# On the number of relevant variables for discrete functions

Vladimir N. Potapov

independent researcher, Siberia

Boolean Functions and their Applications, September 9-13, 2024,

Inter-University Centre Dubrovnik, Croatia

# Boolean functions

$\mathbb{F}_2 = \{0, 1\}$.
$\langle \mathbb{F}_2^n, \oplus \rangle$ is an $n$-dimensional vector space over $\mathbb{F}_2$.
$f : \mathbb{F}_2^n \to \mathbb{F}_2$ is a Boolean function on $n$ variables.

Every Boolean function can be represented in the algebraic normal form (ANF)

$$f(x_1, \ldots, x_n) = \bigoplus_{y \in \mathbb{F}_2^n} M_f(y) x_1^{y_1} \cdots x_n^{y_n}, \tag{1}$$

where $x^0 = 1, x^1 = x$, $M_f : \mathbb{F}_2^n \to \mathbb{F}_2$ is the Möbius transform of $f$.

The weight of $y \in \mathbb{F}_2^n$ is the number of nonzero coordinates of $y$.
The algebraic degree of $f$ is called the maximal degree of the monomial in ANF, i. e., $\deg_{alg}(f) = \max_{M_f(y)=1} \mathrm{wt}(y)$.

# Boolean functions

$\ell_u : \mathbb{F}_2^n \to \mathbb{F}_2$ is a linear function if
$\ell_u(x) = \langle u, x \rangle = u_1 x_1 \oplus u_2 x_1 \oplus \cdots \oplus u_n x_n$, $u \in \mathbb{F}_2^n$,
$\ell_{\mathbf{1}}(x) = x_1 \oplus x_2 \oplus \cdots \oplus x_n$.

# pseudo-Boolean functions

A real-valued function $f : \mathbb{F}_2^n \to \mathbb{R}$ is called a pseudo-Boolean function.
$V = \{f : \mathbb{F}_2^n \to \mathbb{R}\}$ is a $2^n$-dimensional vector space over $\mathbb{R}$.

Every pseudo-Boolean function can be represented in the numerical normal form (NNF)

$$f(x_1, \dots, x_n) = \sum_{y \in \mathbb{F}_2^n} a(y) x_1^{y_1} \cdots x_n^{y_n}, \tag{2}$$

where $x^0 = 1, x^1 = x,\ a(y), x_i \in \mathbb{R}$.

The numerical degree of $f$ is called the maximal degree of the monomial in NNF, i. e., $\deg_{num}(f) = \max_{a(y) \neq 0} \mathrm{wt}(y)$.

# inequalities for degrees

$(-1)^b = 1 - 2b$ if $b \in \{0,1\} \subset \mathbb{R}$.

$$f(x_1,\ldots,x_n) = \bigoplus_{y \in \mathbb{F}_2^n} a(y) x_1^{y_1} \cdots x_n^{y_n},\ a(y) = M_f(y),$$

$$(-1)^{f(x_1,\ldots,x_n)} = \prod_{y \in \mathbb{F}_2^n} (-1)^{a(y) x_1^{y_1} \cdots x_n^{y_n}},$$

$$1 - 2f(x) = \prod_{y \in \mathbb{F}_2^n} (1 - 2a(y) x_1^{y_1} \cdots x_n^{y_n}).$$

$x^2 = x$ if $x \in \{0,1\} \subset \mathbb{R}$ then
$\deg_{alg}(f) \leq \deg_{num}(f) = \deg_{num}((-1)^f)$.

# Walsh–Hadamard transform

The Walsh–Hadamard transform of a Boolean function $f$ is

$$W_f(y) = \sum_{x \in \mathbb{F}_2^n} (-1)^{f(x)} (-1)^{\langle y,x \rangle}.$$

$\mathcal{W}(f) = \{W_f(y) | y \in \mathbb{F}_2^n\}$ is the Walsh spectrum of $f$.

$\{(-1)^{\langle y,x \rangle} : y \in \mathbb{F}_2^n\}$ is an orthogonal basis in $V$.

$$(-1)^f(x) = \frac{1}{2^n} \sum_{y \in \mathbb{F}_2^n} W_f(y)(-1)^{\langle y,x \rangle}.$$

$(-1)^{\langle y,x \rangle} = \prod_{i=1}^n (-1)^{y_i x_i} = \prod_{i=1}^n (1 - 2y_i x_i).$

# Walsh–Hadamard transform

$$(-1)^{f}(x) = \frac{1}{2^n} \sum_{y \in \mathbb{F}_2^n} W_f(y)(-1)^{\langle y,x \rangle}.$$

$(-1)^{\langle y,x \rangle} = \prod_{i=1}^{n} (-1)^{y_i x_i} = \prod_{i=1}^{n} (1 - 2y_i x_i)$.

Then $\deg_{num}(f) = \deg_{num}((-1)^f) = \max_{W_f(y) \neq 0} \mathrm{wt}(y)$.

# Relevant variables

Given a function $f$ on $T^n$, a variable $x_i$, $1 \leq i \leq n$, is called relevant (essential, or effective) if there exist $a_1, \ldots, a_{i-1}, a_{i+1}, \ldots, a_n \in T$ and $b, c \in T$ such that

$$f(a_1, \ldots, a_{i-1}, b, a_{i+1}, \ldots, a_n) \neq f(a_1, \ldots, a_{i-1}, c, a_{i+1}, \ldots, a_n).$$

Denote by $t(f)$ the number of relevant variables of $f$.

From the definitions, $\deg_{alg}(f) \leq t(f)$ and $\deg_{num}(f) \leq t(f)$. Is there any opposite inequality?

(i)consider Boolean function $\ell_{\mathbf{1}}(x) = x_1 \oplus \cdots \oplus x_n$, then $\deg_{alg}(\ell_{\mathbf{1}}) = 1$, $\deg_{num}(\ell_{\mathbf{1}}) = n$, $t(\ell_{\mathbf{1}}) = n$;

(ii)consider real-valued function $\jmath(x) = (-1)^{x_1} + \cdots + (-1)^{x_n} = n - 2(x_1 + \cdots + x_n)$, then $\deg_{num}(\jmath) = 1$, $t(\jmath) = n$.

# Relevant variables

Let $f$ be a Boolean function and $d = \deg_{Num}(f)$. Then

- $t(f) \leq d2^{d-1}$ Nisan and Szegedy (1994);
- $t(f) \leq 6.614 \cdot 2^d$ Chiarelli, Hatami and Saks (2020);
- $t(f) \leq 4.394 \cdot 2^d$ Wellens (2022).

# q-ary Fourier–Hadamard transform

We consider the linear space $V(\mathbb{Z}_q^n)$ of complex valued functions with finite domain $\mathbb{Z}_q^n = (\mathbb{Z}/q\mathbb{Z})^n$. Let $\xi = e^{2\pi i/q}$. We can define characters of $\mathbb{Z}_q^n$ as $\phi_z(x) = \xi^{\langle x,z \rangle}$, where and $\langle x, z\rangle = x_1 z_1 + \cdots + x_n z_n \mod q$ for each $z \in \mathbb{Z}_q^n$.

Consider the expansion of $f \in V(\mathbb{Z}_q^n)$ with respect to the basis of characters

$$f(x) = \frac{1}{q^n} \sum_{z \in \mathbb{Z}_q^n} W_f(z)\phi_z(x),$$

where $W_f(z) = (f, \phi_z)$ are called the Fourier–Hadamard coefficients of $f$.

# degrees of q-ary functions

Below we will consider $\mathbb{Z}_q$ as the set $\{-\frac{q-2}{2}, \ldots, -1, 0, 1, \ldots, q/2\}$ if $q$ is even and as the set $\{-\frac{q-1}{2}, \ldots, -1, 0, 1, \ldots, \frac{q-1}{2}\}$ if $q$ is odd. Define the $m$th degree of $\phi_z$, $z = (z_1, \ldots, z_n)$, as the sum $\deg_m(\phi_z) = \sum_{k=1}^{n} |z_k|^m$.

$$f(x) = \frac{1}{q^n} \sum_{z \in \mathbb{Z}_q^n} W_f(z) \phi_z(x),$$

$$\deg_m(f) = \max_{W_f(z) \neq 0} \deg_m(\phi_z).$$

# degrees of q-ary functions

Let $f$ be a Boolean-valued function on $\mathbb{Z}_q^n$ and $d = \deg_0(f)$. Then

- $t(f) \leq 4.394 \cdot 2^{\lceil \log_2 q \rceil d}$ Filmus and Ihringer (2019), Wellens (2022);
- $t(f) \leq \frac{dq^{d+1}}{4(q-1)}$ Valyuzhenich (2024).

**Theorem**

$t(f) \leq \frac{1}{4}\pi^2 \deg_1(f) q^{\deg_0(f)-1}$;
$t(f) \leq \frac{1}{2}\pi^2 \deg_2(f) q^{\deg_0(f)-2}$.

# Example

For $q = 3$ the presented bounds are weaker than Valyuzhenich's bound.

$q = 4$. Let $h : \mathbb{Z}_4 \to \{0, 1\}$ be defined by the vector of values $(1, 1, 0, 0)$. Consider $f_m : \mathbb{Z}_4^n \to \{0, 1\}$, where
$f_m(x_1, \ldots, x_n) = h(x_1) \cdot h(x_2) \cdots h(x_m)$.
It is clear that $t(f_m) = m$.

The new bound $t(f_m) \leq \frac{\pi^2 m}{32} 4^m$ is slightly better than Valuzhenich's bound $t(f_m) \leq \frac{m 4^m}{3}$.

# Method of the proof

We consider $f : \mathbb{Z}_q^n \to \{0,1\}$ as a 2-coloring of a graph $G$ such that $V(G) = \mathbb{Z}_q^n$.

(i) $I[f]$ is the number of mixed colored edges in a graph, estimation of $I[f]$ by using adjacency matrix of the graph (Nisan and Szegedy)

(ii) Estimation of the Hamming difference between functions from the same invariant subspace of the adjacency matrix (Valyuzhenich)

(iii) Using $Cay(\mathbb{Z}_q^n, S^n) = C_q \square \cdots \square C_q = C_q^n$ instead of $H(n,q) = K_q \square \cdots \square K_q$.