Classical Logic with Partial Functions

Hans de Nivelle

Instytut Informatyki, University of Wrocław, Poland

Abstract. We introduce a semantics for classical logic with partial functions. We believe that the semantics is natural. When a formula contains a subterm in which a function is applied outside of its domain, our semantics ensures that the formula has no truth-value, so that it cannot be used for reasoning. The semantics relies on order of formulas. In this way, it is able to ensure that functions and predicates are properly declared before they are used. We define a sequent calculus for the semantics, and prove that this calculus is sound and complete for the semantics.

1 Introduction

Partial functions occur frequently in mathematics and programming. In high-school, one is taught that one 'should not divide by zero'. Similarly, one is taught that $\log(0)$ and $\tan\frac{\pi}{2}$ 'do not exist'. In programming, partial functions are even more abundant. A pointer can only be dereferenced if it is not the null-pointer. A vector has only a first element if it is non-empty. A file can only be read from if it is in a good state.

One approach to partial functions is what is called *the traditional approach to partial functions* in [5] and [6]: In this approach, **(1)** variables and constants are always defined, and **(2)** formulas are always true or false. Atoms (including equalities) containing undefined subterms are always false. Although the traditional approach takes partiality serious, it does not fit with our view that ill-typed formulas should not be propositions at all. (Because no assumptions should be made about programs containing undefined values.)

For this reason, many authors ([1, 8]) have taken an approach based on three-valued Kleene logic. Three-valued logic is obtained by introducing an extra value $\mathbf{u}$, which is the truth-value for undefined propositions. It is assumed that the truth values are ordered as $\mathbf{f} < \mathbf{u} < \mathbf{t}$. Using this order, $P \vee Q$ can be defined as $\mathrm{MAX}_<(P, Q)$. Negation can be defined from $[\mathbf{f} \Rightarrow \mathbf{t},\ \mathbf{u} \Rightarrow \mathbf{u},\ \mathbf{t} \Rightarrow \mathbf{f}]$. Other operators can be introduced through standard equivalences. The well-definedness approach of [2, 9] is closely related to Kleene logic, although at first it may appear different, due to its proof-theoretic motivation. In the WD-approach, one has to prove that a formula is well-defined before it is used. It can be seen from the definitions in [9] that a formula is not well-defined iff it would take the value $\mathbf{u}$ in Kleene logic.

Kleene logic (and the WD-approach) are closer to our intuitions, but there is a difference: In our view, ill-defined formulas are not *unknown*, but *errors* after which nothing can be assumed. The justification for setting $\mathbf{t} \vee \mathbf{u} = \mathbf{t}$, is the fact

that whichever value **u** will take, the **t** ensures that the disjunction will be true. In our philosophy, nothing should be assumed about error values.

In addition to this philosophy, our system has some other, teachnical features that we believe may be useful: Preconditions of partial functions and types are treated in a unified way, and they are treated inside the logic itself, not by an external type system. This ensures that the logic does not have any built-in restrictions on type systems with which it is used. Both the type and the preconditions of a partial function can be expressed by ordinary formulas, as for example in $\forall x, y\ \mathrm{Nat}(x) \wedge \mathrm{Nat}(y) \to \mathrm{Nat}(x + y)$. Subtraction can be specified as a partial function by the formula: $\forall x, y\ \mathrm{Nat}(x) \wedge \mathrm{Nat}(y) \wedge x \geq y \to \mathrm{Nat}(x - y)$.

In our setting, partial functions are functions that sometimes have results about which nothing can be assumed. If the specification of the function requires that it throws exceptions, then something is assumed about the result. We view exceptions as a form of polymorphism, which is different from partiality. Our system is flexible enough to handle both polymorphism and partiality.

In order to connect preconditions to formulas, we introduce two binary operators: The first operator is the *lazy implication* operator $[A]B$, the second operator is the *lazy conjunction* operator $\langle A\rangle B$. We call the operators 'lazy' because they do not look at the second argument when the first argument is false. (Similar to `&&` and `||` in `C`). Because of this, B needs to be a proposition only when A is true, so that truth of A can be assumed when proving that B is a proposition. In the strict operators $A \to B$ and $A \wedge B$, the second argument must be a proposition independent of A.

We now introduce the syntax and semantics of our system, which we will call PCL (*Partial Classical Logic*).

Definition 1. *The set of* terms *of PCL (*partial classical logic*) is recursively defined by the following rule: If $t_1, \ldots, t_n$ are terms (with $n \geq 0$), and f is a function symbol with arity n, then $f(t_1, \ldots, t_n)$ is also a term. We call function symbols with arity* 0 constants *or* variables*, dependant on how they are used.*

Using the set of terms, we define the set of formulas of PCL recursively as follows:

- $\bot$ *and* $\top$ *are formulas.*
- *Every term A is a formula. We will call formulas of this form* atoms*.*
- *If t_1, t_2 are terms, then $t_1 = t_2$ is a formula.*
- *If A is a formula, then $\neg A$ is a formula.*
- *If A and B are formulas, then $A \wedge B$, $A \vee B$, $A \to B$, and $A \leftrightarrow B$ are formulas.*
- *If A and B are formulas, then $[A]B$ and $\langle A\rangle B$ are formulas.*
- *If x is a variable, A is a formula, then $\forall x\ A$ and $\exists x\ A$ are formulas.*
- *If A is a formula, then* $\mathrm{Prop}(A)$ *is a formula.*

The intuitive meaning of $\mathrm{Prop}(F)$ is 'F is a formula'. The logic is set up in such a way, that type correctness of formulas and terms must be proven within the calculus. As a consequence, there is no syntactic distinction between formulas and terms in Definition 1.

We will now introduce a lattice on non-truth values. It will be used in Definition 3, to ensure that logical operators behave in a predictable way when their arguments are not valid propositions. This has the advantage that many meta-properties of the logic can be formulated as equivalences. For example, without the lattice on non-truth values, $I(A) = I(A \wedge A)$ would not hold as equality. This would have no effect on the provable formulas, because the equality would still hold for the truth values. The lattice is only a trick to make the meta-properties nicer. We do not intend to use the lattice for abstraction, as is proposed in [7].

Definition 2. *Let S be a set. A relation $\sqsubseteq$ is called* a partial order *if it meets the following requirements:* **(1)** *For all $s \in S,\ s \sqsubseteq s$.* **(2)** *For all $s_1, s_2, s_3,\ \ s_1 \sqsubseteq s_2 \wedge s_2 \sqsubseteq s_3 \Rightarrow s_1 \sqsubseteq s_3$.* **(3)** *For all $s_1, s_2,\ s_1 \sqsubseteq s_2 \wedge s_2 \sqsubseteq s_1 \Rightarrow s_1 = s_2$. Let S' be a subset of S. We call $s \in S$ a* lower bound *of S' if for all $s' \in S',\ \ s \sqsubseteq s'$. We call s a greatest lower bound of S' if s is a lower bound of S', and for every lower bound $\hat{s}$ of S', we have $\hat{s} \sqsubseteq s$.*
We write $\sqcap S'$ for the greatest lower bound of S', if it exists. If S' is finite, we write $s_1 \sqcap s_2 \sqcap \cdots \sqcap s_n$ instead of $\sqcap\{s_1, s_2, \ldots, s_n\}$.

It is easily checked that the greatest lower bound is unique if it exists.

Definition 3. *An interpretation $I = (D, \mathbf{f}, \mathbf{t}, \sqsubseteq, [\,])$ is defined by*

- *A domain D.*
- *Two distinct truth constants $\mathbf{f}$ and $\mathbf{t}$, such that both of $\mathbf{f}, \mathbf{t} \in D$,*
- *A partial order $\sqsubseteq$ on $D \backslash \{\mathbf{f}, \mathbf{t}\}$, s.t. every non-empty $D' \subseteq D \backslash \{\mathbf{f}, \mathbf{t}\}$ has a greatest lower bound $\sqcap D'$, which is in $D \backslash \{\mathbf{f}, \mathbf{t}\}$.*
- *a function $[\,]$ that interprets function symbols as follows: If f is a function symbol with arity n, then $[f]$ is a total function from D^n to D.*

As said above, the role of the partial order $\sqsubseteq$ is to obtain predictable behaviour of the logical operators when they are applied on non-Boolean objects.

Definition 4. *Let $I = (D, \mathbf{f}, \mathbf{t}, \sqsubseteq, [\,])$ be an interpretation. We recursively define the* interpretation $I(F)$ *of a formula F as follows:*

- $I(\bot) = \mathbf{f},\ \ I(\top) = \mathbf{t}$.
- *If $F = [f]$, then $I(\ f(t_1, \ldots, t_n)\ ) = F(I(t_1), \ldots, I(t_n))$.*
- *If $I(t_1) = I(t_2)$, then $I(t_1 = t_2) = \mathbf{t}$. Otherwise, $I(t_1 = t_2) = \mathbf{f}$.*
- *If $I(A) = \mathbf{t}$, then $I(\neg A) = \mathbf{f}$. If $I(A) = \mathbf{f}$, then $I(\neg A) = \mathbf{t}$. Otherwise $I(\neg A) = I(A)$.*
- *We characterize the strict binary operators:*
  - *If $I(A) \in \{\mathbf{f}, \mathbf{t}\}$, and $I(B) \notin \{\mathbf{f}, \mathbf{t}\}$, then $I(A \wedge B) = I(A \vee B) = I(A \rightarrow B) = I(A \leftrightarrow B) = I(B)$.*
  - *If $I(A) \notin \{\mathbf{f}, \mathbf{t}\}$, and $I(B) \in \{\mathbf{f}, \mathbf{t}\}$, then $I(A \wedge B) = I(A \vee B) = I(A \rightarrow B) = I(A \leftrightarrow B) = I(A)$.*
  - *If both $I(A), I(B) \notin \{\mathbf{f}, \mathbf{t}\}$, then $I(A \wedge B) = I(A \vee B) = I(A \rightarrow B) = I(A \leftrightarrow B) = I(A) \sqcap I(B)$.*

- *If both of* $I(A), I(B) \in \{\mathbf{f}, \mathbf{t}\}$, *then* $\wedge, \vee, \rightarrow, \leftrightarrow$ *are characterized by the following (standard) truth table:*

$I(A)$	$I(B)$	$I(A \wedge B)$	$I(A \vee B)$	$I(A \rightarrow B)$	$I(A \leftrightarrow B)$
$\mathbf{f}$	$\mathbf{f}$	$\mathbf{f}$	$\mathbf{f}$	$\mathbf{t}$	$\mathbf{t}$
$\mathbf{f}$	$\mathbf{t}$	$\mathbf{f}$	$\mathbf{t}$	$\mathbf{t}$	$\mathbf{f}$
$\mathbf{t}$	$\mathbf{f}$	$\mathbf{f}$	$\mathbf{t}$	$\mathbf{f}$	$\mathbf{f}$
$\mathbf{t}$	$\mathbf{t}$	$\mathbf{t}$	$\mathbf{t}$	$\mathbf{t}$	$\mathbf{t}$

– *We characterize the lazy binary operators:*
  - *If* $I(A) = \mathbf{f}$, *then* $I(\ [A]B\ ) = \mathbf{t}$, *and* $I(\ \langle A\rangle B\ ) = \mathbf{f}$.
  - *If* $I(A) \notin \{\mathbf{f}, \mathbf{t}\}$, *and* $I(B) \in \{\mathbf{f}, \mathbf{t}\}$, *then* $I(\ [A]B\ ) = I(\ \langle A\rangle B\ ) = I(A)$.
  - *If both* $I(A), I(B) \notin \{\mathbf{f}, \mathbf{t}\}$, *then* $I(\ [A]B\ ) = I(\ \langle A\rangle B\ ) = I(A) \sqcap I(B)$.
  - *If* $I(A) = \mathbf{t}$, *then* $I(\ [A]B\ ) = I(\ \langle A\rangle B\ ) = I(B)$.

– *Next come the quantifiers: Let* x *be some variable. Let* F *be a formula. Let* $R = \{\ I^x_d(d) \mid d \in D\}$, *where* I^x_d *is defined as usual.*
  - *If* $R \not\subseteq \{\mathbf{f}, \mathbf{t}\}$, *then* $I(\ \forall x\ F\ ) = I(\ \exists x\ F\ ) = \sqcap(R \backslash \{\mathbf{f}, \mathbf{t}\})$.
  - *If* $R = \{\mathbf{f}\}$, *then* $I(\ \forall x\ F\ ) = I(\ \exists x\ F\ ) = \mathbf{f}$.
  - *If* $R = \{\mathbf{t}\}$, *then* $I(\ \forall x\ F\ ) = I(\ \exists x\ F\ ) = \mathbf{t}$.
  - *If* $R = \{\mathbf{f}, \mathbf{t}\}$, *then* $I(\ \forall x\ F\ ) = \mathbf{f}$ *and* $I(\ \exists x\ F\ ) = \mathbf{t}$.

– *It remains to characterize* Prop. *If* $I(A) \in \{\mathbf{f}, \mathbf{t}\}$, *then* $I(\ \mathrm{Prop}(A)\ ) = \mathbf{t}$. *Otherwise,* $I(\ \mathrm{Prop}(A)\ ) = \mathbf{f}$.

Valid judgments will be represented by sequents.

Definition 5. *A* context *is a finite sequence of formulas* $\Gamma_1, \ldots, \Gamma_n$. *A* sequent *is an object of form* $\Gamma \vdash A$, *in which* Γ *is a context and* A *is a formula.*

We introduce two notions of validity for sequents. The first notion is the standard notion. The second, stronger notion is the notion that we will be using.

Definition 6. *Let* $\Gamma_1, \ldots, \Gamma_n \vdash A$ *be a sequent. We call* $\Gamma_1, \ldots, \Gamma_n \vdash A$ valid *if in every interpretation* $I = (D, \mathbf{f}, \mathbf{t}, \sqsubseteq, [\ ])$, *s.t.* $I(\Gamma_1) = \cdots = I(\Gamma_n) = \mathbf{t}$, *we also have* $I(A) = \mathbf{t}$. *We call the sequent* $\Gamma_1, \ldots, \Gamma_n \vdash A$ strongly valid, *if it is valid, and in addition the context* $\Gamma_1, \ldots, \Gamma_n$ *has the following property: Either for all* i *with* $1 \leq i \leq n$, *we have* $I(\Gamma_i) = \mathbf{t}$, *or for the first* i *with* $1 \leq i \leq n$ *that has* $I(\Gamma_i) \neq \mathbf{t}$, *we have* $I(\Gamma_i) = \mathbf{f}$.

The sequent $A \vdash A$ is valid, but not strongly valid. One can take an interpretation I with $I(A) = \mathbf{e}$, for some $\mathbf{e} \notin \{\mathbf{f}, \mathbf{t}\}$. The sequent $\mathrm{Prop}(A), A \vdash A$ is strongly valid because it is valid, and if $I(A) = \mathbf{e}$, then $I(\mathrm{Prop}(A)) = \mathbf{f}$. Similarly, the sequent $\vdash A \vee \neg A$ is valid, but not strongly valid. The sequent $\mathrm{Prop}(A) \vdash A \vee \neg A$ is strongly valid.

The notion of strong validity captures the fact that functions and predicates have to be declared before they are used. If one has a context Γ_1 and a formula A, for which $\Gamma_1 \not\vdash \mathrm{Prop}(A)$, then there exists an interpretation I, in which $I(\Gamma_1) = \mathbf{t}$ and $I(A) \notin \{\mathbf{f}, \mathbf{t}\}$, so that no sequent of form $\Gamma_1, A, \Gamma_2 \vdash B$ can be strongly valid. The following example illustrates declaration of partial functions, and usage of the lazy operators $\langle\ \rangle$ and $[\ ]$:

F1 $\forall x$ Prop(Nat(x)),
F2 $\forall xy$ Nat(x) $\wedge$ Nat(y) $\rightarrow$ Prop($x \geq y$),
F3 $\forall xy$ [Nat(x) $\wedge$ Nat(y)] $x \geq y \rightarrow$ Nat($x - y$),
F4 $\forall xy$ [Nat(x) $\wedge$ Nat(y)] $x \geq y \rightarrow \exists z$ $\langle$ Nat(z) $\rangle$ $\langle$ $x \geq z$ $\rangle$ $x - z = y$.

In F2, the relation $\geq$ is defined on natural numbers. This can be done with standard implication $\rightarrow$ because Prop($x \geq y$) is always Prop by itself. In F3, subtraction $x - y$ is declared to return Nat on the condition that $x \geq y$. Here lazy implication must be used, because without Nat(x), Nat(y), $\quad x \geq y$ would not be Prop. In F4, $\langle\ \rangle$ must be used with $\exists$ to declare z in Nat, but also to declare $x \geq z$, because otherwise $x - z$ would not be Nat.

We aim to define a sequent calculus that is able to model strong validity. It turns out that definition of this calculus is simpler when one defines a one-sided calculus, in which sequents are refuted instead of proven. The reasons for this are the following: Validity of Prop(A) $\vdash A \vee \neg A$ and the fact that the semantics is based on truth-values, suggest that PCL is essentially classical (in contract to intuitionistic). At the same time, the notion of strong validity depends on the order of formulas in the sequent. Allowing formulas to freely move from the premise to the conclusion in a sequent, which would be needed for classical $\neg$-rules, and simultaneously keeping track of the order of the formulas in the sequent, is tedious. It can be avoided by using one-sided sequents.

Definition 7. *A* one-sided sequent *is an object of form* $\Gamma_1, \ldots, \Gamma_n \vdash$, *in which* $\Gamma_1, \ldots, \Gamma_n$ $(n \geq 0)$ *is a sequence of formulas. We say that* $\Gamma_1, \ldots, \Gamma_n \vdash$ fails *in an interpretation* I *if there is an* i, $(1 \leq i \leq n)$, *s.t.* $I(\Gamma_i) \neq \mathbf{t}$. *We will usually write 'sequent' instead of 'one-sided sequent', since it is always clear from the form which type is meant.*

We say that $\Gamma \vdash$ fails strongly *in* I *if there is an* i, $(1 \leq i \leq n)$, *s.t.* $I(\Gamma_i) = \mathbf{f}$ *and for all* j, $(1 \leq j < i)$, $\quad I(\Gamma_j) = \mathbf{t}$. *If we want to stress that* Γ_i *is the first formula in* Γ *with* $I(\Gamma_i) \neq \mathbf{t}$ *(which implies that* $I(\Gamma_i) = \mathbf{f}$*), then we say that* Γ fails strongly at Γ_i *in* I.

We call the one-sided sequent $\Gamma \vdash$ unsatisfiable *if it fails in every interpretation. We call* Γ strongly unsatisfiable *if it fails strongly in every interpretation.*

Theorem 1. *Let* $\Gamma \vdash A$ *be a sequent.* $\Gamma \vdash A$ *is strongly valid if and only if the one-sided sequent* $\Gamma, \neg A \vdash$ *is strongly unsatisfiable.*

Proof. Write $\Gamma = \Gamma_1, \ldots, \Gamma_n \vdash$ with $n \geq 0$. For convenience, define $\Gamma_{n+1} := \neg A$.

Assume that $\Gamma \vdash A$ is strongly valid. We have to show that the sequent $\Gamma_1, \Gamma_2, \ldots, \Gamma_{n+1} \vdash$ is strongly unsatisfiable. Let I be an arbitrary interpretation. We have to show that there exists an i, $(1 \leq i \leq n+1)$ with property $\Phi(i)$, where $\Phi(i)$ is the property that $I(\Gamma_i) = \mathbf{f}$, and for all j, $(1 \leq j < i)$, $\ I(\Gamma_j) = \mathbf{t}$. We distinguish two cases:

- If for all i, $1 \leq i \leq n$, $\ I(\Gamma_i) = \mathbf{t}$, then it follows from validity of $\Gamma \vdash A$ that $I(A) = \mathbf{t}$, so that $I(\neg A) = \mathbf{f}$. Since $\neg A = \Gamma_{n+1}$, we have $\Phi(n+1)$.
- If there is an i with $1 \leq i \leq n$, s.t. $I(\Gamma_i) \neq \mathbf{t}$, then by strong validity of $\Gamma \vdash A$ (See Definition 6), we have $I(\Gamma_i) = \mathbf{f}$ for the first i with $I(\Gamma_i) \neq \mathbf{t}$. It follows that we have $\Phi(i)$.

In order to show the other direction, assume that $\Gamma_1, \ldots, \Gamma_n, \Gamma_{n+1} \vdash$ is strongly unsatisfiable. We first show that $\Gamma_1, \ldots, \Gamma_n \vdash A$ is valid. Let I be an interpretation. Assume that $I(\Gamma_1) = I(\Gamma_2) = \cdots = I(\Gamma_n) = \mathbf{t}$. It follows from the strong unsatisfiability of $\Gamma_1, \ldots, \Gamma_n, \Gamma_{n+1} \vdash$ that $I(\Gamma_{n+1}) = \mathbf{f}$, so that $I(A) = \mathbf{t}$. Next we show the additional property that makes $\Gamma_1, \ldots, \Gamma_n \vdash A$ strongly valid. If no i has $I(\Gamma_i) \neq \mathbf{t}$, then we are done. Otherwise, let i be the first position where $I(\Gamma_i) \neq \mathbf{t}$. If we would have $I(\Gamma_i) \neq \mathbf{f}$, then this would contradict strong unsatisfiability of the sequent $\Gamma_1, \ldots, \Gamma_n, \Gamma_{n+1} \vdash$, so that the proof is complete.

Using Theorem 1, the conclusion of a sequent can be moved to the left hand side, after which it can be treated in the same way as the other premises. This has the advantage that one can delete half of the rules from the sequent calculus, and it avoids the burden of keeping track of the order of formulas spread between the premises and the conclusions. In order to further simplify the calculus, we use the reduction rules in Figure 1 and Figure 2. Figure 1 contains rules for pushing negation inwards, while Figure 2 contains rules for pushing Prop inwards. Most rules in Figure 1 look familiar, but their validity still needs to be checked in the context of PCL. It can be checked (by case analysis) that for every interpretation I, for each rule $A \Rightarrow B$ in Figure 1 or Figure 2, we have $I(A) = I(B)$, so that the equivalences can be freely used in proofs. Figure 1 and Figure 2 ensure that $\neg$ or Prop never needs to be the main operator of a formula. The only cases where Prop and $\neg$ cannot be eliminated are in formulas of form $\phi_1(\phi_2(A))$, where A is an atom, ϕ_2 is either Prop or nothing, and ϕ_1 is either $\neg$ or nothing. Such formulas play the same role as literals in first-order logic. One can either simplify the sequent completely before proof search, or apply the rules 'lazily,' i.e. only when $\neg$ or Prop stands in the way of a rule application.

Fig. 1. Reduction Rules for $\neg$

$$
\begin{array}{llll}
\neg\bot & \Rightarrow \top, & \neg\top & \Rightarrow \bot \\
\neg\neg A & \Rightarrow A, & & \\
\neg(\ \langle A\rangle B\ ) & \Rightarrow [A]\neg B, & \neg(\ [A]B\ ) & \Rightarrow \langle A\rangle \neg B \\
\neg(A \wedge B) & \Rightarrow \neg A \vee \neg B, & \neg(A \vee B) & \Rightarrow \neg A \wedge \neg B \\
\neg(A \rightarrow B) & \Rightarrow A \wedge \neg B, & \neg(A \leftrightarrow B) & \Rightarrow A \leftrightarrow \neg B \\
\neg\forall x\ F, & \Rightarrow \exists x\ \neg F & \neg\exists x\ F & \Rightarrow \forall x\ \neg F
\end{array}
$$

Figure 3 contains the rules of the sequent calculus Seq_{PCL}. Most rules probably look familiar, but there are pitfalls. For example, the rule for $\wedge$-introduction would be unsound if the second premise would be removed. It would then be possible that in some interpretation $I = (D, \mathbf{f}, \mathbf{t}, \sqsubseteq, [\,])$, one has $I(\Gamma_1) = \mathbf{t}$, $I(A) = \mathbf{f}$, and $I(B) \notin \{\mathbf{f}, \mathbf{t}\}$. In that case the left premise would fail strongly, while the conclusion would fail only weakly. Similarly, the rule for $\forall$-introduction would be unsound if one would not keep a copy of $\forall x\ P(x)$ in the premise before $P(t)$. It could happen that in some interpretation I, $\quad I(P(t)) = \mathbf{t}$, while at the same time $I(\forall x\ P(x)) \notin \{\mathbf{f}, \mathbf{t}\}$.

Fig. 2. Reduction Rules for Prop

$$
\begin{array}{lll}
\mathrm{Prop}(\top) & \Rightarrow \top & \\
\mathrm{Prop}(\bot) & \Rightarrow \top & \\
\mathrm{Prop}(\neg A) & \Rightarrow \mathrm{Prop}(A) & \\
\mathrm{Prop}(\mathrm{Prop}(A)) & \Rightarrow \top & \\
 & & \\
\mathrm{Prop}(A \wedge B) & \Rightarrow \mathrm{Prop}(A) \wedge \mathrm{Prop}(B) & (\text{or } \langle\ \mathrm{Prop}(A)\ \rangle\ \mathrm{Prop}(B)\ ) \\
\mathrm{Prop}(A \vee B) & \Rightarrow \mathrm{Prop}(A) \wedge \mathrm{Prop}(B) & (\text{or } \langle\ \mathrm{Prop}(A)\ \rangle\ \mathrm{Prop}(B)\ ) \\
\mathrm{Prop}(A \to B) & \Rightarrow \mathrm{Prop}(A) \wedge \mathrm{Prop}(B) & (\text{or } \langle\ \mathrm{Prop}(A)\ \rangle\ \mathrm{Prop}(B)\ ) \\
\mathrm{Prop}(A \leftrightarrow B) & \Rightarrow \mathrm{Prop}(A) \wedge \mathrm{Prop}(B) & (\text{or } \langle\ \mathrm{Prop}(A)\ \rangle\ \mathrm{Prop}(B)\ ) \\
 & & \\
\mathrm{Prop}(\ \langle A\rangle B\ ) & \Rightarrow \langle\ \mathrm{Prop}(A)\ \rangle(\ A \to \mathrm{Prop}(B)\ ) & \\
\mathrm{Prop}(\ [A]B\ ) & \Rightarrow \langle\ \mathrm{Prop}(A)\ \rangle(\ A \to \mathrm{Prop}(B)\ ) & \\
 & & \\
\mathrm{Prop}(\forall x\ F) & \Rightarrow \forall x\ \mathrm{Prop}(F) & \\
\mathrm{Prop}(\exists x\ F) & \Rightarrow \forall x\ \mathrm{Prop}(F) & \\
 & & \\
\mathrm{Prop}(t_1 = t_2) & \Rightarrow \top &
\end{array}
$$

If one would remove the A from the second premise in [ ]-introduction, the rule would still be sound, but become too weak for completeness. The problem would show up when $\mathrm{Prop}(B)$ depends on A.

In contrast to standard first-order logic, a sequent of form $\Gamma, A, \neg A \vdash$ is not automatically an axiom. It is possible that $\Gamma \vdash$ fails weakly, or $I(\Gamma) = \mathbf{t}$ and $I(A) \notin \{\mathbf{f}, \mathbf{t}\}$. Both cases are covered by requiring the additional sequent $\Gamma,\ \neg\mathrm{Prop}(A) \vdash$.

We will prove soundness of the rules for $\langle\ \rangle$, $\vee$, and $\exists$. Most of the other rules can be reduced to $\langle\ \rangle$ and $\vee$, by using the equivalences in Figure 4. The remaining rules can be checked by case analysis.

Theorem 2. *Let $\Gamma_{\langle A\rangle B}$ be a sequent of form $\Gamma_1, \ldots, \Gamma_m,\ \langle A\rangle B,\ \Gamma'_1, \ldots, \Gamma'_n \vdash$. Let $\Gamma_{A,B}$ be the sequent $\Gamma_1, \ldots, \Gamma_m, A, B, \Gamma'_1, \ldots, \Gamma'_n \vdash$. Let I be an interpretation. Then $\Gamma_{\langle A\rangle B}$ fails strongly in I iff $\Gamma_{A,B}$ fails strongly in I.*

Proof. Assume that $\Gamma_{\langle A\rangle B}$ fails strongly in I. This means that the first formula F in $\Gamma_{\langle A\rangle B}$, for which $I(F) \neq \mathbf{t}$, has $I(F) = \mathbf{f}$.

- If F is among the Γ_i, then it is immediate that $\Gamma_{A,B}$ fails strongly in I.
- If $F = \langle A\rangle B$, then either $I(A) = \mathbf{f}$, or ($I(A) = \mathbf{t}$ and $I(B) = \mathbf{f}$). Since $I(\Gamma_1) = \cdots = I(\Gamma_m) = \mathbf{t}$, in both cases $\Gamma_{A,B}$ fails strongly in I.
- If F is among the Γ'_j, then F also occurs in $\Gamma_{A,B}$. We know that $I(\Gamma_1) = \cdots = I(\Gamma_m) = \mathbf{t}$. From the fact that $I(\ \langle A\rangle B\ ) = \mathbf{t}$, follows that $I(A) = I(B) = \mathbf{t}$. Since we assumed that $I(\Gamma'_1) = \cdots = I(\Gamma'_{j-1}) = \mathbf{t}$, it follows that F is the first formula in $\Gamma_{A,B}$ for which $I(F) \neq \mathbf{t}$. Since $I(F) = \mathbf{f}$, we know that $\Gamma_{A,B}$ fails strongly in I.

Fig. 3. Rules of Seq_{PCL} :

Rules for $\langle\ \rangle$ and $\vee$

$$\frac{\Gamma_1, A, B, \Gamma_2 \vdash}{\Gamma_1,\ \langle A\rangle\ B,\ \Gamma_2 \vdash} \qquad \frac{\Gamma_1, A, \Gamma_2 \vdash \quad \Gamma_1, B, \Gamma_2 \vdash}{\Gamma_1,\ A \vee B,\ \Gamma_2 \vdash}$$

Rules for $\wedge$ and $[\ ]$

$$\frac{\Gamma_1, A, B, \Gamma_2 \vdash \quad \Gamma_1, B, A, \Gamma_2 \vdash}{\Gamma_1,\ A \wedge B,\ \Gamma_2 \vdash} \qquad \frac{\Gamma_1,\ \neg A,\ \Gamma_2 \vdash \quad \Gamma_1, A, B, \Gamma_2 \vdash}{\Gamma_1,\ [A]B,\ \Gamma_2 \vdash}$$

Rules for $\rightarrow$ and $\leftrightarrow$

$$\frac{\Gamma_1,\ \neg A,\ \Gamma_2 \quad \Gamma_1, B, \Gamma_2 \vdash}{\Gamma_1,\ A \rightarrow B,\ \Gamma_2 \vdash} \qquad \frac{\Gamma_1,\ A, B,\ \Gamma_2 \vdash \quad \Gamma_1,\ \neg B, \neg A,\ \Gamma_2 \vdash}{\Gamma_1,\ A \leftrightarrow B,\ \Gamma_2 \vdash}$$

Rules for $\forall$ and $\exists$

$$\frac{\Gamma_1,\ \forall x\ P(x),\ P(t),\ \Gamma_2 \vdash}{\Gamma_1,\ \forall x\ P(x),\ \Gamma_2 \vdash} \qquad \frac{\Gamma_1,\ P(x),\ \Gamma_2 \vdash}{\Gamma_1,\ \exists x\ P(x),\ \Gamma_2 \vdash}$$

(In the $\forall$-rule, t must be a term. In the $\exists$-rule x must be not free in Γ_1 or Γ_2.)

Equivalence If $A \Rightarrow B$ is an instance of one of the rules in figure 2 or figure 1, then the following derivation is possible:

$$\frac{\Gamma_1, B, \Gamma_2 \vdash}{\Gamma_1, A, \Gamma_2 \vdash}$$

Axioms

$$\frac{\Gamma,\ \neg\mathrm{Prop}(A) \vdash}{\Gamma, A, \neg A \vdash} \qquad \frac{\Gamma,\ \neg\mathrm{Prop}(A) \vdash}{\Gamma, \neg A, A \vdash} \qquad \frac{}{\bot \vdash}$$

Weakening

$$\frac{\Gamma_1, \neg\mathrm{Prop}(A) \vdash \quad \Gamma_1, \Gamma_2 \vdash}{\Gamma_1, A, \Gamma_2 \vdash} \qquad \frac{\Gamma \vdash}{\Gamma, A \vdash} \qquad \frac{\Gamma_1, \Gamma_2 \vdash}{\Gamma_1, \top, \Gamma_2 \vdash}$$

(In the first two rules, A can be an arbitrary formula.)

Contraction, Cut

$$\frac{\Gamma_1, A, \Gamma_2, A, \Gamma_3 \vdash}{\Gamma_1, A, \Gamma_2, \Gamma_3 \vdash} \qquad \frac{\Gamma_1,\ \neg A \vdash \quad \Gamma_1, A, \Gamma_2 \vdash}{\Gamma_1, \Gamma_2 \vdash}$$

(A can be an arbitrary formula.)

Equality

$$\frac{}{\mathrm{Prop}(A), A,\ t_1 = u_1, \ldots, t_n = u_n, \neg A' \vdash} \qquad \frac{}{t_1 = u_1, \ldots, t_n = u_n, t \neq u \vdash}$$

In the first axiom, it must be the case that $A, t_1 = u_1, \ldots, t_n = u_n \models A'$ in the standard theory of equality. In the second axiom, it must be the case that $t_1 = u_1, \ldots, t_n = u_n \vdash t = u$ in the standard theory of equality.

Fig. 4. Reduction of remaining rules to $\langle\ \rangle$ and $\vee$

$\wedge$	$A \wedge B \Rightarrow (\ \langle A\rangle B\ ) \vee (\ \langle B\rangle A\ )$	$\top$	$\langle A\rangle\top \Rightarrow A$
$[\,]$	$[A]B \Rightarrow \neg A \vee (\ \langle A\rangle B\ )$	$\top$	$\langle\top\rangle A \Rightarrow A$
$\rightarrow$	$A \rightarrow B \Rightarrow \neg A \vee B$		
$\leftrightarrow$	$A \leftrightarrow B \Rightarrow (\ \langle A\rangle B\ ) \vee (\ \langle\neg A\rangle\neg B\ )$	$\forall$	$\forall x\ P(x) \Rightarrow \langle\ \forall x\ P(x)\ \rangle\ P(t)$

For the other direction, assume that $\Gamma_{A,B}$ fails strongly in I. Let F be the first formula in $\Gamma_{A,B}$ for which $I(F) \neq \mathbf{t}$. We have $I(F) = \mathbf{f}$.

- If F is among the Γ_i, then it is immediate that $\Gamma_{\langle A\rangle B}$ fails strongly in I.
- If $F = A$, then $I(\ \langle A\rangle B\ ) = \mathbf{f}$, and $I(\Gamma_1) = \cdots = I(\Gamma_m) = \mathbf{t}$, so that $\Gamma_{\langle A\rangle B}$ fails strongly in I at formula A.
- If $F = B$, then we know that $I(A) = \mathbf{t}$, so that $I(\ \langle A\rangle B\ ) = \mathbf{f}$. Since $I(\Gamma_1) = \cdots I(\Gamma_m) = \mathbf{t}$, it follows that $\Gamma_{\langle A\rangle B}$ fails strongly in I at formula B.
- If F is among the Γ'_j, then F also occurs in $\Gamma_{\langle A\rangle B}$, so that it is sufficient to show that there is no formula F' before F in $\Gamma_{\langle A\rangle B}$, s.t. $I(F') \neq \mathbf{t}$. The only candidate is $\langle A\rangle B$, because all other formulas were copied from $\Gamma_{A,B}$. But since we know that $I(A) = I(B) = \mathbf{t}$, it follows that $I(\ \langle A\rangle B\ ) = \mathbf{t}$.

Theorem 3. *Let $\Gamma_{A\vee B}$ be a sequent of form $\Gamma_1, \ldots, \Gamma_m, A \vee B, \Gamma'_1, \ldots, \Gamma'_n \vdash$. Let $\Gamma_A = \Gamma_1, \ldots, \Gamma_m, A, \Gamma'_1, \ldots, \Gamma'_n \vdash$, and let $\Gamma_B = \Gamma_1, \ldots, \Gamma_m, B, \Gamma'_1, \ldots, \Gamma'_n \vdash$. Let I be an interpretation. The sequent $\Gamma_{A\vee B}$ fails strongly in I iff both of Γ_A and Γ_B fail strongly in I.*

Proof. Because of space restriction, we do some handwaving. Using Theorem 2 and Figure 4, we can collapse $\Gamma_1, \ldots, \Gamma_m$ and $\Gamma'_1, \ldots, \Gamma'_n$ into single formulas of form $C_1 = \langle\Gamma_1\rangle \cdots \langle\Gamma_m\rangle\top$ and $C_2 = \langle\Gamma'_1\rangle \cdots \langle\Gamma'_n\rangle\top$.

After the replacement, the proof reduces to showing that $C_1, A\vee B, C_2 \vdash$ fails strongly in I iff both of $C_1, A, C_2 \vdash$ and $C_1, B, C_2 \vdash$ fail strongly in I. This can be checked by case analysis. Each of C_1, A, B, C_2 can be either $\mathbf{f}, \mathbf{t}$ or $\notin \{\mathbf{f}, \mathbf{t}\}$. This results in $3^4 = 81$ cases, which can be checked. [1]

Theorem 4. *Let $\Gamma_\exists$ be a sequent of form $\Gamma_1, \ldots, \Gamma_m,\ \exists x\ P(x),\ \Gamma'_1, \ldots, \Gamma'_n \vdash$. Let Γ_x be the sequent $\Gamma_x = \Gamma_1, \ldots, \Gamma_m,\ P(x),\ \Gamma'_1, \ldots, \Gamma'_n \vdash$. Assume that x is not free in any of the formulas $\Gamma_1, \ldots, \Gamma_m, \Gamma'_1, \ldots, \Gamma'_n$.*

Let $I = (D, \mathbf{f}, \mathbf{t}, \sqsubseteq, [\ ])$ be an arbitrary interpretation. Then $\Gamma_\exists$ fails strongly in I iff for every $d \in D$, the sequent Γ_x fails strongly in $I^x_d = (D, \mathbf{f}, \mathbf{t}, \sqsubseteq, [\ ]^x_d)$.

Proof. In the proof, we make use of the fact that $I(\Gamma_i) = I^x_d(\Gamma_i)$ and $I(\Gamma'_j) = I^x_d(\Gamma'_j)$, because x is not free in Γ_i, Γ'_j.

Assume that $\Gamma_\exists$ fails strongly in I. This means that for the first formula F in $\Gamma_\exists$ with $I(F) \neq \mathbf{t}$, one has $I(F) = \mathbf{f}$.

[1] The cases have been checked by a computer program, together with all cases for the reductions in Figure 1, 2 and 4

- If F is one of the Γ_i, then $I(\Gamma_i) = I^x_d(\Gamma_i) = \mathbf{f}$, and for all i', $(1 \leq i' \leq i)$, $I(\Gamma_{i'}) = I^x_d(\Gamma_{i'}) = \mathbf{t}$, so that Γ_x fails strongly at Γ_i in every I^x_d.
- If F is $\exists x\ P(x)$, then the fact that $I(\ \exists x\ P(x)\ ) = \mathbf{f}$, implies that for every $d \in D$, $I^x_d(\ P(x)\ ) = \mathbf{f}$. Since for every i, $I(\Gamma_i) = I^x_d(\Gamma_i) = \mathbf{t}$, it follows that Γ_x fails strongly at formula $P(x)$ in every interpretation I^x_d.
- If F is one of the Γ'_j, then we know that for every $d \in D$, $I(\Gamma_1) = I^x_d(\Gamma_1) = \cdots = I(\Gamma_m) = I^x_d(\Gamma_m) = \mathbf{t}$. It can be seen from Definition 4 that $I(\ \exists x\ P(x)\ ) = \mathbf{t}$ implies that for every $d \in D$, either $I^x_d(\ P(x)\ ) = \mathbf{f}$, or $I^x_d(\ P(x)\ ) = \mathbf{t}$. If $I^x_d(\ P(x)\ ) = \mathbf{f}$, then Γ_x strongly fails at $P(x)$ in I^x_d. Otherwise, we have $I^x_d(\ P(x)\ ) = \mathbf{t}$ and $I(\Gamma'_1) = I^x_d(\Gamma'_1) = \cdots = I(\Gamma'_{j-1}) = I^x_d(\Gamma'_{j-1}) = \mathbf{t}$, and $I(\Gamma_j) = I^x_d(\Gamma_j) = \mathbf{f}$, so that Γ_x fails strongly at Γ'_j in I^x_d

For the other direction, we use contraposition, so assume that $\Gamma_\exists$ does not fail strongly in I. We show that there exists a $d \in D$, s.t. Γ_x does not fail strongly in I^x_d. We distinguish the following cases:

- The first formula F with $I(F) \neq \mathbf{t}$ is among the Γ_i and $I(\Gamma_i) \neq \mathbf{f}$. Since for all i, $(1 \leq i \leq m)$, $I(\Gamma_i) = I^x_d(\Gamma_i)$, the sequent Γ_x does not fail strongly in any I^x_d.
- The first formula F with $I(F) \neq \mathbf{t}$ is $\exists x\ P(x)$, and $I(\ \exists x\ P(x)\ ) \neq \mathbf{f}$. It follows from Definition 4 that there is a $d \in D$, s.t. $I^x_d(\ P(x)\ ) \notin \{\mathbf{f}, \mathbf{t}\}$. In the corresponding I^x_d, the sequent Γ_x does not fail strongly.
- The first formula F for which $I(F) \neq \mathbf{t}$ is among the Γ'_j, and $I(\Gamma'_j) \neq \mathbf{f}$. Since $I(\ \exists x\ P(x)\ ) = \mathbf{t}$, there exists a $d \in D$, s.t. $I^x_d(\ P(x)\ ) = \mathbf{t}$. In I^x_d, we have $I(\Gamma_1) = I^x_d(\Gamma_1) = \cdots = I(\Gamma_m) = I^x_d(\Gamma_m) = \mathbf{t}$, and $I(\Gamma'_1) = I^x_d(\Gamma'_1) = \cdots = I(\Gamma'_{j-1}) = I^x_d(\Gamma'_{j-1}) = \mathbf{t}$, so that Γ_x does not fail strongly in I^x_d.
- There is no formula F for which $I(F) \neq \mathbf{t}$ in $\Gamma_\exists$. This case is analogeous to the previous case.

2 Completeness

In the previous section we introduced Seq_{PCL} and proved its soundness. In the rest of the paper, we will give an outline of the completeness proof. If there would exist no $\forall$-quantifier, we would already have the completeness proof at this point. The calculus has sufficiently many equivalence preserving rules: For every interpretation I, the conclusion of the rule fails strongly in I iff all premises of the rule strongly fail in I. Using the equivalence preserving rules, it is possible to break down the goal sequent into a set of sequents that contain only (negations of) (Props of) atoms. These simple sequents are either axioms, or there exists a model in which they do not fail strongly. By the equivalence property, this implies that we either have a proof of the original sequent, or a counter interpretation.

In order to include $\forall$ in the completeness proof, we would like to proceed in a standard way: Allow each $\forall$-quantifier to have some fixed set of instances. If no proof can be constructed, then grant each $\forall$-quantifier one instance more. This process either results in a proof, or it leads to an increasing sequence of sets of atoms from which one can read of an interpretation in the limit.

Unfortunately, there is a problem with this approach, which is caused by the fact that in most cases the limit will be infinite. We want to show that the limit sequent does not fail strongly in the limit interpretation I (and that none of the sequents on the way fails strongly in I), but we have no concept of strong failure for infinite sequents. One possible solution would be to introduce infinite sequents. Infinite sequents can be defined by labelling a well-founded set with formulas. The sequent fails strongly if every element in the well-founded set that is labelled with a non-true formula, has an element before it, that is labelled with a false formula. Finite sequents would correspond to linearly ordered, finite sets. It turns out that there is a simpler approach, which avoids introducing special notions for infinite sequents:

Definition 8. *Let $\Gamma = \Gamma_1, \ldots, \Gamma_n \vdash$ be a sequent. We say that Γ is* in Prop normal form *(PNF) if for every Γ_i, either* **(1)** *Γ_i is of form $t_1 = t_2$, $t_1 \neq t_2$, $\mathrm{Prop}(A)$ or $\neg\mathrm{Prop}(A)$, or* **(2)** *there is a $j < i$, s.t. Γ_j has form $\mathrm{Prop}(\Gamma_i)$.*

Lemma 1. *Let $\Gamma \vdash$ be a sequent in PNF. Let I be an interpretation. Then $\Gamma \vdash$ does not fail strongly in I iff for every formula F in Γ, $I(F) = \mathbf{t}$.*

Theorem 5. *If $\mathrm{Seq}_{\mathrm{PCL}}$ is complete for sequents in PNF, then it is complete for all sequents.*

Proof. Assume that $\mathrm{Seq}_{\mathrm{PCL}}$ is complete for sequents in PNF. Let $\Gamma \vdash$ be an arbitrary sequent. Write $\Gamma \vdash$ in the form $\Gamma_1, \ldots, \Gamma_n \vdash$. Let $\#\Gamma \vdash$ be the number of violations of Definition 8 in $\Gamma \vdash$. (This is the number of Γ_i that are not of form $t_1 = t_2$, $t_1 \neq t_2$, $\mathrm{Prop}(A)$, $\neg\mathrm{Prop}(A)$, and for which there also exists no $j < i$ with $\Gamma_j = \mathrm{Prop}(\Gamma_i)$.)

If $\#\Gamma \vdash = 0$, then $\Gamma \vdash$ is in PCL, so that we are done. Otherwise, assume that the first violation of Definition 8 occurs on position i. This implies that the sequent $S_1 = \Gamma_1, \ldots, \Gamma_{i-1}, \neg\mathrm{Prop}(\Gamma_i) \vdash$ is in PNF. If S_1 has no proof, then by PNF-completeness, we know that there exists an interpretation I, in which S_1 does not fail strongly. By Lemma 1, $I(\Gamma_1) = \cdots = I(\Gamma_{i-1}) = I(\neg\mathrm{Prop}(\Gamma_i)) = \mathbf{t}$, so that $I(\mathrm{Prop}(\Gamma_i)) = \mathbf{f}$. This implies that the sequent $\Gamma_1, \ldots, \Gamma_{i-1}, \Gamma_i, \ldots, \Gamma_n \vdash$ fails in I, but not strongly. As a consequence, we have completeness for this case.

If S_1 does have a proof, then we consider the sequent
$S_2 = \Gamma_1, \ldots, \Gamma_{i-1}, \mathrm{Prop}(\Gamma_i), \Gamma_i, \ldots, \Gamma_n \vdash$. Clearly, $\#S_2 = \#(\Gamma \vdash) - 1$, so that we can assume completeness for S_2.

If S_2 has no proof, then there exists an interpretation I, in which S_2 does either not fail at all, or it fails but not strongly. If S_2 does not fail in I, then $\Gamma \vdash$ also does not fail, and we are done. Otherwise, consider the first formula F in S_2, for which $I(F) \neq \mathbf{t}$. If F were among the $\Gamma_1, \ldots, \Gamma_{i-1}$, this would imply that the sequent S_2 fails strongly, due to the fact that S_1 has a proof. From the provability of S_1 follows, that F cannot be $\mathrm{Prop}(\Gamma_i)$. If F would be Γ_i, this would imply that $I(\mathrm{Prop}(\Gamma_i)) = \mathbf{f}$, which contradicts the fact that S_2 is provable. So it must be the case that F is among $\Gamma_{i+1}, \ldots, \Gamma_n$. But this implies that $\Gamma \vdash$ also fails non strongly in I, so that we have completeness in this case as well.

Finally assume that S_2 has a proof. In that case, we can combine the proofs of S_1 and S_2 into a proof of $\Gamma \vdash$ as follows:

$$\frac{\Gamma_1, \ldots, \Gamma_{i-1}, \ \neg\mathrm{Prop}(\Gamma_i) \vdash \qquad \Gamma_1, \ldots, \Gamma_{i-1}, \mathrm{Prop}(\Gamma_i), \Gamma_i, \ldots, \Gamma_n \vdash}{\Gamma_1, \ldots, \Gamma_{i-1}, \Gamma_i, \ldots, \Gamma_n \vdash} \ (cut).$$

The fact that we can restrict our attention to sequents in PNF, simplifies the completeness proof quite a lot. By Lemma 1, we know that we are looking either for a proof, or an interpretation that makes all atoms in the sequent true. Since this does not rely on order anymore, we can use standard techniques to construct the limit of the sequents in the failed proof attempt. We still have to show two things, but they turn out unproblematic: **(1)** It does not happen that, during proof search for a sequent in PNF, one needs to make use of a sequent that is not in PNF. **(2)** All formulas in the orginal sequent are true in the resulting interpretation. In order to do this, we show that a nonsucceeding proof attempt converges towards a saturated set, which is defined as follows:

Definition 9. *Let Σ be a set of formulas. We call Σ* saturated *if it has the following properties:*

- *If $A \in \Sigma$, and A is not of form $t_1 = t_2$, $t_1 \neq t_2$, $\mathrm{Prop}(B)$, or $\neg\mathrm{Prop}(B)$, then $\mathrm{Prop}(A) \in \Sigma$.*
- *$\bot \notin \Sigma$.*
- *There exist no terms t, u, no $n \geq 0$, no sequence of terms $t_1, u_1, \ldots, t_n, u_n$, s.t. $\{t_1 = u_1, \ldots, t_n = u_n, t \neq u\} \subseteq \Sigma$, and $t_1 = u_1, \ldots, t_n = u_n \vdash t = u$ in the standard theory of equality.*
- *There exist no atoms A, A', no $n \geq 0$, no sequence of terms $t_1, u_1, \ldots, t_n, u_n$, s.t. $\{A, \ t_1 = u_1, \ldots, t_n = u_n, \ \neg A'\} \subseteq \Sigma$, and $A, \ t_1 = u_1, \ldots, t_n = u_n \vdash A'$ in the standard theory of equality.*
- *If $\{\ \mathrm{Prop}(A \vee B), \ A \vee B\ \} \subseteq \Sigma$, then either $\{\mathrm{Prop}(A), A\} \subseteq \Sigma$, or $\{\mathrm{Prop}(B), B\} \subseteq \Sigma$.*
- *If $\{\ \mathrm{Prop}(\ \langle A \rangle B\ ), \ \langle A \rangle B\ \} \subseteq \Sigma$, then $\{\mathrm{Prop}(A), \mathrm{Prop}(B), A, B\} \subseteq \Sigma$.*
- *If $\{\ \mathrm{Prop}(\ \exists x\ P(x)\ ), \ \exists x\ P(x)\ \} \subseteq \Sigma$, then there exists a term t, s.t. $\{\ \mathrm{Prop}(\ P(t)\ ), \ P(t)\ \} \subseteq \Sigma$.*
- *If $\{\ \mathrm{Prop}(\ \forall x\ P(x)\ ), \ \forall x\ P(x)\ \} \subseteq \Sigma$, then for every term t that can be formed from the signature of Σ, we have $\{\ \mathrm{Prop}(P(t)), \ P(t)\ \} \subseteq \Sigma$.*
- *For every instance $A \Rightarrow B$ of a rule in Figure 1 or Figure 4, if $\{\mathrm{Prop}(A), A\} \subseteq \Sigma$, then $\{\mathrm{Prop}(B), B\} \subseteq \Sigma$.*
- *For every instance $\mathrm{Prop}(A) \Rightarrow B$ of a rule in Figure 2, if $\mathrm{Prop}(A) \in \Sigma$, but $A \notin \Sigma$, then $B \in \Sigma$.*

Note that, by taking $n = 0$ in the fourth case, the definition of saturated set implies that Σ does not contain a complementary pair of atoms $A, \neg A$. Since our aim is to prove completeness, we need a proof search strategy that converges towards a saturated set in the limit. In order to obtain a saturated set, it is necessary to preserve PNF during proof search. If, for example, one has a sequent of form $\Gamma_1, \mathrm{Prop}(A \wedge B), A \wedge B, \Gamma_2 \vdash$ and tries to prove it from $\Gamma_1, \mathrm{Prop}(A \wedge$

$B), A, B, \Gamma_2 \vdash$, then the new sequent is not in PNF anymore. In this case we can continue proof search by replacing $\mathrm{Prop}(A \wedge B)$ by $\langle \mathrm{Prop}(A) \rangle \mathrm{Prop}(B)$, which in turn can be replaced by $\mathrm{Prop}(A), \mathrm{Prop}(B)$, which is in PNF again. Figures 5, 6, 7 and 8 show that, for the operators $\langle\ \rangle, \vee, \forall$ and $\exists$, it is always possible to continue proof search with sequents in PNF. All of the remaining cases can be reduced to the cases for $\langle\ \rangle$ and $\vee$, using the equivalences in Figures 1, 2 and 4.

In Figure 5, the leftmost sequent is provable, because it is in PNF, and it contains the complementary pair $A, \neg A$. Hence, it is sufficient to continue proof search with the rightmost sequent, which is also in PNF.

Fig. 5. Preservation of PNF under $\langle\ \rangle$-intro

$$\dfrac{\dfrac{\dfrac{}{\Gamma_1,\ \mathrm{Prop}(A), \neg A, A, B, \Gamma_2 \vdash}\ \text{(provable)} \qquad \Gamma_1,\ \mathrm{Prop}(A),\ \mathrm{Prop}(B),\ A, B, \Gamma_2 \vdash}{\Gamma_1,\ \mathrm{Prop}(A),\ \neg A \vee \mathrm{Prop}(B), A, B, \Gamma_2 \vdash}\ (\vee\text{-intro})}{\Gamma_1,\ \langle\ \mathrm{Prop}(A)\ \rangle\ (\ A \rightarrow \mathrm{Prop}(B)\ ),\ \langle A \rangle B,\ \Gamma_2 \vdash}\ (\langle\ \rangle\text{-intro, Equiv Figure 4})$$

$$\dfrac{\Gamma_1,\ \langle\ \mathrm{Prop}(A)\ \rangle\ (\ A \rightarrow \mathrm{Prop}(B)\ ),\ \langle A \rangle B,\ \Gamma_2 \vdash}{\Gamma_1,\ \mathrm{Prop}(\ \langle A \rangle B\ ),\ \langle A \rangle B,\ \Gamma_2 \vdash}\ \text{(Equiv Figure 2)}$$

Fig. 6. Preservation of PNF under $\vee$-intro

$$\dfrac{\dfrac{\Gamma_1,\ \mathrm{Prop}(A),\ \mathrm{Prop}(B),\ A,\ \Gamma_2 \vdash \qquad \Gamma_1,\ \mathrm{Prop}(A),\ \mathrm{Prop}(B), B,\ \ \Gamma_2 \vdash}{\Gamma_1,\ \mathrm{Prop}(A),\ \mathrm{Prop}(B), A \vee B, \Gamma_2 \vdash}\ (\vee\text{-intro})}{\Gamma_1,\ \mathrm{Prop}(\ A \vee B\ ),\ A \vee B,\ \Gamma_2 \vdash}\ \text{(Equiv Figure 2,}\ \langle\ \rangle\text{-intro)}$$

Figure 7 shows how PNF can be preserved when instantiating a $\forall$. In the middle, the proof splits at the cut application. The first formula of the left branch is provable, because it contains the complementary pair $\mathrm{Prop}(P(t)), \neg\mathrm{Prop}(P(t))$, Γ_1 is in PNF, and the remaining formulas $\forall x\ \mathrm{Prop}(\ P(x)\ )$, $\mathrm{Prop}(P(t))$, $\forall x\ P(x)$ can be easily proven Prop in their respective contexts. The right premise of the cut application is in PNF, and has the formulas $\mathrm{Prop}(P(t)), P(t)$ added. Figure 8 branches at the weakening step, and its first premise is provable.

It remains to extract an interpretation $I_\Sigma = (D_\Sigma, \mathbf{f}_\Sigma, \mathbf{t}_\Sigma, \sqsubseteq_\Sigma, [\ ]_\Sigma)$ from the saturated set Σ. This can be done as follows:

- Assume two designated objects $\mathbf{f}, \mathbf{t}$ that are not in the signature of Σ. They will represent the truth values. Let T_Σ be the set of terms that can be

Fig. 7. Preservation of PNF under ∀-intro

$$\dfrac{\dfrac{\dfrac{\dfrac{}{\Gamma_1, \forall x\ \mathrm{Prop}(\ P(x)\ ), \mathrm{Prop}(\ P(t)\ ), \forall x\ P(x),\ \neg\mathrm{Prop}(\ P(t)\ ) \vdash}\ (\forall\text{-intro})}{\Gamma_1,\ \forall x\ \mathrm{Prop}(\ P(x)\ ), \forall x\ P(x),\ \neg\mathrm{Prop}(\ P(t)\ ) \vdash}\ (\text{Equiv Figure 2})}{\Gamma_1,\ \mathrm{Prop}(\ \forall x\ P(x)\ ), \forall x\ P(x),\ \neg\ \mathrm{Prop}(\ P(t)\ ) \vdash} \qquad \Gamma_1,\ \mathrm{Prop}(\ \forall x\ P(x)\ ), \forall x\ P(x),\ \mathrm{Prop}(\ P(t)\ ), P(t), \Gamma_2 \vdash}\ (\text{cut})}{\Gamma_1,\ \mathrm{Prop}(\ \forall x\ P(x)\ ), \forall x\ P(x),\ P(t),\ \Gamma_2 \vdash}\ \forall\text{-intro}$$
$$\Gamma_1,\ \mathrm{Prop}(\ \forall x\ P(x)\ ), \forall x\ P(x), \Gamma_2 \vdash$$

formed from the signature of Σ. Let $\equiv$ be the smallest congruence relation on $T_\Sigma \cup \{\mathbf{f}, \mathbf{t}\}$, s.t.
- for all $t_1, t_2 \in T_\Sigma$, if $(t_1 = t_2) \in \Sigma$, then $t_1 \equiv t_2$,
- for all $t \in T_\Sigma$, if both of $\mathrm{Prop}(t), t \in \Sigma$, then $t \equiv \mathbf{t}$,
- for all $t \in T_\Sigma$, if $\mathrm{Prop}(t) \in \Sigma$, but $t \notin \Sigma$, then $t \equiv \mathbf{f}$.

The domain D_Σ of I_Σ is defined as $(T \cup \{\mathbf{f}, \mathbf{t}\})/\equiv$.

– $\mathbf{f}_\Sigma$ is the element of D_Σ that contains $\mathbf{f}$.
– $\mathbf{t}_\Sigma$ is the element of D_Σ that contains $\mathbf{t}$.
– The choice of $\sqsubseteq_\Sigma$ is not important, so we simply select an arbitrary total order on $D_\Sigma \backslash \{\mathbf{f}_\Sigma, \mathbf{t}_\Sigma\}$.
– The function $[\ ]_\Sigma$ is defined in such a way that for every $t \in T_\Sigma$, the interpretation $I_\Sigma(t)$ is the equivalence class of $\equiv$ in which t falls.

It remains to show that for every formula A, $\quad A \in \Sigma \Leftrightarrow I_\Sigma(A) = \mathbf{t}$. This can be proven by structural induction on A using the properties in Definition 9.

Theorem 6. *Sequent calculus* Seq_{PCL} *is complete: If a sequent* $\Gamma \vdash$ *is not provable in* Seq_{PCL}*, then there exists an interpretation* I *in which* $\Gamma \vdash$ *does not fail strongly.*

3 Conclusions, Future Work

We have introduced a variant of first-order logic that supports partial functions and explicit type reasoning (PCL). We have introduced a semantics for PCL, which captures the intuitive meaning of partiality in a natural way. One of the motivations for introducing geometric resolution in [4] was the expectation that geometric resolution will be better at handling partial functions than standard automated theorem proving techniques. The current paper results from attempts to extend geometric resolution with partial functions. The next step is to extend geometric resolution (and its implementation Geo [3]), so that it can deal with PCL. On the theoretical side, we would like to know whether Seq_{PCL} admits cut elimination.

Fig. 8. Preservation of PNF under ∃-intro

$$\dfrac{\dfrac{\dfrac{\dfrac{\dfrac{\Gamma_1,\ \neg\mathrm{Prop}(\ \forall x\ \mathrm{Prop}(\ P(x)\ )\ \vdash \qquad\qquad \Gamma_1,\ \mathrm{Prop}(\ P(y)\ ),\ P(y),\ \Gamma_2 \vdash}{\Gamma_1,\ \forall x\ \mathrm{Prop}(\ P(x)\ ),\ \mathrm{Prop}(\ P(y)\ ),\ P(y),\ \Gamma_2 \vdash}\ \text{(weakening)}}{\Gamma_1,\ \forall x\ \mathrm{Prop}(\ P(x)\ ),\ P(y),\ \Gamma_2 \vdash}\ (\forall\text{-intro})}{\Gamma_1,\ \forall x\ \mathrm{Prop}(\ P(x)\ ),\ \exists x\ P(x),\ \Gamma_2 \vdash}\ (\exists\text{-intro})}{\Gamma_1,\ \mathrm{Prop}(\ \exists x\ P(x)\ ),\exists x\ P(x),\Gamma_2 \vdash}\ \text{(Equiv Figure 2)}$$

Part of this research was funded by the 'Programme for the Advancement of Computer Science' of the city of Wrocław.

References

1. Sergey Berezin, Clark Barrett, Igor Shikanian, Marsha Chechik, Arie Gurfinkel, and David Dill. A practical approach to partial functions in CVC Lite. In *Selected Papers from the Workshop on Disproving and the Second International Workshop on Pragmatics of Decision Procedures (PDPAR 04)*, volume 125 of *Electronic Notes in Theoretical Computer Science*, pages 13–23. Elsevier, July 2005.
2. Ádám Darvas, Farhad Mehta, and Arsenii Rudich. Efficient well-definedness checking. In Alessandro Armado, Peter Baumgartner, and Gilles Dowek, editors, *International Joint Conference on Automated Reasoning (IJCAR) 2008*, volume 5195 of *LNAI*, pages 100–115. Springer Verlag, 2008.
3. Hans de Nivelle. Theorem prover Geo 2007F. Can be obtained from the author's homepage, September 2007.
4. Hans de Nivelle and Jia Meng. Geometric resolution: A proof procedure based on finite model search. In John Harrison, Ulrich Furbach, and Natarajan Shankar, editors, *International Joint Conference on Automated Reasoning 2006*, volume 4130 of *Lecture Notes in Artificial Intelligence*, pages 303–317, Seattle, USA, August 2006. Springer.
5. William M. Farmer. Mechanizing the traditional approach to partial functions. In W. Farmer, M. Kerber, and M. Kohlhase, editors, *Proceedings of the Workshop on the Mechanization of Partial Functions (associated to CADE 13)*, pages 27–32, 1996.
6. William M. Farmer and Joshua D. Guttman. A set theory with support for partial functions. *Studia Logica*, 66:59–78, 2000.
7. Reiner Hähnle. Many-valued logic, partiality, and abstraction in formal specification languages. *Logic Journal of the IGPL*, 13(4):415–433, 2005.
8. Manfred Kerber and Michael Kohlhase. A mechanization of strong Kleene logic for partial functions. In *Automated Deduction - CADE 12*, volume 814 of *LNAI*, pages 371–385. Springer Verlag, June 1994.
9. Farhad Mehta. A practical approach to partiality - a proof based approach. In Shaoying Liu and Tom Maibaum, editors, *International Conference on Formal Engineering Methods, (ICFEM)*, volume 5256 of *LNCS*, pages 238–257. Springer, 2008.