

Logical Relations for a Logical Framework

sketching [RS13] by Florian Rabe and Kristina Sojakova

Navid Roux¹

KWARC Seminar
Computer Science, FAU Erlangen-Nürnberg

2021-01-27



This work is licensed under a “CC BY-SA 4.0” license.

¹<https://orcid.org/0000-0002-8348-2441>

Overview of this Talk

Logical Relations

class of proof methods applicable on many type theories

Logical Framework

a uniform presentation language to formalize logics/type theories

Logical Relations for a Logical Framework

a uniform notion of “proof by logical relations” in the setting of LF

Highlevel Motivation

To formalize a type theory, we have to formalize

- syntax
- typing rules
- operational semantics
- *and* meta theorems

these three already tedious enough

Meta theorems often employ a “proof by logical relation”.

Formalization entails

w/o this work

- formalizing specific theory of logrels
- limited representation & tool support

w/ this work + ε^{-1}

bold statement, ignorant of literature
but helps beginners get the idea

Highlevel Motivation

To formalize a type theory, we have to formalize

- syntax
- typing rules
- operational semantics
- *and* meta theorems

these three already tedious enough

Meta theorems often employ a “proof by logical relation”.

Formalization entails

w/o this work

- formalizing specific theory of logrels
- limited representation & tool support

w/ this work + ε^{-1}

- **instantiation of uniform notion** of logrels
- general representation & tool support

bold statement, ignorant of literature
but helps beginners get the idea

This Talk

Required background knowledge:

- simply typed lambda calculus
- how to formalize things in a LF

e.g. as in MMT

Goals:

- 1 Introduce logical relations
- 2 Recap logical frameworks, esp. MMT/LF
- 3 Represent toy logical relations in MMT/LF

Next Steps

Logical Relations

class of proof methods applicable on many type theories

Logical Framework

a uniform presentation language to formalize logics/type theories

Logical Relations for a Logical Framework

a uniform notion of “proof by logical relations” in the setting of LF

What are Logical Relations?

An (informal) **class of proof methods** used to prove

- strong normalization
- type safety
- program equivalence
 - correctness
 - theorems-for-free
 - security-typed languages

no infinite evaluation path $t_1 \rightsquigarrow t_2 \rightsquigarrow \dots$

$t : T$ and $t \rightsquigarrow^* t' \Rightarrow t' : T$

e.g. of optimizations

terms of $\forall \alpha. \alpha \rightarrow \alpha$ are the identity
variables of “sensitive” type don’t leak

Simply-Typed Lambda Calculus (STLC)

Definition

Syntax:

t	$::=$	$x \mid \lambda x. t \mid s t$	terms
T	$::=$	$B \mid T_1 \rightarrow T_2$	types
Γ	$::=$	$\emptyset \mid \Gamma, x: T$	contexts

Operational Semantics:

$$\frac{t \rightsquigarrow t'}{\lambda x. t \rightsquigarrow \lambda x. t'} \qquad \frac{}{(\lambda x. s) t \rightsquigarrow s[x \mapsto t]} \qquad \frac{s \rightsquigarrow s'}{s t \rightsquigarrow s' t} \qquad \frac{t \rightsquigarrow t'}{s t \rightsquigarrow s t'}$$

$\mathcal{SN} = \{t \mid \nexists \text{ infinite eval. path } t = t_1 \rightsquigarrow t_2 \rightsquigarrow \dots\}$ set of strongly normalizing terms

Theorem (Strong Normalization)

$$\Gamma \vdash t: T \implies t \in \mathcal{SN}$$

Theorem (Strong Normalization)

$$\Gamma \vdash t : T \implies t \in \mathcal{SN}$$

Proof Attempt: by induction on t

- case x : trivial
- case $\lambda x. s$: invert typing:



Theorem (Strong Normalization)

$$\Gamma \vdash t : T \implies t \in \mathcal{SN}$$

Proof Attempt: by induction on t

- case x : trivial
- case $\lambda x. s$: invert typing:

$$\frac{\Gamma, x : T_1 \vdash s : T_2}{\Gamma \vdash \lambda x. s : T_1 \rightarrow T_2}$$

Together with IH yields $s \in \mathcal{SN}$, hence $\lambda x. s \in \mathcal{SN}$.



Theorem (Strong Normalization)

$$\Gamma \vdash t : T \implies t \in \mathcal{SN}$$

Proof Attempt: by induction on t

- case x : trivial ✓
- case $\lambda x. s$: invert typing: [...] ✓
- case $s \ t$:

Theorem (Strong Normalization)

$$\Gamma \vdash t : T \implies t \in \mathcal{SN}$$

Proof Attempt: by induction on t

- case x : trivial
- case $\lambda x. s$: invert typing: [...]
- case $s t$: invert typing:



$$\frac{\Gamma \vdash s : T_1 \rightarrow T_2 \quad \Gamma \vdash t : T_1}{\Gamma \vdash s t : T_2}$$

Together with IH yields $s, t \in \mathcal{SN}$; but goal is $s t \in \mathcal{SN}$!

what if $s? \lambda x. \dots$?

Theorem (Strong Normalization)

$$\Gamma \vdash t : T \implies t \in \mathcal{SN}$$

Proof Attempt: by induction on t

- case x : trivial ✓
- case $\lambda x. s$: invert typing: [...] ✓
- case $s t$: invert typing: ✗

$$\frac{\Gamma \vdash s : T_1 \rightarrow T_2 \quad \Gamma \vdash t : T_1}{\Gamma \vdash s t : T_2}$$

Together with IH yields $s, t \in \mathcal{SN}$; but goal is $s t \in \mathcal{SN}$!

what if $s? \lambda x. \dots$?

Ideas:

- strengthen IH-condition on s :

$s \in \mathcal{SN}$ and $s t \in \mathcal{SN}$ for arbitrary terms t with $t \in \mathcal{SN}$

- but only on those s of function type

Strengthening the Induction by a Logical Relation

This variant was too weak:

Failed Attempt (SN, naive formulation)

$$\Gamma \vdash t : T \implies t \in \mathcal{SN}$$

Let's try:

Attempt (SN, with naive logrel)

$$\Gamma \vdash t : T \implies P_T(t) \quad \text{where} \quad \left\{ \begin{array}{l} P_B(b) := b \in \mathcal{SN} \\ P_{T_1 \rightarrow T_2}(s) := s \in \mathcal{SN} \wedge \forall t : T_1. P_{T_1}(t) \Rightarrow P_{T_2}(s \ t) \end{array} \right\}$$

- For every type T , specify a relation $P_T(-)$ on terms of type T .
- If that worked, strong normalization would be a corollary.

Attempt (SN, with naive logrel)

$$\Gamma \vdash t : T \implies P_T(t) \quad \text{where} \quad \left\{ \begin{array}{l} P_B(b) := b \in \mathcal{SN} \\ P_{T_1 \rightarrow T_2}(s) := s \in \mathcal{SN} \wedge \forall t : T_1. P_{T_1}(t) \implies P_{T_2}(s \ t) \end{array} \right\}$$

Proof Attempt: by induction on t

- case x : subtle, but doable



Attempt (SN, with naive logrel)

$$\Gamma \vdash t : T \implies P_T(t) \quad \text{where} \quad \left\{ \begin{array}{l} P_B(b) := b \in \mathcal{SN} \\ P_{T_1 \rightarrow T_2}(s) := s \in \mathcal{SN} \wedge \forall t : T_1. P_{T_1}(t) \implies P_{T_2}(s \ t) \end{array} \right\}$$

Proof Attempt: by induction on t

- case x : subtle, but doable ✓

- case $s \ t$: invert typing and use IHs:
$$\frac{\Gamma \vdash s : T_1 \rightarrow T_2 \quad \Gamma \vdash t : T_1}{\Gamma \vdash s \ t : T_2}$$
 ✓

Attempt (SN, with naive logrel)

$$\Gamma \vdash t : T \implies P_T(t) \quad \text{where} \quad \left\{ \begin{array}{l} P_B(b) := b \in \mathcal{SN} \\ P_{T_1 \rightarrow T_2}(s) := s \in \mathcal{SN} \wedge \forall t : T_1. P_{T_1}(t) \implies P_{T_2}(s \ t) \end{array} \right\}$$

Proof Attempt: by induction on t

- case x : subtle, but doable ✓

- case $s \ t$: invert typing and use IHs:
$$\frac{\Gamma \vdash s : T_1 \rightarrow T_2 \quad \Gamma \vdash t : T_1}{\Gamma \vdash s \ t : T_2}$$
 ✓

- case $\lambda x. s$:

Attempt (SN, with naive logrel)

$$\Gamma \vdash t : T \implies P_T(t) \quad \text{where} \quad \left\{ \begin{array}{l} P_B(b) := b \in \mathcal{SN} \\ P_{T_1 \rightarrow T_2}(s) := s \in \mathcal{SN} \wedge \forall t : T_1. P_{T_1}(t) \implies P_{T_2}(s \ t) \end{array} \right\}$$

Proof Attempt: by induction on t

- case x : subtle, but doable ✓

- case $s \ t$: invert typing and use IHs:
$$\frac{\Gamma \vdash s : T_1 \rightarrow T_2 \quad \Gamma \vdash t : T_1}{\Gamma \vdash s \ t : T_2}$$
 ✓

- case $\lambda x. s$: invert typing:

$$\frac{\Gamma, x : T_1 \vdash s : T_2}{\Gamma \vdash \lambda x. s : T_1 \rightarrow T_2}$$

- $(\lambda x. s) \in \mathcal{SN}$: trivial

Attempt (SN, with naive logrel)

$$\Gamma \vdash t : T \implies P_T(t) \quad \text{where} \quad \left\{ \begin{array}{l} P_B(b) := b \in \mathcal{SN} \\ P_{T_1 \rightarrow T_2}(s) := s \in \mathcal{SN} \wedge \forall t : T_1. P_{T_1}(t) \Rightarrow P_{T_2}(s \ t) \end{array} \right\}$$

Proof Attempt: by induction on t

- case x : subtle, but doable ✓

- case $s \ t$: invert typing and use IHs:
$$\frac{\Gamma \vdash s : T_1 \rightarrow T_2 \quad \Gamma \vdash t : T_1}{\Gamma \vdash s \ t : T_2}$$
 ✓

- case $\lambda x. s$: invert typing: ✗

$$\frac{\Gamma, x : T_1 \vdash s : T_2}{\Gamma \vdash \lambda x. s : T_1 \rightarrow T_2}$$

- $(\lambda x. s) \in \mathcal{SN}$: trivial
- $\forall t : T_1. P_{T_1}(t) \Rightarrow P_{T_2}((\lambda x. s) \ t)$: get stuck at $P_{T_2}((\lambda x. s) \ t) \stackrel{?}{=} P_{T_2}(s[x \mapsto t])$

We deviate from the IH on s *just* by a substitution!

Strengthening the Induction by a Logical Relation II

Failed Attempt (SN, naive formulation)

$$\Gamma \vdash t : T \implies t \in \mathcal{SN}$$

Failed Attempt (SN, with naive logrel)

$$\Gamma \vdash t : T \implies P_T(t) \quad \text{where} \quad \left\{ \begin{array}{l} P_B(b) := b \in \mathcal{SN} \\ P_{T_1 \rightarrow T_2}(s) := s \in \mathcal{SN} \wedge \forall t : T_1. P_{T_1}(t) \Rightarrow P_{T_2}(s \ t) \end{array} \right\}$$

This goes through:

Theorem (SN, with logrel)

$$\Gamma \vdash t : T \wedge P_\Gamma(\gamma) \implies P_T(t\gamma) \quad \left\{ \begin{array}{l} P_B(b) := b \in \mathcal{SN} \\ P_{T_1 \rightarrow T_2}(s) := s \in \mathcal{SN} \wedge \forall t : T_1. P_{T_1}(t) \Rightarrow P_{T_2}(s \ t) \\ P_\Gamma(\gamma) := \forall (x : T) \in \Gamma. P_T(x\gamma) \end{array} \right\}$$

Logical Relations: Summary

Motivation:

Theorem (Strong Normalization)

$$\Gamma \vdash t : T \implies t \in \mathcal{SN}$$

- Induction on t failed: IH too weak
- Needed to **strengthen IH based on type of t**

Solution: a “proof by logical relation”

applicable in many type theories

- 1 Define a logical relation $P_{-}(-)$:

for every type T , $P_T(-)$ is a relation on terms of type T

a typed-indexed family of relations

- 2 Prove the “Basic Lemma”

$$\Gamma \vdash t : T \implies P_T(t)$$

- 3 Recover desired theorem as corollary

Next Steps

Logical Relations

class of proof methods applicable on many type theories

Logical Framework

a uniform presentation language to formalize logics/type theories

Logical Relations for a Logical Framework

a uniform notion of “proof by logical relations” in the setting of LF

Logical Framework: Motivation

- There are many logics

FOL, SFOL, HOL, Modal Logic, Dynamic Logics, Discourse Representation Theory, Temporal Logic, Relevant Logic, Set Theories, Extensional Type Theories, Intensional Type Theories, Dependent Type Theories, ...

- Many logics have

- abstract syntax
- binding and substitution
- proof calculi with (schematic) rules & side conditions

“[I]t is important to define a **[uniform] presentation language** for defining logical systems that is a suitable basis for a logic-independent proof development environment.” ([HHP93])

⇒ “Edinburgh Logical Framework”, aka LF

Logical Framework: Motivation

- There are many logics

FOL, SFOL, HOL, Modal Logic, Dynamic Logics, Discourse Representation Theory, Temporal Logic, Relevant Logic, Set Theories, Extensional Type Theories, Intensional Type Theories, Dependent Type Theories, ...

- Many logics have
 - abstract syntax
 - binding and substitution
 - proof calculi with (schematic) rules & side conditions
 - a notion of logical relations

“[I]t is important to define a **[uniform] presentation language** for defining logical systems that is a suitable basis for a logic-independent proof development environment.” ([HHP93])

⇒ “Edinburgh Logical Framework”, aka LF

MMT/LF: A Module System over LF

Definition (MMT/LF Grammar)

Formalize knowledge (set/type theories, logics, ...) into *theories of declarations*:

Thy	$::=$	theory $T = \{Decl^*\}$	theory definition
$Decl$	$::=$	include $T \mid c : A [= A]$	declarations in a theory
A	$::=$	type $\mid c \mid x \mid A A \mid$ $\lambda x:A. A \mid \Pi x:A. A \mid A \rightarrow A$	terms

Example (Propositional Logic)

$A ::= \langle \text{unspecified} \rangle$	atoms	$\text{theory PL} = \left\{ \begin{array}{l} \text{prop: type} \\ \neg: \text{prop} \rightarrow \text{prop} \\ \wedge: \text{prop} \rightarrow \text{prop} \rightarrow \text{prop} \\ \supset: \text{prop} \rightarrow \text{prop} \rightarrow \text{prop} \\ \quad = \lambda p. \lambda q. \neg(p \wedge \neg q) \end{array} \right\}$
$P ::= A \mid \neg P \mid P \wedge P \mid$	propositions	
$P \supset P$		

MMT/LF: A Module System over LF

Definition (MMT/LF Grammar)

Formalize knowledge (set/type theories, logics, ...) into *theories of declarations*:

Thy	$::=$	theory $T = \{Decl^*\}$	theory definition
$Decl$	$::=$	include $T \mid c : A [= A]$	declarations in a theory
A	$::=$	type $\mid c \mid x \mid A A \mid$ $\lambda x:A. A \mid \Pi x:A. A \mid A \rightarrow A$	terms

Example (Propositional Logic)

$A ::= \langle \text{unspecified} \rangle$	atoms	$\text{theory PL} = \left\{ \begin{array}{l} \text{prop: type} \\ \neg: \text{prop} \rightarrow \text{prop} \\ \wedge: \text{prop} \rightarrow \text{prop} \rightarrow \text{prop} \\ \supset: \text{prop} \rightarrow \text{prop} \rightarrow \text{prop} \\ \quad = \lambda p. \lambda q. \neg(p \wedge \neg q) \\ a: \text{prop} \end{array} \right\}$
$P ::= A \mid \neg P \mid P \wedge P \mid$	propositions	
$P \supset P$		

Prop. Logic in MMT/LF

Syntax (as before):

$$\text{theory PL} = \left\{ \begin{array}{l} \text{prop: type} \\ \neg: \text{prop} \rightarrow \text{prop} \\ \wedge: \text{prop} \rightarrow \text{prop} \rightarrow \text{prop} \end{array} \right\}$$

Proof Calculus:

- use judgement-as-types paradigm: $\text{prop. } p \text{ provable} \iff \Vdash p \text{ inhabited}$

$$\text{theory PLND} = \left\{ \begin{array}{l} \text{include PL} \\ \Vdash: \text{prop} \rightarrow \text{type} \end{array} \right\}$$

Prop. Logic in MMT/LF

Syntax (as before):

$$\text{theory PL} = \left\{ \begin{array}{l} \text{prop: type} \\ \neg: \text{prop} \rightarrow \text{prop} \\ \wedge: \text{prop} \rightarrow \text{prop} \rightarrow \text{prop} \end{array} \right\}$$

Proof Calculus:

- use **judgement-as-types** paradigm: $\text{prop. } p \text{ provable} \iff \Vdash p \text{ inhabited}$
- encode schematic rules by dependent function types

$$\text{theory PLND} = \left\{ \begin{array}{l} \text{include PL} \\ \Vdash: \text{prop} \rightarrow \text{type} \\ \Rightarrow_I: \Pi p: \text{prop. } \Vdash p \rightarrow \Vdash \neg \neg p \\ \wedge_I: \Pi p q: \text{prop. } \Vdash p \rightarrow \Vdash q \rightarrow \Vdash p \wedge q \\ \wedge_{EL}: \Pi p q: \text{prop. } \Vdash p \wedge q \rightarrow \Vdash p \\ \dots \end{array} \right\}$$

Next Steps

Logical Relations

class of proof methods applicable on many type theories

Logical Framework

a uniform presentation language to formalize logics/type theories

Logical Relations for a Logical Framework

a uniform notion of “proof by logical relations” in the setting of LF

Recall: Proof by Logical Relation

- 1 Define a logical relation $P_{-}(-)$:
on every type T , a relation $P_T(-)$
- 2 Prove the “Basic Lemma”: $\Gamma \vdash t : T \implies P_T(t)$
- 3 Recover desired theorem as corollary

Recall: Proof by Logical Relation

- 1 Define a logical relation $P_{-}(-)$:
on every type T , a relation $P_T(-)$
- 2 Prove the “Basic Lemma”: $\Gamma \vdash t : T \implies P_T(t)$
- 3 Recover desired theorem as corollary

$$\text{theory PL} = \left\{ \begin{array}{l} \text{prop: type} \\ \neg: \text{prop} \rightarrow \text{prop} \\ \wedge: \text{prop} \rightarrow \text{prop} \rightarrow \text{prop} \end{array} \right\}$$

Recall: Proof by Logical Relation

- 1 Define a logical relation $P_{-}(-)$:
on every type T , a relation $P_T(-)$
- 2 Prove the “Basic Lemma”: $\Gamma \vdash t : T \implies P_T(t)$
- 3 Recover desired theorem as corollary

$$\text{theory PL} = \left\{ \begin{array}{l} \text{prop: type} \\ \neg: \text{prop} \rightarrow \text{prop} \\ \wedge: \text{prop} \rightarrow \text{prop} \rightarrow \text{prop} \end{array} \right\}$$

In MMT/LF, Logical Relations over PL = realizations of

i.e. views with dom. PL_r

$$\text{theory PL}_r = \left\{ \begin{array}{l} \text{include PL} \end{array} \right\}$$

Recall: Proof by Logical Relation

- 1 Define a logical relation $P_{-}(-)$:
on every type T , a relation $P_T(-)$
- 2 Prove the “Basic Lemma”: $\Gamma \vdash t : T \implies P_T(t)$
- 3 Recover desired theorem as corollary

$$\text{theory PL} = \left\{ \begin{array}{l} \text{prop: type} \\ \neg: \text{prop} \rightarrow \text{prop} \\ \wedge: \text{prop} \rightarrow \text{prop} \rightarrow \text{prop} \end{array} \right\}$$

In MMT/LF, Logical Relations over PL = realizations of

i.e. views with dom. PL_r

$$\text{theory PL}_r = \left\{ \begin{array}{l} \text{include PL} \\ \text{prop}_r: \text{prop} \rightarrow \text{type} \end{array} \right\}$$

Recall: Proof by Logical Relation

- 1 Define a logical relation $P_{-}(-)$:
on every type T , a relation $P_T(-)$
- 2 Prove the “Basic Lemma”: $\Gamma \vdash t : T \implies P_T(t)$
- 3 Recover desired theorem as corollary

$$\text{theory PL} = \left\{ \begin{array}{l} \text{prop: type} \\ \neg: \text{prop} \rightarrow \text{prop} \\ \wedge: \text{prop} \rightarrow \text{prop} \rightarrow \text{prop} \end{array} \right\}$$

In MMT/LF, Logical Relations over PL = realizations of

i.e. views with dom. PL_r

$$\text{theory PL}_r = \left\{ \begin{array}{l} \text{include PL} \\ \text{prop}_r : \text{prop} \rightarrow \text{type} \\ \neg_r : \Pi p : \text{prop}. \Pi p^* : \text{prop}_r p. \text{prop}_r (\neg p) \end{array} \right\}$$

Recall: Proof by Logical Relation

- 1 Define a logical relation $P_{-}(-)$:
on every type T , a relation $P_T(-)$
- 2 Prove the “Basic Lemma”: $\Gamma \vdash t : T \implies P_T(t)$
- 3 Recover desired theorem as corollary

$$\text{theory PL} = \left\{ \begin{array}{l} \text{prop: type} \\ \neg: \text{prop} \rightarrow \text{prop} \\ \wedge: \text{prop} \rightarrow \text{prop} \rightarrow \text{prop} \end{array} \right\}$$

In MMT/LF, Logical Relations over PL = realizations of

i.e. views with dom. PL_r

$$\text{theory PL}_r = \left\{ \begin{array}{l} \text{include PL} \\ \text{prop}_r : \text{prop} \rightarrow \text{type} \\ \neg_r : \Pi p : \text{prop}. \Pi p^* : \text{prop}_r p. \text{prop}_r (\neg p) \\ \wedge_r : \Pi p : \text{prop}. \Pi p^* : \text{prop}_r p. \Pi q : \text{prop}. \Pi q^* : \text{prop}_r q. \text{prop}_r (p \wedge q) \end{array} \right\}$$

Recall: Proof by Logical Relation

- 1 Define a logical relation $P_{-}(-)$:
on every type T , a relation $P_T(-)$
- 2 Prove the “Basic Lemma”: $\Gamma \vdash t : T \implies P_T(t)$
- 3 Recover desired theorem as corollary

In MMT/LF: Proofs by Logical Relation over PL

- 1 Define realization R of

i.e. a view $\text{PL}_r \rightarrow R$

$$\text{theory PL}_r = \left\{ \begin{array}{l} \text{include PL} \\ \text{prop}_r : \text{prop} \rightarrow \text{type} \\ \neg_r : \prod p : \text{prop}. \prod p^* : \text{prop}_r p. \text{prop}_r (\neg p) \\ \wedge_r : \prod p : \text{prop}. \prod p^* : \text{prop}_r p. \prod q : \text{prop}. \prod q^* : \text{prop}_r q. \text{prop}_r (p \wedge q) \end{array} \right\}$$

- 2 **Basic Lemma**
- 3 **Open Question**

Recall: Proof by Logical Relation

- 1 Define a logical relation $P_{-}(-)$:
on every type T , a relation $P_T(-)$
- 2 Prove the “Basic Lemma”: $\Gamma \vdash t : T \implies P_T(t)$
- 3 Recover desired theorem as corollary

In MMT/LF: Proofs by Logical Relation over PL

- 1 Define realization R of i.e. a view $\text{PL}_r \rightarrow R$

$$\text{theory } \text{PL}_r = \left\{ \begin{array}{l} \text{include PL} \\ \text{prop}_r : \text{prop} \rightarrow \text{type} \\ \neg_r : \prod p : \text{prop}. \prod p^* : \text{prop}_r p. \text{prop}_r (\neg p) \\ \wedge_r : \prod p : \text{prop}. \prod p^* : \text{prop}_r p. \prod q : \text{prop}. \prod q^* : \text{prop}_r q. \text{prop}_r (p \wedge q) \end{array} \right\}$$

- 2 **Basic Lemma:** $\vdash_{\text{PL}} p : \text{prop} \implies \vdash_R R(p) : \text{prop}_r p$ i.e. $\text{prop}_r p$ inhabited

- 3 Open Question

The Basic Lemma in Detail

Given a realization R of PL_r , we have:

Theorem (Basic Lemma for PL)

$$\vdash_{\text{PL}} p : \text{prop} \implies \vdash_R R(p) : \text{prop}_r p$$

i.e. $\text{prop}_r p$ inhabited

Assume $\vdash_{\text{PL}} p : \text{prop}$ and $\vdash_{\text{PL}} q : \text{prop}$.

Then all these terms are in the relation prop_r :

- p
- $p \wedge q$
- $p \wedge (\neg(q \wedge \neg\neg p))$
- $(q \wedge (p \wedge p \wedge \neg((q \wedge \neg q) \wedge p))) \wedge p \wedge (\neg(q \wedge \neg\neg p))$

The Basic Lemma in Detail

Given a realization R of PL_r , we have:

Theorem (Basic Lemma for PL)

$$\vdash_{\text{PL}} p : \text{prop} \implies \vdash_R R(p) : \text{prop}_r p$$

i.e. $\text{prop}_r p$ inhabited

Assume $\vdash_{\text{PL}} p : \text{prop}$ and $\vdash_{\text{PL}} q : \text{prop}$.

Then all these terms are in the relation prop_r :

- p
- $p \wedge q$
- $p \wedge (\neg(q \wedge \neg\neg p))$
- $(q \wedge (p \wedge p \wedge \neg((q \wedge \neg q) \wedge p))) \wedge p \wedge (\neg(q \wedge \neg\neg p))$

MMT/LF logical relations prove statements all-quantified over terms of an MMT/LF theory.

Examples for MMT/LF Logical Relations

Any “realistic” proof by logical relations would be far too complicated
Instead, we stay in PL and prove

Theorem (Tertium Non Datur)

If $a \vee \neg a$ for all atoms,
then $p \vee \neg p$ for all propositions.

Theorem (Double Negation Elimination)

If $a \Leftrightarrow \neg\neg a$ for all atoms,
then $p \Leftrightarrow \neg\neg p$ for all propositions.

Do you see how both are instances of the Basic Lemma?

Tertium Non Datur (the goal)

If $a \vee \neg a$ for all atoms,
then $p \vee \neg p$ for all propositions.

Basic Lemma for TND (what we get)

$$\vdash_{\text{PL}} p : \text{prop} \implies \vdash_{\text{TND}} \text{TND}(p) : \text{prop}_r p$$

theory TND = {

- include PL
- include PLND
- realize PL_r
- prop_r : prop → type
- = ?
- $\neg_r : \Pi p : \text{prop}. \Pi p^* : \text{prop}_r p. \text{prop}_r (\neg p)$
- = ?
- $\wedge_r : \Pi p : \text{prop}. \Pi p^* : \text{prop}_r p. \Pi q : \text{prop}. \Pi q^* : \text{prop}_r q. \text{prop}_r (p \wedge q)$
- = ?

}

Tertium Non Datur (the goal)

If $a \vee \neg a$ for all atoms,
then $p \vee \neg p$ for all propositions.

Basic Lemma for TND (what we get)

$$\vdash_{\text{PL}} p : \text{prop} \implies \vdash_{\text{TND}} \text{TND}(p) : \text{prop}_r p$$

theory TND = {

- include PL
- include PLND

- realize PL_r
- prop_r : prop → type
 - = $\lambda p. \Vdash p \vee \neg p$
- $\neg_r : \Pi p : \text{prop}. \Pi p^* : \text{prop}_r p. \text{prop}_r (\neg p)$
 - = ?
- $\wedge_r : \Pi p : \text{prop}. \Pi p^* : \text{prop}_r p. \Pi q : \text{prop}. \Pi q^* : \text{prop}_r q. \text{prop}_r (p \wedge q)$
 - = ?

}

Tertium Non Datur (the goal)

If $a \vee \neg a$ for all atoms,
then $p \vee \neg p$ for all propositions.

Basic Lemma for TND (what we get)

$\vdash_{\text{PL}} p : \text{prop} \implies \vdash_{\text{TND}} \text{TND}(p) : \Vdash p \vee \neg p$

theory TND = {

- include PL
- include PLND

- realize PL_r
- prop_r : prop → type
- = $\lambda p. \Vdash p \vee \neg p$
- $\neg_r : \Pi p : \text{prop}. \Pi p^* : \text{prop}_r p. \text{prop}_r (\neg p)$
- = ?
- $\wedge_r : \Pi p : \text{prop}. \Pi p^* : \text{prop}_r p. \Pi q : \text{prop}. \Pi q^* : \text{prop}_r q. \text{prop}_r (p \wedge q)$
- = ?

}

Tertium Non Datur (the goal)

If $a \vee \neg a$ for all atoms,
then $p \vee \neg p$ for all propositions.

$\text{theory TND} = \left\{ \begin{array}{l} \text{include PL} \\ \text{include PLND} \\ \text{realize PL}_r \\ \text{prop}_r : \text{prop} \rightarrow \text{type} \\ \quad = \lambda p. \Vdash p \vee \neg p \\ \neg_r : \Pi p : \text{prop. } \Pi p^* : \text{prop}_r p. \text{prop}_r (\neg p) \\ \quad = ? \\ \wedge_r : \Pi p : \text{prop. } \Pi p^* : \text{prop}_r p. \Pi q : \text{prop. } \Pi q^* : \text{prop}_r q. \text{prop}_r (p \wedge q) \\ \quad = ? \end{array} \right.$	<table border="0" style="width: 100%;"> <tr> <td style="width: 5%; text-align: right;">1</td> <td style="border-left: 1px solid black; padding-left: 5px;">$p \vee \neg p$</td> <td></td> </tr> <tr> <td style="text-align: right;">2</td> <td style="border-left: 1px solid black; padding-left: 5px;"> <table border="0" style="width: 100%;"> <tr> <td style="border-left: 1px solid black; padding-left: 5px;">p</td> <td></td> </tr> </table> </td> <td></td> </tr> <tr> <td style="text-align: right;">3</td> <td style="border-left: 1px solid black; padding-left: 5px;">$\neg \neg p$</td> <td>$\neg_I, 2$</td> </tr> <tr> <td style="text-align: right;">4</td> <td style="border-left: 1px solid black; padding-left: 5px;">$\neg p \vee \neg \neg p$</td> <td>$\vee_{IR}, 3$</td> </tr> <tr> <td style="text-align: right;">5</td> <td style="border-left: 1px solid black; padding-left: 5px;"> <table border="0" style="width: 100%;"> <tr> <td style="border-left: 1px solid black; padding-left: 5px;">$\neg p$</td> <td></td> </tr> </table> </td> <td></td> </tr> <tr> <td style="text-align: right;">6</td> <td style="border-left: 1px solid black; padding-left: 5px;">$\neg p \vee \neg \neg p$</td> <td>$\vee_{IL}, 5$</td> </tr> <tr> <td style="text-align: right;">7</td> <td style="border-left: 1px solid black; padding-left: 5px;">$\neg p \vee \neg \neg p$</td> <td>$\vee_E, 1, 2-4, 5-6$</td> </tr> </table>	1	$p \vee \neg p$		2	<table border="0" style="width: 100%;"> <tr> <td style="border-left: 1px solid black; padding-left: 5px;">p</td> <td></td> </tr> </table>	p			3	$\neg \neg p$	$\neg_I, 2$	4	$\neg p \vee \neg \neg p$	$\vee_{IR}, 3$	5	<table border="0" style="width: 100%;"> <tr> <td style="border-left: 1px solid black; padding-left: 5px;">$\neg p$</td> <td></td> </tr> </table>	$\neg p$			6	$\neg p \vee \neg \neg p$	$\vee_{IL}, 5$	7	$\neg p \vee \neg \neg p$	$\vee_E, 1, 2-4, 5-6$
	1	$p \vee \neg p$																								
	2	<table border="0" style="width: 100%;"> <tr> <td style="border-left: 1px solid black; padding-left: 5px;">p</td> <td></td> </tr> </table>	p																							
	p																									
	3	$\neg \neg p$	$\neg_I, 2$																							
	4	$\neg p \vee \neg \neg p$	$\vee_{IR}, 3$																							
	5	<table border="0" style="width: 100%;"> <tr> <td style="border-left: 1px solid black; padding-left: 5px;">$\neg p$</td> <td></td> </tr> </table>	$\neg p$																							
$\neg p$																										
6	$\neg p \vee \neg \neg p$	$\vee_{IL}, 5$																								
7	$\neg p \vee \neg \neg p$	$\vee_E, 1, 2-4, 5-6$																								

Tertium Non Datur (the goal)

If $a \vee \neg a$ for all atoms,
then $p \vee \neg p$ for all propositions.

$\text{theory TND} = \left\{ \begin{array}{l} \text{include PL} \\ \text{include PLND} \\ \text{realize PL}_r \\ \text{prop}_r : \text{prop} \rightarrow \text{type} \\ \quad = \lambda p. \Vdash p \vee \neg p \\ \neg_r : \Pi p : \text{prop}. \Pi p^* : \text{prop}_r p. \text{prop}_r (\neg p) \\ \quad = \lambda p. \lambda p^*. \vee_E p^* (\lambda p. \vee_{IR} (\neg_I p)) (\lambda np. \vee_{IL} np) \\ \wedge_r : \Pi p : \text{prop}. \Pi p^* : \text{prop}_r p. \Pi q : \text{prop}. \Pi q^* : \text{prop}_r q. \text{prop}_r (p \wedge q) \\ \quad = ? \end{array} \right.$	<table border="0" style="width: 100%;"> <tr> <td style="width: 5%; text-align: right;">1</td> <td style="border-left: 1px solid black; padding-left: 5px;">$p \vee \neg p$</td> <td></td> </tr> <tr> <td style="text-align: right;">2</td> <td style="border-left: 1px solid black; padding-left: 5px;"> <div style="border-left: 1px solid black; padding-left: 5px;">p</div> </td> <td></td> </tr> <tr> <td style="text-align: right;">3</td> <td style="border-left: 1px solid black; padding-left: 5px;">$\neg\neg p$</td> <td>$\neg_I, 2$</td> </tr> <tr> <td style="text-align: right;">4</td> <td style="border-left: 1px solid black; padding-left: 5px;">$\neg p \vee \neg\neg p$</td> <td>$\vee_{IR}, 3$</td> </tr> <tr> <td style="text-align: right;">5</td> <td style="border-left: 1px solid black; padding-left: 5px;"> <div style="border-left: 1px solid black; padding-left: 5px;">$\neg p$</div> </td> <td></td> </tr> <tr> <td style="text-align: right;">6</td> <td style="border-left: 1px solid black; padding-left: 5px;">$\neg p \vee \neg\neg p$</td> <td>$\vee_{IL}, 5$</td> </tr> <tr> <td style="text-align: right;">7</td> <td style="border-left: 1px solid black; padding-left: 5px;">$\neg p \vee \neg\neg p$</td> <td>$\vee_E, 1, 2-4, 5-6$</td> </tr> </table>	1	$p \vee \neg p$		2	<div style="border-left: 1px solid black; padding-left: 5px;">p</div>		3	$\neg\neg p$	$\neg_I, 2$	4	$\neg p \vee \neg\neg p$	$\vee_{IR}, 3$	5	<div style="border-left: 1px solid black; padding-left: 5px;">$\neg p$</div>		6	$\neg p \vee \neg\neg p$	$\vee_{IL}, 5$	7	$\neg p \vee \neg\neg p$	$\vee_E, 1, 2-4, 5-6$
	1	$p \vee \neg p$																				
	2	<div style="border-left: 1px solid black; padding-left: 5px;">p</div>																				
	3	$\neg\neg p$	$\neg_I, 2$																			
	4	$\neg p \vee \neg\neg p$	$\vee_{IR}, 3$																			
	5	<div style="border-left: 1px solid black; padding-left: 5px;">$\neg p$</div>																				
	6	$\neg p \vee \neg\neg p$	$\vee_{IL}, 5$																			
7	$\neg p \vee \neg\neg p$	$\vee_E, 1, 2-4, 5-6$																				

Tertium Non Datur (the goal)

If $a \vee \neg a$ for all atoms,
then $p \vee \neg p$ for all propositions.

Basic Lemma for TND (what we get)

$$\vdash_{\text{PL}} p : \text{prop} \implies \vdash_{\text{TND}} \text{TND}(p) : \Vdash p \vee \neg p$$

theory TND = {

- include PL
- include PLND

- realize PL_r
- $\text{prop}_r : \text{prop} \rightarrow \text{type}$
- $= \lambda p. \Vdash p \vee \neg p$
- $\neg_r : \Pi p : \text{prop}. \Pi p^* : \text{prop}_r p. \text{prop}_r (\neg p)$
- $= \lambda p. \lambda p^*. \vee_E p^* (\lambda p. \vee_{\text{IR}} (\neg_I p)) (\lambda np. \vee_{\text{IL}} np)$
- $\wedge_r : \Pi p : \text{prop}. \Pi p^* : \text{prop}_r p. \Pi q : \text{prop}. \Pi q^* : \text{prop}_r q. \text{prop}_r (p \wedge q)$
- $= \dots$

}

Tertium Non Datur (the goal)

If $a \vee \neg a$ for all atoms,
then $p \vee \neg p$ for all propositions.

Basic Lemma for TND (what we get)

$$\vdash_{\text{PL}} p : \text{prop} \implies \vdash_{\text{TND}} \text{TND}(p) : \Vdash p \vee \neg p$$

theory TND = {

- include PL
- include PLND

- realize PL_r
- $\text{prop}_r : \text{prop} \rightarrow \text{type}$
- $= \lambda p. \Vdash p \vee \neg p$
- $\neg_r : \Pi p : \text{prop}. \Pi p^* : \text{prop}_r p. \text{prop}_r (\neg p)$
- $= \lambda p. \lambda p^*. \forall_E p^* (\lambda \mathfrak{p}. \forall_{\text{IR}} (\neg_I \mathfrak{p})) (\lambda \mathfrak{np}. \forall_{\text{IL}} \mathfrak{np})$
- $\wedge_r : \Pi p : \text{prop}. \Pi p^* : \text{prop}_r p. \Pi q : \text{prop}. \Pi q^* : \text{prop}_r q. \text{prop}_r (p \wedge q)$
- $= \dots$
- $a_r : \text{prop}_r a = \langle \text{encode assumption} \rangle$

}

Double Negation Elimination (the goal)

If $a \Leftrightarrow \neg\neg a$ for all atoms,
then $p \Leftrightarrow \neg\neg p$ for all propositions.

Basic Lemma for DNE (what we get)

$\vdash_{\text{PL}} p : \text{prop} \implies \vdash_{\text{DNE}} \text{DNE}(p) : \text{prop}_r p$

theory DNE = {

- include PL
- include PLND
- realize PL_r
- prop_r : prop → type
- = ?
- $\neg_r : \Pi p : \text{prop}. \Pi p^* : \text{prop}_r p. \text{prop}_r (\neg p)$
- = ?
- $\wedge_r : \Pi p : \text{prop}. \Pi p^* : \text{prop}_r p. \Pi q : \text{prop}. \Pi q^* : \text{prop}_r q. \text{prop}_r (p \wedge q)$
- = ?

}

Double Negation Elimination (the goal)

If $a \Leftrightarrow \neg\neg a$ for all atoms,
then $p \Leftrightarrow \neg\neg p$ for all propositions.

Basic Lemma for DNE (what we get)

$\vdash_{\text{PL}} p : \text{prop} \implies \vdash_{\text{DNE}} \text{DNE}(p) : \text{prop}_r p$

theory DNE = {

- include PL
- include PLND
- realize PL_r
- prop_r : prop → type
- $= \lambda p. \Vdash p \Leftrightarrow \neg\neg p$
- $\neg_r : \Pi p : \text{prop}. \Pi p^* : \text{prop}_r p. \text{prop}_r (\neg p)$
- $= ?$
- $\wedge_r : \Pi p : \text{prop}. \Pi p^* : \text{prop}_r p. \Pi q : \text{prop}. \Pi q^* : \text{prop}_r q. \text{prop}_r (p \wedge q)$
- $= ?$

}

Double Negation Elimination (the goal)

If $a \Leftrightarrow \neg\neg a$ for all atoms,
then $p \Leftrightarrow \neg\neg p$ for all propositions.

Basic Lemma for DNE (what we get)

$\vdash_{\text{PL}} p : \text{prop} \implies \vdash_{\text{DNE}} \text{DNE}(p) : \Vdash p \Leftrightarrow \neg\neg p$

theory DNE = {

- include PL
- include PLND

- realize PL_r
- prop_r : prop → type
- = $\lambda p. \Vdash p \Leftrightarrow \neg\neg p$
- $\neg_r : \Pi p : \text{prop}. \Pi p^* : \text{prop}_r p. \text{prop}_r (\neg p)$
- = ?
- $\wedge_r : \Pi p : \text{prop}. \Pi p^* : \text{prop}_r p. \Pi q : \text{prop}. \Pi q^* : \text{prop}_r q. \text{prop}_r (p \wedge q)$
- = ?

}

Double Negation Elimination (the goal)

If $a \Leftrightarrow \neg\neg a$ for all atoms,
then $p \Leftrightarrow \neg\neg p$ for all propositions.

$\text{theory DNE} = \left\{ \begin{array}{l} \text{include PL} \\ \text{include PLND} \\ \text{realize PL}_r \\ \text{prop}_r : \text{prop} \rightarrow \text{type} \\ \quad = \lambda p. \Vdash p \Leftrightarrow \neg\neg p \\ \neg_r : \prod p : \text{prop. } \prod p^* : \text{prop}_r \text{ p. } \text{prop}_r (\neg p) \\ \quad = ? \\ \wedge_r : \prod p : \text{prop. } \prod p^* : \text{prop}_r \text{ p. } \prod q : \text{prop. } \prod q^* : \text{prop}_r \text{ q. } \text{prop}_r (p \wedge q) \\ \quad = ? \end{array} \right.$	<div style="display: flex; align-items: center;"> <div style="margin-right: 10px;">1</div> <div style="border-left: 1px solid black; padding-left: 10px;"> $p \Leftrightarrow \neg\neg p$ </div> </div>	
	<div style="display: flex; align-items: center;"> <div style="margin-right: 10px;">2</div> <div style="border-left: 1px solid black; padding-left: 10px;"> <div style="border-left: 1px solid black; padding-left: 10px;"> $\neg p$ </div> </div> </div>	
	<div style="display: flex; align-items: center;"> <div style="margin-right: 10px;">3</div> <div style="border-left: 1px solid black; padding-left: 10px;"> <div style="border-left: 1px solid black; padding-left: 10px;"> $\neg\neg(\neg p)$ </div> </div> </div>	$\neg_I, 2$
	<div style="display: flex; align-items: center;"> <div style="margin-right: 10px;">4</div> <div style="border-left: 1px solid black; padding-left: 10px;"> <div style="border-left: 1px solid black; padding-left: 10px;"> $\neg\neg(\neg p)$ </div> </div> </div>	
	<div style="display: flex; align-items: center;"> <div style="margin-right: 10px;">5</div> <div style="border-left: 1px solid black; padding-left: 10px;"> <div style="border-left: 1px solid black; padding-left: 10px;"> $\neg(\neg\neg p)$ </div> </div> </div>	$\text{reit.}, 4$
	<div style="display: flex; align-items: center;"> <div style="margin-right: 10px;">6</div> <div style="border-left: 1px solid black; padding-left: 10px;"> <div style="border-left: 1px solid black; padding-left: 10px;"> $\neg p$ </div> </div> </div>	$\Leftrightarrow_{\text{EL}}, 1, 5$
	<div style="display: flex; align-items: center;"> <div style="margin-right: 10px;">7</div> <div style="border-left: 1px solid black; padding-left: 10px;"> $(\neg p) \Leftrightarrow \neg\neg(\neg p)$ </div> </div>	$\Leftrightarrow_I, 2-3, 4-6$

Double Negation Elimination (the goal)

If $a \Leftrightarrow \neg\neg a$ for all atoms,
then $p \Leftrightarrow \neg\neg p$ for all propositions.

$\text{theory DNE} = \left\{ \begin{array}{l} \text{include PL} \\ \text{include PLND} \\ \text{realize PL}_r \\ \text{prop}_r : \text{prop} \rightarrow \text{type} \\ \quad = \lambda p. \Vdash p \Leftrightarrow \neg\neg p \\ \neg_r : \Pi p : \text{prop}. \Pi p^* : \text{prop}_r p. \text{prop}_r (\neg p) \\ \quad = \lambda p. \lambda p^*. \Leftrightarrow_I (\lambda np. \Rightarrow_I np) (\lambda nnp. \Leftrightarrow_{EL} p^* nnp) \\ \wedge_r : \Pi p : \text{prop}. \Pi p^* : \text{prop}_r p. \Pi q : \text{prop}. \Pi q^* : \text{prop}_r q. \text{prop}_r (p \wedge q) \\ \quad = ? \end{array} \right.$	<table border="0" style="width: 100%;"> <tr> <td style="width: 5%; text-align: right;">1</td> <td style="border-left: 1px solid black; padding-left: 10px;">$p \Leftrightarrow \neg\neg p$</td> <td></td> </tr> <tr> <td style="text-align: right;">2</td> <td style="border-left: 1px solid black; padding-left: 10px;"> <div style="border-left: 1px solid black; padding-left: 10px;"> $\neg p$ </div> </td> <td></td> </tr> <tr> <td style="text-align: right;">3</td> <td style="border-left: 1px solid black; padding-left: 10px;"> <div style="border-left: 1px solid black; padding-left: 10px;"> $\neg\neg(\neg p)$ </div> </td> <td style="padding-left: 20px;">$\Rightarrow_I, 2$</td> </tr> <tr> <td style="text-align: right;">4</td> <td style="border-left: 1px solid black; padding-left: 10px;"> <div style="border-left: 1px solid black; padding-left: 10px;"> $\neg\neg(\neg p)$ </div> </td> <td></td> </tr> <tr> <td style="text-align: right;">5</td> <td style="border-left: 1px solid black; padding-left: 10px;"> <div style="border-left: 1px solid black; padding-left: 10px;"> $\neg(\neg\neg p)$ </div> </td> <td style="padding-left: 20px;">$\text{reit.}, 4$</td> </tr> <tr> <td style="text-align: right;">6</td> <td style="border-left: 1px solid black; padding-left: 10px;"> <div style="border-left: 1px solid black; padding-left: 10px;"> $\neg p$ </div> </td> <td style="padding-left: 20px;">$\Leftrightarrow_{EL}, 1, 5$</td> </tr> <tr> <td style="text-align: right;">7</td> <td style="border-left: 1px solid black; padding-left: 10px;">$(\neg p) \Leftrightarrow \neg\neg(\neg p)$</td> <td style="padding-left: 20px;">$\Leftrightarrow_I, 2-3, 4-6$</td> </tr> </table>	1	$p \Leftrightarrow \neg\neg p$		2	<div style="border-left: 1px solid black; padding-left: 10px;"> $\neg p$ </div>		3	<div style="border-left: 1px solid black; padding-left: 10px;"> $\neg\neg(\neg p)$ </div>	$\Rightarrow_I, 2$	4	<div style="border-left: 1px solid black; padding-left: 10px;"> $\neg\neg(\neg p)$ </div>		5	<div style="border-left: 1px solid black; padding-left: 10px;"> $\neg(\neg\neg p)$ </div>	$\text{reit.}, 4$	6	<div style="border-left: 1px solid black; padding-left: 10px;"> $\neg p$ </div>	$\Leftrightarrow_{EL}, 1, 5$	7	$(\neg p) \Leftrightarrow \neg\neg(\neg p)$	$\Leftrightarrow_I, 2-3, 4-6$
	1	$p \Leftrightarrow \neg\neg p$																				
	2	<div style="border-left: 1px solid black; padding-left: 10px;"> $\neg p$ </div>																				
	3	<div style="border-left: 1px solid black; padding-left: 10px;"> $\neg\neg(\neg p)$ </div>	$\Rightarrow_I, 2$																			
	4	<div style="border-left: 1px solid black; padding-left: 10px;"> $\neg\neg(\neg p)$ </div>																				
	5	<div style="border-left: 1px solid black; padding-left: 10px;"> $\neg(\neg\neg p)$ </div>	$\text{reit.}, 4$																			
	6	<div style="border-left: 1px solid black; padding-left: 10px;"> $\neg p$ </div>	$\Leftrightarrow_{EL}, 1, 5$																			
7	$(\neg p) \Leftrightarrow \neg\neg(\neg p)$	$\Leftrightarrow_I, 2-3, 4-6$																				

Double Negation Elimination (the goal)

If $a \Leftrightarrow \neg\neg a$ for all atoms,
then $p \Leftrightarrow \neg\neg p$ for all propositions.

Basic Lemma for DNE (what we get)

$\vdash_{\text{PL}} p : \text{prop} \implies \vdash_{\text{DNE}} \text{DNE}(p) : \Vdash p \Leftrightarrow \neg\neg p$

theory DNE = {

- include PL
- include PLND

- realize PL_r
- prop_r : prop → type
- = λp. $\Vdash p \Leftrightarrow \neg\neg p$
- ¬_r : Πp : prop. Πp* : prop_r p. prop_r (¬p)
- = λp. λp*. $\Leftrightarrow_{\text{I}} (\lambda np. \Rightarrow_{\text{I}} np) (\lambda nnp. \Leftrightarrow_{\text{EL}} p^* nnp)$
- ∧_r : Πp : prop. Πp* : prop_r p. Πq : prop. Πq* : prop_r q. prop_r (p ∧ q)
- = ...

}

Double Negation Elimination (the goal)

If $a \Leftrightarrow \neg\neg a$ for all atoms,
then $p \Leftrightarrow \neg\neg p$ for all propositions.

Basic Lemma for DNE (what we get)

$\vdash_{\text{PL}} p : \text{prop} \implies \vdash_{\text{DNE}} \text{DNE}(p) : \Vdash p \Leftrightarrow \neg\neg p$

theory DNE = {

- include PL
- include PLND

- realize PL_r
- prop_r : prop → type
- = λp. $\Vdash p \Leftrightarrow \neg\neg p$
- ¬_r : Πp : prop. Πp* : prop_r p. prop_r (¬p)
- = λp. λp*. $\Leftrightarrow_{\text{I}} (\lambda np. \Rightarrow_{\text{I}} np) (\lambda nnnp. \Leftrightarrow_{\text{EL}} p^* nnnp)$
- ∧_r : Πp : prop. Πp* : prop_r p. Πq : prop. Πq* : prop_r q. prop_r (p ∧ q)
- = ...
- a_r : prop_r a = ⟨encode assumption⟩

}

Conclusion

Logical Relations: a class of proof methods

- used to prove meta theorems about type theories strong normalization, type safety, ...
- called for when induction over terms fails and IHs based on their type are required
- pattern of a **proof by logical relation**:
 - 1 Define a logical relation $P_{-}(-)$: for every type T , a relation $P_T(-)$ on terms of T
 - 2 Prove the “Basic Lemma”: $\Gamma \vdash t : T \implies P_T(t)$
 - 3 Recover desired theorem as corollary

Logical Relations in MMT/LF:

only given for PL here

- 1 Define realization R of

$$\text{theory PL}_r = \left\{ \begin{array}{l} \text{include PL} \\ \text{prop}_r : \text{prop} \rightarrow \text{type} \\ \neg_r : \Pi p : \text{prop}. \Pi p^* : \text{prop}_r p. \text{prop}_r (\neg p) \end{array} \right\}$$

- 2 **Basic Lemma:** $\vdash_{\text{PL}} p : \text{prop} \implies \vdash_R R(p) : \text{prop}_r p$

Appetizer for more Pursuit

- Logical relations that relate “modulo view application”

So far: given an MMT/LF theory T ,

MMT/LF logical relations over T prove statements about t
all-quantified over all T -terms t

Now: given MMT/LF view $v: S \rightarrow T$:

MMT/LF logical relations **over** $v: S \rightarrow T$ prove statements about $v(s)$
all-quantified over all S -terms s

e.g. $v = \text{TypeEras}: \text{Church} \rightarrow \text{Curry}$, then prove “TypeEras(Church term) typable”.

- How can we make the Basic Lemma accessible *within* the formalization?

open question!

Further Pointers I

- Logical Relations:

- Concise and to-the-point proof of SN of STLC: [Zil12]

Note the relation for function types there is missing the condition of strong normalization, which I corrected for in my slides; if in doubt, compare with [Sko19].

- Another proof of SN of STLC: [Ahm13] (videos), third-party transcript at [Sko19, ch. 2]

Here, the lambda calculus is equipped with if-then-else constructs, too, making the proof a bit more complicated (on a first read). After SN of STLC, Ahmed considers several extensions of STLC, among others, with recursive types and reference types, and uses logical relations to prove meta theorems about them.

- Unrelated, but interesting: connection of logical relations with automata simulations: [tcs.SE]

- Logical Frameworks:

- MMT System: [Rab17; RM18]
- Edinburgh LF: [HHP93]

- Logical Relations for a Logical Framework:

Further Pointers II

- The article on which this talk is based: [RS13]
- Proof of SN in Twelf: [SS08]

Concerning several ideas, the Twelf system is an ancestor of the MMT system. Hence, it is plausible that any method given in Twelf to prove SN of STLC can be carried over to MMT.

- Details of the mentioned Church to Curry idea: [Rou20, ch. 7]

This concrete exposition of mine gives a logical relation-free account of the Church to Curry idea for the MMT system. A version with logical relations in mind has been implemented as of January 2021, but not yet reported on.

- [Ahm13] Amal Ahmed. “Logical Relations”. Oregon Programming Languages Summer School 2013. July 2013. URL: <https://www.cs.uoregon.edu/research/summerschool/summer13/curriculum.html>.
- [HHP93] Robert Harper, Furio Honsell, and Gordon Plotkin. “A framework for defining logics”. In: *Journal of the Association for Computing Machinery* 40.1 (1993), pp. 143–184.
- [Rab17] Florian Rabe. “How to Identify, Translate, and Combine Logics?” In: *Journal of Logic and Computation* 27.6 (2017), pp. 1753–1798.

Further Pointers III

- [RM18] Florian Rabe and Dennis Müller. “Structuring Theories with Implicit Morphisms”. In: *24th International Workshop on Algebraic Development Techniques 2018*. 2018. URL: https://kwarc.info/people/frabe/Research/RM_implicit_18.pdf.
- [Rou20] Navid Roux. *Structure-Preserving Diagram Operators*. Master Project Report. July 17, 2020. URL: https://gl.kwarc.info/supervision/projectarchive/-/blob/master/2020/Roux_Navid.pdf.
- [RS13] Florian Rabe and Kristina Sojakova. “Logical Relations for a Logical Framework”. In: *ACM Transactions on Computational Logic* (2013). URL: https://kwarc.info/frabe/Research/RS_logrels_12.pdf.
- [Sko19] Lau Skorstengaard. *An Introduction to Logical Relations*. 2019.
- [SS08] C. Schürmann and J. Sarnat. “Structural Logical Relations”. In: *2008 23rd Annual IEEE Symposium on Logic in Computer Science*. 2008, pp. 69–80. DOI: [10.1109/LICS.2008.44](https://doi.org/10.1109/LICS.2008.44). (Visited on 01/26/2020).
- [tcs.SE] Hongjin Liang (<https://cstheory.stackexchange.com/users/2703/hongjin-liang>). *What are the differences between logical relations and simulations?* Theoretical Computer Science Stack Exchange. URL: <https://cstheory.stackexchange.com/q/5427> (version: 2012-06-04). URL: <https://cstheory.stackexchange.com/q/5427>.
- [Zil12] Beta Ziliani. “Strong Normalization for Simply Typed Lambda Calculus”. based on lectures by Derek Dreyer. July 2012. URL: <https://web.archive.org/web/20170829154544/https://people.mpi-sws.org/~dg/teaching/pt2012/sn.pdf> (visited on 01/26/2021).