Constructions of n-variable balanced Boolean functions with maximum absolute value in autocorrelation spectra $< 2^{\frac{n}{2}}$

Deng Tang

Southwest Jiaotong University, Chengdu, China

(Joint work with Subhamoy Maitra, Selçuk Kavut, and Bimal Mandal)

June 19, 2018, Norway

Outline

1. Preliminaries
2. Balanced functions with low absolute indicator derived from $\mathcal{PS}_{ap}$ bent functions
3. Balanced functions with low absolute indicator derived from M-M bent functions

Outline

1. **Preliminaries**
2. Balanced functions with low absolute indicator derived from $\mathcal{PS}_{ap}$ bent functions
3. Balanced functions with low absolute indicator derived from M-M bent functions

Notations

- Let $\mathbb{F}_2^n$ be the n-dimensional vector space over $\mathbb{F}_2 = \{0, 1\}$.
- Let $\mathbb{F}_{2^n}$ be the finite field of order 2^n.
- The support $\mathrm{supp}(a)$ of a vector $a = (a_1, \cdots, a_n) \in \mathbb{F}_2^n$ is defined as the set $\{1 \le i \le n \,|\, a_i \ne 0\}$.
- The Hamming weight of $a \in \mathbb{F}_2^n$ is $\mathrm{wt}(a) = |\mathrm{supp}(a)|$.
- The Hamming distance between two vectors $a, b \in \mathbb{F}_2^n$ is defined as $d_H(a, b) = |\{1 \le i \le n \,|\, a_i \ne b_i\}|$.

Boolean function over $\mathbb{F}_2^n$

Definition

Any mapping from $\mathbb{F}_2^n$ into $\mathbb{F}_2$ is call a Boolean function in n variables.

- $\mathcal{B}_n$ denotes the set of all the n-variable Boolean functions.
- $|\mathcal{B}_n| = 2^{2^n}$ ($2^{2^7} \approx 10^{38}$; constructions are necessary!)
- Any $f \in \mathcal{B}_n$ can be represented by its truth table $f = \left[f(0,\ldots,0,0), f(0,\ldots,0,1),\ldots, f(1,\ldots,1,1)\right]$.
- $f \in \mathcal{B}_n$ is said to be balanced if $\mathrm{wt}(f) = 2^{n-1}$.

Boolean function over $\mathbb{F}_2^n$ (continued)

Definition

Any $f \in \mathcal{B}_n$ can be represented by its algebraic normal form

$$f(x_1, \cdots, x_n) = \bigoplus_{u \in \mathbb{F}_2^n} a_u x^u,$$

where $a_u \in \mathbb{F}_2$ and the term $x^u = \prod_{j=1}^{n} x_j^{u_j}$ is called a monomial.

- The algebraic degree $\deg(f)$ is the maximal value of $w_H(u)$ such that $a_u \neq 0$, and f is called an *affine function* if $\deg(f) \leq 1$.
- For any balanced function $f \in \mathcal{B}_n$, we have $\deg(f) \leq n - 1$.

Boolean function over $\mathbb{F}_{2^n}$

Definition

Any Boolean function in n variables can be defined over $\mathbb{F}_{2^n}$ and uniquely expressed by an univariate polynomial over $\mathbb{F}_{2^n}[x]/(x^{2^n} - x)$

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

where $f^2(x) \equiv f(x) \pmod{x^{2^n} - x}$.

- The algebraic degree under univariate polynomial representation is equal to $\max\{w_H(\bar{i}) \mid f_i \neq 0, 0 \leq i < 2^n\}$, where $\bar{i}$ is the binary expansion of i.

Boolean function over $\mathbb{F}_{2^k}^2$

Definition

Any Boolean function of $2k$ variables can be viewed over $\mathbb{F}_{2^k}^2$ and uniquely expressed by a bivariate polynomial

$$f(x,y) = \sum_{i,j=0}^{2^k-1} f_{i,j} x^i y^j,$$

where f is such that $f(x,y)^2 \equiv f(x,y) \pmod{x^{2^k} - x, y^{2^k} - y}$.

- The algebraic degree in this case is equal to $\max\{w_H(\bar{i}) + w_H(\bar{j}) \mid f_{i,j} \neq 0\}$.

Nonlinearity

Definition

The rth-order nonlinearity of $f \in \mathcal{B}_n$ is defined as its minimum Hamming distance from f to all the n-variable Boolean functions of degree at most r

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

- The first-order nonlinearity of f is simply called the *nonlinearity* of f and is denoted by $nl(f)$.
- The nonlinearity $nl(f)$ is the minimum Hamming distance between f and all the affine functions.
- The sequence $[nl(f), nl_2(f), nl_3(f), \ldots, nl_{n-1}(f)]$ is called the nonlinearity profile of f.

Walsh transform

Definition

The Walsh transform of an n-variable Boolean function f at point $a \in \mathbb{F}_2^n$ is defined as

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

- Over $\mathbb{F}_{2^n}$, the Walsh transform of the Boolean function f at $\alpha \in \mathbb{F}_{2^n}$ can be defined by

$$W_f(\alpha) = \sum_{x \in \mathbb{F}_{2^n}} (-1)^{f(x)+\mathrm{Tr}_1^n(\alpha x)},$$

  where $\mathrm{Tr}_1^n(x) = \sum_{i=0}^{n-1} x^{2^i}$ is the trace function from $\mathbb{F}_{2^n}$ to $\mathbb{F}_2$.
- Over $\mathbb{F}_{2^k}^2$, the Walsh transform at $(\alpha, \beta) \in \mathbb{F}_{2^k} \times \mathbb{F}_{2^k}$ can be defined by

$$W_f(\alpha, \beta) = \sum_{(x,y) \in \mathbb{F}_{2^k} \times \mathbb{F}_{2^k}} (-1)^{f(x,y)+\mathrm{Tr}_1^k(\alpha x+\beta y)}.$$

Compute the nonlinearity

The nonlinearity of a Boolean function $f \in \mathcal{B}_n$ can be computed as

$$
\begin{aligned}
nl(f) &= 2^{n-1} - \frac{1}{2}\max_{a \in \mathbb{F}_2^n} |W_f(a)| \\
&= 2^{n-1} - \frac{1}{2}\max_{\omega \in \mathbb{F}_{2^n}} |W_f(\omega)| \\
&= 2^{n-1} - \frac{1}{2}\max_{(\alpha,\beta) \in \mathbb{F}_{2^{n/2}} \times \mathbb{F}_{2^{n/2}}} |W_f(\alpha,\beta)| \text{ if } n \text{ is even.}
\end{aligned}
$$

Parseval's equality

Parseval's equality

For any Boolean function f on $\mathbb{F}_2^n$,

$$\sum_{u\in\mathbb{F}_2^n} W_f^2(u) = 2^{2n}.$$

- We can deduce that $\max_{u\in\mathbb{F}_2^n} |W_f(u)| \geq 2^{\frac{n}{2}}$ and so $nl(f) \leq 2^{n-1} - 2^{\frac{n}{2}-1}$.
- If $W_f(u) \in \{2^{n/2}, -2^{n/2}\}$ for all $u \in \mathbb{F}_2^n$, then f is called bent.
- For odd n, if $W_f(u) \in \{0, \pm 2^{(n+1)/2}\}$ for all $u \in \mathbb{F}_2^n$, then f is a semi-bent function.

Autocorrelation properties

Definition

The derivative function of any $f \in \mathcal{B}_n$ at a point $\alpha \in \mathbb{F}_2^n$ is defined by

$$D_\alpha f = f(x) + f(x+\alpha).$$

And its autocorrelation function at a point $\beta \in \mathbb{F}_2^n$ is defined by

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

SAC [Webster-Tavares, CRYPTO 1985]

A Boolean function $f \in \mathcal{B}_n$ is said to satisfy strict avalanche criterion (SAC) if

$$C_f(\alpha) = 0 \text{ for all } w_H(\alpha) = 1.$$

Autocorrelation properties (continued)

GAC [Zhang-Zheng, J.UCS 1996]

The global avalanche characteristics (GAC) includes two indicators: the absolute indicator and the sum-of-squares indicator. For any $f \in \mathcal{B}_n$, the absolute indicator is defined as follows

$$\Delta_f = \max_{a \neq 0} |C_f(a)|$$

and the sum-of-squares indicator is defined as follows

$$\sigma_f = \sum_{a \in \mathbb{F}_2^n} C_f^2(a).$$

- Bent functions have the best absolute indicator 0.

Open problems on nonlinearity profile

The nonlinearity profile of Boolean functions relates to the confusion in cryptography, the covering radius of $\mathrm{RM}(r, n)$ and Kerdock codes in coding theory, and Gowers norm.

- The maximal higher-order nonlinearities are open for large variables.
- When $n \geq 8$ is even, bent functions have the largest nonlinearity and the maximal nonlinearity for balanced functions is open.
- When $n \geq 9$ is odd, the maximal nonlinearity is open.

Zhang-Zheng Conjecture on Δ_f

Zhang-Zheng Conjecture [J.UCS 1996]

The absolute indicator of any balanced Boolean function f of algebraic degree no less than 3 is lower-bounded by $2^{\lfloor \frac{n+1}{2} \rfloor}$.

Some counterexamples on Zhang-Zheng Conjecture

- In [Maitra-Sarkar, IEEE TIT 2002], they computed that the Patterson-Wiedemann has $\Delta_f = 160 < 2^{(15+1)/2}$ and obtained a balanced function with $\Delta_f = 216 < 2^{(15+1)/2}$.
- In [Burnett et. al., AJC 2006], three 14-variable balanced functions with $\Delta_f = 104 < 2^{14/2}$ or $\Delta_f = 112 < 2^{14/2}$ have been found.
- In [Gangopadhyay-Keskar-Maitra, DM 2006], a 21-variable function with $\Delta_f < 2^{11}$ has been found (corrected in [Kavut, 2016 DAM]).
- In [Maitra-Sarkar, IEEE TIT 2007], a 9-variable function with $\Delta_f = 24$, a 10-variable function with $\Delta_f = 24$, and two 11-variable functions with $\Delta_f = 56 < 2^{(11+1)/2}$ have been found.
- In [Kavut, 2016 DAM], twenty 21-variable functions with $\Delta_f < 2^{11}$ has been found.

The applications of the autocorrelation function

1. Functions with low absolute indicator can provide diffusion to stream ciphers and S-boxes.
2. Functions with high absolute indicator are weak to cube attacks [Dinur-Shamir, FSE 2011].
3. Functions with high absolute indicator are weak to differential fault attack [Banik-Maitra-Sarkar, CHES 2012].
4. The autocorrelation function can be used to deduce lower bound on higher-order nonlinearity [Carlet, IEEE TIT 2008].
5. The nonlinearity of quadratic functions can be determined by the autocorrelation functions.
6. The number of codewords with weight 3 in punctured Hamming code relies on the autocorrelation function of well-chosen functions.
7. The number of repair sets of many classes of binary locally repairable codes with locality two depends on the autocorrelation function of well-chosen functions.

Outline

1. Preliminaries
2. Balanced functions with low absolute indicator derived from $\mathcal{PS}_{ap}$ bent functions
3. Balanced functions with low absolute indicator derived from M-M bent functions

$\mathcal{PS}_{ap}$ bent function

$\mathcal{PS}_{ap}$ bent function [Dillon's thesis, 1974]

A partial spread affine plane ($\mathcal{PS}_{ap}$) bent function $f(x, y) \in \mathcal{B}_{2k}$ from $\mathbb{F}_{2^{2k}}$ to $\mathbb{F}_2$ is defined as

$$f(x, y) = g(xy^{2^k-2}),$$

where g is a balanced function over $\mathbb{F}_{2^k}$ with $g(0) = 0$.

- Points of $\mathbf{PG}(1, \mathbb{F}_{2^k})$ over $\mathbb{F}_{2^k}$
- Desarguesian spread
- Disjoint k-dimensional subspaces

Boolean functions with very low maximum absolute value

Construction 1 [Tang-Maitra, IEEE TIT 2018]

Let $n = 2k$ and $\lambda, \mu \in \mathbb{F}_{2^k}^*$, where $k \geq 9$ is an odd integer. We construct an n-variable Boolean function over $\mathbb{F}_{2^n}$ as follows

$$f(x,y) = \begin{cases} h_0(y), & \text{if } x = 0 \\ h_1(y), & \text{if } x = \mu \\ s(x,y), & \text{if } x \neq 0 \text{ and } x \neq \mu \end{cases},$$

where $s(x,y) = \mathrm{Tr}_1^k(\frac{\lambda x}{y})$ and h_0, h_1 are two well-chosen functions over $\mathbb{F}_2^k$.

Conditions on h_0, h_1

Theorem [Kavut-Maitra-Tang, WCC 2017]

Let f be the $2k$-variable function generated by Construction 1. Let $t = \max\{|t'| \mid t' \in [-2^{k/2+1} - 3, 2^{k/2+1} + 1]$ and $t' = 0 \pmod 4\}$. If $h_0 \in \mathcal{B}_k$ and $h_1 \in \mathcal{B}_k$ satisfy the following three conditions

1) $t < C_{h_0(\beta)} + C_{h_1(\beta)} < 2^{k+1} - t$ for any $\beta \in \mathbb{F}_{2^k}^*$

2) $|\sum_{y \in \mathbb{F}_{2^k}} (-1)^{h_0(y)+h_1(y+\beta)}| < 2^{k-1}$ for any $\beta \in \mathbb{F}_{2^k}$

3) $-2^{k-1} + t < \sum_{y \in \mathbb{F}_{2^k}} (-1)^{h_0(y+\beta)+\mathrm{Tr}_1^k(\frac{\lambda\alpha}{y})} + \sum_{y \in \mathbb{F}_{2^k}} (-1)^{h_1(y+\beta)+\mathrm{Tr}_1^k(\frac{\lambda(\mu+\alpha)}{y})} < 2^{k-1} - t$ for any $\alpha \in \mathbb{F}_{2^k} \setminus \{0, \mu\}, \beta \in \mathbb{F}_{2^k}$,

then we have $\Delta_f < 2^k$.

Construction on h_0, h_1 for odd k

1. Let g_0, g_1 be two Boolean functions in four variables and their truth tables are given as follows:
   - $g_0 = [0,0,0,0,1,0,0,1,0,0,0,0,0,0,0,0]$;
   - $g_1 = [1,1,1,1,0,1,1,1,0,1,1,1,1,1,1,1]$.
2. Let $t \geq 5$ be an odd number. Let $s_0(y_1,\ldots,y_{t-1})$ and $s_1(y_1,\ldots,y_{t-1})$ be two quadratic bent functions on $\mathbb{F}_2^{t-1}$ such that $w_H(s_0) = w_H(s_1) = 2^{t-2} - 2^{(t-1)/2-1}$ and $\tilde{s_0} + \tilde{s_1}$ is a bent function as well. Define two Boolean functions w_0, w_1 on $\mathbb{F}_2^t$ as $w_0(y_1,\ldots,y_t) = y_t s_0$ and $w_1(y_1,\ldots,y_t) = y_t s_1$.
3. Let $k \geq 9$ be an odd integer. The two Boolean functions h_0 and h_1 on k variables defined as follows:
   - $h_0(y_1,\ldots,y_k) = g_0(y') + w_0(y'')$
   - $h_1(y_1,\ldots,y_k) = g_1(y') + w_1(y'')$

   where $y' = (y_1,y_2,y_3,y_4) \in \mathbb{F}_2^4$, $y'' = (y_5,y_6,\ldots,y_k) \in \mathbb{F}_2^{k-4}$.

Cryptographic properties

Theorem [Tang-Maitra, IEEE TIT 2018]

Let f be the $n = 2k$-variable (k odd) function generated by Construction 1. Then the following statement hold:

- f is balanced;
- $\Delta_f < 2^k - 2^{(k+3)/2}$ for $k \geq 23$;
- $\mathrm{nl}(f) > 2^{n-1} - 7 \cdot 2^{k-3} - 5 \cdot 2^{\frac{k-1}{2}} > 2^{n-1} - 2^{n/2}$;
- f has algebraic degree $n - 1$.

This is the first time that an infinite class of balanced Boolean functions with absolute indicator strictly lesser than 2^k have been exhibited, which can also be viewed as an infinite class of counterexamples against Zhang-Zheng Conjecture.

Construction on h_0, h_1 for even k

1. Let g_0, g_1 be two Boolean functions in five variables and their truth tables are given as follows:
   - $g_0 = [0, 0, 0, 1, 0, 0, 1, 0, 1, 0, 0, 0, 1, 0, 0, 0, 1, 1, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0]$;
   - $g_1 = [1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 0, 0, 0, 0, 1, 1, 1, 0, 1, 1, 1, 0, 1, 1, 1, 1, 1, 1, 1, 1, 1]$.
2. Let $t \geq 5$ be an odd number. Let $s_0(y_1, \ldots, y_{t-1})$ and $s_1(y_1, \ldots, y_{t-1})$ be two quadratic bent functions on $\mathbb{F}_2^{t-1}$ such that $w_H(s_0) = w_H(s_1) = 2^{t-2} - 2^{(t-1)/2-1}$ and $\tilde{s}_0 + \tilde{s}_1$ is a bent function as well. Define two Boolean functions w_0, w_1 on $\mathbb{F}_2^t$ as $w_0(y_1, \ldots, y_t) = y_t s_0$ and $w_1(y_1, \ldots, y_t) = y_t s_1$.
3. Let $k \geq 10$ be an even integer. The two Boolean functions h_0 and h_1 on k variables defined as follows:
   - $h_0(y_1, \ldots, y_k) = g_0(y') + w_0(y'')$
   - $h_1(y_1, \ldots, y_k) = g_1(y') + w_1(y'')$

   where $y' = (y_1, y_2, y_3, y_4, y_5) \in \mathbb{F}_2^5$, $y'' = (y_6, y_7, \ldots, y_k) \in \mathbb{F}_2^{k-5}$.

Cryptographic properties

Theorem [Kavut-Maitra-Tang, WCC 2017]

Let $k \geq 10$ be an even integer and f be the $n = 2k$-variable function generated by Construction 1. Then the following statement hold:

- f is balanced;
- $\Delta_f < 2^k$ for $k \geq 26$;
- $\mathrm{nl}(f) > 2^{n-1} - 13 \cdot 2^{k-4} - 7 \cdot 2^{\frac{k}{2}-1} > 2^{n-1} - 2^{n/2}$;
- f has algebraic degree $n - 1$.

Further results

Searched functions	Number of variables n	Results $(nl(f), \Delta_f, \deg(f))$
h_0, h_1	12	$(1996, 56, 11)$
	14	$(8106, 96, 13)$
	16	$(32604, 160, 15)$
	18	$(130762, 312, 17)$
	20	$(523688, 600, 19)$
	22	$(2096020, 1224, 21)$
	24	$(8386392, 2360, 23)$
	26	$(33550064, 4584, 25)$

- Mustafa Khairallah, Anupam Chattopadhyay, Bimal Mandal, and Subhamoy Maitra, “On Hardware Implementation of Tang-Maitra Boolean Functions”, to be represented at WAIFI 2018.

Outline

1 Preliminaries

2 Balanced functions with low absolute indicator derived from $\mathcal{PS}_{ap}$ bent functions

3 Balanced functions with low absolute indicator derived from M-M bent functions

M-M bent function

M-M bent function [Maiorana-McFarland, 1973]

The class of Maiorana-McFarland (M-M) bent functions on $n = 2k$ variables is defined as

$$h(x, y) = \phi(x) \cdot y + g(x)$$

where $x, y \in \mathbb{F}_2^k$, ϕ is an arbitrary permutation on $\mathbb{F}_2^k$, and g is an arbitrary Boolean function on k variables.

- Huge numbers of bent functions
- Concatenation of linear functions on $\mathbb{F}_2^k$
- $\deg(h) = \deg(\phi) + 1$
- Disjoint spectra

Boolean functions with very low maximum absolute value

Construction 2 [Tang-Kavut-Mandal-Maitra, to be submitted]

Let $n = 2k$ be an even integer no less than 4. We construct an n-variable Boolean function over $\mathbb{F}_2^k \times \mathbb{F}_2^k$ as follows

$$f(x,y) = \begin{cases} u(y), & \text{if } (x,y) \in \{\mathbf{0}\} \times \mathbb{F}_2^k \\ \phi(x) \cdot y, & \text{if } (x,y) \in \mathbb{F}_2^{k*} \times \mathbb{F}_2^{k*} \\ v(x), & \text{if } (x,y) \in \mathbb{F}_2^{k*} \times \{\mathbf{0}\} \end{cases},$$

where ϕ is an arbitrary permutation on $\mathbb{F}_2^k$ such that $\phi(\mathbf{0}) = \mathbf{0}$, and u, v be two Boolean functions over $\mathbb{F}_2^k$ satisfying $u(\mathbf{0}) = v(\mathbf{0}) = \mathbf{0}$ and $w_H(u) + w_H(v) = 2^{k-1}$.

Cryptographic properties

Theorem

Let $n = 2k \geq 4$ and $f \in \mathcal{B}_n$ be a Boolean function generated by Construction 2. Then we have

$$W_f(a,b) = \begin{cases} 0, & \text{if } (a,b) = (\mathbf{0},\mathbf{0}) \\ W_u(b) + W_v(\mathbf{0}), & \text{if } (a,b) \in \{\mathbf{0}\} \times \mathbb{F}_2^{k*} \\ W_u(\mathbf{0}) + W_v(a), & \text{if } (a,b) \in \mathbb{F}_2^{k*} \times \{\mathbf{0}\} \\ (-1)^{\phi^{-1}(b)\cdot a} 2^k + W_u(b) + W_v(a), & \text{if } (a,b) \in \mathbb{F}_2^{k*} \times \mathbb{F}_2^{k*} \end{cases}.$$

and

$$C_f(a,b) = \begin{cases} 2^n, & \text{if } (a,b) = (\mathbf{0},\mathbf{0}) \\ C_u(b) + 2W_{v'}(b) - 2^k, & \text{if } (a,b) \in \{\mathbf{0}\} \times \mathbb{F}_2^{k*} \\ C_v(a) + 2W_u(\phi(a)) - 2^k, & \text{if } (a,b) \in \mathbb{F}_2^{k*} \times \{\mathbf{0}\} \\ 2(-1)^{\phi(a)\cdot b} W_u(\phi(a)) + W_{v''}(b) + 8t, & \text{if } (a,b) \in \mathbb{F}_2^{k*} \times \mathbb{F}_2^{k*} \end{cases}.$$

where $v'(x) = v(\phi^{-1}(x))$, $v''(x) = v(\phi^{-1}(x) + a)$, and t equals 1 if $v(a) = u(b) = 1$ and equals 0 otherwise.

The case for $k = 2t$

- A partial spread of $\mathbb{F}_2^k$ ($k = 2t$) is a set of pairwise supplementary of t-dimensional subspaces of $\mathbb{F}_2^k$. For any $1 \le s \le 2^t + 1$, a partial spread $\mathcal{E}_s$ with $|\mathcal{E}_s| = s$ of $\mathbb{F}_2^k$ can be written as $\mathcal{E}_s = \{E_1, E_2, \ldots, E_s\}$ where E_i's are t-dimensional subspaces of $\mathbb{F}_2^k$ and $E_i \cap E_j = \{\mathbf{0}\}$ for any $1 \le i \ne j \le s$.
- For any $1 \le s \le 2^t + 1$, let $\mathcal{E}_s = \{E_1, E_2, \ldots, E_s\}$ be a partial spread of $\mathbb{F}_2^k$ ($k = 2t$). We define a Boolean function v_s over $\mathbb{F}_2^k$ whose support is $\bigcup_{i=1}^{s} E_i \setminus \{\mathbf{0}\}$.

The case for $k = 2t$ (continued)

Theorem

For any Boolean function $v_s \in \mathbb{F}_2^k$ ($k = 2t$), we have

$$W_{v_s}(a) = \begin{cases} 2^k - 2s(2^t - 1), & \text{if } a = \mathbf{0} \\ -2^{t+1} + 2s, & \text{if } a \in \mathcal{E}'_s \\ 2s, & \text{if } a \notin \mathcal{E}'_s \end{cases},$$

where $\mathcal{E}'_s = \bigcup_{i=1}^{s} E_i^{\perp} \setminus \{\mathbf{0}\}$, and

$$C_{v_s}(\omega) = \begin{cases} 2^k, & \text{if } \omega = \mathbf{0} \\ 2^k + 4s^2 - 2^{t+2}s - 8s + 2^{t+2}, & \text{if } \omega \in \text{supp}(v_s) \\ 2^k + 4s^2 - 2^{t+2}s, & \text{if } \omega \in \mathbb{F}_2^{k*} \setminus \text{supp}(v_s) \end{cases},$$

where $\mathcal{E}'_s = \bigcup_{i=1}^{s} E_i^{\perp} \setminus \{\mathbf{0}\}$.

Results

Theorem

Let $n = 2k = 4t \geq 20$, $v = v_{2^{t-2}} \in \mathbb{F}_2^k$ and $u = u' \in \mathbb{F}_2^k$. Let f be an n-variable Boolean function generated by Construction 2. If $\phi^{-1}(\mathrm{supp}(v_{2^{t-2}}))$ is also a partial spread of $\mathbb{F}_2^k$, then we have

(1) $nl(f) \geq 2^{n-1} - 2^{\frac{n}{2}-1} - 2^{\frac{n}{4}+1}$, and

(2) $\Delta_f \leq 3 \cdot 2^{\frac{n}{2}-2} + 7 \cdot 2^{\frac{n}{4}} < 2^{\frac{n}{2}}$.

Thank You For Your Attention!