Non-Elementary Compression of First-Order Proofs in Deep Inference Using Epsilon-Terms

Cameron Allett

PhD Student at the University of Bath
Supervisor: Willem Heijltjes

The Oxford Advanced Seminar on Informatic Structures
31 May 2024

Introduction

- Aim to better understand the normalisation theory of first-order proofs, in particular Herbrand's Theorem and cut elimination

Introduction

- Aim to better understand the normalisation theory of first-order proofs, in particular Herbrand's Theorem and cut elimination
- Recent interest in developing first-order proof systems which admit non-elementarily smaller cut-free proofs than traditional Gentzen systems

Introduction

- Aim to better understand the normalisation theory of first-order proofs, in particular Herbrand's Theorem and cut elimination
- Recent interest in developing first-order proof systems which admit non-elementarily smaller cut-free proofs than traditional Gentzen systems
- In today's talk:
  - overview deep inference and speedups over traditional proof systems
  - overview Herbrand's Theorem and cut elimination
  - how the epsilon-calculus can help us to understand the non-elementary compression of cut-free proofs and yield new normalisation results

Deep Inference

- More flexible composition mechanism than traditional Gentzen systems using the *open deduction* formalism [Guglielmi, Gundersen, Parigot, 2010]

$$\begin{array}{c} A \\ \phi \Big\| \\ B \end{array} \wedge \begin{array}{c} C \\ \psi \Big\| \\ D \end{array} \equiv \begin{array}{c} A \wedge C \\ \phi\wedge\psi \Big\| \\ B \wedge D \end{array}$$

$$\begin{array}{c} A \\ \phi \Big\| \\ B \end{array} \vee \begin{array}{c} C \\ \psi \Big\| \\ D \end{array} \equiv \begin{array}{c} A \vee C \\ \phi\vee\psi \Big\| \\ B \vee D \end{array}$$

Deep Inference

- More flexible composition mechanism than traditional Gentzen systems using the *open deduction* formalism [Guglielmi, Gundersen, Parigot, 2010]

$$\begin{array}{c}A\\ \phi\Big\Vert\\ B\end{array} \wedge \psi\begin{array}{c}C\\ \Big\Vert\\ D\end{array} \equiv \begin{array}{c}A\wedge C\\ \phi\wedge\psi\Big\Vert\\ B\wedge D\end{array}$$

$$\begin{array}{c}A\\ \phi\Big\Vert\\ B\end{array} \vee \psi\begin{array}{c}C\\ \Big\Vert\\ D\end{array} \equiv \begin{array}{c}A\vee C\\ \phi\vee\psi\Big\Vert\\ B\vee D\end{array}$$

$$\begin{array}{c}A\\ \phi\Big\Vert\\ B\\ \hdashline B\\ \psi\Big\Vert\\ C\end{array} \equiv \begin{array}{c}A\\ \phi;\psi\Big\Vert\\ C\end{array}$$

Deep Inference

- More flexible composition mechanism than traditional Gentzen systems using the *open deduction* formalism [Guglielmi, Gundersen, Parigot, 2010]

$$\begin{array}{c} A \\ \phi \Vert \\ B \end{array} \wedge \begin{array}{c} C \\ \psi \Vert \\ D \end{array} \equiv \begin{array}{c} A \wedge C \\ \phi{\wedge}\psi \Vert \\ B \wedge D \end{array}$$

$$\begin{array}{c} A \\ \phi \Vert \\ B \end{array} \vee \begin{array}{c} C \\ \psi \Vert \\ D \end{array} \equiv \begin{array}{c} A \vee C \\ \phi{\vee}\psi \Vert \\ B \vee D \end{array}$$

$$\begin{array}{c} A \\ \phi \Vert \\ B \\ \hdashline B \\ \psi \Vert \\ C \end{array} \equiv \begin{array}{c} A \\ \phi;\psi \Vert \\ C \end{array}$$

$$\forall x \left(\begin{array}{c} A \\ \phi \Vert \\ B \end{array} \right) \equiv \begin{array}{c} \forall x A \\ \forall x \phi \Vert \\ \forall x B \end{array}$$

$$\exists x \left(\begin{array}{c} A \\ \phi \Vert \\ B \end{array} \right) \equiv \begin{array}{c} \exists x A \\ \exists x \phi \Vert \\ \exists x B \end{array}$$

Deep Inference

- More flexible composition mechanism than traditional Gentzen systems using the *open deduction* formalism [Guglielmi, Gundersen, Parigot, 2010]

$$\begin{array}{c} A \\ \phi \Big\| \\ B \end{array} \wedge \psi \begin{array}{c} C \\ \Big\| \\ D \end{array} \equiv \phi\wedge\psi \begin{array}{c} A \wedge C \\ \Big\| \\ B \wedge D \end{array}$$

$$\begin{array}{c} A \\ \phi \Big\| \\ B \end{array} \vee \psi \begin{array}{c} C \\ \Big\| \\ D \end{array} \equiv \phi\vee\psi \begin{array}{c} A \vee C \\ \Big\| \\ B \vee D \end{array}$$

$$\begin{array}{c} A \\ \phi \Big\| \\ B \\ \hdashline B \\ \psi \Big\| \\ C \end{array} \equiv \phi;\psi \begin{array}{c} A \\ \Big\| \\ C \end{array}$$

$$\forall x \left(\phi \begin{array}{c} A \\ \Big\| \\ B \end{array} \right) \equiv \forall x \phi \begin{array}{c} \forall x A \\ \Big\| \\ \forall x B \end{array}$$

$$\exists x \left(\phi \begin{array}{c} A \\ \Big\| \\ B \end{array} \right) \equiv \exists x \phi \begin{array}{c} \exists x A \\ \Big\| \\ \exists x B \end{array}$$

- Applying inference rules at arbitrary depth inside formulae yields improved normalisation properties

$$K \left\{ \rho \frac{A}{B} \right\}$$

Deep Inference

- Can freely permute inference rules around a derivation due to the more flexible composition mechanism

Deep Inference

- Can freely permute inference rules around a derivation due to the more flexible composition mechanism
- Can permute inference rules to stratify derivations, revealing *decomposition theorems* for many logics not observed in Gentzen systems

$$
\begin{array}{c} \Vert \{\rho_1, \rho_2, \ldots, \rho_n\} \\ A \end{array}
\quad \rightarrow \quad
\begin{array}{c} \Vert \{\rho_1, \ldots, \rho_i\} \\ A' \\ \Vert \{\rho_{i+1}, \ldots, \rho_j\} \\ A'' \\ \Vert \{\rho_{j+1}, \ldots, \rho_n\} \\ A \end{array}
$$

Deep Inference

- Can freely permute inference rules around a derivation due to the more flexible composition mechanism
- Can permute inference rules to stratify derivations, revealing *decomposition theorems* for many logics not observed in Gentzen systems

$$
\begin{array}{c} \Big\Vert \{\rho_1,\rho_2,\dots,\rho_n\} \\ A \end{array}
\quad \rightarrow \quad
\begin{array}{c} \Big\Vert \{\rho_1,\dots,\rho_i\} \\ A' \\ \Big\Vert \{\rho_{i+1},\dots,\rho_j\} \\ A'' \\ \Big\Vert \{\rho_{j+1},\dots,\rho_n\} \\ A \end{array}
$$

  - useful design principle for proof systems, including *combinatorial proofs* [Hughes, 2006]

Deep Inference

- Finer granularity of inference rules: rules may be decomposed into derivations of smaller rules to obtain atomicity

Deep Inference

- Finer granularity of inference rules: rules may be decomposed into derivations of smaller rules to obtain atomicity

$$\mathsf{c}{\downarrow}\,\frac{\forall x(a(x) \wedge b(x)) \vee \forall x(a(x) \wedge b(x))}{\forall x(a(x) \wedge b(x))}$$

Deep Inference

- Finer granularity of inference rules: rules may be decomposed into derivations of smaller rules to obtain atomicity

$$\mathsf{c}{\downarrow}\,\frac{\forall x(a(x)\wedge b(x)) \vee \forall x(a(x)\wedge b(x))}{\forall x(a(x)\wedge b(x))}$$

$$\downarrow$$

$$= \frac{\forall x(a(x)\wedge b(x)) \vee \forall x(a(x)\wedge b(x))}{\forall x \boxed{\mathsf{m}\,\dfrac{\boxed{\forall\,\dfrac{\forall y(a(y)\wedge b(y))}{a(x)\wedge b(x)}} \vee \boxed{\forall\,\dfrac{\forall y(a(y)\wedge b(y))}{a(x)\wedge b(x)}}}{\boxed{\mathsf{ac}{\downarrow}\,\dfrac{a(x)\vee a(x)}{a(x)}} \wedge \boxed{\mathsf{ac}{\downarrow}\,\dfrac{b(x)\vee b(x)}{b(x)}}}}}$$

Deep Inference

- Finer granularity of inference rules: rules may be decomposed into derivations of smaller rules to obtain atomicity

$$\mathsf{c}{\downarrow}\,\frac{\forall x(a(x)\wedge b(x)) \vee \forall x(a(x)\wedge b(x))}{\forall x(a(x)\wedge b(x))}$$

$$\downarrow$$

$$=\,\frac{\forall x(a(x)\wedge b(x)) \vee \forall x(a(x)\wedge b(x))}{\forall x\left[\mathsf{m}\,\frac{\left[\forall\,\frac{\forall y(a(y)\wedge b(y))}{a(x)\wedge b(x)}\right] \vee \left[\forall\,\frac{\forall y(a(y)\wedge b(y))}{a(x)\wedge b(x)}\right]}{\left[\mathsf{ac}{\downarrow}\,\frac{a(x)\vee a(x)}{a(x)}\right] \wedge \left[\mathsf{ac}{\downarrow}\,\frac{b(x)\vee b(x)}{b(x)}\right]}\right]}$$

Deep Inference

- Normalisation results for propositional logic
  - quasipolynomial-complexity cut elimination [Jeřábek, 2008]
  - normalisation procedures which are independent of connective information using *atomic flows* [Gundersen, 2009; Guglielmi, Gundersen, Straßburger, 2010]
  - exponential speedups over cut-free sequent calculus [Bruscoli, Guglielmi, 2009]

Deep Inference

- Normalisation results for propositional logic
  - quasipolynomial-complexity cut elimination [Jeřábek, 2008]
  - normalisation procedures which are independent of connective information using *atomic flows* [Gundersen, 2009; Guglielmi, Gundersen, Straßburger, 2010]
  - exponential speedups over cut-free sequent calculus [Bruscoli, Guglielmi, 2009]

- Can express logics not expressible in the sequent calculus (e.g. self-dual non-commutative binary connectives [Guglielmi, 2007])

Deep Inference

- Normalisation results for propositional logic
  - quasipolynomial-complexity cut elimination [Jeřábek, 2008]
  - normalisation procedures which are independent of connective information using *atomic flows* [Gundersen, 2009; Guglielmi, Gundersen, Straßburger, 2010]
  - exponential speedups over cut-free sequent calculus [Bruscoli, Guglielmi, 2009]
- Can express logics not expressible in the sequent calculus (e.g. self-dual non-commutative binary connectives [Guglielmi, 2007])
- Deep inference systems do not admit the subformula property and have a larger search space than Gentzen systems for proof search

Proof System

$$
\text{i}\downarrow \frac{\mathbf{t}}{A \vee \bar{A}} \qquad \text{w}\downarrow \frac{\mathbf{f}}{A} \qquad \text{c}\downarrow \frac{A \vee A}{A} \qquad \text{s} \frac{A \wedge (B \vee C)}{(A \wedge B) \vee C} \qquad \exists \frac{A(t)}{\exists x A(x)}
$$

$$
\text{i}\uparrow \frac{\bar{A} \wedge A}{\mathbf{f}} \qquad \text{w}\uparrow \frac{A}{\mathbf{t}} \qquad \text{c}\uparrow \frac{A}{A \wedge A} \qquad \text{m} \frac{(A \wedge B) \vee (C \wedge D)}{(A \vee C) \wedge (B \vee D)} \qquad \forall \frac{\forall x A(x)}{A(t)}
$$

$$
\text{r1}\downarrow \frac{\forall x(A(x) \vee B)}{\forall x A(x) \vee B} \qquad \text{r2}\downarrow \frac{\forall x(A(x) \wedge B)}{\forall x A(x) \wedge B} \qquad \text{r3}\downarrow \frac{\exists x(A(x) \vee B)}{\exists x A(x) \vee B} \qquad \text{r4}\downarrow \frac{\exists x(A(x) \wedge B)}{\exists x A(x) \wedge B}
$$

$$
\text{r1}\uparrow \frac{\exists x A(x) \wedge B}{\exists x(A(x) \wedge B)} \qquad \text{r2}\uparrow \frac{\exists x A(x) \vee B}{\exists x(A(x) \vee B)} \qquad \text{r3}\uparrow \frac{\forall x A(x) \wedge B}{\forall x(A(x) \wedge B)} \qquad \text{r4}\uparrow \frac{\forall x A(x) \vee B}{\forall x(A(x) \vee B)}
$$

where $x \notin fv(B)$

+ *equality rules for connective commutativity and associativity, unit equations, quantifier ordering, vacuous quantification and quantifier renaming*

Proof System

$$
\text{i}\!\downarrow \frac{\mathbf{t}}{A \vee \bar{A}} \qquad
\text{w}\!\downarrow \frac{\mathbf{f}}{A} \qquad
\text{c}\!\downarrow \frac{A \vee A}{A} \qquad
\text{s} \frac{A \wedge (B \vee C)}{(A \wedge B) \vee C} \qquad
\exists \frac{A(t)}{\exists x A(x)}
$$

$$
\text{i}\!\uparrow \frac{\bar{A} \wedge A}{\mathbf{f}} \qquad
\text{w}\!\uparrow \frac{A}{\mathbf{t}} \qquad
\text{c}\!\uparrow \frac{A}{A \wedge A} \qquad
\text{m} \frac{(A \wedge B) \vee (C \wedge D)}{(A \vee C) \wedge (B \vee D)} \qquad
\forall \frac{\forall x A(x)}{A(t)}
$$

$$
\text{r1}\!\downarrow \frac{\forall x (A(x) \vee B)}{\forall x A(x) \vee B} \qquad
\text{r2}\!\downarrow \frac{\forall x (A(x) \wedge B)}{\forall x A(x) \wedge B} \qquad
\text{r3}\!\downarrow \frac{\exists x (A(x) \vee B)}{\exists x A(x) \vee B} \qquad
\text{r4}\!\downarrow \frac{\exists x (A(x) \wedge B)}{\exists x A(x) \wedge B}
$$

$$
\text{r1}\!\uparrow \frac{\exists x A(x) \wedge B}{\exists x (A(x) \wedge B)} \qquad
\text{r2}\!\uparrow \frac{\exists x A(x) \vee B}{\exists x (A(x) \vee B)} \qquad
\text{r3}\!\uparrow \frac{\forall x A(x) \wedge B}{\forall x (A(x) \wedge B)} \qquad
\text{r4}\!\uparrow \frac{\forall x A(x) \vee B}{\forall x (A(x) \vee B)}
$$

where $x \notin fv(B)$

+ *equality rules for connective commutativity and associativity, unit equations, quantifier ordering, vacuous quantification and quantifier renaming*

- *Proofs* are derivations with premise **t** (true)

$$
\begin{array}{c} \mathbf{t} \\ \| \\ A \end{array} \quad \equiv \quad \begin{array}{c} \overline{\|} \\ A \end{array}
$$

Proof System

$$\mathsf{i}{\downarrow}\,\frac{\mathbf{t}}{A \vee \bar{A}} \quad \mathsf{w}{\downarrow}\,\frac{\mathbf{f}}{A} \quad \mathsf{c}{\downarrow}\,\frac{A \vee A}{A} \quad \mathsf{s}\,\frac{A \wedge (B \vee C)}{(A \wedge B) \vee C} \quad \exists\,\frac{A(t)}{\exists x A(x)}$$

$$\mathsf{i}{\uparrow}\,\frac{\bar{A} \wedge A}{\mathbf{f}} \quad \mathsf{w}{\uparrow}\,\frac{A}{\mathbf{t}} \quad \mathsf{c}{\uparrow}\,\frac{A}{A \wedge A} \quad \mathsf{m}\,\frac{(A \wedge B) \vee (C \wedge D)}{(A \vee C) \wedge (B \vee D)} \quad \forall\,\frac{\forall x A(x)}{A(t)}$$

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

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

where $x \notin fv(B)$

+ equality rules for connective commutativity and associativity, unit equations, quantifier ordering, vacuous quantification and quantifier renaming

- Every inference rule $\rho{\downarrow}$ has a corresponding *dual* inference rule $\rho{\uparrow}$

$$\rho{\downarrow}\,\frac{A}{B} \qquad \rho{\uparrow}\,\frac{\bar{B}}{\bar{A}}$$

$$\begin{array}{c} A \\ \| \\ B \end{array} \qquad \begin{array}{c} \bar{B} \\ \| \\ \bar{A} \end{array}$$

Quantifier-Shifts

$$\text{r1}{\downarrow}\ \frac{\forall x(A(x) \lor B)}{\forall x A(x) \lor B} \qquad \text{r2}{\downarrow}\ \frac{\forall x(A(x) \land B)}{\forall x A(x) \land B} \qquad \text{r3}{\downarrow}\ \frac{\exists x(A(x) \lor B)}{\exists x A(x) \lor B} \qquad \text{r4}{\downarrow}\ \frac{\exists x(A(x) \land B)}{\exists x A(x) \land B}$$

$$\text{r1}{\uparrow}\ \frac{\exists x A(x) \land B}{\exists x(A(x) \land B)} \qquad \text{r2}{\uparrow}\ \frac{\exists x A(x) \lor B}{\exists x(A(x) \lor B)} \qquad \text{r3}{\uparrow}\ \frac{\forall x A(x) \land B}{\forall x(A(x) \land B)} \qquad \text{r4}{\uparrow}\ \frac{\forall x A(x) \lor B}{\forall x(A(x) \lor B)}$$

where $x \notin fv(B)$

Quantifier-Shifts

$$\text{r1}{\downarrow}\ \frac{\forall x(A(x) \lor B)}{\forall x A(x) \lor B} \qquad \text{r2}{\downarrow}\ \frac{\forall x(A(x) \land B)}{\forall x A(x) \land B} \qquad \text{r3}{\downarrow}\ \frac{\exists x(A(x) \lor B)}{\exists x A(x) \lor B} \qquad \text{r4}{\downarrow}\ \frac{\exists x(A(x) \land B)}{\exists x A(x) \land B}$$

$$\text{r1}{\uparrow}\ \frac{\exists x A(x) \land B}{\exists x(A(x) \land B)} \qquad \text{r2}{\uparrow}\ \frac{\exists x A(x) \lor B}{\exists x(A(x) \lor B)} \qquad \text{r3}{\uparrow}\ \frac{\forall x A(x) \land B}{\forall x(A(x) \land B)} \qquad \text{r4}{\uparrow}\ \frac{\forall x A(x) \lor B}{\forall x(A(x) \lor B)}$$

where $x \notin fv(B)$

- **Theorem** [Aguilera, Baaz, 2019]: For a class of tautologies S due to Statman (1979), there is no elementary function bounding the length of the shortest cut-free **LK** proof of any formula in S by its shortest cut-free $\mathbf{LK} + QS$ proof

Quantifier-Shifts

$$\text{r1}\!\downarrow \frac{\forall x(A(x) \vee B)}{\forall x A(x) \vee B} \qquad \text{r2}\!\downarrow \frac{\forall x(A(x) \wedge B)}{\forall x A(x) \wedge B} \qquad \text{r3}\!\downarrow \frac{\exists x(A(x) \vee B)}{\exists x A(x) \vee B} \qquad \text{r4}\!\downarrow \frac{\exists x(A(x) \wedge B)}{\exists x A(x) \wedge B}$$

$$\text{r1}\!\uparrow \frac{\exists x A(x) \wedge B}{\exists x(A(x) \wedge B)} \qquad \text{r2}\!\uparrow \frac{\exists x A(x) \vee B}{\exists x(A(x) \vee B)} \qquad \text{r3}\!\uparrow \frac{\forall x A(x) \wedge B}{\forall x(A(x) \wedge B)} \qquad \text{r4}\!\uparrow \frac{\forall x A(x) \vee B}{\forall x(A(x) \vee B)}$$

where $x \notin fv(B)$

- **Theorem** [Aguilera, Baaz, 2019]: For a class of tautologies S due to Statman (1979), there is no elementary function bounding the length of the shortest cut-free **LK** proof of any formula in S by its shortest cut-free $\mathbf{LK} + QS$ proof

- **Corollary**: First-order deep-inference systems admit non-elementarily smaller cut-free proofs than **LK**

Herbrand's Theorem

- Existential contraction rules may be understood as case analyses on the existential quantifiers in the premise

$$\text{qc}{\downarrow}\,\frac{\exists x A \vee \exists x A}{\exists x A} \qquad\qquad \text{qc}{\uparrow}\,\frac{\forall x A}{\forall x A \wedge \forall x A}$$

Herbrand's Theorem

- Existential contraction rules may be understood as case analyses on the existential quantifiers in the premise

$$\text{qc}\!\downarrow \frac{\exists x A \vee \exists x A}{\exists x A} \qquad\qquad \text{qc}\!\uparrow \frac{\forall x A}{\forall x A \wedge \forall x A}$$

- A semantically natural operation is thus to extract these case analyses from a proof, deriving a disjunction of terms which witness the existential quantifiers in the conclusion

Herbrand's Theorem

- In a deep-inference setting, Brünnler (2001) has presented a proof of the general version of Herbrand's Theorem in the form of a decomposition theorem

$$
\begin{array}{c} \Big\| \;\text{First-order rules} \\ A \end{array}
\quad \rightarrow \quad
\begin{array}{l}
\forall \vec{x}\; \boxed{\begin{array}{l} \Big\| \;\text{Propositional rules} \\ A' \end{array}} \\
\qquad\quad \Big\| \;\{\exists\} \\
\qquad\quad A'' \\
\qquad\quad \Big\| \;\{\mathsf{r1}\!\downarrow, \mathsf{r2}\!\downarrow, \mathsf{r3}\!\downarrow, \mathsf{r4}\!\downarrow\} \\
\qquad\quad A''' \\
\qquad\quad \Big\| \;\{\mathsf{qc}\!\downarrow\} \\
\qquad\quad A
\end{array}
$$

Herbrand's Theorem

- In a deep-inference setting, Brünnler (2001) has presented a proof of the general version of Herbrand's Theorem in the form of a decomposition theorem

$$
\begin{array}{l} \Big\Vert \text{First-order rules} \\ A \end{array}
\quad \rightarrow \quad
\begin{array}{l}
\forall \vec{x} \boxed{\begin{array}{l} \Big\Vert \text{Propositional rules} \\ A' \end{array}} \\
\quad \Big\Vert \{\exists\} \\
\quad A'' \\
\quad \Big\Vert \{\mathsf{r1}\downarrow,\mathsf{r2}\downarrow,\mathsf{r3}\downarrow,\mathsf{r4}\downarrow\} \\
\quad A''' \\
\quad \Big\Vert \{\mathsf{qc}\downarrow\} \\
\quad A
\end{array}
$$

- $\forall \vec{x} A'$ is called a *Herbrand disjunction for A*

Herbrand's Theorem

- In a deep-inference setting, Brünnler (2001) has presented a proof of the general version of Herbrand's Theorem in the form of a decomposition theorem

$$\begin{array}{c} \Vert \text{First-order rules} \\ A \end{array} \quad \to \quad \begin{array}{c} \forall \vec{x} \boxed{\begin{array}{l} \Vert \text{Propositional rules} \\ A' \end{array}} \\ \Vert \{\exists\} \\ A'' \\ \Vert \{\mathsf{r1}{\downarrow}, \mathsf{r2}{\downarrow}, \mathsf{r3}{\downarrow}, \mathsf{r4}{\downarrow}\} \\ A''' \\ \Vert \{\mathsf{qc}{\downarrow}\} \\ A \end{array}$$

- $\forall \vec{x} A'$ is called a *Herbrand disjunction for A*
- Reduction of undecidable first-order provability to decidable propositional provability

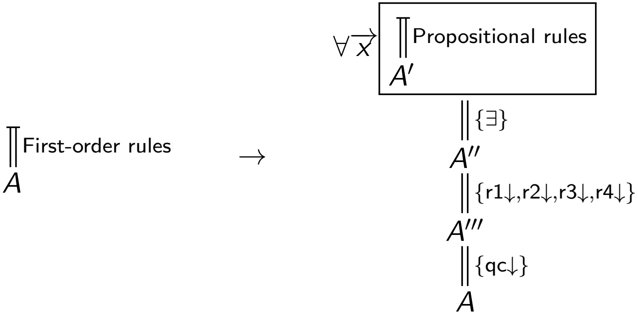
Herbrand's Theorem

- In a deep-inference setting, Brünnler (2001) has presented a proof of the general version of Herbrand's Theorem in the form of a decomposition theorem

$$
\begin{array}{c} \Big\Vert \text{First-order rules} \\ A \end{array}
\quad \rightarrow \quad
\begin{array}{c}
\forall \vec{x} \boxed{\begin{array}{l} \Big\Vert \text{Propositional rules} \\ A' \end{array}} \\
\Big\Vert \{\exists\} \\
A'' \\
\Big\Vert \{\mathsf{r1}\!\downarrow, \mathsf{r2}\!\downarrow, \mathsf{r3}\!\downarrow, \mathsf{r4}\!\downarrow\} \\
A''' \\
\Big\Vert \{\mathsf{qc}\!\downarrow\} \\
A
\end{array}
$$

- $\forall \vec{x} A'$ is called a *Herbrand disjunction for A*
- Reduction of undecidable first-order provability to decidable propositional provability
- Non-elementary blowups in proof complexity

Herbrand's Theorem



- The Herbrand disjunction $\forall\vec{x}A'$ can be interpreted algorithmically as a backtracking game [Coquand, 1995]

Herbrand's Theorem

$$
\begin{array}{c} \Big\Vert \text{First-order rules} \\ A \end{array}
\quad \rightarrow \quad
\begin{array}{c}
\forall \vec{x} \boxed{\begin{array}{l} \Big\Vert \text{Propositional rules} \\ A' \end{array}} \\
\Big\Vert \{\exists\} \\
A'' \\
\Big\Vert \{\mathsf{r1}{\downarrow}, \mathsf{r2}{\downarrow}, \mathsf{r3}{\downarrow}, \mathsf{r4}{\downarrow}\} \\
A''' \\
\Big\Vert \{\mathsf{qc}{\downarrow}\} \\
A
\end{array}
$$

- The Herbrand disjunction $\forall \vec{x} A'$ can be interpreted algorithmically as a backtracking game [Coquand, 1995]
- Equivalence of deep-inference Herbrand proofs and *expansion proofs* [Miller, 1987] demonstrated by Ralph (2010)

Example: The Drinker Paradox

$$
= \frac{\mathbf{t}}{\forall x_1 \forall x_2 \boxed{= \dfrac{\mathbf{t}}{\boxed{\mathsf{w}\!\downarrow \dfrac{\mathbf{f}}{\overline{P}(c)}} \vee \boxed{\mathsf{i}\!\downarrow \dfrac{\mathbf{t}}{P(x_1) \vee \overline{P}(x_1)}} \vee \boxed{\mathsf{w}\!\downarrow \dfrac{\mathbf{f}}{P(x_2)}}}}}
$$

$$
= \frac{\qquad\qquad}{\forall x_1 \forall x_2 ((P(x_1) \vee \overline{P}(c)) \vee (P(x_2) \vee \overline{P}(x_1)))}
$$

$$
\exists \frac{\forall x_1 \forall x_2 ((P(x_1) \vee \overline{P}(c)) \vee (P(x_2) \vee \overline{P}(x_1)))}{\forall x_1 \exists y_2 \forall x_2 ((P(x_1) \vee \overline{P}(c)) \vee (P(x_2) \vee \overline{P}(y_2)))}
$$

$$
\exists \frac{\forall x_1 \exists y_2 \forall x_2 ((P(x_1) \vee \overline{P}(c)) \vee (P(x_2) \vee \overline{P}(y_2)))}{\exists y_1 \forall x_1 \exists y_2 \forall x_2 ((P(x_1) \vee \overline{P}(y_1)) \vee (P(x_2) \vee \overline{P}(y_2)))}
$$

$$
\Big\| \{\mathsf{r1}\!\downarrow, \mathsf{r3}\!\downarrow\}
$$

$$
\mathsf{qc}\!\downarrow \frac{\exists y_1 (\forall x_1 P(x_1) \vee \overline{P}(y_1)) \vee \exists y_2 (\forall x_2 P(x_2) \vee \overline{P}(y_2))}{\exists y (\forall x P(x) \vee \overline{P}(y))}
$$

Herbrand disjunction:

$$
\forall x_1 \forall x_2 (P(x_1) \vee \overline{P}(c) \vee P(x_2) \vee \overline{P}(x_1))
$$

Cut Elimination

- Elimination of cut rules from a proof

$$\text{i}\!\uparrow \frac{A \wedge \overline{A}}{\mathbf{f}}$$

Cut Elimination

- Elimination of cut rules from a proof

$$\text{i}{\uparrow}\,\frac{A \wedge \overline{A}}{\mathbf{f}}$$

- In Gentzen systems, cut rules are permuted up the proof, resulting in non-determinism from certain reduction steps

Cut Elimination

- Elimination of cut rules from a proof

$$\mathsf{i}{\uparrow}\,\frac{A \wedge \overline{A}}{\mathbf{f}}$$

- In Gentzen systems, cut rules are permuted up the proof, resulting in non-determinism from certain reduction steps

- Non-elementary blowups in proof complexity for first-order proofs

Cuts and Quantifier-Shifts

- Cuts on quantifiers are simulated by r1↑ quantifier-shifts and $\forall$ rules

$$
\mathrm{i}{\uparrow}\,\frac{\forall x A(x) \wedge \exists x \overline{A}(x)}{\mathbf{f}}
\quad \rightarrow \quad
=\,\cfrac{\mathrm{r1}{\uparrow}\,\cfrac{=\,\cfrac{\forall x A(x) \wedge \exists x \overline{A}(x)}{\forall y A(y) \wedge \exists x \overline{A}(x)}}{\exists x \boxed{\mathrm{i}{\uparrow}\,\cfrac{\boxed{\forall\,\cfrac{\forall y A(y)}{A(x)}} \wedge \overline{A}(x)}{\mathbf{f}}}}}{\mathbf{f}}
$$

Cuts and Quantifier-Shifts

- Cuts on quantifiers are simulated by r1↑ quantifier-shifts and $\forall$ rules

$$
\text{i}{\uparrow}\,\frac{\forall x A(x) \wedge \exists x \overline{A}(x)}{\mathbf{f}}
\quad \rightarrow \quad
=\frac{\text{r1}{\uparrow}\,\dfrac{=\dfrac{\forall x A(x) \wedge \exists x \overline{A}(x)}{\forall y A(y) \wedge \exists x \overline{A}(x)}}{\exists x \left[\text{i}{\uparrow}\,\dfrac{\left[\forall\,\dfrac{\forall y A(y)}{A(x)} \right] \wedge \overline{A}(x)}{\mathbf{f}} \right]}}{\mathbf{f}}
$$

- Cuts can be reduced to quantifier-shifts and atomic cuts in deep inference

Cut Elimination

- Cut rules may be decomposed to atomic form in deep inference

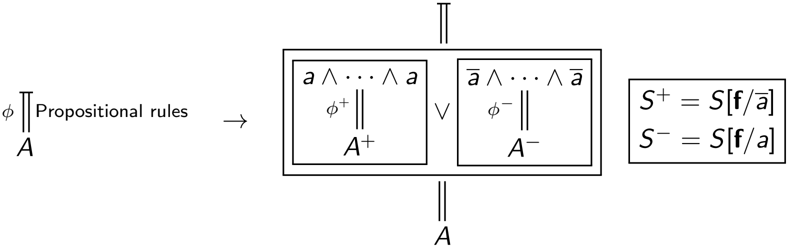
$$\mathsf{ai}\!\uparrow \frac{a \wedge \bar{a}}{\mathbf{f}}$$

Cut Elimination

- Cut rules may be decomposed to atomic form in deep inference

$$\mathsf{ai}\!\uparrow \frac{a \wedge \bar{a}}{\mathbf{f}}$$

- In propositional deep inference, a semantically natural cut-elimination procedure exists, called the *experiments method* [Guglielmi, 2002; Ralph, 2019]

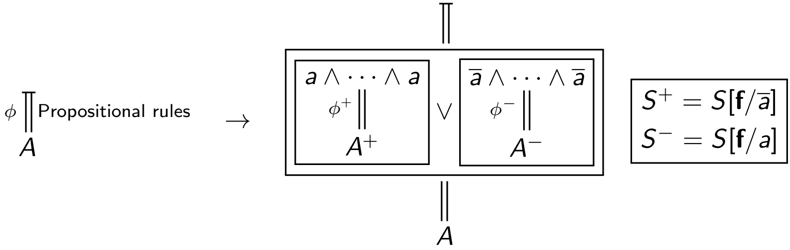


Cut Elimination

- Cut rules may be decomposed to atomic form in deep inference

$$\mathsf{ai}\uparrow \frac{a \wedge \bar{a}}{\mathbf{f}}$$

- In propositional deep inference, a semantically natural cut-elimination procedure exists, called the *experiments method* [Guglielmi, 2002; Ralph, 2019]



- Can be extended to first-order logic by first translating to Herbrand normal form

Relationship Between First-Order Phenomena

- Traditionally, in the sequent calculus, Herbrand's Theorem is proved as a corollary to cut elimination

Relationship Between First-Order Phenomena

- Traditionally, in the sequent calculus, Herbrand's Theorem is proved as a corollary to cut elimination
- Brünnler's proof of Herbrand's Theorem using deep inference does not require cuts to be eliminated from the proof, establishing a kind of independence between Herbrand's Theorem and cut elimination

Relationship Between First-Order Phenomena

- Traditionally, in the sequent calculus, Herbrand's Theorem is proved as a corollary to cut elimination

- Brünnler's proof of Herbrand's Theorem using deep inference does not require cuts to be eliminated from the proof, establishing a kind of independence between Herbrand's Theorem and cut elimination

- Both cut elimination and Herbrand's Theorem eliminate quantifier-shifts, resulting in non-elementary blowups. Can quantifier-shifts help us to understand the relationship between these theorems?

Elimination of Quantifier-Shifts

- Most quantifier-shifts are derivable with other rules, with the exceptions of r1$\downarrow$ and r1$\uparrow$

$$\text{r2}\!\downarrow \frac{\forall x(A(x) \wedge B)}{\forall x A(x) \wedge B} \quad \to \quad = \dfrac{\text{qc}\!\uparrow \dfrac{\forall x(A(x) \wedge B)}{\boxed{\forall x \boxed{A(x) \wedge \boxed{\text{w}\!\uparrow \dfrac{B}{\mathbf{t}}}} \wedge \forall x \boxed{\boxed{\text{w}\!\uparrow \dfrac{A(x)}{\mathbf{t}}} \wedge B}}}}{\forall x A(x) \wedge B}$$

$$\boxed{\begin{array}{c} \text{r1}\!\downarrow \dfrac{\forall x(A(x) \vee B)}{\forall x A(x) \vee B} \\[2em] \text{r1}\!\uparrow \dfrac{\exists x A(x) \wedge B}{\exists x(A(x) \wedge B)} \end{array}}$$

$$\text{r3}\!\downarrow \frac{\exists x(A(x) \vee B)}{\exists x A(x) \vee B} \quad \to \quad = \dfrac{\exists x \boxed{\boxed{\exists \dfrac{A(x)}{\exists y A(y)}} \vee B}}{\exists x A(x) \vee B}$$

$$\text{r4}\!\downarrow \frac{\exists x(A(x) \wedge B)}{\exists x A(x) \wedge B} \quad \to \quad = \dfrac{\exists x \boxed{\boxed{\exists \dfrac{A(x)}{\exists y A(y)}} \wedge B}}{\exists x A(x) \wedge B}$$

Falsifiers

$$\text{r1}{\downarrow}\,\frac{\forall x \boxed{A(x) \vee \boxed{\exists\,\dfrac{B(x)}{\exists y B(y)}}}}{\forall x A(x) \vee \exists y B(y)}$$

- No constructive witness for $\exists y$ given in the derivation

Falsifiers

$$\text{r1}{\downarrow}\ \dfrac{\forall x \boxed{A(x) \vee \boxed{\exists\ \dfrac{B(x)}{\exists y B(y)}}}}{\forall x A(x) \vee \exists y B(y)}$$

- No constructive witness for $\exists y$ given in the derivation

$$\exists y = \begin{cases} e & \text{if there exists some } e \in \mathbb{D} \text{ s.t. } \overline{A}(e) \\ a & \text{for some arbitrary } a \in \mathbb{D}\text{, otherwise} \end{cases}$$

Falsifiers

$$\text{r1}\downarrow \frac{\forall x \boxed{A(x) \vee \boxed{\exists \frac{B(x)}{\exists y B(y)}}}}{\forall x A(x) \vee \exists y B(y)}$$

- No constructive witness for $\exists y$ given in the derivation

$$\exists y = \begin{cases} e & \text{if there exists some } e \in \mathbb{D} \text{ s.t. } \overline{A}(e) \\ a & \text{for some arbitrary } a \in \mathbb{D}\text{, otherwise} \end{cases}$$
$$= [\![\varepsilon_x \overline{A}(x)]\!]_{\mathbb{D}}$$

- Quantifier-shifts conceal the epsilon-calculus!

Epsilon-Calculus

- Expand the language of the predicate calculus by *epsilon-terms*:

$$[\![\varepsilon_x A(x)]\!]_{\mathbb{D}} = \begin{cases} e & \text{if there exists some } e \in \mathbb{D} \text{ s.t. } A(e) \\ a & \text{for some arbitrary } a \in \mathbb{D}\text{, otherwise} \end{cases}$$

Epsilon-Calculus

- Expand the language of the predicate calculus by *epsilon-terms*:

$$[\![\varepsilon_x A(x)]\!]_{\mathbb{D}} = \begin{cases} e & \text{if there exists some } e \in \mathbb{D} \text{ s.t. } A(e) \\ a & \text{for some arbitrary } a \in \mathbb{D}\text{, otherwise} \end{cases}$$

- Introduced by Hilbert (1927) as a tool for developing consistency proofs

Epsilon-Calculus

- Expand the language of the predicate calculus by *epsilon-terms*:

$$[\![\varepsilon_x A(x)]\!]_{\mathbb{D}} = \begin{cases} e & \text{if there exists some } e \in \mathbb{D} \text{ s.t. } A(e) \\ a & \text{for some arbitrary } a \in \mathbb{D}, \text{ otherwise} \end{cases}$$

- Introduced by Hilbert (1927) as a tool for developing consistency proofs
- It is known that the traditional epsilon-calculus admits non-elementarily smaller cut-free proofs than **LK** [Baaz, Lolić, 2024] and may be used to obtain speedups in the computation of Herbrand disjunctions over traditional methods [Baaz, Leitsch, Lolić, 2017]

Epsilon-Calculus

- In the traditional epsilon-calculus, epsilon-terms are introduced by *critical axioms* and quantifiers are encoded by epsilon-terms:

$$CA\,\frac{A(t)}{A(\varepsilon_x A(x))} \qquad \begin{aligned} \exists x A(x) &\equiv A(\varepsilon_x A(x)) \\ \forall x A(x) &\equiv A(\varepsilon_x \overline{A}(x)) \end{aligned}$$

Epsilon-Calculus

- In the traditional epsilon-calculus, epsilon-terms are introduced by *critical axioms* and quantifiers are encoded by epsilon-terms:

$$CA\,\frac{A(t)}{A(\varepsilon_x A(x))} \qquad\qquad \begin{array}{l} \exists x A(x) \equiv A(\varepsilon_x A(x)) \\ \forall x A(x) \equiv A(\varepsilon_x \overline{A}(x)) \end{array}$$

- Epsilon-terms are eliminated by "epsilon substitution", similar in spirit to Herbrand's Theorem

Epsilon-Calculus

- In the traditional epsilon-calculus, epsilon-terms are introduced by *critical axioms* and quantifiers are encoded by epsilon-terms:

$$CA\ \frac{A(t)}{A(\varepsilon_x A(x))} \qquad\qquad \begin{array}{l} \exists x A(x) \equiv A(\varepsilon_x A(x)) \\ \forall x A(x) \equiv A(\varepsilon_x \overline{A}(x)) \end{array}$$

- Epsilon-terms are eliminated by "epsilon substitution", similar in spirit to Herbrand's Theorem

- From [Baaz, Leitsch, Lolić, 2017]:

> Despite the advantages, the ε-calculus has never become popular in computational proof theory of first order logic. The main reasons are the untractability of almost all nonclassical logics by any adaptation of the ε-formalism and the clumsiness of the ε-formalism itself: consider the ε-translation of $\exists x \exists y \exists z$ $A(x, y, z)$: $A(\varepsilon_x\ A(x, \varepsilon_y\ A(x, y, \varepsilon_z\ A(x, y, z)), \varepsilon_z A(x, \varepsilon_y\ A(x, y, \varepsilon_z\ A(x, y, z)), z)),$ $\varepsilon_y\ A(\varepsilon_x\ A(x, \varepsilon_y\ A(x, y, \varepsilon_z A(x, y, z)), \varepsilon_z A(x, \varepsilon_y A(x, y, \varepsilon_z A(x, y, z)), z)), y, \varepsilon_z A(\varepsilon_x$ $A(x, \varepsilon_y\ A(x, y, \varepsilon_z\ A(x, y, z)), \varepsilon_z\ A(x, \varepsilon_y\ A(x, y, \varepsilon_z\ A(x, y, z)), z)), y, z)),\ \varepsilon_z A(\varepsilon_x$ $A(x, \varepsilon_y\ A(x, y, \varepsilon_z\ A(x, y, z)), \varepsilon_z A(x, \varepsilon_y\ A(x, y, \varepsilon_z\ A(x, y, z)), z)),\ \varepsilon_y A(\varepsilon_x\ A(x, \varepsilon_y$ $A(x, y, \varepsilon_z\ A(x, y, z)), \varepsilon_z\ A(x, \varepsilon_y\ A(x, y, \varepsilon_z\ A(x, y, z)), z)),\ y, \varepsilon_z\ A(\varepsilon_x\ A(x, \varepsilon_y\ A(x,$ $y,\ \varepsilon_z\ A(x,\ y,\ z)), \varepsilon_z\ A(x, \varepsilon_y\ A(x, y, \varepsilon_z\ A(x, y, z)), z)), y, z)), z))$.

Falsifier Rule

$$\varepsilon \frac{\forall x(A(x) \vee B(x))}{\forall x A(x) \vee B(\varepsilon_y \overline{A}(y))}$$

Falsifier Rule

$$\varepsilon\,\frac{\forall x(A(x)\lor B(x))}{\forall x A(x)\lor B(\varepsilon_y \overline{A}(y))}$$

$$\mathrm{r1}{\downarrow}\,\frac{\forall x\,\boxed{A(x)\lor \boxed{\exists\,\frac{B(x)}{\exists y B(y)}}}}{\forall x A(x)\lor \exists y B(y)} \quad\to\quad \varepsilon\,\frac{\forall x(A(x)\lor B(x))}{\boxed{\forall x A(x)\lor\boxed{\exists\,\frac{B(\varepsilon_y\overline{A}(y))}{\exists y B(y)}}}}$$

- Existential rules can be permuted down through quantifier-shifts

Falsifier Rule

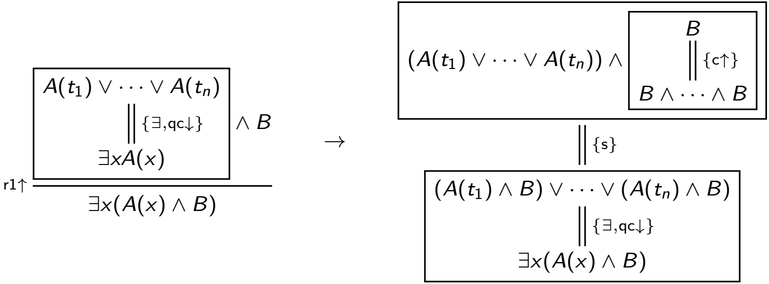
$$\varepsilon \, \frac{\forall x(A(x) \lor B(x))}{\forall x A(x) \lor B(\varepsilon_y \overline{A}(y))}$$

$$\text{r1}{\downarrow} \, \frac{\forall x(A(x) \lor B)}{\forall x A(x) \lor B}$$

- Equivalent to r1↓ when x does not occur free in B

Falsifier Rule

$$\varepsilon\ \frac{\forall x(A(x) \vee B(x))}{\forall x A(x) \vee B(\varepsilon_y \overline{A}(y))}$$



- r1↑ rules may be eliminated using falsifiers – $\exists x A(x)$ may be assigned an explicit disjunction of witnesses $A(t_1) \vee \cdots \vee A(t_n)$

Falsifier Rule

$$\varepsilon \frac{\forall x(A(x) \vee B(x))}{\forall x A(x) \vee B(\varepsilon_y \overline{A}(y))}$$

- Provides a new perspective on quantifier-shifts and non-elementary proof compression
- The epsilon-calculus provides a syntax for expressing non-constructive witnesses to existential quantifiers generated in proofs
- Does not use the cumbersome encodings of quantifiers by epsilon-terms

Extraction of Case Analyses

- A semantically natural operation to perform on a first-order proof is to extract the case analyses

$$\text{qc}\downarrow \frac{\exists x A \vee \exists x A}{\exists x A} \qquad \text{qc}\uparrow \frac{\forall x A}{\forall x A \wedge \forall x A}$$

Extraction of Case Analyses

- A semantically natural operation to perform on a first-order proof is to extract the case analyses

$$\text{qc}\!\downarrow \frac{\exists x A \vee \exists x A}{\exists x A} \qquad\qquad \text{qc}\!\uparrow \frac{\forall x A}{\forall x A \wedge \forall x A}$$

- Herbrand's Theorem also eliminates quantifier-shifts by making the proof constructive, resulting in non-elementary blowups – can falsifiers prevent this?

Extraction of Case Analyses

- A semantically natural operation to perform on a first-order proof is to extract the case analyses

$$\text{qc}{\downarrow}\ \frac{\exists x A \vee \exists x A}{\exists x A} \qquad\qquad \text{qc}{\uparrow}\ \frac{\forall x A}{\forall x A \wedge \forall x A}$$

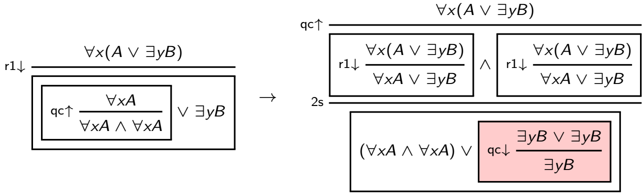
- Herbrand's Theorem also eliminates quantifier-shifts by making the proof constructive, resulting in non-elementary blowups – can falsifiers prevent this?

- Simple case analysis extraction by permuting quantifier contraction rules

Non-Termination of Case Analysis Extraction

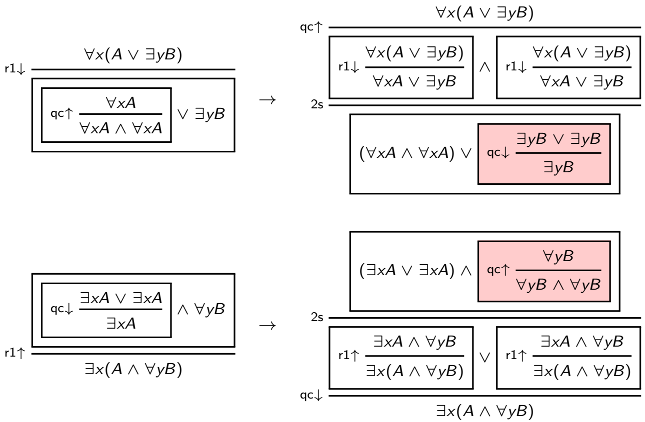
$$\mathsf{r1}\!\downarrow \frac{\forall x(A \vee \exists y B)}{\boxed{\boxed{\mathsf{qc}\!\uparrow \dfrac{\forall x A}{\forall x A \wedge \forall x A}} \vee \exists y B}} \quad \to \quad \begin{array}{rc} \mathsf{qc}\!\uparrow & \forall x(A \vee \exists y B) \\ \hline & \boxed{\mathsf{r1}\!\downarrow \dfrac{\forall x(A \vee \exists y B)}{\forall x A \vee \exists y B}} \wedge \boxed{\mathsf{r1}\!\downarrow \dfrac{\forall x(A \vee \exists y B)}{\forall x A \vee \exists y B}} \\ \mathsf{2s} & \\ \hline & \boxed{(\forall x A \wedge \forall x A) \vee \boxed{\mathsf{qc}\!\downarrow \dfrac{\exists y B \vee \exists y B}{\exists y B}}} \end{array}$$

Non-Termination of Case Analysis Extraction



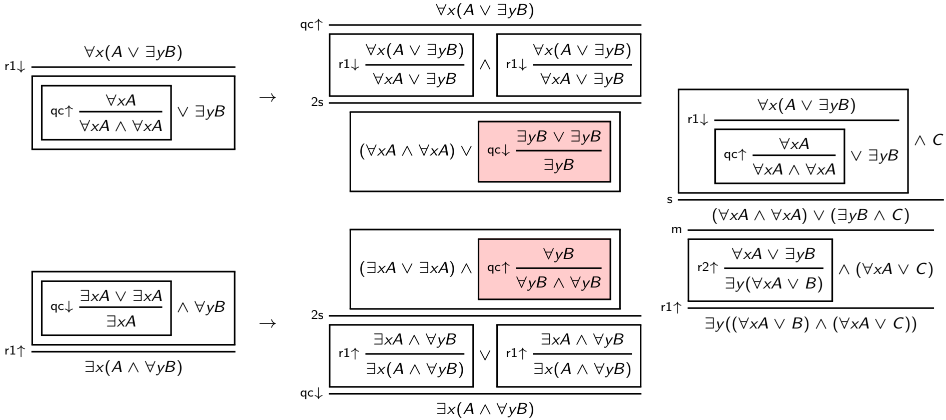
- Superfluous qc↓ rules are introduced, despite the witnesses to the existential quantifiers being equal

Non-Termination of Case Analysis Extraction



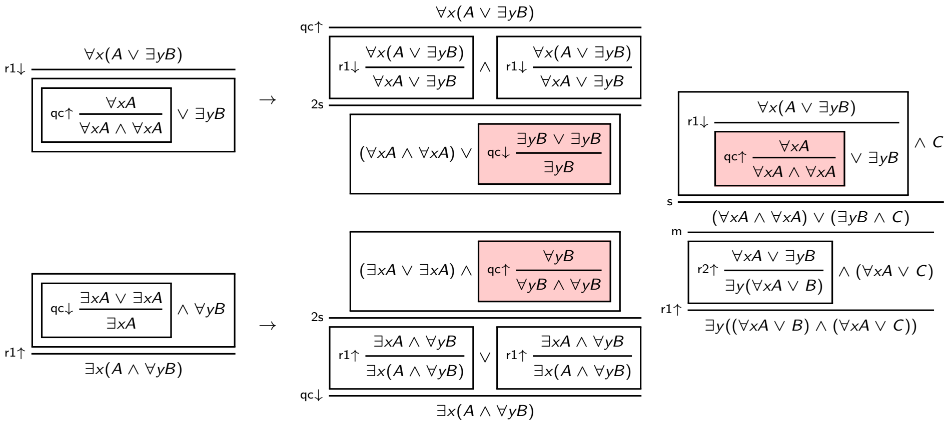
- Superfluous qc↓ rules are introduced, despite the witnesses to the existential quantifiers being equal

Non-Termination of Case Analysis Extraction



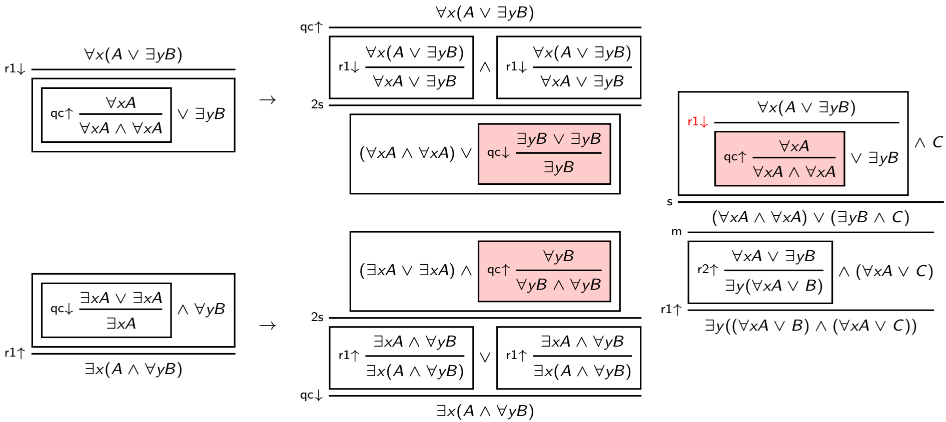
- Superfluous qc↓ rules are introduced, despite the witnesses to the existential quantifiers being equal

Non-Termination of Case Analysis Extraction



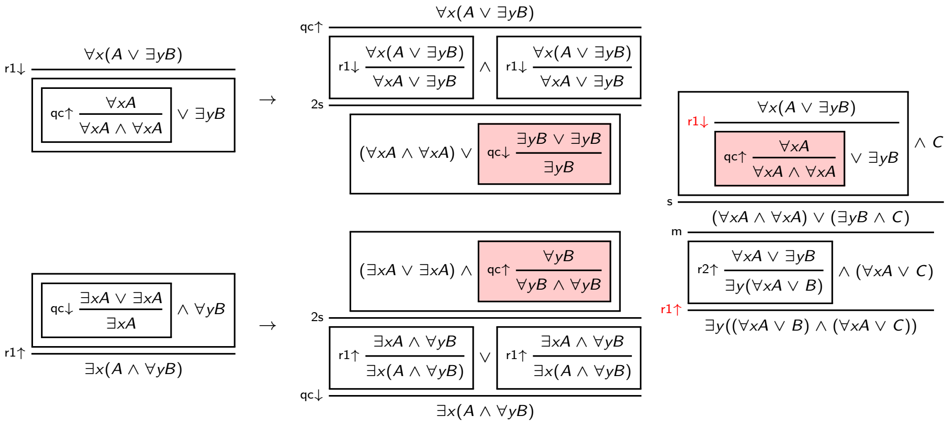
- Superfluous qc↓ rules are introduced, despite the witnesses to the existential quantifiers being equal

Non-Termination of Case Analysis Extraction



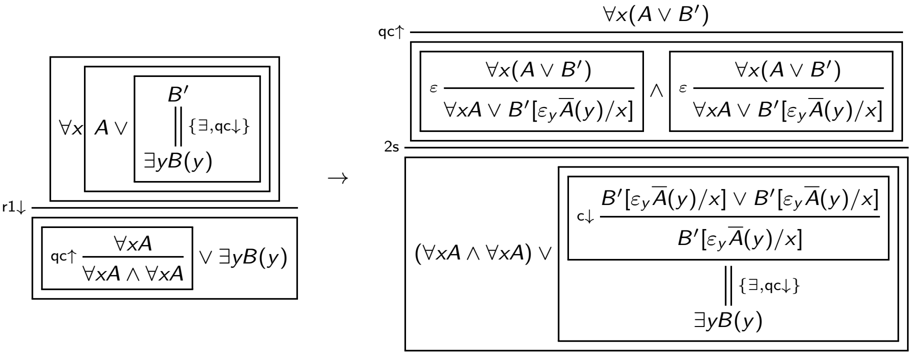
- Superfluous qc↓ rules are introduced, despite the witnesses to the existential quantifiers being equal

Non-Termination of Case Analysis Extraction



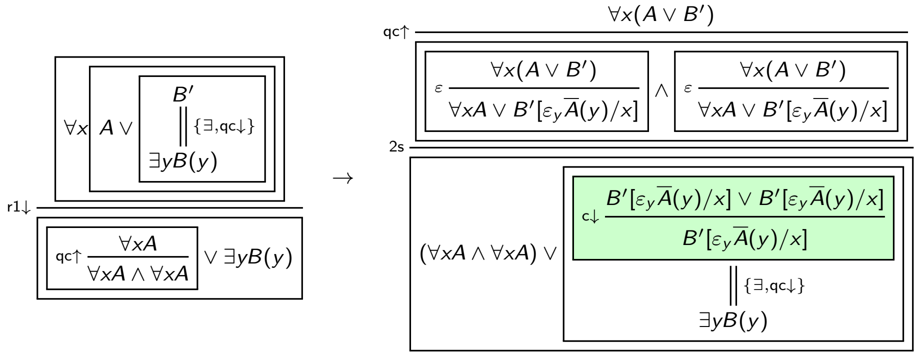
- Superfluous qc↓ rules are introduced, despite the witnesses to the existential quantifiers being equal

Termination Using Falsifiers



where $B' = B(t_1) \vee \cdots \vee B(t_n)$

Termination Using Falsifiers



where $B' = B(t_1) \vee \cdots \vee B(t_n)$

- The more expressive syntax of the epsilon-calculus can express that the terms are equal – there is no need for a case analysis and so no superfluous qc↓ rules are introduced

Extraction of Case Analyses

- Extract case analyses from a first-order proof in three phases:
  - Phase 1: Permute existential contraction rules qc$\downarrow$ down to the bottom of the proof
  - Phase 2: Permute existential instantiation rules $\exists$ down to the bottom of the proof
  - Phase 3: Permute universal cocontraction rules qc$\uparrow$ up the proof until they are eliminated

Extraction of Case Analyses

- Extract case analyses from a first-order proof in three phases:
  - Phase 1: Permute existential contraction rules $\mathsf{qc}\downarrow$ down to the bottom of the proof
  - Phase 2: Permute existential instantiation rules $\exists$ down to the bottom of the proof
  - Phase 3: Permute universal cocontraction rules $\mathsf{qc}\uparrow$ up the proof until they are eliminated

- To begin, eliminate quantifier-shifts as shown

$$\mathsf{r1}\downarrow\frac{\forall x(A(x) \vee B)}{\forall x A(x) \vee B} \quad \to \quad \varepsilon\frac{\forall x(A(x) \vee B)}{\forall x A(x) \vee B}$$

Phase 1: Permute qc↓ rules down

- Duplicate rules inside the context of qc↓ rules:

$$\mathsf{qc}\!\downarrow\dfrac{\exists x K\{A\} \vee \exists x K\{A\}}{\boxed{\exists x K\left\{\boxed{\rho\,\dfrac{A}{B}}\right\}}} \quad\to\quad \mathsf{qc}\!\downarrow\dfrac{\boxed{\boxed{\exists x K\left\{\boxed{\rho\,\dfrac{A}{B}}\right\}} \vee \boxed{\exists x K\left\{\boxed{\rho\,\dfrac{A}{B}}\right\}}}}{\exists x K\{B\}}$$

Phase 1: Permute qc↓ rules down

- Duplicate rules inside the context of qc↓ rules:

$$\mathsf{qc}{\downarrow}\,\frac{\exists x K\{A\} \vee \exists x K\{A\}}{\boxed{\exists x K\left\{\boxed{\rho\,\frac{A}{B}}\right\}}} \quad \rightarrow \quad \mathsf{qc}{\downarrow}\,\cfrac{\cfrac{\boxed{\boxed{\exists x K\left\{\boxed{\rho\,\frac{A}{B}}\right\}} \vee \boxed{\exists x K\left\{\boxed{\rho\,\frac{A}{B}}\right\}}}}{}}{\exists x K\{B\}}$$

- Permutation for r1↑ rules:

$$\mathsf{r1}{\uparrow}\,\frac{\boxed{\boxed{\mathsf{qc}{\downarrow}\,\frac{\exists x A(x) \vee \exists x A(x)}{\exists x A(x)}} \wedge B}}{\exists x (A(x) \wedge B)} \quad \rightarrow \quad \mathsf{qc}{\downarrow}\,\cfrac{\cfrac{\mathsf{s}\,\cfrac{\mathsf{s}\,\cfrac{\boxed{(\exists x A(x) \vee \exists x A(x)) \wedge \boxed{\mathsf{c}{\uparrow}\,\frac{B}{B \wedge B}}}}{(\exists x A(x) \vee (\exists x A(x) \wedge B)) \wedge B}}{\boxed{\boxed{\mathsf{r1}{\uparrow}\,\frac{\exists x A(x) \wedge B}{\exists x (A(x) \wedge B)}} \vee \boxed{\mathsf{r1}{\uparrow}\,\frac{\exists x A(x) \wedge B}{\exists x (A(x) \wedge B)}}}}}{}}{\exists x (A(x) \wedge B)}$$

Phase 2: Permute ∃ rules down

- Rules inside the context of ∃ rules are altered by a substitution:

$$\exists\,\frac{K\{A\}[t/x]}{\boxed{\exists x K\left\{\boxed{\rho\,\frac{A}{B}}\right\}}} \quad\to\quad \exists\,\frac{\boxed{K\left\{\boxed{\rho\,\frac{A}{B}}\right\}[t/x]}}{\exists x K\{B\}}$$

Phase 2: Permute $\exists$ rules down

- Rules inside the context of $\exists$ rules are altered by a substitution:

$$\exists\,\dfrac{K\{A\}[t/x]}{\boxed{\exists x K\left\{\boxed{\rho\,\dfrac{A}{B}}\right\}}} \quad\rightarrow\quad \exists\,\dfrac{\boxed{K\left\{\boxed{\rho\,\dfrac{A}{B}}\right\}[t/x]}}{\exists x K\{B\}}$$

- Permutations for ε rules:

$$\varepsilon\,\dfrac{\boxed{\forall y\left(B(y)\vee K\left\{\boxed{\exists\,\dfrac{A(t)}{\exists x A(x)}}\right\}\right)}}{\forall y B(y)\vee K\{\exists x A\}[\varepsilon_z\overline{B}(z)/y]} \quad\rightarrow\quad \varepsilon\,\dfrac{\forall y(B(y)\vee K\{A(t)\})}{\boxed{\forall y B(y)\vee K\left\{\boxed{\exists\,\dfrac{A(t)}{\exists x A(x)}}\right\}[\varepsilon_z\overline{B}(z)/y]}}$$

$$\varepsilon\,\dfrac{\boxed{\forall y\left(K\left\{\boxed{\exists\,\dfrac{A(t)}{\exists x A(x)}}\right\}\vee B(y)\right)}}{\forall y K\{\exists x A(x)\}\vee B(\varepsilon_z(\overline{K\{\exists x A(x)\}[z/y]}))} \quad\rightarrow\quad \varepsilon\,\dfrac{\forall y(K\{A(t)\}\vee B(y))}{\boxed{\forall y K\left\{\boxed{\exists\,\dfrac{A(t)}{\exists x A(x)}}\right\}\vee B(\varepsilon_z(\overline{K\{A(t)\}[z/y]}))}}$$

Phase 3: Permute qc↑ rules up

- Duplicate rules inside the context of qc↑ rules:

$$\mathsf{qc}\!\uparrow \frac{\boxed{\forall x K\left\{\boxed{\rho\,\frac{B}{A}}\right\}}}{\forall x K\{A\} \wedge \forall x K\{A\}} \quad \to \quad \mathsf{qc}\!\uparrow \frac{\forall x K\{B\}}{\boxed{\boxed{\forall x K\left\{\boxed{\rho\,\frac{B}{A}}\right\}} \wedge \boxed{\forall x K\left\{\boxed{\rho\,\frac{B}{A}}\right\}}}}$$

Phase 3: Permute qc↑ rules up

- Duplicate rules inside the context of qc↑ rules:

$$
\mathsf{qc}\!\uparrow \frac{\boxed{\forall x K\left\{\boxed{\rho\,\dfrac{B}{A}}\right\}}}{\forall x K\{A\} \wedge \forall x K\{A\}}
\quad \rightarrow \quad
\mathsf{qc}\!\uparrow \frac{\forall x K\{B\}}{\boxed{\boxed{\forall x K\left\{\boxed{\rho\,\dfrac{B}{A}}\right\}} \wedge \boxed{\forall x K\left\{\boxed{\rho\,\dfrac{B}{A}}\right\}}}}
$$

- When permuting qc↑ up through ε rules, we employ the following construction, which is invariant under the permutation:

$$
\begin{array}{c}
\boxed{\boxed{\varepsilon\,\dfrac{\forall x(A(x) \vee B(x))}{\forall x A(x) \vee B(\varepsilon_y \overline{A}(y))}} \wedge \cdots \wedge \boxed{\varepsilon\,\dfrac{\forall x(A(x) \vee B(x))}{\forall x A(x) \vee B(\varepsilon_y \overline{A}(y))}}} \\
\Big\| \{\mathsf{s}\} \\
\boxed{(\forall x A(x) \wedge \cdots \wedge \forall x A(x)) \vee \boxed{\begin{array}{c} B(\varepsilon_y \overline{A}(y)) \vee \cdots \vee B(\varepsilon_y \overline{A}(y)) \\ \Big\| \{\mathsf{c}\!\downarrow\} \\ B(\varepsilon_y \overline{A}(y)) \end{array}}}
\end{array}
$$

The Falsifier Decomposition Theorem

$$\begin{array}{c} \phi \Big\Vert \text{First-order rules} \\ A \end{array} \quad \rightarrow \quad \begin{array}{c} \phi' \Big\Vert \text{Propositional rules} + \{\varepsilon, \forall\} \ (\text{SKSg}\varepsilon) \\ A' \\ \Big\Vert \{\exists, \text{qc}\downarrow\} \\ A \end{array}$$

$$\varepsilon \frac{\forall x(A(x) \vee B(x))}{\forall x A(x) \vee B(\varepsilon_y \overline{A}(y))} \qquad \forall \frac{\forall x A(x)}{A(t)}$$

- I call A' a *falsifier disjunction for A*
- I call SKSgε the *falsifier calculus*

The Falsifier Decomposition Theorem

$$\phi \,\Big\|\, \text{First-order rules} \atop A \quad \to \quad \begin{array}{c} \phi' \\ \Big\| \text{ Propositional rules} + \{\varepsilon, \forall\} \text{ (SKSg}\varepsilon\text{)} \\ A' \\ \Big\| \{\exists, \text{qc}\downarrow\} \\ A \end{array}$$

$$\varepsilon \, \frac{\forall x(A(x) \vee B(x))}{\forall x A(x) \vee B(\varepsilon_y \overline{A}(y))} \qquad \forall \, \frac{\forall x A(x)}{A(t)}$$

- I call A' a *falsifier disjunction for* A
- I call SKSgε the *falsifier calculus*
- The following bounds hold:

$$|\phi'| = \exp^{10}(O(|\phi|^2 \ln |\phi|))$$
$$|A'| = \exp^{7}(O(|\phi|^2 \ln |\phi|))$$
$$|\phi'|_\varepsilon = \exp^{12}(O(|\phi|^2 \ln |\phi|))$$
$$|A'|_\varepsilon = \exp^{12}(O(|\phi|^2 \ln |\phi|))$$

The Falsifier Decomposition Theorem

$$\begin{array}{c} \phi \\ \Vert \; \text{First-order rules} \\ A \end{array} \quad \rightarrow \quad \begin{array}{c} \phi' \\ \Vert \; \text{Propositional rules} + \{\varepsilon, \forall\} \text{ (SKSg}\varepsilon\text{)} \\ A' \\ \Vert \; \{\exists, \mathsf{qc}{\downarrow}\} \\ A \end{array}$$

$$\varepsilon \, \frac{\forall x (A(x) \vee B(x))}{\forall x A(x) \vee B(\varepsilon_y \overline{A}(y))} \qquad \forall \, \frac{\forall x A(x)}{A(t)}$$

- I call A' a *falsifier disjunction for* A
- I call SKSgε the *falsifier calculus*
- The following bounds hold:

$$|\phi'| \in \textbf{ELEMENTARY}$$
$$|A'| \in \textbf{ELEMENTARY}$$
$$|\phi'|_\varepsilon \in \textbf{ELEMENTARY}$$
$$|A'|_\varepsilon \in \textbf{ELEMENTARY}$$

- Non-elementarily smaller than Herbrand disjunctions and Herbrand proofs

The Falsifier Decomposition Theorem

$$\begin{array}{c} \phi \\ \Vert \ \text{First-order rules} \\ A \end{array} \quad \to \quad \begin{array}{c} \phi' \\ \Vert \ \text{Propositional rules} + \{\varepsilon, \forall\} \ (\mathsf{SKSg}\varepsilon) \\ A' \\ \Vert \ \{\exists, \mathsf{qc}\!\downarrow\} \\ A \end{array}$$

$$\varepsilon \frac{\forall x (A(x) \vee B(x))}{\forall x A(x) \vee B(\varepsilon_y \overline{A}(y))} \qquad \forall \frac{\forall x A(x)}{A(t)}$$

- Unlike Herbrand's Theorem, we have extracted the case analyses from the proof but left the quantifier-shifts intact, in the form of falsifier rules which introduce epsilon-terms
- Epsilon-terms represent elements which are drawn from the domain non-constructively in the proof
- Does not use the cumbersome encodings of quantifiers by epsilon-terms

Example: The Drinker Paradox

$$
\mathrm{qc}\!\downarrow\dfrac{\begin{array}{c}
\exists\,\dfrac{\exists\,\dfrac{=\dfrac{\mathbf{t}}{\forall x_1\forall x_2\boxed{=\dfrac{\mathbf{t}}{\boxed{\mathrm{w}\!\downarrow\dfrac{\mathbf{f}}{\bar{P}(c)}}\vee\boxed{\mathrm{i}\!\downarrow\dfrac{\mathbf{t}}{P(x_1)\vee\bar{P}(x_1)}}\vee\boxed{\mathrm{w}\!\downarrow\dfrac{\mathbf{f}}{P(x_2)}}}}}\;=}{\forall x_1\forall x_2((P(x_1)\vee\bar{P}(c))\vee(P(x_2)\vee\bar{P}(x_1)))}}{\forall x_1\exists y_2\forall x_2((P(x_1)\vee\bar{P}(c))\vee(P(x_2)\vee\bar{P}(y_2)))}}{\exists y_1\forall x_1\exists y_2\forall x_2((P(x_1)\vee\bar{P}(y_1))\vee(P(x_2)\vee\bar{P}(y_2)))}\\
\Big\Vert\;\{\mathrm{r1}\!\downarrow,\mathrm{r3}\!\downarrow\}\\
\exists y_1(\forall x_1 P(x_1)\vee\bar{P}(y_1))\vee\exists y_2(\forall x_2 P(x_2)\vee\bar{P}(y_2))
\end{array}}{\exists y(\forall x P(x)\vee\bar{P}(y))}
$$

$$
\exists\,\dfrac{\varepsilon\,\dfrac{=\dfrac{\mathbf{t}}{\forall x\boxed{\mathrm{i}\!\downarrow\dfrac{\mathbf{t}}{P(x)\vee\bar{P}(x)}}}}{\forall x P(x)\vee\bar{P}(\varepsilon_y\bar{P}(y))}}{\exists y(\forall x P(x)\vee\bar{P}(y))}
$$

Herbrand disjunction:

$$\forall x_1\forall x_2(P(x_1)\vee\bar{P}(c)\vee P(x_2)\vee\bar{P}(x_1))$$

Falsifier disjunction:

$$\forall x P(x)\vee\bar{P}(\varepsilon_y\bar{P}(y))$$

Example: The Drinker Paradox

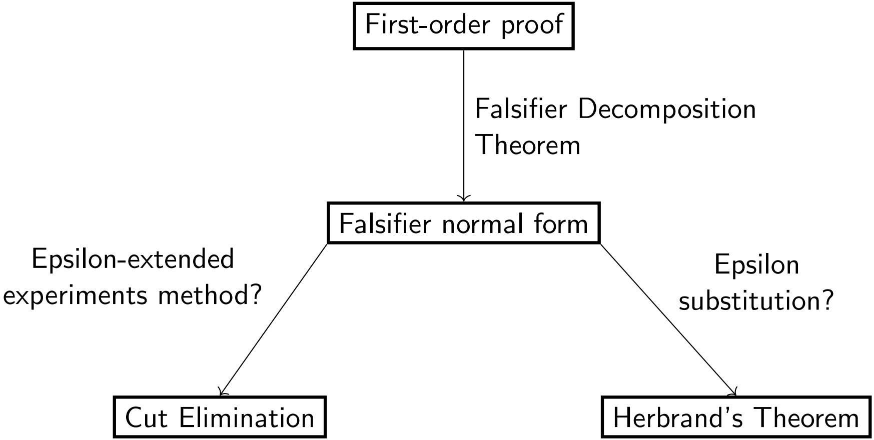
$$\dfrac{\dfrac{\mathbf{t}}{P(\varepsilon_x \overline{P}(x)) \vee \overline{P}(\varepsilon_x \overline{P}(x))}\ \text{i}\!\downarrow}{P(\varepsilon_x \overline{P}(x)) \vee \overline{P}(\varepsilon_y (P(\varepsilon_x \overline{P}(x)) \vee \overline{P}(y)))}\ CA$$

$$\dfrac{\dfrac{\dfrac{\mathbf{t}}{\forall x \boxed{\dfrac{\mathbf{t}}{P(x) \vee \overline{P}(x)}\ \text{i}\!\downarrow}}\ =}{\forall x P(x) \vee \overline{P}(\varepsilon_y \overline{P}(y))}\ \varepsilon}{\exists y (\forall x P(x) \vee \overline{P}(y))}\ \exists$$

$$\boxed{\dfrac{A(t)}{A(\varepsilon_x A(x))}\ CA}$$

$$\boxed{\begin{array}{l} \exists x A(x) \equiv A(\varepsilon_x A(x)) \\ \forall x A(x) \equiv A(\varepsilon_x \overline{A}(x)) \end{array}}$$

Ongoing Work: Falsifiers as an Intermediate Between Herbrand's Theorem and Cut Elimination



Conclusion and ε-agitprop

- A new approach to the epsilon-calculus, guided by considerations of complexity and normalisation

Conclusion and ε-agitprop

- A new approach to the epsilon-calculus, guided by considerations of complexity and normalisation

- A new decomposition theorem for first-order proofs, which does not fully separate the first-order and propositional parts

Conclusion and ε-agitprop

- A new approach to the epsilon-calculus, guided by considerations of complexity and normalisation
- A new decomposition theorem for first-order proofs, which does not fully separate the first-order and propositional parts
- Expanding the language of the predicate calculus by epsilon-terms yields:
  - improved normalisation properties of quantifier-shifts
  - termination of case analysis extraction
  - better understanding of the speedups yielded by quantifier-shifts
  - syntax for expressing non-constructive behaviour of existential witnesses