SUMMARY

T. Karvi

December 2011

Overall Picture

- How an equivalence-based verification proceeds: writing the specifications of the processes in a protocol, combing the processes in the specification, writing the specification of the service, forming the global state graphs (protocol and service) using automated tools, choosing an equivalence, comparing the global state graphs with respect to the chosen equivalence.
- How the verification based on temporal logic proceeds: writing the specification of the protocol, forming the global state graph, writing the temporal logic formulas describing properties of the protocol, verifying that the formulas are true in the model.
- Successful approaches: verification of hardware circuits, reasonably small protocols or systems. If systems are large, global state graphs are enormous and their construction or analysis do not succeed.

AB protocol and Transition Systems

- Able to draw scenarios with different channels and with different approaches to environment.
- Able to draw transition systems with different channels and environments.
- Formal definitions of a transition system.
- Definitions of arrow notations.
- The concept of service and service as a transition system.

Equivalences

- Formal definitions of a relation, equivalence relation.
- Correspondence between equivalence and partition.
- Formal definition of trace equivalence.
- Ad hoc calculation of trace equivalence.
- Formal definition of weak bisimulation equivalence.
- Able to check the weak bisimilarity of transition systems.
- Minimal process with respect to trace and weak bisimulation equivalence: ad hoc construction.

Basic Lotos

- Formal definition of Lotos operators.
- Transition systems from Lotos expressions.
- Congruence properties of Lotos operators.
- Process instantiations.
- Ability to write simple Lotos specifications: AB, FE, channels, etc.

Model Checking

- Formal definition of Kripke structures.
- Ad hoc (or systematic) transformations from transition systems to Kripke structure.
- Formal definitions of LTL formulas.
- Temporal logic operations, old and new.
- Interpretation of typical formulas.
- Determination the equivalence of formulas, truth with respect to a Kripke structure.