A Proof Theory for Model Checking: An Extended Abstract

Quentin Heath
LIX, École Polytechnique
Palaiseau, France

Dale Miller
Inria Saclay and LIX, École Polytechnique
Palaiseau, France

While model checking has often been considered as a practical alternative to building formal proofs, we argue here that the theory of sequent calculus proofs can be used to provide an appealing foundation for model checking. Since the emphasis of model checking is on establishing the truth of a property in a model, we rely on the proof theoretic notion of additive inference rules, since such rules allow provability to directly describe truth conditions. Unfortunately, the additive treatment of quantifiers requires inference rules to have infinite sets of premises and the additive treatment of model descriptions provides no natural notion of state exploration. By employing a focused proof system, it is possible to construct large scale, synthetic rules that also qualify as additive but contain elements of multiplicative inference. These additive synthetic rules—essentially rules built from the description of a model—allow a direct treatment of state exploration. This proof theoretic framework provides a natural treatment of reachability and non-reachability problems, as well as tabled deduction, bisimulation, and winning strategies.

1 Introduction

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 establish using traditional, axiomatic proof techniques such as those describe by Floyd and Hoare [5]. In this extended abstract we show that model checking can be given a proof theoretic foundation using the sequent calculus of Gentzen [6], the linear logic of Girard [7], and a treatment of fixed points [2, 4, 11, 17]. The main purpose of this extended abstract is foundational and conceptual. Our presentation will not shed any new light on the algorithmic aspects of model checking but it will show how model checkers can be seen as having a "proof search" foundation shared with logic programming and (inductive) theorem proving.

Since the emphasis of model checking is on establishing the truth of a property in a model, a natural connection with proof theory is via the use of *additive* connectives and their inference rules. We illustrate in Section 3 how the proof theory of additive connectives naturally leads to the usual notion of truth-table evaluation for propositional connectives. Relying only on additive connectives, however, fails to provide an adequate inference-based approach to model checking since it only rephrases truth-functional semantic conditions and requires rules with potentially infinite sets of premises.

The proof theory of sequent calculus contains additional inference rules, namely, the *multiplicative* inference rules which can be used to encode much of the algorithmic aspects of model checking such as, for example, those related to determining reachability and simulation (or winning strategies). In order to maintain a close connection between model checking and truth in model, we shall put additive inference rules back in the center of our framework but this time these rules will be additive *synthetic* inference rules. The synthesizing process will allow multiplicative connectives and inference rules to appear *inside* the construction of synthetic rules but they will not appear *outside* such synthetic rules. The construction of synthetic inference rules will be governed by the well established proof theoretic notions of *polarization* and *focused proof systems* [1, 8].

I. Cervesato and M. Fernández (Eds): Fourth International Workshop on Linearity 2016 (LINEARITY'16)
EPTCS 238, 2017, pp. 1–10, doi:10.4204/EPTCS.238.1

The connection between the proof theory based on such synthetic inference rules and model checking steps is close enough that certificates for both reachability and non-reachability as well as bisimulation and non-bisimulation are representable as sequent calculus proofs.

2 The basics of the sequent calculus

Let Δ and Γ range over *multisets* of formulas. A *sequent* is either one-sided, written $\vdash \Delta$, or two-sided, written $\Gamma \vdash \Delta$ (we first consider two-sided sequents in Section 5). Inference rules have one sequent as their conclusion and zero or more sequents as premises. We divide inference rules into three groups: the *identity* rules, the *structural* rules, and the *introduction* rules. The following are the two structural rules and two identity rules we consider.

$$\frac{\vdash \Delta}{\vdash B, \Delta}\ \text{weaken} \qquad \frac{\vdash \Delta, B, B}{\vdash \Delta, B}\ \text{contraction} \qquad \frac{}{\vdash B, \neg B}\ \text{initial} \qquad \frac{\vdash \Delta_1, B \quad \vdash \Delta_2, \neg B}{\vdash \Delta_{,1} \Delta_2}\ \text{cut}$$

The negation symbol $\neg(\cdot)$ is used here not as a logical connective but as a function that computes the negation normal form of a formula. The remaining rules of the sequent calculus are introduction rules: for these rules, a logical connective has an occurrence in the conclusion and does not have an occurrence in the premises. (We shall see several different sets of introduction inference rules shortly.)

When a sequent calculus inference rule has two (or more) premises, there are two natural schemes for managing the side formulas (i.e., the formulas not being introduced) in that rule. The following rules illustrate these two choices for conjunction.

$$\frac{\vdash B, \Delta \quad \vdash C, \Delta}{\vdash B \wedge C, \Delta} \qquad \frac{\vdash B, \Delta_1 \quad \vdash C, \Delta_2}{\vdash B \wedge C, \Delta_1, \Delta_2}$$

The choice on the left is the *additive* version of the rule: here, the side formulas in the conclusion are the same in all the premises. The choice on the right is the *multiplicative* version of the rule: here, the various side formulas of the premises are accumulated to be the side formulas of the conclusion. Note that the cut rule above is an example of a multiplicative inference rule. A logical connective with an additive right introduction rule is also classified as additive. In addition, the de Morgan dual and the unit of an additive connective are also additive connectives. Similarly, a logical connective with a multiplicative right-introduction rule is called multiplicative; so are its de Morgan dual and their units.

The multiplicative and additive versions of inference rules are, in fact, inter-admissible if the proof system contains weakening and contraction. In linear logic, where these structural rules are not available, the conjunction and disjunction have additive versions & and $\oplus$ and multiplicative versions $\otimes$ and $\wp$, respectively, and these different versions of conjunction and disjunction are not provably equivalent. Linear logic provides two *exponentials*, namely the ! and ?, that permit limited forms of the structural rules for suitable formulas. The familiar exponential law $x^{n+m} = x^n x^m$ extends to the logical additive and multiplicative connectives since $!(B \& C) \equiv !B \otimes !C$ and $?(B \oplus C) \equiv ?B \wp ?C$.

While we are interested in model checking as it is practiced, we shall be interested in only performing inference in classical logic. One of the surprising things to observe about our proof theoretical treatment of model checking is that almost all of it can be seen as taking place within the proof theory of linear logic, a logic that sits behind classical (and intuitionistic) logic. As a result, the distinction between additive and multiplicative connectives remains an important distinction for our framework. Also, weakening and contraction will not be eliminated completely but will be available for only certain formulas and in certain inference steps (echoing the fact that in linear logic, these structural rules can be applied to formulas annotated with exponentials).

3 Additive propositional connectives

Let $\mathscr{A}$ be the set of formulas built from the propositional connectives $\{\wedge, t, \vee, f\}$ (no propositional constants included). Consider the following small proof system involving one-sided sequents.

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

Here, t is the unit of $\wedge$, and f is the unit of $\vee$. Notice that $\vee$ has two introduction rules while f has none. Also, t and $\wedge$ are de Morgan duals of f and $\vee$, respectively. We say that the multiset Δ is provable if and only if there is a proof of $\vdash \Delta$ using these inference rules. Also, we shall consider no additional inference rules (that is, no contraction, weakening, initial, or cut rules): this inference system is composed only of introduction rules and all of these introduction rules are for *additive* logical connectives.

The following theorem identifies an important property of this purely additive setting. This theorem is proved by a straightforward induction on the structure of proofs.

Theorem 1 (Strengthening) *If Δ is a multiset of $\mathscr{A}$-formulas and $\vdash \Delta$ then $\exists\, B \in \Delta$ such that $\vdash B$.*

This theorem shows that provability of purely additive formulas is independent of their context. It also establishs that the proof system is consistent, since the empty sequent $\vdash \cdot$ is not provable.

The following three theorems state that the missing inference rules of weakening, contraction, initial, and cut are all admissible in this proof system. The first theorem is an immediate consequence of Theorem 1. The following two theorems are proved, respectively, by induction on the structure of formulas and by induction on the structure of proofs.

Theorem 2 (Weakening & contraction admissibility) *Let Δ_1 and Δ_2 be multisets of $\mathscr{A}$-formulas such that Δ_1 is a subset of Δ_2 (when viewed as sets). If $\vdash \Delta_1$ is provable then $\vdash \Delta_2$ is provable.*

Theorem 3 (Initial admissibility) *Let B be a $\mathscr{A}$-formula. Then $\vdash B, \neg B$ is provable.*

Theorem 4 (Cut admissibility) *Let B be an $\mathscr{A}$-formula and let Δ_1 and Δ_2 be multisets of $\mathscr{A}$-formulas. If both $\vdash B, \Delta_1$ and $\vdash \neg B, \Delta_2$ are provable, then there is a proof of $\vdash \Delta_1, \Delta_2$.*

These theorems lead to the following truth-functional semantics for $\mathscr{A}$ formulas: define $v(\cdot)$ as a mapping from $\mathscr{A}$ formulas to booleans such that $v(B)$ is t if $\vdash B$ is provable and is f if $\vdash \neg B$ is provable. Theorem 3 implies that $v(\cdot)$ is always defined and Theorem 4 implies that $v(\cdot)$ is functional (does not map a formula to two different booleans). The introduction rules describe this function *denotationally*: e.g., $v(A \wedge B)$ is the truth-functional conjunction of $v(A)$ and $v(B)$ (similarly for $\vee$).

While this logic of $\mathscr{A}$-formulas is essentially trivial, we will soon introduce much more powerful additive inference rules: their connection to truth functional interpretations (a la model checking principles) will arise from the fact that their provability is not dependent on other formulas in a sequent.

4 Additive first-order structures

We move to first-order logic by adding terms, equality on terms, and quantification.

We shall assume that some *ranked signature* Σ of term constructors is given: such a signature associates to every constructor a natural number indicating that constructor's arity. Term constants are identified with signature items given rank 0. 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.We shall consider only signatures for which there exist Σ-terms: for example, the set $\{f/1, g/2\}$ is not a valid signature. The usual symbols $\forall$ and $\exists$ will be used for the universal and existential quantification over terms. We assume that these quantifiers range over Σ-terms for some fixed signature. The arities of ranked signatures will often not be listed explicitly.

The equality and inequality of terms will be treated as (de Morgan dual) logical connectives in the sense that their meaning is given by the following introduction rules.

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

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

Consider (only for the scope of this section) the following two inference rules for quantification. In these introduction rules, $[t/x]$ denotes the capture-avoiding substitution.

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

Although $\forall$ and $\exists$ form a de Morgan dual pair, the rule for introducing the universal quantifier is not the standard one used in the sequent calculus (we will introduce the standard one later). This rule, which is similar to the ω-rule [14], is an extensional approach to modeling quantification: a universally quantified formula is true if all instances of it are true.

Consider now the logic built with the (additive) propositional constants of the previous section and with equality, inequality, and quantifiers. The corresponding versions of all four theorems in Section 3 holds for this logic. Similarly, we can extend the evaluation function for $\mathscr{A}$-formulas to work for the quantifiers: in particular, $v(\forall x.Bx) = \bigwedge_t v(Bt)$ and $v(\exists x.Bx) = \bigvee_t v(Bt)$. Such a result is not surprising, of course, since we have repeated within inference rules the usual semantic conditions. The fact that these theorems hold indicates that the proof theory we have presented so far offers nothing new over truth functional semantics. Similarly, this bit of proof theory offers nothing appealing to model checking, as illustrated by the following example.

Example 5 *Let Σ contain the ranked symbols $z/0$ and $s/1$ and let us abbreviate the terms 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 $\{\mathbf{0}, \mathbf{1}\}$ and $\{\mathbf{0}, \mathbf{1}, \mathbf{2}\}$, respectively. These sets can be encoded as the predicate expressions $\lambda x.x = \mathbf{0} \vee x = \mathbf{1}$ and $\lambda x.x = \mathbf{0} \vee x = \mathbf{1} \vee x = \mathbf{2}$. The fact that A is a subset of B can be denoted by the formula $\forall x.\neg(Ax) \vee Bx$ 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 $(t \neq \mathbf{0} \wedge t \neq \mathbf{1}) \vee t = \mathbf{0} \vee t = \mathbf{1} \vee t = \mathbf{2}$. Since each of these premises can, of course, be proved, the original formula is provable, albeit with an "infinite proof".

While determining the subset relation between two finite sets is a typical example of a model checking problem, one would not use the above-mentioned inference rule for $\forall$ except in the extreme cases where there is a finite and small set of Σ-terms. As we can see, the additive inference rule for $\forall$-quantification generally leads to "infinitary proofs" (an oxymoron that we now avoid at all costs).

5 Multiplicative connectives

Our departure from purely additive inference rules now seems forced and we continue by adding multiplicative inference rules.

$$\frac{\mathscr{X};\Gamma\vdash A,\Delta \quad \mathscr{X};\Gamma\vdash B,\Delta}{\mathscr{X};\Gamma\vdash A\wedge^- B,\Delta} \qquad \frac{}{\mathscr{X};\Gamma\vdash t^-,\Delta} \qquad \frac{\mathscr{X};\Gamma,A\vdash\Delta}{\mathscr{X};\Gamma,A\wedge^- B\vdash\Delta} \qquad \frac{\mathscr{X};\Gamma,B\vdash\Delta}{\mathscr{X};\Gamma,A\wedge^- B\vdash\Delta}$$

$$\frac{\mathscr{X};\Gamma,A\vdash\Delta \quad \mathscr{X};\Gamma,B\vdash\Delta}{\mathscr{X};\Gamma,A\vee B\vdash\Delta} \qquad \frac{}{\mathscr{X};\Gamma,f\vdash\Delta} \qquad \frac{\mathscr{X};\Gamma\vdash A,\Delta}{\mathscr{X};\Gamma\vdash A\vee B,\Delta} \qquad \frac{\mathscr{X};\Gamma\vdash B,\Delta}{\mathscr{X};\Gamma\vdash A\vee B,\Delta}$$

$$\frac{\mathscr{X};\Gamma\vdash A,\Delta \quad \mathscr{X};\Gamma'\vdash B,\Delta'}{\mathscr{X};\Gamma,\Gamma'\vdash A\wedge^+ B,\Delta,\Delta'} \qquad \frac{}{\mathscr{X};\vdash t^+,} \qquad \frac{\mathscr{X};\Gamma,A,B\vdash\Delta}{\mathscr{X};\Gamma,A\wedge^+ B\vdash\Delta} \qquad \frac{\mathscr{X};\Gamma\vdash\Delta}{\mathscr{X};\Gamma,t^+\vdash\Delta}$$

$$\frac{\mathscr{X};\Gamma,A\vdash B,\Delta}{\mathscr{X};\Gamma\vdash A\supset B,\Delta} \qquad \frac{\mathscr{X};\Gamma\vdash A,\Delta \quad \mathscr{X};\Gamma',B\vdash\Delta'}{\mathscr{X};\Gamma,\Gamma',A\supset B\vdash\Delta,\Delta'}$$

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

When t and s are not unifiable,

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

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

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

Figure 1: Introduction rules for propositional constants, quantifiers, and equality. The $\exists$ rule is restricted so that t is a $\Sigma(\mathscr{X})$-term and the $\forall$ rule is restricted so that $y\notin\mathscr{X}$.

Our first multiplicative connective is the intuitionistic implication: since the most natural treatment of this connective uses two-sided sequents, we make the move away from the one-sided sequents that we have presented so far (see Figure 1). Note that taking the two multiplicative rules of implication right introduction and initial yields a proof system that violates the strengthening theorem (Section 3): the sequent $\vdash p\supset q,p$ is provable while neither $\vdash p\supset q$ nor $\vdash p$ are provable.

A common observation in proof theory is that the curry/uncurry equivalence between $A\supset B\supset C$ and $(A\wedge B)\supset C$ can be mimicked precisely by the proof system: in this case, such precision does not occur with the additive rules for conjunction but rather with the multiplicative version of conjunction. To this end, we add the multiplicative conjunction $\wedge^+$ and its unit t^+ and, for the sake of symmetry, we rename $\wedge$ as $\wedge^-$ and t to t^-. (The plus and minus symbols are related to the polarization of logical connectives that is behind the construction of synthetic connectives.) These two conjunctions and two truth symbols are logically equivalent in classical and intuitionistic logic although they are different in linear logic where it is more traditional to write &, $\top$, $\otimes$, **1** for $\wedge^-$, t^-, $\wedge^+$, t^+, respectively. The "multiplicative false" f^- (written as $\bot$ in linear logic) can be defined as $t\neq t$ (assuming that there is a first-order term t).

Eigenvariables are binders at the sequent level that align with binders within formulas (i.e., quantifiers). Binders are an intimate and low-level feature of logic: the addition of eigenvariables requires redefining the notions of term and sequent.

Let the set $\mathscr{X}$ denote *first-order variables* and let $\Sigma(\mathscr{X})$ denote all terms built from constructors in Σ and from the variables $\mathscr{X}$: in the construction of $\Sigma(\mathscr{X})$-terms, variables act as constructors of arity 0. (We assume that Σ and $\mathscr{X}$ are disjoint.) A $\Sigma(\mathscr{X})$-*formula* is one where all term constructors are taken from Σ and all free variables are contained in $\mathscr{X}$. Sequents are now written as $\mathscr{X};\Gamma\vdash\Delta$: the intended meaning of such a sequent is that the variables in the set $\mathscr{X}$ are bound over the formulas in Γ and Δ. We shall also assume that formulas in Γ and Δ are all $\Sigma(\mathscr{X})$-formulas. All inference rules are modified to account for this additional binding: see Figure 1. The variable y used in the $\forall$ introduction rule is called, of course, an eigenvariable.

The left introduction rules for equality in Figure 1 significantly generalizes the version involving only closed terms by making reference to unifiability and to most general unifiers. In the latter case, the domain of the substitution θ is a subset of $\mathscr{X}$, and the set of variables $\theta\mathscr{X}$ is the result of removing

from $\mathscr{X}$ all the variables in the domain of θ and then adding in all those variables free in the range of θ. This treatment of equality was developed independently by Schroeder-Heister [13] and Girard [9] and has been extended to include simply typed λ-terms [11].

While the use of eigenvariables in proofs allows us to deal with quantifiers with finite proofs, that treatment is not directly related to model theoretic semantics. In particular, the strengthening theorem does not hold for this proof system. As a result, obtaining a soundness and completeness theorem for this logic is no longer trivial.

The inference rules in Figure 1 provide a proper proof of the theorem considered in Example 5.

Example 6 *Let Σ and the sets A and B be as in Example 5. Showing that A is a subset of B requires showing that the formula $\forall x(Ax \supset Bx)$ is provable. That is, we need to find a proof of the sequent $\vdash \forall x.(x = \mathbf{0} \vee x = \mathbf{1}) \supset (x = \mathbf{0} \vee x = \mathbf{1} \vee x = \mathbf{2})$. The following proof of this sequent uses the rules from Figure 1: a double line means that two or more inference rules might be chained together.*

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

The proof in this example is able to account for a simple version of "reachability" in the sense that we only need to consider checking membership in set B for just those elements "reached" in A.

6 Fixed points

A final step in building a logic that can start to provide a foundation for model checking is the addition of least and greatest fixed points and their associated rules for induction and coinduction. Given that processes generally exhibit potentially infinite behaviors and that term structures are not generally bounded in their size, it is important for a logical foundation of model checking to allow for some treatment of infinity. The logic described by the proof system in Figure 1 is a two-sided version of MALL$^=$ (multiplicative additive linear logic extended with first-order quantifiers and equality) [4]. The decidability of this logic is easy to show: as one moves from conclusion to premise in every inference rule, the number of occurrences of logical connectives decrease. As a result, it is a simple matter to write an exhaustive search procedure that must necessarily terminate (such a search procedure can also make use of the decidable procedure of first-order unification).

In order to extend the expressiveness of MALL, Girard added the exponentials !, ? to MALL to get full linear logic [7]. The standard inference rules for exponentials allows for some forms of the contraction rule (Section 2) to appear in proofs and, as a result, provability is no longer decidable. A different approach to extending MALL with the possibility of having unbounded behavior was proposed in [4]: add to MALL$^=$ the least and greatest fixed point operators, written as μ and ν, respectively. The proof theory of the resulting logic, called μMALL$^=$, was been developed in [2] and exploited in a prototype model checker [3].

Fixed point expressions are written as $\mu B\bar{t}$ or $\nu B\bar{t}$, where B is an expression representing a monotonic higher-order abstraction, and $\bar{t}$ is a list of terms; by monotonic, we mean that the higher-order argument of B can only occur in B under even numbers of negations. The unfolding of the fixed point expressions $\mu B\bar{t}$ and $\nu B\bar{t}$ are $B(\mu B)\bar{t}$ and $B(\nu B)\bar{t}$, respectively.

$$\frac{\mathscr{X}\,;\Gamma\vdash B(\mu B)\overline{t},\Delta}{\mathscr{X}\,;\Gamma\vdash \mu B\overline{t},\Delta}\ \mu R \qquad \frac{\mathscr{X}\,;\Gamma,S\overline{t}\vdash\Delta \quad \mathscr{X},\overline{x};BS\overline{x}\vdash S\overline{x}}{\mathscr{X}\,;\Gamma,\mu B\overline{t}\vdash\Delta}\ \mu L$$

$$\frac{\mathscr{X}\,;\Gamma,B(\nu B)\overline{t}\vdash\Delta}{\mathscr{X}\,;\Gamma,\nu B\overline{t}\vdash\Delta}\ \nu L \qquad \frac{\mathscr{X}\,;\Gamma\vdash S\overline{t},\Delta \quad \overline{x};S\overline{x}\vdash BS\overline{x}}{\mathscr{X}\,;\Gamma\vdash \nu B\overline{t},\Delta}\ \nu R$$

Figure 2: Introduction rules for least (μ) and greatest (ν) fixed points

Example 7 *Horn clauses (in the sense of Prolog) can be encoded as purely positive fixed point expressions. For example, here is the Horn clause logic program (using the λProlog syntax, the* `sigma Y\` *construction encodes the quantifier ∃Y) for specifying a (tiny) graph and its transitive closure:*

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

We can translate the `step` *relation into the binary predicate $\cdot \longrightarrow \cdot$ defined by*

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

which only uses positive connectives. Likewise, `path` *can be encoded as the relation path$(\cdot,\cdot)$:*

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

To illustrate unfolding of the adjacency relation, note that unfolding the expression $a\longrightarrow c$ yields the formula $(a=a\wedge^{+}c=b)\vee(a=b\wedge^{+}c=c)\vee(a=c\wedge^{+}c=b)$ which is not provable. Unfolding the expression path(a,c) and performing β-reductions yields the expression $a\longrightarrow c\vee(\exists y.\,a\longrightarrow y\wedge^{+}\text{path}yc)$.

In μMALL$^{=}$, both μ and ν are treated as logical connectives in the sense that they will have introduction rules. They are also de Morgan duals of each other. The inference rules for treating fixed points are given in Figure 2. The rules for induction and coinduction (μL and νR, respectively) use a higher-order variable S which represents the invariant and coinvariant in these rules. As a result, it will not be the case that cut-free proofs will necessarily have the sub-formula properties: the invariant and coinvariant are not generally subformulas of the rule that they conclude. The following unfolding rules are also admissible since they can be derived using induction and coinduction.

$$\frac{\mathscr{X}\,;\Gamma,B(\mu B)\overline{t}\vdash\Delta}{\mathscr{X}\,;\Gamma,\mu B\overline{t}\vdash\Delta} \qquad \frac{\mathscr{X}\,;\Gamma\vdash B(\nu B)\overline{t},\Delta}{\mathscr{X}\,;\Gamma\vdash \nu B\overline{t},\Delta}$$

The introduction rules in Figures 1 and 2 are exactly the introduction rules of μMALL$^{=}$, except for two shallow differences. The first difference is that the usual presentation of μMALL$^{=}$ is via one-sided sequents (here, we use two-sided sequents). The second difference is that we have written many of the connectives differently (hoping that our set of connectives will feel more comfortable to those not familiar with linear logic). To be precise, to uncover the linear logic presentation of formulas, one must translate $\wedge^{-}$, t^{-}, $\wedge^{+}$, t^{+}, $\vee$, and $\supset$ to &, $\top$, $\otimes$, **1**, $\oplus$, and $\multimap$ [7]. Note that the linear implication $B\multimap C$ can be taken as an abbreviation of $\neg B\parr C$.

The following example shows that it is possible to prove some negations using either unfolding (when there are no cycles in the resulting state exploration) or induction.

Example 8 *Below is a proof that the node a is not adjacent to c: the first step of this proof involves unfolding the definition of the adjacency predicate into its description.*

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

A simple proof exists for path(a,c): one simply unfolds the fixed point expression for path$(\cdot,\cdot)$ and chooses correctly when presented with a disjunction and existential on the right of the sequent arrow. Given the definition of the path predicate, the following rules are clearly admissible. We write $\langle t,s\rangle\in Adj$ whenever $\cdot\vdash t\longrightarrow s$ is provable.

$$\dfrac{\mathscr{X}\,;\Gamma\vdash\Delta}{\mathscr{X}\,;\Gamma,path(t,s)\vdash\Delta}\ \langle t,s\rangle\in Adj\qquad\dfrac{\{\mathscr{X}\,;\Gamma,path(s,y)\vdash\Delta\mid\langle t,s\rangle\in Adj\}}{\mathscr{X}\,;\Gamma,path(t,y)\vdash\Delta}$$

The second rule has a premise for every pair $\langle t,s\rangle$ of adjacent nodes: if t is adjacent to no nodes, then this rule has no premises and the conclusion is immediately proved. A naive attempt to prove that there is no path from c to a gets into a loop (using these admissible rules): attempt to prove path$(c,a)\vdash\cdot$ leads to an attempt to prove path$(b,a)\vdash\cdot$ and again attempting to prove path$(c,a)\vdash\cdot$. Such a cycle can be examined to yield an invariant that makes it possible to prove the end-sequent. In particular, the set of nodes reachable from c is $\{b,c\}$, subset of $N=\{a,b,c\}$. The invariant S can be described as the set which is the complement (with respect to $N\times N$) of the set $\{b,c\}\times\{a\}$, or equivalently as the predicate $\lambda x\lambda y.\bigvee_{\langle u,v\rangle\in S}(x=u\wedge^+ y=v)$. With this invariant, the induction rule (μL) yields two premises. The left premise simply needs to confirm that the pair $\langle c,a\rangle$ is not a member of S. The right premise sequent $\bar{x};BS\bar{x}\vdash S\bar{x}$ establishes that S is an invariant for the μB predicate. In the present case, the argument list $\bar{x}$ is just a pair of variables, say, x,z, and B is the body of the path predicate: the right premise is the sequent $x,z\,;\,x\longrightarrow z\vee(\exists y.x\longrightarrow y\wedge^+ Syz)\vdash Sxz$. A formal proof of this follows easily by blindly applying applicable inference rules.

While the rules for fixed points (via induction and coinduction) are strong enough to transform cyclic behaviors into, for example, non-reachabilty or (bi)simulation assertions, these rules are not strong enough to prove other simple facts about fixed points. For example, consider the following two named fixed point expressions used for identifying natural numbers and the ternary relation of addition.

$$\begin{aligned}nat &= \mu\lambda N\lambda n(n=z\vee\exists n'(n=sn'\wedge^+ N\ n'))\\ plus &= \mu\lambda P\lambda n\lambda m\lambda p((n=z\wedge^+ m=p)\vee\exists n'\exists p'(n=sn'\wedge^+ p=sp'\wedge^+ P\ n'\ m\ p'))\end{aligned}$$

The following formula (stating that the addition of two numbers is commutative)

$$\forall n\forall m\forall p.nat\ n\supset nat\ m\supset plus\ n\ m\ p\supset plus\ m\ n\ p$$

is not provable using the inference rules we have described. The reason that this formula does not have a proof is not because the induction rule (μL in Figure 2) is not strong enough or that we are actually sitting inside linear logic: it is because an essential feature of inductive arguments is missing. Consider attempting a proof by induction that the property P holds for all natural numbers. Besides needing to prove that P holds of zero, we must also introduce an arbitrary integer j (corresponding to the eigenvariables of the right premise in μL) and show that the statement $P(j+1)$ reduces to the statement $P(j)$. That is, after manipulating the formulas describing $P(j+1)$ we must be able to find in the resulting argument, formulas describing $P(j)$. Up until now, we have only "performed" formulas (by

applying introduction rules) instead of checking them for equality. More specifically, while we do have a logical primitive for checking equality of terms, the proof system described so far does not have an equality for comparing formulas. As a result, some of the most basic theorems are not provable in this system. For example, there is no proof of $\forall n.(\mathit{nat}\ n \supset \mathit{nat}\ n)$.

Model checking is not the place where we should be attempting proofs involving arbitrary infinite domains: inductive theorem provers are used for that. If we restrict to finite domains, however, proofs appear. For example, consider the less-than binary relation defined as

$$\mathit{lt} = \mu\lambda L\lambda x\lambda y((x = z \wedge^{+} \exists y'.y = sy') \vee (\exists x'\exists y'.x = sx' \wedge^{+} y = sy' \wedge^{+} L\ x'\ y'))$$

The formula $(\forall n.\mathit{lt}\ n\ \mathbf{10} \supset \mathit{lt}\ n\ \mathbf{10})$ has a proof that involves generating all numbers less than 10 and then showing that they are, in fact, all less than 10. Similarly, a proof of the formula $\forall n\forall m\forall p(\mathit{lt}\ n\ \mathbf{10} \supset \mathit{lt}\ m\ \mathbf{10} \supset \mathit{plus}\ n\ m\ p \supset \mathit{plus}\ m\ n\ p)$ exists and consists of enumerating 100 pairs of numbers $\langle n,m\rangle$ and checking that the result of adding $n+m$ yields the same value as adding $m+n$.

The full proof system for $\mu\mathrm{MALL}^{=}$ contains the cut rule and the following two initial rules.

$$\frac{}{\mathscr{X}\ ;\ \mu B\overline{t} \vdash \mu B\overline{t}}\ \mu\ \mathit{init} \qquad \frac{}{\mathscr{X}\ ;\ \nu B\overline{t} \vdash \nu B\overline{t}}\ \nu\ \mathit{init}$$

The more general instance of the initial rule can be eliminated in favor of these two specific instances.

7 Conclusions

Linear logic is usually understood as being an intensional logic whose semantic treatments are quite remote from the simple model theory consideration of first-order logic and arithmetic. Thus, we draw the possibly surprising conclusions that the proof theory of linear logic provides a suitable framework for model checking. Many of the salient features of linear logic—lack of structural rules, two conjunctions and two disjunctions, polarization—play important roles in this framework. The role of linear logic here seems completely different and removed from, say, the use of linear logic to model multiset rewriting and Petri nets [10]: we use it instead as *the logic behind logic*. In order to capture model checking, we need to deal with possibly unbounded behaviors in specifications. Instead of using the rule of contraction (which states, for example, that the hypothesis B can be repeated as the two hypotheses B,B) we have used the theory of fixed points: there, unfolding replaces $\mu B\overline{t}$ with $(B(\mu B)\overline{t})$, thus copying the definition of B. The use of fixed points also allows for the direct and natural applications of the induction and coinduction principles. In the full version of this paper, we show how a focused proof system for $\mu\mathrm{MALL}^{=}$ can be used to describe large scale (synthetic) additive inference rules that are built from smaller scale inference rules that may be multiplicative.

There can be several benefits for establishing and developing model checking within proof theory. One way to integrate theorem provers and model checkers would be to allow them to exchange proof certificates in a common language of formulas and proofs. The logic of $\mu\mathrm{MALL}^{=}$ is close to the logic and proofs used in some inductive theorem provers. Also, linear logic is rich in duality. Certain techniques used in model checking topics should be expected to dualize well. For example, what is the dual notion for least fixed points of the notion of bisimulation-up-to? What does predicate abstraction look like when applied to greatest fixed points? Proof theory is a framework that supports rich abstractions, including term-level abstractions, such as bindings in terms. Thus, moving from model checking using first-order terms to using simply typed λ-terms is natural in proof theory: such proof theoretic investigations of model checking over linguistic structures including binders have been studied in [12] and have been

implemented in the Bedwyr system [3] which has been applied to various model checking problems related to the π-calculus [15, 16].

Acknowledgments. We thank the reviewers of an earlier draft of this abstract for their comments. This work has been funded by the ERC Advanced Grant ProofCert.

References

[1] Jean-Marc Andreoli (1992): *Logic Programming with Focusing Proofs in Linear Logic*. *J. of Logic and Computation* 2(3), pp. 297–347, doi:10.1093/logcom/2.3.297.

[2] David Baelde (2012): *Least and greatest fixed points in linear logic*. *ACM Trans. on Computational Logic* 13(1), doi:10.1145/2071368.2071370.

[3] David Baelde, Andrew Gacek, Dale Miller, Gopalan Nadathur & Alwen Tiu (2007): *The Bedwyr system for model checking over syntactic expressions*. In F. Pfenning, editor: *21th Conf. on Automated Deduction (CADE), LNAI* 4603, Springer, New York, pp. 391–397, doi:10.1007/978-3-540-73595-3_28.

[4] David Baelde & Dale Miller (2007): *Least and greatest fixed points in linear logic*. In N. Dershowitz & A. Voronkov, editors: *International Conference on Logic for Programming and Automated Reasoning (LPAR), LNCS* 4790, pp. 92–106, doi:10.1007/978-3-540-75560-9_9.

[5] E. Allen Emerson (2008): *The Beginning of Model Checking: A Personal Perspective*. In Orna Grumberg & Helmut Veith, editors: *25 Years of Model Checking - History, Achievements, Perspectives, Lecture Notes in Computer Science* 5000, Springer, pp. 27–45, doi:10.1007/978-3-540-69850-0_2.

[6] Gerhard Gentzen (1935): *Investigations into Logical Deduction*. In M. E. Szabo, editor: *The Collected Papers of Gerhard Gentzen*, North-Holland, Amsterdam, pp. 68–131, doi:10.1007/BF01201353.

[7] Jean-Yves Girard (1987): *Linear Logic*. *Theoretical Computer Science* 50, pp. 1–102, doi:10.1016/0304-3975(87)90045-4.

[8] Jean-Yves Girard (1991): *A new constructive logic: classical logic*. *Math. Structures in Comp. Science* 1, pp. 255–296 doi:10.1017/S0960129500001328.

[9] Jean-Yves Girard (1992): *A Fixpoint Theorem in Linear Logic*. An email posting to the mailing list linear@cs.stanford.edu.

[10] Max I. Kanovich (1995): *Petri Nets, Horn programs, Linear Logic and vector games*. *Annals of Pure and Applied Logic* 75(1–2), pp. 107–135, doi:10.1016/0168-0072(94)00060-G.

[11] Raymond McDowell & Dale Miller (2000): *Cut-elimination for a logic with definitions and induction*. *Theoretical Computer Science* 232, pp. 91–119, doi:10.1016/S0304-3975(99)00171-1.

[12] Dale Miller & Alwen Tiu (2005): *A proof theory for generic judgments*. *ACM Trans. on Computational Logic* 6(4), pp. 749–783, doi:10.1145/1094622.1094628.

[13] Peter Schroeder-Heister (1993): *Rules of Definitional Reflection*. In M. Vardi, editor: *8th Symp. on Logic in Computer Science*, IEEE Computer Society Press, IEEE, pp. 222–232, doi:10.1109/LICS.1993.287585.

[14] Helmut Schwichtenberg (1977): *Proof Theory: Some applications of cut-elimination*. In J. Barwise, editor: *Handbook of Mathematical Logic, Studies in Logic and the Foundations of Mathematics* 90, North-Holland, Amsterdam, pp. 739–782, doi:10.1016/S0049-237X(08)71124-8.

[15] Alwen Tiu & Dale Miller (2005): *A Proof Search Specification of the π-Calculus*. In: *3rd Workshop on the Foundations of Global Ubiquitous Computing, ENTCS* 138, pp. 79–101, doi:10.1016/j.entcs.2005.05.006.

[16] Alwen Tiu & Dale Miller (2010): *Proof Search Specifications of Bisimulation and Modal Logics for the π-calculus*. *ACM Trans. on Computational Logic* 11(2), doi:10.1145/1656242.1656248.

[17] Alwen Tiu & Alberto Momigliano (2012): *Cut elimination for a logic with induction and co-induction*. *Journal of Applied Logic* 10(4), pp. 330–367, doi:10.1016/j.jal.2012.07.007.