SMT Solving Modulo Tableau and Rewriting Theories

Guillaume Bury[1] Simon Cruanes[2] David Delahaye[3]

12 July, 2018

(1) Inria/LSV/ENS Paris-Saclay, Cachan, France

(2) Aesthetic Integration, Austin (Texas), USA

(3) LIRMM/Université de Montpellier, Montpellier, France

Introduction

- Integrate Tableau theory as a regular SMT theory for completeness
- Integrate rewriting into SMT for better performances
- Unification modulo rewriting

SMT, SAT and Theory

- All this work is done in the context of an SMT solver
- SMT = SAT + Theory
- SAT = unit propagation + conflict detection/analysis + backtracking
- Clauses can be added to the solver during solving

SMT modulo Tableau

Tableau method

Tableau proof search:

- sequent calculus
- $\Gamma \vdash \bot$
- contraction at each step

$$\frac{A \wedge B}{A, B}$$

$$\frac{A \vee B}{A \qquad B}$$

Boxed formulas

- Boxed formulas: $\lfloor \forall x : \mathbb{N}. x > 0 \rightarrow x + 1 > 0 \rfloor$
- Negations escape boxes: $\lfloor \neg P \rfloor = \neg \lfloor P \rfloor$, $\lfloor \neg\neg P \rfloor = \lfloor P \rfloor$
- Boxed formulas are literals
- Clauses are disjunctions of (negated) boxed formulas:

$$C \equiv \neg \lfloor P \vee Q \rfloor \vee \lfloor P \rfloor \vee \lfloor Q \rfloor$$

- Similar to what is done in Satallax

Tableau theory

- Encode propositional logic into clausal calculus
- Realizes a lazy CNF conversion
- Each time a literal (i.e. a boxed formula) is decided or propagated, add clauses that “unfold” its top logical connective

Tableau theory - example

Let's prove that $F = (A \vee C) \rightarrow (A \vee B \vee C)$

Clauses

- $C_0 = \neg \lfloor A \vee C \rightarrow A \vee B \vee C \rfloor$

Trail

- $\lfloor A \vee C \rightarrow A \vee B \vee C \rfloor \mapsto_0 \bot$

Tableau theory - example

Let's prove that $F = (A \vee C) \rightarrow (A \vee B \vee C)$

Clauses

- $C_0 = \neg\lfloor A \vee C \rightarrow A \vee B \vee C \rfloor$
- $C_1 = \lfloor F \rfloor \vee \lfloor A \vee C \rfloor$
- $C_2 = \lfloor F \rfloor \vee \neg\lfloor A \vee B \vee C \rfloor$

Trail

- $\lfloor A \vee C \rightarrow A \vee B \vee C \rfloor \mapsto_0 \bot$

Tableau theory - example

Let's prove that $F = (A \lor C) \rightarrow (A \lor B \lor C)$

Clauses

- $C_0 = \neg \lfloor A \lor C \rightarrow A \lor B \lor C \rfloor$
- $C_1 = \lfloor F \rfloor \lor \lfloor A \lor C \rfloor$
- $C_2 = \lfloor F \rfloor \lor \neg \lfloor A \lor B \lor C \rfloor$

Trail

- $\lfloor A \lor C \rightarrow A \lor B \lor C \rfloor \mapsto_0 \bot$
- $\lfloor A \lor C \rfloor \mapsto_0 \top$

Tableau theory - example

Let's prove that $F = (A \vee C) \rightarrow (A \vee B \vee C)$

Clauses

- $C_0 = \neg \lfloor A \vee C \rightarrow A \vee B \vee C \rfloor$
- $C_1 = \lfloor F \rfloor \vee \lfloor A \vee C \rfloor$
- $C_2 = \lfloor F \rfloor \vee \neg \lfloor A \vee B \vee C \rfloor$

Trail

- $\lfloor A \vee C \rightarrow A \vee B \vee C \rfloor \mapsto_0 \bot$
- $\lfloor A \vee C \rfloor \mapsto_0 \top$
- $\lfloor A \vee B \vee C \rfloor \mapsto_0 \bot$

Tableau theory - example

Let's prove that $F = (A \lor C) \to (A \lor B \lor C)$

Clauses

- $C_0 = \neg\lfloor A \lor C \to A \lor B \lor C \rfloor$
- $C_1 = \lfloor F \rfloor \lor \lfloor A \lor C \rfloor$
- $C_2 = \lfloor F \rfloor \lor \neg\lfloor A \lor B \lor C \rfloor$
- $C_3 = \neg\lfloor A \lor C \rfloor \lor \lfloor A \rfloor \lor \lfloor C \rfloor$

Trail

- $\lfloor A \lor C \to A \lor B \lor C \rfloor \mapsto_0 \bot$
- $\lfloor A \lor C \rfloor \mapsto_0 \top$
- $\lfloor A \lor B \lor C \rfloor \mapsto_0 \bot$

Tableau theory - example

Let's prove that $F = (A \vee C) \to (A \vee B \vee C)$

Clauses

- $C_0 = \neg\lfloor A \vee C \to A \vee B \vee C \rfloor$
- $C_1 = \lfloor F \rfloor \vee \lfloor A \vee C \rfloor$
- $C_2 = \lfloor F \rfloor \vee \neg\lfloor A \vee B \vee C \rfloor$
- $C_3 = \neg\lfloor A \vee C \rfloor \vee \lfloor A \rfloor \vee \lfloor C \rfloor$
- $C_4 = \lfloor A \vee B \vee C \rfloor \vee \neg\lfloor A \rfloor$
- $C_5 = \lfloor A \vee B \vee C \rfloor \vee \neg\lfloor B \rfloor$
- $C_6 = \lfloor A \vee B \vee C \rfloor \vee \neg\lfloor C \rfloor$

Trail

- $\lfloor A \vee C \to A \vee B \vee C \rfloor \mapsto_0 \bot$
- $\lfloor A \vee C \rfloor \mapsto_0 \top$
- $\lfloor A \vee B \vee C \rfloor \mapsto_0 \bot$

Tableau theory - example

Let's prove that $F = (A \vee C) \rightarrow (A \vee B \vee C)$

Clauses

- $C_0 = \neg\lfloor A \vee C \rightarrow A \vee B \vee C \rfloor$
- $C_1 = \lfloor F \rfloor \vee \lfloor A \vee C \rfloor$
- $C_2 = \lfloor F \rfloor \vee \neg\lfloor A \vee B \vee C \rfloor$
- $C_3 = \neg\lfloor A \vee C \rfloor \vee \lfloor A \rfloor \vee \lfloor C \rfloor$
- $C_4 = \lfloor A \vee B \vee C \rfloor \vee \neg\lfloor A \rfloor$
- $C_5 = \lfloor A \vee B \vee C \rfloor \vee \neg\lfloor B \rfloor$
- $C_6 = \lfloor A \vee B \vee C \rfloor \vee \neg\lfloor C \rfloor$

Trail

- $\lfloor A \vee C \rightarrow A \vee B \vee C \rfloor \mapsto_0 \bot$
- $\lfloor A \vee C \rfloor \mapsto_0 \top$
- $\lfloor A \vee B \vee C \rfloor \mapsto_0 \bot$
- $\lfloor A \rfloor \mapsto_0 \bot$

Tableau theory - example

Let's prove that $F = (A \vee C) \rightarrow (A \vee B \vee C)$

Clauses

- $C_0 = \neg\lfloor A \vee C \rightarrow A \vee B \vee C \rfloor$
- $C_1 = \lfloor F \rfloor \vee \lfloor A \vee C \rfloor$
- $C_2 = \lfloor F \rfloor \vee \neg\lfloor A \vee B \vee C \rfloor$
- $C_3 = \neg\lfloor A \vee C \rfloor \vee \lfloor A \rfloor \vee \lfloor C \rfloor$
- $C_4 = \lfloor A \vee B \vee C \rfloor \vee \neg\lfloor A \rfloor$
- $C_5 = \lfloor A \vee B \vee C \rfloor \vee \neg\lfloor B \rfloor$
- $C_6 = \lfloor A \vee B \vee C \rfloor \vee \neg\lfloor C \rfloor$

Trail

- $\lfloor A \vee C \rightarrow A \vee B \vee C \rfloor \mapsto_0 \bot$
- $\lfloor A \vee C \rfloor \mapsto_0 \top$
- $\lfloor A \vee B \vee C \rfloor \mapsto_0 \bot$
- $\lfloor A \rfloor \mapsto_0 \bot$
- $\lfloor B \rfloor \mapsto_0 \bot$

Tableau theory - example

Let's prove that $F = (A \vee C) \rightarrow (A \vee B \vee C)$

Clauses

- $C_0 = \neg\lfloor A \vee C \rightarrow A \vee B \vee C \rfloor$
- $C_1 = \lfloor F \rfloor \vee \lfloor A \vee C \rfloor$
- $C_2 = \lfloor F \rfloor \vee \neg\lfloor A \vee B \vee C \rfloor$
- $C_3 = \neg\lfloor A \vee C \rfloor \vee \lfloor A \rfloor \vee \lfloor C \rfloor$
- $C_4 = \lfloor A \vee B \vee C \rfloor \vee \neg\lfloor A \rfloor$
- $C_5 = \lfloor A \vee B \vee C \rfloor \vee \neg\lfloor B \rfloor$
- $C_6 = \lfloor A \vee B \vee C \rfloor \vee \neg\lfloor C \rfloor$

Trail

- $\lfloor A \vee C \rightarrow A \vee B \vee C \rfloor \mapsto_0 \bot$
- $\lfloor A \vee C \rfloor \mapsto_0 \top$
- $\lfloor A \vee B \vee C \rfloor \mapsto_0 \bot$
- $\lfloor A \rfloor \mapsto_0 \bot$
- $\lfloor B \rfloor \mapsto_0 \bot$
- $\lfloor C \rfloor \mapsto_0 \bot$

Tableau theory - example

Let's prove that $F = (A \lor C) \to (A \lor B \lor C)$

Clauses

- $C_0 = \neg\lfloor A \lor C \to A \lor B \lor C \rfloor$
- $C_1 = \lfloor F \rfloor \lor \lfloor A \lor C \rfloor$
- $C_2 = \lfloor F \rfloor \lor \neg\lfloor A \lor B \lor C \rfloor$
- $C_3 = \neg\lfloor A \lor C \rfloor \lor \lfloor A \rfloor \lor \lfloor C \rfloor$
- $C_4 = \lfloor A \lor B \lor C \rfloor \lor \neg\lfloor A \rfloor$
- $C_5 = \lfloor A \lor B \lor C \rfloor \lor \neg\lfloor B \rfloor$
- $C_6 = \lfloor A \lor B \lor C \rfloor \lor \neg\lfloor C \rfloor$

Trail

- $\lfloor A \lor C \to A \lor B \lor C \rfloor \mapsto_0 \bot$
- $\lfloor A \lor C \rfloor \mapsto_0 \top$
- $\lfloor A \lor B \lor C \rfloor \mapsto_0 \bot$
- $\lfloor A \rfloor \mapsto_0 \bot$
- $\lfloor B \rfloor \mapsto_0 \bot$
- $\lfloor C \rfloor \mapsto_0 \bot$
- Conflict in C_3 !

Quantified formulas and meta-variables

- Generate epsilon-terms for existentials:

$$C = \neg\lfloor \exists x.P(x) \rfloor \vee \lfloor P(\epsilon(x).P(x)) \rfloor$$

- Generate meta-variables for universals:

$$C = \neg\lfloor \forall x.P(x) \rfloor \vee \lfloor P(X_{\forall x.P(x)}) \rfloor$$

- When a model is found unify formulas that are true with those that are false, to get a substitution on meta-variables
- Instantiate a substitution $\{X_{\forall x.P(x)} \mapsto t\}$:

$$C = \neg\lfloor \forall x.P(x) \rfloor \vee \lfloor P(t) \rfloor$$

Quantified formulas - example

Drinker's paradox:

- $D = \exists x.\ p(x) \rightarrow (\forall y.\ p(y))$

Clauses	Trail
• $C_0 = \neg \lfloor D \rfloor$	

Quantified formulas - example

Drinker's paradox:

- $D = \exists x.\ p(x) \rightarrow (\forall y.\ p(y))$

Clauses

- $C_0 = \neg \lfloor D \rfloor$

Trail

- $\lfloor D \rfloor \mapsto_0 \bot$

Quantified formulas - example

Drinker's paradox:

- $D = \exists x.\ p(x) \rightarrow (\forall y.\ p(y))$
- $E = p(X) \rightarrow \forall y.\ p(y)$

Clauses

- $C_0 = \neg \lfloor D \rfloor$
- $C_1 = \lfloor D \rfloor \vee \lfloor \neg E \rfloor$

Trail

- $\lfloor D \rfloor \mapsto_0 \bot$

Quantified formulas - example

Drinker's paradox:

- $D = \exists x.\ p(x) \rightarrow (\forall y.\ p(y))$
- $E = p(X) \rightarrow \forall y.\ p(y)$

Clauses

- $C_0 = \neg \lfloor D \rfloor$
- $C_1 = \lfloor D \rfloor \vee \lfloor \neg E \rfloor$
- $C_2 = \lfloor E \rfloor \vee \lfloor p(X) \rfloor$
- $C_3 = \lfloor E \rfloor \vee \neg \lfloor \forall y.\ p(y) \rfloor$

Trail

- $\lfloor D \rfloor \mapsto_0 \bot$
- $\lfloor E \rfloor \mapsto_0 \bot$

Quantified formulas - example

Drinker's paradox:

- $D = \exists x.\ p(x) \rightarrow (\forall y.\ p(y))$
- $E = p(X) \rightarrow \forall y.\ p(y)$

Clauses

- $C_0 = \neg \lfloor D \rfloor$
- $C_1 = \lfloor D \rfloor \vee \lfloor \neg E \rfloor$
- $C_2 = \lfloor E \rfloor \vee \lfloor p(X) \rfloor$
- $C_3 = \lfloor E \rfloor \vee \neg \lfloor \forall y.\ p(y) \rfloor$

Trail

- $\lfloor D \rfloor \mapsto_0 \bot$
- $\lfloor E \rfloor \mapsto_0 \bot$
- $\lfloor p(X) \rfloor \mapsto_0 \top$

Quantified formulas - example

Drinker's paradox:

- $D = \exists x.\ p(x) \rightarrow (\forall y.\ p(y))$
- $E = p(X) \rightarrow \forall y.\ p(y)$

Clauses

- $C_0 = \neg\lfloor D \rfloor$
- $C_1 = \lfloor D \rfloor \vee \lfloor \neg E \rfloor$
- $C_2 = \lfloor E \rfloor \vee \lfloor p(X) \rfloor$
- $C_3 = \lfloor E \rfloor \vee \neg\lfloor \forall y.\ p(y) \rfloor$

Trail

- $\lfloor D \rfloor \mapsto_0 \bot$
- $\lfloor E \rfloor \mapsto_0 \bot$
- $\lfloor p(X) \rfloor \mapsto_0 \top$
- $\lfloor \forall y.\ p(y) \rfloor \mapsto_0 \bot$

Quantified formulas - example

Drinker's paradox:

- $D = \exists x.\ p(x) \to (\forall y.\ p(y))$
- $E = p(X) \to \forall y.\ p(y)$

Clauses

- $C_0 = \neg\lfloor D \rfloor$
- $C_1 = \lfloor D \rfloor \vee \lfloor \neg E \rfloor$
- $C_2 = \lfloor E \rfloor \vee \lfloor p(X) \rfloor$
- $C_3 = \lfloor E \rfloor \vee \neg\lfloor \forall y.\ p(y) \rfloor$
- $C_4 = \lfloor \forall y.\ p(y) \rfloor \vee \neg\lfloor p(\tau) \rfloor$

Trail

- $\lfloor D \rfloor \mapsto_0 \bot$
- $\lfloor E \rfloor \mapsto_0 \bot$
- $\lfloor p(X) \rfloor \mapsto_0 \top$
- $\lfloor \forall y.\ p(y) \rfloor \mapsto_0 \bot$

Quantified formulas - example

Drinker's paradox:

- $D = \exists x.\ p(x) \rightarrow (\forall y.\ p(y))$
- $E = p(X) \rightarrow \forall y.\ p(y)$

Clauses

- $C_0 = \neg\lfloor D \rfloor$
- $C_1 = \lfloor D \rfloor \vee \lfloor \neg E \rfloor$
- $C_2 = \lfloor E \rfloor \vee \lfloor p(X) \rfloor$
- $C_3 = \lfloor E \rfloor \vee \neg\lfloor \forall y.\ p(y) \rfloor$
- $C_4 = \lfloor \forall y.\ p(y) \rfloor \vee \neg\lfloor p(\tau) \rfloor$

Trail

- $\lfloor D \rfloor \mapsto_0 \bot$
- $\lfloor E \rfloor \mapsto_0 \bot$
- $\lfloor p(X) \rfloor \mapsto_0 \top$
- $\lfloor \forall y.\ p(y) \rfloor \mapsto_0 \bot$
- $\lfloor p(\tau) \rfloor \mapsto_0 \bot$

Quantified formulas - example

Drinker's paradox:

- $D = \exists x.\ p(x) \rightarrow (\forall y.\ p(y))$
- $E = p(X) \rightarrow \forall y.\ p(y)$
- Unify $p(X)$ and $p(\tau)$

Clauses

- $C_0 = \neg\lfloor D \rfloor$
- $C_1 = \lfloor D \rfloor \vee \lfloor \neg E \rfloor$
- $C_2 = \lfloor E \rfloor \vee \lfloor p(X) \rfloor$
- $C_3 = \lfloor E \rfloor \vee \neg\lfloor \forall y.\ p(y) \rfloor$
- $C_4 = \lfloor \forall y.\ p(y) \rfloor \vee \neg\lfloor p(\tau) \rfloor$

Trail

- $\lfloor D \rfloor \mapsto_0 \bot$
- $\lfloor E \rfloor \mapsto_0 \bot$
- $\lfloor p(X) \rfloor \mapsto_0 \top$
- $\lfloor \forall y.\ p(y) \rfloor \mapsto_0 \bot$
- $\lfloor p(\tau) \rfloor \mapsto_0 \bot$

Quantified formulas - example

Drinker's paradox:

- $D = \exists x.\ p(x) \rightarrow (\forall y.\ p(y))$
- $E = p(X) \rightarrow \forall y.\ p(y)$
- Unify $p(X)$ and $p(\tau)$: $\{X \mapsto \tau\}$

Clauses

- $C_0 = \neg \lfloor D \rfloor$
- $C_1 = \lfloor D \rfloor \vee \lfloor \neg E \rfloor$
- $C_2 = \lfloor E \rfloor \vee \lfloor p(X) \rfloor$
- $C_3 = \lfloor E \rfloor \vee \neg \lfloor \forall y.\ p(y) \rfloor$
- $C_4 = \lfloor \forall y.\ p(y) \rfloor \vee \neg \lfloor p(\tau) \rfloor$

Trail

- $\lfloor D \rfloor \mapsto_0 \bot$
- $\lfloor E \rfloor \mapsto_0 \bot$
- $\lfloor p(X) \rfloor \mapsto_0 \top$
- $\lfloor \forall y.\ p(y) \rfloor \mapsto_0 \bot$
- $\lfloor p(\tau) \rfloor \mapsto_0 \bot$

Quantified formulas - example

- $D = \exists x.\ p(x) \rightarrow (\forall y.\ p(y))$
- $E = p(X) \rightarrow \forall y.\ p(y)$
- $E' = p(\tau) \rightarrow \forall y.\ p(y)$

Clauses

- $C_0 = \neg \lfloor D \rfloor$
- $C_1 = \lfloor D \rfloor \vee \neg \lfloor E \rfloor$
- $C_2 = \lfloor E \rfloor \vee \lfloor p(X) \rfloor$
- $C_3 = \lfloor E \rfloor \vee \neg \lfloor \forall y.\ p(y) \rfloor$
- $C_4 = \lfloor \forall y.\ p(y) \rfloor \vee \neg \lfloor p(\tau) \rfloor$
- $C_5 = \lfloor D \rfloor \vee \neg \lfloor E' \rfloor$

Trail

- $\lfloor D \rfloor \mapsto_0 \bot$
- $\lfloor E \rfloor \mapsto_0 \bot$
- $\lfloor p(X) \rfloor \mapsto_0 \top$
- $\lfloor \forall y.\ p(y) \rfloor \mapsto_0 \bot$
- $\lfloor p(\tau) \rfloor \mapsto_0 \bot$

Quantified formulas - example

- $D = \exists x.\ p(x) \rightarrow (\forall y.\ p(y))$
- $E = p(X) \rightarrow \forall y.\ p(y)$
- $E' = p(\tau) \rightarrow \forall y.\ p(y)$

Clauses

- $C_0 = \neg\lfloor D \rfloor$
- $C_1 = \lfloor D \rfloor \vee \neg\lfloor E \rfloor$
- $C_2 = \lfloor E \rfloor \vee \lfloor p(X) \rfloor$
- $C_3 = \lfloor E \rfloor \vee \neg\lfloor \forall y.\ p(y) \rfloor$
- $C_4 = \lfloor \forall y.\ p(y) \rfloor \vee \neg\lfloor p(\tau) \rfloor$
- $C_5 = \lfloor D \rfloor \vee \neg\lfloor E' \rfloor$

Trail

- $\lfloor D \rfloor \mapsto_0 \bot$
- $\lfloor E \rfloor \mapsto_0 \bot$
- $\lfloor p(X) \rfloor \mapsto_0 \top$
- $\lfloor \forall y.\ p(y) \rfloor \mapsto_0 \bot$
- $\lfloor p(\tau) \rfloor \mapsto_0 \bot$
- $\lfloor E' \rfloor \mapsto_0 \bot$

Quantified formulas - example

- $D = \exists x.\ p(x) \to (\forall y.\ p(y))$
- $E = p(X) \to \forall y.\ p(y)$
- $E' = p(\tau) \to \forall y.\ p(y)$

Clauses

- $C_0 = \neg\lfloor D \rfloor$
- $C_1 = \lfloor D \rfloor \vee \neg\lfloor E \rfloor$
- $C_2 = \lfloor E \rfloor \vee \lfloor p(X) \rfloor$
- $C_3 = \lfloor E \rfloor \vee \neg\lfloor \forall y.\ p(y) \rfloor$
- $C_4 = \lfloor \forall y.\ p(y) \rfloor \vee \neg\lfloor p(\tau) \rfloor$
- $C_5 = \lfloor D \rfloor \vee \neg\lfloor E' \rfloor$
- $C_6 = \lfloor E' \rfloor \vee \lfloor p(\tau) \rfloor$
- $C_7 = \lfloor E' \rfloor \vee \neg\lfloor \forall y.\ p(y) \rfloor$

Trail

- $\lfloor D \rfloor \mapsto_0 \bot$
- $\lfloor E \rfloor \mapsto_0 \bot$
- $\lfloor p(X) \rfloor \mapsto_0 \top$
- $\lfloor \forall y.\ p(y) \rfloor \mapsto_0 \bot$
- $\lfloor p(\tau) \rfloor \mapsto_0 \bot$
- $\lfloor E' \rfloor \mapsto_0 \bot$

Quantified formulas - example

- $D = \exists x.\ p(x) \rightarrow (\forall y.\ p(y))$
- $E = p(X) \rightarrow \forall y.\ p(y)$
- $E' = p(\tau) \rightarrow \forall y.\ p(y)$

Clauses

- $C_0 = \neg\lfloor D \rfloor$
- $C_1 = \lfloor D \rfloor \vee \neg\lfloor E \rfloor$
- $C_2 = \lfloor E \rfloor \vee \lfloor p(X) \rfloor$
- $C_3 = \lfloor E \rfloor \vee \neg\lfloor \forall y.\ p(y) \rfloor$
- $C_4 = \lfloor \forall y.\ p(y) \rfloor \vee \neg\lfloor p(\tau) \rfloor$
- $C_5 = \lfloor D \rfloor \vee \neg\lfloor E' \rfloor$
- $C_6 = \lfloor E' \rfloor \vee \lfloor p(\tau) \rfloor$
- $C_7 = \lfloor E' \rfloor \vee \neg\lfloor \forall y.\ p(y) \rfloor$

Trail

- $\lfloor D \rfloor \mapsto_0 \bot$
- $\lfloor E \rfloor \mapsto_0 \bot$
- $\lfloor p(X) \rfloor \mapsto_0 \top$
- $\lfloor \forall y.\ p(y) \rfloor \mapsto_0 \bot$
- $\lfloor p(\tau) \rfloor \mapsto_0 \bot$
- $\lfloor E' \rfloor \mapsto_0 \bot$
- Conflict in C_6 !

Quantified formulas - more details

- Terms are immutable: meta-variables are never substituted, instead new terms are generated
- Meta-variables are rigid: during unification they can be bound only once
- Need to unify modulo equalities in general

SMT modulo Rewriting

Rewriting system

- Rewrite rule: $l \longrightarrow r$, with $\text{FV}(l) \subseteq \text{FV}(r)$
  - term rewrite rule: l and r are terms
  - formula rewrite rule: l is an atomic formula and r a formula
- $t \longrightarrow t'$ if a subterm/subformula $t_{|\omega} = \sigma(l)$, and $t' = t[\sigma(r)]_{|\omega}$
- A term is in normal form when it can't be rewritten anymore
- We assume the rewrite system is terminating and confluent

Rewriting as a theory

- Similar to Tableau theory, whenever a boxed atomic formula is propagated or decided, normalize it and add a clause:

$$\left(\bigvee_{(l,r)\in T} \neg\lfloor \forall \vec{x}. l \Leftrightarrow r \rfloor\right) \vee \left(\bigvee_{(l,r)\in F} \neg\lfloor \forall \vec{x}. l = r \rfloor\right) \vee \lfloor P \Leftrightarrow P' \rfloor$$

  with:

  - T the set of term rewrite rules used during normalization
  - F the set of formula rewrite rules used during normalization

Rewriting - example

$A \equiv \lfloor (\forall s, t. s \subseteq t \Leftrightarrow \forall x. x \in s \Rightarrow x \in t) \Rightarrow a \subseteq a \rfloor$

$B \equiv \lfloor \forall s, t. s \subseteq t \Leftrightarrow \forall x. x \in s \Rightarrow x \in t \rfloor$ $\quad C \equiv \lfloor a \subseteq a \rfloor$

$D \equiv \lfloor a \subseteq a \Leftrightarrow \forall x. x \in a \Rightarrow x \in a \rfloor$ $\quad E \equiv \lfloor a \subseteq a \Rightarrow \forall x. x \in a \Rightarrow x \in a \rfloor$

$F \equiv \lfloor (\forall x. x \in a \Rightarrow x \in a) \Rightarrow a \subseteq a \rfloor$ $\quad G \equiv \lfloor \forall x. x \in a \Rightarrow x \in a \rfloor$

$H \equiv \lfloor \epsilon_x \in a \Rightarrow \epsilon_x \in a \rfloor$ $\quad I \equiv \lfloor \epsilon_x \in a \rfloor$

Clauses

- $C_1 = \neg A$

Trail

Rewriting - example

$A \equiv \lfloor (\forall s, t. s \subseteq t \Leftrightarrow \forall x. x \in s \Rightarrow x \in t) \Rightarrow a \subseteq a \rfloor$

$B \equiv \lfloor \forall s, t. s \subseteq t \Leftrightarrow \forall x. x \in s \Rightarrow x \in t \rfloor$ $\quad C \equiv \lfloor a \subseteq a \rfloor$

$D \equiv \lfloor a \subseteq a \Leftrightarrow \forall x. x \in a \Rightarrow x \in a \rfloor$ $\quad E \equiv \lfloor a \subseteq a \Rightarrow \forall x. x \in a \Rightarrow x \in a \rfloor$

$F \equiv \lfloor (\forall x. x \in a \Rightarrow x \in a) \Rightarrow a \subseteq a \rfloor$ $\quad G \equiv \lfloor \forall x. x \in a \Rightarrow x \in a \rfloor$

$H \equiv \lfloor \epsilon_x \in a \Rightarrow \epsilon_x \in a \rfloor$ $\quad I \equiv \lfloor \epsilon_x \in a \rfloor$

Clauses

- $\underline{C_1 = \neg A}$

Trail

- $A \mapsto_0 \bot$

Rewriting - example

$\boldsymbol{A \equiv \lfloor (\forall s, t. s \subseteq t \Leftrightarrow \forall x. x \in s \Rightarrow x \in t) \Rightarrow a \subseteq a \rfloor}$

$B \equiv \lfloor \forall s, t. s \subseteq t \Leftrightarrow \forall x. x \in s \Rightarrow x \in t \rfloor$ $C \equiv \lfloor a \subseteq a \rfloor$

$D \equiv \lfloor a \subseteq a \Leftrightarrow \forall x. x \in a \Rightarrow x \in a \rfloor$ $E \equiv \lfloor a \subseteq a \Rightarrow \forall x. x \in a \Rightarrow x \in a \rfloor$

$F \equiv \lfloor (\forall x. x \in a \Rightarrow x \in a) \Rightarrow a \subseteq a \rfloor$ $G \equiv \lfloor \forall x. x \in a \Rightarrow x \in a \rfloor$

$H \equiv \lfloor \epsilon_x \in a \Rightarrow \epsilon_x \in a \rfloor$ $I \equiv \lfloor \epsilon_x \in a \rfloor$

Clauses

- $C_1 = \neg A$
- $C_2 = A \vee B$
- $C_3 = A \vee \neg C$

Trail

- $A \mapsto_0 \bot$

Rewriting - example

$A \equiv \lfloor (\forall s, t. s \subseteq t \Leftrightarrow \forall x. x \in s \Rightarrow x \in t) \Rightarrow a \subseteq a \rfloor$

$B \equiv \lfloor \forall s, t. s \subseteq t \Leftrightarrow \forall x. x \in s \Rightarrow x \in t \rfloor$ $\quad C \equiv \lfloor a \subseteq a \rfloor$

$D \equiv \lfloor a \subseteq a \Leftrightarrow \forall x. x \in a \Rightarrow x \in a \rfloor$ $\quad E \equiv \lfloor a \subseteq a \Rightarrow \forall x. x \in a \Rightarrow x \in a \rfloor$

$F \equiv \lfloor (\forall x. x \in a \Rightarrow x \in a) \Rightarrow a \subseteq a \rfloor$ $\quad G \equiv \lfloor \forall x. x \in a \Rightarrow x \in a \rfloor$

$H \equiv \lfloor \epsilon_x \in a \Rightarrow \epsilon_x \in a \rfloor$ $\quad I \equiv \lfloor \epsilon_x \in a \rfloor$

Clauses

- $C_1 = \neg A$
- $\underline{C_2 = A \vee B}$
- $C_3 = A \vee \neg C$

Trail

- $A \mapsto_0 \bot$
- $B \mapsto_0 \top$

  (rewrite rule)

Rewriting - example

$A \equiv \lfloor (\forall s, t. s \subseteq t \Leftrightarrow \forall x. x \in s \Rightarrow x \in t) \Rightarrow a \subseteq a \rfloor$

$B \equiv \lfloor \forall s, t. s \subseteq t \Leftrightarrow \forall x. x \in s \Rightarrow x \in t \rfloor$ $C \equiv \lfloor a \subseteq a \rfloor$

$D \equiv \lfloor a \subseteq a \Leftrightarrow \forall x. x \in a \Rightarrow x \in a \rfloor$ $E \equiv \lfloor a \subseteq a \Rightarrow \forall x. x \in a \Rightarrow x \in a \rfloor$

$F \equiv \lfloor (\forall x. x \in a \Rightarrow x \in a) \Rightarrow a \subseteq a \rfloor$ $G \equiv \lfloor \forall x. x \in a \Rightarrow x \in a \rfloor$

$H \equiv \lfloor \epsilon_x \in a \Rightarrow \epsilon_x \in a \rfloor$ $I \equiv \lfloor \epsilon_x \in a \rfloor$

Clauses

- $C_1 = \neg A$
- $C_2 = A \vee B$
- $\underline{C_3 = A \vee \neg C}$

Trail

- $A \mapsto_0 \bot$
- $B \mapsto_0 \top$
  (rewrite rule)
- $C \mapsto_0 \bot$

Rewriting - example

$A \equiv \lfloor (\forall s, t. s \subseteq t \Leftrightarrow \forall x. x \in s \Rightarrow x \in t) \Rightarrow a \subseteq a \rfloor$

$B \equiv \lfloor \forall s, t. \boldsymbol{s} \subseteq \boldsymbol{t} \Leftrightarrow \forall x. x \in s \Rightarrow x \in t \rfloor$ $\boldsymbol{C \equiv \lfloor a \subseteq a \rfloor}$

$D \equiv \lfloor a \subseteq a \Leftrightarrow \forall x. x \in a \Rightarrow x \in a \rfloor$ $E \equiv \lfloor a \subseteq a \Rightarrow \forall x. x \in a \Rightarrow x \in a \rfloor$

$F \equiv \lfloor (\forall x. x \in a \Rightarrow x \in a) \Rightarrow a \subseteq a \rfloor$ $G \equiv \lfloor \forall x. x \in a \Rightarrow x \in a \rfloor$

$H \equiv \lfloor \epsilon_x \in a \Rightarrow \epsilon_x \in a \rfloor$ $I \equiv \lfloor \epsilon_x \in a \rfloor$

Clauses

- $C_1 = \neg A$
- $C_2 = A \vee B$
- $C_3 = A \vee \neg C$
- $C_4 = \neg B \vee D$

Trail

- $A \mapsto_0 \bot$
- $B \mapsto_0 \top$
  (rewrite rule)
- $C \mapsto_0 \bot$

Rewriting - example

$A \equiv \lfloor (\forall s, t. s \subseteq t \Leftrightarrow \forall x. x \in s \Rightarrow x \in t) \Rightarrow a \subseteq a \rfloor$

$B \equiv \lfloor \forall s, t. s \subseteq t \Leftrightarrow \forall x. x \in s \Rightarrow x \in t \rfloor$ $C \equiv \lfloor a \subseteq a \rfloor$

$D \equiv \lfloor a \subseteq a \Leftrightarrow \forall x. x \in a \Rightarrow x \in a \rfloor$ $E \equiv \lfloor a \subseteq a \Rightarrow \forall x. x \in a \Rightarrow x \in a \rfloor$

$F \equiv \lfloor (\forall x. x \in a \Rightarrow x \in a) \Rightarrow a \subseteq a \rfloor$ $G \equiv \lfloor \forall x. x \in a \Rightarrow x \in a \rfloor$

$H \equiv \lfloor \epsilon_x \in a \Rightarrow \epsilon_x \in a \rfloor$ $I \equiv \lfloor \epsilon_x \in a \rfloor$

Clauses

- $C_1 = \neg A$
- $C_2 = A \vee B$
- $C_3 = A \vee \neg C$
- $\underline{C_4 = \neg B \vee D}$

Trail

- $A \mapsto_0 \bot$
- $B \mapsto_0 \top$

  (rewrite rule)
- $C \mapsto_0 \bot$
- $D \mapsto_0 \top$

Rewriting - example

$A \equiv \lfloor (\forall s, t. s \subseteq t \Leftrightarrow \forall x. x \in s \Rightarrow x \in t) \Rightarrow a \subseteq a \rfloor$

$B \equiv \lfloor \forall s, t. s \subseteq t \Leftrightarrow \forall x. x \in s \Rightarrow x \in t \rfloor$ $\quad C \equiv \lfloor a \subseteq a \rfloor$

$\boldsymbol{D \equiv \lfloor a \subseteq a \Leftrightarrow \forall x. x \in a \Rightarrow x \in a \rfloor}$ $\quad E \equiv \lfloor a \subseteq a \Rightarrow \forall x. x \in a \Rightarrow x \in a \rfloor$

$F \equiv \lfloor (\forall x. x \in a \Rightarrow x \in a) \Rightarrow a \subseteq a \rfloor$ $\quad G \equiv \lfloor \forall x. x \in a \Rightarrow x \in a \rfloor$

$H \equiv \lfloor \epsilon_x \in a \Rightarrow \epsilon_x \in a \rfloor$ $\quad I \equiv \lfloor \epsilon_x \in a \rfloor$

Clauses

- $C_1 = \neg A$
- $C_2 = A \vee B$
- $C_3 = A \vee \neg C$
- $C_4 = \neg B \vee D$
- $C_5 = \neg D \vee E$
- $C_6 = \neg D \vee F$

Trail

- $A \mapsto_0 \bot$
- $B \mapsto_0 \top$
  (rewrite rule)
- $C \mapsto_0 \bot$
- $D \mapsto_0 \top$

Rewriting - example

$A \equiv \lfloor (\forall s, t. s \subseteq t \Leftrightarrow \forall x. x \in s \Rightarrow x \in t) \Rightarrow a \subseteq a \rfloor$

$B \equiv \lfloor \forall s, t. s \subseteq t \Leftrightarrow \forall x. x \in s \Rightarrow x \in t \rfloor$ $\quad C \equiv \lfloor a \subseteq a \rfloor$

$D \equiv \lfloor a \subseteq a \Leftrightarrow \forall x. x \in a \Rightarrow x \in a \rfloor$ $\quad E \equiv \lfloor a \subseteq a \Rightarrow \forall x. x \in a \Rightarrow x \in a \rfloor$

$F \equiv \lfloor (\forall x. x \in a \Rightarrow x \in a) \Rightarrow a \subseteq a \rfloor$ $\quad G \equiv \lfloor \forall x. x \in a \Rightarrow x \in a \rfloor$

$H \equiv \lfloor \epsilon_x \in a \Rightarrow \epsilon_x \in a \rfloor$ $\quad I \equiv \lfloor \epsilon_x \in a \rfloor$

Clauses

- $C_1 = \neg A$
- $C_2 = A \vee B$
- $C_3 = A \vee \neg C$
- $C_4 = \neg B \vee D$
- $\underline{C_5 = \neg D \vee E}$
- $C_6 = \neg D \vee F$

Trail

- $A \mapsto_0 \bot$
- $B \mapsto_0 \top$
  (rewrite rule)
- $C \mapsto_0 \bot$
- $D \mapsto_0 \top$
- $E \mapsto_0 \top$

Rewriting - example

$A \equiv \lfloor(\forall s,t.s \subseteq t \Leftrightarrow \forall x.x \in s \Rightarrow x \in t) \Rightarrow a \subseteq a\rfloor$

$B \equiv \lfloor\forall s,t.s \subseteq t \Leftrightarrow \forall x.x \in s \Rightarrow x \in t\rfloor$ $\quad C \equiv \lfloor a \subseteq a\rfloor$

$D \equiv \lfloor a \subseteq a \Leftrightarrow \forall x.x \in a \Rightarrow x \in a\rfloor$ $\quad E \equiv \lfloor a \subseteq a \Rightarrow \forall x.x \in a \Rightarrow x \in a\rfloor$

$F \equiv \lfloor(\forall x.x \in a \Rightarrow x \in a) \Rightarrow a \subseteq a\rfloor$ $\quad G \equiv \lfloor\forall x.x \in a \Rightarrow x \in a\rfloor$

$H \equiv \lfloor\epsilon_x \in a \Rightarrow \epsilon_x \in a\rfloor$ $\quad I \equiv \lfloor\epsilon_x \in a\rfloor$

Clauses

- $C_1 = \neg A$
- $C_2 = A \vee B$
- $C_3 = A \vee \neg C$
- $C_4 = \neg B \vee D$
- $C_5 = \neg D \vee E$
- $\underline{C_6 = \neg D \vee F}$

Trail

- $A \mapsto_0 \bot$
- $B \mapsto_0 \top$
  (rewrite rule)
- $C \mapsto_0 \bot$
- $D \mapsto_0 \top$
- $E \mapsto_0 \top$
- $F \mapsto_0 \top$

Rewriting - example

$A \equiv \lfloor (\forall s, t. s \subseteq t \Leftrightarrow \forall x. x \in s \Rightarrow x \in t) \Rightarrow a \subseteq a \rfloor$

$B \equiv \lfloor \forall s, t. s \subseteq t \Leftrightarrow \forall x. x \in s \Rightarrow x \in t \rfloor$ $C \equiv \lfloor a \subseteq a \rfloor$

$D \equiv \lfloor a \subseteq a \Leftrightarrow \forall x. x \in a \Rightarrow x \in a \rfloor$ $E \equiv \lfloor a \subseteq a \Rightarrow \forall x. x \in a \Rightarrow x \in a \rfloor$

$\boldsymbol{F \equiv \lfloor (\forall x. x \in a \Rightarrow x \in a) \Rightarrow a \subseteq a \rfloor}$ $G \equiv \lfloor \forall x. x \in a \Rightarrow x \in a \rfloor$

$H \equiv \lfloor \epsilon_x \in a \Rightarrow \epsilon_x \in a \rfloor$ $I \equiv \lfloor \epsilon_x \in a \rfloor$

Clauses

- $C_1 = \neg A$
- $C_2 = A \vee B$
- $C_3 = A \vee \neg C$
- $C_4 = \neg B \vee D$
- $C_5 = \neg D \vee E$
- $C_6 = \neg D \vee F$
- $C_7 = \neg F \vee \neg G \vee C$

Trail

- $A \mapsto_0 \bot$
- $B \mapsto_0 \top$
  (rewrite rule)
- $C \mapsto_0 \bot$
- $D \mapsto_0 \top$
- $E \mapsto_0 \top$
- $F \mapsto_0 \top$

Rewriting - example

$A \equiv \lfloor (\forall s, t. s \subseteq t \Leftrightarrow \forall x. x \in s \Rightarrow x \in t) \Rightarrow a \subseteq a \rfloor$

$B \equiv \lfloor \forall s, t. s \subseteq t \Leftrightarrow \forall x. x \in s \Rightarrow x \in t \rfloor$ $\quad C \equiv \lfloor a \subseteq a \rfloor$

$D \equiv \lfloor a \subseteq a \Leftrightarrow \forall x. x \in a \Rightarrow x \in a \rfloor$ $\quad E \equiv \lfloor a \subseteq a \Rightarrow \forall x. x \in a \Rightarrow x \in a \rfloor$

$F \equiv \lfloor (\forall x. x \in a \Rightarrow x \in a) \Rightarrow a \subseteq a \rfloor$ $\quad G \equiv \lfloor \forall x. x \in a \Rightarrow x \in a \rfloor$

$H \equiv \lfloor \epsilon_x \in a \Rightarrow \epsilon_x \in a \rfloor$ $\quad I \equiv \lfloor \epsilon_x \in a \rfloor$

Clauses

- $C_1 = \neg A$
- $C_2 = A \vee B$
- $C_3 = A \vee \neg C$
- $C_4 = \neg B \vee D$
- $C_5 = \neg D \vee E$
- $C_6 = \neg D \vee F$
- $\underline{C_7 = \neg F \vee \neg G \vee C}$

Trail

- $A \mapsto_0 \bot$
- $B \mapsto_0 \top$

  (rewrite rule)
- $C \mapsto_0 \bot$
- $D \mapsto_0 \top$
- $E \mapsto_0 \top$
- $F \mapsto_0 \top$
- $G \mapsto_0 \bot$

Rewriting - example

$A \equiv \lfloor (\forall s, t. s \subseteq t \Leftrightarrow \forall x. x \in s \Rightarrow x \in t) \Rightarrow a \subseteq a \rfloor$

$B \equiv \lfloor \forall s, t. s \subseteq t \Leftrightarrow \forall x. x \in s \Rightarrow x \in t \rfloor$ $\quad C \equiv \lfloor a \subseteq a \rfloor$

$D \equiv \lfloor a \subseteq a \Leftrightarrow \forall x. x \in a \Rightarrow x \in a \rfloor$ $\quad E \equiv \lfloor a \subseteq a \Rightarrow \forall x. x \in a \Rightarrow x \in a \rfloor$

$F \equiv \lfloor (\forall x. x \in a \Rightarrow x \in a) \Rightarrow a \subseteq a \rfloor$ $\quad \boldsymbol{G \equiv \lfloor \forall x. x \in a \Rightarrow x \in a \rfloor}$

$H \equiv \lfloor \epsilon_x \in a \Rightarrow \epsilon_x \in a \rfloor$ $\quad I \equiv \lfloor \epsilon_x \in a \rfloor$

Clauses

- $C_1 = \neg A$
- $C_2 = A \vee B$
- $C_3 = A \vee \neg C$
- $C_4 = \neg B \vee D$
- $C_5 = \neg D \vee E$
- $C_6 = \neg D \vee F$
- $C_7 = \neg F \vee \neg G \vee C$
- $C_8 = G \vee \neg H$

Trail

- $A \mapsto_0 \bot$
- $B \mapsto_0 \top$ (rewrite rule)
- $C \mapsto_0 \bot$
- $D \mapsto_0 \top$
- $E \mapsto_0 \top$
- $F \mapsto_0 \top$
- $G \mapsto_0 \bot$

Rewriting - example

$A \equiv \lfloor (\forall s, t. s \subseteq t \Leftrightarrow \forall x. x \in s \Rightarrow x \in t) \Rightarrow a \subseteq a \rfloor$

$B \equiv \lfloor \forall s, t. s \subseteq t \Leftrightarrow \forall x. x \in s \Rightarrow x \in t \rfloor$ $\quad C \equiv \lfloor a \subseteq a \rfloor$

$D \equiv \lfloor a \subseteq a \Leftrightarrow \forall x. x \in a \Rightarrow x \in a \rfloor$ $\quad E \equiv \lfloor a \subseteq a \Rightarrow \forall x. x \in a \Rightarrow x \in a \rfloor$

$F \equiv \lfloor (\forall x. x \in a \Rightarrow x \in a) \Rightarrow a \subseteq a \rfloor$ $\quad G \equiv \lfloor \forall x. x \in a \Rightarrow x \in a \rfloor$

$H \equiv \lfloor \epsilon_x \in a \Rightarrow \epsilon_x \in a \rfloor$ $\quad I \equiv \lfloor \epsilon_x \in a \rfloor$

Clauses

- $C_1 = \neg A$
- $C_2 = A \vee B$
- $C_3 = A \vee \neg C$
- $C_4 = \neg B \vee D$
- $C_5 = \neg D \vee E$
- $C_6 = \neg D \vee F$
- $C_7 = \neg F \vee \neg G \vee C$
- $\underline{C_8 = G \vee \neg H}$

Trail

- $A \mapsto_0 \bot$
- $B \mapsto_0 \top$

  (rewrite rule)
- $C \mapsto_0 \bot$
- $D \mapsto_0 \top$
- $E \mapsto_0 \top$
- $F \mapsto_0 \top$
- $G \mapsto_0 \bot$
- $H \mapsto_0 \bot$

Rewriting - example

$A \equiv \lfloor (\forall s, t. s \subseteq t \Leftrightarrow \forall x. x \in s \Rightarrow x \in t) \Rightarrow a \subseteq a \rfloor$

$B \equiv \lfloor \forall s, t. s \subseteq t \Leftrightarrow \forall x. x \in s \Rightarrow x \in t \rfloor$ $\quad C \equiv \lfloor a \subseteq a \rfloor$

$D \equiv \lfloor a \subseteq a \Leftrightarrow \forall x. x \in a \Rightarrow x \in a \rfloor$ $\quad E \equiv \lfloor a \subseteq a \Rightarrow \forall x. x \in a \Rightarrow x \in a \rfloor$

$F \equiv \lfloor (\forall x. x \in a \Rightarrow x \in a) \Rightarrow a \subseteq a \rfloor$ $\quad G \equiv \lfloor \forall x. x \in a \Rightarrow x \in a \rfloor$

$\boldsymbol{H \equiv \lfloor \epsilon_x \in a \Rightarrow \epsilon_x \in a \rfloor}$ $\quad I \equiv \lfloor \epsilon_x \in a \rfloor$

Clauses

- $C_1 = \neg A$
- $C_2 = A \vee B$
- $C_3 = A \vee \neg C$
- $C_4 = \neg B \vee D$
- $C_5 = \neg D \vee E$
- $C_6 = \neg D \vee F$
- $C_7 = \neg F \vee \neg G \vee C$
- $C_8 = G \vee \neg H$
- $C_9 = H \vee I$
- $C_{10} = H \vee \neg I$

Trail

- $A \mapsto_0 \bot$
- $B \mapsto_0 \top$

  (rewrite rule)
- $C \mapsto_0 \bot$
- $D \mapsto_0 \top$
- $E \mapsto_0 \top$
- $F \mapsto_0 \top$
- $G \mapsto_0 \bot$
- $H \mapsto_0 \bot$

Rewriting - example

$A \equiv \lfloor(\forall s,t.s \subseteq t \Leftrightarrow \forall x.x \in s \Rightarrow x \in t) \Rightarrow a \subseteq a\rfloor$

$B \equiv \lfloor\forall s,t.s \subseteq t \Leftrightarrow \forall x.x \in s \Rightarrow x \in t\rfloor$ $\quad C \equiv \lfloor a \subseteq a\rfloor$

$D \equiv \lfloor a \subseteq a \Leftrightarrow \forall x.x \in a \Rightarrow x \in a\rfloor$ $\quad E \equiv \lfloor a \subseteq a \Rightarrow \forall x.x \in a \Rightarrow x \in a\rfloor$

$F \equiv \lfloor(\forall x.x \in a \Rightarrow x \in a) \Rightarrow a \subseteq a\rfloor$ $\quad G \equiv \lfloor\forall x.x \in a \Rightarrow x \in a\rfloor$

$H \equiv \lfloor\epsilon_x \in a \Rightarrow \epsilon_x \in a\rfloor$ $\quad I \equiv \lfloor\epsilon_x \in a\rfloor$

Clauses

- $C_1 = \neg A$
- $C_2 = A \vee B$
- $C_3 = A \vee \neg C$
- $C_4 = \neg B \vee D$
- $C_5 = \neg D \vee E$
- $C_6 = \neg D \vee F$
- $C_7 = \neg F \vee \neg G \vee C$
- $C_8 = G \vee \neg H$
- $\underline{C_9 = H \vee I}$
- $C_{10} = H \vee \neg I$

Trail

- $A \mapsto_0 \bot$
- $B \mapsto_0 \top$ (rewrite rule)
- $C \mapsto_0 \bot$
- $D \mapsto_0 \top$
- $E \mapsto_0 \top$
- $F \mapsto_0 \top$
- $G \mapsto_0 \bot$
- $H \mapsto_0 \bot$
- $I \mapsto_0 \top$

Rewriting - example

$A \equiv \lfloor (\forall s, t. s \subseteq t \Leftrightarrow \forall x. x \in s \Rightarrow x \in t) \Rightarrow a \subseteq a \rfloor$

$B \equiv \lfloor \forall s, t. s \subseteq t \Leftrightarrow \forall x. x \in s \Rightarrow x \in t \rfloor$ $\quad C \equiv \lfloor a \subseteq a \rfloor$

$D \equiv \lfloor a \subseteq a \Leftrightarrow \forall x. x \in a \Rightarrow x \in a \rfloor$ $\quad E \equiv \lfloor a \subseteq a \Rightarrow \forall x. x \in a \Rightarrow x \in a \rfloor$

$F \equiv \lfloor (\forall x. x \in a \Rightarrow x \in a) \Rightarrow a \subseteq a \rfloor$ $\quad G \equiv \lfloor \forall x. x \in a \Rightarrow x \in a \rfloor$

$H \equiv \lfloor \epsilon_x \in a \Rightarrow \epsilon_x \in a \rfloor$ $\quad I \equiv \lfloor \epsilon_x \in a \rfloor$

Clauses

- $C_1 = \neg A$
- $C_2 = A \vee B$
- $C_3 = A \vee \neg C$
- $C_4 = \neg B \vee D$
- $C_5 = \neg D \vee E$
- $C_6 = \neg D \vee F$
- $C_7 = \neg F \vee \neg G \vee C$
- $C_8 = G \vee \neg H$
- $C_9 = H \vee I$
- $\underline{C_{10} = H \vee \neg I}$

Trail

- $A \mapsto_0 \bot$
- $B \mapsto_0 \top$
  (rewrite rule)
- $C \mapsto_0 \bot$
- $D \mapsto_0 \top$
- $E \mapsto_0 \top$
- $F \mapsto_0 \top$
- $G \mapsto_0 \bot$
- $H \mapsto_0 \bot$
- $I \mapsto_0 \top$
- Unsat!

Finding instanciations modulo Rewriting

Finding instanciations and rewrite rules

- Instanciations are found by unifiying the true predicates with the false predicates whenever a model is found.
- If the problem contains equalities, need to unify modulo equalities
- In presence of rewrite rules, need to unify modulo equalities, and modulo rewrite rules

Rigid Superposition

- Unit Superposition (close to unfailing Knuth-Bendix completion):

$$\frac{s = t \qquad u \bowtie v}{\sigma(u[p \leftarrow t] \bowtie v)} \quad \begin{array}{l} \sigma = \mathrm{mgu}(u_{|p}, s), u_{|p} \notin V \\ \sigma(s) \not< \sigma(t), \sigma(u) \not< \sigma(v) \end{array}$$

- Use rigid variables: look for solutions where each variable is bound at most once
- Each (dis)equality carry a set of substitution
- Applying some rules needs to merge substitutions, which can fail because of rigid variables (for instance $\{X \mapsto a\}$ and $\{X \mapsto b\}$ can not be merged because X is rigid)
- Dual of AVATAR (where a superposition prover calls a SAT solver)

Unit Rigid superposition

- $\sigma \circ \sigma' \triangleq \{x \mapsto (x\sigma)\sigma' | x \in \mathrm{domain}(\sigma)\}$
- $\Sigma \circ \sigma' \triangleq \{\sigma \circ \sigma' | \sigma \in \Sigma\}$.
- $\sigma \leq \sigma'$ if and only if $\exists \sigma''.\ \sigma \circ \sigma'' = \sigma'$.
- $\sigma \uparrow \sigma'$ is the supremum of $\{\sigma, \sigma'\}$ for the order $\leq$, if it exists, or $\bot$
- $\Sigma \uparrow \Sigma' \triangleq \{\sigma \uparrow \sigma' \mid \sigma \in \Sigma, \sigma' \in \Sigma', \sigma \uparrow \sigma' \neq \bot\}$.

$$\text{SN/SP}\ \frac{s \approx t \mid \Sigma \qquad u\ R\ v \mid \Sigma'}{\sigma''(u[p \leftarrow t]\ R\ v) \mid \sigma'''} \quad \text{if} \begin{cases} \sigma'' = \mathrm{mgu}(u_{|p}, s) & u_{|p} \notin V \\ \sigma''(s) \not\preceq \sigma''(t) & \sigma''(u) \not\preceq \sigma''(v) \\ \sigma''' \in (\Sigma \circ \sigma'') \uparrow (\Sigma' \circ \sigma'') \\ R \in \{\approx, \not\approx\} \end{cases}$$

Unit superposition - example

$$
\begin{aligned}
a &\preceq b \\
\text{pair}(\text{fst}(x), \text{snd}(x))) &\longrightarrow x \\
\text{fst}(a) &\approx \text{fst}(b) \\
p(a) &\not\approx p(\text{pair}(\text{fst}(b), X))
\end{aligned}
$$

Unit superposition - example

1	rewrite rule	$\text{pair}(\text{fst}(x), \text{snd}(x))) \longrightarrow x$
2	axiom	$\text{fst}(a) = \text{fst}(b)$
3	axiom	$p(a) \neq p(\text{pair}(\text{fst}(b), X))$
4	rewr(1)	$\text{pair}(\text{fst}(x), \text{snd}(x)) \approx x \mid \{\}$
5	rename(2)	$\text{fst}(a) \approx \text{fst}(b) \mid \{\}$
6	rename(3)	$p(a) \not\approx p(\text{pair}(\text{fst}(b), y)) \mid \{X \mapsto y\}$
7	RN(5,6)	$p(a) \not\approx p(\text{pair}(\text{fst}(a), y)) \mid \{X \mapsto y\}$
8	SN(4,7)	$p(a) \not\approx p(a) \mid \{X \mapsto \text{snd}(a)\}$
9	ER(8)	$\emptyset \mid \{X \mapsto \text{snd}(a)\}$

Experimental results

- Implemented in ArchSat (SMT solver + Tableau + Rewriting)
- Tested using the set axiomatisation of the B method
- Axiomatisation expressed using polymorphism
- 319 lemma taken from the B-Book

319 Problems	ArchSAT	Zenon Modulo	Alt-Ergo
Proofs	272	138	232
Rate	85.3%	43.3%	72.7%
Total time (s)	16.61 (260 proof) + 252.08 (12 last proofs)	2.86	8.42

Conclusion

- Rewriting provides better performances
- Tableau theory is a viable alternative to CNF conversion
- Modularity: both theories presented work well with traditional ground solving in SMT solvers
- Further works:
    - Fine-tune Unit rigid superposition
    - Better instantiation schema, inspired from other Tableau provers