On Affine (Non) Equivalence of Bent Functions

Sugata Gangopadhyay, Indian Institute of Technology, Roorkee

Joint work with Deepmala Sharma, Sumanta Sarkar and Subhamoy Maitra

Deciding "whether two Boolean functions are affine equivalent" is a very important question in Boolean function theory. Walsh spectra, autocorrelation spectra, algebraic degree are frequently used to partially solve this decision problem. However, the problem becomes even more difficult in the case of two bent functions having equal algebraic degree, since any two bent functions have same autocorrelation spectra and same Walsh spectra up to complementation. In this paper we construct an invariant to distinguish between two bent functions of the same degree. This invariant is the frequency distribution of a spectrum consisting of second derivatives of the function under consideration at all pairs of points which form a Gauss-Jordan basis of cardinality 2. First we present an efficient algorithm having $O(n2^{2n})$ time complexity to compute this spectrum. Using this invariant we show that there exist 6 and 8-variable bent functions which are not affine equivalent to rotation symmetric bent functions. Further, we use this invariant to show that there are at least six affine nonequivalent partial spreads bent functions on 8 variables. We come to this conclusion by evaluating the spectrum on the subclass consisting of all the PS^-_{ap} bent functions on 8 variables.

1. Basic Definitions

Let $\mathbb{F}_2$ be the prime field of characteristic 2 and $\mathbb{F}_2^n$ be the n dimensional vector space over $\mathbb{F}_2$. A function from $\mathbb{F}_2^n$ into $\mathbb{F}_2$ is called a Boolean function on n variables. The set of all such functions is denoted by $\mathcal{B}_n$. We denote the group of $n \times n$ invertible linear transformations over $\mathbb{F}_2$ by $GL(n, \mathbb{F}_2)$. Two Boolean functions f, $g \in \mathcal{B}_n$ are said to be affine equivalent if there exists $A \in GL(n, \mathbb{F}_2)$, $b, \lambda \in \mathbb{F}_2^n$ and $\epsilon \in \mathbb{F}_2$ such that $g(x) = f(Ax + b) + \lambda \cdot x + \epsilon$, where $\lambda \cdot x$ is the inner product of λ and x.

Let $a, b \in \mathbb{F}_2^n$ be two distinct nonzero elements such that $a = (z_{n-1}, \ldots, z_0)$, $b = (w_{n-1}, \ldots, w_0)$ respectively, where $z_i, w_i \in \mathbb{F}_2$ for all $i = 0, 1, \ldots n-1$. Suppose $z_{i_1} = z_{i_2} = \ldots = z_{i_r} = 1$ and $z_i = 0$ otherwise where $i_1 > i_2 > \ldots > i_r$. The elements a, b are said to form a Gauss-Jordan basis of cardinality 2 if and only if $w_i = 0$ for all $i \geq i_1$ and $z_j = 0$ where $j = \max\{i : w_i = 1\}$. Let $\mathcal{J}_2$ be the set of all distinct Gauss-Jordan bases of $\mathbb{F}_2^n$ of cardinality 2. It can be checked that the cardinality of $\mathcal{J}_2$, $|\mathcal{J}_2| = \frac{(2^n-1)(2^{n-1}-1)}{3}$. Clearly $|\mathcal{J}_2|$ is the number of all distinct two dimensional subspaces of $\mathbb{F}_2^n$.

The derivative of a function $f \in \mathcal{B}_n$ with respect to $a \in \mathbb{F}_2^n$ is defined as $D_a f(x) = f(x+a)+f(x)$, for all $x \in \mathbb{F}_2^n$. The second derivative at $a, b \in \mathbb{F}_2^n$ is $D_a D_b f(x) = f(x + a + b) + f(x + b) + f(x + a) + f(x)$ for all $x \in \mathbb{F}_2^n$.

2. Technical Results

Suppose $a, b \in \mathbb{F}_2^n$ and $f \in \mathcal{B}_n$. Let $S(f : a, b) = \sum_{x \in \mathbb{F}_2^n} D_a D_b f(x) = \sum_{x \in \mathbb{F}_2^n} (f(x + a + b) + f(x + b) + f(x + a) + f(x))$. Our main result is as follows which we present without proof due to space constraint.

Theorem. *The multiset* $[S(f : a, b) : \{a, b\} \in \mathcal{J}_2]$ *is invariant with respect to affine transformation on* f.

Proof. Suppose $f, g \in \mathcal{B}_n$ are affine equivalent functions. Then there exist $A \in GL(n, \mathbb{F}_2)$, $v, \lambda \in \mathbb{F}_2^n$ and $\epsilon \in \mathbb{F}_2$ such that $g(x) = f(Ax + v) + \lambda \cdot x + \epsilon$. Then for any $\{a, b\} \in \mathcal{J}_2$ we obtain,

$$\begin{aligned}
S(g : a, b) &= \sum_{x \in \mathbb{F}_2^n} (g(x + a + b) + g(x + b) + g(x + a) + g(x)) \\
&= \sum_{x \in \mathbb{F}_2^n} (f(A(x + a + b) + v) + \lambda \cdot (x + a + b) + \epsilon + f(A(x + b) + v) \\
&\quad + \lambda \cdot (x + b) + \epsilon + f(A(x + a) + v) + \lambda \cdot (x + a) + \epsilon + f(Ax + v) + \lambda \cdot x + \epsilon) \\
&= \sum_{x \in \mathbb{F}_2^n} (f(A(x + a + b) + v) + f(A(x + b) + v) + f(A(x + a) + v) + f(Ax + v)) \\
&= \sum_{x \in \mathbb{F}_2^n} (f((Ax + v) + Aa + Ab) + f((Ax + v) + Ab) + f((Ax + v) + Aa) + f(Ax + v)) \\
&= \sum_{x \in \mathbb{F}_2^n} (f(x + Aa + Ab) + f(x + Ab) + f(x + Aa) + f(x)) \\
&\quad \text{(since } x \mapsto Ax + v \text{ is bijective on } \mathbb{F}_2^n) \\
&= S(f : Aa, Ab) = S(f : Aa + Ab, Ab) = S(f : Aa, Aa + Ab).
\end{aligned}$$

It is to be noted that exactly one set among $\{Aa, Ab\}$, $\{Aa+Ab, Ab\}$ and $\{Aa, Aa+Ab\}$ is a Gauss-Jordan basis of cardinality 2. This implies the equality of the two multisets $[S(f : a, b) : \{a, b\} \in \mathcal{J}_2]$ and $[S(g : a, b) : \{a, b\} \in \mathcal{J}_2]$. □

Given a function $f \in \mathcal{B}_n$ we use the multiset $[S(f : a, b) : \{a, b\} \in \mathcal{J}_2]$ as a spectrum related to f. The sum $S(f : a, b) = \sum_{x \in \mathbb{F}_2^n} (D_a f(x + b) + D_a f(x)) = 2^{n-1} - \frac{1}{2} \sum_{x \in \mathbb{F}_2^n} (-1)^{D_a f(x+b) + D_a f(x)} = 2^{n-1} - \frac{1}{2} C_{D_a f}(b)$. Thus $[S(f : a, b) : \{a, b\} \in \mathcal{J}_2]$ can be computed as follows:

(1) For each $a \in \mathbb{F}_2^n$ construct the set $B_a = \{b : a, b \in \mathcal{J}_2\}$.
(2) For each $b \in B_a$ compute $C_{D_a f}(b)$ and $S(f : a, b) = 2^{n-1} - \frac{1}{2} C_{D_a f}(b)$.

The number of points in $\mathcal{J}_2$ is $O(2^{2n})$ and for each pair of points $\{a, b\}$, computing $S(f : a, b)$ has complexity $O(2^n)$. Therefore total complexity of the naive algorithm to compute the above spectrum is $O(2^{3n})$. Interestingly, using Fast Walsh Transform one can obtain a more efficient algorithm to compute this spectrum in $O(n2^{2n})$ time.

The computation from $[W_f^2(0), \ldots, W_f^2(2^n - 1)]$ to $[C_f(0), \ldots, C_f(2^n - 1)]$ can be done in $O(n2^n)$ time complexity by using Fast Walsh Transform due to the relationship $[C_f(0), \ldots, C_f(2^n - 1)] = 2^{-n}[W_f^2(0), \ldots, W_f^2(2^n - 1)]H_n$ obtained in [3]. Now we propose the following algorithm.

Algorithm 1
1. For $a \in \mathbb{F}_2^n$ compute $D_a f$.
2. Compute $[W_{D_a f}(0), \ldots, W_{D_a f}(2^n - 1)]$ by using Fast Walsh Transform.
3. Compute $[W_{D_a f}^2(0), \ldots, W_{D_a f}^2(2^n - 1)]$.
4. Compute $[C_{D_a f}(0), \ldots, C_{D_a f}(2^n - 1)]$ by using Fast Walsh Transform.
5. Repeat step 1 to 4 from each $a \in \mathbb{F}_2^n$.

The following table lists the time complexity of each step:

Step No.	1	2	3	4
Time complexity	$O(2^n)$	$O(n2^n)$	$O(2^n)$	$O(n2^n)$

The total complexity is $O((n + 1)2^{n+1})$. These four steps are to be repeated 2^n times. Therefore the time complexity of computing the spectrum is $O((n + 1)2^{2n+1})$.

3. Implication of our results

Rotation symmetric (RotS) bent functions have been studied extensively in literature (see [7] and the references therein). Experimental results show that there are varied types of bent functions in the rotation symmetric class. Thus there arises a natural question whether all the bent functions (at least on low dimensional spaces) are affine equivalent to rotation symmetric bent functions. By using our invariant we prove that even for n as low as 6 and 8 there exist bent functions which are not affine equivalent to any rotation symmetric bent.

Given $f \in \mathcal{B}_n$ compute the vector $\mathbf{P}(f) = (P_1(f), P_2(f), P_3(f)) \in \mathbb{Z} \times \mathbb{Z} \times \mathbb{Z}$, where $P_1(f)$ is the number of elements $\{a, b\} \in \mathcal{J}_2$ at which $S(f : a, b) = 0$, $P_2(f)$ is the number of elements

$\{a, b\} \in \mathcal{J}_2$ at which $S(f : a, b) = 2^n$ and $P_3(f)$ is the number of elements $\{a, b\} \in \mathcal{J}_2$ at which $0 < S(f : a, b) < 2^n$. We shall refer to $\mathbf{P}(f)$ as the P-vector of f. From the theorem proved above, it is clear that if $f, g \in \mathcal{B}_n$ are such that $\mathbf{P}(f) \neq \mathbf{P}(g)$ then f is not affine equivalent to g.

It is observed that the vector $(35, 56, 560)$ is not a P-vector for any RotS bent function on 6 variables. Thus no rotation symmetric bent function is affine equivalent to the bent function $x_1x_2x_3 \oplus x_2x_4x_5 \oplus x_1x_2 \oplus x_1x_4 \oplus x_2x_6 \oplus x_3x_5 \oplus x_4x_5$ whose P-vector is $(35, 56, 560)$.

Again we observe that the vectors $(651, 736, 9408)$ and $(203, 288, 10304)$ do not appear as a P-vector of any RotS cubic bent on 8 variables. This proves that no rotation symmetric 8-variable cubic bent function is affine equivalent to the bent functions $x_1x_2x_7 \oplus x_3x_4x_7 \oplus x_5x_6x_7 \oplus x_1x_4 \oplus x_3x_6 \oplus x_2x_5 \oplus x_4x_5 \oplus x_7x_8$ or $x_1x_2x_3 \oplus x_2x_4x_5 \oplus x_3x_4x_6 \oplus x_1x_4x_7 \oplus x_3x_5 \oplus x_2x_7 \oplus x_1x_5 \oplus x_1x_6 \oplus x_4x_8$ having P-vectors $(651, 736, 9408)$ and $(203, 288, 10304)$ respectively.

Next we consider the PS^-_{ap} bent functions on 8 variables. For details of PS_{ap} type bents we refer to [4, 5, 6]. It is to be noted that all these bent functions have algebraic degree 4 and algebraic immunity either 3 or 4. This makes them indistinguishable (in terms of affine nonequivalence) using algebraic degree. Two different values of algebraic immunity implies that there are at least two affinely nonequivalent classes if we consider transformations of the type $x \mapsto Ax + b$. However addition of an affine function can change the algebraic immunity by 1 [2]. Thus according to our definition of affine equivalence even this resolution may not be possible. The fastest algorithm to compute algebraic immunity has time complexity $\Omega(2^{2n})$, [1]. Since this algorithm requires solution of large system of linear equations the effective running time of this algorithm is more than the time required for computation of our spectrum. Thus by using the same amount of computation as algebraic immunity we are able to obtain a better distinguisher with respect to affine nonequivalence.

We generate all PS^-_{ap} bents on 8 variables and for each of them compute $[S(f : a, b) : \{a, b\} \in \mathcal{J}_2]$. It is observed that there are 6 distinct such multisets. This proves that there are at least 6 affinely non equivalent PS^-_{ap} (and hence PS) bent functions on 8 variables.

In the following table, the first row contains the possible values of $S(f : a, b)$ attained by these PS^-_{ap} bents. The remaining six rows correspond to the six different frequency distributions. The last column provides the number of functions corresponding to each of the six frequency distributions.

0	16	32	48	64	80	96	112	128	144	160	176	192	# of functions
0	0	0	0	0	0	940	2360	3885	2360	1220	0	30	8160
0	0	0	0	75	0	605	1760	5640	1600	1055	0	60	4080
0	0	0	0	0	0	750	2800	3360	2800	1080	0	5	2040
0	0	0	0	0	0	590	2280	4635	2440	850	0	0	8160
0	0	0	0	0	0	510	2440	4635	2280	930	0	0	1360
35	0	0	0	240	0	640	0	8760	0	640	0	480	510

TABLE 1. Classes of PS^-_{ap} bents on 8-variables that are not affinely equivalent.

REFERENCES

[1] F. Armknecht, C. Carlet, P. Gaborit, S. Künzli, W. Meier, O. Ruatta. Efficient Computation of Algebraic Immunity for Algebraic and Fast Algebraic Attacks. EUROCRYPT 2006, *Lecture Notes in Computer Science* Vol. 4004 (2006) 147-164.

[2] A. Braeken, Y. Borisov, S. Nikova, B. Preneel. Classification of Boolean Functions of 6 Variables or Less with Respect to Cryptographic Properties. International Colloquium on Automata, Languages and Programming ICALP 2005, *Lecture Notes in Computer Science* Vol. 3580, Springer-Verlag, p. 324-334, 2005.

[3] C. Carlet. Partially bent functions. Crypto'92, *Lecture Notes in Computer Science* Vol. 740 (1994) 280 - 291.

[4] C. Carlet. Two new classes of bent functions. Eurocrypt'93, *Lecture Notes in Computer Science* Vol. 765 (1994) 77 - 101.

[5] J. F. Dillon. Elementary Hadamard Difference sets. PhD Thesis, University of Maryland, 1974.

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

[7] S. Kavut, S. Maitra, M. D. Yucel. Search for Boolean Functions with Excellent Profiles in the Rotation Symmetric Class. In IEEE Transactions on Information Theory, 53(5): 1743-1751, May 2007.