Inductive theorem proving based on tree grammars

Stefan Hetzl

Institute of Discrete Mathematics and Geometry
Vienna University of Technology

joint work with S. Eberhard

2nd Workshop on Automated Inductive Theorem Proving
Chalmers University, Gothenburg, Sweden

March 20, 2015

Introduction

- Invariants are (often) non-analytic
  How to find key lemma?
- Consider proofs of instances $A(n)$ of $\forall x\, A(x)$
  E.g. bounded model checking, constructive ω-rule, ...
- Proof-theoretic analysis of structure of instance-proofs
  - Based on Herbrand's theorem and tree grammars
  - Extending method for cut-introduction to induction

Outline

$\Rightarrow$ Cut-elimination and cut-introduction

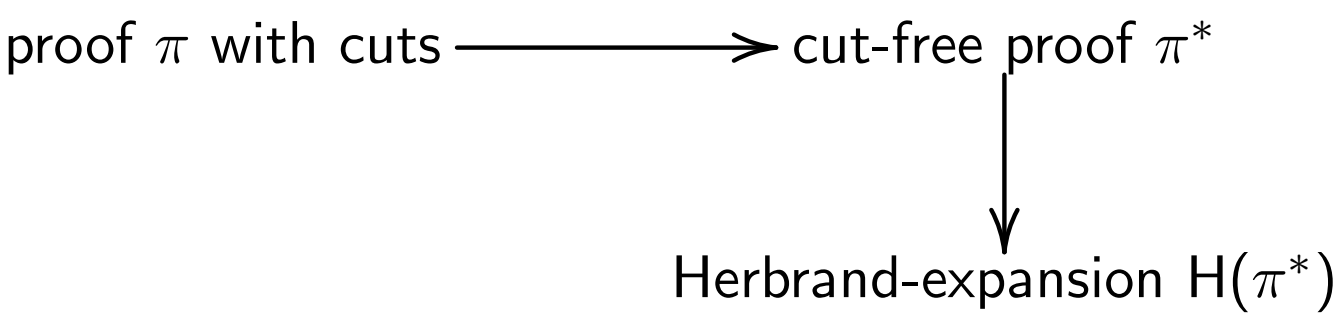
- Inductive theorem proving based on tree grammars
- Example

Cut-elimination and Herbrand's theorem

- The cut rule:

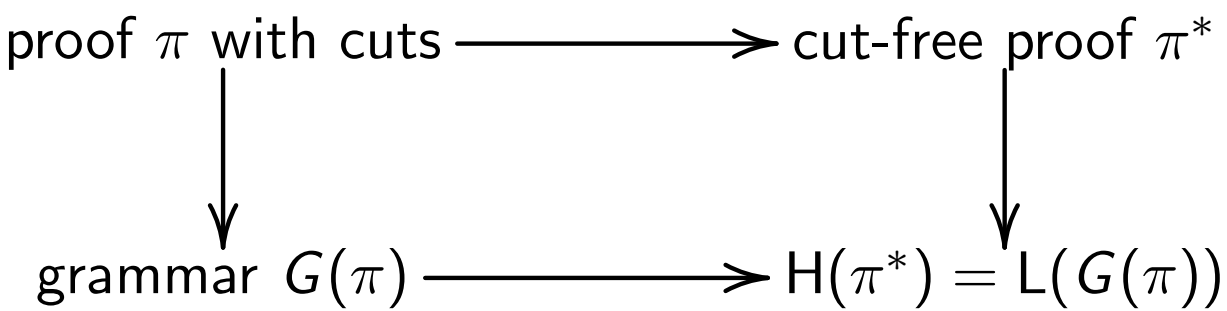
$$\frac{\Gamma \vdash \Delta, A \quad A, \Pi \vdash \Lambda}{\Gamma, \Pi \vdash \Delta, \Lambda}\ \text{cut}$$

- **Cut-elimination theorem** (Gentzen 1934). Every proof can be transformed into a proof without cuts.
- **Herbrand's theorem** (1930). A first-order formula φ is valid iff a finite expansion of φ is a tautology.
  E.g. $\exists x\, A_{\text{qf}}(x)$ expands to $A_{\text{qf}}(t_1) \vee \ldots \vee A_{\text{qf}}(t_n)$
- In total:

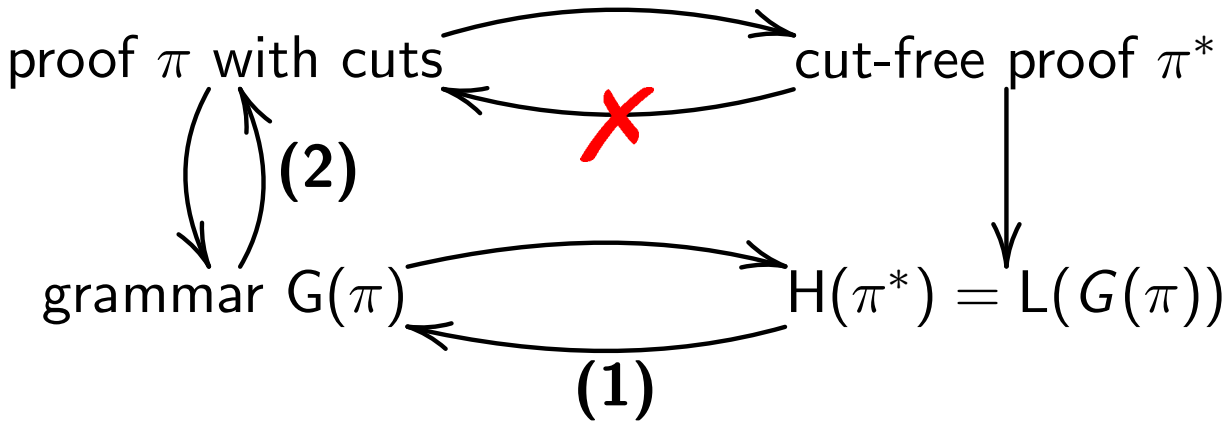


Cut-elimination and tree grammars

- Information of Herbrand-expansion $A_{\text{qf}}(t_1) \vee \ldots \vee A_{\text{qf}}(t_n)$ is $T = \{t_1, \ldots, t_n\}$ – a (finite) tree language.
- **Theorem** (H 2012). If π is a proof with Π_1-cuts then there is a totally rigid acyclic tree grammar $G(\pi)$ s.t. $L(G(\pi))$ is a Herbrand-expansion and $|G(\pi)| \leq |\pi|$.
- In total:



Cut-introduction based on tree grammars



1. Given L, compute G s.t. $L(G) = L$ (or $L(G) \supseteq L$).
2. Solve second-order unification problem, e.g.

$$S(X) \quad \equiv \quad X(\alpha) \to (X(t_1) \wedge X(t_2)) \vdash A(u_1), A(u_2), A(u_3)$$

Find F s.t. $S(F)$ is a tautology

- Quantifier-free
- Every solution gives proof with cuts
- For $S(X)$ induced by grammar for Π_1-cuts: always solvable

Outline

- ✓ Cut-elimination and cut-introduction
- ⇒ Inductive theorem proving based on tree grammars
- ▶ Example

Cut and induction

$$\dfrac{\begin{array}{cc}(\pi_b) & (\pi_s(\alpha)) \\ \Gamma \vdash A(0) & \Gamma, A(\alpha) \vdash A(s\alpha)\end{array}}{\Gamma \vdash A(t)}\ \text{ind}$$

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

$$\dfrac{\dfrac{\begin{array}{cc}(\pi_1) & (\pi_2(0)) \\ \Gamma \vdash A(0) & A(0), \Gamma \vdash A(s0)\end{array}}{\Gamma \vdash A(s0)}\ \text{cut}}{\vdots}$$

$$\dfrac{\begin{array}{cc}\Gamma \vdash A(s^n 0) & A(s^n 0) \vdash A(t)\end{array}}{\Gamma \vdash A(t)}\ \text{cut}$$

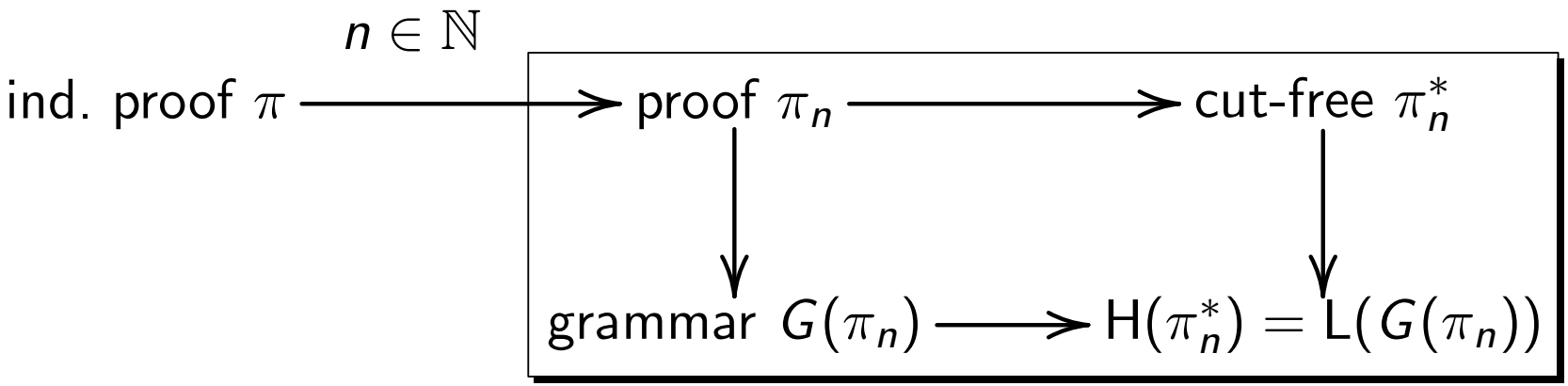
$\Rightarrow$ Induction is infinitary cut

Simple induction proofs

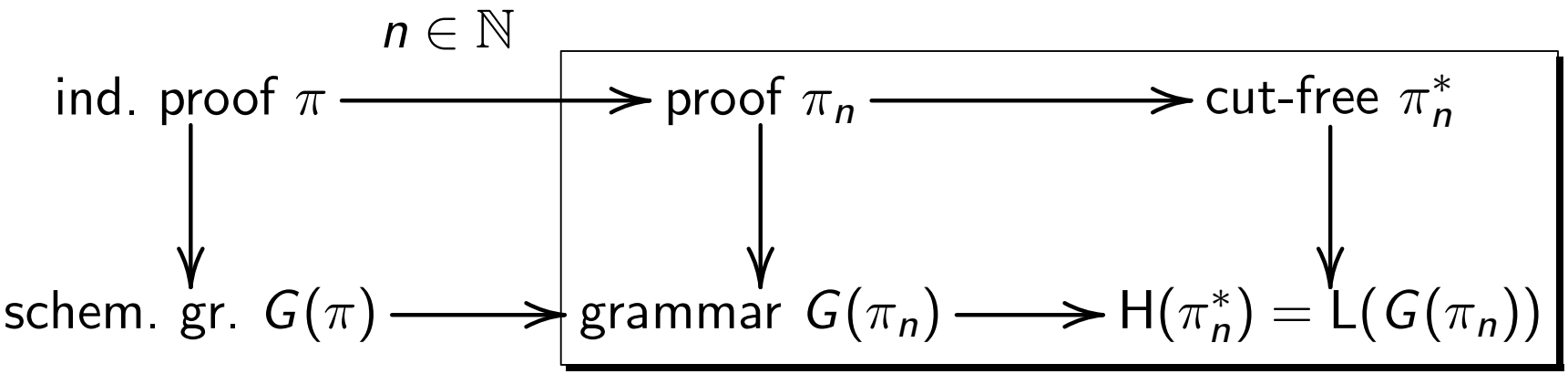
no nested induction, Π_1-invariant

$$\dfrac{\dfrac{\Gamma \vdash \forall y F[\alpha, 0, y] \quad \Gamma, \forall y F[\alpha, \nu, y] \vdash \forall y F[\alpha, s\nu, y]}{\Gamma \vdash \forall y F[\alpha, \alpha, y]} \qquad \Gamma, \forall y F[\alpha, \alpha, y] \vdash B[\alpha]}{\dfrac{\Gamma \vdash B[\alpha]}{\Gamma \vdash \forall x B[x]}}\ \text{cut}$$

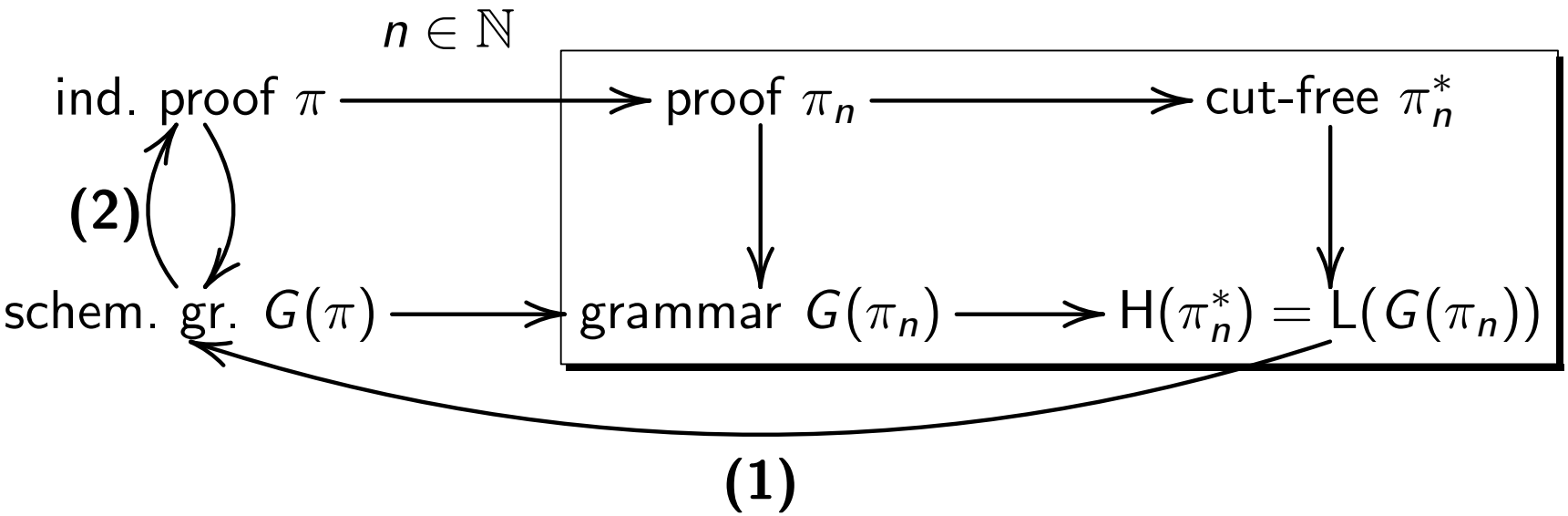
Induction and tree grammars (1/3)



Induction and tree grammars (2/3)



Induction and tree grammars (3/3)



Inductive theorem proving based on tree grammars

1. Compute schematic grammar G from $\{H(\pi_i^*) \mid i \in M \subseteq_{\text{fin}} \mathbb{N}\}$ s.t. $\mathsf{L}(G_i) \supseteq H(\pi_i^*)$ for all $i \in M$.
   - Finding smallest such G by PTIME-translation to MaxSAT
   - No coverage-guarantee for all $i \in \mathbb{N}$

2. Solve unification problem of the form:
   $\Gamma_0 \vdash X[\alpha, 0, \beta]$
   $\Gamma_1, \bigwedge_{1 \leq i \leq n} X[\alpha, \nu, t_i[\alpha, \nu, \gamma]] \vdash X[\alpha, s\nu, \gamma]$
   $\Gamma_2, \bigwedge_{1 \leq i \leq m} X[\alpha, \alpha, u_i[\alpha]] \vdash B[\alpha]$
   - Quantifier-free
   - Every solution gives inductive proof
   - In general: undecidable, but complete algorithm
   - Fast heuristics

The algorithm

Input: background theory Γ, statement $\forall x\, A(x)$

1. Compute instance proofs $\{\pi_i^* : A(i) \mid i \in M \subseteq_{\text{fin}} \mathbb{N}\}$
2. Compute schematic grammar G s.t. $L(G_i) \supseteq H(\pi_i^*)$ for $i \in M$
3. $S(X) :=$ unification problem induced by G
4. (Try to) find an F s.t. $S(F)$ is a tautology
5. $\pi :=$ proof induced by $S(F)$

Output: inductive proof π of $\Gamma \vdash \forall x\, A(x)$

Outline

- ✓ Cut-elimination and cut-introduction
- ✓ Inductive theorem proving based on tree grammars
- ⇒ Example

Example: Factorial (1/4)

- Background theory

$f(0) = 1$	$(f0)$
$f(sx) = sx \cdot f(x)$	$(fST(x))$
$g(x, 0) = x$	$(g0(x))$
$g(x, sy) = g(x \cdot sy, y)$	$(gST(x, y))$
$x \cdot 1 = x$	$(1R(x))$
$1 \cdot x = x$	$(1L(x))$
$(x \cdot y) \cdot z = x \cdot (y \cdot z)$	$(ASSO(x, y, z))$

- Want to prove $g(1, \alpha) = f(\alpha)$
- Needs generalisation to $\forall y\, g(y, \alpha) = y \cdot f(\alpha)$

Example: Factorial (2/4)

- Instance-proof for $n = 2$:

$$\begin{aligned} g(1,2) &= g(1 \cdot 2, 1) = g((1 \cdot 2) \cdot 1, 0) = (1 \cdot 2) \cdot 1 \\ &= ((1 \cdot 2) \cdot 1) \cdot 1 = ((1 \cdot 2) \cdot 1) \cdot f(0) \\ &= (1 \cdot 2) \cdot (1 \cdot f(0)) = (1 \cdot 2) \cdot f(1) \\ &= 1 \cdot (2 \cdot f(1)) = 1 \cdot f(2) = f(2) \end{aligned}$$

- Uses the axiom-instances:
  $gST(1,1), gST(1 \cdot 2, 0), g0((1 \cdot 2) \cdot 1)$
  $fST(1), fST(0), f0$
  $ASSO(1 \cdot 2, 1, f(0)), ASSO(1, 2, f(1))$
  $\ldots$
- Analogous for other n

Example: Factorial (3/4)

- Schematic grammar

$$\begin{aligned}
\tau &\to \mathsf{r}_{f0} \mid \mathsf{r}_{1L}(f(\alpha)) \mid \mathsf{r}_{g0}(\beta) \mid \mathsf{r}_{1R}(\beta) \\
&\quad\ \mathsf{r}_{fST}(\nu) \mid \mathsf{r}_{gST}(\gamma, \nu) \mid \mathsf{r}_{ASSO}(\gamma, s\nu, f(\nu)) \\
\gamma &\to \gamma \cdot s\nu \\
\gamma_{end} &\to 1
\end{aligned}$$

obtained from instance proofs for $M = \{2, 3\}$.

Example: Factorial (4/4)

- Unification problem:

$$f(0) = 1, 1 \cdot f(\alpha) = f(\alpha), g(\beta, 0) = \beta, \beta \cdot 1 = \beta \vdash X[\alpha, 0, \beta]$$

$$f(0) = 1, 1 \cdot f(\alpha) = f(\alpha), f(s\nu) = s\nu \cdot f(\nu), g(\gamma, s\nu) = g(\gamma \cdot s\nu, \nu),$$
$$(\gamma \cdot s\nu) \cdot f(\nu) = \gamma \cdot (s\nu \cdot f(\nu)), X[\alpha, \nu, \gamma \cdot s\nu] \vdash X[\alpha, s\nu, \gamma]$$

$$f(0) = 1, 1 \cdot f(\alpha) = f(\alpha), X[\alpha, \alpha, 1] \vdash g(1, \alpha) = f(\alpha)$$

- Heuristic
  - Start from C_0 :
    $f(0) = 1 \wedge 1 \cdot f(\alpha) = f(\alpha) \wedge g(\beta, 0) = \beta \wedge \beta \cdot 1 = \beta$
  - Forgetful paramodulation, generalization $0 \mapsto \alpha$,
    forgetful resolution (N/A here)
  - Search space of $\sim$ 20 quasi-tautology checks

  $\Rightarrow$ yields $g(\gamma, \alpha) = \gamma \cdot f(\alpha)$

Summary

Gist of this approach:

- Reduction of problem with quantifiers to one without
  - Compute schematic grammar based on ground terms only
  - Schematic grammar fixes many aspects of induction proof

State of theory:

- Cut-elimination: Π_2-cuts
- Cut-introduction: Π_1-cuts
- Induction: a single Π_1-induction

State of implementation (`http://www.logic.at/gapt/`):

- Introduction of one Π_1-cut: done
  (empirical evaluation in IJCAR '14)
- Introduction of Π_1-cuts: almost done
- Induction: starting now