Beyond DRAT: Challenges in Certifying UNSAT\textsuperscript{1}

Bertram Felgenhauer

University of Innsbruck

ARCADE 2017-08-06

\textsuperscript{1} Supported by FWF project P27528
About me

ARCADE

“... bring together key people from various sub-communities of automated reasoning ...”

My research

- term rewriting
- automation
- certification
- CADE reviewing
About UNSAT

Current state

• DRAT is de facto standard proof format for UNSAT
• covers DPLL+CDCL and many preprocessing techniques
• complete in theory
• some techniques are hard to express

Challenge

• certification for such techniques
SAT workflow

input

???-to-CNF

CNF

preprocessor

CNF

SAT solver

sat

unsat

model
SAT workflow

1. Input
2. ?? - to-CNF
3. CNF
4. Preprocessor
5. CNF
6. DRAT
7. SAT solver
8. DRAT checker
9. DRAT

- Sat model
- Unsat
- Ok
SAT workflow

input

???-to-CNF

CNF

preprocessor

CNF

DRAT

SAT solver

DRAT checker

proof assistant

proof

extract

sat

unsat

ok

ok

model

DRAT

Bertram Felgenhauer (UIBK)

Beyond DRAT

ARCADE
DRAT in a nutshell

DRAT

- sequence of clause additions and deletions
- steps preserve satisfiability
- at most one variable changes in each clause addition

Bertram Felgenhauer (UIBK) Beyond DRAT ARCADE 5/7
DRAT in a nutshell

DRAT

• sequence of clause additions and deletions
• steps preserve satisfiability
• at most one variable changes in each clause addition

CADE-26 update: Propagation Redundancy

• some fixed variables may change to fixed values
DRAT and Symmetry Breaking

Symmetry breaking

- symmetries permute satisfying assignments
- add lex-leader constraints
- tedious in DRAT
  - define new variables for variables affected by permutation
  - copy clauses
  - derive lex-leader constraint
  - delete old clauses
  - repeat
- small witnesses exist
- BreakIDCOMiniSatPS won No-Limit track in SAT 2016 competition
Summary

Proposal

- verified implementations allow more complex checkers
  ⇒ add dedicated checking for hard techniques like symmetry breaking

Challenges

- common format
- extensibility
  - symmetry breaking
  - XOR constraints
  - pseudo-boolean constraints
  - ... (domain-specific?)
- partial checkability