Sensitivity conjecture

...or a 1-page proof of an $\approx$ 30 y.o. problem

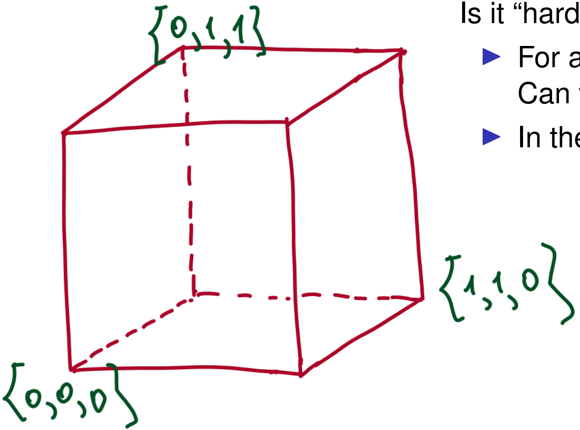
Svyatoslav Gryaznov

PDMI RAS

December 22, 2020

Sensitivity

Let $f\colon \{0,1\}^n \to \{0,1\}$ be a Boolean function.



Is it “hard” to flip its value?

- For a *fixed* input:
  Can we change it by flipping only one bit?
- In the worst case?

Sensitivity

Let $f\colon \{0,1\}^n \to \{0,1\}$ be a Boolean function.
For $x \in Q$ let x^J be a vector with all x_j flipped.

$x = (x_1, x_2, x_3, x_4, x_5, x_6, x_7, x_8)$

$x^{\{3,6\}} = (\dots \overline{x_3} \dots \overline{x_6} \dots)$

- For a fixed input $x \in Q^n$:

$$\mathrm{s}(f,x) = \max\left\{ |J| \;\middle|\; J \subseteq [n] : \forall i \in J.\ f(x) \neq f(x^{\{i\}}) \right\}$$

- In the worst case: $\mathrm{s}(f) = \max_{x \in Q^n} \mathrm{s}(f,x)$

Block sensitivity

What if we can flip not only one bit, but a block of bits?

Block sensitivity

Let $f\colon \{0,1\}^n \to \{0,1\}$ be a Boolean function.
For $x \in Q$ let x^J be a vector with all x_j flipped.

$x = (x_1, x_2, x_3, x_4, x_5, x_6, x_7, x_8)$

$x^{\{3,6\}} = (\ldots\ \bar{x}_3\ \ldots\ \bar{x}_6\ \ldots)$

- For a fixed input $x \in Q^n$:

$$\mathrm{bs}(f,x) = \max\left\{k \;\middle|\; B_1 \sqcup B_2 \sqcup \ldots \sqcup B_k \subseteq [n] : \forall i \in [k].\ f(x) \neq f(x^{B_k})\right\}$$

- In the worst case: $\mathrm{bs}(f) = \max\limits_{x \in Q^n} \mathrm{bs}(f,x)$

$x = (\underbrace{x_1, x_2}_{B_1}, x_3, x_4, x_5, x_6, x_7, \underbrace{x_8}_{B_3})$

B_2 = x_4, x_6

$B_1 \Downarrow x^{B_1}$ $\quad B_2 \Downarrow x^{B_2}$ $\quad B_3 \Downarrow x^{B_3}$

Block sensitivity

How are they related?

Block sensitivity

How are they related?

Obviously, $\mathrm{s}(f) \leq \mathrm{bs}(f)$.

$J = \{i_1, \ldots, i_k\}$ is optimal for $s(f,x)$

$\Downarrow$

Consider $B_j = \{ i_j \} \Rightarrow bs(f,x) \geq k$

Block sensitivity

How are they related?

Obviously, $\mathrm{s}(f) \leq \mathrm{bs}(f)$.

Sensitivity Conjecture [Nisan, Szegedy] (now Theorem [Huang])

$\mathrm{bs}(f) \leq \mathrm{s}(f)^C$, for a fixed constant $C \geq 1$

(It holds for $C = 4$)

Why?

Low-sensitivity (or “smooth”) functions:

Why?

Low-sensitivity (or “smooth”) functions:

- (**Computational**) are easy to compute even in the simplest models (like decision trees).

Why?

Low-sensitivity (or “smooth”) functions:

- (**Computational**) are easy to compute even in the simplest models (like decision trees).
- (**Algebraical**) have low degree as real polynomials.

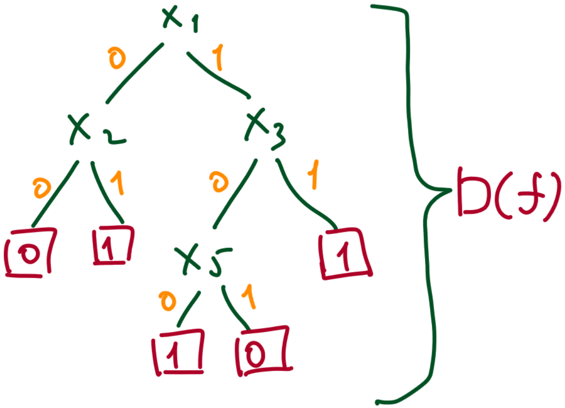
Why?

Low-sensitivity (or “smooth”) functions:

- (**Computational**) are easy to compute even in the simplest models (like decision trees).
- (**Algebraical**) have low degree as real polynomials.
- Combinatorial applications.
- Randomized and quantum query complexity.
- Certificate complexity.
- …

Computational application: Decision trees

$$f\colon \{0,1\}^n \to \{0,1\}$$



(the height of a Christmas tree with presents)

Relation with decision trees

$$\mathrm{bs}(f) \le D(f) \le \mathrm{bs}(f)^3$$

Algebraic application

Polynomial $p\colon \mathbb{R}^n \to \mathbb{R}$ represents f if

$$\text{For all } x \in \{0,1\}^n.\ p(x) = f(x).$$

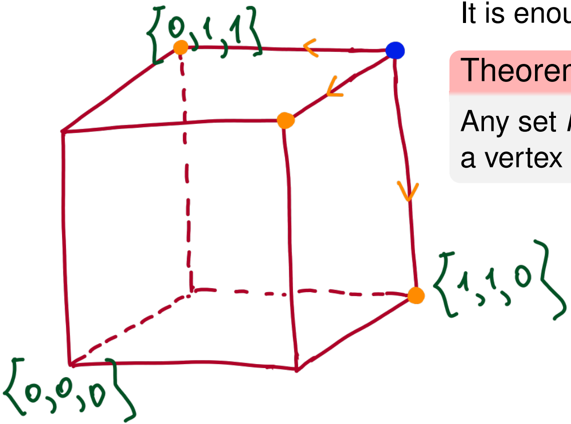
The degree $\deg(f)$ of f is the degree of a unique multilinear p that represents f.

Relation with $\deg f$

$$\sqrt{\mathrm{bs}(f)} \le \deg(f) \le \mathrm{bs}(f)^3$$

Supplementary Theorem

Let $f\colon \{0,1\}^n \to \{0,1\}$ be a Boolean function.



It is enough to prove:

Theorem: vertex with large degree

Any set H of $2^{n-1}+1$ vertices of $\{0,1\}^n$ contains a vertex with degree $\geq \sqrt{n}$.

What we need

Folklore

The linear system of m equations and $m+1$ variables has a non-trivial solution.

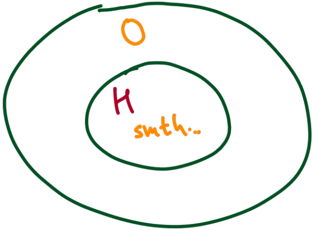
Proof (a simplification by Fedya Petrov)

Not-identically-zero function $f\colon \{0,1\}^n \to \mathbb{R}$:

- $f(x), x \in \{0,1\}^n$ are variables.
- f vanishes outside H: $2^{n-1} - 1$ equations.
- f satisfies **some** other 2^{n-1} equations.

Exists by the theorem above.

$$\begin{cases} f(\bar{H}) = 0 \\ f(y) = \dots, \text{ for all } y \in H \end{cases}$$



Proof: Weight function

For $x = (x_1, \ldots, x_k)$ define

$$w_i(x) = (-1)^{x_1 + \ldots + x_{i-1}}.$$

Clearly:

$$w_i(x) = w_i(x^i).$$

Also:

$$w_i(x) w_j(x) w_i(x^j) w_j(x^i) = -1 \text{ for } i \neq j.$$

Proof: Relations

$$\sqrt{n} \cdot f(y) = \sum_{i=1}^{n} w_i(y) f(y^i), \text{ for all } y \in \{0,1\}^n.$$

They're linearly dependent:
For $y = (x_1, \ldots, x_{n-1}, 0) = x0$:

$$\sqrt{n} \cdot f(x0) = f(x1) + \sum_{i=1}^{n-1} w_i(x) f(x^i 0), \text{ for all } y \in \{0,1\}^n,$$

$$\sqrt{n} \cdot f(x1) = f(x0) - \sum_{i=1}^{n-1} w_i(x) f(x^i 1), \text{ for all } y \in \{0,1\}^n.$$

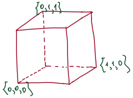
Now substitute the former into the latter.

Proof: QED

Choose $y \in \{0,1\}^n$ s.t. $|f(y)|$ is maximal. From

$$\sqrt{n} \cdot f(y) = \sum_{i=1}^{n} w_i(y) f(y^i), \text{ for all } y \in \{0,1\}^n.$$

it follows that for at least $\sqrt{n}$ elements $f(y^i) \neq 0$, hence they are in H.



Proof: Motivation

There is only 2^{n-1} linearly independent equations since the operator

$$f(y) \mapsto \sum_{i=1}^{n} w_i(y) \cdot f(y^i)$$

has an eigensubspace of dimension 2^{n-1} for the eigenvalue $\sqrt{n}$.

Possibly Part 2

- Why we defined such an operator?

Possibly Part 2

- Why we defined such an operator?
- It can be explained using expander graphs.