Lower bounds on resolution proofs

Craig's Interpolation Theorem If $A(\vec{p}, \vec{q}) \models B(\vec{q}, \vec{r})$ then there is $C(\vec{q})$ such that $A[\vec{p}, \vec{q}] \models C(\vec{q})$ and $C(\vec{q}) \models B(\vec{q}, \vec{r})$.

Circuit A circuit is a sequence of assignments $A_1 A_2 \ldots A_n$ where for any i A_i is of the form

$$\begin{array}{lll} P_i = T & & P_i = P_j \vee P_k \\ P_i = F & \text{Input} & P_i = P_j \wedge P_k \\ P_i = ? & & P_i = \neg P_j \end{array} \Bigg\} \; j,k < i.$$

Size of circuit is # assignments in the sequence.

P/poly A problem $A \in P/poly$ if there are c, k and $\{C_i\}_{i \in \mathbb{N}}$ such that $|C_n| \leq c n^k$ & $\forall x.\ x \in A$ iff $C_{|x|}(x) = T$

NP/poly A problem $A \in NP/poly$ if there are c, k and $\{C_i\}_{i \in \mathbb{N}}$ such that $|C_n| \leq c n^k$ & $\forall x.\ x \in A$ iff $\exists p\ C_{|x|}(x, p) = T$

coNP/poly A problem $A \in coNP/poly$ if there are c, k and $\{C_i\}_{i \in \mathbb{N}}$ such that $|C_n| \leq c n^k$ & $\forall x.\ x \in A$ iff $\forall p\ C_{|x|}(x, p) = T$.

Mundici's Theorem If for every A, B s.t

$A \models B$ there is interpolant C whose circuit has size $\leq poly(|A|, |B|)$ then

$$P/poly = NP/poly \cap coNP/poly.$$

Proof Assume poly-sized interpolants exist for all A, B $A \models B$. Will show that

$NP/poly \cap coNP/poly \subseteq P/poly$.

Let $L \in NP/poly \cap coNP/poly$.

Since $L \in NP/poly$, $\exists \{A_k(\vec{p}, \vec{q})\}$ s.t.

$\forall \vec{q}$. $\vec{q} \in L$ iff $\exists \vec{p}$ $A_{|\vec{q}|}(\vec{p}, \vec{q}) = T$

Since $L \in coNP/poly$ $\exists \{B_k(\vec{q}, \vec{r})\}$ s.t

$\forall \vec{q}$ $\vec{q} \in L$ iff $\forall \vec{r}$ $B_{|\vec{q}|}(\vec{q}, \vec{r}) = T$.

$\forall k$. $A_k(\vec{p}, \vec{q}) \models B_k(\vec{q}, \vec{r})$

$\exists \{C_k\}_{k \in \mathbb{N}}$ s.t. $size(C_k) = poly(A_k, B_k)$
$= poly(k)$

$A_k(\vec{p}, \vec{q}) \models C_k(\vec{q})$ and $C_k(\vec{q}) \models B_k(\vec{q}, \vec{r})$

$\{C_k\}$ solves L

$L \in P/poly$

Theorem Suppose $\Gamma = \{A_i(\vec{p}, \vec{q})\}_{i=1}^{k} \cup \{B_j(\vec{q}, \vec{r})\}_{j=1}^{l}$ and Γ has resolution refutation of length n. Then there is an interpolant $C(\vec{q})$ such that circuit size of C is $O(n)$.

Interpolant C s.t. $\bigwedge_{i=1}^{k} A_i(\vec{p},\vec{q}) \models C(\vec{q})$ and $C(\vec{q}) \wedge \bigwedge_{j=1}^{\ell} B_j(\vec{q},\vec{r})$ is unsatisfiable.

Monotone Circuit is a circuit where there are no assignments of the form $P_i = \neg P_j$.

Theorem Suppose $\Gamma = \{A_i(\vec{p},\vec{q})\}_{i=1}^{k} \cup \{B_j(\vec{q},\vec{r})\}_{j=1}^{\ell}$ and $\vec{q}$ either appear only positively in $\{A_i\}$ or appears only negatively in $\{B_j\}$. Γ has a resolution refutation of length n. Then there is an interpolant C such C has a monotone circuit of size $O(n)$.

$P \subseteq P/poly$

Try to prove that $NP \neq P/poly$.

$\exists L \in NP$ s.t. circuits solving L are exponential or super polynomial

Succeeded in proving that certain NP complete problems have exponential lower bounds on monotone circuit that solve them.

k-color Given a graph $G = (V, E)$ determine if

G is k-colorable.

Proposition For any n, k, there is set of clauses $\text{color}_{n,k}(\vec{q}, \vec{r})$ s.t. a graph G represented by an assignment to $\vec{q}$ is k-colorable iff $\text{color}_{n,k}$ is satisfiable. coloring is given the assignment to $\vec{r}$.

Proof q_{uv} — T if there is an edge (u,v)
r_{vi} — T if there is coloring where vertex v gets color i.

(a) For every vertex u.
$$r_{u1} \vee r_{u2} \vee \dots \vee r_{uk}$$
(b) For every vertex u & color i, j $(i \neq j)$
$$\neg r_{ui} \vee \neg r_{uj}$$
(c) For every u, v and color i $(u \neq v, \quad)$
$$\neg q_{uv} \vee \neg r_{ui} \vee \neg r_{vi}$$

Clique A clique in $G = (V, E)$ is $C \subseteq V$ s.t. $\forall u, v \in C \ (u \neq v) \ (u,v) \in E$.

k-Clique Given graph G, determine if G has a clique of size k.

Proposition For every n, k there is a set of clauses $\text{clique}_{n,k}(\vec{p}, \vec{q})$ s.t. a graph G of size n encoded by $\vec{q}$, has a clique of size k iff

$\text{clique}_{n,k}$ is satisfiable (assignment to $\vec{p}$ gives the clique.)

Proof $q_{uv} = T$ iff (u,v) is edge.

$p_{iu} = T$ iff ith vertex of clique is u.

(a) For every i, $p_{i1} \vee p_{i2} \cdots \vee p_{in}$

(b) For every i, u, v $\neg p_{iu} \vee \neg p_{iv}$ $(u \neq v)$

(c) For every i, j, u $(i \neq j)$ $\neg p_{iu} \vee \neg p_{ju}$.

(d) For every u, v, i, j $(u \neq v, i \neq j)$

$$p_{iu} \wedge p_{jv} \to q_{uv}$$

$$\neg p_{iu} \vee \neg p_{jv} \vee q_{uv}$$

Proposition If a graph G has a clique of size k then G is not $(k-1)$-colorable.

$\forall n, k.$ $\text{clique}_{n,k} \cup \text{color}_{n,k-1}$ is unsatisfiable

Razborov, Alon-Bopanna Any monotone family circuits $\{C_n\}_{n \in \mathbb{N}}$ s.t. C_n evaluates to T on graphs (of size n) that have a k-clique and evaluates F on any graph that is not $k-1$-colorable.

$|C_n|$ is at least $n^{\Omega(\sqrt{k})}$ for any $k \leq n^{1/4}$.

Theorem Any resolution refutation of $\text{clique}_{n,k} \cup \text{color}_{n,k-1}$ must have length at least $n^{\Omega(\sqrt{k})}$ $(k \le n^{1/4})$.

Proof There is monotone interpolant of size $O(m)$ for $\text{clique}_{n,k} \cup \text{color}_{n,k-1}$ where m is length of the refutation.

$$m \geq n^{\Omega(\sqrt{k})}.$$

Satisfiability is NP-complete

Validity is coNP-complete.

Cook-Reckow There is proof system s.t. every tautology has a poly-sized proof iff NP = co NP.

Open Question Frege proof system is super?