Classical Logic with Partial Functions

Wien, 10 March, 2010

Hans de Nivelle
University of Wrocław, Poland

Motivation

- Programs contain partial functions. In principle, partial functions can be made total, but it is unnatural in most cases. Partial functions make it possible to obtain more general interfaces.

  Less general interfaces are harder to use and less often applicable.

- One needs a logic that can deal with partial functions. Nothing can be assumed about ill-defined terms.

Requirements

- We think that types and preconditions should be identified. Both of them are just predicates.
- Since binary preconditions exist, binary types should be also possible.
- There should be no a priori restriction on the type system. (Types are first-class citizens.)

Lazy Operators

We introduce two lazy operators, which mix typing conditions and usual formulas:

lazy implication: Lazy implication $[A]B$ is well-typed if:

- A is well-typed, and
- If A is true, then B is well-typed.

(Standard implication $A \to B$ is well-typed if A and B are well-typed.)

lazy conjunction: Lazy conjunction $\langle A \rangle B$ is well-typed if:

- A is well-typed, and
- If A is true, then B is well-typed.

(Standard conjunction $A \wedge B$ is well-typed if A and B are well-typed.)

Some More Operators

Prop: Prop(A) is allways well-typed. In addition, it is true if A is a well-typed proposition.

(Prop is a logical operator, not a predicate!)

$\forall, \exists$: $\forall x\ P(x)$, $\exists x\ P(x)$ are well-typed if for every x, $P(x)$ is well-typed.

$=$ $t_1 = t_2$ is always well-typed. If you don't want that, it is possible to define your own equality.

Discourse

A discourse $F_1, \ldots, F_n$ is well-typed if, for each i, $\mathrm{Prop}(F_i)$ follows from $F_1, \ldots, F_{i-1}$.

Example of a Discourse

$\forall x\ \mathrm{Prop}(\ \mathrm{Nat}(x)\ ),$

$\mathrm{Nat}(0),$

$\forall x\ \mathrm{Nat}(x) \rightarrow \mathrm{Nat}(\ \mathrm{succ}(x)\ ),$

$\forall xy\ \mathrm{Nat}(x) \wedge \mathrm{Nat}(y) \rightarrow \mathrm{Prop}(x \leq y),$

$\forall xy\ [\ \mathrm{Nat}(x),\ \mathrm{Nat}(y),\ \mathrm{Nat}(z)\ ]\ x \leq y \wedge y \leq z \rightarrow x \leq z,$

$\forall xy\ [\ \mathrm{Nat}(x),\ \mathrm{Nat}(y)\ ]\ y \leq x \rightarrow \mathrm{Nat}(x - y),$

$\forall xy\ [\ \mathrm{Nat}(x),\ \mathrm{Nat}(y)\ ]\ x \leq y \rightarrow \exists z\ \langle\ \mathrm{Nat}(z), x \geq z\ \rangle\ x - z = y.$

Semantics

The semantics in the paper is a bit more complicated, but everything important is present in the following definition:

Definition: An interpretation $I = (D, \mathbf{f}, \mathbf{t}, \mathbf{e}, [\ ])$ is defined by:

- A domain D.
- Two distinct truth values $\mathbf{f}$ and $\mathbf{t}$.
- An error value $\mathbf{e}$.
- A function $[\ ]$ that interprets the function symbols: If f is a function symbol with arity n, then $[f]$ is a total function from D^n to D.

Semantics of Logical Operators (1)

The standard logical operators $\bot, \top, \neg, \vee, \wedge, \rightarrow, \leftrightarrow$:

- $I(\bot) = \mathbf{f},\ I(\top) = \mathbf{t}$.
- If $I(A) \notin \{\mathbf{f}, \mathbf{t}\}$, then $I(\neg A) = \mathbf{e}$.

  If $I(A) \in \{\mathbf{f}, \mathbf{t}\}$, then $I(\neg A)$ is defined as usual.
- If one of $I(A), I(B)$ not in $\{\mathbf{f}, \mathbf{t}\}$, then
  $I(A \vee B) = I(A \wedge B) = I(A \rightarrow B) = I(A \leftrightarrow B) = \mathbf{e}$.

  If both of $I(A), I(B) \in \{\mathbf{f}, \mathbf{t}\}$, then
  $I(A \vee B),\ I(A \wedge B),\ I(A \rightarrow B)$ and $I(A \leftrightarrow B)$ are defined as usual.

Semantics of Logical Operators (2)

- If $I(A) \in \{\mathbf{f}, \mathbf{t}\}$, then $I(\ \mathrm{Prop}(A)\ ) = \mathbf{t}$. Otherwise, $I(\ \mathrm{Prop}(A)\ ) = \mathbf{f}$.
- Let x be a variable, let F be a formula. Let $R = \{I_d^x(F) \mid d \in D\}$.

  If $R \not\subseteq \{\mathbf{f}, \mathbf{t}\}$, then $I(\ \forall x\ F\ ) = I(\ \exists x\ F\ ) = \mathbf{e}$.

  If $R \subseteq \{\mathbf{f}, \mathbf{t}\}$, then $I(\ \forall x\ F\ )$ and $I(\ \exists x\ F\ )$ are defined by the following table:

R	$\forall$	$\exists$
$\{\mathbf{f}\}$	$\mathbf{f}$	$\mathbf{f}$
$\{\mathbf{t}\}$	$\mathbf{t}$	$\mathbf{t}$
$\{\mathbf{f}, \mathbf{t}\}$	$\mathbf{f}$	$\mathbf{t}$

Semantics of $[A]B$ and $\langle A\rangle B$:

$I(A)$	$I(B)$	$I(\ [A]B\ )$	$I(\ \langle A\rangle B\ )$
$\mathbf{f}$	$\cdots$	$\mathbf{t}$	$\mathbf{f}$
$\notin \{\mathbf{f},\mathbf{t}\}$	$\cdots$	$\mathbf{e}$	$\mathbf{e}$
$\mathbf{t}$	$\mathbf{f}$	$\mathbf{f}$	$\mathbf{f}$
$\mathbf{t}$	$\notin \{\mathbf{f},\mathbf{t}\}$	$\mathbf{e}$	$\mathbf{e}$
$\mathbf{t}$	$\mathbf{t}$	$\mathbf{t}$	$\mathbf{t}$

Sequents/Judgements

We define sequents as usual, as objects of form $\Gamma_1, \ldots, \Gamma_n \vdash A$.

A sequent is valid if in every interpretation $I = (D, \mathbf{f}, \mathbf{t}, \mathbf{e}, [\,])$ where $I(\Gamma_1) = \cdots = I(\Gamma_n) = \mathbf{t}$, we have also $I(A) = \mathbf{t}$.

The sequent is strongly valid if in addition, in every interpretation I,

- Either $I(\Gamma_1) = \cdots = I(\Gamma_n) = \mathbf{t}$, or
- the first i with $I(\Gamma_i) \neq \mathbf{t}$ has $I(\Gamma_i) = \mathbf{f}$.

Revelation 3:15-17

15 I know your deeds, that you are neither cold nor hot. I wish
you were either one or the other!

16 So, because you are lukewarm, neither hot nor cold, I am about
to spit you out of my mouth.

17 You say, I am rich; I have acquired wealth and do not need a
thing. But you do not realize that you are wretched, pitiful,
poor, blind and naked.

Intermediate Summary

At this point, we have a complete semantic characterization of classical logic with partial functions.

The notion of strong validity is designed in such a way that sequents can be only strongly valid when they are well-typed.

We call the logic partial classical logic or PCL.

One Sided Sequents (1)

We want to design a sequent calculus for the notion of strong validity in PCL. We have the following situation:

- PCL is truth-value based, i.e. essentially classical. (Because $\mathrm{Prop}(A) \vdash A \vee \neg A$ is strongly valid.)
- It is clear from the notion of strong validity that order of formulas is essential.
- Standard sequent calculus has rules (those for $\neg$ and $\rightarrow$) that move formulas from premiss to conclusion in a sequent.

$\Rightarrow$ Switch to one-sided sequents.

One-Sided Sequents (2)

Definition: A one-sided sequent Γ has form $\Gamma_1, \ldots, \Gamma_n \vdash$, where $\Gamma_1, \ldots, \Gamma_n$ are formulas.

We say that Γ fails in an interpretation I if there is an i, s.t $I(\Gamma_i) \neq \mathbf{t}$.

We say that Γ fails strongly in I if there is an i, s.t $I(\Gamma_i) = \mathbf{f}$ and for all j, $(1 \leq j < i)$, $I(\Gamma_i) = \mathbf{t}$.

We say that Γ is unsatisfiable if Γ fails in every interpretation.

We say that Γ is strongly unsatisfiable if Γ fails strongly in every interpretation.

Proving by Refuting

Theorem Let $\Gamma \vdash A$ be a sequent. The sequent $\Gamma \vdash A$ is strongly valid iff the one sided sequent $\Gamma, \neg A \vdash$ is strongly unsatisfiable.

Proof

So, we can restrict our attention to one-sided sequents.

Examples

Valid, but not strongly valid:

$$A \vdash A.$$

Strongly valid:

$$\mathrm{Prop}(A) \vdash A \vee \neg A.$$

Unsatisfiable, but not strongly:

$$\mathrm{Prop}(A),\ \neg B,\ A \vee B,\ \neg A \vdash$$

Strongly unsatisfiable:

$$\mathrm{Prop}(A),\ \mathrm{Prop}(B),\ \neg B,\ A \vee B, \neg A \vdash$$

Sequent Calculus Seq_{PCL} :

The following two rules are the most important rules of the calculus:

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

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

Theorem For both of the rules holds: The conclusion sequent is strongly unsatisfiable iff all of its premisses are strongly unsatisfiable.

Proof: If you think that this is obvious, then think harder.

Reduction to $\vee$ and $\langle\ \rangle$:

Quite a lot can be reduced to $\vee$ and $\langle\ \rangle$:

$$
\begin{array}{lcl}
A \wedge B & \Rightarrow & (\ \langle A \rangle B\ ) \vee (\ \langle B \rangle A\ ) \\
[A]B & \Rightarrow & \neg A \vee (\ \langle A \rangle B\ ) \\
A \rightarrow B & \Rightarrow & \neg A \vee B \\
A \leftrightarrow B & \Rightarrow & (\ \langle A \rangle B\ ) \vee (\ \langle \neg A \rangle \neg B\ )
\end{array}
$$

$$
\begin{array}{lcl}
\langle A \rangle \top & \Rightarrow & A \\
\langle \top \rangle A & \Rightarrow & A
\end{array}
$$

$$
\forall x\ P(x) \quad \Rightarrow \quad \langle\ \forall x\ P(x)\ \rangle\ P(t)
$$

Pushing $\neg$ out of the way:

Negation can be pushed inwards: (pretty much standard)

$$\neg\bot \Rightarrow \top$$

$$\neg\top \Rightarrow \bot$$

$$\neg\neg A \Rightarrow A$$

$$\neg(\langle A\rangle B) \Rightarrow [A]\neg B$$

$$\neg([A]B) \Rightarrow \langle A\rangle\neg B$$

$$\neg(A \wedge B) \Rightarrow \neg A \vee \neg B$$

$$\neg(A \vee B) \Rightarrow \neg A \wedge \neg B$$

$$\neg(A \rightarrow B) \Rightarrow A \wedge \neg B$$

$$\neg(A \leftrightarrow B) \Rightarrow A \leftrightarrow \neg B$$

$$\neg\forall x\ F \Rightarrow \exists x\ \neg F$$

$$\neg\exists x\ F \Rightarrow \forall x\ \neg F$$

Pushing Prop Inwards

Prop can be pushed inwards until it hits an atom:

$$
\begin{array}{lcl}
\mathrm{Prop}(\top) & \Rightarrow & \top \\
\mathrm{Prop}(\bot) & \Rightarrow & \top \\
\mathrm{Prop}(\neg A) & \Rightarrow & \mathrm{Prop}(A) \\
\mathrm{Prop}(\mathrm{Prop}(A)) & \Rightarrow & \top
\end{array}
$$

$$
\begin{array}{lcl}
\mathrm{Prop}(A \wedge B) & \Rightarrow & \langle\ \mathrm{Prop}(A)\ \rangle\ \mathrm{Prop}(B) \\
\mathrm{Prop}(A \vee B) & \Rightarrow & \langle\ \mathrm{Prop}(A)\ \rangle\ \mathrm{Prop}(B) \\
\mathrm{Prop}(A \rightarrow B) & \Rightarrow & \langle\ \mathrm{Prop}(A)\ \rangle\ \mathrm{Prop}(B) \\
\mathrm{Prop}(A \leftrightarrow B) & \Rightarrow & \langle\ \mathrm{Prop}(A)\ \rangle\ \mathrm{Prop}(B)
\end{array}
$$

Pushing Prop Inwards (2)

$$\begin{array}{lcl}
\mathrm{Prop}(\ \langle A\rangle B\ ) & \Rightarrow & \langle\ \mathrm{Prop}(A)\ \rangle(\ A \to \mathrm{Prop}(B)\ ) \\
\mathrm{Prop}(\ [A]B\ ) & \Rightarrow & \langle\ \mathrm{Prop}(A)\ \rangle(\ A \to \mathrm{Prop}(B)\ )
\end{array}$$

$$\begin{array}{lcl}
\mathrm{Prop}(\forall x\ F) & \Rightarrow & \forall x\ \mathrm{Prop}(F) \\
\mathrm{Prop}(\exists x\ F) & \Rightarrow & \forall x\ \mathrm{Prop}(F)
\end{array}$$

$$\mathrm{Prop}(t_1 = t_2) \quad \Rightarrow \quad \top$$

Some More Rules:

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

The $\exists$-rule has the condition that x must be not free in Γ_1 or Γ_2.

Theorem For both rules holds: The conclusion is strongly unsatisfiable iff the premiss is strongly unsatisfiable.

proof: $\forall$ has some pitfals. The rule for $\exists$ seems standard, but is not standard. (The situation is similar to $\vee$)

Equality Axioms:

$$\frac{}{\text{Prop}(A), A,\ t_1 = u_1, \ldots, t_n = u_n, \neg A' \vdash}$$

$$\frac{}{t_1 = u_1, \ldots, t_n = u_n,\ t \neq u \vdash}$$

For 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. For 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.

Weakening

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

(For both rules, A can be positive or negative.)

Contraction, Cut

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

(A can be a negative formula as well.)

Weakening with Contraction allow a limited form of permutation.

Completeness Proof

Without $\forall$, the proof would have been easy:

Careless treatement of $\forall$ results in infinite sequents, which are problematic.

Definition: A sequent $\Gamma_1, \ldots, \Gamma_n$ 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 exists a $j < i$, s.t. $\Gamma_j = \mathrm{Prop}(\Gamma_i)$.

Lemma Let I be an interpretation. Let Γ be a sequent in PNF. Then

$\Gamma \vdash$ fails strongly in I iff Γ fails in I.

Consequence: For sequents in PNF, strong unsatisfiability and unsatisfiability are the same.

Reduction to PNF

Theorem: If Seq_{PCL} is complete for sequents in PNF, then it is complete for all sequents.

Proof: For a sequent Γ, let $\#\Gamma$ be the number of violations of the definition of PNF.

We assume completeness in case when $\#\Gamma = 0$, and use induction to show completeness for $\#\Gamma > 0$.

Completeness Proof for PNF

The completeness proof for PNF is standard. One must show that PNF can be preserved during proof search.

Conclusions, Future Work

- I believe that PCL is 'the right logic' for verification and applications.
- The sequent calculus is not useful for proof search, nor for proof presentation. Natural deduction is more suitable for proof presentation.
- I came closer to fulfilling a promise in: Hans de Nivelle, Jia Meng, Geometric Resolution: A Proof Procedure Based on Finite Model Search, IJCAR 2006.