# 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

G. Gentzen: *Untersuchungen über das logische Schließen I*, Mathematische Zeitschrift, 39(2), 176–210, 1934

3.11 3.33. Das äußerste Zeichen von $\mathfrak{M}$ sei $\forall$. Dann lautet das Ende der Herleitung:

$$\dfrac{\dfrac{\Gamma_1 \to \Theta_1, \mathfrak{F}\mathfrak{a}}{\Gamma_1 \to \Theta_1, \forall \mathfrak{x}\mathfrak{F}\mathfrak{x}}\,AES \qquad \dfrac{\mathfrak{F}\mathfrak{b}, \Gamma_2 \to \Theta_2}{\forall \mathfrak{x}\mathfrak{F}\mathfrak{x}, \Gamma_2 \to \Theta_2}\,AEA}{\Gamma_1, \Gamma_2 \to \Theta_1, \Theta_2}\,\text{Mischung.}$$

Man wandelt es um zu:

$$\dfrac{\dfrac{\Gamma_1 \to \Theta_1, \mathfrak{F}\mathfrak{b} \qquad \mathfrak{F}\mathfrak{b}, \Gamma_2 \to \Theta_2}{\Gamma_1, \Gamma_2^* \to \Theta_1^*, \Theta_2}\,\text{Mischung}}{\Gamma_1, \Gamma_2 \to \Theta_1, \Theta_2}\,\text{evtl. mehrmalige Verdünnung und Vertauschung.}$$

Über die linke Obersequenz der Mischung, $\Gamma_1 \to \Theta_1, \mathfrak{F}\mathfrak{b}$, schreibt man denselben Herleitungsteil, der vorher über $\Gamma_1 \to \Theta_1, \mathfrak{F}\mathfrak{a}$ stand, doch ersetzt man darin die freie Gegenstandsvariable $\mathfrak{a}$ überall wo sie vorkommt durch $\mathfrak{b}$. Aus der Hilfsbehauptung 3.103 zusammen mit 3.101 geht nun

$\Longrightarrow$ Cut-elimination by local proof rewriting steps

# Cut-Elimination as Proof Rewriting

- **Definition**. Cut-elimination is the relation $\rightarrow$ on proofs obtained from local reduction rules, e.g.:

$$\dfrac{\dfrac{\begin{matrix}(\pi_1)\\ \Gamma \vdash \Delta, A[x\backslash\alpha]\end{matrix}}{\Gamma \vdash \Delta, \forall x\, A}\ \forall_r \qquad \dfrac{\begin{matrix}(\pi_2)\\ A[x\backslash t], \Pi \vdash \Lambda\end{matrix}}{\forall x\, A, \Pi \vdash \Lambda}\ \forall_l}{\Gamma, \Pi \vdash \Delta, \Lambda}\ \text{cut} \quad \rightarrow \quad \dfrac{\begin{matrix}(\pi_1[\alpha\backslash t])\\ \Gamma \vdash \Delta, A[x\backslash t]\end{matrix} \qquad \begin{matrix}(\pi_2)\\ A[x\backslash t], \Pi \vdash \Lambda\end{matrix}}{\Gamma, \Pi \vdash \Delta, \Lambda}\ \text{cut}$$

  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, $\mathbf{LK^{tq}}$, $\bar{\lambda}\mu\tilde{\mu}$, ...).

# 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

# Non-Confluence in First-Order Logic

- 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 $\pi$,
  - $2_0 = 1$, and $2_{n+1} = 2^{2_n}$.

- **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 $2_n$.

- Elimination of Induction

$$\dfrac{\begin{matrix}(\pi_1) \\ \Gamma \vdash \Delta, A(0)\end{matrix} \quad \begin{matrix}(\pi_2) \\ A(\alpha), \Gamma \vdash \Delta, A(s(\alpha))\end{matrix}}{\Gamma \vdash \Delta, A(t)} \text{ ind}$$

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

$$\dfrac{\dfrac{\begin{matrix}(\pi_1) \\ \Gamma \vdash \Delta, A(0)\end{matrix} \quad \begin{matrix}(\pi_2[\alpha\backslash 0]) \\ A(0), \Gamma \vdash \Delta, A(s(0))\end{matrix}}{\begin{matrix}\Gamma \vdash \Delta, A(s(0)) \\ \vdots \\ \Gamma \vdash \Delta, A(s^n(0))\end{matrix}} \text{ cut} \qquad A(s^n(0)) \vdash A(t)}{\Gamma \vdash \Delta, A(t)} \text{ cut}$$

- 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. $\bigvee_{i=1}^{n} A[x \backslash t_i]$ 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 $\mathrm{H}(\pi) = \{A[x \backslash t_1], \ldots, A[x \backslash t_n]\}$
- Given $\pi : \exists x\, A$ with cuts, what can we say about $\mathrm{H}(\pi^*)$ for $\pi \to \pi^*$ and $\pi^*$ cut-free ?

# An Upper Bound

- **Definition**. For a proof $\pi : \exists x\, A$ with $A$ quantifier-free define a regular tree grammar $\mathrm{G}(\pi)$.

- **Theorem** [H '10]. If $\pi : \exists x\, A$ with $A$ quantifier-free and $\pi^*$ cut-free with $\pi \to \pi^*$, then $\mathrm{H}(\pi^*) \subseteq \mathrm{L}(\mathrm{G}(\pi))$.

# 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 $\beta \to u \in R$
  - $\mathsf{L}(G) := \{t \in \mathcal{T}(\Sigma) \mid \alpha \twoheadrightarrow_G t\}$ where
    $\twoheadrightarrow_G$ reflexive and transitive closure of $\to_G$

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

$$R = \{\text{List} \to \text{nil}, \text{List} \to \text{cons}(\text{Nat}, \text{List}),$$
$$\text{Nat} \to 0, \text{Nat} \to s(\text{Nat})\}$$

# Example

$$
\dfrac{
\dfrac{
\dfrac{
\dfrac{\vdash P(a), P(b)}{\vdash \exists x P(x), P(b)}\ \exists_r
}{\vdash \exists x P(x), \exists x P(x)}\ \exists_r
}{\vdash \exists x P(x)}\ c_r
\qquad
\dfrac{
\dfrac{
\dfrac{P(\alpha) \vdash Q(f(\alpha))}{P(\alpha) \vdash \exists x Q(x)}\ \exists_r
\quad
\dfrac{
\dfrac{P(\alpha), Q(\beta) \vdash R(g(\alpha, \beta))}{P(\alpha), Q(\beta) \vdash \exists x R(x)}\ \exists_r
}{P(\alpha), \exists x Q(x) \vdash \exists x R(x)}\ \exists_l
}{P(\alpha) \vdash \exists x R(x)}\ c_l, \mathrm{cut}
}{\exists x P(x) \vdash \exists x R(x)}\ \exists_l
}{\vdash \exists x R(x)}\ \mathrm{cut}
$$

# Example

$$
\dfrac{\dfrac{\dfrac{\vdash P(a), P(b)}{\vdash \exists x P(x), P(b)}\ \exists_r}{\vdash \exists x P(x), \exists x P(x)}\ \exists_r}{\vdash \exists x P(x)}\ c_r
\qquad
\dfrac{\dfrac{P(\alpha) \vdash Q(f(\alpha))}{P(\alpha) \vdash \exists x Q(x)}\ \exists_r \quad \dfrac{\dfrac{P(\alpha), Q(\beta) \vdash R(g(\alpha,\beta))}{P(\alpha), Q(\beta) \vdash \exists x R(x)}\ \exists_r}{P(\alpha), \exists x Q(x) \vdash \exists x R(x)}\ \exists_l}{\dfrac{P(\alpha) \vdash \exists x R(x)}{\exists x P(x) \vdash \exists x R(x)}\ \exists_l}\ c_l, \text{cut}
$$

$$
\dfrac{\vdash \exists x P(x) \qquad \exists x P(x) \vdash \exists x R(x)}{\vdash \exists x R(x)}\ \text{cut}
$$

$\mathrm{G}(\pi) = \langle \varphi, N, \Sigma, R \rangle$ where $N = \{\varphi, \alpha, \beta\}$ and
$R = \{$

# Example

$$
\dfrac{
  \dfrac{
    \dfrac{
      \dfrac{\vdash P(a), P(b)}{\vdash \exists x P(x), P(b)}\ \exists_r
    }{\vdash \exists x P(x), \exists x P(x)}\ \exists_r
  }{\vdash \exists x P(x)}\ c_r
  \qquad
  \dfrac{
    \dfrac{
      \dfrac{P(\alpha) \vdash Q(f(\alpha))}{P(\alpha) \vdash \exists x Q(x)}\ \exists_r
      \qquad
      \dfrac{
        \dfrac{P(\alpha), Q(\beta) \vdash \color{blue}{R(g(\alpha,\beta))}}{P(\alpha), Q(\color{green}{\beta}) \vdash \exists x R(x)}\ \exists_r
      }{P(\alpha), \exists x Q(x) \vdash \exists x R(x)}\ \exists_l
    }{P(\color{red}{\alpha}) \vdash \exists x R(x)}\ c_l, \text{cut}
  }{\exists x P(x) \vdash \exists x R(x)}\ \exists_l
}{\vdash \exists x R(x)}\ \text{cut}
$$

$G(\pi) = \langle \varphi, N, \Sigma, R \rangle$ where $N = \{\color{blue}{\varphi}, \color{red}{\alpha}, \color{green}{\beta}\}$ and
$R = \{\color{blue}{\varphi} \color{blue}{\rightarrow} \color{blue}{R(g(\alpha, \beta))},$

# Example

$$
\dfrac{
\dfrac{\dfrac{\dfrac{\vdash P(a), P(b)}{\vdash \exists x P(x), P(b)}\ \exists_r}{\vdash \exists x P(x), \exists x P(x)}\ \exists_r}{\vdash \exists x P(x)}\ c_r
\qquad
\dfrac{\dfrac{\dfrac{P(\alpha) \vdash Q(f(\alpha))}{P(\alpha) \vdash \exists x Q(x)}\ \exists_r \quad \dfrac{\dfrac{P(\alpha), Q(\beta) \vdash R(g(\alpha, \beta))}{P(\alpha), Q(\beta) \vdash \exists x R(x)}\ \exists_r}{P(\alpha), \exists x Q(x) \vdash \exists x R(x)}\ \exists_l}{P(\alpha) \vdash \exists x R(x)}\ c_l, \text{cut}}{\exists x P(x) \vdash \exists x R(x)}\ \exists_l
}{\vdash \exists x R(x)}\ \text{cut}
$$

$\mathrm{G}(\pi) = \langle \varphi, N, \Sigma, R \rangle$ where $N = \{\varphi, \alpha, \beta\}$ and
$R = \{\varphi \to R(g(\alpha, \beta)), \beta \to f(\alpha),$

# Example

$$\dfrac{\dfrac{\dfrac{\dfrac{\vdash P(a), P(b)}{\vdash \exists x P(x), P(b)}\ \exists_r}{\vdash \exists x P(x), \exists x P(x)}\ \exists_r}{\vdash \exists x P(x)}\ c_r \qquad \dfrac{\dfrac{\dfrac{P(\alpha) \vdash Q(f(\alpha))}{P(\alpha) \vdash \exists x Q(x)}\ \exists_r \quad \dfrac{\dfrac{P(\alpha), Q(\beta) \vdash R(g(\alpha, \beta))}{P(\alpha), Q(\beta) \vdash \exists x R(x)}\ \exists_r}{P(\alpha), \exists x Q(x) \vdash \exists x R(x)}\ \exists_l}{P(\alpha) \vdash \exists x R(x)}\ c_l, \text{cut}}{\exists x P(x) \vdash \exists x R(x)}\ \exists_l}{\vdash \exists x R(x)}\ \text{cut}$$

$\mathrm{G}(\pi) = \langle \varphi, N, \Sigma, R \rangle$ where $N = \{\varphi, \alpha, \beta\}$ and
$R = \{\varphi \to R(g(\alpha, \beta)), \beta \to f(\alpha), \alpha \to a, \alpha \to b\}$

# Example

$$
\dfrac{
\dfrac{
\dfrac{
\dfrac{\vdash P(a), P(b)}{\vdash \exists x P(x), P(b)}\,\exists_r
}{\vdash \exists x P(x), \exists x P(x)}\,\exists_r
}{\vdash \exists x P(x)}\,c_r
\qquad
\dfrac{
\dfrac{
\dfrac{P(\alpha) \vdash Q(f(\alpha))}{P(\alpha) \vdash \exists x Q(x)}\,\exists_r
\quad
\dfrac{
\dfrac{P(\alpha), Q(\beta) \vdash R(g(\alpha, \beta))}{P(\alpha), Q(\beta) \vdash \exists x R(x)}\,\exists_r
}{P(\alpha), \exists x Q(x) \vdash \exists x R(x)}\,\exists_l
}{P(\alpha) \vdash \exists x R(x)}\,c_l, \mathrm{cut}
}{\exists x P(x) \vdash \exists x R(x)}\,\exists_l
}{\vdash \exists x R(x)}\,\mathrm{cut}
$$

$\mathrm{G}(\pi) = \langle \varphi, N, \Sigma, R \rangle$ where $N = \{\varphi, \alpha, \beta\}$ and
$R = \{\varphi \to R(g(\alpha, \beta)), \beta \to f(\alpha), \alpha \to a, \alpha \to b\}$

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

# Extensions

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

# Summary

**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. $\pi \to \pi'$ and $\pi'$ cut-free implies $\mathrm{H}(\pi') \subseteq H$ ?
  known: no for multisets
  yes for $\Sigma_1$-cuts
- Computer science: proof compression by cut-introduction

Thank you!


- M. Baaz, S. Hetzl. *On the non-confluence of cut-elimination*, Journal of Symbolic Logic 76(1), 313–340, 2011
- S. Hetzl. *The Computational Content of Arithmetical Proofs*, to appear in the Notre Dame Journal of Formal Logic
- S. Hetzl. *On the form of witness terms*, Archive for Mathematical Logic 49(5), 529-554, 2010
- S. Hetzl. *Applying Tree Languages in Proof Theory*, Language and Automata Theory and Applications (LATA) 2012, Springer LNCS 7183, 301–312