Tenth Meeting of the

IFIP WG 1.6 on Term Rewriting

July 18, 2008, Hagenberg, Austria

9:15 – 9:45 Johannes Waldmann: *Certified Termination*

9:45 – 10:15 Bernhard Gramlich: *Transformations of Conditional Rewrite Systems Revisited*

10:15 – 10:45 Coffee break

10:45 – 11:30 Maribel Fernández: *Nominal Matching and Alpha-Equivalence Checks*

11:30 – 12:00 Chris Lynch: *Cap E-Unification*

12:00 – 13:30 Lunch

13:30 – 14:15 Ralf Treinen: *Symbolic Protocol Analysis for Monoidal Equational Theories*

14:15 – 14:45 Manfred Schmidt-Schauß: *Semantics of Programming Languages Based on Small-Step Operational Semantics*

14:45 – 15:15 Coffee break

15:15 – 16:15 *Progress Reports and General Discussion*

- *Step 1:* each participant summarizes the current situation at his or her site and/or country
- *Step 2:* general discussion

16:15 – 16:30 Aart Middeldorp: *ISR 2008 Status Report*

16:30 – 17:30 *Business Meeting* (members only)

- next meeting of the working group
- next ISR
- candidates / election of the WG chair and vice-chair
- memberships
- other topics

Johannes Waldmann: ***Certified Termination***

The goal is to have automated termination provers that output certificates for termination that can be verified by an established proof checker (e.g. `Coq`, `Isabelle`).

The central design decision is that the certificate format is both independent of the termination prover that produces it, and of the proof checker that verifies it.

There are several research groups working in that area. In the 2007 Termination Competition, we established the "Certified" category, with several entrants.

We also established the "Workshop on Certified Termination" (Nancy 2007, Leipzig 2008), and my talk will summarize some results and discussions from these meetings, see also `http://termination-portal.org/wiki/WScT08-Minutes-Certification`.

Work on certified termination also helps to advance other areas, e.g., the discussion on the modular structure of the certificates automatically leads to discussion on the modular structure of termination provers. There, the goal is to provide sub-provers as pluggable, re-usable components. This will lower the "entry barrier" for new researchers that want to start working in automated termination.

Bernhard Gramlich: ***Transformations of Conditional Rewrite Systems Revisited***

We revisit known transformations of conditional rewrite systems to unconditional ones in a systematic way. We present a unified framework for describing and classifying such transformations, discuss the major problems arising, and finally present a new transformation which has some advantages as compared to some of the most recent approaches from the literature. (Joint work with Karl Gmeiner)

Chris Lynch: ***Cap E-Unification***

Given a set S of terms, Cap(S) is the set of all terms that can be formed by adding function symbols on top of elements of S. Given S and a term t, the Cap Unification problem is to find a substitution θ such that there is a term $s \in S$ with θ a unifier of s and t. We give a decision procedure for Cap Unification. We also consider Cap E-unification: the Cap Unification problem modulo an equational theory. We show that Cap E-unification is equivalent to the secrecy problem from cryptographic protocol analysis for an active intruder with a bounded number of protocol sessions, where the equational theory represents the intruder abilities. We show conditions where Cap E-Unification is decidable, using an extension of Basic Narrowing called Cap Narrowing. The traditional Dolev-Yao intruder abilities are covered by our decidability result.

Ralf Treinen: ***Symbolic Protocol Analysis for Monoidal Equational Theories (or: How Algebra Helps to Solve Intruder Constraints)***

We consider the design of automated procedures for analyzing the (in)security of cryptographic protocols in the Dolev-Yao model for a bounded number of sessions when we take into account some algebraic properties satisfied by the operators involved in the protocol. This leads to a more realistic model than what we get under the perfect cryptography assumption, but it implies that protocol analysis deals with terms modulo some equational theory instead of terms in a free algebra.

The main goal of this talk is to set up a general approach that works for a whole class of so-called monoidal theories which contains many of the specific cases that have been considered so far in an ad-hoc way, e.g., exclusive or, Abelian groups, exclusive or in combination with the homomorphism axiom.

We follow a classical schema for cryptographic protocol analysis which proves first a locality result and then reduces the insecurity problem to a symbolic constraint solving problem. This approach strongly relies on the correspondence between a monoidal theory E and a semiring Se_E which we use to deal with the symbolic constraints. We show that the well-defined symbolic constraints that are generated by reasonable protocols can be solved provided that unification in the monoidal theory satisfies some additional properties. The resolution process boils down to solving particular quadratic Diophantine equations that are reduced to linear Diophantine equations, thanks to linear algebra results and the well-definedness of the problem. Examples of theories that do not satisfy our additional properties appear to be undecidable, which suggests that our characterization is reasonably tight.

This is joint work with Stéphanie Delaune, Pascal Lafourcade, and Denis Lugiez.

Manfred Schmidt-Schauß: ***Semantics of Programming Languages Based on Small-Step Operational Semantics***

Observational semantics of deterministic and non-deterministic programming languages can be defined using their respective small-step operational semantics (rewrite semantics). In general this provides the coarsest congruence w.r.t. observations, and thus can be seen as a canonical semantics.

We present several methods and techniques to prove correctness of program transformations: may- amd must-convergence, corresponding context lemmas, complete sets of diagrams, and methods to prove correctness of translations between programming languages. We show that the basic methods can be adapted and succesfully applied to rather different kinds of programming languages.

Aart Middeldorp: ***ISR 2008 Status Report***

I present a short report on ISR 2008.