Which proofs can be computed by cut-elimination?

Stefan Hetzl
Institute of Discrete Mathematics and Geometry
Vienna University of Technology

ASL 2012 North American Annual Meeting
Special Session: Structural Proof Theory and Computing

Madison, Wisconsin

April 3, 2012
Gentzen’s proof

3.11 3.33. Das äußerste Zeichen von \( M \) sei \( \forall \). Dann lautet das Ende der Herleitung:

\[
\begin{align*}
\text{AES} & \quad \frac{\Gamma_1 \rightarrow \Theta_1, \forall x \exists x}{\Gamma_1 \rightarrow \Theta_1, \forall x \exists x} \\
\text{AEA} & \quad \frac{\exists b, \Gamma_2 \rightarrow \Theta_2}{\forall x \exists x, \Gamma_2 \rightarrow \Theta_2} \\
\frac{\Gamma_1, \Gamma_2 \rightarrow \Theta_1, \Theta_2}{\text{Mischung}}
\end{align*}
\]

Man wandelt es um zu:

\[
\begin{align*}
\text{Mischung} & \quad \frac{\exists b, \Gamma_2 \rightarrow \Theta_2}{\exists b, \Gamma_2 \rightarrow \Theta_2} \\
\text{evtl. mehrmalige Verdünnung und Vertauschung.}
\end{align*}
\]

Über die linke Obersequenz der Mischung, \( \Gamma_1 \rightarrow \Theta_1, \exists b \), schreibt man denselben Herleitungsteil, der vorher über \( \Gamma_1 \rightarrow \Theta_1, \forall a \) stand, doch ersetzt man darin die freie Gegenstandsvariable \( a \) überall wo sie vorkommt durch \( b \). Aus der Hilfsbehauptung 3.103 zusammen mit 3.101 geht nun

\[ \Rightarrow \] Cut-elimination by local proof rewriting steps
Definition. Cut-elimination is the relation $\rightarrow$ on proofs obtained from local reduction rules, e.g.:

$$
\begin{align*}
\frac{(\pi_1)}{\Gamma \vdash \Delta, A[x \backslash \alpha]} & \quad (\pi_2) \quad \frac{A[x \backslash t], \Pi \vdash \Lambda}{\forall x A, \Pi \vdash \Lambda} & \forall r \\

\frac{\Gamma \vdash \Delta, \forall x A}{\Gamma \vdash \Delta, \forall x A, \Pi \vdash \Lambda} & \frac{\forall x A, \Pi \vdash \Lambda}{\Gamma, \Pi \vdash \Delta, \Lambda} & \text{cut}
\end{align*}
$$

as transitive, compatible closure.

Definition. $\pi$ is in normal form if there is no $\pi'$ with $\pi \rightarrow \pi'$. $\pi$ in normal form iff $\pi$ cut-free.
Properties of Cut-Elimination

- **Definition.** $\Rightarrow$ is called *confluent* if $a \Rightarrow b$ and $a \Rightarrow c$ implies that there is $d$ s.t. $b \Rightarrow d$ and $c \Rightarrow d$.

- **Fact.** $\Rightarrow$ is not confluent.

- **Definition.** $\Rightarrow$ is called *strongly normalising* if there are no infinite reduction sequences.

- **Fact.** $\Rightarrow$ is not strongly normalising.

- **Definition.** A *reduction strategy* is a subrelation of $\Rightarrow$.

- **Fact.** There are confluent and strongly normalising strategies (e.g. Gentzen: uppermost, $\text{LK}^{\text{tq}}$, $\bar{\lambda}\bar{\mu}$, ...).
Motivation

Which proofs can be computed by cut-elimination?

- Computer science:
  Which programming languages can be built on classical proof systems?
  (Curry-Howard correspondence for classical logic)

- Mathematics:
  How sensitive are methods of proof mining to non-deterministic choices?

- Foundational:
  What is the constructive content of classical proofs?
Outline

✓ Motivation

▶ Non-Confluence

▶ Towards a Characterisation
The complexity of cut-elimination:

**Theorem** [Statman ’79, Orevkov ’79]. There is a sequence of proofs \((\pi_n : \varphi_n)_{n \geq 1}\) with \(|\pi_n|\) polynomial in \(n\) s.t. the shortest cut-free proof of \(\varphi_n\) has length \(2^n\).

where

- \(|\pi|\) is the number of inferences in \(\pi\),
- \(2_0 = 1, \text{ and } 2_{n+1} = 2^{2n}\).

**Theorem** [Baaz, H ’11]. There is a sequence of proofs \((\chi_n)_{n \geq 1}\) with \(|\chi_n|\) polynomial in \(n\) s.t. the number of different normal forms of \(\chi_n\) is \(2^n\).
Cut-Elimination in Arithmetical Theories

- Elimination of Induction

\[
\begin{align*}
\frac{(\pi_1)}{\Gamma \vdash \Delta, A(0)} & \quad \frac{(\pi_2)}{A(\alpha), \Gamma \vdash \Delta, A(s(\alpha))} \\
& \quad \frac{\text{ind}}{\Gamma \vdash \Delta, A(t)}
\end{align*}
\]

If \( t \) is variable-free, there is \( n \in \mathbb{N} \) s.t. \( |t| = n \)

\[
\begin{align*}
\frac{(\pi_1)}{\Gamma \vdash \Delta, A(0)} & \quad \frac{(\pi_2[\alpha \backslash 0])}{A(0), \Gamma \vdash \Delta, A(s(0))} \\
& \quad \frac{\text{cut}}{\Gamma \vdash \Delta, A(s(0))} \\
& \quad \vdots \\
& \quad \frac{\Gamma \vdash \Delta, A(s^n(0))}{A(s^n(0)) \vdash A(t)} \\
& \quad \frac{\text{cut}}{\Gamma \vdash \Delta, A(t)}
\end{align*}
\]

- In proof of \( \Sigma_1 \)-sentence there is always a variable-free \( t \).
Non-Confluence in Arithmetic

- $I\Sigma_1$ in sequent calculus:
  - Axioms for minimal arithmetic + rule for $\Sigma_1$-induction
  - Reduction relation for cut-elimination

- **Definition.** $T$ computational extension of $I\Sigma_1$ if it (reasonably) extends inference rules and reduction rules.

- **Theorem** [H ’12]. Let $T$ be a computational extension of $I\Sigma_1$. The number of normal forms of $T$-proofs cannot be bound by a function that is provably total in $T$. 
Outline

✓ Motivation
✓ Non-Confluence
▶ Towards a Characterisation
 Witnesses

- Which aspects of normal forms shall be described? Witnesses!

- **Herbrand's Theorem.** For \( A \) quantifier-free: \( \exists x A \) valid iff there are terms \( t_1, \ldots, t_n \) s.t. \( \bigvee_{i=1}^n A[x \setminus t_i] \) is a tautology. 
  \( \Rightarrow \) “Herbrand-disjunction”

- **Fact.** \( \exists x A \) has a cut-free proof with \( n \) quantifier inferences iff \( \exists x A \) has a Herbrand-disjunction with \( n \) disjuncts. 
  \( \Rightarrow \) Notation \( H(\pi) = \{A[x \setminus t_1], \ldots, A[x \setminus t_n]\} \)

- Given \( \pi: \exists x A \) with cuts, what can we say about \( H(\pi^*) \) for \( \pi \rightarrow \pi^* \) and \( \pi^* \) cut-free?
Definition. For a proof $\pi: \exists x \ A$ with $A$ quantifier-free define a regular tree grammar $G(\pi)$.

Theorem [H ’10]. If $\pi: \exists x \ A$ with $A$ quantifier-free and $\pi^*$ cut-free with $\pi \rightarrow \pi^*$, then $H(\pi^*) \subseteq L(G(\pi))$. 
Regular Tree Grammars

- **Def.** A *regular tree grammar* is a quadruple $G = \langle \alpha, N, \Sigma, R \rangle$
  - *start symbol* $\alpha$
  - set $N$ of *non-terminal symbols* with $\alpha \in N$
  - a signature $\Sigma$, the *terminal symbols* with $\Sigma \cap N = \emptyset$
  - set $R$ of *production rules* $\beta \to t$ where $\beta \in N$ and $t \in \mathcal{T}(\Sigma \cup N)$

- $s \to_G t$ if $s = r[\beta]$ and $t = r[u]$ and $\beta \to u \in R$
- $L(G) := \{ t \in \mathcal{T}(\Sigma) \mid \alpha \to_G t \}$ where $\to_G$ reflexive and transitive closure of $\to_G$

- **Example.** $\langle \text{List}, \{ \text{List, Nat} \}, \{0/0, s/1, \text{nil}/0, \text{cons}/2\}, R \rangle$ for $R = \{ \text{List} \to \text{nil}, \text{List} \to \text{cons(\text{Nat, List})}, \text{Nat} \to 0, \text{Nat} \to s(\text{Nat}) \}$
Example

\[
\begin{align*}
\vdash P(a), P(b) & \quad \exists_r \\
\vdash \exists x P(x), P(b) & \quad \exists_r \\
\vdash \exists x P(x) & \quad \exists_r \\
\end{align*}
\]

\[
\begin{align*}
P(\alpha) & \vdash Q(f(\alpha)) \\
P(\alpha) & \vdash \exists x Q(x) \\
\end{align*}
\]

\[
\begin{align*}
P(\alpha), Q(\beta) & \vdash R(g(\alpha, \beta)) \\
P(\alpha), Q(\beta) & \vdash \exists x R(x) \\
\end{align*}
\]

\[
\begin{align*}
P(\alpha) & \vdash \exists x R(x) \\
\exists x P(x) & \vdash \exists x R(x) \\
\end{align*}
\]

\[
\begin{align*}
\vdash \exists x R(x) \\
\exists x P(x) & \vdash \exists x R(x) \\
\end{align*}
\]

\[
\begin{align*}
\exists r & \\
\exists l & \\
c_{l, \text{cut}} &
\end{align*}
\]
Example

\[
\begin{align*}
\frac{\vdash P(a), P(b)}{\vdash \exists x P(x), P(b)} & \quad \exists_r \quad \frac{\exists_r}{\vdash \exists x P(x)} \quad \frac{\vdash P(\alpha), Q(\beta) \vdash R(g(\alpha, \beta))}{\exists_r} \\
\frac{\vdash P(a), P(b)}{\vdash \exists x P(x), \exists x P(x)} & \quad \exists_r \quad \frac{\vdash P(\alpha) \vdash Q(f(\alpha))}{\vdash \exists x Q(x)} \quad \exists_r \quad \frac{\vdash P(\alpha), Q(\beta) \vdash \exists x R(x)}{\vdash P(\alpha), \exists x Q(x) \vdash \exists x R(x)} \quad \exists_r \\
\frac{\vdash P(\alpha) \vdash \exists x R(x)}{\vdash \exists x P(x) \vdash \exists x R(x)} & \quad \exists_l \quad \frac{\exists_r}{\vdash \exists x R(x)} \\
\frac{\vdash \exists x P(x) \vdash \exists x R(x)}{\vdash \exists x R(x)} & \quad \exists_l \quad \frac{\exists_r}{\vdash \exists x R(x)} \\
\end{align*}
\]

\[G(\pi) = \langle \phi, N, \Sigma, R \rangle \text{ where } N = \{ \phi, \alpha, \beta \} \text{ and } R = \{ \]

14/17
Example

\[
\frac{\vdash P(a), P(b)}{\vdash \exists x P(x), P(b)}\quad \exists_r
\]

\[
\frac{\vdash \exists x P(x), \exists x P(x)}{\vdash \exists x P(x)}\quad \exists_r
\]

\[
\frac{P(\alpha) \vdash \exists x Q(x)}{\exists_r}
\]

\[
\frac{P(\alpha), Q(\beta) \vdash R(g(\alpha, \beta))}{\exists_r}
\]

\[
\frac{P(\alpha) \vdash \exists x Q(x)}{\exists_r}
\]

\[
\frac{P(\alpha), Q(\beta) \vdash \exists x R(x)}{\exists_r}
\]

\[
\frac{P(\alpha) \vdash \exists x R(x)}{\exists_r}
\]

\[
\frac{\exists x P(x) \vdash \exists x R(x)}{\exists_l}
\]

\[
\frac{\exists x P(x) \vdash \exists x R(x)}{\exists_l}
\]

\[
\vdash \exists x R(x)
\]

\[
\exists_l, \text{cut}
\]

\[
\exists_l, \text{cut}
\]

\[
G(\pi) = \langle \varphi, N, \Sigma, R \rangle \text{ where } N = \{\varphi, \alpha, \beta\} \text{ and } R = \{\varphi \rightarrow R(g(\alpha, \beta))\},
\]
Example

\[ \vdash P(a), P(b) \]
\[ \vdash \exists x P(x), P(b) \quad \exists_r \]
\[ \vdash \exists x P(x), \exists x P(x) \quad \exists_r \]
\[ \vdash \exists x R(x) \quad \exists_l \]
\[ \vdash \exists x P(x) \quad \exists_r \]
\[ \vdash \exists x Q(x) \quad \exists_r \]
\[ \vdash P(\alpha), Q(\beta) \vdash R(g(\alpha, \beta)) \quad \exists_r \]
\[ \vdash P(\alpha), \exists x Q(x) \vdash \exists x R(x) \]
\[ \vdash P(\alpha) \vdash Q(f(\alpha)) \quad \exists_r \]
\[ \vdash P(\alpha) \vdash \exists x Q(x) \quad \exists_r \]
\[ \vdash P(\alpha), Q(\beta) \vdash \exists x R(x) \quad \exists_l \]
\[ \vdash \exists x P(x) \vdash \exists x R(x) \quad \exists_l \]
\[ \vdash \exists x R(x) \quad \exists_l \]

\[ G(\pi) = \langle \varphi, N, \Sigma, R \rangle \] where \( N = \{ \varphi, \alpha, \beta \} \) and \( R = \{ \varphi \rightarrow R(g(\alpha, \beta)), \beta \rightarrow f(\alpha) \} \)
Example

\[
\begin{align*}
\frac{\vdash P(a), P(b)}{\vdash \exists x P(x), P(b)} & \quad \exists_r \\
\frac{\vdash \exists x P(x), \exists x P(x)}{\vdash \exists x P(x)} & \quad \exists_r \\
\frac{\vdash \exists x P(x), \exists x P(x)}{\vdash \exists x P(x)} & \quad \exists_r \\
\end{align*}
\]

\[
\begin{align*}
\frac{\vdash P(\alpha), Q(\beta)}{\vdash \exists x R(x)} & \quad \exists_r \\
\end{align*}
\]

\[
\begin{align*}
\frac{\vdash P(\alpha)}{\vdash \exists x Q(x)} & \quad \exists_r \\
\frac{\vdash P(\alpha), \exists x Q(x)}{\vdash \exists x R(x)} & \quad \exists_l \\
\frac{\vdash P(\alpha)}{\vdash \exists x R(x)} & \quad \exists_l \\
\frac{\vdash \exists x R(x)}{\vdash \exists x R(x)} & \quad \exists_l \\
\end{align*}
\]

\[
\begin{align*}
\vdash \exists x P(x), \exists x P(x) & \vdash \exists x R(x) \\
\vdash \exists x P(x) & \vdash \exists x R(x) \\
\vdash \exists x R(x) & \quad \exists_l \\
\end{align*}
\]

\[
\begin{align*}
G(\pi) = \langle \varphi, N, \Sigma, R \rangle \text{ where } N = \{\varphi, \alpha, \beta\} \text{ and } \\
R = \{\varphi \rightarrow R(g(\alpha, \beta)), \beta \rightarrow f(\alpha), \alpha \rightarrow a, \alpha \rightarrow b\}
\end{align*}
\]
G(\pi) = \langle \varphi, N, \Sigma, R \rangle$ where $N = \{ \varphi, \alpha, \beta \}$ and $R = \{ \varphi \to R(g(\alpha, \beta)), \beta \to f(\alpha), \alpha \to a, \alpha \to b \}$

$L(G(\pi)) = \{ R(g(a, f(a)), R(g(a, f(b))), R(g(b, f(a))), R(g(b, f(b)))) \}$
Extensions

- Analogous upper bound for Peano Arithmetic
- Tight bound for proofs with $\Sigma_1$-cuts known
Conclusion

- Many different normal forms . . .
- . . . that do share certain structural properties.
- Formal language theory useful in proof theory

Future Work:

- Tighten upper bound
- Is there a finite upper bound?, i.e.
  Is there, for every $\pi$ a finite $H$ s.t. $\pi \rightarrow \pi'$ and
  $\pi'$ cut-free implies $H(\pi') \subseteq H$?
  known: no for multisets
  yes for $\Sigma_1$-cuts
- Computer science: proof compression by cut-introduction
Thank you!