Extracting a formally verified Subtyping Algorithm for Intersection Types from Ideals and Filters

Jan Bessai[1], Andrej Dudenhefner[1], Boris Düdder[1], and Jakob Rehof[1]

Technical University of Dortmund, Dortmund, Germany
{jan.bessai, boris.duedder, andrej.dudenhefner, jakob.rehof}@cs.tu-dortmund.de

Abstract

The BCD type system of intersection types has been introduced by Barendregt, Coppo and Dezani in [1]. It is derived from a filter lambda model in order to characterize exactly the strongly normalizing terms. Formally, intersection types over variables $\alpha \in \mathbb{V}$

$$\sigma, \tau, \rho ::= \alpha \mid \sigma \to \tau \mid \sigma \cap \tau \mid \omega$$

are related by the least preorder $\leq$ closed under the rules

$$\sigma \leq \omega, \quad \omega \leq \omega \to \omega, \quad \sigma \cap \tau \leq \sigma, \quad \sigma \cap \tau \leq \tau, \quad \sigma \leq \sigma \cap \sigma;$$
$$(\sigma \to \tau) \cap (\sigma \to \rho) \leq \sigma \to \tau \cap \rho;$$
$$\text{If } \sigma \leq \sigma' \text{ and } \tau \leq \tau' \text{ then } \sigma \cap \tau \leq \sigma' \cap \tau' \text{ and } \sigma' \to \tau \leq \sigma \to \tau'.$$

Decidability of this preorder has been shown in [6, 4, 7, 8]. Laurent has formalized the relation in Coq in order to eliminate transitivity cuts from it [5]. Following the ideas presented in [8], we show how to obtain a formally verified subtyping algorithm in Coq. Focusing on the algebraic properties of filters and ideals on the subtype relation, we manage to avoid additional proof infrastructure (e.g. lists of types) and extensions to the core type theory of Coq. When executed inside Coq, the algorithm produces a subtype proof tree for an arbitrary pair of intersection types or a counter proof if the input pair is not subtype related.

Automatic program extraction allows to obtain Haskell and OCaml versions of the algorithm. Extracted code can be used as a reference for randomized testing of manually optimized implementations. We will report on an implemented but not yet machine verified subtype algorithm with $\mathcal{O}(n^2)$ asymptotic runtime behavior.

Proven properties allow to formally show the correspondence between prime ideals and the notion of paths in intersection types, which is mentioned in [9]. Organization into an intersection of paths is an important lemma in proofs for various decision problems, e.g. type inhabitation [3], type matching [2] and type inference [4]. We will demonstrate our implementation and made it publicly[1] available in the hope that it can serve as a platform for exploring formal verification and program extraction of algorithms based on intersection types.

References

[1] H. Barendregt, M. Coppo, and M. Dezani-Ciancaglini. A Filter Lambda Model and the Completeness of Type Assignment. *Journal of Symbolic Logic*, 48(4):931–940, 1983.

[2] Boris Düdder, Moritz Martens, and Jakob Rehof. Intersection Type Matching with Subtyping. In *Proceedings of TLCA'13*, volume 4(6) of *LNCS*. http://dx.doi.org/10.4230/DagRep.4.6.29, 2013.

[1] https://www.github.com/JanBessai/BCD

[3] Boris Düdder, Moritz Martens, Jakob Rehof, and Paweł Urzyczyn. Bounded Combinatory Logic. In *Proceedings of CSL'12*, volume 16 of *LIPIcs*, pages 243–258. Schloss Dagstuhl, 2012.

[4] T. Kurata and M. Takahashi. Decidable properties of intersection type systems. In *TLCA*, volume 902 of *LNCS*, pages 297–311. Springer, 1995.

[5] Olivier Laurent. Intersection types with subtyping by means of cut elimination. *Fundamenta Informaticae*, 121(1-4):203–226, 2012.

[6] Benjamin C Pierce. A decision procedure for the subtype relation on intersection types with bounded variables. Technical Report CMU-CS-89-1693, CMU, 1989.

[7] Jakob Rehof and Paweł Urzyczyn. Finite Combinatory Logic with Intersection Types. In *Proceedings of TLCA'11*, volume 6690 of *LNCS*, pages 169–183. Springer, 2011.

[8] Rick Statman. A Finite Model Property for Intersection Types. In Jakob Rehof, editor, *Proceedings Seventh Workshop on Intersection Types and Related Systems, ITRS 2014, Vienna, Austria, 18 July 2014.*, volume 177 of *EPTCS*, pages 1–9, 2015.

[9] Steffen Van Bakel, Franco Barbanera, Mariangiola Dezani-Ciancaglini, and Fer-Jan de Vries. Intersection types for λ-trees. *Theoretical Computer Science*, 272(1):3–40, 2002.