

Overview of Automated Reasoning

Peter Baumgartner



`Peter.Baumgartner@nicta.com.au`

`http://users.cecs.anu.edu.au/~baumgart/`

What is Automated Reasoning?

Theme

Building push-button technology (software) for mathematical-logical reasoning on computer

Relevant fields

- Mathematical logic and philosophy: formal logics and calculi
- Theoretical computer science: computability theory, complexity theory
- Applied and practical computer science: artificial intelligence, data structures and algorithms

Applications: Software verification, hardware verification, analysing dynamic properties of reactive systems, databases, mathematical theorem proving, planning, diagnosis, knowledge representation (description logics), logic programming, constraint solving

**Automated Reasoning systems parametrized in
logic and reasoning service**

Logics and Reasoning Service: Constraint Solving

The n-queens problem:

Given: An $n \times n$ chessboard

Question: Is it possible to place n queens so that no queen attacks any other?

A solution for $n = 8$

$$p[1] = 6$$

$$p[2] = 3$$

$$p[3] = 5$$

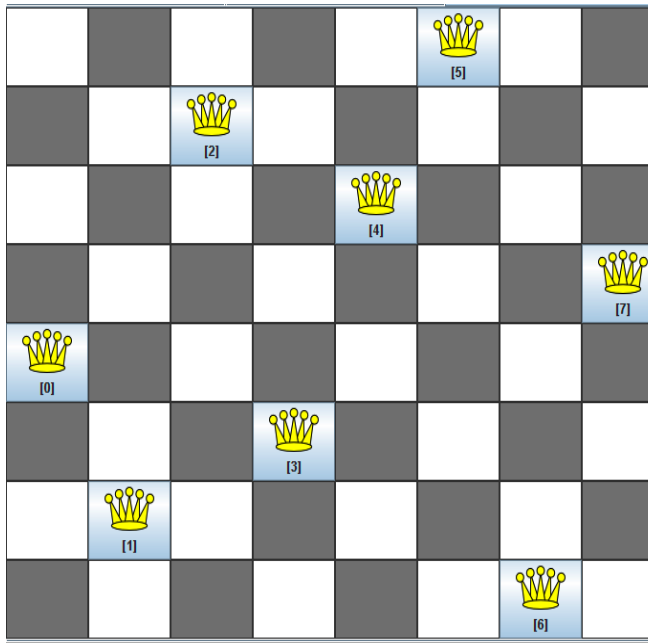
$$p[4] = 8$$

$$p[5] = 1$$

$$p[6] = 4$$

$$p[7] = 2$$

$$p[8] = 7$$



Use a **constraint solver** to find a solution

Logics and Reasoning Service: Constraint Solving

A **Zinc** model, ready to be run by a constraint solver:

```
int: n = 8;
array [1..n] of var 1..n: p;
constraint
    forall (i in 1..n, j in i + 1..n) (
        p[i]      != p[j]
        /\
        p[i] + i != p[j] + j
        /\
        p[i] - i != p[j] - j
    );
solve satisfy; output ["Solution: ", show(p), "\n"];
```

Logic: Integer arithmetic, quantifiers, arrays

Reasoning Service: Constraint solving

Search assignments for all vars $p[1]$ to $p[n]$ such that constraint is satisfied

With n fixed, all variables and i and j range over finite domains.

This is typical for “constraint solving”

Logics and Reasoning Service: Constraint Solving

The same problem, written in sorted first-order logic:

$n : \mathbb{Z}$ (Declaration of n)

$p : \mathbb{Z} \mapsto \mathbb{Z}$ (Declaration of p)

$n = 8$

$\forall i : \mathbb{Z} \ j : \mathbb{Z} \ (1 \leq i \wedge i \leq n \wedge i + 1 \leq j \wedge j < n \Rightarrow$
 $p(i) \neq p(j) \wedge p(i) + i \neq p(j) + j \wedge p(i) - i \neq p(j) - j)$ (Queens)

$p(1) = 1 \vee p(1) = 2 \vee \dots \vee p(1) = 8$ ($p(1) \in \{1, \dots, n\}$)

\vdots

$p(8) = 1 \vee p(8) = 2 \vee \dots \vee p(8) = 8$ ($p(n) \in \{1, \dots, n\}$)

Logic: Integer arithmetic, quantifiers, “free” symbol p

Reasoning Service: Satisfiability: find a satisfying interpretation I (a model)
and evaluate $I(p(1)), \dots, I(p(n))$ to read off the answer

Logics and Reasoning Service: Constraint Solving

Summary so far

- Constraint solvers are applicable when all variables range over **finite** domains. They can exploit this fact when searching for a solution, in particular for “constraint propagation”
- Theorem provers are intended to work on **infinite** domains. In the N-queens example the variables are quantified over finite domains only coincidentally.
- On finite search problems constraint solvers perform usually much better

So, why theorem proving?

Answer: for analysing the problem **for any board size n**

Logical Analysis Example: N-Queens

$$p[1] = 6$$

$$p[2] = 3$$

$$p[3] = 5$$

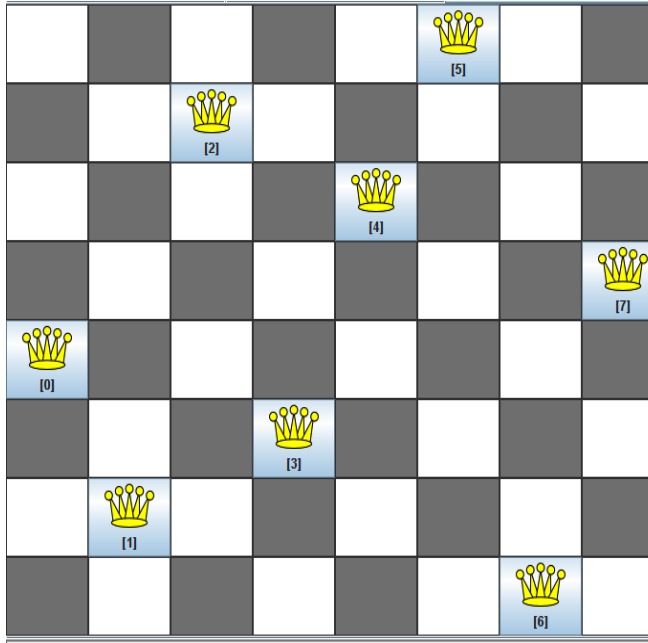
$$p[4] = 8$$

$$p[5] = 1$$

$$p[6] = 4$$

$$p[7] = 2$$

$$p[8] = 7$$



Number of solutions, depending on n :

| n : | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 | 11 | 12 | 13 | 14 | .. | 24 | 25 |
|-----------|---|---|---|---|----|---|----|----|-----|-----|-------|--------|--------|---------|----|---------------------|-----------------------|
| unique: | 1 | 0 | 0 | 1 | 2 | 1 | 6 | 12 | 46 | 92 | 341 | 1,787 | 9,233 | 45,752 | .. | 28,439,272,956,934 | 275,986,683,743,434 |
| distinct: | 1 | 0 | 0 | 2 | 10 | 4 | 40 | 92 | 352 | 724 | 2,680 | 14,200 | 73,712 | 365,596 | .. | 227,514,171,973,736 | 2,207,893,435,808,352 |

“**unique**” is “**distinct**” modulo reflection/rotation symmetry

For efficiency reasons better avoid searching symmetric solutions

Logical Analysis Example: N-Queens

$$p[1] = 6$$

$$p[2] = 3$$

$$p[3] = 5$$

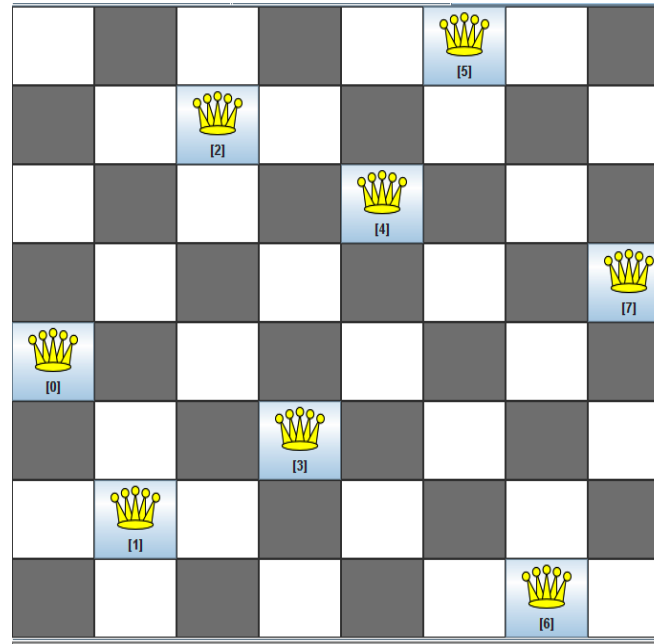
$$p[4] = 8$$

$$p[5] = 1$$

$$p[6] = 4$$

$$p[7] = 2$$

$$p[8] = 7$$



- The n-queens has variable symmetry: mapping $p[i] \mapsto p[n + 1 - i]$ preserves solutions, **for any n**
- Therefore, it is justified to add (to the formalization) a constraint $p[1] < p[n]$, for search space pruning
- But how can we know that the problem has symmetries?
This is a theorem proving task!

Proving Symmetry: Formalization

We need two “copies” (Queens_p) and (Queens_q) of the constraint:

$n : \mathbb{Z}$ (Declaration of n)

$p, q : \mathbb{Z} \mapsto \mathbb{Z}$ (Declaration of p, q)

$perm : \mathbb{Z} \mapsto \mathbb{Z}$ (Declaration of $perm$)

$\forall i : \mathbb{Z} \ j : \mathbb{Z} \ (1 \leq i \wedge i \leq n \wedge i + 1 \leq j \wedge j < n \Rightarrow$
 $p(i) \neq p(j) \wedge p(i) + i \neq p(j) + j \wedge p(i) - i \neq p(j) - j)$ (Queens_p)

$\forall i : \mathbb{Z} \ j : \mathbb{Z} \ (1 \leq i \wedge i \leq n \wedge i + 1 \leq j \wedge j < n \Rightarrow$
 $q(i) \neq q(j) \wedge q(i) + i \neq q(j) + j \wedge q(i) - i \neq q(j) - j)$ (Queens_q)

$\forall i : \mathbb{Z} \ perm(i) = n + 1 - i$ (Def. permutation)

Logic: Integer arithmetic, quantifiers, “free” symbol p

Reasoning Service: Entailment

The above entails $(\text{Queens_p}) \wedge (\forall i : \mathbb{Z} \ q(i) = p(\text{perm}(i))) \Rightarrow (\text{Queens_q})$
which expresses the symmetry property. Use a theorem prover

Logics and Reasoning Service - Spectrum

Logics

Base logic: propositional/first-order/higher-order

Syntactic fragments

(Description Logics, Datalog, ...)

Classical/non-monotonic

Modalities (temporal, deontic, ...)

Over structures (finite trees, graphs,...)

Modulo Theories (equality, arithmetic, ...)

Almost any subset of the left column (potentially) makes sense

**The challenge is to build “decent” calculi/theorem provers:
theoretically analysed, avoiding redundancies, practically useful,
meaningful answers (proofs, models), ...**

Services

Model checking
(evaluation)

Satisfiability
(minimal models)

Validity

Induction

Abduction

Contents

Introduction

Logics and Reasoning Service (already done)

Methods for Automated Theorem Proving

Overview of some widely used general methods

- Propositional SAT solving
- First-order logic and clause normal forms
- Proof Procedures Based on Herbrand's Theorem
- The Resolution calculus
- Instance-based methods
- Model generation

Theory Reasoning

Methods to reason with specific background theories

- Paramodulation (Equality)
- Satisfiability Modulo Theories (SMT)
- Quantifier elimination for linear real arithmetic
- Combining multiple theories

Propositional Logic

Syntax

Propositional Logic

Syntax

- Propositional variables (aka (propositional) atoms) A, B, C

Propositional Logic

Syntax

- Propositional variables (aka (propositional) atoms) A, B, C
- Boolean connectives \neg (negation), \wedge (and), \vee (or), \Rightarrow (implication)

Propositional Logic

Syntax

- Propositional variables (aka (propositional) atoms) A, B, C
- Boolean connectives \neg (negation), \wedge (and), \vee (or), \Rightarrow (implication)
- Parenthesis (and)

Propositional Logic

Syntax

- Propositional variables (aka (propositional) atoms) A, B, C
- Boolean connectives \neg (negation), \wedge (and), \vee (or), \Rightarrow (implication)
- Parenthesis (and)
- A formula is either an atom or some formulas combined with a connective in the proper way. Example: $(A \Rightarrow B) \Rightarrow (B \vee \neg A)$

Propositional Logic

Syntax

- Propositional variables (aka (propositional) atoms) A, B, C
- Boolean connectives \neg (negation), \wedge (and), \vee (or), \Rightarrow (implication)
- Parenthesis (and)
- A formula is either an atom or some formulas combined with a connective in the proper way. Example: $(A \Rightarrow B) \Rightarrow (B \vee \neg A)$

Clause Logic

Propositional Logic

Syntax

- Propositional variables (aka (propositional) atoms) A, B, C
- Boolean connectives \neg (negation), \wedge (and), \vee (or), \Rightarrow (implication)
- Parenthesis (and)
- A formula is either an atom or some formulas combined with a connective in the proper way. Example: $(A \Rightarrow B) \Rightarrow (B \vee \neg A)$

Clause Logic

- A literal is either an atom or the negation of an atom. Example: $A, \neg A$

Propositional Logic

Syntax

- Propositional variables (aka (propositional) atoms) A, B, C
- Boolean connectives \neg (negation), \wedge (and), \vee (or), \Rightarrow (implication)
- Parenthesis (and)
- A formula is either an atom or some formulas combined with a connective in the proper way. Example: $(A \Rightarrow B) \Rightarrow (B \vee \neg A)$

Clause Logic

- A literal is either an atom or the negation of an atom. Example: $A, \neg A$
- A clause is a (possibly empty) disjunction of literals.
Example: $\neg B \vee C \vee \neg D$

Propositional Logic

Syntax

- **Propositional variables** (aka **(propositional) atoms**) A, B, C
- **Boolean connectives** \neg (negation), \wedge (and), \vee (or), \Rightarrow (implication)
- Parenthesis (and)
- A **formula** is either an atom or some formulas combined with a connective in the proper way. Example: $(A \Rightarrow B) \Rightarrow (B \vee \neg A)$

Clause Logic

- A **literal** is either an atom or the negation of an atom. Example: $A, \neg A$
- A **clause** is a (possibly empty) disjunction of literals.
Example: $\neg B \vee C \vee \neg D$
- A formula is in **clause normal form**, or **conjunctive normal form (CNF)** iff it is a conjunction of clauses. Example: $(\neg A \vee B) \wedge A \wedge (\neg B \vee C \vee \neg D)$

Propositional Logic

Syntax

- **Propositional variables** (aka **(propositional) atoms**) A, B, C
- **Boolean connectives** \neg (negation), \wedge (and), \vee (or), \Rightarrow (implication)
- Parenthesis (and)
- A **formula** is either an atom or some formulas combined with a connective in the proper way. Example: $(A \Rightarrow B) \Rightarrow (B \vee \neg A)$

Clause Logic

- A **literal** is either an atom or the negation of an atom. Example: $A, \neg A$
- A **clause** is a (possibly empty) disjunction of literals.
Example: $\neg B \vee C \vee \neg D$
- A formula is in **clause normal form**, or **conjunctive normal form (CNF)** iff it is a conjunction of clauses. Example: $(\neg A \vee B) \wedge A \wedge (\neg B \vee C \vee \neg D)$
- **Most theorem proving methods work with clause logic**
Every formula can be transformed into an equivalent CNF

Propositional Logic

Semantics

Propositional Logic

Semantics

- An **interpretation** I maps every atom to a truth value *True* or *False*

Often I is specified by the set of *True* atoms. Example: if $I = \{A, C, D\}$ then $I(A) = I(C) = I(D) = \text{True}$ and all other atoms are *False*

Propositional Logic

Semantics

- An **interpretation** I maps every atom to a truth value *True* or *False*

Often I is specified by the set of *True* atoms. Example: if $I = \{A, C, D\}$ then $I(A) = I(C) = I(D) = \text{True}$ and all other atoms are *False*

- The semantics of the connectives is fixed by the usual truth tables

Propositional Logic

Semantics

- An **interpretation** I maps every atom to a truth value *True* or *False*

Often I is specified by the set of *True* atoms. Example: if $I = \{A, C, D\}$ then $I(A) = I(C) = I(D) = \text{True}$ and all other atoms are *False*

- The semantics of the connectives is fixed by the usual truth tables
- Every interpretation I extends to a mapping of formulas to truth values by way of recursion and using the semantics of the connectives.

We identify I with this extension. Example: $I(A \wedge (\neg C \vee B)) = \text{False}$

Notation: $I \models F$ iff $I(F) = \text{True}$ (I **satisfies** F , I is a **model** of F)

Propositional Logic

Semantics

- An **interpretation** I maps every atom to a truth value *True* or *False*

Often I is specified by the set of *True* atoms. Example: if $I = \{A, C, D\}$ then $I(A) = I(C) = I(D) = \text{True}$ and all other atoms are *False*

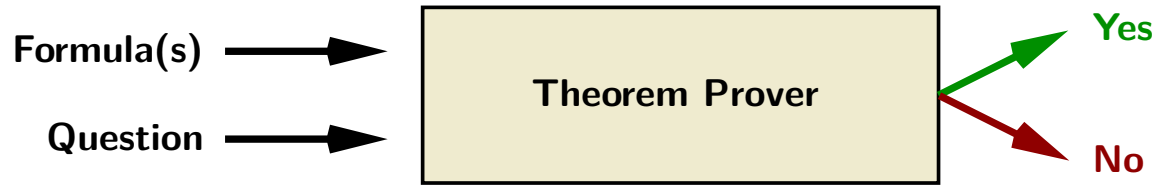
- The semantics of the connectives is fixed by the usual truth tables
- Every interpretation I extends to a mapping of formulas to truth values by way of recursion and using the semantics of the connectives.

We identify I with this extension. Example: $I(A \wedge (\neg C \vee B)) = \text{False}$

Notation: $I \models F$ iff $I(F) = \text{True}$ (I **satisfies** F , I is a **model** of F)

- A formula F is
 - **satisfiable** iff it has a model
 - **unsatisfiable** iff it has no model
 - **valid** iff every interpretation is a model of F
 - **entailed** by a set of formulas M iff every model of every formula in M is a model of F . Notation: $M \models F$

Propositional SAT Solving



Formula: Propositional logic formula ϕ

Question: Is ϕ satisfiable?

(Minimal model? Maximal consistent subsets?)

Theorem Prover:

- Stochastic local search (not covered here)
- DPLL: Davis-Putnam-Logemann-Loveland method, historic (1960s),
one component of current CDCL methods
- CDCL: Conflict-Driven Clause Learning

Problem: the formula ϕ can be **BIG**

DPLL as a Semantic Tree Method

$$(1) A \vee B \quad (2) C \vee \neg A \quad (3) D \vee \neg C \vee \neg A \quad (4) \neg D \vee \neg B$$

$\langle \text{empty tree} \rangle$

$$\{\} \not\models A \vee B$$

$$\{\} \models C \vee \neg A$$

$$\{\} \models D \vee \neg C \vee \neg A$$

$$\{\} \models \neg D \vee \neg B$$

- A Branch stands for an interpretation
- **Purpose of splitting:** satisfy a clause that is currently falsified
- Close branch if some clause is plainly falsified by it (\star)

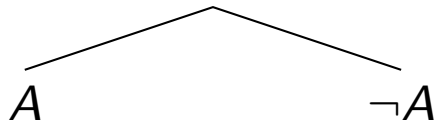
DPLL as a Semantic Tree Method

$$(1) A \vee B$$

$$(2) C \vee \neg A$$

$$(3) D \vee \neg C \vee \neg A$$

$$(4) \neg D \vee \neg B$$



$$\{A\} \models A \vee B$$

$$\{A\} \not\models C \vee \neg A$$

$$\{A\} \models D \vee \neg C \vee \neg A$$

$$\{A\} \models \neg D \vee \neg B$$

- A Branch stands for an interpretation
- **Purpose of splitting:** satisfy a clause that is currently falsified
- Close branch if some clause is plainly falsified by it (\star)

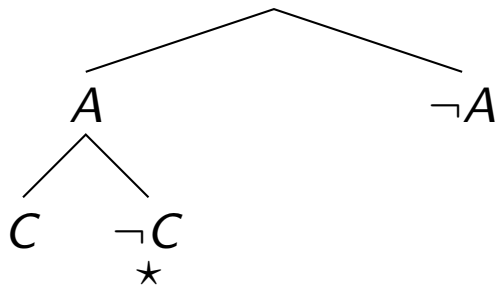
DPLL as a Semantic Tree Method

$$(1) A \vee B$$

$$(2) C \vee \neg A$$

$$(3) D \vee \neg C \vee \neg A$$

$$(4) \neg D \vee \neg B$$



$$\{A, C\} \models A \vee B$$

$$\{A, C\} \models C \vee \neg A$$

$$\{A, C\} \not\models D \vee \neg C \vee \neg A$$

$$\{A, C\} \models \neg D \vee \neg B$$

- A Branch stands for an interpretation
- **Purpose of splitting:** satisfy a clause that is currently falsified
- Close branch if some clause is plainly falsified by it (★)

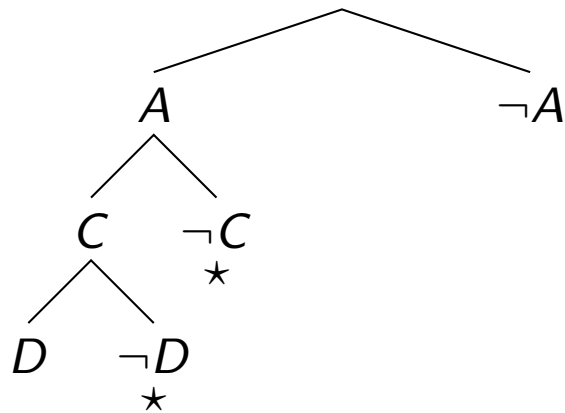
DPLL as a Semantic Tree Method

$$(1) A \vee B$$

$$(2) C \vee \neg A$$

$$(3) D \vee \neg C \vee \neg A$$

$$(4) \neg D \vee \neg B$$



$$\{A, C, D\} \models A \vee B$$

$$\{A, C, D\} \models C \vee \neg A$$

$$\{A, C, D\} \models D \vee \neg C \vee \neg A$$

$$\{A, C, D\} \models \neg D \vee \neg B$$

Model $\{A, C, D\}$ found.

- A Branch stands for an interpretation
- **Purpose of splitting:** satisfy a clause that is currently falsified
- Close branch if some clause is plainly falsified by it (★)

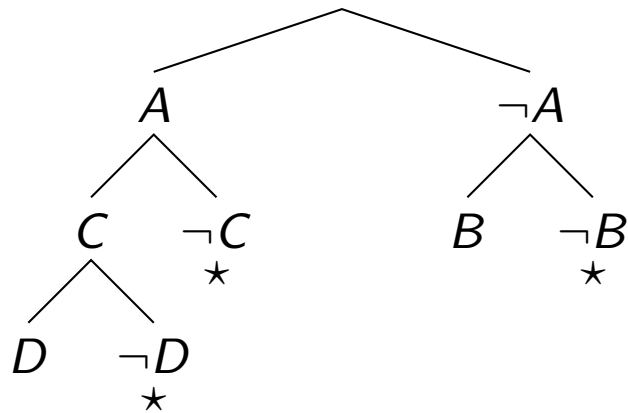
DPLL as a Semantic Tree Method

(1) $A \vee B$

(2) $C \vee \neg A$

(3) $D \vee \neg C \vee \neg A$

(4) $\neg D \vee \neg B$



$$\{B\} \models A \vee B$$

$$\{B\} \models C \vee \neg A$$

$$\{B\} \models D \vee \neg C \vee \neg A$$

$$\{B\} \models \neg D \vee \neg B$$

Model $\{B\}$ found.

- A Branch stands for an interpretation
- **Purpose of splitting:** satisfy a clause that is currently falsified
- Close branch if some clause is plainly falsified by it (★)

DPLL Pseudocode

literal L : a variable A or its negation $\neg A$

clause: a set of literals, e.g., $\{A, \neg B, C\}$, connected by “or”

```
function DPLL( $N$ )    %%  $N$  is a set of clauses, connected by "and"
    while  $N$  contains a unit clause  $\{L\}$ 
         $N := \text{simplify}(N, L)$ ;
    if  $N = \{\}$  then return true;
    if  $\{\} \in N$  then return false;
     $L := \text{choose-literal}(N)$ ;
    if DPLL( $\text{simplify}(N, L)$ ) then return true;
    else return DPLL( $\text{simplify}(N, \neg L)$ );

function  $\text{simplify}(N, L)$     %% also called unit propagation
    remove all clauses from  $N$  that contain  $L$ ;
    delete  $\neg L$  from all remaining clauses;
    return the resulting clause set;
```

Making DPLL Fast – Overview

Conflict Driven Clause Learning (CDCL) solvers extend DPLL:

Lemma learning: add new clauses to the clause set as branches get closed (“conflict driven”)

Goal: reuse information that is obtained in one branch for subsequent derivation steps.

Backtracking: replace chronological backtracking by “dependency-directed backtracking”, aka “backjumping”: on backtracking, skip splits that are not necessary to close a branch

Randomized restarts: every now and then start over, with learned clauses

Variable selection heuristics: what literal to split on. E.g., use literals that occur often

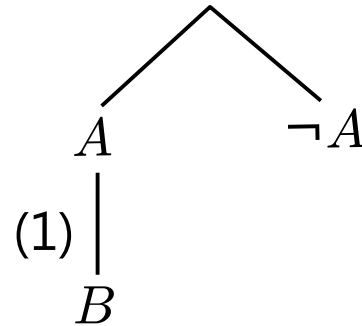
Make unit-propagation fast: 2-watched literal technique

Lemma Learning

"Avoid making the same mistake twice"

$$\begin{array}{ll} \dots & \\ B \vee \neg A & (1) \\ D \vee \neg C & (2) \\ \neg D \vee \neg B \vee \neg C & (3) \end{array}$$

w/o Lemma

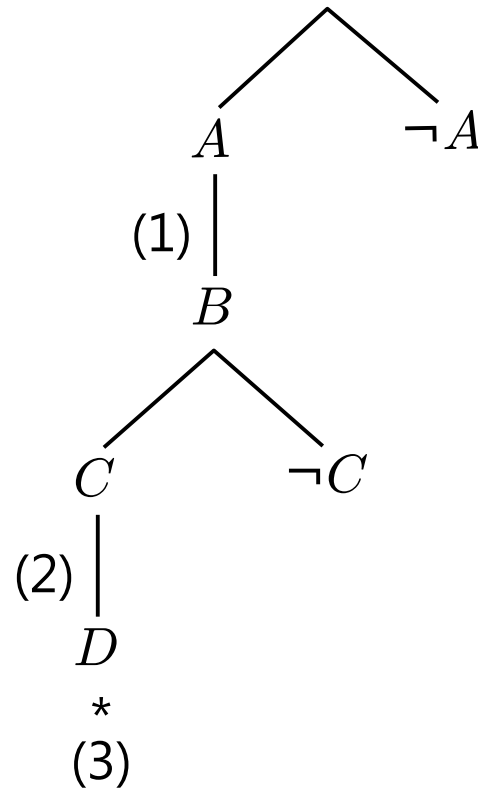


Lemma Learning

"Avoid making the same mistake twice"

$$\begin{array}{ll} \dots & \\ B \vee \neg A & (1) \\ D \vee \neg C & (2) \\ \neg D \vee \neg B \vee \neg C & (3) \end{array}$$

w/o Lemma

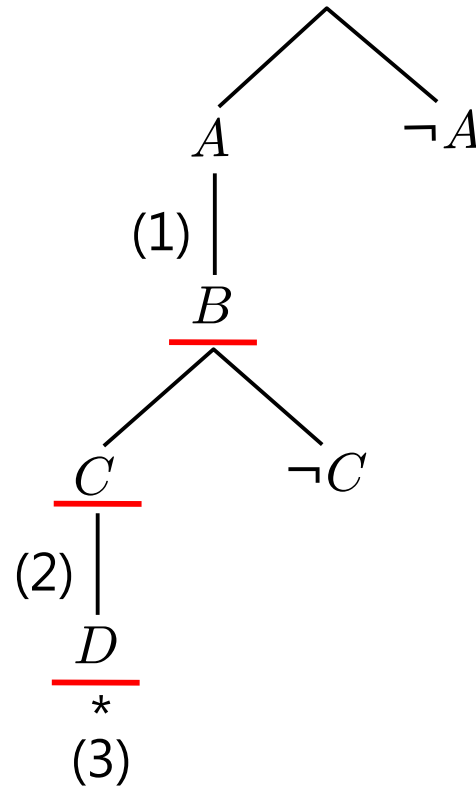


Lemma Learning

"Avoid making the
same mistake twice"

$$\begin{array}{ll} \dots & \\ B \vee \neg A & (1) \\ D \vee \neg C & (2) \\ \underline{\neg D} \vee \underline{\neg B} \vee \underline{\neg C} & (3) \end{array}$$

w/o Lemma



Lemma Learning

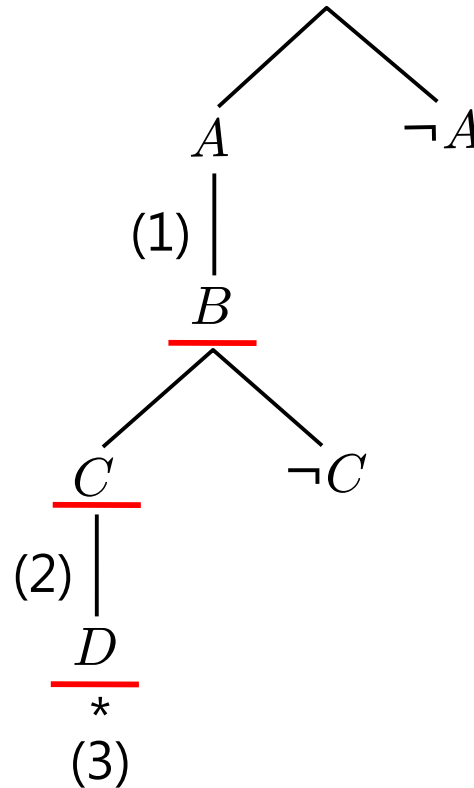
"Avoid making the same mistake twice"

$$\begin{array}{ll} \dots & \\ B \vee \neg A & (1) \\ D \vee \neg C & (2) \\ \underline{\neg D} \vee \underline{\neg B} \vee \underline{\neg C} & (3) \end{array}$$

Lemma Candidates
by Resolution:

$$\underline{\neg D} \vee \neg B \vee \neg C$$

w/o Lemma



Lemma Learning

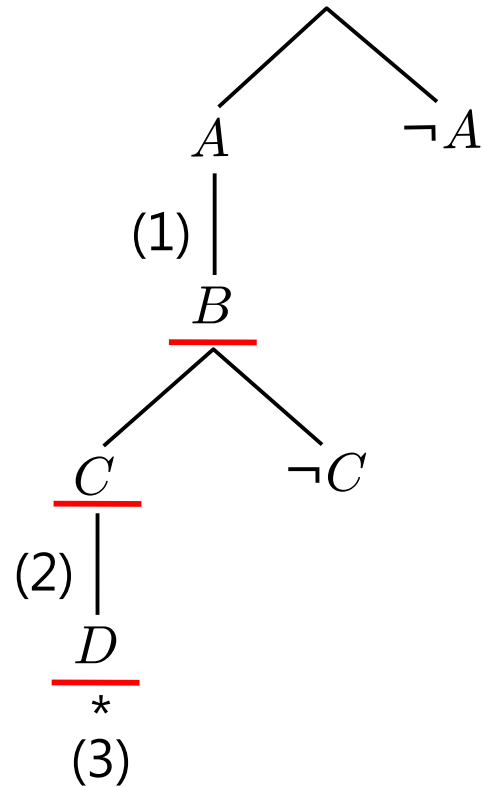
"Avoid making the same mistake twice"

$$\begin{array}{ll} \dots & \\ B \vee \neg A & (1) \\ D \vee \neg C & (2) \\ \underline{\neg D} \vee \underline{\neg B} \vee \underline{\neg C} & (3) \end{array}$$

Lemma Candidates
by Resolution:

$$\frac{\underline{\neg D} \vee \neg B \vee \neg C \quad D \vee \neg C}{\underline{\neg B} \vee \neg C}$$

w/o Lemma



Lemma Learning

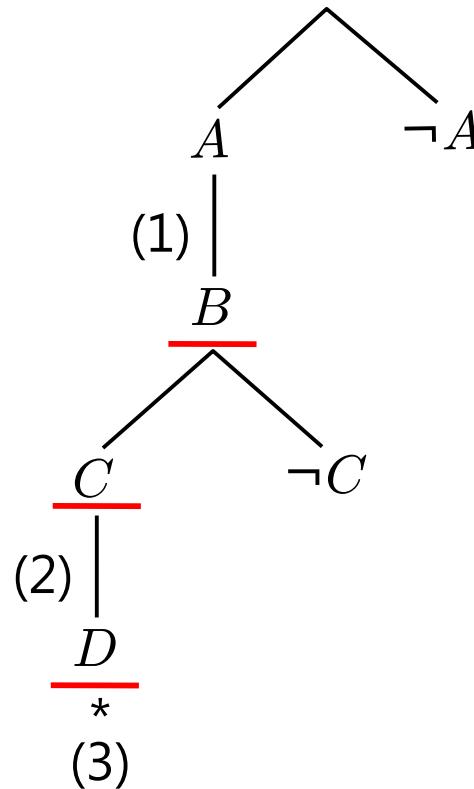
"Avoid making the same mistake twice"

$$\begin{array}{ll} \dots & \\ B \vee \neg A & (1) \\ D \vee \neg C & (2) \\ \underline{\neg D} \vee \underline{\neg B} \vee \underline{\neg C} & (3) \end{array}$$

Lemma Candidates
by Resolution:

$$\begin{array}{rcl} \underline{\neg D} \vee \neg B \vee \neg C & D \vee \neg C & \\ \hline & \underline{\neg B} \vee \neg C & B \vee \neg A \\ & \hline & \underline{\neg C} \vee \neg A \end{array}$$

w/o Lemma



Lemma Learning

"Avoid making the same mistake twice"

...

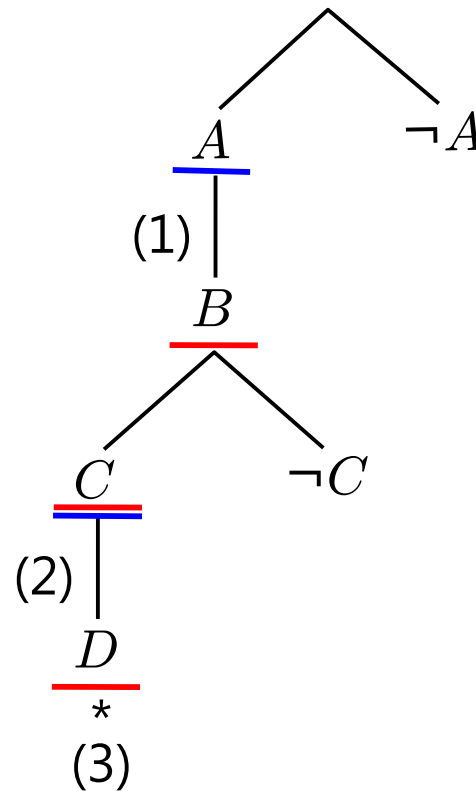
| | |
|--|-----|
| $B \vee \neg A$ | (1) |
| $D \vee \neg C$ | (2) |
| <u>$\neg D \vee \neg B \vee \neg C$</u> | (3) |

**Lemma Candidates
by Resolution:**

| | |
|--|-----------------------------------|
| <u>$\neg D \vee \neg B \vee \neg C$</u> | <u>$D \vee \neg C$</u> |
| <hr/> | |
| <u>$\neg B \vee \neg C$</u> | <u>$B \vee \neg A$</u> |
| <hr/> | |
| <u><u>$\neg C \vee \neg A$</u></u> | |

w/o Lemma

With Lemma



Lemma Learning

"Avoid making the same mistake twice"

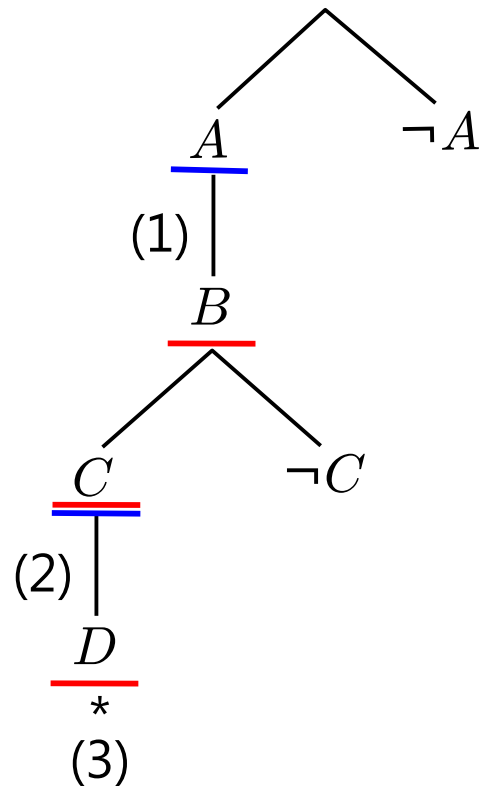
...

| | |
|--|-----|
| $B \vee \neg A$ | (1) |
| $D \vee \neg C$ | (2) |
| <u>$\neg D \vee \neg B \vee \neg C$</u> | (3) |

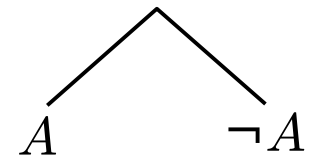
Lemma Candidates
by Resolution:

| | |
|--|-----------------|
| <u>$\neg D \vee \neg B \vee \neg C$</u> | $D \vee \neg C$ |
| <hr/> | |
| $\neg B \vee \neg C$ | $B \vee \neg A$ |
| <hr/> | |
| <u>$\neg C \vee \neg A$</u> | |

w/o Lemma



With Lemma



Lemma Learning

"Avoid making the same mistake twice"

...

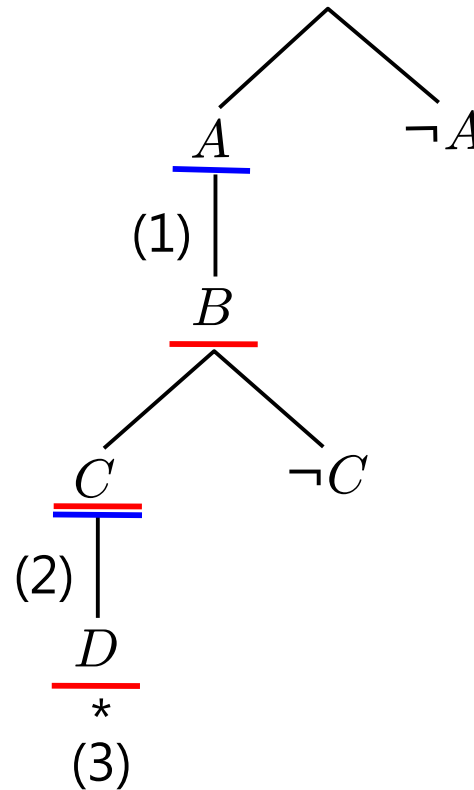
| | |
|--|-----|
| $B \vee \neg A$ | (1) |
| $D \vee \neg C$ | (2) |
| <u>$\neg D \vee \neg B \vee \neg C$</u> | (3) |

Lemma Candidates

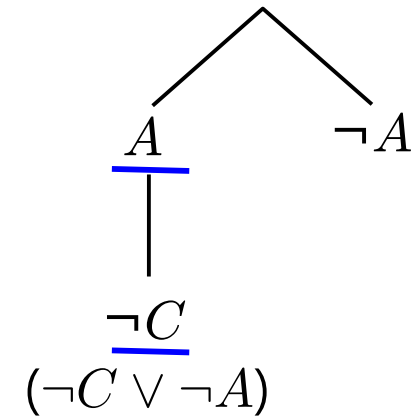
by Resolution:

| | |
|--|-----------------|
| $\neg D \vee \neg B \vee \neg C$ | $D \vee \neg C$ |
| <hr/> | |
| $\neg B \vee \neg C$ | $B \vee \neg A$ |
| <hr/> | |
| <u>$\neg C \vee \neg A$</u> | |

w/o Lemma



With Lemma



Making DPLL Fast

2-watched literal technique

A technique to implement unit propagation efficiently.

- In each clause, select two (currently undefined) “watched” literals.
- For each variable A , keep a list of all clauses in which A is watched and a list of all clauses in which $\neg A$ is watched.
- If an undefined variable is set to 0 (or to 1), check all clauses in which A (or $\neg A$) is watched and watch another literal (that is true or undefined) in this clause if possible.
- As long as there are two watched literals in a n -literal clause, this clause cannot be used for unit propagation, because $n - 1$ of its literals have to be false to provide a unit conclusion.
- Important: Watched literal information need not be restored upon backtracking.

Further Information

The ideas described so far have been implemented in the SAT checker **zChaff**:
Lintao Zhang and Sharad Malik. The Quest for Efficient Boolean Satisfiability Solvers, Proc. CADE-18, LNAI 2392, pp. 295–312, Springer, 2002.

Other Overviews

Robert Nieuwenhuis, Albert Oliveras, Cesare Tinelli. Solving SAT and SAT Modulo Theories: From an abstract Davis-Putnam-Logemann-Loveland procedure to DPLL(T), pp 937–977, Journal of the ACM, 53(6), 2006.

Armin Biere and Marijn Heule and Hans van Maaren and Toby Walsh. Handbook of Satisfiability, IOS Press, 2009.

Contents

Introduction

Logics and Reasoning Service (already done)

Methods for Automated Theorem Proving

Overview of some widely used general methods

- Propositional SAT solving
- First-order logic and clause normal forms
- Proof Procedures Based on Herbrand's Theorem
- The Resolution calculus
- Instance-based methods
- Model generation

Theory Reasoning

Methods to reason with specific background theories

- Paramodulation (Equality)
- Satisfiability Modulo Theories (SMT)
- Quantifier elimination for linear real arithmetic
- Combining multiple theories

First-Order Logic Quiz

A_1 : Socrates is a human

A_2 : All humans are mortal

Translation into first-order logic:

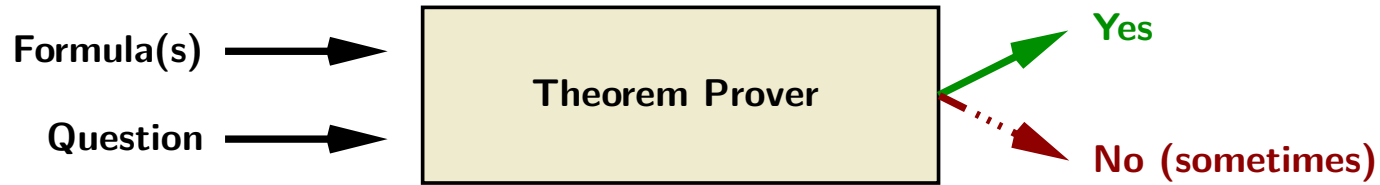
A_1 : $human(socrates)$

A_2 : $\forall x (human(x) \rightarrow mortal(x))$

Which of the following (non-)entailment statements hold true?

1. $\{A_1, A_2\} \models mortal(socrates)$
2. $\{A_1, A_2\} \models mortal(apollo)$
3. $\{A_1, A_2\} \not\models mortal(socrates)$
4. $\{A_1, A_2\} \not\models mortal(apollo)$
5. $\{A_1, A_2\} \models \neg mortal(socrates)$
6. $\{A_1, A_2\} \models \neg mortal(apollo)$

First-Order Logic Reasoning Services



Formula: First-order logic formula ϕ (e.g. the n-queens formulas above)

Usually with equality =

Sometimes from syntactically restricted fragment (e.g., Description logics)

Question: Is ϕ formula valid? (satisfiable?, entailed by another formula?)

Calculi: Superposition (Resolution), Instance-based methods, Tableaux, ...

Issues

- Efficient treatment of equality
- Decision procedure for sub-languages or useful reductions?
- Built-in inference rules for arrays, lists, arithmetics (still open research)

First-Order Logic

“The function f is continuous”, expressed in (first-order) predicate logic:

$$\forall \varepsilon (0 < \varepsilon \rightarrow \forall a \exists \delta (0 < \delta \wedge \forall x (|x - a| < \delta \rightarrow |f(x) - f(a)| < \varepsilon)))$$

Underlying Language

Variables $\varepsilon, a, \delta, x$

Function symbols $0, | _ |, _ - _, f(_)$

Terms are well-formed expressions over variables and function symbols

Predicate symbols $_ < _, _ = _$

Atoms are applications of predicate symbols to terms

Boolean connectives $\wedge, \vee, \rightarrow, \neg$

Quantifiers \forall, \exists

The function symbols and predicate symbols comprise a signature Σ

First-Order Logic

“The function f is continuous”, expressed in (first-order) predicate logic:

$$\forall \varepsilon (0 < \varepsilon \rightarrow \forall a \exists \delta (0 < \delta \wedge \forall x (|x - a| < \delta \rightarrow |f(x) - f(a)| < \varepsilon)))$$

Semantics: $(\Sigma-)$ Algebras, or $(\Sigma-)$ Interpretations

Universe (aka Domain): Set U

Variables \mapsto values in U (mapping is called “assignment”)

Function symbols \mapsto (total) functions over U

Predicate symbols \mapsto relations over U

Boolean connectives \mapsto the usual boolean functions

Quantifiers \mapsto “for all ... holds”, “there is a ..., such that”

Terms \mapsto values in U

Formulas \mapsto Boolean (Truth-) values

Semantics - Example

Let Σ_{PA} be the standard signature of Peano Arithmetic

The standard interpretation \mathbb{N} for Peano Arithmetic then is:

$$U_{\mathbb{N}} = \{0, 1, 2, \dots\}$$

$$0_{\mathbb{N}} : 0$$

$$s_{\mathbb{N}} : n \mapsto n + 1$$

$$+_{\mathbb{N}} : (n, m) \mapsto n + m$$

$$*_{\mathbb{N}} : (n, m) \mapsto n * m$$

$$\leq_{\mathbb{N}} = \{(n, m) \mid n \text{ less than or equal to } m\}$$

$$<_{\mathbb{N}} = \{(n, m) \mid n \text{ less than } m\}$$

Note that \mathbb{N} is just one out of **many possible** Σ_{PA} -interpretations

Semantics - Example

Evaluation of terms and formulas

Under the interpretation \mathbb{N} and the assignment $\beta : x \mapsto 1, y \mapsto 3$ (to evaluate the free variables) we obtain

$$(\mathbb{N}, \beta)(s(x) + s(0)) = 3$$

$$(\mathbb{N}, \beta)(x + y \doteq s(y)) = \text{True}$$

$$(\mathbb{N}, \beta)(\forall z \, z \leq y) = \text{False}$$

$$(\mathbb{N}, \beta)(\forall x \exists y \, x < y) = \text{True}$$

$$\mathbb{N}(\forall x \exists y \, x < y) = \text{True} \quad (\text{Short notation when } \beta \text{ irrelevant})$$

Important Basic Notion: Model

If ϕ is a closed formula, then, instead of $I(\phi) = \text{True}$ one writes

$$I \models \phi \quad (\text{"I is a model of } \phi \text{"})$$

E.g. $\mathbb{N} \models \forall x \exists y \, x < y$

Reasoning Services Semantically

E.g. “entailment”:

Axioms over $\mathbb{R} \wedge \text{continuous}(f) \wedge \text{continuous}(g) \models \text{continuous}(f + g) ?$

Model(I, ϕ): $I \models \phi ?$ (Is I a model for ϕ ?)

Validity(ϕ): $\models \phi ?$ ($I \models \phi$ for every interpretation?)

Satisfiability(ϕ): ϕ satisfiable? ($I \models \phi$ for some interpretation?)

Entailment(ϕ, ψ): $\phi \models \psi ?$ (does ϕ entail ψ ?, i.e.
for every interpretation I : if $I \models \phi$ then $I \models \psi$?)

Solve(I, ϕ): find an assignment β such that $(I, \beta)(\phi) = \text{True}$
(ϕ is not closed)

Solve(ϕ): find an interpretation and assignment β such that $(I, \beta)(\phi) = \text{True}$
(ϕ is not closed)

Additional complication: fix interpretation of some symbols (as in \mathbb{N} above)

Reasoning Services Semantically

E.g. “entailment”:

Axioms over $\mathbb{R} \wedge \text{continuous}(f) \wedge \text{continuous}(g) \models \text{continuous}(f + g) ?$

Model(I, ϕ): $I \models \phi ?$ (Is I a model for ϕ ?)

Validity(ϕ): $\models \phi ?$ ($I \models \phi$ for every interpretation?)

Satisfiability(ϕ): ϕ satisfiable? ($I \models \phi$ for some interpretation?)

Entailment(ϕ, ψ): $\phi \models \psi ?$ (does ϕ entail ψ ?, i.e.
for every interpretation I : if $I \models \phi$ then $I \models \psi$?)

Solve(I, ϕ): find an assignment β such that $(I, \beta)(\phi) = \text{True}$
(ϕ is not closed)

Solve(ϕ): find an interpretation and assignment β such that $(I, \beta)(\phi) = \text{True}$
(ϕ is not closed)

Additional complication: fix interpretation of some symbols (as in \mathbb{N} above)

| |
|---|
| In the following focus on “entailment” |
|---|

Reduction of Entailment to Unsatisfiability

- Suppose we want to prove an entailment $\phi \models \psi$

Reduction of Entailment to Unsatisfiability

- Suppose we want to prove an entailment $\phi \models \psi$
- Equivalently, prove $\models \phi \rightarrow \psi$, i.e. that $\phi \rightarrow \psi$ is valid

Reduction of Entailment to Unsatisfiability

- Suppose we want to prove an entailment $\phi \models \psi$
- Equivalently, prove $\models \phi \rightarrow \psi$, i.e. that $\phi \rightarrow \psi$ is valid
- Equivalently, prove that $\neg(\phi \rightarrow \psi)$ is not satisfiable (unsatisfiable)

Reduction of Entailment to Unsatisfiability

- Suppose we want to prove an entailment $\phi \models \psi$
- Equivalently, prove $\models \phi \rightarrow \psi$, i.e. that $\phi \rightarrow \psi$ is valid
- Equivalently, prove that $\neg(\phi \rightarrow \psi)$ is not satisfiable (unsatisfiable)
- Equivalently, prove that $\phi \wedge \neg\psi$ is unsatisfiable

Reduction of Entailment to Unsatisfiability

- Suppose we want to prove an entailment $\phi \models \psi$
- Equivalently, prove $\models \phi \rightarrow \psi$, i.e. that $\phi \rightarrow \psi$ is valid
- Equivalently, prove that $\neg(\phi \rightarrow \psi)$ is not satisfiable (unsatisfiable)
- Equivalently, prove that $\phi \wedge \neg\psi$ is unsatisfiable

Basis for (predominant) refutational theorem proving

Reduction of Entailment to Unsatisfiability

- Suppose we want to prove an entailment $\phi \models \psi$
- Equivalently, prove $\models \phi \rightarrow \psi$, i.e. that $\phi \rightarrow \psi$ is valid
- Equivalently, prove that $\neg(\phi \rightarrow \psi)$ is not satisfiable (unsatisfiable)
- Equivalently, prove that $\phi \wedge \neg\psi$ is unsatisfiable

Basis for (predominant) refutational theorem proving

Dual problem, much harder: to disprove an entailment $\phi \models \psi$ find a model of $\phi \wedge \neg\psi$

One motivation for (finite) model generation procedures

Normal Forms

Most first-order theorem provers take formulas in **clause normal form**

Why Normal Forms?

- Reduction of logical concepts (operators, quantifiers)
- Reduction of syntactical structure (nesting of subformulas)
- Can be exploited for efficient data structures and control

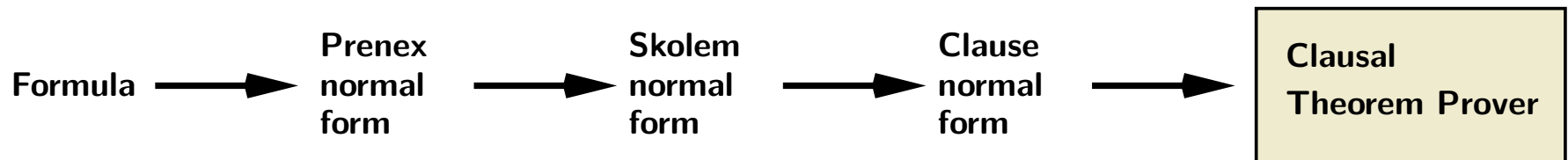
Normal Forms

Most first-order theorem provers take formulas in **clause normal form**

Why Normal Forms?

- Reduction of logical concepts (operators, quantifiers)
- Reduction of syntactical structure (nesting of subformulas)
- Can be exploited for efficient data structures and control

Translation into Clause Normal Form



Prop: the given formula and its clause normal form are equi-satisfiable

Prenex Normal Form

Prenex formulas have the form

$$Q_1 x_1 \dots Q_n x_n F,$$

where F is quantifier-free and $Q_i \in \{\forall, \exists\}$

Prenex Normal Form

Prenex formulas have the form

$$Q_1 x_1 \dots Q_n x_n F,$$

where F is quantifier-free and $Q_i \in \{\forall, \exists\}$

Computing prenex normal form by the rewrite relation \Rightarrow_P :

$$(F \leftrightarrow G) \Rightarrow_P (F \rightarrow G) \wedge (G \rightarrow F)$$

$$\neg Qx F \Rightarrow_P \overline{Q}x \neg F \quad (\neg Q)$$

$$(Qx F \rho G) \Rightarrow_P Qy (F[y/x] \rho G), \text{ } y \text{ fresh, } \rho \in \{\wedge, \vee\}$$

$$(Qx F \rightarrow G) \Rightarrow_P \overline{Q}y (F[y/x] \rightarrow G), \text{ } y \text{ fresh}$$

$$(F \rho Qx G) \Rightarrow_P Qy (F \rho G[y/x]), \text{ } y \text{ fresh, } \rho \in \{\wedge, \vee, \rightarrow\}$$

Here \overline{Q} denotes the quantifier **dual** to Q , i.e., $\overline{\forall} = \exists$ and $\overline{\exists} = \forall$.

In the Example

$$\forall \varepsilon (0 < \varepsilon \rightarrow \forall a \exists \delta (0 < \delta \wedge \forall x (|x - a| < \delta \rightarrow |f(x) - f(a)| < \varepsilon)))$$

$$\Rightarrow_P$$

$$\forall \varepsilon \forall a (0 < \varepsilon \rightarrow \exists \delta (0 < \delta \wedge \forall x (|x - a| < \delta \rightarrow |f(x) - f(a)| < \varepsilon)))$$

$$\Rightarrow_P$$

$$\forall \varepsilon \forall a \exists \delta (0 < \varepsilon \rightarrow 0 < \delta \wedge \forall x (|x - a| < \delta \rightarrow |f(x) - f(a)| < \varepsilon))$$

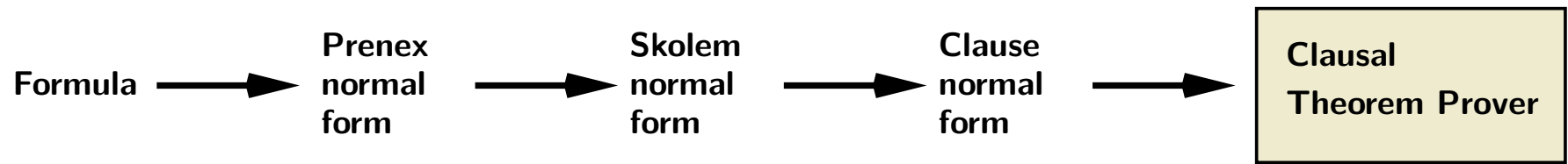
$$\Rightarrow_P$$

$$\forall \varepsilon \forall a \exists \delta (0 < \varepsilon \rightarrow \forall x (0 < \delta \wedge |x - a| < \delta \rightarrow |f(x) - f(a)| < \varepsilon))$$

$$\Rightarrow_P$$

$$\forall \varepsilon \forall a \exists \delta \forall x (0 < \varepsilon \rightarrow (0 < \delta \wedge (|x - a| < \delta \rightarrow |f(x) - f(a)| < \varepsilon)))$$

Skolem Normal Form



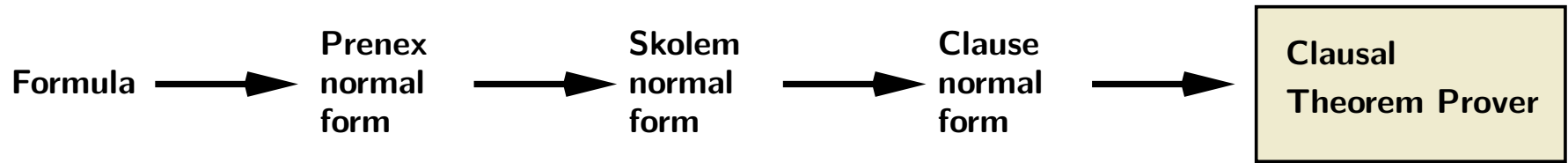
Intuition: replacement of $\exists y$ by a concrete choice function computing y from all the arguments y depends on.

Transformation \Rightarrow_S

$$\forall x_1, \dots, x_n \exists y F \Rightarrow_S \forall x_1, \dots, x_n F[f(x_1, \dots, x_n)/y]$$

where f/n is a new function symbol (**Skolem function**).

Skolem Normal Form



Intuition: replacement of $\exists y$ by a concrete choice function computing y from all the arguments y depends on.

Transformation \Rightarrow_S

$$\forall x_1, \dots, x_n \exists y F \Rightarrow_S \forall x_1, \dots, x_n F[f(x_1, \dots, x_n)/y]$$

where f/n is a new function symbol (**Skolem function**).

In the Example

$$\forall \varepsilon \forall a \exists \delta \forall x (0 < \varepsilon \rightarrow 0 < \delta \wedge (|x - a| < \delta \rightarrow |f(x) - f(a)| < \varepsilon))$$

\Rightarrow_S

$$\forall \varepsilon \forall a \forall x (0 < \varepsilon \rightarrow 0 < d(\varepsilon, a) \wedge (|x - a| < d(\varepsilon, a) \rightarrow |f(x) - f(a)| < \varepsilon))$$

Clausal Normal Form (Conjunctive Normal Form)

Rules to convert the matrix of the formula in Skolem normal form into a conjunction of disjunctions of literals:

$$\begin{array}{ll} (F \leftrightarrow G) & \Rightarrow_K (F \rightarrow G) \wedge (G \rightarrow F) \\ (F \rightarrow G) & \Rightarrow_K (\neg F \vee G) \\ \neg(F \vee G) & \Rightarrow_K (\neg F \wedge \neg G) \\ \neg(F \wedge G) & \Rightarrow_K (\neg F \vee \neg G) \\ \neg\neg F & \Rightarrow_K F \\ (F \wedge G) \vee H & \Rightarrow_K (F \vee H) \wedge (G \vee H) \\ (F \wedge \top) & \Rightarrow_K F \\ (F \wedge \perp) & \Rightarrow_K \perp \\ (F \vee \top) & \Rightarrow_K \top \\ (F \vee \perp) & \Rightarrow_K F \end{array}$$

They are to be applied modulo commutativity of \wedge and \vee

In the Example

$$\forall \varepsilon \forall a \forall x (0 < \varepsilon \rightarrow 0 < d(\varepsilon, a) \wedge (|x - a| < d(\varepsilon, a) \rightarrow |f(x) - f(a)| < \varepsilon))$$

$$\Rightarrow_K$$

$$0 < d(\varepsilon, a) \vee \neg(0 < \varepsilon)$$

$$\neg(|x - a| < d(\varepsilon, a)) \vee |f(x) - f(a)| < \varepsilon \vee \neg(0 < \varepsilon)$$

Note: The universal quantifiers for the variables ε , a and x , as well as the conjunction symbol \wedge between the clauses are not written, for convenience

The Complete Picture

$$F \Rightarrow_P^* Q_1 y_1 \dots Q_n y_n G \quad (G \text{ quantifier-free})$$

$$\Rightarrow_S^* \forall x_1, \dots, x_m H \quad (m \leq n, H \text{ quantifier-free})$$

$$\Rightarrow_K^* \underbrace{\forall x_1, \dots, x_m}_{\text{leave out}} \bigwedge_{i=1}^k \underbrace{\bigvee_{j=1}^{n_i} L_{ij}}_{\text{clauses } C_i}$$

Notions

An **atom** is the (arity respecting) application of a predicate symbol to some terms. A **literal** L is an atom or a negated atom. A **clause** is a disjunction of literals $L_1 \vee \dots \vee L_n$, where $n \geq 0$. The empty clause is written as \square . A **clause set** is a set of clauses, The set $N = \{C_1, \dots, C_k\}$ is called the **clausal (normal) form** (CNF) of F .

Note: Variables in clauses are implicitly universally quantified

Where are we?

Instead of showing that a formula F is unsatisfiable, the proof problem from now is to show that its CNF N is unsatisfiable

A CNF provides a simple syntactic structure, but does not give a clue how to prove unsatisfiability. The naive approach of “checking all interpretations” does not work: In general, there are infinitely many, even uncountably many interpretations for a signature Σ .

So how to do that? “Herbrand theory” provides the answer

Contents

Introduction

Logics and Reasoning Service (already done)

Methods for Automated Theorem Proving

Overview of some widely used general methods

- Propositional SAT solving
- First-order logic and clause normal forms
- Proof Procedures Based on Herbrand's Theorem
- The Resolution calculus
- Instance-based methods
- Model generation

Theory Reasoning

Methods to reason with specific background theories

- Paramodulation (Equality)
- Satisfiability Modulo Theories (SMT)
- Quantifier elimination for linear real arithmetic
- Combining multiple theories

Proof Procedures Based on Herbrand's Theorem

Proving unsatisfiability of a clause set becomes feasible (semi-decidable) by working with the set of its **ground instances** instead. Plan of attack:

Definition: A **ground instance** of a clause is obtained by replacing each of its variables by some variable-free term (“ground term”)

Proof Procedures Based on Herbrand's Theorem

Proving unsatisfiability of a clause set becomes feasible (semi-decidable) by working with the set of its **ground instances** instead. Plan of attack:

Definition: A **ground instance** of a clause is obtained by replacing each of its variables by some variable-free term (“ground term”)

Proposition (Herbrand): Let N be a clause set and N^{gr} be the set of all ground instances of all clauses in N .

N is unsatisfiable iff N^{gr} is unsatisfiable wrt. Herbrand interpretations
(essentially: propositional-logic unsatisfiable)

Proof Procedures Based on Herbrand's Theorem

Proving unsatisfiability of a clause set becomes feasible (semi-decidable) by working with the set of its **ground instances** instead. Plan of attack:

Definition: A **ground instance** of a clause is obtained by replacing each of its variables by some variable-free term (“ground term”)

Proposition (Herbrand): Let N be a clause set and N^{gr} be the set of all ground instances of all clauses in N .

N is unsatisfiable iff N^{gr} is unsatisfiable wrt. Herbrand interpretations
(essentially: propositional-logic unsatisfiable)

Proposition (compactness): N^{gr} is unsatisfiable wrt. Herbrand interpretations iff
some finite subset $M \subseteq N^{\text{gr}}$ is unsatisfiable wrt. Herbrand interpretations

Proof Procedures Based on Herbrand's Theorem

Proving unsatisfiability of a clause set becomes feasible (semi-decidable) by working with the set of its **ground instances** instead. Plan of attack:

Definition: A **ground instance** of a clause is obtained by replacing each of its variables by some variable-free term (“ground term”)

Proposition (Herbrand): Let N be a clause set and N^{gr} be the set of all ground instances of all clauses in N .

N is unsatisfiable iff N^{gr} is unsatisfiable wrt. Herbrand interpretations
(essentially: propositional-logic unsatisfiable)

Proposition (compactness): N^{gr} is unsatisfiable wrt. Herbrand interpretations iff
some finite subset $M \subseteq N^{\text{gr}}$ is unsatisfiable wrt. Herbrand interpretations

Propositional logic phase: Decide the satisfiability of such finite sets M with a SAT solver; **Gilmore's method**

Proof Procedures Based on Herbrand's Theorem

Proving unsatisfiability of a clause set becomes feasible (semi-decidable) by working with the set of its **ground instances** instead. Plan of attack:

Definition: A **ground instance** of a clause is obtained by replacing each of its variables by some variable-free term (“ground term”)

Proposition (Herbrand): Let N be a clause set and N^{gr} be the set of all ground instances of all clauses in N .

N is unsatisfiable iff N^{gr} is unsatisfiable wrt. Herbrand interpretations
(essentially: propositional-logic unsatisfiable)

Proposition (compactness): N^{gr} is unsatisfiable wrt. Herbrand interpretations iff
some finite subset $M \subseteq N^{\text{gr}}$ is unsatisfiable wrt. Herbrand interpretations

Propositional logic phase: Decide the satisfiability of such finite sets M with a SAT solver; **Gilmore's method**

The above recasts usual notions of “Herbrand theory” in our application to clause logic. “Herbrand's Theorem” (1930s) is a stronger version of the two propositions above combined

Ground Instances

Example: Let $N = \{P(a), \neg P(x) \vee P(f(x)), Q(y, z), \neg P(f(f(a)))\}$

Ground Instances

Example: Let $N = \{P(a), \neg P(x) \vee P(f(x)), Q(y, z), \neg P(f(f(a)))\}$

The underlying signature is $\Sigma = \{P/1, Q/2\} \cup \{a/0, f/2\}$

Ground Instances

Example: Let $N = \{P(a), \neg P(x) \vee P(f(x)), Q(y, z), \neg P(f(f(a)))\}$

The underlying signature is $\Sigma = \{P/1, Q/2\} \cup \{a/0, f/2\}$

The **ground terms (of Σ)** are $U^H = \{a, f(a), f(f(a)), f(f(f(a))), \dots\}$
(aka **Herbrand universe**)

Ground Instances

Example: Let $N = \{P(a), \neg P(x) \vee P(f(x)), Q(y, z), \neg P(f(f(a)))\}$

The underlying signature is $\Sigma = \{P/1, Q/2\} \cup \{a/0, f/2\}$

The **ground terms (of Σ)** are $U^H = \{a, f(a), f(f(a)), f(f(f(a))), \dots\}$
(aka **Herbrand universe**)

The **ground instances** of N is the set

$$\begin{aligned} N^{\text{gr}} = & \{P(a)\} \\ & \cup \{\neg P(a) \vee P(f(a)), \neg P(f(a)) \vee P(f(f(a))), \\ & \quad \neg P(f(f(a))) \vee P(f(f(f(a)))), \dots\} \\ & \cup \{Q(a, a), Q(a, f(a)), Q(f(a), a), Q(f(a), f(a)), \dots\} \\ & \cup \{\neg P(f(f(a)))\} \end{aligned}$$

Mapping to Propositional Logic

The **Herbrand base**, i.e., the set of all ground atoms is

$$\begin{aligned} HB = & \{ \underbrace{P(a)}_{A_0}, \underbrace{P(f(a))}_{A_1}, \underbrace{P(f(f(a)))}_{A_2}, \underbrace{P(f(f(f(a))))}_{A_3}, \dots \} \\ & \cup \{ \underbrace{Q(a, a)}_{B_0}, \underbrace{Q(a, f(a))}_{B_1}, \underbrace{Q(f(a), a)}_{B_2}, \underbrace{Q(f(a), f(a))}_{B_3}, \dots \} \end{aligned}$$

By construction, every atom in N^{gr} occurs in HB

Replace in N^{gr} every (ground) atom by its propositional counterpart:

$$\begin{aligned} N_{\text{prop}}^{\text{gr}} = & \{A_0\} \\ & \cup \{ \neg A_0 \vee A_1, \neg A_1 \vee A_2, \neg A_2 \vee A_3, \dots \} \\ & \cup \{B_0, B_1, B_2, B_3, \dots\} \\ & \cup \{ \neg A_2 \} \end{aligned}$$

The subset $\{A_0, \neg A_0 \vee A_1, \neg A_1 \vee A_2, \neg A_2\}$ is unsatisfiable, hence so is N .

Herbrand Proposition

A **Herbrand interpretation** I is an interpretation such that (in the example)

$$U = U^H = \{a, f(a), f(f(a)), f(f(f(a))), \dots\}$$

$$a : a$$

$$f : t \mapsto f(t)$$

In every Herbrand interpretation every ground term is always interpreted as “itself”, e.g. $I(f(f(a))) = f(f(a))$

The universe U^H of ground **terms** justifies expanding clauses into their ground instances instead of using a separate mapping β from variables to U

With the universe U and the interpretation of the function symbols uniquely fixed in every Herbrand interpretation, Herbrand interpretations vary only with the interpretation of the predicate symbols.

This justifies to specify a Herbrand interpretation as a subset of HB , those atoms that are *True* by definition. In the example, e.g., $I = \{P(a), Q(a, f(a))\}$

Herbrand Proposition

Prove idea for the non-trivial direction

- Suppose N has a model $J \models N$

E.g., $U_J = \mathbb{N}$, $a_J : 0$, $f_J : n \mapsto n + 1$, $P_J : n \mapsto n \geq 0$, $Q_J : m, n \mapsto m > n$

Herbrand Proposition

Prove idea for the non-trivial direction

- Suppose N has a model $J \models N$
E.g., $U_J = \mathbb{N}$, $a_J : 0$, $f_J : n \mapsto n + 1$, $P_J : n \mapsto n \geq 0$, $Q_J : m, n \mapsto m > n$
- Define a Herbrand interpretation $I \subseteq HB$ as follows:
For every ground atom $K \in HB$ put $K \in I$ iff $J(K) = \text{True}$
That is, evaluate K in J to get a (the same) truth value for K in I .
Example : $P(f(a)) \in I$ as $0 + 1 \geq 0$

Herbrand Proposition

Prove idea for the non-trivial direction

- Suppose N has a model $J \models N$
E.g., $U_J = \mathbb{N}$, $a_J : 0$, $f_J : n \mapsto n + 1$, $P_J : n \mapsto n \geq 0$, $Q_J : m, n \mapsto m > n$
- Define a Herbrand interpretation $I \subseteq HB$ as follows:

For every ground atom $K \in HB$ put $K \in I$ iff $J(K) = \text{True}$

That is, evaluate K in J to get a (the same) truth value for K in I .

Example : $P(f(a)) \in I$ as $0 + 1 \geq 0$

- Given an atom $A[x]$ (with free variables x) and a ground term t .
Then $I \models A[t]$ iff $(J, [x \mapsto J(t)] \models A[x]$.
Example: let $A[x] = P(f(x))$ and $t = f(f(a))$

$$I \models P(f(f(f(a))))$$

$$\text{iff } J \models P(f(f(f(a)))) \quad (\text{By definition})$$

$$\text{iff } J, [x \mapsto J(f(f(a)))] \models P(f(x)) \quad (\text{Use structural induction})$$

Herbrand Proposition

Prove idea for the non-trivial direction

- Suppose N has a model $J \models N$
E.g., $U_J = \mathbb{N}$, $a_J : 0$, $f_J : n \mapsto n + 1$, $P_J : n \mapsto n \geq 0$, $Q_J : m, n \mapsto m > n$
- Define a Herbrand interpretation $I \subseteq HB$ as follows:

For every ground atom $K \in HB$ put $K \in I$ iff $J(K) = \text{True}$

That is, evaluate K in J to get a (the same) truth value for K in I .

Example : $P(f(a)) \in I$ as $0 + 1 \geq 0$

- Given an atom $A[x]$ (with free variables x) and a ground term t .
Then $I \models A[t]$ iff $(J, [x \mapsto J(t)] \models A[x]$.
Example: let $A[x] = P(f(x))$ and $t = f(f(a))$

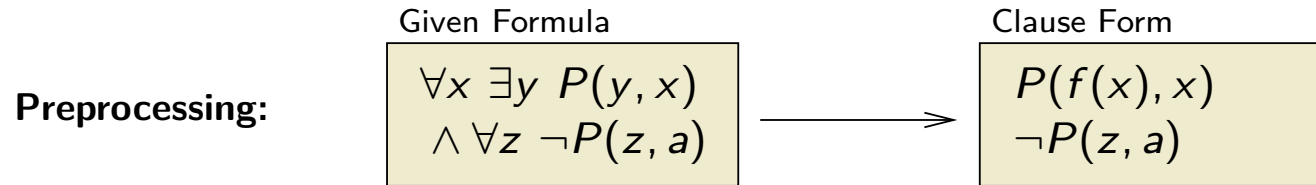
$$I \models P(f(f(f(a))))$$

$$\text{iff } J \models P(f(f(f(a)))) \quad (\text{By definition})$$

$$\text{iff } J, [x \mapsto J(f(f(a)))] \models P(f(x)) \quad (\text{Use structural induction})$$

- From that the proposition follows easily. Compactness: see whiteboard

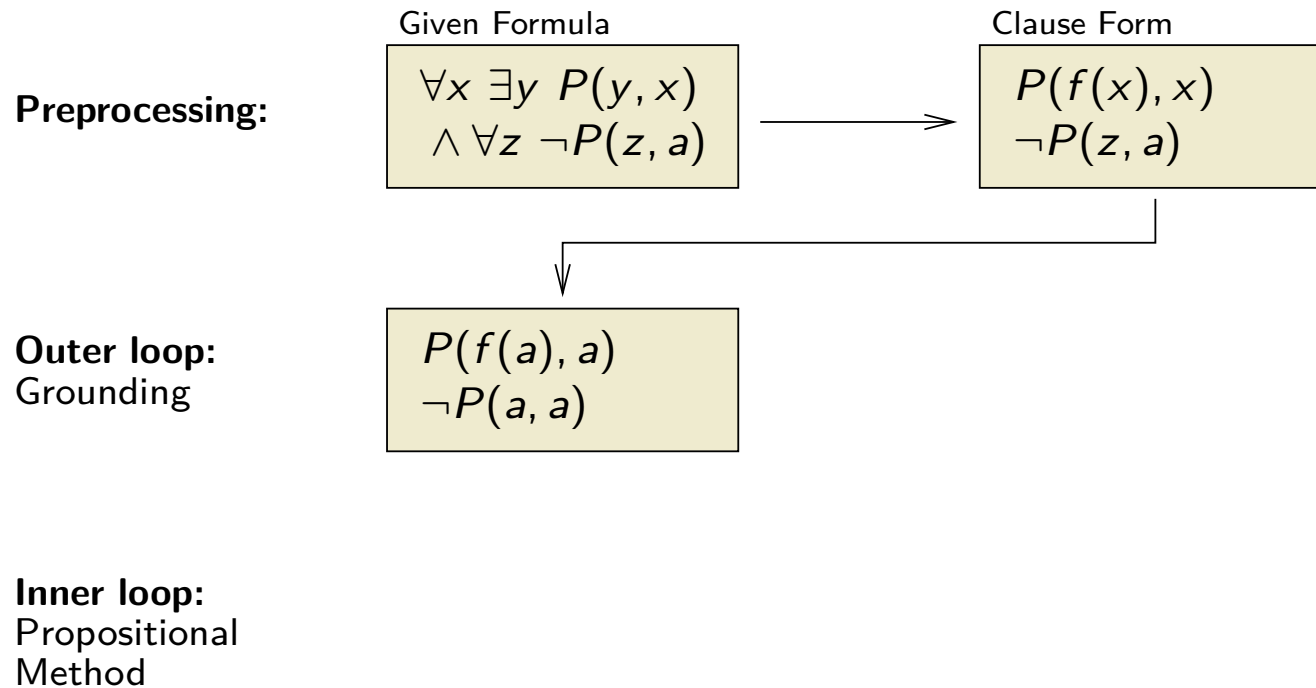
Gilmore's Method - Based on Herbrand's Theorem



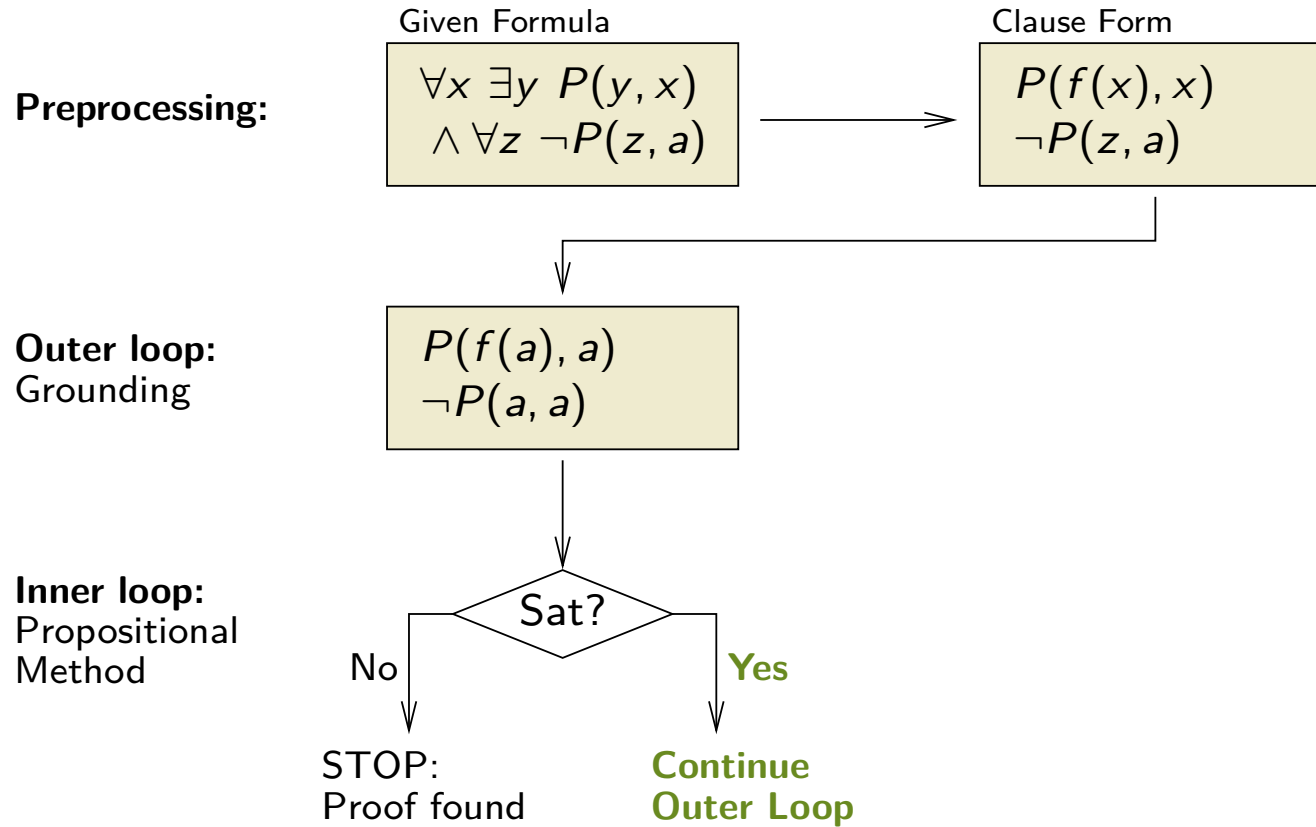
Outer loop:
Grounding

Inner loop:
Propositional
Method

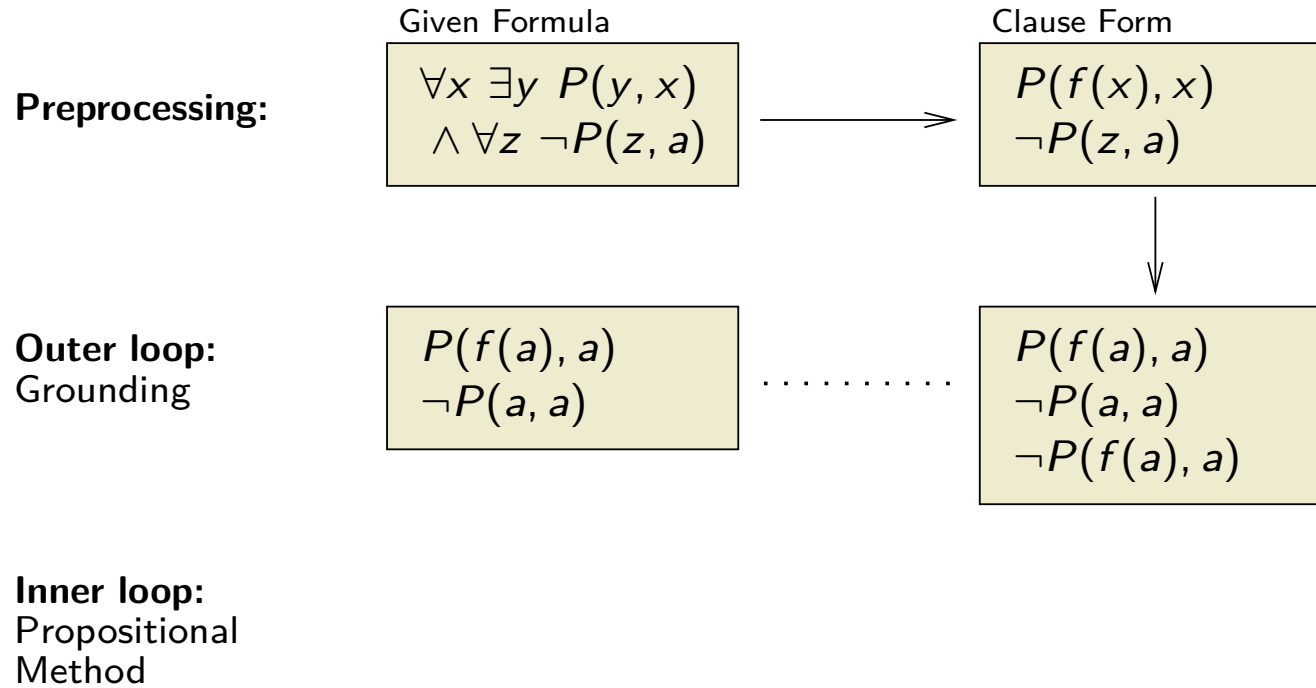
Gilmore's Method - Based on Herbrand's Theorem



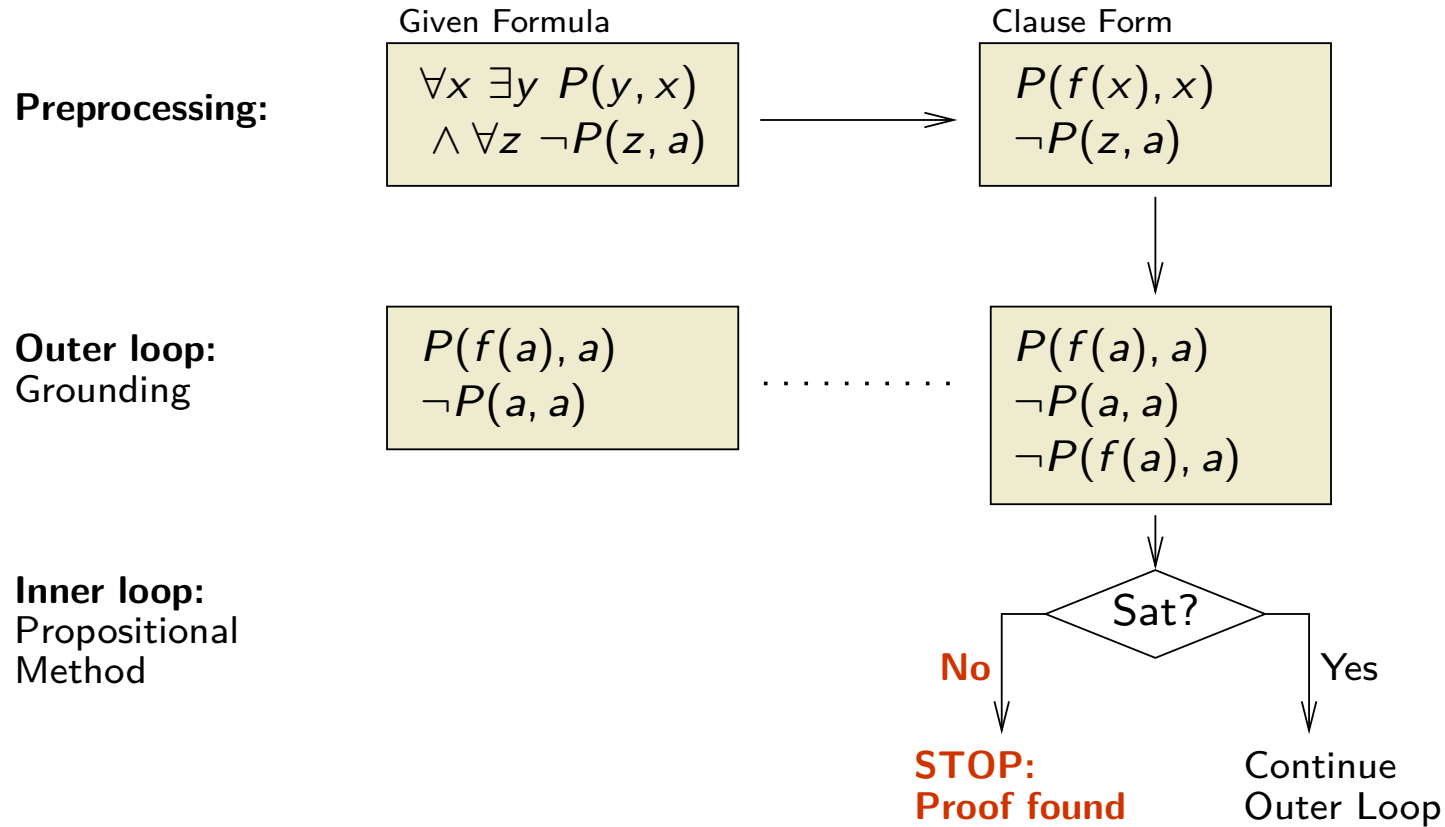
Gilmore's Method - Based on Herbrand's Theorem



Gilmore's Method - Based on Herbrand's Theorem



Gilmore's Method - Based on Herbrand's Theorem



Contents

Introduction

Logics and Reasoning Service (already done)

Methods for Automated Theorem Proving

Overview of some widely used general methods

- Propositional SAT solving
- First-order logic and clause normal forms
- Proof Procedures Based on Herbrand's Theorem
- **The Resolution calculus**
- Instance-based methods
- Model generation

Theory Reasoning

Methods to reason with specific background theories

- Paramodulation (Equality)
- Satisfiability Modulo Theories (SMT)
- Quantifier elimination for linear real arithmetic
- Combining multiple theories

The Resolution Calculus

- Gilmore's method reduces proof search in first-order logic to propositional logic unsatisfiability problems

The Resolution Calculus

- Gilmore's method reduces proof search in first-order logic to propositional logic unsatisfiability problems
- Main problem is the unguided generation of (very many) ground clauses

The Resolution Calculus

- Gilmore's method reduces proof search in first-order logic to propositional logic unsatisfiability problems
- Main problem is the unguided generation of (very many) ground clauses
- All modern calculi address this problem in one way or another, e.g.
 - **Avoidance:** Resolution calculi do not need to generate the ground instances at all

Resolution inferences operate directly on clauses, not on their ground instances

- **Guidance:** Instance-Based Methods are similar to Gilmore's method but generate ground instances in a guided way (see below)

The Resolution Calculus

- Gilmore's method reduces proof search in first-order logic to propositional logic unsatisfiability problems
- Main problem is the unguided generation of (very many) ground clauses
- All modern calculi address this problem in one way or another, e.g.
 - **Avoidance:** Resolution calculi do not need to generate the ground instances at all
Resolution inferences operate directly on clauses, not on their ground instances
 - **Guidance:** Instance-Based Methods are similar to Gilmore's method but generate ground instances in a guided way (see below)

Modern versions of the resolution calculus [Robinson 1965] are (still) the most important calculi for first-order theorem proving today

We first consider the special case for propositional logic

The Propositional Resolution Calculus

Propositional resolution inference rule:

$$\frac{C \vee A \quad \neg A \vee D}{C \vee D}$$

Terminology: $C \vee D$: **resolvent**; A : **resolved atom**

Propositional (positive) factoring inference rule:

$$\frac{C \vee A \vee A}{C \vee A}$$

Terminology: $C \vee A$: **factor**

These are **schematic inference rules**:

C and D – propositional clauses

A – propositional atom

“ \vee ” is considered associative and commutative

Derivations

Let $N = \{C_1, \dots, C_k\}$ be a set of **input clauses** (propositional, for now).

A **derivation (from N)** is a sequence of the form

$$\underbrace{C_1, \dots, C_k}_{\text{Input clauses}}, \underbrace{C_{k+1}, \dots, C_n, \dots}_{\text{Derived clauses}}$$

such that for every $n \geq k + 1$

- C_n is a resolvent of C_i and C_j , for some $1 \leq i, j < n$, or
- C_n is a factor of C_i , for some $1 \leq i < n$.

A **refutation (of N)** is a derivation from N that contains the empty clause \square

Important results:

Soundness: If there is a refutation of N then N is unsatisfiable

Completeness: If N is unsatisfiable then there is a refutation of N

Sample Refutation

1. $\neg A \vee \neg A \vee B$ (given)
2. $A \vee B$ (given)
3. $\neg C \vee \neg B$ (given)
4. C (given)

Sample Refutation

1. $\neg A \vee \neg A \vee B$ (given)
2. $A \vee B$ (given)
3. $\neg C \vee \neg B$ (given)
4. C (given)
5. $\neg A \vee B \vee B$ (Res. 2. into 1.)

Sample Refutation

1. $\neg A \vee \neg A \vee B$ (given)
2. $A \vee B$ (given)
3. $\neg C \vee \neg B$ (given)
4. C (given)
5. $\neg A \vee B \vee B$ (Res. 2. into 1.)
6. $\neg A \vee B$ (Fact. 5.)

Sample Refutation

1. $\neg A \vee \neg A \vee B$ (given)
2. $A \vee B$ (given)
3. $\neg C \vee \neg B$ (given)
4. C (given)
5. $\neg A \vee B \vee B$ (Res. 2. into 1.)
6. $\neg A \vee B$ (Fact. 5.)
7. $B \vee B$ (Res. 2. into 6.)

Sample Refutation

1. $\neg A \vee \neg A \vee B$ (given)
2. $A \vee B$ (given)
3. $\neg C \vee \neg B$ (given)
4. C (given)
5. $\neg A \vee B \vee B$ (Res. 2. into 1.)
6. $\neg A \vee B$ (Fact. 5.)
7. $B \vee B$ (Res. 2. into 6.)
8. B (Fact. 7.)

Sample Refutation

1. $\neg A \vee \neg A \vee B$ (given)
2. $A \vee B$ (given)
3. $\neg C \vee \neg B$ (given)
4. C (given)
5. $\neg A \vee B \vee B$ (Res. 2. into 1.)
6. $\neg A \vee B$ (Fact. 5.)
7. $B \vee B$ (Res. 2. into 6.)
8. B (Fact. 7.)
9. $\neg C$ (Res. 8. into 3.)

Sample Refutation

1. $\neg A \vee \neg A \vee B$ (given)
2. $A \vee B$ (given)
3. $\neg C \vee \neg B$ (given)
4. C (given)
5. $\neg A \vee B \vee B$ (Res. 2. into 1.)
6. $\neg A \vee B$ (Fact. 5.)
7. $B \vee B$ (Res. 2. into 6.)
8. B (Fact. 7.)
9. $\neg C$ (Res. 8. into 3.)
10. \square (Res. 4. into 9.)

Soundness of Propositional Resolution

Proposition

Propositional resolution is sound

Proof:

Let I be an interpretation. To be shown:

1. for resolution: $I \models C \vee A, I \models D \vee \neg A \Rightarrow I \models C \vee D$
2. for factoring: $I \models C \vee A \vee A \Rightarrow I \models C \vee A$

Soundness of Propositional Resolution

Proposition

Propositional resolution is sound

Proof:

Let I be an interpretation. To be shown:

1. for resolution: $I \models C \vee A, I \models D \vee \neg A \Rightarrow I \models C \vee D$
2. for factoring: $I \models C \vee A \vee A \Rightarrow I \models C \vee A$

Ad (i): Assume premises are valid in I . Two cases need to be considered:

(a) A is valid in I , or (b) $\neg A$ is valid in I .

Soundness of Propositional Resolution

Proposition

Propositional resolution is sound

Proof:

Let I be an interpretation. To be shown:

1. for resolution: $I \models C \vee A, I \models D \vee \neg A \Rightarrow I \models C \vee D$

2. for factoring: $I \models C \vee A \vee A \Rightarrow I \models C \vee A$

Ad (i): Assume premises are valid in I . Two cases need to be considered:

(a) A is valid in I , or (b) $\neg A$ is valid in I .

a) $I \models A \Rightarrow I \models D \Rightarrow I \models C \vee D$

Soundness of Propositional Resolution

Proposition

Propositional resolution is sound

Proof:

Let I be an interpretation. To be shown:

1. for resolution: $I \models C \vee A, I \models D \vee \neg A \Rightarrow I \models C \vee D$

2. for factoring: $I \models C \vee A \vee A \Rightarrow I \models C \vee A$

Ad (i): Assume premises are valid in I . Two cases need to be considered:

(a) A is valid in I , or (b) $\neg A$ is valid in I .

a) $I \models A \Rightarrow I \models D \Rightarrow I \models C \vee D$

b) $I \models \neg A \Rightarrow I \models C \Rightarrow I \models C \vee D$

Soundness of Propositional Resolution

Proposition

Propositional resolution is sound

Proof:

Let I be an interpretation. To be shown:

1. for resolution: $I \models C \vee A, I \models D \vee \neg A \Rightarrow I \models C \vee D$

2. for factoring: $I \models C \vee A \vee A \Rightarrow I \models C \vee A$

Ad (i): Assume premises are valid in I . Two cases need to be considered:

(a) A is valid in I , or (b) $\neg A$ is valid in I .

a) $I \models A \Rightarrow I \models D \Rightarrow I \models C \vee D$

b) $I \models \neg A \Rightarrow I \models C \Rightarrow I \models C \vee D$

Ad (ii): even simpler

Completeness of Propositional Resolution

Theorem:

Propositional Resolution is refutationally complete

Completeness of Propositional Resolution

Theorem:

Propositional Resolution is refutationally complete

- That is, if a propositional clause set is unsatisfiable, then Resolution will derive the empty clause \square eventually

Completeness of Propositional Resolution

Theorem:

Propositional Resolution is refutationally complete

- That is, if a propositional clause set is unsatisfiable, then Resolution will derive the empty clause \square eventually
- More precisely: If a clause set is unsatisfiable and closed under the application of the Resolution and Factoring inference rules, then it contains the empty clause \square

Completeness of Propositional Resolution

Theorem:

Propositional Resolution is refutationally complete

- That is, if a propositional clause set is unsatisfiable, then Resolution will derive the empty clause \square eventually
- More precisely: If a clause set is unsatisfiable and closed under the application of the Resolution and Factoring inference rules, then it contains the empty clause \square
- Perhaps easiest proof: semantic tree proof technique (see blackboard)

Completeness of Propositional Resolution

Theorem:

Propositional Resolution is refutationally complete

- That is, if a propositional clause set is unsatisfiable, then Resolution will derive the empty clause \square eventually
- More precisely: If a clause set is unsatisfiable and closed under the application of the Resolution and Factoring inference rules, then it contains the empty clause \square
- Perhaps easiest proof: semantic tree proof technique (see blackboard)
- This result can be considerably strengthened, some strengthenings come for free from the proof

Completeness of Propositional Resolution

Theorem:

Propositional Resolution is refutationally complete

- That is, if a propositional clause set is unsatisfiable, then Resolution will derive the empty clause \square eventually
- More precisely: If a clause set is unsatisfiable and closed under the application of the Resolution and Factoring inference rules, then it contains the empty clause \square
- Perhaps easiest proof: semantic tree proof technique (see blackboard)
- This result can be considerably strengthened, some strengthenings come for free from the proof

| |
|---|
| Propositional resolution is not suitable for first-order clause sets |
|---|

First-Order Resolution

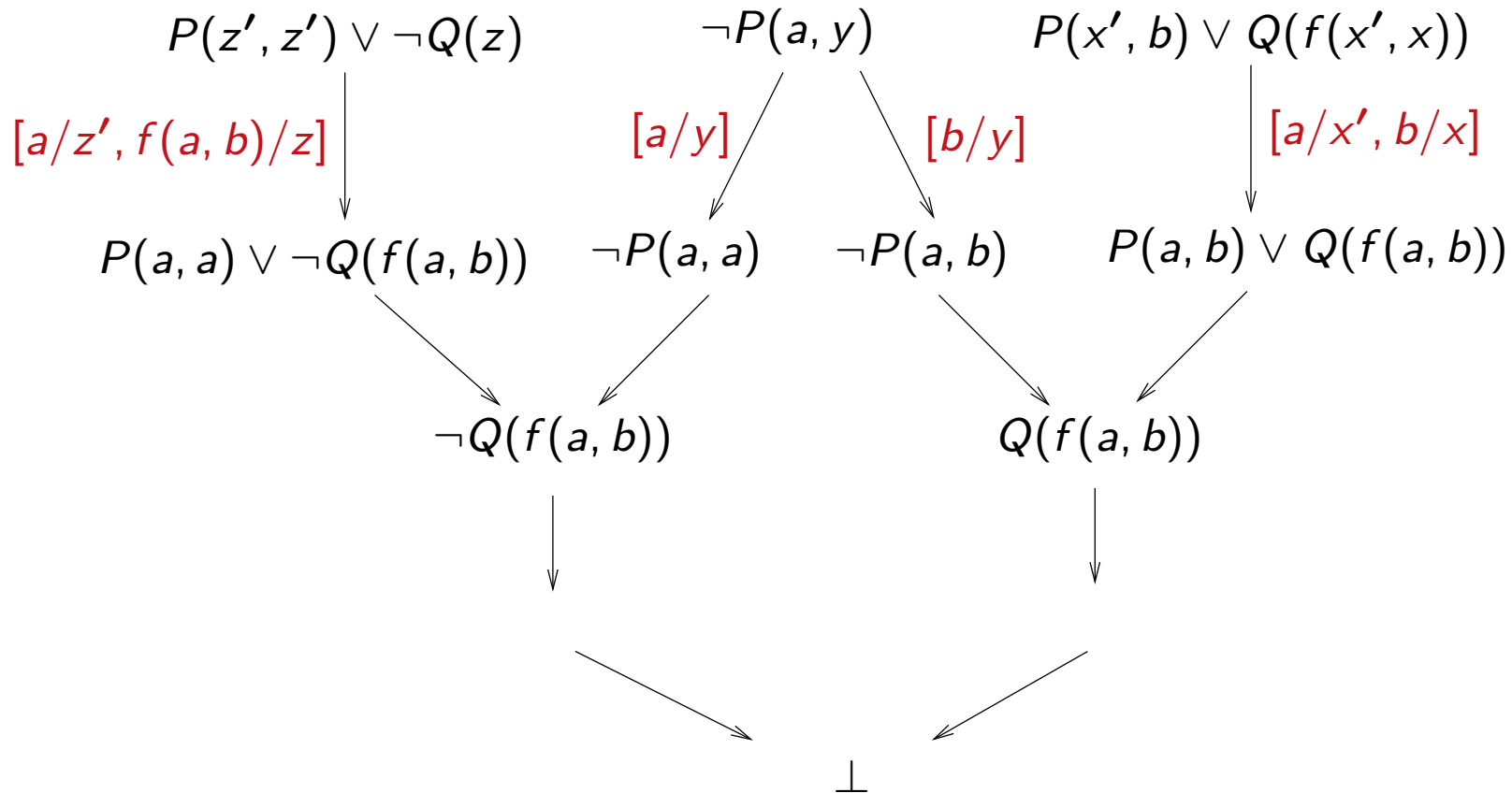
Propositional resolution:

- refutationally complete,
- in its most naive version: not guaranteed to terminate for satisfiable sets of clauses, (improved versions do terminate, however)
- in practice clearly inferior to the DPLL procedure (even with various improvements).

But: in contrast to the DPLL procedure, resolution can be easily extended to non-ground clauses (but see below First-order DPLL)

First-Order Resolution through Instantiation

Idea: instantiate clauses appropriately:



First-Order Resolution through Instantiation

Problems:

- More than one instance of a clause can participate in a proof.
- Even worse: There are infinitely many possible instances.

Observation:

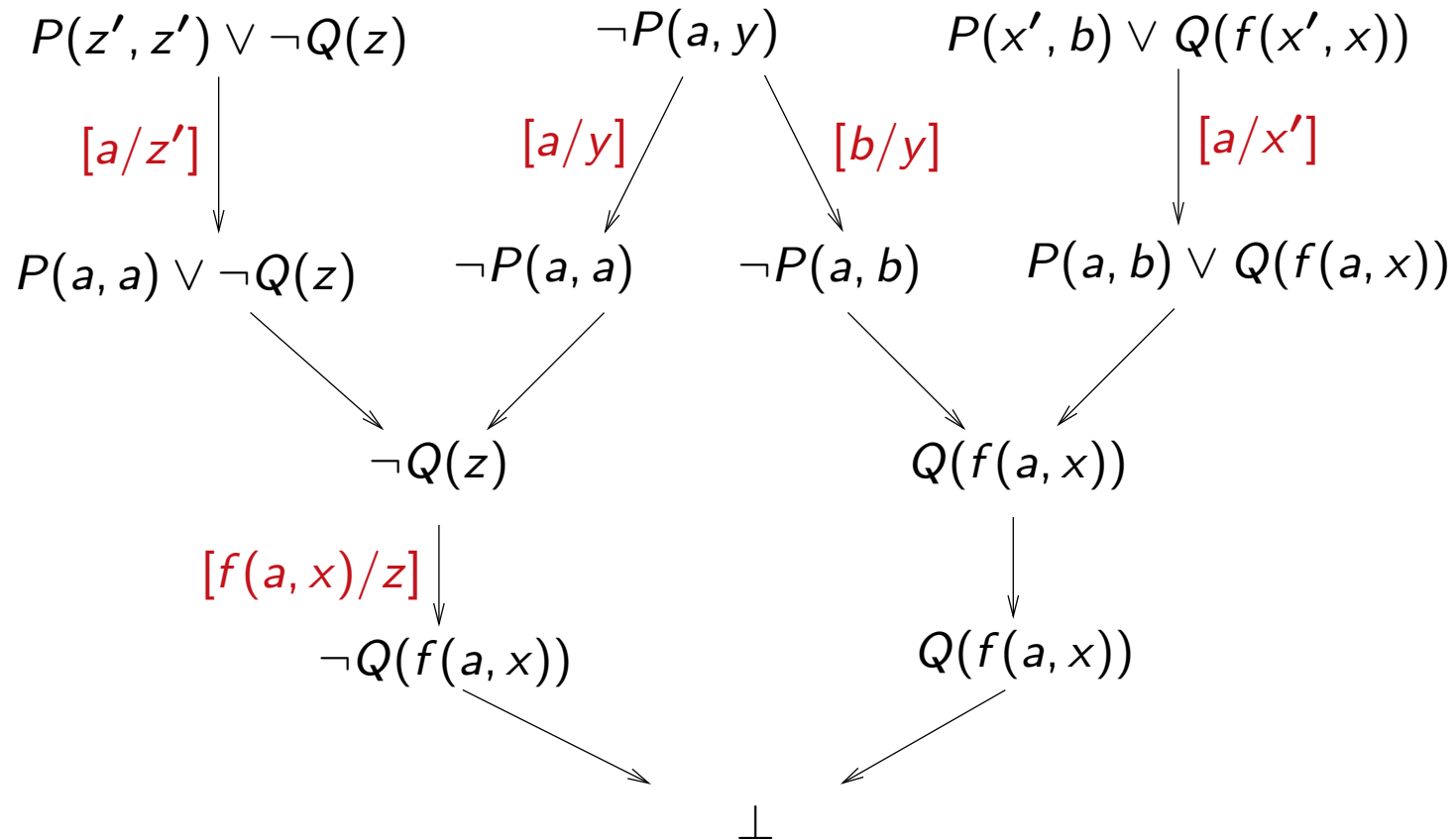
- Instantiation must produce complementary literals (so that inferences become possible).

Idea:

- Do not instantiate more than necessary to get complementary literals.

First-Order Resolution through Instantiation

Idea: do not instantiate more than necessary:



Lifting Principle

Problem: Make saturation of infinite sets of clauses as they arise from taking the (ground) instances of finitely many **first-order** clauses (with variables) effective and efficient.

Idea (Robinson 1965):

- Resolution for first-order clauses:
- **Equality** of ground atoms is generalized to **unifiability** of first-order atoms;
- Only compute **most general** (minimal) unifiers.

First-Order Resolution through Instantiation

Significance: The advantage of the method in (Robinson 1965) compared with (Gilmore 1960) is that unification enumerates only those instances of clauses that participate in an inference. Moreover, clauses are not right away instantiated into ground clauses. Rather they are instantiated only as far as required for an inference. Inferences with non-ground clauses in general represent infinite sets of ground inferences which are computed simultaneously in a single step.

Substitutions and Unifiers

- A **substitution** σ is a mapping from variables to terms which is the identity almost everywhere. Example: $\sigma = [y \mapsto f(x), z \mapsto f(x)]$

Substitutions and Unifiers

- A **substitution** σ is a mapping from variables to terms which is the identity almost everywhere. Example: $\sigma = [y \mapsto f(x), z \mapsto f(x)]$
- A substitution σ is **applied** to a term or atom t by replacing every occurrence of every variable x in t by $\sigma(x)$.

Instead of $\sigma(t)$ one usually writes $t\sigma$

Example, with σ is from above: $P(f(x), y)\sigma = P(f(x), f(x))$

Substitutions and Unifiers

- A **substitution** σ is a mapping from variables to terms which is the identity almost everywhere. Example: $\sigma = [y \mapsto f(x), z \mapsto f(x)]$
- A substitution σ is **applied** to a term or atom t by replacing every occurrence of every variable x in t by $\sigma(x)$.

Instead of $\sigma(t)$ one usually writes $t\sigma$

Example, with σ is from above: $P(f(x), y)\sigma = P(f(x), f(x))$

- A substitution γ is a **unifier** of s and t iff $s\gamma = t\gamma$.

A unifier σ is **most general** iff for every unifier γ of the same terms there is a substitution δ such that $\gamma = \delta \circ \sigma$ ($=: \sigma\delta$). Notation: $\sigma = \text{mgu}(s, t)$

Example:

$s = \text{car}(\text{red}, y, z)$

$t = \text{car}(u, v, \text{ferrari})$

Then $\gamma = [u \mapsto \text{red}, y \mapsto \text{fast}, v \mapsto \text{fast}, z \mapsto \text{ferrari}]$ is a unifier,

and $\sigma = [u \mapsto \text{red}, y \mapsto v, z \mapsto \text{ferrari}]$ is a mgu for s and t .

With $\delta = [v \mapsto \text{fast}]$ obtain $\sigma\delta = \gamma$.

Substitutions and Unifiers

Let $E = \{s_1 \doteq t_1, \dots, s_n \doteq t_n\}$ (s_i, t_i terms or atoms) a multi-set of **equality problems**. A substitution σ is called a **unifier** of E if $s_i\sigma = t_i\sigma$ for all $1 \leq i \leq n$.

If a unifier of E exists, then E is called **unifiable**.

The rule system on the next slide computes a most general unifier of a multiset of equality problems or “fail” (\perp) if none exists.

Rule Based Naive Standard Unification

$$t \doteq t, E \Rightarrow_{SU} E$$

$$f(s_1, \dots, s_n) \doteq f(t_1, \dots, t_n), E \Rightarrow_{SU} s_1 \doteq t_1, \dots, s_n \doteq t_n, E$$

$$f(\dots) \doteq g(\dots), E \Rightarrow_{SU} \perp$$

$$\begin{aligned} x \doteq t, E &\Rightarrow_{SU} x \doteq t, E[t/x] \\ &\text{if } x \in \text{var}(E), x \notin \text{var}(t) \end{aligned}$$

$$\begin{aligned} x \doteq t, E &\Rightarrow_{SU} \perp \\ &\text{if } x \neq t, x \in \text{var}(t) \end{aligned}$$

$$\begin{aligned} t \doteq x, E &\Rightarrow_{SU} x \doteq t, E \\ &\text{if } t \notin X \end{aligned}$$

Main Properties

The above unification algorithm is sound and complete:

Given $E = s_1 \doteq t_1, \dots, s_n \doteq t_n$, exhaustive application of the above rules always terminates, and one of the following holds:

- The result is a set equations in **solved form**, that is, is of the form

$$x_1 \doteq u_1, \dots, x_k \doteq u_k$$

with x_i pairwise distinct variables, and $x_i \notin \text{var}(u_j)$.

In this case, the solved form represents the substitution

$\sigma_E = [x_1 \mapsto u_1, \dots, x_k \mapsto u_k]$ and it is a mgu for E .

- The result is \perp . In this case no unifier for E exists.

First-Order Resolution Inference Rules

$$\frac{C \vee A \quad D \vee \neg B}{(C \vee D)\sigma} \quad \text{if } \sigma = \text{mgu}(A, B) \quad [\text{resolution}]$$

$$\frac{C \vee A \vee B}{(C \vee A)\sigma} \quad \text{if } \sigma = \text{mgu}(A, B) \quad [\text{factoring}]$$

For the resolution inference rule, the premise clauses have to be renamed apart (made variable disjoint)

First-Order Resolution Inference Rules

$$\frac{C \vee A \quad D \vee \neg B}{(C \vee D)\sigma} \quad \text{if } \sigma = \text{mgu}(A, B) \quad [\text{resolution}]$$

$$\frac{C \vee A \vee B}{(C \vee A)\sigma} \quad \text{if } \sigma = \text{mgu}(A, B) \quad [\text{factoring}]$$

For the resolution inference rule, the premise clauses have to be renamed apart (made variable disjoint)

Example

$$\frac{Q(z) \vee P(z, z) \quad \neg P(x, y)}{Q(x)} \quad \text{where } \sigma = [z \mapsto x, y \mapsto x] \quad [\text{resolution}]$$

$$\frac{Q(z) \vee P(z, a) \vee P(a, y)}{Q(a) \vee P(a, a)} \quad \text{where } \sigma = [z \mapsto a, y \mapsto a] \quad [\text{factoring}]$$

Sample Refutation – The Barber Problem

```
set(binary_res). %% This is an "otter" input file
formula_list(sos).
%% Every barber shaves all persons who do not shave themselves:
all x (B(x) -> (all y (-S(y,y) -> S(x,y)))).
%% No barber shaves a person who shaves himself:
all x (B(x) -> (all y (S(y,y) -> -S(x,y)))).
%% Negation of "there are no barbers"
exists x B(x).
end_of_list.
```

otter finds the following refutation (clauses 1 – 3 are the CNF of the above):

```
1 [] -B(x)|S(y,y)|S(x,y).
2 [] -B(x)| -S(y,y)| -S(x,y).
3 [] B($c1).
4 [binary,1.1,3.1] S(x,x)|S($c1,x).
5 [factor,4.1.2] S($c1,$c1).
6 [binary,2.1,3.1] -S(x,x)| -S($c1,x).
10 [factor,6.1.2] -S($c1,$c1).
11 [binary,10.1,5.1] $F.
```

Completeness of First-Order Resolution

Theorem: Resolution is **refutationally complete**

Completeness of First-Order Resolution

Theorem: Resolution is **refutationally complete**

- That is, if a clause set is unsatisfiable, then Resolution will derive the empty clause \square eventually

Completeness of First-Order Resolution

Theorem: Resolution is **refutationally complete**

- That is, if a clause set is unsatisfiable, then Resolution will derive the empty clause \square eventually
- More precisely: If a clause set is unsatisfiable and closed under the application of the Resolution and Factoring inference rules, then it contains the empty clause \square

Completeness of First-Order Resolution

Theorem: Resolution is **refutationally complete**

- That is, if a clause set is unsatisfiable, then Resolution will derive the empty clause \square eventually
- More precisely: If a clause set is unsatisfiable and closed under the application of the Resolution and Factoring inference rules, then it contains the empty clause \square
- Perhaps easiest proof: Herbrand Theorem + Completeness of propositional resolution + **Lifting Lemma**

Lifting Lemma

Lemma 0.1 *Let C and D be variable-disjoint clauses. If*

$$\frac{\begin{array}{c} D \\ \downarrow \sigma \\ D\sigma \end{array} \quad \begin{array}{c} C \\ \downarrow \rho \\ C\rho \end{array}}{C'} \quad [\textit{propositional resolution}]$$

then there exists a substitution τ such that

$$\frac{D \quad C}{C''} \quad [\textit{first-order resolution}]$$
$$\downarrow \tau$$
$$C' = C''\tau$$

Lifting Lemma

An analogous lifting lemma holds for factoring.

Corollary: if N is a set of clauses closed under resolution and factoring, then also the set of all ground instances of all clauses from N is closed under resolution and factoring.

With this result, it only remains to be shown how a given set of clauses can be closed under resolution and factoring. For this use, e.g., the “Given Clause Loop”.

The “Given Clause Loop”

As used in the Otter theorem prover:

Lists of clauses maintained by the algorithm: usable and sos.

Initialize sos with the input clauses, usable empty.

Algorithm (straight from the Otter manual):

While (sos is not empty and no refutation has been found)

1. Let given_clause be the ‘lightest’ clause in sos;
2. Move given_clause from sos to usable;
3. Infer and process new clauses using the inference rules in effect; each new clause must have the given_clause as one of its parents and members of usable as its other parents; new clauses that pass the retention tests are appended to sos;

End of while loop.

Fairness: define clause weight e.g. as “depth + length” of clause.

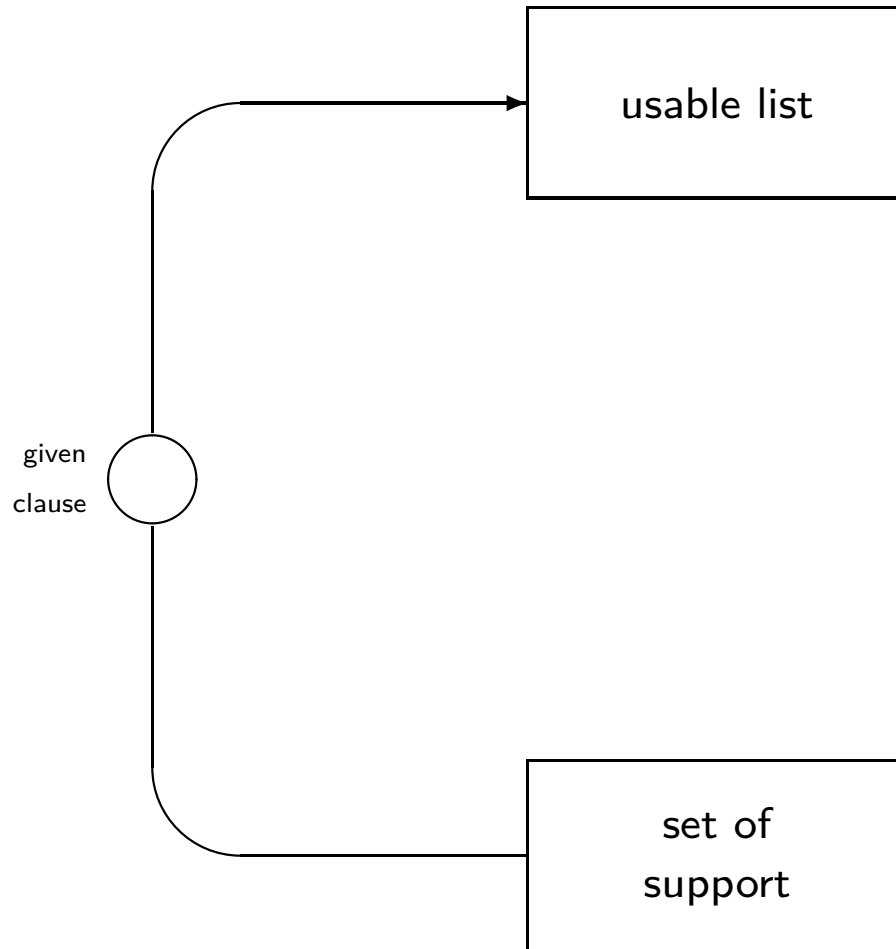
The “Given Clause Loop” - Graphically

The “Given Clause Loop” - Graphically

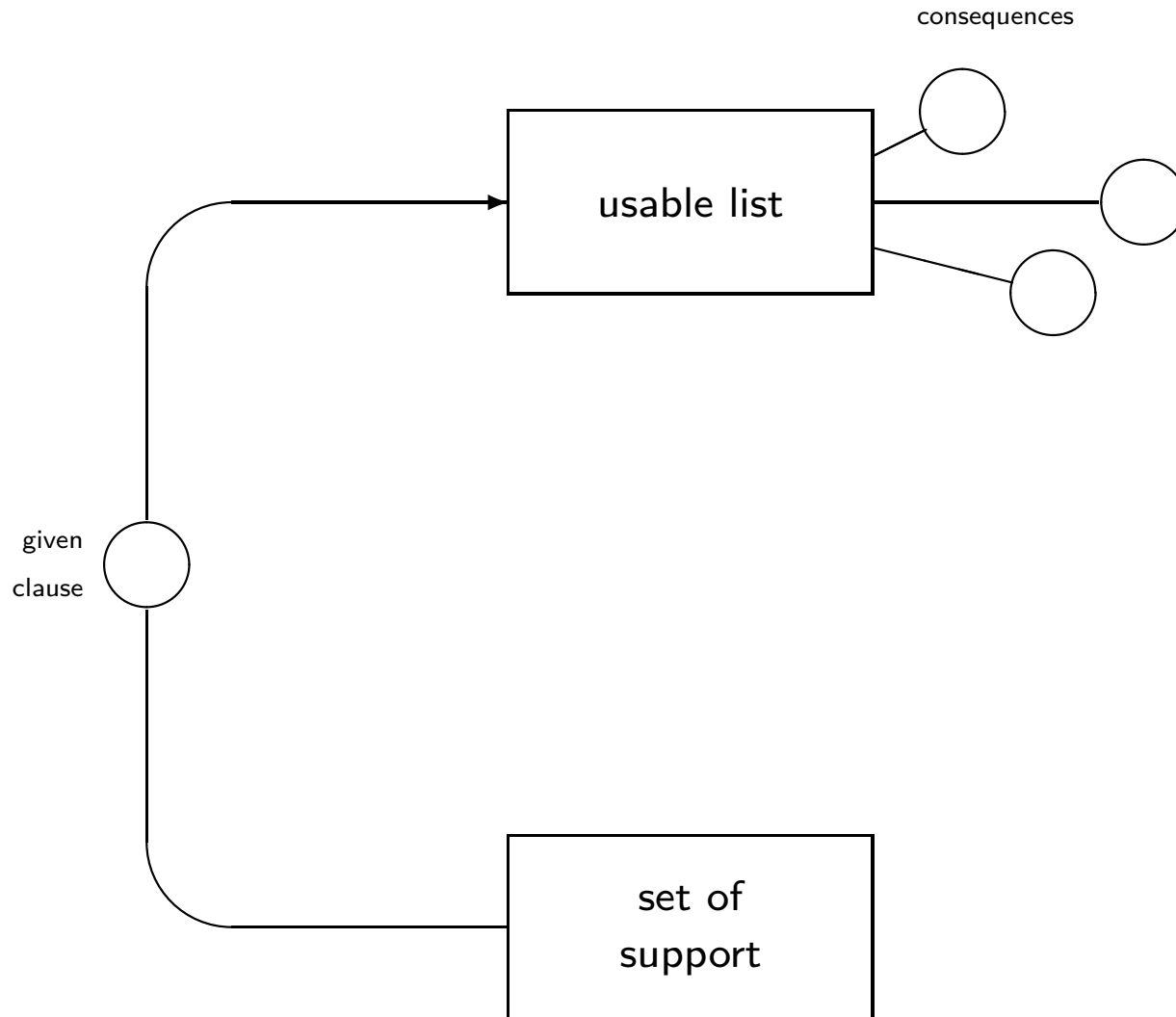
usable list

set of
support

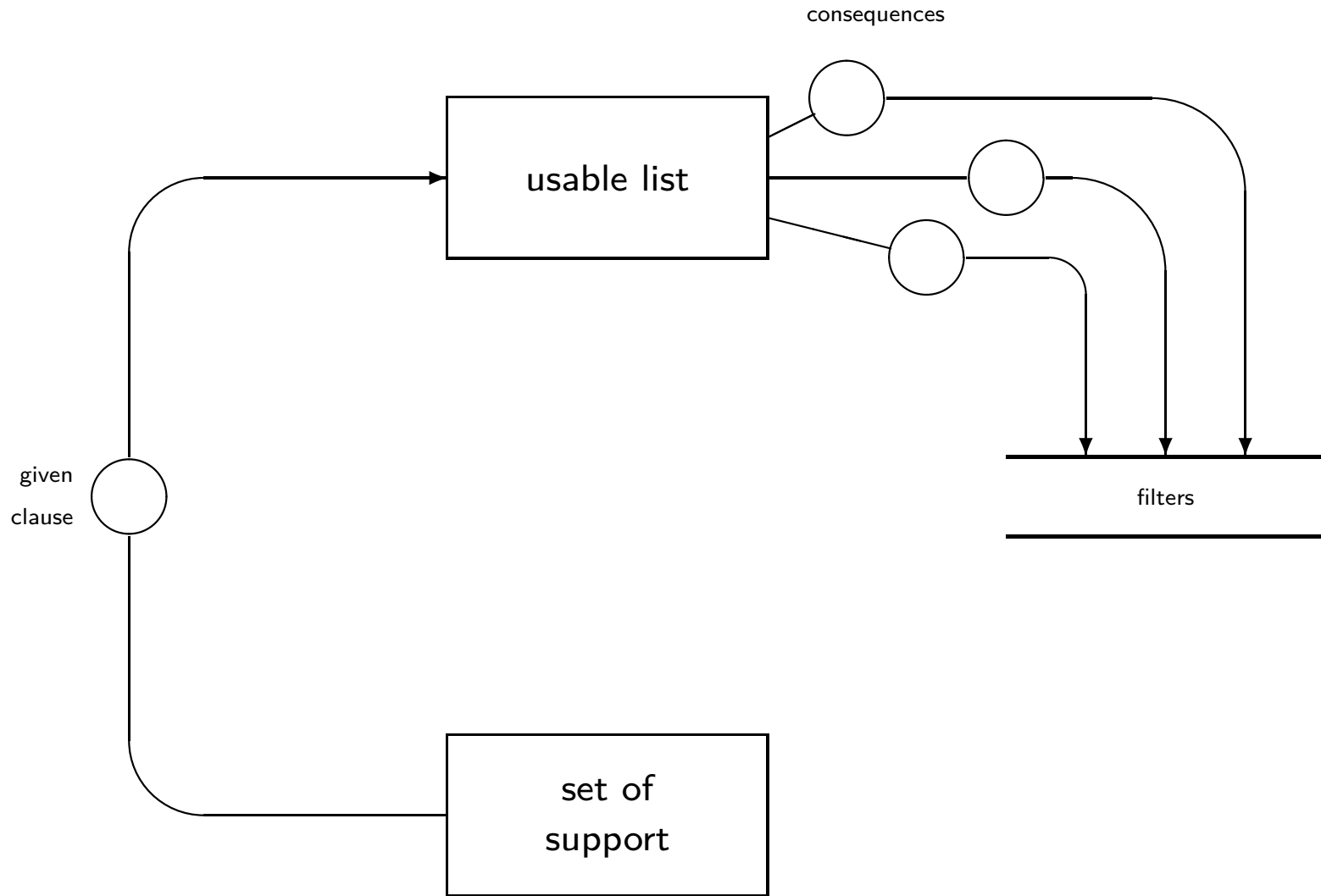
The “Given Clause Loop” - Graphically



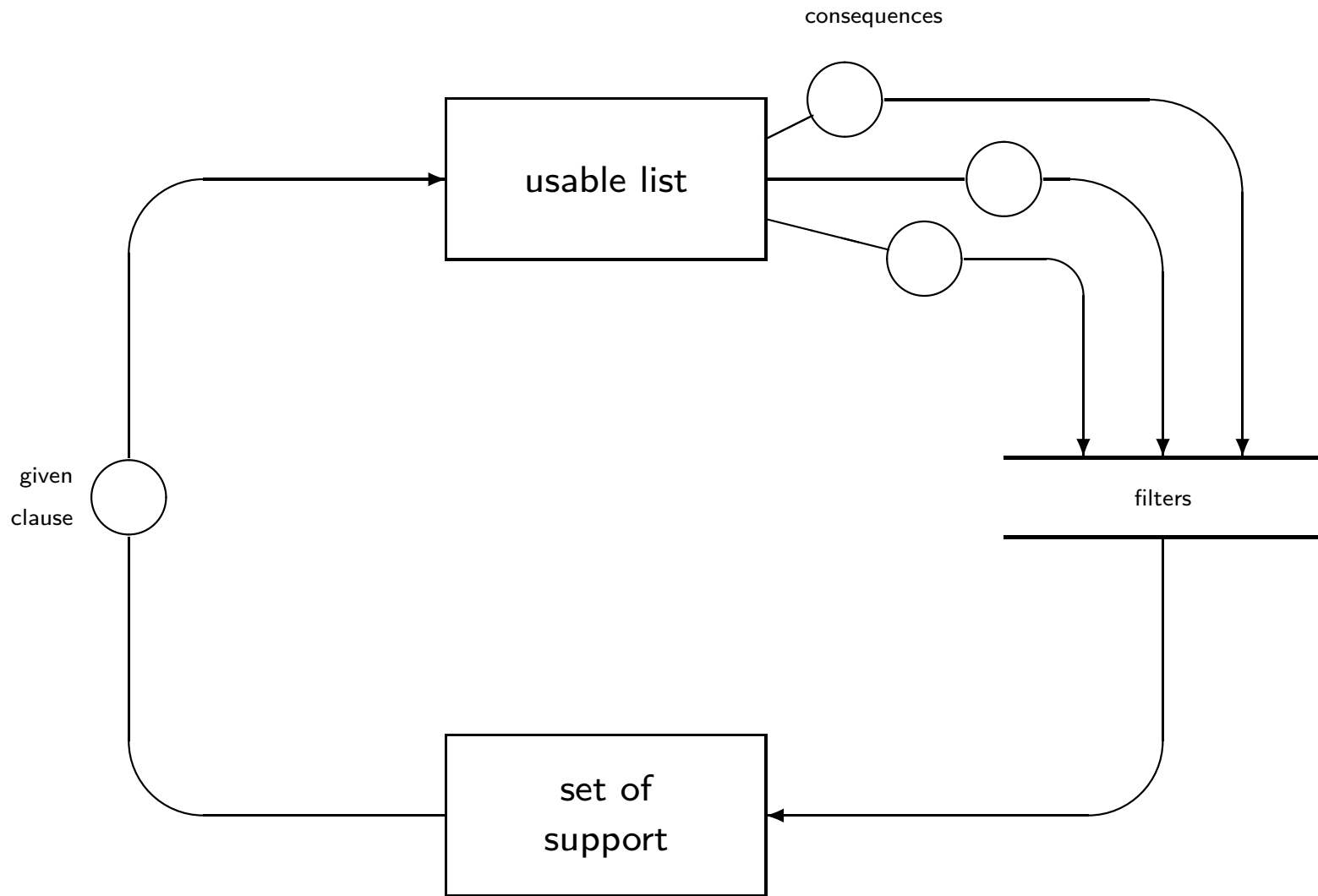
The “Given Clause Loop” - Graphically



The “Given Clause Loop” - Graphically



The “Given Clause Loop” - Graphically



Resolution – Further Topics

Overcoming the search space

- Restricting inference rules, in particular by ordering refinements.
A-ordered resolution permits resolution inferences only if the literals resolved upon are maximal in their parent clauses.
- Resolution strategies, to compute (hopefully small) subsets of the full closure under inference rule applications.
Set-of-support, Linear Resolution, Hyperresolution (see below), and more.
- Deleting clauses that are not needed to find a refutation.
In particular subsumption deletion: delete clause C in presence of a (different) clause D such that $D\sigma \subseteq C$, for some substitution σ .
- Simplification of clauses.

Implementation techniques: in particular term indexing techniques

Hyperresolution

There are **many** variants of resolution. (We refer to [Bachmair, Ganzinger: Resolution Theorem Proving] for further reading.)

One well-known example is hyperresolution (Robinson 1965):

$$\frac{D_1 \vee B_1 \quad \dots \quad D_n \vee B_n \quad C \vee \neg A_1 \vee \dots \vee \neg A_n}{(D_1 \vee \dots \vee D_n \vee C)\sigma}$$

with $\sigma = \text{mgu}(A_1 \doteq B_1, \dots, A_n \doteq B_n)$.

Similarly to resolution, hyperresolution has to be complemented by a factoring inference.

Contents

Introduction

Logics and Reasoning Service (already done)

Methods for Automated Theorem Proving

Overview of some widely used general methods

- Propositional SAT solving
- First-order logic and clause normal forms
- Proof Procedures Based on Herbrand's Theorem
- The Resolution calculus
- Instance-based methods
- Model generation

Theory Reasoning

Methods to reason with specific background theories

- Paramodulation (Equality)
- Satisfiability Modulo Theories (SMT)
- Quantifier elimination for linear real arithmetic
- Combining multiple theories

Instance-Based Methods

Recall:

- Gilmore's method reduces proof search in first-order logic to propositional logic unsatisfiability problems

Instance-Based Methods

Recall:

- Gilmore's method reduces proof search in first-order logic to propositional logic unsatisfiability problems
- Main problem is the unguided generation of (very many) ground clauses

Instance-Based Methods

Recall:

- Gilmore's method reduces proof search in first-order logic to propositional logic unsatisfiability problems
- Main problem is the unguided generation of (very many) ground clauses
- All modern calculi address this problem in one way or another, e.g.
 - **Avoidance:** Resolution calculi do not need to generate the ground instances at all

Resolution inferences operate directly on clauses, not on their ground instances

- **Guidance:** Instance-Based Methods are similar to Gilmore's method but generate ground instances in a guided way

Two-Level Instance-Based Methods

Idea:

- Overlaps of complementary literals produce instantiations (as in resolution);
- However, contrary to resolution, clauses are not recombined.
- Clauses are temporarily grounded – replace every variable by a constant – and checked for unsatisfiability; use an efficient propositional proof method, a “SAT-solver” for that.
- Main variants: (ordered) semantic hyperlinking [Plaisted], resolution-based instance generation (Inst-Gen) [Ganzinger and Korovin].

Resolution-Based Instance Generation

Resolution-based instance generation has only one inference rule:

$$\frac{D \vee B \quad C \vee \neg A}{(D \vee B)\sigma \quad (C \vee \neg A)\sigma} \quad [\text{Inst-Gen}]$$

if $\sigma = \text{mgu}(A, B)$ and at least one conclusion is a proper instance of its premise.

The instance-generation calculus saturates a given clause set under Inst-Gen and periodically passes the ground-instantiated version of the current clause set to a SAT-solver.

A refutation has been found if the SAT-solver determines unsatisfiability.

One-Level Instance-Based Methods

- Other methods **do not** use a SAT-solver as a subroutine;
- Instead, the **same** base calculus is used to generate new clause instances and test for unsatisfiability of grounded data structures.
- Main variants: tableau variants, such as the disconnection calculus [Billon; Letz and Stenz], and a variant of the DPLL procedure for first-order logic, FDPLL [Baumgartner and Tinelli].

Instance-Based Method – FDPLL

Lifted data structures:

| | Propositional Reasoning | First-Order Reasoning |
|----------------|----------------------------|--|
| Clauses | $\neg A \vee B \vee C$ | $\neg P(x, x) \vee P(x, a) \vee Q(x, x)$ |

Instance-Based Method – FDPLL

Lifted data structures:

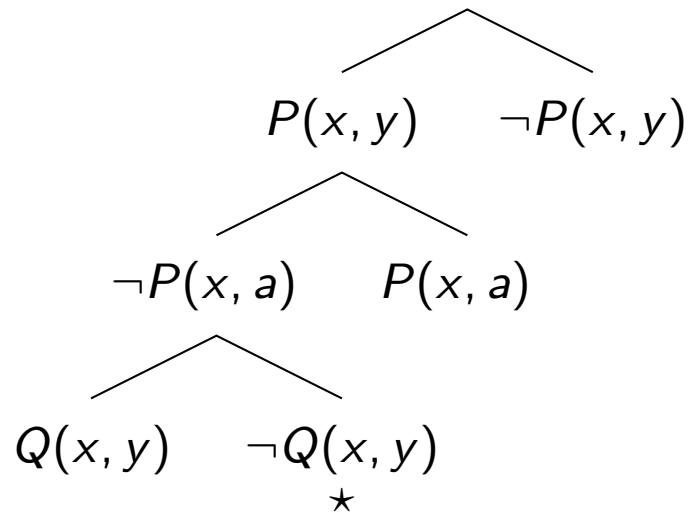
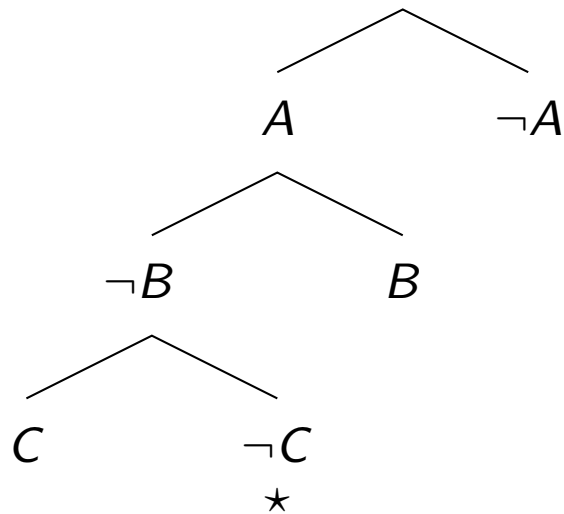
Propositional Reasoning

First-Order Reasoning

Clauses $\neg A \vee B \vee C$

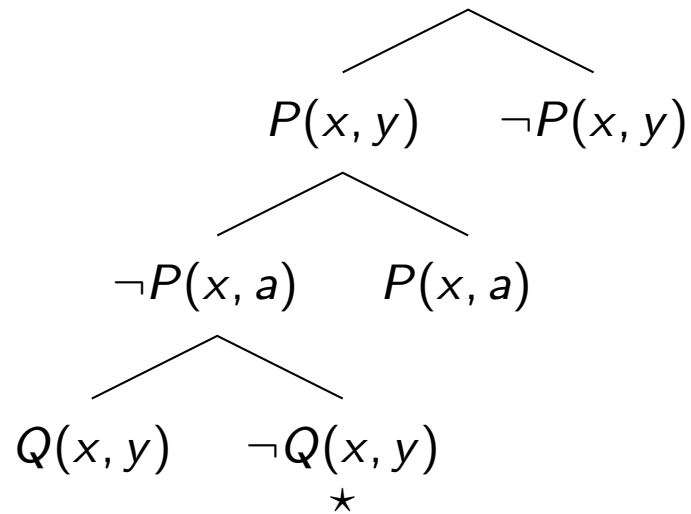
$\neg P(x, x) \vee P(x, a) \vee Q(x, x)$

Trees



First-Order Semantic Trees

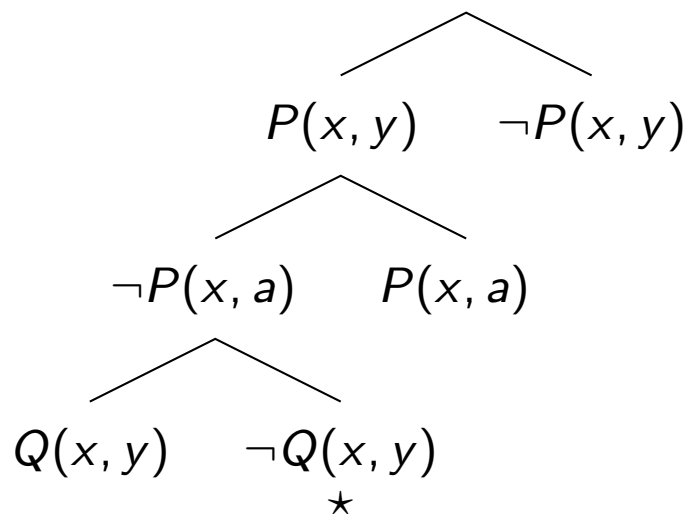
First-Order Semantic Trees



Issues:

- One-branch-at-a-time approach desired

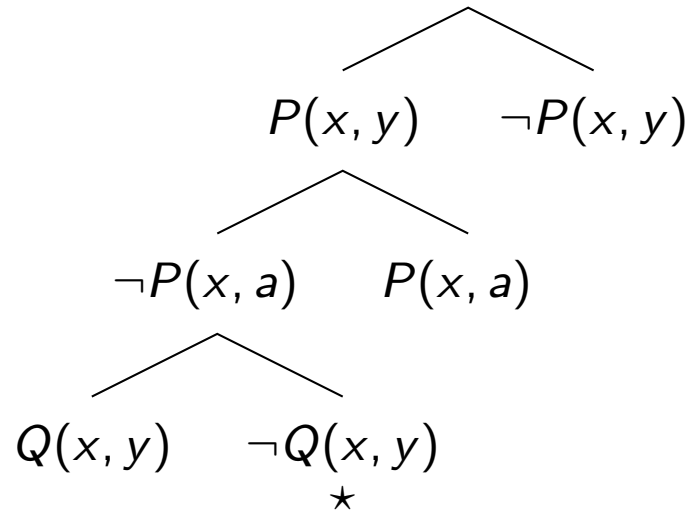
First-Order Semantic Trees



Issues:

- One-branch-at-a-time approach desired
- How to extract an interpretation from a branch?

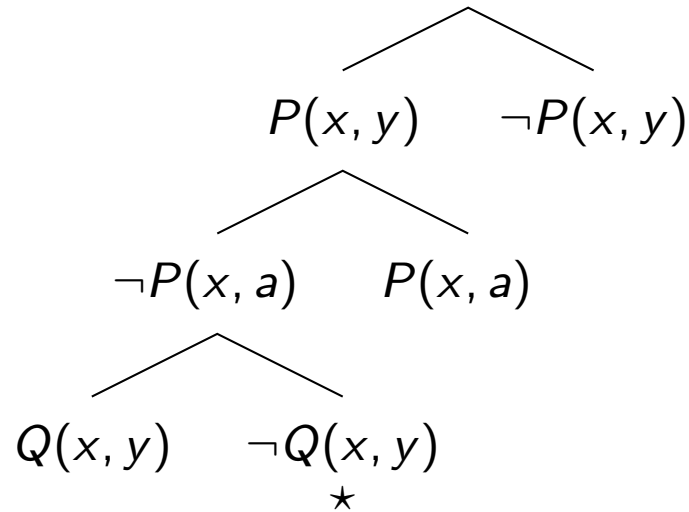
First-Order Semantic Trees



Issues:

- One-branch-at-a-time approach desired
- How to extract an interpretation from a branch?
- When is a branch closed?

First-Order Semantic Trees



Issues:

- One-branch-at-a-time approach desired
- How to extract an interpretation from a branch?
- When is a branch closed?
- How to construct such trees (calculus)?

Extracting an Interpretation from a Branch

Branch \mathcal{B} :

|
 $P(x, y)$

Interpretation $\llbracket \mathcal{B} \rrbracket = \{ \dots \}$:

- A branch literal specifies the truth values for all its ground instances, unless there is a more specific literal specifying opposite truth values.

Extracting an Interpretation from a Branch

Branch \mathcal{B} :

|

$P(x, y)$



Interpretation $\llbracket \mathcal{B} \rrbracket = \{...\}$:

$P(a, a)$

$P(b, a)$

$P(a, b)$

$P(b, b)$

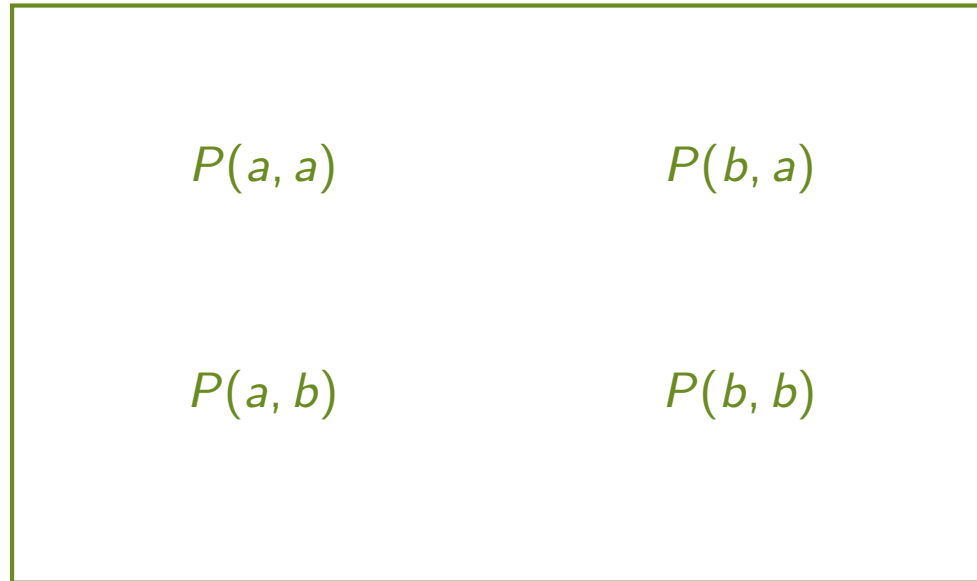
- A branch literal specifies the truth values for all its ground instances, unless there is a more specific literal specifying opposite truth values.

Extracting an Interpretation from a Branch

Branch \mathcal{B} :

$P(x, y)$
|
 $\neg P(a, y)$

Interpretation $\llbracket \mathcal{B} \rrbracket = \{ \dots \}$:



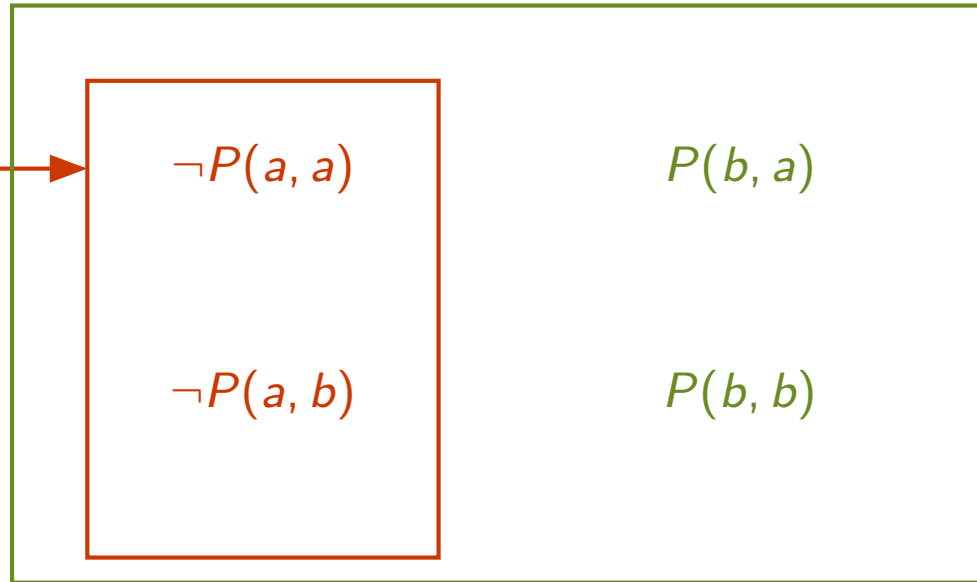
- A branch literal specifies the truth values for all its ground instances, unless there is a more specific literal specifying opposite truth values.

Extracting an Interpretation from a Branch

Branch \mathcal{B} :

$P(x, y)$
|
 $\neg P(a, y)$

Interpretation $\llbracket \mathcal{B} \rrbracket = \{ \dots \}$:



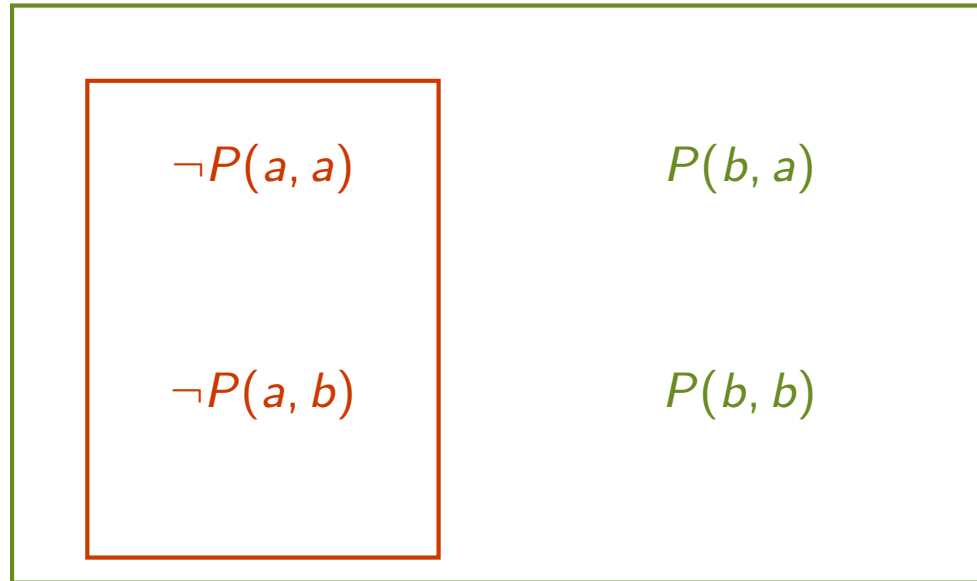
- A branch literal specifies the truth values for all its ground instances, unless there is a more specific literal specifying opposite truth values.

Extracting an Interpretation from a Branch

Branch \mathcal{B} :

$P(x, y)$
—
 $\neg P(a, y)$
—
 $\neg P(b, b)$

Interpretation $\llbracket \mathcal{B} \rrbracket = \{ \dots \}$:



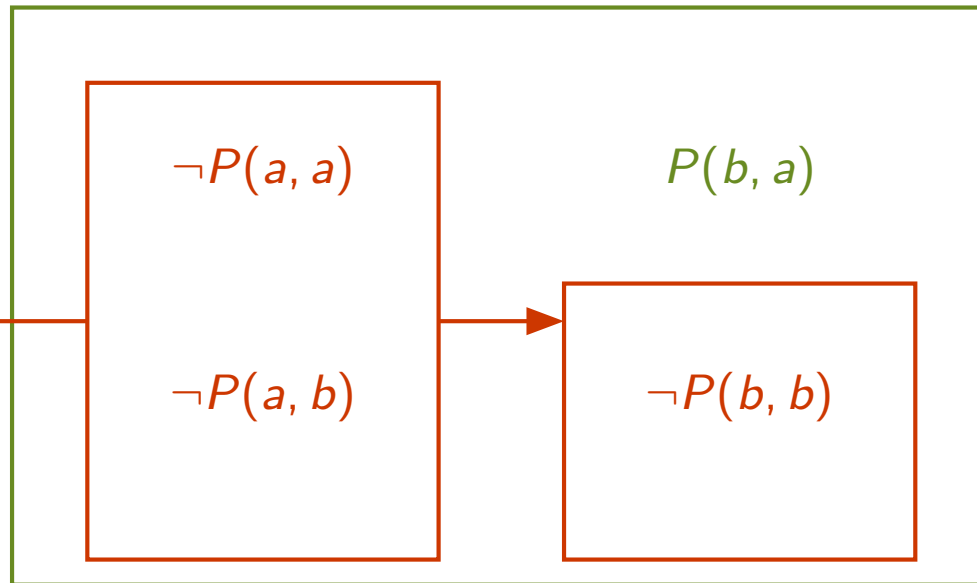
- A branch literal specifies the truth values for all its ground instances, unless there is a more specific literal specifying opposite truth values.

Extracting an Interpretation from a Branch

Branch \mathcal{B} :

$P(x, y)$
—
 $\neg P(a, y)$
—
 $\neg P(b, b)$

Interpretation $\llbracket \mathcal{B} \rrbracket = \{ \dots \}$:



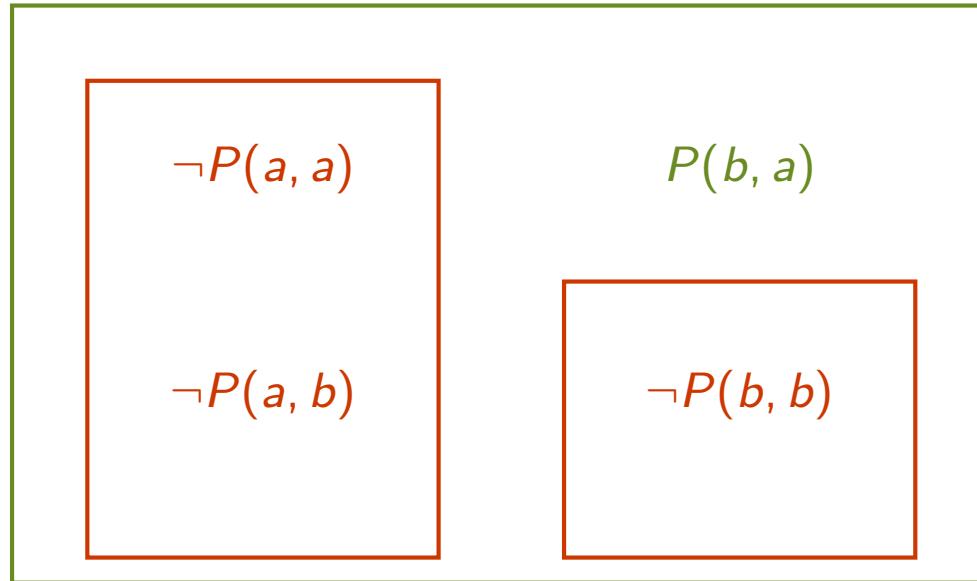
- A branch literal specifies the truth values for all its ground instances, unless there is a more specific literal specifying opposite truth values.

Extracting an Interpretation from a Branch

Branch \mathcal{B} :

$P(x, y)$
—
 $\neg P(a, y)$
—
 $\neg P(b, b)$
—
 $P(a, b)$

Interpretation $\llbracket \mathcal{B} \rrbracket = \{ \dots \}$:



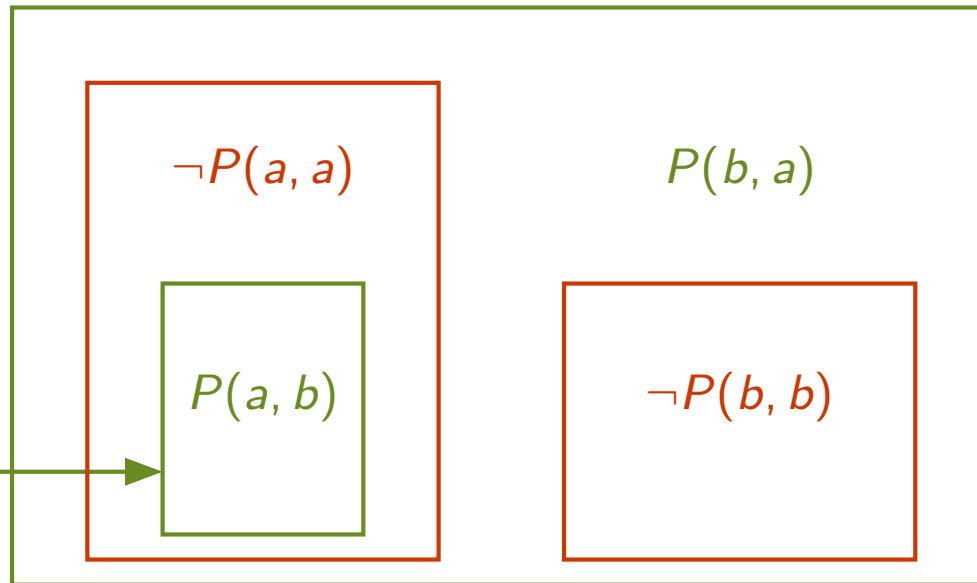
- A branch literal specifies the truth values for all its ground instances, unless there is a more specific literal specifying opposite truth values.

Extracting an Interpretation from a Branch

Branch \mathcal{B} :

$P(x, y)$
—
 $\neg P(a, y)$
—
 $\neg P(b, b)$
—
 $P(a, b)$

Interpretation $\llbracket \mathcal{B} \rrbracket = \{ \dots \}$:



- A branch literal specifies the truth values for all its ground instances, unless there is a more specific literal specifying opposite truth values.

Extracting an Interpretation from a Branch

Branch \mathcal{B} :

$P(x, y)$
|
 $\neg P(a, y)$
|
 $\neg P(b, b)$
|
 $P(a, b)$

Interpretation $\llbracket \mathcal{B} \rrbracket = \{ \dots \}$:

$\{ \quad \neg P(a, a) \quad , \quad P(b, a) \quad ,$

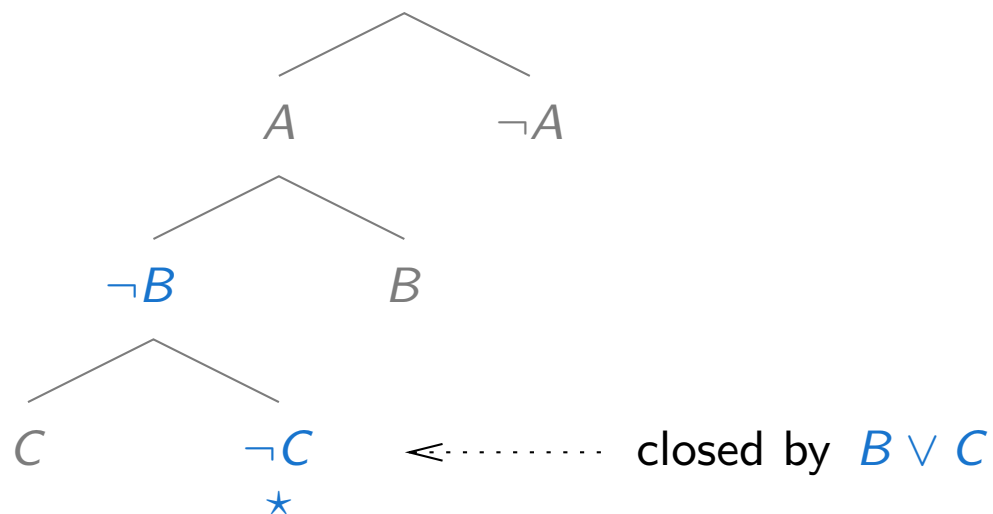
 $P(a, b) \quad , \quad \neg P(b, b) \quad \}$

- A branch literal specifies the truth values for all its ground instances, unless there is a more specific literal specifying opposite truth values.
- The order of literals does not matter.

Calculus: Branch Closure

Purpose: Determine if branch elementary contradicts an input clause.

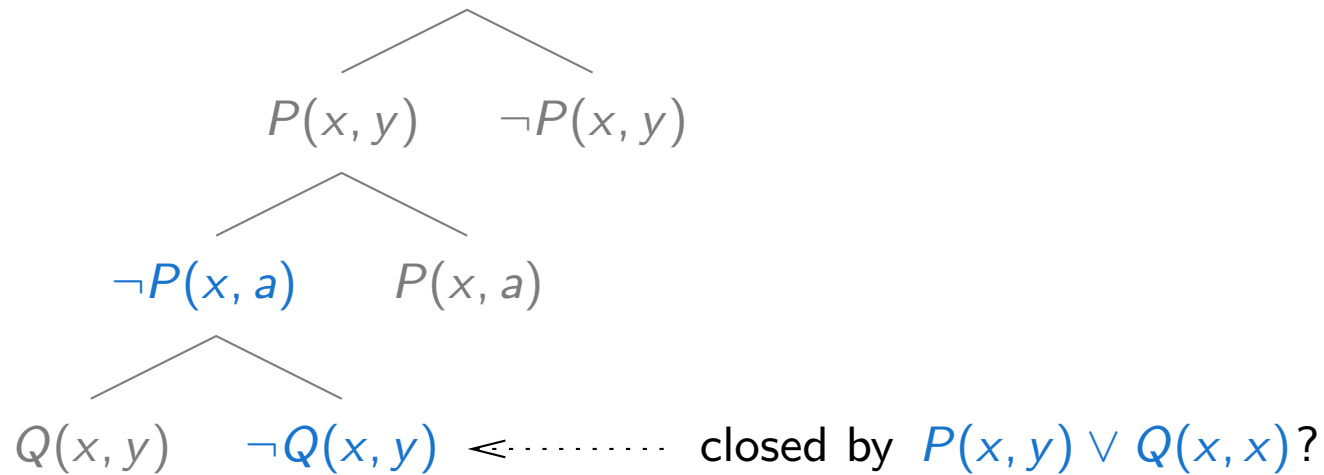
Propositional case:



Calculus: Branch Closure

Purpose: Determine if branch elementary contradicts an input clause.

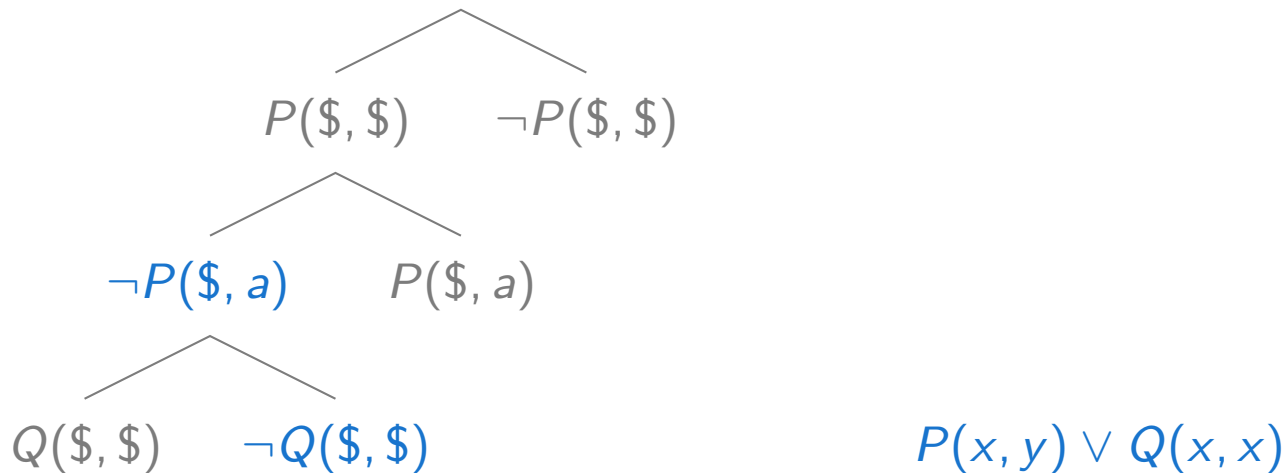
First-Order case:



Calculus: Branch Closure

Purpose: Determine if branch elementary contradicts an input clause.

First-Order case:

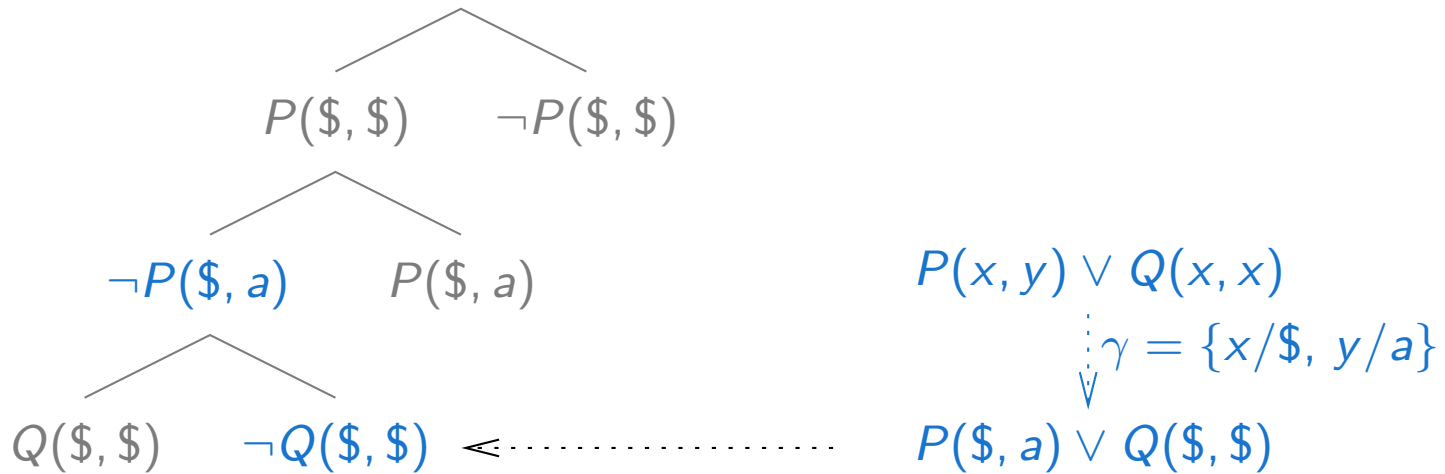


1. Replace **all** variables in tree by a constant \$. Gives propositional tree
- 2.
- 3.

Calculus: Branch Closure

Purpose: Determine if branch elementary contradicts an input clause.

First-Order case:

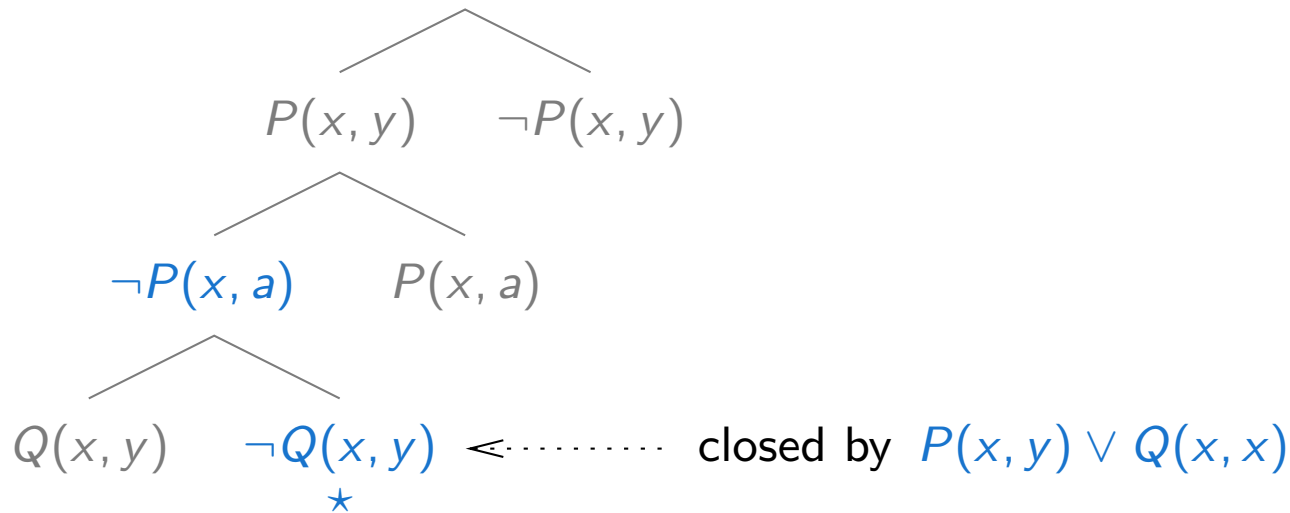


1. Replace all variables in tree by a constant \$. Gives propositional tree
2. Compute matcher γ to propositionally close branch
- 3.

Calculus: Branch Closure

Purpose: Determine if branch elementary contradicts an input clause.

First-Order case:

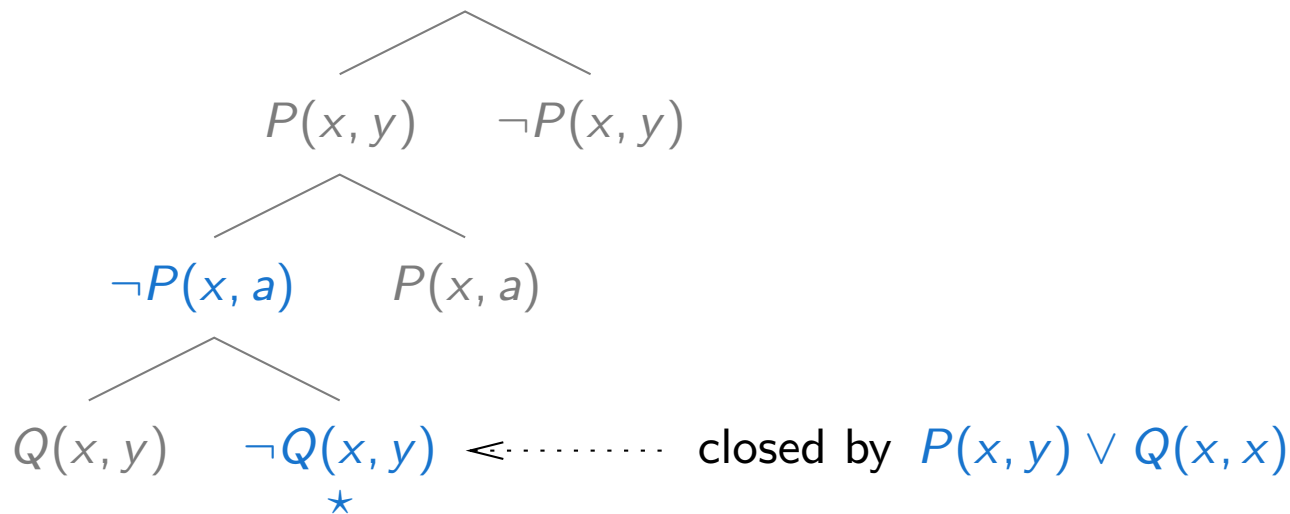


1. Replace all variables in tree by a constant \$. Gives propositional tree
2. Compute matcher γ to propositionally close branch
3. Mark branch as closed (\star)

Calculus: Branch Closure

Purpose: Determine if branch elementary contradicts an input clause.

First-Order case:



1. Replace all variables in tree by a constant \$. Gives propositional tree
2. Compute matcher γ to propositionally close branch
3. Mark branch as closed (\star)

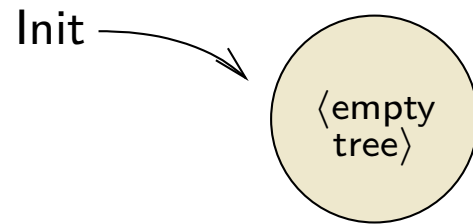
Theorem: FDPLL is sound (because propositional DPLL is sound), and splitting can be done with **arbitrary** literal.

FDPLL Calculus

Input: a clause set \mathcal{S}

Output: “unsatisfiable” or “satisfiable” (if terminates)

Note: Strategy much like in **inner** loop of propositional DPLL:

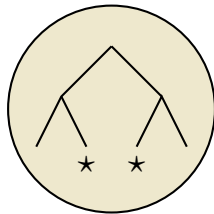


FDPLL Calculus

Input: a clause set \mathcal{S}

Output: “unsatisfiable” or “satisfiable” (if terminates)

Note: Strategy much like in **inner** loop of propositional DPLL:

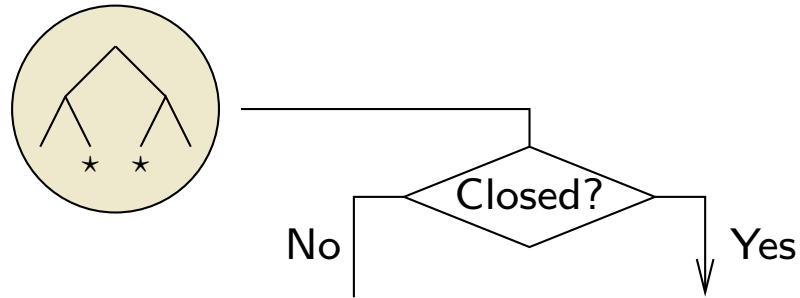


FDPLL Calculus

Input: a clause set \mathcal{S}

Output: “unsatisfiable” or “satisfiable” (if terminates)

Note: Strategy much like in **inner** loop of propositional DPLL:

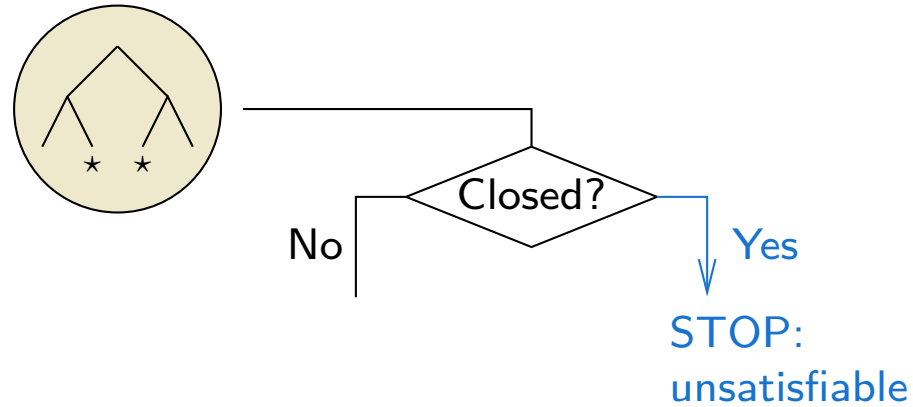


FDPLL Calculus

Input: a clause set \mathcal{S}

Output: “unsatisfiable” or “satisfiable” (if terminates)

Note: Strategy much like in **inner** loop of propositional DPLL:

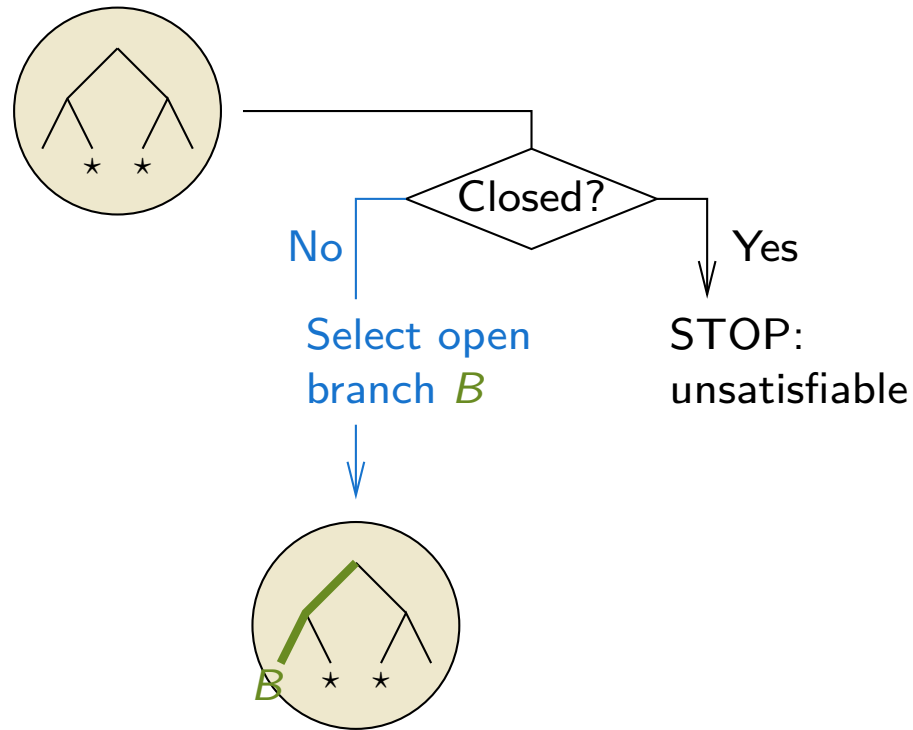


FDPLL Calculus

Input: a clause set \mathcal{S}

Output: “unsatisfiable” or “satisfiable” (if terminates)

Note: Strategy much like in **inner** loop of propositional DPLL:

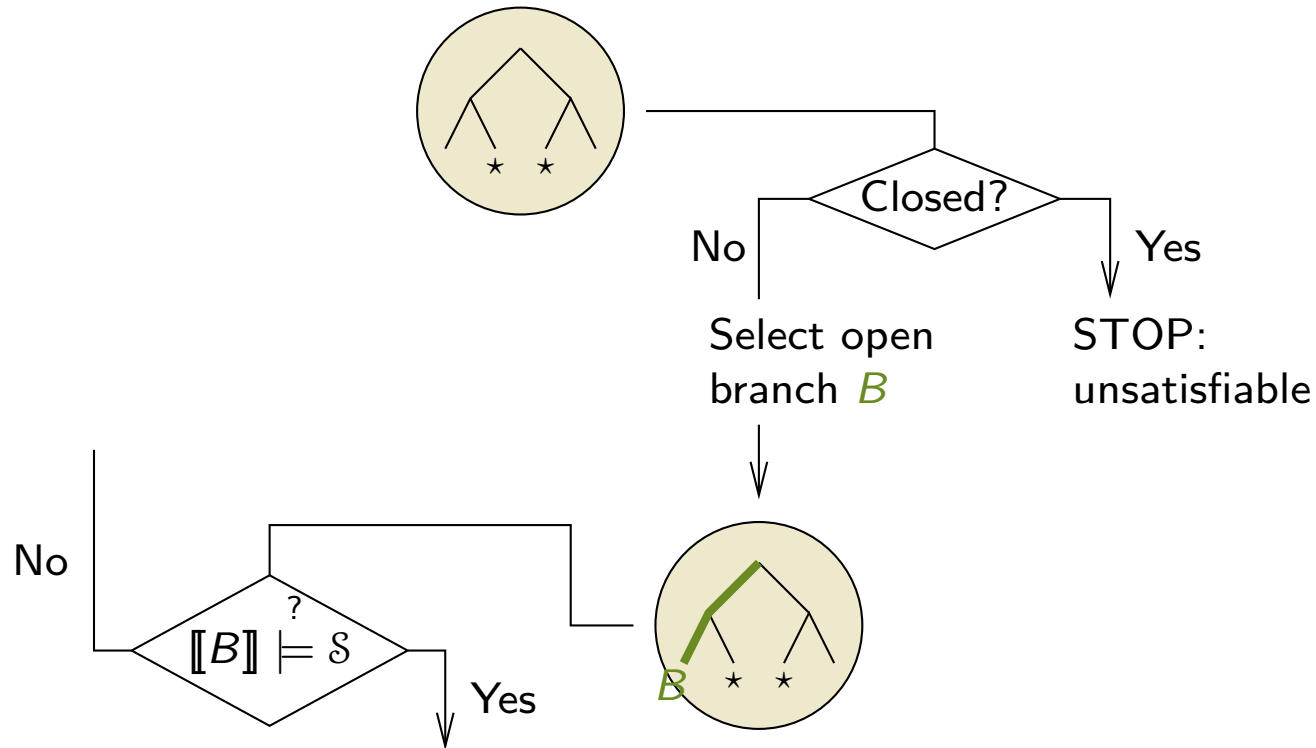


FDPLL Calculus

Input: a clause set \mathcal{S}

Output: “unsatisfiable” or “satisfiable” (if terminates)

Note: Strategy much like in **inner** loop of propositional DPLL:

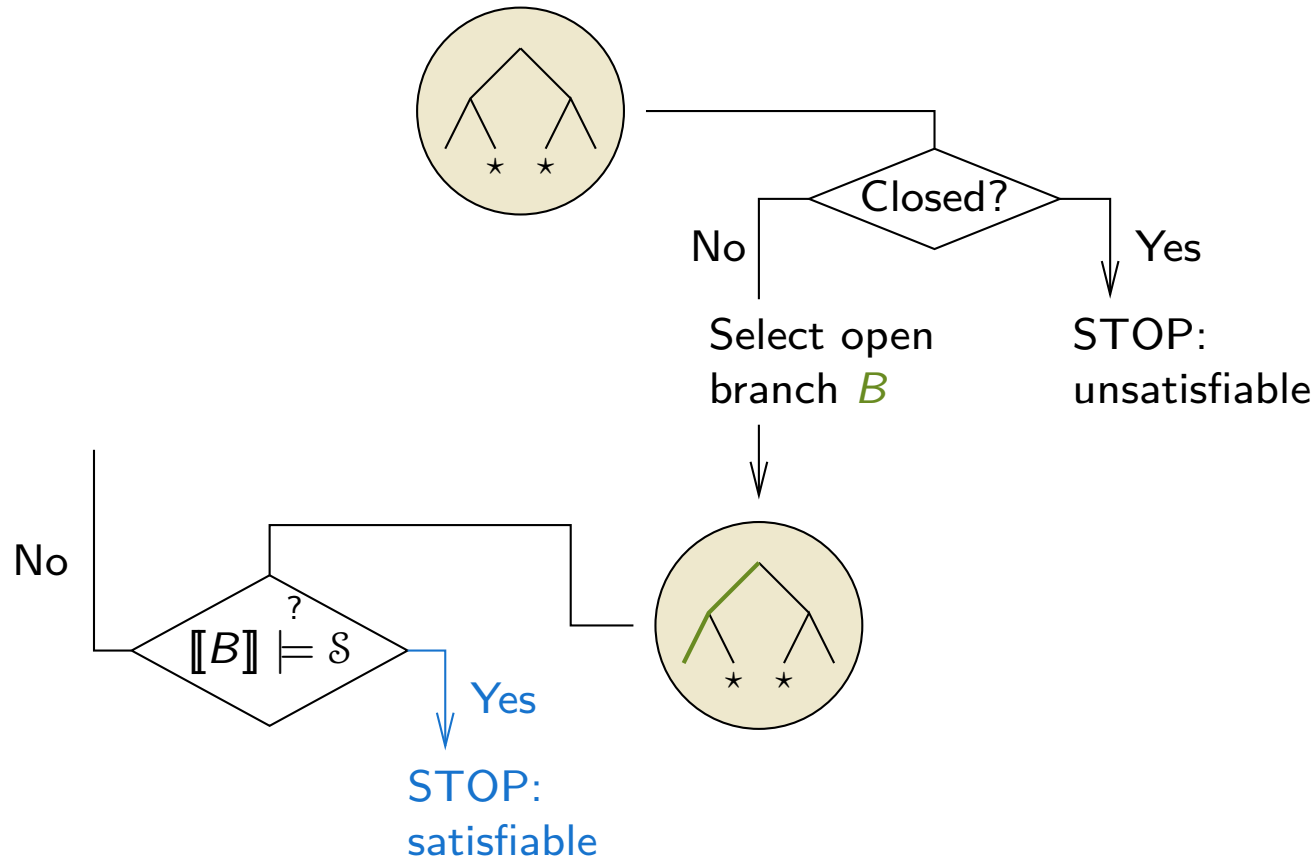


FDPLL Calculus

Input: a clause set \mathcal{S}

Output: “unsatisfiable” or “satisfiable” (if terminates)

Note: Strategy much like in **inner** loop of propositional DPLL:

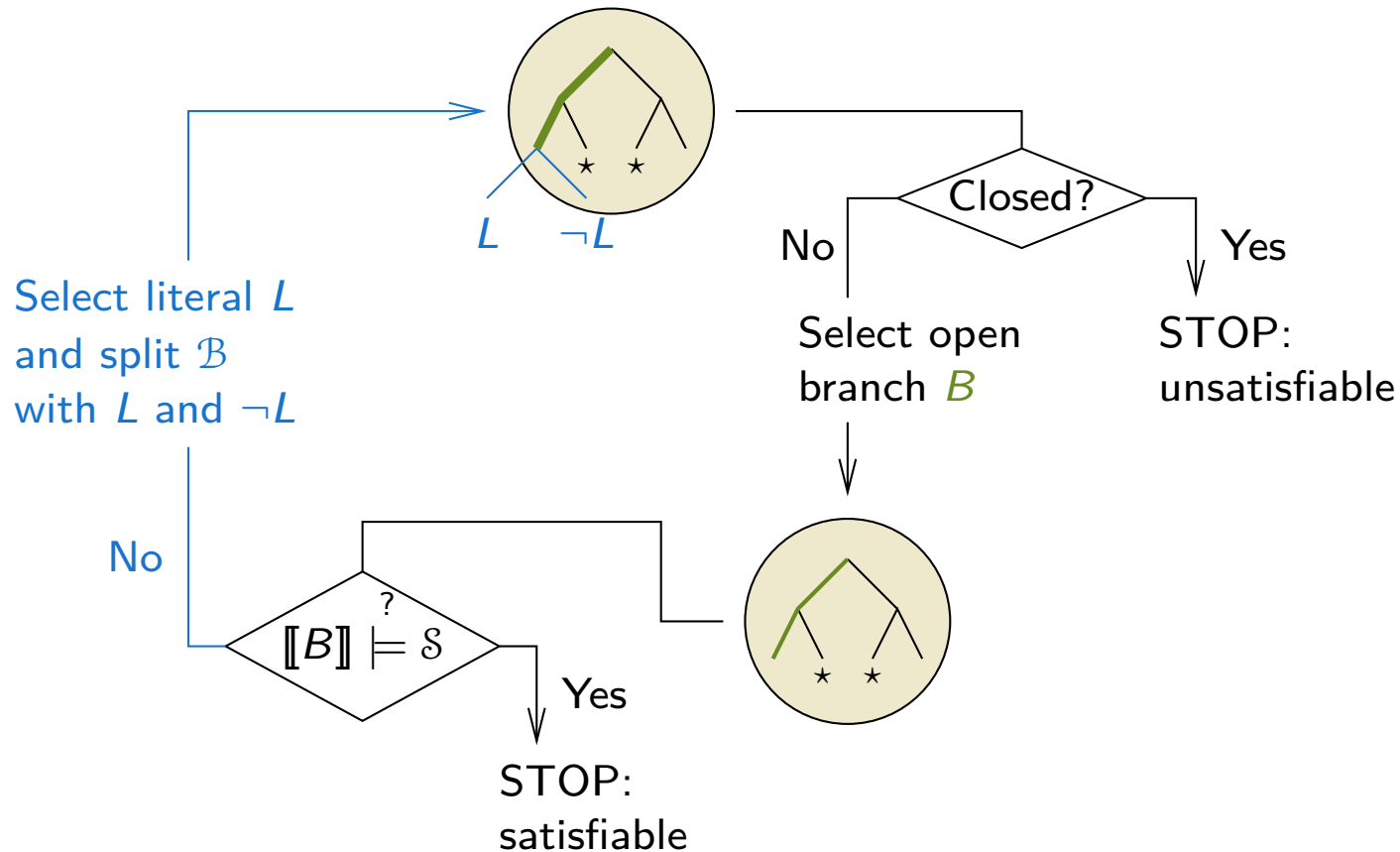


FDPLL Calculus

Input: a clause set \mathcal{S}

Output: “unsatisfiable” or “satisfiable” (if terminates)

Note: Strategy much like in **inner** loop of propositional DPLL:

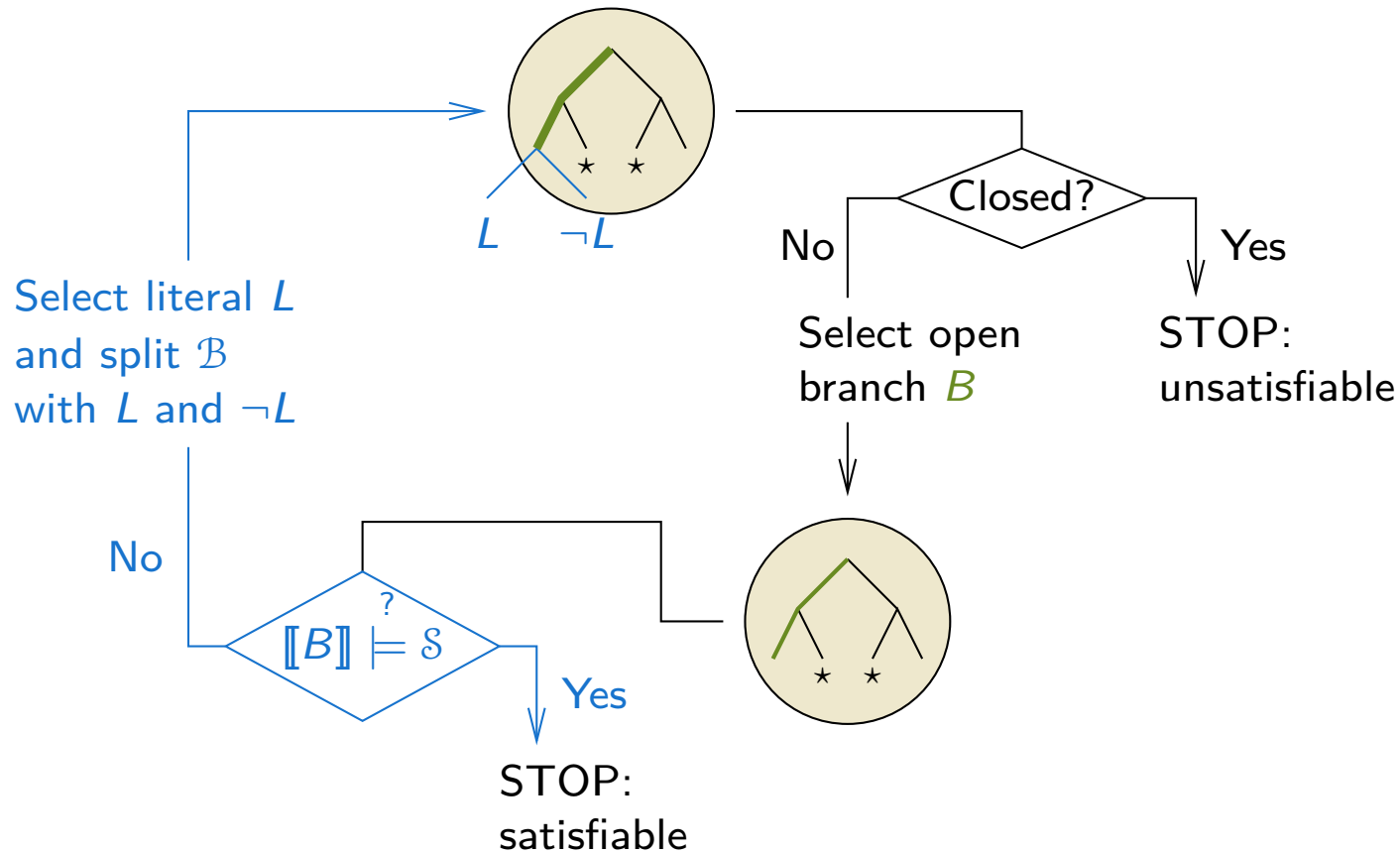


FDPLL Calculus

Input: a clause set \mathcal{S}

Output: “unsatisfiable” or “satisfiable” (if terminates)

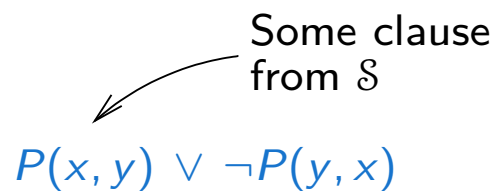
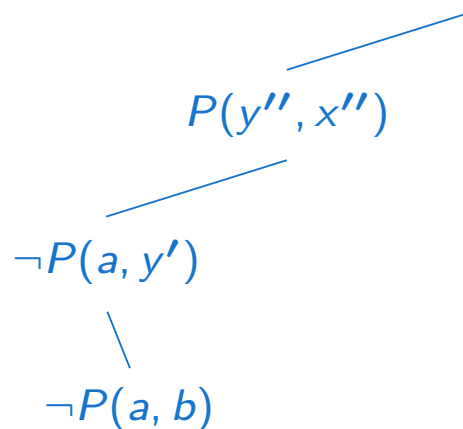
Note: Strategy much like in **inner** loop of propositional DPLL:



Next: Testing $[[B]] \models \mathcal{S}$ and splitting

Calculus: The Splitting Rule

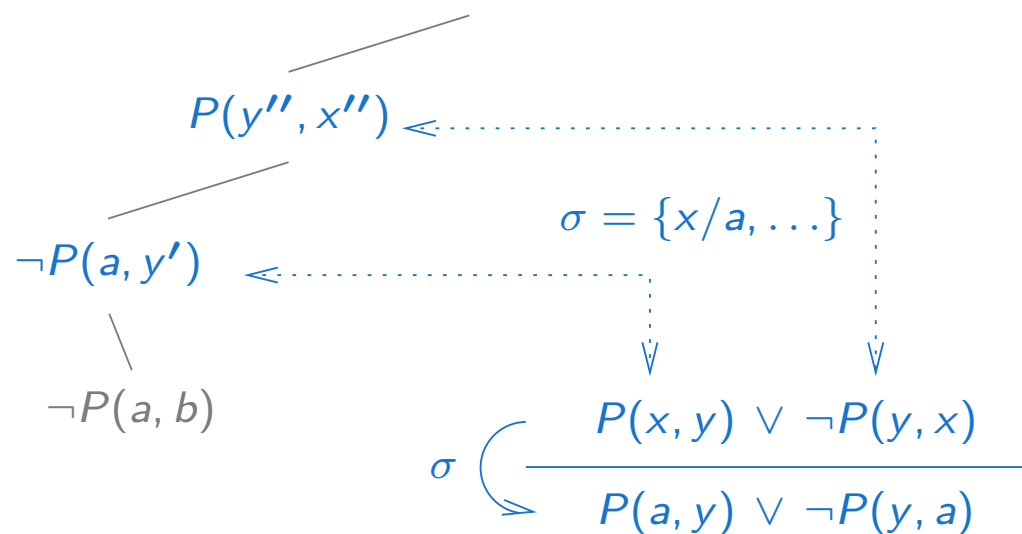
Purpose: Satisfy a clause that is currently “false”



- 1.
- 2.
- 3.

Calculus: The Splitting Rule

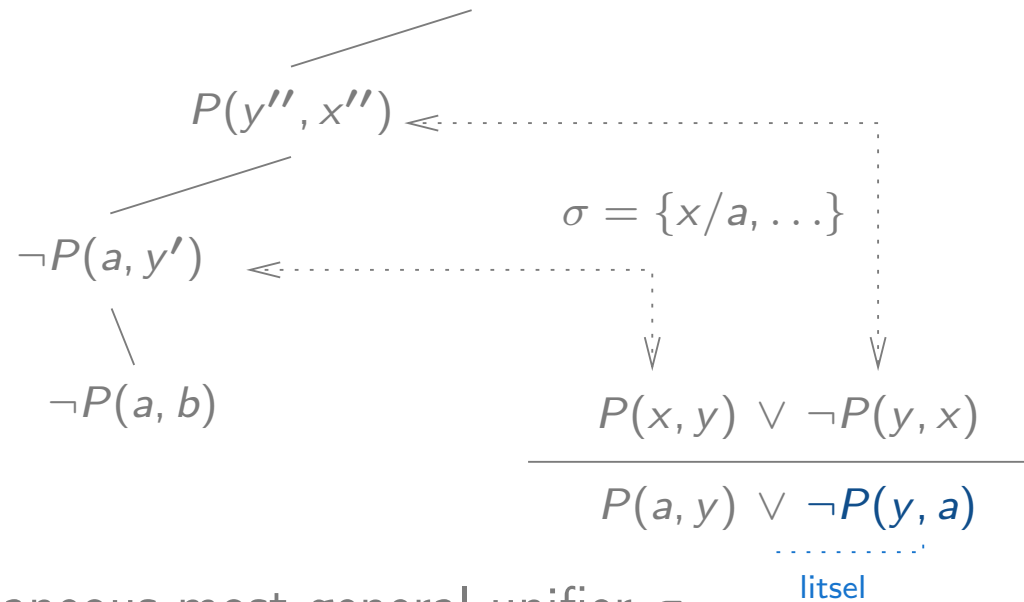
Purpose: Satisfy a clause that is currently “false”



1. Compute simultaneous most general unifier σ
- 2.
- 3.

Calculus: The Splitting Rule

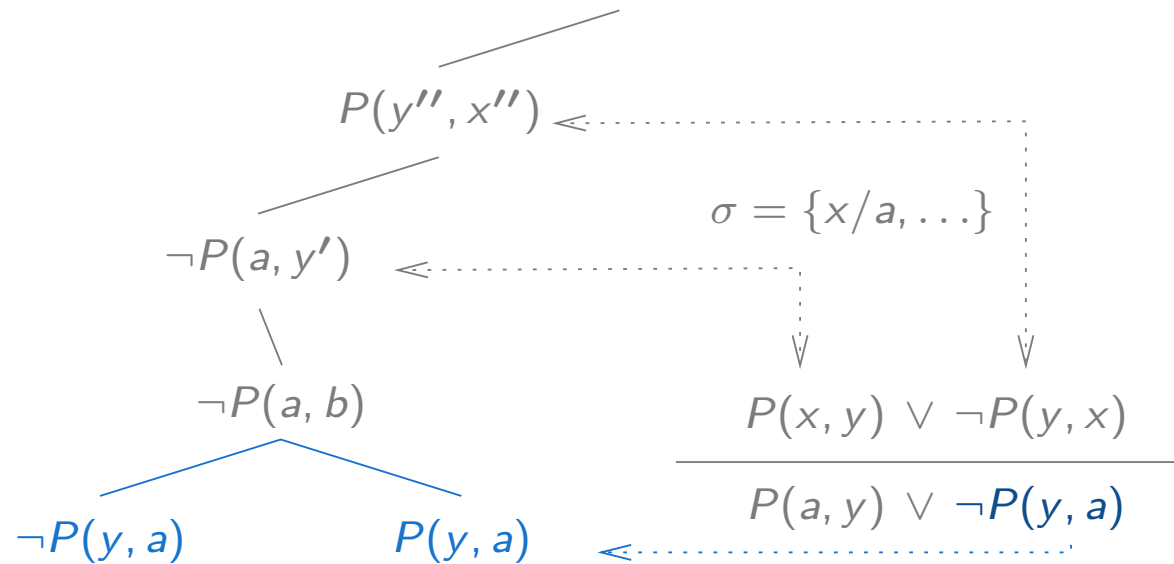
Purpose: Satisfy a clause that is currently “false”



1. Compute simultaneous most general unifier σ
2. Select from clause instance a literal not on branch
- 3.

Calculus: The Splitting Rule

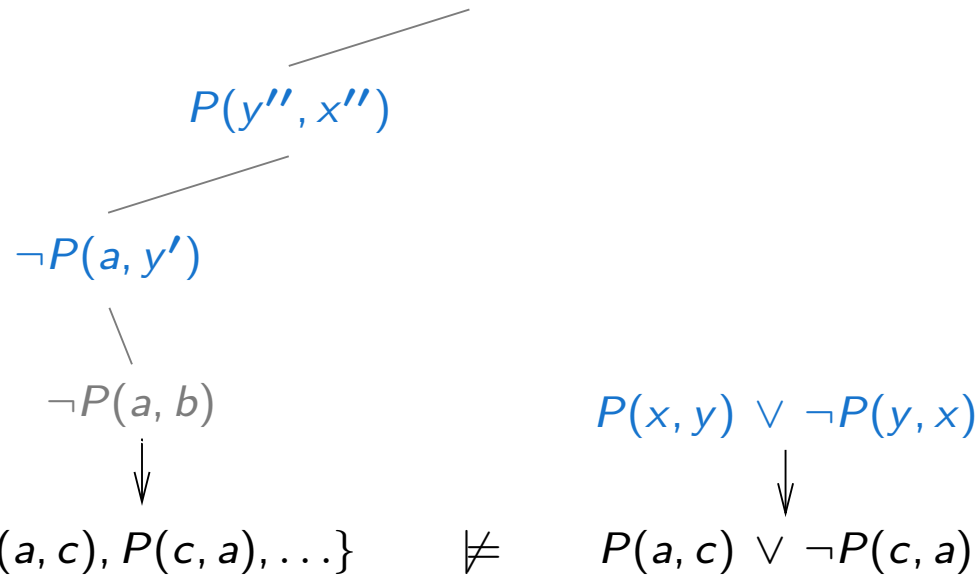
Purpose: Satisfy a clause that is currently “false”



1. Compute simultaneous most general unifier σ
2. Select from clause instance a literal not on branch
3. Split with this literal

Calculus: The Splitting Rule

Purpose: Satisfy a clause that is currently “false”

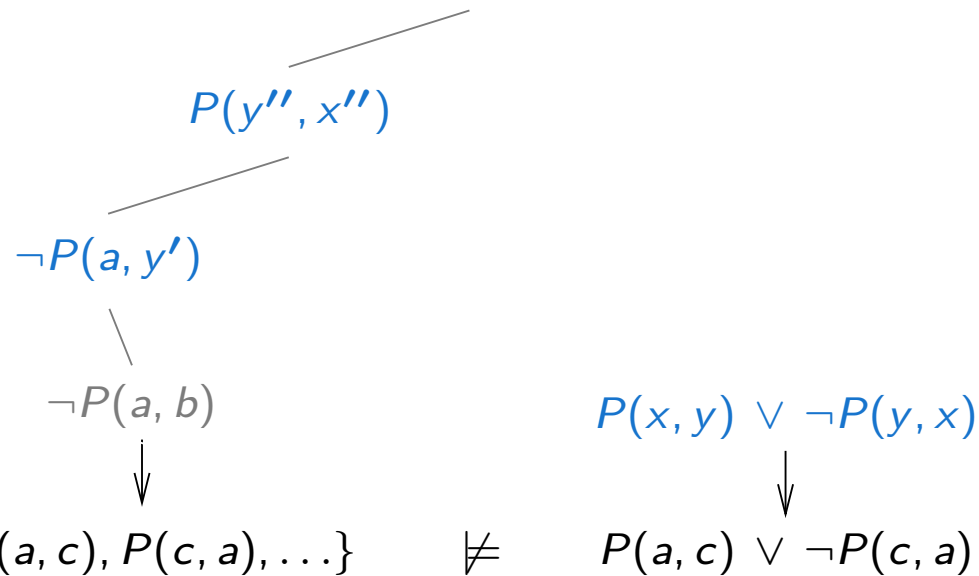


1. Compute simultaneous most general unifier σ
2. Select from clause instance a literal not on branch
3. Split with this literal

This split was really necessary!

Calculus: The Splitting Rule

Purpose: Satisfy a clause that is currently “false”



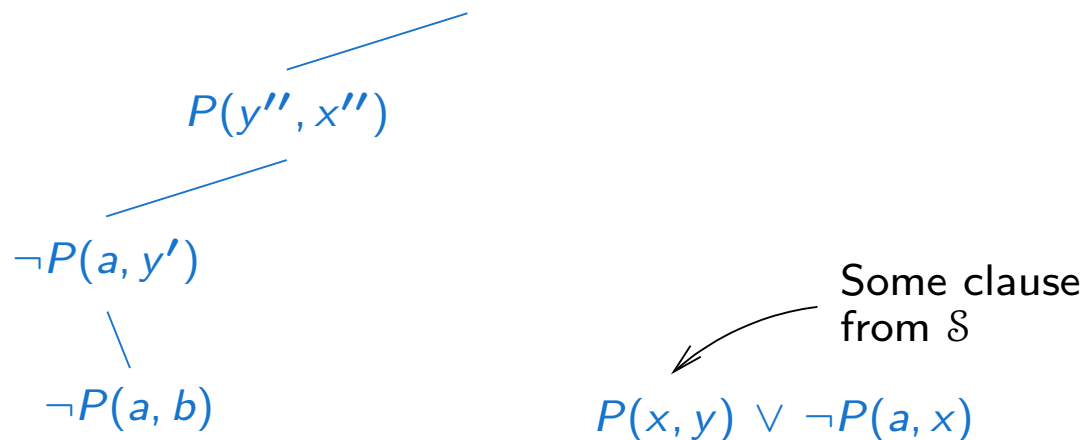
1. Compute simultaneous most general unifier σ
2. Select from clause instance a literal not on branch
3. Split with this literal

This split was really necessary!

Proposition: If $\llbracket \mathcal{B} \rrbracket \neq \mathcal{S}$, then split is applicable to some clause from \mathcal{S}

Calculus: The Splitting Rule – Another Example

Purpose: Satisfy a clause that is currently “false”

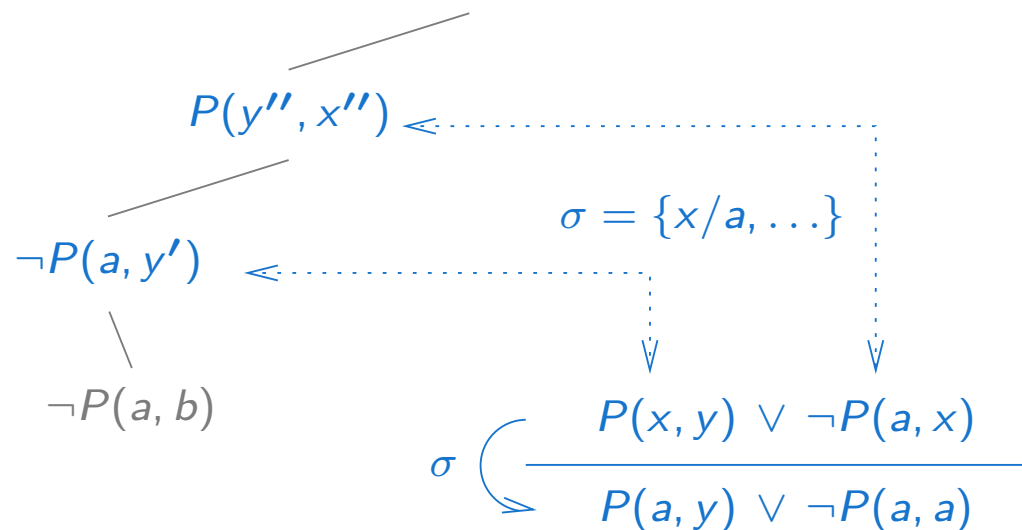


1.

2.

Calculus: The Splitting Rule – Another Example

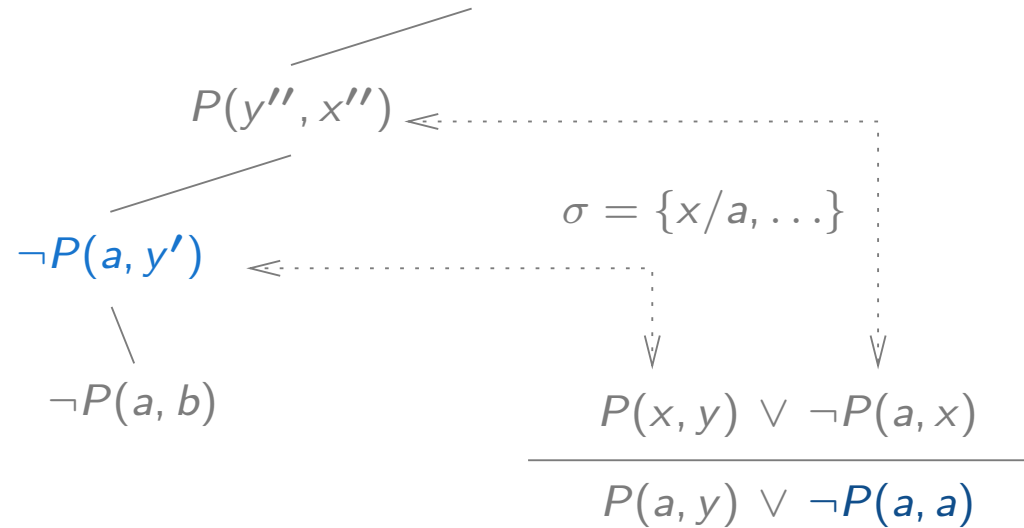
Purpose: Satisfy a clause that is currently “false”



1. Compute MGU σ of clause against branch literals
- 2.

Calculus: The Splitting Rule – Another Example

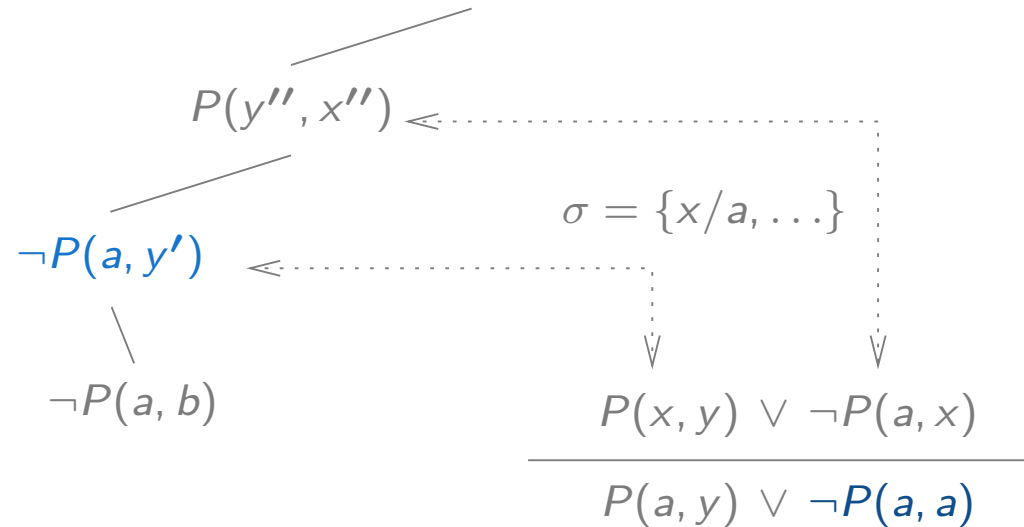
Purpose: Satisfy a clause that is currently “false”



1. Compute MGU σ of clause against branch literals
2. If clause contains “true” literal, then split is not applicable

Calculus: The Splitting Rule – Another Example

Purpose: Satisfy a clause that is currently “false”

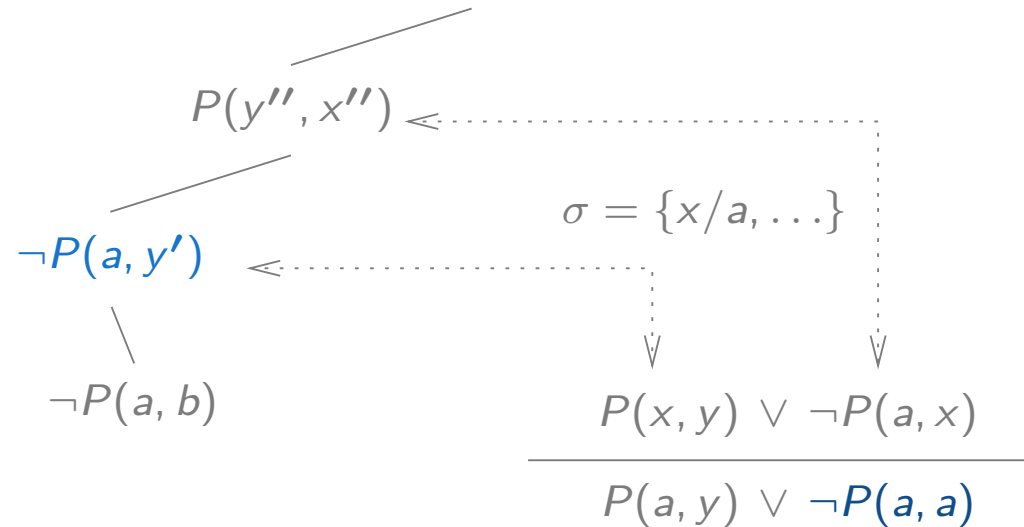


1. Compute MGU σ of clause against branch literals
2. If clause contains “true” literal, then split is not applicable

Non-applicability is a redundancy test

Calculus: The Splitting Rule – Another Example

Purpose: Satisfy a clause that is currently “false”



1. Compute MGU σ of clause against branch literals
2. If clause contains “true” literal, then split is not applicable

Non-applicability is a redundancy test

Proposition: If for no clause split is applicable, $\llbracket \mathcal{B} \rrbracket \models \mathcal{S}$ holds

FDPLL Complete Example

| | | |
|-----|--|---|
| (1) | <code>train(X,Y) ; flight(X,Y).</code> | <code>%% train from X to Y or flight from X to</code> |
| (2) | <code>-flight(koblenz,X).</code> | <code>%% no flight from koblenz to anywhere.</code> |
| (3) | <code>flight(X,Y) :- flight(Y,X).</code> | <code>%% flight is symmetric.</code> |
| (4) | <code>connect(X,Y) :- flight(X,Y).</code> | <code>%% a flight is a connection.</code> |
| (5) | <code>connect(X,Y) :- train(X,Y).</code> | <code>%% a train is a connection.</code> |
| (6) | <code>connect(X,Z) :- connect(X,Y),</code> <code> connect(Y,Z).</code> | <code>%% connection is a transitive relation.</code> |

FDPLL Complete Example

```
(1)  train(X,Y) ; flight(X,Y).          %% train from X to Y or flight from X to
(2)  -flight(koblenz,X).                %% no flight from koblenz to anywhere.
(3)  flight(X,Y) :- flight(Y,X).        %% flight is symmetric.
(4)  connect(X,Y) :- flight(X,Y).        %% a flight is a connection.
(5)  connect(X,Y) :- train(X,Y).         %% a train is a connection.
(6)  connect(X,Z) :- connect(X,Y),      %% connection is a transitive relation.
      connect(Y,Z).
```

Computed Model (as output by implementation)

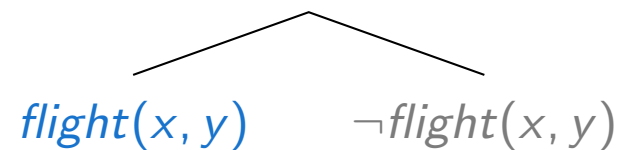
```
(1)  + flight(X, Y)
(2)  - flight(koblenz, X)
(3)  - flight(X, koblenz)
(4)  + train(koblenz, Y)
(5)  + train(Y, koblenz)
(6)  + connect(X, Y)
```

FDPLL Model Computation Example - Derivation

⟨empty tree⟩

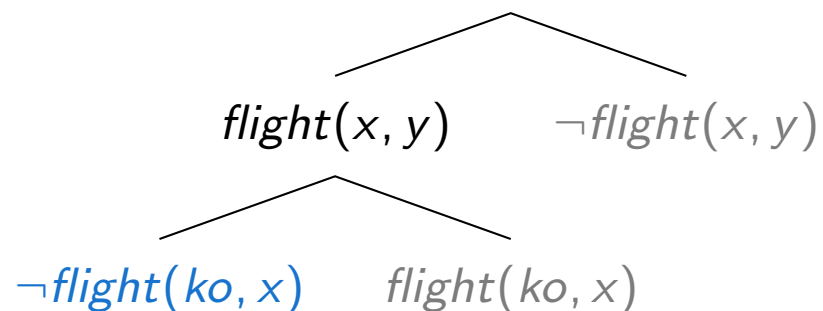
Clause instance used in inference: $\textit{train}(x, y) \vee \textit{flight}(x, y)$

FDPLL Model Computation Example - Derivation



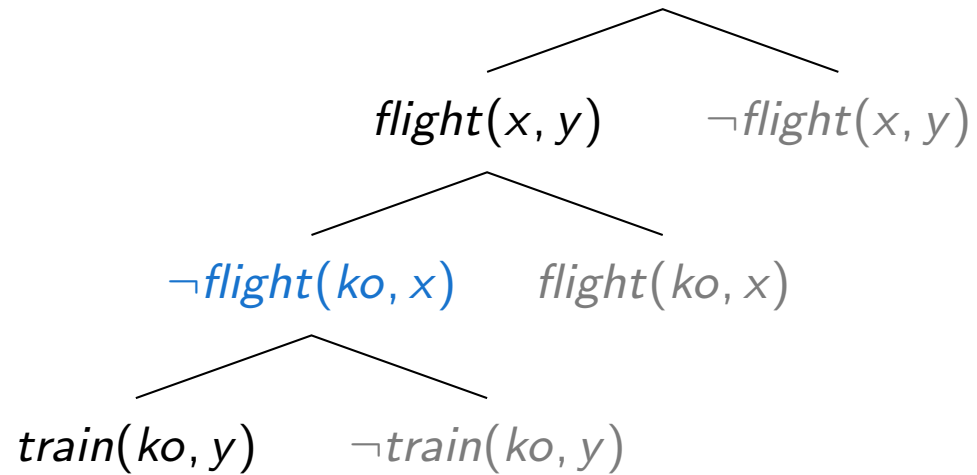
Clause instance used in inference: $\neg flight(ko, x)$

FDPLL Model Computation Example - Derivation



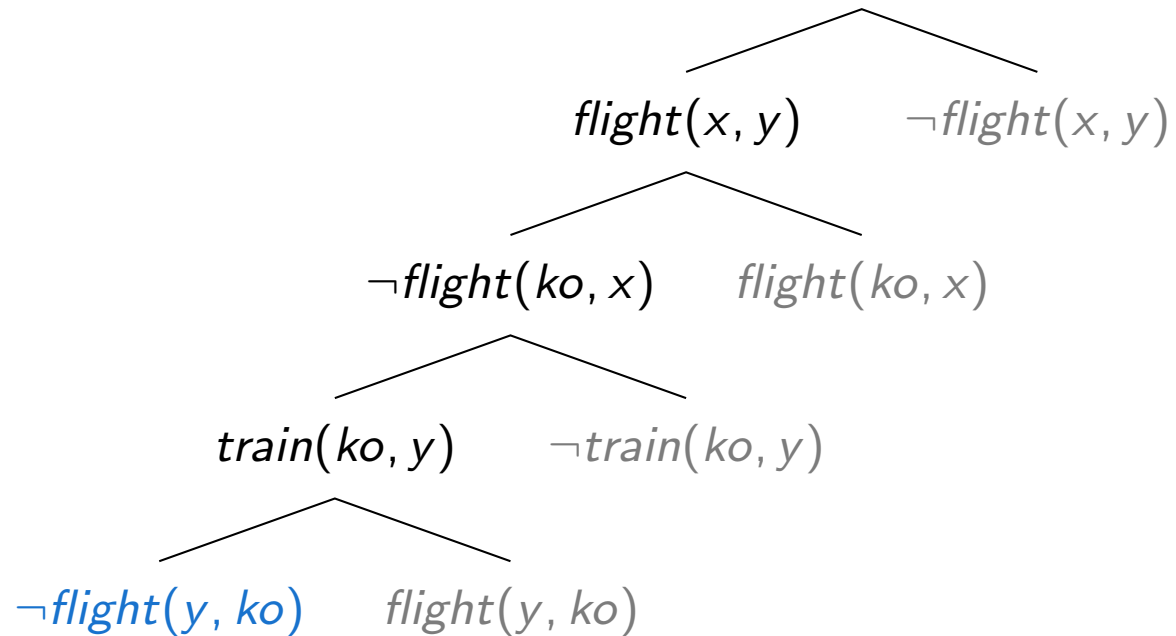
Clause instance used in inference: $train(ko, y) \vee flight(ko, y)$

FDPLL Model Computation Example - Derivation



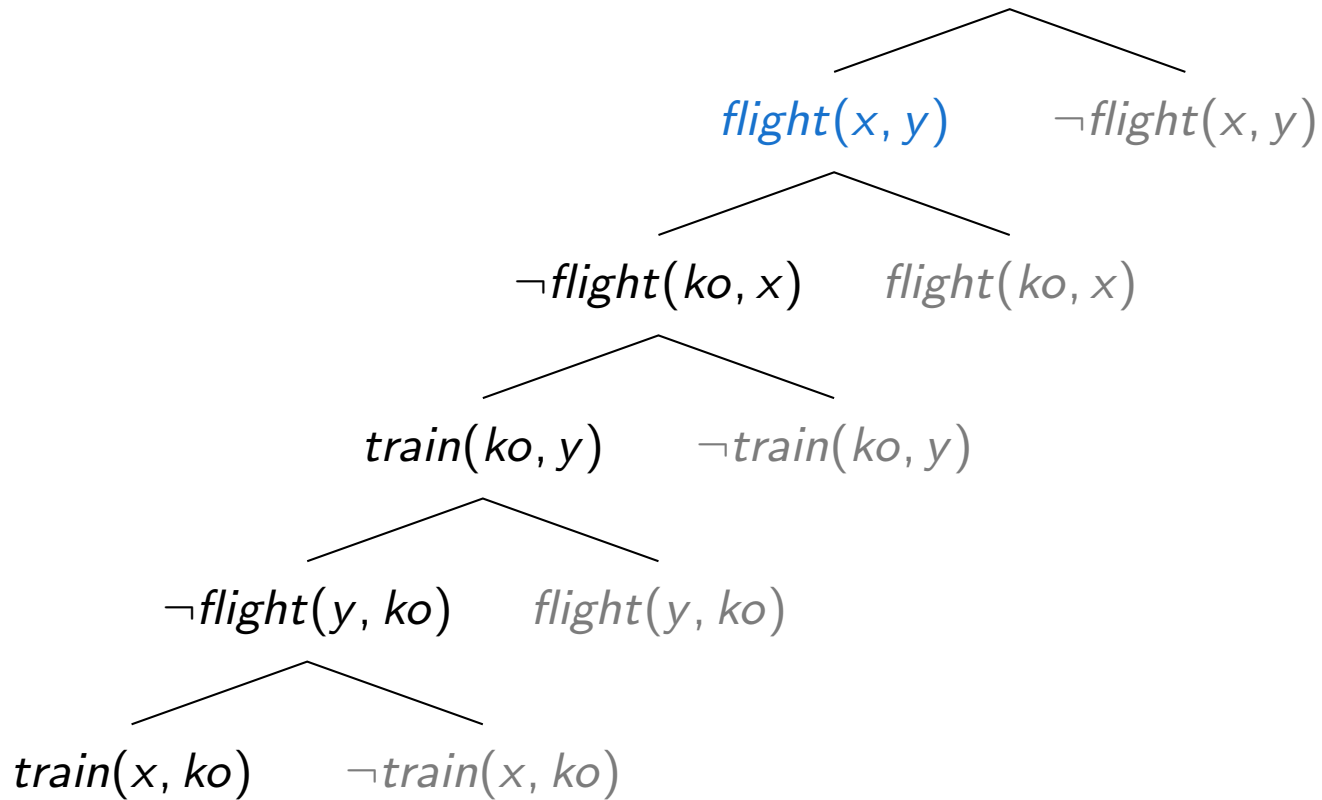
Clause instance used in inference: $flight(ko, y) \vee \neg flight(y, ko)$

FDPLL Model Computation Example - Derivation



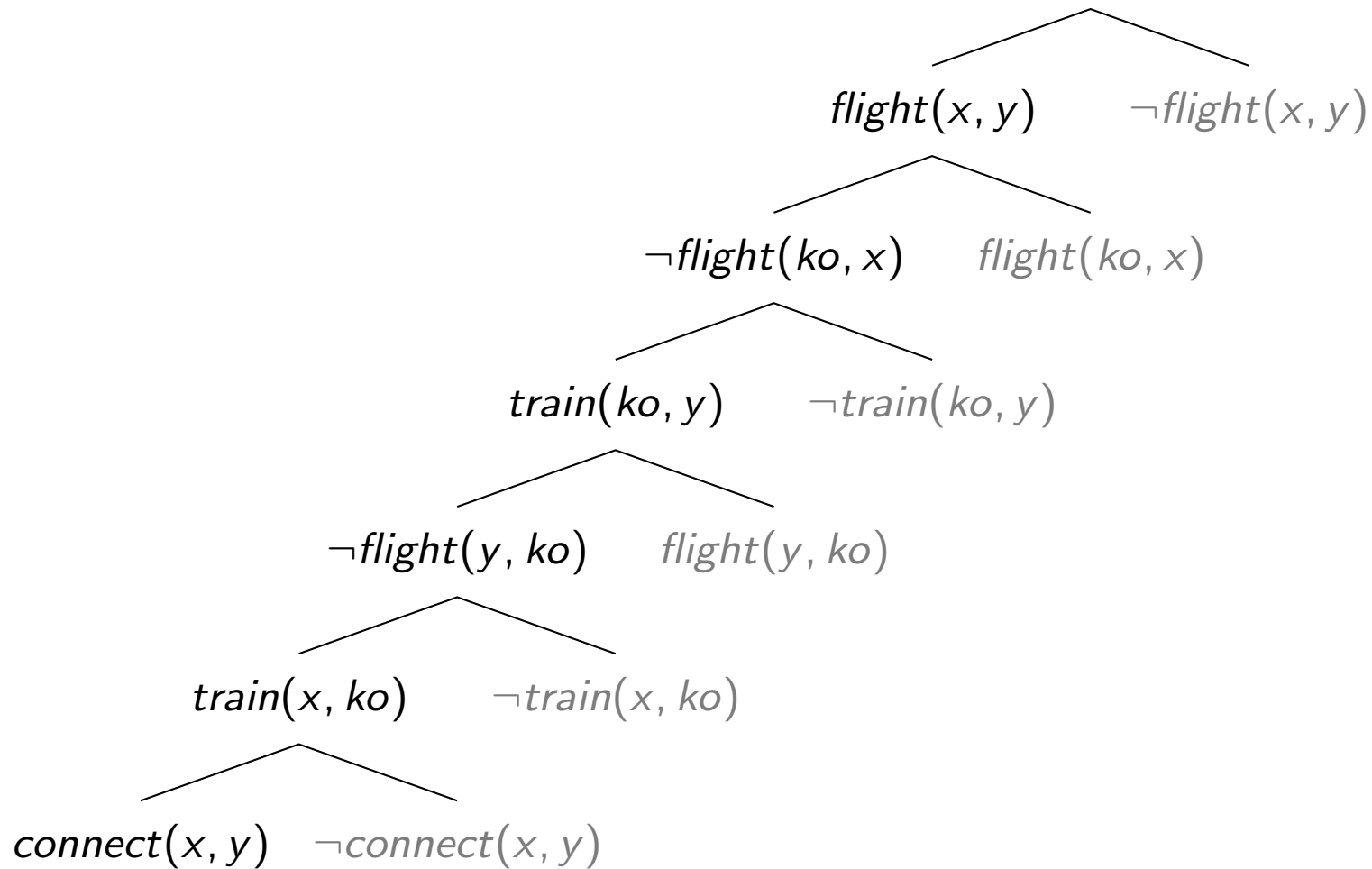
Clause instance used in inference: $train(x, ko) \vee flight(x, ko)$

FDPLL Model Computation Example - Derivation



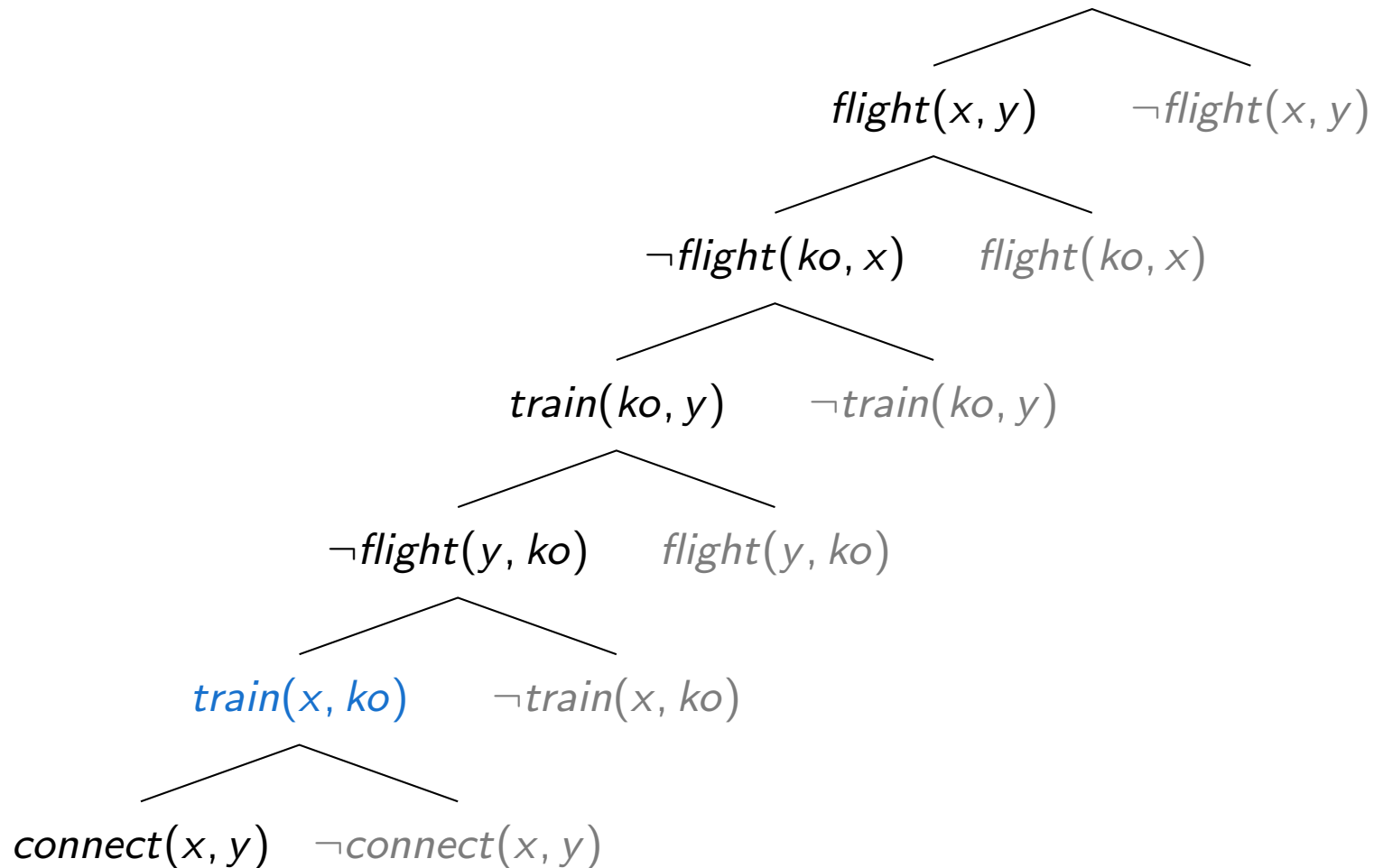
Clause instance used in inference: $connect(x, y) \vee \neg flight(x, y).$

FDPLL Model Computation Example - Derivation



Done. Return “satisfiable with model $\{flight(x, y), \dots, connect(x, y)\}$ ”

FDPLL Model Computation Example - Derivation



Done. Return “satisfiable with model $\{flight(x, y), \dots, connect(x, y)\}$ ”

Redundancy: Instance **not** used in inference: $connect(x, ko) \vee \neg train(x, ko)$

Summary / Properties

Summary

- DPLL data structure lifted to first-order logic level
- Two simple inference rules, controlled by unification
- Computes with interpretations/models
- Semantical redundancy criterion

Summary / Properties

Summary

- DPLL data structure lifted to first-order logic level
- Two simple inference rules, controlled by unification
- Computes with interpretations/models
- Semantical redundancy criterion

Properties

- Soundness and completeness (with fair strategy).
- Extension: More efficient reasoning with **unit clauses** (e.g. $\forall x P(x, a)$)
- Proof convergence (avoids backtracking the semantics trees)
- Decides function-free clause logic (Bernays-Schönfinkel class)
Covers e.g. Basic modal logic, Description logic, DataLog
Returns model in satisfiable case
- Can be combined with Resolution, equality inference rules

Calculi in Comparison

Consider a transitivity clause $P(x, z) \leftarrow P(x, y) \wedge P(y, z)$.

[Bachmair & Ganzinger, Handbook AR 2001], [Fermüller et. al., Handbook AR 2001]

Resolution:

$$P(x, z') \leftarrow P(x, y) \wedge P(y, z) \wedge P(z, z')$$

$$P(x, z'') \leftarrow P(x, y) \wedge P(y, z) \wedge P(z, z') \wedge P(z', z'')$$

Does not terminate for function-free clause sets

Complicated to extract model

Very good on other classes, Equality

Rigid Variable Approaches:

$$P(x', z') \leftarrow P(x', y') \wedge P(y', z')$$

$$P(x'', z'') \leftarrow P(x'', y'') \wedge P(y'', z'')$$

Tableaux and Connection Methods

Unpredictable number of variants, weak redundancy test

Difficult to avoid unnecessary (!) backtracking

Difficult to extract model

Calculi in Comparison

Consider a transitivity clause $P(x, z) \leftarrow P(x, y) \wedge P(y, z)$.

Instance Based Methods:

$$P(x, z) \leftarrow P(x, y) \wedge P(y, z)$$

$$P(a, z) \leftarrow P(a, y) \wedge P(y, b)$$

FDPLL, Model Evolution,
Inst-Gen, Disconnection Tableaux,
Overview paper on my web page

Weak redundancy criterion (no subsumption)

Need to keep clause instances (memory problem)

Clauses do not become longer (cf. Resolution)

May delete variant clauses (cf. Rigid Variable Approach)

Contents

Introduction

Logics and Reasoning Service (already done)

Methods for Automated Theorem Proving

Overview of some widely used general methods

- Propositional SAT solving
- First-order logic and clause normal forms
- Proof Procedures Based on Herbrand's Theorem
- The Resolution calculus
- Instance-based methods
- **Model generation**

Theory Reasoning

Methods to reason with specific background theories

- Paramodulation (Equality)
- Satisfiability Modulo Theories (SMT)
- Quantifier elimination for linear real arithmetic
- Combining multiple theories

Model Generation

For every FOL formula F exactly one of these three cases applies:

1. F is unsatisfiable

(Complete) theorem prover will detect this eventually (in theory)

2. F is satisfiable with only infinite models

Example: $nat(0)$

$lt(x, succ(N)) \leftarrow nat(x)$

$nat(succ(x)) \leftarrow nat(x)$

$lt(x, z) \leftarrow lt(x, y) \wedge lt(y, z)$

$\neg lt(x, x)$

Sometimes resolution refinements help to detect such cases

3. F is satisfiable with a finite model

A **finite model-finder** will detect this eventually (in theory)

The rest of this section is concerned with computing finite models.

Model Generation

Two main applications:

- To disprove a “false” theorem by means of a counterexample, i.e., a “countermodel”
- A model provides the expected answer, as in the n-queens puzzle

Some applications

Planning: Can be formalised as propositional satisfiability problem.

[Kautz& Selman, AAAI96; Dimopolous et al, ECP97]

Diagnosis: Minimal models of *abnormal* literals (circumscription). [Reiter, AI87]

Databases: View materialisation, View Updates, Integrity Constraints.

Nonmonotonic reasoning: Various semantics (GCWA, Well-founded, Perfect, Stable, . . .), all based on minimal models. [Inoue et al, CADE 92]

Software Verification: Counterexamples to conjectured theorems.

Theorem proving: Counterexamples to conjectured theorems.

Finite models of quasigroups, (MGTP/G). [Fujita et al, IJCAI 93]

Example - Discourse Representation

Natural Language Processing:

- Maintain models $\mathcal{I}_1, \dots, \mathcal{I}_n$ as different readings of discourses:

$$\mathcal{I}_i \models BG\text{-}Knowledge \cup Discourse_so_far$$

Example - Discourse Representation

Natural Language Processing:

- Maintain models $\mathcal{I}_1, \dots, \mathcal{I}_n$ as different readings of discourses:

$$\mathcal{I}_i \models BG\text{-}Knowledge \cup Discourse_so_far$$

- Consistency checks (“Mia’s husband loves Sally. She is not married.”)

$$BG\text{-}Knowledge \cup Discourse_so_far \not\models \neg New_utterance$$

iff $BG\text{-}Knowledge \cup Discourse_so_far \cup New_utterance$ is **satisfiable**

Example - Discourse Representation

Natural Language Processing:

- Maintain models $\mathcal{I}_1, \dots, \mathcal{I}_n$ as different readings of discourses:

$$\mathcal{I}_i \models BG\text{-}Knowledge \cup Discourse_so_far$$

- Consistency checks (“Mia’s husband loves Sally. She is not married.”)

$$BG\text{-}Knowledge \cup Discourse_so_far \not\models \neg New_utterance$$

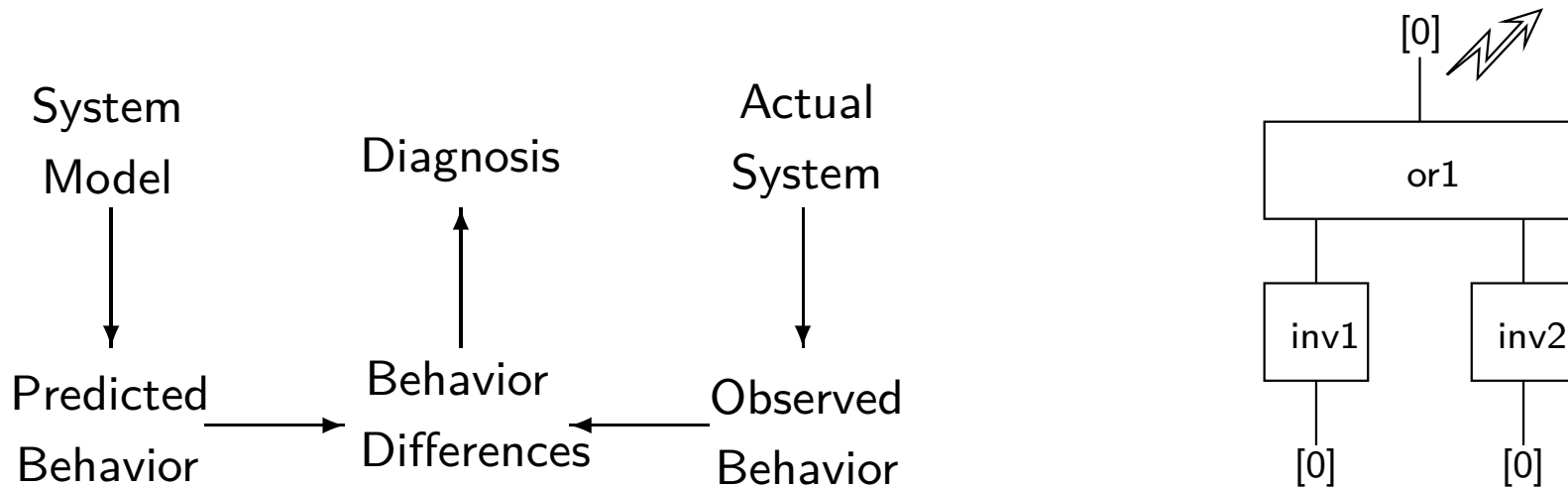
iff $BG\text{-}Knowledge \cup Discourse_so_far \cup New_utterance$ is **satisfiable**

- Informativity checks (“Mia’s husband loves Sally. She is married.”)

$$BG\text{-}Knowledge \cup Discourse_so_far \not\models New_utterance$$

iff $BG\text{-}Knowledge \cup Discourse_so_far \cup \neg New_utterance$ is **satisfiable**

Example - Model-Based Diagnosis [Reiter 87]



Formal Treatment:

$COMP$ = Components

SD = System description, components are allowed to perform “abnormal”

OBS = Observations

Def. **Diagnosis**: Some minimal $\Delta \subseteq COMP$ such that

$SD \cup OBS \cup \{ab(\Delta)\} \cup \{\neg ab(COMP - \Delta)\}$ is satisfiable

Formal Treatment

System Description $SD =$

OR1: $\neg(ab(or1)) \rightarrow high(or1, o) \leftrightarrow (high(or1, i1) \vee high(or1, i2))$

INV1: $\neg(ab(inv1)) \rightarrow high(inv1, o) \leftrightarrow \neg(high(inv1, i))$

INV2: $\neg(ab(inv2)) \rightarrow high(inv2, o) \leftrightarrow \neg(high(inv2, i))$

CONN1: $high(inv1, o) \leftrightarrow high(or1, i1)$

CONN2: $high(inv2, o) \leftrightarrow high(or1, i2)$

Observations $OBS =$

LOW_INV1_I: $\neg(high(inv1, i))$

LOW_INV1_I: $\neg(high(inv2, i))$

LOW_OR1_O: $\neg(high(or1, o))$

Task: Find minimal $\Delta \subseteq \{ab(or1), ab(inv1), ab(inv2)\}$ such that

$SD \cup OBS \cup \Delta \cup \neg\overline{\Delta}$ is satisfiable

Example - Group Theory

The following axioms specify a group

$$\forall x, y, z : (x * y) * z = x * (y * z) \quad (\text{associativity})$$

$$\forall x : e * x = x \quad (\text{left -- identity})$$

$$\forall x : i(x) * x = e \quad (\text{left -- inverse})$$

Does

$$\forall x, y : x * y = y * x \quad (\text{commutat.})$$

follow?

Example - Group Theory

The following axioms specify a group

$$\forall x, y, z : (x * y) * z = x * (y * z) \quad (\text{associativity})$$

$$\forall x : e * x = x \quad (\text{left -- identity})$$

$$\forall x : i(x) * x = e \quad (\text{left -- inverse})$$

Does

$$\forall x, y : x * y = y * x \quad (\text{commutat.})$$

follow?

No, it does not

Example - Group Theory

Counterexample: a group with finite domain of size 6, where the elements 2 and 3 are not commutative: Domain: $\{1, 2, 3, 4, 5, 6\}$

$e : 1$

| | | | | | | |
|-------|---|---|---|---|---|---|
| $i :$ | 1 | 2 | 3 | 4 | 5 | 6 |
| | 1 | 2 | 3 | 5 | 4 | 6 |

| | | | | | | | |
|-------|---|---|---|---|---|---|---|
| | | 1 | 2 | 3 | 4 | 5 | 6 |
| | 1 | 1 | 2 | 3 | 4 | 5 | 6 |
| | 2 | 2 | 1 | 4 | 3 | 6 | 5 |
| $*$: | 3 | 3 | 5 | 1 | 6 | 2 | 4 |
| | 4 | 4 | 6 | 2 | 5 | 1 | 3 |
| | 5 | 5 | 3 | 6 | 1 | 4 | 2 |
| | 6 | 6 | 4 | 5 | 2 | 3 | 1 |

Finite Model Finding

Def: A formula F has the **finite model property** iff F has a model with a finite domain. (The finite model property is undecidable.)

Question here: how to compute (“efficiently”) finite models?

Today’s finite model finders all follow a generate-and-test approach:

- Given a formula F in clause normal form.
- For each **domain size** $n = 1, 2, \dots$ transform F into a clause set $G(F, n)$ such that $G(F, n)$ is satisfiable iff F is satisfiable with the domain $D = \{1, 2, \dots, n\}$

For each n , use a theorem prover to determine if $G(F, n)$ is satisfiable.

If so, stop and report the model. Otherwise continue.

Group Theory Example – $G(F, n)$ as Reduction to SAT

| | |
|----------------|--|
| Domain: | $\{1, 2\}$ |
| Clauses: | $\{p(a) \vee f(x) = a\}$ |
| Flattened: | $p(y) \vee f(x) = y \vee a \neq y$ |
| Instances: | $p(1) \vee f(1) = 1 \vee a \neq 1$ $p(2) \vee f(1) = 1 \vee a \neq 2$ $p(1) \vee f(2) = 1 \vee a \neq 1$ $p(2) \vee f(2) = 1 \vee a \neq 2$ |
| Totality: | $a = 1 \vee a = 2$ $f(1) = 1 \vee f(1) = 2$ $f(2) = 1 \vee f(2) = 2$ |
| Functionality: | $a \neq 1 \vee a \neq 2$ $f(1) \neq 1 \vee f(1) \neq 2$ $f(2) \neq 1 \vee f(2) \neq 2$ |

A model is obtained by setting the blue literals true

Difficult Example

- Consider the clause set consisting of the $n \cdot (n - 1)/2 + 1$ unit clauses:

$$P(c_1, \dots, c_n)$$

$$\neg P(x_1, \dots, x_{i-1}, x, x_{i+1}, \dots, x_{j-1}, x, x_{j+1}, \dots, x_n)$$

- The model must contain (at least) n domain elements.
- Example for $n = 3$:

| <i>Clauses</i> | <i>Model</i> |
|-------------------------|--------------|
| $p(c_1, c_2, c_3)$ | $c_1 = 1$ |
| $\neg p(x_1, x_1, x_3)$ | $c_2 = 2$ |
| $\neg p(x_1, x_2, x_1)$ | $c_3 = 3$ |
| $\neg p(x_1, x_2, x_2)$ | $p(1, 2, 3)$ |

- Guess: For which n do propositional model finders give up?

Difficult Example

- Answer: $n = 8$.
- There are n^{n-1} instances of the clause
 $\neg p(x_1, \dots, x_{i-1}, x, x_{i+1}, \dots, x_{j-1}, x, x_{j+1}, \dots, x_n)$.
- Memory consumption is the main bottleneck.
- Encoding in function-free clause logic requires only quadratically many clauses (savings are on not having to apply the domain substitutions γ). But instance-based methods are not the solution either. Scalability remains the issue.

Contents

Introduction

Logics and Reasoning Service (already done)

Methods for Automated Theorem Proving

Overview of some widely used general methods

- Propositional SAT solving
- First-order logic and clause normal forms
- Proof Procedures Based on Herbrand's Theorem
- The Resolution calculus
- Instance-based methods
- Model generation

Theory Reasoning

Methods to reason with specific background theories

- Paramodulation (Equality)
- Satisfiability Modulo Theories (SMT)
- Quantifier elimination for linear real arithmetic
- Combining multiple theories

Theory Reasoning

Let T be a first-order theory of signature Σ and L be a class of Σ -formulas.

- T can be given as a set of axioms (e.g., the theory of groups), or
- T can be given as a class of interpretations (e.g., the standard model of peano arithmetic)

The T -validity Problem

- Given ϕ in L , is it the case that $T \models \phi$? More accurately:
- Given ϕ in L , is it the case that $T \models \forall \phi$?

Examples

- “0/0, s/1, +/2, =/2, ≤/2” $\models \exists y.y > x$
- The theory of equality $E \models \phi$ (ϕ arbitrary formula)
- “An equational theory” $\models \exists s_1 = t_1 \wedge \dots \wedge s_n = t_n$
(E-Unification problem)
- “Some group theory” $\models s = t$ (Word problem)

The T -validity problem is decidable (even semi-decidable) only for restricted L and T

Approaches to Theory Reasoning

Theory-Reasoning in Automated First-Order Theorem Proving

- Semi-decide the T -validity problem, $T \models \phi$?
- ϕ arbitrary first-order formula, T set of formulas (axioms for T)
- Generality is strength and weakness at the same time
- Really successful only for specific instance:
 T = equality, inference rules like paramodulation (see below)

Satisfiability Modulo Theories (SMT)

- Decide the T -validity problem, $T \models \phi$?
- Usual restriction: ϕ is quantifier-free, i.e. all variables implicitly universally quantified
- Applications in particular to formal verification

Simple example where T = “arrays+integers”:

$$\{m \geq 0 \wedge a[i] \geq 0\} \quad a[i] := a[i] + m \quad \{a[i] \geq 0\}$$

Equality

Reserve a binary predicate symbol \approx (“equality”).

Intuitively, we expect that from the clauses

$$P(a) \quad a \approx b \quad b \approx c \quad f(x) \approx x \quad f(x) \approx g(x)$$

it follows, e.g.,

$$P(g(f(c)))$$

This requires to fix the meaning of \approx . Two options:

- Semantically: define $\approx = \{(d, d) \mid d \in U\}$
(Recall that predicate symbols are interpreted as relations, U is the universe)
- Syntactically: add **equality axioms** to the given clause set

The semantic approach cannot be used in conjunction with Herbrand models, but the syntactic approach can.

Handling Equality Naively - Equality Axioms

Let F be a first-order clause set with equality. The clause set $EqAx(F)$ consists of the clauses

$$x \approx x$$

$$x \approx y \rightarrow y \approx x$$

$$x \approx y \wedge y \approx z \rightarrow x \approx z$$

$$x_1 \approx y_1 \wedge \cdots \wedge x_n \approx y_n \rightarrow f(x_1, \dots, x_n) \approx f(y_1, \dots, y_n)$$

$$x_1 \approx y_1 \wedge \cdots \wedge x_m \approx y_m \wedge P(x_1, \dots, x_m) \rightarrow P(y_1, \dots, y_m)$$

for every n -ary function symbol f occurring in F and every m -ary predicate symbol P occurring in F .

$EqAx(F)$ are the axioms of a congruence relation on terms and atoms.

It holds: F is satisfiable, where \approx is defined semantically as in the previous slide, if and only if $F \cup EqAx(\Sigma)$ is satisfiable, where \approx is left undefined.

Handling Equality Naively - Equality Axioms

By giving the equality axioms explicitly, first-order problems with equality can in principle be solved by a standard resolution prover or instance-based method.

But this is unfortunately not efficient (mainly due to the transitivity and congruence axioms).

Modern systems “build-in” equality by dedicated inference rules, which are (restricted) versions of the **Paramodulation** inference rule.

Recapitulation: Resolution

Resolution: inference rules:

Ground case:

Resolution:
$$\frac{D' \vee A \quad C' \vee \neg A}{D' \vee C'}$$

Non-ground case:

$$\frac{D' \vee A \quad C' \vee \neg A'}{(D' \vee C')\sigma}$$

where $\sigma = \text{mgu}(A, A')$.

Factoring:
$$\frac{C' \vee A \vee A}{C' \vee A}$$

$$\frac{C' \vee A \vee A'}{(C' \vee A)\sigma}$$

where $\sigma = \text{mgu}(A, A')$.

Paramodulation

Ground inference rules:

Paramodulation:
$$\frac{D' \vee t \approx t' \quad C' \vee L[t]}{D' \vee C' \vee L[t']}$$

Equality Resolution:
$$\frac{C' \vee s \not\approx s}{C'}$$

In the Paramodulation rule, $L[t]$ means that the literal L contains the term t , and $L[t']$ means that one occurrence of t in L has been replaced by t' .

Paramodulation

First-order inference rules:

Paramodulation:
$$\frac{D' \vee t \approx t' \quad C' \vee L[u]}{(D' \vee C' \vee L[t'])\sigma}$$

where $\sigma = \text{mgu}(t, u)$ and u is not a variable.

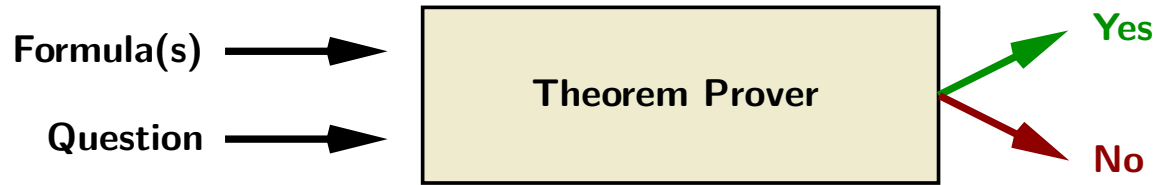
Equality Resolution:
$$\frac{C' \vee s \not\approx s'}{C'\sigma}$$

where $\sigma = \text{mgu}(s, s')$.

These are the main inference rules for equality reasoning. Together with the Resolution and Factoring inference rules, and an additional inference rule (not shown here), one obtains a refutationally complete and sound calculus.

The calculus can still be considerably improved by means of ordering restrictions.

Satisfiability Modulo Theories (SMT)



Formula: first-order logic formula ϕ , over equality and other theories

Question: Is ϕ valid? (satisfiable? entailed by another formula?)

$$\models_{\text{NUL}} \forall l (c = 5 \rightarrow \text{car}(\text{cons}(3 + c, l)) \doteq 8)$$

Theorem Prover: DPLL(T), translation into SAT, first-order provers

Issue: essentially undecidable for non-variable free fragment (\forall -quantifier left of \models):

$$P(0) \wedge (\forall x P(x) \rightarrow P(x + 1)) \models_{\mathbb{N}} \forall x P(x)$$

Design a “good” prover anyways (ongoing research)

Checking Satisfiability Modulo Theories

Given: A quantifier-free formula ϕ (implicitly existentially quantified)

Task: Decide whether ϕ is T -satisfiable

(T -validity via “ $T \models \forall \phi$ ” iff “ $\exists \neg\phi$ is not T -satisfiable”)

Approach: eager translation into SAT

- Encode problem into a T -equisatisfiable propositional formula
- Feed formula to a SAT-solver
- Example: $T =$ equality (Ackermann encoding)

Approach: lazy translation into SAT

- Couple a SAT solver with a given decision procedure for T -satisfiability of ground literals, “DPLL(T)”
- For instance if T is “equality” then the Nelson-Oppen congruence closure method can be used
- If T is “linear arithmetic”, a quantifier elimination method (see below)

Lazy Translation into SAT

$$g(a) = c \wedge f(g(a)) \neq f(c) \vee g(a) = d \wedge c \neq d$$

Theory: Equality

Lazy Translation into SAT

$$\underbrace{g(a) = c}_1 \wedge \underbrace{f(g(a)) \neq f(c)}_{\bar{2}} \vee \underbrace{g(a) = d}_3 \wedge \underbrace{c \neq d}_{\bar{4}}$$

Lazy Translation into SAT

$$\underbrace{g(a) = c}_1 \wedge \underbrace{f(g(a)) \neq f(c)}_{\bar{2}} \vee \underbrace{g(a) = d}_3 \wedge \underbrace{c \neq d}_{\bar{4}}$$

- Send $\{1, \bar{2} \vee 3, \bar{4}\}$ to SAT solver.

Lazy Translation into SAT

$$\underbrace{g(a) = c}_1 \wedge \underbrace{f(g(a)) \neq f(c)}_{\bar{2}} \vee \underbrace{g(a) = d}_3 \wedge \underbrace{c \neq d}_{\bar{4}}$$

- Send $\{1, \bar{2} \vee 3, \bar{4}\}$ to SAT solver.
- SAT solver returns model $\{1, \bar{2}, \bar{4}\}$.
Theory solver finds $\{1, \bar{2}\}$ ***E-unsatisfiable***.

Lazy Translation into SAT

$$\underbrace{g(a) = c}_1 \wedge \underbrace{f(g(a)) \neq f(c)}_{\bar{2}} \vee \underbrace{g(a) = d}_3 \wedge \underbrace{c \neq d}_{\bar{4}}$$

- Send $\{1, \bar{2} \vee 3, \bar{4}\}$ to SAT solver.
- SAT solver returns model $\{1, \bar{2}, \bar{4}\}$.
Theory solver finds $\{1, \bar{2}\}$ *E-unsatisfiable*.
- Send $\{1, \bar{2} \vee 3, \bar{4}, \bar{1} \vee 2\}$ to SAT solver.

Lazy Translation into SAT

$$\underbrace{g(a) = c}_1 \wedge \underbrace{f(g(a)) \neq f(c)}_{\bar{2}} \vee \underbrace{g(a) = d}_3 \wedge \underbrace{c \neq d}_{\bar{4}}$$

- Send $\{1, \bar{2} \vee 3, \bar{4}\}$ to SAT solver.
- SAT solver returns model $\{1, \bar{2}, \bar{4}\}$.
Theory solver finds $\{1, \bar{2}\}$ *E-unsatisfiable*.
- Send $\{1, \bar{2} \vee 3, \bar{4}, \bar{1} \vee 2\}$ to SAT solver.
- SAT solver returns model $\{1, 2, 3, \bar{4}\}$.
Theory solver finds $\{1, 3, \bar{4}\}$ *E-unsatisfiable*.

Lazy Translation into SAT

$$\underbrace{g(a) = c}_1 \wedge \underbrace{f(g(a)) \neq f(c)}_{\bar{2}} \vee \underbrace{g(a) = d}_3 \wedge \underbrace{c \neq d}_{\bar{4}}$$

- Send $\{1, \bar{2} \vee 3, \bar{4}\}$ to SAT solver.
- SAT solver returns model $\{1, \bar{2}, \bar{4}\}$.
Theory solver finds $\{1, \bar{2}\}$ **E-unsatisfiable**.
- Send $\{1, \bar{2} \vee 3, \bar{4}, \bar{1} \vee 2\}$ to SAT solver.
- SAT solver returns model $\{1, 2, 3, \bar{4}\}$.
Theory solver finds $\{1, 3, \bar{4}\}$ **E-unsatisfiable**.
- Send $\{1, \bar{2} \vee 3, \bar{4}, \bar{1} \vee 2, \bar{1} \vee \bar{3} \vee 4\}$ to SAT solver.
SAT solver finds $\{1, \bar{2} \vee 3, \bar{4}, \bar{1} \vee 2, \bar{1} \vee \bar{3} \vee 4\}$ **unsatisfiable**.

Lazy Translation into SAT: Summary

- Abstract T -atoms as propositional variables
- SAT solver computes a model, i.e. satisfying boolean assignment for propositional abstraction (or fails)
- Solution from SAT solver may not be a T -model. If so,
 - Refine (strengthen) propositional formula by incorporating reason for false solution
 - Start again with computing a model

Optimizations

Theory Consequences

- The theory solver may return consequences (typically literals) to guide the SAT solver

Online SAT solving

- The SAT solver continues its search after accepting additional clauses (rather than restarting from scratch)

Preprocessing atoms

- Atoms are rewritten into normal form, using theory-specific atoms (e.g. associativity, commutativity)

Several layers of decision procedures

- “Cheaper” ones are applied first

Example Theory: Linear Arithmetic

Linear Rational Arithmetic (LRA) is the interpretation

$$I_{LA} = (\mathbb{Q}, (+_{\mathcal{A}_{LA}}, -_{\mathcal{A}_{LA}}, *_{\mathcal{A}_{LA}}), (\leq_{\mathcal{A}_{LA}}, \geq_{\mathcal{A}_{LA}}, <_{\mathcal{A}_{LA}}, >_{\mathcal{A}_{LA}}))$$

where $+_{\mathcal{A}_{LA}}, -_{\mathcal{A}_{LA}}, *_{\mathcal{A}_{LA}}, \leq_{\mathcal{A}_{LA}}, \geq_{\mathcal{A}_{LA}}, <_{\mathcal{A}_{LA}}, >_{\mathcal{A}_{LA}}$ are the “standard” interpretations of $+, -, *, \leq, \geq, <, >$, respectively.

The Problem

Within the DPLL(T) framework it is enough to design a decision procedure for LRA-satisfiability of sets N (conjunctions) of literals. Note that (hence) all variables in N are implicitly existentially quantified

Example:

$$N = \{2x \leq y, y < 6, 3 < y, 1 < x\}$$

Question: Is there an assignment β for the variables x and y such that $(I_{LA}, \beta) \models N$?

Some Important LA Equivalences

The following equivalences are valid for all LA terms s, t :

$$\neg s \geq t \leftrightarrow s < t$$

$$\neg s \leq t \leftrightarrow s > t \quad (\text{Negation})$$

$$(s = t) \leftrightarrow (s \leq t \wedge s \geq t) \quad (\text{Equality})$$

$$s \geq t \leftrightarrow t \leq s$$

$$s > t \leftrightarrow t < s \quad (\text{Swap})$$

With \lesssim we abbreviate $<$ or \leq .

The Fourier-Motzkin Procedure

```
boolean FM(Set  $N$  of LA atoms) {  
  if ( $N = \emptyset$ ) return true;  
  elsif ( $N$  is ground) return  $I_{\text{LA}}(N)$ ;  
  else {  
    select a variable  $x$  from  $N$ ;  
    transform all atoms in  $N$  containing  $x$  into  $s_i \lesssim x, x \lesssim t_j$   
    and the subset  $N'$  of atoms not containing  $x$ ;  
    compute  $N^* := \{s_i \lesssim_{i,j} t_j \mid s_i \lesssim_i x \in N, x \lesssim_j t_j \in N \text{ for all } i, j\}$   
    where  $\lesssim_{i,j}$  is strict iff at least one of  $\lesssim_i, \lesssim_j$  is strict  
    return FM( $N' \cup N^*$ );  
  }  
}
```

Properties of the Fourier-Motzkin Procedure

- Any ground set N of linear arithmetic atoms can be easily decided.
- $\text{FM}(N)$ terminates on any N as in recursive calls N has strictly less variables.
- The set $N' \cup N^*$ is worst case of size $O(|N|^2)$.
- $\text{FM}(N)=\text{true}$ iff N is satisfiable in I_{LA} .
- The procedure was invented by Fourier (1826), forgotten, and then rediscovered by Dines (1919) and Motzkin (1936).
- There are more efficient methods known, e.g., the simplex algorithm.
- As said, the Fourier-Motzkin Procedure decides the satisfiability of a set (conjunction) of linear arithmetic atoms, which is what is needed to build a sound and complete DPLL(T)-solver.

Combining Theories

Theories:

- \mathcal{R} : theory of rationals
 $\Sigma_{\mathcal{R}} = \{\leq, +, -, 0, 1\}$
- \mathcal{L} : theory of lists
 $\Sigma_{\mathcal{L}} = \{=, \text{hd}, \text{tl}, \text{nil}, \text{cons}\}$
- \mathcal{E} : theory of equality
 Σ : free function and predicate symbols

Problem: Is

$$x \leq y \wedge y \leq x + \text{hd}(\text{cons}(0, \text{nil})) \wedge P(h(x) - h(y)) \wedge \neg P(0)$$

satisfiable in $\mathcal{R} \cup \mathcal{L} \cup \mathcal{E}$?

Nelson-Oppen Combination Method

G. Nelson and D.C. Oppen: *Simplification by cooperating decision procedures*, ACM Trans. on Programming Languages and Systems, 1(2):245-257, 1979.

Given:

- $\mathcal{T}_1, \mathcal{T}_2$ first-order theories with signatures Σ_1, Σ_2
- $\Sigma_1 \cap \Sigma_2 = \emptyset$
- ϕ quantifier-free formula over $\Sigma_1 \cup \Sigma_2$

Obtain a decision procedure for satisfiability in $\mathcal{T}_1 \cup \mathcal{T}_2$ from decision procedures for satisfiability in \mathcal{T}_1 and \mathcal{T}_2 .

Nelson-Oppen Combination Method

Variable abstraction + equality propagation:

$$x \leq y \wedge y \leq x + \text{hd}(\text{cons}(0, \text{nil})) \wedge P(h(x) - h(y)) \wedge \neg P(0)$$

Nelson-Oppen Combination Method

Variable abstraction + equality propagation:

$$x \leq y \wedge y \leq x + \underbrace{\text{hd}(\text{cons}(0, \text{nil}))}_{v_1} \wedge \underbrace{P(\underbrace{h(x)}_{v_3} - \underbrace{h(y)}_{v_4})}_{v_2} \wedge \neg P(\underbrace{0}_{v_5})$$

Nelson-Oppen Combination Method

Variable abstraction + equality propagation:

$$x \leq y \wedge y \leq x + \underbrace{\text{hd}(\text{cons}(0, \text{nil}))}_{v_1} \wedge P(\underbrace{h(x)}_{v_3} - \underbrace{h(y)}_{v_4}) \wedge \neg P(\underbrace{0}_{v_5})$$

v_2

| \mathcal{R} | \mathcal{L} | \mathcal{E} |
|------------------|---------------|---------------|
| <hr/> | | |
| $x \leq y$ | | $P(v_2)$ |
| $y \leq x + v_1$ | | $\neg P(v_5)$ |

Nelson-Oppen Combination Method

Variable abstraction + equality propagation:

$$x \leq y \wedge y \leq x + \underbrace{\text{hd}(\text{cons}(0, \text{nil}))}_{v_1} \wedge \underbrace{P(\underbrace{h(x)}_{v_3} - \underbrace{h(y)}_{v_4})}_{v_2} \wedge \neg P(\underbrace{0}_{v_5})$$

| \mathcal{R} | \mathcal{L} | \mathcal{E} |
|-------------------|---|---------------|
| $x \leq y$ | | $P(v_2)$ |
| $y \leq x + v_1$ | | $\neg P(v_5)$ |
| $v_2 = v_3 - v_4$ | $v_1 = \text{hd}(\text{cons}(v_5, \text{nil}))$ | $v_3 = h(x)$ |
| $v_5 = 0$ | | $v_4 = h(y)$ |

Nelson-Oppen Combination Method

Variable abstraction + equality propagation:

$$x \leq y \wedge y \leq x + \underbrace{\text{hd}(\text{cons}(0, \text{nil}))}_{v_1} \wedge P(\underbrace{h(x)}_{v_3} - \underbrace{h(y)}_{v_4}) \wedge \neg P(\underbrace{0}_{v_5})$$

$\underbrace{\hspace{10em}}_{v_2}$

| \mathcal{R} | \mathcal{L} | \mathcal{E} |
|-------------------|---|---------------|
| $x \leq y$ | | $P(v_2)$ |
| $y \leq x + v_1$ | | $\neg P(v_5)$ |
| $v_2 = v_3 - v_4$ | $v_1 = \text{hd}(\text{cons}(v_5, \text{nil}))$ | $v_3 = h(x)$ |
| $v_5 = 0$ | | $v_4 = h(y)$ |
| | $v_1 = v_5$ | |

Nelson-Oppen Combination Method

Variable abstraction + equality propagation:

$$x \leq y \wedge y \leq x + \underbrace{\text{hd}(\text{cons}(0, \text{nil}))}_{v_1} \wedge \underbrace{P(\underbrace{h(x)}_{v_3} - \underbrace{h(y)}_{v_4})}_{v_2} \wedge \neg P(\underbrace{0}_{v_5})$$

| \mathcal{R} | \mathcal{L} | \mathcal{E} |
|-------------------|---|---------------|
| $x \leq y$ | | $P(v_2)$ |
| $y \leq x + v_1$ | | $\neg P(v_5)$ |
| $v_2 = v_3 - v_4$ | $v_1 = \text{hd}(\text{cons}(v_5, \text{nil}))$ | $v_3 = h(x)$ |
| $v_5 = 0$ | | $v_4 = h(y)$ |
| $x = y$ | $v_1 = v_5$ | |

Nelson-Oppen Combination Method

Variable abstraction + equality propagation:

$$x \leq y \wedge y \leq x + \underbrace{\text{hd}(\text{cons}(0, \text{nil}))}_{v_1} \wedge \underbrace{P(\underbrace{h(x)}_{v_3} - \underbrace{h(y)}_{v_4})}_{v_2} \wedge \neg P(\underbrace{0}_{v_5})$$

| \mathcal{R} | \mathcal{L} | \mathcal{E} |
|-------------------|---|---------------|
| $x \leq y$ | | $P(v_2)$ |
| $y \leq x + v_1$ | | $\neg P(v_5)$ |
| $v_2 = v_3 - v_4$ | $v_1 = \text{hd}(\text{cons}(v_5, \text{nil}))$ | $v_3 = h(x)$ |
| $v_5 = 0$ | | $v_4 = h(y)$ |
| $x = y$ | $v_1 = v_5$ | $v_3 = v_4$ |

Nelson-Oppen Combination Method

Variable abstraction + equality propagation:

$$x \leq y \wedge y \leq x + \underbrace{\text{hd}(\text{cons}(0, \text{nil}))}_{v_1} \wedge P(\underbrace{h(x)}_{v_3} - \underbrace{h(y)}_{v_4}) \wedge \neg P(\underbrace{0}_{v_5})$$

v_2

| \mathcal{R} | \mathcal{L} | \mathcal{E} |
|-------------------|---|---------------|
| $x \leq y$ | | $P(v_2)$ |
| $y \leq x + v_1$ | | $\neg P(v_5)$ |
| $v_2 = v_3 - v_4$ | $v_1 = \text{hd}(\text{cons}(v_5, \text{nil}))$ | $v_3 = h(x)$ |
| $v_5 = 0$ | | $v_4 = h(y)$ |
| $x = y$ | $v_1 = v_5$ | $v_3 = v_4$ |
| $v_2 = v_5$ | | |

Nelson-Oppen Combination Method

Variable abstraction + equality propagation:

$$x \leq y \wedge y \leq x + \underbrace{\text{hd}(\text{cons}(0, \text{nil}))}_{v_1} \wedge P(\underbrace{h(x)}_{v_3} - \underbrace{h(y)}_{v_4}) \wedge \neg P(\underbrace{0}_{v_5})$$

$\underbrace{\hspace{10em}}_{v_2}$

| \mathcal{R} | \mathcal{L} | \mathcal{E} |
|-------------------|---|---------------|
| $x \leq y$ | | $P(v_2)$ |
| $y \leq x + v_1$ | | $\neg P(v_5)$ |
| $v_2 = v_3 - v_4$ | $v_1 = \text{hd}(\text{cons}(v_5, \text{nil}))$ | $v_3 = h(x)$ |
| $v_5 = 0$ | | $v_4 = h(y)$ |
| $x = y$ | $v_1 = v_5$ | $v_3 = v_4$ |
| $v_2 = v_5$ | | \perp |

Conclusions

- Talked about the role of first-order theorem proving
- Talked about some standard techniques (Normal forms of formulas, Resolution calculus, unification, Instance-based method, Model computation)
- Talked about DPLL and Satisfiability Modulo Theories (SMT)

Further Topics

- Redundancy elimination, efficient equality reasoning, adding arithmetics to first-order theorem provers
- FOTP methods as decision procedures in special cases
E.g. reducing planning problems and temporal logic model checking problems to function-free clause logic and using an instance-based method as a decision procedure
- Implementation techniques
- Competition CASC and TPTP problem library
- Instance-based methods (a lot to do here, cf. my home page)
Attractive because of complementary features to more established methods

Further Reading

- Wikipedia article on [Automated Theorem Proving](https://en.wikipedia.org/wiki/Automated_theorem_proving)
`en.wikipedia.org/wiki/Automated_theorem_proving`
- Wikipedia article on [Boolean Satisfiability Problem](https://en.wikipedia.org/wiki/Boolean_satisfiability_problem) (propositional logic)
`en.wikipedia.org/wiki/Boolean_satisfiability_problem`
- Wikipedia article on [Satisfiability Modulo Theories \(SMT\)](https://en.wikipedia.org/wiki/Satisfiability_Modulo_Theories)
`en.wikipedia.org/wiki/Satisfiability_Modulo_Theories`
- A good textbook with an emphasis on theory reasoning (arithmetic, arrays) for software verification:
 Aaron Bradley and Zohar Manna, *The Calculus of Computation*, Springer, 2007
- Another good one, on what the title says, comes with OCaml code:
 John Harrison. *Handbook of Practical Logic and Automated Reasoning*, Cambridge University Press, 2009

Implemented Systems

- The TPTP (Thousands of Problems for Theorem Provers) is a library of test problems for automated theorem proving
`www.tptp.org`
- The automated theorem prover **SPASS** is an implementation of the “modern” version of resolution with equality, the superposition calculus, and comes with a comprehensive set of examples and documentation. A good choice to start with.
`www.spass-prover.org`
- `users.cecs.anu.edu.au/~baumgart/systems/`