COMS 6998: Lower Bounds in Theoretical Computer Science Sep 17, 2013

Lecture 3 – Degree and Block Sensitivity; Evasiveness

Instructor: *Xi Chen* Scribe: *Yuan Kang*

1 Relationship between Degree and Block Sensitivity

Last time we proved the following theorem:

Theorem 1. *If a single-variable polynomial, $p : \mathbb{R} \to \mathbb{R}$, has the following properties:*

- $\forall i \in \{0, 1, \ldots, n\} : p(i) \in [b_1, b_2]$ *for some constants* b_1, b_2.
- $\exists x \in [0, n] : |p'(x)| \geq c$, *for some constant* c.

Then $deg(p) \geq \sqrt{\frac{cn}{c+b_2-b_1}}$.

We want to use it to prove the following theorem:

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

Proof. Let $b = bs(f), d = \deg(f)$.

Without loss of generality assume that:

1. $x = \vec{0}$ is the string that contains b disjoint, sensitive blocks. If that is not the case, then we can prove the inequality with $f_1(x) = f(x \oplus m)$, where m is the string that satisfies the condition for $bs(f) = b$. We will denote the sensitive blocks by $A_1, \ldots, A_b$. Note that they all have 0-bits, only.
2. $f(\vec{0}) = 0$. Otherwise, we can use $f_1(x) = 1 - f(x)$.

Let us also assign the unique, multilinear polynomial $p : \mathbb{R}^n \to \mathbb{R}$, which we know has the following properties:

1. $\deg(p) = d$
2. $\forall x \in \{0, 1\}^n : p(x) = f(x)$

Let us define a function q, that takes as input a bit for each sensitive block. In particular:

$$q(y_1, \ldots, y_b) \quad = \quad p(x_1, \ldots, x_n)$$

Where $\forall i \in [n]$, we replace x_i as follows.

$$\begin{cases} \text{if } \exists j \in [b], \text{ st. } i \in A_j, \text{ set } x_i = y_j \\ \text{else, set } x_i = 0 \end{cases}$$

q has the following properties:

1. Since q just replaces the inputs of p with constants and inputs of q, we know that q is a multilinear polynomial, where $\deg(q) \leq \deg(p) = d$

2. $\forall y \in \{0,1\}^b, q(y) \in \{0,1\}$. [1]

3. By our assumption, $q(\vec{0_b}) = p(\vec{0_n}) = 0$.

   On the other hand, flipping exactly one bit in $\vec{0_b}$ is equivalent to flipping exactly one sensitive block in $\vec{0_n}$. Specifically, if we define $\vec{e_i} \in \{0,1\}^b$ to have only one 1-bit, at position $i \in [b]$, $q(\vec{e_i})$ flips all the bits x_j, where $j \in A_i$, while the rest remain 0. So by the definition of sensitive blocks, $q(\vec{e_i}) = p(\vec{0}^{(A_i)}) = 1$.

Now we symmetrize q. If we define S_b as the set of all b-size permutations, define $q^{sym}(x) = \frac{1}{b!}\sum_{\pi \in S_b} q(\pi(x))$. It is easy to see that q^{sym} has the following properties:

1. q^{sym} is also a multilinear polynomial , where $\deg(q^{sym}) \leq \deg(q) = d$. [2]

2. q^{sym} is symmetric. In other words

$$\forall \pi \in S_b, \forall x \in \{0,1\}^b, q^{sym}(x) = q^{sym}(\pi(x))$$

[3]

We introduce an additional lemma to turn the multilinear polynomial into a single-variable polynomial, so that we can use the aforementioned theorem.

Lemma 3. *For a symmetric function, $q^{sym} : \{0,1\}^b \to \{0,1\}$, of degree d', there exists a function, $r : \{0,\ldots,b\} \to \{0,1\}$, so that $\forall x \in \{0,1\}^b, q^{sym}(x) = r(|x|)$, and deg$(r) \leq d'$.*

Proof. Since q^{sym} is symmetric, we can inductively prove that the polynomial is of the form:

$$q^{sym} = \sum_{i=0}^{d'} c_i V_i$$

Where c_i is some constant, and V_i contains all the monomials of i variables. [4]

This form gives us the single-variable function:

$$r(|y|) = \sum_{i=0}^{d'} c_i \binom{|y|}{i}$$

[1] This is because q passes a subset of $\{0,1\}^n$ into p, which must output 0 or 1.

[2] q^{sym} permutes the input variables of q, adds the results together, and divides them by a constant.

[3] This property holds, because when either x or $\pi(x)$ is passed into the symmetrization formula, the term for $\pi'(\pi(x))$ in the second sum corresponds to exactly one term, $\pi''(x)$ in the first sum, since the composition, $\pi'' = \pi'\pi$, is also a permutation.

[4] Clearly a constant multilinear polynomial is of the form c_0. When we inductively add on terms of the next degree, k, each new monomial must have the same coefficient, c_k. Otherwise, if there is a k-degree monomial of a different coefficient, its contribution, if only all of its bits are set to 1, is different from the contribution of some other k-degree monomial, with its respective input.

We can replace V_i with $\binom{|y|}{i}$, because the value of V_i is exactly the number of monomials with all of its i bits set to 1, and since V_i contains all ways to choose i 1-bits from a set of $|y|$, there are $\binom{|y|}{i}$ such monomials. Moreover $\binom{|y|}{i} = \frac{1}{i!}\prod_{j=0}^{i-1}(|y|-j)$, which is a polynomial over $|y|$, of degree $i \leq d'$, so r is a polynomial over $|y|$ of degree at most d'. □

In addition to the results of the lemma, our r has these additional properties:

1. $r(0) = q^{sym}(\vec{0_b}) = \frac{1}{b!}\sum_{\pi\in S_b} q(\vec{0_b}) = \frac{1}{b!}\sum_{\pi\in S_b} 0 = 0$.
2. $r(1) = q^{sym}(\vec{e_i}) = \frac{1}{b!}\sum_{\pi\in S_b} q(\pi(\vec{e_i})) = \frac{1}{b!}\sum_{\pi\in S_b} 1 = 1$.
3. $\forall i \in \{2,\ldots,b\} : r(i) \in [0,1]$, since r must still output 0 or 1, as did q^{sym} and q.

When we combine the first two properties, the Mean Value Theorem tells us that there exists $x \in [0,1] \subseteq [0,n]$, where $r'(x) = \frac{1-0}{1-0} = 1$.

Based on the relationship between the polynomials we constructed, and Theorem 1:

$$\begin{aligned} \deg(f) = \deg(p) \geq \deg(q) \geq \deg(q^{sym}) \geq \deg(r) &\geq \sqrt{\frac{b}{2}} \\ \deg(f) &\geq \sqrt{\frac{b}{2}} \\ 2(\deg(f))^2 &\geq b \end{aligned}$$

□

Overall, using the inequalities from the past lectures, we have:

$$\deg(f) \leq D(f) \leq (bs(f))^3 \leq (2(\deg(f))^2)^3 = 8(\deg(f))^6$$

2 Evasiveness Conjectures and Theorems

2.1 Graph Properties and the AKR Conjecture

We begin with defining the terms used in the AKR conjecture.

Definition 4. *$x \in \{0,1\}^{\binom{n}{2}}$ represents the graph, $G = ([n], E)$, where for each potential edge $\{i,j\}$, $x_{\{i,j\}} = 1 \Leftrightarrow \{i,j\} \in E$.*

Definition 5. *A graph property is the boolean function, $f : \{0,1\}^{\binom{n}{2}} \to \{0,1\}$, if for any two graphs,*

$x \in \{0,1\}^{\binom{n}{2}}, y \in \{0,1\}^{\binom{n}{2}}$:

$$\begin{aligned} \textit{If} \quad & \exists \text{ permutation } \pi \in S_n, \text{ so that } x_{\{i,j\}} = y_{\{\pi(i),\pi(j)\}}, \forall i \in [n], j \in [n] \\ \textit{Then} \quad & f(x) = f(y) \end{aligned}$$

Intuitively, we mean that f is independent of labeling, and that it has the same value for 2 isomorphic graphs.

Note that, in spite of similarities, a graph property is not the same as a symmetric function. To permute an edge, all edges sharing an endpoint must also be permuted, while for a symmetric property, any permutation of the bits is allowed.

Definition 6. *A boolean function, $f : \{0,1\}^n \to \{0,1\}$ is monotone iff $f(x) \leq f(y)$ for all $x \leq y$, by which we mean $\forall i \in [n] : x_i \leq y_i$.*

There are many non-trivial examples of graph properties that are monotone, such as connectivity, or where $1 - f(x)$ is monotone, such as planarity. So far, all the examples we know are evasive. This gives rise to the AKR conjecture:

Definition 7. *AKR Conjecture:*

Every non-constant, monotone graph property is evasive, ie. $D(f) = \binom{n}{2}$.

We do know the following:

- $D(f) = \Omega(\binom{n}{2})$. But we do not know if the factor must be 1.
- If n is a prime power p^k, then f is evasive. We will prove this from a more general theorem.

2.2 General Evasiveness

We can generalize the AKR conjecture. But we also need some other generalized definitions first:

Definition 8. *A boolean function, $f : \{0,1\}^n \to \{0,1\}$ is invariant with relation to permutation $\pi \in S_n$, if $\forall x \in \{0,1\}^n : f(x) = f(\pi(x))$.*

Definition 9. *A boolean function, $f : \{0,1\}^n \to \{0,1\}$ is invariant with relation to permutation set $S \subseteq S_n$, if $\forall \pi \in S$, f is invariant with relation to π.*

Definition 10. *A permutation group, $S \subseteq S_n$, is transitive if $\forall i \in [n], j \in [n] : \exists \pi \in S$ st. $\pi(i) = j$. In other words, any particular position can be permuted to another position.*

Definition 11. *Evasiveness Conjecture:*

A non-constant, monotone, boolean function, $f : \{0,1\}^n \to \{0,1\}$ that is invariant with relation to a transitive permutation group, $S \subseteq S_b$, is evasive.

This implies the AKR conjecture, since the set of all the possible node permutations form a group, and let us permute any edge (ie. any two nodes) to any edge.

We can prove the conjecture for the case of a prime power, $n = p^k$. We will need some more definitions and lemmas.

Definition 12. $f^{-1}(0) = \{x \in \{0,1\}^n : f(x) = 0\}$
Likewise, $f^{-1}(1) = \{x \in \{0,1\}^n : f(x) = 1\}$.

The next two lemmas relate to evasiveness and the number of inverses.

Lemma 13. *If* $|f^{-1}(0)|$ *(respectively* $|f^{-1}(1)|$*) is odd, then* $D(f) = n$*, ie.* f *is evasive.*

Proof. Assume non-evasiveness, so that all leaves have a depth of at most $n-1$.

So if we pick a leaf of value 0 (respectively 1), of depth $d \leq n-1$, we know that the distinct [5] strings that will take the path to this leaf will have d bits specified, and will vary in the remaining $n-d$ bits. So there are 2^{n-d} strings that take the path to this leaf, which is an even number, since $n-d \geq 1$. So each 0-leaf (respectively 1-leaf) contributes an even number to $|f^{-1}(0)|$ (respectively $|f^{-1}(1)|$), which is then even. □

The next, stronger lemma is what we will use for the theorem we will prove, but it relies on the same principles:

Lemma 14. *If* f *is not evasive,* $f^{-1}(0)$ *(respectively* $f^{-1}(1)$*) must have the same number of strings with even and odd Hamming weights.*

Proof. Again, assume non-evasiveness.

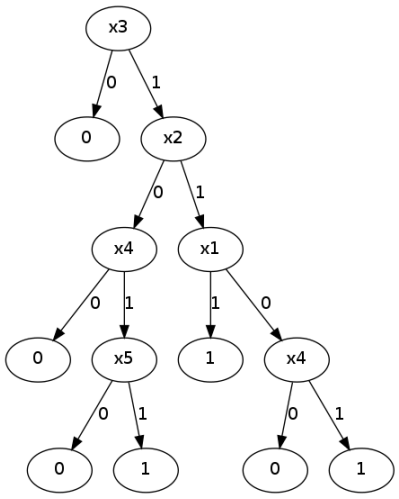
So if we pick a leaf of value 0 (respectively 1), which must have depth $d \leq n-1$, the strings that take the path to this leaf will vary by $n-d \geq 1$ unspecified bits. So a string, x, that ends in this leaf is in $f^{-1}(0)$ (respectively $f^{-1}(1)$). We can flip the parity of its Hamming weight, while still keeping it in $f^{-1}(0)$ (respectively $f^{-1}(1)$), by flipping its last unspecified bit, ie. by changing its Hamming weight by 1. So there is a one-to-one relationship between the strings with even and odd Hamming weights in $f^{-1}(0)$ (respectively $f^{-1}(1)$), so that they are same in number. □

Example 15. *Define the following function:*

$$f(x) = \begin{cases} 1, & \textit{if there are 3 consecutive 1's} \\ 0, & \textit{otherwise} \end{cases}$$

f *is evasive for* $n = 7$*, but not for* $n = 5$*. For example, we can construct the following tree of depth* 4*.*

[5] A string cannot end at multiple leaves, because then the string would have to have both values at the first node where the paths split



We have 8 *strings in* $f^{-1}(1)$, 4 *of which have even Hamming weight, and* 4 *of which have odd Hamming weight. The leaf reached by* $x_3 \to x_2 \to x_1 \to 1$, *of depth* 3 *contributes* $2^{5-3} = 4$ *strings, where* $11100, 11111$ *have odd Hamming weight, and* $11101, 11110$ *have even Hamming weight. The leaf reached by* $x_3 \to x_2 \to x_4 \to x_5 \to 1$, *of depth* 4 *contributes* $2^{5-4} = 2$ *strings, where* 00111 *has odd Hamming weight, and* 10111 *has even Hamming weight. Likewise, the leaf reached by* $x_3 \to x_2 \to x_1 \to x_4 \to 1$, *of depth* 4 *contributes* 2 *strings, where* 01110 *has odd Hamming weight, and* 01111 *has even Hamming weight.*

Theorem 16. *(Rivest-Vuillemin)*
If n *is a prime power* ($n = p^k$), $f : \{0,1\}^n \to \{0,1\}$ *is invariant with relation to a transitive permutation group,* S, *and* $f(\vec{0}) \neq f(\vec{1})$, *then* f *is evasive.*

Proof. For the proof, we will be counting over what we call orbits:

Definition 17. *For a transitive permutation group,* S*:*
$\forall x \in \{0,1\}^n$: *orbit*$(x) = \{\pi(x) : \pi \in S\}$
It has the following properties:

1. $y \in$ *orbit*$(x) \Rightarrow x \in$ *orbit*(y), *by the existence of inverses in groups.*
2. $y \in$ *orbit*$(x) \Rightarrow |y| = |x|$
3. *This implies that orbit*$(\vec{0}) = \{\vec{0}\}$, *and orbit*$(\vec{1}) = \{\vec{1}\}$

We will show that $|\text{orbit}(x)|$ is divisible by p, as long as $x \notin \{\vec{0}, \vec{1}\}$, and then we will show that the number of strings of even and odd Hamming weights is not the same.

$$\begin{aligned} \sum_{y \in \text{orbit}(x)} |y| &= \sum_{y \in \text{orbit}(x)} |x| \\ &= |\text{orbit}(x)||x| \end{aligned}$$

Alternatively, we can express the sum as:

$$\begin{aligned}\sum_{y\in\text{orbit}(x)} |y| &= \sum_{y\in\text{orbit}(x)}\sum_{i\in[n]} y_i \\ &= \sum_{i\in[n]}\sum_{y\in\text{orbit}(x)} y_i \\ &\quad \text{The inner sum is constant, since we can permute } i \\ &\quad \text{to any other } j\in[n] \text{ by transitivity, so lets fix } i=1 \\ &= n\sum_{y\in\text{orbit}(x)} y_1\end{aligned}$$

$$\therefore n|\sum_{y\in\text{orbit}(x)} |y| \Rightarrow n|(|\text{orbit}(x)||x|)$$

$\forall x \notin \{\vec{0},\vec{1}\}$, we know that $1 \le |x| \le n-1$, so $|x|$ cannot be divisible by n, so it does not contain all the k prime factors, p, which means that $|\text{orbit}(x)|$ must contain the remaining prime factors, p. [6] So $p|(|\text{orbit}(x)|)$.

Now let us count the elements of $f^{-1}(0)$. Only complete orbits can be included in the set, by the invariance property. Without loss of generality, let us assume that $\vec{0} \in f^{-1}(0)$. Otherwise, we can perform the same proof with $f^{-1}(1)$. Because of our assumption, $f^{-1}(0)$ contains $\text{orbit}(\vec{0}) = \{\vec{0}\}$, but not $\text{orbit}(\vec{1}) = \{\vec{1}\}$, else $f(\vec{0}) = f(\vec{1}) = 0$. In addition, $f^{-1}(0)$ contains a union of, say l additional, disjoint [7] orbits. Lets denote these orbits by $\text{orbit}(x_i)$, where $i \in [l]$.

We are interested in showing that the number of elements in $f^{-1}(0)$ with even Hamming weight, subtracted by the number of elements in $f^{-1}(0)$ with odd Hamming weight is non-zero. We can rewrite the difference, and split it according to the previous categorization:

$$\begin{aligned}\sum_{y\in f^{-1}(0)} (-1)^{|y|} &= (-1)^{|\vec{0}|} + \sum_{i\in[l]}\sum_{y\in\text{orbit}(x_i)} (-1)^{|y|} \\ &= (-1)^0 + \sum_{i\in[l]}\sum_{y\in\text{orbit}(x_i)} (-1)^{|x_i|} \\ &= 1 + \sum_{i\in[l]} |\text{orbit}(x_i)|(-1)^{|x_i|}\end{aligned}$$

We know that the terms of the sum are divisible by p, due to the $|\text{orbit}(x_i)|$ factor, so the sum must by a multiple of p, which means that it is not -1, which is needed to cancel out the first term:

$$\sum_{y\in f^{-1}(0)} (-1)^{|y|} \neq 1-1=0$$

So the number of strings with even and odd Hamming weights in $f^{-1}(0)$ is not equal. This fails the condition in Lemma 14, so f must be evasive.

[6] More formally, if we assume the opposite, $|\text{orbit}(x)|$ and n are relatively prime, since n's factors are either 1 or divisible by p. So n must divide $|x|$, which we have said is not possible.

[7] By the closure of the permutations in S, inclusion in an orbit is transitive. And since we know that it is symmetric, inclusion in an orbit is an equivalence relationship. That means that two orbits are either identical or disjoint.

□