LIX

École Polytechnique

The Realm of Cut-Elimination

Incorporating Tables into Proofs

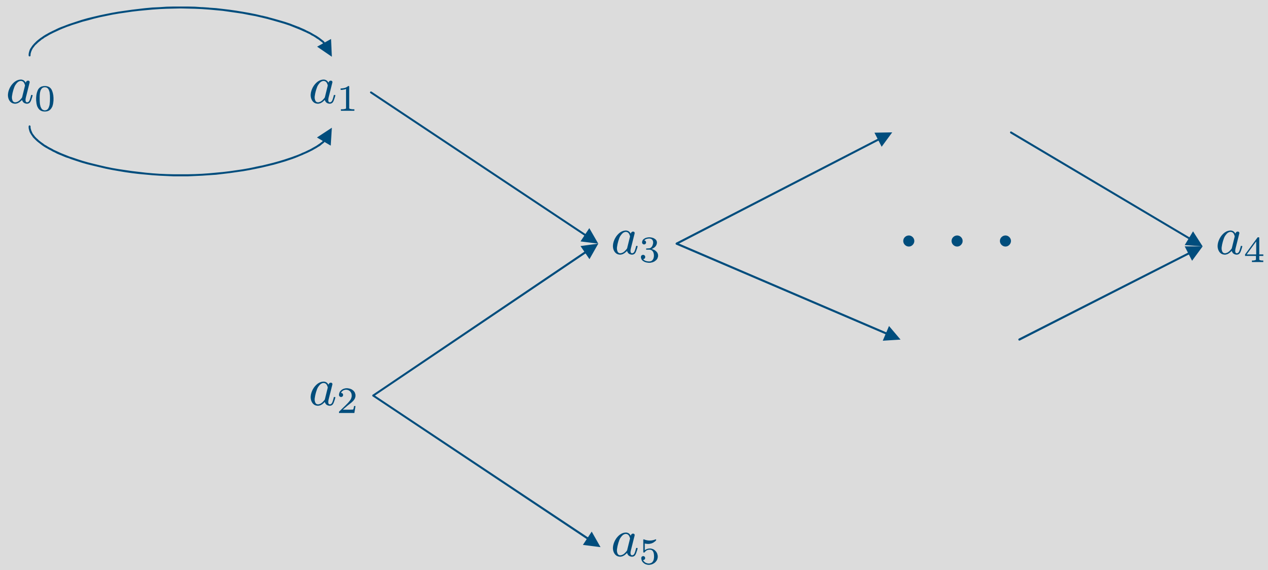
by Vivek Nigam & Dale Miller

14^{th} of May, 2007

Agenda

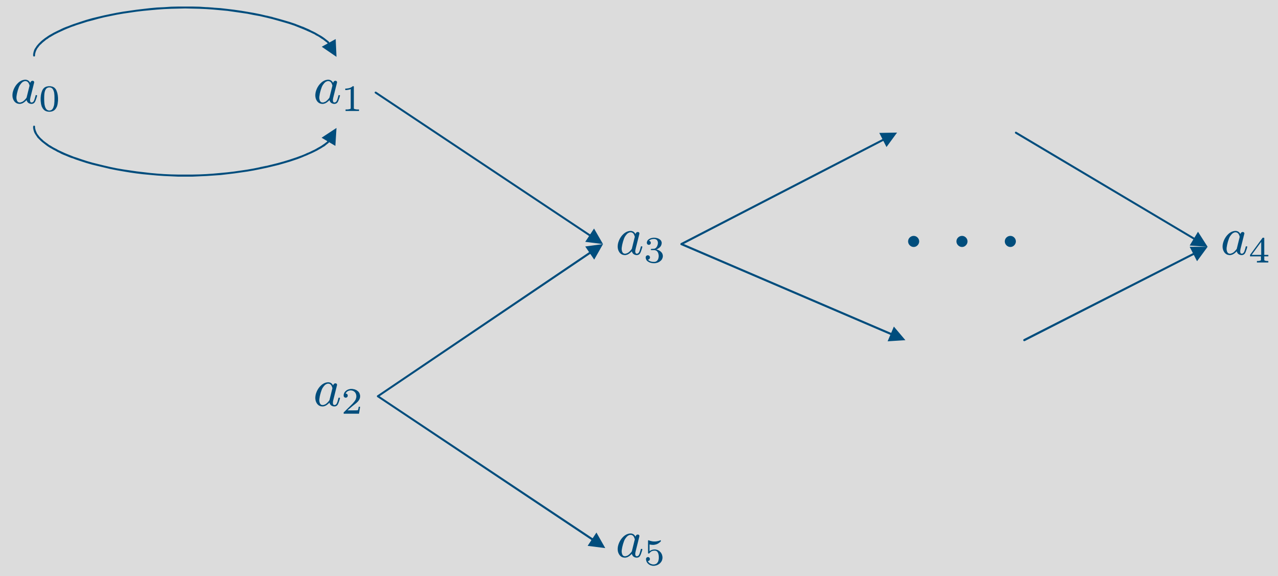
- **Motivational Examples**
- Focusing
- Finite Successes and Finite Failures
- Applications
- Conclusions and Future Works

$$
\begin{tikzcd}
a_0 \arrow[r, bend left] \arrow[r, bend right] & a_1 \arrow[dr] & & & \\
& & a_3 \arrow[r, shift left] \arrow[r, shift right] & \cdots \arrow[r, shift left] \arrow[r, shift right] & a_4 \\
& a_2 \arrow[ur] \arrow[dr] & & & \\
& & a_5 & &
\end{tikzcd}
$$



$\forall x(path\,x\,x)$
$\forall x \forall y \forall z(\mathrm{arr}\ x\ z \wedge path\ z\ y \supset path\ x\ y)$

$path\ a_1\ a_4 \wedge path\ a_2\ a_4$



$\forall x (path\, x\, x)$
$\forall x \forall y \forall z (\mathrm{arr}\ x\ z \wedge \mathrm{path}\ z\ y \supset \mathrm{path}\ x\ y)$

$path\ a_1\ a_4 \wedge path\ a_2\ a_4$

Common Subgoal

$path\ a_3\ a_4$

- The common subgoal is computed twice.

How to avoid this declaratively:

How to avoid this declaratively:

Cuts are not that bad

- Introduce with a cut the common subgoal

$$\frac{\mathcal{P} \vdash A \qquad \mathcal{P}, A \vdash A \wedge G}{\mathcal{P} \vdash A \wedge G}\ cut$$

How to avoid this declaratively:

Cuts are not that bad

- Introduce with a cut the common subgoal

$$\frac{\mathcal{P} \vdash A \quad \mathcal{P}, A \vdash A \wedge G}{\mathcal{P} \vdash A \wedge G}\ cut$$

Another example (without cuts)

- Change to an equivalent goal:

$$A \wedge G \equiv A \wedge (A \supset G)$$

How to avoid this declaratively:

Cuts are not that bad

- Introduce with a cut the common subgoal

$$\frac{\mathcal{P} \vdash A \quad \mathcal{P}, A \vdash A \wedge G}{\mathcal{P} \vdash A \wedge G}\ cut$$

Another example (without cuts)

- Change to an equivalent goal:

$$A \wedge G \equiv A \wedge (A \supset G)$$

But we are only increasing non-determinism:

- The are now more proofs for the goal;
- How to give a purely **proof theoretic solution** where common subgoals aren't re-proven.

Agenda

- Motivational Examples
- **Focusing**
- Finite Successes and Finite Failures
- Applications
- Conclusions and Future Works

LJF system [Liang & Miller]

$$\frac{[N,\Gamma] \xrightarrow{N} [R]}{[N,\Gamma] \longrightarrow [R]}\ D_l \qquad \frac{[\Gamma] -_P\!\!\rightarrow}{[\Gamma] \longrightarrow [P]}\ D_r \qquad \frac{[\Gamma], P \longrightarrow [R]}{[\Gamma] \xrightarrow{P} [R]}\ R_l \quad \frac{[\Gamma] \longrightarrow N}{[\Gamma] -_N\!\!\rightarrow}\ R_r$$

$$\frac{[\Gamma, N_a], \Theta \longrightarrow \mathcal{R}}{[\Gamma], \Theta, N_a \longrightarrow \mathcal{R}}\ []_l \quad \frac{[\Gamma], \Theta \longrightarrow [P_a]}{[\Gamma], \Theta \longrightarrow P_a}\ []_r$$

$$\frac{}{[\Gamma] \xrightarrow{A_n} [A_n]}\ I_l \quad \frac{}{[\Gamma, A_p] -_{A_p}\!\!\rightarrow}\ I_r$$

$$\frac{}{[\Gamma], \Theta, \bot \longrightarrow \mathcal{R}}\ false_l \quad \frac{[\Gamma], \Theta \longrightarrow \mathcal{R}}{[\Gamma], \Theta, true \longrightarrow \mathcal{R}}\ true_l \quad \frac{}{[\Gamma] -_{true}\!\!\rightarrow}\ true_r$$

$$\frac{[\Gamma], \Theta, A, B \longrightarrow \mathcal{R}}{[\Gamma], \Theta, A \wedge B \longrightarrow \mathcal{R}}\ \wedge_l \quad \frac{[\Gamma] -_A\!\!\rightarrow \quad [\Gamma] -_B\!\!\rightarrow}{[\Gamma] -_{A \wedge B}\!\!\rightarrow}\ \wedge_r \qquad \frac{[\Gamma] -_A\!\!\rightarrow \quad [\Gamma] \xrightarrow{B} [R]}{[\Gamma] \xrightarrow{A \supset B} [R]}\ \supset_l \quad \frac{[\Gamma], \Theta, A \longrightarrow B}{[\Gamma], \Theta \longrightarrow A \supset B}\ \supset_r$$

$$\frac{[\Gamma], \Theta, A \longrightarrow \mathcal{R}}{[\Gamma], \Theta, \exists y A \longrightarrow \mathcal{R}}\ \exists_l \quad \frac{[\Gamma] -_{A[t/x]}\!\!\rightarrow}{[\Gamma] -_{\exists x A}\!\!\rightarrow}\ \exists_r \quad \frac{[\Gamma] \xrightarrow{A[t/x]} [R]}{[\Gamma] \xrightarrow{\forall x A} [R]}\ \forall_l \quad \frac{[\Gamma], \Theta \longrightarrow A}{[\Gamma], \Theta \longrightarrow A}\ \forall_r$$

Playing with polarities

$\{a, a \supset b, b \supset c\}$

Playing with polarities

$\{a, a \supset b, b \supset c\}$

b is negative

$$
\begin{prooftree}
\AxiomC{}
\RightLabel{I_r}
\UnaryInfC{$[\Gamma]{-_a\to}$}
\AxiomC{}
\RightLabel{I_l}
\UnaryInfC{$[\Gamma] \xrightarrow{b} [b]$}
\RightLabel{$\supset_l$}
\BinaryInfC{$[\Gamma] \xrightarrow{a \supset b} [b]$}
\RightLabel{D_l}
\UnaryInfC{$[\Gamma] \longrightarrow [b]$}
\UnaryInfC{$[\Gamma] \longrightarrow b$}
\RightLabel{R_r}
\UnaryInfC{$[\Gamma]{-_b\to}$}
\AxiomC{}
\RightLabel{I_l}
\UnaryInfC{$[\Gamma] \xrightarrow{c} [c]$}
\RightLabel{$\supset_l$}
\BinaryInfC{$[\Gamma] \xrightarrow{b \supset c} [c]$}
\end{prooftree}
$$

Playing with polarities

$$\{a, a \supset b, b \supset c\}$$

b is negative

$$\dfrac{\dfrac{\dfrac{\dfrac{\dfrac{\dfrac{}{[\Gamma]-_a\!\!\to}\,I_r \qquad \dfrac{}{[\Gamma] \xrightarrow{b} [b]}\,I_l}{[\Gamma] \xrightarrow{a\supset b} [b]}\,\supset_l}{[\Gamma] \longrightarrow [b]}\,D_l}{[\Gamma] \longrightarrow b}}{[\Gamma]-_b\!\!\to}\,R_r \qquad \dfrac{}{[\Gamma] \xrightarrow{c} [c]}\,I_l}{[\Gamma] \xrightarrow{b\supset c} [c]}\,\supset_l$$

b is positive

$$\dfrac{\dfrac{}{[\Gamma]-_a\!\!\to}\,I_r \qquad \dfrac{\dfrac{\dfrac{\dfrac{\dfrac{}{[b,\Gamma]-_b\!\!\to}\,I_r \qquad \dfrac{}{[b,\Gamma] \xrightarrow{c} [c]}\,I_l}{[b,\Gamma] \xrightarrow{b\supset c} [c]}\,\supset_l}{[b,\Gamma] \longrightarrow [c]}\,D_l}{[\Gamma], b \longrightarrow [c]}}{[\Gamma] \xrightarrow{b} [c]}\,R_l}{[\Gamma] \xrightarrow{a\supset b} [c]}\,\supset_l$$

Changing polarities doesn't affect provability:

$$LJF^t$$

$$\mathcal{P}; \Gamma \longrightarrow G$$

$$\frac{\mathcal{P}; [\Gamma] \longrightarrow [L_1] \qquad \cdots \qquad \mathcal{P}; [\Gamma] \longrightarrow [L_n] \qquad \mathcal{P} \cup \Delta_P; [\Gamma \cup \Delta_L] \longrightarrow [R]}{\mathcal{P}; [\Gamma] \longrightarrow [R]}\ mc$$

Changing polarities doesn't affect provability:

$$LJF^t$$

$$\mathcal{P}; \Gamma \longrightarrow G$$

$$\frac{\mathcal{P}; [\Gamma] \longrightarrow [L_1] \qquad \cdots \qquad \mathcal{P}; [\Gamma] \longrightarrow [L_n] \qquad \mathcal{P} \cup \Delta_P; [\Gamma \cup \Delta_L] \longrightarrow [R]}{\mathcal{P}; [\Gamma] \longrightarrow [R]}\ mc$$

Proposition: *LJF*^{t} is sound and complete w.r.t. *LJF*

Agenda

- Motivational Examples
- Focusing
- **Finite Successes and Finite Failures**
- Applications
- Conclusions and Future Works

Tables are a partially ordered set of lemmas

$\mathcal{T} = \langle \mathcal{A}, \prec \rangle$ $\Rightarrow$

Multi Cut Derivation

$$\dfrac{\Gamma \longrightarrow A_1 \quad \cdots \quad \Gamma \longrightarrow A_n \quad \begin{array}{c} \Pi \\ \Gamma, A_1, \ldots, A_n \longrightarrow G \end{array}}{\Gamma \longrightarrow G}\ mc$$

Tables are a partially ordered set of lemmas

$\mathcal{T} = \langle \mathcal{A}, \prec \rangle$ $\Longrightarrow$

Multi Cut Derivation

$$\dfrac{\Gamma \longrightarrow A_1 \quad \cdots \quad \Gamma \longrightarrow A_n \quad \overset{\Pi}{\Gamma, A_1, \ldots, A_n \longrightarrow G}}{\Gamma \longrightarrow G}\ mc$$

Where do tables come from:

- Interactive theorem proving – Boyer & Moore;
- Logic Programming – *Memoization*;
- In *Proof Carrying Code*, can be extracted from an known proof (e.g. depth first traversal);

Consider: Horn Theory and Tables composed only of atoms

Proposition 1. *Let Γ be a set of Horn clauses, $A \in \mathcal{P} \cap \Gamma$, and Ξ be an arbitrary LJF^t proof tree for $\mathcal{P}; [\Gamma] -_G \rightarrow$. Then every occurrence of a sequent with right-hand side the atom A is the conclusion of an $I_r^t(A)$ rule.*

Consider: Horn Theory and Tables composed only of atoms

Proposition 1. *Let Γ be a set of Horn clauses, $A \in \mathcal{P} \cap \Gamma$, and Ξ be an arbitrary LJF^t proof tree for $\mathcal{P}; [\Gamma] -_G \rightarrow$. Then every occurrence of a sequent with right-hand side the atom A is the conclusion of an $I_r^t(A)$ rule.*

Coming back to the Example

$$
\dfrac{
\dfrac{
\dfrac{
\dfrac{}{\{\mathrm{path}\ a_3\ a_4\}; [\Gamma, \mathrm{path}\ a_3\ a_4] \xrightarrow{\mathrm{arr}\, a_1\, a_3} [\mathrm{arr}\, a_1\, a_3]}\ I_l^t
}{\{\mathrm{path}\ a_3\ a_4\}; [\Gamma, \mathrm{path}\ a_3\ a_4] \longrightarrow [\mathrm{arr}\, a_1\, a_3]}
}{\{\mathrm{path}\ a_3\ a_4\}; [\Gamma, \mathrm{path}\ a_3\ a_4] -_{\mathrm{arr}\, a_1\ a_3} \rightarrow}
\quad
\dfrac{}{\{\mathrm{path}\ a_3\ a_4\}; [\Gamma, \mathrm{path}\ a_3\ a_4] -_{\mathrm{path}\ a_3\ a_4} \rightarrow}\ I_r^t
}{
\dfrac{\{\mathrm{path}\ a_3\ a_4\}; [\Gamma, \mathrm{path}\ a_3\ a_4] -_{\mathrm{arr}\, a_1\ a_3 \wedge \mathrm{path}\ a_3\ a_4} \rightarrow}{\{\mathrm{path}\ a_3\ a_4\}; [\Gamma, \mathrm{path}\ a_3\ a_4] \longrightarrow [\mathrm{path}\ a_1\ a_4]}\ D_l^t, \forall_l^t, \forall_l^t, \forall_l^t, \supset_l^t
}
$$

Consider: Horn Theory and Tables composed by atoms

Proposition 1. *Let Γ be a set of Horn clauses, $A \in \mathcal{P} \cap \Gamma$, and Ξ be an arbitrary LJF^t proof tree for $\mathcal{P}; [\Gamma] -_G \rightarrow$. Then every occurrence of a sequent with right-hand side the atom A is the conclusion of an $I^t_r(A)$ rule.*

Coming back to the Example

$$\frac{\Gamma \longrightarrow A \qquad \Gamma \longrightarrow G}{\Gamma \longrightarrow A \wedge G} \Longrightarrow \frac{\mathcal{P}; [\Gamma] \longrightarrow [A] \qquad \mathcal{P} \cup \{A\}; [\Gamma, A] \longrightarrow [A \wedge G]}{\mathcal{P}; [\Gamma] \longrightarrow [A \wedge G]}\ mc$$

Consider: Horn Theory and Tables composed by literals

Use definitions (FOLD – McDowell & Miller):

$$\frac{\{\mathcal{P}; [\Gamma\theta], \Theta\theta \longrightarrow \mathcal{R}\theta \mid \theta = mgu(H, A) \text{ for some clause } H \stackrel{\Delta}{=} B\}}{\mathcal{P}; [\Gamma], \Theta, A \longrightarrow \mathcal{R}} \ \text{Def}_l, A \notin \mathcal{P}$$

$$\frac{\mathcal{P}; [\Gamma] -_{B\theta}\!\!\rightarrow}{\mathcal{P}; [\Gamma] -_{A}\!\!\rightarrow} \ \text{Def}_r, A \notin \mathcal{P}, \ \text{where } H \stackrel{\Delta}{=} B, \text{ and} H\theta = A$$

Consider: Horn Theory and Tables composed by literals

Use definitions (FOLD – McDowell & Miller):

$$\frac{\{\mathcal{P};[\Gamma\theta],\Theta\theta \longrightarrow \mathcal{R}\theta \mid \theta = mgu(H,A) \text{ for some clause } H \stackrel{\Delta}{=} B\}}{\mathcal{P};[\Gamma],\Theta,A \longrightarrow \mathcal{R}} \ \mathrm{Def}_l,\ A \notin \mathcal{P}$$

$$\frac{\mathcal{P};[\Gamma]{-}_{B\theta}{\rightarrow}}{\mathcal{P};[\Gamma]{-}_{A}{\rightarrow}} \ \mathrm{Def}_r,\ A \notin \mathcal{P},\ \text{where } H \stackrel{\Delta}{=} B,\ \text{and} H\theta = A$$

Theorem 1. *Let $\mathcal{D}$ be a set of definitions, Γ be a set of literals with positive polarity, and $L \in \Gamma$. Let Ξ be an arbitrary proof tree of $\mathcal{P};[\Gamma]{-}_{G}{\rightarrow}$ in $FO\lambda^{\Delta t}$, then all subproofs Ξ' of Ξ, that prove the literal L, are trivial.*

Agenda

- Motivational Examples
- Focusing
- Finite Successes and Finite Failures
- **Applications**
- Conclusions and Future Works

Declarative Interpretation for *Memoization*

Both finite successes and finite failures are stored in a table, and if:

- There is another attempt to prove a **finite success**, the proof search ends with success;
  - **Follows from the previous result;**

Declarative Interpretation for *Memoization*

Both finite successes and finite failures are stored in a table, and if:

- There is another attempt to prove a **finite success**, the proof search ends with success;
  - **Follows from the previous result;**
- There is another attempt to prove a **finite failure**, this proof search fails immediately
  - **Follows from the following result:**

Proposition 1. *Let A be an atom such that $\Gamma \longrightarrow A$ is not provable in $FO\lambda^{\Delta}$, and $A \in \mathcal{P}$. Let Ξ be an arbitrary $FO\lambda^{\Delta t}$ derivation for $\mathcal{P}; [\Gamma] -_G \rightarrow$. Then all sequents in Ξ, with right-hand side A, are open leafs.*

Proof Carrying Code – Table as Proof Objects

If tables are used as proof objects they seem to enjoy the following crucial properties:

- Small
- Easy to Check,
- Flexible

Proposition 1. *Let Ξ be a LJF proof of $\Gamma \longrightarrow G$, and let $\mathcal{T}$ be a table obtained from Ξ. There exists a proof for $mcd(\mathcal{T}, \Gamma \longrightarrow G)$ such that all of its branches have trivial proofs.*

Agenda

- Motivational Examples
- Focusing
- Finite Successes and Finite Failures
- Applications
- **Conclusions and Future Works**

Conclusions and Future Works

- **Extend these results to stronger logics**
  - Hereditary Harrop Formulas;
  - mu-Mall (Sequent calculus with Induction and Co-induction).
- **Investigate connections with Interactive Theorem Proving**
  - Use a sequence of lemmas to prove a theorem in such a way that the gaps between them are “easy” to be found.