EXPERIENCES OF TEACHING FORMAL METHODS IN HIGHER EDUCATION

Zoltán Istenes
Eötvös Loránd University, Faculty of Informatics
Budapest, Hungary
istenes@inf.elte.hu

Abstract

Formal methods are mathematically-based techniques for the specification, development and verification of software and hardware systems. Through these formal methods, the systems reliability, robustness and safety can be verified and proved mathematically.

At the Formal Methods in Computer Science Education (FORMED 2008) workshop researchers and teachers have meet to discuss their experiences of teaching formal methods in higher education. This workshop revealed and clarified several interesting points; this paper only deals with the following ones. First of all, what are the main problems and advantages of teaching formal methods in the higher education curricula? What are the available and most adequate tools and modelling environments to use to teach formal methods in the higher education? What are the experiences of teaching formal methods and finally what methodologies to follow? This paper focuses mainly on the formal B-method.

Keywords
Formal methods, B-method, higher education, modelling, Rodin, Deploy

1. Introduction

Nowadays there is an increasing need of not only "big" but "secure" computer systems.

Due to the special need for safety critical, verified and proved systems, the use of new software technology methods started to become more widespread. Different possibilities exist for specifying, designing and coding software systems; one of them is the formal method. In formal methods, the syntax and semantics of a system description are described with mathematical tools. These methods also allow to model different computer software systems, to specify formally, to verify and to prove mathematically the model’s properties.

Due to the above mentioned reasons, in the present days, formal methods have increased their importance in both the industry and in the computer science curricula of higher education. In higher education, the task arises in choosing an appropriate formal method and finding its most opportune place in the curricula, taking in consideration both its underlying specification language and both its supporting software tools.

The use of formal methods requires and helps the development of rigorous and high-level abstraction skills, which are also the essential objectives of modern computing curricula. On one hand, these skills have a larger area of applicability, even beyond software engineering; on the other hand, the development of abstraction skills through formal methods is more challenging than the traditional education of programming.

The goal of this presentation is to introduce the formal methods, especially the B-method, its negative and positive sides, its tools and environments, to finally present and share the different experiences of teaching formal methods in higher education.
2. The use of formal methods in the higher education

2.1. Problems of teaching formal methods in the higher education

Even thought, there exist several large scale industrial applications of formal methods (see later in section 3.1.), in the higher education, during the lectures and practical works, only relatively small (“toy”) examples can be treated, so the students do not always see the real world utility and applicability of these formal methods.

The formal method teaching courses are often isolated from the other courses [17]. During the whole curricula, the use of these rigorous formal methods is not well enough integrated or used neither by the students nor by the other subject teachers. If the students don’t see the use of the formal methods in other areas or in their professional future, they will definitely not be motivated in learning or mastering them.

The use of formal methods requires rigorous, “mathematical” reasoning. Students often feel a certain fear of mathematics and rarely see its utility. However, choosing wisely the examples, the use of formal methods does not necessary require a very high level of mathematics. The mathematical courses should “prepare” better the students for the concepts of reasoning (“logic”) widely reused in the formal methods. Well prepared, the students could find a very good application area of mathematics in the formal methods.

2.2. Advantages of teaching formal methods in the higher education

Ad hoc program development is inappropriate to construct large systems [1] or safety critical systems and is also unacceptable in a higher education environment, where the scientific or engineering programming approaches are highly preferred, required and taught.

Formal software development can easily overcome these problems by providing and requiring a clear system modelling.

The use of formal methods facilitates a better understanding and overlook on both the algorithms and data structures [23].

Through these formal methods, students can soon familiarize with very important concepts of the computer science such as for example; system modelling, specification, design, implementation, invariant properties or integrity of operations, etc.

Through the use of formal methods in the system design, students are “forced” to reason about the system and are less able to use their “empirical intuitions”. Concerning their system design, the students are basically obliged to apply a scientific and/or engineering approach [24]

The B formal method is especially educative from a system architecture point of view, since this method separates clearly the “what” from the “how” witch is an extremely important educational concept. The possibilities to model a system at different levels of abstraction, namely the opportunity to specify at a high level of abstraction and to refine the model gradually to finally arrive at the implementation level are also very important educational benefits of the B-method.

3. Tools and environments to teach formal methods in higher education

There exist many notations, methods and tools for formal methods [2][3]. In this paper, we focus on the B-method, since this method has both a formal syntax and formal semantic whereas it permits not only to specify, to refine but to implement formal models as well.

3.1. The B-method

Both the B language and the B-method were initiated by Jean-Raymond Abrial[4].The B language is based around abstract machine notation and is related to the Z notation (also originated by Jean-Raymond Abrial). The software development method based on B is known as the B-method.

---

1 This B is now called “Classical B”.
The B-method has both tool support and significant safety critical industrial applications, such as for example: the Automatic Train Protection for the French railway company or the automatic train control for driverless Paris Metro Line 14, smartcards or for Peugeot automobiles...

The method is also used and taught in more than 100 universities.

3.2. Tools and environments of the B-method

Two commercial products are available to assist the B-method, one of them is the B-Toolkit [5] from the B-Core Ltd. [6] and the other one is the Atelier B [7] from the Clearsy Company [8]. Both of them were originally developed for industrial and professional use, but presently educational licences are also available. We have to admit: these tools are quite expensive for the universities; these high prices disadvantage severely the spread of the use of these tools.

Fortunately, a couple of years ago, Clearsy released the B4free [9] which was a free set of tools for the development of B models. B4free with the Click’n’Prove [10] environment allowed to write and prove B models and with the also free JBTools [11] even automatic code generation for Java and C# was possible. The use of these different tools was not easy, due to annoying incompatibilities amongst themselves. During a long time, a serious lack of good, free and open environments remained unsolved.

At the end of 2008, Clearsy released the Atelier B 4.0 for free, which was the successor of its already existing commercial product. We hope and do believe that this free environment will help the spread of the use of the formal B-method.

3.3. New tools of the Event-B

The Event-B [12] is an evolution of the B-method [13][14], developed also by Jean-Raymond Abrial.

The Event-B is a formal method for system-level modelling and analysis. The key features of the Event-B are the use of set theory as a modelling notation, the use of refinement to represent systems at different abstraction levels and the use of mathematical proof to verify consistency between refinement levels.

To support the Event-B, the Rodin platform was developed. The Rodin development was partly funded by the European Union IST Project RODIN from 2004 to 2007 [15].

The Rodin Platform is an Eclipse-based IDE for Event-B that provides effective support for refinement and mathematical proof. The platform is an open source, contributes to the Eclipse framework and is further extendable with plug-ins. Plug-ins permit to visualize, animate the Event-B models and to translate them into or from other formalisms such as UML, etc.

The development and the propagation of the Rodin platform is continuous and is supported by the European Union ICT Project DEPLOY, starting from 2008 until 2012 [16].

4. Methodologies, practices and experiences in teaching formal methods in higher education

4.1. Teaching formal methods at the Eötvös Loránd University

At the Eötvös Loránd University, Faculty of Informatics, the students meet formal methods several times at different levels during their curriculum; from their first use of semiformal methods during their first semester, until their use of formal methods at MSc level.

A semi-formal method is first used during the lectures of “Introduction of programming”, which has a formal, mathematical semantics, but not a formal syntax. Hence it can be proved, but only manually (“by hand”) and not automatically. This mathematical semantic is fruitful because it facilitates the introduction of the formal methods.

---

2 The author has no affiliation with or financial interest in the above mentioned companies.

3 Versions before the free Atelier B 4.0.

4 at the time of writing this paper the beta test state, on Linux, Macintosh and Windows platform
Naturally, the semantic is not limited to only one concrete tool. Later in their studies, students learn to use the Unified Modelling Language (UML) and start to familiarize with formal semantic, temporal logic and algebraic type theories.

In an optional lecture, students can learn to use the B-method. During these courses semiformal and formal tools and techniques are connected, the previously learnt methods are integrated into the B-method and the B-method is also used to prove the correctness of programming theorems, UML models, design pattern, and part of applications [22]. Unfortunately, most of the times, the teachers of these formal methods are much more enthusiastic, than their students…

4.2. Conferences and workshops about formal methods

Several conferences and workshops are held, every year, dealing with the different aspects of teaching formal methods in higher education, such as for example the “Teaching Formal Methods: Practice and Experience” in 2006 [19], the “Formal Methods in Computer Science Education” in 2008 [20] or “The B-method: from Research to Teaching” in 2008 [21]. These events permit both the researchers and the university teachers to discuss both their results and experiences in teaching formal methods.

More and more experiences are accumulated about the different methodologies, practices or pitfalls of teaching formal methods. Nowadays better and better tools, environments, materials, exercises and practical works are available and no negligibly, for free! The easy use and intelligibility of the Rodin platform also helped significantly the spread the B-method.

Several good sets of plug-ins exist already for the Rodin platform, but its open platform allows and aids the development of even more new extensions. These plug-ins facilitate not only the manipulation and the understanding of the B-method or the B-models, but they also help to link the formal methods to the other subjects, such as for example: the conversion plug-in from UML to B.

Some Universities have already started to use the Rodin platform and have switched from the Classical B to the Event-B.

5. Conclusion

Teaching formal methods in higher education, in computer science, in software engineering and in computer engineering helps the students to model, to understand and to prove in a better way the correctness of the different software systems. The easy availability of several free tools and materials also helps notably the spread of the teaching of formal methods.

It occurs clearly, that formal methods slowly but surely do gain their places within the higher education curricula.

References