Proof Notations and Cut-Elimination

Klaus Aehlig

Finding Witnesses From Proofs

- assume $d \vdash \forall x \exists y \varphi(x, y)$
- can find witness as follows
  - for $a \in \mathbb{N}$ get $d[\underline{a}/x] \vdash \exists y \varphi(\underline{a}, y)$
  - translate into propositional logic, unfolding induction
  - do cut-elimination

    hence only have cuts on Δ_0-formulae
  - follow a path through the proof

    via sequents $\Delta, \exists y \varphi(\underline{a}, y)$, with Δ quantifier-free and false
  - ... till the $\exists$-intro with the correct witness is found
- Works in BA as well—but there we care about proof size!

Proof Notations

- Will have to care about efficiency of proof transformations
- Full proofs are usually big; however, we'll stick to a single path $\rightsquigarrow$ use efficient proof notations!
- Notation system is a set $\mathcal{D}$ with functions
  - for the last inference, derived formula, and cut-rank
  - $d[i]$ giving a *notation* for the i'th subderivation of d
  - $o(d)$ giving the height of the derivation (denoted by) d
- Paths are given by the $\rightarrow$ relation, where $d \rightarrow d'$ iff $\exists i. d' = d[i]$

Continuous Cut-Elimination

- Need efficient notations for cut-reduction…
  …just let $\mathsf{E}d$ *be the name(!) of the cut-reduced derivation.*
- Still need efficient computation of last inference, etc.
- For proofs ending in cut, have to inspect the subderivations
  …which might end in cuts as well.

$\therefore$ introduce a void logical rule

$$\frac{\Gamma}{\Gamma}\,\mathcal{R}$$

to keep the access local

Reductions due to Cut-Elimination

- Inversion

$$\mathsf{I}\left(\dfrac{\cdots \qquad \overset{|}{A_i} \qquad \cdots}{\bigwedge_i A_i}\bigwedge\right) \quad = \quad \dfrac{\mathsf{I}\left(\overset{|}{A_j}\right)}{A_j}\,\mathcal{R}$$

- Admissible cut

$$\mathsf{R}\left(\dfrac{\overset{|}{A_j}}{\bigvee_i A_i}\bigvee^j,\ \ \bigwedge_i \overset{|}{\neg A_i}\right) \quad = \quad \dfrac{\mathsf{R}\left(\overset{|}{A_j}, \bigwedge_i \overset{|}{\neg A_i}\right) \qquad \mathsf{I}\left(\overset{|}{A_j}\right)}{\emptyset}\,(\text{Cut})$$

- Cut-rank reduction

$$\mathsf{E}\left(\dfrac{\overset{|}{C} \qquad \overset{|}{\neg C}}{\emptyset}\right) \quad = \quad \dfrac{\mathsf{R}\left(\mathsf{E}\left(\overset{|}{C}\right), \mathsf{E}\left(\overset{|}{\neg C}\right)\right)}{\emptyset}\,\mathcal{R}$$

Cut-Elimination, Summary

For $\mathcal{D}$ a notation system, cut-elimination gives these reductions.

$$\frac{d \to d' \text{ in } \mathcal{D}}{d \to d'} \qquad \frac{d \to d'}{\mathsf{I}d \to \mathsf{I}d'} \qquad \frac{e \to e'}{\mathsf{R}de \to \mathsf{R}de'}$$

$$\frac{d \to d'}{\mathsf{E}d \to \mathsf{E}d'} \qquad \frac{}{\mathsf{R}de \to \mathsf{I}d} \qquad \frac{d \to d' \qquad d \to d''}{\mathsf{E}d \to \mathsf{R}(\mathsf{E}d')(\mathsf{E}d'')}$$

Let's consider this as a term-rewrite system and analyse the size…

Bounds

- Assume $|d| \leq s$ for $d \in \mathcal{D}$. Define $\vartheta_s(d)$ and $o(d)$ for $d \in \mathsf{E}\mathcal{D}$.

$$\vartheta_s(d) = s, \text{ provided } d \in \mathcal{D}$$

$$\vartheta_s(\mathsf{I}d) = \vartheta_s(d) + 1 \qquad o(\mathsf{I}d) = o(d)$$

$$\vartheta_s(\mathsf{R}de) = \max\{|d|{+}1{+}\vartheta_s(e)\ ,\ \vartheta_s(d){+}1\} \quad o(\mathsf{R}de) = o(d) + o(e)$$

$$\vartheta_s(\mathsf{E}d) = o(d)(\vartheta_s(d) + 2) \qquad o(Ed) = 2^{o(d)} - 1$$

- then $d \to d'$ implies $o(d) > o(d')$ as usual
- Moreover $|d| \leq \vartheta_s(d)$.
- ...and this is an invariant!

$$d \to d' \qquad \Longrightarrow \qquad \vartheta_s(d) \geq \vartheta_s(d')$$

Bounds (cont'd)

We show that $d \to d'$ implies $\vartheta_s(d) \geq \vartheta_s(d')$.

- $\mathsf{R}de \to \mathsf{R}de'$ [recall: $\vartheta_s(\mathsf{R}de) = \max\{|d|{+}1{+}\vartheta_s(e)\ ,\ \vartheta_s(d){+}1\}$]

$$\begin{aligned}\vartheta_s(\mathsf{R}de')(s) \quad &= \max\{|d|{+}1{+}\vartheta_s(e')(s)\ ,\ \vartheta_s(d)(s){+}1\}\\ &\leq \max\{|d|{+}1{+}\vartheta_s(e)(s)\ ,\ \vartheta_s(d)(s){+}1\} = \vartheta_s(\mathsf{R}de)\end{aligned}$$

- The case $\mathsf{R}de \to \mathsf{I}d$ is trivial. [as $\vartheta_s(\mathsf{I}d) = \vartheta_s(d) + 1$]
- $\mathsf{E}d \to \mathsf{R}(\mathsf{E}d')(\mathsf{E}d'')$ [recall: $\vartheta_s(\mathsf{E}d) = o(d)(\vartheta_s(d) + 2)$]

$$\begin{aligned}&\vartheta_s(\mathsf{R}(\mathsf{E}d')(\mathsf{E}d''))(s)\\ =\quad & \max\{|d'|{+}2{+}o(d'')(\vartheta_s(d'')(s){+}2)\ ,\ o(d')(\vartheta_s(d')(s) + 2)\}\\ \leq\quad & \max\{\vartheta_s(d)(s){+}2{+}(o(d) - 1)(\vartheta_s(d)(s){+}2)\ ,\ (o(d) - 1)(\vartheta_s(d)(s) + 2)\}\\ =\quad & \vartheta_s(d)(s){+}2{+}(o(d) - 1)(\vartheta_s(d)(s){+}2) = o(d)(\vartheta_s(d)(s){+}2) = \vartheta_s(\mathsf{E}d)(s)\end{aligned}$$

Consequences

- $\vartheta_s(e)$ bounds the size of *all* notations for subproofs of e
  note: $\vartheta_s(e) \geq \vartheta_s(e') \geq \vartheta_s(e'') \geq \ldots$ *for* $e \to e' \to e'' \to \ldots$

- Let d_a be a derivations of logarithmic height
  (with constant size notations)

$$\begin{aligned}\vartheta_s(\mathsf{EE}d_a) &= o(\mathsf{E}d_a) \cdot (\vartheta_s(\mathsf{E}d_a) + a) \\ &= (2^{\log|a|} - 1) \cdot (\log|a| \cdot (s+2) + 2) \\ &= |a|^{O(1)}\end{aligned}$$

$\therefore$ searching a witness through the proof $\mathsf{EE}d_a$ is a PLS problem
(even tough the path is exponentially long)

- In particular this applies to the Σ_1^b-consequences of S_2^2