3}$.*

2.2 The subclass associated to $\pi_2(y) = y(\mathrm{Tr}_\ell^t(y) + \alpha y)$

We next consider a class of permutation polynomials constructed by Blokhuis [1] and referred to by Laigle-Chapuy [13].

Theorem 11 ([1], [13] Theorem 2)**.** *Let $t = k\ell$, where k be an odd and $\ell > 1$ be any positive integer. Then the following polynomial is a bilinear permutation over $\mathbb{F}_{2^t}$ of the form*

$$\pi(x) = x(\mathrm{Tr}_\ell^t(x) + \alpha x),$$

where $\alpha \in \mathbb{F}_{2^\ell} \setminus \mathbb{F}_2$ and $\mathrm{Tr}_\ell^t(x) = \sum_{i=0}^{k-1} x^{2^{\ell i}}$.

Using this class of permutations we construct a class of cubic Maiorana-McFarland bent functions. Let $t = k\ell$, where k be an odd and $\ell > 1$ be any positive integer. A function $g : \mathbb{F}_{2^t} \times \mathbb{F}_{2^t} \longrightarrow \mathbb{F}_2$ defined by

$$g(x,y) = \mathrm{Tr}_1^t\left(xy\,\mathrm{Tr}_\ell^t(y) + \alpha xy^2\right), \text{ for all } (x,y) \in \mathbb{F}_{2^t} \times \mathbb{F}_{2^t}, \tag{17}$$

is a cubic Maiorana-McFarland bent. We prove that if $k > 1$, then the functions g belonging to this class do not have any affine derivative.

Theorem 12. *Let $t = k\ell$, where k be an odd and $\ell > 1$ be any positive integer. If $k > 1$, then the cubic Maiorana-McFarland bent function g defined as in* (17) *has no affine derivative.*

Proof. Let (a,b) be an any element of $\mathbb{F}_{2^t} \times \mathbb{F}_{2^t}$.

$$\begin{aligned} D_{(a,b)}g(x,y) &= g(x,y) + g(x+a, y+b) \\ &= \mathrm{Tr}_1^t\left(xy\mathrm{Tr}_\ell^t(y) + (x+a)(y+b)\mathrm{Tr}_\ell^t(y+b) + \alpha xy^2 + \alpha(x+a)(y+b)^2\right) \\ &= \mathrm{Tr}_1^t\left(a\left(y\mathrm{Tr}_\ell^t(y) + \alpha y^2\right) + (x+a)\left(y\mathrm{Tr}_\ell^t(b) + b\mathrm{Tr}_\ell^t(y) + b\mathrm{Tr}_\ell^t(b) + \alpha b^2\right)\right). \end{aligned}$$

Let $a \neq 0$. Since $y\mathrm{Tr}_\ell^t(y) + \alpha y^2 = 0 \Longleftrightarrow y = 0$ or $Tr_\ell^t(y) = \alpha y \Longleftrightarrow y = 0$. Thus, if $a \neq 0$, $D_{(a,b)}g$ is a quadratic function. Let us consider $a = 0$, so

$$D_{(0,b)}g(x,y) = \mathrm{Tr}_1^t\left(x\left(y\mathrm{Tr}_\ell^t(b) + b\mathrm{Tr}_\ell^t(y)\right) + x\left(b\mathrm{Tr}_\ell^t(b) + \alpha b^2\right)\right),$$

which is an affine function if and only if $p(y) = y\mathrm{Tr}_\ell^t(b) + b\mathrm{Tr}_\ell^t(y)$ is constant for all $y \in \mathbb{F}_{2^t}$. If that is so, since $p(0) = 0$, then $p(y) = y\mathrm{Tr}_\ell^t(b) + b\mathrm{Tr}_\ell^t(y) = 0$, for all y, in particular, for $y = 1$, we get $b + \mathrm{Tr}_\ell^t(b) = 0$, that is,

$$y\mathrm{Tr}_\ell^t(b) + b\mathrm{Tr}_\ell^t(y) = 0 \Longrightarrow y + \mathrm{Tr}_\ell^t(y) = 0 \Longrightarrow y \in \mathbb{F}_{2^\ell}.$$

Thus $p(y)$ is not a constant function for all $y \in \mathbb{F}_{2^t}$. Therefore g does not posses any affine derivative. □

Remark 13. *If $k = 1$, then $t = \ell$ and for any $(a,b) \in \mathbb{F}_{2^t} \times \mathbb{F}_{2^t}$,*

$$D_{(a,b)}g(x,y) = Tr_1^t((1+\alpha)(xb^2 + a(y+b)^2)),$$

which is an affine function. Therefore, if $k = 1$, then a function g of the form as in (17) *has affine derivatives. Thus, if $k = 1$, then f_i and g are affine inequivalent, where f_i and g are defined as in* (11) *and* (17)*, respectively.*

Theorem 14. *Suppose $n = 2t$ and g be defined as in* (17)*. The number of distinct 2-dimensional subspaces corresponding to constant second-derivatives of g is*

$$\frac{2^{-3\ell-1}\left(2^{2(2\ell+t)} + 2^{4\ell+t+1} - 2^{5\ell+t} - 5\cdot 2^{3\ell+2t} + 2^{5\ell+2t} - 2^{2(\ell+t)} + 2^{3\ell+1} + 2^{4t}\right)}{3}.$$

Proof. Let $V = \langle (a,b),(c,d)\rangle$ be any 2-dimensional subspace of $\mathbb{F}_{2^t} \times \mathbb{F}_{2^t}$.

$$\begin{aligned} D_V g(x,y) = \mathrm{Tr}_1^t\big((ad+bc)\mathrm{Tr}_\ell^t(y) + \left(a\mathrm{Tr}_\ell^t(d) + c\mathrm{Tr}_\ell^t(b)\right)y + \left(ad\mathrm{Tr}_\ell^t(d) + cb\mathrm{Tr}_\ell^t(b)\right) \\ + \left(b\mathrm{Tr}_\ell^t(d) + d\mathrm{Tr}_\ell^t(b)\right)x + (a+c)\left(b\mathrm{Tr}_\ell^t(d) + d\mathrm{Tr}_\ell^t(b)\right) + \alpha(ad^2 + cb^2)\big). \end{aligned}$$

Case 1: Let $b = 0$ and $d = 0$. Then $D_V g(x, y) = 0$, for all $(x, y) \in \mathbb{F}_{2^t} \times \mathbb{F}_{2^t}$. Thus, with respect to any 2-dimensional subspace of $\mathbb{F}_{2^t} \times \{0\}$, the second order derivative of g is 0. The number of such 2-dimensional subspaces is $\frac{(2^t-1)(2^{t-1}-1)}{3}$.
Case 2: Let $b = 0$ and $d \neq 0$. Then

$$D_V g(x, y) = \mathrm{Tr}_1^t \left(ad\mathrm{Tr}_\ell^t(y) + a\mathrm{Tr}_\ell^t(d)y + ad\mathrm{Tr}_\ell^t(d) + \alpha ad^2 \right). \tag{18}$$

Since

$$\begin{aligned} \mathrm{Tr}_1^t \left(ad\mathrm{Tr}_\ell^t(y) \right) &= \mathrm{Tr}_1^t \left(ad \left(y + y^{2^\ell} + y^{2^{2\ell}} + \cdots + y^{2^{(k-1)\ell}} \right) \right) \\ &= \mathrm{Tr}_1^t \left(y \left(ad + (ad)^{2^{(k-1)\ell}} + (ad)^{2^{(k-2)\ell}} + \cdots + (ad)^{2^\ell} \right) \right) \\ &= \mathrm{Tr}_1^t \left(y \, \mathrm{Tr}_\ell^t(ad) \right). \end{aligned}$$

From (18), we have

$$D_V g(x, y) = \mathrm{Tr}_1^t \left((\mathrm{Tr}_\ell^t(ad) + a\mathrm{Tr}_\ell^t(d))y + ad\mathrm{Tr}_\ell^t(d) + \alpha ad^2 \right),$$

which is constant if and only if

$$\mathrm{Tr}_\ell^t(ad) + a\mathrm{Tr}_\ell^t(d) = 0. \tag{19}$$

Subcase (i): Let $a \in \mathbb{F}_{2^\ell}$. Then equation (19) is satisfied for all $d \in \mathbb{F}_{2^t}$. Therefore, d can be chosen in $2^t - 1$ ways and a in $2^\ell - 1$ ways. Thus, the number of 2-dimensional subspaces on which the second-derivatives of g are constants is equal to $(2^\ell - 1)2^{t-1}(2^t - 1)$.
Subcase (ii): Let $a \in \mathbb{F}_{2^t} \setminus \mathbb{F}_{2^\ell}$. Then $\mathrm{Tr}_\ell^t(ad) + a\mathrm{Tr}_\ell^t(d) = 0$ if and only if $\mathrm{Tr}_\ell^t(d) = 0$ and $\mathrm{Tr}_\ell^t(ad) = 0$. Since both are $(k-1)$-dimensional $\mathbb{F}_{2^\ell}$-subspaces of $\mathbb{F}_{2^t}$, d can be chosen in $2^{t-2\ell}$ ways and a in $2^t - 2^\ell$ ways. Thus, the number of such 2-dimensional subspaces is $(2^t - 2^\ell)2^{t-1}(2^{t-2\ell} - 1)$.
Case 3 Let $b \neq 0$ and $d \neq 0$ and $b = d$. Then the subspace generated by $\{(a, b), (c, d)\}$ is equal to the subspace generated by $\{(a + c, b + d), (c, d)\} = \{(a + c, 0), (c, d)\}$, which is the same as in the previous case.
Case 4: Let $b \neq 0$ and $d \neq 0$ and $b \neq d$. Then $D_V g(x, y)$ is constant if and only if

$$b\mathrm{Tr}_\ell^t(d) + d\mathrm{Tr}_\ell^t(b) = 0, \quad \text{for all } \ x \in \mathbb{F}_{2^t} \tag{20}$$

and we get the implications

$$\begin{aligned} &\mathrm{Tr}_1^t((ad + bc)\mathrm{Tr}_\ell^t(y) + (a\mathrm{Tr}_\ell^t(d) + c\mathrm{Tr}_\ell^t(b))y) = 0, \\ &\mathrm{Tr}_1^t((\mathrm{Tr}_\ell^t(ad + bc) + (a\mathrm{Tr}_\ell^t(d) + c\mathrm{Tr}_\ell^t(b)))y) = 0, \ \text{ for all } \ y \in \mathbb{F}_{2^t}, \\ &\mathrm{Tr}_\ell^t(ad + bc) = a\mathrm{Tr}_\ell^t(d) + c\mathrm{Tr}_\ell^t(b). \end{aligned} \tag{21}$$

Subcase (i): Let $\mathrm{Tr}_\ell^t(b) = 0$ and $\mathrm{Tr}_\ell^t(d) = 0$. The dimension of $\ker(\mathrm{Tr}_\ell^t)$ is $t - \ell$, where $\ker(\mathrm{Tr}_\ell^t) = \{x \in \mathbb{F}_{2^t} : \mathrm{Tr}_\ell^t(x) = 0\}$. Thus, d can be chosen in $2^{t-\ell} - 1$ ways and b in $2^{t-\ell} - 2$ ways. From (21), we get $\mathrm{Tr}_\ell^t(ad + bc) = 0$, so $\mathrm{Tr}_\ell^t(ad) = \mathrm{Tr}_\ell^t(cb) = \lambda \in \mathbb{F}_{2^\ell}$. For fixed b and d and for each $\lambda \in \mathbb{F}_{2^\ell}$, a and c both can be chosen in $2^{t-\ell}$ ways. Thus, the number of such distinct 2-dimensional subspaces is $\frac{2^{2t-\ell}(2^{t-\ell}-1)(2^{t-\ell-1}-1)}{3}$.

Subcase (*ii*): Let $\mathrm{Tr}_\ell^t(b) = 0$ but $\mathrm{Tr}_\ell^t(d) \neq 0$ or $\mathrm{Tr}_\ell^t(b) \neq 0$ but $\mathrm{Tr}_\ell^t(d) = 0$. Then, from (20), $b = 0$ or $d = 0$ respectively, which is impossible.
Subcase (*iii*): Let $\mathrm{Tr}_\ell^t(b) \neq 0$ and $\mathrm{Tr}_\ell^t(d) \neq 0$. From (20), we get

$$d = \frac{\mathrm{Tr}_\ell^t(d)}{\mathrm{Tr}_\ell^t(b)} b, \text{ that is, } d = \beta b, \text{ where } \beta = \frac{\mathrm{Tr}_\ell^t(d)}{\mathrm{Tr}_\ell^t(b)} \in \mathbb{F}_{2^\ell}^* \text{ and } \beta \neq 1.$$

For each $b \in \mathbb{F}_{2^t}^*$, d can be chosen in $2^\ell - 2$ ways. From (21), we get

$$\mathrm{Tr}_\ell^t(b(a\beta + c)) = (a\beta + c)\mathrm{Tr}_\ell^t(b). \tag{22}$$

Equation (22) has a solution if and only if $a\beta + c \in \mathbb{F}_{2^\ell}$, so, $c = a\beta + \beta_1$, where $\beta_1 \in \mathbb{F}_{2^\ell}$. Then for any fixed a, c can be chosen in 2^ℓ ways. Therefore the number of such 2-dimensional distinct subspaces is $\frac{2^{t+\ell}(2^t-1)(2^{\ell-1}-1)}{3}$. Adding all the cases we get our count. □

In what follows we demonstrate affine inequivalence among the cubic bent functions constructed above. To do this we use Theorem 7 proved in [11]. However, it is to be remembered that the use of the properties of higher-order derivatives to decide affine inequivalence between bent function was introduced by Dillon [9] way back in the seventies.

Remark 15. *Let $n = 2t$ be a fixed positive integer. In Theorem* 14*, we proved that the number of* 2*-dimensional subspaces with respect to which the second-order derivatives of g are constants depends on ℓ. Thus, for any fixed n, for different choices of ℓ the number of distinct* 2*-dimensional subspaces to constant second derivatives of the corresponding functions are different. Therefore, for any fixed n, for different choices of ℓ the corresponding cubic Maiorana-McFarland bent functions are affine inequivalent.*

Example 16. *Let $n = 30$. Then $t = 15$ and possible values of ℓ are* 3*,* 5*, and* 15*. If $\ell = 15$, then $k = 1$ and, the bent function corresponding to $\ell = 15$ has an affine derivative. Also from Table* 1*, we get the cubic bent functions corresponding to $\ell = 3$, $\ell = 5$ and $\ell = 15$ are mutually affine inequivalent.*

Let $n = 2t$, and $n_1(e)$ and $n_2(\ell)$ be the number of 2-dimensional subspaces of $\mathbb{F}_{2^t} \times \mathbb{F}_{2^t}$ on which the second-derivatives of f_i and g (defined as in (11) and (17), respectively) are constants. Then

$$n_1(e) = \frac{(2^t - 1)(2^{t+e-1}(2^e + 1) - (2^t + 1))}{3} \tag{23}$$

and

$$\begin{aligned} n_2(\ell) =& \frac{(2^t - 1)(2^{t+\ell}(2^{\ell-1} - 1) + 2^{t-1} - 1) + 2^{2t-\ell}(2^{t-\ell} - 1)(2^{t-\ell-1} - 1)}{3} \\ &+ 2^{t-1}((2^\ell - 1)(2^t - 1) + (2^t - 2^\ell)(2^{t-2\ell} - 1)). \end{aligned} \tag{24}$$

Lemma 17. *If $\ell \geq e$, then $n_2(\ell) > n_1(e)$, where $n_1(e)$ and $n_2(\ell)$ are defined as in* (23) *and* (24)*, respectively.*

Proof. We first compute the difference

$$\begin{aligned} n_2(\ell)-n_1(e) &= (2^\ell-1)2^{t-1}(2^t-1)+(2^t-2^\ell)2^{t-1}(2^{t-2\ell}-1) \\ &\quad -(2^t-1)2^{t-1}(2^e-1)+\frac{2^{2t-\ell}(2^{t-\ell}-1)(2^{t-\ell-1}-1)}{3} \\ &\quad +\frac{2^{t+\ell}(2^t-1)(2^{\ell-1}-1)}{3}-\frac{2^{t+e}(2^t-1)(2^{e-1}-1)}{3}. \end{aligned}$$

If $\ell = e$, then $\ell < t$ and $n_2(\ell) - n_1(e) > 0$. Again if $\ell > e$ then $n_2(\ell) - n_1(e) > 0$ since

$$(2^\ell-1)2^{t-1}(2^t-1)-(2^t-1)2^{t-1}(2^e-1) > 0$$

and

$$\frac{2^{t+\ell}(2^t-1)(2^{\ell-1}-1)}{3}-\frac{2^{t+e}(2^t-1)(2^{e-1}-1)}{3} > 0.$$

□

Corollary 18. *If $\ell \geq e$, then f_i and g are affine inequivalent, where f_i and g are defined as in* (11) *and* (17)*, respectively.*

We compare $n_1(e)$ and $n_2(\ell)$ in Table 1, for different values of n.

	$n=6$	$n=10$	$n=12$	$n=18$	
	$e=1;\ell=3$	$e=1;\ell=5$	$e=2;\ell=2$	$e=1;\ell=9$	$e=3;\ell=3$
$n_1(e)$	35	651	12075	174251	3052203
$n_2(\ell)$	651	174251	53675	11453115051	25287339

$n=20$		$n=30$	
$e=2;\ell=2$	$e=1;\ell=3$	$e=3;\ell=5$	$e=5;\ell=15$
3142315	879630115	12526594731	188614879915
2831415467	3775311936432811	6052134955691	192153583564270240

Table 1: The number of 2-dimensional subspaces on which the second-derivative of the cubic Maiorana-McFarland bent functions f and g are constants.

3 Conclusion

In this article, we prove that cubic Maiorana-McFarland bent functions which are constructed by using some known types of permutation polynomials (see [1, 13]) have no affine derivative. Consequently, we have obtained many affine inequivalent classes of bent function within the functions under consideration.

Acknowledgement: The authors thanks the anonymous referees and the editor for useful comments that has improved the technical and editorial quality of the article. Bimal Mandal thanks IIT Roorkee for the research grant.

References

[1] A. Blokhuis, R. S. Coulter, M. Henderson and C. M. O'Keefe, *Permutations amongst the Dembowski-Ostrom polynomials*, in: 1999 Finite Fields and Applications, Springer, 2001, pp. 37–42.

[2] A. Canteaut and P. Charpin, *Decomposing bent functions*, IEEE Trans. Inform. Theory 49 (8) (2003), 2004–2019.

[3] P. Camion, C. Carlet, P. Charpin, and N. Sendrier, *On Correlation-Immune Functions*, in Proc. CRYPTO, LNCS 576, Springer-Verlag, 1992, pp. 86–100.

[4] C. Carlet, *Two new classes of bent functions*, in: Proc. EUROCRYPT '93, LNCS vol. 765, Springer, 1994, pp. 77–101.

[5] C. Carlet, *Recursive lower bounds on the nonlinearity profile of Boolean functions and their applications*, IEEE Trans. Inform. Theory 54 (3) (2008), 1262–1272.

[6] P. Charpin and S. Sarkar, *Polynomials with Linear Structure and Maiorana–McFarland Construction*, IEEE Trans. Inform. Theory 57:6 (2011), 3796–3804.

[7] R. S. Coulter, *On the evaluation of a class of Weil sums in characteristic* 2, New Zealand J. Math. 28 (1999), 171–184.

[8] T. W. Cusick, P. Stănică, Cryptographic Boolean Functions and Applications, Academic Press, San Diego, CA, 2009.

[9] J. F. Dillon, *Elementary Hadamard difference sets*, in: Proceedings of 6th S. E. Conference on Combinatorics, Graph Theory, and Computing, Utility Mathematics, Winnipeg, 1975, pp. 237–249.

[10] S. Gangopadhyay, S. Sarkar and R. Telang, *On the lower bounds of the second order nonlinearities of some Boolean functions*, Information Sciences 180 (2010), 266–273.

[11] S. Gangopadhyay, *Affine inequivalence of cubic Maiorana-McFarland type bent functions*, Discrete Appl. Math. 161 (2013), 1141–1146.

[12] X.-D. Hou, *Cubic bent functions*, Discrete Math. 189 (1998), 149–161.

[13] Y. Laigle-Chapuy, *A note on a class of quadratic permutations over* $\mathbb{F}_{2^n}$, Proc. AECC 2007, LNCS 4851, pp. 130–137.

[14] F. J. MacWilliams and N. J. A. Sloane, The theory of error–correcting codes, North-Holland, Amsterdam, 1977.

[15] O. S. Rothaus, *On bent functions*, J. Combin. Theory – Series A, 20 (1976), 300–305.

[16] T. Siegenthaler, *Correlation-immunity of nonlinear combining functions for cryptographic applications*, IEEE Trans. Inf. Theory 30:5 (1984), 776–780.