

A Formal Correspondence between OMDoc with Alternative Proofs and the $\overline{\lambda\mu\tilde{\mu}}$ -Calculus

Serge Autexier

DFKI GmbH & CS Department, Saarland University
Saarbrücken, Germany

Claudio Sacerdoti-Coen

Department of Computer Science
University of Bologna, Italy

MKM'06, 11th August 2006

Wokingham, UK

Motivation – MKM'05



A Generic Proof *Datastructure*: [Autexier,Benzmüller,Dietrich,Meier,Wirth]

- Calculus independent representation of proof attempts
- At different levels of granularity and alternative subproofs
- View = selection of specific granularity and subproof alternative
- Can be serialized to OMDOC proofs (Except for alternative subproofs)
- Problem: PDS and OMDOC lack semantics specification

Investigation of $\bar{\lambda}\mu\tilde{\mu}$ -calculus as a proof format [Sacerdoti-Coen]

- Intuitionistic fragment has straightforward translation into pseudo-natural language (rendering semantics)
- Proof terms in the classical fragment can be translated into the intuitionistic fragment
- Question: Is the classical fragment necessary to exploit the $\bar{\lambda}\mu\tilde{\mu}$ -calculus as a proof format?

What did we do?



Use $\bar{\lambda}\mu\tilde{\mu}$ -calculus to provide a semantics for OMDOC + Alternatives (= PDS)

- Choose a fragment of $\bar{\lambda}\mu\tilde{\mu}$ -calculus as proof terms which is suitable to represent alternative proofs

What did we do?

Use $\bar{\lambda}\mu\tilde{\mu}$ -calculus to provide a semantics for OMDOC + Alternatives (= PDS)

- Choose a fragment of $\bar{\lambda}\mu\tilde{\mu}$ -calculus as proof terms which is suitable to represent alternative proofs
- Defined **rendering semantics** $[\cdot]_{\bar{\lambda}\mu\tilde{\mu}}$ for $\bar{\lambda}\mu\tilde{\mu}$ -calculus fragment

What did we do?

Use $\bar{\lambda}\mu\tilde{\mu}$ -calculus to provide a semantics for OMDOC + Alternatives (= PDS)

- Choose a fragment of $\bar{\lambda}\mu\tilde{\mu}$ -calculus as proof terms which is suitable to represent alternative proofs
- Defined **rendering semantics** $[\cdot]_{\bar{\lambda}\mu\tilde{\mu}}$ for $\bar{\lambda}\mu\tilde{\mu}$ -calculus fragment
- Defined OMDOC proofs with alternatives

What did we do?

Use $\bar{\lambda}\mu\tilde{\mu}$ -calculus to provide a semantics for OMDOC + Alternatives (= PDS)

- Choose a fragment of $\bar{\lambda}\mu\tilde{\mu}$ -calculus as proof terms which is suitable to represent alternative proofs
- Defined **rendering semantics** $[[\cdot]]_{\bar{\lambda}\mu\tilde{\mu}}$ for $\bar{\lambda}\mu\tilde{\mu}$ -calculus fragment
- Defined OMDOC proofs with alternatives
- Defined **rendering semantics** $[[\cdot]]_O$ for OMDOC proofs

What did we do?

Use $\bar{\lambda}\mu\tilde{\mu}$ -calculus to provide a semantics for OMDOC + Alternatives (= PDS)

- Choose a fragment of $\bar{\lambda}\mu\tilde{\mu}$ -calculus as proof terms which is suitable to represent alternative proofs
- Defined **rendering semantics** $[\cdot]_{\bar{\lambda}\mu\tilde{\mu}}$ for $\bar{\lambda}\mu\tilde{\mu}$ -calculus fragment
- Defined OMDOC proofs with alternatives
- Defined **rendering semantics** $[\cdot]_O$ for OMDOC proofs
- Defined translation from $\bar{\lambda}\mu\tilde{\mu}$ to OMDOC

What did we do?

Use $\bar{\lambda}\mu\tilde{\mu}$ -calculus to provide a semantics for OMDOC + Alternatives (= PDS)

- Choose a fragment of $\bar{\lambda}\mu\tilde{\mu}$ -calculus as proof terms which is suitable to represent alternative proofs
- Defined **rendering semantics** $[\cdot]_{\bar{\lambda}\mu\tilde{\mu}}$ for $\bar{\lambda}\mu\tilde{\mu}$ -calculus fragment
- Defined OMDOC proofs with alternatives
- Defined **rendering semantics** $[\cdot]_O$ for OMDOC proofs
- Defined translation from $\bar{\lambda}\mu\tilde{\mu}$ to OMDOC
- and translation from OMDOC to $\bar{\lambda}\mu\tilde{\mu}$

What did we do?



Use $\bar{\lambda}\mu\tilde{\mu}$ -calculus to provide a semantics for OMDOC + Alternatives (= PDS)

- Choose a fragment of $\bar{\lambda}\mu\tilde{\mu}$ -calculus as proof terms which is suitable to represent alternative proofs
- Defined **rendering semantics** $[[\cdot]]_{\bar{\lambda}\mu\tilde{\mu}}$ for $\bar{\lambda}\mu\tilde{\mu}$ -calculus fragment
- Defined OMDOC proofs with alternatives
- Defined **rendering semantics** $[[\cdot]]_O$ for OMDOC proofs
- Defined translation from $\bar{\lambda}\mu\tilde{\mu}$ to OMDOC
- and translation from OMDOC to $\bar{\lambda}\mu\tilde{\mu}$
- Such that

What did we do?

Use $\bar{\lambda}\mu\tilde{\mu}$ -calculus to provide a semantics for OMDOC + Alternatives (= PDS)

- Choose a fragment of $\bar{\lambda}\mu\tilde{\mu}$ -calculus as proof terms which is suitable to represent alternative proofs
- Defined **rendering semantics** $[\cdot]_{\bar{\lambda}\mu\tilde{\mu}}$ for $\bar{\lambda}\mu\tilde{\mu}$ -calculus fragment
- Defined OMDOC proofs with alternatives
- Defined **rendering semantics** $[\cdot]_O$ for OMDOC proofs
- Defined translation from $\bar{\lambda}\mu\tilde{\mu}$ to OMDOC
- and translation from OMDOC to $\bar{\lambda}\mu\tilde{\mu}$
- Such that
 1. $\text{OmdocTo}\bar{\lambda}\mu\tilde{\mu}$ and $\bar{\lambda}\mu\tilde{\mu}\text{ToOmdoc}$ are inverse functions (almost!)

What did we do?

Use $\bar{\lambda}\mu\tilde{\mu}$ -calculus to provide a semantics for OMDOC + Alternatives (= PDS)

- Choose a fragment of $\bar{\lambda}\mu\tilde{\mu}$ -calculus as proof terms which is suitable to represent alternative proofs
- Defined **rendering semantics** $\llbracket \cdot \rrbracket_{\bar{\lambda}\mu\tilde{\mu}}$ for $\bar{\lambda}\mu\tilde{\mu}$ -calculus fragment
- Defined OMDOC proofs with alternatives
- Defined **rendering semantics** $\llbracket \cdot \rrbracket_O$ for OMDOC proofs
- Defined translation from $\bar{\lambda}\mu\tilde{\mu}$ to OMDOC
- and translation from OMDOC to $\bar{\lambda}\mu\tilde{\mu}$
- Such that
 1. $\text{OmdocTo}\bar{\lambda}\mu\tilde{\mu}$ and $\bar{\lambda}\mu\tilde{\mu}\text{ToOmdoc}$ are inverse functions (almost!)
 2. $\llbracket \text{OMDOC-Proof} \rrbracket_O$ and $\llbracket \text{OmdocTo}\bar{\lambda}\mu\tilde{\mu}(\text{OMDOC-Proof}) \rrbracket_{\bar{\lambda}\mu\tilde{\mu}}$ have the same informative content.

$\bar{\lambda}\mu\tilde{\mu}$ -Fragment Used to Encode Proofs with Alternatives

$\bar{\lambda}\mu\tilde{\mu}$ -Calculus



Commands

$c ::= \langle v || E \rangle$

Terms

$v ::= x$
| $\lambda x : T.v$
| $\mu\alpha : T.c$

Environments

$E ::= \alpha$
| $v \circ E$
| $\tilde{\mu}x : T.c$

- “Intuitionistic” fragment = allow exactly one continuation variable \star
- Otherwise “classical” fragment
- Intuitionistic fragment Curry-Howard to Gentzen LJ sequent calculus
- Classical fragment Curry-Howard to Gentzen LK sequent calculus

Properties



Reduction rules:

$$\langle \mu\alpha : T.c \mid E \rangle \triangleright c\{E/\alpha\}$$

$$\langle v \mid \tilde{\mu}x : T.c \rangle \triangleright c\{v/x\}$$

$$\langle \lambda x : T.v_1 \mid v_2 \circ E \rangle \triangleright \langle v_2 \mid \tilde{\mu}x : T.v_1 \circ E \rangle$$

η -like rules:

$$\mu\text{-expansion: } v \Rightarrow \mu\alpha : T.\langle v \mid \alpha \rangle$$

$$\tilde{\mu}\text{-expansion: } E \Rightarrow \tilde{\mu}x : T.\langle x \mid E \rangle$$

- First two reduction rules may form a critical pair (call-by-value vs. call-by-name)
- Comparing the fragments

Fragment	Deterministic?	Rendering natural?
Intuitionistic	Yes	Yes
Classical	No	No

Encoding Alternatives in $\bar{\lambda}\mu\tilde{\mu}$



- A proof with alternatives must non-deterministically reduce to either alternative proof.

Encoding Alternatives in $\bar{\lambda}\mu\tilde{\mu}$

- A proof with alternatives must non-deterministically reduce to either alternative proof.
- Encode alternative proof as critical pair

$$\mathit{alt}_r^T(t_1, t_2) := \mu\star : T.\langle \mu_- : T.\langle t_1 || \star \rangle || \tilde{\mu}_- : T.\langle t_2 || \star \rangle \rangle$$

Encoding Alternatives in $\bar{\lambda}\mu\tilde{\mu}$

- A proof with alternatives must non-deterministically reduce to either alternative proof.
- Encode alternative proof as critical pair

$$\boxed{alt_r^T(t_1, t_2) := \mu\star : T.\langle \mu_- : T.\langle t_1 || \star \rangle || \tilde{\mu}_- : T.\langle t_2 || \star \rangle \rangle}$$

- A proof with alternatives lives in the classical fragment

Encoding Alternatives in $\bar{\lambda}\mu\tilde{\mu}$

- A proof with alternatives must non-deterministically reduce to either alternative proof.
- Encode alternative proof as critical pair

$$\boxed{alt_r^T(t_1, t_2) := \mu\star : T.\langle \mu_- : T.\langle t_1 || \star \rangle || \tilde{\mu}_- : T.\langle t_2 || \star \rangle \rangle}$$

- A proof with alternatives lives in the classical fragment
- A view is obtained by deciding on how to reduce the critical pairs

$$alt_r^T(t_1, t_2) \triangleright \mu\star : T.\langle t_1 || \star \rangle \quad (\equiv_{\mu-Exp} t_1)$$

$$alt_r^T(t_1, t_2) \triangleright \mu\star : T.\langle t_2 || \star \rangle \quad (\equiv_{\mu-Exp} t_2)$$

Encoding Alternatives in $\bar{\lambda}\mu\tilde{\mu}$

- A proof with alternatives must non-deterministically reduce to either alternative proof.
- Encode alternative proof as critical pair

$$\boxed{alt_r^T(t_1, t_2) := \mu\star : T.\langle \mu_- : T.\langle t_1 || \star \rangle || \tilde{\mu}_- : T.\langle t_2 || \star \rangle \rangle}$$

- A proof with alternatives lives in the classical fragment
- A view is obtained by deciding on how to reduce the critical pairs

$$alt_r^T(t_1, t_2) \triangleright \mu\star : T.\langle t_1 || \star \rangle \quad (\equiv_{\mu-Exp} t_1)$$

$$alt_r^T(t_1, t_2) \triangleright \mu\star : T.\langle t_2 || \star \rangle \quad (\equiv_{\mu-Exp} t_2)$$

- A view is a proof term in the intuitionistic fragment

Used Fragment of $\bar{\lambda}\mu\tilde{\mu}$ -Calculus

- We used $\mu_- : T.c$ and $\tilde{\mu}_- : T.c$ to denote that the bound continuation/variable does not occur in c (Affine Binders)
- Intuitionistic Fragment \subset Used-Fragment
 \subset Affine Fragment \subset Classical Fragment
- Intuitionistic Fragment: μ binds only the single \star
- Affine Fragment: Any μ either binds only the single \star or is *affine*
- Affine binders can only occur in two positions:
 - ▶ First subterm of a command:
 $\langle \lambda x_1 : T_1 \dots \lambda x_n : T_n. \mu_- : T.c \mid \mid E \rangle$ (Spine position)
 - ▶ First subterm of a “cons” environment:
 $\lambda x_1 : T_1 \dots \lambda x_n : T_n. \mu_- : T.c \circ E$ (Argument position)

$\overline{\lambda\mu\tilde{\mu}}$ -Fragment: Rendering Semantics



Commands

$c ::= \langle v' || E \rangle \quad \llbracket v' \rrbracket \llbracket E \rrbracket$
 | $\langle \mu_- : T.c_1$
 $|| \tilde{\mu}_- : T.c_2 \rangle$ we provide two alternative proofs
 first proof: $\boxed{\hookrightarrow}$
 $\llbracket c_1 \rrbracket$
 alternative proof: $\boxed{\hookrightarrow}$
 $\llbracket c_2 \rrbracket$

Environments

$E ::= \star \quad \boxed{\leftarrow}$ done
 | $\tilde{\mu}x : T.c$ we proved $T(x)$
 $\llbracket c \rrbracket$
 | $a \circ E$ and $\llbracket a \rrbracket$
 $\llbracket E \rrbracket$

SpineTerms

$v' ::= x$ by x
 | $?$ by a conjecture
 | v **if** $v = \mu\star : T.\langle v' || \tilde{\mu}x : T.\langle x || \star \rangle \rangle$ **then**
 by x (that proves T as follows $\boxed{\hookrightarrow}$
 $\llbracket \langle v || \star \rangle \rrbracket$
else
 by some proof (in detail $\boxed{\hookrightarrow}$
 $\llbracket \langle v || \star \rangle \rrbracket$

Terms

$v ::= \lambda x : T.v$ suppose $T(x)$
 $\llbracket v \rrbracket$
 | $\mu\star : T.c$ we need to prove T
 $\boxed{\hookrightarrow} \llbracket c \rrbracket$

$\overline{\lambda\mu\tilde{\mu}}$ -Fragment:

Rendering Semantics



Commands

$c ::= \langle v' || E \rangle \quad \llbracket v' \rrbracket \llbracket E \rrbracket$
| $\langle \mu_- : T.c_1$
| $|| \tilde{\mu}_- : T.c_2 \rangle$ we provide two alternative proofs

first proof: $\boxed{\hookrightarrow}$

$\llbracket c_1 \rrbracket$

alternative proof: $\boxed{\hookrightarrow}$

$\llbracket c_2 \rrbracket$

Environments

$E ::= \star \quad \boxed{\leftarrow}$ done
| $\tilde{\mu}x : T.c$ we proved $T(x)$
 $\llbracket c \rrbracket$
| $a \circ E$ and $\llbracket a \rrbracket$
 $\llbracket E \rrbracket$

Arguments

$a ::= x$ by x
| a' $\llbracket a' \rrbracket$

Complex Arguments

$a' ::= \mu\star : T.c$ a proof of T $\boxed{\hookrightarrow}$
 $\llbracket c \rrbracket$
| $\lambda x : T.a'$ under hypothesis $T(x)$
 $\llbracket a' \rrbracket$



OMDOC Proofs with Alternatives

Abstract OMDOC



$PROOF ::= \text{hyp } L:F;PROOF$
| $\text{alt}(PROOF_1 \mid PROOF_2)$
| $\text{derive } L : F JUST;PROOF$
| $\text{derive } _ : F JUST$

$JUST ::= \text{method } M(ARG_1 \dots ARG_n) OPTEXP$
| $\text{plan}(ARG_1 \dots ARG_n) (F PROOF)$
| $\text{sketch}(ARG_1 \dots ARG_n)$

$OPTEXP ::= \text{nil} \mid (F PROOF)$

$ARG ::= L \mid (F PROOF)$

- Added construct for **alternatives**
- Only consider hypothesis and derivation steps that have **exactly one** formal formula (FMP)
- No local declarations and definitions (for sake of simplicity)
- Derived formula in final proof step has no label

Abstract OMDOC



$PROOF$	$:=$	hyp $L:F;PROOF$	$JUST$	$:=$	method $M(ARG_1 \dots ARG_n)$ $OPTEXP$
		alt($PROOF_1$ $PROOF_2$)			plan($ARG_1 \dots ARG_n$) $(F PROOF)$
		derive $L : F JUST;PROOF$			sketch($ARG_1 \dots ARG_n$)
		derive $_ : F JUST$	$OPTEXP$	$:=$	nil $(F PROOF)$
			ARG	$:=$	L $(F PROOF)$

■ Justifications:

- ▶ Method: reference to a used method
- ▶ Plan: description of a subproof
- ▶ Sketch: Wiedijk's "proof sketches", "Gap" steps in OMDOC terminology

■ Arguments: Either a label (of a premise) or a fact with its proof

top-down proof step = at least one fact with proof

bottom-up proof step = only labels (only premises are used)

Rendering Semantics for OMDOC

$\llbracket \text{hyp } L:F, \text{PROOF} \rrbracket := \text{“Assume } F(L) \llbracket \text{PROOF} \rrbracket \text{”}$

$\llbracket \text{derive } L : F \text{ method } M(\text{ARG}_1, \dots, \text{ARG}_k) \text{ OPTEXP; PROOF} \rrbracket$
 $:= \text{“By } M \llbracket (\text{ARG}_1, \dots, \text{ARG}_k) \rrbracket^{al} \llbracket \text{OPTEXP} \rrbracket^o \text{ we prove } F(L); \llbracket \text{PROOF} \rrbracket \text{”}$

$\llbracket \text{derive } L : F \text{ plan}(\text{ARG}_1, \dots, \text{ARG}_k) (F' \text{ PROOF}); \text{PROOF} \rrbracket$
 $:= \text{“We prove } F(L) \llbracket (\text{ARG}_1, \dots, \text{ARG}_k) \rrbracket^{al} \llbracket (F' \text{ PROOF}) \rrbracket^o; \llbracket \text{PROOF} \rrbracket \text{”}$

$\llbracket \text{derive } L : F \text{ sketch}(\text{ARG}_1, \dots, \text{ARG}_k); \text{PROOF} \rrbracket$
 $:= \text{“We show } F(L) \llbracket (\text{ARG}_1, \dots, \text{ARG}_k) \rrbracket^{al}; \llbracket \text{PROOF} \rrbracket \text{”}$

$\llbracket \text{derive } _ : F \text{ method } M(\text{ARG}_1, \dots, \text{ARG}_k) \text{ OPTEXP} \rrbracket$
 $:= \text{“By } M \llbracket (\text{ARG}_1, \dots, \text{ARG}_k) \rrbracket^{al} \llbracket \text{OPTEXP} \rrbracket^o \text{ we proved } F; \boxed{\leftarrow} \text{”}$

$\llbracket \text{derive } _ : F \text{ plan}(\text{ARG}_1, \dots, \text{ARG}_k) \vdots (F' \text{ PROOF}) \ddots \rrbracket$
 $:= \text{“We proved } F \llbracket (\text{ARG}_1, \dots, \text{ARG}_k) \rrbracket^{al} \llbracket (F' \text{ PROOF}) \rrbracket^o; \boxed{\leftarrow} \text{”}$

$\llbracket \text{derive } _ : F \text{ sketch}(\text{ARG}_1, \dots, \text{ARG}_k) \rrbracket$
 $:= \text{“We can obtain } F \llbracket (\text{ARG}_1, \dots, \text{ARG}_k) \rrbracket^{al}; \boxed{\leftarrow} \text{”}$

$\llbracket \text{alt}(\text{PROOF}_1 \mid \text{PROOF}_2) \rrbracket := \text{“Either } \boxed{\hookrightarrow} \llbracket \text{PROOF}_1 \rrbracket$
 $\text{or } \boxed{\hookrightarrow} \llbracket \text{PROOF}_2 \rrbracket \text{”}$

$\llbracket () \rrbracket^{al} := \text{“”}$ $\llbracket (\text{ARG}_1, \dots, \text{ARG}_k) \rrbracket^{al} := \text{“from } \llbracket \text{ARG}_1 \rrbracket^a, \dots, \text{ and } \llbracket \text{ARG}_k \rrbracket^a \text{”}$

$\llbracket \text{nil} \rrbracket^o := \text{“”}$ $\llbracket (F \text{ PROOF}) \rrbracket^a := \text{“} F \text{ (proved by } \llbracket \text{PROOF} \rrbracket \text{)”}$

$\llbracket L \rrbracket^a := \text{“} L \text{”}$ $\llbracket \vdots (F \text{ PROOF}) \ddots \rrbracket^o := \text{“(Indetail : } \llbracket \text{PROOF} \rrbracket \text{)”}$



Translations

OMDOC to $\bar{\lambda}\mu\tilde{\mu}$ -Calculus



$$\llbracket \text{hyp } L:F; \text{PROOF} \rrbracket_{F \rightarrow F'}^t = \lambda L : F. \llbracket \text{PROOF} \rrbracket_{F'}^t$$

$$\llbracket \text{derive } _ : F \text{ JUST} \rrbracket_F^t = \mu \star : F. \langle \llbracket \text{JUST} \rrbracket_1^j \mid \llbracket \text{JUST} \rrbracket_2^j(\star) \rangle$$

$$\llbracket \text{derive } L:F \text{ JUST}; \text{PROOF} \rrbracket_{F'}^t = \mu \star : F'. \langle \llbracket \text{JUST} \rrbracket_1^j \mid \llbracket \text{JUST} \rrbracket_2^j(\tilde{\mu}L : F. \underline{\llbracket \text{PROOF} \rrbracket_{F'}^t} \mid \star) \rangle$$

$$\llbracket \text{alt}(\text{PROOF}_1 \mid \text{PROOF}_2) \rrbracket_F^t = \text{alt}_r^F(\llbracket \text{PROOF}_1 \rrbracket_F^t, \llbracket \text{PROOF}_2 \rrbracket_F^t)$$

$$\llbracket \text{sketch}(\text{ARG}_1 \dots \text{ARG}_n) \rrbracket_1^j = ?$$

$$\llbracket \text{sketch}(\text{ARG}_1 \dots \text{ARG}_n) \rrbracket_2^j(E) = \llbracket \text{ARG}_1 \rrbracket^a \circ \dots \circ \llbracket \text{ARG}_n \rrbracket^a \circ E$$

$$\llbracket \text{plan}(\text{ARG}_1 \dots \text{ARG}_n) \cdot (F \text{ PROOF}) \rrbracket_1^j = \llbracket \text{PROOF} \rrbracket_F^t$$

$$\llbracket \text{plan}(\text{ARG}_1 \dots \text{ARG}_n) \cdot (F \text{ PROOF}) \rrbracket_2^j(E) = \llbracket \text{ARG}_1 \rrbracket^a \circ \dots \circ \llbracket \text{ARG}_n \rrbracket^a \circ E$$

$$\llbracket \text{method } M(\text{ARG}_1 \dots \text{ARG}_n) \cdot (F \text{ PROOF}) \rrbracket_1^j = \mu \star : F. \langle \llbracket \text{PROOF} \rrbracket_F^t \mid \tilde{\mu}M : F. \langle M \mid \star \rangle \rangle$$

$$\llbracket \text{method } M(\text{ARG}_1 \dots \text{ARG}_n) \cdot (F \text{ PROOF}) \rrbracket_2^j(E) = \llbracket \text{ARG}_1 \rrbracket^a \circ \dots \circ \llbracket \text{ARG}_n \rrbracket^a \circ E$$

$$\llbracket \text{method } M(\text{ARG}_1 \dots \text{ARG}_n) \text{ nil} \rrbracket_1^j = M$$

$$\llbracket \text{method } M(\text{ARG}_1 \dots \text{ARG}_n) \text{ nil} \rrbracket_2^j(E) = \llbracket \text{ARG}_1 \rrbracket^a \circ \dots \circ \llbracket \text{ARG}_n \rrbracket^a \circ E$$

$$\llbracket L \rrbracket^a = L$$

$$\llbracket (F \text{ PROOF}) \rrbracket^a = \llbracket \text{PROOF} \rrbracket_F^t$$

OMDOC to $\bar{\lambda}\mu\tilde{\mu}$ -Calculus



$$\llbracket \text{hyp } L:F; \text{PROOF} \rrbracket_{F \rightarrow F'}^t = \lambda L : F. \llbracket \text{PROOF} \rrbracket_{F'}^t$$

$$\llbracket \text{derive } _ : F \text{ JUST} \rrbracket_F^t = \mu \star : F. \langle \llbracket \text{JUST} \rrbracket_1^j \mid \llbracket \text{JUST} \rrbracket_2^j(\star) \rangle$$

$$\llbracket \text{derive } L:F \text{ JUST}; \text{PROOF} \rrbracket_{F'}^t = \mu \star : F'. \langle \llbracket \text{JUST} \rrbracket_1^j \mid \llbracket \text{JUST} \rrbracket_2^j(\tilde{\mu}L : F. \underline{\llbracket \text{PROOF} \rrbracket_{F'}^t} \mid \star) \rangle$$

$$\llbracket \text{alt}(\text{PROOF}_1 \mid \text{PROOF}_2) \rrbracket_F^t = \text{alt}_r^F(\llbracket \text{PROOF}_1 \rrbracket_F^t, \llbracket \text{PROOF}_2 \rrbracket_F^t)$$

$$\llbracket \text{sketch}(\text{ARG}_1 \dots \text{ARG}_n) \rrbracket_1^j = ?$$

$$\llbracket \text{sketch}(\text{ARG}_1 \dots \text{ARG}_n) \rrbracket_2^j(E) = \llbracket \text{ARG}_1 \rrbracket^a \circ \dots \circ \llbracket \text{ARG}_n \rrbracket^a \circ E$$

$$\llbracket \text{plan}(\text{ARG}_1 \dots \text{ARG}_n) \text{ (F PROOF)} \rrbracket_1^j = \llbracket \text{PROOF} \rrbracket_F^t$$

$$\llbracket \text{plan}(\text{ARG}_1 \dots \text{ARG}_n) \text{ (F PROOF)} \rrbracket_2^j(E) = \llbracket \text{ARG}_1 \rrbracket^a \circ \dots \circ \llbracket \text{ARG}_n \rrbracket^a \circ E$$

$$\llbracket \text{method } M(\text{ARG}_1 \dots \text{ARG}_n) \text{ (F PROOF)} \rrbracket_1^j = \mu \star : F. \langle \llbracket \text{PROOF} \rrbracket_F^t \mid \tilde{\mu}M : F. \langle M \mid \star \rangle \rangle$$

$$\llbracket \text{method } M(\text{ARG}_1 \dots \text{ARG}_n) \text{ (F PROOF)} \rrbracket_2^j(E) = \llbracket \text{ARG}_1 \rrbracket^a \circ \dots \circ \llbracket \text{ARG}_n \rrbracket^a \circ E$$

$$\llbracket \text{method } M(\text{ARG}_1 \dots \text{ARG}_n) \text{ nil} \rrbracket_1^j = M$$

$$\llbracket \text{method } M(\text{ARG}_1 \dots \text{ARG}_n) \text{ nil} \rrbracket_2^j(E) = \llbracket \text{ARG}_1 \rrbracket^a \circ \dots \circ \llbracket \text{ARG}_n \rrbracket^a \circ E$$

$$\llbracket L \rrbracket^a = L$$

$$\llbracket (\text{F PROOF}) \rrbracket^a = \llbracket \text{PROOF} \rrbracket_F^t$$

$\bar{\lambda}\mu\tilde{\mu}$ -Calculus to OMDOC



$$\llbracket \lambda x : T.v \rrbracket = \text{hyp } x : T; \llbracket v \rrbracket$$

$$\llbracket \mu\star : T.\langle v \mid v_1 \circ \dots \circ v_n \circ \star \rangle \rrbracket = \text{derive } _ : T \llbracket v \rrbracket^m (\llbracket v_1 \rrbracket^a, \dots, \llbracket v_n \rrbracket^a)$$

$$\llbracket \mu\star : T.\langle v \mid v_1 \circ \dots \circ v_n \circ \tilde{\mu}x : T'.c \rangle \rrbracket = \text{derive } x : T' \llbracket v \rrbracket^m (\llbracket v_1 \rrbracket^a, \dots, \llbracket v_n \rrbracket^a); \llbracket \mu\star : T.c \rrbracket$$

† $\llbracket x \rrbracket =$ ruled out

$$\llbracket alt_r^T(v_1, v_2) \rrbracket = \text{alt}(\llbracket v_1 \rrbracket \mid \llbracket v_2 \rrbracket)$$

$$\llbracket x \rrbracket^m(ARG_1, \dots, ARG_n) = \text{method } x(ARG_1 \dots ARG_n)$$

$$\llbracket ? \rrbracket^m(ARG_1, \dots, ARG_n) = \text{sketch}(ARG_1, \dots, ARG_n)$$

○ $\llbracket \mu\star : T.\langle v \mid \tilde{\mu}x : T.\langle x \mid \star \rangle \rangle \rrbracket^m(ARG_1, \dots, ARG_n) = \text{method } x(ARG_1 \dots ARG_n) \ddot{\llbracket v \rrbracket}$

$\llbracket v \rrbracket^m(ARG_1, \dots, ARG_n) = \text{plan}(ARG_1 \dots ARG_n) \ddot{\llbracket v \rrbracket}$ for $v \notin \{x, ?, \mu\star : T.\langle v \mid \tilde{\mu}x : T.\langle x \mid \star \rangle \}\}$

$$\llbracket x \rrbracket^a = x$$

$$\llbracket \mu\star : T.c \rrbracket^a = (T \llbracket \mu\star : T.c \rrbracket)$$

$$\llbracket alt_r^T(v_1, v_2) \rrbracket^a = (T \llbracket alt_r^T(v_1, v_2) \rrbracket)$$

$$\llbracket \lambda x_1 : T_1 \dots \lambda x_n : T_n. \mu\star : T.c \rrbracket^a = (T_1 \Rightarrow \dots \Rightarrow T_n \Rightarrow T \llbracket \lambda x_1 : T_1 \dots \lambda x_n : T_n. \mu\star : T.c \rrbracket)$$

$$\llbracket \lambda x_1 : T_1 \dots \lambda x_n : T_n. alt_r^T(v_1, v_2) \rrbracket^a = (T_1 \Rightarrow \dots \Rightarrow T_n \Rightarrow T \llbracket \lambda x_1 : T_1 \dots \lambda x_n : T_n. alt_r^T(v_1, v_2) \rrbracket)$$

† $\llbracket \lambda x_1 : T_1 \dots \lambda x_n : T_n. x \rrbracket^a =$ ruled out

○ Necessary to make the translation the inverse of the other

† Never used when applied on terms obtained from OMDOC



Example

Example Textbook Proof



Irrationality of $\sqrt{12}$

1. *The proof is by contradiction*
2. *We assume $\text{rat}(\sqrt{12})$;*
3. *We show there are n, m , such that*
$$\text{int}(n) \wedge \text{int}(m) \wedge \neg \text{commondiv}(n, m) \wedge \sqrt{12} = \frac{n}{m};$$
4. *By Lemma $\sqrt{z} = \frac{x}{y} \Rightarrow z \times y^2 = x^2$ we know $12 \times m^2 = n^2$;*
5. *We show $\text{commondiv}(n, m)$;*
6. *We have a contradiction.*

OMDOC Proof



derive $_ : \neg rat(\sqrt{12})$

method ProofByContradiction $((rat(\sqrt{12}) \Rightarrow \perp$

hyp $L_0 : rat(\sqrt{12})$;

derive $L_1 : int(n) \wedge int(m) \wedge \neg commondiv(n, m) \wedge \sqrt{12} = \frac{n}{m}$

plan(L_0) $(rat(\sqrt{12}) \Rightarrow int(n) \wedge int(m) \wedge \neg commondiv(n, m) \wedge \sqrt{12} = \frac{n}{m}$

hyp $L_{10} : rat(\sqrt{12})$; derive $L_{11} : \exists y:int, z:int. \sqrt{12} = \frac{y}{z} \wedge \neg commondiv(y, z)$

method ApplyLemma(Rat-Criterion, L_{10}) ;

derive $_ : int(n) \wedge int(m) \wedge \neg commondiv(n, m) \wedge \sqrt{12} = \frac{n}{m}$

method decomposition(L_{11}))

derive $L_2 : 12 \times m^2 = n^2$ method ApplyLemma($\sqrt{z} = \frac{x}{y} \Rightarrow z \times y^2 = x^2, L_1$) ;

derive $L_3 : commondiv(n, m)$

plan(L_2) $(12 \times m^2 = n^2 \Rightarrow commondiv(n, m)$

hyp $L_{30} : 12 \times m^2 = n^2$

alt (derive $L_{31} : div(n, 3) \wedge div(m, 3)$

method and-I ($div(n, 3) \dots$) ($div(m, 3) \dots$); ...

| derive $L_{34} : div(n, 2) \wedge div(m, 2)$

method and-I ($div(n, 2) \dots$) ($div(m, 2) \dots$); ...);

derive $_ : \perp$ method Contradiction(L_1, L_3))

$\bar{\lambda}\mu\tilde{\mu}$ -Proof obtained by Translation

$\mu\star : \neg rat\sqrt{12}$.

\langle ProofByContradiction

$\parallel \lambda L_0 : rat(\sqrt{12})$.

$\mu\star : \perp$. \langle $\mu\star : rat(\sqrt{12}) \Rightarrow int(n) \wedge int(m) \wedge \neg commondiv(n, m) \wedge \sqrt{12} = \frac{n}{m}$.

$\lambda L_{10} : rat(\sqrt{12})$.

\langle ApplyLemma \parallel

Rat-Criterion $\circ L_{10} \circ \tilde{\mu}L_{11} : \exists y:int, z:int. \sqrt{12} = \frac{y}{z} \wedge \neg commondiv(y, z)$.

\langle decomposition $\parallel L_{11} \circ \star \rangle$

$\parallel L_0 \circ \tilde{\mu}L_1 : int(n) \wedge int(m) \wedge \neg commondiv(n, m) \wedge \sqrt{12} = \frac{n}{m}$.

\langle ApplyLemma \parallel

$\llbracket \sqrt{z} = \frac{x}{y} \Rightarrow z \times y^2 = x^2 \rrbracket \circ L_1$

$\circ \tilde{\mu}L_2 : 12 \times m^2 = n^2$.

\langle $\lambda L_{30} : 12 \times m^2 = n^2$.

$alt_r(\mu\star : commondiv(n, m))$.

\langle and-I $\parallel \llbracket (div(n, 3) \dots) \rrbracket \circ \llbracket (div(m, 3) \dots) \rrbracket \circ$

$\tilde{\mu}L_{31} : div(n, 3) \wedge div(m, 3) \cdot \langle \llbracket \dots \rrbracket, \parallel \star \rangle \rangle$,

$\mu\star : commondiv(n, m)$.

\langle and-I $\parallel \llbracket (div(n, 2) \dots) \rrbracket \circ \llbracket (div(m, 2) \dots) \rrbracket \circ$

$\tilde{\mu}L_{34} : div(n, 2) \wedge div(m, 2) \cdot \langle \llbracket \dots \rrbracket, \parallel \star \rangle \rangle$

$\parallel L_2 \circ \tilde{\mu}L_3 : commondiv(n, m)$.

\langle Contradiction $\parallel L_1 \circ L_3 \circ \star \rangle \circ \star \rangle \rangle$

Rendered OMDOC Proof



Proof: *By ProofByContradiction from $\text{rat}(\sqrt{12}) \Rightarrow \perp$*

(proved by: Assume $\text{rat}(\sqrt{12})$ (L_0))

We prove $\text{int}(n) \wedge \text{int}(m) \wedge \neg \text{commondiv}(n, m) \wedge \sqrt{12} = \frac{n}{m}$ (L_1) from L_0

(In details: Assume $\text{rat}(\sqrt{12})$ (L_{10}) By ApplyLemma from Rat-Criterion and L_{10} we prove

$\exists y:\text{int}, z:\text{int}. \sqrt{12} = \frac{y}{z} \wedge \neg \text{commondiv}(y, z)$ (L_{11}))

By decomposition from L_{11} we proved

$\text{int}(n) \wedge \text{int}(m) \wedge \sqrt{12} = \frac{n}{m} \wedge \neg \text{commondiv}(n, m)$);

By ApplyLemma from $\sqrt{z} = \frac{x}{y} \Rightarrow z \times y^2 = x^2$ and L_1 we prove $12 \times m^2 = n^2$ (L_2);

We prove $\text{commondiv}(n, m)$ (L_3) from L_2

(In details:

Assume $12 \times m^2 = n^2$ (L_{30}))

Either by and-I from $\text{div}(n, 3)$ (proved by $[[\dots]]$) and $\text{div}(m, 3)$ (proved by $[[\dots]]$) we proved $\text{div}(n, 3) \wedge \text{div}(m, 3)$ (L_{31}); ...

Or by and-I from $\text{div}(n, 2)$ (proved by $[[\dots]]$) and $\text{div}(m, 2)$ (proved by $[[\dots]]$) we proved $\text{div}(n, 2) \wedge \text{div}(m, 2)$ (L_{34}); ...)

By Contradiction from L_1 and L_3 we proved \perp)

Rendered $\bar{\lambda}\mu\tilde{\mu}$ -Proof



Proof: we need to prove $\neg rat(\sqrt{12})$

by ProofByContradiction and the hypothesis $rat(\sqrt{12})$ (L_0) a proof of \perp

by some proof

(in detail: we need to prove $rat(\sqrt{12}) \Rightarrow int(n) \wedge int(m) \wedge$

$\neg commondiv(n, m) \wedge \sqrt{12} = \frac{n}{m}$: Suppose $rat(\sqrt{12})$ (L_{10}); By ApplyLemma and

Rat-Criterion and L_0 we proved $\exists y:int, z:int. \sqrt{12} = \frac{y}{z} \wedge \neg commondiv(y, z)$

(L_{11}). By decomposition and L_{11} . Done)

and L_0 we proved $int(n) \wedge int(m) \wedge \neg commondiv(n, m) \wedge \sqrt{12} = \frac{n}{m}$;

By ApplyLemma and $\sqrt{z} = \frac{x}{y} \Rightarrow z \times y^2 = x^2$ and L_1 we proved $12 \times m^2 = n^2$ (L_2);

By some proof

(in detail: Suppose $12 \times m^2 = n^2$ (L_{30}); we provide two alternative proofs:

First proof: we need to prove $commondiv(n, m)$: By and-I and

$\llbracket (div(n, 3) \dots) \rrbracket \llbracket (div(m, 3) \dots) \rrbracket$ we proved $div(n, 3) \wedge div(m, 3)$; $\llbracket \dots \rrbracket$ Done.

Second proof: we need to prove $commondiv(n, m)$: By and-I and $\llbracket (div(n, 2) \dots) \rrbracket$

$\llbracket (div(m, 2) \dots) \rrbracket$ we proved $div(n, 2) \wedge div(m, 2)$; $\llbracket \dots \rrbracket$ Done.)

and L_2 we have proved $commondiv(n, m)$ (L_3);

By Contradiction and L_1 and L_3 done.

Analysis



- Almost equivalent informative content in both natural language explanations
- Main differences are omission of repetitions of the thesis:
 1. in the two alternative proofs the local thesis is restated in the $\bar{\lambda}\mu\tilde{\mu}$ -calculus, but not in OMDoc; “we need to prove that . . .”
 2. at the end of the first expanded proof OMDoc states again what has been proved while the $\bar{\lambda}\mu\tilde{\mu}$ -calculus does not. “We proved . . .”
- Possible to work on renderings to obtain two syntactically closer texts
- But of limited interest:
 - ▶ We are already convinced that the informative content is equivalent
 - ▶ Neither of the two is really more readable or natural than the other.

Conclusions

- Pure classical fragment of the $\bar{\lambda}\mu\tilde{\mu}$ -calculus necessary (for alternative proofs, proofs at different level of granularity)
- Correspondence between OMDOC proofs and $\bar{\lambda}\mu\tilde{\mu}$ -calculus
- Clear understanding of OMDOC proofs (and hence PDS)
 - Enables studies of properties for OMDOC proofs (cut-elimination)
- Natural language rendering only used to check “adequacy” of translations (Real presentation of proofs in natural language is something else)
- Faced difficulties as guide to adjust/extend the OMDOC proof language (Future work)
 - ▶ We used already an extension that clarifies the role of proofs at different levels of granularity and adds alternative proofs
- Find properties of bigger $\bar{\lambda}\mu\tilde{\mu}$ -calculus fragments used as a proof format