A Natural Proof System for Herbrand's Theorem

Logical Foundations for Computer Science, 2018

Benjamin Ralph

University of Bath

January 8, 2018

Herbrand's Theorem (1930)

5. Théorème fondamental.

5. Théorème. 1^0. *Une proposition de propriété B, d'ordre p est vraie; et la connaissance de p permet de fabriquer sa démonstration.*

"*Herbrand's proof is hard to follow*" (Bernays)

What is Herbrand's theorem about? Why is it of interest?

- A "reduction" of first-order logic to propositional logic.
- A "reduction" of undecidable first-order logic to decidable propositional logic.
- Proof theory: we can obtain a separation of a first-order proof into first-order and propositional parts, joined by a Herbrand disjunction.

An example

There exist two irrational numbers a and b such that a^b is rational.

FO: $\exists a, b \in \mathbb{R}(\overline{\mathbb{Q}}(a) \wedge \overline{\mathbb{Q}}(b) \wedge \mathbb{Q}(a^b))$

$\swarrow \qquad \searrow$

$\exists a, b(\overline{\mathbb{Q}}(a) \wedge \overline{\mathbb{Q}}(b) \wedge \mathbb{Q}(a^b)) \quad \vee \quad \exists a, b(\overline{\mathbb{Q}}(a) \wedge \overline{\mathbb{Q}}(b) \wedge \mathbb{Q}(a^b))$

$\downarrow \qquad \downarrow$

Prop: $\overline{\mathbb{Q}}(\sqrt{2}) \wedge \overline{\mathbb{Q}}(\sqrt{2}) \wedge \mathbb{Q}(\sqrt{2}^{\sqrt{2}}) \quad \vee \quad \overline{\mathbb{Q}}(\sqrt{2}^{\sqrt{2}}) \wedge \overline{\mathbb{Q}}(\sqrt{2}) \wedge \mathbb{Q}(2)$

$\downarrow \qquad \downarrow$

Taut: $\mathbb{Q}(\sqrt{2}^{\sqrt{2}}) \quad \vee \quad \overline{\mathbb{Q}}(\sqrt{2}^{\sqrt{2}})$

Herbrand Proof (Buss 1991)

Theorem (Herbrand's theorem)

A first-order formula A is valid if and only if A has a Herbrand proof. A Herbrand proof of A consists of a prenexification $A^\star$ of a strong $\vee$-expansion of A plus a witnessing substitution σ for $A^\star$.

A *Herbrand Proof* consists of:

1. Expansion of existential subformulae.
2. Prenexification
3. Term assignment.
4. Propositional tautology check.

Another Example

Sleeper's Formula: There is someone in this room such that, if they are asleep, then everyone in the room is asleep.

$$\exists x[\bar{P}x \vee \forall y Py]$$

Another Example

Sleeper's Formula: There is someone in this room such that, if they are asleep, then everyone in the room is asleep.

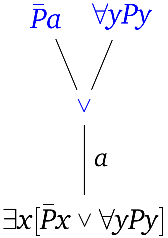
$$\bar{P}a \vee \forall y Py$$

$$\Big|\, a$$

$$\exists x[\bar{P}x \vee \forall y Py]$$

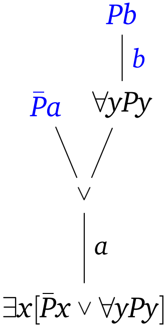
Another Example

Sleeper's Formula: There is someone in this room such that, if they are asleep, then everyone in the room is asleep.



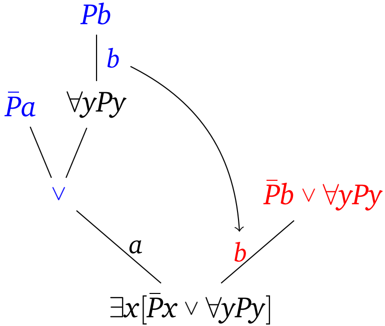
Another Example

Sleeper's Formula: There is someone in this room such that, if they are asleep, then everyone in the room is asleep.



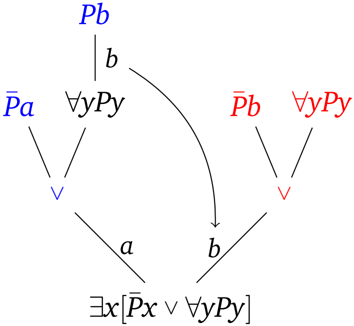
Another Example

Sleeper's Formula: There is someone in this room such that, if they are asleep, then everyone in the room is asleep.



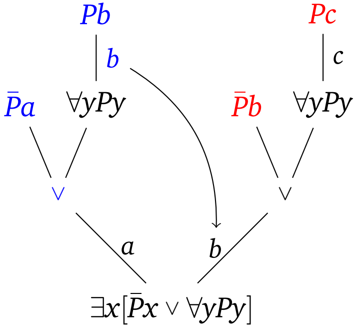
Another Example

Sleeper's Formula: There is someone in this room such that, if they are asleep, then everyone in the room is asleep.



Another Example

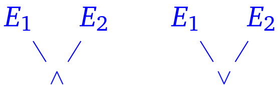
Sleeper's Formula: There is someone in this room such that, if they are asleep, then everyone in the room is asleep.



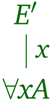
Expansion Proofs (Miller 1987)

Expansion trees are recursive structures produced from literal leaves and the following nodes:

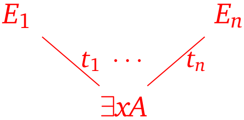
- $\wedge$ and $\vee$ nodes:



- $\forall$ nodes:

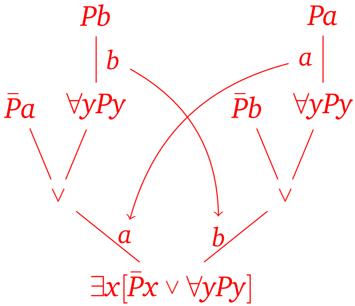


- $\exists$ nodes:



An expansion tree is correct if the Deep formula is a tautology and the dependency relation on the edges is acyclic.

Incorrect Expansion Tree



Proof Systems

What would a proof system designed around Herbrand's Theorem look like?

1. Herbrand Proofs are proofs in the formalism.

$$\begin{array}{c} \Big\Vert \, \mathit{Prop} \\ H(A) \\ \Big\Vert \, \mathit{FO} \\ A \end{array}$$

2. Construction of proofs in the formalism reflects construction of expansion proofs.

$$E_1 \approx \begin{array}{c} \phi_1 \Vert \\ A_1 \end{array} \ \& \ E_2 \approx \begin{array}{c} \phi_2 \Vert \\ A_2 \end{array} \implies \begin{array}{ccc} E_1 & & E_2 \\ e_1 \backslash & & / e_2 \\ & \star & \end{array} \approx \begin{array}{c} \phi_1 \Vert \\ A_1 \end{array} \star \begin{array}{c} \phi_2 \Vert \\ A_2 \end{array}$$

Problems

Both of these are not natural features of sequent calculus proof systems.

1. Herbrand proofs are proofs in the formalism.

Problem: In (Brünnler (2003) it is shown that the following property is impossible to obtain in a sequent calculus system with multiplicative rules.

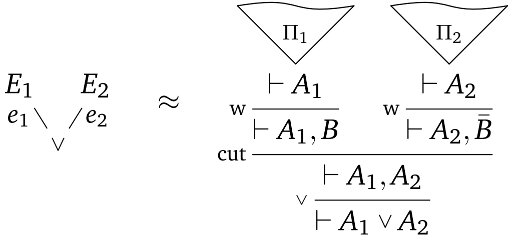
“Proofs can be separated into two phases (seen bottom-up): The lower phase only contains instances of contraction. The upper phase contains instances of the other rules, but no contraction. No formulae are duplicated in the upper phase.”

Problems

Both of these are not natural features of sequent calculus proof systems.

2. Construction of proofs in the formalism reflects construction of expansion proofs.

Problem: The obvious way to compose two sequent calculus proofs by disjunction introduces a cut.



Open Deduction

$$\begin{array}{c} A \\ \Phi \, \Vert \\ B \end{array} \qquad\qquad \begin{array}{c} C \\ \Psi \, \Vert \\ D \end{array}$$

Open Deduction

1. Inference Rule $\sigma \in \mathcal{S}$:

$$\sigma \frac{\begin{array}{c} A \\ \Phi \| \\ B \end{array}}{\begin{array}{c} C \\ \Psi \| \\ D \end{array}}$$

2. Binary Connective $\star \in \{\wedge, \vee\}$:

$$\begin{array}{c} A \\ \Phi \| \\ B \end{array} \star \begin{array}{c} C \\ \Psi \| \\ D \end{array} = \begin{array}{c} A \star C \\ \Phi \star \Psi \| \\ B \star D \end{array}$$

3. Quantifier $Qx, Q \in \{\forall, \exists\}$:

$$Qx \left[\begin{array}{c} A \\ \phi \| \\ B \end{array} \right] = \begin{array}{c} QxA \\ Qx\phi \| \\ QxB \end{array}$$

Example

$$
\mathsf{qi}\uparrow \dfrac{\mathsf{t}}{\mathsf{n}\downarrow \dfrac{\forall x \left[\mathsf{w}\downarrow \dfrac{Px}{\bar{P}a \vee Px} \right]}{\exists x \forall x \left[\bar{P}x \vee Py \right]} \vee \exists x \left[\mathsf{r1}\downarrow \dfrac{\mathsf{w}\downarrow \dfrac{\bar{P}x}{\bar{P}x \vee \forall y Py}}{\forall y \left[\bar{P}x \vee Py \right]} \right]}
$$

$$
\mathsf{qc}\downarrow \dfrac{\cdots}{\exists x \forall y \left[\bar{P}x \vee Py \right]}
$$

Herbrand Proof

1. Expansion of existential subformulae.
2. Prenexification
3. Term assignment.
4. Propositional tautology check.

Inference Rules

1. For expansion of existential subformulae we have the existential contraction rule:

$$\mathsf{qc}{\downarrow}\,\frac{\exists x A \vee \exists x A}{\exists x A}$$

2. For prenexification we have four rules:

$$\mathsf{r1}{\downarrow}\,\frac{\forall x[A \vee B]}{\forall x A \vee B} \quad \mathsf{r2}{\downarrow}\,\frac{\forall x(A \wedge B)}{(\forall x A \wedge B)} \quad \mathsf{r3}{\downarrow}\,\frac{\exists x[A \vee B]}{\exists x A \vee B} \quad \mathsf{r4}{\downarrow}\,\frac{\exists x(A \wedge B)}{\exists x A \wedge B}$$

(where B is free for x)

3. For term assignment we have the rule:

$$\mathsf{n}{\downarrow}\,\frac{A[t/x]}{\exists x A}$$

KS

For propositional tautology check we have the propositional open deduction proof system KS.

Structural rules

$$\mathsf{ai}{\downarrow}\,\frac{\mathsf{t}}{a \vee \bar{a}} \qquad \mathsf{ac}{\downarrow}\,\frac{a \vee a}{a} \qquad \mathsf{aw}{\downarrow}\,\frac{\mathsf{f}}{a}$$

identity *contraction* *weakening*

Logical rules

$$\mathsf{s}\,\frac{A \wedge [B \vee C]}{(A \wedge B) \vee C} \qquad \mathsf{m}\,\frac{(A \wedge B) \vee (C \wedge D)}{[A \vee C] \wedge [B \vee D]}$$

switch *medial*

KSh1

$$\mathsf{KSh1} = \boxed{\mathsf{KS}:\quad \mathsf{ai}\!\downarrow \frac{\mathsf{t}}{a \vee \bar{a}} \qquad \mathsf{ac}\!\downarrow \frac{a \vee a}{a} \qquad \mathsf{aw}\!\downarrow \frac{\mathsf{f}}{a} \qquad \mathsf{s}\,\frac{A \wedge [B \vee C]}{(A \wedge B) \vee C} \qquad \mathsf{m}\,\frac{(A \wedge B) \vee (C \wedge D)}{[A \vee C] \wedge [B \vee D]}}$$

$$+$$

$$\boxed{\mathsf{r1}\!\downarrow \frac{\forall x [A \vee B]}{[\forall x A \vee B]} \qquad \mathsf{r2}\!\downarrow \frac{\forall x (A \wedge B)}{(\forall x A \wedge B)} \qquad \mathsf{n}\!\downarrow \frac{A[t/x]}{\exists x A} \qquad \mathsf{r3}\!\downarrow \frac{\exists x [A \vee B]}{[\exists x A \vee B]} \qquad \mathsf{r4}\!\downarrow \frac{\exists x (A \wedge B)}{(\exists x A \wedge B)} \qquad \mathsf{qc}\!\downarrow \frac{\exists x A \vee \exists x A}{\exists x A}}$$

Herbrand Proof in KSh1

A KSh1 proof is a *Herbrand proof* if it is in the following form:

$$\begin{array}{c} \Vert \mathsf{KS} \\ \forall \vec{x} B[\vec{t}/\vec{y}] \\ \Vert \{\mathsf{n}\!\downarrow\} \\ Q\{B\} \\ \Vert \{\mathsf{r1}\!\downarrow, \mathsf{r2}\!\downarrow, \mathsf{r3}\!\downarrow, \mathsf{r4}\!\downarrow\} \\ A' \\ \Vert \{\mathsf{qc}\!\downarrow\} \\ A \end{array}$$

Theorem (Brünnler, 2006)

Every proof in KSh1 *can be converted to a Herbrand proof*.

Proof.

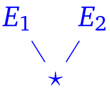
Via cut elimination. □

Herbrand Proof Example

$$
\mathsf{r3}\!\downarrow\dfrac{
\mathsf{n}\!\downarrow\dfrac{
=\dfrac{\mathsf{t}}{\forall y_1 \forall y_2 \left[=\dfrac{\mathsf{ai}\!\downarrow\dfrac{\mathsf{t}}{Py_1 \vee \bar{P}y_1} \vee \left[\mathsf{aw}\!\downarrow\dfrac{\mathsf{f}}{\bar{P}c} \vee \mathsf{aw}\!\downarrow\dfrac{\mathsf{f}}{Py_2}\right]}{[\bar{P}c \vee Py_1] \vee [\bar{P}y_1 \vee Py_2]} \right]}
}{
\exists x_1 \left[\mathsf{r1}\!\downarrow\dfrac{\forall y_1 \left[\mathsf{r3}\!\downarrow\dfrac{\mathsf{n}\!\downarrow\dfrac{[\bar{P}x_1 \vee Py_1] \vee [\bar{P}y_1 \vee Py_2]}{\exists x_2 \left[\mathsf{r1}\!\downarrow\dfrac{\forall y_2 \left[[\bar{P}x_1 \vee Py_1] \vee [\bar{P}x_2 \vee Py_2] \right]}{[\bar{P}x_1 \vee Py_1] \vee \forall y_2 [\bar{P}x_2 \vee Py_2]} \right]}}{[\bar{P}x_1 \vee Py_1] \vee \exists x_2 \forall y_2 [\bar{P}x_2 \vee Py_2]} \right]}{\forall y_1 [\bar{P}x_1 \vee Py_1] \vee \exists x_2 \forall y_2 [\bar{P}x_2 \vee Py_2]} \right]
}
}{
\mathsf{qc}\!\downarrow\dfrac{\exists x_1 \forall y_1 [\bar{P}x_1 \vee Py_1] \vee \exists x_2 \forall y_2 [\bar{P}x_2 \vee Py_2]}{\exists x \forall y [\bar{P}x \vee Py]}
}
$$

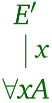
More Inference Rules

- ⋆ nodes are simulated by horizontal composition of derivations:



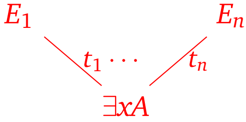
$$\approx \quad \begin{array}{c} A \\ \Phi \Vert \\ B \end{array} \star \begin{array}{c} C \\ \Vert \Psi \\ D \end{array}$$

- ∀ nodes are simulated by the rules r1↓ and r2↓:



$$\approx \quad \mathsf{r1}{\downarrow}\,\frac{\forall x[A \vee B]}{\forall x A \vee B} \qquad \mathsf{r2}{\downarrow}\,\frac{\forall x(A \wedge B)}{\forall x A \wedge B}$$

- ∃ nodes are simulated by h↓, the *Herbrand expander*:



$$\approx \quad \mathsf{h}{\downarrow}\,\frac{\exists x A \vee A[t/x]}{\exists x A}$$

KSh2

$$\mathsf{KSh2} = \underbrace{\mathsf{ai}\!\downarrow \frac{\mathsf{t}}{a \vee \bar{a}} \quad \mathsf{ac}\!\downarrow \frac{a \vee a}{a} \quad \mathsf{aw}\!\downarrow \frac{\mathsf{f}}{a} \quad \mathsf{s} \frac{A \wedge [B \vee C]}{(A \wedge B) \vee C} \quad \mathsf{m} \frac{(A \wedge B) \vee (C \wedge D)}{[A \vee C] \wedge [B \vee D]}}_{\mathsf{KS}}$$

$$+$$

$$\mathsf{r1}\!\downarrow \frac{\forall x[A \vee B]}{[\forall x A \vee B]} \quad \mathsf{r2}\!\downarrow \frac{\forall x(A \wedge B)}{(\forall x A \wedge B)} \quad \mathsf{h}\!\downarrow \frac{\exists x A \vee A[t/x]}{\exists x A} \quad \exists\mathsf{w}\!\downarrow \frac{\mathsf{f}}{\exists x A}$$

Herbrand Normal Form

A KSh2 proof of the form below is said to be in *Herbrand Normal Form*:

$$\begin{array}{c} \| \; \mathsf{KS} \\ \forall \vec{x} H_\phi(A) \\ \| \; \{\exists\mathsf{w}\!\downarrow\} \\ \forall \vec{x} H^+_\phi(A) \\ \| \; \{\mathsf{r1}\!\downarrow, \mathsf{r2}\!\downarrow, \mathsf{h}\!\downarrow\} \\ A \end{array}$$

HNF Proof Example

$$
\mathsf{r1}{\downarrow}\,\dfrac{
=\,\dfrac{
=\,\dfrac{\mathsf{t}}{\forall y_1 \forall y_2 \left[\mathsf{ai}{\downarrow}\,\dfrac{\mathsf{t}}{Py_1 \vee \bar{P}y_1} \vee \left[\mathsf{aw}{\downarrow}\,\dfrac{\mathsf{f}}{\bar{P}c} \vee \mathsf{aw}{\downarrow}\,\dfrac{\mathsf{f}}{Py_2} \right] \right]}
}{
\forall y_1 \left[\mathsf{r1}{\downarrow}\,\dfrac{\forall y_2 \left[\left[\exists\mathsf{w}{\downarrow}\,\dfrac{\mathsf{f}}{\exists x \forall y \left[\bar{P}x \vee Py \right]} \vee \left[\bar{P}y_1 \vee Py_2 \right] \right] \vee \left[\bar{P}c \vee Py_1 \right] \right]}{\mathsf{r1}{\downarrow}\,\dfrac{\forall y_2 \left[\exists x \forall y \left[\bar{P}x \vee Py \right] \vee \left[\bar{P}y_1 \vee Py_2 \right] \right]}{\mathsf{h}{\downarrow}\,\dfrac{\exists x \forall y \left[\bar{P}x \vee Py \right] \vee \forall y_2 \left[\bar{P}y_1 \vee Py_2 \right]}{\exists x \forall y \left[\bar{P}x \vee Py \right]}} \vee \left[\bar{P}c \vee Py_1 \right]} \right]
}
}{
\mathsf{h}{\downarrow}\,\dfrac{\exists x \forall y \left[\bar{P}x \vee Py \right] \vee \forall y_1 \left[\bar{P}c \vee Py_1 \right]}{\exists x \forall y \left[\bar{P}x \vee Py \right]}
}
$$

Theorems

Theorem

A formula has a proof in HNF iff it has a Herbrand proof.

Theorem

If ϕ is a proof in HNF, then we can construct an expansion proof E_ϕ of A.

Theorem

If E is an expansion proof of A, then we can construct a proof ϕ_E of A in HNF.

$$\begin{array}{c} {}^{HP}\Pi \\ A \end{array} \longleftrightarrow \begin{array}{c} {}^{HNF}\Pi \\ A \end{array} \longleftrightarrow \begin{array}{c} {}^{EP}\Pi \\ A \end{array}$$

Further Work

- Extending KSh2 with cut, and proving cut elimination.
- Comparing with the cut elimination procedures for expansion proofs in Heijltjes (2010), Alcolei et al. (2017).
- Situating this work in the context of recent work by Aler Tubella and Guglielmi on a general theory of normalisation for open deduction.