Proof Complexity for Circuit Classes

Klaus Aehlig

Comprehension in Propositional Proofs

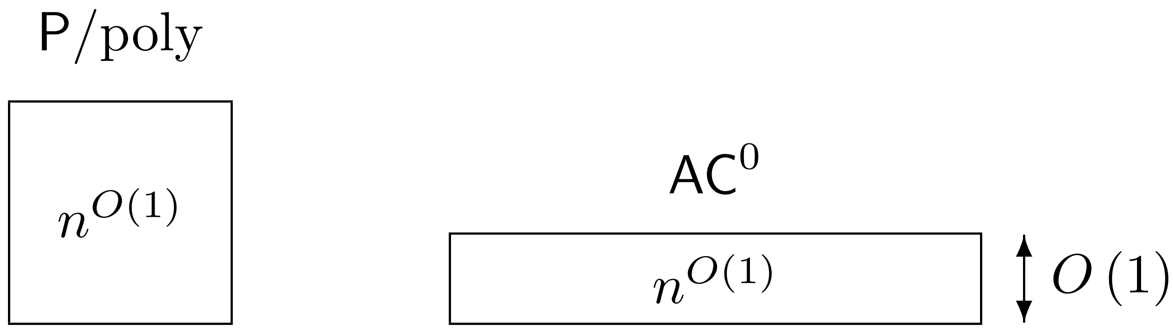
- Extension Rule in Propositional Logic

$$p \leftrightarrow A$$

- several variables $\rightsquigarrow$ several rules needed

! irrespectively of whether the new variables are interdependent

- But dependencies make a big difference in computation



$\ldots$ and proof theory was always more interested in heights.

Comprehension (cont'd)

- Dependence matters $\rightsquigarrow$ have a rule that honours independence

$$\frac{\Gamma, \neg(p_1 \leftrightarrow \varphi_1), \ldots, \neg(p_k \leftrightarrow \varphi_k)}{\Gamma}$$

  $\overrightarrow{p}$ *disjoint and new*

- How does this influence height? What is this rule used for?

$\rightsquigarrow$ Comprehension rule, in a setting with

$$\frac{\Gamma, A(\overrightarrow{a})}{\Gamma, \forall_k \overrightarrow{p} A(\overrightarrow{p})} \qquad \frac{\Gamma, A(\overrightarrow{\wp})}{\Gamma, \exists_k \overrightarrow{p} A(\overrightarrow{p})}$$

Note: only atoms as witnesses!

The Comprehension Axiom

...is provable for those φ we allow comprehension for.

$$
\dfrac{\dfrac{\dfrac{\cdots \qquad \dfrac{}{(p_i \leftrightarrow \varphi_i), \neg(p_i \leftrightarrow \varphi_i)} \qquad \cdots}{\bigwedge_k (p_i \leftrightarrow \varphi_i), \neg(p_1 \leftrightarrow \varphi_1), \ldots, \neg(p_k \leftrightarrow \varphi_k)}\ \bigwedge_k}{\exists_k \overrightarrow{p} \bigwedge_k (p_i \leftrightarrow \varphi_i), \neg(p_1 \leftrightarrow \varphi_1), \ldots, \neg(p_k \leftrightarrow \varphi_k)}\ \exists_k}{\exists_k \overrightarrow{p} \bigwedge_k (p_i \leftrightarrow \varphi_i)}\ \text{comprehension}
$$

To relate the calculus to AC^0, we require the $\overrightarrow{\varphi}$ *quantifier free*.

Quantified Propositional Logic

- Have seen quantifier-rules and comprehension already
- Rest of quantified propositional logic is canonical

$$\frac{}{\Gamma, p, \bar{p}} \qquad \frac{\ldots \qquad \Gamma, A_i \qquad \ldots}{\Gamma, \bigwedge_k A_1 \ldots A_k} \bigwedge_k \qquad \frac{\Gamma, A_j}{\Gamma, \bigvee_k A_1 \ldots A_k} \bigvee_k^j$$

Iteration

- Now proof height should correspond to circuit height
- Can we make this formal by showing lower bounds?
  circuit height is sequential time...

$\rightsquigarrow$ what is an inherently sequential principle?

- When iterating a function $0, f(0), f(f(0)), f(f(f(0))) \ldots$
  the evaluations of f have to be done one after another

  ...provided the domain/range of f is big enough!

Relativised Computation

Big domain?

- add a predicate on bit-strings $\alpha_k(\wp_1, \ldots, \wp_k)$, $\bar{\alpha}_k(\wp_1, \ldots, \wp_k)$
  again, only allow $\mathrm{T}, \mathrm{F}, p, \bar{p}$ *as arguments*
- Extensionality of α, but otherwise uninterpreted.
- Now we can code $f\colon [2^n] \to [2^n]$ by its bit-graph
  the i'th bit of $f(a)$ *is given by* $\alpha_{n+\log(n)}(i, a)$

Iteration Principle

Iterating a function 0, $f(0)$, $f(f(0))$, $f(f(f(0)))$ ...

- How to express $f^\ell(0) = b$ for $\ell \gg n$, say $\ell \in [2^n]$?

$\rightsquigarrow$ Add another predicate to check the answers!
Use $\alpha_{2n}(\ell, b)$ to stand for $f^\ell(0) = b$

- Iteration principle $\Phi_{n,\ell}$

$$\exists_{4n} \overrightarrow{p}\,\overrightarrow{p}\,'\overrightarrow{q}\,\overrightarrow{q}\,'[\text{ “}f^\ell(0) = \overrightarrow{p}\text{” } \vee \neg\text{“}f^0(0) = 0\text{”}$$
$$\vee(\text{“}\overrightarrow{q}\,' = \overrightarrow{q} + 1\text{” } \wedge \text{ “}f^{\overrightarrow{q}}(0) = \overrightarrow{p}\text{” } \wedge$$
$$\text{“}f(\overrightarrow{p}\,) = \overrightarrow{p}\,'\text{” } \wedge \neg\text{“}f^{\overrightarrow{q}\,'}(0) = \overrightarrow{p}\,'\text{”})\ ]$$

$\boxed{\textbf{Boundedness}}$

- Assume $\vdash^h \Phi_{n,\ell}$. Want to show $\ell \leq h$.

$\rightsquigarrow$ find a path through the proof with all sequents of the form $\Phi_{n,\ell}, \Delta$ with Δ quantifier-free and false

- On this path reveal f only a little bit

  α contains exponentially many bits of information!

$\rightsquigarrow$ consider *partial* function $f\colon [2^n] \rightharpoonup [2^n]$

- f is ℓ-sequential, if for some $k \leq \ell$

$$0, f(0), f^2(0), \ldots, f^k(0)$$

  are defined but $f^k(0) \notin \mathsf{dom}(f)$.

Extending Partial Functions

- Keep f still s-sequential after having followed a path for s steps
- If $f(a)$ is defined, this fixes $\alpha_{n+\log(n)}(i,a)$ in the obvious way.
- …have to fix "$f^b(0) = c$" as well
- Recall: … $f^k(0) \notin \mathsf{dom}(f)$
  so values in the domain are "forbidden" for future extensions!

∴ can set "$f^b(0) = c$" to false, if $c \in \mathsf{dom}(f)$ and $f^b(0)$ undefined
  in particular, $c \in \mathsf{dom}(f)$ forces "$f^b(0) = c$" to have a truth value

- To extend $\mathsf{dom}(f)$ by M, just pick $a \notin M \cup \mathsf{dom}(f)$ and set $f'(x) = a$ for the new x
  the new f' is then $s+1$ sequential and compatible to the "$f^b(0) = c$" already fixed

Conclusions

- Note: in the proof we only used that at each rule only a small number of α values had to be fixed

  So we can add a rule

$$\frac{\ldots \qquad \Gamma, \Delta_i \qquad \ldots}{\Gamma} \qquad \Delta_1, \ldots, \Delta_k \vdash \emptyset$$

  for quantifier-free Δ_i.

$\therefore$ Good target calculus for propositional translation
(true first-order rules don't matter)

$\rightsquigarrow$ strength measure for theories with clear computational meaning