NUI MAYNOOTH

IRISH RESEARCH COUNCIL
An Chomhairle um Thaighde in Éirinn

A Logical Framework for

Integrating Software Models via Refinement

Marie Farrell mfarrell@cs.nuim.ie

Principles of Programming Research Group, Department of Computer Science,

National University of Ireland Maynooth

Supervisors: Dr. Rosemary Monahan & Dr. James Power

Abstract:

A software system is a model of a real-world entity or process, which must accurately represent relevant properties from the domain of application, as well as addressing concerns such as robustness, correctness and performance. Modern software development focuses on model-driven engineering: the construction, maintenance and integration of software models, ranging from formal design documents through to program code. Each model of a system represents different aspects of that system, and will often use its own modelling language, formalism and tools. Thus a central question in software development is how we can map between these different models while preserving their semantics and other relevant properties. In particular, we ask how we can correctly combine information from models which focus on different aspects of the software system, so that the software system as a whole can be modelled through their integration.

In software development it is common to model software at different levels of abstraction, starting with a very high level abstract specification and finishing with a detailed concrete implementation. In formal software engineering we can map between these levels of abstraction in a verifiable way through a process known as refinement. In contrast to the approach used in model-driven engineering, refinement typically happens within a single modelling language. The goal of this project is to fully integrate this process of formal refinement into the model-driven engineering approach so that models expressed in different modelling languages, formalisms and tools can be combined within one formal framework in a provable correct way. The resulting framework will support the sharing of refinement steps, and their associated proofs, between different modelling environments. The impact will be an improved software development process which allows the integration of software models, which focus on different aspects of the software, modelled at different levels of abstraction. The overall consequence will be the provision of a solid mathematical foundation for Model Driven Engineering.

This talk will focus on the Event B formal specification language, π-institutions and my progress to date