PeRIPLO

Proof tRansformer and Interpolator for Propositional LOgic

Simone Fulvio Rollini

Formal Verification Lab, University of Lugano

July 14th, 2013

Outline

Outline

Outline

Outline

- Open-source tool built on MiniSAT 2.2.0

PeRIPLO

Tool Description

- Open-source tool built on MiniSAT 2.2.0
- Born from OpenSMT for SAT-based model checking

PeRIPLO

Tool Description

- Open-source tool built on MiniSAT 2.2.0
- Born from OpenSMT for SAT-based model checking
- Features
  - SAT-solving

PeRIPLO

Tool Description

- Open-source tool built on MiniSAT 2.2.0
- Born from OpenSMT for SAT-based model checking
- Features
  - SAT-solving
  - Proof compression

PeRIPLO

Tool Description

- Open-source tool built on MiniSAT 2.2.0
- Born from OpenSMT for SAT-based model checking
- Features
  - SAT-solving
  - Proof compression
  - Interpolants generation (single and collections)

PeRIPLO

Tool Description

- Open-source tool built on MiniSAT 2.2.0
- Born from OpenSMT for SAT-based model checking
- Features
  - SAT-solving
  - Proof compression
  - Interpolants generation (single and collections)
- On demand development

- Interface:

- Interface:
  - Configuration file

- Interface:
  - Configuration file
  - Application Programming Interface

- Interface:
  - Configuration file
  - Application Programming Interface
- Input:

- Interface:
  - Configuration file
  - Application Programming Interface
- Input:
  - Propositional formula (SMT-LIB2 format)

- Interface:
  - Configuration file
  - Application Programming Interface
- Input:
  - Propositional formula (SMT-LIB2 format)
- Output:

- Interface:
  - Configuration file
  - Application Programming Interface
- Input:
  - Propositional formula (SMT-LIB2 format)
- Output:
  - Sat/Unsat

- Interface:
  - Configuration file
  - Application Programming Interface
- Input:
  - Propositional formula (SMT-LIB2 format)
- Output:
  - Sat/Unsat
  - Refutation

- Interface:
  - Configuration file
  - Application Programming Interface
- Input:
  - Propositional formula (SMT-LIB2 format)
- Output:
  - Sat/Unsat
  - Refutation
  - Interpolants

PeRIPLO

Usage

- Interface:
  - Configuration file
  - Application Programming Interface
- Input:
  - Propositional formula (SMT-LIB2 format)
- Output:
  - Sat/Unsat
  - Refutation
  - Interpolants
  - Various statistics

Outline

SAT

- Propositional satisfiability

SAT

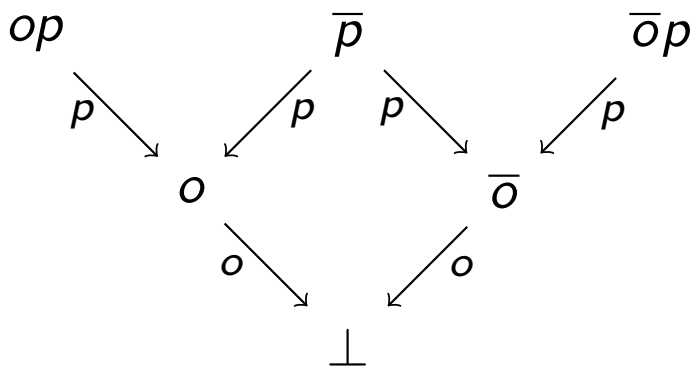
- Propositional satisfiability
- Resolution proof system

SAT

- Propositional satisfiability
- Resolution proof system
- Set of clauses $\{op, \overline{p}, \overline{o}p\}$

SAT

- Propositional satisfiability
- Resolution proof system
- Set of clauses $\{op, \overline{p}, \overline{o}p\}$
- Resolution proof DAG



Compression Framework

- SAT-solving

Compression Framework

- SAT-solving
  - DPLL CDCL
  - Generic

Compression Framework

- SAT-solving
  - DPLL CDCL
  - Generic
- Post-processing approach

Compression Framework

- SAT-solving
  - DPLL CDCL
  - Generic
- Post-processing approach
- Compression algorithms

Compression Framework

- SAT-solving
  - DPLL CDCL
  - Generic
- Post-processing approach
- Compression algorithms
  - Structural hashing at proof chains level [C10]
  - Lower unit clauses [FMP11]
  - Local Transformation Framework [BRST10,RBS10]
  - Structural hashing at proof level
  - Removal pivots redundancies along paths [BFHSS08,FMP11]

Implementation in PeRIPLO

```
begin
    LowerUnits();
    for i=1 to number of iterations do
        StructuralHashing();
        RecyclePivotsWithIntersection();
        for i=1 to number of traversals do
            ReduceAndExpose();
        end
    end
end
```

Experimental Evaluation

SAT Challenge 2012, SATLIB, CMU BMC

	#Bench	RedNodes	RedCore	RedEdges	TranTime(s)	Ratio
LU	180	1.49%	0.00%	1.89%	2.89	0.09
SH	180	6.17%	0.00%	6.89%	2.43	0.08
RPI	180	25.74%	1.17%	28.12%	7.15	0.20
RE 3	180	3.95%	0.07%	4.73%	13.23	0.31
LU+SH+RPI	180	31.04%	1.09%	34.13%	13.05	0.32

LU+SH+RPI+RE	#Bench	RedNodes	RedCore	RedEdges	TranTime(s)	Ratio
2,3	180	37.85%	1.51%	41.95%	24.19	0.46
3,3	180	40.09%	1.68%	44.50%	32.94	0.54

References


S.F. Rollini, R. Bruttomesso and N. Sharygina
An Efficient and Flexible Approach to Resolution Proof Reduction.
HVC 2010.


R. Bruttomesso, S.F. Rollini, N. Sharygina and A. Tsitovich
Flexible Interpolation with Local Proof Transformations.
ICCAD 2010.


S.F. Rollini, R. Bruttomesso, N. Sharygina and A. Tsitovich
Resolution Proof Transformation for Compression and Interpolation.
http://arxiv.org/abs/1307.2028


S.F. Rollini
PeRIPLO - Tool Description.
http://verify.inf.unisi.ch/periplo.html

Outline

Propositional Interpolation

- Resolution proof of unsatisfiability

Propositional Interpolation

- Resolution proof of unsatisfiability
- Single interpolants

Propositional Interpolation

- Resolution proof of unsatisfiability
- Single interpolants
- Collections of interpolants

Propositional Interpolation

- Resolution proof of unsatisfiability
- Single interpolants
- Collections of interpolants
- Interpolation properties in model checking

Propositional Interpolation

Interpolants Generation

- Interpolant I for unsatisfiable $A \wedge B$

Propositional Interpolation

Interpolants Generation

- Interpolant I for unsatisfiable $A \wedge B$
- Different procedures [P97,McM04,DKPW10]

Propositional Interpolation

Interpolants Generation

- Interpolant I for unsatisfiable $A \wedge B$
- Different procedures [P97,McM04,DKPW10]
- Generation approach

Propositional Interpolation

Interpolants Generation

- Interpolant I for unsatisfiable $A \wedge B$
- Different procedures [P97,McM04,DKPW10]
- Generation approach
  - Derivation of unsatisfiability resolution proof of $A \wedge B$

Propositional Interpolation

Interpolants Generation

- Interpolant I for unsatisfiable $A \wedge B$
- Different procedures [P97,McM04,DKPW10]
- Generation approach
  - Derivation of unsatisfiability resolution proof of $A \wedge B$
  - Computation of I from proof structure

Labeled Interpolation Systems

Propositional Interpolation

- Interpolation parametric in labeling function [DKPW10]

Labeled Interpolation Systems

Propositional Interpolation

- Interpolation parametric in labeling function [DKPW10]
- Interpolant determined by proof and labeling L

Labeled Interpolation Systems

Propositional Interpolation

- Interpolation parametric in labeling function [DKPW10]
- Interpolant determined by proof and labeling L
- Generalization of [P97,McM04] (P, M, M')

Labeled Interpolation Systems

Propositional Interpolation

- Interpolation parametric in labeling function [DKPW10]
- Interpolant determined by proof and labeling L
- Generalization of [P97,McM04] (P, M, M')
- Strength comparison reduced to labeling comparison

Labeling Lattice

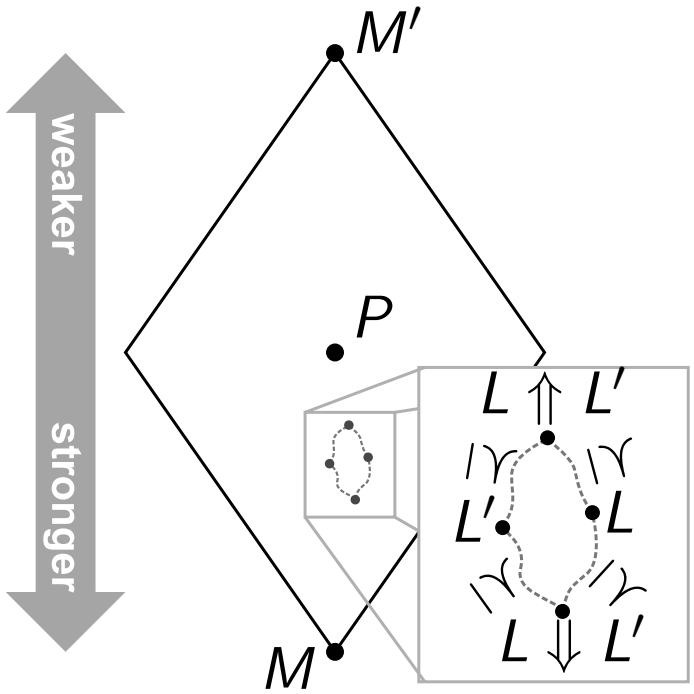
Labeled Interpolation Systems

- $L_1 \preceq L_2 \quad \Longrightarrow \quad I_1 \rightarrow I_2$

Labeling Lattice

Labeled Interpolation Systems

- $L_1 \preceq L_2 \quad \Longrightarrow \quad I_1 \rightarrow I_2$
- Labeling lattice



Labeled Interpolation Systems

Interpolant Strength

- Focus on interpolant strength

Labeled Interpolation Systems

Interpolant Strength

- Focus on interpolant strength
- Strength affects overapproximation coarseness

Labeled Interpolation Systems

Interpolant Strength

- Focus on interpolant strength
- Strength affects overapproximation coarseness
- Strength can affect verification performance, convergence

- Path Interpolation [JM06]

- Path Interpolation [JM06]
- Symmetric Interpolation / Simultaneous Abstraction [JM05]

- Path Interpolation [JM06]
- Symmetric Interpolation / Simultaneous Abstraction [JM05]
- State-Transition Interpolation [AGC12]

- Path Interpolation [JM06]
- Symmetric Interpolation / Simultaneous Abstraction [JM05]
- State-Transition Interpolation [AGC12]
- Tree Interpolation [MR13]

Labeled Interpolation Systems and Interpolation Properties

- Systematic exploitation of interpolant strength in model checking

Labeled Interpolation Systems and Interpolation Properties

- Systematic exploitation of interpolant strength in model checking
- Unsatisfiable formula $\tau_1 \wedge \ldots \wedge \tau_m$

Labeled Interpolation Systems and Interpolation Properties

- Systematic exploitation of interpolant strength in model checking
- Unsatisfiable formula $\tau_1 \wedge \ldots \wedge \tau_m$
- Generation of multiple interpolants $I_1, \ldots, I_n$

Labeled Interpolation Systems and Interpolation Properties

- Systematic exploitation of interpolant strength in model checking
- Unsatisfiable formula $\tau_1 \wedge \ldots \wedge \tau_m$
- Generation of multiple interpolants $I_1, \ldots, I_n$
- Generation of each I_i with different L_i

Labeled Interpolation Systems and Interpolation Properties

- Systematic exploitation of interpolant strength in model checking
- Unsatisfiable formula $\tau_1 \wedge \ldots \wedge \tau_m$
- Generation of multiple interpolants $I_1, \ldots, I_n$
- Generation of each I_i with different L_i
- Interpolation property requirements

Labeled Interpolation Systems and Interpolation Properties

- Systematic exploitation of interpolant strength in model checking
- Unsatisfiable formula $\tau_1 \wedge \ldots \wedge \tau_m$
- Generation of multiple interpolants $I_1, \ldots, I_n$
- Generation of each I_i with different L_i
- Interpolation property requirements
- Identification of constraints on $L_1, \ldots, L_n$

Interpolation Property Requirements

Simultaneous Abstraction

- Requirement: $I_1 \wedge \ldots \wedge I_n$ UNSAT

Interpolation Property Requirements

Simultaneous Abstraction

- Requirement: $I_1 \wedge \ldots \wedge I_n$ UNSAT
- Satisfied for: $L_1, \ldots, L_n \preceq$ Pudlák [RSS12]

Interpolation Property Requirements

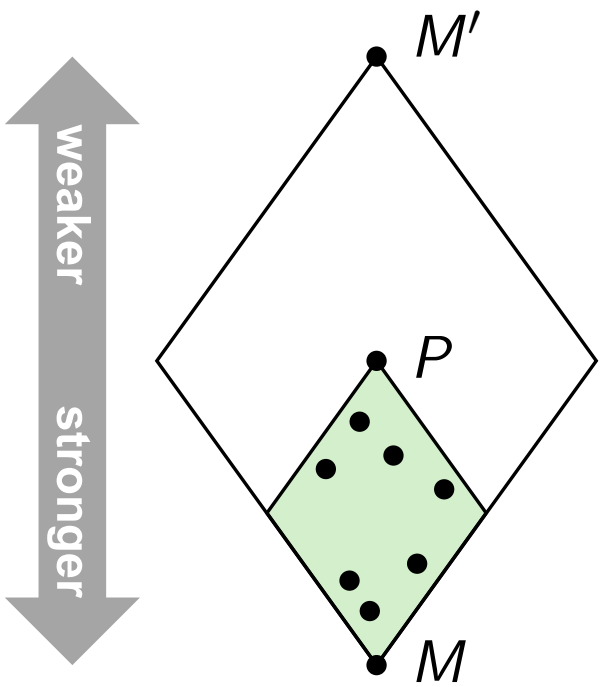
Simultaneous Abstraction

- Requirement: $I_1 \wedge \ldots \wedge I_n$ UNSAT
- Satisfied for: $L_1, \ldots, L_n \preceq$ Pudlák [RSS12]
- Not satisfied in general for: $L_i \succ$ Pudlák [GRS13]

Interpolation Property Requirements

Simultaneous Abstraction

- Requirement: $I_1 \wedge \ldots \wedge I_n$ UNSAT
- Satisfied for: $L_1, \ldots, L_n \preceq$ Pudlák [RSS12]
- Not satisfied in general for: $L_i \succ$ Pudlák [GRS13]



Interpolation in PeRIPLO

- Labeled Interpolation Systems

Interpolation in PeRIPLO

- Labeled Interpolation Systems
- Single interpolants

Interpolation in PeRIPLO

- Labeled Interpolation Systems
- Single interpolants
- Collection of interpolants

Interpolation in PeRIPLO

- Labeled Interpolation Systems
- Single interpolants
- Collection of interpolants
  - (Generalized) Simultaneous Abstraction
  - Path Interpolation
  - State-transition Interpolation
  - Tree Interpolation

Interpolation in PeRIPLO

- Labeled Interpolation Systems
- Single interpolants
- Collection of interpolants
  - (Generalized) Simultaneous Abstraction
  - Path Interpolation
  - State-transition Interpolation
  - Tree Interpolation
- Independent verification of interpolants and requirements

References

S.F. Rollini, O. Sery and N. Sharygina
Leveraging Interpolant Strength in Model Checking.
CAV 2012.

A. Gurfinkel, S.F. Rollini, and N. Sharygina
Interpolation Properties and SAT-based Model Checking.
http://arxiv.org/abs/1212.4650 , ATVA 2013

Summary

- PeRIPLO framework
  - Input, output, usage
- Proof compression
- Interpolation in model checking
- http://verify.inf.unisi.ch/periplo.html