Huang's Proof of the Sensitivity Conjecture & Its Implications

Scott Aaronson (UT CS Dept.)
UT Math Club, Nov. 30, 2021

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

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

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

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

E.g., $S(\text{AND}_n) = n$, only because of all-1 input.
  - $\neg \text{ AND}$
E.g., \( \text{SHANNON}_{AB} \), only because of all-T input
\[
S\left( \text{AND} \bigoplus \text{OR} \right) = 2
\]

\[
\begin{array}{c|cc|}
\text{AND} & 0 & 1 \\
\hline
0 & 0 & 0 \\
1 & 0 & 1 \\
\end{array}
\]

\[
\begin{array}{c|c|}
\text{OR} & 0 & 1 \\
\hline
0 & 0 & 1 \\
1 & 1 & 1 \\
\end{array}
\]

\[bs(f) = \text{Block sensitivity of } f \quad (\text{Nisan } 1991)\]

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

\[f(01110100)\]

\[\forall f, \quad 0 \leq s(f) \leq bs(f) \leq n\]

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

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

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

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

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

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

\[\deg(E) = 2 \text{ since } E(x, y, z) = 1 - x - y - z + xy + xz + yz\]

\[\deg(f) = \text{approximate degree of } f\]

Min. degree of a polynomial \( p: \mathbb{R}^n \rightarrow \mathbb{R}\)

\[p = f + y + 1 \sim 1.11\]
min. degree of a polynomial \( p: \mathbb{R}^n \rightarrow \mathbb{R} \) such that \( \| p(x) - f(x) \| \leq \frac{1}{3} \) \( \forall x \in \mathbb{R}^n \)

\( D(f) = \) 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., \( D(f) \leq 6s(f)^3 \) \( \deg(f) \leq Q(f) \)

\( Q(f) \geq \sqrt{6s(f)} \) \( 6s(f) \leq \deg(f)^2 \)

\( D(f) \leq 6s(f) \deg(f) \)

(ignoring multiplicative constants)

With one glaring exception:

For all we know, \( s(f) \geq 1 \) has been...
For all we knew, sensitivity could've been exponentially smaller than the rest, for some $f$!

Best known: $bs(f) = O(\varepsilon^{5(f)} \sqrt{s(f)})$

(Kenyon & Kutin 2004)

**The Sensitivity Conjecture (Nisan-Szegedy 1992)**

There exists a $C$ s.t. $\forall f$, $bs(f) \leq s(f)C$

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

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

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

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
\[ \hat{f}(x_1, \ldots, x_n) := f(x_1, \ldots, x_n) \Theta (x_1 + \cdots + x_n \pmod{2}) \]

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 non-zero correlation with \( x_1 + \cdots + x_n \pmod{2} \)

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

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

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

\[ |S| = 2^{n-1} \]

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

\[
\begin{pmatrix}
0 & 1 & 1 & 1 & 1 & 0 & 0 & 0 \\
1 & 0 & 1 & 1 & 1 & 0 & 0 & 0 \\
1 & 1 & 0 & 1 & 1 & 0 & 0 & 0 \\
1 & 1 & 1 & 0 & 1 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 1 & 1 & 1 \\
0 & 0 & 0 & 0 & 0 & 1 & 1 & 1 \\
0 & 0 & 0 & 0 & 0 & 1 & 1 & 1 \\
0 & 0 & 0 & 0 & 0 & 1 & 1 & 1
\end{pmatrix}
\]
\[
\begin{pmatrix}
1 & 0 & 0 & 0 & 1 \\
0 & 1 & 0 & 0 & 0
\end{pmatrix}
\]

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

\[
A_2 = \begin{pmatrix} 1 & 1 \\
1 & 0 
\end{pmatrix}, \\
A_n = \begin{pmatrix} A_{n-1} & I \\
I & -A_{n-1} \end{pmatrix}
\]

E.g., \[A_2 = \begin{pmatrix} 0 & 1 & 1 & 0 \\
1 & 0 & 0 & 1 \\
1 & 0 & 0 & -1 \\
0 & 1 & -1 & 0 
\end{pmatrix}\]

\[
A_3 = \begin{pmatrix}
0 & 1 & 1 & 0 & 0 & 0 \\
1 & 0 & 0 & 1 & 0 & 0 \\
1 & 0 & 0 & -1 & 0 & 0 \\
0 & 1 & 1 & 0 & 0 & 0 \\
1 & 0 & 0 & -1 & 0 & 0 \\
0 & 1 & -1 & 0 & 0 & 1 \\
0 & 0 & 0 & 1 & 0 & -1 \\
0 & 0 & 0 & -1 & 0 & 1 \\
0 & 0 & 1 & -1 & 0 & 0 \\
0 & 0 & -1 & 0 & 1 & 0 \\
\end{pmatrix}
\]

**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:** \((0 \ 1)^2 = (1 \ 0)\).

Now suppose \(A_{n-1} = (n-1)I\); then
\[ A_n^2 = \begin{pmatrix} A_{n-1} & I \\ I & -A_{n-1} \end{pmatrix} = \begin{pmatrix} A_{n-1}^2 + I & 0 \\ 0 & A_{n-1}^2 + I \end{pmatrix} = nI. \]

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

**Step 5.** 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 \( \vec{y} \) such that \( x \in S \Rightarrow \vec{y}_x = 0 \).

Let \( W \) be the \( +\sqrt{n} \)-eigenspace of \( A_n \).

Then \( \begin{cases} \dim(V_S) = |S| \geq 2^{n-1} + 1, \\ \dim(W) = 2^{n-1} \\ \Rightarrow \dim(V_S \cap W) \geq 1. \end{cases} \)

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

\[
\begin{bmatrix}
0 & 1 & 0 & \cdots \\
1 & 0 & 0 & 1 \\
1 & 0 & 0 & -1 \\
0 & 1 & -1 & 0 \\
\end{bmatrix}
\begin{bmatrix}
\ast & \ast \\
0 & 1 & 0 & \ast \\
0 & 0 & 0 & 1 \\
0 & 0 & 1 & 0 \\
\end{bmatrix}
\begin{bmatrix}
V_1 \\
V_2 \\
V_3 \\
V_4 \\
V_5 \\
0 \\
0 \\
\end{bmatrix}
\rightarrow \begin{bmatrix}
V_1 \\
V_2 \\
V_3 \\
V_4 \\
V_5 \\
0 \\
0 \\
\end{bmatrix}
\]

is the \( +\sqrt{n} \) eigenvector \( \vec{v} \)

**Step 6.** Let \( \Delta(S) = \max_{x \in S} \text{(number of neighbors of } x \text{ in } S) \).

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

**Lemma:** $|\lambda| \leq \Delta(S)$.

**Proof:** Let $V_x$ be the coordinate of $\overrightarrow{V}$ $A_\lambda \overrightarrow{V} = \lambda \overrightarrow{V}$ with the largest absolute value. Then

$$|\lambda V_x| = |(A_\lambda \overrightarrow{V})_x| \leq \sum_{y \in S} |(A_\lambda \overrightarrow{V})_y| |V_y| \leq \Delta(S) |V_x|.$$

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

$$D(f) = O(Q(f)^5) \quad \forall f$$

A., Ben-David, Kothari, Rao, Tal 2020:

Using Huang’s Sensitivity Theorem, we improved this to

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

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

Idea: Given $f: \mathbb{F}_2^n \rightarrow \{0,1\}$, define
the $2^2 \times 2^2$ 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 spectral sensitivity of $f$, be $\lambda_{\max}(A_f)$.

We can reinterpret Huang as showing:

$$ \sum_{\deg(f)} \leq \lambda(f) \leq s(f) $$

But one can also show:

$$ \lambda(f) \leq Q(f) $$

Hence

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

So

$$ D(f) \leq 6s(f) \cdot \deg(f) \leq Q(f)^4 $$

(Midrijanis 2004)

We also showed:

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

$$ \Rightarrow \deg(f) \leq \lambda(f)^2 \leq \overline{\deg}(f)^2 $$
solving another 30-year-old open problem of Nisan & Szegedy, on the largest possible separation between degree & approximate degree 
(previously only $\deg(f) \leq \deg(f)^6$ was known)

Thanks!