Math 267a - Propositional Proof Complexity

Lecture #11: 27 February 2002

Lecturer: Sam Buss

Scribe Notes by: Liz Arentzen

1 Monotone Craig Interpolation

Monotone Craig Interpolation provides another way to obtain exponential lower bounds on Resolution proofs.

1.1 Propositional Case

Theorem 1 *Let $\phi = \phi(\vec{p}, \vec{q})$ be a formula in which the $\vec{p}$ variables occur only positively. Also, suppose that $\models \phi \to \psi$ where $\psi(\vec{p}, \vec{r})$. Then there exists an interpolant $C(\vec{p})$ such that the $\vec{p}$ variables occur only positively in C.*

Formulae are built with $\wedge$, $\vee$, $\neg$.

Definition An occurrence is positive if and only if it is under the scope of an even number of $\neg$ signs.

Note that application of De Morgan's Laws or the distributive laws does not affect whether a particular occurrence is positive.

Lemma 2 *Let the variables in $\vec{p}$ be $p_1, p_2, \ldots, p_k$ and let the variables $\vec{p}\,'$ be $p'_1, p'_2, \ldots, p'_k$. If $p_i \to p'_i$ is true $\forall i$ for some truth assignment, then $C(\vec{p})$ is true $\Rightarrow C(\vec{p}\,')$ is true, assuming that the variables of $\vec{p}$ occur only positively in C. (This last property is called* monotonicity.*)*

Proof By induction on size of C.

Proof (of Theorem 1) $\phi(\vec{p}, \vec{q}) \to \psi(\vec{p}, \vec{r})$ is the same as $\exists \vec{q}\, \phi(\vec{p}, \vec{q}) \to \forall \vec{r}\, \psi(\vec{p}, \vec{r})$. Then let

$$C(\vec{p}) \doteq \bigvee_{\substack{\text{all T/F settings} \\ \text{of the variables in } \vec{q}}} \phi(\vec{p}, \vec{q}). \tag{1}$$

The p's occur only positively so we can see that this interpolant has the proper form.

Alternately, it can be shown that a fitting interpolant is

$$C(\vec{p}) \doteq \bigwedge_{\substack{\text{all T/F settings} \\ \text{of the variables in } \vec{r}}} \psi(\vec{p}, \vec{r}). \tag{2}$$

1.2 Resolution Case

Theorem 3 *Let $\Gamma = \Gamma(\vec{p}, \vec{q})$ be a set of clauses, and let $\Delta = \Delta(\vec{p}, \vec{r})$ be a set of clauses.*

Assume that the $\vec{p}$ variables occur only positively in Δ (that is, there are no $\neg p_i$'s in clauses in Δ), or assume that the $\vec{p}$ variables occur only negatively in Γ (that is, there are no p_i's in clauses in Γ). Also assume $\Gamma \cup \Delta$ is unsatisfiable (i.e. has a refutation). Then there is an interpolant $C(\vec{p})$ such that $\forall$ truth assignments τ

if $\bar{\tau}(C(\vec{p})) = T$, then $\exists$ clause $C \in \Gamma$ such that $\tau(C) =$False,

if $\bar{\tau}(C(\vec{p})) = F$, then $\exists$ clause $C \in \Delta$ such that $\tau(C) =$False,

and such that the $\vec{p}$ variables occur only positively in C.

Proof

Let

$$C(\vec{p}) \doteq \bigwedge_{\substack{\text{all T/F settings}\\ \text{of the variables in } \vec{q}}} \bigvee_{C \in \Gamma} \neg C(\vec{p}, \vec{q}). \tag{3}$$

That $C(\vec{p})$ will be a fitting interpolant is immediate from the fact that if $\Delta \cup \Gamma$ is unsatisfiable

$$\bigwedge_{C \in \Delta} C \Rightarrow \bigvee_{C \in \Gamma} \neg C. \tag{4}$$

Alternately we may let

$$C(\vec{p}) \doteq \bigvee_{\substack{\text{all T/F settings}\\ \text{of the variables in } \vec{r}}} \bigwedge_{C \in \Delta} C(\vec{p}, \vec{r}). \tag{5}$$

Theorem 4 *Let R be a refutation of $\Gamma \cup \Delta$ of size s. Then $C(\vec{p})$ can be written with monotone circuit size $O(s)$. If R is tree-like, $C(\vec{p})$ has monotone formula size $O(s)$.*

Theorem 5 *(Restatement of part of Theorem 4) Let Γ consist of clauses containing $\vec{q}$'s and negative occurrences of $\vec{p}$'s. Let Δ consist of clauses containing $\vec{r}$'s and $\vec{p}$'s. (Note that we make no assumption on whether these $\vec{p}$ occur positively or negatively in the clauses of Δ.) If R is a refutation of $\Gamma \cup \Delta$, then there exists an interpolant ϕ, such that the size of ϕ is $O($number of steps in $R)$.*

Definition For C a clause in R, we let ϕ_C be defined by

1. $\phi_C = T$ if $C \in \Gamma$
2. $\phi_C = F$ if $C \in \Delta$
3. $\phi_C = \phi_{C_1 \cup \{p_i\}} \vee (p_i \wedge \phi_{C_2 \cup \{\bar{p}_i\}})$ if C is such that

$$\frac{C_1 \cup \{p_i\} \quad C_2 \cup \{\bar{p}_i\}}{C = C_1 \cup C_2}$$

4. $\phi_C = \phi_{C_1 \cup \{q_i\}} \wedge \phi_{C_2 \cup \{\bar{q}_i\}}$ if C is such that

$$\frac{C_1 \cup \{q_i\} \quad C_2 \cup \{\bar{q}_i\}}{C = C_1 \cup C_2}$$

5. $\phi_C = \phi_{C_1 \cup \{r_i\}} \vee \phi_{C_2 \cup \{\bar{r}_i\}}$ if C is such that

$$\frac{C_1 \cup \{r_i\} \quad C_2 \cup \{\bar{r}_i\}}{C = C_1 \cup C_2}$$

Definition For C a clause, let $C^\Gamma = C \cap \{q_i, \bar{q}_i, \bar{p}_i : i \geq 0\}$ and let $C^\Delta = C \cap \{p_i, \bar{p}_i, r_i, \bar{r}_i : i \geq 0\}$.

Claim For all τ, $\forall C \in R$,

A. if $\tau \not\models C^\Gamma$ and $\tau(\phi_C) = T$, then $\exists D \in \Gamma$ such that $\tau \not\models D$.

B. if $\tau \not\models C^\Delta$ and $\tau(\phi_C) = F$, then $\exists D \in \Delta$ such that $\tau \not\models D$.

Proof of this claim will imply that $\phi_\emptyset$ works as an interpolant, since $\emptyset^\Gamma = \emptyset = \emptyset^\Delta$, which is not satisfied by any τ.

Proof (of Claim)
Proof is by induction on inferences in R.

1. $C \in \Gamma$. Then $\phi_C = T$. $C \in \Gamma \Rightarrow C^\Gamma = C \cap \{q_i, \bar{q}_i, \bar{p}_i : i \geq 0\} = C$. Then if $\tau \not\models C^\Gamma$, $\tau \not\models C$, and so trivially $\exists C \in \Gamma$ such that $\tau \not\models C$.

2. $C \in \Delta$. Then $\phi_C = F$. $C \in \Delta \Rightarrow C^\Delta = C$. Hence if $\tau \not\models C^\Delta$, trivially $\exists C \in \Delta$ such that $\tau \not\models C$.

3. $C = C_1 \cup C_2$ with $\frac{C_1 \cup \{p_i\} \quad C_2 \cup \{\bar{p}_i\}}{C = C_1 \cup C_2}$. Then $\phi_C = \phi_{C_1 \cup \{p_i\}} \vee (p_i \wedge \phi_{C_2 \cup \{\bar{p}_i\}})$.

    (a) Suppose $\tau \not\models C^\Gamma$ and $\tau(\phi_C) = T$. Note that $(C_1 \cup \{p_i\})^\Gamma = C_1^\Gamma$. Then $\tau \not\models (C_1 \cup \{p_i\})^\Gamma$, since $C_1^\Gamma \subseteq C^\Gamma$ and $\tau \not\models C^\Gamma$ imply that $\tau \not\models C_1^\Gamma$.

    i. If $\tau(\phi_{C_1 \cup \{p_i\}}) = T$, then since we have $\tau \not\models (C_1 \cup \{p_i\})^\Gamma$, by the induction hypothesis we are done.

    ii. Otherwise, $\tau(p_i \wedge \phi_{C_2 \cup \{\bar{p}_i\}}) = T$. Thus $\tau(\phi_{C_2 \cup \{\bar{p}_i\}}) = T$. Also $\tau(p_i) = T$, so $\tau \not\models \{\bar{p}_i\}$. Note $\{\bar{p}_i\} = \{\bar{p}_i\}^\Gamma$, so $\tau \not\models \{\bar{p}_i\}^\Gamma$. Also $C_2^\Gamma \subseteq C^\Gamma$ and $\tau \not\models C^\Gamma$ imply $\tau \not\models C_2^\Gamma$. Thus $\tau \not\models C_2^\Gamma \cup \{\bar{p}_i\}^\Gamma$ and hence as $C_2^\Gamma \cup \{\bar{p}_i\}^\Gamma = (C_2 \cup \{\bar{p}_i\})^\Gamma$, we get $\tau \not\models (C_2 \cup \{\bar{p}_i\})^\Gamma$. Since we have $\tau(\phi_{C_2 \cup \{\bar{p}_i\}}) = T$ and $\tau \not\models (C_2 \cup \{\bar{p}_i\})^\Gamma$, the induction hypothesis applies.

    (b) Suppose $\tau \not\models C^\Delta$ and $\tau(\phi_C) = F$

    i. If $\tau(p_i) = T$, then $\tau \not\models (C_2 \cup \{\bar{p}_i\})^\Delta$. Also $\tau(\phi_{C_2 \cup \{\bar{p}_i\}}) = F$. Then the induction hypothesis applies.

    ii. If $\tau(p_i) = F$, then $\tau \not\models (C_1 \cup \{p_i\})^\Delta$ and $\tau(\phi_{C_1 \cup \{p_i\}}) = F$. Then the induction hypothesis applies.

4. $C = C_1 \cup C_2$ with $\frac{C_1 \cup \{q_i\} \quad C_2 \cup \{\bar{q}_i\}}{C = C_1 \cup C_2}$. Then $\phi_C = \phi_{C_1 \cup \{q_i\}} \wedge \phi_{C_2 \cup \{\bar{q}_i\}}$.

    (a) Suppose $\tau \not\models C^\Gamma$ and $\tau(\phi_C) = T$. $\tau(\phi_C) = T$ implies that $\tau(\phi_{C_1 \cup \{q_i\}}) = \tau(\phi_{C_2 \cup \{\bar{q}_i\}}) = T$. Either $\tau \not\models (C_1 \cup \{q_i\})^\Gamma$ (if $\tau(q_i) = F$) or $\tau \not\models (C_2 \cup \{\bar{q}_i\})^\Gamma$ (if $\tau(q_i) = T$). In either case, the induction hypothesis applies.

(b) Suppose $\tau \not\models C^\Delta$ and $\tau(\phi_C) = F$. Note that $(C_1 \cup \{q_i\})^\Delta = C_1^\Delta$ and $(C_2 \cup \{\bar{q}_i\})^\Delta = C_2^\Delta$. So $\tau \not\models (C_1 \cup \{q_i\})^\Delta$ and $\tau \not\models (C_2 \cup \{\bar{q}_i\})^\Delta$. Also, since $\tau(\phi_C) = F$, either $\tau(\phi_{C_1 \cup \{q_i\}}) = F$ or $\tau(\phi_{C_2 \cup \{\bar{q}_i\}}) = F$ so in either case the induction hypothesis applies.

5. $C = C_1 \cup C_2$ with $\frac{C_1 \cup \{r_i\} \quad C_2 \cup \{\bar{r}_i\}}{C = C_1 \cup C_2}$. Then $\phi_C = \phi_{C_1 \cup \{r_i\}} \vee \phi_{C_2 \cup \{\bar{r}_i\}}$.

   (a) Suppose $\tau \not\models C^\Gamma$ and $\tau(\phi_C) = T$. Note that $(C_1 \cup \{r_i\})^\Gamma = C_1^\Gamma$, and $(C_2 \cup \{\bar{r}_i\})^\Gamma = C_2^\Gamma$. Hence $\tau \not\models (C_1 \cup \{r_i\})^\Gamma$ and $\tau \not\models (C_2 \cup \{\bar{r}_i\})^\Gamma$. Also, $\tau(\phi_{C_1 \cup \{r_i\}}) = T$ or $\tau(\phi_{C_2 \cup \{\bar{r}_i\}}) = T$. Then the induction hypothesis applies to whichever one equals T.

   (b) Suppose $\tau \not\models C^\Delta$ and $\tau(\phi_C) = F$. $\tau(\phi_C) = F$ implies $\tau(\phi_{C_1 \cup \{r_i\}}) = \tau(\phi_{C_2 \cup \{\bar{r}_i\}}) = F$. Either $\tau \not\models (C_1 \cup \{r_i\})^\Delta$ (if $\tau(r_i) = F$) or $\tau \not\models (C_2 \cup \{\bar{r}_i\})^\Delta$ (if $\tau(r_i) = T$). In either case, the induction hypothesis applies.

Notice that ϕ is monotone in the p_i's.

1.3 Exponential Lower Bounds on Resolution Proofs for Clique and Coloring

Definition A k-coloring of a graph is an assignment of k colors to vertices such that no adjacent vertices have the same color.

Definition A k-clique in a graph is a subset consisting of k nodes such that for any pair of nodes in the subset there is an edge in the graph which joins them.

Theorem 6 *A graph cannot have both a $k+1$ clique and a k-coloring.*