Upper bounds on the numbers of binary plateaued and bent functions

V. N. Potapov
Sobolev Institute of Mathematics, vpotapov@math.nsc.ru

30th July 2023

1 Introduction

Bent functions are maximally nonlinear boolean functions with an even number of variables and are optimal combinatorial objects. In cryptography, bent functions are used in block ciphers. They are the source of nonlinearity and provide confusion in cryptosystems. Moreover, bent functions have many theoretical applications in discrete mathematics. Full classification of bent functions would be very useful for combinatorics and cryptography. But constructive classifications and enumerations of bent functions in n variables are likely impossible for large n.

The numbers of n-variable bent functions are only known for $n \leq 8$. There exist 8 bent functions for $n = 2$, 896 for $n = 4$, approximately $2^{32.3}$ for $n = 6$ and $2^{106.3}$ for $n = 8$ [5]. Thus, lower and upper asymptotic bounds on the number of bent functions are very interesting. Currently, there exists a drastic gap between the upper and lower bounds of this number. Let $\mathcal{N}(n) = \log_2 |\mathcal{B}(n)|$, where $\mathcal{B}(n)$ is the set of boolean bent functions in n variables. The best known asymptotic lower bound on the number of boolean bent functions is proven in [9]. It holds $\mathcal{N}(n) \geq \frac{3n}{4}2^{n/2}(1 + o(1))$ as n is even and $n \to \infty$. This bound is slightly better than the bound $\mathcal{N}(n) \geq \frac{n}{2}2^{n/2}(1 + o(1))$ based on the Maiorana–McFarland construction of bent functions.

It is well known (see e.g. [2], [4], [6]) that the algebraic degree of a boolean bent function in n variables is at most $n/2$. Therefore, $\mathcal{N}(n) \leq \sum\limits_{i=0}^{n/2} \binom{n}{i} = 2^{n-1} + \frac{1}{2}\binom{n}{n/2}$. The bounds in [3] and [1] are of type $\mathcal{N}(n) \leq 2^{n-1}(1+o(1))$. A better upper bound $\mathcal{N}(n) \leq \frac{3}{4} \cdot 2^{n-1}(1+o(1))$ is proven in [7]. In this paper we improve it. We obtained that $\mathcal{N}(n) < \frac{11}{16} \cdot 2^{n-1}(1+o(1))$ (Theorem 2). Note that Tokareva's conjecture (see [10] and [6]) of the decomposition of boolean functions into sums of bent functions implies that $\mathcal{N}(n) \geq \frac{1}{2}2^{n-1} + \frac{1}{4}\binom{n}{n/2}$.

The bounds mentioned above are asymptotic. We can use the suggested method to find a non-asymptotic upper bound. But for fixed $n = 6$ and $n = 8$ such bound is greater than the number of $\frac{2}{3} \cdot 2^{n-1}$ in two times. The main reason of this difference lies in the cardinality of the middle layer of the n-dimensional boolean cube. This cardinality is asymptotically negligible, but that is not the case for $n = 6$ and $n = 8$.

The new upper bound on the number of bent functions is based on new asymptotic upper bound on the number of s-plateaued boolean functions in n variables (Theorem 1). s-Plateaued functions are a generalization of bent functions, which are the same as 0-plateaued functions. Plateaued functions can combine important cryptographic properties of nonlinearity and correlation immunity.

The method of the proof of the listed above bounds implies a storage algorithm for bent and plateaued functions. The number of bits required by the algorithm is equal to the corresponding upper bound.

2 Walsh–Hadamard transform

Let $\mathbb{F} = \{0,1\}$. The set $\mathbb{F}^n$ is called a boolean hypercube (or a boolean n-cube). $\mathbb{F}^n$ equipped with coordinate-wise modulo 2 addition $\oplus$ can be considered as an n-dimensional vector space. Define by $\langle x,y\rangle = x_1y_1 \oplus \cdots \oplus x_ny_n$ the inner product of vectors x and y.

Let G be a function that maps from the boolean hypercube to real numbers. Denote by $\widehat{G}(y) = \sum\limits_{x\in\mathbb{F}^n} G(x)(-1)^{\oplus\langle x,y\rangle}$ the Fourier transform of G. We can define the Walsh–Hadamard transform of a boolean function $f : \mathbb{F}^n \to \mathbb{F}$ by the formula $W_f(y) = \widehat{(-1)^f}(y)$. A boolean function b is called a bent function if $W_b(y) = \pm 2^{n/2}$ for all $y \in \mathbb{F}^n$. It is easy to see that n-variable bent functions exist only if n is even. A boolean function p is called an s-plateaued function if $W_p(y) = \pm 2^{(n+s)/2}$ or $W_p(y) = 0$ for all $y \in \mathbb{F}^n$. So, bent functions are 0-plateaued functions. 1-Plateaued functions are called near-bent.

From Parseval's identity $\sum\limits_{y\in\mathbb{F}^n} \widehat{H}^2(y) = 2^n \sum\limits_{x\in\mathbb{F}^n} H^2(x)$, where $H : \mathbb{F}^n \to \mathbb{C}$, it follows straightforwardly:

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

It is well known (see e.g. [2]) that for any function $H, G : \mathbb{F}^n \to \mathbb{C}$ it holds

$$\widehat{H * G} = \widehat{H}\cdot\widehat{G}, \qquad \widehat{(\widehat{H})} = 2^n H \qquad \text{and} \qquad 2^n H * G = \widehat{\widehat{H}\cdot\widehat{G}}, \tag{1}$$

where $H * G(z) = \sum\limits_{x\in\mathbb{F}^n} H(x)G(z\oplus x)$ is a convolution. Let Γ be a subspace of hypercube. Denote by $\Gamma^\perp$ a dual subspace, i.e., $\Gamma^\perp = \{y \in \mathbb{F}^n : \forall x \in \Gamma, \langle x,y\rangle = 0\}$. Let $\mathbf{1}_S$ be an indicator function for $S \subset \mathbb{F}^n$. It is easy to see that for every subspace Γ it holds $\widehat{\mathbf{1}_{\Gamma^\perp}} = 2^{n-\dim\Gamma}\mathbf{1}_\Gamma$. By (1) we have

$$H * \mathbf{1}_{\Gamma^\perp} = 2^{-\dim\Gamma}\widehat{\widehat{H}\cdot\mathbf{1}_\Gamma} \tag{2}$$

for any subspace $\Gamma \subset \mathbb{F}^n$.

Denote by $\mathrm{supp}(G) = \{x \in \mathbb{F}^n : G(x) \neq 0\}$ a support of G. We need the following known property of bent functions (see e.g. [6]).

Proposition 2. *Let f be an n-variable bent function and let Γ be a hyperplane. Consider $h = f \cdot \mathbf{1}_\Gamma$ as an $(n-1)$-variable function. Then h is a 1-plateaued function.*

3 Möbius transform

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

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

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.

Denote by $b(n,r)$ the cardinality of a ball $B_{n,r}$ with radius r in $\mathbb{F}^n$, i.e., $b(n,r) = |\{x \in \mathbb{F}^n : \mathrm{wt}(x) \le r\}|$. By properties of the Möbius transform, the number of n-variable boolean functions with degree $\deg f \le r$ is equal to $2^{b(n,r)}$.

Lemma 1 ([7])**.** *Suppose that f and g are n-variable boolean functions and* $\max\{\deg(f), \deg(g)\} \le r$. *If $f|_{B_{n,r}} = g|_{B_{n,r}}$ then $f = g$.*

Lemma 2 ([2], Theorem 2)**.** *Let f be an n-variable boolean function. Suppose for every $v \in \mathbb{F}^n$ it holds $\widehat{(-1)^f}(v) = 2^k m(v)$, where $m(v)$ is integer. Then* $\deg(f) \le n - k + 1$.

Corollary 1 ([2], Proposition 96)**.** *The degree of n-variable s-plateaued functions is not greater than $\frac{n-s}{2} + 1$.*

Note that degrees of bent (0-plateaued) functions is $n/2$ at most (see e.g. [2], [4], [6]). But for 1-plateaued function the bound $\frac{n+1}{2}$ is tight.

Proposition 3. *Let f be an n-variable bent function. Then for any hyperplane Γ the degree of the boolean function $h = \mathrm{supp}(\widehat{(-1)^f \cdot \mathbf{1}_\Gamma})$ is not greater than $n/2$.*

4 Subspace distribution

We will use the following well-known criterium (see, e.g. [2], Proposition 96).

Lemma 3. *An n-variable boolean function f is s-plateaued if and only if* $(-1)^f * (-1)^f * (-1)^f = 2^{n+s}(-1)^f$.

Consider an n-variable s-plateaued boolean function f and any fixed $x \in \mathbb{F}^n$. There are $V = \frac{(2^n-1)(2^n-2)}{6}$ 2-dimensional affine subspaces which contain x. Let $S(x)$ be a number of the subspaces that contain an odd number of zero values of f. By Lemma 3 we obtain

Corollary 2. *For any fixed $x \in \mathbb{F}^n$, $\frac{S(x)}{V} = \frac{1}{2} - \frac{1}{2} \cdot \frac{2^{n+s} - 3 \cdot 2^n + 2}{(2^n-1)(2^n-2)}$.*

Thus we have two equations: $\frac{S(x)}{V} = \frac{1}{2} + \frac{1}{2(2^{n-1}-1)}$ for every bent function and $\frac{S(x)}{V} = \frac{1}{2} + \frac{1}{2(2^n-1)}$ for every 1-plateaued function. We will use the following property of bent and plateaued functions.

Proposition 4 ([2], [4], [6])**.** *Let $f : \mathbb{F}^n \to \mathbb{F}$ be an s-plateaued function, let $A : \mathbb{F}^n \to \mathbb{F}^n$ be a non-degenerate affine transformation and let $\ell : \mathbb{F}^n \to \mathbb{F}$ be an affine function. Then $g = (f \circ A) \oplus \ell$ is an s-plateaued function.*

Functions f and g from Proposition 4 are called AE-equivalent. It is easy to see that the cardinality of any equivalence class is not greater than $a_n = 2^{n^2+n+1}(1+o(1))$. Note that two AE-equivalent functions f and g have the same algebraic degree as $\deg(f) > 1$.

There are 8 boolean 2-variable functions such that take value 0 even times. All of them are affine. 6 of them take value 0 two times and the other take value 0 four or zero times. Consider a 2-dimensional affine subspace Γ and an n-variable boolean function g. Let g take value 0 even times on Γ. It is easy to see that 3/4 among functions of the set $\{g \oplus \ell : \ell \text{ is an affine function}\}$ take value 0 two times and the other take value 0 four or zero times. Consequently, from Propositions 2 and 4 we deduced:

Corollary 3. *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.

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 $p_0' \log_2 6 + 2p_1 \le 1 + \frac{3}{8}\log_2 6 = \alpha \approx 1.969$ bits by Shannon's theorem.

5 Main results

Denote by $\hbar$ Shannon's entropy function, i.e., $\hbar(p) = -p\log p - (1-p)\log(1-p)$ for $p \in (0,1)$. Let $\mathcal{N}(n,s)$ be the binary logarithm of the number of n-variable s-plateaued boolean functions. 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 and Proposition 1 we obtain inequality:

$$\mathcal{N}(n,s) \le 2^n \left(\hbar(\frac{1}{2^s})(1+o(1)) + \frac{1}{2^s} \right). \tag{3}$$

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

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

The main idea of the proof is the following. Let f be an s-plateaued function. We count the number of possible restrictions of W_f into $(n-2)$-dimensional face by (3). Let we have such restrictions of W_f. By (2) we recover f on the ball with an appropriate radius. By Corollary 3 and the entropy estimation α we find the number of bits needed for this recovering. By Lemma 1 and Corollary 1 we restore f in full.

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

The proof is similar to the previous one. By Proposition 2 the restriction of a bent function into a hyperplane is a 1-plateaued function. We have counted these functions in Theorem 1 (b). Then we count the number of 1-plateaued function in $(n-1)$ variables corresponding to one n-variable bent function. Completed proofs are available in [8].

References

[1] S.V. Agievich, "On the continuation to bent functions and upper bounds on their number," Prikl. Diskr. Mat. Suppl., no. 13, 2020, pp. 18–21 (in Russian).

[2] C. Carlet, *Boolean Functions for Cryptography and Coding Theory.* Cambridge University Press, 562 pages, 2020.

[3] C. Carlet and A. Klapper, "Upper bounds on the number of resilient functions and of bent functions," Proceedings of the 23rd Symposium on Information Theory in the Benelux, Louvain-La-Neuve, Belgium. 2002.

[4] C. Carlet and S. Mesnager, "Four decades of research on bent functions," Des. Codes Cryptogr., vol. 78(1), 2016, pp. 5–50.

[5] P. Langevin, G. Leander, P. Rabizzoni, P. Veron, and J.-P. Zanotti. "Counting all bent functions in dimension eight 99270589265934370305785861242880," In Des. Codes Cryptography 59 (1-3), pages 193-205, 2011.

[6] S. Mesnager, *Bent Functions: Fundamentals and Results.* Springer International Publishing Switzerland, 2016.

[7] V.N. Potapov, "An Upper Bound on the Number of Bent Functions," 2021 XVII International Symposium on Problems of Redundancy in Information and Control Systems (25-29 October 2021 Moscow, Russia).IEEE, 2021. P. 95–96.

[8] V.N. Potapov, "Upper bounds on the numbers of binary plateaued and bent functions," DOI:10.48550/arXiv.2303.16547

[9] V.N. Potapov, A.A. Taranenko, Yu.V. Tarannikov, "Asymptotic bounds on numbers of bent functions and partitions of the Boolean hypercube into linear and affine subspaces," *Designs, Codes and Cryptography*, 2023. DOI: 10.1007/s10623-023-01239-z

[10] N. Tokareva, "On the number of bent functions from iterative constructions: lower bounds and hypothesis," Adv. Math. Commun., vol. 5(4), 2011, pp. 609–621.