Egon Börger (Pisa)

From Programming Languages to Business Processes

System Modeling, Verification and Validation

Mathematical Rigour in Computer Science
Festkolloquium (Peter Schmitt's 60th Birthday)
Karlsruhe May 2008

boerger@di.unipi.it
Università di Pisa, Dipartimento di Informatica, Italy

Really: From Logic Languages to ...

- Models . . .
  - *of classes of logical formulae* (axiom systems)
    - Predicate Logic, Model Theory, Set Theory: studying models (Tarski structures) concerning
      - their existence (consistency/Entscheidungsproblem)
      - their structural properties
      - relations among (classes of) them
      - methods to construct them
  - *of computation*: Recursion Theory and Theory of Algorithms, studying means to measure expressivity and complexity
- 10.5.1974: My first talk in Karlsruhe, at Inst. Ang.Inf. (H. Maurer), of a series on *Algorithmic Decision Problems* (1978, 1981, 1987)
- 15.07.-26.07.1975 Meeting P. Schmitt at European Logic Colloquium and Summer School (Clermont-Ferrand)

Cooperation with Logic and CS colleagues in Karlsruhe

- *Logic and Machines: Decision Problems and Complexity*
  Münster 1984, LNCS 171
  – Kleine Büning, Diana Schmidt, Sperschneider
- *Rödding Gedenkschrift*, 1987, LNCS 270
  Brüggemann, Klein, Kleine Büning, Kummer, Lettmann, Ottmann, Sperschneider
- *Proc. CSL'87* (the first CSL) in Karlsruhe, LNCS 329
  Heisel, Karpinski, Kleine Büning, *P. Schmitt*, Reif, Stephan
- *EACSL founded* on 14.7.1992 in Dagstuhl with participation of P. Schmitt

- *Tableau paper* with P. Schmitt in J. Log.& Comp. (1997)
- P. Schmitt (with U. Glässer) editor of *Proc. 5th Intern. ASM Workshop* held 1998 in Magdeburg as part of GI Meeting

Models of (Semantics of) Programming Languages

- Debate on *declarative versus operational* semantics ("is the compiler the definition of a language"?) and on *executable specifications*
  - case of PROLOG: still logic?
  - 1989: ASM model of Prolog (to become ISO standard definition)
- validation used as companion to verification: run a system (simulation, mechanical or by Gedankenexperiment) to experiment with and analyze intended meanings ('scenarios')
  - 17.1.1990: presentation of the Prolog model in a talk in KA
  - meeting P. Schmitt at IBM Scientific Center in Heidelberg (1989/90)
- issue of *parallelism*: hard to reduce to logic alone
  - work with P. Schmitt on ASM model of Colmerauer's Prolog III (CSL'90 Heidelberg)
    - identifying problems and clarifying critical issues (e.g. freeze feature for delaying execution until a certain term is known)
    - applied to other parallel Prologs (E. Riccobene in KA)

Verification of Programming Language Implementations

- correctness proof for compilation of *Prolog2WAM* code via successive refinement steps of ASM model of Prolog to ASM model of WAM
  - KIV verification of the proof: Ahrendt, Schellhorn (1997-1999)
  - KIV implementation and verification of ASM refinement concept
    - recent application by Schellhorn to verify Mondex electronic purse
- verifying *Occam2Transputer* compilation and *architectural design* methods (in particular pipelining for RISC architectures and massively parallel processors)
  - Verifix project (Goos, Langmaack, von Henke) where ASMs are used to model both the compiler and the involved processors
    - challenge: product-line reuse for prover-based verification of
      - *Java2JVM* (AsmGofer simulator, J. Schmid)
      - *C#2.NETCLR* (AsmL simulator, G. Fruja)
- talks in KA: 1990, March 1995, June 1995, 1996, 2001

Rules for Modeling Prolog, Prolog III, etc.

if *DataCond* **and** *CtlCond* **and** *EventCond*

then

DataOp

CtlOp

EventOp

where

EventCond = still some clause to be tried

CtlCond = current constraint solvable

DataCond = involved terms known

DataOp = unification of involved terms

CtlOp = propagation of constraint solution

EventOp = forward control to next alternative or backtracking

Rules for Modeling Business Processes (e.g. BPMN)

work triggered by sabbatical at SAP Research (Karlsruhe) in 2005

if $DataCond$ **and** $CtlCond$ **and** $EventCond$ **then**

DataOp

CtlOp

EventOp

where

$DataCond/Op =$ about business process data

$CtlCond/Op =$ about internal process control (token passing)

$EventCond/Op =$ about communication (mssg passing)

work supported by Humboldt Research Award (joint with B. Thalheim)

system models: Tarski structures, but focus on rigorous description, validation and verification of their dynamics and on linking model behaviour at hierarchies of levels of abstraction

References

- E. Börger and P. Schmitt: *A formal operational semantics for languages of type Prolog III*. Proc. CSL'90
- E. Börger and P. Schmitt: *A Description of the Tableau Method using Abstract State Machines*. J. Log. & Comp. 1997
- R. Stärk, J. Schmid, E. Börger, *Java and the Java Virtual Machine: Definition, Verification, Validation*.
  – Springer-Verlag 2001.
- E. Börger and B. Thalheim: *A Method for Verifiable and Validatable Business Process Modeling* (to appear LNCS 2008)