A proof theory for model checking

Dale Miller

Inria Saclay & LIX, École Polytechnique
Palaiseau, France

Online Worldwide Seminar on Logic and Semantics (OWLS)
10 May 2021

Based on a paper co-authored with Q. Heath in the
Journal of Automated Reasoning, 2019.

Historically speaking

Model checking was introduced in the early 1980's as a way to establish properties about (concurrent) computer programs that were hard or impossible to do then using traditional, axiomatic proof techniques of Floyd and Hoare.

If you cannot prove a property, at least you can get help looking for counterexamples: e.g., a path to a state where two processes are both in their critical section.

Model checking was a reaction against theorem proving.

I will argue that model checking can, in fact, be given an appealing proof theoretical foundation.

Proof theoretical ingredients

Some historical high-points.

- Gentzen's sequent calculus [1935]
- Girard's linear logic [1987]
- Andreoli's focused proof system for linear logic [1991]
- Schroeder-Heister's and Girard's treatment of equality and fixed points [1992]
- Baelde, McDowell, M, and Tiu developed proof theory for least and greatest fixed points [1997-2012].

All these developments, except for the first, came after the start of model checking.

Why promote a proof theoretic framework?

Proof theory can provide certificates for model checking.

It provides a framework for integrating inductive theorem prover and model checking since they operate with the same (or similar) logics and proofs structures.

Generalizations of model checking are natural to consider: proof theory has no problem allowing states to be complex linguistic expressions, even with bindings (e.g., π-calculus).

It has proved valuable to provide a proof-theoretic framework for logic programming (going back to 1986). Maybe doing the same with model checking will also be valuable.

Two ways to move beyond MALL

A quick synopsis for the expert in linear logic:

MALL is a propositional logic without contraction and weakening: $\otimes, 1, \oplus, 0, \wp, \bot, \&, \top$. It is decidable.

1. Girard [1987] added the *exponentials* $(!, ?)$ to get linear logic.
2. Baelde and M [2007] added *fixed points* to get μMALL.

Goal: illustrate how (first-order) μMALL is better suited for model checkingthan linear logic.

Two ways to move beyond MALL

A quick synopsis for the expert in linear logic:

MALL is a propositional logic without contraction and weakening: $\otimes, 1, \oplus, 0, \wp, \bot, \&, \top$. It is decidable.

1. Girard [1987] added the *exponentials* $(!, ?)$ to get linear logic.
2. Baelde and M [2007] added *fixed points* to get μMALL.

Goal: illustrate how (first-order) μMALL is better suited for model checkingthan linear logic.

Note:

- Fixed point unfolding resembles contraction: $\mu B\bar{t} = B(\mu B)\bar{t}$.
- If B is *purely positive*, then $B \equiv !\, B$. In MALL: no interesting such formulas. In μMALL: a rich collection of such formulas.

What is an additive inference rule?

Truth is central to the way that model checking is understood. The notion of *additive* inference rules seem to be a treatment of truth.

- Linear logic provides examples of additive inference rules.
- Hintikka games provide another treatment: two player use a board containing one formula.
- No comma is needed in a sequent.
- etc

Instead of attempting a definition, we state four properties of a class of additive connectives that seem desirable to maintain.

Additive connectives

Let $\mathcal{A}$ be the set of formulas built from the propositional connectives $\{\wedge, \mathit{tt}, \vee, \mathit{ff}\}$ (no propositional constants included). The unit of $\wedge$ is tt and the unit of $\vee$ is ff.

Consider the proof system given by the following one-sided sequent calculus inference rules.

$$\frac{\vdash B_1, \Delta \quad \vdash B_2, \Delta}{\vdash B_1 \wedge B_2, \Delta} \qquad \frac{}{\vdash \mathit{tt}, \Delta} \qquad \frac{\vdash B_1, \Delta}{\vdash B_1 \vee B_2, \Delta} \qquad \frac{\vdash B_2, \Delta}{\vdash B_1 \vee B_2, \Delta}$$

Notice that $\vee$ has two introduction rules while ff has none.

The de Morgan duals are tt / $\wedge$ with ff / $\vee$. By $\neg B$ we mean the de Morgan dual of all connectives in B.

The multiset Δ is provable if and only if there is a proof of $\vdash \Delta$ using these inference rules.

Some properties of additive connectives

Let Δ, Δ' be multisets of $\mathcal{A}$-formulas and let B be an $\mathcal{A}$-formula.

Theorem (Strengthening)

If $\vdash \Delta$ *has a proof, then there is a* $B \in \Delta$ *such that* $\vdash B$.

Theorem (Weakening & contraction admissibility)

If $\Delta \subseteq \Delta'$ *and* $\vdash \Delta$ *is provable then* $\vdash \Delta'$ *is provable.*

Theorem (Initial admissibility)

$\vdash B, \neg B$ *is provable.*

Theorem (Cut admissibility)

If $\vdash B, \Delta$ *and* $\vdash \neg B, \Delta'$, *then* $\vdash \Delta, \Delta'$.

Truth-tables evaluation

These properties allow the following definition.

Define $v(\cdot) : \mathcal{A} \longrightarrow \{tt, ff\}$ such that

- $v(B) = tt$ if $\vdash B$ is provable and
- $v(B) = ff$ if $\vdash \neg B$ is provable.

Initial admissibility implies that $v(\cdot)$ is total.

Cut admissibility implies that $v(\cdot)$ is functional.

The introduction rules yield the truth-table definition for $v(\cdot)$: e.g., $v(A \wedge B)$ is the truth-functional conjunction of $v(A)$ and $v(B)$ (similarly for $\vee$).

Of course, the logic of $\mathcal{A}$-formulas is essentially trivial. To strengthen this logic, we add first-order terms and quantification.

Term equality and quantification

A *ranked signature* Σ associates to every constructor a natural number indicating that constructor's arity.

A *Σ-term* is a (closed) term built from only constructors in Σ and obeying the rank restrictions.

For example, if Σ is $\{a/0, b/0, f/1, g/2\}$, then a, $(f\ a)$, and $(g\ (f\ a)\ b)$ are all Σ-terms.

$$\frac{}{\vdash t = t, \Delta} \qquad \frac{}{\vdash t \neq s, \Delta}\ t \text{ and } s \text{ differ}$$

Here, t and s are Σ-terms for some ranked signature Σ.

$$\frac{\vdash B[t/x], \Delta}{\vdash \exists x.B, \Delta}\ \exists \qquad \frac{\{\ \vdash B[t/x], \Delta\ \mid\ \Sigma\text{-term } t\ \}}{\vdash \forall x.B, \Delta}\ \forall\text{-ext}$$

These rules are *additive* but at the cost of being *infinitary*.

There is no algorithm here

Let Σ contain the ranked symbols $z/0$ and $s/1$. Abbreviate z, $(s\ z)$, $(s\ (s\ z))$, $(s\ (s\ (s\ z)))$, etc by $\mathbf{0}$, $\mathbf{1}$, $\mathbf{2}$, $\mathbf{3}$, etc.

Let A and B be the set of terms $\{0, 1\}$ and $\{0, 1, 2\}$, respectively. These sets can be encoded as the predicate expressions

$$\lambda x.\ x = \mathbf{0} \vee x = \mathbf{1} \quad \text{and} \quad \lambda x.\ x = \mathbf{0} \vee x = \mathbf{1} \vee x = \mathbf{2}.$$

The fact that $A \subseteq B$ can be denoted by the formula $\forall x. \neg(A\,x) \vee B\,x$ or, equivalently, as

$$\forall x.(x \neq \mathbf{0} \wedge x \neq \mathbf{1}) \vee x = \mathbf{0} \vee x = \mathbf{1} \vee x = \mathbf{2}$$

Proving this formula requires an infinite number of premises of the form $(t \neq \mathbf{0} \wedge t \neq \mathbf{1}) \vee t = \mathbf{0} \vee t = \mathbf{1} \vee t = \mathbf{2}$.

Outline of the rest of this talk

- Introduce *multiplicative* inference rules and connectives.
- Introduce *focusing proof systems* as a formal mechanism to define synthetic inference rules.
- Define *additive synthetic inference rules*
- Define *switchable formulas*
- *Theorem:* Synthetic inference rules based on switchable formulas are additive synthetic inference rules.
- *Conclusion:* The proof theory of switchable formulas in linear logic provides a foundation for model checking.

Two treatments for implication

The additive treatment of implication: *material implication*.

$$\frac{\vdash \neg A, \Delta}{\vdash A \supset B, \Delta} \qquad \frac{\vdash B, \Delta}{\vdash A \supset B, \Delta}$$

Gentzen introduced (two-sided) sequents in order to provide a different and more familiar form of inference rule for implications.

The multiplicative treatment of implication: *hypothetical reasoning*.

$$\frac{\Gamma, A \vdash B, \Delta}{\Gamma \vdash A \supset B, \Delta}$$

Contexts are essential: the strengthening theorem does not hold anymore.

$$\frac{p \vdash q, p}{\vdash p \supset q, p}$$

Multiplicative connectives: implication and conjunction

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

Currying $A \supset B \supset C \equiv (A \wedge B) \supset C$ yields a multiplicative conjunction.

$$\frac{\Gamma, A, B \vdash \Delta}{\Gamma, A \wedge^+ B \vdash \Delta} \qquad \frac{\Gamma_1 \vdash A, \Delta_1 \qquad \Gamma_2 \vdash B, \Delta_2}{\Gamma_1, \Gamma_2 \vdash A \wedge^+ B, \Delta_1, \Delta_2}$$

For symmetry, we rename $\wedge$ as $\wedge^-$ and tt to tt^-.

In linear logic, one writes $\&$, $\top$, $\otimes$, 1 for $\wedge^-$, tt^-, $\wedge^+$, tt^+.

Similar, $\supset$ corresponds to $\multimap$ in linear logic. The multiplicative disjunction plays no central role here. The multiplicative false ff^- exists as $t \neq t$ (for closed term t).

Multiplicative connectives: quantifiers and eigenvariables

The multiplicative treatment of quantifiers employs *eigenvariables*.

Let the set $\mathcal{X}$ denote *first-order variables*.

Let $\Sigma(\mathcal{X})$ denote all terms built from constructors in Σ and from the variables $\mathcal{X}$: variables act as constructors of arity 0.

Sequents are now written as $\mathcal{X}\,;\,\Gamma \vdash \Delta$: the variables in $\mathcal{X}$ are bound over the formulas in Γ and Δ: formulas in Γ and Δ are $\Sigma(\mathcal{X})$-formulas.

$$\frac{\mathcal{X}\,;\,\Gamma \vdash B[t/x], \Delta}{\mathcal{X}\,;\,\Gamma \vdash \exists x.B, \Delta}\ \exists \qquad \frac{\mathcal{X}, y\,;\,\Gamma \vdash B[y/x], \Delta}{\mathcal{X}\,;\,\Gamma \vdash \forall x.B, \Delta}\ \forall$$

where t is a $\Sigma(\mathcal{X})$-term and $y \notin \mathcal{X}$. Dually, for the left introduction rules.

Equality with open terms

When t and s are not unifiable,

$$\frac{}{\mathcal{X}\,;\,\Gamma, t = s \vdash \Delta} \qquad \frac{}{\mathcal{X}\,;\,\Gamma \vdash t \neq s, \Delta}$$

Otherwise, set $\theta = \mathsf{mgu}(t, s)$:

$$\frac{\theta\mathcal{X}\,;\,\theta\Gamma \vdash \theta\Delta}{\mathcal{X}\,;\,\Gamma, t = s \vdash \Delta} \qquad \frac{\theta\mathcal{X}\,;\,\theta\Gamma \vdash \theta\Delta}{\mathcal{X}\,;\,\Gamma \vdash t \neq s, \Delta}$$

Here, $\theta\mathcal{X}$ is the result of removing from $\mathcal{X}$ variables in the domain of θ and then adding the variables free in the codomain of θ.

This treatment of equality was developed independently by Schroeder-Heister and Girard in [1991/92]. Unification is a black box attached to sequent calculus.

This treatment has been extended to simply typed λ-terms and this has been implemented in Bedwyr and Abella.

Return to the subset example

Let $\Sigma = \{z/0, s/1\}$ and let the sets A and B be

$$\lambda x.\ x = \mathbf{0} \vee x = \mathbf{1} \quad \text{and} \quad \lambda x.\ x = \mathbf{0} \vee x = \mathbf{1} \vee x = \mathbf{2}.$$

We now have a finite proof of $A \subseteq B$.

$$\dfrac{\dfrac{\dfrac{\dfrac{}{\cdot\,;\,\cdot \vdash \mathbf{0} = \mathbf{0}}}{\cdot\,;\,\cdot \vdash \mathbf{0} = \mathbf{0} \vee \mathbf{0} = \mathbf{1} \vee \mathbf{0} = \mathbf{2}}}{x;\, x = \mathbf{0} \vdash x = \mathbf{0} \vee x = \mathbf{1} \vee x = \mathbf{2}} \quad \dfrac{\dfrac{\dfrac{}{\cdot\,;\,\cdot \vdash \mathbf{1} = \mathbf{1}}}{\cdot\,;\,\cdot \vdash \mathbf{1} = \mathbf{0} \vee \mathbf{1} = \mathbf{1} \vee \mathbf{1} = \mathbf{2}}}{x;\, x = \mathbf{1} \vdash x = \mathbf{0} \vee x = \mathbf{1} \vee x = \mathbf{2}}}{\dfrac{x\,;\, x = \mathbf{0} \vee x = \mathbf{1} \vdash x = \mathbf{0} \vee x = \mathbf{1} \vee x = \mathbf{2}}{\cdot\,;\,\cdot \vdash \forall x.(x = \mathbf{0} \vee x = \mathbf{1}) \supset (x = \mathbf{0} \vee x = \mathbf{1} \vee x = \mathbf{2})}}$$

This proof accounts for reachability: we only consider checking membership in set B for those elements "reached" in A.

Fixed points

The least fixed point μ and greatest fixed point ν are actually a series of operators depending on the arity of the relationship they define. We leave this arity implicit. Unfolding $\mu B t_1 \dots t_n$ and $\nu B t_1 \dots t_n$ yields

$$B(\mu B) t_1 \dots t_n \quad \text{and} \quad B(\nu B) t_1 \dots t_n, \quad \text{respectively.}$$

$$\frac{\mathcal{X} \,;\, \Gamma \vdash B(\mu B)\bar{t}, \Delta}{\mathcal{X} \,;\, \Gamma \vdash \mu B \bar{t}, \Delta}\ \mu R \qquad \frac{\mathcal{X} \,;\, B(\mu B)\bar{t}, \Gamma \vdash \Delta}{\mathcal{X} \,;\, \mu B \bar{t}, \Gamma \vdash \Delta}\ \mu L$$

$$\frac{\mathcal{X} \,;\, \Gamma, B(\nu B)\bar{t} \vdash \Delta}{\mathcal{X} \,;\, \Gamma, \nu B \bar{t} \vdash \Delta}\ \nu L \qquad \frac{\mathcal{X} \,;\, \Gamma \vdash \Delta, B(\nu B)\bar{t}}{\mathcal{X} \,;\, \Gamma \vdash \Delta, \nu B \bar{t}}\ \nu R$$

Rules for μ-unfolding on the left and ν-unfolding on the right are admissible.
Induction and coinduction rules (using invariants) are not displayed here.

Horn clauses yield least fixed points

Prolog specification of a (tiny) graph and its transitive closure:

```
step a b.  step b c.  step c b.
path X Z :- step X Z.
path X Z :- step X Y, path Y Z.
```

`step` as a least fixed point expression:

$$\mu(\lambda A \lambda x \lambda y.\, (x = a \wedge^{+} y = b) \vee (x = b \wedge^{+} y = c) \vee (x = c \wedge^{+} y = b))$$

`path` as a fixed point expression:

$$\mu(\lambda A \lambda x \lambda z.\, \texttt{step}\ x\ z \vee (\exists y.\, \texttt{step}\ x\ y \wedge^{+} A\, y\, z)).$$

Focusing terminology: $=$, $\wedge^{+}$, $\vee$, $\exists$, and μ are *positive connectives*.
Horn clause definitions correspond to *purely positive* expressions.

Reachability proof

There is no proof that there is a step from a to c.

$$\dfrac{\dfrac{\mathit{fail}}{\vdash (a = a \wedge^{+} c = b) \vee (a = b \wedge^{+} c = c) \vee (a = c \wedge^{+} c = b)}}{\vdash \mathtt{step}\ a\ c}$$

There is a proof that there is a path from a to c.

$$\dfrac{\dfrac{\dfrac{\vdash \mathtt{step}\ a\ b \qquad \vdash \mathit{path}\, b\, c}{\vdash \mathtt{step}\ a\ b \wedge^{+} \mathit{path}\, b\, c}}{\vdash \exists y.\, \mathtt{step}\ a\ y \wedge^{+} \mathit{path}\, y\, c}}{\vdash \mathtt{step}\ a\ c \vee (\exists y.\, \mathtt{step}\ a\ y \wedge^{+} \mathit{path}\, y\, c)}}{\vdash \mathit{path}(a, c)}$$

Non-reachability proof

Below is a proof that the node a is not adjacent to c.

$$\dfrac{\dfrac{\dfrac{}{a = a, c = b \vdash \cdot}}{a = a \wedge^{+} c = b \vdash \cdot} \quad \dfrac{\dfrac{}{a = b, c = c \vdash \cdot}}{a = b \wedge^{+} c = c \vdash \cdot} \quad \dfrac{\dfrac{}{a = c, c = b \vdash \cdot}}{a = c \wedge^{+} c = b \vdash \cdot}}{\dfrac{(a = a \wedge^{+} c = b) \vee (a = b \wedge^{+} c = c) \vee (a = c \wedge^{+} c = b) \vdash \cdot}{\texttt{step}\ a\ c \vdash \cdot}}$$

In general, proofs by negation-as-finite-failure yield sequent calculus proofs in this setting.

If the underlying graph has cycles, then we need to strengthen the proof rules to contain induction.

More examples

Definitions of relations for natural numbers, addition, less-than.

$$\begin{aligned}
nat =& \mu\lambda N\lambda n(n = z \vee \exists n'(n = s\ n' \wedge^+ N\ n')) \\
plus =& \mu\lambda P\lambda n\lambda m\lambda p\ ((n = z \wedge^+ m = p) \vee \\
& \qquad \exists n'\exists p'(n = s\ n' \wedge^+ p = s\ p' \wedge^+ P\ n'\ m\ p')) \\
lt =& \mu\lambda L\lambda x\lambda y((x = z \wedge^+ \exists y'.y = sy') \vee \\
& \qquad (\exists x'\exists y'.x = sx' \wedge^+ y = sy' \wedge^+ L\ x'\ y'))
\end{aligned}$$

The following formula requires induction to be proved.

$$\forall n\forall m\forall p(nat\ n \supset nat\ m \supset plus\ n\ m\ p \supset plus\ m\ n\ p)$$

The following formula can be proved by a model checker.

$$\forall n\forall m\forall p(lt\ n\ \mathbf{10} \supset lt\ m\ \mathbf{10} \supset plus\ n\ m\ p \supset plus\ m\ n\ p)$$

Synthetic inference rules via focusing

Negative connectives have invertible right-introduction rules.
Positive connectives have (generally) non-invertible right-introduction rules.

Sequents in the focused proof system come in three styles.

- *up-arrow* sequents: $\mathcal{X} : \mathcal{N} \Uparrow \Gamma \vdash \Delta \Uparrow \mathcal{P}$.
- *left-down-arrow* sequent: $\mathcal{X} : \mathcal{N} \Downarrow B \vdash \mathcal{P}$.
- *right-down-arrow* sequent: $\mathcal{X} : \mathcal{N} \vdash B \Downarrow \mathcal{P}$.

B is the *focus* of these $\Downarrow$-sequents.

Storage on left: $\mathcal{N}$ is a multiset of negative formulas
Storage on right: $\mathcal{P}$ is a multiset of positive formulas

Both Δ and Γ can be either *lists* or *multisets* of formulas.

$\mathcal{X}$ is a variable signature as we have seen before.

A focused proof system: the $\Uparrow$ rules

$$\frac{\Sigma\theta : \mathcal{N}\theta \Uparrow \Gamma\theta \vdash \Delta\theta \Uparrow \mathcal{P}\theta}{\mathcal{X} : \mathcal{N} \Uparrow s = t, \Gamma \vdash \Delta \Uparrow \mathcal{P}}\dagger \qquad \frac{\Sigma\theta : \mathcal{N}\theta \Uparrow \cdot \vdash \cdot \Uparrow \mathcal{P}\theta}{\mathcal{X} : \mathcal{N} \Uparrow \cdot \vdash s \neq t \Uparrow \mathcal{P}}\dagger \qquad \frac{}{\mathcal{X} : \mathcal{N} \Uparrow s = t, \Gamma \vdash \Delta \Uparrow \mathcal{P}}\ddagger$$

$$\frac{}{\mathcal{N} \Uparrow \cdot \vdash \cdot \Uparrow s \neq t, \Delta, \mathcal{P}}\ddagger \qquad \frac{\mathcal{N} \Uparrow \Gamma \vdash \Delta \Uparrow \mathcal{P}}{\mathcal{N} \Uparrow tt^+, \Gamma \vdash \Delta \Uparrow \mathcal{P}} \qquad \frac{\mathcal{N} \Uparrow \cdot \vdash \Delta \Uparrow \mathcal{P}}{\mathcal{N} \Uparrow \cdot \vdash ff^-, \Delta \Uparrow \mathcal{P}}$$

$$\frac{\mathcal{N} \Uparrow A_1, \Gamma \vdash \Delta \Uparrow \mathcal{P} \qquad \mathcal{N} \Uparrow A_2, \Gamma \vdash \Delta \Uparrow \mathcal{P}}{\mathcal{N} \Uparrow A_1 \vee A_2, \Gamma \vdash \Delta \Uparrow \mathcal{P}}$$

$$\frac{\mathcal{N} \Uparrow \cdot \vdash A_1 \Uparrow \mathcal{P} \qquad \mathcal{N} \Uparrow \cdot \vdash A_2 \Uparrow \mathcal{P}}{\mathcal{N} \Uparrow \cdot \vdash A_1 \wedge^- A_2 \Uparrow \mathcal{P}}$$

$$\frac{\mathcal{N} \Uparrow A_1, A_2, \Gamma \vdash \Delta \Uparrow \mathcal{P}}{\mathcal{N} \Uparrow A_1 \wedge^+ A_2, \Gamma \vdash \Delta \Uparrow \mathcal{P}} \qquad \frac{\mathcal{N} \Uparrow A_1 \vdash A_2, \Delta \Uparrow \mathcal{P}}{\mathcal{N} \Uparrow \cdot \vdash A_1 \supset A_2, \Delta \Uparrow \mathcal{P}} \qquad \frac{}{\mathcal{N} \Uparrow ff^+, \Gamma \vdash \Delta \Uparrow \mathcal{P}}$$

$$\frac{}{\mathcal{N} \Uparrow \cdot \vdash tt^-, \Delta \Uparrow \mathcal{P}} \qquad \frac{\mathcal{X}, y : \mathcal{N} \Uparrow C\,y, \Gamma \vdash \Delta \Uparrow \mathcal{P}}{\mathcal{X} : \mathcal{N} \Uparrow \exists x.\, C\,x, \Gamma \vdash \Delta \Uparrow \mathcal{P}} \qquad \frac{\mathcal{X}, y : \mathcal{N} \Uparrow \cdot \vdash C\,y, \Delta \Uparrow \mathcal{P}}{\mathcal{X} : \mathcal{N} \Uparrow \cdot \vdash \forall x.\, C\,x, \Delta \Uparrow \mathcal{P}}$$

$$\frac{\mathcal{N} \Uparrow B(\mu B)\bar{t}, \Gamma \vdash \Delta \Uparrow \mathcal{P}}{\mathcal{N} \Uparrow \mu B\,\bar{t}, \Gamma \vdash \Delta \Uparrow \mathcal{P}} \qquad \frac{\mathcal{N} \Uparrow \cdot \vdash B(\nu B)\bar{t}, \Delta \Uparrow \mathcal{P}}{\mathcal{N} \Uparrow \cdot \vdash \nu B\,\bar{t}, \Delta \Uparrow \mathcal{P}}$$

Proviso $\dagger$: $\theta = mgu(s, t)$ and $\ddagger$: s and t not unifiable.

A focused proof system: $\Downarrow$ and structural rules

$$\frac{}{\mathcal{N} \Downarrow t \neq t \vdash \mathcal{P}} \qquad \frac{}{\mathcal{N} \vdash t = t \Downarrow \mathcal{P}} \qquad \frac{}{\mathcal{N} \Downarrow \mathit{ff}^- \vdash \mathcal{P}} \qquad \frac{}{\mathcal{N} \vdash \mathit{tt}^+ \Downarrow \mathcal{P}}$$

$$\frac{\mathcal{N}_1 \cdot \vdash A_1 \Downarrow \mathcal{P}_1 \quad \mathcal{N}_2 \Downarrow A_2 \vdash \mathcal{P}_2}{\mathcal{N}_1, \mathcal{N}_2 \Downarrow A_1 \supset A_2 \vdash \mathcal{P}_1, \mathcal{P}_2} \qquad \frac{\mathcal{N}_1 \vdash A_1 \Downarrow \mathcal{P}_1 \quad \mathcal{N}_2 \vdash A_2 \Downarrow \mathcal{P}_2}{\mathcal{N}_1, \mathcal{N}_2 \vdash A_1 \wedge^+ A_2 \Downarrow \mathcal{P}_1, \mathcal{P}_2}$$

$$\frac{\mathcal{N} \Downarrow A_i \vdash \mathcal{P}}{\mathcal{N} \Downarrow A_1 \wedge^- A_2 \vdash \mathcal{P}} \qquad \frac{\mathcal{N} \vdash A_i \Downarrow \mathcal{P}}{\mathcal{N} \vdash A_1 \vee A_2 \Downarrow \mathcal{P}}$$

$$\frac{\mathcal{N} \Downarrow C\ t \vdash \mathcal{P}}{\mathcal{N} \Downarrow \forall x.\, C\ x \vdash \mathcal{P}} \qquad \frac{\mathcal{N} \vdash C\ t \Downarrow \mathcal{P}}{\mathcal{N} \vdash \exists x.\, C\ x \Downarrow \mathcal{P}}$$

$$\frac{\mathcal{N} \Downarrow B(\nu B)\bar{t} \vdash \mathcal{P}}{\mathcal{N} \Downarrow \nu B\ \bar{t} \vdash \mathcal{P}} \qquad \frac{\mathcal{N} \vdash B(\mu B)\bar{t} \Downarrow \mathcal{P}}{\mathcal{N} \vdash \mu B\ \bar{t} \Downarrow \mathcal{P}}$$

store

$$\frac{\mathcal{N}, N \Uparrow \Gamma \vdash \Delta \Uparrow \mathcal{P}}{\mathcal{N} \Uparrow N, \Gamma \vdash \Delta \Uparrow \mathcal{P}} \qquad \frac{\mathcal{N} \Uparrow \cdot \vdash \Delta \Uparrow P, \mathcal{P}}{\mathcal{N} \Uparrow \cdot \vdash P, \Delta \Uparrow \mathcal{P}}$$

release

$$\frac{\mathcal{N} \Uparrow P \vdash \cdot \Uparrow \mathcal{P}}{\mathcal{N} \Downarrow P \vdash \mathcal{P}} \qquad \frac{\mathcal{N} \Uparrow \cdot \vdash N \Uparrow \mathcal{P}}{\mathcal{N} \vdash N \Downarrow \mathcal{P}}$$

decide

$$\frac{\mathcal{N} \Downarrow N \vdash \mathcal{P}}{\mathcal{N}, N \Uparrow \cdot \vdash \cdot \Uparrow \mathcal{P}} \qquad \frac{\mathcal{N} \vdash P \Downarrow \mathcal{P}}{\mathcal{N} \Uparrow \cdot \vdash \cdot \Uparrow P, \mathcal{P}}$$

Synthetic inference rules

Sequents of the form $\mathcal{X} : \mathcal{N} \Uparrow \cdot \vdash \cdot \Uparrow \mathcal{P}$ are *border* sequents.

Synthetic inference rules have border sequents as conclusion and as premises.

A border sequent $\mathcal{X} : \mathcal{N} \Uparrow \cdot \vdash \cdot \Uparrow \mathcal{P}$ where $\mathcal{P} \cup \mathcal{N}$ is a singleton multiset is called a *singleton* border sequent.

Such a sequent is of the form

$$\mathcal{X} : N \Uparrow \cdot \vdash \cdot \Uparrow \cdot \quad \text{or} \quad \mathcal{X} : \cdot \Uparrow \cdot \vdash \cdot \Uparrow P$$

These sequent represent proving $\neg N$ (for a negative formula N) or proving P (for a positive formula P).

Only the decide rules can have such a sequent as its conclusion and there is only one choice for the focus.

Synthetic inference rules: purely positive formulas

$$P := tt^{+} \mid t = s \mid \mu\lambda A\lambda\bar{x}.P \mid P \wedge^{+} P \mid P \vee P \mid \exists x.P$$

Consider a border sequent with a purely positive P on the right.

$$\frac{\begin{array}{c}\Xi \\ \mathcal{X} : \cdot \vdash P \Downarrow \cdot\end{array}}{\mathcal{X} : \cdot \Uparrow \cdot \vdash \cdot \Uparrow P}$$

If a complete proof Ξ exists, it is entirely one $\Downarrow$-phase.

An entire Prolog-like computations can be forced into one phase.

Additive synthetic connectives

In order to build on *additive synthetic connectives*, we need to restrict occurrence of the multiplicative connectives $\supset$ and $\wedge^+$.

A μMALL$^=$ formula is *switchable* if

- whenever a subformula $C \wedge^+ D$ occurs negatively (under an odd number of implications), either C or D is purely positive;
- whenever a subformula $C \supset D$ occurs positively (under an even number of implications), either C is purely positive or D is purely negative.

Note: purely positive formulas and purely negative formulas are switchable.

An occurrence of a formula B in a sequent is *switchable* if it appears on the right-hand side (resp. left-hand side) and B (resp. $B \supset ff^-$) is switchable.

Example: simulation

Let $P \xrightarrow{A} Q$ be a labeled transition system between processes and actions. Assume it is defined as a purely positive expression.

If $p, q \in P$ and $a \in A$ then both $P \xrightarrow{A} Q$ and $(P \xrightarrow{A} Q) \supset \mathit{ff}^-$ are switchable formulas.

The following fixed point expressions define simulation and bisimulation.

$$\nu\big(\lambda S \lambda p \lambda q.\, \forall a \forall p'.\, p \xrightarrow{a} p' \supset \exists q'.\, q \xrightarrow{a} q' \wedge^+ S\, p'\, q'\big)$$

$$\begin{aligned}\nu(\lambda B \lambda p \lambda q. \quad & (\forall a \forall p'.\, p \xrightarrow{a} p' \supset \exists q'.\, q \xrightarrow{a} q' \wedge^+ B\, p'\, q') \\ & \wedge^- (\forall a \forall q'.\, q \xrightarrow{a} q' \supset \exists p'.\, p \xrightarrow{a} p' \wedge^+ B\, q'\, p'))\end{aligned}$$

These are switchable formulas. Note that bisimulation has both conjunctions.

Switchable formulas yield additive synthetic rules

The following theorem is proved by a simple induction on the structure of μMALL$^{=}$ proofs.

Theorem

A μMALLF$^{=}$ derivation of either

$$\cdot : A \Uparrow \cdot \vdash \cdot \Uparrow \cdot \quad \textit{or} \quad \cdot : \cdot \Uparrow \cdot \vdash \cdot \Uparrow A,$$

where the occurrence of A is switchable, is composed of only additive synthetic inference rules.

An example of a synthetic inference rules

$$
\cfrac{\cfrac{\cdots \qquad \cfrac{\cfrac{\cfrac{\cfrac{\cdot : \cdot \Uparrow \cdot \vdash sim(p_i, q_i) \Uparrow \cdot}{\cdot : \cdot \vdash sim(p_i, q_i) \Downarrow \cdot}}{\cdot : \cdot \vdash \exists Q'.q_0 \xrightarrow{a_i} Q' \wedge^+ sim(p_i, Q') \Downarrow \cdot}\ C}{\cdot : \cdot \Uparrow \cdot \vdash \cdot \Uparrow \exists Q'.q_0 \xrightarrow{a_i} Q' \wedge^+ sim(p_i, Q')}}{\cdot : \cdot \Uparrow \cdot \vdash \exists Q'.q_0 \xrightarrow{a_i} Q' \wedge^+ sim(p_i, Q') \Uparrow \cdot} \qquad \cdots}{P', A : \cdot \Uparrow p_0 \xrightarrow{A} P' \vdash \exists Q'.q_0 \xrightarrow{A} Q' \wedge^+ sim(P', Q') \Uparrow \cdot}\ B}{\cdot : \cdot \Uparrow \cdot \vdash sim(p_0, q_0) \Uparrow \cdot}\ A
$$

A contain introduction rules for unfolding, $\forall$, and $\supset$.

B consists of $\Uparrow$ rules that generate all a_i, p_i such that $p_0 \xrightarrow{a_i} p_i$.

C is a sequence of $\Downarrow$ rules that prove that $q_0 \xrightarrow{a_i} q_i$.

Finally, the top-most inference rule is a release rule.

Some applications

The model checker *Bedwyr* implements proof search in μMALL.

The interactive theorem prover *Abella* is based an intuitionistic extension containing also induction and coinduction.

We have used this proof theory to design the following proof certificates for model checking queries.

- A path in a graph can be proof certificate for *reachability*.
- A connected component can be a proof certificate for *non-reachability*.
- A bisimulation can be a proof certificate for *bisimilarity*.
- A Hennessy-Milner modal formula can be a proof certificate for *non-bisimilarity*.

Conclusion

Multiplicative Additive Linear Logic (MALL) plus connectives for first-order terms ($\forall$, $=$, μ, ν) provides a natural setting for many model checking queries.

Additive connectives has a clear relationship to model theory.

To be more expressive and finitary, we allow multiplicative rules but limit their use to the construction of additive synthetic inference rules.

The proof theory of switchable formulas in linear logic provides a foundation for model checking.