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

Diagram:

- Query
- Proof System
- Reduction
- SAT Solver
- Derivable?
Gen2sat: a SAT-based Tool for Pure Analytic Gentzen Calculi

Yoni Zohar
Gen2sat: a SAT-based Tool for Pure Analytic Gentzen Calculi
Gen2sat: a SAT-based Tool for Pure Analytic Gentzen Calculi
**Analytic Pure Sequent Calculi**

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

\[
A_1, \ldots, A_n \Rightarrow B_1, \ldots, B_m \iff A_1 \land \ldots \land A_n \supset B_1 \lor \ldots \lor B_m
\]

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

\[
\begin{array}{c}
\checkmark \quad \Gamma, A \Rightarrow B, \Delta \\
\hline
\Gamma \Rightarrow A \supset B, \Delta
\end{array}
\quad
\begin{array}{c}
\times \quad \Gamma, A \Rightarrow B \\
\hline
\Gamma \Rightarrow A \supset B
\end{array}
\]

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

Yoni Zohar

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

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

  
  $A_1, \ldots, A_n \Rightarrow B_1, \ldots, B_m \iff A_1 \land \ldots \land A_n \supset B_1 \lor \ldots \lor B_m$

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

  \[
  \begin{array}{c}
  \checkmark \\
  \Gamma, A \Rightarrow B, \Delta \\
  \hline
  \Gamma \Rightarrow A \supset B, \Delta \\
  \end{array} \quad \quad \begin{array}{c}
  \times \\
  \Gamma, A \Rightarrow B \\
  \hline
  \Gamma \Rightarrow A \supset B \\
  \end{array}
  \]

- 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 $\Gamma$ and $\Delta$ are finite sets.

$$A_1, \ldots, A_n \Rightarrow B_1, \ldots, B_m \iff A_1 \land \ldots \land A_n \supset B_1 \lor \ldots \lor B_m$$

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

\[
\begin{align*}
&\checkmark \quad \Gamma, A \Rightarrow B, \Delta \\
&\qquad \frac{\Gamma \Rightarrow A \supset B, \Delta}{\Gamma \Rightarrow A \supset B}
\end{align*}
\]

\[
\begin{align*}
&\times \quad \Gamma, A \Rightarrow B \\
&\frac{\Gamma \Rightarrow A \supset B}{\Gamma \Rightarrow A \supset B}
\end{align*}
\]

- A calculus is ⊗-analytic if $\vdash \Gamma \Rightarrow \Delta$ implies that there is a derivation of $\Gamma \Rightarrow \Delta$ using only $\text{sub}^\circ(\Gamma \Rightarrow \Delta)$.

- $\text{sub}^\circ(A) = \text{sub}(A) \cup \{\circ B \mid \circ \in \circ, B \in \text{sub}(A) \setminus \{A\}\}$. 

Yoni Zohar

Gen2sat: a SAT-based Tool for Pure Analytic Gentzen Calculi
Sequents have the form $\Gamma \Rightarrow \Delta$, where $\Gamma$ and $\Delta$ are finite sets.

$A_1, \ldots, A_n \Rightarrow B_1, \ldots, B_m \iff A_1 \land \ldots \land A_n \supset B_1 \lor \ldots \lor B_m$

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

\[
\begin{align*}
\checkmark & \quad \Gamma, A \Rightarrow B, \Delta \\
\hline
\Gamma \Rightarrow A \supset B, \Delta 
\end{align*}
\]

\[
\begin{align*}
\times & \quad \Gamma, A \Rightarrow B \\
\hline
\Gamma \Rightarrow A \supset B 
\end{align*}
\]

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

$\text{sub}^\otimes(A) = \text{sub}(A) \cup \{\circ B \mid \circ \in \otimes, B \in \text{sub}(A) \setminus \{A\}\}$.

Many logics have analytic pure sequent calculi: classical logic, many-valued logics, paraconsistent logics, etc.
### The Propositional Fragment of $\textbf{LK}$ [Gentzen 1934]

#### Structural Rules:

- **$(id)$**
  \[
  \frac{\Gamma, A \Rightarrow A, \Delta}{\Gamma, A \Rightarrow A, \Delta}
  \]

- **$(W \Rightarrow)$**
  \[
  \frac{\Gamma \Rightarrow \Delta}{\Gamma, A \Rightarrow \Delta}
  \]

- **$(cut)$**
  \[
  \frac{\Gamma, A \Rightarrow \Delta \quad \Gamma \Rightarrow A, \Delta}{\Gamma \Rightarrow \Delta}
  \]

- **$(\Rightarrow W)$**
  \[
  \frac{\Gamma \Rightarrow \Delta}{\Gamma \Rightarrow A, \Delta}
  \]

#### Logical Rules:

- **$(\neg \Rightarrow)$**
  \[
  \frac{\Gamma \Rightarrow A, \Delta}{\Gamma, \neg A \Rightarrow \Delta}
  \]

- **$(\wedge \Rightarrow)$**
  \[
  \frac{\Gamma, A, B \Rightarrow \Delta}{\Gamma, A \wedge B \Rightarrow \Delta}
  \]

- **$(\lor \Rightarrow)$**
  \[
  \frac{\Gamma, A \Rightarrow \Delta \quad \Gamma, B \Rightarrow \Delta}{\Gamma, A \lor B \Rightarrow \Delta}
  \]

- **$(\rightarrow \Rightarrow)$**
  \[
  \frac{\Gamma \Rightarrow A, \Delta \quad \Gamma \Rightarrow B, \Delta}{\Gamma \Rightarrow A \rightarrow B, \Delta}
  \]

- **$(\neg \rightarrow)$**
  \[
  \frac{\Gamma \Rightarrow A, \Delta}{\Gamma \Rightarrow \neg A, \Delta}
  \]

- **$(\rightarrow \neg)$**
  \[
  \frac{\Gamma \Rightarrow A, \Delta \quad \Gamma \Rightarrow B, \Delta}{\Gamma \Rightarrow A \wedge B, \Delta}
  \]

- **$(\Rightarrow \lor)$**
  \[
  \frac{\Gamma \Rightarrow A, \Delta \quad \Gamma \Rightarrow B, \Delta}{\Gamma \Rightarrow A \lor B, \Delta}
  \]

- **$(\Rightarrow \rightarrow)$**
  \[
  \frac{\Gamma \Rightarrow A, \Delta \quad \Gamma \Rightarrow B, \Delta}{\Gamma \Rightarrow A \rightarrow B, \Delta}
  \]
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.

\[ \Gamma, A, B \Rightarrow \Delta \]
\[ \Gamma, A \land B \Rightarrow \Delta \]

\[ \Gamma \Rightarrow A, \Delta \]
\[ \Gamma \Rightarrow B, \Delta \]
\[ \Gamma \Rightarrow A \land B, \Delta \]

\[ \Gamma \Rightarrow A, B, \Delta \]
\[ \Gamma \Rightarrow A \lor B, \Delta \]

\[ \Rightarrow \land \]

\[ \Rightarrow \lor \]

\[ \Rightarrow \Rightarrow \]

\[ \Rightarrow \supset \]

\[ \Rightarrow \subset \]

\[ \Gamma \Rightarrow B, \Delta \]
\[ \Gamma \Rightarrow A \supset B, \Delta \]

\[ \Gamma \Rightarrow A \subset B, \Delta \]
A \{\neg\}-analytic pure calculus for Ł₃ is obtained by augmenting the positive fragment of \textbf{LK} with some pure rules. For example:

\[(\neg \supset \Rightarrow)\]
\[\frac{\Gamma, A, \neg B \Rightarrow \Delta}{\Gamma, \neg(A \supset B) \Rightarrow \Delta}\]

\[(\Rightarrow \neg \supset)\]
\[\frac{\Gamma \Rightarrow A, \Delta \quad \Gamma \Rightarrow \neg B, \Delta}{\Gamma \Rightarrow \neg(A \supset B), \Delta}\]
Gen2sat supports analytic pure calculi.
Gen2sat supports ⊗-analytic pure calculi
Gen2sat supports ⊗-analytic pure calculi augmented with impure rules of the form:

\[
\frac{\Gamma \Rightarrow \Delta}{\ast \Gamma \Rightarrow \ast \Delta}
\]
Gen2sat supports ⊗-analytic pure calculi augmented with impure rules of the form:

\[
\frac{Γ \Rightarrow Δ}{*Γ \Rightarrow *Δ}
\]

Unary modalities that are often employed in temporal logics.
Gen2sat supports ⊗-analytic pure calculi augmented with impure rules of the form: \[
\frac{\Gamma \Rightarrow \Delta}{\ast \Gamma \Rightarrow \ast \Delta}
\]

Unary modalities that are often employed in temporal logics.

\[KF / KD! / KDalt1\]

X-fragment of LTL + □ in (multi-)modal logic of functional models

\[
\begin{align*}
(\neg \Rightarrow) & \quad \frac{\Gamma \Rightarrow A, \Delta}{\Gamma, \neg A \Rightarrow \Delta} & (\Rightarrow \neg) & \quad \frac{\Gamma \Rightarrow A \Rightarrow \Delta}{\Gamma \Rightarrow \neg A, \Delta} \\
(^\wedge \Rightarrow) & \quad \frac{\Gamma, A, B \Rightarrow \Delta}{\Gamma, A \wedge B \Rightarrow \Delta} & (\Rightarrow ^\wedge) & \quad \frac{\Gamma \Rightarrow A, \Delta \Gamma \Rightarrow B, \Delta}{\Gamma \Rightarrow A \wedge B, \Delta} \\
(^\lor \Rightarrow) & \quad \frac{\Gamma, A \Rightarrow \Delta \Gamma, B \Rightarrow \Delta}{\Gamma, A \lor B \Rightarrow \Delta} & (\Rightarrow ^\lor) & \quad \frac{\Gamma \Rightarrow A, B, \Delta}{\Gamma \Rightarrow A \lor B, \Delta} \\
(^\supset \Rightarrow) & \quad \frac{\Gamma \Rightarrow A, \Delta \Gamma, B \Rightarrow \Delta}{\Gamma, A \supset B \Rightarrow \Delta} & (\Rightarrow ^\supset) & \quad \frac{\Gamma, A \Rightarrow B, \Delta}{\Gamma \Rightarrow A \supset B, \Delta}
\end{align*}
\]

\[
\frac{\Gamma \Rightarrow \Delta}{\Box \Gamma \Rightarrow \Box \Delta}
\]
Gen2sat supports ⊗-analytic pure calculi augmented with impure rules of the form: \[\frac{\Gamma \Rightarrow \Delta}{\ast \Gamma \Rightarrow \ast \Delta}\]

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 "\(q\ said\)".

\[
\begin{align*}
\land & \Rightarrow \quad \frac{\Gamma, A, B \Rightarrow \Delta}{\Gamma, A \land B \Rightarrow \Delta} \\
\lor & \Rightarrow \quad \text{none} \\
\supset & \Rightarrow \quad \frac{\Gamma \Rightarrow A, \Delta \quad \Gamma \Rightarrow B, \Delta}{\Gamma \Rightarrow A \supset B, \Delta}
\end{align*}
\]

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**

$$
\begin{align*}
A \Rightarrow & \quad \Rightarrow \neg A \\
A \Rightarrow & \quad \neg \neg A \Rightarrow
\end{align*}
$$

Corresponding semantic conditions:

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

This semantics is *not* truth-functional.

**Soundness and Completeness**

$s$ is provable in $G$  
\[\iff\]
$s$ 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**

\[
\begin{align*}
A & \Rightarrow \\
\Rightarrow & \neg A \\

A & \Rightarrow \\
\neg \neg A & \Rightarrow
\end{align*}
\]

Corresponding semantic conditions:

1. If \( v(A) = F \) then \( v(\neg A) = T \)
2. If \( v(A) = F \) then \( v(\neg \neg A) = F \)

This semantics is *not* truth-functional.

**Soundness and Completeness**

\[ s \text{ is provable in } G \text{ using } \mathcal{F}\text{-formulas} \iff s \text{ is satisfied by every } G\text{-legal valuation with domain } \mathcal{F} \]
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**

\[
\begin{align*}
A & \Rightarrow \\
\Rightarrow & \neg A \\
\end{align*}
\]

\[
\begin{align*}
A & \Rightarrow \\
\neg \neg A & \Rightarrow
\end{align*}
\]

Corresponding semantic conditions:

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

This semantics is not truth-functional.

**Analytic Soundness and Completeness**

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

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

$$
\begin{align*}
A & \Rightarrow \neg A \\
A & \Rightarrow \neg \neg A
\end{align*}
$$

Corresponding semantic conditions:

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

This semantics is not truth-functional.

Analytic Soundness and Completeness

$s$ is provable in $G$ if and only if $s$ is satisfied by every $G$-legal valuation with domain $\text{sub}^\circ(s)$
Reduction to SAT

In the presence of Next operators, we use Kripke models.

Correctness is trickier: Constructing a Kripke model from an assignment.

Gen2sat: a SAT-based Tool for Pure Analytic Gentzen Calculi
In the presence of Next operators, we use Kripke models

Correctness is trickier: Constructing a Kripke model from an assignment
\[ A_1, \ldots, A_n \Rightarrow B_1, \ldots, B_m \]

**Rule Reduction**

- 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
$A_1, \ldots, A_n \Rightarrow B_1, \ldots, B_m$

$\text{rule}_1$

$\text{rule}_2$

$\text{rule}_3$

$\text{rule}_4$

clause 1

clause 2

clause 3

clause 4

clause 5

clause 6

clause 7

clause 8

clause 9

clause 10

SAT

SAT assignment

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

\[ A_1, \ldots, A_n \Rightarrow B_1, \ldots, B_m \]

\text{rule}_1 \quad \text{rule}_2 \quad \text{rule}_3 \quad \text{rule}_4

\begin{align*}
\text{clause 1} \\
\text{clause 2} \\
\text{clause 3} \\
\text{clause 4} \\
\text{clause 5} \\
\text{clause 6} \\
\text{clause 7} \\
\text{clause 8} \\
\text{clause 9} \\
\text{clause 10}
\end{align*}

\text{UNSAT core} \quad 2, 4, 8

Yoni Zohar

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