The Safe Lambda Calculus

William Blum
Linacre College

D.Phil. Thesis
Michaelmas Term 2008

Abstract

We consider a syntactic restriction for higher-order grammars called *safety* that constrains occurrences of variables in the production rules according to their type-theoretic order. We transpose and generalize this restriction to the setting of the simply-typed lambda calculus, giving rise to what we call the *safe lambda calculus*. We analyze its expressivity and obtain a result in the same vein as Schwichtenberg's 1976 characterization of the simply-typed lambda calculus: the numeric functions representable in the safe lambda calculus are exactly the multivariate polynomials; thus conditional is not definable. We also give a similar characterization for representable word functions. We then examine the complexity of deciding beta-eta equality of two safe simply-typed terms and show that this problem is PSPACE-hard. The safety restriction is then extended to other applied lambda calculi featuring recursion and references such as PCF and Idealized Algol (IA for short).

The next contribution concerns game semantics. We introduce a new concrete presentation of this semantics using the theory of *traversals*. It is shown that the *revealed game denotation* of a term can be computed by traversing some souped-up version of the term's abstract syntax tree using adequately defined traversal rules. Based on this presentation and via syntactic reasoning we obtain a game-semantic interpretation of safety: the strategy denotations of safe lambda-terms satisfy a property called *P-incremental justification* which says that the player's moves are always justified by the last pending opponent's move of greater order occurring in the player's view.

Next we look at models of the safe lambda calculus. We show that these are precisely captured by *Incremental Closed Categories*. A game model is constructed and is shown to be fully abstract for safe IA. Further, it is effectively presentable: two terms are equivalent just if they have the same set of complete *O-incrementally justified* plays—where O-incremental justification is defined as the dual of P-incremental justification.

Finally we study safety from the point of view of algorithmic game semantics. We observe that in the third-order fragment of IA, the addition of unsafe contexts is conservative for observational equivalence. This implies that all the upper complexity bounds known for the lower-order fragments of IA also hold for the safe fragment; we show that the lower-bounds remain the same as well. At order 4, observational equivalence is known to be undecidable for IA. We conjecture that for the order-4 *safe* fragment of IA, the problem is reducible to the DPDA-equivalence problem and is thus decidable.