Introspective Kripke models and normalisation-by-evaluation for the $\lambda^{\Box}$-calculus

Miëtek Bak[1]

Least Fixed Ltd, Cambridge, UK

Abstract

We consider the $\lambda^{\Box}$-calculus, an extension of the simply typed λ-calculus with a *type of quoted programs* that corresponds to the $\Box$ connective of the modal logic S4. We present a novel class of *introspective Kripke models,* constructed in continuation-passing style, and prove the syntax of the $\lambda^{\Box}$-calculus sound and complete with respect to these models. We fully formalise the arguments in Agda, a dependently typed total functional programming language based on intensional type theory. The composition of our soundness and completeness proofs is an Agda program that performs normalisation-by-evaluation for the $\lambda^{\Box}$-calculus.

Keywords: constructive logic, continuation-passing style, completeness, Curry-Howard correspondence, intensionality, intuitionistic logic, Kripke semantics, meta-programming, modal logic S4, normalisation-by-evaluation, quotation, self-interpretation, typed λ-calculus

1 Introduction

I'd like to have a total functional programming language that works like Lisp; that is, a language that allows programs to be quoted, inspected, and evaluated, in which types are propositions and programs are proofs. Some people have been using the modal logic S4 for similar purposes. I quickly found a reasonable λ-calculus based on S4, that is, the $\lambda^{\Box}$-calculus, and I set out to write an interpreter for it.

$$\frac{\Delta \ni A}{\Delta ; \Gamma \vdash A} \qquad \frac{\Delta ; \varnothing \vdash A}{\Delta ; \Gamma \vdash \Box A} \qquad \frac{\Delta ; \Gamma \vdash \Box A \quad \Delta, A ; \Gamma \vdash C}{\Delta ; \Gamma \vdash C}$$

It's well-known that if we prove a language sound and complete with respect to some class of models, then an interpreter falls out — as long as the proofs are constructive. Unfortunately, all I could find was classical proofs of completeness for S4, and so I decided to do the proofs myself.

[1] mietek@bak.io

This paper is electronically published in
Electronic Notes in Theoretical Computer Science
URL: www.elsevier.nl/locate/entcs

It's also well-known how to prove STLC sound and complete with respect to intuitionistic Kripke semantics. Since the $\lambda^{\Box}$-calculus is an extension of STLC, I thought it should be simple to extend intuitionistic Kripke semantics and obtain the desired proofs. Famous last words! Eventually, I realised that the interpretation of $\Box A$ should be a syntactically-justified interpretation of A; that is, a pair consisting of a derivation of A and an interpretation of A.

$$\Delta;\Gamma \Vdash \Box A \;=\; \forall\,\Delta' \supseteq \Delta, \Gamma' \supseteq \Gamma.\; \Delta';\Gamma' \;{}^{\mathsf{m}}{\Vdash}\; A$$

$$\Delta;\Gamma \;{}^{\mathsf{m}}{\Vdash}\; A \;=\; \Delta;\varnothing \vdash A \;\times\; \Delta;\Gamma \Vdash A$$

This puts the syntax in the semantics — peeks beneath the veil sooner than expected. We can still keep the abstraction of a Kripke semantics, as long as we can discard it when we need to. We define an *introspective Kripke model* as a tuple with a set of worlds, $\mathcal{W}$, and other things.

$$\mathfrak{M} \;=\; \langle\, \mathcal{W},\, \mathcal{V},\, -\!\geq\!-,\, \mathsf{id_a},\, -\circ_{\mathsf{a}}-,\, \mathsf{acc_v},\, \lfloor - \rfloor,\, \lfloor - \rfloor_{\mathsf{a}} \,\rangle$$

Now, we can try to write the interpretation of $\Box A$ using the model.

$$\mathfrak{M} \,|\, w \Vdash \Box A \;=\; \forall\, w' \geq w.\; \mathfrak{M} \,|\, w' \;{}^{\mathsf{m}}{\Vdash}\; A$$

$$\mathfrak{M} \,|\, w \;{}^{\mathsf{m}}{\Vdash}\; A \;=\; {}^{\mathsf{m}}\lfloor w \rfloor;\varnothing \vdash A \;\times\; \mathfrak{M} \,|\, w \Vdash A$$

However, adding this interpretation to intuitionistic Kripke semantics allows us to prove soundness, but not completeness. The problem with proving completeness with respect to the modified semantics is similar to the problem with proving completeness of full STLC, with disjunction and the empty type. Some people have already come up with a solution to that, which is a CPS transformation of the semantics.

$$\mathfrak{M} \,|\, w \Vdash \Box A \;=\; \forall\, w' \geq w.\; \mathfrak{M} \,|\, w' \;{}^{\mathsf{mk}}{\Vdash}\; A$$

$$\mathfrak{M} \,|\, w \;{}^{\mathsf{mk}}{\Vdash}\; A \;=\; {}^{\mathsf{m}}\lfloor w \rfloor;\varnothing \vdash A \;\times\; \mathfrak{M} \,|\, w \;{}^{\mathsf{k}}{\Vdash}\; A$$

$$\mathfrak{M} \,|\, w \;{}^{\mathsf{k}}{\Vdash}\; A \;=\; \forall\, C, w' \geq w.\; \frac{\forall\, w'' \geq w'.\; \dfrac{\mathfrak{M} \,|\, w'' \Vdash A}{\lfloor w'' \rfloor \vdash_{\mathsf{nm}} C}}{\lfloor w' \rfloor \vdash_{\mathsf{nm}} C}$$

It turns out that CPS transforming the modified semantics allows us to prove soundness and completeness, and so, to write an interpreter for the $\lambda^{\Box}$-calculus. I've done that now, and I think this interpreter can be used to decide $\beta\eta$-equivalence according to the following convertibility relation, but I haven't managed to prove this yet.

$$\Delta;\Gamma \vDash A \;=\; \forall\, \mathfrak{M}, w.\; \frac{\mathfrak{M} \,|\, w \;{}^{\mathsf{mk}}{\Vdash^{\star}}\; \Delta \quad \mathfrak{M} \,|\, w \;{}^{\mathsf{k}}{\Vdash^{\star}}\; \Gamma}{\mathfrak{M} \,|\, w \;{}^{\mathsf{k}}{\Vdash}\; A}$$

$$\uparrow\!- : \frac{\Delta;\Gamma \vdash A}{\Delta;\Gamma \vDash A} \qquad \downarrow\!- : \frac{\Delta;\Gamma \vDash A}{\Delta;\Gamma \vdash_{\mathsf{nm}} A}$$

To prove completeness, we need a canonical model. We first prove soundness and completeness with respect to this canonical model, and then use that to prove completeness proper.

$$\mathfrak{M}_{\mathsf{u}} = \langle\, \mathsf{Cx},\ (\Delta;\Gamma)\,x \mapsto \Delta;\Gamma \vdash_{\mathsf{nm}}{}^{\mathsf{tv}}\, x,\ -\!\supseteq^2\!-,\ \mathsf{id}^2_{\mathsf{e}},\ -\!\circ^2_{\mathsf{e}}\!-,\ \mathsf{ren}^2_{\mathsf{nm}},\ \mathsf{id},\ \mathsf{id}\,\rangle$$

$$\Uparrow_{\mathsf{u}} - : \frac{\Delta;\Gamma \vdash_{\mathsf{nt}} A}{\Delta;\Gamma\ {}^{\mathsf{k}}\!\Vdash A} \qquad \Downarrow_{\mathsf{u}} - : \frac{\Delta;\Gamma\ {}^{\mathsf{k}}\!\Vdash A}{\Delta;\Gamma \vdash_{\mathsf{nm}} A}$$

Acknowledgements

The author is deeply grateful to Andreas Abel, Guillaume Allais, Ahmad Salim Al-Sibahi, Roy Dyckhoff, Michael Gabbay, Paolo Giarrusso, Tom Jack, Roman Kireev, Jerzy Marcinkowski, Darryl McAdams, Conor McBride, Dominic Orchard, Maciej Piróg, Ida Szubert, Tarmo Uustalu, Andrea Vezzosi, and Tomasz Wierzbicki, for many fruitful discussions over the years.

Furthermore, the author thanks Sergei Artemov, Andrej Bauer, Jacques Carette, Danko Ilik, Alex Kavvos, Jon Sterling, the anonymous reviewers, and the participants of IMLA'17, for comments that helped improve this work.

Citations

Abel (2013) [1]. Alechina *et al.* (2001) [2]. Altenkirch (1993) [3]. Altenkirch, Hofmann, and Streicher (1995) [4]. Altenkirch and Reus (1999) [5]. Artemov (2001) [6]. Artemov and Bonelli (2007) [7]. Bauer (2016) [8]. Berger and Schwichtenberg (1991) [9]. Bierman and de Paiva (2000) [10]. Boolos (1994) [11]. Božić and Došen (1984) [12]. Brown and Palsberg (2016) [13]. Chapman (2009) [15]. C. Coquand (1993) [16]. C. Coquand (2002) [17]. T. Coquand and Dybjer (1997) [18]. Danvy (1996) [19]. Danvy, Keller, and Puech (2014) [20]. Davies and Pfenning (2001) [21]. de Bruijn (1972) [14]. Dybjer and Filinski (2002) [22]. Dyckhoff (2016) [23]. Ewald (1986) [24]. Fischer Servi (1984) [25]. Fitting (2005) [26]. Gabbay and Nanevski (2013) [27]. Girard *et al.* (1989) [28]. Gödel (1933) [29]. Iemhoff (2001) [30]. Ilik (2010) [31]. Ilik (2013) [32]. Joachimski and Matthes (2003) [33]. Kovacs (2017) [34]. Kripke (1965) [35]. Lindley (2005) [36]. Martin-Löf (1975) [37]. McBride (2005) [38]. McCarthy *et al.* (1962) [39]. McKinsey and Tarski (1948) [40]. Meyer and Wand (1985) [41]. Mkrtychev (1997) [42]. Nanevski (2002) [43]. Nanevski (2004) [44]. Nanevski, Pfenning, and Pientka (2008) [45]. Norell (2007) [46]. Ono (1977) [47]. Pfenning and Davies (2001) [48]. Pientka and Abel (2015) [49]. Plotkin and Stirling (1986) [50]. Sheard (2001) [51]. Simpson (1994) [52]. Stump (2016) [53]. Turner (2004) [54]. Wadler (2015) [55]. Wickline, Lee, and Pfenning (1998) [56]. Wijesekera (1990) [57].

References

[1] Abel, A., "Normalization by evaluation: dependent types and impredicativity," Habilitation thesis, Ludwig-Maximilians-Universität München (2013).
http://www.cse.chalmers.se/~abela/habil.pdf

[2] Alechina, N., M. Mendler, V. de Paiva and E. Ritter, *Categorical and Kripke semantics for constructive S4 modal logic*, in: *Computer Science Logic (CSL'01)*, LNCS **2142** (2001), pp. 292–307.
http://doi.org/10.1007/3-540-44802-0_21

[3] Altenkirch, T., *Proving strong normalization of CC by modifying realizability semantics*, in: *Types for Proofs and Programs (TYPES'93)*, LNCS **806** (1993), pp. 3–18.
http://doi.org/10.1007/3-540-58085-9_70

[4] Altenkirch, T., M. Hofmann and T. Streicher, *Categorical reconstruction of a reduction free normalization proof*, in: *Category Theory and Computer Science (CTCS'95)*, (LNCS) **953** (1995), pp. 182–199.
http://doi.org/10.1007/3-540-60164-3_27

[5] Altenkirch, T. and B. Reus, *Monadic presentations of lambda terms using generalized inductive types*, in: *Computer Science Logic (CSL'99)*, LNCS **1683** (1999), pp. 453–468.
http://doi.org/10.1007/3-540-48168-0_32

[6] Artemov, S. N., *Explicit provability and constructive semantics*, Bulletin of Symbolic Logic **7** (2001), pp. 1–36.
http://doi.org/10.2307/2687821

[7] Artemov, S. N. and E. Bonelli, *The intensional lambda calculus*, in: *Logical Foundations of Computer Science (LFCS'07)*, LNCS **4514** (2007), pp. 12–25.
http://doi.org/10.1007/978-3-540-72734-7_2

[8] Bauer, A., *On self-interpreters for Gödel's System T*, in: *Types for Proofs and Programs (TYPES'16)*, 2016, accepted.
http://math.andrej.com/wp-content/uploads/2016/01/self-interpreter-for-T.pdf

[9] Berger, U. and H. Schwichtenberg, *An inverse of the evaluation functional for typed lambda-calculus*, in: *Logic in Computer Science (LICS'91)* (1991), pp. 203–211.
http://doi.org/10.1109/LICS.1991.151645

[10] Bierman, G. M. and V. de Paiva, *On an intuitionistic modal logic*, Studia Logica **65** (2000), pp. 383–416.
http://doi.org/10.1023/A:1005291931660

[11] Boolos, G., *An S4-preserving proof-theoretical treatment of modality*, in: *The Logic of Provability*, Cambridge University Press, 1994 pp. 155–164.
http://doi.org/10.1017/CBO9780511625183.014

[12] Božić, M. and K. Došen, *Models for normal intuitionistic modal logics*, Studia Logica **43** (1984), pp. 217–245.
http://doi.org/10.1007/BF02429840

[13] Brown, M. and J. Palsberg, *Breaking through the normalization barrier: a self-interpreter for F-omega*, in: *Principles of Programming Languages (POPL'16)* (2016), pp. 5–17.
http://doi.org/10.1145/2837614.2837623

[14] de Bruijn, N. G., *Lambda calculus notation with nameless dummies, a tool for automatic formula manipulation, with application to the Church-Rosser theorem*, Indagationes Mathematicae (Proceedings) **75** (1972), pp. 381–392.
http://doi.org/10.1016/1385-7258(72)90034-0

[15] Chapman, J. M., "Type checking and normalisation," Ph.D. thesis, University of Nottingham (2009).
http://jmchapman.github.io/papers/thesis.pdf

[16] Coquand, C., *From semantics to rules: a machine assisted analysis*, in: *Computer Science Logic (CSL'93)*, LNCS **832** (1993), pp. 91–105.
http://doi.org/10.1007/BFb0049326

[17] Coquand, C., *A formalised proof of the soundness and completeness of a simply typed lambda-calculus with explicit substitutions*, Higher-Order and Symbolic Computation **15** (2002), pp. 57–90.
http://doi.org/10.1023/A:1019964114625

[18] Coquand, T. and P. Dybjer, *Intuitionistic model constructions and normalization proofs*, Mathematical Structures in Computer Science **7** (1997), pp. 75–94.
http://doi.org/10.1017/S0960129596002150

[19] Danvy, O., *Type-directed partial evaluation*, in: *Principles of Programming Languages (POPL'96)* (1996), pp. 242–257.
http://doi.org/10.1145/237721.237784

[20] Danvy, O., C. Keller and M. Puech, *Typeful normalization by evaluation*, in: *Types for Proofs and Programs (TYPES'14)* (2014), pp. 72–88.
http://doi.org/10.4230/LIPIcs.TYPES.2014.72

[21] Davies, R. and F. Pfenning, *A modal analysis of staged computation*, Journal of the ACM **48** (2001), pp. 555–604.
http://doi.org/10.1145/382780.382785

[22] Dybjer, P. and A. Filinski, *Normalization and partial evaluation*, in: *Applied Semantics (APPSEM'00)*, LNCS **2395**, Springer, 2002 pp. 137–192.
http://doi.org/10.1007/3-540-45699-6_4

[23] Dyckhoff, R., *Some remarks on proof-theoretic semantics*, in: *Advances in Proof-Theoretic Semantics*, Trends in Logic **43**, Springer, 2016 pp. 79–93.
http://doi.org/10.1007/978-3-319-22686-6_5

[24] Ewald, W. B., *Intuitionistic tense and modal logic*, Journal of Symbolic Logic **51** (1986), pp. 166–179.
http://doi.org/10.2307/2273953

[25] Fischer Servi, G., *Axiomatizations for some intuitionistic modal logics*, Rendiconti del Seminario Matematico Università Politecnico di Torino **42** (1984), pp. 179–194, to appear online.
http://www.seminariomatematico.unito.it/rendiconti/cartaceo/42-3.html

[26] Fitting, M., *The logic of proofs, semantically*, Annals of Pure and Applied Logic **132** (2005), pp. 1–25.
http://doi.org/10.1016/j.apal.2004.04.009

[27] Gabbay, M. J. and A. Nanevski, *Denotation of contextual modal type theory: syntax and meta-programming*, Journal of Applied Logic **11** (2013), pp. 1–29.
http://doi.org/10.1016/j.jal.2012.07.002

[28] Girard, J.-Y., P. Taylor and Y. Lafont, "Proofs and Types," Cambridge University Press, 1989.
http://paultaylor.eu/stable/prot.pdf

[29] Gödel, K., *Eine Interpretation des intuitionistischen Aussagenkalküls*, in: *Kurt Gödel: Collected Works, Vol. I: Publications 1929–1936*, Oxford University Press, 1933/1986 pp. 300–303.
http://global.oup.com/academic/product/collected-works-9780195039641

[30] Iemhoff, R., "Provability logic and admissible rules," Ph.D. thesis, University of Amsterdam (2001).
http://phil.uu.nl/~iemhoff/Mijn/Papers/proeve.pdf

[31] Ilik, D., "Constructive completeness proofs and delimited control," Ph.D. thesis, École Polytechnique X (2010).
http://pastel.archives-ouvertes.fr/tel-00529021

[32] Ilik, D., *Continuation-passing style models complete for intuitionistic logic*, Annals of Pure and Applied Logic **164** (2013), pp. 651–662.
http://doi.org/10.1016/j.apal.2012.05.003

[33] Joachimski, F. and R. Matthes, *Short proofs of normalization for the simply-typed λ-calculus, permutative conversions and Gödel's T*, Archive for Mathematical Logic **42** (2003), pp. 59–87.
http://doi.org/10.1007/s00153-002-0156-9

[34] Kovács, A., "A machine-checked correctness proof of normalization by evaluation for simply typed lambda calculus," Master's thesis, Eötvös Loránd University (2017).
http://github.com/AndrasKovacs/stlc-nbe/blob/separate-PSh/thesis.pdf

[35] Kripke, S. A., *Semantical analysis of intuitionistic logic I*, Studies in Logic and the Foundations of Mathematics **40** (1965), pp. 92–130.
http://doi.org/10.1016/S0049-237X(08)71685-9

[36] Lindley, S., "Normalisation by evaluation in the compilation of typed functional programming languages," Ph.D. thesis, University of Edinburgh (2005).
http://www.era.lib.ed.ac.uk/handle/1842/778

[37] Martin-Löf, P., *An intuitionistic theory of types: predicative part*, Studies in Logic and the Foundations of Mathematics **80** (1975), pp. 73–118.
http://doi.org/10.1016/S0049-237X(08)71945-1

[38] McBride, C., *Epigram: practical programming with dependent types*, in: *Advanced Functional Programming (AFP'05)*, LNCS **832** (2005), pp. 91–105.
http://doi.org/10.1007/11546382_3

[39] McCarthy, J., P. W. Abrahams, D. J. Edwards, T. P. Hart and M. I. Levin, "LISP 1.5 Programmer's Manual," MIT Press, 1962.
http://softwarepreservation.org/projects/LISP/book/LISP%201.5%20Programmers%20Manual.pdf

[40] McKinsey, J. C. C. and A. Tarski, *Some theorems about the sentential calculi of Lewis and Heyting*, Journal of Symbolic Logic **13** (1948), pp. 1–15.
http://doi.org/10.2307/2268135

[41] Meyer, A. R. and M. Wand, *Continuation semantics in typed lambda-calculi*, in: *Logics of Programs (LP'85)*, LNCS **193**, Springer, 1985 pp. 219–224.
http://doi.org/10.1007/3-540-15648-8_17

[42] Mkrtychev, A., *Models for the logic of proofs*, in: *Logical Foundations of Computer Science (LFCS'97)*, LNCS **1234**, Springer, 1997 pp. 266–275.
http://doi.org/10.1007/3-540-63045-7_27

[43] Nanevski, A., *Meta-programming with names and necessity*, in: *International Conference on Functional Programming (ICFP'02)* (2002), pp. 206–217.
http://doi.org/10.1145/581478.581498

[44] Nanevski, A., "Functional programming with names and necessity," Ph.D. thesis, Carnegie Mellon University (2004).
https://software.imdea.org/~aleks/thesis/CMU-CS-04-151.pdf

[45] Nanevski, A., F. Pfenning and B. Pientka, *Contextual modal type theory*, ACM Transactions on Computational Logic **9** (2008), pp. 23:1–23:49.
http://doi.org/10.1145/1352582.1352591

[46] Norell, U., "Towards a practical programming language based on dependent type theory," Ph.D. thesis, Chalmers University of Technology (2007).
http://www.cse.chalmers.se/~ulfn/papers/thesis.pdf

[47] Ono, H., *On some intuitionistic modal logics*, Publications of the Research Institute for Mathematical Sciences **13** (1977), pp. 687–722.
http://doi.org/10.2977/prims/1195189604

[48] Pfenning, F. and R. Davies, *A judgmental reconstruction of modal logic*, Mathematical Structures in Computer Science **11** (2001), pp. 511–540.
http://doi.org/10.1017/S0960129501003322

[49] Pientka, B. and A. Abel, *Well-founded recursion over contextual objects*, in: *Typed Lambda Calculi and Applications (TLCA'15)*, 2015, pp. 273–287.
http://doi.org/10.4230/LIPIcs.TLCA.2015.273

[50] Plotkin, G. D. and C. Stirling, *A framework for intuitionistic modal logics*, in: *Theoretical Aspects of Reasoning about Knowledge (TARK'86)* (1986), pp. 399–406.
http://tark.org/proceedings/tark_mar19_86/p399-plotkin.pdf

[51] Sheard, T., *Accomplishments and research challenges in meta-programming*, in: *Semantics, Applications, and Implementation of Program Generation (SAIG'01)*, LNCS **2196**, Springer, 2001 pp. 2–44.
http://doi.org/10.1007/3-540-44806-3_2

[52] Simpson, A., "The proof theory and semantics of intuitionistic modal logic," Ph.D. thesis, University of Edinburgh (1994).
http://homepages.inf.ed.ac.uk/als/Research/thesis.pdf

[53] Stump, A., *Intuitionistic logic and Kripke semantics*, in: *Verified Functional Programming in Agda*, ACM and Morgan & Claypool, 2016 pp. 215–246.
http://doi.org/10.1145/2841316

[54] Turner, D. A., *Total functional programming*, Journal of Universal Computer Science **10** (2004), pp. 751–768.
http://doi.org/10.3217/jucs-010-07-0751

[55] Wadler, P., *Propositions as types*, Communications of the ACM **58** (2015), pp. 75–84.
http://doi.org/10.1145/2699407

[56] Wickline, P., P. Lee and F. Pfenning, *Run-time code generation and Modal-ML*, in: *Programming Language Design and Implementation (PLDI'98)* (1998), pp. 224–235.
http://doi.org/10.1145/277650.277727

[57] Wijesekera, D., *Constructive modal logics I*, Annals of Pure and Applied Logic **50** (1990), pp. 271–301.
http://doi.org/10.1016/0168-0072(90)90059-B