

# Nominal Reasoning in the Theorem Prover Isabelle/HOL

## Topic: Logic, Mechanised Verification

Nominal Methods Group<sup>1</sup>  
Technical University Munich  
Munich, Germany

Christian Urban  
urbanc[at]in.tum.de

Nominal Logic was recently introduced by Prof. Andrew Pitts<sup>2</sup> to simplify mechanised verifications of programming language definitions. There issues about binders and  $\alpha$ -equivalence usually cause considerable difficulties. Our group has implemented the nominal logic framework of Pitts in the theorem prover Isabelle/HOL.<sup>3</sup> This theorem prover is one of the mainstream theorem provers (well over 100 users worldwide) and is mainly developed in Munich.

The proposed project involves formalising one result by Pitts<sup>4</sup> using our nominal datatype package. The result establishes which operations on names can co-exist with a programming language construct for name binding that enforces  $\alpha$ -equivalence via a type system. This work seems difficult to formalise using established techniques. So the main aim of this project is to give more evidence about the viability of the nominal logic work.

Knowledge about logic are essential; previous exposure to theorem provers (for example Coq) are of great advantage.

<sup>1</sup> <http://isabelle.in.tum.de/nominal/>

<sup>2</sup> <http://www.cl.cam.ac.uk/~amp12>

<sup>3</sup> <http://isabelle.in.tum.de>

<sup>4</sup> <http://www.cl.cam.ac.uk/~amp12/papers/genun/genun.pdf>

A previous internship in the nominal methods group was done by Christine Tasson from École Polytechnique. This project led to a refereed publication at the international conference CADE.

(<http://www4.in.tum.de/~urbanc/Publications/nom-cade-05.ps>)