(Versions of) Modal Type Theory

Giuseppe Primiero

Department of Computer Science
Middlesex University, London
www.cs.mdx.ac.uk/people/giuseppe-primiero/

Kent University

Variations on a Theme

- Monadic Versions
- Constructive Versions
- Judgemental Versions
- Categorical Versions
- Homotopical Versions

Variations on a Theme

- Monadic Versions
- Constructive Versions
- Judgemental Versions
- Categorical Versions
- Homotopical Versions

Monads and Modalities [Moggi, 1991, Benton et al., 1998, Kobayashi, 1997]

- distinction between computation and value
- a strong monad $T(A)$ models computations of value A
- a computation of type A is the *possibility* of a value of type A (e.g. non-termination)
- modalities are (co-)monads in the sub-universe of propositions
- special case: Grothendieck topology

Constructive Modal Logics [de Paiva et al., 2004]

- Existence of a Proof-Theory with computational content
- Modalities as syntactic reflections of the intensional level of proofs
- Calculi for semantics of programs
- (Typed) λ-Calculus / Curry-Howard / Natural-Deduction

Categories

- extended Curry-Howard relating categories to (Typed) λ-Calculus / logics
- Models of IS4 using simplicial sets and lower-dimensional topology [Goubault-Larrecq and Goubault, 2003]
- duality between topological spaces and frames
- generalisation of frames to categorical spans [Hermida, 2011]
- categories for CS4 [Alechina et al., 2001]

The Judgemental Reconstruction [Pfenning and Davies, 2001]

- Modal Logic grounded on the proposition/judgement distinction
- Based on different meaning explanations for $\Box$ and $\Diamond$
- Natural Deduction for Intuitionistic Modal Logic
- New formulation for the Lax logic [Fairtlough and Mendler, 1997] and monadic [Moggi, 1991] interpretations.

The Judgemental Schema

$$\underbrace{\overbrace{A}^{proposition} \quad \textit{is true}}_{judgement}$$

to know A *true* is to know what count as $a : A$

Introduction and Elimination

- For each judgement, an Introduction and an Elimination rule are given to define its meaning, e.g.

$$\frac{A \text{ true} \qquad B \text{ true}}{A \wedge B \text{ true}} \wedge\mathrm{I} \qquad \frac{A \wedge B \text{ true}}{A \text{ true}} \wedge\mathrm{E}_L$$

- *Local Soundness*: rules are not too strong
- *Local Completeness (a.k.a. local expansion)*: elimination rules can be applied to reconstruct the original judgement (e.g. for $\wedge$, both eliminations are needed)

Hypothetical Judgements: $J_1, \ldots, J_n \vdash J$

$$\frac{}{\Gamma, A\ true, \Gamma' \vdash A\ true}\ \text{hyp}$$

Categorical Judgements

Definition (Validity)

1. If $\cdot \vdash A\ \mathit{true}$ then $A\ \mathit{valid}$
2. If $A\ \mathit{valid}$ then $\Gamma \vdash A\ \mathit{true}$

$\Box$ as Validity

$$\frac{A\ \mathit{prop}}{\Box A\ \mathit{prop}}\ \Box\text{formation}$$

$$\frac{\Delta; \cdot \vdash A\ \mathit{true}}{\Delta; \Gamma \vdash \Box A\ \mathit{true}}\ \Box\ \mathrm{I}$$

$$\frac{\Delta; \Gamma \vdash \Box A\ \mathit{true} \qquad \Delta; A\ \mathit{valid}; \Gamma \vdash C\ \mathit{true}}{\Delta; \Gamma \vdash C\ \mathit{true}}\ \Box\ \mathrm{E}$$

$\Diamond$ as possible truth

$$\frac{A\ \mathit{prop}}{\Diamond A\ \mathit{prop}}\ \Diamond\text{formation}$$

$$\frac{\Delta; \Gamma \vdash A\ \mathit{poss}}{\Delta; \Gamma \vdash \Diamond A\ \mathit{true}}\ \Diamond\ \text{I} \qquad \frac{\Delta; \Gamma \vdash \Diamond A\ \mathit{true} \qquad \Delta; A\ \mathit{true} \vdash C\ \mathit{poss}}{\Delta; \Gamma \vdash C\ \mathit{poss}}\ \Diamond\ \text{E}$$

Meta-properties

- Substitution principles for truth and validity
- Substitution principles for *A true* and *A poss*
- Local Soundness and Completeness

The contextual interpretation [Nanevski et al., 2008]

- A *valid* means true in any world
- A *valid*$[\Psi]$ means A *true* in every world where the propositions $B_1, \ldots, B_n$ in Ψ are true
- valid assumptions can be similarly generalised
- applications to staged computation and meta-variables (based on values vs. computations)

Contextual Validity

$$\frac{\Delta; \Psi \vdash A \ \mathit{true}}{\Delta; \Gamma \vdash A \ \mathit{valid}[\Psi]}$$

$$\frac{(\Delta, u :: A \ \mathit{valid}[\Psi], \Delta'); \Gamma \vdash \Psi}{(\Delta, u :: A \ \mathit{valid}[\Psi], \Delta'); \Gamma \vdash A \ \mathit{true}} \ \text{ctxhyp}$$

Contextual Necessity

$$\frac{\Delta; \Psi \vdash A\ \mathit{true}}{\Delta; \Gamma \vdash [\Psi]A\ \mathit{true}}\ \Box\mathsf{I}$$

$$\frac{\Delta; \Gamma \vdash [\Psi]A\ \mathit{true} \qquad (\Delta, u :: A\ \mathit{valid}[\Psi]); \Gamma \vdash C\ \mathit{true}}{\Delta; \Gamma \vdash C\ \mathit{true}}\ \Box\mathsf{E}$$

Verification under open assumptions [Primiero, 2012]

$$A_1, \ldots, A_n \vdash A \; true$$

says that A is true, unless $A_1, \ldots, A_n$ are refuted (i.e. one does not have them proven, but holds them as such)

Type for categorically justified judgements

$$\frac{A \ type \qquad a : A}{A \ true} \quad \text{Truth Definition}$$

Standard constructors

$$\frac{a : A \qquad b : B}{(a, b) : A \wedge B \ \ true} \ I\wedge$$

$$\frac{A \wedge B \ \ true}{a : A} \ (l)E\wedge \qquad \frac{A \wedge B \ \ true}{b : B} \ (r)E\wedge$$

$$\frac{a : A}{l(a) : A \vee B \ \ true} \ \text{Left I}\vee \quad \frac{b : B}{r(b) : A \vee B \ \ true} \ \text{Right I}\vee$$

$$\frac{A \vee B \ \ true \qquad A \rightarrow C \ \ true \qquad B \rightarrow C \ \ true}{C \ \ true} \ \text{E}\vee$$

$$\frac{a : A \qquad A \ true \vdash b : B}{a(b) : A \rightarrow B \ \ true} \ I \rightarrow \qquad \frac{A \rightarrow B \ \ true \qquad a : A}{(a)b : B} \ E \rightarrow$$

Type_{inf} for refutable judgements

$$\frac{a : A}{\neg A \to \bot} \quad I\bot$$

$$\frac{\neg(A \to \bot)}{A\ type_{inf}} \quad \text{Informational Type formation}$$

$$\frac{A\ type_{inf} \qquad x : A}{A\ true^{*}} \quad \text{Hypothetical Truth Definition}$$

Non-standard Constructors

$$\frac{A\ type_{inf} \qquad x : A \vdash B\ type_{inf}}{x : A \vdash B\ true^*}$$

$$\frac{A\ type_{inf} \qquad x : A \vdash B\ true^*}{((x)b) : A \supset B\ true}\ \mathrm{I}\supset \qquad \frac{A \supset B\ true \qquad A\ type[x/a]}{B\ true}\ \mathrm{E}\supset$$

$$\frac{A\ type_{inf} \qquad x : A \vdash B\ type_{inf} \qquad a : A}{(x(b))(a) = b[a/x] : B\ type[a/x]} \quad \beta\text{-conversion}$$

Modalities

$$A\ \mathit{true} \Leftrightarrow \emptyset \vdash a : A$$

$$A\ \mathit{true} \Leftrightarrow \emptyset \vdash A\ \mathit{true} \Leftrightarrow \Box(A\ \mathit{true}).$$

$$A\ \mathit{true}^{*} \Leftrightarrow \Gamma \vdash A\ \mathit{true} \Leftrightarrow \Diamond(A\ \mathit{true})$$

Formation Rules

$$\frac{}{\Gamma, a : A, \Delta \vdash A\ true}\ \text{Premise Rule}$$

$$\frac{}{\Gamma, x : A, \Delta \vdash A\ true^*}\ \text{Hypothesis Rule}$$

$$\frac{a : A}{\Box(A\ true)}\ \Box\text{-Formation} \qquad \frac{x : A}{\Diamond(A\ true)}\ \Diamond\text{-Formation}$$

Judgemental Modalities

- $\Box(A\ true)$: A is true in any given epistemic state, independently from any refutable condition (either there are none, or all of them have been secured);

- $\Diamond(A\ true)$: A holds true only in some given epistemic states in which certain conditions are not refuted.

Contexts

Definition (Necessitation Context)

For any context Γ, $\Box\Gamma$ is given by $\bigcup\{\Box(A\ true) \mid \text{ for all } A \in \Gamma\}$.

Definition (Normal Context)

For any context Γ, $\Diamond\Gamma$ is given by
$\bigcup\{\circ(A\ true) \mid \circ = \{\Box, \Diamond\} \text{ and } \Diamond(A\ true) \text{ for at least one } A \in \Gamma\}$.

$\Box$ Intro and Elimination Rules

$$\frac{\Gamma \vdash A \ true}{\Box\Gamma \vdash \Box(A \ true)} \ \mathrm{I}\Box$$

$$\frac{\Box\Gamma \vdash \Box(A \ true) \qquad \Delta, a : A \vdash b : B}{\Gamma, \Delta \vdash B \ true} \ \mathrm{E}\Box$$

$\Diamond$ Intro and Elimination Rules

$$\frac{\Gamma, x : A \vdash B \;\; true^{*}}{\Box\Gamma, \Diamond(A \;\; true) \vdash \Diamond(B \;\; true)} \; \mathsf{I}\Diamond$$

$$\frac{\Gamma, \Delta \vdash A \;\; true^{*} \qquad \Box\Gamma, \Diamond(A \;\; true) \vdash \Diamond(B \;\; true)}{\Gamma, \Delta \vdash B \;\; true^{*}} \; \mathsf{E}\Diamond$$

Meta-properties

- Substitution on terms is satisfied for A *true* and A *true**
- Local soundness and completeness are provable
- Weakening, Contraction, Exchange

Extension to multi-modalities

- extension to indexed modalities for distributed data accessibility [Primiero, 2010]
- extension to multi-modalities
- interpretation for mobile code and values for error resolution [Primiero, 2016]

Modalities

- computation as a process: run_i
- output of the process: *exec*

Modalities

- computation as a process: run_i
- output of the process: $exec$

Definition (Contexts)

$$\Gamma_i := \{run_i(\alpha), \ldots, run_i(\nu) \mid x_1 : \alpha, \ldots, y_i : \nu\}$$
$$\Delta_i := \{exec(\alpha), \ldots, exec(\nu) \mid a_1 : \alpha, \ldots, n_i : \nu\}$$

Modalities

- computation as a process: run_i
- output of the process: $exec$

Definition (Contexts)

$$\Gamma_i := \{run_i(\alpha), \dots, run_i(\nu) \mid x_1 : \alpha, \dots, y_i : \nu\}$$
$$\Delta_i := \{exec(\alpha), \dots, exec(\nu) \mid a_1 : \alpha, \dots, n_i : \nu\}$$

$$exec(\alpha) \equiv run_i((\alpha \supset \bot) \supset \bot)$$

$$run_i(\alpha) \equiv exec((\alpha \rightarrow \bot) \rightarrow \bot)$$

A fragment of the rules

$$\frac{}{\Delta_i, a_i : \alpha \vdash \mathit{exec}(\alpha)}\ \text{Value}$$

$$\frac{\Delta_i, a_i : \alpha \vdash \mathit{exec}(\alpha)}{\Delta_i \vdash \mathit{access}@_i(a : \alpha)}\ @\text{I} \qquad \frac{\Delta_i; \Gamma_i \vdash \mathit{access}@_i(a : \alpha)}{\Delta_i; \Gamma_i, x_i : \alpha \vdash \mathit{run}_i(\alpha)}\ @\text{E}$$

$\Box$ as global portability

$$\frac{\Gamma_i, x_j : \alpha \vdash run_j(\alpha) \qquad \Box_i\Gamma, [x_j/a_j] : \alpha \vdash exec(\alpha)}{BROAD(\Box_{i\cup j}\Gamma, \alpha)} \text{ RPC1}$$

$$\frac{BROAD(\Box_{i\cup j}\Gamma, \alpha) \qquad \Box_i\Gamma \vdash access@_i(a:\alpha)}{\Box_i\Gamma, a_i : \alpha \vdash exec(\alpha)} \text{ PORT1}$$

$\Diamond$ as local portability

$$\frac{\Gamma_i, x_j : \alpha \vdash run_j(\alpha) \qquad \Diamond_i \Gamma \vdash run_j(\alpha)}{SEND(\Diamond_{i \cap j} \Gamma, \alpha)} \text{ RPC2}$$

$$\frac{SEND(\Diamond_{i \cap j} \Gamma, \alpha) \qquad \Diamond_i \Gamma \vdash run_j(\alpha)}{[\Diamond_i / \Box_i]\Gamma, [x_j / a_j] : \alpha \vdash exec(\alpha)} \text{ PORT2}$$

Failures: errors of resources access.

$$\frac{\Box_i\Gamma, t_j : \tau \vdash exec(\upsilon) \qquad BROAD(\Box_{i\cup j}\Gamma, \tau)}{\Box_i\Gamma, access@_j(t' : \tau') \vdash fail@_{i\cup j}(\upsilon) \quad (t' \neq t; \tau' \neq \tau)} \text{ FailPort1}$$

$$\frac{\Box_i\Gamma, access@_j(t' : \tau') \vdash fail@_{i\cup j}(\upsilon) \qquad \Box_i\Gamma, t_j : \tau \vdash exec(\tau)}{\Box_i\Gamma, [t'_j : \tau' / t_j : \tau] \vdash exec(\upsilon)} \text{ HFP1}$$

Failures: errors of location access.

$$\frac{\Box_i\Gamma; x_j : \tau \vdash run_{i\cap j}(\upsilon) \qquad SEND(\Diamond_{i\cap j}\Gamma, \tau)}{\Diamond_i\Gamma, access@_{k>j}(t:\tau) \vdash fail@_{i\cap j}(\upsilon)}\ \text{FailPort2}$$

$$\frac{\Diamond_i\Gamma, access@_{k>j}(t:\tau) \vdash fail@_{i\cap j}(\upsilon) \qquad \Diamond_i\Gamma, x_j : \tau \vdash run_{i\cap j}(\tau)}{\Diamond_i\Gamma, [t_k/x_j] : \tau \vdash run_{i\cap j}(\upsilon)}\ \text{HandleFP2}$$

Final Observations

- Modalities increase the expressive power of type systems
- Several applications to programming are possible; to linguistic? philosophy of math/physics?
- Further analyses of multi-modalities possible, several sets of bridging axioms
- Further work: verification in Coq, application to CloudHaskell

Thanks!
(More) Questions?

References I

Alechina, N., Mendler, M., de Paiva, V., and Ritter, E. (2001).
Categorical and Kripke Semantics for Constructive S4 Modal Logic.
In Fribourg, L., editor, *Computer Science Logic, 15th International Workshop, CSL 2001. 10th Annual Conference of the EACSL, Paris, France, September 10-13, 2001, Proceedings*, volume 2142 of *Lecture Notes in Computer Science*, pages 292–307. Springer.

Benton, P. N., Bierman, G. M., and de Paiva, V. (1998).
Computational Types from a Logical Perspective.
J. Funct. Program., 8(2):177–193.

de Paiva, V., Goré, R., and Mendler, M. (2004).
Editorial.
J. Log. Comput., 14(4):439–446.

References II

Fairtlough, M. and Mendler, M. (1997).
Propositional Lax Logic.
Inf. Comput., 137(1):1–33.

Goubault-Larrecq, J. and Goubault, É. (2003).
On the geometry of intuitionistic S4 proofs .
Homology, homotopy and applications, 5(2).

Hermida, C. (2011).
A categorical outlook on relational modalities and simulations.
Inf. Comput., 209(12):1505–1517.

Kobayashi, S. (1997).
Monad as Modality.
Theor. Comput. Sci., 175(1):29–74.

References III

Moggi, E. (1991).
Notions of Computation and Monads.
Inf. Comput., 93(1):55–92.

Nanevski, A., Pfenning, F., and Pientka, B. (2008).
Contextual modal type theory.
ACM Trans. Comput. Log., 9(3).

Pfenning, F. and Davies, R. (2001).
A judgmental reconstruction of modal logic.
Mathematical Structures in Computer Science, 11(4):511–540.

References IV

Primiero, G. (2010).
A Multi-Modal Dependent Type Theory for Representing Data Accessibility in a Network.
In Simpson, A., editor, *International Workshop on Proof Systems for Program Logics, PSPL 2010, Edinburgh, Scotland, UK, July 10, 2010*, volume 12 of *EPiC Series*, pages 17–22. EasyChair.

Primiero, G. (2012).
A contextual type theory with judgemental modalities for reasoning from open assumptions.
LOGIQUE ET ANALYSE, 220:579–600.

Primiero, G. (2016).
A Modal Type System for Error Handling.
Technical report, Middlesex University London.