CS-Note[*] 85

Andrew Ireland
February 4, 2005

NuSPADE goes to York: Trip Report

1 Introduction

On February 28th 2001, I visited the High Integrity Systems Engineering (HISE) research group within Computer Science at the University of York (Trip report 326). At that time I presented an overview of proof planning and outlined the aims of the NuSPADE project[1], which started in the summer of 2001. February 2nd, fours years on, I returned to York to present the results of the project and give a demo of NuSPADE. The feedback I received was very positive, what follows is a summary of the associated Q/A session:

Susan Stepney: The SHOLIS project [an industrial case study provided by Praxis] was previously verified, so it must have contained hand-crafted annotations ...

AI: That is correct, we turned off the hand-crafted annotations for the purposes of our experiment.

Susan Stepney: Did you compare the generated annotations with the hand-crafted annotations?

AI: Not in great detail, but they were essentially the same.

Ana Cavalcanti: What would be involved in applying NuSPADE to the problem of proving a different class of [SPARK] properties?

AI: It would potentially involve developing new proof methods and associated tactics. However, as we found with the exception freedom application, we were able to reuse some existing methods.

Alan Frisch: Your use of constraint solving was demonstrated for universally quantified goals. Is that always the case?

AI: It appears to be the case for this class of verification problems.

Steve King: Does your program analyser exploit annotations introduced by the programmer?

AI: No, it works only with the program code. If we did [exploit programmer annotations] we would have to check that the programmer's annotations were consistent with generated annotations. Typically programmers do not provide any proof annotations.

Jim Woodcock was very encouraging with regards to our participation at the IFIP Working Conference on the Program Verifier Challenge – to take place in October 2005 (Zurich). The Dependable Systems Evolution workshop that was planned to take place at ETAPS 2005 in Edinburgh has been delayed. It will now take place in July at FM 2005 in Newcastle.

[*]Notes in this series are for ϵ-baked ideas, for $1 \geq \epsilon \geq 0$. Only exceptionally should they be cited or distributed outwith the NuSPADE project (EPSRC GR/R24081).

[1]*Automatic Guidance for the Formal Verification of High Integrity Ada* EPSRC grant GR/R24081: `http://www.macs.hw.ac.uk/nuspade`