Maynooth University
National University of Ireland Maynooth

IRISH RESEARCH COUNCIL
An Chomhairle um Thaighde in Éirinn

An Analysis of Refinement Calculi

Marie Farrell

Principles of Programming Research Group, Department of Computer Science,

Maynooth University

Supervisors: Dr. Rosemary Monahan & Dr. James Power

mfarrell@cs.nuim.ie

Abstract:

The notion of systematically verifying a system at an abstract level and then to reuse the abstract proofs as the system stepwise evolves into a final product is a very attractive concept in software engineering. It allows the developer to make sure the system has no flaws at a very basic level before complexity is introduced. Since this complexity is introduced gradually we can prove correctness at each level of abstraction. This avoids the arduous task of trying to verify the completed system and then finding that there was a problem with some basic aspect thereof that would have been found promptly in an abstract specification. There are many tools that support refinement and they are often a primary choice when a developer decides to build a mission/safety critical system.

These tools are all built with some form of refinement calculus in mind. The theory and mathematics behind refinement calculi is of upmost importance when it comes to proving the correctness of a refined system. Refinement is typically carried out within a single formalism but it may be advantageous to have the ability to specify different parts of the system using refinement in various formalisms. The aim of this PhD is to provide a framework that will facilitate the sharing of proofs and refinements between formalisms. In line with this, a comprehensive study of refinement calculi has been carried out and this talk will provide an overview of the different theories with examples of refinement and bestow details of the mathematical structures at play and why we need them.