Overview of NASA Langley's Formal Methods Program

by

Ricky W. Butler

NASA Langley Research Center

May 10, 1995

Goals Of Our Formal Methods Program

- **To make formal methods practical for use on life critical systems developed in the United States.**
- **To orchestrate the transfer of this technology to industry through use of carefully designed demonstration projects.**

NASA Langley's Research Strategy

- **Build strong team at LaRC.**
- **Leverage huge investment of ARPA and National Security Agency through use of FM technology that they nurtured.**
- **Use contracts with the leading U.S. formal methods research teams.**
- **Establish joint projects with FM researchers and established aerospace engineering teams (e.g. Rockwell Collins, Honeywell, Boeing).**
- **Concentrate on the technically challenging areas of digital design (especially in avionics) that are currently beyond the state-of-the-practice.**
- **Initiate demonstration projects in problem domains where current formal methods are adequate.**

Although Tool Development Has Not Been Emphasized ...

- NASA Langley has not sponsored the development of any general-purpose theorem provers.

- However, the technology transfer projects have lead to significant improvements in the Prototype Verification System (PVS) theorem prover that SRI International is developing.

- Some domain-specific tools are being sponsored:
  - VHDL-analysis tool [ORA]
  - Tablewise [ORA]
  - Derivational Reasoning System (DRS) [Derivation Systems Inc.]

Scope of Program is Large

- Formal Methods appropriate for one problem domain may be totally inappropriate for other problem.
- Specific domains in which our program has concentrated:
  - architectural-level fault tolerance,
  - clock-synchronization,
  - interactive consistency,
  - design of hardware devices such as microprocessors, memory management units, DMA controllers,
  - asynchronous communication protocols,
  - design and verification of application-specific integrated circuits (ASICS),
  - Space Shuttle software,
  - navigation software,
  - decision tables,
  - railroad signaling systems.
- We are also interested in applying formal methods to many different portions of the life-cycle, such as (1) requirements analysis, (2) high-level design, (3) detailed design, and (4) implementation.

Technology Transfer Strategy

- **Get involved with (i.e. influence) standards activities (e.g. NIST, DO178B).**

- **Work with/influence FAA.**

- **Demonstrate techniques on realistic designs.**

- **Sponsor joint research projects using both formal methods contractors and aerospace contractors.**

Technology Transfer Projects

1. **Rockwell Collins AAMP5**
2. **Boeing PIU Project**
3. **Space Shuttle Jet-Select Project**
4. **Honeywell Navigation**
5. **Charles Stark Draper FTPP Scoreboard Project**
6. **Honeywell Software Development (Tinkerbell)**
7. **Union Switch and Signal**
8. **Rockwell Collins AAMP-FV**
9. **Honeywell SafeBus Project**

Transfer of Formal Methods to Industry Has Been Slow in the Past

Why?

- **Long learning curve:**
  - **FM not part of traditional engineering curriculum**
  - **the tools are not production-quality**
  - **the tools have few or no examples for specific problem domains.**

- **Many competing methods: the best are now only beginning to stand out.**

- **Cost/benefit relationship not favorable for many applications: situation has improved considerably over last 5-10 years, and improving this relationship is the major goal of our research program.**

- **Large investment by DARPA and NSA in tool development but did not fund technology transfer projects.**

Also Libraries Are Needed

There is a sizable effort associated with the development of the background mathematical theories needed for a particular problem domain.

- **Libraries would be reusable and in the long run "cost-effective"**
- **But, initial costs are a deterrent for industry.**

Therefore, one of the goals of the NASA Langley program is to build a large body of background theories needed for aerospace applications. Langley has helped develop PVS libraries:

- **bitvectors library for hardware verification**
- **IEEE floating point standard**
- **finite sets**
- **majority**
- **summations**

Finelli/Di Vito Inject Formal Methods Into DO178B

George Finelli, a member of the verification subcommittee of the RTCA group that developed the DO-178B standard and Ben Di Vito wrote a section on formal methods that was included in DO-178B:

12.3.1. Formal Methods: Formal methods involve the use of formal logic, discrete mathematics, and computer-readable languages to improve the specification and verification of software. These methods could produce an implementation whose operational behavior is known with confidence tobe within a defined domain. In their most thorough application, formal methods could be equivalent to exhaustive analysis of a system with respect to its requirements. Such analysis could provide:

- Evidence that the system is complete and correct with respect to its requirements.
- Determination of which code, software requirements or ... satisfy the next higher level of software requirements.

... The goal of applying formal methods is to prevent and eliminate requirements, design and code errors throughout the software development processes. Thus, formal methods are complementary to testing....

Formal methods may be applied to software development processes with consideration of these factors:

Levels of the design refinement : The use of formal methods begins by specifying software high-level requirements in a formal specification language and verifying by formal proofs that they satisfy system requirements, especially constraints on acceptable operation. The next lower level of requirements are then shown to satisfy the high-level requirements. Performing this process down to the Source Code provides evidence that the software satisfies system requirements. Application of formal methods can start and stop with any consecutive levels ...

Coverage of software requirements and software architecture : Formal methods may be applied to software requirements that: (1) Are safety-related, (2) Can be defined by discrete mathematics, (3) involve complex behavior, such as concurrency, distributed processing, redundancy management, and synchronization.

Degree of rigor : Formal methods include these increasingly rigorous levels: ...

The use of formal specifications alone forces requirements to be unambiguous. Manual proof is a well-understood process that can be used when there is little detail. Automatically checked or generated proofs can aid the human proof process and offer a higher degree of dependability, especially for more complicated proofs.

RTCA committees

Currently, members of the Langley staff are involved in:

- **SC-180 (Airborne Electronic Hardware)**
- **SC-182 (Minimal Operating Performance Standard for an Airborne Computer Resource)**

Some Lessons Learned

- **Modern formal specification languages such as PVS (which support higher order logic and a rich type system) provide a means of writing specifications that** *can be read and understood* **by engineers.**

- **Formal specification alone can reveal bugs not found by traditional V&V techniques. Formal Verification can uncover additional errors and provide increased confidence in the correctness of the system design.**

- **There is a sizable up-front cost associated with transferring formal methods into a commercial company. The two major components of this cost are:**

  1. **Training the industrial experts to use the formal techniques (especially in verification).**
  2. **The formal methods experts must learn the problem domain in detail (to develop effective formal methods).**

Some Lessons Learned (Continued)

- **Finding a person inside the company who is knowledgeable of the problem domain, is a proponent of formal methods, and is an active participant in the project is essential.**

- **The formal methods researchers must be willing to adapt their methods to the problem domain rather than fight to change the existing methodologies to conform to their needs.**

- **Without the significant increases in hardware speed, level 3 formal methods would still be impractical.**

- **Efficient automatic deduction can greatly facilitate the useability of a theorem prover.**

NASA Langley's Formal Methods (FM) Program

- **The tremendous scientific *potential* of formal methods has been recognized by theoreticians for a long time, BUT**
- **The formal techniques had remained the province of a few academians with only a few exceptions such as the Transputer and CICS.**
- **Starting in 1991, NASA Langley initiated several aggressive projects designed to move FM into productive use in the aerospace community:**
  - Boeing PIU Project (1991)
  - Charles Stark Draper FTPP Scoreboard Project (1991)
  - Allied Signal Hybrid Fault Models (1992)
  - Shuttle Tile Project (1992)
  - Space Shuttle Jet-Select Project (1993)
  - Honeywell Navigation (1993)
  - Rockwell Collins AAMP5 (1993)
  - Honeywell Software Development: Tinkerbell (1994)
  - Union Switch and Signal (1994)
  - Rockwell Collins AAMP-FV (1995)
  - Honeywell SafeBus Project (1995)
- **NASA's program has advanced FM in the United States to the point where commercial exploitation of FM is imminent.**