Second NASA Formal Methods Workshop 1992

Compiled by
Sally C. Johnson
C. Michael Holloway
and Ricky W. Butler
NASA Langley Research Center
Hampton, Virginia

Proceedings of a workshop sponsored by the National Aeronautics and Space Administration, Washington, D.C., and held at Langley Research Center Hampton, Virginia August 11–13, 1992

NOVEMBER 1992
Contents

Introduction ................................................................. 3

Workshop Agenda .......................................................... 5

A Brief Overview of NASA Langley’s Research Program in Formal Methods .......... 9

Welcome and Introduction
by Chuck Meissner, Jr. (NASA Langley Research Center) ...................... 23

Why Formal Methods?
by Ricky Butler (NASA Langley Research Center) ......................... 27

Tutorial: Design Specification Techniques
by Ben DiVito (ViGYAN) ......................................................... 43

Tutorial: Code Verification Techniques
by Michael Holloway (NASA Langley Research Center) .................... 49

The FAA DFCS Handbook Formal Methods Chapter
by John Rushby (SRI International) ............................................... 55

Survey of State-of-Practice: Formal Methods in Industry
by Dan Craigan (ORA Canada) ............................................. 61

Formal Modelisation
by Susan Gerhart (National Science Foundation) ................................ 71

Formal Methods Technology Insertion Into FTPP
by Rick Harper (Charles Stark Draper Labs) .................................. 75

Formal Methods at IBM Federal Systems
by David Hamilton (IBM Federal Systems) .................................... 83

Reliable Computing Platform
by Ben DiVito (ViGYAN) .......................................................... 89

Clock Synchronization: Verification and Implementation
by Paul Miner (NASA Langley Research Center) .............................. 101

NASA’s Strategy for Technology Transfer
by Sally Johnson (NASA Langley Research Center) ......................... 107
Verification of FTPP Scoreboard and Spectool
by Mark Bickford (Odyssey Research Associates, Inc.) ........................................ 111

Boeing's Work in Formal Methods
by Dave Fura (The Boeing Company) ............................................................. 127

DO-178B and Formal Methods
by George Finelli (NASA Langley Research Center) ......................................... 133

Introduction to the Boyer-Moore Theorem Prover
by Warren Hunt (Computational Logic, Inc.) .................................................. 137

Introduction to PVS
by Natarajan Shankar (SRI International) ..................................................... 149

Logical Foundations of Computing over the Floating Point Reals
by Richard Platek (Odyssey Research Associates, Inc.) ....................................... 161

Formal Safety Analysis
by Nancy Leveson (University of California at Irvine) ...................................... 175

The FM9001
by Warren Hunt (Computational Logic, Inc.) .................................................... 199

Derivational Techniques for Hardware
by Steve Johnson (Indiana University) ............................................................ 215

Results of Workshop Survey ................................................................. 223

List of Attendees ............................................. 237
Introduction

This publication contains copies of the material presented at the Second NASA Langley Formal Methods Workshop held at the NASA Langley Research Center August 11–13, 1992. The purpose of the workshop was to bring together formal methods researchers and aerospace industry engineers to investigate new opportunities for applying formal methods to aerospace problems. The first part of the workshop was tutorial in nature. The second part of the workshop explored the potential of formal methods to solve current aerospace design and verification problems. The third part of the workshop involved on-line demonstrations of state-of-the-art formal verification tools. Finally, a detailed survey was filled in by the attendees; the results of the survey are compiled in this report.

The workshop was attended by aerospace industry engineers and managers, interested government representatives from FAA, NSA, NCSC, and DARPA, NASA Langley formal-methods contractors, university professors, and NASA personnel. A list of attendees is included in this publication.
Second NASA Langley Formal Methods Workshop
H. J. E. Reid Conference Center

Tuesday, August 11, 1992

7:30  Bus Leaves Radisson Hotel for Reid Conference Center
8:00 – 8:30  Late Registration
8:30 – 8:45  Welcome and Introduction
  Charles Meissner, Jr., Head, System Validation Methods Branch
8:45 – 9:30  Why Formal Methods?
  Ricky Butler, NASA Langley Research Center
9:30 – 10:45 Tutorial: Formal Methods
  Ben DiVito, VIGYAN
  Michael Holloway, NASA Langley Research Center
10:45 – 11:00 Break
11:00 – 11:30 The FAA DFCS Handbook — Formal Methods Chapter
  John Rushby, SRI International
11:30 – 12:30 Survey of State-of-Practice Formal Methods in Industry
  Dan Craigan, ORA Canada
12:30 – 1:30 Lunch in NASA Cafeteria
1:30 – 2:00 Formal Modelling
  Susan Gerhart, National Science Foundation
2:00 – 2:30 Formal Methods Technology Insertion into FTPP
  Rick Harper, Charles Stark Draper Labs
2:30 – 3:00 Break
3:00 – 3:40 Formal Methods at IBM Federal Systems
  David Hamilton, IBM Federal Systems
3:40 – 4:40 Reliable Computing Platform
  Ben DiVito, VIGYAN
4:40 – 5:00 Clock Synchronization Verification and Implementation
  Paul Miner, NASA Langley Research Center
5:00  Bus Leaves Reid Conference Center for Radisson Hotel
6:30 – 9:00 Workshop Dinner at the Radisson Hotel

Final Agenda - 1
Wednesday, August 12, 1992

8:00  Bus Leaves Radisson Hotel for Reid Conference Center
8:30 – 8:45 NASA's Strategy for Technology Transfer
      Sally Johnson, NASA Langley Research Center
8:45 – 9:15 Verification of FTPP Scoreboard and Spectool
      Mark Bickford, Odyssey Research Associates, Inc.
9:15 – 9:45 Boeing's Work In Formal Methods
      Dave Fura, The Boeing Company
9:45 – 10:00 DO-178B and Formal Methods
      George Finelli, NASA Langley Research Center
10:00 – 10:30 Break
10:30 – 11:10 Introduction to the Boyer-Moore Theorem Prover
      David Russinoff, Computational Logic, Inc.
11:10 – 11:50 Introduction to PVS
      Natarajan Shankar, SRI International
11:50 – 12:30 Logical Foundations of Computing over the Floating Point Reals
12:30 – 1:30 Lunch In NASA Cafeteria
1:30 – 2:10 Formal Safety Analysis
      Nancy Leveson, University of California at Irvine
2:10 – 2:45 The FM9001
      Warren Hunt, Computational Logic, Inc.
2:45 – 3:00 Break
3:00 – 4:00 Panel: Degree of Mechanization In Formal Methods
      Paul Miner, NASA Langley Research Center, Moderator
      Nancy Leveson, University of California at Irvine
      John Rushby, SRI International
4:00 – 6:00 Exhibits of Formal Methods Tools and Techniques
5:00 – 6:00 Cash Bar Social
6:00  Bus Leaves Reid Conference Center for Radisson Hotel
<table>
<thead>
<tr>
<th>Time</th>
<th>Event</th>
</tr>
</thead>
<tbody>
<tr>
<td>8:00</td>
<td>Bus Leaves Radisson Hotel for Reid Conference Center</td>
</tr>
<tr>
<td>8:30 – 9:00</td>
<td>Derivational Techniques for Hardware</td>
</tr>
<tr>
<td></td>
<td>Steven Johnson, Indiana University</td>
</tr>
<tr>
<td>9:00 – 10:00</td>
<td>Panel: Issues in Hardware Verification</td>
</tr>
<tr>
<td></td>
<td>Victor Carreno, NASA Langley Research Center, Moderator</td>
</tr>
<tr>
<td></td>
<td>Mark Bickford, Odyssey Research Associates, Inc.</td>
</tr>
<tr>
<td></td>
<td>Warren Hunt, Computational Logic, Inc.</td>
</tr>
<tr>
<td></td>
<td>Steven Johnson, Indiana University</td>
</tr>
<tr>
<td></td>
<td>Phillip Windley, University of Idaho</td>
</tr>
<tr>
<td>10:00 – 10:15</td>
<td>Break</td>
</tr>
<tr>
<td></td>
<td>Michael Holloway, NASA Langley Research Center, Moderator</td>
</tr>
<tr>
<td></td>
<td>Ben DiVito, VIGYAN</td>
</tr>
<tr>
<td></td>
<td>Damir Jamsek, Odyssey Research Associates, Inc.</td>
</tr>
<tr>
<td></td>
<td>Miriam Lesser, Cornell University</td>
</tr>
<tr>
<td></td>
<td>John Rushby, SRI International</td>
</tr>
<tr>
<td>11:15 – 11:45</td>
<td>Formal Methods Survey Completion</td>
</tr>
<tr>
<td>11:45 – 12:00</td>
<td>Closing Remarks</td>
</tr>
<tr>
<td></td>
<td>Ricky Butler, NASA Langley Research Center</td>
</tr>
<tr>
<td>12:00</td>
<td>Bus Leaves Reid Conference Center for Radisson Hotel</td>
</tr>
<tr>
<td></td>
<td>(for those not attending the technical review)</td>
</tr>
</tbody>
</table>
A Brief Overview of NASA Langley's Research Program in Formal Methods

System Validation Methods Branch
NASA Langley Research Center
Hampton, Virginia
September 21, 1992

Abstract

This paper presents an overview of NASA Langley's research program in formal methods. The major goal of this work is to bring formal methods technology to a sufficiently mature level for use by the United States aerospace industry. Towards this goal, work is underway to design and formally verify a fault-tolerant computing platform suitable for advanced flight control applications. Also several direct technology transfer efforts have been initiated that apply formal methods to critical subsystems of real aerospace computer systems. The research team consists of six NASA civil servants and contractors from Boeing Military Aircraft Company, Computational Logic Inc., Odyssey Research Associates, SRI International, University of California at Davis, and Vigyan Inc.

Motivation

NASA Langley Research Center has been developing techniques for the design and validation of flight critical systems for over two decades. Although much progress has been made in developing methods which can accommodate physical failures, the design flaw remains a serious problem [2, 3, 4, 5, 6, 7, 8].

A recent report by the National Center For Advanced Technologies \(^1\) has identified "Provably Correct System Specification" and "Verification Formalism For Error-Free Specification" as key areas of research for future avionics software and ultrareliable electronics systems [9]. Aerospace engineers attending the NASA-LaRC Flight Critical Digital Systems Technology Workshop [10] listed techniques for the validation of concurrent and fault-tolerant computer systems high on the list of research priorities for NASA.

---

*This is an updated version of the a paper entitled "NASA Langley’s Research Program in Formal Methods" presented at COMPASS 91 [1].

\(^1\)A technical council funded by the Aerospace Industries Association of America (AIA) that represents the major U.S. aerospace companies engaged in the research, development and manufacture of aircraft, missiles and space systems and related propulsion, guidance, control and other equipment.
A further motivation for the use of formal methods is the practical limitations of life-testing methods to quantify reliability in the ultrareliable domain. Unfortunately, the quantification of reliability in the presence of design faults has been found to be infeasible whether applied to hardware or software (standard or fault-tolerant) [11]. Therefore the use of non-statistical method is necessary.

Formal Methods

Formal methods are the applied mathematics of computer systems engineering. There are many different types of formal methods with various degrees of rigor. The following is a useful (first-order) taxonomy of the degrees of rigor in formal methods:

Level-1: Formal specification of all or part of the system.
Level-2: Formal specification at two or more levels of abstraction and paper and pencil proofs that the detailed specification implies the more abstract specification.
Level-3: Formal proofs checked by a mechanical theorem prover.

Level 1 represents the use of mathematical logic or a specification language that has a formal semantics to specify the system. This can be done at several levels of abstraction. For example, one level might enumerate the required abstract properties of the system, while another level describes an implementation which is algorithmic in style. Level 2 formal methods goes beyond level 1 by developing pencil-and-paper proofs that the more concrete levels logically imply the more abstract-property oriented levels. Level 3 is the most rigorous application of formal methods. Here one uses a semi-automatic theorem prover to make sure that all of the proofs are valid. The Level 3 process of convincing a mechanical prover is really a process of developing an argument for an ultimate skeptic who must be shown every detail.

It is also important to realize that formal methods is not an all-or-nothing approach. The application of formal methods to the most critical portions of a system is a pragmatic and useful strategy. Although a complete formal verification of a large complex system is impractical at this time, a great increase in confidence in the system can be obtained by the use of formal methods at key locations in the system.

Research Team

The Langley formal methods program involves both in-house researchers and industrial/academic researchers working under contract to NASA Langley. Currently the in-house team consists of six civil servants and one in-house contractor (Vigyan Inc.). NASA Langley has awarded three contracts specifically devoted to formal methods (from the competitive NASA RFP 1-22-9130.0238). The selected contractors were SRI International, Computational Logic Inc., and Odyssey Research Associates. The three contracts are five-year, task assignment contracts with total spending authority at approximately $2.5M per contract. Another task-assignment contract with Boeing Military Aircraft Company (BMAC) is being used to
explore formal methods as well. Through this contract BMAC is funding research at the University of California at Davis and California Polytechnic State University to assist them in the use of formal methods in aerospace applications.

NASA Langley's Research Strategy

The basic strategy of the research effort is to apply existing formal methods to challenging aerospace designs. This strategy leverages the huge investment of DARPA and National Security Agency in development of tools and concentrates on the problems specific to the aerospace problem domain. We have sought to build a strong inhouse research program as well as use contracts with the leading U.S. formal methods research teams (i.e. SRI, CLI, ORA) and aerospace industrial teams (BMAC, Draper Labs). In the short term we are seeking to apply formal methods to critical subsystems. In the medium term we are designing and verifying a reliable computing platform. Only in the long-term will we seek to make production-quality verification tools that are easily used by design engineers without overly specialized, detailed knowledge of formal methods.

The design of a digital flight control system involves two dissimilar activities:

1. design and implementation of control laws
2. design of the fault-tolerant computing platform which executes the control laws

Although these design activities are intimately connected, they require uniquely different skills. The first activity requires knowledge of feedback control theory and aerodynamics as well as numerical methods. The second activity requires knowledge of fault-tolerance theory and computer architecture. Although both activities are essential, we are concentrating at this time on the second activity. To facilitate the development and demonstration of tools and techniques to support the second activity, a reliable computing platform (RCP) is being developed. Also, several tasks are underway to facilitate the transfer of formal methods technology to aerospace industry.

The Reliable Computing Platform

The Reliable Computing Platform (RCP) dispatches the control-law application tasks and executes them on redundant processors. The reliable computing platform performs the necessary fault-tolerant functions and provides an interface to the network of sensors and actuators.

The RCP consists of both hardware and software components. A real-time operating system provides the applications software developer with a reliable mechanism for dispatching periodic tasks on a fault-tolerant computing base that appears to him as a single ultra-reliable processor. Traditionally, an operating system has been implemented as an executive (or main program) that invokes subroutines implementing the application tasks. Communication between the tasks has been accomplished by use of shared memory. This strategy is effective for systems with nominal reliability requirements where a simplex processor can
be used. For ultra-reliable systems, the additional responsibility of providing fault tolerance makes this approach untenable.

For these reasons, the operating system and replicated computer architecture must be designed together so they mutually support the goals of the RCP. A multi-level hierarchical specification of the RCP is shown in figure 1.

![Diagram](image)

**Figure 1: Hierarchical Specification of the Reliable Computing Platform (RCP)**

The top level of the hierarchy describes the operating system as a function that sequentially invokes application tasks. This view of the operating system will be referred to as the uniprocessor specification (US), which is formalized as a state transition system and forms the basis of the specification for the RCP. Fault tolerance is achieved by voting results computed by the replicated processors operating on the same inputs. Interactive consistency checks on sensor inputs and voting of actuator outputs require synchronization of the replicated processors. The second level in the hierarchy (RS) describes the operating system as a synchronous system where each replicated processor executes the same application tasks. The existence of a global time base, an interactive consistency mechanism and a reliable voting mechanism are assumed at this level. Level 3 of the hierarchy breaks a frame into four sequential phases. This allows a more explicit modeling of interprocessor communication and the time phasing of computation, communication, and voting. At the fourth level, the assumptions of the synchronous model must be discharged. Rushby and von Henke [12] report on the formal verification of Lamport and Melliar-Smith's [13] interactive-convergence clock synchronization algorithm. This algorithm can serve as a foundation for the implementation of the replicated system by bounding the amount of asynchrony in the system so that it can duplicate the functionality of the DS model. Dedicated hardware implementations of the clock synchronization function are a long-term goal. The LE model is currently under development. This model describes the actions on each local processor delineating how each processor schedules tasks, votes results and rewrites its own local memory with voted values. Of primary importance in this specification is the utilization of a memory management
unit by the local executive in order to prevent the overwriting of incorrect memory locations while recovering from the effects of a transient fault. There will probably be another level of specification introduced before the final implementation in hardware and software is reached. The research activity will culminate in a detailed design and prototype implementation. Figure 2 depicts the generic hardware architecture assumed for implementing the replicated system. Single-source sensor inputs are distributed by special purpose hardware executing a Byzantine agreement algorithm. Replicated actuator outputs are all delivered in parallel to the actuators, where force-sum voting occurs. Interprocessor communication links allow replicated processors to exchange and vote on the results of task computations. As previously suggested, clock synchronization hardware may be added to the architecture as well.

The hardware architecture is a classic N-modular redundant (NMR) system with a small number \( N \) of processors. Single-source sensor inputs are distributed by special purpose hardware executing a Byzantine agreement algorithm. Replicated actuator outputs are all delivered in parallel to the actuators, where force-sum voting occurs. Interprocessor communication links allow replicated processors to exchange and vote on the results of task computations. This is illustrated in figure 2.

\[ \text{Figure 2: Generic hardware architecture.} \]

**The Division of Labor**

The in-house team at NASA has been orchestrating the effort to apply formal methods to the RCP. The design problem has been decomposed into several separate activities, some of
which are being investigated by contractual teams and others by the in-house team. The efforts are roughly divided as follows:

- in-house: system architecture, clock synchronization
- SRI: Clock synchronization, fault-tolerance
- CLI: Byzantine Agreement Circuits, clock synchronization
- ORA: Byzantine Agreement Circuits, applications
- BMAC: Hardware Verification, formal requirements analysis

**NASA In-house Work**

The in-house team has concentrated on the system architecture for the RCP. The top two levels of the RCP were originally formally specified in standard mathematical notation and connected via mathematical (i.e. level 2 formal methods) proof[14, 15]. Under the assumption that a majority of processors are working in each frame, the proof establishes that the replicated system computes the same results as a single processor system not subject to failures. Sufficient conditions were developed that guarantee that the replicated system recovers from transient faults within a bounded amount of time. SRI subsequently generalized the models and constructed a mechanical proof in Ehdm [16]. Next, the NASA inhouse team developed the third and fourth level models. The top two levels and the two new models were then specified in Ehdm and all of the proofs were done mechanically using the Ehdm 5.2 prover [17, 18].

Inhouse work is underway to design and implement a fault-tolerant clock synchronization circuit capable of recovery from transient faults [19, 20]. The circuit is being implemented using programmable logic devices (PLDs) and FOXI fiber optic communications chips [21].

**Contractual Efforts**

**SRI International**

The redundancy management strategies of virtually all fault-tolerant systems depend upon some form of voting which in turn depends upon synchronization. Although in many systems the clock synchronization function has not been decoupled from the applications (e.g. the redundant versions of the applications synchronize by messages), research and experience have led us to believe that solving the synchronization problem independently from the applications design can provide significant simplification of the system [22, 23]. The operating system is built on top of this clock-synchronization foundation. Of course, the correctness of this foundation is essential. Thus, the clock synchronization algorithm and its implementation are prime candidates for formal methods. The verification strategy shown in figure 3 is being explored. The top-level in the hierarchy is an abstract property of the form:

\[ \forall \text{non-faulty } p, q : |C_p(t) - C_q(t)| < \delta \]

where \( \delta \) is the maximum clock skew guaranteed by the algorithm as long as a sufficient number of clocks (and the processors they are attached to) are working. The function \( C_p(t) \)
Figure 3: Hierarchical Verification of Clock Synchronization

gives the value of clock $p$ at real time $t$. The middle level in the hierarchy is a mathematical definition of the synchronization algorithm. The bottom level is a detailed digital design of a circuit that implements the algorithm. The bottom level is sufficiently detailed to make translation into silicon straight forward.

The verification process involves two important steps: (1) verification that the algorithm satisfies the maximum skew property and (2) verification that the digital circuitry correctly implements the algorithm. The first step has already been completed by SRI International. The first such proof was accomplished during the design and verification of SIFT [13]. The proof was done by hand in the style of most journal proofs. More recently this proof step has been mechanically verified using the Ehdm theorem prover [12]. In addition, SRI has mechanically verified Schneider's clock synchronization paradigm [24] using Ehdm[25]. A further generalization was found at NASA Langley [20]. The design of a digital circuit to distribute clock values in support of fault-tolerant synchronization has been completed by SRI International and is currently being formally verified.\textsuperscript{3}

SRI is currently writing a chapter for the FAA Digital Systems Validation Handbook Volume III on formal methods[26]. The handbook provides detailed information about digital system design and validation and is used by the FAA certifiers.

\textbf{Computational Logic Inc.}

Fault-tolerant systems, although internally redundant, must deal with single-source information from the external world. For example, a flight control system is built around the notion of feedback from physical sensors such as accelerometers, position sensors, pressure sensors, etc. Although these can be replicated (and they usually are), the replicates do not produce identical results. In order to use bit-by-bit majority voting all of the computational replicates must operate on identical input data. Thus, the sensor values (the complete redundant suite) must be distributed to each processor in a manner which guarantees that all working processors receive exactly the same value even in the presence of some faulty processors. This is the classic Byzantine Generals problem [27]. CLI is investigating the formal verifica-

\textsuperscript{2}The bounded delay assumption was shown to follow from the other assumptions of the theory.

\textsuperscript{3}Unlike the NASA inhouse circuit, the SRI intent is that the convergence algorithm be implemented in software.
tion of such algorithms and their implementation. They have formally verified the original Marshall, Shostak, and Lamport version of this algorithm using the Boyer Moore theorem prover [28]. They have also implemented this algorithm down to the register-transfer level and demonstrated that it implements the mathematical algorithm [29] and then subsequently verified the design down to a hardware description language (HDL) developed at CLI [30].

CLI has reproduced the SRI verification of the interactive convergence algorithm using the Boyer-Moore theorem prover [31]. CLI has also developed a formal model of asynchronous communication and demonstrated its utility by formally verifying a widely used protocol for asynchronous communication called the bi-phase mark protocol, also known as “Bi-Φ-M,” “FM” or “single density” [32]. It is one of several protocols implemented by microcontrollers such as the Intel 82530 and is used in the Intel 82C501AD Ethernet Serial Interface.

**Odyssey Research Associates**

ORA has also been investigating the formal verification of Byzantine Generals algorithms. They have focused on the practical implementation of a Byzantine-resilient communications mechanism between Mini-Cayuga micro-processors [33, 34, 35]. The Mini-Cayuga is a small but formally verified microprocessor developed by ORA. It is a research prototype and has not been fabricated. The communications circuitry would serve as a foundation for a fault-tolerant architecture. It was designed assuming that the underlying processors were synchronized (say by a clock synchronization circuit). The issues involved with connecting the Byzantine communications circuit with a clock synchronization circuit and verifying the combination has not yet been explored.

Another task that has been started with ORA is to apply their Ada verification tools to aerospace applications. This effort consists of two subtasks. The first subtask is to verify some utility routines obtained from the NASA Goddard Space Flight Center and the NASA Lewis Research Center using their Ada Verification Tool named Penelope [36]. This subtask was accomplished in two steps: (1) a formal specification of the routines and (2) formal verification of the routines. Both steps uncovered errors in the routines [37]. The second subtask was to formally specify the mode-control panel logic of a Boeing-737 experimental aircraft system using Larch (the specification language used by Penelope) [38].

A joint project between ORA and Charles Stark Draper Laboratory (CSDL) has been initiated. The CSDL has been funded by NASA Langley to build fault-tolerant computer systems for over two decades. They have recently become interested in the use of formal methods to increase confidence in their designs. ORA has formally specified an important circuit (called the scoreboard) of the Fault-Tolerant Parallel Processor (FTPP) [39] in Caliban [40]. Work is currently underway to formally verify the circuit.

**Boeing Military Aircraft Co.**

The Boeing Company has been sponsored by NASA Langley to develop advanced validation and verification techniques for fly-by-wire systems. As part of the project, Boeing is exploring the use of formal methods. The goal of this work is two-fold: 1) technology transfer of formal methods to Boeing, and 2) assessment of formal methods technology maturity.
NASA Langley has been involved in a cooperative research partnership with Boeing to facilitate the acceptance and adoption of this high-risk, high-payoff technology by Boeing. The first step was to demonstrate that formal verification of “real” hardware devices is, in fact, feasible. The first Boeing tasks concentrated on applying the HOL hardware verification methodology to a set of hardware devices. With the assistance of a subcontract with U. C. Davis, Boeing verified a set of hardware devices, including a microprocessor[41], a floating-point coprocessor similar to the Intel 8087 but smaller[42, 43], a direct memory access (DMA) controller similar to the Intel 8237A but smaller[44], and a set of memory-management units[45, 46]. U. C. Davis also developed the generic-interpreter theory to aid in the formal specification and verification of hardware devices[47, 48, 49], and a horizontal-integration theory for composing verified devices into a system[50, 51, 52, 53].

After demonstrating the feasibility of verifying standard hardware devices, Boeing was ready to apply the methodology to a set of proprietary hardware devices being developed inhouse for use in a number of aeronautics and space applications. NASA sponsored a Boeing engineer to work with the Processor Interface Unit (PIU) design team to formally specify and verify the device. Although the NASA contract with Boeing will end in FY93, Boeing has already capitalized on the NASA program and has started their own IR&D effort to continue applying formal methods to the set of devices.

The cooperative research effort with Boeing has helped NASA Langley to assess the maturity of formal methods technology with respect to state-of-the-practice digital flight-control systems. First, Boeing was tasked to analyze the suitability of the VIPER chip for application to digital flight controls and to assess the design/verification methodology used on the VIPER[54]4. The generic-interpreter and horizontal-integration theories developed at U. C. Davis provide models to guide the specification and verification of hardware devices. Application of formal methods to the PIU has demonstrated that formal methods can be practically applied to the digital hardware devices being developed by Boeing today and has given NASA insight on how to make the process more cost effective.

Work is also progressing on a methodology for formal requirements analysis for aircraft systems[58, 59]. This work, being performed under a subcontract to California Polytechnic State University, includes development of a Wide-Spectrum Requirements Specification Language (WSRSL) and prototype tools to support the language. A set of requirements for an Advanced Subsonic Civil Transport (ASCT) developed by a Boeing engineer under previous NASA funding is being rewritten in WSRSL to demonstrate the use of the language and toolset. Since WSRSL is a formal language, the specification can be formally analyzed for syntactic correctness, completeness, and consistency. NASA Langley is currently evaluating WSRSL as a candidate requirements specification tool for the fly-by-light/power-by-wire project. Future plans include possible development of an automatic translator to Ehdm (SRI International’s theorem prover) to facilitate verification of functional correctness as well.

4NASA Langley has just completed a 3 year Memorandum of Understanding (MOU) with the U.K. Royal Signals and Radar Establishment (RSRE) in formal methods. The MOU focused on the VIPER microprocessor and the verification methodology used in its development. Computational Logic Inc. and Langley inhouse researchers also performed assessments of the VIPER project[55, 56, 57].
NASA FM Repository

An anonymous FTP account has been set up at Langley to make the research results readily available. Formal specifications, research papers, and other useful information will be stored in machine-readable form. To access this repository, one must issue the following command: "ftp airl6.larc.nasa.gov". One then supplies "anonymous" as the user name and his FTP address as the password.

Summary

Although the NASA program covers a wide-spectrum of theoretical and practical problem domains, it is strongly focused on the goal of designing a fault-tolerant reliable computing base which can support real-time control applications. Much progress has already been made in applying formal methods to critical subsystems such as clock synchronization, Byzantine agreement, voting, etc. The challenge ahead is to integrate all of these activities to accomplish a complete verification of the total RCP system and to continue the transfer of this technology to the aerospace industry.

References


[54] Levitt, Karl; and et. al.: Formal Verification of a Microcoded VIPER using HOL. to be published as a NASA CR, 1992.


Welcome and Introduction

Charles Meissner, Jr.
Head, System Validation Methods Branch
NASA Langley Research Center
WELCOME AND INTRODUCTION

FORMAL METHODS WORKSHOP
NASA LANGLEY RESEARCH CENTER
AUGUST 11-13, 1992

Charles W. Meissner, Jr.
NASA Langley Research Center

NASA ORGANIZATION
VERTICAL CUT TO SVMB
ULTRARELIABLE DIGITAL AVIONICS

CONTROL SYSTEMS BECOMING THE PRACTICAL EQUIVALENT OF PRIMARY STRUCTURE
- U.S. FAR 1309-1 Requires P(fail)<10^{-9} for statistical compliance
- Reliability can't be estimated to this level
- Experienced engineering and operational judgement used for compliance

FAULT-TOLERANT DIGITAL SYSTEMS ARE NECESSARY FOR PRACTICAL REALIZATION OF ADVANCED CONTROL
- Analog functionality insufficient for advanced control
- Analog too high in size, weight, power
- Digital system components not adequately reliable - use redundancy to increase reliability
FORMAL METHODS FOR
FLIGHT-CRITICAL SYSTEMS

• The only scientifically satisfactory approach to aspects of the
digital validation process is through reasoning.

• Formal methods may become important sooner than is
  commonly supposed in the aerospace community.

• SVMB has put an emphasis on formal methods.

• Industry/FAA focus is essential feature of our formal methods
  work.
Why Formal Methods?

Ricky Butler
System Validation Methods Branch
NASA Langley Research Center
Why Formal Methods?

by

Ricky W. Butler
NASA Langley Research Center

August 11, 1992

Outline

- The Digital Flight Control System Validation Problem
- What is Formal Methods?
- Introduction to the Formal Specification and Verification
  - code verification
  - design verification
  - hardware verification
  - formal requirements specification (phonebook example)
- Limitations of Formal Methods

A Small Sample of Aerospace Design Errors:

- F14 lost to uncontrollable spin, traced to tactical software. [SEN 9 5]
- F18: plane crashed due to missing exception condition, pilot OK. [SEN 6 2]
- AFTI-F16—Asynchronous operation, skew, and sensor noise led each channel to declare others failed in flight test 44. Flown home on a single channel. Other potentially disastrous bugs detected in flight tests 15 and 36.
- X29 bug detected by simulation after 162 “at-risk” flights. Analysis showed that the bug could have led to instability and consequent loss-of-aircraft.
- HiMAT crash landed without landing gear due to a design flaw. Traced to timing change in the software that had survived extensive testing.
Validation of Ultra-Reliable Systems

Decomposes into two sub-problems:

1. Quantification of probability of system failure due to physical failure.
2. Establishing that Design Errors are not present.

(Note. Quantification of 2. is infeasible)

Three Basic Approaches to Overcoming the Design Error Problem

- Testing (Lots of it)
- Design Diversity (i.e. Software Fault-Tolerance: N-version programming, recovery blocks, etc.)
- Fault Avoidance:
  - Formal Specification/Verification
  - Automatic Program Synthesis
  - Reusable Modules

Life Testing

Basic Observation:

$10^{-9}$ probability of failure estimate for a 1 hour mission

Requires

$> 10^9$ hours of testing

( $10^9$ hours = 114,000 years)

Design Diversity

1. Separate Design/Implementation Teams
2. Same Specification
3. Multiple Versions
4. Non-exact Threshold Voters
5. Hope design flaws manifest errors independently or nearly so.
What Enables Ultra-Reliability Quantification For Physical Failure

- The only thing that enables quantification of ultra-reliability for hardware systems with respect to physical failure is the INDEPENDENCE ASSUMPTION.
- The independence assumption has been rejected at the 99% confidence level in several experiments for low reliability software.
- The independence assumption cannot be validated for high reliability software because of the exorbitant test times required.

THUS:
- It is not possible\(^1\) to scientifically establish that design diversity achieves ultra-reliability.
- Design diversity creates an "illusion" of ultra-reliability.

\(^1\)within feasible amounts of testing time

Classical vs. Computer Systems

<table>
<thead>
<tr>
<th>Classical Systems</th>
<th>Computer Systems</th>
</tr>
</thead>
<tbody>
<tr>
<td>continuous state space</td>
<td>discrete state space</td>
</tr>
<tr>
<td>smooth transitions</td>
<td>abrupt transitions</td>
</tr>
<tr>
<td>finite testing and interpolation OK</td>
<td>finite testing inadequate, interpolation unsound</td>
</tr>
<tr>
<td>mathematical modeling</td>
<td>prototyping and testing</td>
</tr>
<tr>
<td>build to withstand additional stress</td>
<td>build to specific assumptions</td>
</tr>
<tr>
<td>predictable</td>
<td>surprising</td>
</tr>
</tbody>
</table>

Why is Software\(^1\) so Hard to get Right?

- In software, there's nothing to go wrong but the design
- Our intuition and experience is with continuous systems—but software is about discontinuous behavior
- Have to separately reason about or test millions of sequences of discrete state transitions
- And all the design complexity in modern systems is in the software (VLSI has the same characteristics as software)
- Complexity exceeds our (unaided) intellectual grasp

\(^1\)Everything said here applies to digital hardware as well
The Characteristics of Formal Methods

- Specification of system using languages based on mathematical logic
- Rigorous specification of desired properties as well as implementation details
- Mathematical proof that the implementation meets the desired abstract properties
- Use of semi-automatic theorem provers to ensure the correctness of the proofs

In principle, formal methods can accomplish the equivalent of exhaustive testing, if applied all the way from requirements to implementation.

Applied Mathematics and Engineering

- Established engineering disciplines use applied mathematics
  - As a notation for describing systems
  - As an analytical tool for calculating and predicting the behavior of systems
- Computers can provide speed and accuracy for the calculations

Applied Mathematics and Software Engineering (cont.)

- The applied mathematics of software is formal logic
- Formal Logic can provide
  - A notation for describing software designs—formal specification
  - A calculus for analyzing and predicting the behavior of systems—formal verification
- Computers can provide speed and accuracy for the calculations
Formal Logic

- Formal means “to do with form”
- Formal logic provides rules for constructing arguments that are sound because of their form, and independent of their meaning
- Example
  - That animal is a cat
  - All cats are sneaky
  - Therefore that animal is sneaky

Proof and Truth

- Logic provides rules of calculation that enable valid conclusions to be deduced from premises
- The calculation is called a proof
- If the premises are true statements about the world, then the soundness theorems of logic guarantee that the conclusion is also a true statement about the world
- Assumptions about the world made explicit, separated from rules of deduction

Formal Methods and Applied Mathematics

- Logic provides the foundation for all mathematics
- But traditional applications of mathematics have been to continuous systems, where highly developed bodies of theory (e.g., aerodynamics) remove practitioners from the elementary logical underpinnings
- But computer systems operate in a discrete domain, their operation is essentially a sequence of decisions, and each application is new
- Therefore have to develop a specific theory about each one, directly in logic

Formal Methods

Formal Specification: Use of notations derived from formal logic to describe
  - assumptions about the world in which a system will operate
  - requirements that the system is to achieve
  - a design to accomplish those requirements

Formal Verification: Use of methods from formal logic to
  - analyze specifications for certain forms of consistency, completeness
  - prove that the design will satisfy the requirements, given the assumptions
  - prove that a more detailed design implements a more abstract one
Draft Interim Defense Standard 00-55

Quote from the forward to the Draft Standard:

The Steering Group “has determined that the current approach which is based on system testing and oversight of the design process will, in the long-term, become cumbersome and inefficient for the assurance of the safety of increasingly sophisticated software”.

“The Steering Group therefore proposes the adoption of Formal Design Methods, based on rigorous mathematical principles, for the implementation of safety-critical computer software”.

Mathematics of Formal Methods

The mathematics of Formal Methods include:
- predicate calculus (1st order logic)
- recursive function theory
- lambda calculus
- programming language semantics
- discrete mathematics—number theory, abstract algebra, etc.

Levels of Formal Methods

Level 0: Static Code Analysis (No semantic analysis)
Level 1: Specification using mathematical logic or language with a formal semantics (i.e. meaning expressible in logic)
Level 2: Formal Specification + Hand Proofs
Level 3: Formal Specification + Mechanical Proofs

Higher levels of rigor provide greater confidence but at greater cost.

European emphasis: Focus on Level 1. Ahead in the transfer of this technology to industry.


Domain of Formal Methods

Degree of rigor
- rigor-moartis
- level 3
- level 2
- level 1

Completeness
(How much of the system did the pro cover?)

Phase of life-cycle
- requirements
- high-level design
- detailed design
- implementation
The Maturity of An Engineering Discipline

A good measure of the maturity of an engineering discipline is the amount and sophistication of the mathematics routinely used in the design of system within its domain.

- much of hardware design (especially design above the gate-level) is still ad-hoc.
- almost all software design is ad-hoc. Although there is a significant body of theoretical work, virtually none of it is used in the development of software today. (Exception: use of VDM and Z in Europe)

Introduction to the Formal Specification and Verification

Formal Specification Example

Ado Procedure

type ARRAY is array(POSITIVE range 0) of INTEGER;
procedure SEARCH(A: in ARRAY; N, X: in INTEGER; Y: out INTEGER);

English Specification

The procedure searches an array “A” of length “N” for a value “X”. If it finds the element, then “Y” is equal to the “index” of the array element that is equal to “X” on exit from the return. If there is no element of the array equal to “X,” then Y is equal to “0” on exit.

Formal Specification

pre-condition: N > 0
post-condition:

\[ X = A[Y] \land (1 \leq Y \leq N) \lor \{Y = 0 \land \exists k : (1 \leq k \leq N) \land A[k] \neq X]\]

With some syntactic help:

pre-condition: N > 0
post-condition: IF \{Y : 1 \leq k \leq N \land A[k] \neq X\} THEN \{Y = 0\} ELSE \{X = A[Y] \land (1 \leq Y \leq N)\}

Example of Code Verification

function Lookup(var A: array[...N] of integer; s: integer): 1..N;
var i, m, n: 1..N; label 11;
\{ (s < N) \land \text{sorted}(A) \land (A[i] \leq s < A[N])\}
begin m := 1; n := N;
\{ (m \leq n) \land \text{sorted}(A) \land (A[m] \leq s < A[n])\}
while m + 1 \leq n do
begin i := (m + n) \div 2;
\{s < A[i]\} then n := i
else if A[i] < s then m := i
also begin Lookup := i; \{A[Lookup] = s\} goto 11 end
end;
\{m + 1 = n\} \land \text{sorted}(A) \land (A[n] \leq s < A[N])\}
if A[n] \neq s then \{\exists k : (1 \leq k \leq N) \land (A[k] = s)\} goto 11
also Lookup := m;
11: end;
\{A[Lookup] = s\} \lor \{\exists k : (1 \leq k \leq N) \land (A[k] = s)\}
where \text{sorted}(A) = \forall i, j : (1 \leq i < j \leq N) \lor (A[i] < A[j])\}
Verification Conditions

1. \(\{(s < n) \land \text{sorted}(A) \land (A[s] \leq s < A[n])\}\)
   \(\supset\) \(\{(s < n) \land \text{sorted}(A) \land (A[s] \leq s < A[n])\}\)
2. \(\{A[\text{Lookup}] = s\} \supset \{A[\text{Lookup}] = s\}\)
3. \(\{(m + s = n) \land \text{sorted}(A) \land (A[m] \leq s < A[m]) \land (A[m] = n)\} \supset \{A[m] = n\}\)
4. \(\{\text{Failure}\} \supset \{\text{Failure}\}\)
5. \(\{(m + s = n) \land \text{sorted}(A) \land (A[m] \leq s < A[m]) \land (A[m] \neq n)\}
   \supset \{-\exists k(k \leq h \leq n) \land (A[k] = n)\}\)
6. \(\{(m < n) \land \text{sorted}(A) \land (A[m] \leq s < A[m]) \land (m + s < n)\}
   \land (A[m + n] \div s) \geq n \land (s \geq A[m + n] \div s)\}
   \supset \{A[m + n] \div s) = n\}
7. \(\{(m < n) \land \text{sorted}(A) \land (A[m] \leq s < A[m]) \land (m + s < n)\}
   \land (A[m + n] \div s) = n \land (s \geq A[m + n] \div s)\}
   \supset \{A[m + n] \div s) + = n\} \land \text{sorted}(A) \land (A[m + n] \div s) \leq s < A[n]\}
8. \(\{(m < n) \land \text{sorted}(A) \land (A[m] \leq s < A[m]) \land (m + s < n)\}
   \land (A[m + n] \div s) = n \land (s < A[m + n] \div s)\}
   \supset \{(m + s = (m + n) \div s) \land \text{sorted}(A) \land (A[m] \leq s < A[m + n] \div s)\}\)

Formal Verification—Hierarchical Approach

Formal program specification is very detailed.

Need abstract high-level specification.

Hierarchical Verification

PROVE: \(EXEC_1(Map(S_1(t))) = Map(EXEC_1(t), S_1(t + 1))\)
Hardware Example of a Mapping

<table>
<thead>
<tr>
<th>Macro level</th>
<th>Micro level</th>
</tr>
</thead>
<tbody>
<tr>
<td>ac pc sp mem</td>
<td>ac pc sp mem mx ir sfe</td>
</tr>
</tbody>
</table>

Map

Formal Specification of Hardware (Predicate Style)

```
Mult(i, i, a, done) = done(i) \land
Next(i, i)(done) \land
Stable(i, i)(a) \land
Stable(i, i)(a) \subseteq
\alpha(i) = i, i \times i, i
```

Where

```
Stable(i, i)(f) = \forall t. \leq t < t, \therefore f(t) = f(t)
Next(i, i)(f) = t < t, \land f(t) \land (\forall t. t < t, \therefore \neg f(t))
```

Examples of Proof Hierarchies

**MICROPROCESSOR**

- Instruction-level
- Major state machine
- Block model
- Gate-level model

**FAULT- TOLERANT O.S.**

- Single-processor view
- Synchronous replicated
- Asynchronous distributed
- Abstract h/w, s/w

Formal Specification of Hardware Implementation

Components

```
Load(d, i, o, v) = \langle \text{load}, d(i) = v(i) \rangle
Reg(i, a) = \langle \text{reg}, i(a) = a(i) \rangle
Prep(i, a) = \langle \text{prep}, i(a) = 0 \rangle
Dec(i, a) = \langle \text{dec}, i(a) = \neg a(i) \rangle
Sim(i, a) = \langle \text{sim}, i(a) = a(i) \rangle
Zero(i, a) = \langle \text{zero}, i(a) = 0 \rangle
Or(i, a) = \langle \text{or}, i(a) = \lor a(i) \rangle
```

Mult Implementation

```
Mul(i, i, a, done) =
(\forall k. k \leq k \leq k, \therefore f(k) = f(i, k)
\land \forall k. k \leq k \leq k, \therefore \neg f(k)
\land \forall k. k \leq k \leq k, \therefore \neg f(k)
\land \forall k. k \leq k \leq k, \therefore \neg f(k)
\land \forall k. k \leq k \leq k, \therefore \neg f(k)
```

35
Hardware Verification

**Mathematically Prove:**

\[ \text{Mult}(a, b, c) = \text{Mult}(a, b, c) \]

Let's prove:


\[ \text{Mark}(d, e, f, g) = \text{Rear}(a) \land \text{Add}(b, c, d) \]

\[ \text{Dec}(i, f) \land \text{Mark}(j, k, l) \land \text{Max}(d, e, f, g, h) \]

\[ \text{Neg}(i, f) \land \text{Dec}(j, k, l) \land \text{Dec}(m, n, o, p) \]

\[ \text{Zero}(e) \land \text{Max}(q, r, s, t, u) \land \text{Zero}(v, w, x, y, z) \]

\[ \text{OrGent}(b, c, d) \land \text{Flip}(e, f, g, h) \]

---

Phone Book Example

**Requirements for an Electronic Phone Book**

- Phone book shall store the phone numbers of a city.
- There shall be easy way to retrieve a phone number given a name.
- It shall be possible to add and delete entries from the phone book.

---

**Formal Requirements Specification**

- How do we represent the phone book mathematically?
  1. A set of ordered pairs of names and number. Adding and deleting entries via set addition and deletion.
  2. Function whose domain is all possible names and range is all phone numbers. Adding and deleting entries via modification of function values.
  3. Function whose domain is only names currently in phone book and range is phone numbers. Adding and deleting entries via modification of the function domain and values. (Z style)

Let's start with approach 2.

In traditional mathematical notation, we would write:

Let \( N = \) set of names

\[ P = \text{set of phone numbers} \]

**book : N \rightarrow P**

How do we indicate that we do not have a phone number for all possible names, only for names of real people?

We decide to use a special number, that could never really occur in real life, e.g. 000-0000. We don't have to specify the implemented value of this special number we can just give it a name: \( n_0 \in N \).

Now we can define an empty phone book. In traditional notation, we would write:

\[ \text{emptybook} : N \rightarrow P \]

\[ \text{emptybook}(\text{nm}) \equiv n_0 \]
Accessing an Entry

Let \( N = \text{set of names} \)
\( P = \text{set of phone numbers} \)
\( \text{book} : N \rightarrow P \)
\( n_0 \in N \)
\( B = \text{set of functions} : N \rightarrow P \)
\( \text{FindPhone} : B \times N \rightarrow P \)
\( \text{FindPhone}(bk, name) = bk(name) \)

Note that \( \text{FindPhone} \) is a higher-order function since its first argument is a function.

Specifying Adding/Deleting an Entry

Let \( N = \text{set of names} \)
\( P = \text{set of phone numbers} \)
\( \text{book} : N \rightarrow P \)
\( n_0 \in N \)
\( B = \text{set of functions} : N \rightarrow P \)
\( \text{AddPhone} : B \times N \times P \rightarrow B \)
\( \text{AddPhone}(bk, name, num)[x] = \begin{cases} bk(x) & \text{if } x \neq name \\ num & \text{if } x = name \end{cases} \)
\( \text{DelPhone} : B \times N \rightarrow B \)
\( \text{DelPhone}(bk, name)[x] = \begin{cases} bk(x) & \text{if } x \neq name \\ n_0 & \text{if } x = name \end{cases} \)

Some Realizations

- Our specification does not rule out the possibility of someone having a "\( n_0 \)" phone number
- We have not allowed multiple phone numbers per name
- Our specification does not say anything about whether or not the user should be warned if a deletion is requested on a name not in the city

HOW DO WE REMEDY THESE DEFICIENCIES?

Complete Spec

Let \( N = \text{set of names} \)
\( P = \text{set of phone numbers} \)
\( \text{book} : N \rightarrow P \)
\( n_0 \in N \)
\( B = \text{set of functions} : N \rightarrow P \)
\( \text{FindPhone} : B \times N \rightarrow P \)
\( \text{FindPhone}(bk, name) = bk(name) \)
\( \text{AddPhone} : B \times N \times P \rightarrow B \)
\( \text{AddPhone}(bk, name, num)[x] = \begin{cases} bk(x) & \text{if } x \neq name \\ num & \text{if } x = name \end{cases} \)
\( \text{DelPhone} : B \times N \rightarrow B \)
\( \text{DelPhone}(bk, name)[x] = \begin{cases} bk(x) & \text{if } x \neq name \\ n_0 & \text{if } x = name \end{cases} \)

Can test spec with some putative theorems:

LEMMATA (putative 1): \( \text{FindPhone} \circ \text{AddPhone} = \text{AddPhone} \circ \text{FindPhone} = \text{book} \)
LEMMATA (putative 2): \( \text{book}(name) = n_0 \supset \text{DelPhone} \circ \text{AddPhone} = \text{book} \)
Deficiency 1

Our specification does not rule out the possibility of someone having a \( \text{"n"} \) phone number:

**A SOLUTION:**

Let \( N \) be a set of names
\[ V = \text{\{valid, invalid\}} \]
\( P \) be a set of phone numbers
\( \mathcal{P} \) be a set of pairs \( (P, V) \)
\( \text{book} : N \rightarrow \mathcal{P} \)
\( B \) be a set of functions \( N \rightarrow \mathcal{P} \)

FindPhone : \( B \times N \rightarrow \mathcal{P} \)
FindPhone\((b, n)\) = \( b(n) \)

AddPhone : \( B \times N \times \mathcal{P} \rightarrow B \)

\[
\text{AddPhone}(b, n, p)(x) = \begin{cases} 
  b(x) & \text{if } x \neq n \\
  (\text{\small num, valid}) & \text{if } x = n 
\end{cases}
\]

DelPhone : \( B \times N \rightarrow B \)

\[
\text{DelPhone}(b, n)(x) = \begin{cases} 
  b(x) & \text{if } x \neq n \\
  (\text{\small \text{\"n\}}, \text{\small invalid}) & \text{if } x = n 
\end{cases}
\]

Deficiency 2 (cont.)

Let \( N \) be a set of names
\( P \) be a set of phone numbers
\( \text{\small book} : N \rightarrow 2^P \)
\( \mathcal{P} \) be a set of functions \( N \rightarrow 2^P \)

\[
\text{emptyBook}(n) \equiv \phi
\]

FindPhone : \( B \times N \rightarrow \mathcal{P} \)
FindPhone\((b, n)\) = \( b(n) \)

AddPhone : \( B \times N \times \mathcal{P} \rightarrow B \)

\[
\text{AddPhone}(b, n, p)(x) = \begin{cases} 
  b(x) & \text{if } x \neq n \\
  b(n) \cup \{\text{\small num}\} & \text{if } x = n 
\end{cases}
\]

DelPhone : \( B \times N \rightarrow B \)

\[
\text{DelPhone}(b, n)(x) = \begin{cases} 
  b(x) & \text{if } x \neq n \\
  \phi & \text{if } x = n 
\end{cases}
\]

Deficiency 2

We have not allowed multiple phone numbers per name: (THE REQUIREMENTS DID NOT SPECIFY WHETHER THIS IS NEEDED OR NOT)

**A SOLUTION:**

Let \( N \) be a set of names
\( P \) be a set of phone numbers
\( \text{\small book} : N \rightarrow 2^P \)
\( \mathcal{P} \) be a set of functions \( N \rightarrow 2^P \)

\[
\text{emptyP}(n) \equiv \phi
\]

FindPhone : \( B \times N \rightarrow \mathcal{P} \)
FindPhone\((b, n)\) = \( b(n) \)

AddPhone : \( B \times N \times \mathcal{P} \rightarrow B \)

\[
\text{AddPhone}(b, n, p)(x) = \begin{cases} 
  b(x) & \text{if } x \neq n \\
  b(n) \cup \{\text{\small num}\} & \text{if } x = n 
\end{cases}
\]

DelPhone : \( B \times N \rightarrow B \)

\[
\text{DelPhone}(b, n)(x) = \begin{cases} 
  b(x) & \text{if } x \neq n \\
  \phi & \text{if } x = n 
\end{cases}
\]

Deficiency 2 (cont. again)

We notice that the function \( \text{DelPhone} \) deletes all of the phone numbers associated with a name. Should the system be able to just remove one phone number associated with the name? (REQUIREMENTS DID NOT COVER THIS SITUATION EITHER.) If so, we must define an additional function:

\[
\text{DelPhoneNum} : B \times N \times \mathcal{P} \rightarrow B
\]

\[
\text{DelPhoneNum}(b, n, p)(x) = \begin{cases} 
  b(x) & \text{if } x \neq n \\
  b(n) \setminus \{\text{\small num}\} & \text{if } x = n 
\end{cases}
\]

\[
\text{DelPhoneNum}(b, n, p)(x) = \begin{cases} 
  b(x) & \text{if } x \neq n \\
  \phi & \text{if } x = n 
\end{cases}
\]
Some Observations

- Our specification is abstract. The functions are defined over infinite domains.
- As one translates the requirements into mathematics, many things that are usually left out of English specifications are explicitly enumerated.
- The formal process exposes ambiguities and deficiencies in the requirements. Must chose between

\[ \text{book} : N \rightarrow P \]
\[ \text{book} : N \rightarrow \mathbb{N} \]

- Putative theorem proving and scrutiny reveals deficiencies in the formal specification.

PVS Spec of Phonebook Example

```
phonebook: THEORY
BEGIN

name: TYPE
name0: name
ph_number: TYPE
null_number: ph_number
book: TYPE = [name \rightarrow ph_number]

nm: VAR name
emptybook(nm): ph_number = null_number
bk: VAR book
FindPhone(bk, nm): ph_number = bk(nm)

num: VAR ph_number
AddPhone(bk, nm, num): book = bk WITH [nm := num]
DelPhone(bk, nm): book = bk WITH [nm := null_number]

END phonebook
```

Z Approach

```
Phonebook:
   known: P NAME
   phone: NAME \rightarrow PHONE

    known = dom phone

AddPhone:
   name?: NAME
   number?: PHONE

    name? \& known
    phone' = phone U \{ name? \rightarrow number? \}
```

Revised Requirements

Original Requirements
- phone book shall store the phone numbers of a city
- There shall be easy way to retrieve a phone number given a name
- It shall be possible to add and delete entries from the phone book

Revised Requirements
- For each name in the city, a set of phone numbers shall be stored (SHOULD WE LIMIT THE NUMBER?)
- There shall be easy way to retrieve the phone numbers given a name
- It shall be possible to add a new name and phone number.
- It shall be possible to add new phone numbers to an existing name.
- It shall be possible to delete a name
- It shall be possible to delete one of several phone numbers associated with a name.
- the user shall be warned if a deletion is requested on a name not in the city
- the user shall be warned if a deletion of a non-existent phone number is requested
Some More Observations

- There are many different ways to formally specify.
- No matter what representation you chose you are making some decisions that bias the implementation.
- The goal is to minimize this bias and yet be complete.
- The process of formalizing the requirements can reveal problems and deficiencies and lead to a better English requirements document as well.

Limitations of Formal Methods

Myth
A formally verified system will be perfect.

Reality
Formal verification finds bugs other methods can’t reach.

(But other methods (e.g. testing) find bugs outside of the scope of formal verification)

The bottom line
Any validation is only as good as the model.
Simulators use operational models.
Formal verification can also use axiomatic models.
What Makes a Technique a “Formal Method?”

FORMAL METHOD = LOGIC + CS language concepts

Important Attributes:
- logic based (e.g. ∀,∃, ⊃ stuff)
- CS language concepts (e.g. data types, module-structure, generics)
- should be able to express what is done without saying how it is done (i.e. non-procedural)
- formal semantics
- feasible to build useful tools which support analysis

Expressibility Vs. Proving Efficiency

There is a trade-off between the expressiveness of the specification language and the difficulty of building a theorem prover.

- propositional calculus (truth table is a decision procedure)
- predicate calculus (semi-decidable via resolution)
- recursive function theory (undecidable)
- higher order logic (undecidable)

<table>
<thead>
<tr>
<th>restricted logic</th>
<th>automated proving</th>
<th>expression logic</th>
<th>proof checking</th>
</tr>
</thead>
<tbody>
<tr>
<td>Boyer, Moore, Heine, Holz, Califano</td>
<td>ETPS</td>
<td>HOL, PVS</td>
<td></td>
</tr>
</tbody>
</table>

* no theorem prover available
Tutorial
Design Specification Techniques

Ben DiVito
ViGYAN
Tutorial on Design Specification Techniques

Ben L. Di Vito
VIGYAN, Inc.
30 Research Drive
Hampton, VA 23666
August 11, 1992

Outline

- Formal specification concepts
- Statement of example problem
- Definition of system state
- State invariant
- Operation specifications
- Maintaining the invariant
- Specification properties
- Hierarchical specification and verification

Formal Specification Concepts

Requirements specification or high level design for many classes of (sub)systems can be represented using state machine models:

- We introduce an abstract representation of system state
  - It may require building up a suitable collection of type definitions
  - Additional types, constants, and functions are introduced as needed to support subsequent formalization
- We specify a set of operations or system services that can be invoked by users of the system across an appropriate interface
  - Operations may have input and output parameters
  - Operations may cause the system state to be updated
  - Operations may have pre-conditions that must be satisfied for legitimate invocation
  - Operations have post-conditions that express the net effect of executing or performing the operation

Specification Concepts (Cont'd)

- We may attach an invariant to the system state to formalise our notions of well-definedness
- Operations should be shown to maintain the invariant after every invocation
- Desired properties may be expressed as predicates involving the system state and operations, and proved as positive theorems that follow from the formalization
- The formal specification may be used as one layer of a hierarchical specification and verification structure
Statement of Example Problem

We wish to specify an automated airline seat assignment system that meets the following requirements:

1. The system shall execute seat assignment transactions for any scheduled airline flight on behalf of passengers or their agents.
2. The system shall establish and maintain a centralised database of seat assignments.
3. The system shall support a fleet having different aircraft types.
4. Seats shall be assigned to individual passengers in order of arrival.
5. Passengers shall be allowed to specify preferences for seat type (e.g., window or aisle).
6. Seats shall be filled in front-to-back, left-to-right order.
7. Rows and seats shall be designated using a numeric index (one-based).
8. The system shall provide the following operations or transactions:
   - Make a new seat assignment
   - Cancel an existing seat assignment

Definition of System State

For each flight $f$ in the system database, we record a set of seat assignments:

- Each seat assignment is a triple $(r, s, p)$ for row $r$, seat $s$, and passenger $p$.
- The system state is a mapping from flight identifier into that flight's current set of seat assignments
- Initially, each flight has no assignments

```
seat_assignment: TYPE = RECORD row: row, seat: seat, pass: passenger END
flight_assignments: TYPE = set[seat_assignment]
assign_state: TYPE = function[flight -> flight_assignments]
initial_state: function[flight -> flight_assignments] =
   (LAMBDA flt: emptyset[seat_assignment])
```

Basic Type Declarations

FROM type declarations of our basic data items:

- row: nat
  (* Max number of rows *)
- seats: nat
  (* Max number of seats per row *)
- n: VAR nat
- row: TYPE FROM nat WITH (LAMBDA n: 1 <= n AND n <= rows)
- seat: TYPE FROM nat WITH (LAMBDA n: 1 <= n AND n <= seats)
- flight: TYPE
  (* Flight identifier/descriptor *)
- plane: TYPE
  (* Aircraft type *)
- preference: TYPE
  (* Seat preference *)
- passenger: TYPE
  (* Passenger identifier *)

Aircraft Seat Layout

We assume a simple two-dimensional representation for airplane seating:

- Accommodates a maximum number of rows and seats per row
- Requires us to indicate whether a (row, seat) pair exists for a given aircraft type
Support Functions

We assume several uninterpreted functions to answer questions about our aircraft:

- seat_exists: function[plane, row, seat -> bool]
- meets_pref: function[plane, row, seat, preference -> bool]
- aircraft: function[flight -> plane]

We need to express the condition that there are no available seats up to the point (r,s) in the aircraft meeting the passenger's preference:

$$\forall tt, ss: tt \leq r \land ss \leq s \land \text{meets}_p(\text{aircraft}(flit), tt, ss, pr) \Rightarrow \exists a: a \in \text{air}(flit) \land a.\text{row} = tt \land a.\text{seat} = ss$$

- pref_filled: function[assem_state, flight, row, seat, preference -> bool] =
  
  $$(\text{LAMBDA} aa, flt, r, s, pr:/ $$
  
  $$(\text{FORALL} tt, ss: tt \leq r \land ss \leq s \land \text{meets}_p(\text{aircraft}(flit), tt, ss, pr) \Rightarrow$$
  
  $$\exists a: a \in \text{air}(flit) \land a.\text{row} = tt \land a.\text{seat} = ss)$$

Specifying Operations

Our method of formally specifying operations is based on a relational technique:

- We use a relation to express the post-condition under which a state transition is allowable.
- The predicate relates the value of system state before the operation is invoked to the value of system state after invocation.
- The condition only constrains allowable behavior; it does not prescribe it.

If S_i and S_f are the state values before and after executing the operation, then the relations representing post-conditions have the form:

$$\text{operation_spec}(P_1, \ldots, P_n, S_i, S_f)$$

where $P_1, \ldots, P_n$ denote the parameters at the operation interface (additional conventions are needed for return values, exceptions, etc.)

State Invariant

The system state is subject to two types of anomalies:

1. Assigning nonexistent seats to passengers
2. Assigning multiple seats to a single passenger

Prevention of (1) can be formalized as follows:

$$\forall a, flit: e \in \text{air}(flit) \Rightarrow \exists \text{seat_exists}(\text{aircraft}(flit), a.\text{row}, a.\text{seat})$$

- existence: function[assem_state -> bool] =
  
  $$(\text{LAMBDA} aa: (\text{FORALL} a, flt: \text{member}(a, as(flit)) \text{IMPLIES}$$
  
  $$\text{seat_exists}(\text{aircraft}(flit), a.\text{row}, a.\text{seat}))$$

Prevention of (2) can be formalized as follows:

$$\forall a, b, flit: a \in \text{air}(flit) \land b \in \text{air}(flit) \land a.\text{pass} = b.\text{pass} \Rightarrow a = b$$

- uniqueness: function[assem_state -> bool] =
  
  $$(\text{LAMBDA} aa: (\text{FORALL} a, b, flit:$$
  
  $$\text{member}(a, as(flit)) \text{AND member}(b, as(flit))$$
  
  $$\text{AND a.\text{pass} = b.\text{pass} IMPLIES a = b})$$

The overall state invariant is the conjunction of the two:

- assem_invariant: function[assem_state -> bool] =
  
  $$(\text{LAMBDA} aa: \text{existence}(aa) \text{AND uniqueness}(aa))$$

Seat Assignment Operations

The first operation is cancel_asn[flit, pass], which cancels the seat assignment for passenger pass on flight flit:

- cancel_asn: function[flight, passenger, assem_state, assem_state -> bool] =
  
  $$(\text{LAMBDA} fit, pass, S1, S2:$
  
  $$(\text{FORALL} f: \text{IF } f = fit$$
  
  $$(\text{THEN} (\text{FORALL} a: \text{member}(a, S2(f))) \text{IFF}$$
  
  $$\text{member}(a, S1(f)) \text{AND a.\text{pass} /= pass})$$
  
  $$\text{ELSE } S2(f) = S1(f))$$

The specification is split into two cases:

1. All seat assignment sets for flights other than flit are unchanged.
2. For flight flit, all assignments on behalf of passenger pass are removed (there should be at most one).
Seat Assignment Operations (Cont'd)

The second operation is make_assn(flt, pass, pref), which makes a seat assignment, if possible, for passenger pass on flight flt, returning a boolean value indicating whether a seat was available:

\[
\text{make\_assn: function(fl, p, pref, as, avail) = (LAMBDA flt, pass, pref, S1, S2, avail: IF pref\_filled(S1, flt, rows, seats, pref) THEN avail = false AND S2 = S1 ELSE avail = true AND (EXISTS r, s: (LET a := (REC row := r, seat := s, pass := pass) IN S2 = S1 WITH ((flt) := add(a, S1((flt))))) AND seat\_exists(aircraft(flt), r, s) AND NOT pref\_filled(S1, flt, r, s, pref) AND pref\_filled(S2, flt, r, s, pref)))}
\]

The specification is again split into two cases:
1. If no seats are available meeting the passenger's preference, no assignment is made and the state remains unchanged.
2. Otherwise, an assignment is made by adding a triple for the first seat satisfying the stated preference to the assignment set for flight flt.

Maintaining the Invariant

To establish that the state invariant is preserved by every operation, we must prove two theorems of the form:

\[I(S_0) \land \text{op\_spec(...) } \implies I(S_1)\]

where \(S_0\) and \(S_1\) are the before and after values of system state, and \(\text{op}\) represents the system operation.

For our example, the required theorems can be expressed as follows:

**cancel\_assn\_inv:** LEMMA \(\text{assn\_invariant}(S_1) \land \text{cancel\_assn}(fl, p, S_1) \implies \text{assn\_invariant}(S_2)\)

**make\_assn\_inv:** LEMMA \(\text{assn\_invariant}(S_1) \land \text{make\_assn}(fl, p, pref, S_1, S_2, avail) \implies \text{assn\_invariant}(S_2)\)

Proof that First Operation Maintains Invariant

We sketch below a proof that the cancel\_assn operation maintains the state invariant assn\_invariant.

1. We begin with the original conjecture:
   \(\text{assn\_invariant}(S_1) \land \text{cancel\_assn}(fl, p, S_1, S_2) \implies \text{assn\_invariant}(S_2)\)

2. Next, we expand the invariant predicate and split into two cases. First, we prove the existence case.

   \(\text{existence}(S_1) \land \text{cancel\_assn}(fl, p, S_1, S_2) \implies \text{existence}(S_2)\)

3. Expanding the predicates yields:

   \((\forall a, fl: a \in S_1(fl) \Rightarrow \text{seat\_exists(aircraft(fl), a, row, a, seat)}) \land (\forall f: IF f = fl \Rightarrow (\forall a: a \in S_1(fl) IFF (a \in S_1(fl) \land a, pass \neq pass)))) \land (\forall f: S_1(fl) = S_1(fl))\)

   \(\therefore (\forall a, fl: a \in S_2(fl) \Rightarrow \text{seat\_exists(aircraft(fl), a, row, a, seat)})\)

Proof (Cont'd)

4. Consider two cases. If \(f \neq fl\), then \(S_2(fl) = S_1(fl)\) and hence \(a \in S_2(fl)\) is equivalent to \(a \in S_1(fl)\) from which the conclusion follows. Otherwise, we obtain:

   \((\forall a, fl: a \in S_1(fl) \Rightarrow \text{seat\_exists(aircraft(fl), a, row, a, seat)}) \land (\forall a, fl: (a \in S_1(fl) \land a, pass \neq pass) \Rightarrow \text{seat\_exists(aircraft(fl), a, row, a, seat)})\)

5. After rewriting to the form:

   \((a \in S_1(fl) \land a, pass \neq pass) \land (a \in S_1(fl) \Rightarrow \text{seat\_exists(aircraft(fl), a, row, a, seat)})\)

   \(\therefore \text{seat\_exists(aircraft(fl), a, row, a, seat)}\)

   we see that the conclusion follows.

6. Returning to the uniqueness case, we must establish:

   \(\text{uniqueness}(S_1) \land \text{cancel\_assn}(fl, p, S_1, S_2) \implies \text{uniqueness}(S_2)\)
Proof (Cont'd)

7. This produces:

\[(\forall a, b, flt : a \in S(flt) \land b \in S(flt) \land a.pas = b.pas \supset a = b) \land\]

\[(\forall f : \text{flt}, \text{flt} = flt \]

\[\text{THEN} (\forall a : a \in S(flt) \land F \{a \in S(flt) \land a.pas \neq \text{pass}\})\]

\[\text{ELSE } S(a[f]) = S(t[f]\}

\[\supset \]

\[\forall a, b, flt : a \in S(flt) \land b \in S(flt) \land a.pas = b.pas \supset a = b\]

8. Again, consider two cases. If \(j \neq \text{flt}\), then \(S(a[f]) = S(t[j])\) and hence \(a \in S(a[f])\) is equivalent to \(a \in S(t[j])\) and \(b \in S(a[f])\) is equivalent to \(b \in S(t[j])\), from which the conclusion follows. Otherwise, we obtain:

\[(\forall a, b, flt : a \in S(flt) \land b \in S(flt) \land a.pas = b.pas \supset a = b)\]

\[\supset \]

\[\forall a, b, flt : (a \in S(flt) \land a.pas \neq \text{pass}) \land (b \in S(flt) \land b.pas \neq \text{pass}) \land a.pas = b.pas \supset a = b)\]

9. Simplifying as before will establish that \(a = b\).

Q.E.D.

Hierarchical Specification and Verification

- We have specified only one layer of design in a hierarchy
- A next step might be to refine the specification into a more detailed, lower level description, e.g., in terms of more concrete data structures and operations.
- It would then be possible to prove that the lower level specification correctly implements the upper level one.
- Such an activity would constitute a design proof.
- This can be carried out across several layers of a design hierarchy.
- The process may stop at some point because further refinement of the formalism is no longer cost-effective, but the high level specifications and proofs are still valuable.

System Properties

Usually there are several types of system properties that are of interest to formalize and prove:

1. Properties about critical system operation derived from high level requirements.

2. Partial theorems used to confirm our understanding of the specified system.

An example of (2) is the property that if the system is in state \(S_1\), and we make a new assignment and then immediately cancel it, we should return to the same system state:

\[
\text{make-cancel: Lemma make-assn(flt, pass, pref, S1, S2, avail)} \]

\[\text{AND cancel-assn(flt, pass, S2, S3)}\]

\[\text{IMPLIES S1 = S3}\]

Summary

A simple design problem was postulated and formally specified using ENDM.

- System state and supporting types formalized.
- State invariant formalized.
- Operations specified.
- Operations shown to maintain state invariant.
- Hierarchical specification techniques outlined.
Tutorial
Code Verification Techniques

C. Michael Holloway
System Validation Methods Branch
NASA Langley Research Center
Tutorial on Code Verification Techniques

C. Michael Holloway
NASA Langley Research Center
11 August 1992

Outline

• Some benefits of formal code verification
• The general method for verifying code
• A specific example verification
• How the process is mechanized

Formal Code Verification

Formal methods allow us to address the code correctness problem analytically instead of empirically:

• Software systems are treated as as mathematical objects, which allows reasoning about them
• Specifications are expressed precisely in an unambiguous notation
• Proofs are constructed to demonstrate that specifications are met for all values of input domain
• Proof method replaces test cases by a static analysis – theoretically achieves the effect of exhaustive testing.
• Proofs are not limited to functional correctness: any system property (for example, safety or security) that can be specified can also be proved.

Method of Proof

1. Introduce assertions to characterize key program states.
2. Analyze execution path structure – path begins and ends with assertions.
3. Show that if each path begins with its initial assertion true, and execution reaches the end of the path, its final assertion is true.

\{
\text{Initial assertion}
\} \\
\land \text{Conditions under which path taken} \\
\implies \\
\text{Final assertion under variable substitutions due to assignments}
Method of Proof (continued)

- The method of inductive assertions requires that each loop is cut by a loop invariant — achieves proof by induction.

Software Example: Linear Search

English Specification

The function searches an integer array "A" looking for a value "x". If the value is found, then the function returns the index of the array element that is equal to "x"; otherwise the function returns "0".

Software Example: Linear Search

Formal Specification

Let y denote the function return value:

**Pre-condition:** |A| ≥ 0

**Post-condition:**

\[ (1 \leq y \leq |A|) \land x = A[y] \land (\forall k (1 \leq k < y) \lor A[k] \neq x)) \lor (y = 0 \land (\forall k (1 \leq k \leq |A|) \lor A[k] \neq x)) \]

Software Example: Linear Search

Ada Code

```ada
type GENERAL_INT_ARRAY is ARRAY(POSITIVE range <>) of INTEGER;
subtype INT_ARRAY is GENERAL_INT_ARRAY(1 .. SIZE);

function LSEARCH (A: INT_ARRAY; x: INTEGER) return INTEGER is
    I: INTEGER := 1;
begnin
    while (I <= A'LENGTH) loop
        if (x = A(I)) then
            I := I + 1;
        else
            return I;
        end if;
    end loop;
return 0;
end LSEARCH;
```
Execution Path Analysis

The following paths must be considered:

1. A → C: Never entering the loop
2. A → B: Initial entry into loop
3. B → D: Exit from loop because item is found
4. B → C: Exit from loop because i > |A| (item not found)
5. B → B: Another iteration through the loop

Verification Conditions and Proof (continued)

Path 4
\[ 1 \leq i \leq |A| \land (\forall k \ (1 \leq k < i) \land \forall k \neq x) \land x \neq \forall k \land i + 1 > |A| \]
\[ 0 = 0 \land (\forall k \ (1 \leq k \leq |A|) \land \forall k \neq x) \]
    simplifying yields
\[ i = |A| \land (\forall k \ (1 \leq k \leq |A|) \land \forall k \neq x) \]
\[ \forall k \ (1 \leq k \leq |A|) \land \forall k \neq x \]

Path 5
\[ 1 \leq i \leq |A| \land (\forall k \ (1 \leq k < i) \land \forall k \neq x) \land x \neq \forall k \land i + 1 \leq |A| \]
\[ 1 \leq i + 1 \leq |A| \land (\forall k \ (1 \leq k < i + 1) \land \forall k \neq x) \]

Q.E.D.
Notes on the Proof

- We have shown partial correctness: for all input values that meet the pre-condition, the function returns the correct value if it terminates.
- We have not shown total correctness: that the function is partially correct and that it terminates.
- Demonstrating termination is a separate issue, which requires a slightly different proof technique.
- For the example program, showing termination informally is simple.

Mechanizing the Process

- Machine-readable specification languages are widely available.
- Verification condition generation is readily automated.
- Assertions must be supplied by human analyst.
- Correctness problem converted to theorem proving problem.
- Theorem proving is partially automated.

Mechanizing the Process (continued)

- Important trade-offs exist.
  - Specification languages/logics should be expressive to allow formalization of realistic problems.
  - More expressive languages complicate and slow down mechanical theorem proving.

Mechanical Theorem Provers

- Provide more reliable proofs than hand methods.
  - Theorems shallow but numerous.
  - Contain substantial detail, much of it irrelevant.
- Provide benefits of automation.
  - Discovering proofs.
  - Storing and replaying proofs.
  - Accumulating deductive knowledge.
Mechanical Theorem Provers (continued)

- Two general types
  - Automatic: Attempt proofs without human intervention (expensive in machine resources)
  - Interactive: Require user direction in proof process (expensive in human resources)
- Primary limitation is provers' lack of "education"

Concluding Remarks

- We have discussed the basic ideas of code verification
  - Possible benefits
  - Simple example
  - Mechanization
- You will not hear much more about code verification during this workshop
The FAA DFCS Handbook
Formal Methods Chapter

John Rushby
SRI International
How Airplanes Get Certified

- The certification authority establishes the certification basis in consultation with the applicant
- Certification basis is the baseline of regulations with which the applicant must show compliance
- If existing regulations are not adequate, may apply special conditions for new and novel technologies and methods
- Applicant proposes Means Of Compliance (MOC) and associated Plan for Software Aspects of Certification

How Airplanes Get Certified (ctd)

- Based on System Safety Assessment and other lifecycle data, certification authority reports any problems with MOC; iterate until satisfied
- Certification authority determines that system, including software, complies with certification basis; done by evaluating lifecycle processes and products against the Plan; evaluations may occur at any time during lifecycle; may involve on-site evaluations, witnessing of lifecycle processes
DO-178B (ED-12)

- "Software Considerations in Airborne Systems and Equipment Certification" (Draft 6)
- Major revision to DO-178A
- Produced by Requirements and Technical Concepts for Aviation and EUROCAE WG-12
- Industry-accepted guidelines for meeting certification requirements
- Based on very formalized software development process; extensive documentation, reviews and analyses of the products of each lifecycle process
- Formal methods included among "alternative methods"

FAA Formal Methods Chapter

- A chapter on Formal Methods for the FAA Digital Systems Validation Handbook (a guide to certifiers)
- Sponsored by FAA Technical Center, Atlantic City
- Explains technical basis for formal methods
- Their use in specification and verification of software and hardware requirements, designs, and implementations
- Identifies benefits, weaknesses, difficulties
- Suggests factors for consideration when formal methods are offered in support of certification (cf. DO-178B)

FAA Formal Methods Chapter

- The chapter is not
  - A primer on formal methods
  - A prescription for using formal methods (cf. UK 00-55 or US "Orange Book" for Computer Security)
  - An endorsement of specific methods or tools
  - Finished (but is very nearly so)

- The chapter is
  - A very detailed exposition of issues in application of formal methods to critical systems
  - Addressed to an audience wider than certifiers (developers, managers, engineers)

Appendices

- Introduction to formal logic (up through set theory and higher-order logic)
- Examples
  - Code verification (square root)
  - Hardware verification (full adder)
  - Abstract data type and its implementation (stack)
  - Design-level modelization (library)
  - Algorithm (Oral Messages algorithm for Interactive Consistency)
Extent of Application of Formal Methods

- Cannot (and need not) apply formal methods everywhere

- Four axes of selectivity:
  - Components
  - Properties
  - Lifecycle phases
  - Levels of rigor

Selected System Properties

- May not need to verify all functional properties

- Often, absence of specific malfunctions is most important property

- May be able to deal with these by fault-tree analyses and other techniques derived from system safety engineering; these can be done formally, but are different from conventional formal methods

Selected System Components

- Hazard analysis, system failure severity, and software criticality levels
- FAA failure effect severities: catastrophic (10^{-9} per hour), hazardous/severe-major, major, minor, no effect
- Must consider malfunction and unintended function as well as loss of function
- DO-178B assigns software criticality levels A through E according to maximum failure severity
- May be able to lower criticality levels of large bodies of software by providing components that limit consequences of failure
  - Partitioning (fault containment)
  - Monitoring
  - Centralized redundancy management

Lifecycle Phases

- Pros and cons of applying formal methods in early and late lifecycle phases

- Late lifecycle
  - Pro: That's what runs
  - Con: Size of description is large; must often leave purely functional world of ordinary logic (i.e., need VCGs, Hoare sentences); traditional methods are very effective

- Early lifecycle
  - Pro: That's where the serious errors are; that's where the concern is; few other rigorous techniques available
  - Con: Front-loads development time and cost
Validation of Specifications

- How do you gain confidence that your specifications are right?
- Internal consistency
  - Strong typechecking
  - Definitional principle
  - Exhibition of models
  - Modules and parameters
- External fidelity
  - Review
  - Analysis ("challenges")

Levels of Formal Methods

0. No use of formal methods

1. Use the ideas of formal methods, but ad-hoc notation, proofs based on informal argument, tools are pencil and eraser (the way conventional mathematics is done)

2. Formalize and maybe mechanize specification language and methodology, retain pencil and eraser for proofs

3. Full mechanization with automated theorem proving or checking

Benefits of Formal Methods

- Precise, unambiguous specifications, force early attention to detail
- Notions of completeness
- Ability to do validation early in lifecycle
- Proofs reveal assumptions
- And errors—tool of discovery, not just of certification
- Lead to improved understanding of possible system behaviors; allow it to be documented
- Guarantees?

Fallibilities of Formal Methods

- Naur's position
- DeMillo, Lipton and Perlis' position
- Fetzer's position
Formal Methods and Tools

- Traditions and styles of tools
- Design issues and tradeoffs
- Language issues
- Support for theorem proving lifecycle
- Soundness

Some Successful Applications of Formal Methods

- CICS
- Tektronix
- SACEM
- Secure systems

Formal Methods and Certification

- The impossibility of quantification
- "Engineering judgment" relies on confident understanding of all possible system behaviors: formal methods allows you write that understanding down and subject it to analysis
- Formal methods expand design space for "confident understanding"
- Relation to "Design For Validation"
- Commentary on DO-178B (formal methods allow analysis to replace or supplement reviews)

Summary

- Not an introduction to formal methods
- A comprehensive, detailed, but accessible discussion of issues concerning formal methods in support of critical systems certification
- Reasonably nonpartisan
- Should be of use to developers as well as certifiers, and to other domains than aircraft
- Available for review in a couple of weeks
Survey of State-of-Practice
Formal Methods in Industry

Dan Craigan
ORA Canada
Overview of Presentation

Survey of State-of-Practice: Formal Methods in Industry

Dan Craigen
ORA Canada
dan@ora.on.ca

NASA Langley, Virginia
11 August 1992

Purpose, sponsors and researchers

- To provide an authoritative record on the practical experience to date.

- To better inform industry and government bodies developing standards and regulations.

- To provide pointers to future research and technology transfer needs.

- Value added: Case studies and analysis.

Purpose, sponsors and researchers

- AECB, NIST, NRL.

- Dan Craigen, Susan Gerhart, Ted Ralston.
Method for Conducting Survey Process

• Initial questionnaire.
• Literature review.
• Structured interviews (Second questionnaire).
• Raw notes, case report, review.
• Review committee.

Method for Conducting Survey Questionnaires

• Initial questionnaire and structured interview.
• Literature review.
• Structured interviews (Second questionnaire).
• Raw notes, case report, review.
• Review committee.

Method for Conducting Survey Analytic framework

• Product features.
• Process features.
• FM R&D summary.
• Key events and timing.

Method for Conducting Survey Product Features

• Client satisfaction.
• Cost.
• Impact of product.
• Quality.
• Time-to-market.
Method for Conducting Survey

Process Features

- Cost.
- Impact of process.
- Pedagogical.
- Tools.
- Design.
- Developing reusable components.
- Using existing reusable components.
- Maintainability.
- Requirements capture.
- V&V.

FM R&D Summary

- Methods: specification; design and implementation; validation and verification. [uses]
- Tools: language processors; automated reasoning; other tools. [tools]
- Recommendations to FM community. [needs]

Method for Conducting Survey

Key Events and Timing

- Starter.
- Booster.
- Status.
Cases: An Overview

- **CASE**
  - SSADM toolset; commercial; Z.
  - 340pgs Z/English; 550 schemas; 37KLOC obj. C; 16.5 lines/day

- **CICS**
  - Transaction processing; commercial; Z; PS/2 tools.
  - 268KLOC new/modified code;
    50KLOC traced to Z specs;
    9% improvement in cost;
    60% reduction in APARS.

Cases: An Overview

- **LaCoS**
  - Engine management and a distributed controller; ESPRIT and commercial;
    Raise [Method].

- **Multinet Gateway**
  - Network security; NCSC; GVE, etc.
  - 10pgs math; 80pgs Gypsy; 6KLOC OS.

- **SACEM**
  - Automatic train protection system; safety critical and RER; B, Hoare triples; B tool.
  - 9KLOC verified code; Total of 315,000 person hours.

Cases: An Overview

- **Cleanroom**
  - COBOL structuring and Attitude control; commercial and government;
    functional specs. and testing. [Method]
  - 80KLOC; (20KLOC reused; 18KLOC changed; 34KLOC new)
  - 34 lines/day; error rate of 3.4/KLOC (1/20th industry average).

- **Darlington**
  - Shutdown system; regulatory; A-7 style and program function tables.

  - SDS1: 1362LOC Fortran; 1185LOC Assembler
  - SDS2: 13KLOC Pascal (??).

Cases: An Overview

- **TBACS**
  - Smartcard security application; security; FDM.
  - 300 lines of FDM; 2500lines of C.

- **Tektronix (oscilloscope)**
  - Reusable software architecture; commercial;
    Z; Fuzz.
  - 200KLOC of code; 15pgs of Z specs (twice).

- **TCAS**
  - CAS Logic and surveillance; regulatory; state charts with DNF tables.
  - 7KLOC of pseudocode; specs about the same size.
Cases: An Overview

- Transputer
  - T-800 FPU, VCP; commercial; Z, HOL, mathematics.
  - FPU: 100pgs Z; 4KLOC Occam; VCP about $10^6$ states.

- HP-AIB
  - real-time data-base; commercial; HP-SL.
  - 55pgs HP-SL; 1290 lines of spec and design; 4390 lines of code.

Example case: TCAS

- Traffic Alert and Collision Avoidance System.
- TCAS I, II, III.
- Grand Canyon collision.
- Time span from early 80s. Leveson in June 1990.

TCAS

- Players: RTCA Inc. (SC 147), FAA, UC Irvine, Mitre, Lincoln Labs.
- Interview profile: Leveson, Nivert, Lubkowski, White.
- CAS Logic and surveillance system.
- 7 KLOC pseudocode.
- 700 pages English description. [Terminated]
- Loss of intellectual control.

- FM for safety analysis. [model checking and automated deduction]
- Statecharts.
- DNF tables for conditions.
- Iteration on notation.
- Strong support from SC 147 and industry.
- Currently at IV&V [15 yrs over 8 months].
**Product features**

<table>
<thead>
<tr>
<th>Feature</th>
<th>Rating</th>
</tr>
</thead>
<tbody>
<tr>
<td>Client satisfaction</td>
<td>n/a</td>
</tr>
<tr>
<td>Cost</td>
<td>n/a</td>
</tr>
<tr>
<td>Impact of product</td>
<td>n/a</td>
</tr>
<tr>
<td>Quality</td>
<td>n/a</td>
</tr>
<tr>
<td>Time to market</td>
<td>n/a</td>
</tr>
</tbody>
</table>

**General process features**

<table>
<thead>
<tr>
<th>Feature</th>
<th>Rating</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cost</td>
<td>n/a</td>
</tr>
<tr>
<td>Impact of process</td>
<td>+</td>
</tr>
<tr>
<td>Pedagogical</td>
<td>+</td>
</tr>
<tr>
<td>Tools</td>
<td>n/a</td>
</tr>
</tbody>
</table>

**Specific process features**

<table>
<thead>
<tr>
<th>Feature</th>
<th>Rating</th>
</tr>
</thead>
<tbody>
<tr>
<td>Design</td>
<td>+</td>
</tr>
<tr>
<td>Developing r. comp.</td>
<td>n/a</td>
</tr>
<tr>
<td>Reusing r. comp.</td>
<td>n/a</td>
</tr>
<tr>
<td>Maintainability</td>
<td>n/a</td>
</tr>
<tr>
<td>Reqs. capture</td>
<td>+</td>
</tr>
<tr>
<td>V&amp;V</td>
<td>n/a</td>
</tr>
</tbody>
</table>

---

**TCAS (Key Events)**

- **Starter**: FAA seeking better reqts. for deployed and troublesome system; Leveson looking for demo project.

- **Booster**: SC 147 willing to accept new approach; Readable notation.

- **Status**: CAS Logic formalism and pseudocode in IV&V. Surveillance logic current.

---

**TCAS (R&D)**

- **Tools**: LaTeX.

- **Needs**:
  - Safety analysis tool.
  - Automated deduction and model checking.
  - Well-formedness checker.
  - Foundational issues.

- **Conclusions**: successful transition and application.
Tools (Usage)

- CASE (SSADM): Prototype Z parser and type-checker.
- CICS: PS/2 based toolsuite w/ editor, type-checker, semantic analyser (Z).
- Cleanroom: Editors, waste paper basket.
- Darlington: Microsoft Excel.
- LaCoS: Raise toolset.
- Multinet: GVE, Extractor.

Tools (Needs)

- CASE (SSADM): schema expander, enhanced editor, browsing and X-ref.
- CICS: schema expander, semantic analyzer (for all Z), configuration management.
- Cleanroom: Extracting and tracking verification events.
- Darlington: automated deduction, POG, bookkeeping.
- LaCoS: Experience with automated reasoning tools.

Tools (Usage)

- SACEM: B.
- TBACS: FDM, scrolling, pencil and paper X-ref.
- Tektronix: Fuzz editor, typechecker and pretty printer.
- TCAS: LaTeX.
- Transputer: Occam transformation system, in-house refinement checker.
- HP: HP-SL syntax checker.
Tools (Analysis)

Did the formal methods tools help or hinder the development of the product?
Were the tools reliable?

<table>
<thead>
<tr>
<th>CA</th>
<th>CI</th>
<th>CL</th>
<th>DA</th>
<th>LA</th>
<th>MG</th>
<th>SA</th>
<th>TB</th>
<th>TE</th>
<th>TC</th>
<th>TR</th>
<th>HP</th>
</tr>
</thead>
<tbody>
<tr>
<td>-</td>
<td>+</td>
<td>n/a</td>
<td>0</td>
<td>0</td>
<td>+</td>
<td>n/a</td>
<td>0</td>
<td>+</td>
<td>n/a</td>
<td>0</td>
<td>+</td>
</tr>
</tbody>
</table>

• Not a large role (lack of tool support).

• Problems due to newness and primitiveness.

• Need for language checkers, bookkeeping.

• Don’t be too ambitious.

• Automated deduction in critical applications.

Observations

Features:

• Methods: state machine; 1st-order predicate calculus; reviewability; complete refinement.

• Tools: Language processors; bookkeeping; browsing; x-ref.

• Needs: Integration with other V&V; concurrency and timing; lower barriers of entry.

Observations

Features:

• Definite positive influence on design, requirements, V&V, and pedagogical.

• Positive influence on 'impact on process' and quality.

• Neutral on cost.

Tools (Needs)

• Tektronix: schema expander, refinement proof tool, pre-condition calculator.

• TCAS: safety analysis tool, automated deduction, language checker, soundness.

• Transputer: refinement checker for large state spaces.

• HP: Language checker and better notation (not ambitious!).

20

31

32
Availability of Report

- Availability within 2-3 months.

- Send email to dan@ora.on.ca, or mail to:

  Dan Craigen  
  ORA Canada  
  265 Carling Avenue, Suite 506  
  Ottawa, Ontario K1S 2E1  
  Canada
Formal Modelisation

Susan Gerhart
National Science Foundation
Modelisation

Sure you’ve proved it correct, but what does the system REALLY do?

Susan L. Gerhart
sgerhart@nsf.gov

Subjects:
The SACEM Case (continued from Dan Craigen’s presentation)—how FM was embedded in an industrial process

Issues of "modelisation"

Software Engineering for a "Formal Methodist"

Requirements: Mathematical model of the system that allows property exploration
Specification: "the system" expressed in mathematical notations
Design: Operation decompositions and data refinements
Implementation: Code + Assumptions + Assumptions
Validation: Spec. + Evaluation or proofs of properties
Verification: Identification and discharge of correctness obligations
Documentation: Prose and diagrams that go with the mathematical notation
Life Cycle: Get the specification right and agreed upon

Background Point of View

SACEM:
Train control for the Paris Metro

The Job:
Shorten the train intervals to 2 minutes to avoid a new Paris line and convince the Paris Transit Authority the system was safe and build up an international business in safe train control systems

Who:
GEC Alsthom/Marva/SEE + Paris Transit Authority

The Process:
1976: Decided had to go with new software and hardware
1980s: Exploring fault tolerance, discovered proof of correctness techniques, did safety studies, built prototypes, verified code on line, found new way to specify and verify, worked with authorities to demonstrate safety, brought on-line
1990s: Demonstrated capability on other systems, commercializing looks used in the process

The Results:
Verification was demonstrated as an addition to simulation, without excess cost and with significant added assurance
Specification and modelisation matured and an industrial process was defined

SACEM System

Safety Curve

Challenges:
- Different kinds of "rolling stock" to detect, some protected and some not
- Variations in track beacon technology, tunnels & trains
- Getting the train "home" when it’s system does fail
- Encoded single processor (rather than complex synchronized multi processor) - as fail safe as possible
SACEM lessons for Formal Methods

An industrial process has been put in place that is evolving toward:
- Understood and documented
- Measured and predictable
- Regarded as cost effective
- Tool supported
- Probably comparable to MOD 0055

Many techniques can play together, 
(although not in concert yet)
- SADT for graphical system decomposition and analysis
- FSM (Graphical) simulator
- Hazard analysis
- Operational scenarios (600 of them)
- Real-time design simulation
- Prototyped system
- Code verification & specification refinement

Technology Transfer problems could be overcome
A manager understood and stuck with it
- The customer was educated (and did their own thing)
- Proving could be credibly compromised
- Modelling will help synthesize their results

SACEM Background

<table>
<thead>
<tr>
<th></th>
<th>formal proof</th>
<th>module testing</th>
<th>functional testing</th>
<th>re-specification</th>
</tr>
</thead>
<tbody>
<tr>
<td>Total</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>V&amp;V = 1.5 x Development</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Validation Effort

<table>
<thead>
<tr>
<th></th>
<th>Train. Track</th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Number of procedures proven formally</td>
<td>111 21</td>
<td>Number of procedures covered in some global tests</td>
<td>120 33</td>
<td></td>
</tr>
<tr>
<td>Number of procedures tested semi globally</td>
<td>79 67</td>
<td>Number of procedures tested globally</td>
<td>180 167</td>
<td></td>
</tr>
</tbody>
</table>

SACEM Background Table

<table>
<thead>
<tr>
<th></th>
<th>maintained spec</th>
<th>outermost guided by design</th>
<th>refined down</th>
<th>very refined</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>maintained code</td>
<td>internal most following headers, not body</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Modelling

The process of getting all the stakeholders to understand and agree that the working description conveys the intended system. Subsumes requirements analysis, mathematical modeling, etc.

In SACEM:
- Tracks, trains, beacons, encoded mproc...
- Safety principles
- The description notation itself
- The process of using the description

Problems encountered with modelling in SACEM:
- Laborious code description disconnected from "the theorem"
- Concurrency difficult to express in top level model
- Different representations, different analyses were used for assurance (see tools list)
- Many kinds of system views: car, railway switching, microprocessor developer, formal verifier
- Refinements were OK, but there was a code gap (now generated)

Carry-over from Requirements Analysis

Given a language and tools, how do you express the requirements and model the system?

Translate English and diagrams to sets, logic, etc.
- and translate back and forth, but
- how do you read and check these?
- what diagrammatic techniques match FM?

CORE, JSD, GIST, SADT etc. provide:
- standard system representations
- ways to get different viewpoints
- domain modeling techniques

Software process modeling offers:
- Guidelines for use
- Baseline for data collection and eventual metrics
- Opportunities for integration, e.g. with testing
- Basic appearance of managability
Modellisation Process

Identification
- Entities
- Constraints among entities
- Operations and their parameters

Representation
- Entities become values of a type
- Types must be defined to construct, modify, and examine their contents
- Representation issues are considered, e.g., ordering, duplication, primitive types, attributes
- Additional properties of the data types from requirements

Operations defined with their parameters
- Restrictions are expressed as preconditions
- Its effects are defined in terms of parameter values before and after execution
- System invariants are formulated from properties that the system is required or expected to have.
- Invariants are proved by induction

(And a collection of definitions is built up)

Summary

SACEM Case
- “Complete” application of formal methods
- Shows potential for integration of FM into broader system engineering
- Displays interaction of problem domain and formalization

Modellisation
- Process aspect to add to FMs as languages & tools
- Integration of standard computer science with application domains

Challenge to FM Vendors:
- write down your process model
- show how modellisation is performed

The limitations of the model are identified, e.g.
- Omitted operations or data details
- Implicit definitions
- Assumptions about the operating environment (system and users)
- Degree of concurrency expressed
- Reliability of communication media
- Performance, resource, and security requirements that must be met by the implementation

A plan for using the model is developed, e.g.
- Identifying the riskiest or least understood part for further analysis or refinement
- Iteration toward more extensive models
- Formal proof of properties of the model
- Validation, e.g., by prototyping from the model
- Reviews, inspections, and other peer analyses
- Animation of the model
- Scenarios to stimulate response from customers
Formal Methods Technology Insertion Into FTPP

Rick Harper
Charles Stark Draper Labs
Formal Methods Technology Insertion into The Fault Tolerant Parallel Processor

presented at the
Second NASA Langley Formal Methods Workshop
11-13 August 1992

presented by

Rick Harper
Advanced Computer Architectures Group
The Charles Stark Draper Laboratory, Inc.
Cambridge, MA 02139

Formal Methods Technology Insertion into the FTPP

Objective:

Use formal specification and verification of critical FTPP hardware and software components to reduce the incidence of common-mode failures due to specification and implementation errors

Formal methods do not help avoid many sources of common-mode failures

environmentally-induced faults: EMI, radiation, heat, water, corrosives, sand (!)

Formal methods are not the only solution to common-mode fault avoidance, removal, and tolerance

Mature components, standards compliance, design automation tools, ruthless persecution of complexity, conservative design practices, simulation, testing, various CMF detection/recovery mechanisms

Fault Tolerant Parallel Processor (FTPP)

High-throughput high-reliability/availability computer for hard real-time applications

Uses many Processing Elements (PEs) in parallel for high throughput

Uses redundant PEs for high reliability

Tolerates arbitrary failure manifestations ("Byzantine Resilient")

Designed primarily to tolerate uncorrelated hardware faults

Programmed in Ada
Fault Tolerant Parallel Processor (FTPP)

- Can trade throughput (parallelism) for reliability (redundancy) in real-time
- Can be dynamically reconfigured to optimize mission reliability and availability
- Supports mixed simplex, triplex, and quadruplex redundancy
- Allows heterogeneous processing resources
- Parallelism - transparent to programmer
- Fault tolerance - transparent to programmer

Current FTPP Applications

- "The Army Fault Tolerant Architecture (AFTA) Program"
  - Funded by: Army Electronics Integration Directorate / NASA
  - Application: Helicopter TF/TA/NOE/FCS
- "Heterogeneous FTPP"
  - Funded by: Army Strategic Defense Command
  - Application: Battle Management
- "Fault Tolerant IMU Processor"
  - Funded by: a commercial aerospace company
  - Application: IMU processing

Cluster 3 (C3) FTPP

Third-generation FTPP

- Processing Elements
  - Support 3 to 40 PEs per cluster
  - 660x0s, 80960s, MIPS R3000s, i860s, or DSP32C signal processors
- Network Elements
  - 100 Mbit/sec fiber optic interchannel links facilitate fault containment and physical dispersion
  - Standard bus interface to Processing Elements
- Software
  - XGAda™-based operating system with CSDL extensions

FTPP C3 Architecture
Layered View of FTPP

Processing Element
Formally specified / verified microprocessor can be used in FTPP.
Processors interface to FTPP over standard bus (e.g., VMEbus).
Not all processors in FTPP need be formally verified.
Could use small number of formally verified processors to form quad or triplex Byzantine resilient core VG which runs a simple verified kernel.
Core VG responsible for monitoring other VGs (including CMFs) and resetting offenders using voted_reset capability of NE.
Throughput of core VG not an issue...can get desired throughput adding higher-throughput VGs in a heterogeneous parallel processing configuration.
All VGs communicate using BRVC.

Components of FTPP Suitable for Formal Methods Insertion

Processing Element
Network Element
FCR Backplane Bus
VG Synchronization Software
Task Scheduling Software
Inter-VG Communication Software
FDIR Software

NASA Formal Methods Workshop 11-13 August 1992

Components of FTPP Suitable for Formal Methods Insertion

Processing Element
Network Element
FCR Backplane Bus
VG Synchronization Software
Task Scheduling Software
Inter-VG Communication Software
FDIR Software

NASA Formal Methods Workshop 11-13 August 1992
Network Element Architecture

FCR Backplane Bus
Backplane bus used for PE-NE communication
NE partitioned into bus-dependent and bus-independent sections
Can retrofit NE to formally specified/verified backplane bus by modifying bus-dependent section
Formal model of backplane bus needed
Backplanes are a common component of many systems
A formally specified and verified backplane could find wide use in critical systems
Powerful building block for ultrareliable systems:
Formally specified and verified processor resident on formally specified and verified backplane bus card

Byzantine Resilient Virtual Circuit
Inter-VG Communication Abstraction
Messages sent by non-faulty members of a source VG are correctly delivered to the non-faulty members of recipients
Non-faulty members of recipient VGs receive messages in the order sent by the non-faulty members of the source VG
Non-faulty members of recipient VGs receive messages in identical order
The absolute times of arrival of corresponding messages at the members of recipient VGs differ by a known upper bound $\delta$
The time between a valid message transmission request and message delivery possesses a known upper bound $\tau$
The BRVC abstraction is supported by the NEs

VG Synchronization
VGs are synchronized upon periodic timer interrupts (e.g., at 100 Hz)
Timer interrupts occur within a bounded skew on all members of VG
Upon timer interrupt a VG performs a synchronizing act (i.e., message passing using BRVC)
Send message to self
Await reception
Rate Group Scheduler

FTPP C3 uses timer-based preemptive rate group scheduler

Variant of rate-monotonic scheduling optimized for iterative task suites having harmonic iteration rates

Tasks interact only at frame boundaries

FTPP OS schedules appropriate tasks at each frame boundary

<table>
<thead>
<tr>
<th>Frame Boundary</th>
<th>Completed RGs</th>
<th>Started RGs</th>
</tr>
</thead>
<tbody>
<tr>
<td>1-0</td>
<td>1,2,3,4</td>
<td>1,2,3,4</td>
</tr>
<tr>
<td>0-1</td>
<td>1,2,3,4</td>
<td>1,2,3,4</td>
</tr>
<tr>
<td>1-2</td>
<td>1,2,3,4</td>
<td>1,2,3,4</td>
</tr>
<tr>
<td>2-3</td>
<td>1,2,3,4</td>
<td>1,2,3,4</td>
</tr>
<tr>
<td>3-4</td>
<td>1,2,3,4</td>
<td>1,2,3,4</td>
</tr>
<tr>
<td>4-5</td>
<td>1,2,3,4</td>
<td>1,2,3,4</td>
</tr>
<tr>
<td>5-6</td>
<td>1,2,3,4</td>
<td>1,2,3,4</td>
</tr>
<tr>
<td>6-7</td>
<td>1,2,3,4</td>
<td>1,2,3,4</td>
</tr>
</tbody>
</table>

Inter-VG Communication

FTPP tasks communicate using message passing queue

OS call places message onto outgoing queue to NE

FTPP OS determines destination VG from task-to-VG mapping table

OS transmits message queue to destination VG using BRVC

Recipient VG's OS reads message from NE and places into destination task input message queue

All scheduling and inter-VG communication assertions are independent of VG redundancy level

Fault Recovery

Many recovery policies possible in FTPP

Reduce redundancy level

Reintegrate faulted component

Replace faulted component with spare

System FDIR determines appropriate recovery action and either

transmits recovery commands to local FDI for localized recovery or

performs global system-level recovery

Must show that system FDIR determines correct recovery action as a function of diagnosed component

Must show that local or system FDIR correctly carries out specified recovery
Heterogeneous Kernels on FTPP

Not all kernels in FTPP need be identical as long as they can communicate using BRVC.

FTPP can host rate group scheduler on production VGs and small formally verified kernel on formally verified VGs.

*Message passing through BRVC subsumes synchronization so the formally verified kernel would not explicitly perform synchronization of redundant sites.*

The formally verified VG would execute the system FDIR function.

Work In Progress: Scoreboard Specification and Verification

Currently collaborating with ORA to formally specify Scoreboard.

Scoreboard is a critical component of FTPP.

Comprises approximately 50% of NE circuitry.

Enforces BRVC abstraction.

Business Model:

FM experts working closely with engineering staff having little exposure to formal methods.

Separate funding (Draper not specifically funded to collaborate).

Scoreboard described in VHDL and constructed using automated synthesis (Synopsys).

VHDL used as common language between Draper and ORA.

Conclusions from Scoreboard Specification and Verification

Formalization of Scoreboard requirements uncovered several specification omissions and ambiguities.

Collaboration would have been closer and impact on design greater if Draper had been specifically funded to participate.

Incremental cost on a $2.4M brassboard development program is small.

Benefit to cost ratio is very high during the conceptual study and detailed design phases.

Work Planned and Critical Needs

**Work Planned**

Components similar to remainder of NE (i.e., FTC, voter) have been formally specified/verified.

Would like to adapt this work to FTPP.

Actively seeking FV processor to design into FTPP.

Planning to develop selected subset of RCP software for FTPP.

**Critical Needs**

Viable processor.

Formal subset of VHDL, with nonempty intersection of synthesizable and formal subsets.

Continued formalization of FTPP NE.

Formal model for FCR backplane bus.

Formalization of critical OS functionality.

Business model for formal methods insertion.
Formal Methods at
IBM Federal Systems

David Hamilton
IBM Federal Systems
Introduction and Purpose

- To cover
  1. Some IBM involvement in Formal Methods (FM) projects
  2. A perspective on difficulties of technology transfer (beyond a single project)

- Purpose is not to
  - sell the "IBM approach"
  - argue against feasibility of FM

- Purpose is to
  - learn from other FM technology transfer projects
  - suggest some possible future directions

Harlan Mills and SEW

- Mills led massive software engineering education program
  - Software Engineering Workshop was cornerstone
    - 2 week course
    - Taught to all programmers
    - Required to pass final exam

- SEW centered on mathematically-based verification
  - Functional instead of axiomatic
    - model oriented instead of property oriented
    - designed to scale up (stepwise refinement)
    - easier for programmers to understand
  - 2 pieces
    1. Deriving program functions
      - Trace tables (basically manual symbolic execution)
      - Recursion instead of loop invariants
    2. Module-oriented
      - abstract data types
      - constraints/closure on state data (abstract state machine)
**Harlan Mills and SEW ...**

- SEW designed to be practical  
  - relatively informal  
  - scaled up via abstraction/refinement  
  - lots of examples and exercises  
  - final test: pass/fail  
- Advocated for all programming, not just critical parts  
- no support beyond education  
  - no tools  
  - no consulting  
- General reaction was that it was impractical  
  - too tedious  
  - seemed only for toy problems  
- Did not gain widespread use

**Cleanroom**

- Named after silicon chip manufacturing environment  
- Built on SEW foundation, adding  
  - Continuous inspections (SEW style verification)  
  - Statistical testing (MTTF prediction)  
- Advertised through case studies, not classes  
- Demonstration projects using highly skilled developers  
- To demonstrate benefits  
- To show it can be done, it is practical  
- Demonstrations projects were success stories

**Cleanroom ...**

- Showcase project was COBOL/SF  
  - Transforms unstructured COBOL into structured COBOL  
  - 52,000 SLOCS developed using Cleanroom  
  - Results  
    - 740 SLOCS / labor month  
    - 3.4 errors / KSLOC (before first execution) (70 avg incl. UT)  
    - no error ever found during operational use  
- Advocacy of Cleanroom continues  
  - Widespread use not yet attained  
  - But there is a lot of interest in Cleanroom

**SEDL**

- Intended to support SEW/Cleanroom verification concepts  
- Built as an extension to Ada  
- SEDL compiler generates Ada  
- Supports design execution  
  - though SEDL generated code may be inefficient  
- Includes  
  - Abstract data types (set, list, map, etc.)  
  - User defined data models  
    - model vs. representation  
    - constraints  
  - Supports mathematical notation  
    - (X in CHARACTER : x /= 'Q')  
    - exists X in S : P(X) and exists Y in T : P(Y)  
    - P > 1 and not (exists Q in 2..P-1 : P rem Q = 0)  
- Use of SEDL is not widespread
Other Projects and Approaches

- Application above the code level
  - Development of a "Box Structures" design language
  - Development of a "Box Structures" approach to requirements
- Results
  - SA/SD approach to design most popular new approach
  - Requirements still written in English
- Emphasis on SEW concepts
  - Concepts generally well accepted
  - Loss of rigor reduces mathematical basis

Note on Quality Emphasis

- Software quality has extreme emphasis
  - Great emphasis on process improvement
  - Serious attention given to quality goals and measurement
  - Quality motivation programs
    - awards and recognition
    - Manned Flight Awareness program
- There is willingness to work hard and invest for quality
- The question is not what or how much but how
  - FM is generally perceived as not helping

Summary

- Goal was to increase the use of formal mathematical approaches to software development (beyond a single project)
  1. First through education
  2. Then through demonstration projects
  3. Then through tool support
  4. Then by making methods more practical
  5. Finally through direct support (consulting)
- There have been successes
  - not nearly as widespread as desired
- This story is not unique to FM
  - The problem is with technology transfer, not with technology

Conclusions

- Conclusion: Technology Transfer is very hard, even with
  - extensive education
  - tools support
  - demonstrated successes
- Possible future directions
  - More consulting ("hand holding") (product champions)
  - Use only a core group (FM may just not be for everybody)
  - Require use of FM (selected groups)
  - Success story close to home
    - technology transfer diminishes rapidly as a function of distance
    - long term commitment is required (success story requires continued follow-up)
  - Different formal method(s)
  - Different tools (e.g., theorem prover)
Reliable Computing Platform

Ben DiVito
ViGYAN
Flight Control Problem

- closed-loop feedback control system
- life-critical
- failure prob $< 10^{-9}$ for 10-hour mission
Hierarchical View of a Flight Control System

Application Task Characteristics

1. The set of tasks is fixed
2. Hard deadlines
3. Multi-rate cyclic scheduling
4. Minimal jitter
5. Upper bound on task execution time
6. Precedence constraints

Research Objectives

- Establish hardware/software platform for ultra-reliable computing
- Use fault-tolerant computer architecture to compensate for physical hardware faults
- Use formal methods to prevent design and implementation errors
  - Specify and mechanically verify using EHDxM
  - Incorporate emerging technology as needed
- Construct reliability model to quantify reliability estimate
Design Philosophy

Competing objectives:

1. Increased design complexity can be used to achieve more sophisticated fault-tolerant architectures — increased tolerance of physical hardware faults for given cost

2. Decreased design complexity will lead to fewer design flaws — increased avoidance of design faults

Most fault-tolerant systems emphasize (1) at the expense of (2) — we seek a more balanced tradeoff

* Functionality of RCP is modest (currently)—simpler than what can be built in practice today.
* But we have traded this off to achieve provability—better than what we have today.
* Technology advances will narrow the gap.
* We are trying to push one part of the envelope.

Formal Methods is Enabling Technology For Synchronous Design

- Design flaw in sync. algorithm is a logical single-point failure
- Clock synchronization notoriously difficult
- Without rigorous demonstration of synchronization, there can be little confidence in the system
- Formal Verification has been successfully applied to clock sync problems

First Design Decisions

Ultrareliability $\rightarrow$ Fault Tolerance $\rightarrow$ Redundancy

Redundancy $\rightarrow$ Voting

(Exact-match)

Interactive Consistency

EMI/HIRF Threat $\rightarrow$ Transient-burst Immunity
Reliable Computing Platform

RCP supports execution of tasks for real-time control applications

Special-purpose hardware enables exact match voting:
- Distributed agreement front end
- Clock synchronization subsystem

RCP's Sequence Of Operation

1. compute
   - frame started by clock interrupt
   - execute all tasks scheduled in current frame
   - multiple frames constitute a cycle

2. broadcast
   - broadcast outputs of task execution to other processors
   - usually just a subset of the outputs are broadcast

3. vote
   - vote broadcast data
   - replace memory with voted values

4. sync
   - execute sync algorithm
   - wait for next clock interrupt

Vote Location/Frequency

option 1: At the instruction level
   — Synchronization must be tight
option 2: At the task level
   — After task completion
   — Loose synchronization
option 3: Asynchronous
   — End up synchronizing in control laws

Task Execution in RCP

Task results are assigned to different cells within the state:

Frame 1 Task 1 \( S[1] := f_1(u, S[7]) \)
Frame 1 Task 2 \( S[2] := f_1(S[1]) \)
Frame 2 Task 3 \( S[3] := f_4(u, S[3]) \)
Frame 2 Task 4 \( S[4] := f_1(S[3]) \)
Frame 3 Task 5 \( S[5] := f_2(u) \)
Frame 4 Task 6 \( S[6] := f_4(u, S[4]) \)
Frame 4 Task 7 \( S[7] := f_1(S[5], S[6]) \)
Various Purposes of Voting

1. Voting at the actuators. This approach does not offer recovery from transient faults which can corrupt the state of a good processor unless it is combined with some scheme for periodically voting all the global processor states.

2. Voting the entire processor state (e.g. all memory). This approach deals with transients but requires a large CPU overhead.

3. Voting only the state which is not recoverable from sensor input. This approach also deals with transients but involves increased complexity.

4. Voting to detect faults. Used in reconfigurable systems.

Reliability Modeling

Reliability Model of Quadruplex Version of System

\[ \lambda_T = \text{transient fault rate} \]
\[ \lambda_P = \text{permanent fault rate} \]
\[ \rho = \text{rate of flushing effects of a transient} \]

Summary Of Major Design Decisions

Design simplicity is emphasized to promote mathematical analysis

- RCP is non-reconfigurable
- RCP is frame-synchronous
- Scheduling deterministic abstract axiomatic model
- Internal voting is used to recover (within a bounded time) the state of a processor affected by a transient fault

Consequences of non-reconfigurable architecture:

- Voting serves no fault detection function
- Transient fault recovery need not be rapid
- Reliability models predict recovery time of one minute is adequate

Therefore, favor infrequent voting to reduce overhead

- Selective voting occurs at end of frame after all computation

Transient Fault Recovery (N=4)

\[ P_T \]

Mean Time to Recover From Transient (hours) [ln. 1/\rho]

- Shape of curve same for larger N
- The locations of the inflection points do not significantly change as N is increased
Previous Efforts

- SIFT
- FTMP
- FTP
- MAFT
- M^2FCS
- AIPS

FEATURES
- All had reconfiguration
- FTMP used instruction-level voting
- Only SIFT/MAFT applied formal methods
  - MAFT: Level 2 formal methods applied to critical algorithms
  - SIFT: Level 3 formal methods applied to fault-masking and reconfiguration design

Relationship Between Formal Methods and the Reliability Analysis

Formal Methods:
Proves formulas of the form:

\[
\text{ENOUGH\_WORKING\_HARDWARE} \Rightarrow \text{PROPER\_OPERATION}
\]

Reliability Analysis:
Calculates the following probability:

\[
\text{Prob}[ \text{ENOUGH\_WORKING\_HARDWARE} ]
\]

Verification Approach

Recovering from Transient Processor Faults

We allow processors to recover their state incrementally over multiple frames.

Processors have three fault modes:
- Faulty — permanent or transient
- Recovering — persists for $N_R$ frames after disappearance of fault
- Working — fully recovered

All theorems about state machine correctness are predicated on the assumption that a majority of working processors exists in each frame.
Hierarchical Design and Analysis of RCP

Goals:
- Remove redundancy management from application domain
- Show that fault-tolerant system achieves same effect as an ultra-reliable uniprocessor
  - Provided faults are limited

Uniprocessor System Model (US)
Fault-tolerant Replicated Synchronous Model (RS)
Fault-tolerant Distributed Synchronous Model (DS)
Fault-tolerant Distributed Asynchronous Model (DA)

Local Executive Model (LE)
Hardware/Software Implementation

Framework For Proving Design Correctness

Design layers formalized as nondeterministic state machines
- State represents memory contents and hardware states
- Transition relation specifies allowable state transitions
Non-determinism models arbitrary behavior by faulty components

Interpretation maps lower level states into higher level states

\[ s_i \xrightarrow{\text{Map}} N_i \xrightarrow{l_i} \]
\[ s_{i+1} \xrightarrow{\text{Map}} N_{i+1} \]

Need to show that diagram "commutes" to establish that layer \( i+1 \) correctly implements layer \( i \):

\[ N_{i+1}(s_{i+1}, l_{i+1}) \supset N_i(\text{Map}(s_{i+1}), \text{Map}(l_{i+1})) \]

Generalized Framework For Design Proofs

\[ s' \xrightarrow{N'(s', l', u)} l' \]
\[ s \xrightarrow{\text{Map}} N_i(s, l, u) \]

We must prove two theorems to show that lower level spec \( L \) correctly implements upper level spec \( U \):

Initial maps: Theorem initial \( L(s) \supset \text{initial } U(\text{Map}(s)) \)

Frame-commutes: Theorem reachable(s) \& N_i(s, l, u) \supset N'_i(\text{Map}(s), \text{Map}(l), u)

Consider only states reachable via allowable state transitions

Restriction to reachable states allows state invariants to be expressed and proved using a specialized induction schema.
Bounded Asynchrony

Extended state machine model used to capture timed behavior
- Clock time snapshots included in DA states
- Nominal durations modeled (state occupancy)
- Mappings to real time introduced

Existing clock synchronization theory available
- Based on Interactive Convergence algorithm
- Previously formalized and proved using ERM
- We assume clock hardware separate from processor
  - Faulty clock impairs processor, but not vice versa

Limitations
- Requires two-thirds majority of nonfaulty clocks
- Unable to tolerate transient faults

Main Result

Assuming:
- Particular workload and user-selected vote pattern satisfies required abstract properties (Discharged for three examples)
- Clock synchronization properties (later to be refined into hardware circuit tolerant of transient faults)
- Enough functioning hardware in every frame
  - Majority of working processors
  - Two-thirds majority of nonfaulty clocks

Then under the cumulative state mapping $M = D\text{map} \circ D\text{snap} \circ R\text{snap}$,
$DA$ has the same effect as $US$:
1. $DA_{\text{initial}}(a) \supset US_{\text{initial}}(M(a))$
2. $\text{reachable}(a) \land DA_{\text{frame}}(a, i, u) \supset US_{\text{frame}}(M(a), M(i), u)$

where $u$ denotes external inputs

This result has been formalized and proved mechanically using ERM.

Representation of State Vectors

<table>
<thead>
<tr>
<th>US:</th>
<th>Param: TYPE</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>RS:</th>
<th>ARRAY [processors] OF</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>healthy: nat</td>
</tr>
<tr>
<td></td>
<td>processor: Processor</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>DS:</th>
<th>phase: phases</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>ARRAY [processors] OF</td>
</tr>
<tr>
<td></td>
<td>healthy: nat</td>
</tr>
<tr>
<td></td>
<td>processor: Processor</td>
</tr>
<tr>
<td></td>
<td>mailbox: Mthres</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>DA:</th>
<th>phase: phases</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>sys-period: nat</td>
</tr>
<tr>
<td></td>
<td>ARRAY [processors] OF</td>
</tr>
<tr>
<td></td>
<td>healthy: nat</td>
</tr>
<tr>
<td></td>
<td>processor: Processor</td>
</tr>
<tr>
<td></td>
<td>mailbox: Mthres</td>
</tr>
<tr>
<td></td>
<td>ilock: logical, locktime</td>
</tr>
<tr>
<td></td>
<td>cum-delta: number</td>
</tr>
</tbody>
</table>
**US Transition Relation**

Top level requirement is the US transition relation:

\[ N_{US}: \text{Definition function}\{\text{Pstate, Pstate, inputs -> bool}\} = \]
\[ (\lambda s, i, u: (\exists t: (\forall t': \]
\[ s(t), \text{healthy} > 0 \]
\[ \lor \text{good.value.sent}(s, u, h(t)) \land \text{voted.final.state}(s, i, w, h, i)) ) \]
\[ \land \text{allowable.faults}(s, i)) \]

WHERE:

allowable.faults: function[RState, RState -> bool] =
\[ (\lambda s, i: \text{maj.working}(i) \]
\[ \land (\forall t: (t, \text{healthy}) > 0 \lor t(i), \text{healthy} = 1 + s(i).\text{healthy})) \]

good.values.sent: function[RState, inputs, MBvec -> bool] =
\[ (\lambda s, w, i: (\forall j: \]
\[ s(j).\text{healthy} > 0 \lor w(j) = f_{s}(f_{u}(u, s(i)), \text{proc.state})) ) \]

voted.final.state: function[RState, RState, inputs, MBmatrices, processors -> bool] =
\[ (\lambda s, i, u, h, i: (i(i), \text{proc.state} = f_{s}(f_{u}(u, s(i)), \text{proc.state}), h(i)))) \]

**RS State Vector**

<table>
<thead>
<tr>
<th>RS: ARRAY [processors] OF</th>
<th>healthy: nat</th>
</tr>
</thead>
<tbody>
<tr>
<td>proc_state: Pstate</td>
<td></td>
</tr>
</tbody>
</table>

* healthy:
  - 0 when a processor is faulty
  - Otherwise, it indicates the number of state transitions since the last transient fault.
* proc_state:
  - computation state of the processor.
  - takes values from the same domain as used in the US specification.

**DEFINITIONS:**

- A permanent fault is indicated by a perpetual healthy = 0.
- A recovering processor has a value of healthy less than the constant recovery_period, whose value depends on the task schedule and voting pattern.
- A processor is said to be working whenever healthy ≥ recovery_period.

**Sample Interpretations for Vote/Scheduling Functions**

The three sample interpretations correspond to three types of voting:

- Continuous voting \[ N_{R} = 2 \]
  - This specifies that the entire state will be voted every frame.
  - Not very practical, but proof that it satisfies application task properties is simple
- Cyclic voting \[ N_{R} = M + 1 \]
  - This specifies that only the data produced during the frame will be voted.
  - SIFT approach
- Minimal voting
  - Vote only portion of state that will not be recovered from new sensor values
  - Construct vote pattern to ensure each cycle of graph is cut by at least one vote.
  - \[ N_{R} \] is a function of data dependencies and specific vote pattern
**DS Specification**

- Decompose frame into four phases:
  - phases: TYPE (compute, broadcast, vote, sync)
- Explicitly model interprocessor communication via a mailbox mechanism

**DS Transition Relation**

\[
\text{frame} \cdot \text{N} \cdot \text{dec} \cdot \text{function} \cdot \text{DS} \cdot \text{state}, \text{DS} \cdot \text{state}, \text{inputs} \rightarrow \text{bool} =
\]

\[
(\lambda x, y, z : (x, y, z) \cdot \text{N} \cdot \text{dec}(x, y, z) \cdot \text{N} \cdot \text{dec}(y, x) \cdot \text{N} \cdot \text{dec}(z, x, u) \cdot \text{N} \cdot \text{dec}(x, y, u) \cdot \text{N} \cdot \text{dec}(y, x, u) \cdot \text{N} \cdot \text{dec}(z, x, u))
\]

\[
\begin{align*}
\text{N} \cdot \text{dec}(x, y, z) &: \text{phase 1} \rightarrow \text{compute} \\
\text{N} \cdot \text{dec}(y, x, u) &: \text{phase 2} \rightarrow \text{broadcast} \\
\text{N} \cdot \text{dec}(x, y, u) &: \text{phase 3} \rightarrow \text{vote} \\
\text{N} \cdot \text{dec}(z, x, u) &: \text{phase 4} \rightarrow \text{sync}
\end{align*}
\]

**DA Model: Key Concepts (Definition Of a Clock)**

- A clock is modeled as a function from clock time $T$ to real time $t$

**NOTATION:**

- $c(T) = \text{an\ uncorrected\ (non-synchronized)\ clock}$
- $r(t)(T) = \text{the\ synchronized\ clock\ during\ its\ } t\ \text{th\ frame}$

**Definition Of Synchronization**

**KEY PROPERTY OF CLOCK SYNCHRONIZATION SUBSYSTEM:**

**Theorem 1:**

\[
S1A(i) \supset (\forall p, q : (\forall T : \\
\text{nonfaulty.clocks}(p, i) \land \text{nonfaulty.clocks}(q, i) \land T \in R^{(i)}) \\
\supset (|r(t)(T) - r(t')(T)| \leq \delta))
\]

**Theorem 2:**

\[
|Cor_{p}^{(i)} - Cor_{q}^{(i)}| < \delta
\]

WHERE

- $S1A : \text{function[period} \rightarrow \text{bool}] = (\lambda i : \text{enough.clocks}(i))$
- $\text{enough.clocks} : \text{function[period} \rightarrow \text{bool}] =
  (\lambda i : 3 \cdot \text{num.good.clocks}(i, m))$
  \[
  \text{enough.clocks}(i) = (3 \cdot \text{num.good.clocks}(i, m)) > 3 \cdot \text{mapp}
  \]
DA Transition Relation

\[ N_a \text{ includes the advance of local clock time for each transition} \]

\[ N_a(x, i, t) \text{ function}[\text{exec state, exec state, inputs} \rightarrow \text{bool}] = \]

\[ (\lambda x, i, u : \text{enough hardware}(t) \]
\[ \land l.\text{phase} = \text{next phase}(x, \text{phase}) \]
\[ \land (\forall i : \text{if } x.\text{phase} = \text{sync} \]
\[ \quad \text{then } N_a(x, i, i) \]
\[ \text{else } l.\text{proc}(i) \land \text{healthy} = x.\text{proc}(i) \land \text{healthy} \]
\[ \land l.\text{proc}(i).\text{cum}.\text{delta} = \]
\[ x.\text{proc}(i).\text{cum}.\text{delta} \]
\[ \land l.\text{sync}.\text{period} = x.\text{sync}.\text{period} \]
\[ \land (\text{non faulty clock}(i, x.\text{sync}.\text{period}) \]
\[ \land \text{clock advanced}(x.\text{proc}(i), l.\text{clock}, \]
\[ l.\text{proc}(i), l.\text{clock}, \]
\[ \text{duration}(x.\text{phase})] \]
\[ \land (x.\text{phase} = \text{compute} \lor N_a(x, i, i)) \]
\[ \land (x.\text{phase} = \text{broadcast} \lor N_a(x, i, i)) \]
\[ \land (x.\text{phase} = \text{vote} \lor N_a(x, i, i)) \]
\[ \text{end if})] \]

Summary

- Simple fault-tolerant design postulated and refined to a design that models the effects of bounded asynchrony

- Formal four-level hierarchical specification of design constructed

- Mechanical verifications performed

- Reliability model constructed

- Will continue with more detailed design and verification

- Will extend functionality later
Clock Synchronization
Verification and Implementation

Paul Miner
Systems Validation Methods Branch
NASA Langley Research Center
Clock Synchronization Verification and Implementation

Paul S. Miner
Peter A. Padilla
William Torres

NASA Langley Research Center
Hampton, VA 23681
August 11, 1992

Specification of Clock Synchronization

A formal specification of the clock synchronization system is drawn from Shankar's mechanical verification (using DEHTM) of Schneider's general paradigm for fault-tolerant clock synchronization. The main result, given that the implementation satisfies certain constraints, is

Theorem 1 (bounded skew) For any two logical clocks $VC_p$ and $VC_q$ that are nonfaulty at real time $t$,

$$|VC_p(t) - VC_q(t)| \leq \delta$$

Example System

Algorithm

A generalized view of the algorithm employed by each clock $p$ is:

```plaintext
  do forever {
    exchange clock values
    determine adjustment for this interval
    determine local time to apply correction
    when time, apply correction}
```

The general algorithm is parameterized by a convergence function that determines both the magnitude and time of adjustment.
Theory

- Derived from Shankar's EVM verification of Schneider's general theory.
- Mechanically checked proof of some of Shankar's constraints using new assumptions.
- Hand proof of general approach for transient recovery, some mechanical proofs completed.
- Demonstration that conditions of revised theory can be satisfied.

Design and Implementation

- Design attempts to use same basic approach for initialization, transient fault recovery, and maintenance of synchronization.
- Abstract design derived from formal theory.
- Implementation is an instance of abstract design.
- Characteristics of Implementation:
  - Four clock design.
  - Point-to-point optical communication.
  - 10Mhz frequency.
  - External control for experimentation.

Verification Overview

Design

- Employs the fault-tolerant midpoint convergence function from Welch and Lynch's algorithm.
  - Discard the $F$ largest and $F$ smallest clock readings.
  - Return the midpoint of the range of the remaining readings.
  - Average of 2nd and 3rd reading for four clock system.
- Transmit synchronization signal at fixed point in each interval.
  - Estimate remote clock's value from difference between actual and expected arrival time of signal.
- $\delta \leq 11$ ticks; approximately one $\mu$sec.
- Exploit properties of convergence function for initialization and transient recovery.
Initialization

- Interval duration is $R$ ticks.
- Transmit offset of $R/2$ gives largest window for reading remote clock.
- If $N - F$ signals observed within $< R/2 - x$, system converges within $\log_2(R/2)$ intervals.
- If fewer than $N - F$ signals observed, either
  - compute no correction (Assumed Perfection), or
  - compute correction as if missing signals arrived at end of interval (End of Interval).

Each option exhibits pathological cases. For a four clock system, a 2-2 split is possible. The End of Interval approach combined with a simple time-out guarantees initialization, unless a malicious fault is present.

- Simulation results confirm expected behavior.

Block Diagram

 transient recovery

Revise mechanical theory includes uninstantiated predicate that defines a nearly recovered clock.

A clock is working in the current interval, if it was either working or nearly recovered in the previous interval (and a sufficient number of other clocks were working).

Sufficient conditions for the final recovery step are included as assumptions in the mechanical theory.

The necessary proofs to discharge the assumptions have similar structure to those needed for the general theory.

For four clock system (using End of Interval), recovery conditions satisfied within two intervals.

Implementation

- Off the shelf fiber-optic communication devices
- Remainder of design uses programmable logic devices (PLDs)
- 0.8192 msec interval, 1.1 $\mu$sec skew
- 10MHz frequency
- Synchronization state information available
- Experimental control allows emulation of Byzantine faults
- Both initialization options available
- Key parameters can be modified to explore performance trade-offs
Simulation of Algorithm

2-2 Split. No jitter or drift

Simulation of Algorithm

2-2 Split. With jitter and drift

Simulation of Algorithm

Upset Response, No Permanent Faults

Concluding Remarks

- General theory for clock synchronization revised to provide simpler verification conditions.
- Fault-tolerant clock synchronization system designed to meet requirements of formal theory.
- Design attempts to use the same basic algorithm for proven initialization, transient recovery, and maintenance of synchronization.
- Implementation uses off-the-shelf communication circuits and PLDs.
- Simulation results confirm behavior predicted by theory.
NASA’s Strategy for Technology Transfer

Sally Johnson
Systems Validation Methods Branch
NASA Langley Research Center
GOAL

Technology Transfer to Industry

One of NASA's major goals is to provide the U.S. aerospace industry with the tools and techniques they will need to be world-class competitors in the coming decades.
Technology Transfer

Working with Industry

- Boeing PIU hardware verification
- Boeing SVM hardware verification
- CSDL/ORA Scoreboard hardware verification
- ORA Verification of Ada application software from NASA Goddard and Johnson
  
  - Formal specification and verification of calendar utilities
  - Mode-control panel logic of Boeing 737 experimental system specified in Larch
- Currently pursuing future projects
Working with the FAA

- Digital Systems Validation Handbook Chapter
- Tutorial presentation to SWAT (Software Advisory Team)
- Formal specification of GCS application
- RTCA committee DO 178B standard
Verification of FTPP Scoreboard
and Spectool

Mark Bickford
Odyssey Research Associates, Inc.
Moving Formal Methods into Practice

Verifying the FTIP Scoreboard: Phase 1
Results

Mark Bickford
Mandayam Srivas
ORI Corporation
301 Gates Drive
Ithaca, NY 14850

NASA Contract NAS1-18972, Task 5
Context:

- AFTA - NASA/Army
- FTPP - Charles Stark Draper Laboratory
- Byzantine resilient virtual bus Scoreboard

Phase 1 Goals:

- Formulate abstract requirements
- Describe high-level design
- Verify that the design meets some of the requirements

Outline

1. FTPP overview
2. Scoreboard
3. Requirements
4. Scoreboard design description
5. Abstraction hierarchy
6. Proofs
7. Conclusions
The FTPP Logical Configuration

Byzantine-Resilient Virtual Circuit

1. **Reliable delivery**: Messages between virtual groups are delivered.

2. **Group consensus**: Each nonfaulty member of a group will receive identical copies of the message delivered to the group.

3. **Order preservation**: All non-faulty members of a group receive messages in identical order.

4. **Synchronous operation**: Non-faulty members of a group receive corresponding messages simultaneously within $\delta$
Network Element Cycle

- Exchange Request (LERP):
  - IBNF: ready to receive
  - OBNE: ready to send
  - DEST: destination VID
  - Other message data

  **SERP: Poll of LERPs for each PE Scoreboard:**

  - Vote SERP → VSERP
  - Validate and approve messages
Valid Message:

1. Majority of source group have OBNE
2. Majority of dest group have IBNF
3. Other validity conditions

Approval:

1. Unanimity or timeout for IBNF, OBNE
2. DEST unique
3. Broadcast takes precedence

Requirements:

- Abstract view of scoreboard state
- Abstract operations: clear_tmo, update_ct, process_serp
- Actual Behavior = Expected Behavior (provided Liveness)
- Expected Behavior → Constraints
Abstract View of the Scoreboard

Scoreboard
  tmo
  timer
  bndng
  bsrc

Status
  opin
  msgs

Rest of Network Element

SERP
CT

Actual Behavior

Approvedmsgs

FinalState

Requirements Level

Step Level

Idle
Message-to-send
Continue
Step

© 1992 ORA Corporation
SL-0041
12

© 1992 ORA Corporation
SL-0041
13
ActualBehavior s =
<<ApproveMsgs s, FinalState s>>

ApprovedMsgs s = MsgOut (trui (Step s))
FinalState s = Final (trui (Step s))

trui s = [s], is_idle s
    s : trui (Step s)

MsgOut [] = []
MsgOut [s] = []
MsgOut (s1:s2:more)
    (is_sent s1 & ~(is_send s2)); =
        ABS-msgof s1 : MsgOut more
MsgOut (s1:s2:more) = MsgOut (s2:more)

Final [s] = s
Final (a:x) = Final x

Requirements - Constraint Form

ApprovalCond 'S' 'vid' :=
    'OBNTimeoutCond S vid' = 'False'
    & 'IBNTimeoutCond S
        (voteddstn S vid) = 'False'
    & 'votedobs S vid' = 'True'
    & 'votedbns S
        (voteddstn S vid)' = 'True'

If no broadcast is pending and a message is not broadcast,
then a message must be sent if the message satisfies the
general approval conditions.

Nth n s = ithof n (ApprovedMsgs s)
(vid) (s)
((En) 'srcvidof (Nth n s) = 'vid')
    <-> ApprovalCond 'SBABS s' 'vid',
    No_bp_and_not_bcast 'SBABS s' 'vid'
Controller state Machine

C1 (opin = process_new_serp)
C2 vids_done
C3 bpsdag
C4 "(bok)
C5 c_obne & ((bcst & valid) | ("bcst & c_lbnf))
C6 bcst
C7 vids_done
C8 (opin = continue)
C9 (opin = continue)
Main Theorem

MAIN_THEOREM ::= 
    (StartSerp 's' 'Succ n'
     & ProperABS 's'
     & Liveness 's')
    => 'ActualBehavior s' = 'ExpBehavior s'

Msglemma ::= 
    (ProperABS 's'
     & StartSerp 's' 'Succ n'
     & Liveness 's'
     => 'Msgs(ActualBehavior s)'
       = 'expected_messages s'
    ExpBehavior s =
        <<expected_msgs s, expected_final s>>

expected_msgs s{bpendingof (ABS_bpendingof s)} =
    bcst_approved s
expected_msgs s =
    exp_msgs_from_check (VotedSerp s)
    (ABS_lkupof s)

exp_msgs_from_check vs lkup =
    checked_msgs (all-clear vs fn num)
    vs lkup

checked_msgs bok vserp lkup =
    bcst_truncate bok
    (sieve_dest (message_list vserp lkup))

Ambiguities:

☐ Must validity of pending broadcast be rechecked?
☐ Should invalid broadcast be sent to null?
☐ More than one message to null?
☐ Free-running timer or freeze?
Proof of MsgLemma:

- Use Vlemma, Clemma, Slemma.
- Four cases:
  1. Check → Idle
  2. Check → Bcost → Idle
  3. Check → Send → Idle
  4. Check → Send → Check
- Induction on length (exp_mgs s)
  \[ \text{exp_mgs} \left( \text{SBStep} \left( \text{CheckStep} \ s \right) \right) = \text{tl} \left( \text{exp_mgs} \ s \right) \]
- General lemmas about map, filter, fromto, all

Macro-Step lemmas

Vlemma :=

'Behavior (true (Step s))' =
  'Behavior (true (VoteStep s)),
  StartSerp 's' 'Succ s''

Clemma :=

'Behavior (true s)'' =
  'Behavior (true (CheckStep s))''
  NormalSerp '(ABS_msgof s)''

Slemma :=

'Behavior (true s)'' =
  'Xcons (ABS_msgof s),
  (Behavior (true (SBStep s))),
  is_send s'='true' & Liveness 's'
Proof of Vlemma:

- Strengthen induction hyp
- Formulate loop invariant
- Lemma2 :=
  \[(i::\text{NAT})(n::\text{NAT})\]
  \[\text{iterate } i \text{ Step } s' = \text{`VotingStep } i \text{ s'},\]
  \[\text{StartSerp } s' \text{ 'n' } \& \text{ 'i <= n' = 'True'}\]

New Techniques:

- Semi-automatic abstraction used to find definition of Step
- Theory files added to Clio
Phase 2:
- Verify actual design
- VHDL semantics
- Abstract to Phase 1 level

Conclusions:
- Good abstract spec
- High-level design
- Main properties proved
- Ambiguities clarified
- Errors (in our design) discovered
- High level lemmas reusable
Boeing's Work in Formal Methods

Dave Fura
The Boeing Company
Application of Formal Methods within the Boeing Defense & Space Group

Presented by
David Fura
The Boeing Company
Seattle, Washington

Motivation

SAFETY CRITICAL APPLICATIONS:

Military Aircraft
- Air Force F-22 fighter aircraft
- Army Comanche Light Helicopter (LH)
- Marine Corps Osprey V-22 tiltrotor
- Navy A-X attack aircraft
- Air Force Multirole Fighter (MRF)

Launch Vehicles
- NASA/Air Force National Launch System (NL3)

Space Transportation Systems
- Moon-Mars Initiative

Objectives

TO FORMALLY VERIFY SYSTEMS FOR SAFETY CRITICAL APPLICATIONS, INCLUDING BOTH HARDWARE AND SOFTWARE.

Fault Tolerant Computing Platform
Vehicle Management System

Targeted systems:
- IFTAS (Integrated Fault-Tolerant Avionics System),
- FTEP (Fault-Tolerant Embedded Processor).
Objectives (cont’d)

To develop an integrated design/verification environment incorporating formal and test-based techniques:

- Improved simulation practices reduce testing time and increase coverage.
- Formal verification used for safety-critical applications.

Transferring Formal Methods Ideas to Simulation:

- Interpreter models
- Methods of abstraction:
  - Temporal
  - Data
  - Notions of “correctness”

Improvements:
- Chip- and system-level simulation models.
- Facilitated test vector selection and application.
- Automated test result certification.

Background Work

University of California, Davis
(K. Lewis)

Cal Poly,
San Luis Obispo
(G. Fisher)

Component Composition Theory

AVM1 Central Processing Unit (CPU)
IEEE Floating-Point Unit (FPU)

Memory Management Unit (MMU)
Direct-Memory Access (DMA) Controller

VIper Central Processing Unit (CPU)

Generic Interpreter Theory

Input/Requirements Specification Language

FTEP Subsystem Configuration

A family of ultra reliable high performance embedded processors based on a set of common hardware/software building blocks:

Key:
- PMM: Processor-Memory Module
- IOM: Input Output Module
- CIM: Core Interface Module
### Example HOL Code

**Logic Gates:**

- \( \neg A \lor B \lor C \lor D \Rightarrow z \)  

**Complex Combinational Logic:**

- \( \neg A \lor B \lor C \lor z = ((A \land B) = (e \land f \land g)) \)

**Latches:**

- \( D = Q \lor D \rightarrow Q \land (t \land s) = (Q \land (t \land s)) \)

### PIU Specification Summary

**SUMMARY OF RESULTS:**

- The PIU design specification was formalized in HOL using a 5-level specification hierarchy, using existing tools/techniques (i.e., Windley's Generic Interpreter Theory):
  - The lowest level is a structural representation corresponding to the design that was input to a silicon compiler (model size: 260 state variables, 50 outputs).
  - The highest level is a behavioral representation of the entire chip (model size: 150 state variables, 20 outputs).
  - A number of design mistakes were uncovered during the specification process.
  - A modeling approach was identified for the requirements specification.
  - A prototype translator was developed and used to convert, into HOL, suitably formatted descriptions written in the simulation language M.
SUMMARY OF PROBLEMS ENCOUNTERED:

- Some standard HOL low-level component models failed to work correctly when applied to the PIU design.
  - Fixed by straightforward modifications to the models.

- Transaction-level behavior of the PIU cannot be modeled as single state transitions of a finite-state machine (FSM), thus it cannot be modeled using Windley's Generic Interpreter Theory.
  - Being addressed by Windley as part of NASA Contract Tasks 9 and 10.

- Generating the specification models for the PIU was a labor-intensive process requiring an enormous amount of effort and time.
  - The M-to-HOL translator developed by Windley will help in future specifications, but more work is needed in automating this process.

ABSTRACTION TECHNIQUES:

Temporal Abstraction: relating time at two different levels of a specification hierarchy.
Data Abstraction: relating data values at two different levels.

Example: Automating test result certification.

Correct behavior

Incorrect behavior

Formal methods have an important role to play in the aerospace industry:

Application: Correctness proofs for hardware, software, and system implementations.

Application: Representation of requirements and specifications.
(II has been suggested that 70% of our problems are associated with incomplete requirements and specifications.)

Difficult problems remain to be solved:

Problem: Modeling approaches for requirements and specifications need refinement and integration into existing specification hierarchies.
(For example, transaction-level model - how many others will be needed?)

Problem: Tools to efficiently generate correct formal specifications from industry-standard CAD models need development.

Problem: Tools to increase verification efficiency need development.
DO-178B and Formal Methods

George Finelli
Assistant Head, System Validation Methods Branch
NASA Langley Research Center
DO-178B AND FORMAL METHODS

George B. Finelli

Formal Methods Workshop
August 12, 1992
NASA Langley Research Center

RTCA BACKGROUND

- RTCA:
  - Requirements and Technical Concepts for Aviation
  - Formerly Radio Technical Commission for Aeronautics
  - Funded by FAA and industry to provide forums
  - Joint activity with European Organization for Civil Aviation
    Electronics (EUROCAE)
  - DO-178—Software Considerations in Airborne Systems and
    Equipment Certification (November 1981)
  - DO-178A (March 1985)
  - DO-178B:
    - Currently at Draft 7 ("Final Draft")
    - Process initiated October 1989
    - Final Pannel meeting—October 1992
    - Special Committee 167—Digital Avionics Software

SC-167 BACKGROUND

- Open public forum
- Terms of Reference (TOR) derived between RTCA and FAA
- Plenary and Working Group Meetings
- EUROCAE "shadow" meetings, than joint meetings (January 1991)
- 5 Working Groups:
  - System Issues
  - Software Development
  - Software Verification
  - Quality Assurance and Configuration Management

TABLE OF CONTENTS

1.0 Introduction
2.0 System Aspects Relating to Software Development
3.0 Software Life Cycles
4.0 Software Planning Process
5.0 Software Development Processes
6.0 Software Development Process
7.0 Software Configuration Management
8.0 Software Quality Assurance Process
9.0 Certification Liaison Process
10.0 Airborne System
11.0 Software Life Cycle Data
12.0 Additional Considerations
HISTORY OF TEXT ON FORMAL METHODS

- Topic addressed by Working Group 2 (Software Verification) under TOR 2 (…nature and degree of analysis, verification, test...activities.)
- Succession of position papers and presentations on Formal Methods
- Received working group joint approval
- Decided in plenary to become part of Alternative Methods section
  (under control of WG2)
- Received joint approval with Working Group 2
- Received Plenary approval
- First appeared in Draft 6, April 1992
- Currently Draft 7 has been released for final review
  - RTCA Phone: 202-833-9339; FAX 202-833-9434

SUMMARY OF FORMAL METHODS SECTION

- Introductory paragraphs (2) describing general concepts, objectives, and relationship to testing
- Discussion of factors to consider in applying Formal Methods
  - Framework for trade-off against other methods
  - Not an "all-or-nothing" proposition

FORMAL METHODS TEXT

12.0 ADDITIONAL CONSIDERATIONS

12.3 ALTERNATIVE METHODS—General guidance for using alternative methods "...to replace or supplement methods used to satisfy one or more objectives of this document"

12.3.1 FORMAL METHODS

FORMAL METHODS APPLICATION FACTORS

1. Levels of Design Hierarchy

2. Coverage of software requirements and software architecture

3. Degree of rigor

[Diagram of Formal Methods Application Factors]
Introduction to
the Boyer–Moore Theorem Prover

Warren Hunt
Computational Logic, Inc.
The Nqthm Logic and Theorem Prover

J Strother Moore

April, 1992

Outline

In this talk we will sketch

• the Nqthm logic,
• its use to formalize and reason about computing machines, and
• the Nqthm mechanization.

Background

"Nqthm" is the name of both

• a mathematical logic and
• a computer program that mechanizes deduction in that logic.

Nqthm is sometimes called "the Boyer-Moore system."

The Nqthm Logic

The Nqthm logic is

• a first-order, quantifier-free logic providing
• inductively defined data types (e.g., integers and lists) and
• recursively defined functions.

In general, a mathematical logic is defined by

- a formal language,
- a set of axioms expressing assumed truths in the language, and
- a set of inference rules permitting the derivation of "new" truths from "old" ones.

Nqthm also contains extension principles by which one can soundly add new axioms to the logic.

Infix Syntax

\[(\text{QUOTIENT \ (T IMES \ N \ (SUB1 \ N)) \ 2})\]

is printed as

\[(n \times (n - 1)) / 2.\]

\[(\text{IMPLIES \ (PROPER-\text{LISTP} \ X) \ \ (E QUAL \ (REVERSE \ (REVERSE \ X)) \ X))}\]

is printed as

\[\text{proper-listp}(x) \rightarrow \text{reverse} (\text{reverse}(x)) = x.\]

The Nqthm Language

A term is either a variable symbol or an n-ary function symbol followed by n terms. We enclose function applications in parentheses.

Here are some Nqthm terms:

\[(\text{QUOTIENT \ (T IMES \ N \ (SUB1 \ N)) \ 2})\]

\[(\text{IMPLIES \ (PROPER-\text{LISTP} \ X) \ \ (E QUAL \ (REVERSE \ (REVERSE \ X)) \ X))}\]

Boyer and Moore's Personal Thoughts on Infix

Infix is provided to help us communicate our results to those who do not happily read Lisp.

We think that serious users of the theorem prover would be harmed more than helped by its adoption as the interface syntax.
Axioms  

Propositional Calculus and Equality  

AXIOM: true() ≠ false() (abbreviated by t ≠ f)  

AXIOM: x = f → if x then y else z endif = z.  

AXIOM: x ≠ f → if x then y else z endif = y.  

DEFINING AXIOM:  

\[ p \land q \]  

≡  

if \( p \)  

then if \( q \) then t else f endif  

else f endif.  

etc.

---

Ordered Pairs (Lists)  

AXIOM: listp(cons(x, y)).  

AXIOM: car(cons(x, y)) = x.  

AXIOM: cdr(cons(x, y)) = y.  

AXIOM: ¬ listp(x) → car(x) = 0.  

AXIOM: ¬ listp(x) → cdr(x) = 0.  

etc.

---

Peano Arithmetic  

AXIOM: zero() ∈ N (abbreviated by 0 ∈ N)  

AXIOM: add1(x) ∈ N.  

AXIOM: add1(x) ≠ 0.  

AXIOM: \( x ∈ N \rightarrow \text{sub1}(\text{add1}(x)) = x. \)  

etc.

---

Rules of Inference  

In addition to the rules of inference for propositional calculus and equality, Nqthm provides  

- Instantiation. From the theorem \( p(x) \) one may derive the theorem \( p(\alpha) \) for any term \( \alpha \).  
- Induction. For example, from the theorem \( p(0) \) and the theorem \( (x ∈ N \land x ≠ 0 \land p(x-1)) \rightarrow p(x) \), one may derive the theorem \( (x ∈ N) \rightarrow p(x) \).
Extension Principles

- Shell Principle. One may add axioms defining new inductively constructed "data types" following a certain schema.

- Constraint Principle. One may add axioms introducing new function symbols with arbitrary properties provided one exhibits old function symbols ("witnesses") with those properties.

- Definitional Principle. One may add axioms defining new recursive functions provided certain syntactic restrictions are met and each recursion can be proved to terminate.

Suppose 'step' is the state transition function.

Then the machine is formalized with:

\[
\text{DEFINITION:} \\
m(s, n) = \\
\text{if } n = 0 \\
\quad \text{then } s \\
\text{else } m(\text{step}(s), n-1) \text{ endif.}
\]

A theorem about this machine is:

\[
\text{THEOREM:} \\
m(s, i+j) = m(m(s, i), j).
\]

Using Nqthm Logic to Formalize a Computing Machine

Shell Introduction.

Let a state be constructed by \( st(pc, stk, mem, haltedp, defe) \), where

- \( pc \) is the location, in defe, of the "current instruction;"
- \( stk \) is a stack recording the currently active subroutine calls;
- \( mem \) is a list recording the values of successive memory locations;
- \( haltedp \) is a flag indicating whether the state is "running," "halted," or "erroneous;"
- \( defe \) is a list of programs, each of which is a named list of instructions.
An example state is

\[
\text{st}(' (\text{main} . 0), \text{nil},
\text{'}(0\ 1\ 2\ 3\ 4\ 5\ 6\ 7\ \ldots),
\text{f},
\text{'}((\text{main} (\text{movi} 0\ 77)
\text{movi} 1\ 88)
\text{call}\ \text{times}
\text{ret}))
\text{(times}\ \text{movi} 2\ 0)
\text{jump} 0\ 5
\text{add} 2\ 1
\text{subi} 0\ 1
\text{jump} 1
\text{ret}))
\]

We define the state transition function, 'step', so that it takes a state and returns the 'next' state.

\[
\text{DEFINITION:}
\text{step}(s) =
\text{if haltedp}(s)
\text{then } s
\text{else execute(fetch(pc(s), def(s)), s) endif,}
\]

where

\[
\text{DEFINITION:}
\text{execute}(x, s) =
\text{let } op = \text{if } \text{movi} \text{then movi(a, b, s)
else op = 'add then add(a, b, s)
else op = 'jump then jump(a, b, s)
else op = 'call then call(a, s)
else ... endif
endlet.
\]
Another theorem about 'm' is

**THEOREM:**
\[ r_0 \in \mathbb{N} \]
\[ \text{fetch}(pc, defs) = ' \text{(call times)} \]
\[ \text{assoc}' \text{times}, defs)' = ' \text{times} \]
\[ \begin{cases} \text{(movi 2 0)} & \text{(jumpz 0 5)} \\
\text{(add 2 1)} & \text{(subi 0 1)} \\
\text{(jump 1)} & \text{(ret)} \end{cases} \]
\[ \rightarrow \]
\[ m(st(pc, stk, \text{list}^*(r_0, r_1, r_2, \text{mem}), f, \text{def}s), 4+4\times r_0) \]
\[ = st(\text{add1-pc}(pc), stk, \text{list}^*(0, r_1, r_2, \text{mem}), f, \text{defs}). \]

---

The machine 'm' is unrealistically simple. More interesting machines have been defined in the Nqthm logic:

- NDL (hardware description language of LSI Logic, Inc.)
- FM8502 (a microprocessor designed and verified by CLI)
- Pito (a stack-based assembly language)
- Micro-Gypsy (a subset of Gypsy)
- KIT (a multiprocessor implemented on a uniprocessor)
- FM9001 (a microprocessor designed, verified, and fabricated by CLI)
- MC68020 (a commercial microprocessor by Motorola, Inc.)

---

**Execution of Nqthm Logic**

\[ s_0 \]

\[ m(s_0, 315) \]

\[ \begin{align*}
\text{st}'(\text{main . 0}), \\
\text{nil}, \\
'(0 1 2 3) \\
f, \\
'(\text{main} \\
\text{(movi 0 77)} \\
\text{(movi 1 88)} \\
\text{(call times)} \\
\text{(ret)}) \\
\text{times} \\
\text{(movi 2 0)} \\
\text{(jumpz 0 5)} \\
\ldots
\end{align*} \]

---

Given two formalized machines, 'hi' and 'lo,' one can derive relations between them, e.g.,

**THEOREM:**
\[ \text{good-hi-statep}(s) \rightarrow \text{hi}(s, n) = \text{up}(\text{lo}(\text{down}(s), \text{clk}(s, n))). \]
The CLI Short Stack (1987)

Input to COMPIL

Functional Instantiation (a derived inference rule)

The Output of REIFY

THEOREM:
\[ m(s, i+j) = m(m(s, i), j). \]

can be constructed without knowing anything about 'step.'

It is a general property of any "iterated step function," i.e., any 'm' whose definition is

DEFINITION:
\[ m(s, n) = \]

if \( n = 0 \)
then \( s \)
else \( m(step(s), n-1) \) endif,

for some 'step' function.
This can be formalized by

- introducing 'step' without defining it (i.e., by constraining it to be any function);
- defining 'm' in terms of the undefined 'step'; and then
- proving $m(s, i+j) = m(m(s, i), j)$.

If you functionally instantiate

**DEFINING AXIOM:**

\[
m(s, n) =
\begin{align*}
&\text{if } n = 0 \\
&\text{then } s \\
&\text{else } m(\text{step}(s), n-1) \text{ endif},
\end{align*}
\]

replacing 'm' by 'Ada' and 'step' by 'Ada-step,' you get

**THEOREM:**

\[
\text{Ada}(s, n) =
\begin{align*}
&\text{if } n = 0 \\
&\text{then } s \\
&\text{else } \text{Ada}(\text{Ada-step}(s), n-1) \text{ endif}.
\end{align*}
\]

Suppose later some very complicated machine, e.g., 'Ada', has been defined in terms of some very complicated 'Ada-step.' It is possible to derive

\[
\text{Ada}(s, i+j) = \text{Ada}(\text{Ada}(s, i), j).
\]

from

\[
m(s, i+j) = m(m(s, i), j)
\]

by functional instantiation, replacing 'm' by 'Ada' and 'step' by 'Ada-step,'

provided one can show that the axioms used in the original proof are true of the new functions.

**The Nqthm Theorem Prover**

The Nqthm system is an interactive computer program which can be used to help discover and check proofs of theorems in the Nqthm logic.

Some facts about Nqthm:

- It is fully documented in *A Computational Logic Handbook*.
- It is distributed without fee (but under license) by CLI.
- It is heavily used at CLI and elsewhere to formalize and reason about computational problems.
Nqthm consists of about 1 Mb of Common Lisp source code developed by Boyer and Moore (often in response to users' needs or suggestions) over the past 21 years.

There are over 16,000 theorems in its standard benchmark now. These 11 Mb of examples, contributed by 20 users, are distributed with the system.

Nqthm's behavior is determined by previously proved theorems.

The theorem
proper-listp(x) → reverse(reverse(x)) = x,
when used as a rewrite rule, is interpreted to mean:
replace "reverse(reverse(x))"
by "x,
provided "proper-listp(x)" can be established.
The experienced user "programs" proof strategies into Nqthm by carefully selecting the theorems to be proved.

A typical interchange between the user and Nqthm:

- The user submits a theorem to prove.
- Nqthm applies its proof techniques, guided by its data base. It prints a running commentary on its progress.
- The user reads the commentary and discovers that Nqthm is failing because it does not "know" a certain rule.
- The user aborts the proof.
- The user formulates the appropriate theorems and starts over.

**THEOREM:** app(app(a, b), c) = app(a, app(b, c)).

Proof. Call the conjecture *1. Perhaps we can prove it by induction. Three inductions are suggested by terms in the conjecture. They merge into two likely candidate inductions. However, only one is unflawed. We will induct according to the following scheme:

\((\text{listp}(a) \land \text{p}(\text{cdr}(a), b, c)) \rightarrow \text{p}(a, b, c))\)

\((\neg \text{listp}(a) \rightarrow \text{p}(a, b, c)).\)

Linear arithmetic and the lemma cdr-leafp can be used to prove that the measure count(a) decreases according to the well-founded relation '<' in each induction step of the scheme. The above induction scheme leads to two new goals:

**Case 2.** (listp(a) ∧ app(app(cdr(a), b), c) = app(cdr(a), app(b, c)))

\(→ \text{app}(a, b, c) = \text{app}(a, \text{app}(b, c)),\)

which simplifies, applying the lemmas cdr-cons and car-cons, and opening up the definition of 'app', to 1.

**Case 1.** ¬listp(a) → app(app(a, b), c) = app(a, app(b, c)),

which simplifies, unfolding the function 'app', to 1.

That finishes the proof of *1. Q.E.D.
Experience users generally use a mixed strategy in which the basic outline of the proof is discovered "off-line," and subsequent theorem proving allows gaps to be filled. 

**Lemma 1.1.1**
LEMMA 1.2
THEOREM 1
LEMMA 2.1
THEOREM 2
MAIN THEOREM

Each theorem proved adds one or more new rules to the data base. **Lemma 1.1.1** (rule 1.1.1)
LEMMA 1.2 (rule 1.1.2)
THEOREM 1 (rule 1.2.1)
THEOREM 2 (rule 2.1.1)
MAIN THEOREM (rule 3.1.1)

Experience used Nqthm as a very helpful assistant. Some users experience Nqthm as a very helpful assistant.

**Proof Maintenance**

The user who initially submits the theorems, in this order (due to thorough analysis of the problem) experiences difficulties discovering the MAIN THEOREM or a proof checker. The user who starts by submitting the MAIN THEOREM and is forced by the theorem prover to discover difficulties discovering the MAIN THEOREM or a proof checker.

**Interaction Styles**

Such users experience Nqthm as unhelpful. Experience Nqthm as unhelpful.
When the main theorem is changed "slightly" the old strategy often still works.

LEMMATA 1.1.1 (rule 1.1.1)
LEMMATA 1.1 (rule 1.1)
LEMMATA 1.2 (rule 1.2)
THEOREM 1 (rule 1)
LEMMATA 2.1 (rule 2.1)
THEOREM 2 (rule 2)
THEOREM 3 (rule 3)
MAIN THEOREM

If not, the failure leads, via the normal process, to a reformulation of some of the lemmas.

Nqthm-1992

We are about to release a new version of Nqthm, providing:

- constrained function introduction,
- functional instantiation,
- support for enabling/disabling theories,
- \texttt{cond}, \texttt{case}, \texttt{let}, \texttt{list*}, and "backquote" notation,
- improved performance on large case analyses,
- improved performance when many rules are disabled,
- "endorsement" tools for event scripts,
- over 11Mb of endorsed example scripts, and
Introduction to PVS

Natarajan Shankar
SRI International
This talk is a short tutorial on specification and verification, using PVS as an illustrative example.

- Background to PVS
- Overview of PVS
- Some Examples

Background: Past Experience

Considerable accumulated experience on verification at SRI

Systems developed at SRI include: Boyer-Moore Prover, HDM, OBJ, STP, EHDM, etc.

Other Systems used include: Affirm, RRL, Gypsy, Muse, etc.

Verifications include: Byzantine fault-tolerant clock synchronization, Byzantine Agreement, Gödel's first incompleteness theorem, and many others.

Background: EHDM

Designed at SRI around 1984.

A specification environment based on higher-order logic with parametric modules, implementation mappings, Hoare logic prover, etc.

Theorem prover based on skolemization, manual instantiation, and Shostak's decision procedures.

Example verifications include: Byzantine fault-tolerant clock synchronization, Ramsey theorem, Byzantine Agreement, Fault-masking and Transient recovery, etc.
**Background: Lessons Learnt**

Decision procedures are extremely useful but only a small part of what is needed.

Highly automatic theorem provers are inappropriate: difficult to control, and provide very little useful feedback.

Low-level proof checkers are inefficient (both in machine and human terms), and also fail to yield a satisfactory proof.

Logics with limited expressibility are easily mechanizable, but place a large burden on the specifier.

Some highly expressive notations are nice for pencil-and-paper work, but might be difficult to adequately mechanize.

**PVS**

Started in mid-1990.

The goal was to combine clear notation with a productive proof development environment to produce machine-checked, yet "humanly readable" proofs.

PVS was primarily influenced by EHDM, but also adapts ideas on language and inference from IMPLY, Boyer-Moore prover, LCF, HOL, ML, Nuprl, Veritas, OBJ, and many other systems.

PVS consists of a core language definition, parser, typechecker, and proof checker.

Contributors to PVS include Sam Owre, John Rushby, Friedrich von Henke, David Cyrluk, Judy Crow, Carl Witty, and Steven Phillips.

**PVS: Overview**

PVS has been used to check proofs of
- the Boyer-Moore majority algorithm
- ordered binary tree insertion
- a version of the Schröder-Bernstein theorem
- Byzantine Agreement
- a pipelined processor (due to Saxe), and other hardware examples.

These proofs can typically be completed in less than a day.

**Overview: Decision Procedures**

PVS proofs make heavy use of arithmetic decision procedures. Any THEOREM below is automatically proved. CONJECTURES are either false or unproved by decision procedures.

```plaintext
arithmetic : THEORY
BEGIN
  x,y,v: VAR number
  arith: THEOREM
    x < 2*v AND y < 3*v IMPLIES 3*x < 10*v
  hadarith: CONJECTURE
    x < 2*v AND y < 3*v IMPLIES 3*x < 17*v
  hadarithb: CONJECTURE
    x=0 AND y=0 IMPLIES x=y=0
  haddiv: CONJECTURE
    (x/y) > 5 IMPLIES y > (x+y)
  gooddiv: CONJECTURE
    y=0 AND (x/y) > 5 IMPLIES x > (x+y)
  anotherdiv: THEOREM
    y /= 0 AND (x/y) > 5 IMPLIES ((x+y)/y) > 0
  i, j, k: VAR int
  instrath: THEOREM
    2*i < 5 AND i > 1 IMPLIES i = 2
  hadarithb: CONJECTURE
    2*x < 5 AND x > 1 IMPLIES x = 2
END arithmetic
```
Type Correctness Conditions

Denominator for division must be non-zero.
Typechecking the previous theory generates type correctness conditions. baddiv.TCC is not provable, hence a type error.

```
begin
  x, y, z: VAR number
end

badarith: CONJECTURE
  x * y AND y < 5 IMPLIES x < 5
```

```
bigarith: CONJECTURE
  x * y AND y < 5 IMPLIES x < 15
```

```
baddiv: CONJECTURE
  (x / y) > v IMPLIES x > (y * v)
```

```
% Subtype TCC generated for y
baddiv, TCC: OBVIOUS (FORALL (y: number): y < 0)
```

```
gooddiv: CONJECTURE
  y = 0 AND (x / y) > v IMPLIES (x > v)
```

```
anotherdiv: THEOREM
  y = 0 AND (x / y) > (v / y) IMPLIES ((x - v) / y) > 0
```

```
s, j, k: VAR int
```

```
interarith: THEOREM 2 * 0 AND 1 IMPLIES x > 0
```

```
badarith2: CONJECTURE 2 * x < 0 IMPLIES x < 0
```

END arithmetic
```

Example: Binary Trees

Binary trees can be defined as abstract datatypes.

The following datatype declaration introduces the constructor leaf with recognizer leaf?, and constructor node with accessors val, left, and right, and recognizer node?.

Typechecking this datatype declaration generates the theories binary_tree.adt and binary_tree_rec.mod (shown below).

```
binary_tree[T: TYPE] : DATATYPE
begin
  leaf : leaf?
  node(val: T, left: binary_tree, right: binary_tree) : node?
end binary_tree
```

```
abstract datatype theory

binary_tree_adt[T: TYPE] : THEORY
begin
  binary_tree: TYPE
  leaf, node: PROD(binary_tree)
  leaf: (leaf?)
  node: (node?)

  node(T, binary_tree, binary_tree -> (node?)

  val: (node?) -> T
  left: (node?) -> binary_tree
  right: (node?) -> binary_tree

  leaf_extensionality: AXIOM (FORALL (leaf_var: leaf?): leaf = leaf_var)
  node_extensionality: AXIOM
    (FORALL (node?, var: (node?): node?)
      node(val(node?, var), left(node?, var), right(node?, var))
      = node?, var)

  val, node: AXIOM
    (FORALL (node?, var: T), (node2, var: binary_tree),
      (node3, var: binary_tree):
      val(node(node?, var, node2, var, node3, var))
      = node?, var)

  left, node: AXIOM
    (FORALL (node?, var: T), (node2, var: binary_tree),
      (node3, var: binary_tree):
      left(node(node?, var, node2, var, node3, var)) = node2, var)

  right, node: AXIOM
    (FORALL (node?, var: T), (node2, var: binary_tree),
      (node3, var: binary_tree):
      right(node(node?, var, node2, var, node3, var)) = node3, var)
```

```
binary_tree_disjoint: AXIOM
  (FORALL (node?, var: binary_tree):
    NOT (leaf?(binary_tree_var) AND node?(binary_tree_var)))
```

```
binary_tree_inclusive: AXIOM
  (FORALL (binary_tree_var: binary_tree):
    leaf?(binary_tree_var) OR node?(binary_tree_var))
```

```
binary_tree_induction: AXIOM
  (FORALL (p: PROD(binary_tree)):
    p(leaf)
    AND
    (FORALL (node?, var: T), (node2, var: binary_tree),
      (node3, var: binary_tree):
      p(node2, var) AND p(node3, var)
      IMPLIES p(node(node?, var, node2, var, node3, var)))
    IMPLIES (FORALL (binary_tree_var: binary_tree): p(binary_tree_var))
```

152
Ordered Binary Trees

Example Proof

Recursion combinator
Ordered? insert.1:

[-1] ordered?(leaf)

---------
[1] ordered?(node(s, s, leaf, leaf))

Rule? (rewrite "ordered?" +)
Rewriting using ordered?,
this simplifies to:
ordered?.insert.1:

[-1] ordered?(leaf)

---------
[1] (checkall(LAMBDA (y: T): y = x, leaf)
AND checkall(LAMBDA (y: T): x < y, leaf)
AND ordered?(leaf) AND ordered?(leaf))

Rule? (assert)
Inserting decision procedures,
this simplifies to:
ordered?.insert.1:

[-1] ordered?(leaf)

---------
[1] checkall(LAMBDA (y: T): y = x, leaf)
AND checkall(LAMBDA (y: T): x < y, leaf)

Rule? (auto-rewrite "binary_tree_rec[T, booq]")
Installing automatic rewrite:
binary_tree_rec[T, booq],
this simplifies to:
ordered?.insert.1:

[-1] ordered?(leaf)

---------
[1] checkall(LAMBDA (y: T): y = x, leaf)
AND checkall(LAMBDA (y: T): x < y, leaf)

ordered?.insert.2:

---------
[1] (FORALL (nodal.var: T), (node2.var: binary.tree),
(node3.var: binary.tree):
(FORALL (x: T):
ordered?(node2.var) IMPLIES ordered?(insert(x, node2.var)))
AND
(FORALL (x: T):
ordered?(node3.var) IMPLIES ordered?(insert(x, node3.var)))
IMPLIES
(FORALL (x: T):
ordered?(node1.var, node2.var, node3.var))
IMPLIES ordered?(insert(x, node(node1.var,
node2.var, node3.var))))

Rule? (skolem?)
For the top quantifier in 1, we introduce Skolem constants:
(node1.var!4 node2.var!6 node3.var!8)
this simplifies to:
ordered?.insert.2:

---------
[1] (FORALL (x: T):
ordered?(node2.var!6) IMPLIES ordered?(insert(x, node2.var!6)))
AND
(FORALL (x: T):
ordered?(node3.var!8) IMPLIES ordered?(insert(x, node3.var!8)))
IMPLIES
(FORALL (x: T):
ordered?(node1.var!4, node2.var!6, node3.var!8))
IMPLIES ordered?(insert(x, node(node1.var!4,
node2.var!6, node3.var!8)))

Rule? (skolem?)
For the top quantifier in 1, we introduce Skolem constants: (s?)
this simplifies to:
ordered?.insert.2:

---------
[1] (FORALL (x: T):
ordered?(node2.var!6) IMPLIES ordered?(insert(x, node2.var!6)))
AND
(FORALL (x: T):
ordered?(node3.var!8) IMPLIES ordered?(insert(x, node3.var!8)))
IMPLIES
(FORALL (x: T):
ordered?(node1.var!4, node2.var!6, node3.var!8))
IMPLIES ordered?(insert(x!7, node(node1.var!4,
node2.var!6, node3.var!8)))
Rule7 (rewrite "ordered?" +)
Rewriting using ordered?,
this simplifies to:
ordered?, insert, 2 :
[-1] (FORALL (x: T):
ordered?((node2.var;6)
IMPLIES ordered?(insert(x, node2.var;6))))
[-2] (FORALL (x: T):
ordered?((node3.var;6)
IMPLIES ordered?(insert(x, node3.var;6))))

------
(1) (checkall(λ(y: T): y <= node1.var;4, node2.var;6)
AND ordered?((node2.var;6)
AND ordered?((node3.var;6)))
IMPLIES ordered?(insert(x17, node1.var;4, node2.var;6, node3.var;6)))

Rule7 (dahump)
Applying disjunctive simplification,
this simplifies to:
ordered?, insert, 2 :
[-1] (FORALL (x: T):
ordered?((node2.var;6)
IMPLIES ordered?(insert(x, node2.var;6))))
[-2] (FORALL (x: T):
ordered?((node3.var;6)
IMPLIES ordered?(insert(x, node3.var;6))))
[-3] checkall(λ(y: T): y <= node1.var;4, node2.var;6)
[-4] checkall(λ(y: T): y <= node1.var;4, node2.var;6)
[-5] ordered?((node2.var;6)
[-6] ordered?((node3.var;6)

------
(1) ordered?(insert(x17, node1.var;4, node2.var;6, node3.var;6))

ordered?, insert, 2 :
[-1] (FORALL (x: T):
ordered?((node2.var;6)
IMPLIES ordered?(insert(x, node2.var;6))))
[-2] (FORALL (x: T):
ordered?((node3.var;6)
IMPLIES ordered?(insert(x, node3.var;6))))
[-3] checkall(λ(y: T): y <= node1.var;4, node2.var;6)
[-4] checkall(λ(y: T): y <= node1.var;4, node2.var;6)
[-5] ordered?((node2.var;6)
[-6] ordered?((node3.var;6)

------
(1) ordered?(insert(x17, node1.var;4, node2.var;6, node3.var;6))

Rule7 (HM-H)
Lifting IF-conditions to the top level,
this simplifies to:
ordered?, insert, 2.1 :
[-1] x17 <= node1.var;4
[-2] (FORALL (x: T):
ordered?((node2.var;6)
IMPLIES ordered?(insert(x, node2.var;6))))
[-3] (FORALL (x: T):
ordered?((node3.var;6)
IMPLIES ordered?(insert(x, node3.var;6))))
[-4] checkall(λ(y: T): y <= node1.var;4, node2.var;6)
[-5] checkall(λ(y: T): y <= node1.var;4, node2.var;6)
[-6] ordered?((node2.var;6)
[-7] ordered?((node3.var;6)

------
(1) ordered?(insert(x17, node1.var;4, node2.var;6, node3.var;6))

Rule7 (rewrite "ordered?" +)
Rewriting using ordered?,
this simplifies to:
ordered?, insert, 2.1 :
[-1] x17 <= node1.var;4
[-2] (FORALL (x: T):
ordered?((node2.var;6)
IMPLIES ordered?(insert(x, node2.var;6))))
[-3] (FORALL (x: T):
ordered?((node3.var;6)
IMPLIES ordered?(insert(x, node3.var;6))))
[-4] checkall(λ(y: T): y <= node1.var;4, node2.var;6)
[-5] checkall(λ(y: T): y <= node1.var;4, node2.var;6)
[-6] ordered?((node2.var;6)
[-7] ordered?((node3.var;6)

------
(1) checkall(λ(y: T): y <= node1.var;4, node2.var;6)
AND checkall(λ(y: T): node1.var;4 <= y, node3.var;6)
AND ordered?((insert(x17, node2.var;6),
node3.var;6))
Rule? (quant7)

Found substitution:
x gets s7,

Instatiating quantified variables, this simplifies to:

 ordered?.insert.2.1:

-1) ordered?(insert(s7, node2.var16))
-2) s7 <= node1.var14
-3) (forall (x: T):
     ordered?(insert(x, node2.var16))
     implies ordered?(insert(x, node3.var16)))
-4) checkall((lambda (y: T): y <= node1.var14), node2.var16)
-5) checkall((lambda (y: T): model.var14 <= y), node3.var16)
-6) ordered?(node2.var16)
-7) ordered?(node3.var16)

-----------

1) checkall((lambda (y: T): y <= node1.var14), model.var14)
   and checkall((lambda (y: T): model.var14 <= y), node3.var16)
   and ordered?(insert(s7, node2.var16))
   and ordered?(node3.var16)

Rule? (rewritre "ordered7" -)

Rewriting using ordered?, this simplifies to:

 ordered?.insert.2.2:

-1) (forall (x: T):
     ordered?(node2.var16)
     implies ordered?(insert(x, node2.var16)))
-2) ordered?(node2.var16)
-3) checkall((lambda (y: T): y <= node1.var14), node2.var16)
-4) checkall((lambda (y: T): model.var14 <= y), node3.var16)
-5) ordered?(node2.var16)
-6) ordered?(node3.var16)

-----------

1) s7 <= node1.var14
2) checkall((lambda (y: T): y <= node1.var14), node2.var16)
   and checkall((lambda (y: T): model.var14 <= y),
     insert(s7, node3.var16))
   and ordered?(node2.var16)
   and ordered?(insert(s7, node3.var16))

Rule? (quant7-2)

Found substitution:
x gets s7,

Instatiating quantified variables, this simplifies to:

 ordered?.insert.2.1:

-1) ordered?(insert(s7, node2.var16))
-2) s7 <= node1.var14
-3) ordered?(node3.var16)
-4) checkall((lambda (y: T): y <= node1.var14), node2.var16)
-5) checkall((lambda (y: T): model.var14 <= y), node3.var16)
-6) ordered?(node2.var16)
-7) ordered?(node3.var16)

-----------

1) checkall((lambda (y: T): node1.var14 <= y), node2.var16)
2) s7 <= node1.var14
Rule! (rewrite "ordered7_insert_step")

Rewriting using ordered7_insert_step, this simplifies to:

\[ \text{ordered7_insert.2.2} : \]

\[
\begin{align*}
[-1] & \text{ordered7(insert(s, node1.var16))} \\
[-2] & (\forall x: x \leq y \Rightarrow \text{ordered7(node2.var16)}) \\
[-3] & \text{checkall(\lambda y: y \leq node1.var16, node2.var16)} \\
[-4] & \text{checkall(\lambda y: y \leq node1.var16, node2.var16)} \\
[-5] & \text{ordered7(node2.var16)} \\
[-6] & \text{ordered7(node1.var16)} \\
\end{align*}
\]

\[ \text{----------------} \]

\[
\begin{align*}
[1] & \text{node1.var16 \leq x17} \\
[2] & \text{checkall(\lambda y: y \leq node1.var16, } \\
& \quad \text{insert(s, node3.var16)} \} \\
[3] & x17 \leq \text{node1.var16} \\
\end{align*}
\]

Rule? (typepred "obt.<='

Adding type constraints for obt.<=',

this simplifies to:

\[ \text{ordered7_insert.2.2} : \]

\[
\begin{align*}
[-1] & \text{ordered7(insert(s, node1.var16))} \\
[-2] & (\forall x: x \leq y \Rightarrow \text{ordered7(node2.var16)}) \\
[-3] & \text{checkall(\lambda y: y \leq node1.var16, node2.var16)} \\
[-4] & \text{checkall(\lambda y: y \leq node1.var16, node2.var16)} \\
[-5] & \text{ordered7(node2.var16)} \\
[-6] & \text{ordered7(node1.var16)} \\
\end{align*}
\]

\[ \text{----------------} \]

\[
\begin{align*}
[1] & \text{node1.var16 \leq x17} \\
[2] & \text{checkall(\lambda y: y \leq node1.var16, } \\
& \quad \text{insert(s, node3.var16)} \} \\
[3] & x17 \leq \text{node1.var16} \\
\end{align*}
\]

Rule? (prop$)

By propositional simplification,

This completes the proof of ordered7_insert.2.2.

This completes the proof of ordered7_insert.2.

Q.E.D.

Save the new proof? (Yes or No) yes

Would you like a brief printout of the proof? (Yes or No) yes

ordered7_insert.1:

\[ \text{----------------} \]

\[
\begin{align*}
[1] & \text{ordered7(leaf)} \Rightarrow \text{ordered7(insert(s, leaf))} \\
\end{align*}
\]

For the top quantifier in \( s \), we introduce Skolem constants: \( (x:3) \)

Applying disjunctive simplification,

Rewriting using insert, ordered7_insert.1.

Invoking decision procedures, instating automatic rewrites: binary.tree.rec, leave.

Splitting conjunctions, which yields 2 subgoals:

ordered7_insert.1.1:

\[ \text{----------------} \]

\[
\begin{align*}
[1] & \text{ordered7(leaf)} \\
\end{align*}
\]

Rewriting using checkall, ordered7_insert.1.1.

This completes the proof of ordered7_insert.1.1.

ordered7_insert.1.2:

\[ \text{----------------} \]

\[
\begin{align*}
[1] & \text{ordered7(leaf)} \\
\end{align*}
\]

Rewriting using checkall, ordered7_insert.1.2.

This completes the proof of ordered7_insert.1.2.
ordered?.insert.2

[1]

(FORALL (node1.var: T), (node2.var: binary.tree),
  (node3.var: binary.tree):
  ordered?(node2.var) IMPLIES ordered?(insert(s, node2.var)))
  AND
  (FORALL (s: T):
    ordered?(node3.var)
    IMPLIES ordered?(insert(s, node3.var)))
IMPLIES
  (FORALL (x: T):
    ordered?(node1.var, node2.var, node3.var)
    IMPLIES
    ordered?(insert(x, node1.var, node2.var, node3.var))))

For the top quantifier in 1, we introduce Skolem constants:
(node1.var14 node2.var16 node3.var16)
Applying disjunctive simplification.
For the top quantifier in 1, we introduce Skolem constants: (x17)
Rewriting using ordered?.
Applying disjunctive simplification.
Rewriting using insert.
Lifting IF-conditions to the top level.
By propositional simplification.
which yields 3 subgoals:

ordered?.insert.2.2

[1] (FORALL (s: T):
  ordered?(node2.var16)
  IMPLIES ordered?(insert(s, node2.var16)))
[2] (FORALL (s: T):
  ordered?(node3.var16)
  IMPLIES ordered?(insert(s, node3.var16)))
[3]  (checkall((LAMBDA (y: T): y < node1.var14), node2.var16))
  (checkall((LAMBDA (y: T): node1.var14 < y), node3.var16))
  ordered?(node2.var16)
  ordered?(node3.var16)
[4] x17 < node1.var14
[5] ordered?(node1.var14, node2.var16, insert(x17, node3.var16))

Rewriting using ordered?.
Instantiating quantified variables.
By propositional simplification.
Rewriting using ordered?.insert.1.
Adding type constraints for obj.4.
Rewriting using total.ordered?.
Instantiating quantified variables.
By propositional simplification.
This completes the proof of ordered?.insert.2.2.

Q.E.D.

Notes on the Language

The core logic is a simply typed higher-order logic.

Specifications are structured into parametric theories.
Types can be parameters.
Assumptions can be used to constrain the parameters.

Set-like predicate subtypes can be defined.
These make the domains and ranges of operations explicit.

Theorem proving is employed to carry out typechecking.

Automatic facility for generating abstract datatype theories.
Notes on the Proof checker

Sequent representation for proof goals.

Backwards proof construction by applying reductions.

Heavy use of powerful decision procedures for equality and inequality.

Powerful primitive inference steps.
Roughly twenty such steps.

Strategy mechanism for encapsulating proof patterns.

Ability to save and rerun proofs and partial proofs, and display proofs.

Conclusions

PVS exploits the synergy between language and inference.

The combination of powerful inference steps: decision procedures, rewriting, propositional simplification, etc., makes it effective to develop proofs that are both certified and convincing.

Future goals:

• To enhance the language to further exploit the inference capabilities
• To generate readable proof outlines
• To make proofs robust and easier to maintain
Logical Foundations of Computing over the Floating Point Reals

Richard Platek
Odyssey Research Associates, Inc.
Logical Foundations of Computations over the Reals

Richard Platek
Odyssey Research Associates
ORA

12 August 1992
NASA FM Workshop
Basic Problem

What does it mean to say that a given program "computes" a real valued function such as sine $x$ or $e^x$ when it never really does?

Classical answer:

The program computes an approximation which is "sufficiently accurate"

But what does that mean?
Two Fundamental Problem Areas

- Scientific Computations
  - simulations, calculation of engineering solutions, numerical experiments to explore theories, "number crunching" as part of experiments
  - correctness is vital for decision making

- Embedded Computations
  - computers as part of continuous systems
    - sense-compute-activate

Botton Up Interpretation

We reason at the level of the CPU and Floating Point processor so that we can calculate tight error bounds and we use numerical analysis techniques to estimate the accuracy of the computation.

Perfectly fine, but too concrete

A. Numerical Programs are not written in machine language or assembler. They are written in higher order languages like Fortran, C, Ada. The concrete analysis is not portable across CPU's.

B. The concrete analysis is not portable across FPP's. We should reason in terms of the IEEE floating point standard or the Brown model.

In particular, our specs and proofs should be independent of the word length of the machine reals except in so far as the word length is knowable at the programming language level (e.g., Ada's float'small)
Verifying floating point computations

- Algebraic properties of floating point operations are a mess; and detailed descriptions are highly implementation dependent.
- Little automated support exists.
- We are incorporating support for both quantitative and qualitative error analysis into Penelope.

This talk concerns qualitative error analysis.

Sources of error

- Roundoff error
- (Mathematical) Truncation error
- Implementation strategies (modeled by non-determinism)
Example of Compiler Implementation Strategies

In both C and Ada the statements

\[ x := y \times z; \]

\[ \text{if } x = y \times z \text{ then } w := 0 \text{ else } w := 1 \text{ end;} \]

may set \( w \) to either 0 or 1 !!!

---

Qualitative error analysis

Intuitively: prove programs under the assumption that various sources of error are present but "negligible"

Not equivalent to assuming that error is non-existent
Qualitative analysis of roundoff error: asymptotic correctness

Mathematical model via limits

If a program is run on increasingly accurate machines, then its answer approaches the specified result in the limit.

Mathematical model via algebra

Use a model of "approximate reasoning."

The algebraic model is easier to use

Algebra for approximate reasoning

Introduce additional predicates on the "real numbers"

\[ x \approx y \]  \( x \) is close to \( y \)
\[ x \not\approx y \]  \( x \) is not close to \( y \)
\[ x \lesssim y \]  \( x < y \) or \( x \) is close to \( y \)
\[ x \not\lesssim y \]  \( x < y \) and \( x \) is not close to \( y \)

Relations to standard operations

\[ x = y \Rightarrow x \approx y \]
\[ x \not\lesssim y \Rightarrow x < y \Rightarrow x \leq y \Rightarrow x \lesssim y \]
**Substitution in Approximate Reasoning**

If $f$ is continuous, $x \approx y \Rightarrow f(x) \approx f(y)$

Therefore,

$$x \approx x_1 \text{ and } y \approx y_1 \Rightarrow x + y \approx x_1 + y_1$$

But comparisons are not continuous

$$x \approx y \text{ and } x \leq z \text{ does not imply } y \leq z$$

---

**Algebra of approximate reasoning**

Mechanical translation of (many) facts of ordinary algebra to facts of approximate algebra.

For example:

$$(x + 1)^2 > x$$

translates to

$$(x + 1)^2 \geq x$$
**Modeling Ada floating point operations**

Introduce specification predicate for each basic operation

\[ fplus(x, y, z): \]

\[ z \text{ is a possible result of evaluating } x + y \]

Sample property:

\[ fplus(x, y, z) \Rightarrow z \approx x + y \]

\[ fle(x, y, b): \]

\[ b \text{ is a possible result of evaluating } x \leq y \]

Sample properties:

\[ fle(x, y, \text{true}) \Rightarrow x \leq y \]
\[ fle(x, y, \text{false}) \Rightarrow x \geq y \]

---

**Example specification and proof**

```plaintext
function mysqrt(a, small : in float) return float;

should compute the square root of a to within small
```
Naive specification of `mysqrt`

IN a \( \geq 0.0 \) and small \( > 0.0 \)
RETURN \( z \) SUCH THAT \( |z^2 - a| \leq \text{small} \)

Amended specification of `mysqrt`

IN a \( \geq 0.0 \) and small \( \geq 0.0 \)
RETURN \( z \) SUCH THAT \( |z^2 - a| \leq \text{small} \)
Calculation will use Newton's method

For any $a \geq 0$,

$$\sqrt{a} = \lim_{n \to \infty} x_n$$

where

$$x_0 = a + 1$$

$$x_{n+1} = \frac{1}{2}(x_n + a/x_n)$$

Code for mysqrt

```pascal
function mysqrt (...) is
  x : float;
begin
  if (a <= small) then
    return 0.0;
  end if;
  x := a + 1.0;
  while (x*x-a >= small) loop
    x := (x+(a/x))/2.0;
  end loop;
  return x;
end mysqrt;

Loop invariant annotation:

small, x, a, (x^2 - a) \geq 0.0```

© ORA Corp, 1992
Proving termination of the loop

Proving termination of the loop

Loop bound annotation:

loop bound \( x^2 - a \)
contraction 1/4
lower bound small

Accurate Square Root

function sqrt (a:= in float) return float

is

begin

return mysqrt (a, float'small);

end;
Embedded Systems

Want to be able to reason about computer controlled real world systems. Want to know what the system does in real space/time.

The total system can be described by logico-differential equations.

Example

State variables

\[ x(t : \text{Real}) : \text{Real} \]
\[ y(k : \text{Int}) : \text{Int} \]

Transition Relations

\[
\frac{dx}{dt} = f(x(t), y(t))
\]
\[ y(k+1) = g(x(t), y(k)) \]
\[ d_u = \text{max integer } \leq t \]
Formal Safety Analysis

Nancy Leveson
University of California at Irvine
A System Engineering Approach:

- Identify system hazards

- Evaluate or prioritize hazards

- As define required functionality and allocate to components:
  - Apply formal hazard analysis to emerging design
  - Optimize design for safety and other constraints
  - Identify and resolve potential conflicts

Results in identification of particular behaviors of individual components that could contribute to a system hazard.

- After completing allocation of functionality, do system and subsystem hazard analysis to ensure requirements specification of each component consistent with system safety constraints.

- Design and build components with safety constraints in mind (design safety into individual components).
A Safety-Oriented Software Methodology

- System Requirements Specification and Analysis
  Modelling language
  Analysis Criteria and Procedures

- System Hazard Analysis
  Determine whether system can reach a hazardous state if:
  - Performs as specified
  - Plausible or likely failures occur
  Special and standard hazard analysis techniques

- Design for Safety
  Design for protect against safety failures
  Analyze design for safety
  To aid in construction of safety features
  To minimize and protect safety-critical code
  To produce a verifiable and certifiable design.

- Code Verification
  Informal, formal, semi-formal techniques
  Software Fault Tree Analysis
Modelling language

Analysis Criteria and Procedures

- System Hazard Analysis
  Determine whether system can reach a hazardous state if:
  - Performs as specified
  - Plausible or likely failures occur

Special and standard hazard analysis techniques

- Design for Safety
  Design for protect against safety failures
  Analyze design for safety
  - To aid in construction of safety features
  - To minimize and protect safety-critical code
  - To produce a verifiable and certifiable design.

- Code Verification
  Informal, formal, semi-formal techniques
  Software Fault Tree Analysis
SOFTWARE HAZARD AND REQUIREMENTS ANALYSIS

SOFTWARE HAZARD ANALYSIS

1) If operates "correctly," will any hazardous states result?

2) If there are failures, will hazards result?

   Single failures?

   Multiple failures?
**Inductive Approaches**

- Reasoning from individual to general
- Determine what system states possible
- Postulate particular fault or initiating condition and attempt to ascertain effect on system operation
  
  e.g. How will loss of some particular control surface affect flight of aircraft

- For complex systems, impossible to identify all possible component failure modes

**Deductive Approaches**

- Reasoning from general to specific
- Determine how given system state can occur
- Postulate system has failed in certain way and try to find out what behavior could cause or contribute to it
  
  e.g. Plane crashes, what could have caused it?

**Figure 2. A Petri Net Graph with the Next State Shown**
Figure 4c: A Petri net graph with an interlock (I)

Reachability graph for Figure 4c
Adding Failures to the Analysis

Types of control failures:

- a required event that does not occur
- an undesired event
- an incorrect sequence of required events
- two incompatible events occurring simultaneously
- timing failures in event sequences
  - exceeding maximum time constraints between events
  - failing to ensure minimum time constraints between events
- durational failures

Figure 5a. Desired Event $t_1$ Does Not Occur

Figure 5b. Undesired Event $t_1$ Occurs
faulty state: every path to it from the initial state contains a failure transition.

Recoverable: after the occurrence of a failure, the control of the process is not lost, and in an acceptable amount of time, it will return to normal execution.

1) the number of faulty states is finite
2) there are no terminal faulty states
3) there are no directed loops containing only faulty states
4) the sum of the max times on all paths from the failure transition to a correct state is less than a predefined acceptable amount of time.

Correct behavior path: a path in the failure reachability graph from the initial state to a final state which contains no failure transitions.

Fault Tolerant Process:
1) a correct behavior path is a subsequence of every path from the initial state to any terminal state.
2) the sum of the maximum times on all paths is less than a predefined acceptable amount of time.

Fail-Safe: all paths from a failure F contain only low-risk states.
PETRI NET MODELS

Have developed analysis procedures to:

- identify hazards and safety-critical single and multiple failure sequences
- determine software safety requirements including timing requirements
- analyze the design for safety and fault tolerance
- guide in the use of failure detection and recovery procedures

Analysis of Completeness in Requirements Specification

- Most of accidents involve software requirements deficiencies. Many (if not most) of failures associated with requirements involve incompleteness.

- Completeness (informally): Requirements must be sufficient to distinguish the desired behavior of the software from that of any other, undesired program that might be designed.

- Completeness vs. sufficiency

- Relative to life cycle phase.
Approaches to finding errors in requirements specifications:

- Prototyping
- Executable specifications
- Scenarios
- Informal reviews
- Formal modeling and analysis

Build model of software behavior and its interface with other components and analyze to ensure behavior and properties of model match desired behavior and properties.

GENERAL APPROACH:

1) Model the:
   - Required black-box behavior of the software.
   - Interfaces with the rest of the system.
   - Basic assumptions about behavior of other components in system or environment.

2) Analyze model to:
   - Ensure modeled software behavior implements required control function.
   - Ensure modeled software behavior satisfies required constraints (including safety).
   - Ensure modeled system behavior is fault tolerant and robust in the event of component failures.
   - Identify and resolve conflicts and tradeoffs.

REQUIRES:

- A formal modeling language
- Analysis criteria and algorithms
- Validation on a realistic testbed
The RSM is denoted as a seven-tuple \((\Sigma, Q, q_0, P_T, P_O, \delta, \gamma)\) where:

- \(\Sigma\) is the set of input/output variables, \(I\) and \(O\).
- \(Q\) is the set of states of the control component \(C\).
- \(q_0 \in Q\) is the initial state of \(C\); the software is in this state before startup.
- \(P_T\) is the set predicates on the values and timing of the inputs \((I)\). They state change in the RSM.
- \(P_O\) is the set of predicates on the outputs \((O)\).
- \(\delta\) is the state transition function \(Q \times P_T\) to \(Q\).
- \(\gamma\) is the trigger-to-output relationship \(Q \times P_T\) to \(P_O\).
Figure 2: Block diagram of the temperature control system.

\[ I \uparrow ^\text{Low} \| \text{Out(Rod1, down)} \]

No Rods Moved

\[ I \uparrow ^\text{High} \| \text{Out(Rod1, down)} \]

Rod1 Moved

\[ \text{TimeOut(Rod1)} \]

Figure 3: A fragment of an RSM

\[ \text{Low} = v(I) < C^*K \]
\[ \text{High} = v(I) \geq C^*K \]

\[ \text{TimeOut}(x) = t > t(x) + 30 \]

\[ \text{Out}(O, x) = O \uparrow \land (v(O) = x) \]

**CRITERIA AND HEURISTICS**

- Input/Output variables (Σ)
- States (Q, q₀)
  - Startup and Shutdown Modes
- Trigger Predicates (Pᵣ)
  - Tautology Requirements
  - Essential Value Assumptions
  - Essential Timing Assumptions
  - Properly bounded ranges
  - Capacity and Load
  - Minimum arrival rates, etc.
Criterion 6.1 Every state must have a behavior (transition) defined for every possible input. Formally,

\[ \forall I, q \exists q_1, p : (\delta(q, p) = q_1) \land (p \in P_T) \]

where \( I \in \Sigma, q, q_1 \in Q \) and \( P_T \) is defined as in section 4.

Criterion 6.2 The logical OR (\( \lor \)) of the input predicates on the transitions out of any state must form a tautology:

\[ \models \lor p_i \]

where the \( p_i \)'s are the input predicates leading out of the state of interest.

Criterion 6.3 Every state must have a behavior (transition) defined in case there is no input for a given period of time, i.e., a timeout.

Criterion 6.4 The RSM must to be deterministic. Let \( p_i \) represent the input predicate on the \( i \)th transition out of a state. Then deterministic behavior is guaranteed by:

\[ \forall i \forall j (i \neq j) \Rightarrow \neg (p_i \land p_j) \]

- Output Predicates (\( P_O \))
  - Environmental capacity assumptions
  - Data Age
  - Latency

- Trigger-to-Output Relationship (\( \gamma \))
  - Graceful Degradation and Hysterisis
  - Responsiveness and Spontaneity (Feedback)
Transitions (δ)

Basic Reachability
Recurrent Behavior
Reversibility
Reachability of Safe States
Path Robustness
Constraint Analysis

**Reversibility**

Criterion 9.3  Reversibility of an operation \( x \) (performed in a state \( q_x \)) by an operation \( y \) (performed in a state \( q \in Q_x \)) requires a path between \( q_x \) and a state belonging to \( Q_y \). Formally,

\[
\exists q \exists s : (\delta(q_x, s) = q) \land (\phi(s)).
\]

where \( q \in Q_y \).

**Path Robustness**

Criterion 9.5  Soft and hard-failure modes should be eliminated for all hazard-reducing outputs. Formally, let \( Q_x \) and \( Q_y \) be the sets of states where actions \( x \) and \( y \) are performed. The loss of the ability to receive \( I \) is a soft-failure mode for the paths from action \( x \) to action \( y \) iff

\[
\exists q \forall q_1, s[(\delta(q, s) = q_1) \Rightarrow (\neg \phi(s) \lor I \top)]
\]

where \( q \in Q_x \) and \( q_1 \in Q_y \).

The loss of the ability to receive \( I \) is a hard-failure mode iff

\[
\forall q \forall q_1, s[(\delta(q, s) = q_1) \Rightarrow (\neg \phi(s) \lor I \top)]
\]

where \( q \in Q_x \) and \( q_1 \in Q_y \).
Path robustness and safety:

- Soft failure mode: loss of ability to receive an particular input could inhibit a particular output event.
- Hard failure mode: loss will inhibit the event.
- The more failure modes a set of requirements contains, whether soft or hard, the less robust will be the system that is correctly built to that specification.

Note that robustness in this sense is not only attribute that needs to be considered when specifying requirements and may not even be desirable, e.g., may conflict with safety.

An unsafe state should have at least one, and possibly several, hard failure modes for the production of an unsafe output command: No input received from proper authority, no weapons launch.

A fail-safe system should have no soft failure modes, much less hard ones, on paths between dangerous and safe states.

Criterion 9.4 There must be no paths to undesired hazardous states.

\[ \forall q_0, q_h, s \ (\delta(q_0, s) \neq q_h) \lor \neg \phi(s_i) \]

where \( q_0 \in Q_s \) and \( q_h \in Q_h \).

Criterion 9.5 Every path from a hazardous state must lead to a safe state:

\[ \forall q_h, s \ (\delta(q_h, s) = q) \land \phi(s_i) \Rightarrow (q \in Q_s) \]

Criterion 9.6 If a safe state cannot be reached from a hazardous state a path from that state must lead to minimum risk states

\[ \forall q_h \ (\forall q_0, s \ (\delta(q_0, s) \neq q_h) \lor \neg \phi(s_i)) \Rightarrow \forall s, q \ (\delta(q_h, s) = q) \land \phi(s_i) \Rightarrow q \in Q_{Min,\text{Risk}}) \]
TESTBED: TCAS II - Traffic Alert and Collision Avoidance System

- Family of airborne devices functioning independently of the ground-based ATC system.
- Provides traffic advisories to assist pilots in avoiding intruder aircraft.
- Provides resolution advisories (recommended escape maneuvers) in a vertical direction to avoid conflicting traffic.
- Communicates with intruder aircraft, TCAS systems, transponders on intruder aircraft, pilot, and ground-based radar beacon system.
- Used by airline aircraft and larger commuter and business aircraft.
- We will provide a system requirements specification and a safety analysis of the specification.

Design Criteria for the Same Line:

- Black box behavior only
- Simplicity
- Consistency, conciseness
- Unambiguous, unambiguous language must have a
- Readable, readable, readable, readable, readable, readable
- Use notation to best convey type of information
- Graphs, symbols, tables
- When necessary, choose usability over workability
- Information exposure
Contents

1 High Level Requirements
   1.1 Goals 6
   1.2 Constraints 15

2 Environment
   2.1 Component Communication Interfaces 30
   2.2 Communication Protocols 93
   2.3 Behavioral Assumptions 105

3 TCAS
   3.1 Own Aircraft 168
   3.2 Other Aircraft 193
   3.3 Mode S Ground Station 279

A Glossary 287
B Reference Algorithms 291
C Notation 307
Figure 1.2: Own-Aircraft
Variable: Own-Alt-Radio
Location: Own-Aircraft_10
Source: Radio Altimeter
Type: Integer
Expected Range: -20...2150
Granularity: 1...10 is acceptable
Units: Feet
Load: 1/s for CAS, (hardware sends more often)

Exception handling information: Need valid data indicator. CAS should have a period of coasting before ignoring radio altitude when data is no longer valid. Large negative values must be handled.

Description: Feet above ground level (AGL)
Comments: Hardware differ in available range. A smaller range will cause radio altitude status to become invalid at a lower altitude above ground than intended by the CAS logic, thus affecting logic switchpoints based on altitude above ground. Hardware can be analog or digital. Analog input to TCAS box is in a voltage range that must be converted to ft. Digital input is in binary via 429 data word.

Transition(s): Threat —> Other-Traffic
Location: Other-Aircraft = Intruder-Status_88
Trigger Event: Effective-SL-Evaluated-Event
Condition:

<table>
<thead>
<tr>
<th>AND</th>
<th>OR</th>
</tr>
</thead>
<tbody>
<tr>
<td>Other-Alt-Reporting_14 = True</td>
<td>F</td>
</tr>
<tr>
<td>Bearing-Valid_14</td>
<td>F</td>
</tr>
<tr>
<td>Range-Valid_14</td>
<td>F</td>
</tr>
<tr>
<td>Proximate-Traffic-Condition_133</td>
<td>F</td>
</tr>
<tr>
<td>Potential-Threat-Condition_124</td>
<td>F</td>
</tr>
</tbody>
</table>

Output Action: Intruder-Status-Evaluated-Event
Description:
Columns 1-2 Non-altitude-reporting and either the bearing or range inputs are invalid.
Column 3 Non-altitude-reporting and both range and bearing are valid, but neither the processor potential threat classification criteria are satisfied.
Macro: Proximate-Traffic-Condition
Definition:

<table>
<thead>
<tr>
<th>Condition</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Other-Air-Status_{46} in state airborne</td>
<td>T</td>
</tr>
<tr>
<td>Other-Tracked-Ranger_{46} &lt; 6.0 nm{PROXAB}</td>
<td>T</td>
</tr>
<tr>
<td>Other-Alt-Reporting_{46} = True</td>
<td>T</td>
</tr>
<tr>
<td>Own-Tracked-Alt_{154} ≥ 15500 ft{ABOVMMC}</td>
<td>T</td>
</tr>
<tr>
<td>Current-Vertical-Separation_{135} &lt; 1200 ft{PROXAB}</td>
<td>F</td>
</tr>
</tbody>
</table>

AND OR

Description: To be considered in Proximity the intruder must be within a range < 6.0 nm{PROXAB}. Additionally, if the intruder is altitude reporting, its relative altitude must be within 1200 ft{PROXAB}. If the intruder is not altitude reporting, then it considered proximate traffic only if own altitude is below 15500 ft{ABOVMMC} and the bearing and range reports are considered valid.

MOPS Ref. TRAFFIC_ADVISORY.Proximity_test.

Function: Climb-Goal
Return type: (-10000...+∞)
Definition:

\[
\text{Climb-Goal} = \begin{cases} 
-10000 \text{ ft/min}_{\text{P, CLIMB}} & \text{if } \text{Composite-RA}_{46} \text{ in state No-RA or} \\
-2000 \text{ ft/min}_{\text{P, CLIMB}} & \text{if } \text{Climb-VSL in state No-Climb-VSL or} \\
-1000 \text{ ft/min}_{\text{P, CLIMB}} & \text{if } \text{Climb-VSL in state VSL2000 or} \\
-500 \text{ ft/min}_{\text{P, CLIMB}} & \text{if } \text{Climb-VSL in state VSL1000 or} \\
0 \text{ ft/min}_{\text{P, CLIMB}} & \text{if } \text{Climb-VSL in state VSL500 or} \\
\text{max}(1500 \text{ ft/min}, \text{Alt-Rate-Pos-RA}_{46}\{\text{Each}\}) & \text{if } \text{Composite-RA}_{46} \text{ in state Climb-\text{Nomin} or} \\
2500 \text{ ft/min}_{\text{P, CLIMB}} & \text{if } \text{Composite-RA}_{46} \text{ in state Climb-\text{Incr} or} \\
\end{cases}
\]

Note: If Alt-Rate-Pos-RA_{46}[i] is not defined for Other-Aircraft_{77}[i], then do not consider it into the max above. Also note that all positive RA's are in the same direction.

Reference: MOPS: Determine_goal_rate (p. 389).
TOOLS

- **Simulator (Fall '92)**
  formal semantics definition of language done

- **Test Data Generator (Elaine Weyuker-NYU)**

- **Analysis Tools**
  [model checker]
  [automatic deduction]
  "completeness" and robustness checker
  (semantic analyzer)
  software hazard analyzer
  risk assessment and system hazard analyses
  e.g. FMEA
  FMECA
  Fault Trees

- **Development Tools**

ANALYSIS

- Software Hazard Analysis

- Semantic Analysis of Requirements
  "Completeness"
  Robustness

- System Engineering Analyses

ASSESSMENT
The FM9001

Warren Hunt
Computational Logic, Inc.
A Formal HDL and its use in the FM9001 Verification

Warren A. Hunt, Jr.
Bishop C. Brock

Computational Logic Incorporated
1717 West Sixth Street, Suite 230
Austin, Texas 78703-4776

Tel: +1 512 322 9951
FAX: +1 512 322 0656
Hunt@CLI.COM

Talk Topics

- Hardware Verification
- The FM9001
- Examples of our HDL
- The FM9001 proof effort
- Conclusions
Solution Approach

We use the Boyer-Moore logic as our hardware specification vehicle.

Some benefits of using a formal logic are:

- logic expressions are quite compact,
- single interpretation of each logical formula, and
- clearly defined set of axioms and rules of inference exists.

A mechanization of the Boyer-Moore logic, known as the Boyer-Moore theorem prover, provides us with:

- a definition and formula data-base manager,
- an automatic theorem prover and interactive proof checker, and
- the ability to execute our (hardware) definitions.

Hardware Verification: What Is It?

We envision providing a mathematical statement, which we call a formula manual, that completely specifies the operation of a hardware component.

With respect to digital systems, we want to:

- completely replace programmer's manuals,
- fully replace timing diagrams, interface specifications, power requirements, etc., with clear, precise formulas.

- provide a perfectly clear foundation upon which systems can be built.
Boyer-Moore Logic Usage

Within the Boyer-Moore logic we:
- axiomatize properties of digital logic circuits,
- formalize our HDL, and
- write specifications.

The mechanization of the logic insists on:
- uniqueness of definitions and
- rigorous proofs.

The mechanization allows very large proofs to be constructed—larger than can be carried out by hand.

The FM9001 Fabrication

This fabrication effort is a test-of-concept; that is, can we manufacture mathematically modeled circuits and get them working?

We are attempting to deal mathematically with as many engineering issues as possible; for example, our implementation description includes the test logic.

The FM9001 microprocessor is a 32-bit, general-purpose microprocessor with:
- 32-bit addressing,
- 16 general-purpose registers,
- two-address architecture,
- 5 addressing modes,
- a 16-function ALU, and
- conditional result assignment.
### The FM9001 Architecture

The FM9001 implementation architecture has:
- a pipelined, hard-wired control unit;
- a programmable program counter; and
- three asynchronous inputs: reset, data acknowledgement, and hold.

The FM9001 internal state (except for the register file) is connected together into a scan chain.

The FM9001 register file can be tested using the scan chain.

The next slide displays the FM9001 internal architecture.

---

**Table: Operation Codes**

<table>
<thead>
<tr>
<th>OP-CODE</th>
<th>OPERATION</th>
<th>DESCRIPTION</th>
<th>STORE-CC</th>
<th>CONDITION</th>
</tr>
</thead>
<tbody>
<tr>
<td>0000</td>
<td>b &lt; a</td>
<td>Move</td>
<td>0000</td>
<td>Carry clear</td>
</tr>
<tr>
<td>0001</td>
<td>b &lt; a + 1</td>
<td>Increment</td>
<td>0001</td>
<td>Carry set</td>
</tr>
<tr>
<td>0010</td>
<td>b &lt; a + b + c</td>
<td>Add with carry</td>
<td>0010</td>
<td>Overflow clear</td>
</tr>
<tr>
<td>0011</td>
<td>b &lt; a + a</td>
<td>Add</td>
<td>0011</td>
<td>Overflow set</td>
</tr>
<tr>
<td>0100</td>
<td>b &lt; 0 - a</td>
<td>Negative</td>
<td>0100</td>
<td>Not negative</td>
</tr>
<tr>
<td>0101</td>
<td>b &lt; a - 1</td>
<td>Decrement</td>
<td>0101</td>
<td>Negative</td>
</tr>
<tr>
<td>0110</td>
<td>b &lt; a - c</td>
<td>Subtract with borrow</td>
<td>0110</td>
<td>Not zero</td>
</tr>
<tr>
<td>1111</td>
<td>b &lt; b - a</td>
<td>Subtract</td>
<td>1111</td>
<td>Zero</td>
</tr>
<tr>
<td>1000</td>
<td>b &lt; a &gt;&gt; 1</td>
<td>Rotate right through carry</td>
<td>1000</td>
<td>Higher</td>
</tr>
<tr>
<td>1001</td>
<td>b &lt; a &gt; 1</td>
<td>Arithmetic shift right</td>
<td>1001</td>
<td>Lower or same</td>
</tr>
<tr>
<td>1010</td>
<td>b &lt; a &gt; 1</td>
<td>Logical shift right</td>
<td>1010</td>
<td>Greater or equal</td>
</tr>
<tr>
<td>1011</td>
<td>b &lt;&lt; bXOR a</td>
<td>XOR</td>
<td>1011</td>
<td>Less</td>
</tr>
<tr>
<td>1100</td>
<td>b &lt;&lt; b OR a</td>
<td>OR</td>
<td>1100</td>
<td>Greater</td>
</tr>
<tr>
<td>1101</td>
<td>b &lt;&lt; b AND a</td>
<td>AND</td>
<td>1101</td>
<td>Less or equal</td>
</tr>
<tr>
<td>1110</td>
<td>b &lt; NOT a</td>
<td>NOT</td>
<td>1110</td>
<td>True</td>
</tr>
<tr>
<td>1111</td>
<td>b &lt; a</td>
<td>Move</td>
<td>1111</td>
<td>Pulse</td>
</tr>
</tbody>
</table>
The FM9001 Signal Groups

Quite a number of pins are allocated to testing purposes.
The FM9001 Pinout

An FM9001 Factorial Program

```plaintext
start update

speed = over reg
regA

fact (move t f (tos- ) (loc) ) ; Link r14,0
(move t f ) ; Link toc
(add t f toc )

(move t f z2 ) ; X-1 -> R0
(add t f z2 )
(dac t ovn r0 )

(move la f po ) ; X-1 <- 0, jump
(value fact-1)

(move t f ) ; Push X-1

(move t f ) ; Push return address
(value fact-back)

(sub t f po ) ; Relative subroutine call
(value (difference fact-back fact)))

fact-back (move t f z2 ) ; X -> R1
(add t f z2 )

(move t f z1 )

(move t f ) ; Return to FACT-END
(value fact-end)

(move t f po )

(value multiply)

fact-1 (move t f z0 ) ; Return 1

fact-end (move t f toc ) ; Unlink

(move t f toc )

(move t f po )
```

---

Copyright © 1991 Computational Logic Inc.  fm9001.msc 10 3 December 1991

---

Copyright © 1991 Computational Logic Inc.  fm9001.msc 12 3 December 1991
The FM9001 Specification levels

The FM9001 is specified at four levels:

- user,
- two-valued,
- four-valued, and
- netlist.

Each level is specified as an interpreter, except the netlist level.

The netlist is given meaning with our unit-clock simulator.
**The FM9001 Implementation Specification**

Our HDL provides our lowest-level model for the FM9001 implementation:

- every internal gate and register is described, and
- every I/O pad buffer is defined.

Our HDL specification also includes all of the internal test logic.

We have proved the correctness of our FM9001 HDL description.

---

**A Formal HDL**

We have formalized a netlist-based, hierarchically-structured, occurrence-oriented hardware description language (HDL) using the Boyer-Moore logic.

- A predicate recognizes well-formed circuits.
- An interpreter defines the logical semantics.

Well-formed circuits contain:

- well-formed module, input, and output names;
- no combinational loops;
- no loading and fanout violations; and
- no wire type (clock, Boolean, tri-state) mismatches.
Circuit Examples

(HALF-ADDER (A B))
(SUM CARRY)
((G0 (SUM) B XOR (A B))
(G1 (CARRY) B AND (A B)))
NIL)

A
B
CARRY
SUM

The following full-adder specification refers twice to the half-adder specification above.

(FULL-ADDER (A B C))
(SUM CARRY)
((T0 (SUM CARRY1) HALF-ADDER (A B))
(T1 (SUM CARRY2) HALF-ADDER (SUM1 C))
(T2 (CARRY) B OR (CARRY1 CARRY2)))
NIL)

A
B
CARRY1
CARRY
CARRY2
SUM

Translating Into LSI Logic Format

With just a few lines of Lisp program code, we are able to convert our full-adder boxlist into a form acceptable to LSI Logic.

COMPILE;
DEFINITIONS;
MODULES FULL-ADDER;

(FULL-ADDER (A B C))
(SUM CARRY)
((T0 (SUM CARRY1) FULL-ADDER (A B))
(T1 (SUM CARRY2) FULL-ADDER (SUM C))
(T2 (CARRY) SUM (CARRY1 CARRY2)))
NIL)

END MODULES;

MODULES HALF-ADDER;

(HALF-ADDER (A B))
(SUM CARRY)
((G0 (SUM) B XOR (A B))
(G1 (CARRY) B AND (A B)))
NIL)

END MODULES;
END COMPILE;
END;

Copyright © 1991 Computational Logic Inc.  Im9001.mac 17  3 December 1991
Copyright © 1991 Computational Logic Inc.  Im9001.mac 18  3 December 1991
A Circuit with Tri-state and Latches

The following is a circuit with two latches that can exchange values over a tri-state bus.

Module **M1** defines the module used on both ends of the bus.

\[
\begin{align*}
M1 & \text{(CLK EN SEL D Q)} \\
& \text{(Q)} \\
& \text{(MUX (B) B-IF (SEL D Q))} \\
& \text{(LATCH (A AN) FD1 (B CLK))} \\
& \text{(TBUF (Q) T-BUF (EN A)))} \\
& \text{LATCH}
\end{align*}
\]

Module **M2** defines a bus interconnecting two M1 modules.

\[
\begin{align*}
M2 & \text{(CLK EN0 EN1 SEL0 SEL1 D0 D1)} \\
& \text{(Q)} \\
& \text{(OCC0 (Q0) M1 (CLK EN0 SEL0 D0 Q))} \\
& \text{(OCC1 (Q1) M1 (CLK EN1 SEL1 D1 Q))} \\
& \text{(WIRE (Q) T-WIRE (Q0 Q1)))} \\
& \text{(OCC0 OCC1))}
\end{align*}
\]

This is similar to the FM8502 memory interface.
**Verified Synthesis**

Using our HDL, we have been able to verify that circuit generating programs synthesize correct circuits.

We perform synthesis by:
- writing circuit generator programs,
- verifying the circuit generator programs, and
- then executing the generators to generate correct circuits by construction.

In other words, a synthesized circuit has already been proved correct.

---

**An ALU Generator**

We have an arbitrary size, 16-function ALU generator which is:
- programmable—ALUs with different internal structure can be produced;
- "intelligent"—internal buffers are only added when needed; and
- has been verified to generate correct $n$-bit, gate-level ALU descriptions.
ALU Generator Output Summary

Summarized below are some characteristics of the ALUs generated by our verified ALU generator.

<table>
<thead>
<tr>
<th>ALU Characteristics</th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Size</td>
<td>Gate Count</td>
<td>Fanout</td>
<td>Delay</td>
</tr>
<tr>
<td>1 bit</td>
<td>126</td>
<td>8</td>
<td>12</td>
</tr>
<tr>
<td>2 bits</td>
<td>149</td>
<td>8</td>
<td>14</td>
</tr>
<tr>
<td>4 bits</td>
<td>196</td>
<td>8</td>
<td>17</td>
</tr>
<tr>
<td>8 bits</td>
<td>297</td>
<td>8</td>
<td>22</td>
</tr>
<tr>
<td>16 bits</td>
<td>491</td>
<td>8</td>
<td>26</td>
</tr>
<tr>
<td>32 bits</td>
<td>890</td>
<td>8</td>
<td>30</td>
</tr>
<tr>
<td>64 bits</td>
<td>1665</td>
<td>8</td>
<td>35</td>
</tr>
<tr>
<td>128 bits</td>
<td>3227</td>
<td>8</td>
<td>39</td>
</tr>
</tbody>
</table>

It only takes a few seconds to generate these ALUs.

The FM9001 Netlist

The FM9001 netlist is constructed by a Boyer-Moore function.

Most of the modules in the netlist are synthesized from n-bit module descriptions.

The FM9001 netlist contains over 91,000 characters in 2215 lines.

There are 85 modules that reference 1800 primitives of 48 types.

On average, each primitive output is connected to 3.4 other primitives.

There are 95 I/O pins, 32 are bi-directional.
The FM9001 Correctness Theorem

An abstract statement of the proof is below.

\( \exists \text{implementation}, \exists \text{clock} \)

\[ \text{FM9001\_specification}(\text{user\_state}, n) = \text{map\_up}(\text{simulate}(\text{map\_down}(\text{user\_state}), \text{implementation}, \text{clock})) \]

We break the statement of the proof into five pieces.

Prettyprinted

<table>
<thead>
<tr>
<th>Lines</th>
<th>User-level semantics of FM9001</th>
<th>Statement of theorem</th>
<th>Semantics of HDL</th>
<th>FM9001 implementation description</th>
<th>Existential witness for the clock</th>
</tr>
</thead>
<tbody>
<tr>
<td>915</td>
<td></td>
<td>197</td>
<td>3459</td>
<td>3479</td>
<td>1942</td>
</tr>
<tr>
<td>9992</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

The FM9001 Mechanical Proof

Our FM9001 definition and lemma input script contains 2957 entries; these entries expand into 4851 theorem prover events.

For the Boyer-Moore theorem prover to check the FM9001 input script takes about 4 hours on a Sun SparcStation 2.

A comparison to some other proofs is given below (see A Computational Logic Handbook.)

<table>
<thead>
<tr>
<th>Number of lines in understandable statement</th>
<th>Concept depth of statement</th>
<th>Max concept depth in proof</th>
<th>Number of supporters</th>
<th>Lines of supporters</th>
<th>Depth of proof</th>
</tr>
</thead>
<tbody>
<tr>
<td>85 FM901</td>
<td>991</td>
<td>157</td>
<td>152</td>
<td>230</td>
<td>2171</td>
</tr>
<tr>
<td>84 Goedel</td>
<td>864</td>
<td>48</td>
<td>40414</td>
<td>1741</td>
<td>20002</td>
</tr>
<tr>
<td>91 FM9001</td>
<td>1112</td>
<td>120</td>
<td>128</td>
<td>1894</td>
<td>28784</td>
</tr>
</tbody>
</table>
Testing the FM9001

We needed to be able to test the FM9001, as the manufacturing process is flawed.

Our testing approach is to build a design that can be tested using a single, stuck-at-fault model.

Notice on the next slide the duplication of the undefined and undetectable faults.

<table>
<thead>
<tr>
<th>SIMULATION PARAMETERS</th>
<th>FDC's</th>
<th>FAULTS REPRESENTED</th>
</tr>
</thead>
<tbody>
<tr>
<td>Total Faults</td>
<td>9559</td>
<td>13098</td>
</tr>
<tr>
<td>Faults tied to MC/0 or /1/</td>
<td>0</td>
<td>11</td>
</tr>
<tr>
<td>Total Faults Sampled</td>
<td>9163</td>
<td>12633</td>
</tr>
<tr>
<td>Faults included this run</td>
<td>1367</td>
<td>1418</td>
</tr>
<tr>
<td>Faults excluded this run</td>
<td>0</td>
<td>0</td>
</tr>
</tbody>
</table>

PAST CUMULATIVE RESULTS

Version
A Fault Coverage (%) : 73.09 - 76.69 76.17 - 79.01
B Fault Coverage (%) : 82.01 - 84.77 85.29 - 88.36
C Fault Coverage (%) : 82.80 - 87.18 86.43 - 89.61
D Fault Coverage (%) : 85.06 - 89.20 88.26 - 91.92
E Fault Coverage (%) : 82.06 - 89.20 88.26 - 91.92
F Fault Coverage (%) : 85.06 - 89.20 88.26 - 91.92
G Fault Coverage (%) : 85.19 - 89.28 88.56 - 91.97
H Fault Coverage (%) : 85.75 - 97.76 95.66 - 98.38

Undetectable FM9001 Faults

No notes caused an oscillation

OSC = CROSSED OSCILLATION

CLOCK-PAD (V1) : 0 8740 9040 0
CLOCK-PAD (PO) : 1 8740 9040 0
MONITOR (V2) : 0 9060 9040 0
MONITOR (V1) : 0 9060 9040 0
V1-PAD (V1) : 0 9760 9040 0
V1-PAD (PO) : 0 9760 9040 0
V2-PAD (V1) : 0 9760 9040 0
V2-PAD (PO) : 0 9760 9040 0

THD = TYDI TO HE/0/
MONITOR (V1) : 1 9060 9040 0
MONITOR (V2) : 1 9060 9040 0
V1-PAD (V1) : 1 9760 9040 0
V2-PAD (V1) : 1 9760 9040 0

THD = TYDI TO HE/1/
ADD-O/PADS/0.0 (ME/0) : 1 9075 9077 9040 0
ADD-O/PADS/0.0 (ME/1) : 1 9075 9077 9040 0
DATA-NOS-PADS/0.0 (ME/0) : 1 9075 9077 9040 0
DATA-NOS-PADS/0.0 (ME/1) : 1 9075 9077 9040 0

BOOT/RES/0.0 (CF) : 1 9075 9077 9040 0
BOOT/RES/0.0 (CF) : 1 9075 9077 9040 0
BOOT/DATA-O/PADS/0.0 (CF) : 1 9075 9077 9040 0

UDF = CROSSED UNDEFINED OUTPUT

ADD-O/PADS/0.0 (ME/0) : 0 1299 1299 9040 0
ADD-O/PADS/0.0 (ME/1) : 0 1299 1299 9040 0
ADD-O/PADS/0.0 (ME/2) : 0 1299 1299 9040 0
ADD-O/PADS/0.0 (ME/3) : 0 1299 1299 9040 0

DATA-NOS-PADS/0.0 (ME/0) : 0 1299 1299 9040 0
DATA-NOS-PADS/0.0 (ME/1) : 0 1299 1299 9040 0

BOOT/RES/0.0 (RES/0) : 1 9442 9442 9040 0
BOOT/RES/0.0 (RES/1) : 1 9442 9442 9040 0

UDF = UNDETECTED

Copyright © 1991 Computational Logic Inc.  Im9001.mac: 27 3 December 1991
Conclusions

A hardware description language has been formalized.

The FM9001 user-level specification has a mechanically proved implementation.

We hope this effort represents a start towards the notion of a formula manual.

It was a lot more work than we expected. Why? Because of the formalization of many engineering issues.

We believe that formalization of the design process is more important than this specific verification exercise.
Derivational Techniques for Hardware

Steve Johnson
Indiana University
Design Derivation*
Steven D. Johnson
and Dhakshar Bose
Computer Science Department
Indiana University

Design derivation
formal system
• a language, rules of syntax
• transformations, rules of reasoning
formalization
• representing designs as expressions
• representing designing as an inference process

For example, verification
• proof of an implementation, $E \vdash I \Rightarrow S$
• derivation of an implementation, $S \Rightarrow I$
Deduction and Derivation...

- They have a lot in common
- Reflect common modes of reasoning
- Involve "proof engineering"
- Should be integrated

Digital Design Derivation system (DDD)
- An interactive transformation system based on first-order* functional expressions
- Specialized for digital system derivation

DDD as a formal system
- A core of secure algebra
- Extensibility
- Derivation management

Modes of expression
Single Pulser

"SI' generates a unit pulse for every pulse received"

```
define (SP In) "Out
where
  X = (cons 0 In)
  Out = (and X (not In))

In = (0, 0, 1, 1, 1, 0, 0, 0,...)
X = (0, 0, 0, 1, 1, 1, 0, 0,...)
Out = (0, 0, 0, 0, 0, 1, 0, 0,...)
```

Behavior to structure:

```
define (FAC n) = (F n 1)
where
  (F u v) = (if (zero? u)
    v
    (F (dec u) (mp y u v)))

define (FACsystem n) = (list V R)
where
  U = (cons n (DCR U))
  V = (cons 1 (HFT U V))
  R = (ZERO? U)
```
FM8501 specification [Hunt]

(define (FACsystem n) = (list V R)
  where
  U = (consp n (dcr U))
  V = (consp 1 (mpy U V))
  R = (zero? U)

FM8501 implementation [Hunt]

(define (FAC n) = (FOn 1)
  where
  (FO u v) = (if (zero? u)
                            V
                            (F1 u (mpy u v)))
  (F1 u v) = (FO (dcr u) v)
Block diagram of BIGmachine

Architecture derived from SOFT

Superimposed architectures

Detail of a local factorization
Physical organization of FM8501

Experiments with FM8501/2

Procedural abstraction

define (FAC n) = (F n 1)
where
(F u v) = (if (zero? u)
       v
       (F (dcr u) (MPY u v)))

define (MPY n m) = (N n m 0)
where
(N w x y) = (if (zero? w)
       y
       (if (even? w)
           (N (/2 w) x (+ (*2 y)))
           (N (/2 w) x (+ (*2 y) x)))))
Incorporating procedures

\[
\text{define } (\text{FAC } n) = (F \ n \ 1 \ 0) \\
\text{where} \\
(F \ u \ v \ w) = (if \ (\text{zero? } u) \\
\quad v \\
(M \ u \ v \ w)) \\
(M \ u \ v \ w) = (if \ (\text{zero? } u) \\
\quad (F \ (\text{dcr } z) \ v \ 0 \ 0) \\
\quad (if \ (\text{even? } u) \\
\quad (M \ (/2 \ u) \ v \ (+2 \ u) \ x) \\
\quad (M \ (/2 \ u) \ v \ (+ (+2 \ u) \ v) \ x)))
\]

Sequential Decomposition

\[
(F0 \ u \ v \ w \ dm) = \\
(if \ (\text{zero? } u) \\
\quad v \\
(\text{cons} \ (\text{list} \ 1 \ u \ v) \\
(F1 \ u \ v \ (> \ m) \ (> \ dm))))
\]

Design derivation

Construction of an implementation by equivalence preserving transformations.

\[
E_0 \Rightarrow E_1 \Rightarrow E_2 \Rightarrow \cdots \Rightarrow E_k
\]

- maintaining the global view
- making local transformations
- mundane design
- no "complete" algebra
- fixes "equivalence"
- inhibits cleverness

Interactive verification
Results of Workshop Survey

Each participant at the workshop was asked to complete a detailed survey. Fifty-three people returned the survey; this section presents the results.

For each question asked on the survey, the specific question is reproduced and the answers to the question are tabulated below. If a person circled multiple answers to a question for which only one answer was expected, the results were weighted. For example, in response to question 2, one Formal methods developer circled both b and c. This was tabulated as 0.5 for b and 0.5 for c.

Totals or averages are given where appropriate. Not every person answered every question on the survey, so the totals for different questions may vary.

1. What is the nature of your organization?
   a. University
   b. Formal methods developer
   c. Government
   d. Aerospace industry

<table>
<thead>
<tr>
<th>Question 1</th>
<th>a</th>
<th>b</th>
<th>c</th>
<th>d</th>
<th>e</th>
</tr>
</thead>
<tbody>
<tr>
<td>Industry</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>22</td>
<td>6</td>
</tr>
<tr>
<td>Government</td>
<td>0</td>
<td>0</td>
<td>14</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>University</td>
<td>2</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>FM Developers</td>
<td>0</td>
<td>9</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
</tbody>
</table>

   Note: Six people did not believe that the four listed choices accurately described the nature of their organization. The specific answers given were: transportation, railway transportation, non-profit R&D org, industry/commercial, other, and don't know. For the purpose of recording the answers, these 6 surveys are grouped with Industry.

2. What is your primary job function?
   a. Basic research
   b. Applied research
   c. Product development
   d. Management
   e. Other

<table>
<thead>
<tr>
<th>Question 2</th>
<th>a</th>
<th>b</th>
<th>c</th>
<th>d</th>
<th>e</th>
</tr>
</thead>
<tbody>
<tr>
<td>Industry</td>
<td>1</td>
<td>17</td>
<td>5</td>
<td>2</td>
<td>3</td>
</tr>
<tr>
<td>Government</td>
<td>1</td>
<td>5</td>
<td>0</td>
<td>4</td>
<td>3</td>
</tr>
<tr>
<td>University</td>
<td>1</td>
<td>1</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>FM Developers</td>
<td>3</td>
<td>1.5</td>
<td>0.5</td>
<td>4</td>
<td>0</td>
</tr>
<tr>
<td>Totals</td>
<td>6</td>
<td>24.5</td>
<td>5.5</td>
<td>10</td>
<td>6</td>
</tr>
</tbody>
</table>

3. Please rate your understanding of formal methods theory and practice:
   a. Novice
   b. Somewhat familiar
   c. Knowledgable
   d. Considerable
   e. Expert

<table>
<thead>
<tr>
<th>Question 3</th>
<th>a</th>
<th>b</th>
<th>c</th>
<th>d</th>
<th>e</th>
</tr>
</thead>
<tbody>
<tr>
<td>Industry</td>
<td>8</td>
<td>10</td>
<td>6</td>
<td>4</td>
<td>0</td>
</tr>
<tr>
<td>Government</td>
<td>6</td>
<td>4</td>
<td>3</td>
<td>0</td>
<td>1</td>
</tr>
<tr>
<td>University</td>
<td>0</td>
<td>0</td>
<td>1</td>
<td>1</td>
<td>1</td>
</tr>
<tr>
<td>FM Developers</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>1</td>
<td>8</td>
</tr>
<tr>
<td>Totals</td>
<td>14</td>
<td>14</td>
<td>9</td>
<td>6</td>
<td>10</td>
</tr>
</tbody>
</table>

1NASA Langley personnel involved in planning and conducting the workshop did not fill out a survey.
Note: One of the goals of the workshop was to attract people with widely varying understanding of formal methods. These numbers suggest that this goal was met.

4. What is the general level of awareness of formal methods within your organization?
   a. None
   b. Minimal
   c. Sparse
   d. Moderate
   e. Considerable

<table>
<thead>
<tr>
<th>Question 4</th>
<th>a</th>
<th>b</th>
<th>c</th>
<th>d</th>
<th>e</th>
</tr>
</thead>
<tbody>
<tr>
<td>Industry</td>
<td>7</td>
<td>13</td>
<td>4</td>
<td>1</td>
<td>3</td>
</tr>
<tr>
<td>Government</td>
<td>4</td>
<td>8</td>
<td>1</td>
<td>0</td>
<td>1</td>
</tr>
<tr>
<td>University</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>2</td>
<td>0</td>
</tr>
<tr>
<td>FM Developers</td>
<td>0</td>
<td>0</td>
<td>1</td>
<td>0</td>
<td>8</td>
</tr>
<tr>
<td>Totals</td>
<td>11</td>
<td>21</td>
<td>6</td>
<td>3</td>
<td>12</td>
</tr>
</tbody>
</table>

5. Before attending this workshop, how would you have rated the state-of-the-art of formal methods in terms of its potential for immediate application?
   a. Not usable
   b. Needs more time
   c. Nearly ready
   d. Ready now
   e. Has been ready

<table>
<thead>
<tr>
<th>Question 5</th>
<th>a</th>
<th>b</th>
<th>c</th>
<th>d</th>
<th>e</th>
</tr>
</thead>
<tbody>
<tr>
<td>Industry</td>
<td>4</td>
<td>16</td>
<td>4</td>
<td>3</td>
<td>1</td>
</tr>
<tr>
<td>Government</td>
<td>2</td>
<td>5</td>
<td>4</td>
<td>1</td>
<td>1</td>
</tr>
<tr>
<td>University</td>
<td>0</td>
<td>1</td>
<td>1</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>FM Developers</td>
<td>0</td>
<td>0</td>
<td>6</td>
<td>1</td>
<td>1</td>
</tr>
<tr>
<td>Totals</td>
<td>6</td>
<td>22</td>
<td>15</td>
<td>5</td>
<td>3</td>
</tr>
</tbody>
</table>

Note: Three FM developers, one who answered d and two who answered c augmented their responses with the comment “for some applications.”

6. Now that you've attended this workshop, how would you rate the state-of-the-art of formal methods in terms of its potential for immediate application?
   a. Not usable
   b. Needs more time
   c. Nearly ready
   d. Ready now
   e. Has been ready

<table>
<thead>
<tr>
<th>Question 6</th>
<th>a</th>
<th>b</th>
<th>c</th>
<th>d</th>
<th>e</th>
</tr>
</thead>
<tbody>
<tr>
<td>Industry</td>
<td>1</td>
<td>16</td>
<td>8</td>
<td>3</td>
<td>0</td>
</tr>
<tr>
<td>Government</td>
<td>0</td>
<td>4</td>
<td>6</td>
<td>2</td>
<td>0</td>
</tr>
<tr>
<td>University</td>
<td>0</td>
<td>0</td>
<td>2</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>FM Developers</td>
<td>0</td>
<td>0</td>
<td>7</td>
<td>1</td>
<td>1</td>
</tr>
<tr>
<td>Totals</td>
<td>1</td>
<td>20</td>
<td>23</td>
<td>6</td>
<td>1</td>
</tr>
</tbody>
</table>

Note 1: See note for Question 5.
Note 2: The results to this question demonstrate that the workshop did alter some people's perceptions of the state-of-the-art. Particularly interesting is that before the workshop, the perception of the state of the art by nine people was at one or the other extreme, but after the workshop, the number of people at one or the other extreme was reduced to two.
7. Please rate the extent to which formal methods is practiced today within your organization:
   a. Never       b. Seldom       c. Sporadically
   d. Occasionally e. Often

<table>
<thead>
<tr>
<th>Question 7</th>
<th>a</th>
<th>b</th>
<th>c</th>
<th>d</th>
<th>e</th>
</tr>
</thead>
<tbody>
<tr>
<td>Industry</td>
<td>15</td>
<td>9</td>
<td>2</td>
<td>1</td>
<td>1</td>
</tr>
<tr>
<td>Government</td>
<td>9</td>
<td>3</td>
<td>0</td>
<td>2</td>
<td>0</td>
</tr>
<tr>
<td>University</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>1</td>
<td>1</td>
</tr>
<tr>
<td>FM Developers</td>
<td>1</td>
<td>0</td>
<td>2</td>
<td>1</td>
<td>5</td>
</tr>
<tr>
<td>Totals</td>
<td>25</td>
<td>12</td>
<td>4</td>
<td>5</td>
<td>7</td>
</tr>
</tbody>
</table>

Note: One FM developer answered a, and added the comment “on our own systems.”

8. When do you think that formal methods will be used often in your company?
   a. 0-2 years       b. 2-5 years       c. 5-10 years
   d. 10-20 years     e. Never

<table>
<thead>
<tr>
<th>Question 8</th>
<th>a</th>
<th>b</th>
<th>c</th>
<th>d</th>
<th>e</th>
</tr>
</thead>
<tbody>
<tr>
<td>Industry</td>
<td>5</td>
<td>7</td>
<td>12</td>
<td>3</td>
<td>1</td>
</tr>
<tr>
<td>Government</td>
<td>4</td>
<td>3</td>
<td>2</td>
<td>0</td>
<td></td>
</tr>
<tr>
<td>University</td>
<td>1</td>
<td>0</td>
<td>1</td>
<td>0</td>
<td></td>
</tr>
<tr>
<td>FM Developers</td>
<td>5</td>
<td>2</td>
<td>1</td>
<td>0</td>
<td></td>
</tr>
<tr>
<td>Totals</td>
<td>15</td>
<td>12</td>
<td>17</td>
<td>5</td>
<td>1</td>
</tr>
</tbody>
</table>

Note: An individual from industry answered c with the comment “unless required by customers earlier.”

9. How difficult do you feel it is to put formal methods into practice?
   a. Extremely       b. Very       c. Moderately
   d. Somewhat        e. None at all

<table>
<thead>
<tr>
<th>Question 9</th>
<th>a</th>
<th>b</th>
<th>c</th>
<th>d</th>
<th>e</th>
</tr>
</thead>
<tbody>
<tr>
<td>Industry</td>
<td>7</td>
<td>9</td>
<td>12</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Government</td>
<td>2</td>
<td>7</td>
<td>4</td>
<td>1</td>
<td>0</td>
</tr>
<tr>
<td>University</td>
<td>0</td>
<td>1</td>
<td>1</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>FM Developers</td>
<td>2</td>
<td>3</td>
<td>4</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Totals</td>
<td>11</td>
<td>20</td>
<td>21</td>
<td>1</td>
<td>0</td>
</tr>
</tbody>
</table>

10. Are you personally inclined to apply formal methods on a design project in the near future?
    a. Strongly inclined       b. Moderately inclined    c. Indifferent
    d. Not inclined            e. Would quit first
11. How well prepared are the professionals in your organization through education and previous training to absorb the technology of formal methods?
   a. Minimally  
   b. Somewhat  
   c. Adequately  
   d. Receptive  
   e. Well prepared

<table>
<thead>
<tr>
<th>Question 10</th>
<th>a</th>
<th>b</th>
<th>c</th>
<th>d</th>
<th>e</th>
</tr>
</thead>
<tbody>
<tr>
<td>Industry</td>
<td>13</td>
<td>9</td>
<td>1</td>
<td>5</td>
<td>0</td>
</tr>
<tr>
<td>Government</td>
<td>8</td>
<td>6</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>University</td>
<td>2</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>FM Developers</td>
<td>6</td>
<td>3</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Totals</td>
<td>29</td>
<td>18</td>
<td>1</td>
<td>5</td>
<td>0</td>
</tr>
</tbody>
</table>

12. In your organization, which of the following obstacles exist that inhibit or prevent the use of formal methods? (check all that apply)
   - Management believes it is impractical  
   - Engineering staff believes it is impractical  
   - Lack of sufficient knowledge about formal methods  
   - Lack of required skills  
   - Up-front cost too high  
   - Have had negative experiences in the past  
   - Do not believe it is useful  
   - No obstacles exist

<table>
<thead>
<tr>
<th>Question 11</th>
<th>a</th>
<th>b</th>
<th>c</th>
<th>d</th>
<th>e</th>
</tr>
</thead>
<tbody>
<tr>
<td>Industry</td>
<td>15</td>
<td>8</td>
<td>3</td>
<td>0</td>
<td>2</td>
</tr>
<tr>
<td>Government</td>
<td>7</td>
<td>7</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>University</td>
<td>0</td>
<td>1</td>
<td>1</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>FM Developers</td>
<td>1</td>
<td>0</td>
<td>0</td>
<td>1</td>
<td>7</td>
</tr>
<tr>
<td>Totals</td>
<td>23</td>
<td>16</td>
<td>4</td>
<td>1</td>
<td>9</td>
</tr>
</tbody>
</table>

**Note:** An industry representative checked *No obstacles exist*, but added the comment "except funding."

13. How would you rate the potential benefits of using formal methods?
   a. Negligible  
   b. Somewhat useful  
   c. Moderately useful  
   d. Helpful  
   e. Significant
Question 13

<table>
<thead>
<tr>
<th></th>
<th>a</th>
<th>b</th>
<th>c</th>
<th>d</th>
<th>e</th>
</tr>
</thead>
<tbody>
<tr>
<td>Industry</td>
<td>0</td>
<td>5</td>
<td>1</td>
<td>4</td>
<td>18</td>
</tr>
<tr>
<td>Government</td>
<td>0</td>
<td>0</td>
<td>1</td>
<td>4</td>
<td>9</td>
</tr>
<tr>
<td>University</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>1</td>
<td>1</td>
</tr>
<tr>
<td>FM Developers</td>
<td>0</td>
<td>0</td>
<td>1</td>
<td>3</td>
<td>5</td>
</tr>
<tr>
<td><strong>Totals</strong></td>
<td>0</td>
<td>5</td>
<td>3</td>
<td>12</td>
<td>33</td>
</tr>
</tbody>
</table>

*Note:* A person from industry circled e, but added the caveat, “if it does all that is advertised.”

14. How would you rate the costs of formal methods technology relative to the costs of current practice?
   a. Excessively higher  
   b. Somewhat higher  
   c. Equivalent  
   d. Somewhat lower  
   e. Much lower

<table>
<thead>
<tr>
<th></th>
<th>a</th>
<th>b</th>
<th>c</th>
<th>d</th>
<th>e</th>
</tr>
</thead>
<tbody>
<tr>
<td>Industry</td>
<td>4</td>
<td>13</td>
<td>5</td>
<td>4</td>
<td>2</td>
</tr>
<tr>
<td>Government</td>
<td>2</td>
<td>8</td>
<td>0</td>
<td>0.5</td>
<td>1.5</td>
</tr>
<tr>
<td>University</td>
<td>0</td>
<td>2</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>FM Developers</td>
<td>0</td>
<td>2</td>
<td>5</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td><strong>Totals</strong></td>
<td>6</td>
<td>25</td>
<td>10</td>
<td>4.5</td>
<td>3.5</td>
</tr>
</tbody>
</table>

*Note 1:* A government representative circled e and added “over system life cycle.”  
*Note 2:* An industry person circled a, with the additional comment “don’t see FM replacing anything --- it only adds confidence and cost to date.”

15. How aggressively would you recommend your management pursue the use of formal methods technology?
   a. Forget it  
   b. Keep up with developments  
   c. Attempt small pilot projects  
   d. Attempt larger applications  
   e. Full speed ahead

<table>
<thead>
<tr>
<th></th>
<th>a</th>
<th>b</th>
<th>c</th>
<th>d</th>
<th>e</th>
</tr>
</thead>
<tbody>
<tr>
<td>Industry</td>
<td>0</td>
<td>6</td>
<td>20</td>
<td>2</td>
<td>0</td>
</tr>
<tr>
<td>Government</td>
<td>0</td>
<td>0.5</td>
<td>10.5</td>
<td>2</td>
<td>1</td>
</tr>
<tr>
<td>University</td>
<td>0</td>
<td>0</td>
<td>2</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>FM Developers</td>
<td>0</td>
<td>0.5</td>
<td>2</td>
<td>4.5</td>
<td>1</td>
</tr>
<tr>
<td><strong>Totals</strong></td>
<td>0</td>
<td>7</td>
<td>34.5</td>
<td>8.5</td>
<td>2</td>
</tr>
</tbody>
</table>

*Note:* One industry representative answered c and added the comment “to completion!”

16. How much empirical evidence on the benefits of formal methods do you feel is available for managers to make informed decisions regarding its use?
   a. Insufficient  
   b. Nearly sufficient  
   c. Adequate  
   d. More than adequate  
   e. Plentiful
Question 16

<table>
<thead>
<tr>
<th></th>
<th>a</th>
<th>b</th>
<th>c</th>
<th>d</th>
<th>e</th>
</tr>
</thead>
<tbody>
<tr>
<td>Industry</td>
<td>22</td>
<td>2</td>
<td>3</td>
<td>0</td>
<td>1</td>
</tr>
<tr>
<td>Government</td>
<td>8</td>
<td>2</td>
<td>3</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>University</td>
<td>1</td>
<td>0</td>
<td>1</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>FM Developers</td>
<td>4</td>
<td>3</td>
<td>0</td>
<td>0</td>
<td>2</td>
</tr>
<tr>
<td>Totals</td>
<td>35</td>
<td>7</td>
<td>7</td>
<td>0</td>
<td>3</td>
</tr>
</tbody>
</table>

17. Rate the importance of reusable formal verifications such as verified clock synchronization circuits and verified software modules.
   a. None at all  
   b. Somewhat  
   c. Moderately  
   d. Very  
   e. Extremely

Question 17

<table>
<thead>
<tr>
<th></th>
<th>a</th>
<th>b</th>
<th>c</th>
<th>d</th>
<th>e</th>
</tr>
</thead>
<tbody>
<tr>
<td>Industry</td>
<td>2</td>
<td>2</td>
<td>7</td>
<td>6</td>
<td>10</td>
</tr>
<tr>
<td>Government</td>
<td>0</td>
<td>5</td>
<td>4</td>
<td>3</td>
<td>0</td>
</tr>
<tr>
<td>University</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>1</td>
<td>1</td>
</tr>
<tr>
<td>FM Developers</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>4</td>
<td>4</td>
</tr>
<tr>
<td>Totals</td>
<td>2</td>
<td>7</td>
<td>11</td>
<td>14</td>
<td>15</td>
</tr>
</tbody>
</table>

18. Rate the importance of generic tools (such as, semi-automatic theorem provers, specification language typecheckers) that can be applied to software/hardware development.
   a. None at all  
   b. Somewhat  
   c. Moderately  
   d. Very  
   e. Extremely

Question 18

<table>
<thead>
<tr>
<th></th>
<th>a</th>
<th>b</th>
<th>c</th>
<th>d</th>
<th>e</th>
</tr>
</thead>
<tbody>
<tr>
<td>Industry</td>
<td>0</td>
<td>2</td>
<td>5</td>
<td>11</td>
<td>10</td>
</tr>
<tr>
<td>Government</td>
<td>0</td>
<td>1</td>
<td>4</td>
<td>6</td>
<td>3</td>
</tr>
<tr>
<td>University</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>2</td>
</tr>
<tr>
<td>FM Developers</td>
<td>0</td>
<td>0</td>
<td>2</td>
<td>2</td>
<td>5</td>
</tr>
<tr>
<td>Totals</td>
<td>0</td>
<td>3</td>
<td>11</td>
<td>19</td>
<td>20</td>
</tr>
</tbody>
</table>

19. Rate the importance of the capability of formal methods to produce trustworthy solutions of difficult problems in computer science.
   a. None at all  
   b. Somewhat  
   c. Moderately  
   d. Very  
   e. Extremely

Question 19

<table>
<thead>
<tr>
<th></th>
<th>a</th>
<th>b</th>
<th>c</th>
<th>d</th>
<th>e</th>
</tr>
</thead>
<tbody>
<tr>
<td>Industry</td>
<td>1</td>
<td>3</td>
<td>5</td>
<td>12</td>
<td>7</td>
</tr>
<tr>
<td>Government</td>
<td>0</td>
<td>1</td>
<td>4</td>
<td>4</td>
<td>5</td>
</tr>
<tr>
<td>University</td>
<td>0</td>
<td>1</td>
<td>0</td>
<td>1</td>
<td>0</td>
</tr>
<tr>
<td>FM Developers</td>
<td>0</td>
<td>0</td>
<td>1</td>
<td>2</td>
<td>6</td>
</tr>
<tr>
<td>Totals</td>
<td>1</td>
<td>5</td>
<td>10</td>
<td>19</td>
<td>18</td>
</tr>
</tbody>
</table>

228
Note: An industry person wrote: "(a) who cares (practically) about CS? (c) for real problems. We need trustworthy solutions to real problems!"

20. Where in the life-cycle do you feel formal methods can be applied most cost-effectively?
   a. Requirements  b. High-level design  c. Detailed design
   d. Implementation  e. Maintenance

<table>
<thead>
<tr>
<th>Question 20</th>
<th>a</th>
<th>b</th>
<th>c</th>
<th>d</th>
<th>e</th>
</tr>
</thead>
<tbody>
<tr>
<td>Industry</td>
<td>15.5</td>
<td>8</td>
<td>3.5</td>
<td>0.5</td>
<td>0.5</td>
</tr>
<tr>
<td>Government</td>
<td>9.33</td>
<td>2.83</td>
<td>1.33</td>
<td>0.5</td>
<td>0</td>
</tr>
<tr>
<td>University</td>
<td>0.45</td>
<td>0.45</td>
<td>0.45</td>
<td>0.45</td>
<td>0.2</td>
</tr>
<tr>
<td>FM Developers</td>
<td>1.67</td>
<td>5.67</td>
<td>0.33</td>
<td>0</td>
<td>0.33</td>
</tr>
<tr>
<td>Totals</td>
<td>26.95</td>
<td>18.95</td>
<td>5.61</td>
<td>1.45</td>
<td>1.03</td>
</tr>
</tbody>
</table>

21. Where in the life-cycle do you feel formal methods can yield the most significant benefits, irrespective of cost?
   a. Requirements  b. High-level design  c. Detailed design
   d. Implementation  e. Maintenance

<table>
<thead>
<tr>
<th>Question 21</th>
<th>a</th>
<th>b</th>
<th>c</th>
<th>d</th>
<th>e</th>
</tr>
</thead>
<tbody>
<tr>
<td>Industry</td>
<td>20.33</td>
<td>2.83</td>
<td>3.33</td>
<td>0</td>
<td>0.5</td>
</tr>
<tr>
<td>Government</td>
<td>9.33</td>
<td>1.83</td>
<td>0.83</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>University</td>
<td>1.33</td>
<td>0.33</td>
<td>0.33</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>FM Developers</td>
<td>1.5</td>
<td>1.5</td>
<td>3</td>
<td>1</td>
<td>1</td>
</tr>
<tr>
<td>Totals</td>
<td>32.5</td>
<td>6.5</td>
<td>4.5</td>
<td>1</td>
<td>1.5</td>
</tr>
</tbody>
</table>

22. How long does it take to become proficient in formal methods?
   a. Less than 2 weeks  b. 2 weeks to 1 month  c. 1 to 6 months
   d. 6 months to 1 year  e. 1 to 5 years

<table>
<thead>
<tr>
<th>Question 22</th>
<th>a</th>
<th>b</th>
<th>c</th>
<th>d</th>
<th>e</th>
</tr>
</thead>
<tbody>
<tr>
<td>Industry</td>
<td>0</td>
<td>0</td>
<td>2</td>
<td>16</td>
<td>9</td>
</tr>
<tr>
<td>Government</td>
<td>0</td>
<td>0</td>
<td>1</td>
<td>5</td>
<td>6</td>
</tr>
<tr>
<td>University</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>2</td>
</tr>
<tr>
<td>FM Developers</td>
<td>0</td>
<td>0</td>
<td>1</td>
<td>7</td>
<td>0</td>
</tr>
<tr>
<td>Totals</td>
<td>0</td>
<td>0</td>
<td>4</td>
<td>28</td>
<td>17</td>
</tr>
</tbody>
</table>

Note 1: Two people, one from government and one from industry, said that the answer to this question was "dependent on background."

Note 2: A person from a university circled e, and annotated the answer with "or more."

23. What is your opinion of the following statement: "Proficiency in formal methods requires a high degree of mathematical sophistication."
   a. Agree strongly  b. Agree  c. No opinion
   d. Disagree  e. Disagree strongly
Question 23

<table>
<thead>
<tr>
<th>a</th>
<th>b</th>
<th>c</th>
<th>d</th>
<th>e</th>
</tr>
</thead>
<tbody>
<tr>
<td>Industry</td>
<td>9</td>
<td>14</td>
<td>1</td>
<td>2</td>
</tr>
<tr>
<td>Government</td>
<td>5</td>
<td>6</td>
<td>1</td>
<td>1</td>
</tr>
<tr>
<td>University</td>
<td>0</td>
<td>1</td>
<td>0</td>
<td>1</td>
</tr>
<tr>
<td>FM Developers</td>
<td>0</td>
<td>6</td>
<td>0</td>
<td>2</td>
</tr>
<tr>
<td>Totals</td>
<td>14</td>
<td>27</td>
<td>2</td>
<td>6</td>
</tr>
</tbody>
</table>

Note: An industry representative circled a, but added, "but it shouldn't be the case!"

24. To each of the following areas assign a number from 1 to 5 to denote the importance of the area. Use 1 to denote that the area is extremely important, and 5 to denote that the area is not important at all. Please assign a 0 to any area about which you have no opinion.

- Basic modeling techniques
- Code verification (especially for Ada)
- Education and training
- Integrated verification systems
- Mechanical theorem provers
- Reusable deductive theories (libraries of definitions and theories)
- Reusable, verified software libraries
- Special purpose verification tools (such as Spectool, DDD, & Penelope)
- Specification languages
- Worked examples

### Question 24: Industry

<table>
<thead>
<tr>
<th></th>
<th>0</th>
<th>1</th>
<th>2</th>
<th>3</th>
<th>4</th>
<th>5</th>
<th>Avg.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Model. Tech.</td>
<td>3</td>
<td>11</td>
<td>8</td>
<td>4</td>
<td>2</td>
<td>0</td>
<td>1.9</td>
</tr>
<tr>
<td>Code Verif.</td>
<td>4</td>
<td>10</td>
<td>5</td>
<td>6</td>
<td>3</td>
<td>0</td>
<td>2.1</td>
</tr>
<tr>
<td>Education</td>
<td>2</td>
<td>15</td>
<td>10</td>
<td>0</td>
<td>0</td>
<td>1</td>
<td>1.5</td>
</tr>
<tr>
<td>Int. Ver. Sys.</td>
<td>4</td>
<td>10</td>
<td>6</td>
<td>5</td>
<td>3</td>
<td>0</td>
<td>2.0</td>
</tr>
<tr>
<td>Mech. T. Prov.</td>
<td>4</td>
<td>2</td>
<td>11</td>
<td>7</td>
<td>4</td>
<td>0</td>
<td>2.5</td>
</tr>
<tr>
<td>R. Ded. Theo.</td>
<td>5</td>
<td>5</td>
<td>11</td>
<td>3</td>
<td>4</td>
<td>0</td>
<td>2.3</td>
</tr>
<tr>
<td>R. Soft. Lib.</td>
<td>2</td>
<td>7</td>
<td>11</td>
<td>3</td>
<td>5</td>
<td>0</td>
<td>2.2</td>
</tr>
<tr>
<td>Sp. Purp. Tool</td>
<td>5</td>
<td>0</td>
<td>7</td>
<td>14</td>
<td>2</td>
<td>0</td>
<td>2.8</td>
</tr>
<tr>
<td>Spec. Langs.</td>
<td>1</td>
<td>14</td>
<td>8</td>
<td>3</td>
<td>1</td>
<td>1</td>
<td>1.8</td>
</tr>
<tr>
<td>Examples</td>
<td>2</td>
<td>11</td>
<td>9</td>
<td>4</td>
<td>2</td>
<td>0</td>
<td>1.9</td>
</tr>
</tbody>
</table>

### Question 24: Government

<table>
<thead>
<tr>
<th></th>
<th>0</th>
<th>1</th>
<th>2</th>
<th>3</th>
<th>4</th>
<th>5</th>
<th>Avg.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Model. Tech.</td>
<td>2</td>
<td>5</td>
<td>4</td>
<td>0</td>
<td>0</td>
<td>2</td>
<td>2.1</td>
</tr>
<tr>
<td>Code Verif.</td>
<td>2</td>
<td>4</td>
<td>2</td>
<td>5</td>
<td>0</td>
<td>1</td>
<td>2.3</td>
</tr>
<tr>
<td>Education</td>
<td>0</td>
<td>6</td>
<td>0</td>
<td>5</td>
<td>0</td>
<td>2</td>
<td>2.4</td>
</tr>
<tr>
<td>Int. Ver. Sys.</td>
<td>3</td>
<td>0</td>
<td>2</td>
<td>4</td>
<td>2</td>
<td>1</td>
<td>3.2</td>
</tr>
<tr>
<td>Mech. T. Prov.</td>
<td>1</td>
<td>3</td>
<td>2</td>
<td>3</td>
<td>1</td>
<td>2</td>
<td>2.7</td>
</tr>
<tr>
<td>R. Ded. Theo.</td>
<td>2</td>
<td>1</td>
<td>2</td>
<td>4</td>
<td>3</td>
<td>1</td>
<td>3.1</td>
</tr>
<tr>
<td>R. Soft. Lib.</td>
<td>1</td>
<td>2</td>
<td>2</td>
<td>4</td>
<td>3</td>
<td>1</td>
<td>2.9</td>
</tr>
<tr>
<td>Sp. Purp. Tool</td>
<td>4</td>
<td>1</td>
<td>2</td>
<td>4</td>
<td>1</td>
<td>1</td>
<td>2.9</td>
</tr>
<tr>
<td>Spec. Langs.</td>
<td>1</td>
<td>4</td>
<td>3</td>
<td>2</td>
<td>1</td>
<td>2</td>
<td>2.5</td>
</tr>
<tr>
<td>Examples</td>
<td>1</td>
<td>6</td>
<td>2</td>
<td>2</td>
<td>0</td>
<td>2</td>
<td>2.2</td>
</tr>
</tbody>
</table>
Question 24: University

<table>
<thead>
<tr>
<th></th>
<th>0</th>
<th>1</th>
<th>2</th>
<th>3</th>
<th>4</th>
<th>5</th>
<th>Avg.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Model. Tech.</td>
<td>1</td>
<td>1</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>1.0</td>
</tr>
<tr>
<td>Code Verif.</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>-</td>
<td>-</td>
</tr>
<tr>
<td>Education</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>-</td>
<td>-</td>
</tr>
<tr>
<td>Int. Ver. Sys.</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>-</td>
<td>-</td>
</tr>
<tr>
<td>Mech. T. Prov.</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>-</td>
<td>-</td>
</tr>
<tr>
<td>R. Ded. Theo.</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>-</td>
<td>-</td>
</tr>
<tr>
<td>R. Soft. Lib.</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>-</td>
<td>-</td>
</tr>
<tr>
<td>Sp. Purp. Tool</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>-</td>
<td>-</td>
</tr>
<tr>
<td>Spec. Langs.</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>-</td>
<td>-</td>
</tr>
<tr>
<td>Examples</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>-</td>
<td>-</td>
</tr>
</tbody>
</table>

Question 24: FM Developers

<table>
<thead>
<tr>
<th></th>
<th>0</th>
<th>1</th>
<th>2</th>
<th>3</th>
<th>4</th>
<th>5</th>
<th>Avg.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Model. Tech.</td>
<td>0</td>
<td>6</td>
<td>2</td>
<td>1</td>
<td>0</td>
<td>0</td>
<td>1.4</td>
</tr>
<tr>
<td>Code Verif.</td>
<td>0</td>
<td>3</td>
<td>2</td>
<td>2</td>
<td>1</td>
<td>1</td>
<td>2.4</td>
</tr>
<tr>
<td>Education</td>
<td>0</td>
<td>6</td>
<td>2</td>
<td>1</td>
<td>0</td>
<td>0</td>
<td>1.4</td>
</tr>
<tr>
<td>Int. Ver. Sys.</td>
<td>0</td>
<td>5</td>
<td>1</td>
<td>2</td>
<td>1</td>
<td>0</td>
<td>1.9</td>
</tr>
<tr>
<td>Mech. T. Prov.</td>
<td>0</td>
<td>3</td>
<td>3</td>
<td>2</td>
<td>1</td>
<td>0</td>
<td>2.1</td>
</tr>
<tr>
<td>R. Ded. Theo.</td>
<td>0</td>
<td>3</td>
<td>6</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>1.7</td>
</tr>
<tr>
<td>R. Soft. Lib.</td>
<td>0</td>
<td>4</td>
<td>2</td>
<td>4</td>
<td>0</td>
<td>0</td>
<td>2.0</td>
</tr>
<tr>
<td>Sp. Purp. Tool</td>
<td>0</td>
<td>3</td>
<td>2</td>
<td>1</td>
<td>3</td>
<td>0</td>
<td>2.4</td>
</tr>
<tr>
<td>Spec. Langs.</td>
<td>0</td>
<td>3</td>
<td>6</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>1.7</td>
</tr>
<tr>
<td>Examples</td>
<td>0</td>
<td>5</td>
<td>2</td>
<td>1</td>
<td>1</td>
<td>0</td>
<td>1.8</td>
</tr>
</tbody>
</table>

Note 1: Answers of 0 were ignored in calculating the averages.

Note 2: For a few respondents, the answers to this question seemed inconsistent with answers to other questions. We suspect that some people may have failed to read the question carefully, and as a result reversed the ordering (that is, used 5 to denote extreme importance and 1 to denote no importance); however, we recorded their responses as given.

25. To each of the following tools and techniques assign a number from 1 to 5 to denote your perception of the usefulness of the tool/technique. Use 1 to denote that you believe the tool/technique may be extremely useful, and 5 to denote that you believe the tool/technique is useless. Please assign a 0 to any tool/technique about which you have no opinion.

- --- Boyer-Moore
- --- DDD
- --- HOL
- --- Modelisation
- --- Penelope
- --- PVS/Ehdm
- --- Spectool
- --- EVES
- --- Nuprl
- --- Safety analysis

231
### Question 25: Industry

<table>
<thead>
<tr>
<th></th>
<th>0</th>
<th>1</th>
<th>2</th>
<th>3</th>
<th>4</th>
<th>5</th>
<th>Avg.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Boyer-Moore</td>
<td>9</td>
<td>1</td>
<td>4</td>
<td>10</td>
<td>3</td>
<td>1</td>
<td>2.9</td>
</tr>
<tr>
<td>HOL</td>
<td>8</td>
<td>1</td>
<td>7</td>
<td>6</td>
<td>5</td>
<td>1</td>
<td>2.9</td>
</tr>
<tr>
<td>Penelope</td>
<td>12</td>
<td>0</td>
<td>9</td>
<td>4</td>
<td>3</td>
<td>0</td>
<td>2.6</td>
</tr>
<tr>
<td>Spectool</td>
<td>16</td>
<td>0</td>
<td>6</td>
<td>4</td>
<td>2</td>
<td>0</td>
<td>2.7</td>
</tr>
<tr>
<td>DDD</td>
<td>19</td>
<td>0</td>
<td>2</td>
<td>4</td>
<td>3</td>
<td>0</td>
<td>3.1</td>
</tr>
<tr>
<td>Modelisation</td>
<td>14</td>
<td>5</td>
<td>2</td>
<td>3</td>
<td>2</td>
<td>2</td>
<td>2.6</td>
</tr>
<tr>
<td>PVS/Ehdm</td>
<td>5</td>
<td>6</td>
<td>10</td>
<td>5</td>
<td>1</td>
<td>1</td>
<td>2.2</td>
</tr>
<tr>
<td>EVES</td>
<td>20</td>
<td>0</td>
<td>3</td>
<td>3</td>
<td>1</td>
<td>1</td>
<td>3.0</td>
</tr>
<tr>
<td>Nuprl</td>
<td>23</td>
<td>0</td>
<td>3</td>
<td>0</td>
<td>1</td>
<td>1</td>
<td>3.0</td>
</tr>
<tr>
<td>Safety Analysis</td>
<td>8</td>
<td>14</td>
<td>3</td>
<td>2</td>
<td>1</td>
<td>0</td>
<td>1.5</td>
</tr>
</tbody>
</table>

### Question 25: Government

<table>
<thead>
<tr>
<th></th>
<th>0</th>
<th>1</th>
<th>2</th>
<th>3</th>
<th>4</th>
<th>5</th>
<th>Avg.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Boyer-Moore</td>
<td>7</td>
<td>1</td>
<td>3</td>
<td>2</td>
<td>0</td>
<td>0</td>
<td>2.2</td>
</tr>
<tr>
<td>HOL</td>
<td>8</td>
<td>2</td>
<td>0</td>
<td>3</td>
<td>0</td>
<td>0</td>
<td>2.2</td>
</tr>
<tr>
<td>Penelope</td>
<td>11</td>
<td>1</td>
<td>1</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>1.5</td>
</tr>
<tr>
<td>Spectool</td>
<td>13</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>-</td>
</tr>
<tr>
<td>DDD</td>
<td>12</td>
<td>0</td>
<td>1</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>2.0</td>
</tr>
<tr>
<td>Modelisation</td>
<td>8</td>
<td>1</td>
<td>2</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>1.7</td>
</tr>
<tr>
<td>PVS/Ehdm</td>
<td>7</td>
<td>3</td>
<td>1</td>
<td>2</td>
<td>0</td>
<td>0</td>
<td>1.8</td>
</tr>
<tr>
<td>EVES</td>
<td>12</td>
<td>0</td>
<td>0</td>
<td>1</td>
<td>0</td>
<td>0</td>
<td>3.0</td>
</tr>
<tr>
<td>Nuprl</td>
<td>12</td>
<td>0</td>
<td>0</td>
<td>1</td>
<td>0</td>
<td>0</td>
<td>3.0</td>
</tr>
<tr>
<td>Safety Analysis</td>
<td>5</td>
<td>5</td>
<td>1</td>
<td>1</td>
<td>0</td>
<td>1</td>
<td>1.9</td>
</tr>
</tbody>
</table>

### Question 25: University

<table>
<thead>
<tr>
<th></th>
<th>0</th>
<th>1</th>
<th>2</th>
<th>3</th>
<th>4</th>
<th>5</th>
<th>Avg.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Boyer-Moore</td>
<td>0</td>
<td>1</td>
<td>1</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>1.7</td>
</tr>
<tr>
<td>HOL</td>
<td>0</td>
<td>0</td>
<td>2</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>2.0</td>
</tr>
<tr>
<td>Penelope</td>
<td>1</td>
<td>0</td>
<td>1</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>2.0</td>
</tr>
<tr>
<td>Spectool</td>
<td>1</td>
<td>0</td>
<td>1</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>2.0</td>
</tr>
<tr>
<td>DDD</td>
<td>1</td>
<td>0</td>
<td>1</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>2.0</td>
</tr>
<tr>
<td>Modelisation</td>
<td>2</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>-</td>
</tr>
<tr>
<td>PVS/Ehdm</td>
<td>0</td>
<td>2</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>1.0</td>
</tr>
<tr>
<td>EVES</td>
<td>0</td>
<td>0</td>
<td>1</td>
<td>1</td>
<td>0</td>
<td>0</td>
<td>2.5</td>
</tr>
<tr>
<td>Nuprl</td>
<td>0</td>
<td>0</td>
<td>2</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>2.0</td>
</tr>
<tr>
<td>Safety Analysis</td>
<td>1</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>1</td>
<td>0</td>
<td>4.0</td>
</tr>
</tbody>
</table>

### Question 25: FM Developers

<table>
<thead>
<tr>
<th></th>
<th>0</th>
<th>1</th>
<th>2</th>
<th>3</th>
<th>4</th>
<th>5</th>
<th>Avg.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Boyer-Moore</td>
<td>0</td>
<td>0</td>
<td>5</td>
<td>1</td>
<td>0</td>
<td>0</td>
<td>2.2</td>
</tr>
<tr>
<td>HOL</td>
<td>0</td>
<td>0</td>
<td>3</td>
<td>2</td>
<td>2</td>
<td>0</td>
<td>2.9</td>
</tr>
<tr>
<td>Penelope</td>
<td>0</td>
<td>3</td>
<td>0</td>
<td>2</td>
<td>2</td>
<td>0</td>
<td>2.4</td>
</tr>
<tr>
<td>Spectool</td>
<td>1</td>
<td>3</td>
<td>0</td>
<td>3</td>
<td>0</td>
<td>0</td>
<td>2.0</td>
</tr>
<tr>
<td>DDD</td>
<td>2</td>
<td>0</td>
<td>1</td>
<td>3</td>
<td>0</td>
<td>1</td>
<td>3.2</td>
</tr>
<tr>
<td>Modelisation</td>
<td>3</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>0</td>
<td>2.5</td>
</tr>
<tr>
<td>PVS/Ehdm</td>
<td>0</td>
<td>1</td>
<td>5</td>
<td>1</td>
<td>0</td>
<td>0</td>
<td>2.0</td>
</tr>
<tr>
<td>EVES</td>
<td>1</td>
<td>1</td>
<td>3</td>
<td>2</td>
<td>0</td>
<td>0</td>
<td>2.2</td>
</tr>
<tr>
<td>Nuprl</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>1</td>
<td>4</td>
<td>2</td>
<td>4.1</td>
</tr>
<tr>
<td>Safety Analysis</td>
<td>2</td>
<td>1</td>
<td>2</td>
<td>1</td>
<td>1</td>
<td>0</td>
<td>2.4</td>
</tr>
</tbody>
</table>
Note: See the notes for Question 24.

26. How expressive should a formal language be?
   a. Very expressive (such as Z and VDM)
   b. To the level of higher-order logic
   c. To the level of 1st order logic
   d. To the level of Prolog
   e. To the level of propositional calculus

<table>
<thead>
<tr>
<th>Question 26</th>
<th>a</th>
<th>b</th>
<th>c</th>
<th>d</th>
<th>e</th>
</tr>
</thead>
<tbody>
<tr>
<td>Industry</td>
<td>14</td>
<td>6</td>
<td>2</td>
<td>1</td>
<td>0</td>
</tr>
<tr>
<td>Government</td>
<td>2</td>
<td>4</td>
<td>0</td>
<td>0</td>
<td>1</td>
</tr>
<tr>
<td>University</td>
<td>1</td>
<td>0.5</td>
<td>0.5</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>FM Developers</td>
<td>3</td>
<td>4</td>
<td>2</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Totals</td>
<td>20</td>
<td>14.5</td>
<td>4.5</td>
<td>1</td>
<td>1</td>
</tr>
</tbody>
</table>

Note: Four people, one from industry and three from government, did not answer this question, but wrote the following comments instead: "depends on application," "to understanding of user," "this needs to be decided on the basis of the domain of application requirements," and "depends on when it is used."

27. How important is it to have a specification language that can mimic the notation typically employed in the problem domain?
   a. None at all
   b. Somewhat
   c. Moderately
   d. Very
   e. Extremely

<table>
<thead>
<tr>
<th>Question 27</th>
<th>a</th>
<th>b</th>
<th>c</th>
<th>d</th>
<th>e</th>
</tr>
</thead>
<tbody>
<tr>
<td>Industry</td>
<td>0</td>
<td>3</td>
<td>5</td>
<td>12</td>
<td>6</td>
</tr>
<tr>
<td>Government</td>
<td>0</td>
<td>2</td>
<td>3</td>
<td>2</td>
<td>5</td>
</tr>
<tr>
<td>University</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>1</td>
<td>1</td>
</tr>
<tr>
<td>FM Developers</td>
<td>0</td>
<td>0</td>
<td>3</td>
<td>4</td>
<td>2</td>
</tr>
<tr>
<td>Totals</td>
<td>0</td>
<td>5</td>
<td>11</td>
<td>19</td>
<td>14</td>
</tr>
</tbody>
</table>

Note 1: A member of the government answered e, and included the comment: "to be accepted by the engineers and program managers."

Note 2: Another government representative did not circle an answer, but wrote "It must not necessarily mimic but must be readable by experts in the problem domain."

28. How important is the availability of powerful decision procedures in a theorem prover (for example, decision procedures for linear arithmetic and propositional calculus)?
   a. None at all
   b. Somewhat
   c. Moderately
   d. Very
   e. Extremely

<table>
<thead>
<tr>
<th>Question 28</th>
<th>a</th>
<th>b</th>
<th>c</th>
<th>d</th>
<th>e</th>
</tr>
</thead>
<tbody>
<tr>
<td>Industry</td>
<td>0</td>
<td>3</td>
<td>8</td>
<td>7</td>
<td>5</td>
</tr>
<tr>
<td>Government</td>
<td>0</td>
<td>1</td>
<td>3</td>
<td>3</td>
<td>2</td>
</tr>
<tr>
<td>University</td>
<td>0</td>
<td>0</td>
<td>1</td>
<td>1</td>
<td>0</td>
</tr>
<tr>
<td>FM Developers</td>
<td>0</td>
<td>0</td>
<td>1</td>
<td>2</td>
<td>6</td>
</tr>
<tr>
<td>Totals</td>
<td>0</td>
<td>4</td>
<td>13</td>
<td>13</td>
<td>13</td>
</tr>
</tbody>
</table>
29. To each of the following areas assign a number from 1 to 5 to denote your opinion as to the importance of NASA sponsoring work in the area. Use 1 to denote that you believe it is extremely important for NASA to sponsor work in the area, and 5 to denote that you believe NASA should not sponsor any work in the area.

--- Theoretical research (for example, developing theorem provers)
--- Applied research (for example, pilot projects applying formal methods)
--- Joint projects between traditional engineering groups and formal methods experts
--- Workshops such as this one

### Question 29: Industry

<table>
<thead>
<tr>
<th>Area</th>
<th>0</th>
<th>1</th>
<th>2</th>
<th>3</th>
<th>4</th>
<th>5</th>
<th>Avg.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Theoretical Research</td>
<td>0</td>
<td>8</td>
<td>5</td>
<td>7</td>
<td>3</td>
<td>5</td>
<td>2.7</td>
</tr>
<tr>
<td>Applied Research</td>
<td>0</td>
<td>19</td>
<td>6</td>
<td>0</td>
<td>0</td>
<td>3</td>
<td>1.6</td>
</tr>
<tr>
<td>Joint Projects</td>
<td>0</td>
<td>23</td>
<td>2</td>
<td>1</td>
<td>0</td>
<td>1</td>
<td>1.3</td>
</tr>
<tr>
<td>Workshops</td>
<td>0</td>
<td>17</td>
<td>7</td>
<td>2</td>
<td>2</td>
<td>0</td>
<td>1.6</td>
</tr>
</tbody>
</table>

### Question 29: Government

<table>
<thead>
<tr>
<th>Area</th>
<th>0</th>
<th>1</th>
<th>2</th>
<th>3</th>
<th>4</th>
<th>5</th>
<th>Avg.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Theoretical Research</td>
<td>0</td>
<td>3</td>
<td>5</td>
<td>1</td>
<td>4</td>
<td>0</td>
<td>2.5</td>
</tr>
<tr>
<td>Applied Research</td>
<td>0</td>
<td>10</td>
<td>1</td>
<td>1</td>
<td>0</td>
<td>1</td>
<td>1.5</td>
</tr>
<tr>
<td>Joint Projects</td>
<td>0</td>
<td>9</td>
<td>3</td>
<td>0</td>
<td>1</td>
<td>0</td>
<td>1.5</td>
</tr>
<tr>
<td>Workshops</td>
<td>0</td>
<td>11</td>
<td>1</td>
<td>0</td>
<td>0</td>
<td>1</td>
<td>1.4</td>
</tr>
</tbody>
</table>

### Question 29: University

<table>
<thead>
<tr>
<th>Area</th>
<th>0</th>
<th>1</th>
<th>2</th>
<th>3</th>
<th>4</th>
<th>5</th>
<th>Avg.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Theoretical Research</td>
<td>0</td>
<td>0</td>
<td>1</td>
<td>1</td>
<td>0</td>
<td>0</td>
<td>2.5</td>
</tr>
<tr>
<td>Applied Research</td>
<td>0</td>
<td>2</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>1.0</td>
</tr>
<tr>
<td>Joint Projects</td>
<td>0</td>
<td>1</td>
<td>1</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>1.5</td>
</tr>
<tr>
<td>Workshops</td>
<td>0</td>
<td>1</td>
<td>1</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>1.5</td>
</tr>
</tbody>
</table>

### Question 29: FM Developers

<table>
<thead>
<tr>
<th>Area</th>
<th>0</th>
<th>1</th>
<th>2</th>
<th>3</th>
<th>4</th>
<th>5</th>
<th>Avg.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Theoretical Research</td>
<td>0</td>
<td>4</td>
<td>2</td>
<td>2</td>
<td>1</td>
<td>0</td>
<td>2.0</td>
</tr>
<tr>
<td>Applied Research</td>
<td>0</td>
<td>5</td>
<td>4</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>1.4</td>
</tr>
<tr>
<td>Joint Projects</td>
<td>0</td>
<td>5</td>
<td>4</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>1.4</td>
</tr>
<tr>
<td>Workshops</td>
<td>0</td>
<td>2</td>
<td>4</td>
<td>2</td>
<td>1</td>
<td>0</td>
<td>2.2</td>
</tr>
</tbody>
</table>

**Note:** See the notes for Question 24.

Questions 30-32 were not multiple choice. Only a few representative comments from each organizational category are included below. These comments are presented exactly as given; no editing has been done. For these questions, Government and University participants have been grouped together.

30. What formal methods have you used?

**Industry:** Boyer-Moore, cleanroom, Clio, EHDM, HOL, Spec Tool, temporal logic, VDM, Z

**Gov & Univ:** Boyer-Moore, cleanroom, DDD, EHDM, HOL, VDM
FM Developers: Boyer-Moore, Clio, EHDM, EVES, HOL, PVS, Penelope, SDVS, Spectool, temporal logic, Z

31. In what applications and parts of the life-cycle have you used formal methods?

Industry: requirements modeling, design, and testing, conceptual study, detailed design, verification of algorithms, implementation

Gov & Univ: software requirements, high level requirements, avionics software, missile systems, electronic message systems, design, implementation, academic research projects

FM Developers: hardware designs, microcode, detailed design, algorithms, high-level HW design

32. Any additional comments?

Industry:

- "Workshops of this type where interested industries can attend and participate are excellent opportunities for technology transfer. I would encourage NASA to continue this type of interaction."
- "I would very much like to see a survey of (1) methods (2) languages & (3) tools presenting PROs & CONs of each. As a novice wanting to enter the field, where do I start?"
- "Tools are very important to this effort. Paper and pencil will not spread to industry."
- "It would have been nice to actually solve some simple problems using a formal technique rather than seeing lots of talks about proofs."
- "Suitable applications of FMs was not elaborated on. I still cannot say 'where' one should apply 'what' FM."
- "Need to separate HW FM's from SW FM's."
- "This is one of the only forums I have attended that has had equal representation from the software and hardware community sharing roughly equal concerns and a common interest in a technology of equal value and benefit to each community."
- "You are overcautious about overselling. ..."

Gov & Univ:

- "We must find a way to better find errors in Req'mts"
- "It is important for NASA to take a leadership position in Formal Methods for civilian aerospace applications."
- "FM appears to be currently the most feasible means of adding rigor and consistency to the software development process."
- "Keep holding this workshop!"
- "I really wish copies of slides had been available at the conference. It would greatly simplify notetaking."

FM Developers:

- "There is no 'royal road' to FM for industry."
- "FM is powerful for educating designers."
- "Formal methods are no panacea"
NASA Formal Methods Workshop Attendees

Jorgen B. Andersen
Honeywell, Inc.
Box 21111
Phoenix, AZ 85036-1111

Bob Baker
Research Triangle Institute
PO Box 12194
Research Triangle Park, NC 27709-2194
rlb@rti.rti.org

Mark Bickford
Odyssey Research Associates, Inc.
301 Dates Drive
Ithaca, NY 14850
email: mark@oracorp.com

Bhaskar Bose
Indiana University
215 Lindley Hall
Bloomington, IN 47405

Daniele Bozzolo
Union Switch and Signal, Inc.
5800 Corporate Drive
Pittsburgh, PA 15237

Ricky W. Butler
NASA Langley Research Ctr.
Mail Stop 130
Hampton, VA 23681-0001
email: rwb@air16.larc.nasa.gov

Jim Caldwell
NASA Langley Research Center
Mail Stop 130
Hampton, VA 23681-0001
email: caldwell@cs.cornell.edu

Victor Carreno
NASA Langley Research Center
Mail Stop 130
Hampton, VA 23681-0001
email: vac@air16.larc.nasa.gov

Jerome F. Coffel
Honeywell, Inc.
3660 Technology Drive
MN65-3240
Minneapolis, MN 55418
email: jcoffel@src.honeywell.com

Richard Covington
NASA Jet Propulsion Laboratory
MS 125-233
4800 Oak Grove Drive
Pasadena, CA 91109

Dan Craigen
ORA Canada
265 Carling Avenue
Suite 506
Ottawa, Ontario K1S 2E1
CANADA
email: dan@ora.on.ca

Ronald T. Crocker
Motorola, Inc.
1501 West Shure Drive
Arlington Heights, IL 60004
email: crocker@mot.com

Mark Crosland
Boeing
MS 88-12
P.O. Box 3707
Seattle, WA 98124

Jim Dabney
Intermetrics, Inc.
1100 Hercules
Suite 300
Houston, TX 77058

Mike DeWalt
FAA
ANM-106N
1601 Lind Avenue, S.W.
Renton, WA 98055-4056
Larry Lacy  
Rockwell International Corp.  
Collins Flight Control  
400 Collins Road NE  
Cedar Rapids, IA 52498

Jay Lala  
C. S. Draper Laboratory, Inc.  
555 Technology Square  
Cambridge, MA 02139  
email: lala@draper.com

H. Grady Lee  
Vitro Corporation  
400 Virginia Ave., SW  
Suite 825  
Washington, DC 20024

Miriam Leeser  
Cornell University  
School of Electrical Engineering  
Phillips Hall  
Ithaca, NY 14853-5401  
email: mel@ee.cornell.edu

Nancy Leveson  
University of California at Irvine  
ICS Dept.  
Orvome, CA 92717

Beth Levy  
The Aerospace Corporation  
Mail Station M1/099  
PO Box 92957  
Los Angeles, CA 90009-2957  
email: blevy@aero.org

Patrick Lincoln  
SRI International  
333 Ravenswood Ave.  
Menlo Park, CA 94025

Charles W. Meissner, Jr.  
NASA Langley Research Ctr.  
Mail Stop 130  
Hampton, VA 23681-0001  
email: c.w.meissner@larc.nasa.gov

Steven Miller  
Rockwell International  
Collins Commercial Avionics  
400 Collins Road NE  
Cedar Rapids, IA 52498

Paul Miner  
NASA Langley Research Ctr.  
Mail Stop 130  
Hampton, VA 23681-0001  
email: psm@air16.larc.nasa.gov

John Munro  
Martin Marietta Energy Systems, Inc.  
Oak Ridge National Laboratory  
P.O. Box 2008  
Oak Ridge, TN 37831-6008

Philip Newcomb  
Boeing Computer Services  
P.O. Box 24346  
MS 7L-64  
Seattle, WA 98124-0346  
email: philu@atc.boeing.com

Stephen Nicoud  
Boeing Computer Services  
P.O. Box 24346  
MS 7L-64  
Seattle, WA 98124-0346  
email: stephen@boeing.com

Eric Peterson  
Honeywell, Inc.  
Air Transport Systems Div.  
Box 21111  
Phoenix, AZ 85036-1111

Richard Platek  
Odyssey Research Associates, Inc.  
301A Dates Drive  
Ithaca, NY 14850

Joseph Profeta  
Union Switch and Signal, Inc.  
5800 Corporate Drive  
Pittsburgh, PA 15237
Chris Walter
Allied Signal Aerospace Company
Aerospace Technology Center
9140 Old Annapolis Road
MD 108
Columbia, MD  21045-1998
dd:  chris@batc.allied.com

Robert E. Waterman
NASA Goddard Space Flt. Center
Code 302
Bldg. 6, Rm. 5-229
Greenbelt, MD  20771

Isaiah White
Boeing Defense & Space Group
P.O. Box 3999, MS 8H-09
Seattle, WA  98124-2499

Lloyd Williams
Software Engineering Research
264 Ridgeview Lane
Boulder, CO  80302

Phil Windley
University of Idaho
Computer Science Department
Moscow, ID  83843
dd:  windley@cs.uidaho.edu

Robert Wyman
Lawrence Livermore National Lab.
P.O. Box 808
Livermore, CA  94550
This report documents the Second NASA Langley Formal Methods Workshop held at the NASA Langley Research Center, August 11-13, 1992. The primary goal of the workshop was to bring together formal methods researchers and aerospace industry engineers to investigate new opportunities for applying formal methods to aerospace problems. The first part of the workshop was tutorial in nature. The second part of the workshop explored the potential of formal methods to address current aerospace design and verification problems. The third part of the workshop involved on-line demonstrations of state-of-the-art formal verification tools. Also a detailed survey was filled in by the attendees; the results of the survey are compiled in this report.

**13. ABSTRACT (Maximum 200 words)**

This report documents the Second NASA Langley Formal Methods Workshop held at the NASA Langley Research Center, August 11-13, 1992. The primary goal of the workshop was to bring together formal methods researchers and aerospace industry engineers to investigate new opportunities for applying formal methods to aerospace problems. The first part of the workshop was tutorial in nature. The second part of the workshop explored the potential of formal methods to address current aerospace design and verification problems. The third part of the workshop involved on-line demonstrations of state-of-the-art formal verification tools. Also a detailed survey was filled in by the attendees; the results of the survey are compiled in this report.

**14. SUBJECT TERMS**

Formal methods; Digital flight control; Verification; Specification; Design proof

**15. NUMBER OF PAGES**

243

**16. PRICE CODE**

A11

**17. SECURITY CLASSIFICATION OF REPORT**

Unclassified

**18. SECURITY CLASSIFICATION OF THIS PAGE**

Unclassified

**19. SECURITY CLASSIFICATION OF ABSTRACT**

Unclassified

**20. LIMITATION OF ABSTRACT**

Unclassified