On the form of witness terms

Stefan Hetzl
INRIA Saclay – Île-de-France
École Polytechnique

Logic Colloquium 2009
July 31, 2009

Motivation

- Cut-elimination one of the central tools of proof theory
- Cut-elimination applied to mathematical proofs
- non-deterministic $\Rightarrow$ mathematically different results
- Characterization of possible results ?
- Methods: witness terms

Herbrand's theorem

- **Herbrand's Thm.** If $\exists \bar{x} A(\bar{x})$ is valid, then there are tuples of terms $\bar{t}_i$ s.t. $\bigvee_{i=1}^{k} A(\bar{t}_i)$ is a tautology.
- Algebraic structure of the set of Herbrand-disjunctions of $\exists \bar{x} A(\bar{x})$:

$$\{\ \{A(\bar{t}_i) \mid i \in I\}\ \mid\ I \subseteq \mathbb{N}, \bigvee_{i \in I} A(\bar{t}_i) \text{ tautology}\}$$

  Least upper bound ?

- $\mathrm{H}(\pi)$ ... quantifier-free instances of end-formula
- **Prop**. If $\pi \rightarrow \pi^*$ then there is a set Σ of substiutions s.t. $\mathrm{H}(\pi^*) = \mathrm{H}(\pi)\Sigma$.

Example

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

$$\mathrm{H}(\pi) = \{C(g(\alpha, \beta))\}$$

Define set of base substitutions $\mathrm{B}(\pi)$ of π.

Example:

$$
\dfrac{
\dfrac{\dfrac{\dfrac{\vdash A(a), A(b)}{\vdash \exists x A(x), A(b)}\;\exists_r}{\vdash \exists x A(x), \exists x A(x)}\;\exists_r}{\vdash \exists x A(x)}\;c_r
\qquad
\dfrac{\dfrac{
\dfrac{A(\alpha) \vdash B(f(\alpha))}{A(\alpha) \vdash \exists x B(x)}\;\exists_r
\quad
\dfrac{\dfrac{A(\alpha), B(\beta) \vdash C(g(\alpha,\beta))}{A(\alpha), B(\beta) \vdash \exists x C(x)}\;\exists_r}{A(\alpha), \exists x B(x) \vdash \exists x C(x)}\;\exists_l
}{A(\alpha) \vdash \exists x C(x)}\;c_l, \mathrm{cut}}{\exists x A(x) \vdash \exists x C(x)}\;\exists_l
}{\vdash \exists x C(x)}\;\mathrm{cut}
$$

$$\mathrm{B}(\pi) = \{[\alpha \leftarrow a], [\alpha \leftarrow b], [\beta \leftarrow f(\alpha)]\}$$

Regular Tree Grammars

- **Def**. A *regular tree grammar* is a quadruple $G = (\alpha, N, F, R)$
  - *axiom* α
  - set N of *non-terminal symbols* with $\alpha \in N$
  - set F of *terminal symbols* with $F \cap N = \varnothing$
  - set R of production rules $\beta \to t$ where
    $\beta \in N$ and $t \in \mathrm{T}(F \cup N)$
  - $s \to_G t$ if $s = r[\beta]$ and $t = r[u]$ and $\beta \to u \in R$
  - $\mathrm{L}(G) := \{t \in \mathrm{T}(F) \mid \alpha \twoheadrightarrow_G t\}$ where
    $\twoheadrightarrow_G$ reflexive and transitive closure of $\to_G$

The Upper Bound

- **Def.** For a proof π of a Σ_1-sentence define $\mathrm{G}(\pi) := (\varphi, N, F, R)$ where $N = \{\varphi, \alpha_1, \dots, \alpha_n\}$, $F = \Sigma(\pi)$ and $R = \{\varphi \to A \mid A \in \mathrm{H}(\pi)\} \cup \{\alpha \to t \mid [\alpha \leftarrow t] \in \mathrm{B}(\pi)\}$.
- **Theorem.** Let π be a proof of a Σ_1-sentence. Let π^* be a cut-free proof with $\pi \to \pi^*$. Then $\mathrm{H}(\pi^*) \subseteq \mathrm{L}(\mathrm{G}(\pi))$.
- Upper bound, but not *least* upper bound.

Cut-Elimination in PA

- **Thm**. If π is a PA-proof of a Σ_1-sentence $\exists x\ F(x)$, then $\pi \to \pi^*$ where π^* is cut- and induction-free.
- **Def**. For a proof π of $\exists x\ F(x)$, write $\mathrm{W}(\pi)$ for the terms inserted for x in π.
- If π^* is a cut- and induction-free proof of $\exists x\ F(x)$ and $\mathrm{W}(\pi^*) = \{t_1, \ldots, t_n\}$ then $\mathrm{PA} \vdash F(t_1) \vee \ldots \vee F(t_n)$.
- Adapt base substitutions to

$$\frac{\Gamma \vdash \Delta, F(0) \quad F(y), \Pi \vdash \Lambda, F(y')}{\Gamma, \Pi \vdash \Delta, \Lambda, F(t)}\ \mathrm{ind}$$

The Upper Bound in PA

- **Theorem.** Let π be a PA-proof of a Σ_1-sentence. Let π^* be a cut- and induction-free proof with $\pi \to \pi^*$. Then $\mathsf{W}(\pi^*) \subseteq \mathsf{L}(\mathsf{G}(\pi))$.

- uniformity: $\pi : \forall x \exists y\, F(x, y)$, $\pi(\alpha) : \exists y\, F(\alpha, y)$

$$\mathsf{G}(\pi(\bar{n})) = \mathsf{G}(\pi(\alpha))[\alpha \leftarrow \bar{n}]$$

Example (1/3)

- For all $m \geqslant 2$ and $n \geqslant 1$ there is a number between n and $m^2 \cdot n$ which can be written as a sum of two squares.
- $S(\overline{n})$ true iff there are $n_1, n_2 \in \mathbb{N}$ with $n_1^2 + n_2^2 = n$
  $A(m, n, k) \;:=\; n < k \wedge k \leqslant m^2 \cdot n \wedge S(k)$
- $\pi :=$

$$
\dfrac{\dfrac{\dfrac{\vdots}{\vdash \overline{1} < \overline{2} \wedge \overline{2} \leqslant (\mu'')^2 \cdot \overline{1} \wedge S(\overline{2})}}{\vdash \exists k\, A(\mu'', \overline{1}, k)}\ \exists_r \qquad \dfrac{(\mathrm{IS})}{\exists k\, A(\mu'', \nu_0', k) \vdash \exists k\, A(\mu'', \nu_0'', k)}\ \exists_l}{\dfrac{\vdash \exists k\, A(\mu'', \nu', k)}{\vdash \forall m \forall n \exists k\, A(m'', n', k)}\ \forall_r, \forall_r}\ \mathrm{ind}
$$

Example (2/3)

- IS :=

$$\dfrac{\dfrac{\dfrac{\begin{array}{c}\vdots\\ \nu_0'' < \kappa, A(\mu'', \nu_0', \kappa) \vdash A(\mu'', \nu_0'', \kappa)\end{array}}{\nu_0'' < \kappa, A(\mu'', \nu_0', \kappa) \vdash \exists k\, A(\mu'', \nu_0'', k)}\ \exists_r}{A(\mu'', \nu_0', \kappa) \vdash \exists k\, A(\mu'', \nu_0'', k), \neg \nu_0'' < \kappa}\ \neg_r \qquad (\mathrm{IS}')}{A(\mu'', \nu_0', \kappa) \vdash \exists k\, A(\mu'', \nu_0'', k)}\ \mathrm{cut}$$

- IS$'$:=

$$\dfrac{\dfrac{(\mathrm{IS}_1') \qquad (\mathrm{IS}_2') \qquad (\mathrm{IS}_3')}{\neg \nu_0'' < \kappa, A(\mu'', \nu_0', \kappa) \vdash A(\mu'', \nu_0'', (\mu'')^2 \cdot \kappa)}\ \wedge_l^*, w_l, \wedge_r^*}{\neg \nu_0'' < \kappa, A(\mu'', \nu_0', \kappa) \vdash \exists k\, A(\mu'', \nu_0'', k)}\ \exists_r$$

- IS$_1'$ proves $\nu_0' < \kappa \vdash \nu_0'' < (\mu'')^2 \cdot \kappa$
- IS$_2'$ proves $\neg \nu_0'' < \kappa \vdash (\mu'')^2 \cdot \kappa \leqslant (\mu'')^2 \cdot \nu_0''$
- IS$_3'$ proves $S(\kappa) \vdash S((\mu'')^2 \cdot \kappa)$

Example (3/3)

- $\mathsf{G}(\pi(\mu,\nu)) = (\tau, N, F, R)$ with $\tau, \kappa, \nu_0 \in N$ and $R =$

$$
\begin{array}{lll}
\tau \to \overline{2} & \kappa \to \overline{2} & \nu_0 \to 0 \\
\tau \to \kappa & \kappa \to \kappa & \nu_0 \to \nu_0' \\
\tau \to (\mu'')^2 \cdot \kappa & \kappa \to (\mu'')^2 \cdot \kappa & \mathrm{R}^*
\end{array}
$$

Example (3/3)

- $\mathsf{G}(\pi(\mu,\nu)) = (\tau, N, F, R)$ with $\tau, \kappa, \nu_0 \in N$ and $R =$

$$
\begin{aligned}
\tau &\to \overline{2} & \qquad \kappa &\to \overline{2} \\
\tau &\to \kappa & \qquad \kappa &\to \kappa \\
\tau &\to (\mu'')^2 \cdot \kappa & \qquad \kappa &\to (\mu'')^2 \cdot \kappa
\end{aligned}
$$

Example (3/3)

- $\mathsf{G}(\pi(\mu, \nu)) = (\tau, N, F, R)$ with $\tau, \kappa, \nu_0 \in N$ and $R =$

$$\tau \rightarrow \overline{2}$$
$$\tau \rightarrow \tau$$
$$\tau \rightarrow (\mu'')^2 \cdot \tau$$

Example (3/3)

- $\mathsf{G}(\pi(\mu,\nu)) = (\tau, N, F, R)$ with $\tau, \kappa, \nu_0 \in N$ and $R =$

$$\tau \to \overline{2}$$
$$\tau \to (\mu'')^2 \cdot \tau$$

Example (3/3)

- $G(\pi(\mu,\nu)) = (\tau, N, F, R)$ with $\tau, \kappa, \nu_0 \in N$ and $R =$

$$\tau \to \overline{2}$$
$$\tau \to (\mu'')^2 \cdot \tau$$

- Every witness is of the form $2 \cdot m^{2i}$
  - No odd sums of two squares
  - No Pythagorean triples
  - The argument

    between n and $2 \cdot n$ there is a power of two

    cannot be obtained (for $m \geqslant 3$).

Conclusion

- Upper bound on reachable witness terms
- Characterized by regular tree grammar
- First-order logic, Peano-arithmetic

Future Work:

- Characterization of the *least* upper bound
- Computational use