Upper bounds on the numbers of binary plateaued and bent functions

Vladimir N. Potapov

Sobolev Institute of Mathematics, Russia

Boolean Functions and their Applications, Voss, Norway, September 3-8, 2023

Boolean functions

$\mathbb{F} = \{0, 1\}$. $\mathbb{F}^n$ is the n-dimensional Boolean hypercube.
$\langle \mathbb{F}^n, \oplus \rangle$ is an n-dimensional vector space over $\mathbb{F}$.
$f : \mathbb{F}^n \to \mathbb{F}$ is a Boolean function on n variables.

$\ell : \mathbb{F}^n \to \mathbb{F}$ is a linear function if
$\ell(x) = \langle u, x \rangle = u_1 x_1 \oplus u_2 x_1 \oplus \cdots \oplus u_n x_n,\ u \in \mathbb{F}^n$.

The Walsh–Hadamard transform of f is

$$W_f(u) = \sum_{x \in \mathbb{F}^n} (-1)^{\langle u,x \rangle \oplus f(x)}.$$

$\{W_f(u) | u \in \mathbb{F}^n\}$ is the Walsh spectrum of f.

$(-1)^f : \mathbb{F}^n \to \mathbb{R}$
$V = \{G : \mathbb{F}^n \to \mathbb{R}\}$ is a 2^n-dimensional vector space over $\mathbb{R}$.
$\{(-1)^{\langle u,x \rangle} : u \in \mathbb{F}^n\}$ is an orthogonal basis in V.

Boolean bent functions

Definition

A Boolean function f in n variables is said to be a bent function if the Walsh spectrum of f consists of $\pm 2^{n/2}$.

Definition

A Boolean function f in n variables is said to be a s-plateaued function if the Walsh spectrum of f consists of $\pm 2^{(n+s)/2}$ and 0.

Boolean bent functions exist if and only if n is even.
The Parseval identity $\sum_{u \in \mathbb{F}^n} |W_f(u)|^2 = 2^{2n}$.

Proposition

For every s-plateaued function, a proportion of nonzero values of its Walsh–Hadamard transform is equal to $\frac{1}{2^s}$.

Algebraic degree

Denote by $\mathrm{wt}(z)$ a number of units in $z \in \mathbb{F}^n$. Every boolean function f can be represented as a polynomial

$$f(x_1, \ldots, x_n) = \bigoplus_{y \in \mathbb{F}^n} M[f](y) x_1^{y_1} \cdots x_n^{y_n},$$

where $x^0 = 1, x^1 = x$, and $M[f] : \mathbb{F}^n \to \mathbb{F}$ is the Möbius transform of f. Note that $M[M[f]] = f$ for each boolean function. The degree of this polynomial is called the algebraic degree of f.

Proposition

The algebraic degree of bent functions is not greater than $n/2$ if $n \geq 4$.

Known upper bounds on the number of bent functions

Let $\mathcal{N}(n, s)$ be the binary logarithm of the number of n-variable s-plateaued Boolean functions.

Proposition

Since the algebraic degree of bent functions is bounded by $n/2$, we have

$$\mathcal{N}(n, 0) \leq \frac{1}{2} \cdot 2^n + \frac{1}{2}\binom{n}{n/2}.$$

Carlet, Klapper (2002) and Agievich (2020) slightly improved the upper bounds, but asymptotically $\mathcal{N}(n, 0)$ remained the same.

Theorem (P., 2021)

$$\mathcal{N}(n, 0) \leq \frac{3}{8} \cdot 2^n + o(2^n).$$

Main results

Denote by h Shannon's entropy function, i.e.,
$h(p) = -p\log p - (1-p)\log(1-p)$ for $p \in (0,1)$.
Since the Walsh–Hadamard transform is a bijection, $\mathcal{N}(n,s)$ is not greater than the number of bits such that is sufficient to identify W_f for an s-plateaued function f. Therefore, by Shannon's theorem we obtain inequality:

$$\mathcal{N}(n,s) \leq 2^n \left(h(\frac{1}{2^s})(1+o(1)) + \frac{1}{2^s} \right).$$

Main results

Denote by $b(n,r)$ the cardinality of a ball $B_{n,r}$ with radius r in $\mathbb{F}^n$, i.e., $b(n,r) = |\{x \in \mathbb{F}^n : \mathrm{wt}(x) \le r\}|$.

Theorem 1

$\mathcal{N}(n,s) \le (\alpha b(n-2, \lceil \frac{n-s}{2} \rceil + 1) + 2^{n-2}(h(\frac{1}{2^s}) + \frac{1}{2^s}))(1+o(1))$ where $s > 0$ is fixed and $n \to \infty$.

Let Γ be a 2-dimensional face (axes-aligned plane) of the hypercube and let $f : \mathbb{F}^n \to \mathbb{F}$ be an s-plateaued function. There exists a non-degenerate affine transformation A and an affine function ℓ such that the s-plateaued function $g = (f \circ A) \oplus \ell$ satisfies the following conditions.
(a) The number of faces $\Gamma \oplus y$, $y \in \mathbb{F}^n$, that contain an odd number of zero values of g, is less than 2^{n-3}.
(b) Among the faces $\Gamma \oplus y$, $y \in \mathbb{F}^n$, that contain an even number of zero values of g, not less than one fourth part contain four or zero values 0.

Main results

(a) The number of faces $\Gamma \oplus y$, $y \in \mathbb{F}^n$, that contain an odd number of zero values of g, is less than 2^{n-3}.
(b) Among the faces $\Gamma \oplus y$, $y \in \mathbb{F}^n$, that contain an even number of zero values of g, not less than one fourth part contain four or zero values 0.
Let p_0 be a probability of an even number of zero values in a 2-dimensional face and let p_1 be a probability of an odd number of zero values in a 2-dimensional face. Moreover, p_0' is the probability of two zero value in a 2-dimensional face and $p_0' < 3p_0/4$. How many bits on average we need to find four values $(-1)^{g(x)}$ from their sum in a 2-dimensional face? Under conditions (a) and (b) from the corollary, it is sufficient
$p_0' \log_2 6 + 2p_1 \leq 1 + \frac{3}{8} \log_2 6 = \alpha \approx 1.969$ bits by Shannon's theorem.

Main results

Let $\mathcal{N}_0(n,1)$ be the binary logarithm of the number of *n*-variable 1-plateaued boolean functions which are obtained by a restriction of $(n+1)$-variable bent functions into hyperplanes.

Theorem 2

$\mathcal{N}_0(n,1) \leq b(n-2, \frac{n+1}{2})(\alpha + \frac{3}{2})(1+o(1))$ as $n \to \infty$.

Main results

Theorem 3

$\mathcal{N}(n,0) \leq \mathcal{N}_0(n-1,1) + 2^{n-3}(1+o(1)) \approx \frac{11}{32}2^n(1+o(1))$ as $n \rightarrow \infty$.

Proof. The restriction of a bent function into a hyperplane is a 1-plateaued function. We have counted these functions in Theorem 2. Then we count the number of 1-plateaued function in $(n-1)$ variables corresponding to one n-variable bent function.

Propositions

1. The degree of n-variable s-plateaued functions is not greater than $\frac{n-s}{2}+1$.
2. Suppose that f and g are n-variable boolean functions and $\max\{\deg(f), \deg(g)\} \leq r$. If $f|_{B_{n,r}} = g|_{B_{n,r}}$ then $f = g$.

Lower bounds of the number of bent functions

Class of bent f.	Asymptotics of $\log_2$ of cardinality
MM family	$\log_2 \lvert\mathcal{M}(n)\rvert = \frac{n}{2} \cdot 2^{n/2}(1 + o(1))$
completed MM family	$\log_2 \lvert\mathcal{M}^{\#}(n)\rvert = \frac{n}{2} \cdot 2^{n/2}(1 + o(1))$
$\mathcal{C}$ class	$\log_2 \lvert\mathcal{C}(n)\rvert = \frac{n}{2} \cdot 2^{n/2}(1 + o(1))$
$\mathcal{D}$ class	$\log_2 \lvert\mathcal{D}(n)\rvert = \frac{n}{2} \cdot 2^{n/2}(1 + o(1))$
Agievich class	$\log_2 \lvert A(n)\rvert = \frac{n}{2} \cdot 2^{n/2}(1 + o(1))$
special subclass of $\mathcal{PS}$	$\log_2 \lvert\mathcal{PS}_{ap}(n)\rvert = 2^{n/2}(1 + o(1))$
GMM family	$\log_2 \lvert K(n,1)\rvert = \frac{3n}{4} \cdot 2^{n/2}(1 + o(1))$

Theorem (P., Taranenko, Tarannikov, 2023)

$\mathcal{N}(n, 0) \geq \frac{3n}{4} \cdot 2^{n/2}(1 + o(1))$.