Hindawi
Discrete Dynamics in Nature and Society
Volume 2017, Article ID 9627840, 3 pages
https://doi.org/10.1155/2017/9627840

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

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^n} with an even n are preferred due to hardware and software requirements. No APN permutation over F_{2^n} 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^n} 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^n} 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 $D_aF(x) = F(x + a) - F(x)$ are 2–1 on F_{2^n} (i.e., $D_aF(x) = D_aF(y)$ if and only if $x = y$ or $x + a = y$) for all $a \in F_{2^n} \setminus \{0\}$. Almost bent (AB) function is a kind of APN function.

Definition 2. Every mapping $F : F_{2^n} \to F_{2^n}$ can be unique represented in the form $F(x) = \sum_{i=0}^{2^n-1} a_i x^i$, 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 $j_1 \cdots j_n \in Z_2^n$ as $j = \sum_{k=1}^{n} j_k 2^{n-k}$, called the n bits binary representation 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^n} is not j itself but the number of support $\mathrm{supp}(j) = \{k : j_k \neq 0\}$, called the weight of j and denoted as $wt(j)$. The degree of mapping $F : F_{2^n} \to F_{2^n}$ is $\deg F = \max\{wt(i) : a_i \neq 0\}$, the highest degree of all nonzero monomials in its ANF. For example, linear mappings on F_{2^n} are in the form $L(x) = \sum_{i=0}^{n-1} l_i x^{2^i}$. Trace mapping $\mathrm{tr}(x) = \sum_{i=0}^{n-1} x^{2^i}$ 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 $F' = A_1 \circ F \circ A_2 + A$ 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 linear mapping $L(x)$ such that $F(x) + L(x)$ is permuted on F_{2^n}.*

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

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

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

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

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

3. Main Result and Proof

If $D_a F(x) = 0$ 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 $Ax + b = 0$ has no solution based on linear algebra. If $D_a F(x)$ 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 $\mathrm{tr}(a^3) = 0$, then $\mathrm{tr}(a^3 D_{a^{-1}}(x^3 + \mathrm{tr}(x^9) + L(x))) = \mathrm{tr}(a^3 L(a^{-1}) + 1)$. If $\mathrm{tr}(a^3 L(a^{-1})) = 0$ when $\mathrm{tr}(a^3) = 0$, then $[\mathrm{tr}(a^3) + 1]\,\mathrm{tr}(a^3 L(a^{-1})) = 0$ for any a. Obviously, $L(x) = b^2 x + bx^2$ and $L(x) = \mathrm{tr}(bx)$ satisfy the identity. Theorem 8 will show that all kinds of $L(x)$ satisfying the identity are the adding of the two kinds above.

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

$$L(x) = (l_1 + b)^2 x + (l_1 + b) x^2 + \mathrm{tr}(bx). \tag{1}$$

Proof. Initially,

$$\begin{aligned} &\left(\mathrm{tr}\left(a^3\right) + 1\right) \mathrm{tr}\left(a^3 L\left(a^{-1}\right)\right) \\ &\quad = \mathrm{tr}\left(a^3 \left(\mathrm{tr}\left(a^3\right) + 1\right) L\left(a^{-1}\right)\right) \\ &\quad = \mathrm{tr}\left(\left(\left(\sum_{i=0}^{n-1} a^{3(2^i+1)}\right) + a^3\right) L\left(a^{-1}\right)\right). \end{aligned} \tag{2}$$

The exponents $3(2^i+1)+(-2^j)$ and $3+(-2^j)$ (plus negative will be denoted as minus for convenience) can be divided into the following orbits:

1: $3-2^0, 3-2^1, 3(2^0+1)-2^1, 3(2^0+1)-2^2, 3(2^1+1)-2^0, 3(2^1+1)-2^3, 3(2^{n-1}+1)-2^2, 3(2^{n-1}+1)-2^{n-1}$.

$101\cdots1$: $3-2^j$ $(2 \le j \le n-1)$, $3(2^0+1)-2^j$ $(j = 0$ or $3 \le j \le n-1)$, $3(2^i+1)-2^j$ $(2 \le i \le n-2,\ j = i+2)$ or $j = i+2$ and 101 of $3(2^1+1)-2^2$ and $3(2^{n-1}+1)-2^1$ and 1011 of $3(2^3+1)-2^4$ and $3(2^{n-3}+1)-2^1$.

$10\cdots011$: $3(2^i+1)-2^j$ $(2 \le i \le n-2,\ j = 0, 1, i, i+1)$, 100011 of $3(2^1+1)-2^{n-2}$ and $3(2^{n-1}+1)-2^{n-3}$, 111 of $3(2^1+1)-2^1$ and $3(2^{n-1}+1)-2^0$.

$101\cdots10\cdots011$: $3(2^i+1)-2^j$, $4 \le i \le n-2$, $3 \le j \le i-1$ or $i+3 \le j \le n-1$.

$10001\cdots1$: $3(2^1+1)-2^j$ and $3(2^{n-1}+1)-2^j$ with j unequal to $n-2$ and $n-3$. The condition $n \ge 9$ can distinguish this class from 10100011. □

The following equations were formulated based on Lemma 7:

$$\begin{aligned}
1:&\quad l_0^{1/2} + l_1 + l_1^{1/4} + l_2^{1/2} + l_0^{1/8} + l_3 + l_{n-1}^{1/4} + l_2^2 = 0\\
101\cdots1:&\quad l_j + l_{j+1}^{1/2} + l_{j+2} + l_2^{2^j} = 0 \quad (2 \le j \le n-3)\\
101:&\quad l_{n-1} + l_0^{1/2} + l_2^{1/2} + l_1 = 0\\
1011:&\quad l_{n-2} + l_{n-1}^{1/2} + l_0 + l_2^{1/4} + l_4^{1/4} + l_1^2 = 0\\
100011:&\quad l_{n-2} + l_{n-3}^2 + l_4^{1/4} + l_0^4 + l_6^{1/4} + l_1^8 = 0\\
111:&\quad l_1 + l_0^2 + l_3 + l_1^4 + l_0^{1/2} + l_{n-2}^2 = 0\\
10\cdots011:&\quad l_3 + l_0^8 + l_5 + l_1^{16} = 0\\
&\quad l_i + l_0^{2^i} + l_{i+2} + l_1^{2^{i+1}} = 0 \quad (5 \le i \le n-3)\\
101\cdots10\cdots011:&\quad l_i = l_{n+i-j}^{2^j} = 0 \quad (3 \le i \le n-3,\ 2 \le j \le n-i-1).
\end{aligned} \tag{3}$$

The last equation implies that $l_i = l_j^{2^{i-j}}$ for all $3 \le i, j \le n-1$. We let $b = l_{n-1}^2$; then $l_i = b^{2^i}$ for all $3 \le i \le n-1$.

We let $j = n-3$ in the second equation; thus, $l_{n-3} + l_{n-2}^{1/2} + l_{n-1} + l_2^{2^{n-3}} = l_{n-1} + l_2^{2^{n-3}} = 0$. Therefore, $l_2 = b^4$.

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

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

$x^3 + \mathrm{tr}(x^9) + L(x)$ cannot be permuted unless $L(x)$ is in the form $ax^2 + a^2x + \mathrm{tr}(bx)$. Thus only $x^3 + \mathrm{tr}(x^9) + ax^2 + a^2x + \mathrm{tr}(bx)$ should be considered. If $y = x + a$, then it is equal to $y^3 + \mathrm{tr}(y^9) + \mathrm{tr}(by + a^8y + ay^8) + a^3 + \mathrm{tr}(a^9 + ab)$, only different in a constant with $y^3 + \mathrm{tr}(y^9) + \mathrm{tr}(b'y)$, in which $b' = b + a^8 + a^{1/8}$.

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

Proof. x^3 is permuted on F_{2^n} because n is odd; its inverse is x^t in which $\mathrm{supp}(t) = \{1, 3, \ldots, n\}$. So the theorem is equal to $x + \mathrm{tr}(x^3) + \mathrm{tr}(bx^t)$ which is not permuted. There is $D_1(x + \mathrm{tr}(x^3) + \mathrm{tr}(bx^t)) = D_1\,\mathrm{tr}(bx^t) = \mathrm{tr}(b\sum_{j\in\Lambda} x^j)$, in which $\Lambda = \{0 \le j \le 2^n - 1 : \mathrm{supp}(j) \subset \mathrm{supp}(t)\}$. Every j with $j_1 = j_n = 1$ satisfies $i \notin c(j)$ if $i \in \Lambda \setminus \{j\}$, which means $\mathrm{tr}(bx^j)$ has no similar terms with $\mathrm{tr}(bx^i)$; and $|c(j)| = n$, which means the terms in $\mathrm{tr}(bx^j)$ 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 $\Lambda \cap c(j) = \{j\}$, which means bx^j is not similar to other terms in $\mathrm{tr}(b\sum_{j\in\Lambda} x^j)$. Thus ANF of $\mathrm{tr}(b\sum_{j\in\Lambda} x^j)$ is not 1. According to Definitions 2 and 3, there exists $x \in F_{2^n}$ such that $\mathrm{tr}(bx^t) = \mathrm{tr}(b(x+1)^t)$. However, $x+\mathrm{tr}(x^3)$ is equal to $x+1+\mathrm{tr}(x+1)^3$. □

4. Conclusions

The AB class in [11] when $n \ge 9$ 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 $\mathrm{tr}_{m/n}$ 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

[1] R. Gold, "Maximal recursive sequences with 3-valued recursive cross-correlation functions (corresp.)," *IEEE Transactions on Information Theory*, vol. 14, no. 1, pp. 154–156, 1968.

[2] T. Kasami, "The weight enumerators for several classes of subcodes of the 2nd order binary Reed-Muller codes," *Information and Control*, vol. 18, no. 4, pp. 369–394, 1971.

[3] A. Canteaut, P. Charpin, and H. Dobbertin, "Binary m-sequences with three-valued crosscorrelation: a proof of Welch's conjecture," *IEEE Transactions on Information Theory*, vol. 46, no. 1, pp. 4–8, 2000.

[4] Y. Niho, *Multi-valued cross-correlation functions between two maximal linear recursive sequences [Ph.D. thesis]*, 1972.

[5] H. Dobbertin, "Almost perfect nonlinear power functions on GF(2^n): a new case for n Divisible by 5," in *Finite Fields and Applications*, pp. 113–121, Springer, Berlin, Germany, 2001.

[6] C. Bracken, E. Byrne, N. Markin, and G. McGuire, "New families of quadratic almost perfect nonlinear trinomials and multinomials," *Finite Fields and Their Applications*, vol. 14, no. 3, pp. 703–714, 2008.

[7] L. Budaghyan, C. Carlet, and A. Pott, "New classes of almost bent and almost perfect nonlinear polynomials," *IEEE Transactions on Information Theory*, vol. 52, no. 3, pp. 1141–1152, 2006.

[8] L. Budaghyan, C. Carlet, P. Felke, and G. Leander, "An infinite class of quadratic APN functions which are not equivalent to power mappings," in *Proceedings of the IEEE International Symposium on Information Theory (ISIT '06)*, pp. 2637–2641, Seattle, Wash, USA, July 2006.

[9] L. Budaghyan, C. Carlet, P. Felke, and G. Leander, "Another class of quadratic APN binomials over F_{2^n}: the case divisible by 4," in *Proceedings of the International Workshop on Coding and Cryptography (WCC '07)*, pp. 49–58, Versailles, France, 2007.

[10] L. Budaghyan and C. Carlet, "Classes of quadratic APN trinomials and hexanomials and related structures," *IEEE Transactions on Information Theory*, vol. 54, no. 5, pp. 2354–2357, 2008.

[11] L. Budaghyan, C. Carlet, and G. Leander, "Constructing new APN functions from known ones," *Finite Fields and Their Applications*, vol. 15, no. 2, pp. 150–159, 2009.

[12] J. Dillon, "APN polynomials: an update," http://maths.ucd.ie/~gmg/Fq9Talks/Dillon.pdf.

[13] T. P. Berger, A. Canteaut, P. Charpin, and Y. Laigle-Chapuy, "On almost perfect nonlinear functions over F_{2^n}," *IEEE Transactions on Information Theory*, vol. 52, no. 9, pp. 4160–4170, 2006.

[14] F. J. MacWilliams and N. J. Sloane, *The Theory of Error-Correcting Codes*, North Holland Publishing, Amsterdam, Netherlands, 1977.

[15] Y. Li and M. Wang, "The nonexistence of permutations EA-equivalent to certain AB functions," *IEEE Transactions on Information Theory*, vol. 59, no. 1, pp. 672–679, 2013.