Huang's Proof of the Sensitivity Conjecture & Its Implications

Scott Aaronson (UT CS Dept.)

UT Math Club, Nov. 30, 2021

Boolean functions: $f: \{0,1\}^n \to \{0,1\}$

Examples: AND(x,y,z)
MAJ(x,y,z)
XOR$(x,y,z) = x+y+z \pmod 2$
OR(AND(x,y), AND(z,w))
$xy + (1-x)z$
⋮

Theoretical computer scientists care about many different ways to measure the "complexity" of Boolean functions.

Examples:

$s(f)$ = Sensitivity of f
= max # of input bits $i \in \{1,\ldots,n\}$ such that flipping them changes f $(f(x) \neq f(x^i))$

E.g., $s(\mathrm{AND}_n) = n$, only because of all-1 input
-(AND

E.g., $s(AND_n) = n$, only because of all-1 input

$$s\left(\begin{array}{c} AND \\ OR \quad OR \end{array}\right) = 2 \qquad \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}$$

$bs(f)$ = Block sensitivity of f (Nisan 1991)

Same as $s(f)$ except we look at maximum # of disjoint blocks of input bits such that flipping them changes f.

$$f(0\,1\,1\,0\,1\,0)$$

$$\forall f, \quad 0 \le s(f) \le bs(f) \le n$$

(Roughly) largest known separation between $s(f)$ & $bs(f)$: Rubinstein's Function (1995)

$$\sqrt{n}\left\{\underbrace{\begin{matrix} 0&0&0&0&0&0 \\ 0&0&0&1&0&0 \\ 1&1&1&0&0&0 \\ 0&0&0&1&1&0 \\ 0&1&0&1&0&0 \\ 0&0&0&0&0&1 \end{matrix}}_{\sqrt{n}}\right.$$

Is there at least one row with 2 consecutive 1's & everything else 0?

$$bs(\text{Rubinstein}) \sim \frac{n}{2}$$

$$s(\text{Rubinstein}) \sim 2\sqrt{n}$$

$\deg(f)$ = degree of f as a polynomial over $\mathbb{R}$

e.g. $E(x,y,z) = \begin{cases} 1 & \text{if } x=y=z \\ 0 & \text{otherwise} \end{cases}$

$\deg(E) = 2$ since $E(x,y,z) = 1 - x - y - z + xy + xz + yz$

$\widetilde{\deg}(f)$ = approximate degree of f

min. degree of a polynomial $p: \mathbb{R}^n \to \mathbb{R}$

min. degree of a polynomial $p: \mathbb{R}^n \to \mathbb{R}$ such that $|p(x) - f(x)| \leq \frac{1}{3} \quad \forall x \in \{0,1\}^n$

$D(f)$ = Deterministic query complexity of f
Minimum # of input bits queried by any algorithm (on a worst-case input)

$R(f)$ = Randomized query complexity of f

$Q(f)$ = Quantum query complexity

And many more...

By the late 90s, almost all of these measures were known to be polynomially related for all f

E.g., $D(f) \leq bs(f)^3 \qquad \widetilde{\deg}(f) \leq Q(f)$

$Q(f) \geq \sqrt{bs(f)} \qquad bs(f) \leq \deg(f)^2$

$D(f) \leq bs(f)\deg(f)$

$\vdots$ (ignoring multiplicative constants)

With one glaring exception:

$s(f) \longleftrightarrow$ $bs(f)$ $\deg(f)$ $D(f)$ $R(f)$ $\widetilde{\deg}(f)$ $Q(f)$ ...

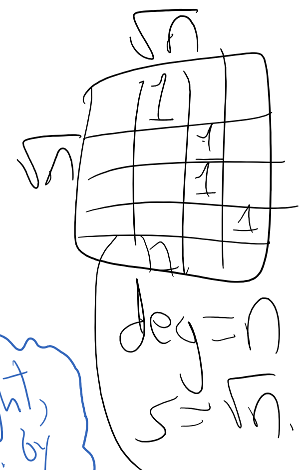
For all we knew, sensitivity could've been

For all we knew, sensitivity could've been exponentially smaller than the rest, for some f!

Best known: $bs(f) = O(e^{s(f)}\sqrt{s(f)})$
(Kenyon & Kutin 2004)

$$\boxed{\begin{array}{l}\text{The Sensitivity Conjecture (Nisan-Szegedy 1992)} \\ \text{There exists a } C \text{ s.t. } \forall f,\ bs(f) \leq s(f)^C\end{array}}$$

Was a central open problem in discrete math for 27 years. Finally proved by Hao Huang in August 2019.



Theorem: $\forall f$ $\quad s(f) \geq \sqrt{\deg(f)}$.

& this is tight, as shown e.g. by AND of ORs

As a corollary, $bs(f) \leq \deg(f)^4$!

2

Incredibly, Huang's proof was ~1 page long! So I can show it to you.

Step 1. Suffices to show that if $\deg(f) = n$, then $s(f) \geq \sqrt{n}$.

For if $\deg(f) = d < n$, then just restrict f to the input bits covered by some degree-d monomial.

Step 2 (Gotsman-Linial 1992). Consider

$$\hat{f}(x_1,\ldots,x_n) := f(x_1,\ldots,x_n) \oplus x_1+\cdots+x_n \pmod 2$$

Can check: $\forall x, i,\ f(x) \neq f(x^i) \Leftrightarrow \hat{f}(x) = \hat{f}(x^i)$

"sensitivity becomes anti-sensitivity"

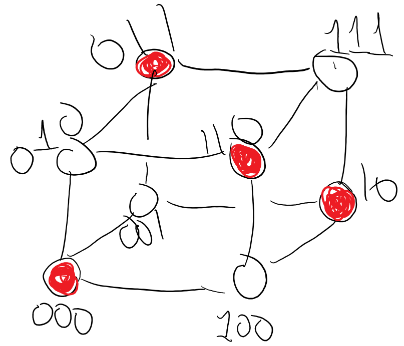
Furthermore, $\deg(f) = n \Leftrightarrow f$ has a nonzero correlation with $x_1+\cdots+x_n \pmod 2$ $\Leftrightarrow$

$$|\{x : \hat{f}(x) = 0\}| \neq |\{x : \hat{f}(x) = 1\}|$$

So let $S = \{x : \hat{f}(x) = 0\}$ or $\{x : \hat{f}(x) = 1\}$, whichever is larger. Then it suffices to prove the following:

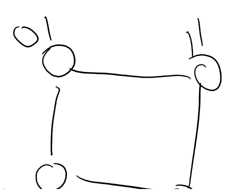
Gotsman-Linial Conjecture. Let $S \subseteq \{0,1\}^n$ with $|S| \geq 2^{n-1}+1$. Then some $x \in S$ has at least $\sqrt{n}$ neighbors in S.

$|S| = 2^{n-1}$:

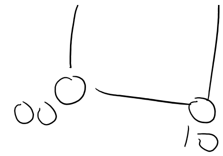


Step 3. To prove Gotsman-Linial, consider the adjacency matrix of the Boolean cube:

$$\begin{array}{c c}
 & \begin{array}{cccc} 00 & 01 & 10 & 11 \end{array} \\
\begin{array}{c} 00 \\ 01 \\ 10 \\ 11 \end{array} & \begin{pmatrix} 0 & 1 & 1 & 0 \\ 1 & 0 & 0 & 1 \\ 1 & 0 & 0 & 1 \\ 0 & 1 & 1 & 0 \end{pmatrix}
\end{array}$$



$$\begin{array}{c|cccc} 10 & 1 & 0 & 0 & 1 \\ 11 & 0 & 1 & 1 & 0 \end{array}\Bigg)$$



Or rather, a variant of the adjacency matrix where we judiciously change some 1's to -1's:

$$A_1 = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}, \quad A_n = \left(\begin{array}{c|c} A_{n-1} & I \\ \hline I & -A_{n-1} \end{array}\right)$$

e.g., $A_2 = \begin{pmatrix} 0 & 1 & 1 & 0 \\ 1 & 0 & 0 & 1 \\ 1 & 0 & 0 & -1 \\ 0 & 1 & -1 & 0 \end{pmatrix}$

$$A_3 = \left(\begin{array}{cccc|cccc} 0 & 1 & 1 & 0 & 1 & 0 & 0 & 0 \\ 1 & 0 & 0 & 1 & 0 & 1 & 0 & 0 \\ 1 & 0 & 0 & -1 & 0 & 0 & 1 & 0 \\ 0 & 1 & -1 & 0 & 0 & 0 & 0 & 1 \\ \hline 1 & 0 & 0 & 0 & 0 & -1 & -1 & 0 \\ 0 & 1 & 0 & 0 & -1 & 0 & 0 & -1 \\ 0 & 0 & 1 & 0 & -1 & 0 & 0 & 1 \\ 0 & 0 & 0 & 1 & 0 & -1 & 1 & 0 \end{array}\right)$$

$\vdots$

Step 4.

Lemma: A_n's eigenvalues are $\sqrt{n}$ & $-\sqrt{n}$, both with multiplicity 2^{n-1}

Proof: We'll show by induction that $A_n^2 = nI$.

Base case: $\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}^2 = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$.

Now suppose $A_{n-1}^2 = (n-1)I$; then

$$A_n^2 = \begin{pmatrix} A_{n-1} & I \\ I & -A_{n-1} \end{pmatrix}^2 = \begin{pmatrix} A_{n-1}^2 + I & 0 \\ 0 & A_{n-1}^2 + I \end{pmatrix} = nI.$$

Thus, A_n's eigenvalues must all be $\sqrt{n}$ or $-\sqrt{n}$.
Since $\mathrm{Tr}(A_n) = 0$, half must be $\sqrt{n}$ & half $-\sqrt{n}$. ∎

<u>Step 5</u>. Let $S \subseteq \{0,1\}^n$ with $|S| \geq 2^{n-1}+1$.
Let V_S be the subspace of $\mathbb{R}^{2^n}$ consisting of all vectors $\vec{v}$ such that $x \notin S \Rightarrow \vec{v}_x = 0$.
Let W be the $+\sqrt{n}$-eigenspace of A_n.
Then
$$\begin{cases} \dim(V_S) = |S| \geq 2^{n-1}+1, \\ \dim(W) = 2^{n-1} \end{cases}$$
$$\Rightarrow \dim(V_S \cap W) \geq 1.$$

I.e., A_n has at least one $+\sqrt{n}$ eigenvector $\vec{v}$ that's entirely supported on S

$$S \quad \left(\begin{array}{cccc|cccc} 0 & 1 & 1 & 0 & 1 & 0 & 0 & 0 \\ 1 & 0 & 0 & 1 & 0 & 1 & 0 & 0 \\ 1 & 0 & 0 & -1 & 0 & 0 & 1 & 0 \\ 0 & 1 & -1 & 0 & 0 & 0 & 0 & 1 \\ \hline 1 & 0 & 0 & 0 & 0 & -1 & -1 & 0 \\ 0 & 1 & 0 & 0 & -1 & 0 & 0 & -1 \\ 0 & 0 & 1 & 0 & -1 & 0 & 0 & 1 \\ 0 & 0 & 0 & 1 & 0 & -1 & 1 & 0 \end{array}\right) \left(\begin{array}{c} v_1 \\ v_2 \\ v_3 \\ 0 \\ \hline v_4 \\ v_5 \\ 0 \\ 0 \end{array}\right) \leftarrow \text{the } +\sqrt{n} \text{ eigenvector } \vec{v}$$

<u>Step 6</u>. Let $\Delta(S) = \max_{x \in S} (\#\text{ of neighbors of } x \text{ in } S)$.
Let $A_n \vec{v} = \lambda \vec{v}$ (max degree of induced

Let $A_n\vec{v} = \lambda\vec{v}$. (max degree of induced subgraph)

<u>Lemma</u>: $|\lambda| \leq \Delta(S)$.

<u>Proof</u>: Let v_x be the coordinate of $\vec{v}$ $A_n\vec{v} = \lambda\vec{v}$ with the largest absolute value. Then

$$|\lambda v_x| = |(A_n\vec{v})_x| \leq \sum_{y \in S} |(A_n)_{x,y}||v_y| \leq \Delta(S)|v_x|.$$

But $\lambda = \sqrt{n}$, so $\Delta(S) \geq \sqrt{n}$ as well!

Q.E.D.

Since 1998, the best known relationship between classical & quantum query complexities of Boolean functions was

$$D(f) = O(Q(f)^6) \;\; \forall f$$

A., Ben-David, Kothari, Rao, Tal 2020: Using Huang's Sensitivity Theorem, we improved this to

$$D(f) = O(Q(f)^4) \;\; \forall f$$

(shown to be tight by Ambainis et al. 2015)

<u>Idea</u>: Given $f: \{0,1\}^n \to \{0,1\}$, define

the "$2^n \times 2^n$" matrix A_f by

$$(A_f)_{x,y} = \begin{cases} 1 & \text{if } x \,\&\, y \text{ are neighbors } \& \ f(x) \neq f(y) \\ 0 & \text{otherwise.} \end{cases}$$

Let $\lambda(f)$, the <u>spectral sensitivity</u> of f, be $\lambda_{max}(A_f)$.

We can reinterpret Huang as showing:

$$\boxed{\sqrt{\deg(f)} \leq \lambda(f) \leq s(f)}$$

But one can also show:

$$\boxed{\lambda(f) \leq Q(f)}$$

Hence

$$\deg(f) \leq Q(f)^2.$$

So

$$D(f) \leq bs(f) \cdot \deg(f) \qquad \text{(Midrijanis 2004)}$$
$$\leq Q(f)^4.$$

We also showed:

$$\lambda(f) \leq \widetilde{\deg}(f)$$

$$\Rightarrow \deg(f) \leq \lambda(f)^2 \leq \widetilde{\deg}(f)^2$$

solving another 30-year-old open problem of Nisan & Szegedy, on the largest possible separation between degree & approximate degree (previously only $\deg(f) \leq \widetilde{\deg}(f)^6$ was known)

Thanks!