COMS E6998.003: Lower Bounds in Theoretical Computer Science Sep 10, 2013

Lecture Sep 10, 2013

Instructor: *Xi Chen* Scribes: *Anthi Orfanou*

1 Deterministic complexity measures and their relations

In the previous lecture we have seen that it holds that $D(f) \geq C(f) \geq bs(f) \geq s(f)$ for boolean functions $f : \{0,1\}^n \to \{0,1\}$. It is an open question if $D(f)$ can be upper bounded by a power of $s(f)$, e.g. if $(s(f))^{100} \geq D(f) \geq s(f)$.

Example 1. *Let $n = 4k^2$ and let f be a function that takes as input a boolean matrix of dimensions $2k \times 2k$. The function outputs 1 if there is a row of the form $0^a 110^b$ for $a, b \geq 0$, otherwise it outputs 0. For the above function we have that:*

- *$s_x(f) = \sqrt{n}$ for the worst case input x with one row congaing exactly two consecutive 1 that allows you many ways to change the value by flipping a bit.*
- *$bs(f) = n/2$, for the zero matrix input were we need to flip two consecutive bits that count as a block to 1 to change the function's output.*
- *$D(f) = n$.*

The above example is the biggest gap we have between the $s(f), bs(f)$ measures. It is an open question whether there are functions f for which $bs(f) >> (s(f))^2$. Another open questions is whether there is a constant k such that $bs(f) \leq O(s^k(f))$ for all functions f.

Theorem 2. *It holds that $D(f) \leq (bs(f))^3$.*

Proof. We need to show the following:

I. $C(f) \leq s(f) \cdot bs(f)$

II. $D(f) \leq C_1(f) \cdot bs(f),\ D(f) \leq C_0(f)$

Lemma 3. *If $B \subseteq [n]$ is a minimal sensitive block for x then $|B| \leq s(f)$*

Proof. As B is a minimal sensitive block for x we have that $f(x) \neq f(x^{(B)})$. If we pick an $i \in B$ then it must be the case that $f(x) = f(x^{(B-\{i\})}) \neq f(x^{(B)})$ since B is minimal. Thus we have $s(f) \geq s_{x^{(B)}}(f) \geq |B|$. □

Proof. **(I.)** : Given x, f we need to find a certificate C for x with $|C| \leq s(f) \cdot bs(f)$. Let $B_1, \ldots, B_b$ be disjoint minimal sensitive blocks for x with $b = bs_x(f)$. Thus we have that $|B_i| \leq s(f)$. Our goal is to show that $C = \cup_i B_i$ is a certificate for x. If it wasn't there would be a a y such that $y/c = x/c$ but $f(y) \neq f(x)$. Thus there is a B such that $B \cap C = \emptyset$ and by having $y = x^{(B)}$ we contradict the fact that $b = bs_x(f)$.

□

Proof. **(II.)** : (The proof is for $C_1(f)$, similarly for $C_0(f)$). For this part we design an algorithm A deciding $f(x)$:

- Maintain a set $X \subseteq \{0,1\}^n$ which contains all strings that are consistent with the query results so far (initially $X = \{0,1\}^n$).
- Repeat $bs(f)$ many times:
  - Check is all $x \in X$ have the same $f(x) = b$. If yes then output b.
  - If there is a $y \in X$ with $f(y) = 1$:
    - We can find a certificate C of y with $|C| = C_y(f)$. If there is no such C we return 0.
    - We query all variables in C that have not yet been queried.
    - We update X.
- We check if all $x \in X$ have the same $f(x)$.

The above algorithm terminates with $bs(f)$ loops and queries $C_1(f)$ variables in each iteration. For correctness proof we assume towards contradiction that during the check step that there is a $z \in \{0,1\}^n$ such that $f(z) = 0$ that survived. In loop 1 we picked a y_1 that is consistent with all queries so far and all variables in C_1 are queried.

Claim 4. *There is a $B_1 \subseteq C_1$ such that B_1 is sensitive block for z.*

Then in loop 2 we pick a y_2 that is consistent will queries so far and C_2 is a certificate for y_2 (with $f(y_2) = 1$). Thus all variables in $C_2 - C_1$ are queried.

Claim 5. *There is a $B_2 \subseteq C_2 - C_1$ such that B_2 is a sensitive block for z.*

C_2 will have some bits same as C_1 along with new bits. We know that $z/C_2 \neq y_2/C_2$ and $z/C_1 \neq y_2/C_1$. By the end of the algorithm we have $b+1$ disjoint sensitive blocks $B_1, \ldots, B_{b+1}$ ($B_i \subseteq C_i - C_{i-1}$) for z contradicting the block sensitivity being $bs(f)$.

□

□

2 The degree of a function

Definition 6. *We define the degree of $f : \{0,1\}^n \to \{0,1\}$ $deg(f)$ as the degree of the polynomial $p : \mathbb{R}^n \to \mathbb{R}$ such that $p(x) = f(x)$ for all $x \in \{0,1\}^n$.*

We observe that the above polynomial will be a multilinear polynomial, i.e. a polynomial of the form $p(x) = \sum_{S \subseteq [n]} a_S \prod_{i \in S} x_i$.

Lemma 7. *For every f there is a unique multilinear polynomial p such that $p(x) = f(x)$ over all $x \in \{0,1\}^n$.*

The degree of f $deg(f)$ will be the degree of this unique p, so it is well defined.

Example 8. *Let $n = 3^k$ and consider the function consisting of k levels of the function $E(x_1x_2x_3)$ which is 1 there are either 1 or 2 "1" in $(x_1x_2x_3)$, otherwise it is 0.*

We have that $deg(f) = 2^k$ and the corresponding polynomial is $p_E = x_1 + x_2 + x_3 - x_1x_2 - x_2x_3 - x_1x_3$ over all $x \in \{0,1\}^3$. It also holds that $D(f) = 3^k$.

Theorem 9. *It holds that $D(f) \geq deg(f)$.*

Proof. We can see that from constructively by following a path along the decision tree of f of depth d. For example the path (x_1) with value $0 \to (x_2)$ with value $1 \to (x_3)$ with value $0 \to 1$, from the root of the decision tree to a leaf with value 1 can be represented as $(1 - x_1)x_2(1 - x_3)$. Thus the degree of the polynomial representing each path is at most $D(f)$. □

Theorem 10. *It holds that $D(f) \leq O(deg^4(f))$.*

To show that we need to prove that:

A. $bs(f) \leq 2(deg(f))^2$

B. $D(f) \leq (deg(f))^2 \cdot bs(f) \leq (deg(f))^4$.

Lemma 11. *Markov brother's inequality: For every polynomial $p : \mathbb{R} \to \mathbb{R}$ of degree d it holds that*

$$\max_{x\in[-1,1]} |p'(x)| \leq d^2 \max_{x\in[-1,1]} |p(x)|.$$

Corollary 12. *If for a polynomial p of degree d we have $c \leq p(x) \leq d$ for $a \leq x \leq b$ then*

$$\max_{x\in[a,b]} |p'(x)| \leq d^2 \frac{d-c}{b-a}.$$

Theorem 13. *For a polynomial $p : \mathbb{R} \to \mathbb{R}$ with $b_1 \leq p(i) \leq b_2$ for all integers $0 \leq i \leq n$ and $|p'(x)| \geq c$ for some $0 \leq x \leq n$ it holds that $deg(p) \geq \sqrt{cn/(c + b_2 - b_1)}$.*

Proof. Let $\beta = \max\{0, \max_{0\leq x\leq n} p(x) - b_2, max_{0\leq x\leq n} b_1 - p(x)\}$.

- Case $\beta = 0$: Then we apply the corollary for $a = 0,\ b = n,\ c = b_1,\ d = b_2$ so that we have $(deg(p))^2 \frac{b_2-b_1}{n} \geq c \Rightarrow deg(p) \geq \sqrt{\frac{nc}{b_2-b_1}}$.
- Case $\beta > 0$, $b = \max_{0\leq x\leq n}$. Then we apply the corollary for $a = 0,\ b = n,\ c = b_1 - \beta,\ d = b_2 + \beta$ so that we have $(deg(p))^2 \frac{b_2-b_1+2\beta}{n} \geq c$. In this case there must be a x with $|p'(X)| \geq 2\beta$ so we can use 2β in the place of c, having that $(deg(p))^2 \frac{b_2-b_1+2\beta}{n} \geq 2\beta$. From the above we conclude that $\frac{(deg(p))^2}{n} \geq \max\{\frac{c}{b_2-b_1+2\beta}, \frac{2\beta}{b_2-b_1+2\beta}\}$

□

To prove theorem 10 [A.] we need to prove that $deg(f) \geq \sqrt{\frac{b}{2}}$ with $b = bs(f)$. The full proof is given in the following lecture. For now we describe the steps towards that.

First we consider a polynomial p of degree $deg(f) = d$ such that $p(x) = f(x)$ for all $x \in \{0,1\}^n$.

- We construct a new polynomial $g(y_1 \dots y_b)$ from p with: $deg(g) \leq deg(f)$, $g(\vec{0}) = 0$ and $g(\vec{e_i}) = 1$.

- We construct a symmetric function h from g (due to Minsky-Papert), being $h(x)\sum_{\pi\in S_b}\frac{g(x_\pi)}{b!}$. A symmetric function is a function that its outcome does not change if we permute the input variables.
  - The function h is symmetric as its value depends only on the Hamming weight of the input. That is there is a function $f^*:[0,n]\to\mathbb{R}$ such that $h(x)=h^*(|x|)$.
  - h^* has degree $\leq deg(g)(\leq deg(f))$ and $h^*(0)=0, h^*(1)=1$.
  - We can now use the corollary on h^*