Synthetic connectives and their proof theory

Dale Miller

INRIA & Ecole Polytechnique

21 July 2011

14th International Congress of Logic, Methodology and Philosophy of Science, Nancy, France, 19-26 July 2011

Section C: Methodological and Philosophical Issues of Particular Sciences

Subsection C1: Logic, Mathematics and Computer Science.

Interests in the sequent calculus

For mathematical logic:

- Gentzen's proof of consistency of first order logics and Peano Arithmetic. Ordinal analysis.

For logic more generally:

- One of several frameworks for describing proofs in many logics.

For computer science:

- A framework for computing (*a la* proof search), model checking, and theorem proving.

Two early attempts at Unity in Logic

Gentzen's sequent calculi (LJ/LK)

- classical and intuitionistic logic differed by restriction on structural rules on the right of the sequent arrow.
- One cut-elimination procedure worked for both logics.

Church's Simple Theory of Types (STT)

- One framework for propositional, first-order, and higher-order logics.

Their combination provides a framework that accounts for a great deal computation logic ...

Two early attempts at Unity in Logic

Gentzen's sequent calculi (LJ/LK)

- classical and intuitionistic logic differed by restriction on structural rules on the right of the sequent arrow.
- One cut-elimination procedure worked for both logics.

Church's Simple Theory of Types (STT)

- One framework for propositional, first-order, and higher-order logics.

Their combination provides a framework that accounts for a great deal computation logic ...

... but the sequent calculus is too "unstructured" for immediate employment in computer science.

A quick primer on the sequent calculus

Sequents are pairs $\Gamma \vdash \Delta$ where

- Γ, the *left-hand-side*, is a multiset of formulas; and
- Δ, the *right-hand-side*, is a multiset of formulas.

N.B. Gentzen used lists instead of multisets.

Inference rules: two structural rules

There are two sets of these: *contraction, weakening*.

$$\frac{\Gamma, B, B \vdash \Delta}{\Gamma, B \vdash \Delta}\ cL \qquad \frac{\Gamma \vdash \Delta, B, B}{\Gamma \vdash \Delta, B}\ cR$$

$$\frac{\Gamma \vdash \Delta}{\Gamma, B \vdash \Delta}\ wL \qquad \frac{\Gamma \vdash \Delta}{\Gamma \vdash \Delta, B}\ wR$$

N.B. Gentzen's use of lists of formulas required him to also have an *exchange* rule.

Inference rules: two identity rules

There are exactly two identity rules: *initial, cut*.

$$\frac{}{B \vdash B}\ init \qquad \frac{\Gamma_1 \vdash \Delta_1, B \qquad B, \Gamma_2 \vdash \Delta_2}{\Gamma_1, \Gamma_2 \vdash \Delta_1, \Delta_2}\ cut$$

Notice the repeated use of the variable B in these rules.

In general: all instances of both of these rules can be *eliminated* except for *init* when B is atomic.

In arithmetic, where all predicates are defined, *init* can be eliminated too.

Inference rules: introduction rules (some examples)

$$\frac{\Gamma, B_i \vdash \Delta}{\Gamma, B_1 \wedge B_2 \vdash \Delta}\ \wedge L \qquad \frac{\Gamma \vdash \Delta, B \qquad \Gamma \vdash \Delta, C}{\Gamma \vdash \Delta, B \wedge C}\ \wedge R$$

$$\frac{\Gamma, B \vdash \Delta \qquad \Gamma, C \vdash \Delta}{\Gamma, B \vee C \vdash \Delta}\ \vee L \qquad \frac{\Gamma \vdash \Delta, B_i}{\Gamma \vdash \Delta, B_1 \vee B_2}\ \vee R$$

$$\frac{\Gamma_1 \vdash \Delta_1, B \qquad \Gamma_2, C \vdash \Delta_2}{\Gamma_1, \Gamma_2, B \supset C \vdash \Delta_1, \Delta_2}\ \supset L \qquad \frac{\Gamma, B \vdash \Delta, C}{\Gamma \vdash \Delta, B \supset C}\ \supset R$$

$$\frac{\Gamma, B[t/x] \vdash \Delta}{\Gamma, \forall x\, B \vdash \Delta}\ \forall L \qquad \frac{\Gamma \vdash \Delta, B[y/x]}{\Gamma \vdash \Delta, \forall x\, B}\ \forall R\dagger$$

$$\frac{\Gamma, B[y/x] \vdash \Delta}{\Gamma, \exists x\, B \vdash \Delta}\ \exists L\dagger \qquad \frac{\Gamma \vdash \Delta, B[t/x]}{\Gamma \vdash \Delta, \exists x\, B}\ \exists R$$

Permutations of inference rules

$$\dfrac{\dfrac{\Gamma, p, r \vdash s, \Delta \qquad \Gamma, q, r \vdash s, \Delta}{\Gamma, p \vee q, r \vdash s, \Delta}\ \vee L}{\Gamma, p \vee q \vdash r \supset s, \Delta}\ \supset R$$

$$\dfrac{\dfrac{\Gamma, p, r \vdash s, \Delta}{\Gamma, p \vdash r \supset s, \Delta}\ \supset R \qquad \dfrac{\Gamma, q, r \vdash s, \Delta}{\Gamma, q \vdash r \supset s, \Delta}\ \supset R}{\Gamma, p \vee q \vdash r \supset s, \Delta}\ \vee L$$

Provability defined

A **C**-proof (*classical proof*) is any proof using these inference rules.

An **I**-proof (*intuitionistic proof*) is a **C**-proof in which the right-hand side of all sequents contain either 0 or 1 formula.

Let Δ be a finite set of formulas and let B be a formula.

Write $\Delta \vdash_C B$ and $\Delta \vdash_I B$ if the sequent $\Delta \longrightarrow B$ has, respectively, a **C**-proof or an **I**-proof.

Cut elimination

Theorem. If a sequent has a **C**-proof (respectively, **I**-proof) then it has a cut-free **C**-proof (respectively, **I**-proof).

This theorem was stated and proved by Gentzen 1935.

Gentzen invented the sequent calculus so that he could formulate one proof of this *Hauptsatz* for both classical *and* intuitionistic logic.

Structural rules are used to describe the difference between these logics.

There are many other ways to describe the difference between them (excluded middle, constructive vs non-constructive, Kripke semantics, etc).

Consequences of cut elimination

Theorem. Logic is consistency: It is impossible for there to be a proof of B and $\neg B$.

Proof. Assume that $\vdash B$ and $B \vdash$ have proofs. By cut, $\vdash$ has a proof. Thus, it also has a cut-free proof, but this is impossible.

Theorem. A cut-free proof system of a sequent is composed only of subformula of formulas in the root sequent.

Proof. Simple inspection of all rules other than cut. (Assuming first-order quantification here.)

Should I eliminate cuts in general?

Consequences of cut elimination

Theorem. Logic is consistency: It is impossible for there to be a proof of B and $\neg B$.

Proof. Assume that $\vdash B$ and $B \vdash$ have proofs. By cut, $\vdash$ has a proof. Thus, it also has a cut-free proof, but this is impossible.

Theorem. A cut-free proof system of a sequent is composed only of subformula of formulas in the root sequent.

Proof. Simple inspection of all rules other than cut. (Assuming first-order quantification here.)

Should I eliminate cuts in general? **NO!** Cut-free proofs of interesting mathematical statement often do not exists in nature.

If you are using cut-free proofs, you are probably modeling computation or model checking.

Addressing various choices doing proof search

Issue 1: The cut-rule can always be chosen.
Solution: Search for only cut-free proofs. Or build next generation theorem provers than can pick lemmas...

Addressing various choices doing proof search

Issue 1: The cut-rule can always be chosen.
Solution: Search for only cut-free proofs. Or build next generation theorem provers than can pick lemmas...

Issue 2: The structural rules of weakening and contraction can be applied (almost) anytime.
Solution: Build these rules into the other rules.

Addressing various choices doing proof search

Issue 1: The cut-rule can always be chosen.
Solution: Search for only cut-free proofs. Or build next generation theorem provers than can pick lemmas...

Issue 2: The structural rules of weakening and contraction can be applied (almost) anytime.
Solution: Build these rules into the other rules.

Issue 3: What term to use in the $\exists$R and $\forall$L rules?
Solution: Use logic variables and unification (standard theorem proving technology).

Addressing various choices doing proof search

Issue 1: The cut-rule can always be chosen.
Solution: Search for only cut-free proofs. Or build next generation theorem provers than can pick lemmas...

Issue 2: The structural rules of weakening and contraction can be applied (almost) anytime.
Solution: Build these rules into the other rules.

Issue 3: What term to use in the $\exists$R and $\forall$L rules?
Solution: Use logic variables and unification (standard theorem proving technology).

Issue 4: Of the thousands of non-atomic formulas in a sequent, which should be selected for introduction?
Solution:

Addressing various choices doing proof search

Issue 1: The cut-rule can always be chosen.
Solution: Search for only cut-free proofs. Or build next generation theorem provers than can pick lemmas...

Issue 2: The structural rules of weakening and contraction can be applied (almost) anytime.
Solution: Build these rules into the other rules.

Issue 3: What term to use in the $\exists$R and $\forall$L rules?
Solution: Use logic variables and unification (standard theorem proving technology).

Issue 4: Of the thousands of non-atomic formulas in a sequent, which should be selected for introduction?
Solution: Good question. We concentrate on this issue next using

focused proof systems. .

Some "focusing" behavior

Given the inference figure (a variant of $\supset$L), where A is atomic.

$$\frac{\Gamma \longrightarrow G \qquad \Gamma, D \overset{\Xi}{\longrightarrow} A}{\Gamma \longrightarrow A}\text{, provided } G \supset D \in \Gamma$$

can we restrict the last inference rule in Ξ?

In intuitionistic logic, we can insist that Ξ ends with either

- an introduction rule for D (if D is not atomic) or
- an initial rule with $A = D$ (if D is atomic).

Backchaining as focusing behavior

Let D be the formula (for atomic A')

$$\forall\bar{x}_1(G_1 \supset \forall\bar{x}_2(G_2 \supset \cdots \forall\bar{x}_n(G_n \supset A')\ldots))$$

and consider the sequent $\Gamma, D \vdash A$, for atomic A.

We can insist that if one applies a left introduction rule on D, then that choice cascades into a series of $\forall$L, $\supset$L, and initial rule.

$$\frac{\Gamma, D \vdash G_1\theta \quad \cdots \quad \Gamma, D \vdash G_n\theta \qquad A = A'\theta}{\Gamma, D \vdash A}\ \textit{backchain}$$

If we have only $\forall$ and $\supset$, then this rule schema can *replace* all left-introduction rules.

This cascade of introduction rules is called a *focus*.

Backward and forward chaining

$$\frac{\Gamma \longrightarrow a \qquad \Gamma, b \longrightarrow G}{\Gamma, a \supset b \longrightarrow G} \; a, b \text{ are atoms, focus on } a \supset b$$

Negative atoms: The right branch is trivial; i.e., $b = G$. Continue with $\Gamma \longrightarrow a$ (backward chaining).
Positive atoms: The left branch is trivial; i.e., $\Gamma = \Gamma', a$. Continue with $\Gamma', a, b \longrightarrow G$ (forward chaining).

Let Γ contain $fib(0,0)$, $fib(1,1)$, and

$$\forall n \forall f \forall f' [fib(n,f) \supset fib(n+1,f') \supset fib(n+2, f+f')].$$

The nth Fibonacci number is F iff $\Gamma \vdash fib(n, F)$. What's its complexity?

Backward and forward chaining

$$\frac{\Gamma \longrightarrow a \qquad \Gamma, b \longrightarrow G}{\Gamma, a \supset b \longrightarrow G} \quad a, b \text{ are atoms, focus on } a \supset b$$

Negative atoms: The right branch is trivial; i.e., $b = G$. Continue with $\Gamma \longrightarrow a$ (backward chaining).

Positive atoms: The left branch is trivial; i.e., $\Gamma = \Gamma', a$. Continue with $\Gamma', a, b \longrightarrow G$ (forward chaining).

Let Γ contain $fib(0, 0)$, $fib(1, 1)$, and

$$\forall n \forall f \forall f' [fib(n, f) \supset fib(n + 1, f') \supset fib(n + 2, f + f')].$$

The nth Fibonacci number is F iff $\Gamma \vdash fib(n, F)$. What's its complexity?
If $fib(\cdot, \cdot)$ is negative then the unique proof is *exponential* in n.
If $fib(\cdot, \cdot)$ is positive then the shortest proof is *linear* in n.

Various focusing-like proof system

Uniform proofs [M, Nadathur, Scedrov, 1987] describes goal-directed search and backchaining (in higher-order logic).

LLF: [Andreoli, 1992]: a focused proof system for linear logic.

LKT/LKQ/LK$^\eta$: focusing systems for classical logic [Danos, Joinet, Schellinx,1993]

LJQ [Herbelin, 1995] permits forward-chaining proof. *LJQ'* [Dyckhoff & Lengrand, 2007] extends it.

λRCC [Jagadeesan, Nadathur, Saraswat, 2005] mixes forward chaining and backward chaining (in a subset of intuitionistic logic).

LJF [Liang & M, 2009] allows forward and backward proof in all of intuitionistic logic. LJT, LJQ, λRCC, and LJ are subsystems.

LKF (following) provides focusing for all of classical logic.

Invertible rules and the negative phase

Some inference rules are *invertible*, *e.g.*,

$$\frac{A, \Gamma \longrightarrow B}{\Gamma \longrightarrow A \supset B} \qquad \frac{\Gamma \longrightarrow A \qquad \Gamma \longrightarrow B}{\Gamma \longrightarrow A \wedge B} \qquad \frac{\Gamma \longrightarrow B[y/x]}{\Gamma \longrightarrow \forall x.B}$$

First focusing principle: when proving a sequent, apply invertible rules exhaustively and in any order.

This is the *negative phase* of proof search: if formulas are "processes" in an "environment," then these formulas "evolve" without communications ("asynchronously") with the environment.

Non-invertible rules and the positive phase

Some inference rules are not generally invertible, *e.g.*,

$$\frac{\Gamma_1 \longrightarrow A \quad \Gamma_2 \longrightarrow B}{\Gamma_1, \Gamma_2 \longrightarrow A \wedge B} \qquad \frac{\Gamma \longrightarrow B[t/x]}{\Gamma \longrightarrow \exists x.B}$$

Some *backtracking* is generally necessary within proof search using these inference rules.

Second focusing principle: non-invertible rules are applied in a "chain-like" fashion.

This is the *positive phase* of proof search.

Extending the neg/pos distinction to atoms

Focusing proof systems extend the neg/pos distinction to atoms but this extension is *arbitrary*.

We shall assume that all atoms are assigned a *bias*, that is, they are either positive or negative.

A *positive formula* is either a positive atom or has a top-level connective whose right-introduction rule is not invertible.

A *negative formula* is either a negative atom or has a top-level connective whose right-introduction rules is invertible.

The full picture behind focusing

Andreoli (1992) was the first to give a focused proof system for a full logic (linear logic).

The proof system for MALL (multiplicative-additive linear logic) is remarkably elegant and unambiguous.

Some complexity arises from using the exponentials (!, ?): in particular, exponentials terminate focusing phases.

We present two focused proof systems:

- LKF for *classical logic*
- LKF extended with *fixed points* and *equality* (arithmetic).

Classical logic and one-sided sequents

Two conventions for dealing with classical logic.

- Formulas are in *negation normal form*.
  - $B \supset C$ is replaced with $\neg B \vee C$,
  - negations are pushed to the atoms
- Sequents will be one-sided. In particular, the two sided sequent

$$B_1, \ldots, B_n \vdash C_1, \ldots, C_m$$

will be converted to

$$\vdash \neg B_1, \ldots, \neg B_n, C_1, \ldots, C_m.$$

LKF: Focusing for Classical Logic

Formulas are *polarized* as follows.

- atoms are assigned bias (either $+$ or $-$), and
- $\wedge$ $\vee$, t, and f are annotated with either $+$ or $-$.
  Thus: $\wedge^-$, $\wedge^+$, $\vee^-$, $\vee^+$, t^-, t^+, f^-, f^+.

LKF is a focused, one-sided sequent calculus with the sequents

$$\vdash \Theta \Uparrow \Gamma \qquad \text{and} \qquad \vdash \Theta \Downarrow B$$

Here, Θ is a multiset of positive formulas and negative literals, Γ is a multiset of formulas, and B is a formula.

LKF : focused proof systems for classical logic

$$\frac{}{\vdash \Theta \Uparrow \Gamma, t^-} \qquad \frac{\vdash \Theta \Uparrow \Gamma, A \qquad \vdash \Theta \Uparrow \Gamma, B}{\vdash \Theta \Uparrow \Gamma, A \wedge^- B}$$

$$\frac{\vdash \Theta \Uparrow \Gamma}{\vdash \Theta \Uparrow \Gamma, f^-} \qquad \frac{\vdash \Theta \Uparrow \Gamma, A, B}{\vdash \Theta \Uparrow \Gamma, A \vee^- B} \qquad \frac{\vdash \Theta \Uparrow \Gamma, A[y/x]}{\vdash \Theta \Uparrow \Gamma, \forall x A}$$

LKF : focused proof systems for classical logic

$$\frac{}{\vdash \Theta \Uparrow \Gamma, t^-} \qquad \frac{\vdash \Theta \Uparrow \Gamma, A \qquad \vdash \Theta \Uparrow \Gamma, B}{\vdash \Theta \Uparrow \Gamma, A \wedge^- B}$$

$$\frac{\vdash \Theta \Uparrow \Gamma}{\vdash \Theta \Uparrow \Gamma, f^-} \qquad \frac{\vdash \Theta \Uparrow \Gamma, A, B}{\vdash \Theta \Uparrow \Gamma, A \vee^- B} \qquad \frac{\vdash \Theta \Uparrow \Gamma, A[y/x]}{\vdash \Theta \Uparrow \Gamma, \forall x A}$$

$$\frac{}{\vdash \Theta \Downarrow t^+} \qquad \frac{\vdash \Theta \Downarrow A \qquad \vdash \Theta \Downarrow B}{\vdash \Theta \Downarrow A \wedge^+ B} \qquad \frac{\vdash \Theta \Downarrow A_i}{\vdash \Theta \Downarrow A_1 \vee^+ A_2} \qquad \frac{\vdash \Theta \Downarrow A[t/x]}{\vdash \Theta \Downarrow \exists x A}$$

LKF : focused proof systems for classical logic

$$\frac{}{\vdash \Theta \Uparrow \Gamma, t^-} \qquad \frac{\vdash \Theta \Uparrow \Gamma, A \qquad \vdash \Theta \Uparrow \Gamma, B}{\vdash \Theta \Uparrow \Gamma, A \wedge^- B}$$

$$\frac{\vdash \Theta \Uparrow \Gamma}{\vdash \Theta \Uparrow \Gamma, f^-} \qquad \frac{\vdash \Theta \Uparrow \Gamma, A, B}{\vdash \Theta \Uparrow \Gamma, A \vee^- B} \qquad \frac{\vdash \Theta \Uparrow \Gamma, A[y/x]}{\vdash \Theta \Uparrow \Gamma, \forall x A}$$

$$\frac{}{\vdash \Theta \Downarrow t^+} \qquad \frac{\vdash \Theta \Downarrow A \qquad \vdash \Theta \Downarrow B}{\vdash \Theta \Downarrow A \wedge^+ B} \qquad \frac{\vdash \Theta \Downarrow A_i}{\vdash \Theta \Downarrow A_1 \vee^+ A_2} \qquad \frac{\vdash \Theta \Downarrow A[t/x]}{\vdash \Theta \Downarrow \exists x A}$$

Init	Store	Release	Decide
$\dfrac{}{\vdash \neg P_a, \Theta \Downarrow P_a}$	$\dfrac{\vdash \Theta, C \Uparrow \Gamma}{\vdash \Theta \Uparrow \Gamma, C}$	$\dfrac{\vdash \Theta \Uparrow N}{\vdash \Theta \Downarrow N}$	$\dfrac{\vdash P, \Theta \Downarrow P}{\vdash P, \Theta \Uparrow \cdot}$

P positive; P_a positive literal; N negative;
C positive formula or negative literal.

About the structural rules in LKF

The only form of *contraction* is in the Decide rule

$$\frac{\vdash P, \Theta \Downarrow P}{\vdash P, \Theta \Uparrow \cdot}$$

The only occurrence of *weakening* is in the Init rule.

$$\frac{}{\vdash \neg P_a, \Theta \Downarrow P_a}$$

Thus negative non-atomic formulas are treated *linearly* (in the sense of linear logic).

Only positive formulas are contracted.

Results about LKF

Let B be a first-order logic formula and let $\hat{B}$ result from B by placing $+$ or $-$ on t, f, $\wedge$, and $\vee$ (there are exponentially many such placements).

Theorem. B is a first-order theorem if and only if $\hat{B}$ has an LKF proof. [Liang & M, TCS 2009]

Different polarizations do not change *provability* but can radically change *proofs*.

Recall the Fibonacci series example: an exponential time algorithm or a linear time algorithm depending only on bias assignment for atoms.

The abstraction behind focused proofs

If we ignore the internal structure of phases and consider only their boundaries, then we have moved from *micro-rules* (introduction rules) to *macro-rules* (pos or neg phases).

The *decide depth* of an LKF proofs is the maximum number of *Decide* rules along any path starting from the end-sequent.

This measurement counts “bi-poles”: one positive phase followed by a negative phase.

An example

Let a, b, c be positive atoms and let Θ contain the formula $a \wedge^+ b \wedge^+ \neg c$.

$$
\dfrac{\dfrac{}{\vdash \Theta \Downarrow a}\ \mathit{Init} \quad \dfrac{}{\vdash \Theta \Downarrow b}\ \mathit{Init} \quad \dfrac{\dfrac{\vdash \Theta, \neg c \Uparrow \cdot}{\vdash \Theta \Uparrow \neg c}}{\vdash \Theta \Downarrow \neg c}\ \mathit{Release}}{\dfrac{\vdash \Theta \Downarrow a \wedge^+ b \wedge^+ \neg c}{\vdash \Theta \Uparrow \cdot}\ \mathit{Decide}}\ \mathit{and}
$$

This derivation is possible iff Θ is of the form $\neg a, \neg b, \Theta'$. Thus, the "macro-rule" is

$$
\frac{\vdash \neg a, \neg b, \neg c, \Theta' \Uparrow \cdot}{\vdash \neg a, \neg b, \Theta' \Uparrow \cdot}
$$

Two certificates for propositional logic: negative

Use $\wedge^-$ and $\vee^-$. Their introduction rules are invertible. The initial "macro-rule" is huge, having all the clauses in the conjunctive normal form of B as premises.

$$
\dfrac{\cdots \qquad \dfrac{\dfrac{}{\vdash L_1, \ldots, L_n \Downarrow L_i}\ \mathit{Init}}{\vdash L_1, \ldots, L_n \Uparrow \cdot}\ \mathit{Decide} \qquad \cdots}{\dfrac{\vdots}{\vdash \cdot \Uparrow B}}
$$

A proof "certificate" can specify the complementary literals for each premise or it can ask the checker to *search* for such pairs.

Proof certificates can be tiny but require exponential time for checking.

Of course, good proofs contain “information”

Let B be a propositional formula with a large conjunctive normal form.

Consider the tautology $C = (p \vee B) \vee \neg p$.

A *negative focused proof* computes the conjunctive normal form of C and then observing that each disjunct contains p and $\neg p$.

The use of positive polarities allows us to provide a more clever proof.

Two certificates for propositional logic: positive

Below is a proof involving positive biased connectives.

$$
\begin{prooftree}
\AxiomC{}
\UnaryInfC{$\vdash (p \vee^+ B) \vee^+ \neg p, \neg p \Downarrow p$}
\doubleLine
\RightLabel{${\color{blue}\ast}$}
\UnaryInfC{$\vdash (p \vee^+ B) \vee^+ \neg p, \neg p \Downarrow (p \vee^+ B) \vee^+ \neg p$}
\RightLabel{Decide}
\UnaryInfC{$\vdash (p \vee^+ B) \vee^+ \neg p, \neg p \Uparrow \cdot$}
\UnaryInfC{$\vdash (p \vee^+ B) \vee^+ \neg p \Uparrow \neg p$}
\UnaryInfC{$\vdash (p \vee^+ B) \vee^+ \neg p \Downarrow \neg p$}
\RightLabel{${\color{blue}\ast}$}
\UnaryInfC{$\vdash (p \vee^+ B) \vee^+ \neg p \Downarrow (p \vee^+ B) \vee^+ \neg p$}
\RightLabel{Decide}
\UnaryInfC{$\vdash (p \vee^+ B) \vee^+ \neg p \Uparrow \cdot$}
\UnaryInfC{$\vdash \cdot \Uparrow (p \vee^+ B) \vee^+ \neg p$}
\end{prooftree}
$$

Clever choices $\ast$ are injected twice. The structure of B is avoided.

Herbrand's Theorem is a simple corollary

Herbrand's Theorem.
Let B be a quantifier-free first-order formula. $\exists\bar{x}.B$ is a theorem if and only if there is an $n \geq 1$ and substitutions $\theta_1, \ldots, \theta_n$ such that $B\theta_1 \vee \cdots \vee B\theta_n$ is tautologous.

This theorem is easily proved by the completeness of LKF.

- Polarize the propositional connectives all negatively.
- Replace *Decide* on $\exists\bar{x}.B$ followed by substitution $\theta_i B$ with a *Decide* on $B\theta_1 \vee^+ \cdots \vee^+ B\theta_n$ and select $\theta_i B$.
- The rest of the macro-level inference rules are unchanged.

Arithmetic via equality and fixed points

We shall add

- first-order *term equality* and
- *fixed points* (for recursive definitions)

We follow developments by Girard [1992], Schroeder-Heister [1993], and Baelde, McDowell, M, & Tiu [1996-2008].

Both equality ($=$, $\neq$) and fixed point definition (μ, ν) are *logical connectives:* that is, they are defined by introduction rules.

Equality as logical connective

Introductions rules

$$\frac{}{\vdash \Theta \Downarrow t = t} \qquad \frac{}{\vdash \Theta \Uparrow \Gamma, s \neq t}\ \ddagger \qquad \frac{\vdash \Theta\sigma \Uparrow \Gamma\sigma}{\vdash \Theta \Uparrow \Gamma, s \neq t}\ \dagger$$

$\ddagger$ s and t are not unifiable.
$\dagger$ s and t to be unifiable and σ to be their mgu

N.B. Unification was used before to *implement* inference rules: here, unification is in the *definition* of the rule.

Some theorems about equality

Equality is an equivalence relation...

- $\forall x\ [x = x]$
- $\forall x, y\ [x = y \supset y = x]$
- $\forall x, y, z\ [x = y \wedge y = z \supset x = z]$

and a congruence.

- $\forall x, y\ [x = y \supset (f\ x) = (f\ y)]$
- $\forall x, y\ [x = y \supset (p\ x) \supset (p\ y)]$

Let 0 denote zero and s denote successor.

- $\forall x\ [0 \neq (s\ x)]$
- $\forall x, y\ [(s\ x) = (s\ y) \supset x = y]$

A hint of model checking

Encode a non-empty set of first order terms $S = \{s_1, \ldots, s_n\}$ $(n \geq 1)$ as the one-place predicate

$$\hat{S} = [\lambda x.\ x = s_1 \vee^+ \cdots \vee^+ x = s_n]$$

If S is empty, then define $\hat{S}$ to be $[\lambda x.\ f^+]$. Notice that

$$s \in S \quad \text{if and only if} \quad \vdash\ \hat{S}\ s.$$

A hint of model checking

Encode a non-empty set of first order terms $S = \{s_1, \ldots, s_n\}$ $(n \geq 1)$ as the one-place predicate

$$\hat{S} = [\lambda x.\ x = s_1 \vee^+ \cdots \vee^+ x = s_n]$$

If S is empty, then define $\hat{S}$ to be $[\lambda x.\ f^+]$. Notice that

$$s \in S \quad \text{if and only if} \quad \vdash\ \hat{S}\ s.$$

The statement

$$\forall x \in \{s_1, \ldots, s_n\}.P(x) \quad \text{becomes} \quad \forall x.[\hat{S}x \supset Px].$$

$$\cfrac{\cfrac{\vdash P(s_1) \Uparrow \cdot}{\vdash P(x) \Uparrow x \neq s_1} \qquad \cdots \qquad \cfrac{\vdash P(s_n) \Uparrow \cdot}{\vdash P(x) \Uparrow x \neq s_n}}{\vdash \cdot \Uparrow \forall x.[x \neq s_1 \wedge^- \cdots \wedge^- x \neq s_n] \vee^- P(x)}$$

Fixed Points as connectives

The *fixed points* operators μ and ν are De Morgan duals and simply unfold.

$$\frac{\vdash \Theta \Uparrow \Gamma, B(\nu B)\bar{t}}{\vdash \Theta \Uparrow \Gamma, \nu B\bar{t}} \qquad \frac{\vdash \Theta \Downarrow B(\mu B)\bar{t}}{\vdash \Theta \Downarrow \mu B\bar{t}}$$

B is a formula with $n \geq 0$ variables abstracted; $\bar{t}$ is a list of n terms.

μ and ν denotes neither the least nor the greatest fixed point. That distinction arises if we add the rules of induction and co-induction.

Examples of fixed points

Natural numbers: terms over 0 for zero and s for successor. Two ways to define predicates over numbers.

$$\begin{array}{rcl} nat\ 0 & \texttt{:-} & true. \\ nat\ (s\ X) & \texttt{:-} & nat\ X. \\ leq\ 0\ Y & \texttt{:-} & true. \\ leq\ (s\ X)\ (s\ Y) & \texttt{:-} & leq\ X\ Y. \end{array}$$

These logic programs can be given as fixed point expressions.

$$nat = \mu(\lambda p \lambda x.(x = 0) \vee^+ \exists y.(s\ y) = x \wedge^+ p\ y)$$

$$leq = \mu(\lambda q \lambda x \lambda y.(x = 0) \vee^+ \exists u \exists v.(s\ u) = x \wedge^+ (s\ v) = y \wedge^+ q\ u\ v).$$

Horn clause specifications correspond to *purely positive* fixed points (mutual recursions requires standard encoding techniques).

Putting computation into an inference rule

Consider proving the positive focused sequent

$$\vdash \Theta \Downarrow (leq\ m\ n \wedge^+ N_1) \vee^+ (leq\ n\ m \wedge^+ N_2),$$

where m, n are natural numbers and N_1, N_2 are negative formulas.
There are exactly two possible macro rules:

$$\frac{\vdash \Theta \Downarrow N_1}{\vdash \Theta \Downarrow (leq\ m\ n \wedge^+ N_1) \vee^+ (leq\ n\ m \wedge^+ N_2)}\ \text{for } m \leq n$$

$$\frac{\vdash \Theta \Downarrow N_2}{\vdash \Theta \Downarrow (leq\ m\ n \wedge^+ N_1) \vee^+ (leq\ n\ m \wedge^+ N_2)}\ \text{for } n \leq m$$

A macro inference rule can contain an entire Prolog-style computation.

Example: One step transitions in CCS

As inference rules in SOS (structured operational semantics):

$$\frac{}{A.P \xrightarrow{A} P} \qquad \frac{P \xrightarrow{A} R}{P + Q \xrightarrow{A} R} \qquad \frac{Q \xrightarrow{A} R}{P + Q \xrightarrow{A} R}$$

$$\frac{P \xrightarrow{A} P'}{P|Q \xrightarrow{A} P'|Q} \qquad \frac{Q \xrightarrow{A} Q'}{P|Q \xrightarrow{A} P|Q'}$$

These can be written as Prolog clauses and as a fixed point definition for the three place predicate $\cdot \xrightarrow{\cdot} \cdot$

Example: a proof system for simulation

Consider proofs involving simulation.

$$sim\ P\ Q \ \equiv\ \forall P' \forall A[\ P \xrightarrow{A} P' \supset \exists Q'\ [Q \xrightarrow{A} Q' \wedge sim\ P'\ Q'\ ]].$$

Here, $P \xrightarrow{A} P'$ is a purely positive fixed point expression.

The definition of simulation is exactly two "macro connectives".

- $\forall P' \forall A[P \xrightarrow{A} P' \supset \cdot\ ]$ is a negative "macro connective". There are no choices in expanding this macro rule.
- $\exists Q'[Q \xrightarrow{A} Q' \wedge^{+} \cdot\ ]$ is a positive "macro connective". There can be choices for continuation Q'.

These macro-rules now match exactly the sense of simulation (similar also to winning strategies).

Maximal multifocusing

Allowing multiple foci is a trivial extension:

$$\frac{\vdash \Delta, \Theta \Downarrow \Delta}{\vdash \Delta, \Theta \Uparrow \cdot}$$

where Δ is a non-empty multiset of positive formulas.

This rule allows modeling “parallel actions” in proofs. Instead of just $\alpha \;;\; \beta$ and $\beta \;;\; \alpha$, we also have $\alpha \mid \beta$.

Maximal multifocusing leads to natural candidates for canonical proof structures: e.g., proof nets for MALL [Chaudhuri, M, Saurin, 2008].

Future work: broad spectrum proof certificates

Sequent calculus and focusing proof systems provide:

- The *atoms* of inference (the introduction rules)
- The structure of focusing provides us with the *rules of chemistry*: which atoms stick together and which do not.
- Engineered proofs system can be made form *molecules* of inference.

Future work: broad spectrum proof certificates

Sequent calculus and focusing proof systems provide:

- The *atoms* of inference (the introduction rules)
- The structure of focusing provides us with the *rules of chemistry*: which atoms stick together and which do not.
- Engineered proofs system can be made form *molecules* of inference.

An approach to a general notion of *proof certificate*:

- The world's provers print their proof evidence using appropriately engineered molecules of inference.
- A universal proof checker implements only the atoms of inference and the rules of chemistry.

Future work: broad spectrum proof certificates

Sequent calculus and focusing proof systems provide:

- The *atoms* of inference (the introduction rules)
- The structure of focusing provides us with the *rules of chemistry*: which atoms stick together and which do not.
- Engineered proofs system can be made form *molecules* of inference.

An approach to a general notion of *proof certificate*:

- The world's provers print their proof evidence using appropriately engineered molecules of inference.
- A universal proof checker implements only the atoms of inference and the rules of chemistry.

See the two recent draft submissions:

- "Communicating and trusting proofs: The case for broad spectrum proof certificates"
- "A proposal for broad spectrum proof certificates"

The end

Thank you