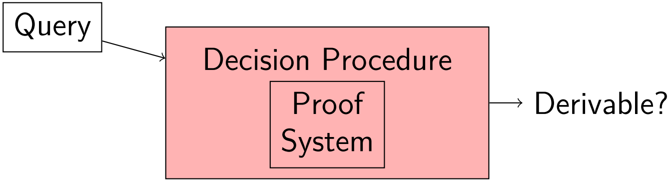
Gen2sat: a SAT-based Tool for Pure Analytic Gentzen Calculi

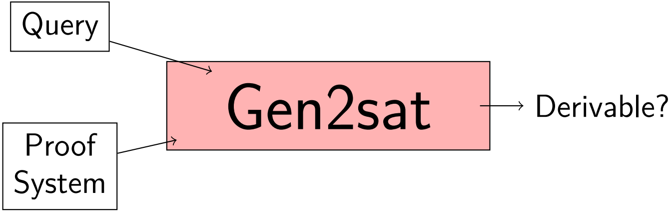
Yoni Zohar – Tel Aviv University

Joint work with Ori Lahav and Anna Zamansky

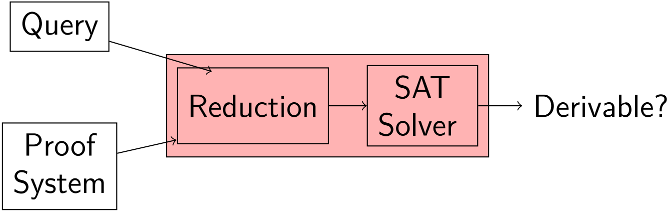
ASL North American Annual Meeting
2017

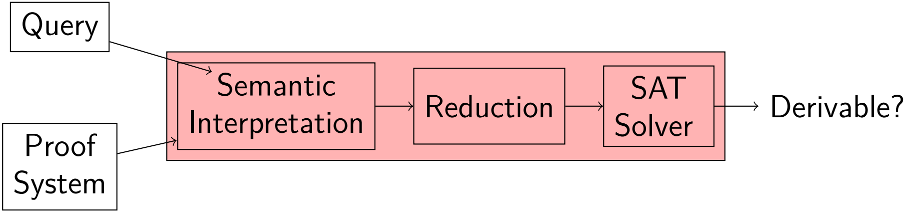
Gen2sat



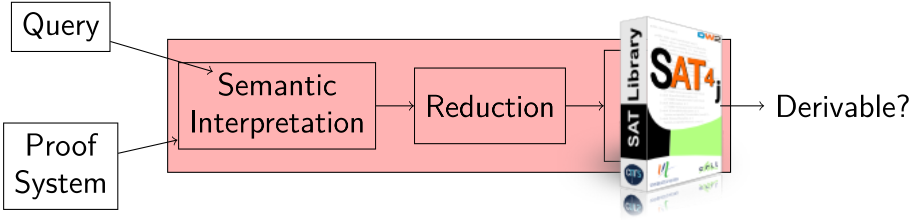

Query
Proof System
Gen2sat
Derivable?

Gen2sat

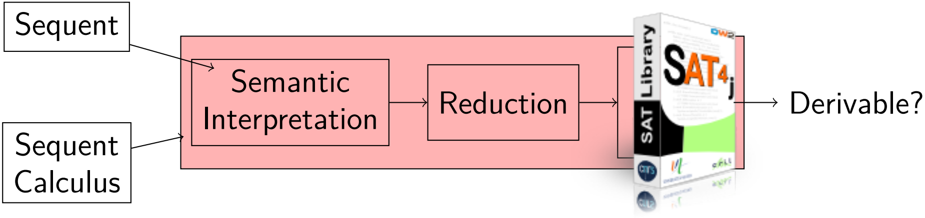



Query
Proof System
Semantic Interpretation
Reduction
SAT Solver
Derivable?

Gen2sat


Query
Proof System
Semantic Interpretation
Reduction
SAT Library
SAT4j
Derivable?

Gen2sat


Sequent
Sequent Calculus
Semantic Interpretation
Reduction
SAT Library
SAT4j
Derivable?

Analytic Pure Sequent Calculi

- *Sequents* have the form $\Gamma \Rightarrow \Delta$, where Γ and Δ are finite sets.

$$A_1, \ldots, A_n \Rightarrow B_1, \ldots, B_m \quad \leadsto \quad A_1 \wedge \ldots \wedge A_n \supset B_1 \vee \ldots \vee B_m$$

- *Pure sequent calculi* are propositional sequent calculi that include all usual structural rules, and a finite set of pure logical rules [Avron '91]:

$$\checkmark \ \frac{\Gamma, A \Rightarrow B, \Delta}{\Gamma \Rightarrow A \supset B, \Delta} \qquad X \ \frac{\Gamma, A \Rightarrow B}{\Gamma \Rightarrow A \supset B}$$

Analytic Pure Sequent Calculi

- *Sequents* have the form $\Gamma \Rightarrow \Delta$, where Γ and Δ are finite sets.

$$A_1, \ldots, A_n \Rightarrow B_1, \ldots, B_m \quad \rightsquigarrow \quad A_1 \wedge \ldots \wedge A_n \supset B_1 \vee \ldots \vee B_m$$

- *Pure sequent calculi* are propositional sequent calculi that include all usual structural rules, and a finite set of pure logical rules [Avron '91]:

$$\checkmark \ \frac{\Gamma, A \Rightarrow B, \Delta}{\Gamma \Rightarrow A \supset B, \Delta} \qquad X \ \frac{\Gamma, A \Rightarrow B}{\Gamma \Rightarrow A \supset B}$$

- A calculus is *analytic* if $\vdash \Gamma \Rightarrow \Delta$ implies that there is a derivation of $\Gamma \Rightarrow \Delta$ using only *sub* $(\Gamma \Rightarrow \Delta)$.

Analytic Pure Sequent Calculi

- *Sequents* have the form $\Gamma \Rightarrow \Delta$, where Γ and Δ are finite sets.

$$A_1, \ldots, A_n \Rightarrow B_1, \ldots, B_m \quad \leftrightsquigarrow \quad A_1 \wedge \ldots \wedge A_n \supset B_1 \vee \ldots \vee B_m$$

- *Pure sequent calculi* are propositional sequent calculi that include all usual structural rules, and a finite set of pure logical rules [Avron '91]:

$$\checkmark \; \frac{\Gamma, A \Rightarrow B, \Delta}{\Gamma \Rightarrow A \supset B, \Delta} \qquad \text{✗} \; \frac{\Gamma, A \Rightarrow B}{\Gamma \Rightarrow A \supset B}$$

- A calculus is *$\circledcirc$-analytic* if $\vdash \Gamma \Rightarrow \Delta$ implies that there is a derivation of $\Gamma \Rightarrow \Delta$ using only $sub^{\circledcirc}(\Gamma \Rightarrow \Delta)$.
- $sub^{\circledcirc}(A) = sub(A) \cup \{\circ B \mid \circ \in \circledcirc, B \in sub(A) \setminus \{A\}\}$.

Analytic Pure Sequent Calculi

- *Sequents* have the form $\Gamma \Rightarrow \Delta$, where Γ and Δ are finite sets.

$$A_1, \ldots, A_n \Rightarrow B_1, \ldots, B_m \quad \leadsto \quad A_1 \wedge \ldots \wedge A_n \supset B_1 \vee \ldots \vee B_m$$

- *Pure sequent calculi* are propositional sequent calculi that include all usual structural rules, and a finite set of pure logical rules [Avron '91]:

$$\checkmark \; \frac{\Gamma, A \Rightarrow B, \Delta}{\Gamma \Rightarrow A \supset B, \Delta} \qquad \text{X} \; \frac{\Gamma, A \Rightarrow B}{\Gamma \Rightarrow A \supset B}$$

- A calculus is *$\circledcirc$-analytic* if $\vdash \Gamma \Rightarrow \Delta$ implies that there is a derivation of $\Gamma \Rightarrow \Delta$ using only $sub^{\circledcirc}(\Gamma \Rightarrow \Delta)$.
- $sub^{\circledcirc}(A) = sub(A) \cup \{\circ B \mid \circ \in \circledcirc, B \in sub(A) \setminus \{A\}\}$.

- Many logics have analytic pure sequent calculi: classical logic, many-valued logics, paraconsistent logics, etc.

Examples

The Propositional Fragment of **LK** [Gentzen 1934]

Structural Rules:

$$(id)\ \frac{}{\Gamma, A \Rightarrow A, \Delta} \qquad (cut)\ \frac{\Gamma, A \Rightarrow \Delta \quad \Gamma \Rightarrow A, \Delta}{\Gamma \Rightarrow \Delta}$$

$$(W \Rightarrow)\ \frac{\Gamma \Rightarrow \Delta}{\Gamma, A \Rightarrow \Delta} \qquad (\Rightarrow W)\ \frac{\Gamma \Rightarrow \Delta}{\Gamma \Rightarrow A, \Delta}$$

Logical Rules:

$$(\neg \Rightarrow)\ \frac{\Gamma \Rightarrow A, \Delta}{\Gamma, \neg A \Rightarrow \Delta} \qquad (\Rightarrow \neg)\ \frac{\Gamma, A \Rightarrow \Delta}{\Gamma \Rightarrow \neg A, \Delta}$$

$$(\wedge \Rightarrow)\ \frac{\Gamma, A, B \Rightarrow \Delta}{\Gamma, A \wedge B \Rightarrow \Delta} \qquad (\Rightarrow \wedge)\ \frac{\Gamma \Rightarrow A, \Delta \quad \Gamma \Rightarrow B, \Delta}{\Gamma \Rightarrow A \wedge B, \Delta}$$

$$(\vee \Rightarrow)\ \frac{\Gamma, A \Rightarrow \Delta \quad \Gamma, B \Rightarrow \Delta}{\Gamma, A \vee B \Rightarrow \Delta} \qquad (\Rightarrow \vee)\ \frac{\Gamma \Rightarrow A, B, \Delta}{\Gamma \Rightarrow A \vee B, \Delta}$$

$$(\supset \Rightarrow)\ \frac{\Gamma \Rightarrow A, \Delta \quad \Gamma, B \Rightarrow \Delta}{\Gamma, A \supset B \Rightarrow \Delta} \qquad (\Rightarrow \supset)\ \frac{\Gamma, A \Rightarrow B, \Delta}{\Gamma \Rightarrow A \supset B, \Delta}$$

Examples

Primal Infon Logic [Gurevich,Neeman '09]

- An extremely efficient propositional logic developed in Microsoft.
- One of the main logical engines behind the authorization language DKAL.
- Provides a balance between expressivity and efficiency.

$$(\wedge \Rightarrow)\quad \frac{\Gamma, A, B \Rightarrow \Delta}{\Gamma, A \wedge B \Rightarrow \Delta} \qquad (\Rightarrow \wedge)\quad \frac{\Gamma \Rightarrow A, \Delta \quad \Gamma \Rightarrow B, \Delta}{\Gamma \Rightarrow A \wedge B, \Delta}$$

$$(\vee \Rightarrow)\quad \textit{none} \qquad (\Rightarrow \vee)\quad \frac{\Gamma \Rightarrow A, B, \Delta}{\Gamma \Rightarrow A \vee B, \Delta}$$

$$(\supset \Rightarrow)\quad \frac{\Gamma \Rightarrow A, \Delta \quad \Gamma, B \Rightarrow \Delta}{\Gamma, A \supset B \Rightarrow \Delta} \qquad (\Rightarrow \supset)\quad \frac{\Gamma \Rightarrow B, \Delta}{\Gamma \Rightarrow A \supset B, \Delta}$$

Examples

Łukasiewicz 3-valued Logic [Avron '03]

A $\{\neg\}$-analytic pure calculus for Ł$_3$ is obtained by augmenting the positive fragment of **LK** with some pure rules. For example:

$$(\neg \supset \Rightarrow) \quad \frac{\Gamma, A, \neg B \Rightarrow \Delta}{\Gamma, \neg(A \supset B) \Rightarrow \Delta}$$

$$(\Rightarrow \neg \supset) \quad \frac{\Gamma \Rightarrow A, \Delta \qquad \Gamma \Rightarrow \neg B, \Delta}{\Gamma \Rightarrow \neg(A \supset B), \Delta}$$

Next Operators

- Gen2sat supports analytic pure calculi

Next Operators

- Gen2sat supports $\circledcirc$-analytic pure calculi

Next Operators

- Gen2sat supports $\circledcirc$-analytic pure calculi augmented with impure rules of the form: $\dfrac{\Gamma \Rightarrow \Delta}{*\Gamma \Rightarrow *\Delta}$

Next Operators

- Gen2sat supports $\circledcirc$-analytic pure calculi augmented with impure rules of the form: $\dfrac{\Gamma \Rightarrow \Delta}{*\Gamma \Rightarrow *\Delta}$
- Unary modalities that are often employed in temporal logics.

Next Operators

- Gen2sat supports $\circledcirc$-analytic pure calculi augmented with impure rules of the form: $\dfrac{\Gamma \Rightarrow \Delta}{*\Gamma \Rightarrow *\Delta}$
- Unary modalities that are often employed in temporal logics.

$KF/KD!/KDalt1$

X-fragment of $LTL + \Box$ in (multi-)modal logic of functional models

$$(\neg \Rightarrow)\ \frac{\Gamma \Rightarrow A, \Delta}{\Gamma, \neg A \Rightarrow \Delta} \qquad (\Rightarrow \neg)\ \frac{\Gamma, A \Rightarrow \Delta}{\Gamma \Rightarrow \neg A, \Delta}$$

$$(\wedge \Rightarrow)\ \frac{\Gamma, A, B \Rightarrow \Delta}{\Gamma, A \wedge B \Rightarrow \Delta} \qquad (\Rightarrow \wedge)\ \frac{\Gamma \Rightarrow A, \Delta \quad \Gamma \Rightarrow B, \Delta}{\Gamma \Rightarrow A \wedge B, \Delta}$$

$$(\vee \Rightarrow)\ \frac{\Gamma, A \Rightarrow \Delta \quad \Gamma, B \Rightarrow \Delta}{\Gamma, A \vee B \Rightarrow \Delta} \qquad (\Rightarrow \vee)\ \frac{\Gamma \Rightarrow A, B, \Delta}{\Gamma \Rightarrow A \vee B, \Delta}$$

$$(\supset \Rightarrow)\ \frac{\Gamma \Rightarrow A, \Delta \quad \Gamma, B \Rightarrow \Delta}{\Gamma, A \supset B \Rightarrow \Delta} \qquad (\Rightarrow \supset)\ \frac{\Gamma, A \Rightarrow B, \Delta}{\Gamma \Rightarrow A \supset B, \Delta}$$

$$\frac{\Gamma \Rightarrow \Delta}{\Box\Gamma \Rightarrow \Box\Delta}$$

Next Operators

- Gen2sat supports $\circledcirc$-analytic pure calculi augmented with impure rules of the form: $\dfrac{\Gamma \Rightarrow \Delta}{*\Gamma \Rightarrow *\Delta}$
- Unary modalities that are often employed in temporal logics.

Primal Infon Logic with Quotations

- "*said*" operators are indispensable for applications.
- Each principle q has an operator "q *said*".

$(\wedge \Rightarrow)$ $\dfrac{\Gamma, A, B \Rightarrow \Delta}{\Gamma, A \wedge B \Rightarrow \Delta}$ $(\Rightarrow \wedge)$ $\dfrac{\Gamma \Rightarrow A, \Delta \quad \Gamma \Rightarrow B, \Delta}{\Gamma \Rightarrow A \wedge B, \Delta}$

$(\vee \Rightarrow)$ *none* $(\Rightarrow \vee)$ $\dfrac{\Gamma \Rightarrow A, B, \Delta}{\Gamma \Rightarrow A \vee B, \Delta}$

$(\supset \Rightarrow)$ $\dfrac{\Gamma \Rightarrow A, \Delta \quad \Gamma, B \Rightarrow \Delta}{\Gamma, A \supset B \Rightarrow \Delta}$ $(\Rightarrow \supset)$ $\dfrac{\Gamma \Rightarrow B, \Delta}{\Gamma \Rightarrow A \supset B, \Delta}$

$$\frac{\Gamma \Rightarrow \Delta}{q \ said \ \Gamma \Rightarrow q \ said \ \Delta} \text{ for every principal q}$$

Practically the same clauses as in [Bjorner et al.'11]

Semantics for Pure Calculi

- Pure calculi correspond to *two-valued valuations* [Béziau '01].
- By joining the semantic conditions of all rules in a calculus G, we obtain the set of *G-legal* valuations.

Example

$$\frac{A \Rightarrow}{\Rightarrow \neg A} \qquad \frac{A \Rightarrow}{\neg\neg A \Rightarrow}$$

Corresponding semantic conditions:

1. If $v(A) = \mathrm{F}$ then $v(\neg A) = \mathrm{T}$
2. If $v(A) = \mathrm{F}$ then $v(\neg\neg A) = \mathrm{F}$

This semantics is not truth-functional.

Soundness and Completeness

s is provable in G

$$\Longleftrightarrow$$

s is satisfied by every G-legal valuation

Semantics for Pure Calculi

- Pure calculi correspond to *two-valued valuations* [Béziau '01].
- By joining the semantic conditions of all rules in a calculus G, we obtain the set of *G-legal* valuations.

Example

$$\frac{A \Rightarrow}{\Rightarrow \neg A} \qquad \frac{A \Rightarrow}{\neg\neg A \Rightarrow}$$

Corresponding semantic conditions:

1. If $v(A) = \mathrm{F}$ then $v(\neg A) = \mathrm{T}$
2. If $v(A) = \mathrm{F}$ then $v(\neg\neg A) = \mathrm{F}$

This semantics is not truth-functional.

Soundness and Completeness

$$s \text{ is provable in } G \text{ using } \mathcal{F}\text{-formulas}$$
$$\Longleftrightarrow$$
$$s \text{ is satisfied by every } G\text{-legal valuation with domain } \mathcal{F}$$

Semantics for Pure Calculi

- Pure calculi correspond to *two-valued valuations* [Béziau '01].
- By joining the semantic conditions of all rules in a calculus G, we obtain the set of *G-legal* valuations.

Example

$$\frac{A \Rightarrow}{\Rightarrow \neg A} \qquad \frac{A \Rightarrow}{\neg\neg A \Rightarrow}$$

Corresponding semantic conditions:

1. If $v(A) = \mathrm{F}$ then $v(\neg A) = \mathrm{T}$
2. If $v(A) = \mathrm{F}$ then $v(\neg\neg A) = \mathrm{F}$

This semantics is not truth-functional.

Analytic Soundness and Completeness

s is provable in G using $sub^{\circledcirc}(s)$-formulas

$$\Longleftrightarrow$$

s is satisfied by every G-legal valuation with domain $sub^{\circledcirc}(s)$

Semantics for Pure Calculi

- Pure calculi correspond to *two-valued valuations* [Béziau '01].
- By joining the semantic conditions of all rules in a calculus G, we obtain the set of *G-legal* valuations.

Example

$$\frac{A \Rightarrow}{\Rightarrow \neg A} \qquad \frac{A \Rightarrow}{\neg\neg A \Rightarrow}$$

Corresponding semantic conditions:

1. If $v(A) = \mathrm{F}$ then $v(\neg A) = \mathrm{T}$
2. If $v(A) = \mathrm{F}$ then $v(\neg\neg A) = \mathrm{F}$

This semantics is not truth-functional.

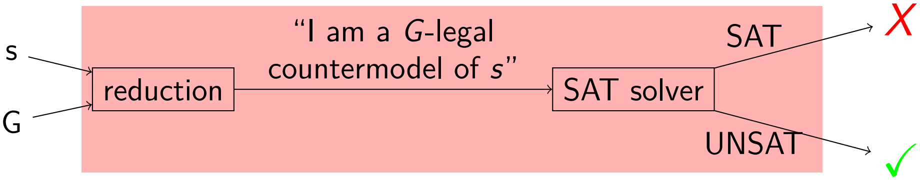
Analytic Soundness and Completeness

s is provable in G

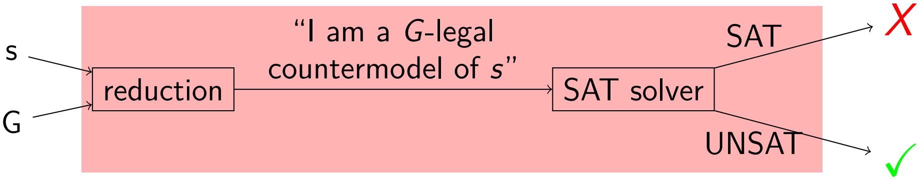
$$\Longleftrightarrow$$

s is satisfied by every G-legal valuation with domain $sub^{\circledcirc}(s)$

Reduction to SAT

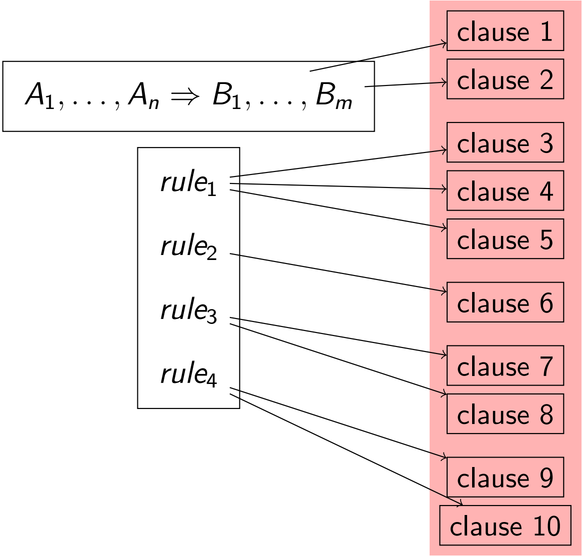


Reduction to SAT

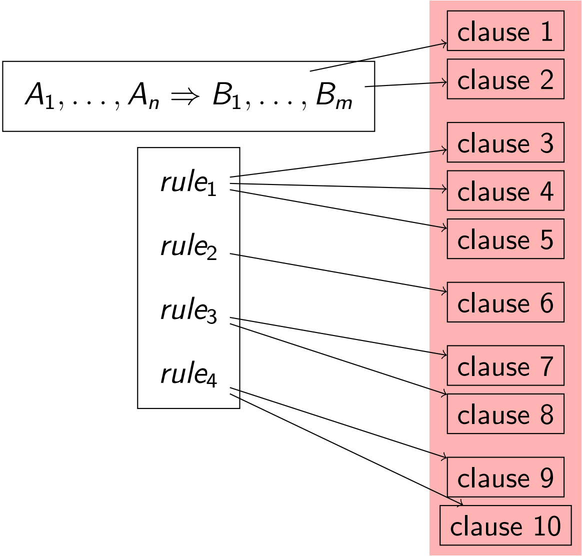


- In the presence of Next operators, we use Kripke models
- Correctness is trickier: Constructing a Kripke model from an assignment

Reduction


$A_1, \ldots, A_n \Rightarrow B_1, \ldots, B_m$
$rule_1$
$rule_2$
$rule_3$
$rule_4$
clause 1
clause 2
clause 3
clause 4
clause 5
clause 6
clause 7
clause 8
clause 9
clause 10

Reduction

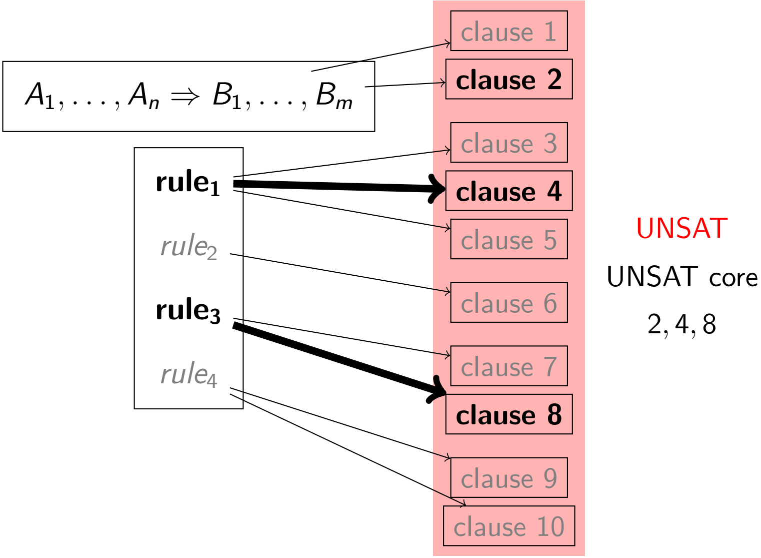


SAT

SAT assignment

$A_1 = false, A_2 = true, \ldots$

Reduction



$A_1, \ldots, A_n \Rightarrow B_1, \ldots, B_m$
rule$_1$
rule$_2$
rule$_3$
rule$_4$
clause 1
clause 2
clause 3
clause 4
clause 5
clause 6
clause 7
clause 8
clause 9
clause 10
UNSAT
UNSAT core
2, 4, 8

Command-line Interface

```
>cat dolev_yao.txt
```

```
connectives: P:2, E:2
rule: =>a; =>b / =>aPb
rule: a=> / aPb=>
rule: b=> / aPb=>
rule: =>a; =>b / =>aEb
rule: =>b; a=> / aEb=>
analyticity:
inputSequent: (((m1 P m2 ) E k) E k),k=>m1
```

```
>java -jar gen2sat.jar dolev_yao.txt
```

```
provable
There's a proof that uses only these rules:
[=>b; a=> / a E b=>, a=> / a P b=>]
```

Command-line Interface

```
>cat primal.txt
```

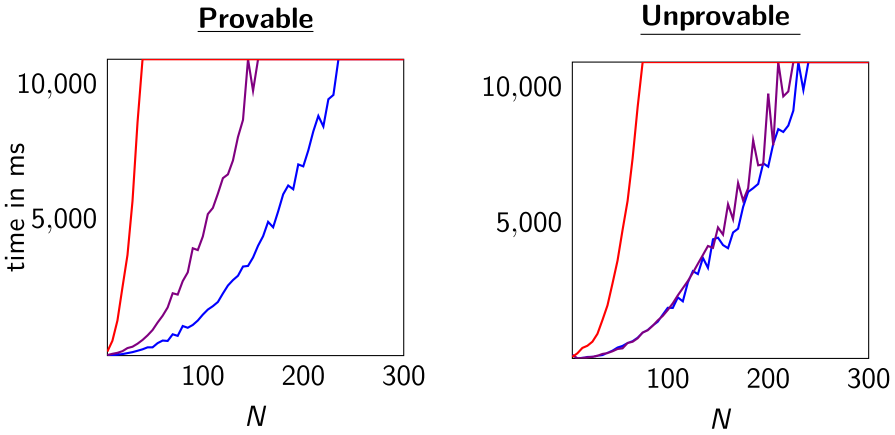
```
connectives: AND:2,IMPLIES:2
nextOperators: q1 said, q2 said, q3 said
rule: =>p1; =>p2 / =>p1 AND p2
rule: p1,p2=> / p1 AND p2=>
rule: =>p2 / =>p1 IMPLIES p2
rule: =>p1; p2=> / p1 IMPLIES p2=>
analyticity:
inputSequent: =>q1said (p IMPLIES p)
```

```
>java -jar gen2sat.jar primal.txt
```

```
unprovable
Countermodel:
q1said p=false, q1said(p IMPLIES p)=false
```

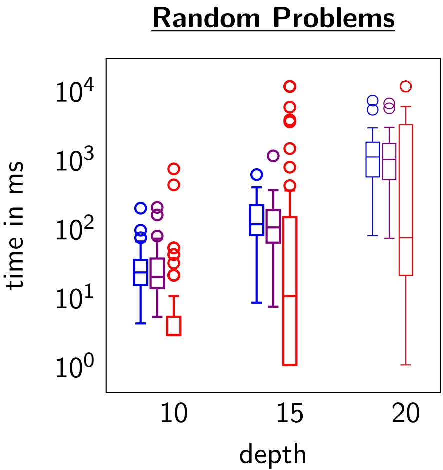
Evaluation

- input: $\{\neg\}$-analytic calculus for Łukasiewicz 3-valued logic [Avron'03]
- Gen2sat$_m$, Gen2sat, MetTeL
- Problems for Łukasiewicz infinite-valued logic [Rothenberg'07]



Evaluation

- input: $\{\neg\}$-analytic calculus for Łukasiewicz 3-valued logic [Avron'03]
- Gen2sat$_m$, Gen2sat, MetTeL



Educational Pilot

Background:

- Purpose: increasing students' engagement and motivation.
- Gen2sat is a natural candidate for such a task, as it leaves all heuristic considerations to the SAT-solver.
- The assignment was to present a minimal test plan with maximal coverage, as well as finding (intensionally planted) bugs.

Preliminary results:

- 13 students participated, all got 70%-85% coverage.
- Some used 0-ary and 3-ary connectives.
- The bugs were found by some of the students.
- Feedback:
  - "it helped me see the variety of different connectives and rules"
  - "for me thinking of the extreme cases was really illuminating"
  - "I wish all of the course assignments were more of this type"
  - ...

Conclusions

We have seen:

- A generic tool for deciding derivability in analytic pure (and some impure) sequent calculi
- The actual search is done by a SAT-solver
- Based on a semantic interpretation

Future work:

- Automatically detect analyticity (when possible)
- Integrate with a theorem prover
- Support more logics

Conclusions

We have seen:

- A generic tool for deciding derivability in analytic pure (and some impure) sequent calculi
- The actual search is done by a SAT-solver
- Based on a semantic interpretation

Future work:

- Automatically detect analyticity (when possible)
- Integrate with a theorem prover
- Support more logics

Thank you!