The Logical Basis of System Correctness

Robert L. Constable

Cornell University, Ithaca, USA

The principal focus of these lectures will be the synthesis of algorithms and protocols from constructive proofs that specifications are achievable. The practice of creating correct-by-construction functional and procedural programs is well established, and many examples are widely known. We will briefly consider the functional case as a way of motivating the case of distributed protocols.

The lectures will explain new synthesis techniques for distributed systems using the notion of event structures and the associated logic of events developed by Mark Bickford and me starting in 2003. My article in the proceedings of the 2005 summer school provides one example of our approach. In these lectures I will systematically develop the new theory and illustrate the synthesis method.

Much of the lecture material is on the Nuprl Web page at `www.nuprl.org`. It is included in the section called Math Library.

Course Outline

Lecture 1 A Computation System and Functional Types

Lecture 2 Types and Classes

Lecture 3 Event Systems and Types for Concurrency

Lecture 4 A Logic of Events

References

1. R. Constable. *Information-Intensive Proof Technology*, In: Proof and Computation, Proc. of Marktoberdorf Summer School 2003, H. Schwichtenberg, K. Spies (eds), IOS Press, 2005

2. R. Constable. *Naive Computational Type Theory*, In: Proof and System Reliability, H. Schwichtenberg, R. Steinbrüggen (eds),pp:213-259, Kluwer, 2002,

3. M. Bickford, R. Constable. *A Logic of Events*, TR2003-1893, Cornell University, Computer Science Department

4. M. Bickford, R. Constable, J. Halpern, S. Petride. *Knowledge-Based Synthesis of Distributed Systems Using Event Structures*, In: Proc. of the LPAR-11, Lecture Notes in Artificial Intelligence, pp: 449-465, Springer, 2005.

5. N. Lynch. *Distributed Algorithms*, Morgan Kaufman Publishers, 1996.

6. M. Bickford. *Event Systems, an on-line formalization*, 2005
   `www.cs.cornell.edu/Info/People/sfa/Nuprl/EventSystems/`