SHANGHAI JIAO TONG UNIVERSITY

SCHOOL OF ELECTRONIC INFORMATION AND ELECTRICAL ENGINEERING

Higher order nonlinearity of bent functions

Zhaole Li

2022/11/1

Boolean functions

- We call n-variable Boolean functions or Boolean functions in dimension n the functions from the n-dimensional vector space $\mathbb{F}_2^n$ over $\mathbb{F}_2$ to $\mathbb{F}_2$.
- Their set is denoted by $\mathcal{B}_n$, where n is the number of variables of Boolean functions.
- Given a basis, the field $\mathbb{F}_{2^n}$ can be identified with the vector space $\mathbb{F}_2^n$. Thus the input of Boolean functions will also be considered in the field $\mathbb{F}_{2^n}$.

- Truth Table:

x_1	x_2	x_3	$f(x)$
0	0	0	0
0	0	1	1
0	1	0	0
0	1	1	0
1	0	0	0
1	0	1	1
1	1	0	0
1	1	1	1

corresponding to 3-variable Boolean function $f(x_1, x_2, x_3) = x_1x_2x_3 + x_2x_3 + x_3$ in ANF.

- Algebraic Normal Form:

$$f(x_1, \ldots, x_n) = \bigoplus_{I \subseteq \{1,\ldots,n\}} a_I \left(\prod_{i \in I} x_i \right).$$

- Univariate Representation:

$$f(x) = \sum_{i=0}^{2^n-1} \delta_i x^i.$$

Definition

Let $F = \mathbb{F}_{2^m}$, $K = \mathbb{F}_{2^n}$ where $m \mid n$. We may view F as a subfield of K. If α is an element of K, its trace relative to the subfield F is defined as follows:

$$\mathrm{tr}_F^K(\alpha) = \alpha + \alpha^{2^m} + \alpha^{2^{2m}} + \cdots + \alpha^{2^{\frac{n}{m}-1}m}.$$

When no confusion is likely to arise, we will simply write the trace function as $\mathrm{tr}_m^n(\alpha)$.

Remark:

Trace function tr_m^n is a F-linear tranformation from K onto F and is balanced.

Definition

We call the Walsh transform of a Boolean function f the Fourier transform of the function $(-1)^{f(x)}$, and we denote it by W_f:

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

Definition

The Hamming distance between $f, g \in \mathcal{B}_n$ is given by

$$d_H(f,g) = |\{x \in \mathbb{F}_2^n | f(x) \neq g(x)\}|.$$

Definition (Algebraic Degree)

The degree of Boolean function f is denoted by $deg(f)$ and is called the algebraic degree of the function: $deg(f) = \max\{|I| : a_I \neq 0\}$, where $|I|$ denotes the size of I.

Example

$f = x_1x_2x_3 + x_2x_3 + x_3$ is a 3-variable Boolean function over $\mathbb{F}_2^n$ with $deg(f) = 3$. The Hamming distance between f and $g = x_3$ is 1.

Remark:

The Hamming distance between Boolean function f and affine function $l_a = a \cdot x$ equals

$$d_H(f, l_a) = 2^{n-1} - \frac{W_f(a)}{2}.$$

The rth-order nonlinearity for Boolean functions

The rth-order nonlinearity is an important parameter of a Boolean function f:

Definition (rth-order Nonlinearity)

The rth-order nonlinearity of f is defined as the minimum Hamming distance from f to all the functions of algebraic degrees at most r:

$$nl_r(f) = \min_{g \in \mathcal{B}_n, deg(g) \leq r} d_h(f, g).$$

Remark:

The first-order nonlinearity of f is usually called the nonlinearity of f and is denoted by $nl(f)$. The nonlinearity can be computed through the Walsh transform:

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

Assume $k \geq 3$, we are aimed to give a lower bound on the third-order nonlinearity of the simplest $\mathcal{PS}$ bent function

$$f(x,y) = \mathrm{tr}_1^k\left(\frac{\lambda x}{y}\right) \tag{1}$$

where $(x,y) \in \mathbb{F}_{2^k}^2$, $\lambda \in \mathbb{F}_{2^k}^*$, $\mathrm{tr}_1^k(x) = \sum_{i=0}^{n-1} x^{2^i}$ is the trace function from $\mathbb{F}_{2^k}$ to $\mathbb{F}_2$ and $\frac{x}{y}$ is defined to be 0 if $y = 0$.

The Walsh transform of the second-order derivative

Let us consider the Walsh transform of the second-order derivative of f at points $\alpha=(\alpha_1,\alpha_2),\beta=(\beta_1,\beta_2)\in\mathbb{F}_{2^k}^2$.
We have

$$
\begin{aligned}
&W_{D_\beta D_\alpha f}(\mu,\nu)\\
&=\sum_{x\in\mathbb{F}_{2^k}}\sum_{y\in\mathbb{F}_{2^k}}(-1)^{\mathrm{tr}_1^k\left(\frac{\lambda x}{y}+\frac{\lambda(x+\alpha_1)}{y+\alpha_2}+\frac{\lambda(x+\beta_1)}{y+\beta_2}+\frac{\lambda(x+\alpha_1+\beta_1)}{y+\alpha_2+\beta_2}+\mu x+\nu y\right)}\\
&=\sum_{y\in\mathbb{F}_{2^k}}(-1)^{\mathrm{tr}_1^k\left(\frac{\lambda\alpha_1}{y+\alpha_2}+\frac{\lambda\beta_1}{y+\beta_2}+\frac{\lambda(\alpha_1+\beta_1)}{y+\alpha_2+\beta_2}+\nu y\right)}\\
&\quad\times\sum_{x\in\mathbb{F}_{2^k}}(-1)^{\mathrm{tr}_1^k\left(\left(\frac{\lambda}{y}+\frac{\lambda}{y+\alpha_2}+\frac{\lambda}{y+\beta_2}+\frac{\lambda}{y+\alpha_2+\beta_2}+\mu\right)x\right)}\\
&=\begin{cases}2^k\sum_{y\in S}(-1)^{\mathrm{tr}_1^k\left(\frac{\lambda\alpha_1}{y+\alpha_2}+\frac{\lambda\beta_1}{y+\beta_2}+\frac{\lambda(\alpha_1+\beta_1)}{y+\alpha_2+\beta_2}+\nu y\right)}, & \text{if } \frac{\lambda}{y}+\frac{\lambda}{y+\alpha_2}+\frac{\lambda}{y+\beta_2}+\frac{\lambda}{y+\alpha_2+\beta_2}=\mu \text{ has sol}\\ 0, & \text{otherwise.}\end{cases}
\end{aligned}
$$

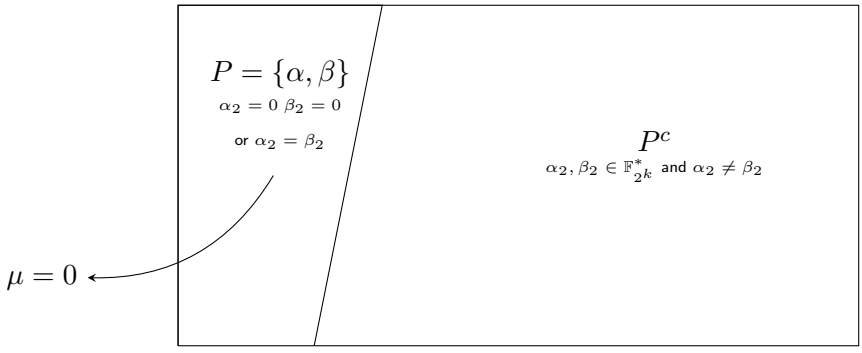
The solutions of the equation

Consider the solutions of the equation:

$$\frac{\lambda}{y}+\frac{\lambda}{y+\alpha_2}+\frac{\lambda}{y+\beta_2}+\frac{\lambda}{y+\alpha_2+\beta_2}=\mu. \tag{2}$$

- If $\alpha_2=\beta_2$ or $\alpha_2=0$ or $\beta_2=0$, then equation (**??**) has 0 solution when $\mu\neq 0$ and has 2^k solutions otherwise;
- If $\alpha_2,\beta_2\in\mathbb{F}_{2^k}^*,\ \alpha_2\neq\beta_2$, then equation (**??**) has $0,4$ or 8 solutions.

The partition of α, β



Partition based on α and β

The solutions of the equation

Consider the solutions of the equation:

$$\frac{\lambda}{y}+\frac{\lambda}{y+\alpha_2}+\frac{\lambda}{y+\beta_2}+\frac{\lambda}{y+\alpha_2+\beta_2}=\mu. \tag{2}$$

If $\alpha_2,\beta_2\in\mathbb{F}_{2^k}^*,\ \alpha_2\neq\beta_2$:

- If $\{0,\alpha_2,\beta_2,\alpha_2+\beta_2\}$ are solutions of (**??**), then we have a condition:

$$\lambda(\alpha_2^2+\beta_2^2+\alpha_2\beta_2)+\mu(\alpha_2^2\beta_2+\alpha_2\beta_2^2)=0. \tag{3}$$

- If $\{y_0,y_0+\alpha_2,y_0+\beta_2,y_0+\alpha_2+\beta_2\}$ are solutions of (**??**), then we have a condition:

$$\mu\neq 0,\mathrm{tr}_1^k\left(\frac{\lambda\alpha_2}{\mu\beta_2(\alpha_2+\beta_2)}\right)=0 \text{ and } \mathrm{tr}_1^k\left(\frac{\lambda\beta_2}{\mu\alpha_2(\alpha_2+\beta_2)}\right)=0. \tag{4}$$

The solutions of the equation

- Note that we can always find

$$\mu = \frac{\lambda(\alpha_2^2 + \beta_2^2 + \alpha_2\beta_2)}{\alpha_2^2\beta_2 + \alpha_2\beta_2^2}$$

satisfying condition (**??**) for α_2, β_2, leading to at least 4 solutions for equation (**??**).

- Thus, for all points $\alpha = (\alpha_1, \alpha_2), \beta = (\beta_1, \beta_2) \in \mathbb{F}_{2^k}^2$ such that $\alpha_2, \beta_2 \in \mathbb{F}_{2^k}^*$ and $\alpha_2 \neq \beta_2$, there always exist (μ, ν) such that

$$W_{D_\beta D_\alpha f}(\mu, \nu) = 2^k \sum_{y \in S} (-1)^{\mathrm{tr}_1^k\left(\frac{\lambda\alpha_1}{y+\alpha_2} + \frac{\lambda\beta_1}{y+\beta_2} + \frac{\lambda(\alpha_1+\beta_1)}{y+\alpha_2+\beta_2} + \nu y\right)}$$

where $\{0, \alpha_2, \beta_2, \alpha_2 + \beta_2\} \subseteq S$.

The solutions of the equation

- For all points $\alpha = (\alpha_1, \alpha_2), \beta = (\beta_1, \beta_2) \in \mathbb{F}_{2^k}$ such that $\alpha_2, \beta_2 \in \mathbb{F}_{2^k}^*$ and $\alpha_2 \neq \beta_2$, when condition (**??**) holds true, μ is determined, thus we can check whether condition (**??**) is true or false:
  - If condition (**??**) is false, then

$$S = \{0, \alpha_2, \beta_2, \alpha_2 + \beta_2\}.$$

  - If condition (**??**) is true, then

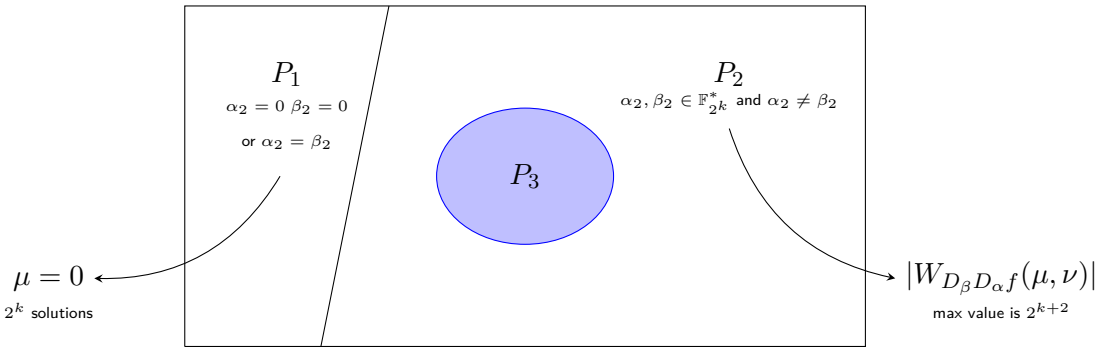
$$S = \{0, \alpha_2, \beta_2, \alpha_2 + \beta_2, y_0, y_0 + \alpha_2, y_0 + \beta_2, y_0 + \alpha_2 + \beta_2\}.$$

- If $S = \{0, \alpha_2, \beta_2, \alpha_2 + \beta_2\}$, we have

$$W_{D_\beta D_\alpha f}(\mu, \nu) = \begin{cases} 2^{k+2} \cdot (-1)^{f^*}, \text{if } \operatorname{tr}_1^k(\mu\alpha_1 + \nu\alpha_2) = 0 \text{ and } \operatorname{tr}_1^k(\mu\beta_1 + \nu\beta_2) = 0 \\ 0, \text{ otherwise.} \end{cases}$$

where $f^* = \operatorname{tr}_1^k\left(\frac{\lambda\alpha_1}{y'+\alpha_2} + \frac{\lambda\beta_1}{y'+\beta_2} + \frac{\lambda(\alpha_1+\beta_1)}{y'+\alpha_2+\beta_2} + \nu y'\right)$ and $y' \in S$.
Note that we always have $v \in \mathbb{F}_{2^k}$ such that $\operatorname{tr}_1^k(\mu\alpha_1 + \nu\alpha_2) = 0$ and $\operatorname{tr}_1^k(\mu\beta_1 + \nu\beta_2) = 0$ by Lemma (**??**), so we conclude $\max_{\mu,\nu} |W_{D_\beta D_\alpha f}(\mu, \nu)| = 2^{k+2}$ for all points $\alpha = (\alpha_1, \alpha_2), \beta = (\beta_1, \beta_2) \in \mathbb{F}_{2^k}^2$ such that $\alpha_2, \beta_2 \in \mathbb{F}_{2^k}^*$, $\alpha_2 \neq \beta_2$ and $S = \{0, \alpha_2, \beta_2, \alpha_2 + \beta_2\}$.

The partition of α, β



Partition based on α and β

- If $S = \{0, \alpha_2, \beta_2, \alpha_2+\beta_2, y_0, y_0+\alpha_2, y_0+\beta_2, y_0+\alpha_2+\beta_2\}$, we have

$$W_{D_\beta D_\alpha f}(\mu,\nu) = \begin{cases} 2^{k+3}\cdot(-1)^{f_0^{**}}, \text{if } \mathrm{tr}_1^k(\mu\alpha_1+\nu\alpha_2)=0, \mathrm{tr}_1^k(\mu\beta_1+\nu\beta_2)=0 \text{ and } f_0^{**}+f_1^{**}=0 \\ 0, \text{ otherwise.} \end{cases}$$

where $f_0^{**}+f_1^{**} = \mathrm{tr}_1^k\left(\frac{\lambda\alpha_1}{\alpha_2}+\frac{\lambda\beta_1}{\beta_2}+\frac{\lambda(\alpha_1+\beta_1)}{\alpha_2+\beta_2}+\frac{\lambda\alpha_1}{y+\alpha_2}+\frac{\lambda\beta_1}{y+\beta_2}+\frac{\lambda(\alpha_1+\beta_1)}{y+\alpha_2+\beta_2}+\nu y\right)$ and $y \in \{y_0, y_0+\alpha_2, y_0+\beta_2, y_0+\alpha_2+\beta_2\}$.

We need to prove two things:

- There exists $\mu \in \mathbb{F}_{2^k}$ such that S has 8 elements, i.e. condition (**??**) and (**??**) are both true.
- And there exists $\nu \in \mathbb{F}_{2^k}$ satisfying

$$\begin{cases} \mathrm{tr}_1^k(\mu\alpha_1 + \nu\alpha_2) = 0 \\ \mathrm{tr}_1^k(\mu\beta_1 + \nu\beta_2) = 0 \\ f_0^{**} + f_1^{**} = 0. \end{cases} \tag{5}$$

- Since we will always find $\mu = \frac{\lambda(\alpha_2^2+\beta_2^2+\alpha_2\beta_2)}{\alpha_2^2\beta_2+\alpha_2\beta_2^2} \in \mathbb{F}_{2^k}^*$ making condition (**??**) true, we take μ into condition (**??**) to get

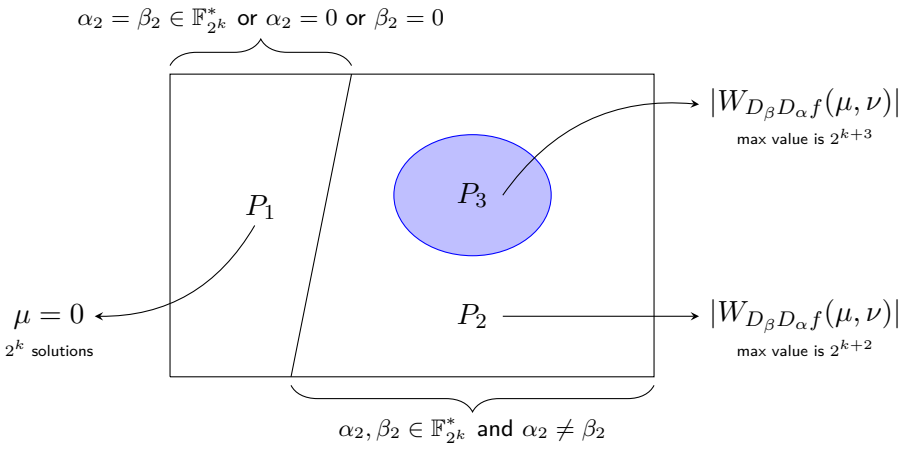
$$\begin{cases} \mathrm{tr}_1^k\left(\dfrac{1}{\gamma^2+\gamma+1}\right) = 0 \\ \mathrm{tr}_1^k\left(\dfrac{\gamma^2}{\gamma^2+\gamma+1}\right) = 0. \end{cases} \qquad (*)$$

  where $\gamma = \frac{\beta_2}{\alpha_2} \in \mathbb{F}_{2^k} \setminus \mathbb{F}_4$.

- According to Lemma (**??**), the number of $\gamma = \frac{\beta_2}{\alpha_2}$ satisfying equations above is L.

- According to Lemma (**??**), there always exist $\nu \in \mathbb{F}_{2^k}$ that equations (**??**) hold true, which means:
  - There always exist (μ, ν) s.t. $\max_{\mu,\nu} |W_{D_\beta D_\alpha f}(\mu, \nu)| = 2^{k+3}$ for all points $\alpha = (\alpha_1, \alpha_2), \beta = (\beta_1, \beta_2) \in \mathbb{F}_{2^k}^2$ such that $\alpha_2, \beta_2 \in \mathbb{F}_{2^k}^*$, $\alpha_2 \neq \beta_2$ and $\gamma = \frac{\beta_2}{\alpha_2}$ satisfies equation (**??**).
  - Therefore, we can always find (μ, ν) s.t. $\max_{\mu,\nu} |W_{D_\beta D_\alpha f}(\mu, \nu)| = 2^{k+2}$ with $\alpha_2, \beta_2 \in \mathbb{F}_{2^k}^*, \alpha_2 \neq \beta_2$ and $\gamma = \frac{\beta_2}{\alpha_2}$ in other cases.

Figure: The partition of α, β



Conclusion

For every points $\alpha = (\alpha_1, \alpha_2) \in \mathbb{F}_{2^k} \times \mathbb{F}_{2^k}^*$, there exist L different β_2 contributing to $|W_{D_\beta D_\alpha f}(\mu, \nu)| = 2^{k+3}$, $2^k - 2 - L$ different β_2 leading to $|W_{D_\beta D_\alpha f}(\mu, \nu)| = 2^{k+2}$, while β_1 can be any element of $\mathbb{F}_{2^k}$.
Thus, for all points $\alpha = (\alpha_1, \alpha_2), \beta = (\beta_1, \beta_2) \in \mathbb{F}_{2^k} \times \mathbb{F}_{2^k}^*$ with $\alpha_2 \neq \beta_2$,

Lemma

Lemma

Assume $k \geq 2$, let $N_{i,j} = \left|\left\{x \in \mathbb{F}_{2^k} \middle| \mathrm{tr}_1^k(\theta_1 x + \gamma_1) = i, \mathrm{tr}_1^k(\theta_2 x + \gamma_2) = j\right\}\right|$ where $\gamma_1, \gamma_2 \in \mathbb{F}_{2^k}$ and $\theta_1, \theta_2 \in \mathbb{F}_{2^k}^*$ are distinct, then $N_{0,0} = 2^{k-2}$.

Proof.

We have $N_{0,0} + N_{0,1} + N_{1,0} + N_{1,1} = 2^k$ and $N_{0,0} + N_{0,1} = 2^{k-1}$, $N_{1,1} + N_{0,1} = 2^{k-1}$, then we get $N_{0,0} = N_{1,1}$. Besides,
$N_{0,0} + N_{1,1} = \left|\left\{x \in \mathbb{F}_{2^k} \middle| \mathrm{tr}_1^k((\theta_1 + \theta_2)x + (\gamma_1 + \gamma_2)) = 0\right\}\right| = 2^{k-1}$ since $\theta_1 \neq \theta_2$.
Therefore $N_{0,0} = 2^{k-2}$. □

Lemma

Assume $k \geq 3$, *let*
$N_{i_1,i_2,i_3} = \left|\left\{x \in \mathbb{F}_{2^k} \middle| \mathrm{tr}_1^k(\theta_1 x + \gamma_1) = i_1, \mathrm{tr}_1^k(\theta_2 x + \gamma_2) = i_2, \mathrm{tr}_1^k(\theta_3 x + \gamma_3) = i_3\right\}\right|$,
where $\gamma_1, \gamma_2, \gamma_3 \in \mathbb{F}_{2^k}$ *and* $\theta_1, \theta_2, \theta_3 \in \mathbb{F}_{2^k}^*$ *are distinct and satisfy* $\theta_3 \neq \theta_1 + \theta_2$. *Then* $N_{0,0,0} = 2^{k-3}$.

Proof.

The equations

$$\begin{cases} N_{0,0,0} + N_{0,0,1} = 2^{k-2} \\ N_{0,0,0} + N_{0,1,0} = 2^{k-2} \\ N_{0,0,0} + N_{1,0,0} = 2^{k-2}. \end{cases} \tag{6}$$

will lead to $N_{0,0,1} = N_{0,1,0} = N_{1,0,0}$. With the same reason we also obtain $N_{0,1,1} = N_{1,0,1} = N_{1,1,0}$.

Because $\theta_1 + \theta_2 + \theta_3 \neq 0$, we can get equations:

$$\begin{aligned} & N_{1,0,1} + N_{1,1,0} + N_{0,1,1} + N_{0,0,0} \\ =& \left| \left\{ x \in \mathbb{F}_{2^k} \middle| \mathrm{tr}_1^k \left((\theta_1 + \theta_2 + \theta_3) x + (\gamma_1 + \gamma_2 + \gamma_3) \right) = 0 \right\} \right| \\ =& 2^{k-1}. \end{aligned} \tag{7}$$

Proof.

Combine $N_{0,0,1} = N_{0,1,0} = N_{1,0,0}$, $N_{0,1,1} = N_{1,0,1} = N_{1,1,0}$, equations (**??**) with equations $N_{0,0,0} + N_{0,0,1} + N_{0,1,0} + N_{0,1,1} = 2^{k-1}$, we obtain the result $N_{0,0,1} = N_{0,1,1}$. Therefore from equations (**??**) and equations (**??**) we have

$$\begin{cases} N_{0,0,0} + N_{0,0,1} = 2^{k-2} \\ N_{0,0,0} + 3N_{0,0,1} = 2^{k-1}. \end{cases} \tag{8}$$

and the solution is $N_{0,0,0} = N_{0,0,1} = 2^{k-3}$. □

SHANGHAI JIAO TONG UNIVERSITY

Thank You

Zhaole Li · Higher order nonlinearity of bent functions