On second-order nonlinearities of some $\mathcal{D}_0$ type bent functions

Sugata Gangopadhyay
(Joint work with Brajesh Kumar Singh)

Department of Mathematics, Indian Institute of Technology Roorkee
gsugata@gmail.com

Central European Conference on Cryptology
Bedlewo, Poland
June 10–12, 2010

Boolean functions

- A Boolean function f on n variables is a mapping :

$$f : \{0,1\}^n \rightarrow \{0,1\}.$$

- Boolean function can be represented by a truth table.

$$f : \{0,1\}^4 \rightarrow \{0,1\}$$

x_4	x_3	x_2	x_1	f
0	0	0	0	0
0	0	0	1	1
0	0	1	0	1
0	0	1	1	1
0	1	0	0	1
0	1	0	1	1
0	1	1	0	0
0	1	1	1	0
1	0	0	0	0
1	0	0	1	0
1	0	1	0	0
1	0	1	1	0
1	1	0	0	0
1	1	0	1	0
1	1	1	0	0
1	1	1	1	0

- Also represented by the 2^n-length string $[f(0), f(1), \ldots, f(2^n - 1)]$
- The number of all n-variable Boolean functions is 2^{2^n}.

Boolean functions

- Let $\mathbb{F}_2$ be the prime field of characteristic 2.
- A Boolean function f is a function from $\mathbb{F}_2^n$ to $\mathbb{F}_2$.
- Alternatively Boolean functions can be thought of as functions from $\mathbb{F}_{2^n}$ to $\mathbb{F}_2$.
- Let $\mathcal{B}_n$ be the set of all Boolean functions on n variables.

Algebraic Normal Form (ANF)

- The algebraic normal form (ANF) of $f \in \mathcal{B}_n$ is

$$f(x_1, x_2, \ldots, x_n) = \sum_{a=(a_1,\ldots,a_n)\in\mathbb{F}_2^n} \mu_a \left(\prod_{i=1}^{n} x_i^{a_i}\right),$$

  where $\mu_a \in \mathbb{F}_2$.
- The algebraic degree of f,
  $\deg(f) := \max\{wt(a) : \mu_a \neq 0, a \in \mathbb{F}_2^n\}$.

Nonlinearity

- $dist : \mathcal{B}_n \times \mathcal{B}_n \longrightarrow \mathbb{Z}$ defined by $dist(f, g) = |\{x \in \mathbb{F}_2^n : f(x) \neq g(x)\}|$, for all $f, g \in \mathcal{B}_n$, is said to be the Hamming distance between f and g.
- Nonlinearity of $f \in \mathcal{B}_n$ is defined as $nl(f) = \min_{l \in \mathcal{A}_n}\{dist(f, l)\}$ where $\mathcal{A}_n$ is the set of affine functions on n variables.
- Alternatively the nonlinearity of f is its distance from $RM(1, n)$, the Reed-Muller code of order 1 and size 2^n.

Nonlinearity and Walsh Transformation

- The Walsh transform $f \in \mathcal{B}_n$ at $\lambda \in \mathbb{F}_2^n$ is defined as follows:

$$W_f(\lambda) = \sum_{x \in \mathbb{F}_2^n} (-1)^{f(x)+\lambda \cdot x}.$$

- $$nl(f) = 2^{n-1} - \frac{1}{2} \max_{\lambda \in \mathbb{F}_{2n}} |W_f(\lambda)|.$$

  It is to be noted that the Walsh spectrum of $f \in \mathcal{B}_n$ can be computed in time $O(n2^n)$ and hence the nonlinearity.

Upper bound of nonlinearity

- Parseval's identity

$$\sum_{\lambda \in \mathbb{F}_{2^n}} W_f(\lambda)^2 = 2^{2n}$$

- $|W_f(\lambda)| \geq 2^{n/2}$, which implies $nl(f) \leq 2^{n-1} - 2^{\frac{n}{2}-1}$.

Bent functions: functions with maximum nonlinearity

- A Boolean function $f \in \mathcal{B}_n$, where n is even is said to be bent if and only if $|W_f(\lambda)| = 2^{n/2}$ for all $\lambda \in \mathbb{F}_2^n$.
- From this it follows that bent functions have maximum nonlinearity namely $2^{n-1} - 2^{\frac{n}{2}-1}$ for even n.

Nonlinearity to nonlinearity profile

- Suppose f is a Boolean function on n variables. For every non-negative integer $r \leq n$, we denote by $nl_r(f)$ the rth-order nonlinearity of f, which is the minimum Hamming distance of f and all functions of algebraic degree at most r.
- Alternatively the rth-order nonlinearity of an n variable Boolean function f is its distance from $RM(r, n)$, the r order Reed-Muller code of size 2^n.
- The sequence of values $nl_r(f)$, for r ranging from 1 to $n - 1$, is said to be the nonlinearity profile of f.
- Unlike the first-order nonlinearity there is no fast algorithm to determine second or higher-order nonlinearities.

Lower bounds on nonlinearity profile

- (Carlet 2008) C. Carlet, Recursive lower bounds on the nonlinearity profile of Boolean functions and their applications, IEEE Trans. Inform. Theory 54 (3) (2008) 1262-1272.
- (Fouquet and Tavernier 2008) R. Fourquet and C. Tavernier, An improved list decoding algorithm for the second order Reed-Muller codes and its applications, Des. Codes Cryptotogr. 49 (2008) 323-340.

Derivatives of Boolean function

- The derivative of $f \in \mathcal{B}_n$ with respect to $a \in \mathbb{F}_2^n$ is defined by

$$D_a f(x) := f(x) + f(x + a)$$

- The rth-order derivative of f with respect to V is defined by

$$D_V f(x) := D_{a_1} \dots D_{a_r} f(x)$$

Where V be an r-dimensional subspace of $\mathbb{F}_2^n$ generated by $a_1, \dots, a_r$.

Proposition 2 (Carlet 2008)

- Let f be n variable Boolean function and r be a positive integer smaller than n, then we have

$$nl_r(f) \geq \frac{1}{2} \max_{a \in \mathbb{F}_2^n} nl_{r-1}(D_a f)$$

- In particular, for $r = 2$

$$nl_2(f) \geq \frac{1}{2} \max_{a \in \mathbb{F}_2^n} nl(D_a f).$$

Proposition 3 and Corollary 2 (Carlet 2008)

- Let f be any n variable Boolean function and r be a positive integer smaller than n, Then we have $nl_r(f) \geq 2^{n-1} - \frac{1}{2}\sqrt{2^{2n} - 2\sum_{a\in\mathbb{F}_2^n} nl_{r-1}(D_a f)}$.
- Let f be any n variable function and r a positive integer smaller than n. Assume that, for some nonnegative integers M and m, we have $nl_{r-1}(D_a f) \geq 2^{n-1} - M2^m$ for every nonzero $a \in \mathbb{F}_2^n$. Then

$$
\begin{aligned}
nl_r(f) &\geq 2^{n-1} - \frac{1}{2}\sqrt{(2^n-1)M2^{m+1} + 2^n} \\
&\approx 2^{n-1} - \sqrt{M}2^{\frac{n+m-1}{2}}
\end{aligned}
\quad (1)
$$

Quadratic Boolean functions

- Suppose $g \in \mathcal{B}_n$ is a quadratic function. The bilinear form associated with g is defined by $B(x, y) = g(0) + g(x) + g(y) + g(x + y)$.
- The kernel of $B(x, y)$ is the subspace of $\mathbb{F}_2^n$ defined by

$$\mathcal{E}_g = \{x \in \mathbb{F}_2^n : B(x, y) = 0 \text{ for all } y \in \mathbb{F}_2^n\}.$$

Quadratic Boolean functions

- Suppose $g \in \mathcal{B}_n$ is a quadratic function. The kernel of $B(x, y)$
$$\mathcal{E}_g = \{a \in \mathbb{F}_2^n : D_a g = \text{ constant } \}.$$
- A. Canteaut, P. Charpin and G. M. Kyureghyan, A new class of monomial bent functions, Finite Fields and their Applications 14 (2008) 221-241.

Walsh spectrum of quadratic Boolean functions

If $g : \mathbb{F}_2^n \to \mathbb{F}_2$ is a quadratic boolean function and $B(x, y)$ is the quadratic form associated to it, then the Walsh Spectrum of g depends only on the dimension, k, of the kernel, $\mathcal{E}_g$, of $B(x, y)$. The weight distribution of the Walsh spectrum of g is:

$W_g(\mu)$	number of μ
0	$2^n - 2^{n-k}$
$2^{(n+k)/2}$	$2^{n-k-1} + (-1)^{f(0)} 2^{(n-k-2)/2}$
$-2^{(n+k)/2}$	$2^{n-k-1} - (-1)^{f(0)} 2^{(n-k-2)/2}$

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

Lower bounds of second-order nonlinearities of cubic Boolean functions

- If f is a cubic Boolean function the $D_a f$ is at most quadratic.
- It possible to get good estimates of the nonlinearities of $D_a f$ for all $a \in \mathbb{F}_2^n$ to obtain estimates of the lower bounds of second-order nonlinearities of cubic Boolean functions.
- This technique is used in several recent papers for cubic bent functions.

Lower bounds of second-order nonlinearities of cubic Boolean functions

- If $f(x,y) = Tr_1^p(xy^{2^i+1})$, where $x, y \in \mathbb{F}_{2^p}, n = 2p, n \geq 6$ and i is an integer such that $1 \leq i < p$, $\gcd(2^p - 1, 2^i + 1) = 1$ and $\gcd(i, p) = e$, then

$$nl_2(f) \geq 2^{n-1} - \frac{1}{2}\sqrt{2^{(\frac{3n}{2}+e)} - 2^{(\frac{3n}{4}+\frac{e}{2})} + 2^n(2^{(\frac{n}{4}+\frac{e}{2})} - 2^e + 1)}.$$

- 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.

Lower bounds of second-order nonlinearities of cubic Boolean functions

$n = 2p$	6	10	12
i	$1, 2$	$1, 2, 3, 4$	$2, 4$
$e = \gcd(i, p)$	1	1	2
Lower bounds in (Gangopadhyay et al.)	15	378	1524
Hamming distances in (Fourquet et al.)	18	400	1760

Construction $\mathcal{D}_0$ type bent functions

- Let $n = 2p$, π is a permutation on $\mathbb{F}_2^p$. $f(x, y) = \pi(y) \cdot x$ is a Maiorana-McFarland type bent.
- Following is the $\mathcal{D}_0$ type bent constructed by Carlet:

$$h(x, y) = x \cdot \pi(y) + \prod_{j=1}^{p}(x_j + 1)$$

  where$x = (x_1, \ldots, x_n)$
- C. Carlet, Two new classes of bent functions, in Proc. EUROCRYPT '93, LNCS vol. 765, Springer, 1994, pp. 77-101.

Walsh transforms of derivatives of $\mathcal{D}_0$ type bent functions

Let $h(x,y) = f(x,y) + g(x)$, where $n = 2p$, $x, y \in \mathbb{F}_2^p$, $f(x,y) = x \cdot \pi(y)$, $g(x) = \prod_{i=1}^{p}(x_i + 1)$ and π is a permutation on $\mathbb{F}_2^p$ then

- The Walsh transform of $D_{(a,b)}h$ at $(\mu, \eta) \in \mathbb{F}_2^p \times \mathbb{F}_2^p$ is

$$W_{D_{(a,b)}h}(\mu,\eta) = W_{D_{(a,b)}f}(\mu,\eta) - 2[(-1)^{\mu\cdot a} + (-1)^{\eta\cdot b}]W_{a\cdot\pi}(\eta)$$

- $|W_{D_{(a,b)}h}(\mu,\eta)| \le |W_{D_{(a,b)}f}(\mu,\eta)| + 4|W_{a\cdot\pi}(\eta)|$.

Proof outline

Let $h(x,y) = f(x,y) + g(x)$, $g(x) = \prod_{i=1}^{p}(x_i + 1)$ and $(a,b) \in \mathbb{F}_2^p \times \mathbb{F}_2^p$, with $a \neq 0$. Then

$$g(x) + g(x+a) = \begin{cases} 1, & \text{if } (x,y) \in (\{0\} \times \mathbb{F}_2^p) \bigcup (\{a\} \times \mathbb{F}_2^p), \\ 0, & \text{otherwise .} \end{cases}$$

The Walsh transform of $D_{(a,b)}h$ at $(\mu,\eta) \in \mathbb{F}_2^p \times \mathbb{F}_2^p$ is

$$\begin{aligned} W_{D_{(a,b)}h}(\mu,\eta) &= \sum_{(x,y)\in\mathbb{F}_2^p\times\mathbb{F}_2^p} (-1)^{f(x+a,y+b)+f(x,y)+g(x+a)+g(x)+\mu\cdot x+\eta\cdot y} \\ &= \sum_{(x,y)\in\mathbb{F}_2^p\times\mathbb{F}_2^p} (-1)^{f(x+a,y+b)+f(x,y)+\mu\cdot x+\eta\cdot y} \\ &- 2 \sum_{(x,y)\in\{0,a\}\times\mathbb{F}_2^p} (-1)^{f(x+a,y+b)+f(x,y)+\mu\cdot x+\eta\cdot y} \end{aligned}$$

Proof outline

$$= W_{D_{(a,b)}f}(\mu,\eta) - 2[\sum_{y\in\mathbb{F}_2^p}(-1)^{f(0,y+b)+f(a,y)+\mu\cdot a+\eta\cdot y}$$

$$+ \sum_{y\in\mathbb{F}_2^p}(-1)^{f(a,y+b)+f(0,y)+\eta\cdot y}]$$

$$= W_{D_{(a,b)}f}(\mu,\eta) - 2[(-1)^{\mu\cdot a}\sum_{y\in\mathbb{F}_2^p}(-1)^{a\cdot\pi(y)+\eta\cdot y}$$

$$+ (-1)^{\eta\cdot b}\sum_{y\in\mathbb{F}_2^p}(-1)^{a\cdot\pi(y+b)+\eta\cdot(y+b)}]$$

$$= W_{D_{(a,b)}f}(\mu,\eta) - 2[(-1)^{\mu\cdot a} + (-1)^{\eta\cdot b}]W_{a\cdot\pi}(\eta)$$

Thus, $\mid W_{D_{(a,b)}h}(\mu,\eta) \mid \leq \mid W_{D_{(a,b)}f}(\mu,\eta) \mid + 4 \mid W_{a\cdot\pi}(\eta) \mid$

Main Theorem

Let $h(x,y) = tr_1^p(xy^{2^i+1}) + \prod_{i=1}^{p}(x_i+1)$, where $n = 2p$, $x, y \in \mathbb{F}_2^p$, i is integer such that $1 \leq i \leq p$, $\gcd(2^i+1, 2^p-1) = 1$, and $\gcd(i,p) = e$, then

$$nl_2(h) \geq 2^{2p-1} - \frac{1}{2}\sqrt{2^{3p+e} + 2^{2p}(1-2^e) + 5(2^{\frac{5p+e}{2}} - 2^{\frac{3p+e}{2}})}.$$

Proof outline

Let $h(x,y) = tr_1^p(xy^{2^i+1}) + \prod_{i=1}^{p}(x_i+1)$, where $n = 2p$, $x, y \in \mathbb{F}_2^p$, i is integer such that $1 \leq i \leq p$, $\gcd(2^i+1, 2^p-1) = 1$, and $\gcd(i,p) = e$, then nonlinearity of $D_{(a,b)}h$ is

$$nl(D_{(a,b)}h) \geq \begin{cases} 2^{2p-1} - 2^{p+e-1}, & \text{if } a = 0 \text{ and } b \neq 0, \\ 2^{2p-1} - 2^{p+e-1} - 2^{\frac{p+e+2}{2}}, & \text{if } a \neq 0 \text{ and } b \neq 0, \\ 2^{2p-1} - 2^{\frac{3p+e-2}{2}} - 2^{\frac{p+e+2}{2}}, & \text{if } a \neq 0 \text{ and } b = 0. \end{cases}$$

Proof outline

- $$\sum_{(a,b)\in\mathbb{F}_{2^p}\times\mathbb{F}_{2^p}} nl(D_{(a,b)}h)$$
  $$\geq (2^p-1)(2^{2p-1}-2^{p+e-1})+(2^p-1)(2^{2p-1}-2^{\frac{3p+e-2}{2}}-2^{\frac{p+e+2}{2}})$$
  $$+(2^p-1)(2^p-1)(2^{2p-1}-2^{p+e-1}-2^{\frac{p+e+2}{2}})$$
  $$=2^{4p-1}-2^{3p+e-1}-2^{2p-1}(1-2^e)-5(2^{\frac{5p+e-2}{2}}-2^{\frac{3p+e-2}{2}})$$
- $$nl_2(h)\geq 2^{n-1}-\frac{1}{2}\sqrt{2^{2n}-2\sum_{(a,b)\in\mathbb{F}_2^p\times\mathbb{F}_2^p} nl(D_{(a,b)}h)}.$$

Comparisons

$n = 2p$	6	10	12
i	$1, 2$	$1, 2, 3, 4$	$2, 4$
$e = \gcd(i, p)$	1	1	2
Lower bounds in (Gangopadhyay et al.)	15	378	1524
Hamming distances in (Fourquet et al.)	18	400	1760
Lower bounds of D_0 type considered	10	351	1466

Another class of functions

- Let $h(x, y) = tr_1^p(x(y^{2^{m+1}+1} + y^3 + y)) + \prod_{i=1}^p (x_i + 1)$, where $n = 2p$, $x, y \in \mathbb{F}_2^p$, m is integer such that $p = 2m + 1$, then

$$nl_2(h) \geq 2^{2p-1} - \frac{1}{2}\sqrt{2^{3p+2} - 3 \cdot 2^{2p} + 5 \cdot (2^{\frac{5p+3}{2}} - 2^{\frac{3p+3}{2}})}.$$

- S. Sarkar and S. Gangopadhyay, On the Second Order Nonlinearity of a Cubic Maiorana-McFarland Bent Function, Finite Fields and their Applications, Fq 9, Dublin, Ireland, July 13-17, 2009.

Conclusions

- We identify a class of bent functions, with maximum algebraic degree, having good second order nonlinearity.
- Finding out bounds of the nonlinearity profile of these functions is an open question.

Acknowledgements

- The authors thank Projet SECRET, INRIA - Rocquencourt for travel support to present this paper.
- Brajesh Kumar Singh's research is supported by Council for Scientific and Industrial Research India.

THANK YOU

QUESTIONS PLEASE