A Survey of Formal Methods in Software Development

Dines Bjørner, DTU Informatics and
Fredsvej 11, DK-2840 Holte, Danmark

October 27, 2012
E–Mail: bjorner@gmail.com, URL: www.imm.dtu.dk/~dibj

Abstract

The use of formal methods and formal techniques in industry is steadily growing.

- In this survey we shall
  - characterise what we mean by **software development;**
  - characterise what we mean by a **formal method;**
  - briefly overview a **history of formal specification languages** — some of which are:
    - **VDM** (Vienna Development Method, 1974–...),
    - **Z** (Z for Zermelo Fraenkel, 1980–...),
    - **RAISE** (Rigorous Approach to Industrial Softw.Eng., 1987–...)
    - **Event B** (B for Bourbaki, 1990/2000–...) and
    - **Alloy**;
  - and outline the basics of a formal development using, for example, RAISE:
    - first developing a **domain description D**,
    - then a **requirements prescription R**,
    - and finally a **software design S** —
    - **showing (arguing or formally proving)** that **S**, in the context of **D** satifies (is **correct** with respect to) **R**.
- We shall then
  - mention industries in Japan, Europe and USA which, in a number of projects, uses formal methods;
  - discuss what it takes for an industry to do so;
  - discuss what education candidates for these industries need,
  - that is, which courses must be part of a BSc/MSc Software Engineering curriculum
- Finally we shall comment on
  - **distinctions** between formal methods and formal techniques;
  - **limitations** of mono-language formalisations, hence need for multi-language formalisation (**Petri Nets, MSC, StateChart, Temporal Logics**);
  - the **sociology** of university and industry acceptance of formal methods;
  - the **inevitability** of the use of formal software development methods;
  - while referring to **seminal monographs and textbooks** on formal methods.

Seminal Textbooks

1. **VDM:**
   - D. Bjørner and C. B. Jones, editors. *The Vienna Development Method: The Meta-Language*, volume 61 of *LNCS*. Springer, 1978.
   - D. Bjørner and C. B. Jones, editors. *Formal Specification and Software Development*. Prentice-Hall, 1982.
   - J. Fitzgerald and P. G. Larsen. *Modelling Systems – Practical Tools and Techniques in Software Development*. Cambridge University Press, The Edinburgh Building, Cambridge CB2 2RU, UK, 1998.
2. **Z:** J. C. P. Woodcock and J. Davies. *Using Z: Specification, Proof and Refinement*. Prentice Hall International Series in Computer Science, 1996.
3. **RAISE:** D. Bjørner. Software Engineering,
   - Vol.1: *Abstraction and Modelling*,
   - Vol.2: *Specification of Systems and Languages*,
   - Vol.3: *Domains, Requirements and Software Design*.

   Texts in Theoretical Computer Science, the EATCS Series. Springer, 2006.
   See book covers below.
4. **B, Event B:** J.-R. Abrial. The B Book: Assigning Programs to Meanings *and* Modeling in Event-B: System and Software Engineering. Cambridge University Press, Cambridge, England, 1996 and 2009
5. **Alloy:** D. Jackson. *Software Abstractions: Logic, Language, and Analysis*. The MIT Press, Cambridge, Mass., USA, April 2006. ISBN 0-262-10114-9.