Summary of the work done by WG 2.2

Report to IFIP TC-2 by E.-R. Olderog
submitted on 28 January 1999

IFIP WG 2.2 on "Formal Description of Programming Concepts" was established 1965 as one of the first IFIP Working Groups. Its currently over 30 members are leading experts in the *theory and practice of formal methods* for the specification, verification and design of software and systems. Such formal methods provide a basis for both better understanding and better implementing systems.

Members of WG 2.2 shaped various styles of semantics, i.e. formal description techniques, comprising *denotational*, *operational*, *algebraic* and *logical semantics*. Currently, the most prominent area is that of *reactive systems*, i.e. of systems that are continuously interacting with their environments. Examples of such systems range from simple vending machines to controllers of physical plants. Members of WG 2.2 investigate various semantic models of reactive systems, their specification and verification, and tools for their analysis and design. This includes in particular the study of concurrent systems as well as *embedded real-time* and *hybrid* systems. We are proud that our member Amir Pnueli, who coined the term "reactive system", has won the 1997 ACM Turing Award.

More generally, members of WG 2.2 are working on a wide range topics listed below. Advances in these topics are presented and discussed intensively during the annual meetings of WG 2.2 to which also a number of observers as candidates for future membership are invited.

- *Foundations of computation* :

  Calculi that provide a basis for functional programming or systems with concurrency and mobility are studied. Formal type systems for functional, concurrent and object-oriented programming languages are developed. Types provide finitary logical descriptions of language semantics and so they can be used to reason about properties of programs.

- *Formal description of specification concepts* :

  Graphic specification techniques are possible means for bridging the gap between application and computer science experts. Such specification techniques are widely used, for example, in the area for telecommunication (message sequence charts). Suitable formal semantics for such graphic techniques is one of the topics discussed at WG 2.2.

  Another more general topic is the relationship and integration of different formal specification techniques as a basis for correct system design.

- *Formal description of programming concepts* :

  Using techniques from denotational, operational and algebraic semantics essential parts of languages with concurrency concepts, most recently parts of coordination languages like Linda or object-oriented languages like Java, have been formally described.

- *Concepts of verification* :

  Verification is concerned with the proof of desirable properties (e.g. safety and liveness) of programs and systems. To this end, suitable concepts of program, process and data refinement have been investigated and Hoare-style proof systems and compositional proof methods have been developed.

- *Tool-supported verification* :

  Formal verification concepts are only a prerequisite of actually proving that certain properties hold. A practically crucial next stage is a tool supported approach to verification. More recently, WG 2.2 has attracted some new members who are pushing this approach to the limits. This concerns both the fully automatic verification of (essentially) finite state systems known as "model checking" and the interactive verification using theorem provers.

- *Correct system design* :

  Verification of properties is just one activity during the design of a system. Considering the whole design process requires the development of suitable methodologies and combination of techniques and tools. Members address various aspects of this task ranging from conceptual frameworks to tool-supported environments.

- *Applications* :

  During the annual meetings of WG 2.2 also case studies from applications areas like telecommunication, real-time embedded systems and hybrid systems are discussed. These may stem from industrial contacts and projects that some members maintain.

Relation to practice

Their is no direct formal relation of WG 2.2 to industrial practice. However, at least a third of the members actively look at industrial problems and use them as a stimulation for their research work. This is done by tackling industrially motivated case studies and by developing application specific formal methods which make the best use of a variety of foundational results. Some members also have or had projects with or funded by industrial partners.

Some examples of successful applications of formal methods to industrial problems suggest that a fine tuning and combination of several formal methods for specific application domains is the winning idea.

Communication of results

The official activities of WG 2.2 include Working Conferences in 1977, 1982, 1986, 1990, 1994 and 1998, and State-of-the-Art Seminars 1989 in Brazil, 1992 in India and 1996 in China, which significantly contributed to the dissemination of our results. The last three Working Conferences were organized jointly with WG 2.3 and in 1994 also with WG 2.1.

Additionally, members of WG 2.2 are active in promoting the development and application of formal methods e.g. by publishing text books and monographs, by organising conferences and workshops, in particular those on comparative case studies (published as books), by participation in nationally and internationally funded projects, or simply by presenting their work at conferences, seminars and lectures on formal methods aimed at practical applications and at industry-oriented courses.