On Herbrand's Theorem

David M. Cerna & Anela Lolic

July 26$^{\text{th}}$, 2019

Outline

- Herbrand's theorem describes the relationship between First-Order Logic (FOL) and Propositional Logic (PL).
- While quantifiers may range over infinite domains, Herbrand's theorem shows that the validity of FOL statements is dependent on a finite set of substitutions.
- If one instead considers arithmetic theories which include induction this elegant relationship is lost.
- However, under certain conditions the infinite set of substitutions may be described finitistically, thus generalizing Herbrand's theorem, and once again bridging the finite and infinite.

Background: Gentzen's Sequent Calculus

- The sequent calculus applies inferences to objects referred to as sequents $\Delta \vdash \Pi$, where Δ and Π are multisets of well-formed formula. Chaining inferences forms proof trees.
- Semantically a sequent means *given* Δ *we may derive* Π.
- Note that, this interpretation implies that Δ is essentially a conjunction of formula and Π is a disjunction.
- The sequent calculus Inferences are as follows:

  Axiom Inferences

$$\frac{}{A \vdash A}\,\mathrm{Ax}$$

Gentzen's Sequent Calculus

Structural Inferences

$$\frac{\Gamma \vdash \Delta}{D, \Gamma \vdash \Delta}\ \text{w:l} \qquad \frac{\Gamma \vdash \Delta}{\Gamma \vdash \Delta, D}\ \text{w:r}$$

$$\frac{D, D, \Gamma \vdash \Delta}{D, \Gamma \vdash \Delta}\ \text{c:l} \qquad \frac{\Gamma \vdash \Delta, D, D}{\Gamma \vdash \Delta, D}\ \text{c:r}$$

$$\frac{\Gamma \vdash \Delta, C \qquad C, \Gamma' \vdash \Delta'}{\Gamma, \Gamma' \vdash \Delta, \Delta'}\ \text{cut}$$

Gentzen's Sequent Calculus

Logical Inferences

$$\frac{\Gamma \vdash \Delta, D}{\neg D, \Gamma \vdash \Delta}\ \neg{:}\mathrm{l} \qquad \frac{D, \Gamma \vdash \Delta}{\Gamma \vdash \Delta, \neg D}\ \neg{:}\mathrm{r} \qquad \frac{C, \Gamma \vdash \Delta}{C \wedge D, \Gamma \vdash \Delta}\ \wedge{:}\mathrm{l}$$

$$\frac{D, \Gamma \vdash \Delta}{C \wedge D, \Gamma \vdash \Delta}\ \wedge{:}\mathrm{l} \qquad \frac{\Gamma \vdash \Delta, C}{\Gamma \vdash \Delta, C \vee D}\ \vee{:}\mathrm{r} \qquad \frac{\Gamma \vdash \Delta, D}{\Gamma \vdash \Delta, C \vee D}\ \vee{:}\mathrm{r}$$

$$\frac{\Gamma \vdash \Delta, C \qquad \Gamma \vdash \Delta, D}{\Gamma \vdash \Delta, C \wedge D}\ \wedge{:}\mathrm{r} \qquad \frac{C, \Gamma \vdash \Delta \qquad D, \Gamma \vdash \Delta}{C \vee D, \Gamma \vdash \Delta}\ \vee{:}\mathrm{l}$$

$$\frac{C, \Gamma \vdash \Delta, D}{\Gamma \vdash \Delta, C \to D}\ {\to}{:}\mathrm{r} \qquad \frac{\Gamma \vdash \Delta, C \qquad D, \Gamma \vdash \Delta}{C \to D, \Gamma \vdash \Delta}\ {\to}{:}\mathrm{l}$$

Gentzen's Sequent Calculus

Quantifier Inferences

$$\frac{\Gamma \vdash \Delta, F(\alpha)}{\Gamma \vdash \Delta, \forall x F(x)}\ \forall\text{:r} \qquad \frac{F(t), \Gamma \vdash \Delta}{\forall x F(x), \Gamma \vdash \Delta}\ \forall\text{:l}$$

$$\frac{\Gamma \vdash \Delta, F(t)}{\Gamma \vdash \Delta, \exists x F(x)}\ \exists\text{:r} \qquad \frac{F(\alpha), \Gamma \vdash \Delta}{\exists x F(x), \Gamma \vdash \Delta}\ \exists\text{:l}$$

- Note that for $\exists : l$ and $\forall : r$ α may not occur in Γ or Δ. These rules are referred to as strong quantification, i.e. require an eigenvariable, the other rules are referred to as weak.

Gentzen's Sequent Calculus

Quantifier Inferences

$$\frac{\Gamma \vdash \Delta, F(\alpha)}{\Gamma \vdash \Delta, \forall x F(x)} \forall\text{:r} \qquad \frac{F(t), \Gamma \vdash \Delta}{\forall x F(x), \Gamma \vdash \Delta} \forall\text{:l}$$

$$\frac{\Gamma \vdash \Delta, F(t)}{\Gamma \vdash \Delta, \exists x F(x)} \exists\text{:r} \qquad \frac{F(\alpha), \Gamma \vdash \Delta}{\exists x F(x), \Gamma \vdash \Delta} \exists\text{:l}$$

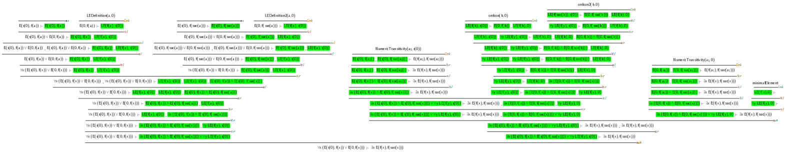
- Note that for $\exists : l$ and $\forall : r$ α may not occur in Γ or Δ. These rules are referred to as strong quantification, i.e. require an eigenvariable, the other rules are referred to as weak.

Equational Axioms

$$\frac{}{\vdash x = x} \text{Re} \qquad \frac{}{x_1 = y_1, \cdots, x_n = y_n, P(x_1, \cdots, x_n) \vdash P(y_1, \cdots, y_n)} P_=$$

$$\frac{}{x_1 = y_1, \cdots, x_n = y_n \vdash f(x_1, \cdots, x_n) = f(y_1, \cdots, y_n)} f_=$$

Example Sequent Proof with Cut

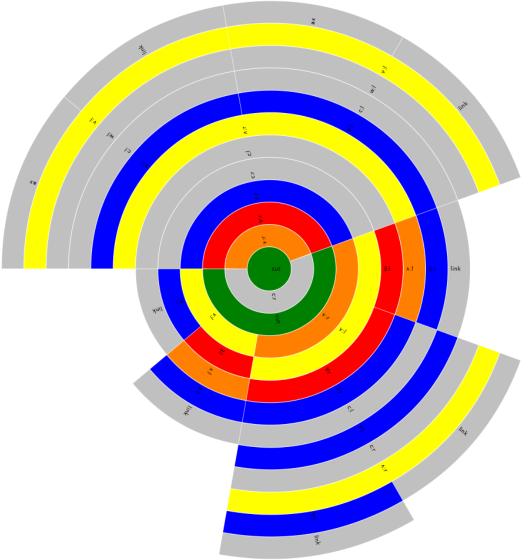


- Green sequents represent cuts.

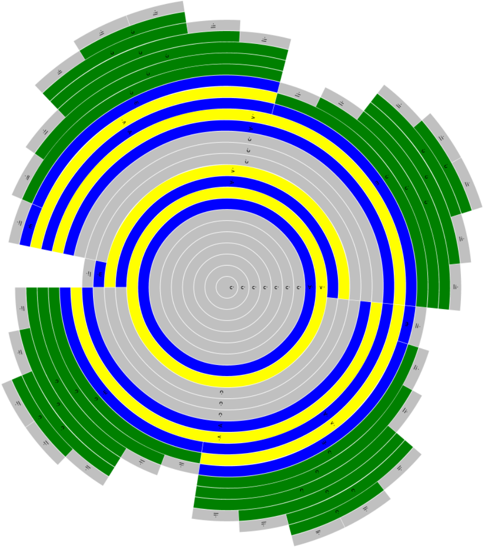
Example Sequent Proof without Cut

- Cannot eliminate atomic equational cuts.

Example Sequent Proof with Cut Sun Burst



Example Sequent Proof without Cut Sun Burst



Induction and the LK-calculus

- The theory of Peano arithmetic may by formalized as a theory extension of the LK-calculus with equality.
- Other than the axioms for successor, addition, and multiplication, one needs to add the following inference:

$$\frac{\Pi \vdash \Delta, \varphi(0) \qquad \Pi, \varphi(\alpha) \vdash \Delta, \varphi(s(\alpha))}{\Pi \vdash \Delta, \varphi(\beta)}\ \text{IND}$$

- Alternatively one could consider adding the ω-rule which requires a proof of each instance of the main formula:

$$\frac{\Pi \vdash \Delta, \varphi(n) \qquad \forall n \in \mathbb{N}}{\Pi \vdash \Delta, \varphi(\beta)}\ \omega$$

- Without restrictions, the ω-rule is seemingly useless for practical cases.

Finitely describable sequences

- Fortunately, the primitive recursive ω-rule [J. Shoenfield 1959] is expressive enough to prove totality of all functions provably total in Peano arithmetic.
- Great a useful ω-rule, but how does one develop a finite description of a proof sequence?
- Maybe a little more specific, what can we do with $\varphi(0), \cdots, \varphi(n)$ for $n < \infty$?
- This is the topic of "Inductive theorem proving based on tree grammars" by S. Eberhard and S. Hetzl (2015).

Cut-freeness and the Herbrand Instances

- Not just any $\varphi(0), \cdots, \varphi(n)$ will do, we need the proofs to have particular properties.

Cut-freeness and the Herbrand Instances

- Not just any $\varphi(0), \cdots, \varphi(n)$ will do, we need the proofs to have particular properties.
- They should be proofs of the same statement.

Cut-freeness and the Herbrand Instances

- Not just any $\varphi(0), \cdots, \varphi(n)$ will do, we need the proofs to have particular properties.
- They should be proofs of the same statement.
- They should also be cut-free.
- Cut-free proofs, other than being massive and being produced by theorem provers have particular properties.

Cut-freeness and the Herbrand Instances

- Not just any $\varphi(0), \cdots, \varphi(n)$ will do, we need the proofs to have particular properties.
- They should be proofs of the same statement.
- They should also be cut-free.
- Cut-free proofs, other than being massive and being produced by theorem provers have particular properties.

Theorem (Mid-Sequent Theorem)

Let S be a sequent of prenex formulas then there exists a cut-free proof π of S s.t. π contains a sequent S' s.t.

- *S' is quantifier free.*
- *Every inference above S' is structural or propositional.*
- *Every inference below S' is structural or a quantifier inference.*

Cut-freeness and the Herbrand Instances

- Not just any $\varphi(0), \cdots, \varphi(n)$ will do, we need the proofs to have particular properties.
- They should be proofs of the same statement.
- They should also be cut-free.
- Cut-free proofs, other than being massive and being produced by theorem provers have particular properties.

Theorem (Mid-Sequent Theorem)

Let S be a sequent of prenex formulas then there exists a cut-free proof π of S s.t. π contains a sequent S' s.t.

- *S' is quantifier free.*
- *Every inference above S' is structural or propositional.*
- *Every inference below S' is structural or a quantifier inference.*

- What if we limit S to a sequent only containing weak quantification.

Cut-freeness and the Herbrand Instances

- No strong quantification means no eigenvariables and thus all terms are existential witnesses.
- Collecting those witnesses gives us Herbrand's Theorem

Cut-freeness and the Herbrand Instances

- No strong quantification means no eigenvariables and thus all terms are existential witnesses.
- Collecting those witnesses gives us Herbrand's Theorem

Theorem (Herbrand's Theorem)

Let S be a sequent of the form $\forall\bar{x}\varphi(\bar{x}) \vdash \exists\bar{x}\psi(\bar{x})$. S is valid if and only if there exists a sequence of term vectors $\bar{t}_1, \cdots, \bar{t}_n$ s.t.

$$\bigwedge_{i=0}^{k} \varphi(\bar{t}_i) \vdash \bigvee_{i=0}^{k} \psi(\bar{t}_i)$$

is valid.

Cut-freeness and the Herbrand Instances

- No strong quantification means no eigenvariables and thus all terms are existential witnesses.
- Collecting those witnesses gives us Herbrand's Theorem

Theorem (Herbrand's Theorem)

Let S be a sequent of the form $\forall \bar{x}\varphi(\bar{x}) \vdash \exists \bar{x}\psi(\bar{x})$. S is valid if and only if there exists a sequence of term vectors $\bar{t}_1, \cdots, \bar{t}_n$ s.t.

$$\bigwedge_{i=0}^{k} \varphi(\bar{t}_i) \vdash \bigvee_{i=0}^{k} \psi(\bar{t}_i)$$

is valid.

- Cut-free (weakly quantified end sequent) $\Longrightarrow$ *weak* mid-sequent $\Longrightarrow$ Herbrand instances.

Using First-Order Instance Proofs

- Let $\varphi(\beta)$ be quantifier-free, Δ only contains weakly quantified formula, and $\Delta \vdash \varphi(\beta)$ the main sequent of a sound application of the ω-rule.
- Furthermore, each of the instance proofs $\varphi(n)$ for $n \in \mathbb{N}$ is provable without induction.
- We can ask a first-order theorem prover for a proof π_n of $\varphi(n)$.
- Each π_n is cut-free (atomic cuts don't count) and thus the Herbrand instances H_n may be extracted.

Non-Injectivity Assertion

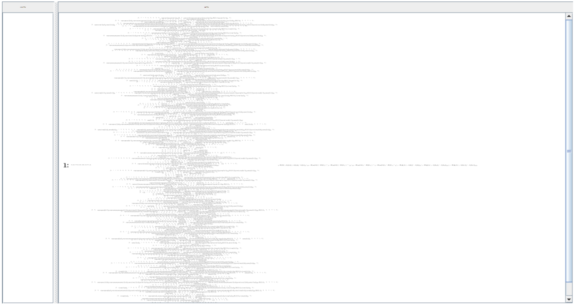
- The formula F(n) is defined as follows:

$$\forall x \left(\bigvee_{i=0}^{n} f(x) = i \right) \wedge \left(\bigwedge_{i}^{n} \forall x \forall y \neg \left(s(x) \leq y \wedge f(x) = i \wedge f(y) = i \right) \right)$$

$$\wedge \forall x \forall y \forall z \left(max(x,y) \leq z \rightarrow (x \leq z \wedge y \leq z) \right) \wedge \forall x (x \leq x)$$

- Note that $\vdash \forall n \neg F(n)$ is provable in arithmetic.
- but there are many ways to prove $F(\alpha) \vdash$ for $\alpha \in \mathbb{N}$

SPASS Herbrand Instances $F(2)$



- These Herbrand instances where found using SPASS.
- Below are the Herbrand instances found by cut-elimination for $F(1)$.

Cut-elimination Herbrand Instances $F(1)$

$$
\exists p\, \exists q \quad
\begin{matrix}
\langle\, \mathrm{max}(z,z)\ ,\ \mathrm{max}(g(\mathrm{max}(z,g(\mathrm{max}(z,z)))),g(\mathrm{max}(z,z)))\,\rangle \\
\langle\, \mathrm{max}(z,g(\mathrm{max}(g(\mathrm{max}(z,z)),z)))\ ,\ \mathrm{max}(g(\mathrm{max}(z,g(\mathrm{max}(g(\mathrm{max}(z,z)),z)))),g(\mathrm{max}(g(\mathrm{max}(z,z)),z)))\,\rangle \\
\langle\, \mathrm{max}(z,z)\ ,\ \mathrm{max}(z,g(\mathrm{max}(z,z)))\,\rangle \\
\langle\, \mathrm{max}(z,z)\ ,\ \mathrm{max}(g(\mathrm{max}(z,z)),z)\,\rangle \\
\langle\, \mathrm{max}(z,g(\mathrm{max}(z,z)))\ ,\ \mathrm{max}(g(\mathrm{max}(z,g(\mathrm{max}(z,z)))),g(\mathrm{max}(z,z)))\,\rangle \\
\langle\, \mathrm{max}(g(\mathrm{max}(z,z)),z)\ ,\ \mathrm{max}(z,g(\mathrm{max}(g(\mathrm{max}(z,z)),z)))\,\rangle \\
\langle\, \mathrm{max}(g(\mathrm{max}(z,z)),z)\ ,\ \mathrm{max}(g(\mathrm{max}(z,g(\mathrm{max}(g(\mathrm{max}(z,z)),z)))),g(\mathrm{max}(g(\mathrm{max}(z,z)),z)))\,\rangle
\end{matrix}
\quad (\ \mathrm{LE}(p, c
$$

- If you look closely (and know the problem) you will see that it is just counting natural numbers.

SPASS Herbrand Instances $F(1)$

$$\textbf{1:}\ \forall A_0 \forall B \forall C \begin{array}{c} \langle\ g^2(U)\ ,\ g(U)\ ,\ \max(g^2(U), g(U))\ \rangle \\ \langle\ g(U)\ ,\ g^2(U)\ ,\ \max(g(U), g^2(U))\ \rangle \\ \langle\ g(U)\ ,\ g(U)\ ,\ \max(g(U), g(U))\ \rangle \end{array} (\ \neg\ LEQ(\max(A_0, B), C)\ \vee\ LEQ(B, C)\ )$$

$$\textbf{2:}\ \forall A_0 \forall B \forall C \begin{array}{c} \langle\ g^2(U)\ ,\ g(U)\ ,\ \max(g^2(U), g(U))\ \rangle \\ \langle\ g(U)\ ,\ g^2(U)\ ,\ \max(g(U), g^2(U))\ \rangle \\ \langle\ g(U)\ ,\ g(U)\ ,\ \max(g(U), g(U))\ \rangle \end{array} (\ \neg\ LEQ(\max(A_0, B), C)\ \vee\ LEQ(A_0, C)\ )$$

$$\textbf{3:}\ \forall A \begin{array}{c} \langle\ g(U)\ \rangle \\ \langle\ \max(g(U), g(U))\ \rangle \\ \langle\ U\ \rangle \\ \langle\ \max(g^2(U), g(U))\ \rangle \\ \langle\ \max(g(U), g^2(U))\ \rangle \end{array} (\ E(f(A), s(0))\ \vee\ E(f(A), 0)\ )$$

$$\textbf{4:}\ \forall A \begin{array}{c} \langle\ g(U)\ \rangle \\ \langle\ \max(g(U), g(U))\ \rangle \\ \langle\ \max(g(U), g^2(U))\ \rangle \\ \langle\ \max(g^2(U), g(U))\ \rangle \end{array} LEQ(A, A)$$

$$\textbf{5:}\ \forall B_1 \forall A_2 \begin{array}{c} \langle\ U\ ,\ \max(g^2(U), g(U))\ \rangle \\ \langle\ U\ ,\ g(U)\ \rangle \\ \langle\ U\ ,\ \max(g(U), g(U))\ \rangle \\ \langle\ g(U)\ ,\ \max(g(U), g^2(U))\ \rangle \end{array} (\ (\ \neg\ LEQ(g(B_1), A_2)\ \vee\ \neg\ E(f(B_1), s(0))\ )\ \vee\ \neg\ E(f(A_2), s(0))\ )$$

$$\textbf{6:}\ \forall B_0 \forall A_1 \begin{array}{c} \langle\ U\ ,\ g(U)\ \rangle \\ \langle\ U\ ,\ \max(g(U), g(U))\ \rangle \\ \langle\ g(U)\ ,\ \max(g^2(U), g(U))\ \rangle \\ \langle\ U\ ,\ \max(g(U), g^2(U))\ \rangle \end{array} (\ (\ \neg\ LEQ(g(B_0), A_1)\ \vee\ \neg\ E(f(B_0), 0)\ )\ \vee\ \neg\ E(f(A_1), 0)\ )$$

- This is $F(1)$ found by SPASS.

Thank you for your time (if it exists).