ARGO - Automated Reasoning GrOup

Filip Marić

Faculty of Mathematics,
University of Belgrade

30. 3. 2013.

Overview

1 About our group

2 SAT/SMT solving

3 ATP in geometry

4 Formalizations in ITP

5 Software verification tools

6 Applications in education

7 Other work

Overview

1 About our group

2 SAT/SMT solving

3 ATP in geometry

4 Formalizations in ITP

5 Software verification tools

6 Applications in education

7 Other work

General information

- Based at the Department of Computer Science at the Faculty of Mathematics, University of Belgrade
- http://argo.matf.bg.ac.rs
- Current members: 2 PhD and 8 PhD students

General information

Interested in various areas of automated reasoning

- SAT/SMT solving
- Automated theorem proving (e.g. in geometry)
- Interactive theorem proving (Isabelle/HOL)
- Softvare verification
- Applications in Education
- ...

Projects

- COST Action IC0901,
- bilateral joint research grant SNF SCOPES IZ73Z0_127979 with LARA (EPFL),
- bilateral joint research grant Pavle Savić/Egide with Uni. Strasbourg.

Events

- regular seminar
- 5 workshops (FATPA – Formal and Automated Theorem Proving and Applications) organized
- Our members have participated in many events (workshops, conferences, summer schools) and visited several other groups

Publications in previous 3 years

- 13 peer-reviewed conference/workshop publications (IJCAR, FM, SAT, VSTTE, Calculemus, MKM, ADG, ...)
- 11 journal publications (JAR, IST, AIR, TCS, LMCS, IDA, Informatica, EPTCS)

Overview

1 About our group

2 SAT/SMT solving

3 ATP in geometry

4 Formalizations in ITP

5 Software verification tools

6 Applications in education

7 Other work

URSA – Uniform reduction to SAT/SMT

- An approach for solving a wide class of constraint satisfaction problems.
- Problems are specified by writing a test in an imperative C-like language.
- Tests are automatically converted to SAT/SMT formulae and efficient solvers are used to find values that satisfy the tests.
- Tools: URSA (Janičić), UrBiVA (Marić Janičić), Ursa Major (Marić, Janičić).
- Current application — chess problems (Maliković, Janičić).

Toy example

URSA example

Alice picked a number and added 3. Then she doubled what she got. If the sum of the two numbers that Alice got is 12, what is the number that she picked?

```
B = A + 3; C = 2 * B; assert(B + C == 12);
```

The assertion evaluates to $A + 3 + 2 \cdot (A + 3) = 12$ and further to SAT or SMT instance yielding a solution $A = 1$.

Publications on uniform reduction to SAT/SMT

- P. Janičić: Uniform Reduction to SAT, LMCS 8(3), 2012.
- F. Marić, P. Janičić: URBiVA: Uniform Reduction to Bit-Vector Arithmetic, IJCAR 2010.

SMT solver implementation

- ArgoSMT (Banković)
- A parallel (multithreaded) SMT solver.
- Open source and flexible architecture.

Publications on implementing SMT solvers

- M. Banković: ArgoSMTExpression: an SMT-LIB 2.0 compliant expression library, Pragmatics of SAT, 2012.
- M. Banković, F. Marić: An Alldifferent Constraint Solver in SMT, SMT Workshop, 2010.

Machine learning, statistics and applications in SAT

- There are many efficient SAT solvers.
- Solver performance is usually governed by many input parameters.
- Is it possible to choose a solver and its suitable input parameters so that it performs best on a given SAT instance?
- Choice is made statically, based only on syntactic characteristics of the input SAT instance.
- Many machine-learning based approaches exist (e.g., SATZilla).

ArgoSmArT family of tools

- ArgoSmArT (Nikolić) – classifies SAT instances into families and chooses the best solver for the family the instance is classified into.
- ArgoSmArT-kNN (Nikolić) – for each instance finds k nearest neighbors and chooses the best solver for on those k instances.

Applications in CSP

- meSAT (Stojadinović) – a tool that reduces CSP problems to SAT (and SMT) supporting several different encodings.
- ArgoSmArT-kNN algorithm used to select an encoding suitable for a given instance.

Publications on machine learning, statistics and applications in SAT

- M. Nikolić, F. Marić, P. Janičić: Simple Algorithm Portfolio for SAT, Artificial Intelligence Review, 2011.
- M. Nikolić: Statistical Methodology for Comparison of SAT Solvers, SAT, 2010.

Overview

1 About our group

2 SAT/SMT solving

3 ATP in geometry

4 Formalizations in ITP

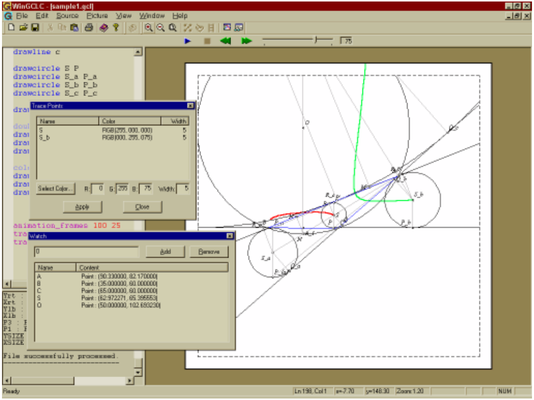
5 Software verification tools

6 Applications in education

7 Other work

Tools – GCLC

- GCLC - Geometric Construction Language, P. Janičić
  - a tool for visualizing and teaching geometry, and for producing mathematical illustrations,



Tools – GCLC

- GCLC has 3 integrated theorem provers:
  - Gröbner bases,
  - Simple Wu's method,
  - Area method.

Tools – OGP

- OGP - OpenGeoProver, I. Petrović
  - open source implementation in JAVA
  - 2 provers based on algebraic methods
    - Simple Wu's method,
    - Gröbner bases method.
  - It is beeing integrated into GeoGebra.

Understanding Triangle Construction Problems

- A careful analysis of one family of triangle construction problems (Marinković, Janičić).
- Detecting a small core of underlying geometry knowledge.
- Result is a small set of definitions, lemmas and primitive construction steps and a simple algorithm for automated solving of problems from this family.

Publications on ATP in geometry

- P. Janičić: Geometry Construction Language, Journal of Automated Reasoning, 44(1-2), 2010.
- P. Janičić, J. Narboux, P. Quaresma: The Area Method: A Recapitulation, Journal of Automated Reasoning.
- F. Marić, I. Petrović, D. Petrović, P. Janičić: Formalization and Implementation of Algebraic Methods in Geometry, THedu, 2011.
- V. Marinković, P. Janičić: Towards Understanding Triangle Construction Problems, MKM, 2012.

Coherent (geometric) logic

- A fragment of FOL with formulas

$$\forall \vec{x}(A_1 \wedge \ldots \wedge A_n \rightarrow \exists \vec{y_1} C_1 \vee \ldots \vee \exists \vec{y_m} C_m)$$

- Allows both quantifiers together with a simple complete proof procedure – forward ground reasoning.
- Direct, readable proofs. Simple generation of formal proofs.

Tools

- Euclid (Janičić) – tailored only for geometry theorem proving.
- ArgoCLP (Stojanović, Pavlović) – full coherent logic, only basic forward reasoning.
- ArgoCaLyPso (Nikolić) – a novel algorithm that combines forward reasoning with CDCL SAT solving techniques.

Applications of coherent logic

- Analysis of axiomatic systems of geometry (Stojanović).
- Generate readable, text-book proofs for Tarski's geometry.

Publications on Coherent logic

- S. Stojanović, V. Pavlović, P. Janičić: A Coherent Logic Based Geometry Theorem Prover Capable of Producing Formal and Readable Proofs, ADG, 2010.
- S. Stojanović, V. Pavlović, P. Janičić: Automated Generation of Formal and Readable Proofs in Geometry Using Coherent Logic, ADG postproceedings, 2011.
- M. Nikolić, P. Janičić: CDCL-Based Abstract State Transition System for Coherent Logic, MKM 2012.

Overview

1 About our group

2 SAT/SMT solving

3 ATP in geometry

4 Formalizations in ITP

5 Software verification tools

6 Applications in education

7 Other work

Formalization of geometry

- Current focus on models of geometry.
- Descartes plane is a model of Hilbert and Tarski axioms.
- Poincare disk in Complex plane is a model of Hyperbolic axioms.
- Investigate meta-theoretic properties.

Frankl's conjecture

- A family is union-closed if for every two sets from the family their union is also in the family.
- Frankl's conjecture (1979.): For every union-closed family there is an element occurring in at least half of the sets.
- Conjecture is verified for families up to certain size by complex algorithms.
- In our work we formally verified these algorithms and their underlying mathematics.

Publications on formalization of mathematics

- D. Petrović, F. Marić: Formalizing Analytic Geometries, ADG, 2012.
- F. Marić, M. Živković, B. Vučković: Formalizing Frankl's Conjecture: FC-families, Calculemus, 2012.

Software verification in ITP

- Verification of CDCL SAT solvers:
  - Verification of abstract state-transition systems for SAT.
  - Shallow embedding into Isabelle/HOL.
  - Hoare logic verification of imperative code.
- Verification of Incremental Simplex algorithm (used in most state-of-the-art SMT solvers).
  - A stepwise refinement approach.
  - Shallow embedding into Isabelle/HOL with code generation.

Software verification

- F. Marić: Formal Verification of a Modern SAT Solver by Shallow Embedding into Isabelle/HOL, TCS, 411(50), 2010.
- F. Marić, P. Janičić: Formal Correctness Proof for DPLL Procedure, Informatica 21(1), 2010.
- F. Marić, P. Janičić: Formalization of Abstract State Transition Systems for SAT, LMCS 7(3), 2011.
- M. Spasić, F. Marić: Formalization of Incremental Simplex Algorithm by Stepwise Refinement, FM, 2012.

Overview

1 About our group
2 SAT/SMT solving
3 ATP in geometry
4 Formalizations in ITP
5 Software verification tools
6 Applications in education
7 Other work

LAV

- LAV is a Low level Automatic software Verification tool built on top of the LLVM compiler infrastructure.
- Open source.
- Combines symbolic execution, SAT encoding of program's control-flow and some features of bounded model checking.
- Generates correctness conditions that are passed to a suitable SMT solver (Boolector, MathSAT, Yices, or Z3).

Publications on software verification

- M. Vujošević-Janičić, V. Kunčak: Development and Evaluation of LAV: an SMT-Based Error Finding Platform, VSTTE, 2012.

Overview

1 About our group

2 SAT/SMT solving

3 ATP in geometry

4 Formalizations in ITP

5 Software verification tools

6 Applications in education

7 Other work

- GCLC
- Formalizations of mathematics.
- Automated Evaluation of Students' Assignments.
    - Automated testing.
    - Software verification.
    - Similarity with the model solutions.

Publications on Applications in Education

- M. Vujošević-Janičić, Mladen Nikolić, Dušan Tošić, Viktor Kunčak: Software Verification and Graph Similarity for Automated Evaluation of Students' Assignments, Information and Software Technology, 2013.

Overview

1 About our group

2 SAT/SMT solving

3 ATP in geometry

4 Formalizations in ITP

5 Software verification tools

6 Applications in education

7 Other work

Other publications

- T. Hengl, M. Nikolić, R. MacMillan: Mapping Efficiency and Information Content, International Journal of Applied Earth Observation and Geoinformation, 2012.
- P. Janičić: Automated Reasoning: Some Successes and New Challenge, CECiiS 2011 (Invited lecture).
- M. Nikolić: Measuring Similarity of Graph Nodes by Neighbor Matching, Intelligent Data Analysis, 2013.

Conclusions

- ARGO – Automated Reasoning GrOup
- We are interested in many different areas of automated and interactive theorem proving.
- Also, in applying other areas in automated reasoning (machine learning, statistics, geometry).
- We have organized a series of successful workshops on formal and automated theorem proving (FATPA).
- `http://argo.matf.bg.ac.rs/`