The question of separation in Linear Logic

Lorenzo Tortora de Falco
Dipartimento di Filosofia
Università Roma III
tortora@uniroma3.it

Abstract

The discovery of the Curry-Howard correspondence (in the sixties) led to the "proofs-as-programs" paradigm: a proof is a program whose execution corresponds to perform cut-elimination. This approach allowed to rephrase the very old and basic question of equality of proofs as "how can we identify/distinguish proofs (or programs) computing the same function?" The most natural answer that I know is the following: "two proofs are different when (as computational processes) they interact differently with the other proofs". In other terms, two proofs are different when their difference shows up interactively. Roughly speaking, a logical system enjoys separation when the difference between every two syntactically different (cut-free) proofs shows up interactively.

The most well-known example of separation theorem is Böhm theorem (1968) for pure λ-calculus: if t, t' are two distinct closed $\beta\eta$-normal terms, then there exists a context $C[\ ]$ s.t. $C[t] \simeq_\beta 0$ and $C[t'] \simeq_\beta 1$. Another way of stating the theorem is to say that it is possible to define an order relation (i.e. a T_0 topology) on the $\beta\eta$-equivalence classes of (normalizable) λ-terms. Later on, this kind of question has been studied by Friedman and Statman for the simply typed λ-calculus, leading to what is often called "typed Böhm theorem".

Recently (so many years after Böhm theorem), there has been a renewal of interest in the question of separation, and of course this is not an accident: the lack of results was essentially due to the absence of interesting logical systems where proofs could be represented in a nice "canonical" way. Indeed, recall for example that (in a "proofs-as-programs" perspective) permutation of rules is the nightmare of Gentzen's sequent calculus LK. From this point of view, the only "nice" old logical system is natural deduction for minimal logic (i.e. the simply typed λ-calculus), for which the problem had been solved by Friedman and Statman's results.

The works on classical logic and on linear logic of the past 15 years have led to a much better way of representing proofs: the main point is that to separate $[\pi]$ and $[\pi']$ (where $[\pi]$ is the equivalence class of the proof π w.r.t. cut-elimination) is equivalent to separate π_0 and π'_0, where π_0 is *the canonical representative* of the equivalence class $[\pi]$. For example, in (some suitable fragment of) linear logic, π_0 will be the unique normal form of the proof-net π (after η-expansion): the separation problem is reduced to the same problem on the set of cut-free (and η-expanded) proof-nets. The existence of such canonical representatives is of course a tremendous improvement with respect to systems like -say- LK.

We'll discuss the question of separation for various fragments of linear logic, presenting some positive and some negative results.