Monotone Circuit Lower Bounds.

CS254
Chris Pollett
Dec 4, 2006.

Outline

- Monontone Circuits
- Crude Circuits
- Erdos-Rado Lemma
- Bounds of False Positives/Negatives
- Razborov's Lower Bounds for $\mathrm{Clique}_{n,k}$

Monotone Circuits

- We earlier saw that if we could prove super-polynomial lower bounds on circuit size for some NP language we would know that P/poly≠NP and hence P≠NP.
- Such lower bound results are hard to obtain.
- We also know that at least as far as the CVP goes monotone circuits are also P-complete, so in some sense are at least as hard as nonmonotone circuits.
- Maybe, it is easier to prove circuit lower bounds for monotone circuits?
- Is it possible to express any NP-complete problem so that it could even be solved by monotone circuits?

$\text{CLIQUE}_{n,k}$

- We have seen that whether a graph has a clique of size k is NP-complete. Call the n node version of this problem $\text{CLIQUE}_{n,k}$.
- One can also build monotone exponential size circuits to test if a graph G=(V,E) of n nodes has a clique of size k:
  - The inputs g_{ij} correspond to the entries of the adjacency matrix for G.
  - There are $\binom{n}{2}$ gates such g_{ij} and a given one is true iff there is an edge from i to j in G.
  - For each subset S of V, with $|S|=k$, we have an AND of the $O(k^2)$ many gates which correspond to a clique on this set of vertices.
  - We then have a big OR over the $\binom{n}{k}$ many different subsets S.
  - This circuit thus has size $O(k^2\binom{n}{k})$.

Razborov's Theorem

Thm. There is a constant c such that for large enough n all monotone circuits for $CLIQUE_{n,k}$ with $k = (n)^{1/4}$ have size at least $2^{c(n)^{1/8}}$.

Proof. Let G=(V,E) be a graph. Call a circuit which tests for whether any element in a family of subset $X_1,\ldots, X_m$ of V forms a clique a *crude circuit*. We'll denote a crude circuit by $CC(X_1,\ldots, X_m)$. So the circuit we gave on the last slide is a crude circuit over subsets of V of size k. We are going to show how to approximate any monotone circuit for $CLIQUE_{n,k}$ by a crude circuit...

More on Crude Circuits

- Let $k = (n)^{1/4}$ and let $l=(n)^{1/8}$.
- We will also make use of numbers p and M which will be fixed later but where p is also about $(n)^{1/8}$ and where M is about $(p-1)^l l!$
- Notice $2\binom{\ell}{2} \leq k$.
- Each crude circuit for our approximation will have X_i's with $|X_i| \leq l$ and the total number of X_i's will be some $m \leq M$.
- We approximate any monotone circuit C for $CLIQUE_{n,k}$ inductively. (On the HW you can imagine building approximate circuits for each line of the circuit in the file.)
- In the base case, an input gate g_{ij} to C can be viewed as a crude circuit $CC(\{i,j\})$.
- For the induction, let X and Y be two families of at most M nodes, and let CC(X) and CC(Y) be our approximation of C up to some gate which is either an AND or an OR…

Erdos-Rado Lemma

- We could try to approximate and OR as CC($X \cup Y$), but this may lead to a family of size >M.
- A *sunflower* is a family of p sets $\{P_1,...,P_p\}$ where P_i are called *petals*, each of cardinality $\leq l$, such that all pairs of sets in the family have the same intersection (the *core* of the sunflower).

Lemma (Erdos-Rado). Let Z be a family of more than $M=(p-1)^l l!$ nonempty sets, each of cardinality l or less. Then Z must contain a sunflower of size p.

Approximate Circuits

- *Plucking* a sunflower is the act of replacing the sets in a sunflower by its core.
- Suppose $X \cup Y$ has more than M sets. Then it has a sunflower and we can replace that sunflower by its core and repeat until we get down to M subsets. Call this operation pluck($X \cup Y$).
- So we define the crude circuit for OR to be CC(pluck($X \cup Y$)).
- We define the crude circuit for AND to be:

  $CC(pluck(\{X_i \cup Y_j \mid X_i \text{ is in } X \text{ and } Y_j \text{ is in } Y \text{ and } |X_i \cup Y_j| \leq l\}))$
- We next get bounds on the errors induced by our approximations…

False Positives and Negatives

- A *positive example* is a graph with $\binom{k}{2}$ edges connecting k nodes in all possible ways and with no other edges. So a circuit for $CLIQUE_{n,k}$ should output **true** on all $\binom{n}{k}$ such examples.
- A *negative example* is the outcome of the following experiment: Color the nodes with k-1 distinct colors. Then join by an edge any two nodes that are colored differently. This graph have any cliques of size k. So our circuit should output **false** on all $(k-1)^n$ such examples.
- A **false positive** is introduced by our approximation of an OR gate if when a negative example is fed to the inputs of our two original crude circuits for the inputs of the gate and both output **false**, but the approximation for the gate returns **true.** A **false positive** can also occur if for some coloring at least one of the constituent crude circuits returns **false,** but the approximation of their ANDs returns **true**.
- Similarly, a **false negative** is introduced by our approximation of a OR gate, if for some positive example at least one of constituent circuits output **true**, but the approximate OR computes **false**. A **false negative** can also occur if for some positive example both input crude circuits evaluate to true**,** but the approximation of their ANDs returns **false**.

Bounds on False Positives and False Negatives

Lemma I. Each approximation step introduces at most $M^2 2^{-p}(k-1)^n$ false positives.

Lemma II. Each approximation step introduces at most $M^2\binom{n-\ell-1}{k-\ell-1}$ false negatives.

On the other hand, we have:

Lemma III. Every crude circuit either is identically **false** (and thus is wrong on all positive examples), or outputs **true** on at least half of the negative examples.

Proof Sketch III. If a crude circuit is not identically **false**, then it accepts at least those graphs which have a clique on some set Z of nodes with $|Z| \le l < (k)^{1/2}/2$. But one can show that at least half of the colorings of the n vertices of G assign different colors to each of the nodes of Z, and so half of the negative examples involving Z will accept falsely.

Conclusion

- Define p= $(n)^{1/8}$log n, $l = (n)^{1/8}$.
- So M = $(p-1)^l l! < 2^{1/3(n)^{\{1/8\}}}$ for large n.
- Since each approximation step introduces

$M^2\binom{n-\ell-1}{k-\ell-1}$ false negatives, if the final crude circuit is identically false, all positive examples must have been made false by these false negatives. So the circuit size is at least $\binom{n}{k}/(M^2\binom{n-\ell-1}{k-\ell-1})$ This is at least $1/M^2(n-l/k)^l$ which is at least $2^{c(n)^{\{1/8\}}}$ for c =1/12. On the other hand, Lemma III states there are at least $1/2(k-1)^n$ negatives examples on which the output is true. The Z's causing these errors must have been introduced as false positives and each step can at most introduce $M^2 2^{-p}(k-1)^n$ of them. So we conclude the original circuit must have had size $2^{p-1}/M^2 > 2^{c(n)^{\{1/8\}}}$.