Craig’s interpolation theorem and proof complexity

$$\begin{tikzcd}[row sep=small]
 & & & NP \arrow[dr] & & \\
L \arrow[r] & NL \arrow[r] & P \arrow[ur] \arrow[dr] & & PSPACE \arrow[r] & EXP \\
 & =coNL & & coNP \arrow[ur] & =NPSPACE &
\end{tikzcd}$$

Open Problems

- Is $P = NP$?
- Is $P = NP \cap coNP$?
  - * Problems in $NP \cap coNP$ were later shown to be in P. Examples Linear programming and primality.
  - * Some problems in $NP \cap coNP$ not known to be in P.
- Is $NP = coNP$?

Cook-Levin Theorem The satisfiability problem for propositional logic is NP-complete.

Corollary The validity problem for propositional logic is coNP-complete.

Proof Membership in coNP: Proof that a formula is not valid is a truth assignment under which the formula evaluates to F.

Hardness If $A \leq_p B$ then $\bar{A} \leq_p \bar{B}$

$L \in coNP$. $\quad \bar{L} \in NP$

Reduction f from $\bar{L}$ to Satisfiability.

$x \in \bar{L} \iff f(x)$ is satisfiable

$x \in L \iff f(x)$ is satisfiable

$x \in L \iff f(x)$ is unsatisfiable $\iff \neg f(x)$ is valid.

Definition A proof system is super if every tautology has a "short" (polynomially) proof in the proof system

Cook-Reckow Theorem If there is a super proof system for propositional logic then $NP = coNP$.

Notation List of propositions $p_1 \ldots p_n$ denote by $\vec{p}$

$A(\vec{p})$ to denote that $occ(A) \subseteq \vec{p}$.

Craig's Interpolation Theorem If

$A(\vec{p}, \vec{q}) \models B(\vec{q}, \vec{r})$ then there a $C(\vec{q})$

such that $A(\vec{p}, \vec{q}) \models C(\vec{q})$ and

$C(\vec{q}) \models B(\vec{q}, \vec{r})$

Proof For a truth valuation v, and $\vec{q}$

$v\restriction_{\vec{q}} : \vec{q} \to \{T, F\}$.

$M = \{ v\restriction_{\vec{q}} \mid v \models A(\vec{p}, \vec{q}) \}$ ← finite set.

Let $M = \{ v_1, v_2 \ldots v_k \}$ and $\vec{q} = \{ q_1 \ldots q_m \}$

$C = \bigvee_{i=1}^{k} (c_1^i \wedge c_2^i \ldots c_m^i)$ where

$c_j^i = \{ q_j$ if $v_i(q_j) = T$

$$c_j^i = \begin{cases} q_j & \text{if } v_i(q_j) = T \\ \neg q_j & \text{if } v_i(q_j) = F \end{cases}$$

$A \models C$: $v \models A$ then $v\restriction_q \in M$ and $v \models C$

$C \models B$: Let v s.t $v \not\models B$.

Let consider v' s.t $v\restriction_{\vec{q},\vec{r}} = v'\restriction_{\vec{q},\vec{r}}$.

$A \models B \Rightarrow v \not\models A$.

$v' \not\models B \Rightarrow v' \not\models A$

$v\restriction_{\vec{q}} \notin M \Rightarrow v \not\models C$

$\text{Size}(C) = O(2^m)$

Open Question Are there polynomial sized interpolants for "all formulas"?

Circuit Is a sequence $L_1, L_2 \ldots L_n$ s.t. each line L_i is one of the following forms.

$P_i = T$	$P_i = P_j \wedge P_k$	$j, k < i$
$P_i = F$	$P_i = P_j \vee P_k$	$j, k < i$
$P_i = ?$	$P_i = \neg P_j$	$j < i$

Size of circuit $= n$.

$\text{Inputs}(C) = \{ P_i \mid P_i = ? \in C \}$

Given assignment to $\text{Inputs}(C)$, $\text{val}(C)$ is just the value P_n.

Example $P_1 = ?$

$P_2 = ?$ $\Big\}$ $P_3 \wedge (p_1 \vee p_2)$

$$P_3 = ?$$
$$P_4 = P_1 \wedge P_2$$
$$P_5 = P_3 \vee P_4$$

Definition A problem $A \in P/poly$ if there constants l, k and $\{C_i\}_{i \in \mathbb{N}}$ s.t.

$\forall n \quad size(C_n) \leq l\, n^k \quad |input(C_n)| = n.$

$\forall x \quad x \in A$ iff $C_{|x|}(x) = T$

A problem $A \in NP/poly$ if there l, k and $\{C_i\}_{i \in \mathbb{N}}$ s.t.

$\forall n. \quad size(C_n) \leq l\, n^k$

$\forall x. \quad x \in A$ iff $\exists p.\ C_{|x|}(x, p) = T$

A problem $A \in coNP/poly$ if $\exists\, l, k$ and $\{C_i\}_{i \in \mathbb{N}}$ s.t $\forall n. \quad size(C_n) \leq l\, n^k$

$\forall x \quad x \in A$ iff $\forall p.\ C_{|x|}(x, p) = T$

Open Problem

$$P/poly \stackrel{?}{=} NP/poly \cap coNP/poly$$

Mundici Theorem If $\forall A, B$ s.t $A \models B$ there is an interpolant C whose circuit size is $poly(|A|, |B|)$ Then

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

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

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

$\exists \{A_i(\vec{p},\vec{q})\}_{i \in \mathbb{N}}$ and $\{B_i(\vec{q},\vec{r})\}_{i \in \mathbb{N}}$

s.t. $\forall \vec{q} \in L$ iff $\exists \vec{p} \; A_{|\vec{q}|}(\vec{p},\vec{q}) = \top$

iff $\forall \vec{r} \; B_{|\vec{q}|}(\vec{q},\vec{r}) = -$