SAT-based Decision Procedure for Analytic Pure Sequent Calculi

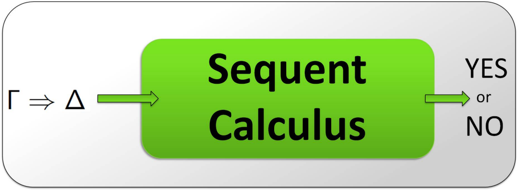
Ori Lahav Yoni Zohar

Tel Aviv University

IJCAR 2014

Sequent Calculi

- Sequent calculi are a prominent proof-theoretic framework.
- Suitable for a variety of logics:
  - Classical logic, intuitionistic logic
  - Modal logics, intermediate logics, bi-intuitionistic logic
  - Many-valued logics, fuzzy logics
  - Paraconsistent logics
  - Substructural logics, relevance logics
- Our goal: effectively reduce the derivability problem in a given propositional sequent calculus to SAT.



Pure Sequent Calculi

- We take *sequents* to be objects of the form $\Gamma \Rightarrow \Delta$, where Γ and Δ are finite sets of formulas.

- Intuition:

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

- Special instance 1: Δ has one element: $\Gamma \Rightarrow A$.
- Special instance 2: Γ is empty: $\Rightarrow A$

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

$$\frac{\Gamma, A \Rightarrow B, \Delta}{\Gamma \Rightarrow A \supset B, \Delta} \qquad \text{but not} \qquad \frac{\Gamma, A \Rightarrow B}{\Gamma \Rightarrow A \supset B}$$

Examples

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

Structural Rules:

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

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

Logical Rules:

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

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

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

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

Examples

Primal Infon Logic [Gurevich,Neeman '09]

- An extremely efficient propositional logic.
- One of the main logical engines behind DKAL (Distributed Knowledge Authorization Language).
- 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

da Costa's Paraconsistent Logic **C**$_1$ [Avron, Konikowska, Zamansky '12]

A pure calculus for **C**$_1$ is obtained by augmenting the positive fragment of **LK** with the following rules:

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

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

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

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

Examples

A System for Dolev-Yao Intruder Model [Comon-Lundh, Shmatikov '02]

- A basic deductive model of the intruder's capabilities.

$$\textit{Pairing}\quad \frac{\Gamma \vdash A \quad \Gamma \vdash B}{\Gamma \vdash \langle A, B\rangle} \qquad \textit{Encryption}\quad \frac{\Gamma \vdash A \quad \Gamma \vdash B}{\Gamma \vdash [A]_B}$$

$$\textit{Unpairing}\quad \frac{\Gamma \vdash \langle A, B\rangle}{\Gamma \vdash A} \qquad \textit{Unpairing}\quad \frac{\Gamma \vdash \langle A, B\rangle}{\Gamma \vdash B}$$

$$\textit{Decryption}\quad \frac{\Gamma \vdash [A]_B \quad \Gamma \vdash B}{\Gamma \vdash A} \qquad \textit{Axioms}\quad \frac{}{\Gamma \vdash A}\ \textit{if } A \in \Gamma$$

- Equivalent to the pure sequent calculus:

$$\frac{\Gamma \Rightarrow A, \Delta \quad \Gamma \Rightarrow B, \Delta}{\Gamma \Rightarrow \langle A, B\rangle, \Delta} \qquad \frac{\Gamma \Rightarrow A, \Delta \quad \Gamma \Rightarrow B, \Delta}{\Gamma \Rightarrow [A]_B\,, \Delta}$$

$$\frac{\Gamma \Rightarrow \langle A, B\rangle, \Delta}{\Gamma \Rightarrow A, \Delta} \qquad \frac{\Gamma \Rightarrow \langle A, B\rangle, \Delta}{\Gamma \Rightarrow B, \Delta} \qquad \frac{\Gamma \Rightarrow [A]_B\,, \Delta \quad \Gamma \Rightarrow B, \Delta}{\Gamma \Rightarrow A, \Delta}$$

Analyticity

Definition

A calculus is *analytic* if $\vdash \Gamma \Rightarrow \Delta$ implies that there is a derivation of $\Gamma \Rightarrow \Delta$ using only subformulas of $\Gamma \cup \Delta$.

- This notion may be based on more liberal definitions of subformulas (e.g., usual subformulas and their negations).
- If a pure calculus is analytic then it is decidable.
- All calculi presented so far (and many more) are analytic.

There is a *simple* reduction of derivability in analytic pure calculi to SAT.

Semantics for Pure Calculi

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

Example (Sequent Calculus for $\mathbf{C_1}$)

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

Corresponding semantic conditions:

1. If $v(A) = \mathrm{F}$ then $v(\neg A) = \mathrm{T}$
2. If $v(A) = \mathrm{F}$ then $v(\neg\neg A) = \mathrm{F}$
3. If $v(A) = \mathrm{T}$ and $v(\neg A) = \mathrm{T}$ then $v(\neg(A \wedge \neg A)) = \mathrm{F}$
4. If $v(\neg A) = \mathrm{F}$ and $v(\neg B) = \mathrm{F}$ then $v(\neg(A \wedge B)) = \mathrm{F}$

This semantics is non-deterministic.

Soundness and Completeness

Soundness and Completeness

The sequent $\Gamma \Rightarrow \Delta$ is provable in G iff every G-legal valuation is a model of $\Gamma \Rightarrow \Delta$.

Definition

G is semantically analytic if every G-legal **partial** valuation whose domain is closed under subformulas can be extended to a **full** G-legal valuation.

Example

Consider the rules $\frac{\Rightarrow A}{\neg A \Rightarrow}$ and $\frac{\Rightarrow A}{\Rightarrow \neg A}$.

The partial valuation $\lambda x \in \{p\} . \mathrm{T}$ cannot be extended.

Theorem

A calculus is analytic iff it is semantically analytic.

Soundness and Completeness

Soundness and Completeness

The sequent $\Gamma \Rightarrow \Delta$ is provable in G using only formulas of $\mathcal{F}$ iff every G-legal valuation whose domain is $\mathcal{F}$ is a model of $\Gamma \Rightarrow \Delta$.

Definition

G is semantically analytic if every G-legal **partial** valuation whose domain is closed under subformulas can be extended to a **full** G-legal valuation.

Example

Consider the rules $\dfrac{\Rightarrow A}{\neg A \Rightarrow}$ and $\dfrac{\Rightarrow A}{\Rightarrow \neg A}$.

The partial valuation $\lambda x \in \{p\} . \mathrm{T}$ cannot be extended.

Theorem

A calculus is analytic iff it is semantically analytic.

Reduction to SAT

- The semantic conditions are expressible in propositional classical logic.
- Given $\Gamma \Rightarrow \Delta$, we build a SAT-instance that says:
  - "I satisfy Γ, but not Δ"
  - "I am a G-legal valuation"

Reduction to SAT

Given an analytic pure calculus G and a sequent $\Gamma \Rightarrow \Delta$:

- Assign a variable x_A to every formula A.
- Generate a clause $\{x_A\}$ for every $A \in \Gamma$ and $\{\overline{x_A}\}$ for every $A \in \Delta$.
- Generate a set of clauses for each semantic condition of G applied on all formulas.

Theorem

$\Gamma \Rightarrow \Delta$ is provable in G iff this generated set of clauses is UNSAT.

Reduction to SAT

- The semantic conditions are expressible in propositional classical logic.
- Given $\Gamma \Rightarrow \Delta$, we build a SAT-instance that says:
  - "I satisfy Γ, but not Δ"
  - "I am a G-legal valuation"

Reduction to SAT

Given an analytic pure calculus G and a sequent $\Gamma \Rightarrow \Delta$:

- Assign a variable x_A to every formula A.
- Generate a clause $\{x_A\}$ for every $A \in \Gamma$ and $\{\overline{x_A}\}$ for every $A \in \Delta$.
- Generate a set of clauses for each semantic condition of G applied on subformulas of $\Gamma \cup \Delta$.

Theorem

$\Gamma \Rightarrow \Delta$ is provable in G iff this generated set of clauses is UNSAT.

The Case of Propositional Primal Logic

Example (Semantics)

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

Semantic Reading:

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

Example (Reduction to SAT)

$\Gamma \Rightarrow \Delta$ is provable iff the following set of clauses is UNSAT:

- Singleton clauses $\{x_A\}$ for every $A \in \Gamma$ and $\{\overline{x_A}\}$ for every $A \in \Delta$.
- Two clauses for every formula $A \supset B$ occurring in $\Gamma \Rightarrow \Delta$:

$$\{\overline{x_A}, x_B, \overline{x_{A \supset B}}\} \qquad \{\overline{x_B}, x_{A \supset B}\}$$

Next Operators

- Unary modalities: $*_1, *_2, \dots$
- Often employed in temporal logics.
- $\Box$ and $\Diamond$ in the modal logic (**KD**!) of functional Kripke models.

$$(*i) \qquad \frac{\Gamma \Rightarrow \Delta}{*\Gamma \Rightarrow *\Delta}$$

Example

In primal infon logic, **Next** operators serve as quotations, that are indispensable for access control logics.

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

Theorem

The addition of $(*i)$ preserves analyticity.

Semantics for Pure Calculi with **Next** Operators

- Pure calculi with **Next** operators are characterized by two-valued functional Kripke models.

Definition (Functional Kripke Model)

A functional Kripke model is a triple $\langle W, \mathcal{R}, \mathcal{V} \rangle$:

- W is a set of states (possible worlds).
- $\mathcal{R}$ assigns a function $R_* : W \to W$ to every **Next** operator $*$.
- $\mathcal{V}$ assigns a valuation $v_w : Frm_{\mathcal{L}} \to \{\mathrm{F}, \mathrm{T}\}$ to every $w \in W$, such that:

$$v_w(*A) = v_{R_*(w)}(A).$$

Soundness and Completeness

$\Gamma \Rightarrow \Delta$ is provable in G iff every G-legal Kripke model is a model of $\Gamma \Rightarrow \Delta$.

The stronger version of the theorem works as well.

Reduction to SAT

Instead of relying on *subformulas*, this reduction uses *local formulas*.

Definition (Local Formulas)

$$\frac{}{\vec{*}A_i \leq \vec{*}(\diamond(A_1, \ldots, A_n))} \qquad \frac{}{A \leq A} \qquad \frac{A \leq B \qquad B \leq C}{A \leq C}$$

Correctness is now more challenging:

We prove that a Kripke counter-model can be constructed from a satisfying assignment (using the fact that the calculus is analytic).

Corollary

Analytic pure calculi with **Next** *operators can be decided by a SAT solver.*

Time Complexity

- The reduction is poly-time computable.
- A calculus is *k-closed* if each of its rules contains k formulas such that all other formulas in the rule are subformulas of them.
- The reduction for a k-closed calculus requires $O(n^k)$ time.
- All calculi presented above are 1-closed $\Longrightarrow$ linear time reduction.

Horn Calculi

Definition (Horn Pure Calculi)

In each rule: $\begin{array}{c}\#\text{ of premises with non-empty left side}\\ +\\ \#\text{ of formulas in the right side of the conclusion}\end{array} \leq 1$

The SAT instances associated with Horn calculi consist of Horn clauses.

Corollary

Every analytic 1*-closed Horn pure calculus (with* **Next** *operators) can be decided in linear time using a HORNSAT solver.*

Examples of Horn Calculi

- Dolev-Yao Intruder Deduction.
- Primal infon logic with quotations.

Extensions of Primal Logic

- It is possible to extend the calculus for primal logic (with quotations) with additional axiom schemes, e.g.:
  - $\Rightarrow A \supset A$
  - $\Rightarrow B \supset (A \supset B)$
  - $\Rightarrow (A \wedge B) \supset A$
  - $\Rightarrow (A \wedge B) \supset B$
  - $A \vee A \Rightarrow A$
  - $A \vee (A \wedge B) \Rightarrow A$
  - $(A \wedge B) \vee A \Rightarrow A$
- Bottom can be also added, and simple interactions between $\perp$, $\supset$ and $\vee$ can be recovered:
  - $\perp \Rightarrow$
  - $\Rightarrow \perp \supset A$
  - $\perp \vee A \Rightarrow A$
  - $A \vee \perp \Rightarrow A$
- This will bring us a bit closer to a more intuitive multimodal logic.

Conclusions

We have seen:

- Uniform reduction of derivability in analytic pure calculi to SAT.
- Extension to some non-pure calculi (with **Next** operators).
- Linear time decision procedure for Horn calculi.

Future work:

- Are there other useful logics that can be reduced to polynomial SAT fragments (e.g. dual-Horn, 2-SAT)?
- Extend the reduction to other modalities.

Conclusions

We have seen:

- Uniform reduction of derivability in analytic pure calculi to SAT.
- Extension to some non-pure calculi (with **Next** operators).
- Linear time decision procedure for Horn calculi.

Future work:

- Are there other useful logics that can be reduced to polynomial SAT fragments (e.g. dual-Horn, 2-SAT)?
- Extend the reduction to other modalities.

Thank you!