Formal Methods in Software Engineering

Dr. Aamer Nadeem
Department of Computer Science
Mohammad Ali Jinnah University, Islamabad

Third International Conference on Open-Source Systems and Technologies, 19-22 December 2009, Lahore, Pakistan
Presentation Overview

- What are Formal Methods
- Why Formal Methods
- Software Horror Stories
- Some Myths about Formal Methods
- Industrial Applications of Formal Methods
- Overture – Open Source Toolset for VDM++
- Future of Formal Methods
WHAT ARE FORMAL METHODS?
What are Formal Methods?

- Mathematical approaches to the design and analysis of systems
- Correspond to mathematical techniques used in other fields of engineering, such as
  - Finite element analysis for bridges and other structures
  - Fluid dynamics for airplane wings and streamlined cars
- Various fields of Engineering have ways to model the designs and phenomena of concern in some branch of mathematics
- This has advantages such as
  - Calculations can be done to predict and explore properties of interest
  - Designs can be analyzed prior to construction
...What are Formal Methods?

- Unfortunately, software engineers are more inclined towards *Hack and Test* approach, i.e.,
  - Let us build the software and run it a few times to see what happens

- Formal methods bring discipline to software development

- Can be applied to all phases of software development
  - Specification
  - Design
  - Implementation
  - Verification / Testing
What are Formal Methods?

- Application of formal methods in early phases brings highest returns

- Some well-known Formal Languages include
  - Z
  - Object-Z
  - VDM-SL
  - VDM++
  - B Method
  - SOFL

- Based on
  - Set theory
  - First order logic
...What are Formal Methods?

- Allow the developer to build a *mathematical model of the system*
- The model can be built at various levels of abstraction
- A formal model is an abstract, precise, unambiguous and complete description of system (or subsystem).
- The model allows to carry out a rigorous analysis
- Through the use of tools, the model can be checked for properties of interest, such as:
  - Consistency
  - Deadlock freedom
  - Satisfaction of high-level requirements
  - Correctness of proposed design
What are Formal Methods?

- Through the process of *Refinement*, the abstract model is transformed to a more concrete one which eventually leads to the implementation.
- The refinement process is not fully automated.
- *Model checking* and *Theorem proving* techniques allow verification of the model.
WHY FORMAL METHODS?
Why Formal Methods?

- In recent years, the role of software in critical systems has changed from auxiliary to primary
- Dependence of human life on computer systems is growing day by day
- Computers are now being used in
  - Railway interlocking systems
  - Air traffic control systems
  - Aircraft navigation
  - Automobile: Anti-lock braking and Airbag systems
  - Nuclear reactor control systems
  - Medicine: Radiation therapy systems, etc.
...Why Formal Methods?

- Our reliance of critical systems is increasingly outweighing our trust in such systems
- Software complexity is rapidly increasing
- The users have a right to demand correctness
- Software engineers have the responsibility to provide correctness
...Why Formal Methods?

- Fault free software is impossible to create, because exhaustive testing is impossible.
- Errors introduced in early phases of life cycle are the most costly and difficult to remove.
- The use of formal methods reduces the possibility of errors in early phases of life cycle.
- This pays off in the later phases.
- However, formal methods do not guarantee that the software will be fault free.
- Testing is still required.
- Formal methods also provide an opportunity to automate the testing process.
...Why Formal Methods?

- A PC manufacturer’s warranty for Microsoft Windows software and accompanying hardware:
  - “the SOFTWARE will perform substantially in accordance with the accompanying written materials for a period of ninety (90) days from the date of receipt”
  - “any Microsoft hardware accompanying the SOFTWARE will be free from defects in materials and workmanship under normal use and service for a period of one (1) year from the date of receipt”

- Microsoft is world’s biggest software manufacturer*

- Above warranty statement clearly shows Microsoft’s lack of confidence in its software products

*Source: http://www.softwaretop100.org
Why Formal Methods?

- A hardware manufacturer’s warranty:
  - "ACCTON warrants to the original owner that the product delivered in this package will be free from defects in material and workmanship for the lifetime of the product"

- ACCTON is a manufacturer of intelligent hubs

- It is clear that reliability of software is viewed as poor even by the largest software companies in the world
...Why Formal Methods?

Average Defect Density of Delivered Software

<table>
<thead>
<tr>
<th>CMM Level</th>
<th>Defects/KLOC</th>
</tr>
</thead>
<tbody>
<tr>
<td>Level 1</td>
<td>7.50</td>
</tr>
<tr>
<td>Level 2</td>
<td>6.24</td>
</tr>
<tr>
<td>Level 3</td>
<td>4.73</td>
</tr>
<tr>
<td>Level 4</td>
<td>2.29</td>
</tr>
<tr>
<td>Level 5</td>
<td>1.05</td>
</tr>
<tr>
<td>Praxis</td>
<td>0.04</td>
</tr>
</tbody>
</table>

Why Formal Methods?

- Formal methods do not produce perfect software, but
  - Reduce defect density in the delivered product
  - Contrary to the popular belief, formal methods lower overall development cost
  - This is because the bugs introduced in early phases of life cycle and discovered in later phases are the most costly
  - Formal methods eliminate such bugs in early phases
...Why Formal Methods?

Cost of correcting a requirements defect
SOFTWARE HORROR STORIES
Ariane 5 Rocket Explosion, 1996

- European Space Agency’s $7 billion project
- Exploded in its maiden flight within 40 seconds of lift-off
- Cause of failure was a software error – an attempt to convert a 64-bit floating point number to a 16-bit integer

Source
- www.math.psu.edu/dna/disasters/ariane.html
Airbag Recall

- BMW, German automobile manufacturer, is known for producing high quality automobiles
- A software bug in BMW’s electronic airbag system caused its deployment for no reason
- BMW had to recall 1000’s of cars
- General Motors (GM) recalled over one million cars for a similar airbag fault
Mars Climate Orbiter’s Loss, 1999

- Launched by NASA in Dec. 1998
- Disappeared in Sep. 1999
- The satellite either burnt up or broke apart
- The cause was the software failure to convert English units of force to metric system units

Source
Therac-25 Accidents, 1987

- AECL’s Therac-25 is a radiation therapy machine for treatment of cancer patients
- The radiation dose given to patients is controlled by a software
- A bug in the software caused over-dosage accidents
- Six accidents were reported between 1985 and 1987
- Out of the six accidents, four resulted in death of patients, two resulted in serious disfigurement and disability

Source
- courses.cs.vt.edu/~cs3604/lib/Therac_25/Therac_1.html
Patriot Missile Failure, 1991

- In the first Gulf War, a US Patriot Missile failed to intercept an Iraqi scud missile.
- As a result an army barrack was hit in Dhahran.
- The accident caused death of 28 US soldiers.
- Later investigation revealed the cause was a computer arithmetic error which inaccurately calculated the time since boot.

Source:
- [www.ima.umn.edu/~arnold/disasters/patriot.html](http://www.ima.umn.edu/~arnold/disasters/patriot.html)
Chinook Helicopter Crash, 1994

- Royal Air Force (RAF) Chinook ZD-576 crashed in Scotland
- All four crew members and 25 passengers were killed
- The investigation found problems with the Full Authority Digital Electronic Control (FADEC) software of the helicopter

Source:
MYTHS ABOUT FORMAL METHODS
Some Myths about Formal Methods

● Myth 1:
  ■ FMs *guarantee* perfect software

● Facts:
  ■ FMs only enhance reliability of software
  ■ 100% fault free software is not guaranteed
  ■ Testing is required to complement the use of FMs

● Myth 2:
  ■ FMs increase the development cost

● Facts:
  ■ Experience shows development cost is actually reduced
  ■ Greater investment in early phases pays off in later phases
...Some Myths about Formal Methods

• Myth 3:
  ■ FMs delay the development

• Facts:
  ■ The analysis and design phases may be delayed
  ■ But, the overall development time is actually reduced

• Myth 4:
  ■ FMs must not be mixed with informal methods

• Fact:
  ■ In practice only critical parts of a large system are modeled using FMs
...Some Myths about Formal Methods

- Myth 5:
  - FMs are only useful in safety critical systems

- Facts:
  - FMs may be used for any system
  - The benefits of FMs can be derived from any system

- Myth 6:
  - FMs need mathematicians

- Fact:
  - FMs are based on simple mathematics and logic
...Some Myths about Formal Methods

- Myth 7:
  - FMs are all about proving programs correct

- Fact:
  - FMs can be applied in all phases of system development

- Myth 8:
  - Not tools are available for FMs

- Facts:
  - The situation has changed over past 10-15 years
  - Commercial tools are now available to supports FMs
INDUSTRIAL APPLICATIONS OF FORMAL METHODS
Some Industrial Applications of FMFs

- **IBM CICS (Customer Information Control System)**
  - A large IBM software product
  - Licensed to over 40,000 organizations worldwide
  - FMGs applied since 1982
  - Heavy use of Z specification language in all new CICS modules
  - More time is spent specification stages
  - But, total development time significantly reduced
  - Product service time dramatically reduced
  - IBM continues to broaden its use of FMGs
...Some Industrial Applications of FMs

- Inmos T800 FPU Chip Development
  - Use of FMs discovered a hitherto undiscovered fault in IEEE floating point numbers
  - The overall time to delivery was reduced
  - Only one fault was found in first mask iteration
  - Second mask iteration was put to production
  - In perspective, without FMs, similar chips have 10 to 100 faults in first mask iteration
  - 4 to 10 mask iterations spread over a year or so are required without FMs
...Some Industrial Applications of FM s

- NASA’s Deep Space 1
  - Deep Space 1 mission launched in Dec. 1998
  - Heavily relies on software
  - Millennium Remote Agent software is an AI system to manage the control, guidance and autonomous robotic systems on board
  - Software is considered mission-critical
  - Developed over many years with practically unlimited budget and extremely experienced software engineers
  - A small group used FM s to analyze components of software
  - Found 5 errors, one of which was a significant design flaw
OVERTURE – AN OPEN-SOURCE TOOLSET FOR FORMAL METHODS
Overture – An Open-Source Project

- An open-source project that supports VDM++ language
- Allows mapping UML diagrams to VDM++ and vice versa
- Supports syntax and type checking of formal models
- Supports execution and debugging of formal models
- Generates proof obligations

Source: http://www.overturetool.org
FUTURE OF FORMAL METHODS
Future of Formal Methods

- In recent past, formal methods have moved from the classroom to the industry
- Due to the increasing role of software in critical systems, the use of formal methods is growing
- However, there is a need to integrate formal methods into the existing software process models
- Tool support on formal methods is still scarce – most of the tools are academic versions only
- There is a need for greater industry-level tools
Bertrand Meyer, a pioneer in object technology, says:

“ A more mathematical approach is inevitable. Professional software development—not the everyday brand practiced by the public at large—will become more like a true engineering discipline, applying mathematical techniques. I don't know how long this evolution will take, but it will happen. The basic theory is there, but much work remains to make it widely applicable.”
Thankyou