LECTURE NOTES

#16 Mar 27, 1995
#17 Mar 30, 1995
Jing Wu

Theorem For $k = n^{\frac{1}{4}}$, k-clique requires monotone circuits of size $n^{\Omega(\sqrt{k})}$

Remark If this could be done for *every* monotone problem in NP, this would imply $P \neq NP$.

A *slice function* f is one function such that for all n, there exists m such that

$$\begin{aligned} f(x) &= 0 \quad \text{if } \sum x_i < m \\ f(x) &= 1 \quad \text{if } \sum x_i > m \end{aligned}$$

Note that all slice functions are monotone. There are slice functions that are NP-complete. One can prove that the monotone circuit complexity of a slice function f is not much greater than the (non-monotone) circuit complexity of f. Thus we may expect that it is not always easy to prove lower bounds on monotone circuit complexity.

Basic idea: Every monotone circuit for k-clique C is "approximated" by a monotone depth 2 circuit $\tilde{C}$. The circuit has m "$\wedge$" gates with fan in $\leq \binom{l}{2}$ on the first level, each detects a clique of size no more than $l (= \sqrt{k})$. All the outputs of the m "$\wedge$" gates connected to an "$\vee$" gate. (The circuit just check the presence, but not absence).

What we will show is

1. If C is a small monotone circuit, then for most k-cliques G, $\widetilde{C}(G) \leq C(G)$ and for most complete $(k-1)$-partite graphs G, $\widetilde{C}(G) \geq C(G)$

2. Every approximator either outputs 0 on most k-cliques or outputs 1 on most $(k-1)$-partite graphs

First we are going to prove the following lemma:

Sunflower Lemma Let F be a collection of sets, each of size $\leq l$. If $|F| > (p-1)^l l!$, then there is a sunflower with p petals. (A sunflower with p petals is a collection of sets $S_1, \ldots, S_p$ such that for all $i < j$ and $k < l$, $S_i \cap S_j = S_k \cap S_l$.)

Proof By induction on l:
Basis: $l = 1$, choose p disjoint singletons.
Induction: Let M be a maximal collection of disjoint sets in F, $M = \{A_1, A_2, \cdots, A_n\}$, Let $S = \bigcup_{i=1}^{r} A_i$. If $r \geq p$ we have done.

Otherwise $|S| \leq l(p-1)$. Since M is maximal, S intersects every element of F. There is some $i \in S$, such that i is in $\geq 1/(p-1)l$ of the elements of F.

Let F'=$\{B - \{i\} : i \in B \in F\}$. $|F|$'$\geq |F|/(p-1)l > \frac{(p-1)^l l!}{(p-1)} = (p-1)^{(l-1)}(l-1)!$

Let $B_1 - \{i\}$, $B_2 - \{i\}$, $\cdots$, $B_p - \{i\}$ be a sunflower in F'. Then B_1, B_2, $\cdots$, B_p is our sunflower.

1

We will build $\widetilde{C}$ from C, Starting at the leaves, that is, for each gate g of C, consider the function computed at g, we will build an approximator for that function.

- If g is a leaf, we are done.
- If g is an $\vee$ gate, $g = h_1 \vee h_2$, define $g = h_1 \sqcup h_2$ as follows:

1. If $h_1 = \{S_1, S_2, \cdots, S_{m_1}\}$, $h_2 = \{T_1, T_2, \cdots, T_{m_2}\}$ (S_i, T_j, $1 \leq i \leq m_1, 1 \leq j \leq m_2$ are sets of vertices (each set of size at most l) and $|h_1 \cup h_2| \leq m$), then set $g = h_1 \cup h_2$. Otherwise $h_1 \cup h_2$ contains a sunflower of p petals. Replace those p sets with their center.
2. If there are still more than m sets, repeat it until there are no more sunflowers.

- If $g = h_1 \wedge h_2$, define $h_1 \sqcap h_2$ as follows:

  Let $h_1 = \{S_1, S_2, \cdots, S_{m_1}\}$, $h_2 = \{T_1, T_2, \cdots, T_{m_2}\}$, $h_1 \wedge h_2 = \{S_i \wedge T_j : 1 \leq i \leq m_1, 1 \leq j \leq m_2\}$

  1. Consider $\{S_i \cup T_j : 1 \leq i \leq m_1, 1 \leq j \leq m_2\}$
  2. remove any such $S_i \cup T_j$, such that $|S_i \cup T_j| > l$,
  3. replace sunflowers with their centers(plucking), until there are no more sunflowers (so there are $\leq$ m sets remaining).

In what follows, we will use the following values for l, p, and m: ($l = \sqrt{k}, p = 10\sqrt{k}\log n, m = (p-1)^l l!$)

Lemma 1 Every $\widetilde{C}$ is either identically 1, or it outputs 1 on at least half of the $(k-1)$-coloured graphs

Lemma 2 For all but at most

$$Size(C) \cdot m^2 \begin{pmatrix} n-l-1 \\ k-l-1 \end{pmatrix} \leq Size(C) \cdot m^2 (\frac{k}{n})^{l+1} \begin{pmatrix} n \\ k \end{pmatrix}$$

k-cliques G, $C(G) \leq \widetilde{C}(G)$

Lemma 3 For all but at most

$$Size(C) \cdot [\frac{m^2}{2^p}](k-1)^n$$

$(k-1)$-partite graphs G , $C(G) \geq \widetilde{C}(G)$

Theorem For $k \leq n^{\frac{1}{4}}$, monotone circuits for k-clique need size $n^{\Omega(\sqrt{k})}$

Before proving these lemmas, we will first see how they lead us to our theorem.

Proof By Lemma 1, we have 2 cases, if $\widetilde{C}$ is identically 1, then Lemma 2 says that

$$Size(C)m^2(\frac{k}{n})^{l+1} \begin{pmatrix} n \\ k \end{pmatrix} \geq \begin{pmatrix} n \\ k \end{pmatrix}.$$

(That is, the set of cliques such that $C(g) > \widetilde{C} = 0$ is the set of *all* cliques.) So

$$Size(C) \geq \frac{(\frac{n}{k})^{l+1}}{m^2} \geq \frac{(n^{\frac{3}{4}})^{\sqrt{k}}}{[(10\sqrt{k}\log n - 1)^{\sqrt{k}} \cdot \sqrt{k}!]^2} \geq \frac{n^{\frac{3}{4}\sqrt{k} - \frac{5}{8}\sqrt{k}}}{100} = n^{\Omega(\sqrt{k})}$$

If case 2 holds, then by lemma 3,

$$Size(C)\cdot[\frac{m^2}{2^p}](k-1)^n \geq \frac{1}{2}(k-1)^n$$

$$Size(C) \geq \frac{1}{2}\cdot\frac{2^p}{m^2} \geq \frac{1}{2}\cdot\frac{2^{(10\sqrt{k}\log n)}}{[(10\sqrt{k}\log n-1)^{\sqrt{k}}\cdot\sqrt{k}!]^2} \geq \frac{1}{2}\frac{n^{10\sqrt{k}-\frac{5}{8}\sqrt{k}}}{100} = n^{\Omega(\sqrt{k})}$$

$\boxed{1}$

Now we are going to prove the lemmas:

Proof of Lemma 1

$$\widetilde{C} = \bigvee_{i=1}^{r}(\text{clique on set } A_i), |A_i| \leq l, 1 \leq i \leq r$$

If $r = 0$, then claim holds.

$r = 1$, Let A_1 be given, then C_1 accepts G iff there is a clique on A_1 iff all vertices in A_1 have different colours.

Consider a randomly chosen $(k-1)$-coloured graph, Probability that G is not accepted

$$\begin{aligned} &= Prob[\exists i,j \in A_1, i,j \text{ have the same colour}] \\ &\leq \binom{l}{2}\frac{1}{k-1} \\ &= \frac{\sqrt{k}(\sqrt{k}-1)}{2}\cdot\frac{1}{k-1} \\ &= \frac{k-\sqrt{k}}{k-1}\cdot\frac{1}{2} < \frac{1}{2} \end{aligned}$$

If $r > 1$, the result also holds, because $\widetilde{C}$ accepts at least as many G as in the case above. $\boxed{1}$

Proof of Lemma 2 If G is the k-clique, such that

$$C(G) = 1 \text{ but } \widetilde{C}(G) = 0$$

then it must be the case that there is some gate g in C such that $g = h_1 \vee h_2$ and in $\widetilde{C}$ the approximator built for g rejects G but the approximator for one of h_1, h_2 accepts G, or $g = h \wedge h_2$ and both h_1 and h_2 accept G but g rejects.

We will show that any such g can affect no more than

$$m^2 (\frac{k}{n})^{l+1} \binom{n}{k}$$

cliques.

Note that if our approximator on h_1 accepts G, that means that there is some clique A included in the clique in G, that is detected by our approximator for h_1. But our approximator for $h_1 \vee h_2$ looks for a clique on some subset of A.

So in case 1, our approximator for $g \geq h_1 \sqcup h_2$. So the first problem gate is not of type 1.

Now consider $g = h_1 \wedge h_2$, Let A be the set of vertices containing the k-clique G. We are assuming that there is some $S_i \subseteq A$ and some $T_j \subseteq A$, so that $\widetilde{h_1}$ detects a clique on S_i and $\widetilde{h_2}$ detects a clique on T_i. But our approximator $\tilde{g}$ rejects A. Note that in G, there is a clique on $S_i \cup T_j$. It must be the case that $|S_i \cup T_j| > l$, because otherwise $\tilde{g}$ accepts G. Note that there are at most m^2 such (s_i, t_j) pairs associated with gate g.

There are no more than $\binom{n-l-1}{k-l-1}$ such k-cliques in G for fixed S_i and T_j. Thus the number of such k-cliques is no more than

$$m^2 \binom{n-l-1}{k-l-1} \leq m^2 (\frac{k}{n})^{l+1} \binom{n}{k}$$

$\boxed{1}$

Proof of Lemma 3 If G is a $(k-1)$-coloured graph such that

$$C(G) = 0 \text{ but } \widetilde{C}(G) = 1$$

then it must be the case as above

1. $g = h_1 \vee h_2$ such that $\tilde{g}$ accepts G but $\widetilde{h_1}$ and $\widetilde{h_2}$ reject G.
2. $g = h_1 \wedge h_2$ such that $\tilde{g}$ accepts G but one of $\widetilde{h_1}$ or $\widetilde{h_2}$ reject G.

We will show that any such g can affect no more than

$$\frac{m^2}{2^p}(k-1)^n$$

of the $(k-1)$-coloured graphs.

First consider $g = h_1 \vee h_2$. So $\tilde{g}$ is built from $\widetilde{h_1}$ and $\widetilde{h_2}$ from plucking.

Let

$$\widetilde{h_1} = \bigvee(\text{clique on } S_1, S_2, \cdots, S_{m_1})$$

$$\widetilde{h_2} = \bigvee(\text{clique on } T_1, T_2, \cdots, T_{m_2})$$

$\widetilde{h_1}$ and $\widetilde{h_2}$ each reject G iff each S_i and T_j are *not* "properly coloured".

This means that there is some sunflower in the list $S_1, S_2, \cdots, S_{m_1}$ and $T_1, T_2, \cdots, T_{m_2}$ such that G properly colours the center but G does not properly colour any of the petals.

Let $A_1, A_2, \cdots, A_p$ be the sets in this sunflower.

$$\begin{aligned}
& Prob[\text{none of } A_1, A_2, \cdots, A_p \text{ is properly coloured but the centre is}] \\
\leq\ & Prob[A_1, A_2, \cdots, A_p \text{ is not properly coloured} | \text{the centre is properly coloured}] \\
=\ & \prod_{i=1}^{n} Prob[A_i \text{ is not properly coloured} | \text{the centre is properly coloured}] \\
\leq\ & \prod_{i=1}^{n} Prob[A_i \text{ is not properly coloured}] \leq \frac{1}{2^p}
\end{aligned}$$

And at last, if we notice that we will do plucking for m^2 time, the result follows naturally. $\boxed{1}$