FORMAL SPECIFICATION AND MECHANICAL VERIFICATION

P.M. Melliar-Smith

Rapporteurs: Mr. J. Black
Dr. F. Cristian

Abstracts:

1. The Formal Specification and Mechanical Verification of SIFT: A Fault-Tolerant Flight Control System

This lecture will contain an outline of SIFT, its exceptional reliability requirement, and the need for verification rather than measurement to confirm that reliability. In the analysis of SIFT, a clear distinction was made between design verification and program verification, and the resulting design specifications and proof hierarchy will be exhibited. The lecture will give an outline of the STP verification system, the many-sorted quantified first-order logic with schemas used in STP, and the development of proofs in STP. During the proof of SIFT, much was learned about the effects of scale on verification, and about man-machine interaction during verification.

2. A System for Formal Specification and Mechanical Verification

Based on our experience with the proof of SIFT, a new verification system is being designed and implemented. The lecture will describe our objectives for the system, a new specification language, and our approach to the use of Hoare sentences and state functions for the specification and verification of programs. Of particular importance in this system is the relationship between man and machine, based on complete decision procedures for well-defined logical domains and on human understanding of the proof at a higher level.

3. The Specification and Verification of Asynchronous Distributed Systems

This lecture will describe an approach to the specification and verification of distributed systems, using a temporal logic based on the S4 modal logic. The temporal logic will be introduced, and a novel decision procedure for it will be described. Alternative styles of specification using temporal logic will be illustrated, with examples from communication protocols. The importance of design proof for asynchronous systems, and the use of service and protocol specifications for design proof, will be discussed.

References:

P.M. Melliar-Smith , R.L. Schwartz, "Formal Specification and Mechanical Verification of SIFT: a Fault-Tolerant Flight Control System", IEEE Trans. on Computers, Vol. C-31, No. 7 (July 1982), pp. 616-630.

R.E. Shostak, R.L. Schwartz, P.M. Melliar-Smith, "STP: a Mechanical Logic for Specification and Verification", in Proc. 6th Conference on Automated Deduction, Lecture Notes in Computer Science, Vol. 138, Springer Verlag (1982).

R.L. Schwartz, P.M. Melliar-Smith, "From State Machines to Temporal Logic: Specification Methods for Protocol Standards", IEEE Trans. on Communications, Vol. COM-30, (December, 1982).