On plateaued Boolean functions with the same spectrum support

Yuriy Tarannikov

Lomonosov Moscow State University

August 25, 2016

Boolean function

The *Boolean function* f is a map $\mathbf{F}_2^n \to \mathbf{F}_2$.
$\mathbf{F}_2^n$ is a linear n-dimensional vector space over $\mathbf{F}_2$ but it also can be considered as a vector set V^n or n-dimensional Boolean cube (or hypercube, or Hamming graph).

$$B^n = B^n(V^n, E^n).$$

$\mathrm{supp}(f) = \{x \in \mathbf{F}_2^n \mid f(x) = 1\}$ is the *support* of f.

$B^n[\mathrm{supp}(f)]$ — subgraph of B^n induced by $supp(f)$.

$\mathrm{wt}(f) = |\mathrm{supp}(f)|$ is the *weight* of f.
$\bar{f} = f \oplus 1$ is the negation of f;
$\mathrm{supp}(\bar{f}) = V^n \setminus \mathrm{supp}(f)$
f is balanced if $wt(f) = \mathrm{wt}(\bar{f}) = 2^{n-1}$.

Walsh coefficients

Definition

The Walsh Transform of a Boolean function f is the integer-valued function on $\mathbf{F}_2^n$ defined as follows:

$$W_f(u) = \sum_{x \in \mathbf{F}_2^n} (-1)^{f(x)+<u,x>}.$$

For each $u \in \mathbf{F}_2^n$ the value $W_f(u)$ is called the Walsh coefficient or the spectral coefficient.

$< u, x >= u_1 x_1 + \cdots + u_n x_n$ is a scalar product.

Fourier coefficients

$$F_f(u) = \sum_{x \in \mathbf{F}_2^n} f(x)(-1)^{<u,x>}$$

$$W_f(u) = 2^n \delta_u^0 - 2F_f(u).$$

Sometimes Walsh coefficients are called Fourier coefficients too especially if f is defined at $\{-1, 1\}^n$.

Inversion formula

Inversion formula:

$$(-1)^{f(x)} = 2^{-n} \sum_{u \in F_2^n} W_f(u)(-1)^{<u,x>}$$

$\{(-1)^{<u,x>}\}|_{x \in \mathbf{F}_2^n}$ — is the orthogonal basis in 2^n-dimensional vector space $\mathbf{R}^{2^n}$.

$2^{-n} W_f(u)$ — expansion coefficients.

Inversion formula is a criterion for $\{W(u)\}|_{u \in \mathbf{F}_2^n}$ to correspond to some Boolean function.

Titsworth's Theorem

Another criterion for $\{W(u)\}|_{u\in\mathbf{F}_2^n}$ to correspond to some Boolean function:

Titsworth's Theorem

$\{W(u)\}|_{u\in\mathbf{F}_2^n}$ corresponds to some Boolean function iff

a) $\sum\limits_{u\in\mathbf{F}_2^n} W^2(u) = 2^{2n}$ (Parseval's identity);

b) $\sum\limits_{u\in\mathbf{F}_2^n} W(u)W(u+s) = 0$ for any $s \in \mathbf{F}_2^n$, $s \neq 0$.

Nonlinearity

The Hamming distance $d(x', x'')$ between two vectors x' and x'' is the number of components where vectors x' and x'' differ. For given function f from $\mathbf{F}_2^n$ the minimum of distances $d(f, l)$ where l runs the set of all affine functions on $\mathbf{F}_2^n$ is called *the nonlinearity* of f and denoted by $\mathrm{nl}(f)$.

The nonlinearity of a function f on $\mathbf{F}_2^n$ is expressed via its Walsh coefficients by formula

$$\mathrm{nl}(f) = 2^{n-1} - \frac{1}{2} \max_{u \in \mathbf{F}_2^n} |W_f(u)|.$$

Nonlinearity is invariant under any affine transformation of $\mathbf{F}_2^n$.

Bent functions

The Boolean function is called *the bent function* if the values of its Walsh coefficients at all vectors are exactly $\pm 2^{n/2}$. Bent functions exist for all even n and do not exist for all odd n. A bent function is the function with maximum possible nonlinearity $2^{n-1} - 2^{(n/2)-1}$ among all functions of n variables for even n.

f is bent iff $W_f(u) = \pm 2^{n/2}$ for any $u \in \mathbf{F}_2^n$
2-valued Walsh spectrum

Plateaued functions

f is called *plateaued* iff for some integer c we have $W_f(u) \in \{0, \pm 2^c$ for any $u \in \mathbf{F}_2^n$.

3-valued Walsh spectrum

Weight of f via $W_f(0)$.

f is balanced if $\mathrm{wt}(f) = \mathrm{wt}(\bar{f}) = 2^{n-1}$.

f is balanced iff $W_f(0) = 0$.

$\mathrm{wt}(f) = 2^{n-1} - \frac{1}{2}W_f(0)$

Resiliency (correlation immunity)

A Boolean function f is called *correlation-immune* of order m if $\mathrm{wt}(f') = \mathrm{wt}(f)/2^m$ for any its subfunction f' of $n - m$ variables. The balanced correlation-immune function of order m is called *m-resilient*. In other words, a Boolean function f is called m-resilient if $\mathrm{wt}(f') = 2^{n-m-1}$ for any its subfunction f' of $n - m$ variables.

A function f on $\mathbf{F}_2^n$ is correlation-immune of order m iff $W_f(u) = 0$ for all vectors $u \in \mathbf{F}_2^n$ such that $1 \leq |u| \leq m$.

In general, the order of correlation immunity is not invariant under affine transformation but it is invariant under isometric transformations.

If for a Boolean function f:
$W_f(u) \neq 0 \Rightarrow |u| \in \{0, m\}$
then f corresponds to 2-color perfect coloring or equitable partition.
$\mathbf{F}_2^n = \mathrm{supp}(f) \bigsqcup \mathrm{supp}(\bar{f})$
$B^n[\mathrm{supp}(f)]$ is $(n - c_1)$-regular
$B^n[\mathrm{supp}(\bar{f})]$ is $(n - c_2)$-regular

$$\frac{c_1 + c_2}{2} = m$$

$$\mathrm{wt}(f) \cdot c_1 = (2^n - \mathrm{wt}(f)) \cdot c_2, \qquad \mathrm{wt}(f) = 2^{n-1} - \frac{1}{2} W_f(0)$$

If additionally $W_f(0) = 0$ (i. e. f is balanced) then $c_1 = c_2 = m$.

Fon-Der-Flaass Theorem

Let $f(x_1, \ldots, x_n)$ be nonconstant unbalanced correlation immune of order m. Then

$$m \leq \frac{2n}{3} - 1.$$

Moreover, if $m = \frac{2n}{3} - 1$ then $\left(\mathrm{supp}(f), \mathrm{supp}(\bar{f})\right)$ is an equitable partition.

Khalyavin's proof of Fon-Der-Flaass Theorem

f is unbalanced $\Rightarrow W_f(0) \neq 0$
f in nonconstant $\Rightarrow \exists s \neq 0 : \ W_f(s) \neq 0$
f is m-CI $\Rightarrow \forall u,\ 1 \leq |u| \leq m : \ W_f(u) = 0 \Rightarrow |s| \geq m+1$
By Titsworth's Theorem $\sum_{u \in \mathbf{F}_2^n} W(u)W(u+s) = 0$
In the last sum nonzero equal summands for $u = 0, s$
Suppose that $m > \frac{2n}{3} - 1$. Then $|u|, |s| > \frac{2n}{3} \Rightarrow |u+s| < \frac{2n}{3}$
So, the sum has exactly two equal nonzero summands and sum is 0, contradiction
If $m = \frac{2n}{3} - 1$ then the only possibility for other nonzero summands in the sum is $|u|, |s|, |u+s| = \frac{2n}{3}$
So, $W_f(u) \neq 0$ follows $|u| \in \{0, m+1\} \Rightarrow \left(\mathrm{supp}(f), \mathrm{supp}(\bar{f})\right)$ is an equitable partition

Families of equitable partitions on Fon-Der-Flaass bound

$$S_f = \begin{pmatrix} 0 & 0 & 0 \\ 0 & 1 & 1 \\ 1 & 0 & 1 \\ 1 & 1 & 0 \end{pmatrix} \qquad S_f = \begin{pmatrix} 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 1 & 1 & 1 \\ 0 & 1 & 0 & 1 & 1 & 1 \\ 0 & 1 & 1 & 0 & 1 & 1 \\ 0 & 1 & 1 & 1 & 0 & 1 \\ 0 & 1 & 1 & 1 & 1 & 0 \\ 1 & 0 & 0 & 1 & 1 & 1 \\ 1 & 0 & 1 & 0 & 1 & 1 \\ 1 & 0 & 1 & 1 & 0 & 1 \\ 1 & 0 & 1 & 1 & 1 & 0 \\ 1 & 1 & 0 & 0 & 1 & 1 \\ 1 & 1 & 0 & 1 & 0 & 1 \\ 1 & 1 & 0 & 1 & 1 & 0 \\ 1 & 1 & 1 & 0 & 0 & 1 \\ 1 & 1 & 1 & 0 & 1 & 0 \\ 1 & 1 & 1 & 1 & 0 & 0 \end{pmatrix}$$

Transform $x_i \to y_{i,1} \oplus \cdots \oplus y_{i,l}$ for all $i = 1, \ldots, n$ keeps the property of a function to be an equitable partition but does not change cardinality and rank of the spectrum support.

$x_i \to y_{i,1} \oplus y_{i,2} \oplus y_{i,3}$, $i = 1, 2, 3$:

$$S_f = \begin{pmatrix} 0 & 0 & 0 \\ 0 & 1 & 1 \\ 1 & 0 & 1 \\ 1 & 1 & 0 \end{pmatrix} \to S_{f'} = \begin{pmatrix} 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 1 & 1 & 1 & 1 & 1 \\ 1 & 1 & 1 & 0 & 0 & 0 & 1 & 1 & 1 \\ 1 & 1 & 1 & 1 & 1 & 1 & 0 & 0 & 0 \end{pmatrix}$$

c-regular functions

If $c_1 = c_2 = c$ then f is called c-regular

$f(x_1, \ldots, x_n)$ is c-regular $\Rightarrow$
$\Rightarrow$ $f(x_1, \ldots, x_n) \oplus x_1 \oplus \cdots \oplus x_n$ is $(n-c)$-regular

$f(x_1, \ldots, x_n)$ is c-regular $\Rightarrow$
$\Rightarrow$ $f(x_1, \ldots, x_n) \oplus x_{n+1}$ is $(c+1)$-regular
(x_{n+1} is a linear variable)

$f(x_1, \ldots, x_n)$ is c-regular $\Rightarrow$
$\Rightarrow$ $g(x_1, \ldots, x_{n+1}) = f(x_1, \ldots, x_n)$ is c-regular
(x_{n+1} is a fictitious (nonessential) variable)

Let $c = \text{const}$, $c \geq 2$.
Then the maximal n such that there exists a c-regular function of n essential variables satisfies

$$3 \cdot 2^{c-1} - 2 \leq \max n \leq c \cdot 2^{c-1}$$

or (reformulation)

For given n the minimal possible c such that there exist c-regular function of n essential variables satisfies

$$\min c = \log_2 n + O(\log_2 \log_2 n)$$

Comparing with Simon–Wegener Theorem

Simon–Wegener Theorem
f depends of n variables, all variables are essential
In $B^n[\mathrm{supp}(f)]$ for any $x \in \mathrm{supp}(f)$: $\deg(f) \geq n - c$
In $B^n[\mathrm{supp}(\bar{f})]$ for any $x \in \mathrm{supp}(\bar{f})$: $\deg(f) \geq n - c$
Then $\min c = (1/2)\log_2 n + O(\log_2 \log_2 n)$

Theorem for regular functions (T. 2001)
f depends of n variables, all variables are essential
In $B^n[\mathrm{supp}(f)]$ for any $x \in \mathrm{supp}(f)$: $\deg(f) = n - c$
In $B^n[\mathrm{supp}(\bar{f})]$ for any $x \in \mathrm{supp}(\bar{f})$: $\deg(f) = n - c$
Then $\min c = \log_2 n + O(\log_2 \log_2 n)$

Plateaued functions with the same Walsh spectrum support

It is given the Walsh spectrum support S_f

It is given that f is plateaued

$|S_f| = 4^h$, $W_f \in \{0, \pm 2^{n-h}\}$

To reconstruct f t. i. to define signs of Walsh coefficients from S_f.

Motivation from autocorrelation coefficients

Autocorrelation coefficients $\Delta_f : \mathbf{F}_2^n \to [-2^n, 2^n]$

$$\Delta_f(u) = \sum_{x \in \mathbf{F}_2^n} (-1)^{f(x)+f(x+u)}$$

$$\Delta_f(u) = 2^{-n} \sum_{x \in \mathbf{F}_2^n} W_f^2(x)(-1)^{<u,x>}$$

$$W_f^2(v) = \sum_{u \in \mathbf{F}_2^n} \Delta_f(u)(-1)^{<u,v>}$$

So, if we know all autocorrelation coefficients of f then we know only all squares of Walsh coefficients, i. e. we don't know signs of Walsh coefficients.

Necessary conditions on matrix of S_f

Some structural conditions and prohibited configurations

Study placements of $\pm$ by means of Titsworth's Theorem

$\sum_{u \in \mathbf{F}_2^n} W(u)W(u+s) = 0$ for any $s \in \mathbf{F}_2^n$, $s \neq 0$.

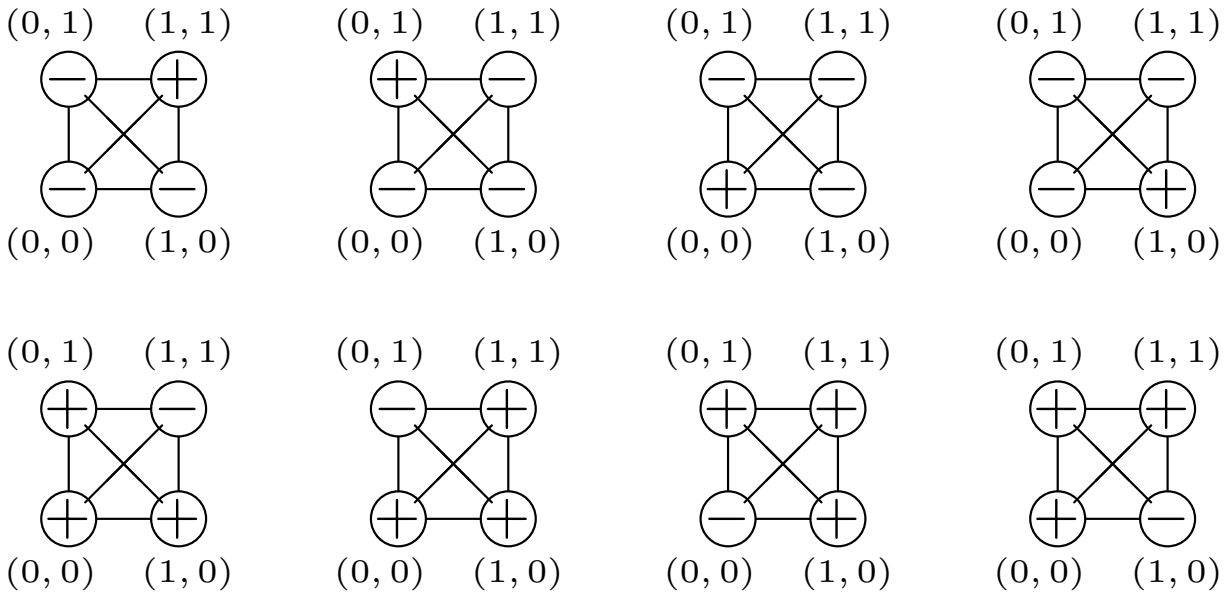
f is plateaued $\Rightarrow$ all nonzero Walsh coefficients are equal by absolute value.

Divide K_{S_f} into subclasses of parallel edges. For each direction the number of edges with the same signs at their ends must be equal to the number of edges with different signs at their ends

$|S_f| = 4$ case

4 vectors from S_f must satisfy $x^1 + x^2 + x^3 + x^4 = 0$.

It is possible to shift S_f by an affine transformation to $\{(0, 0, \dots), (0, 1, \dots), (1, 0, \dots), (1, 1, \dots)\}$. Affine rank of S_f is 2.



8 functions with given spectrum support S_f, $|S_f| = 4$.

$|S_f| = 16$ case

$4 \leq$ Affine rank of $S_f \leq 6$ (proven theoretically).

Number of ways to place $\pm$ is

$$\begin{cases} 7 \cdot 2^7 & \text{if} \quad \text{Affine rank of } S_f \text{ is } 4, \\ 3 \cdot 2^7 & \text{if} \quad \text{Affine rank of } S_f \text{ is } 5, \\ 2^7 & \text{if} \quad \text{Affine rank of } S_f \text{ is } 6 \end{cases}$$

(computer search fact)

Some examples

Bent functions, $S_f = \mathbf{F}_2^n$, n is even. The number of n-variable bent functions is unknown for $n > 8$.
$99270589265934703057858612428 80 \approx 2^{106}$ for $n = 8$
(Langevin, Leander 2011)

$[9, 4, 240]$-CI functions
$S_f = \{x \in \mathbf{F}_2^9 \mid |x| \in \{0, 5, 6, 7, 8\}\}$.
$\binom{9}{0} + \binom{9}{5} + \binom{9}{6} + \binom{9}{7} + \binom{9}{8} = 256 = 4^4$
Beginning with 2000 false proofs that such function does not exists
Khalyavin (2010) had constructed the function with such parameters (advanced algorithms + computer search)

$[17, 8, 2^{16} - 2^8]$-CI functions
$S_f = \{x \in \mathbf{F}_2^{17} \mid |x| \in \{0, 9, 10, 11, 12, 13, 14, 15, 16\}\}$
Open problem

Recursive sequence of Boolean functions

$n_{k+1} = 2n_k + 2$, $k = 0, 1, \ldots$, $n_0 = 4$.

$f_0 \in P_2^{(4)}$, $f_0(x_1, x_2, x_3, x_4) = (x_1 \oplus x_2)(x_3 \oplus x_4) \oplus x_1 \oplus x_3$

$f_{k+1} \in P_2^{(n_k+1)}$, $n_{k+1} = 2n_k + 2$,

$(x, y, z) \in \mathbf{F}_2^{n_{k+1}}$, $x, y \in \mathbf{F}_2^{n_k}$, $z \in \mathbf{F}_2^2$

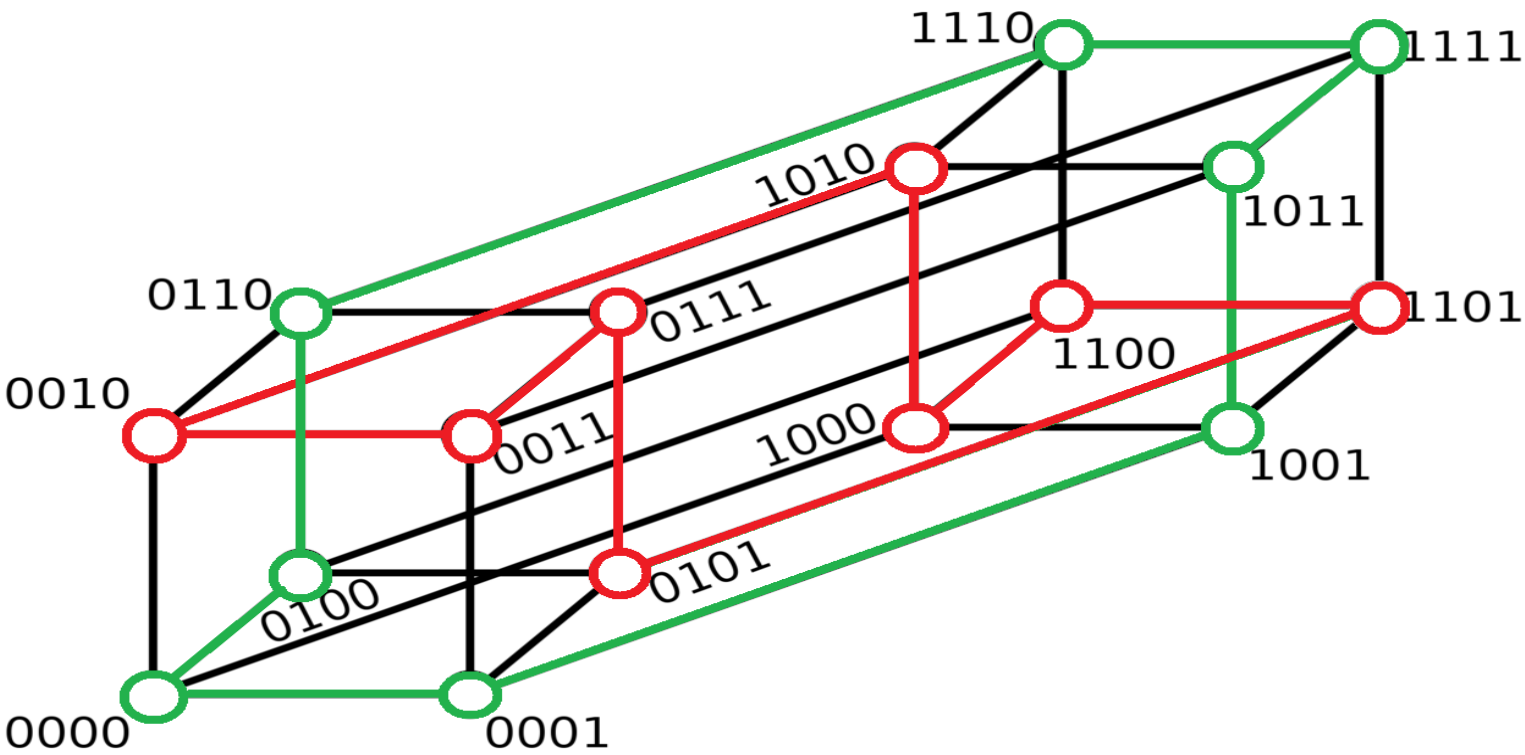
$f_{k+1}(x, y, z) =$

$(z_1 \oplus z_2 \oplus 1)(f_k(x) \oplus \langle 1^{n_k}, y \rangle) \oplus (z_1 \oplus z_2)(f_k(y) \oplus \langle 1^{n_k}, x \rangle) \oplus z_1$.

$n_k = 6 \cdot 2^k - 2$,

f is plateaued

f_0 as 2-regular function



$B^4[\mathrm{supp}(f)]$ — red, 2-regular
$B^4[\mathrm{supp}(\bar{f})]$ — green, 2-regular

Correspondent Walsh spectra

A_k is the matrix for S_{f_k}, $A_0 = \begin{pmatrix} 1 & 0 & 1 & 0 \\ 1 & 0 & 0 & 1 \\ 0 & 1 & 1 & 0 \\ 0 & 1 & 0 & 1 \end{pmatrix}$

$$A_k = \left(\begin{array}{ccc|c} & & & 0 \;\; 1 \\ A_{k-1} & 1\ldots1 & & \vdots \;\; \vdots \\ & & & 0 \;\; 1 \\ \hline & & & 1 \;\; 0 \\ A_{k-1} & 1\ldots1 & & \vdots \;\; \vdots \\ & & & 1 \;\; 0 \\ \hline & & & 0 \;\; 1 \\ 1\ldots1 & A_{k-1} & & \vdots \;\; \vdots \\ & & & 0 \;\; 1 \\ \hline & & & 1 \;\; 0 \\ 1\ldots1 & A_{k-1} & & \vdots \;\; \vdots \\ & & & 1 \;\; 0 \end{array}\right)$$

$|M_{k+1}|=2|M_k|^2$

$|M_k|=2^{4\cdot 2^k-1}$

$(n-k-2)$-regular functions

Symmetries

T_n is the group of shifts
$g_t \in T_n$, $g_t : f(x) \to f(x+t)$, $|T_n| = 2^n$

$J_{T_n}(f) = \{t \in \mathbf{F}_2^n : f(x) + f(x+t) = 0\}$ is the inertia group of the function f relative to the group T_n

Lemma. Any action of T_n does not change S_f
$\Rightarrow \{f_k\}_{T_{n_k}} \subseteq M_k$.

$|J_{T_{n_k}}(f_k)| = 2^{2^{k+1}-1}$

$|\{f_k\}_{T_{n_k}}| = \frac{|T_{n_k}|}{|J_{T_{n_k}}(f_k)|} = 2^{4 \cdot 2^k - 1} = |M_k|$

Thus, $\{f_k\}_{T_{n_k}} = M_k$

Bound on rank via $|S_f|$

$|S_f| = s$ (sparsity)

Rank of S_f is $O\left(\sqrt{s}\log_2 s\right)$ (Sanyal 2014)

Address function Add_s:

$$Add_m(x_1, \ldots, x_m, y_0, \ldots, y_{2^m-1}) = y_{(x_1,\ldots,x_m)}$$

Add_m is plateaued, $S_{Add_m} = \{xy \mid |y| = 1\}$.
$|S_{Add_m}| = s = 4^m$, rank of S_{Add_m} is $2^m + m \sim \sqrt{s}$.

For our example $|S_f| = s = 4^h$, affine rank of S_f is $2^{h+1} - 2 \sim 2\sqrt{s}$.

Open problems

To prove or to disprove that the function f_k constructed above is extremal:

- $f_k \bigoplus_{i=1}^{n} x_i$ has maximal possible number of essential variables among $(k+2)$-regular functions for fixed k;
- f_k has maximal possible number n of variables for fixed k such that $B^n[\mathrm{supp}(f)]$ is connected $(k+2)$-regular and $B^n[\mathrm{supp}(\bar{f})]$ is connected $(k+2)$-regular;
- f_k has maximal possible number of nonlinear variables for $(n-k-3)$-resilient functions;
- f_k has maximal possible affine rank among all (plateaued) functions with $|S_f| = 4^{k+1}$.