How to Prove False using the Variable Convention*

Christian Urban

TU Munich (urbanc@in.tum.de)

Abstract. Bound variables play an important role in many branches of formal methods. Nearly all informal proofs involving bound variables make use of the variable convention. This poster shows by giving an example that this convention is in general an unsound reasoning principle, i.e. one can by using it prove false.

Summary of the Poster's Content

The variable convention is perhaps one of the most frequently used reasoning principles when reasoning about syntax involving binders. Barendregt formulates this convention in his classic book as follows:

> **Variable Convention:** If $M_1, \ldots, M_n$ occur in a certain mathematical context (e.g. definition, proof), then in these terms all bound variables are chosen to be different from the free variables.

However this convention is in general an unsound reasoning principle, which can be used to prove *false*. To see this, consider the following inductively defined two-place relation taking two α-equated lambda-terms as arguments:

$$\frac{}{x \mapsto x}\ \text{Var} \qquad \frac{}{t_1\, t_2 \mapsto t_1\, t_2}\ \text{App} \qquad \frac{t \mapsto t'}{\lambda x.t \mapsto t'}\ \text{Lam}$$

Note that the last rule reads "for all x, t and t', if $t \mapsto t'$ is in the relation, then so is $\lambda x.t \mapsto t'$". The following property can be "proved" using the variable convention.

Faulty Lemma: Suppose $t \mapsto t'$. If $y \notin FV(t)$ then $y \notin FV(t')$.

"Proof" By induction on the inductive relation. The Var- and App-cases boil down to straightforward implications.

In the Lam-case we have the induction hypothesis if $y \notin FV(t)$ then $y \notin FV(t')$ and the assumption $y \notin FV(\lambda x.t)$. The goal is to show $y \notin FV(t')$. We use the variable convention to infer that $y \neq x$ where x is the bound variable from $\lambda x.t$ and y is the free variable from the lemma. Using this fact, we know that $y \notin FV(\lambda x.t)$ holds if and only if $y \notin FV(t)$ holds. Hence we can use the induction hypothesis to conclude also this case.

Counter Example: We can easily verify that $\lambda x.x \mapsto x$ is in the relation and $x \notin FV(\lambda x.x)$ holds. But $x \notin FV(x)$ is clearly false.

Nominal Isabelle, a package for the theorem prover Isabelle, has enough infrastructure so that one can use the variable convention in *formal* proofs by structural and rule induction, but in the latter case only for relations that are *variable convention compatible*.

* This work arose from joint work with Michael Norrish, Stefan Berghofer and Randy Pollack.