Research Article

Class of Quadratic Almost Bent Functions That Is EA-Inequivalent to Permutations

Xinyang Zhang and Meng Zhou

School of Mathematics and Systems Science, Beihang University, No. 37, Xueyuan Road, Haidian District, Beijing 100191, China

Correspondence should be addressed to Xinyang Zhang; zhangxinyang99889@qq.com

Received 15 February 2017; Revised 9 April 2017; Accepted 11 April 2017; Published 13 August 2017

Academic Editor: Allan C. Peterson

Copyright © 2017 Xinyang Zhang and Meng Zhou. This is an open access article distributed under the Creative Commons Attribution License, which permits unrestricted use, distribution, and reproduction in any medium, provided the original work is properly cited.

The permutation relationship for the almost bent (AB) functions in the finite field is a significant issue. Li and Wang proved that a class of AB functions with algebraic degree 3 is extended affine- (EA-) inequivalent to any permutation. This study proves that another class of AB functions, which was developed in 2009, is EA-inequivalent to any permutation. This particular AB function is the first known quadratic class EA-inequivalent to permutation.

1. Introduction

Almost perfect nonlinear (APN) and almost bent (AB) functions and significant theoretical meanings have been extensively applied in finite field theory. The search for new APN (see Definition 1) and AB (which also implies APN property) functions has become an interesting topic. Power functions have six known classes of APN functions, namely, Gold [1], Kasami [2], Welch [3, 4], Niho [4], Inverse, and Dobbertin [5]. Apart from power functions, APN function also has several known classes. Accordingly, [6–11] show that all results are quadratic functions (the meaning of degree is a little different, see Definitions 2 and 3).

In the design of a block cipher, permutations over $F_{2^m}$ with an even $n$ are preferred due to hardware and software requirements. No APN permutation over $F_{2^m}$ with an even $n$ was determined until Dillon [12] in 2009. Thus, the Big APN problem emerged: Does such function exist? This problem is still open for $n \geq 8$. Berger et al. in [13] provided a significant solution for the Big APN problem: if the components of an APN function over $F_{2^m}$ with an even $n$ are plateaued, then a bent component exists, which is not permuted. This result is negative for quadratic functions because quadratic implies reaching a plateau [14]. If $F_{2^m}$ is changed by an odd $n$, then the plateaued APN functions are equal to the AB functions based on the result of [3]. The AB functions are conjectured to be EA-equivalent (see Definition 4) to the permutations. In 2013, Li and Wang [15] proved that the infinite class in [7] is EA-inequivalent to any permutation.

Definition 1. $F(x)$ is called almost perfect nonlinear (APN) function on $F_{2^n}$ if $D_1F(x) = F(x + a) - F(x)$ are 2–1 on $F_{2^n}$ (i.e., $D_1F(x) = D_2F(y)$ if and only if $x = y$ or $x + a = y$) for all $a \in F_{2^m} \setminus \{0\}$. Almost bent (AB) function is a kind of APN function.

Definition 2. Every mapping $F : F_{2^m} \rightarrow F_{2^n}$ can be unique represented in the form $F(x) = \sum_{i=0}^{2^m-1} a_i x^i$, called the algebraic normal form (ANF) of mapping $F$. ANF is zero (i.e., $a_i = 0$ for any $0 \leq i \leq 2^n - 1$) if and only if mapping is zero (i.e., $F(x) = 0$ for any $x$).

Definition 3. Every $0 \leq j \leq 2^n - 1$ is equal to an $n$ tuple $j_1 \cdots j_n \in \mathbb{Z}_2^n$ as $j = \sum_{k=1}^{n} j_k 2^{n-k}$, called the monomial of $j$. Integer $j$ and $n$ tuple $j_1 \cdots j_n$ will be regarded as the same from here. The degree of monomial $x^j$ on $F_{2^m}$ is not $j$ but the number of support $\text{supp}(j) = \{k : j_k \neq 0\}$, called the weight of $j$ and denoted as $wt(j)$. The degree of mapping $F : F_{2^n} \rightarrow F_{2^m}$ is $\deg F = \max\{wt(j) : a_i \neq 0\}$, the highest degree of all nonzero monomials in its ANF. For example, linear mappings on $F_{2^n}$ are in the form $L(x) = \sum_{i=0}^{n-1} l_i x^i$. Trace mapping $\text{tr}(x) = \sum_{i=0}^{n-1} x_i$ is a linear mapping only of values 0 or 1.
**Definition 4.** Two mappings \( F \) and \( F \) over \( F_{2^n} \) are called extended affine- (EA-) equivalent if there are affine permutations \( A_1, A_2, \) and \( A \) over \( F_{2^n} \) such that \( F^i \) = \( A_1 \circ F \circ A_2 + A \) and affine-equivalent if \( A = 0 \).

**2. Methods and Tools**

**Lemma 5.** \( F(x) \) over \( F_{2^n} \) is EA-equivalent to permutation if and only if there is a linear mapping \( L(x) \) such that \( F(x) + L(x) \) is permuted over \( F_{2^n} \).

**Proof.** If \( A_1 \circ F \circ A_2 + A \) is permuted, then \( A_1^{-1} \circ (A_1 \circ F \circ A_2 + A) \circ A_2^{-1} = F \) is also permuted over \( F_{2^n} \). \( A_1^{-1} \circ A \circ A_2^{-1} = \sum_{i=0}^{n-1} l_i x^i + c \) denotes that \( F(x) + \sum_{i=0}^{n-1} l_i x^i \), thereby permuted over \( F_{2^n} \).

Circulation and cycle are introduced to identify and combine similar terms in \( \text{tr}(\sum_{i=0}^{2^n-1} a_i x^i) \).

**Definition 6.** Consider the circulation mapping \( g : Z_2^n \rightarrow Z_2^n \) defined as \( g(j_1 j_2 \cdots j_n) = j_2 \cdots j_n j_1 \), which means \( 2^2 \) when \( j \leq 2^{n-1} - 1 \) or \( 2^{n-1} + 1 \) when \( j \geq 2^n \). \( g(j) : i \in Z \) is called the circulation orbit of \( j \) and its order \( |c(j)| = \min \{ i \in N^* : g(j) = j \} \) minimal positive period of \( j \).

The lemma below is obvious since \( \text{tr}(a_j x^i) \) and \( \text{tr}(a_j x^i) \) have no similar terms when \( i \neq c(j) \).

**Lemma 7.** \( \text{tr}(\sum_{i=0}^{2^n-1} a_i x^i) = 0 \) if and only if \( \text{tr}(\sum_{i \in c(j)} a_i x^i) = 0 \) for every \( 0 \leq j \leq 2^n - 1 \).

**3. Main Result and Proof**

If \( D\alpha F(x) = 0 \) has no solution for any \( a \in F_{2^n} \setminus \{0\} \), then \( F(x) \) is permuted. If \( a \) exists, such that \( a^T (Ax + b) = 1 \), then \( Ax + b \) has no solution based on linear algebra. If \( D\alpha F(x) \) is \( 2 - 1 \), then rank \( A = n - 1 \) and \( a \), which satisfies \( a^T A = 0 \), is unique. Furthermore, \( a \) satisfies \( a^T b = 1 \).

If \( \text{tr}(a^3) = 0 \), then \( \text{tr}(a^3 D\alpha x^3 + \text{tr}(x^3) + L(x)) = \text{tr}(a^3 L(a^{-1}) + 1) \). If \( \text{tr}(a^3 L(a^{-1})) = 0 \) when \( \text{tr}(a^3) = 0 \), then

\[
[\text{tr}(a^3) + 1] \text{tr}(a^3 L(a^{-1})) = 0 \quad \text{for any } a. \quad \text{Obviously, } L(x) = b^2 x + bx^3 \quad \text{and } L(x) = \text{tr}(bx) \text{ satisfy the identity. Theorem 8 will show that all kinds of } L(x) \text{ satisfying the identity are the adding of the two kinds above.}
\]

**Theorem 8.** One assumes that \( n \geq 9 \) and \( L(x) = \sum_{i=0}^{n-1} l_i x^i \) over \( F_{2^n} \). If \( \text{tr}(a^3) + 1 \text{ tr}(a^3 L(a^{-1})) = 0 \), then

\[
L(x) = (l_1 + b)^2 x + (l_1 + b) x^2 + \text{tr}(bx). \quad (1)
\]

**Proof.** Initially,

\[
\left( \text{tr}(a^3) + 1 \right) \text{tr}(a^3 L(a^{-1})) = \text{tr}(a^3 (\text{tr}(a^3) + 1) L(a^{-1})) = \text{tr} \left( \left( \sum_{i=0}^{n-1} a_i^3 (2^{i+1}) \right) + a^3 \right) L(a^{-1}). \quad (2)
\]

The exponents \( 3(2^i+1) + (-2^i) \) and \( 3(2^i) \) were added as minus for convenience can be divided into the following orbits:

\[
1: 3 - 2^0, 3 - 2^1, 3(2^0+1) - 2^1, 3(2^0+1) - 2^2, 3(2^1+1) - 2^3, 3(2^1+1) - 2^4, 3(2^1+1) - 2^5, 3(2^1+1) - 2^6, 3(2^1+1) - 2^7, 3(2^1+1) - 2^8, 3(2^1+1) - 2^9.
\]

The solutions are found by solving the linear equations generated by the orbits.

The following equations were formulated based on Lemma 7:

\[
\begin{align*}
1: & \quad l_1^1 + l_1 + l_1^4 + l_2^1 + l_2^4 + l_5 + l_5^1 + l_5^4 + l_5^2 = 0 \\
101 \cdots 1: & \quad l_j + l_{j+1}^1 + l_{j+2} + l_{j+2}^1 = 0 \quad (2 \leq j \leq n - 3) \\
101: & \quad l_{n-j} + l_{n-j}^1 + l_{n-j}^4 + l_{n-j}^2 + l_{j} = 0 \\
1011: & \quad l_{n-j}^1 + l_{n-j}^1 + l_{n-j}^4 + l_{n-j}^1 + l_{j} = 0 \\
100011: & \quad l_{n-j}^1 + l_{n-j}^1 + l_{n-j}^4 + l_{n-j}^1 + l_{j} = 0 \\
111: & \quad l_j + l_j^1 + l_j^4 + l_j^1 + l_j^4 + l_j^2 = 0 \\
10 \cdots 011: & \quad l_j + l_j^1 + l_j^4 + l_j^1 = 0 \quad (5 \leq i \leq n - 3) \\
101 \cdots 10 \cdots 011: & \quad l_i = 0 \quad (3 \leq i \leq n - 3, 2 \leq j \leq n - i).\end{align*}
\]
The last equation implies that $l_i = l_{i+1}^{j+1}$ for all $3 \leq i, j \leq n-1$. We let $b = l_1^{2}$; then $l_i = b^{2^i}$ for all $3 \leq i \leq n-1$.

We let $j = n-3$ in the second equation; thus, $l_{n-3} = l_1^{2^j} + l_{n-2}^{2^j} = l_{n-3}^{2^j}$. Therefore, $l_5 = b^8$.

Moreover, $l_{n-1} = b^{2^{j+1}}$ and $l_2 = b^4$ are substituted into the third equation; thus, $(l_0 + b)^{2^j} = l_1^{2^j} + b^4$.

Therefore, $L(x) = (l_1 + b^3)x^2 + (l_1 + b^3)x^2 + \text{tr}(bx)$.

$x^3 + \text{tr}(x^3) + L(x)$ cannot be permuted unless $L(x)$ is in the form $ax^2 + ax^2 + ax^2 + \text{tr}(bx)$ should be considered. If $y = x + a$, then it is equal to $x^3 + \text{tr}(y^3) + \text{tr}(by + a^3y + b^3y) + a^3 + \text{tr}(a^3 + ab)$, only different in a constant with $y^3 + \text{tr}(y^3) + \text{tr}(b^3y)$, in which $b^3 = b + a + a^3/8$.

**Theorem 9.** $x^3 + \text{tr}(x^3) + \text{tr}(bx)$ with $n \geq 5$ odd is not permuted.

Proof. $x^3$ is permuted on $F_2^n$ because $n$ is odd; its inverse is $x^3$ in which $\text{supp}(i) = \{1, 3, \ldots, n\}$. So the theorem is equal to $x + \text{tr}(x^3) + \text{tr}(bx)$ which is not permuted. There is $D_1(x + \text{tr}(x^3) + \text{tr}(bx^3)) = D_1(x + \text{tr}(bx^3)) = \text{tr}(b \sum_{i=\Lambda} x^{i})$, in which $\Lambda = \{0 \leq j \leq 2^n - 1 : \text{supp}(j) \subset \text{supp}(i)\}$.

Every $j$ with $j_1 = j_n = 1$ satisfies $i \notin \Lambda$ if $i \in \Lambda \setminus \{j\}$, which means $\text{tr}(bx^3)$ has no similar terms with $\text{tr}(bx^3)$; and $\text{tr}(j) = n$, which means the terms in $\text{tr}(bx^3)$ are not similar to each other. Since $j_1$ and $j_n$ will be adjacent after circulation, when $j_1 = j_n = 1$ there is $\Lambda \cap \text{tr}(j) = \{j\}$, which means $bx^3$ is not similar to other terms in $\text{tr}(b \sum_{j \in \Lambda} x^j)$. Thus ANF of $\text{tr}(b \sum_{j \in \Lambda} x^j)$ is not 1. According to Definitions 2 and 3, there exists $x \in F_2^n$ such that $\text{tr}(bx^3) = \text{tr}(bx(x+1)^3)$. However, $x + \text{tr}(x^3)$ is equal to $x + 1 + \text{tr}(x+1)^3$.

4. Conclusions

The AB class in [11] when $n \geq 9$ is EA-inequivalent to permutations. However, distinguishing whether the AB class is CCZ-equivalent to permutations is still unknown. Furthermore, the relationship of the permutations of the APN classes in [6, 8–10] and class with $\text{tr}_{m/n}$ in [7] is unknown. The solution to these problems will be a significant topic in algebra and cryptography in the future.

Conflicts of Interest

The authors declare that they have no conflicts of interest.

Acknowledgments

This work is partly supported by NSFC Project 11271040.

References


