ETAPS Daily

Issue 6 — Thursday, 29 March 2012

Thank you!

Yesterday at the banquet you were entertained by C-Jam, the cello quartet of Pärt Tarvas and some of his colleagues from the Estonian National Symphonic Orchestra (ERSO) (`http://www.c-jam.eu`). We hope you liked them, we tried very hard to get them to play for us. We thank you for the kind words we heard about our organization—it is an honor and a pleasure for us to host you here.

LEARN ABOUT THIS PLACE

Estonia: some numerical geography

The area of Estonia is 45 227 sq km (approx. the size of the Netherlands or Denmark). There are more than 1500 islands. Saaremaa (2671 sq km) is the 2nd largest island of the Baltic Sea. Estonia has 3794 km of coastline and more than 1400 lakes, Lake Peipsi (3555 sq km) is the 4th largest lake in Europe.

We are very proud of the intellectural heights ascended to during ETAPS 2012 in Estonia. Geographically, Estonia's heights are not quite so stratospheric. Estonia's highest point is called Suur Munamägi ("Big Egg Hill"). Its peak is 318 m above sea level. The longest river is Võhandu (162 km).

WE ARE PROUD OF YOU

ETAPS 2012 best papers

Yesterday at the banquet, the recipients of the ETAPS 2012 best paper awards were are announced and congratulated. The winners are:

- EAPLS: "Language-Theoretic Abstraction Refinement" by Zhenyue Long, Georgel Calin, Rupak Majumdar and Roland Meyer (FASE)
- EASST: "Fine Slicing: Theory and Applications for Computation Extraction" by Aharon Abadi, Ran Ettinger and Yishai A. Feldman (FASE) and "Pushdown Model Checking for Malware Detection" by Fu Song and Tayssir Touili (TACAS)
- EATCS: "Effective Characterizations of Simple Fragments of Temporal Logic Using Prophetic Automata" by Sebastian Preugschat and Thomas Wilke (FoSSaCS)

Weather forecast

Today	Tomorrow	Saturday
2 ‖ 7 °C	1 ‖ 5 °C	-2 ‖ 2 °C

They promise snow for Saturday?!?

Last conference starting

In the TACAS plenary talk in the morning, our very own **Holger Hermanns** will talk about quantitative modelling of power grids. In the afternoon **François Bodin** will give a CC plenary talk about programming of heterogeneous many-cores.
These conferences will have regular sessions today:

CC Compiler Construction

FASE Foundational Aspects of Software Engineering

FoSSaCS Foundations of Software Science and Computation Structures

TACAS Tools for Analysis and Construction of Systems

ETAPS
EUROPEAN JOINT CONFERENCES ON THEORY & PRACTICE OF SOFTWARE

`http://www.etaps.org/2012`

ETAPS 2012 local organizers

ETAPS DAILY INTERVIEWS BRUNO BLANCHET

ProVerif, Cryptoverif

ProVerif is being used already for 10 years. How much has it affected protocol design in practice? How much should it have affected?

ProVerif has mostly been used not in protocol construction, but in verification of the existing protocols. For example, it has been applied to already deployed protocols such as TLS and DAA. ProVerif is used mostly as a researcher tool, not much in industry.

In the future, I hope that ProVerif will be more widely used in industry and used earlier in the design phase of protocols. That is one of the goals of the recent improvements in the interface of ProVerif.

What about Cryptoverif: what impact does it have in practice?

By the moment, Cryptoverif has less impact in practice, as it is more recent. ProVerif is being used more often.

How important is computational soundness? Is symbolic analysis sufficient?

It is definitely important to have computational proofs of the protocols. If an attack is found in the symbolic model, it is sufficient since the computational adversary is more powerful and may conduct the same attack in the computational model. On the other hand, if the protocol seems to be secure in the symbolic model, it does not mean that it is secure also in the computational model. Also, some proofs are easier in the computational model—for example, equivalence proofs. ■

ETAPS DAILY INTERVIEWS GEORG GOTTLOB

UML-lean

How do the complexity-theoretic results about the query complexity of Datalog± translate into the time and memory requirements of the analysis of UML diagrams in practice?

For (unrestricted) Lean UML Class Diagrams (UCDs), under which query answering is tractable in data complexity, the given diagram and the query can be compiled into a Datalog query. Such a query can be executed using a standard Datalog engine, for which efficient implementations exist (e.g., DLV). For the restricted formalism, query answering is highly tractable in data complexity; reasoning can be reduced to answering select-project-join SQL queries by means of standard database technology. The set of logical assertions that we obtain from a Lean UCD has polynomial size with respect to the given diagram. In practical terms, this means that a diagram can be transformed into a form that can be automatically manipulated without an exponential memory consumption. Finally, an instantiation of a diagram can be efficiently stored in a relational database.

Why namely these non-diagrammatic constructs in UML-lean? What is the significance of this choice in theory and in practice?

It is not possible to express diagrammatically that the intersection of three or more classes of a UCD is empty. This constraint occurs very often in practice, however. It-can be easily expressed by means of negative constraints. Moreover, the often used assumption that two or more classes have a most-specific class is again not representable diagrammatically; this justifies the use of most-specific class constraints. Finally, in a UCD we can only specify the type of an attribute. However, a useful modeling construct is to restrict also the type of the domain of an attribute (if seen as a binary relation); domain-type constraints provide this modeling feature. Domain-type constraints can be expressed in description logics by means of general inclusion axioms among qualified existential restrictions and concepts. Lean UCDs can be combined with arbitrary negative constraints and guarded tuple-generating dependencies (TGDs) without losing tractability of query answering in data complexity. But unrestricted use of guarded rules causes increase of combined complexity. ■