Theories in Context - Model Evolution Modulo Integer Arithmetics

Peter Baumgartner

NICTA, Canberra, Australia

Cesare Tinelli

University of Iowa, USA

Problem Statement

- **Applications** of automated deduction often require reasoning modulo some form of (integer) arithmetic, e.g. LIA
- **SMT solvers**, e.g. DPLL(T)-based, can do that
  - Very successful for the quantifier free case, i.e. $\models \forall\Phi$
  - Rely on instantiation heuristics for non-quantifier free case, $\forall\Psi \models \forall\Phi$
- **First-order provers** support free symbols and quantifiers natively
  - But don't have built-in arithmetic or need CSUs

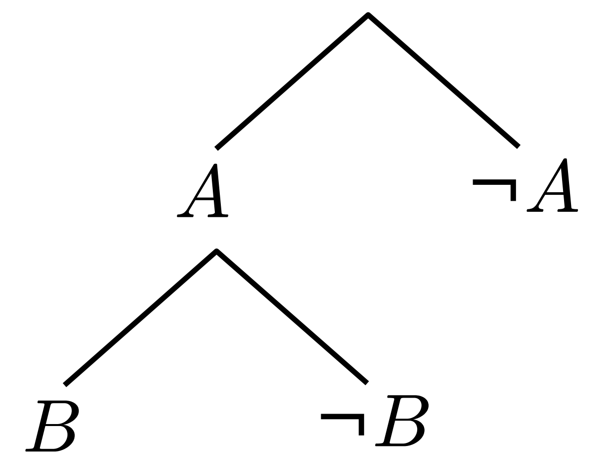
Our approach

- (Non-ground) clauses with LIA constraints over $\mathbb{N}$
- Free constants ("parameters") range over finite domains, e.g. a:[1 .. 10]
- New sound and complete calculus ME(LIA)
  - Model Evolution + black-box validity checker for $\forall\exists$ LIA fragment

DPLL procedure

Input: Propositional clause set

Output: Model or „unsatisfiable"



Algorithm components:

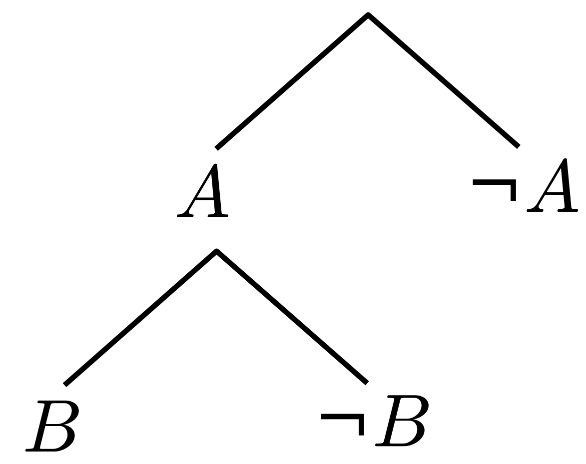
- Propositional semantic tree
  enumerates interpretations
- Propagation
- Split
- Backjumping

$$\{A, B\} \stackrel{?}{\models} \neg A \lor \neg B \lor C \lor D$$

DPLL procedure

Input: Propositional clause set

Output: Model or „unsatisfiable"



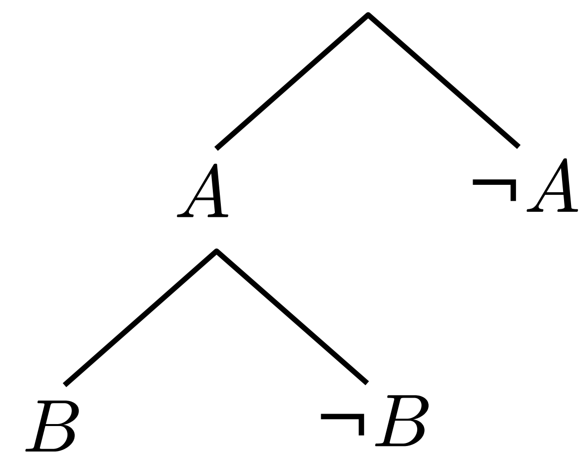
Algorithm components:

- Propositional semantic tree enumerates interpretations
- Propagation
- Split
- Backjumping

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

DPLL procedure

Input: Propositional clause set
Output: Model or „unsatisfiable"



Algorithm components:

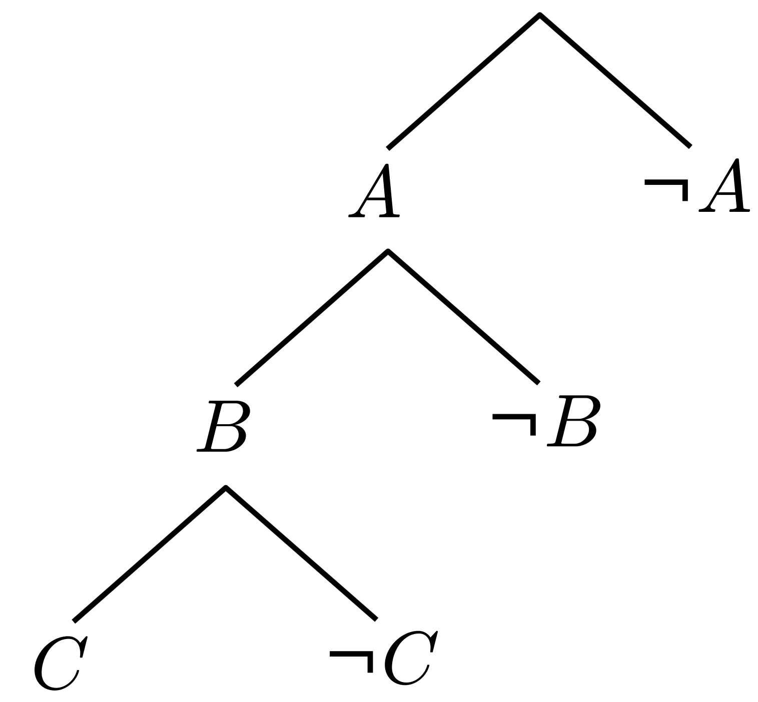
- Propositional semantic tree
  enumerates interpretations
- Propagation
- Split
- Backjumping

$$\{A, B\} \stackrel{?}{\models} \cancel{\neg A} \lor \cancel{\neg B} \lor C \lor D \qquad ✗$$

DPLL procedure

Input: Propositional clause set
Output: Model or „unsatisfiable"

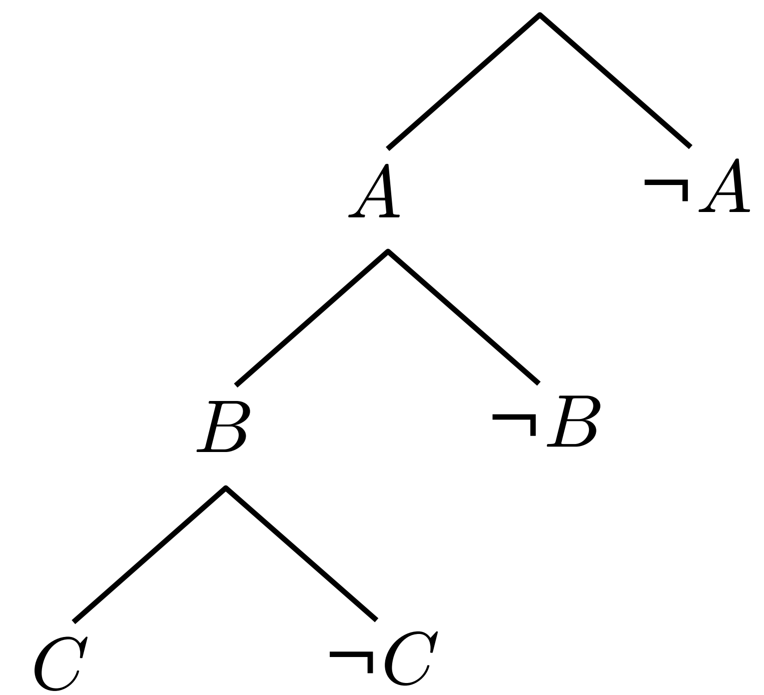
Algorithm components:
- Propositional semantic tree
  enumerates interpretations
- Propagation
- Split
- Backjumping



$$\{A, B\} \overset{?}{\models} \cancel{\neg A} \vee \cancel{\neg B} \vee C \vee D \qquad ✗$$

DPLL procedure

Input: Propositional clause set
Output: Model or „unsatisfiable"



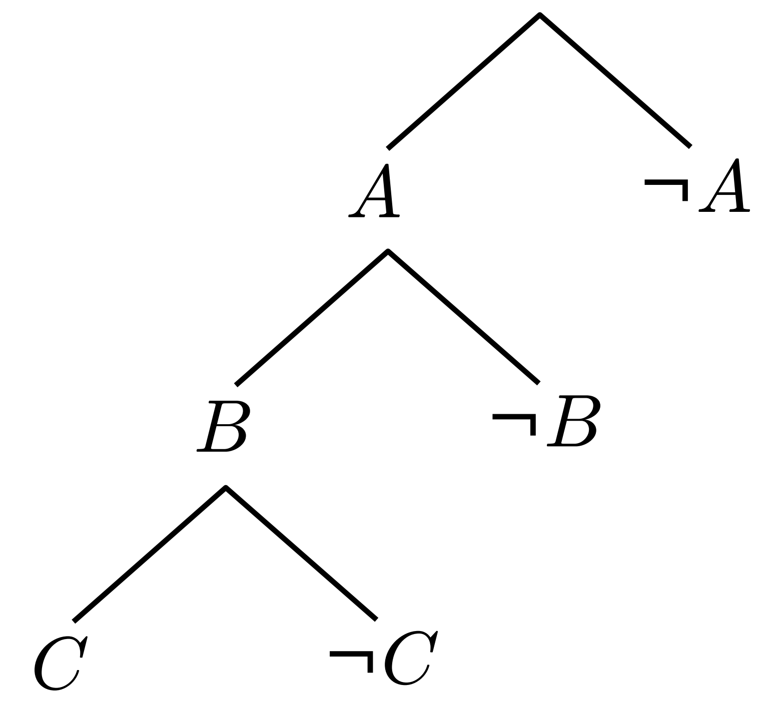
Algorithm components:
- Propositional semantic tree
  enumerates interpretations
- Propagation
- Split
- Backjumping

$$\{A, B\} \stackrel{?}{\models} \cancel{\neg A} \vee \cancel{\neg B} \vee C \vee D$$ ✗

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

DPLL procedure

Input: Propositional clause set
Output: Model or „unsatisfiable"



Algorithm components:

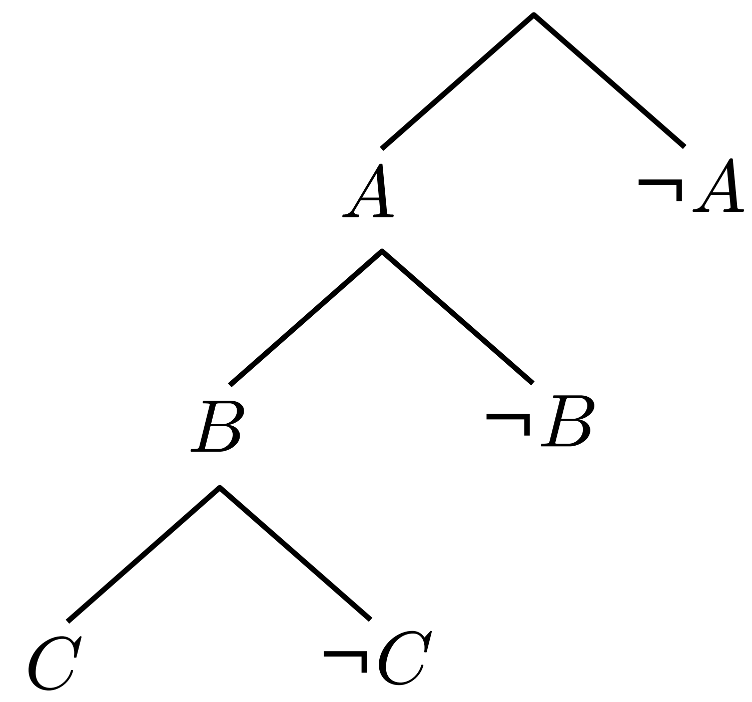
- Propositional semantic tree enumerates interpretations
- Propagation
- Split
- Backjumping

$$\{A, B\} \overset{?}{\models} \cancel{\neg A} \vee \cancel{\neg B} \vee C \vee D$$ ✗

$$\{A, B, C\} \overset{?}{\models} \cancel{\neg A} \vee \cancel{\neg B} \vee C \vee D$$ ✓

DPLL procedure

Input: Propositional clause set
Output: Model or „unsatisfiable"



Algorithm components:

- Propositional semantic tree
  enumerates interpretations
- Propagation
- Split
- Backjumping

$$\{A, B\} \overset{?}{\models} \cancel{\neg A} \vee \cancel{\neg B} \vee C \vee D \quad ✗$$

$$\{A, B, C\} \overset{?}{\models} \cancel{\neg A} \vee \cancel{\neg B} \vee C \vee D \quad ✓$$

ME - lifting to first-order level

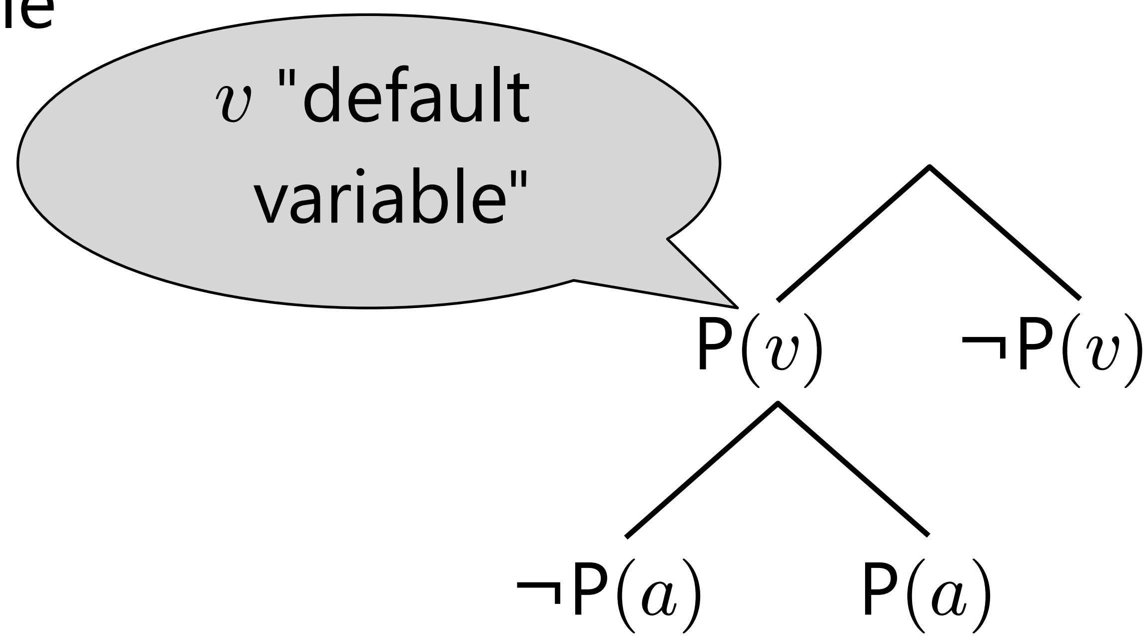
ME as First-Order DPLL

Input: First-order clause set

Output: Model or „unsatisfiable"
if termination

Algorithm components:

- First-order semantic tree
  enumerates interpretations
- Propagation
- Split
- Backjumping

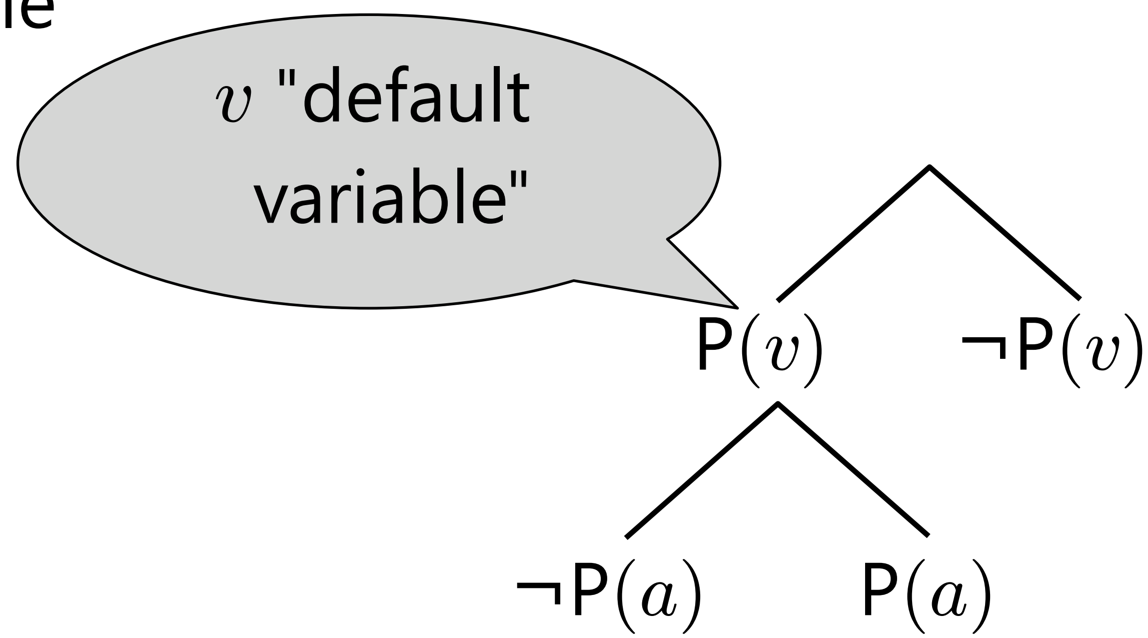


$$\{\mathsf{P}(v), \neg\mathsf{P}(\mathsf{a})\} \overset{?}{\models} \mathsf{P}(x) \vee \mathsf{Q}(x)$$

ME as First-Order DPLL

Input: First-order clause set

Output: Model or „unsatisfiable"
if termination



Algorithm components:

- First-order semantic tree
  enumerates interpretations
- Propagation
- Split
- Backjumping

$$\{\mathsf{P}(v), \neg\mathsf{P}(\mathsf{a})\} \overset{?}{\models} \mathsf{P}(x) \vee \mathsf{Q}(x)$$

Interpretation induced by a branch?

Interpretation Induced by a Branch

Branch B

$\mathsf{P}(x, y)$

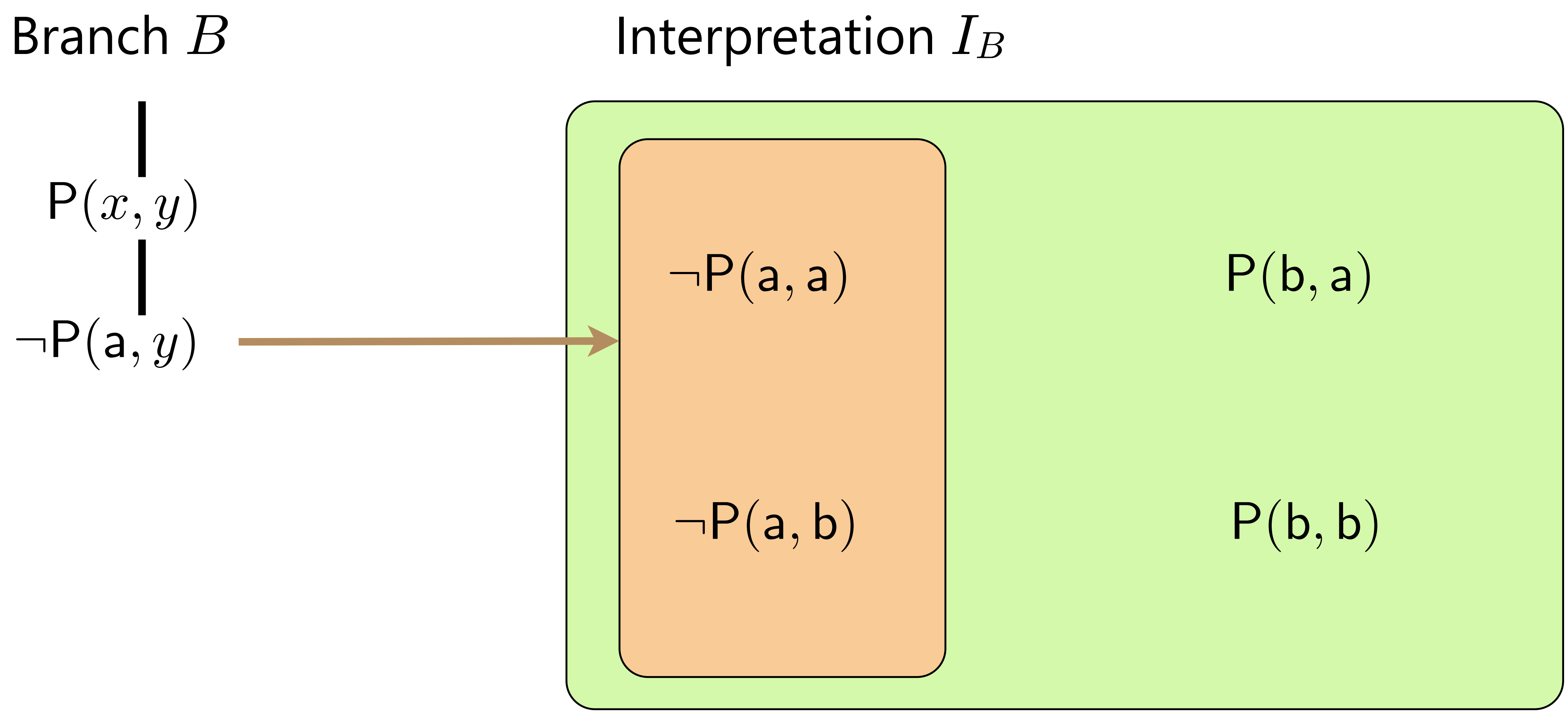
Interpretation I_B

$\mathsf{P}(\mathsf{a}, \mathsf{a})$ $\mathsf{P}(\mathsf{b}, \mathsf{a})$

$\mathsf{P}(\mathsf{a}, \mathsf{b})$ $\mathsf{P}(\mathsf{b}, \mathsf{b})$

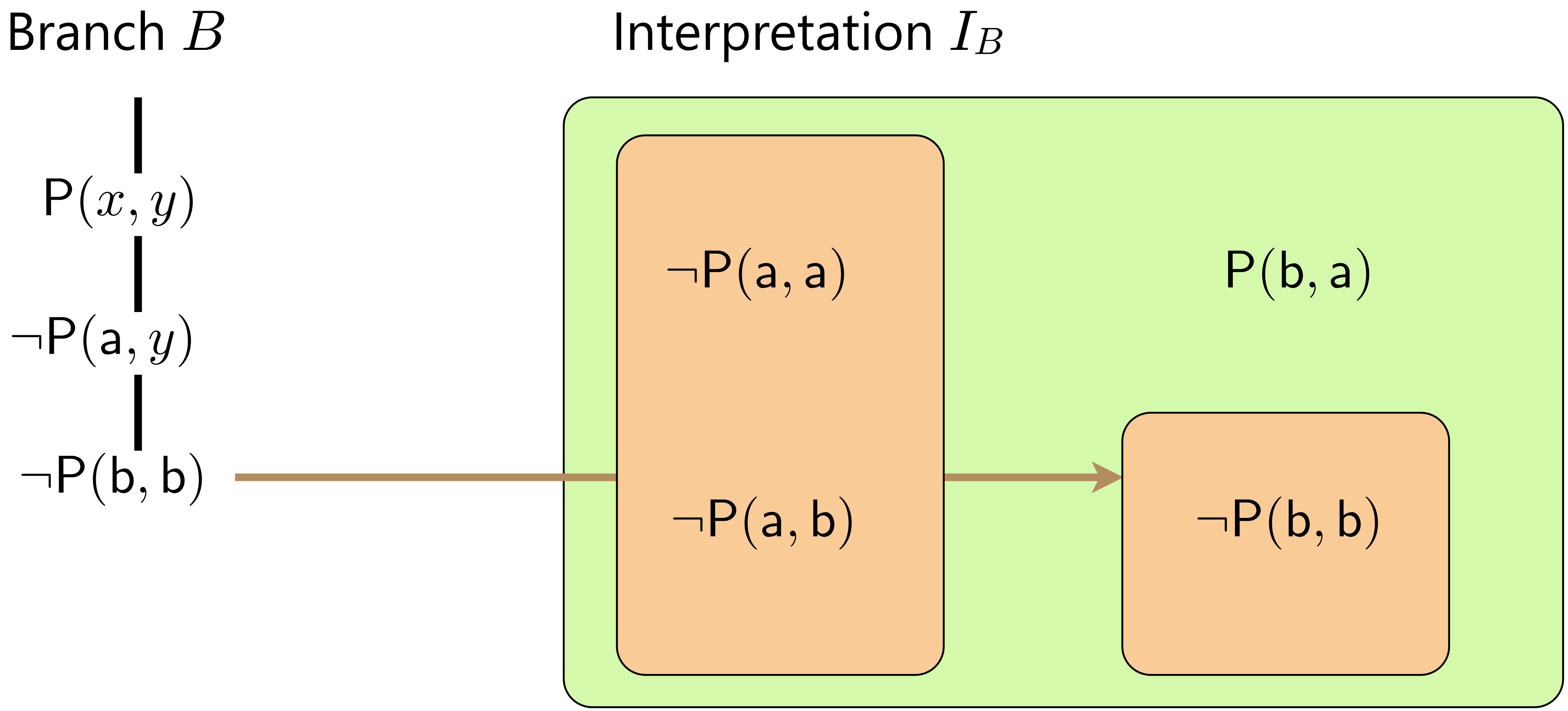
- A branch literal specifies a truth value for all its ground instances, unless there is a more specific literal specifying the opposite truth value

Interpretation Induced by a Branch



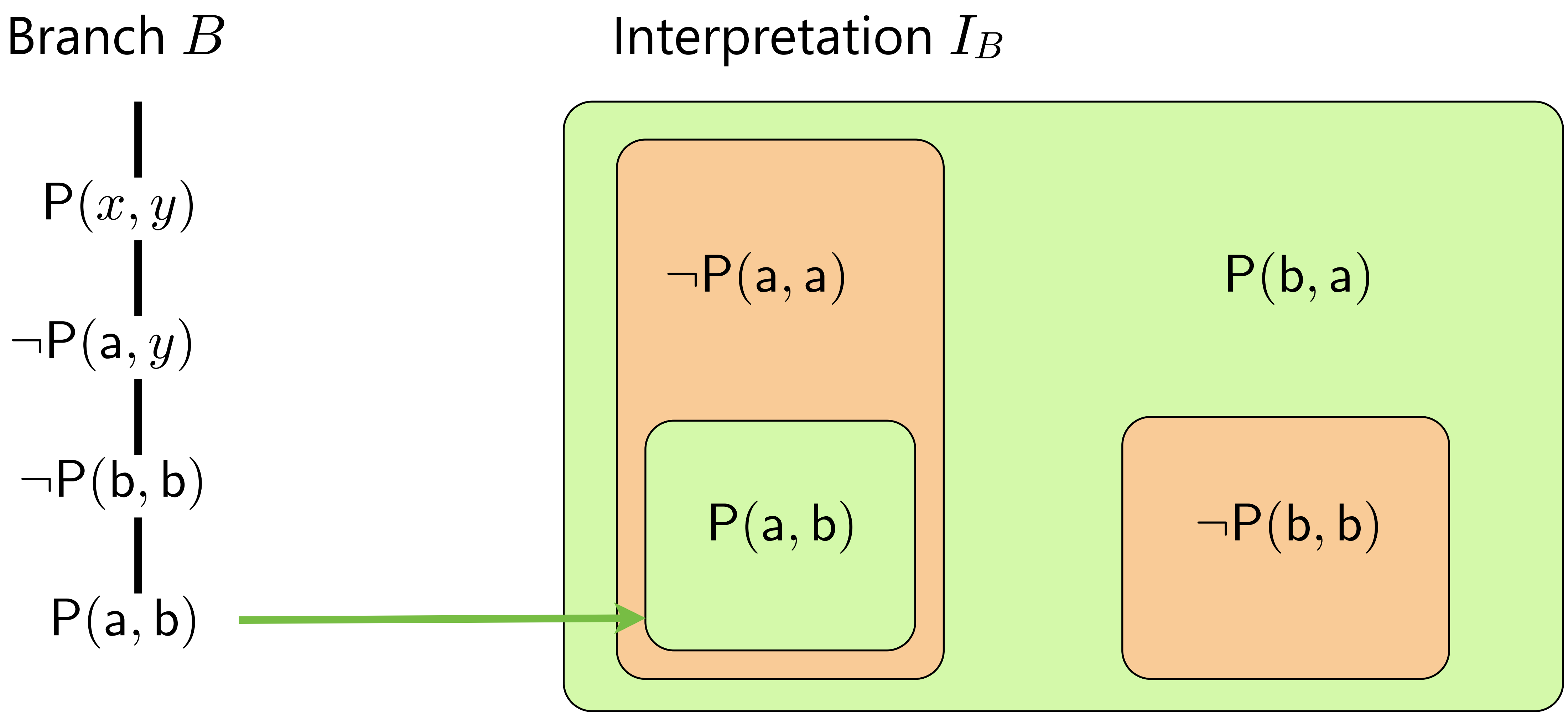
- A branch literal specifies a truth value for all its ground instances, unless there is a more specific literal specifying the opposite truth value

Interpretation Induced by a Branch



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

Interpretation Induced by a Branch



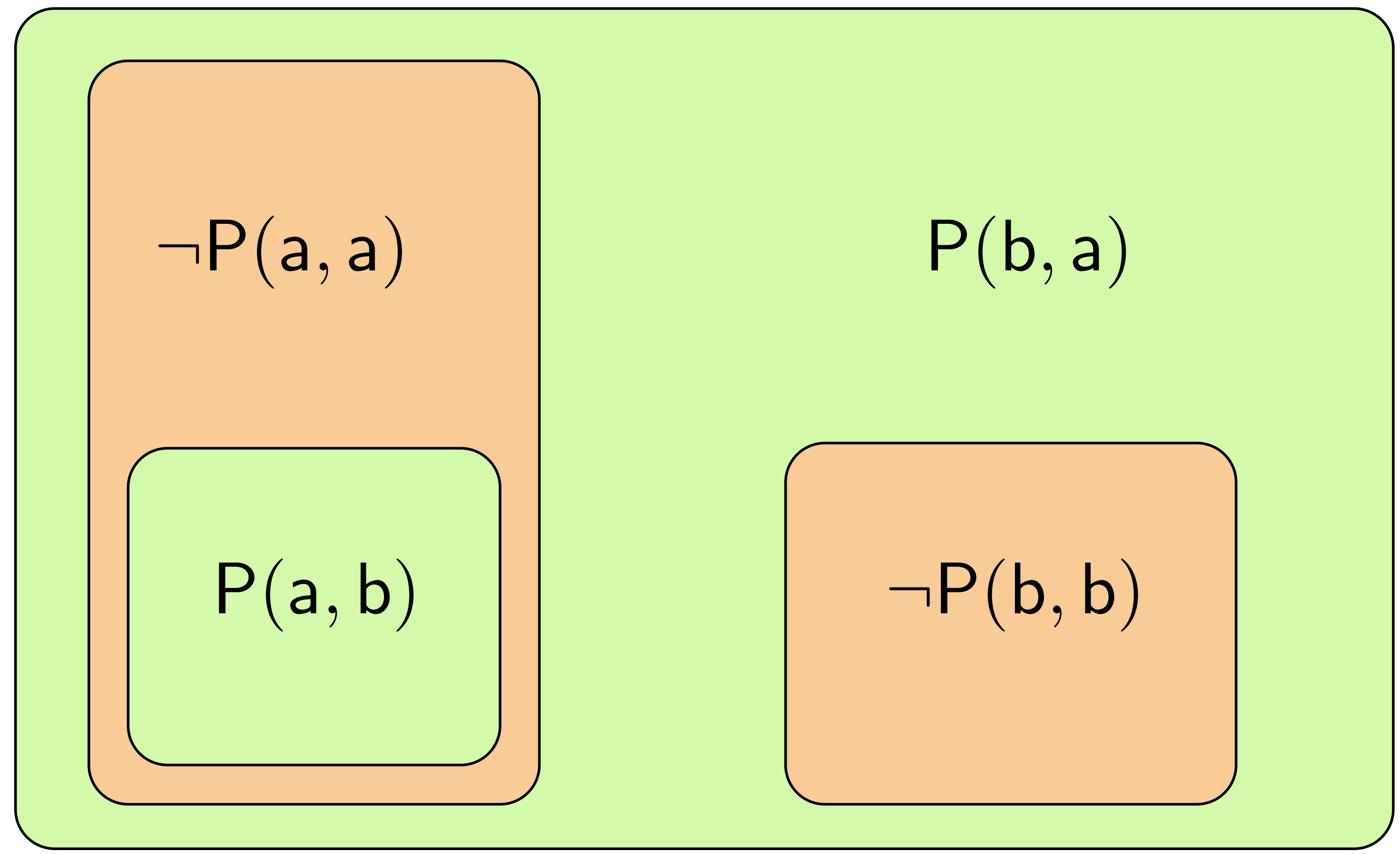
- A branch literal specifies a truth value for all its ground instances, unless there is a more specific literal specifying the opposite truth value

Interpretation Induced by a Branch

Branch B

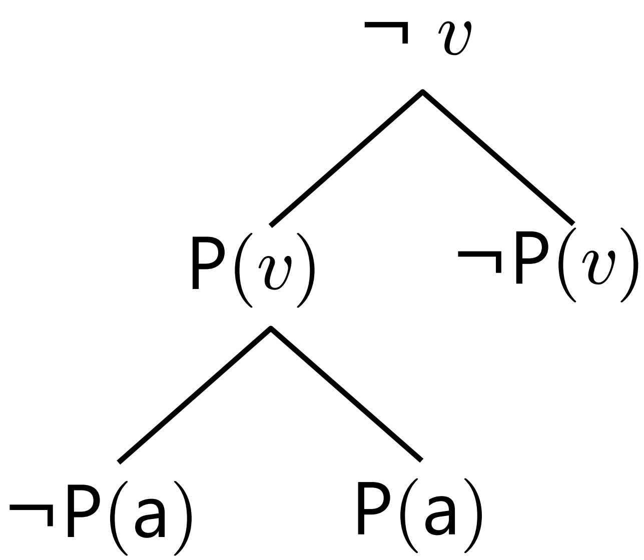
$$\{\ \mathsf{P}(x,y)\ ,\quad \neg\mathsf{P}(\mathsf{a},y)\ ,\quad \neg\mathsf{P}(\mathsf{b},\mathsf{b})\ ,\quad \mathsf{P}(\mathsf{a},\mathsf{b})\ \}$$

Interpretation I_B



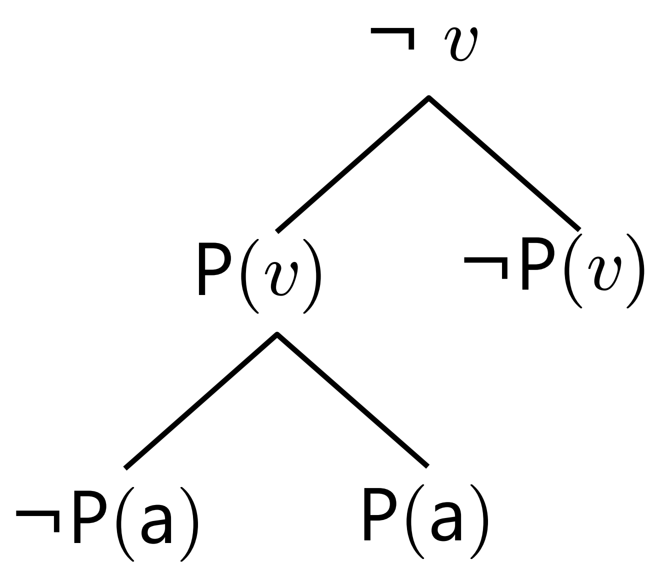
- A branch literal specifies a truth value for all its ground instances, unless there is a more specific literal specifying the opposite truth value
- **The order of the literals on the branch is irrelevant**

Inference Rule: Split



$$\{\neg v, \mathsf{P}(v), \neg\mathsf{P}(\mathsf{a})\} \overset{?}{\models} \mathsf{P}(x) \vee \mathsf{Q}(x)$$

Inference Rule: Split



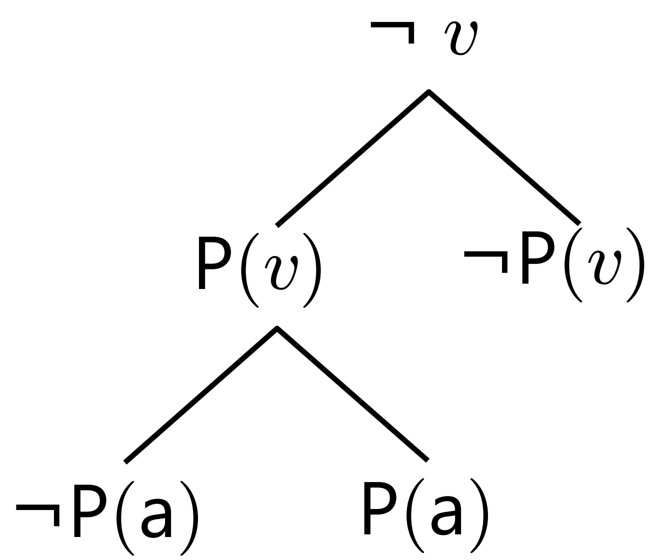
Branch: $\{\neg v, P(v), \neg P(a)\}$

True: $P(b)$

False: $\neg P(a)$, $\neg Q(a)$, $\neg Q(b)$

$$\{\neg v, P(v), \neg P(a)\} \overset{?}{\models} P(x) \lor Q(x)$$

Inference Rule: Split



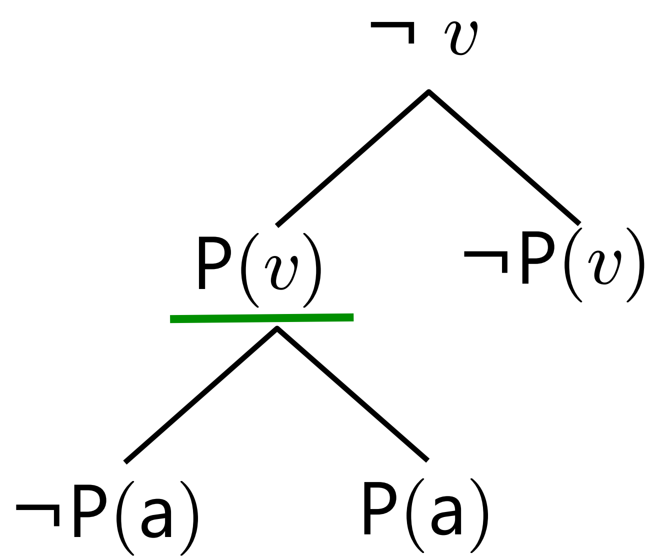
Branch: $\{\neg v, \mathsf{P}(v), \neg\mathsf{P}(\mathsf{a})\}$

True: $\mathsf{P}(\mathsf{b})$

False: $\neg\mathsf{P}(\mathsf{a})$, $\neg\mathsf{Q}(\mathsf{a})$, $\neg\mathsf{Q}(\mathsf{b})$

$$\{\neg v, \mathsf{P}(v), \neg\mathsf{P}(\mathsf{a})\} \overset{?}{\models} \mathsf{P}(x) \vee \mathsf{Q}(x)$$

Inference Rule: Split



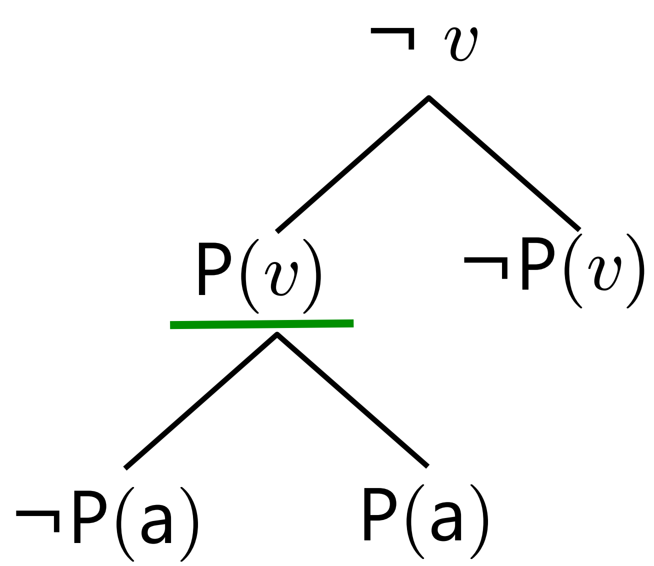
Branch: $\{\neg v, \mathsf{P}(v), \neg\mathsf{P}(\mathsf{a})\}$

True: $\mathsf{P}(\mathsf{b})$

False: $\neg\mathsf{P}(\mathsf{a})$, $\neg\mathsf{Q}(\mathsf{a})$, $\neg\mathsf{Q}(\mathsf{b})$

$$\{\neg v, \mathsf{P}(v), \neg\mathsf{P}(\mathsf{a})\} \overset{?}{\models} \mathsf{P}(x) \vee \mathsf{Q}(x)$$

Inference Rule: Split



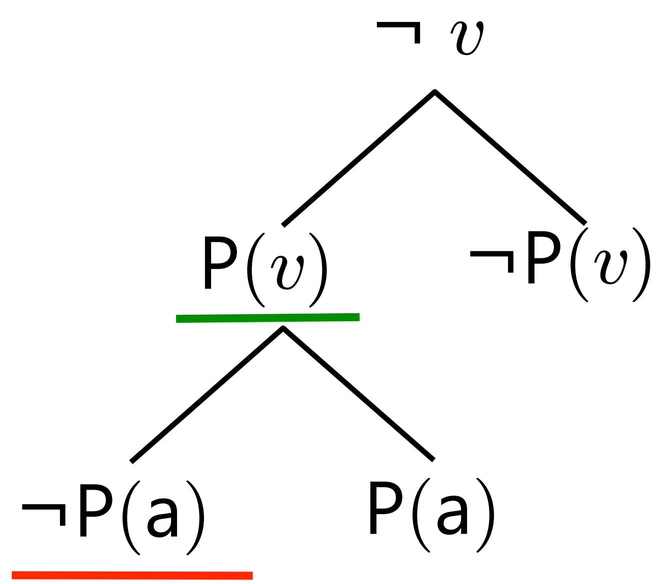
Branch: $\{\neg v, \mathsf{P}(v), \neg\mathsf{P}(\mathsf{a})\}$

True: $\mathsf{P}(\mathsf{b})$

False: $\neg\mathsf{P}(\mathsf{a}), \neg\mathsf{Q}(\mathsf{a}), \neg\mathsf{Q}(\mathsf{b})$

$$\{\neg v, \mathsf{P}(v), \neg\mathsf{P}(\mathsf{a})\} \overset{?}{\models} \mathsf{P}(x) \vee \mathsf{Q}(x)$$

Inference Rule: Split



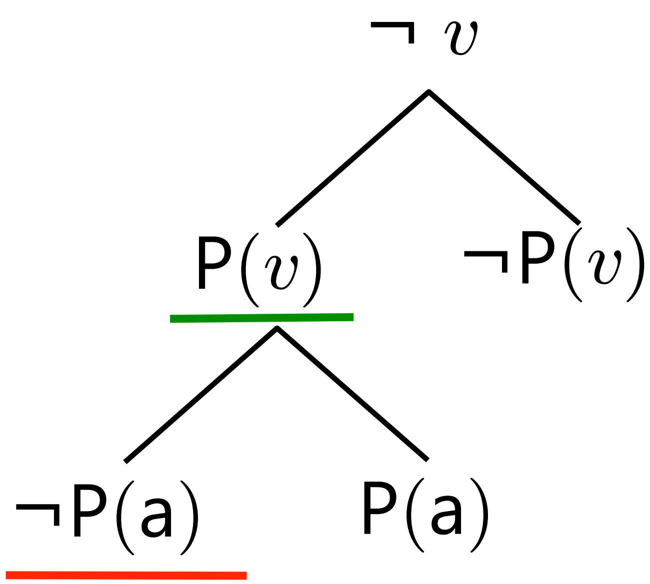
Branch: $\{\neg v, \mathsf{P}(v), \neg\mathsf{P}(\mathsf{a})\}$

True: $\mathsf{P}(\mathsf{b})$

False: $\neg\mathsf{P}(\mathsf{a}),\ \neg\mathsf{Q}(\mathsf{a}),\ \neg\mathsf{Q}(\mathsf{b})$

$$\{\neg v, \mathsf{P}(v), \neg\mathsf{P}(\mathsf{a})\} \overset{?}{\models} \mathsf{P}(x) \vee \mathsf{Q}(x)$$

Inference Rule: Split



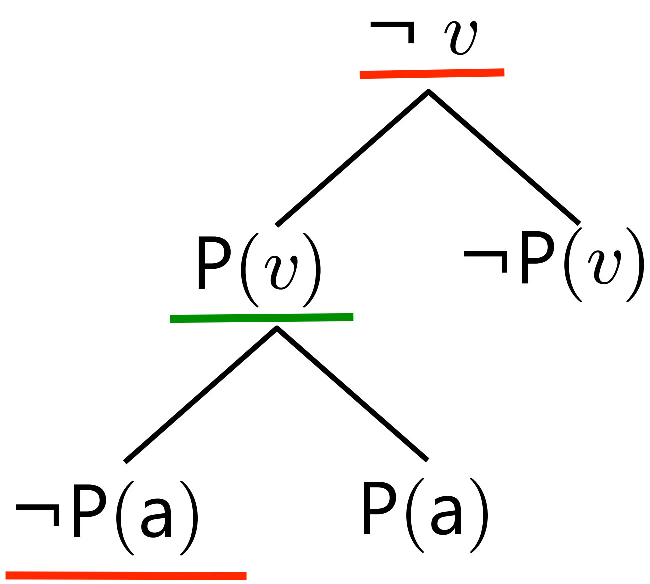
Branch: $\{\neg v, \mathsf{P}(v), \neg\mathsf{P}(\mathsf{a})\}$

True: $\mathsf{P}(\mathsf{b})$

False: $\neg\mathsf{P}(\mathsf{a})$, $\neg\mathsf{Q}(\mathsf{a})$, $\neg\mathsf{Q}(\mathsf{b})$

$$\{\neg v, \mathsf{P}(v), \neg\mathsf{P}(\mathsf{a})\} \overset{?}{\models} \mathsf{P}(x) \vee \mathsf{Q}(x)$$

Inference Rule: Split



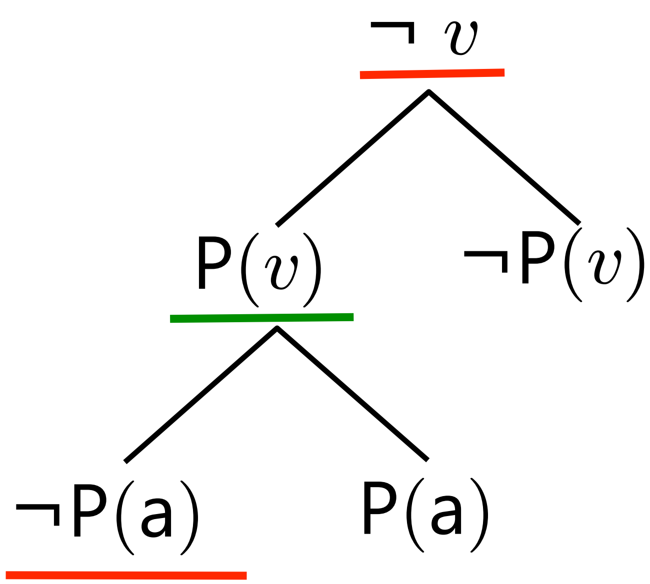
Branch: $\{\neg v, \mathsf{P}(v), \neg\mathsf{P}(\mathsf{a})\}$

True: $\mathsf{P}(\mathsf{b})$

False: $\neg\mathsf{P}(\mathsf{a})$, $\neg\mathsf{Q}(\mathsf{a})$, $\neg\mathsf{Q}(\mathsf{b})$

$$\{\neg v, \mathsf{P}(v), \neg\mathsf{P}(\mathsf{a})\} \overset{?}{\models} \mathsf{P}(x) \vee \mathsf{Q}(x)$$

Inference Rule: Split



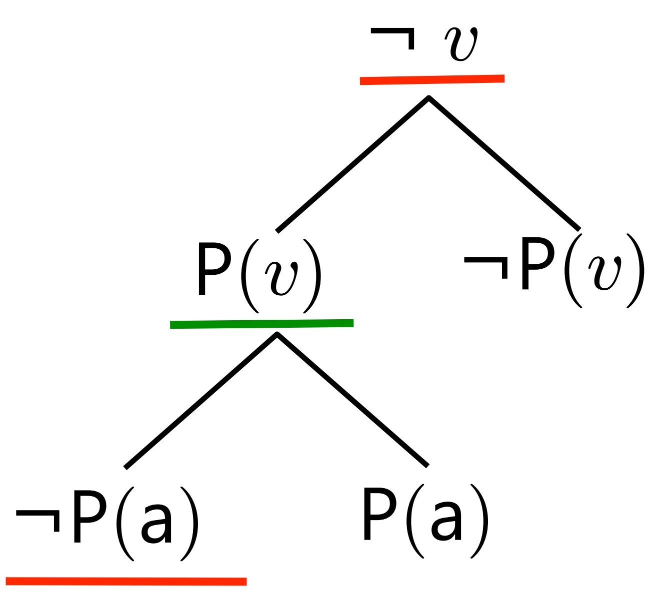
Branch: $\{\neg v, \mathsf{P}(v), \neg\mathsf{P}(\mathsf{a})\}$

True: $\mathsf{P}(\mathsf{b})$

False: $\neg\mathsf{P}(\mathsf{a})$, $\neg\mathsf{Q}(\mathsf{a})$, $\neg\mathsf{Q}(\mathsf{b})$

$$\{\neg v, \mathsf{P}(v), \neg\mathsf{P}(\mathsf{a})\} \stackrel{?}{\models} \mathsf{P}(x) \vee \mathsf{Q}(x) \quad ✗$$

Inference Rule: Split



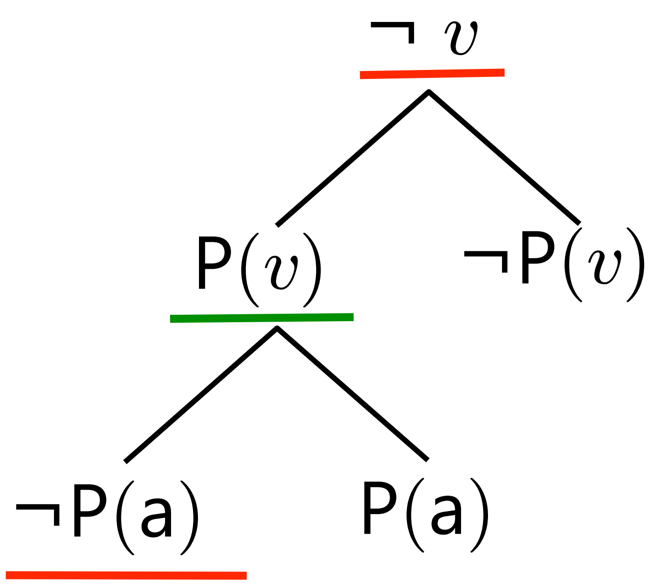
Branch: $\{\neg v, \mathsf{P}(v), \neg\mathsf{P}(\mathsf{a})\}$

True: $\mathsf{P}(\mathsf{b})$

False: $\neg\mathsf{P}(\mathsf{a})$, $\neg\mathsf{Q}(\mathsf{a})$, $\neg\mathsf{Q}(\mathsf{b})$

$$\{\neg v, \mathsf{P}(v), \neg\mathsf{P}(\mathsf{a})\} \overset{?}{\models} \mathsf{P}(x) \vee \mathsf{Q}(x) \quad ✗ \quad \xrightarrow{\text{Context Unifier}} \quad \mathsf{P}(\mathsf{a}) \vee \mathsf{Q}(\mathsf{a})$$

Inference Rule: Split



Branch: $\{\neg v, \mathsf{P}(v), \neg\mathsf{P}(\mathsf{a})\}$

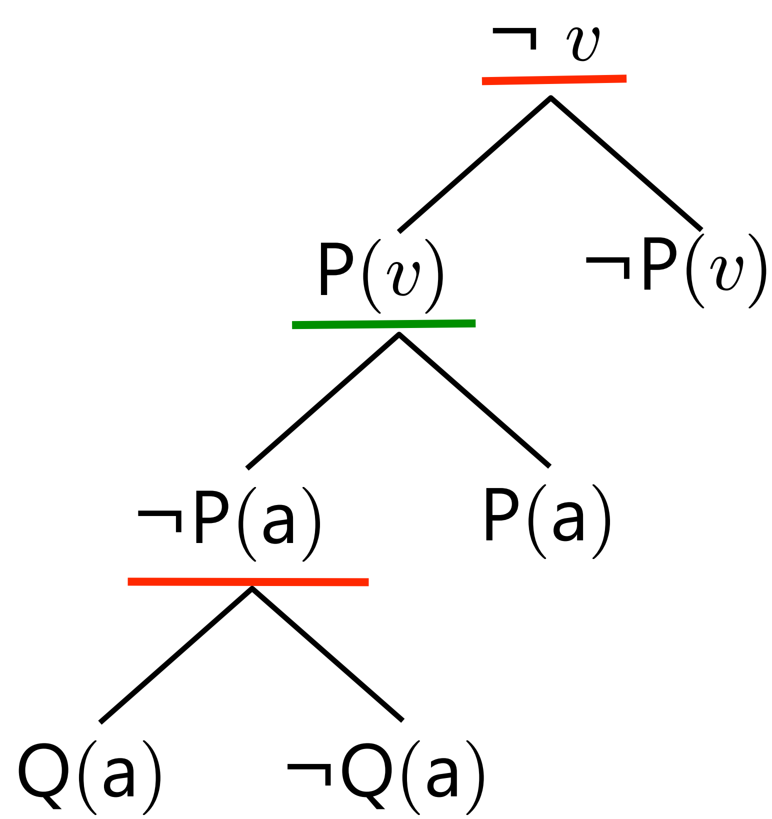
True: $\mathsf{P}(\mathsf{b})$

False: $\neg\mathsf{P}(\mathsf{a})$, $\neg\mathsf{Q}(\mathsf{a})$, $\neg\mathsf{Q}(\mathsf{b})$

$$\{\neg v, \mathsf{P}(v), \neg\mathsf{P}(\mathsf{a})\} \overset{?}{\models} \mathsf{P}(x) \vee \mathsf{Q}(x) \quad ✗ \quad \xrightarrow{\text{Context Unifier}} \quad \mathsf{P}(\mathsf{a}) \vee \mathsf{Q}(\mathsf{a})$$

Split

Inference Rule: Split



Branch: $\{\neg v, \mathsf{P}(v), \neg\mathsf{P}(\mathsf{a})\}$

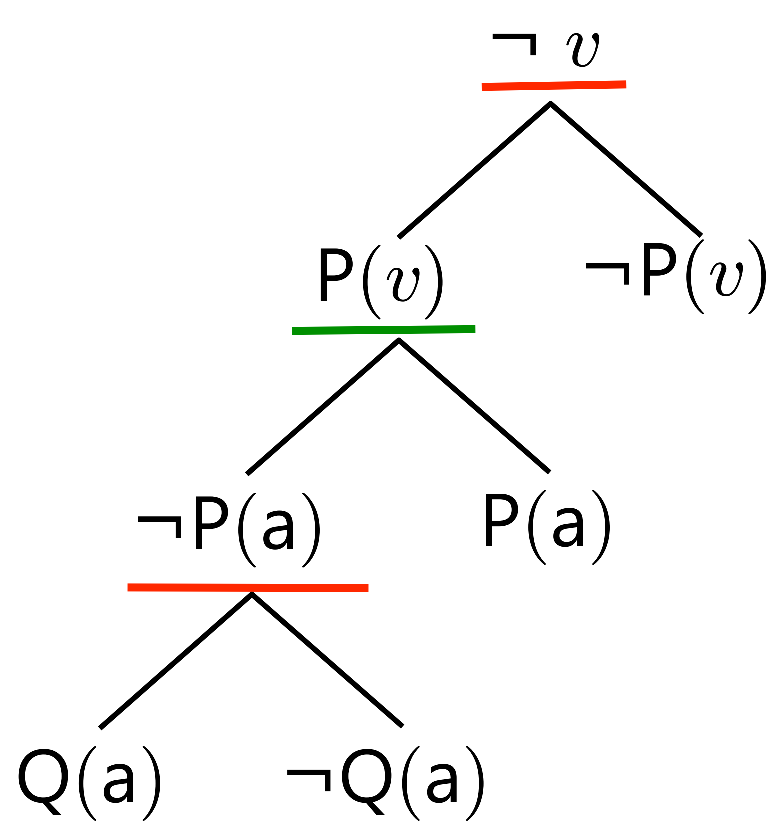
True: $\mathsf{P}(\mathsf{b})$

False: $\neg\mathsf{P}(\mathsf{a})$, $\neg\mathsf{Q}(\mathsf{a})$, $\neg\mathsf{Q}(\mathsf{b})$

$$\{\neg v, \mathsf{P}(v), \neg\mathsf{P}(\mathsf{a})\} \overset{?}{\models} \mathsf{P}(x) \vee \mathsf{Q}(x) \quad ✗ \quad \xrightarrow{\text{Context Unifier}} \quad \mathsf{P}(\mathsf{a}) \vee \underline{\mathsf{Q}(\mathsf{a})}$$

Split

Inference Rule: Split



Branch: $\{\neg v, \mathsf{P}(v), \neg\mathsf{P}(\mathsf{a})\}$

True: $\mathsf{P}(\mathsf{b})$

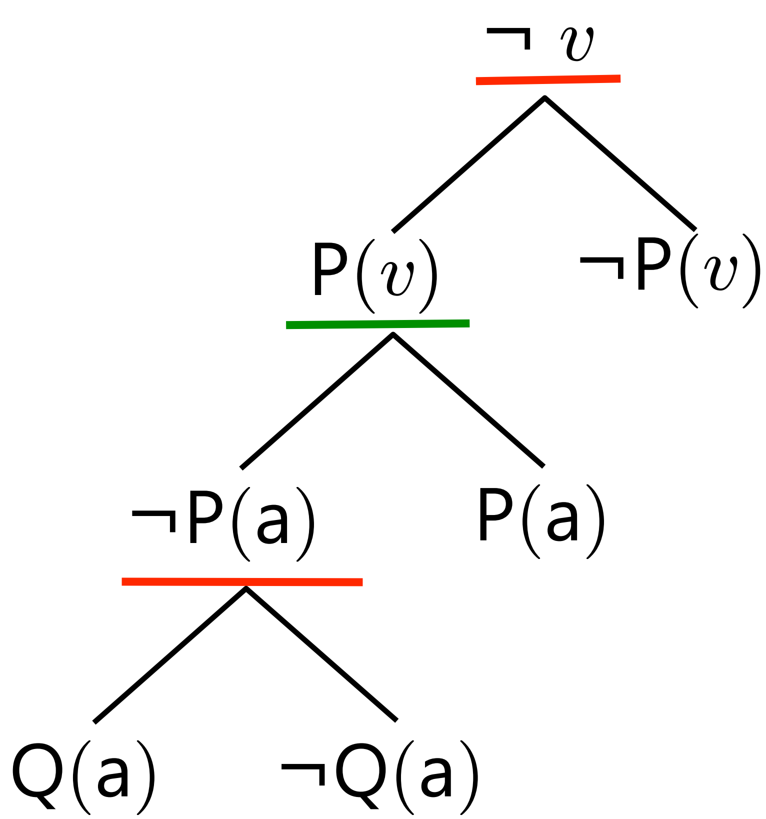
False: $\neg\mathsf{P}(\mathsf{a})$, $\neg\mathsf{Q}(\mathsf{a})$, $\neg\mathsf{Q}(\mathsf{b})$

$$\{\neg v, \mathsf{P}(v), \neg\mathsf{P}(\mathsf{a})\} \overset{?}{\models} \mathsf{P}(x) \lor \mathsf{Q}(x) \quad ✗ \quad \xrightarrow{\text{Context Unifier}} \quad \mathsf{P}(\mathsf{a}) \lor \underline{\mathsf{Q}(\mathsf{a})}$$

Split

$$\{\neg v, \mathsf{P}(v), \neg\mathsf{P}(\mathsf{a}), \mathsf{Q}(\mathsf{a})\} \overset{?}{\models} \mathsf{P}(x) \lor \mathsf{Q}(x)$$

Inference Rule: Split



Branch: $\{\neg v, \mathsf{P}(v), \neg\mathsf{P(a)}\}$

True: $\mathsf{P(b)}$

False: $\neg\mathsf{P(a)}$, $\neg\mathsf{Q(a)}$, $\neg\mathsf{Q(b)}$

Branch: $\{\neg v, \mathsf{P}(v), \neg\mathsf{P(a)}, \mathsf{Q(a)}\}$

True: $\mathsf{P(b)}$, $\mathsf{Q(a)}$

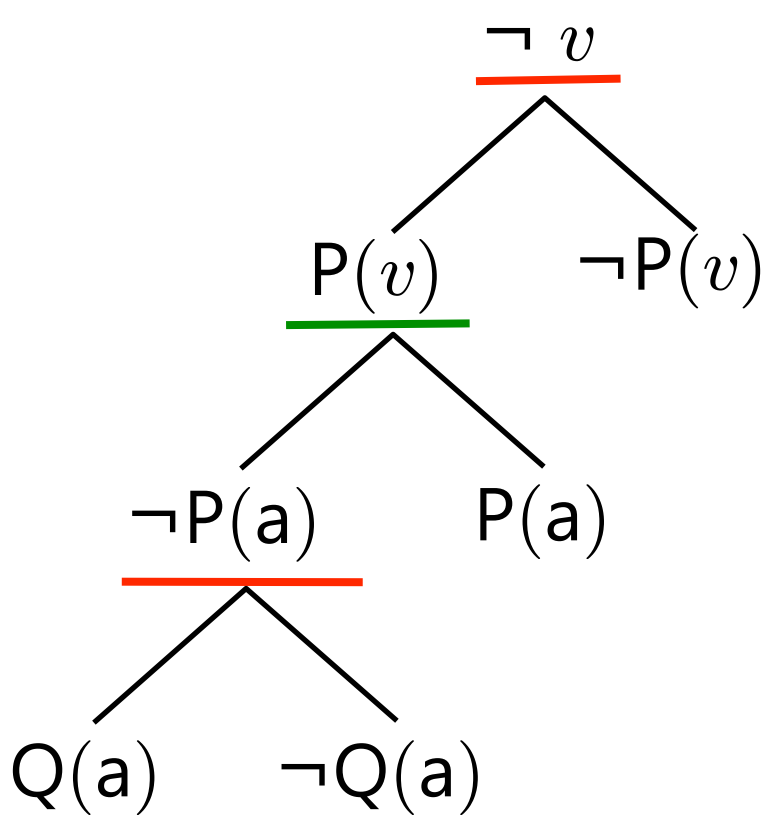
False: $\neg\mathsf{P(a)}$, $\neg\mathsf{Q(b)}$

$$\{\neg v, \mathsf{P}(v), \neg\mathsf{P(a)}\} \overset{?}{\models} \mathsf{P}(x) \vee \mathsf{Q}(x) \quad ✗ \quad \xrightarrow{\text{Context Unifier}} \quad \mathsf{P(a)} \vee \mathsf{Q(a)}$$

Split

$$\{\neg v, \mathsf{P}(v), \neg\mathsf{P(a)}, \mathsf{Q(a)}\} \overset{?}{\models} \mathsf{P}(x) \vee \mathsf{Q}(x)$$

Inference Rule: Split



Branch: $\{\neg v, \mathsf{P}(v), \neg\mathsf{P}(\mathsf{a})\}$

True: $\mathsf{P}(\mathsf{b})$

False: $\neg\mathsf{P}(\mathsf{a})$, $\neg\mathsf{Q}(\mathsf{a})$, $\neg\mathsf{Q}(\mathsf{b})$

Branch: $\{\neg v, \mathsf{P}(v), \neg\mathsf{P}(\mathsf{a}), \mathsf{Q}(\mathsf{a})\}$

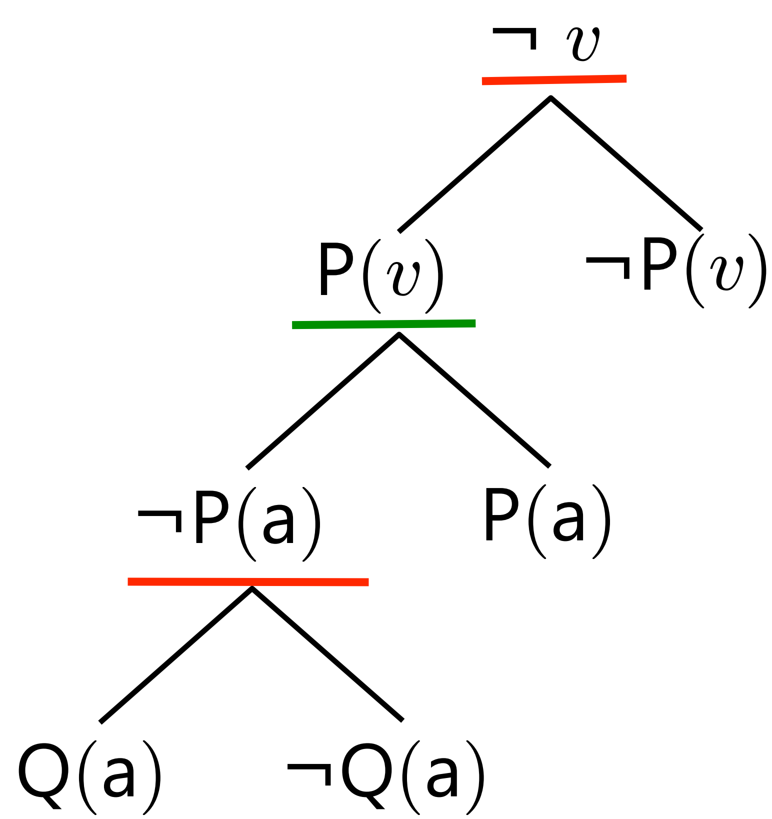
True: $\mathsf{P}(\mathsf{b})$, $\mathsf{Q}(\mathsf{a})$

False: $\neg\mathsf{P}(\mathsf{a})$, $\neg\mathsf{Q}(\mathsf{b})$

$$\{\neg v, \mathsf{P}(v), \neg\mathsf{P}(\mathsf{a})\} \overset{?}{\models} \mathsf{P}(x) \vee \mathsf{Q}(x) \quad ✗ \quad \xrightarrow{\text{Context Unifier}} \quad \dfrac{\mathsf{P}(\mathsf{a}) \vee \mathsf{Q}(\mathsf{a})}{\text{Split}}$$

$$\{\neg v, \mathsf{P}(v), \neg\mathsf{P}(\mathsf{a}), \mathsf{Q}(\mathsf{a})\} \overset{?}{\models} \mathsf{P}(x) \vee \mathsf{Q}(x)$$

Inference Rule: Split



Branch: $\{\neg v, P(v), \neg P(a)\}$

True: $P(b)$

False: $\neg P(a)$, $\neg Q(a)$, $\neg Q(b)$

Branch: $\{\neg v, P(v), \neg P(a), Q(a)\}$

True: $P(b)$, $Q(a)$

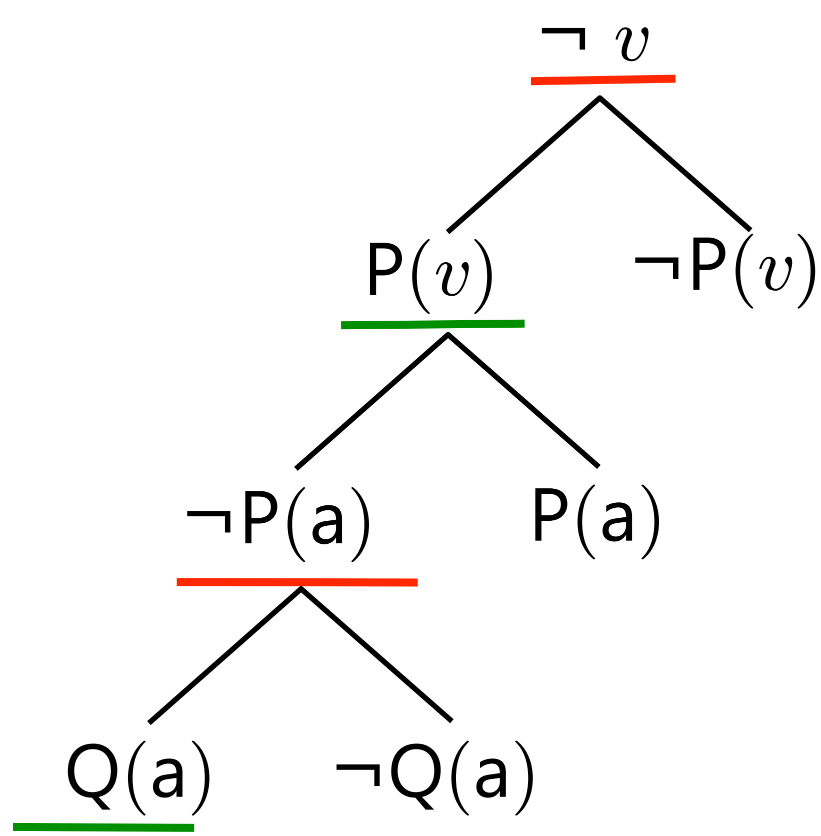
False: $\neg P(a)$, $\neg Q(b)$

$$\{\neg v, P(v), \neg P(a)\} \overset{?}{\models} P(x) \vee Q(x) \quad ✗ \quad \xrightarrow{\text{Context Unifier}} \quad P(a) \vee Q(a)$$

$$\{\neg v, P(v), \neg P(a), Q(a)\} \overset{?}{\models} P(x) \vee Q(x)$$

Split

Inference Rule: Split



Branch: $\{\neg v, \mathsf{P}(v), \neg\mathsf{P}(\mathsf{a})\}$

True: $\mathsf{P}(\mathsf{b})$

False: $\neg\mathsf{P}(\mathsf{a}), \neg\mathsf{Q}(\mathsf{a}), \neg\mathsf{Q}(\mathsf{b})$

Branch: $\{\neg v, \mathsf{P}(v), \neg\mathsf{P}(\mathsf{a}), \mathsf{Q}(\mathsf{a})\}$

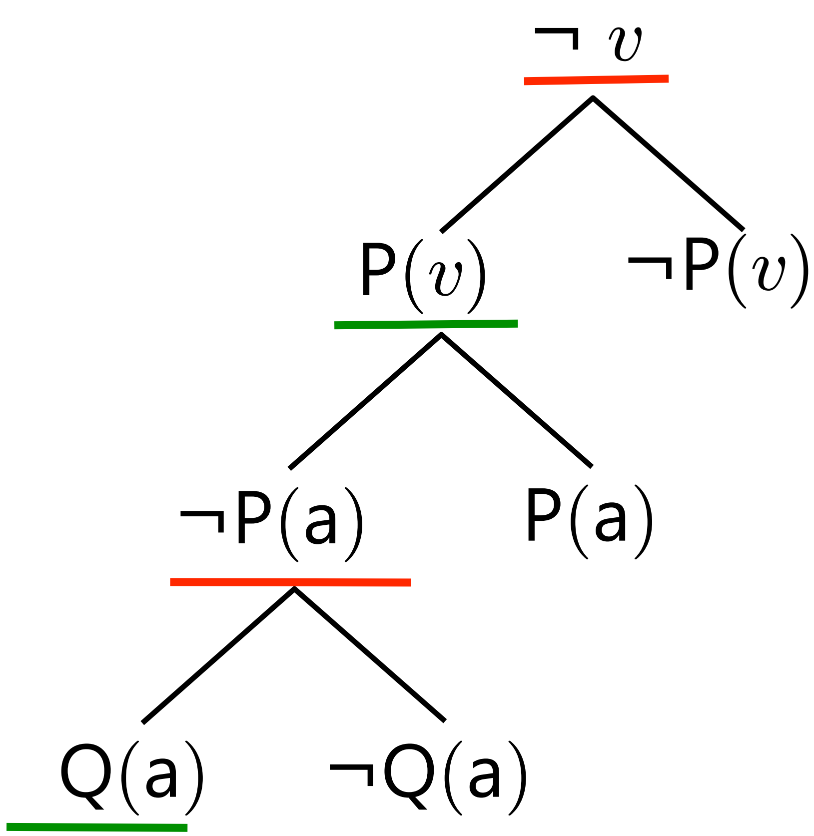
True: $\mathsf{P}(\mathsf{b}), \mathsf{Q}(\mathsf{a})$

False: $\neg\mathsf{P}(\mathsf{a}), \neg\mathsf{Q}(\mathsf{b})$

$$\{\neg v, \mathsf{P}(v), \neg\mathsf{P}(\mathsf{a})\} \overset{?}{\models} \mathsf{P}(x) \vee \mathsf{Q}(x) \quad ✗ \quad \xrightarrow{\text{Context Unifier}} \quad \dfrac{\mathsf{P}(\mathsf{a}) \vee \mathsf{Q}(\mathsf{a})}{\text{Split}}$$

$$\{\neg v, \mathsf{P}(v), \neg\mathsf{P}(\mathsf{a}), \mathsf{Q}(\mathsf{a})\} \overset{?}{\models} \mathsf{P}(x) \vee \mathsf{Q}(x)$$

Inference Rule: Split



Branch: $\{\neg v, \mathsf{P}(v), \neg\mathsf{P}(\mathsf{a})\}$

True: $\mathsf{P}(\mathsf{b})$

False: $\neg\mathsf{P}(\mathsf{a}),\ \neg\mathsf{Q}(\mathsf{a}),\ \neg\mathsf{Q}(\mathsf{b})$

Branch: $\{\neg v, \mathsf{P}(v), \neg\mathsf{P}(\mathsf{a}), \mathsf{Q}(\mathsf{a})\}$

True: $\mathsf{P}(\mathsf{b}),\ \mathsf{Q}(\mathsf{a})$

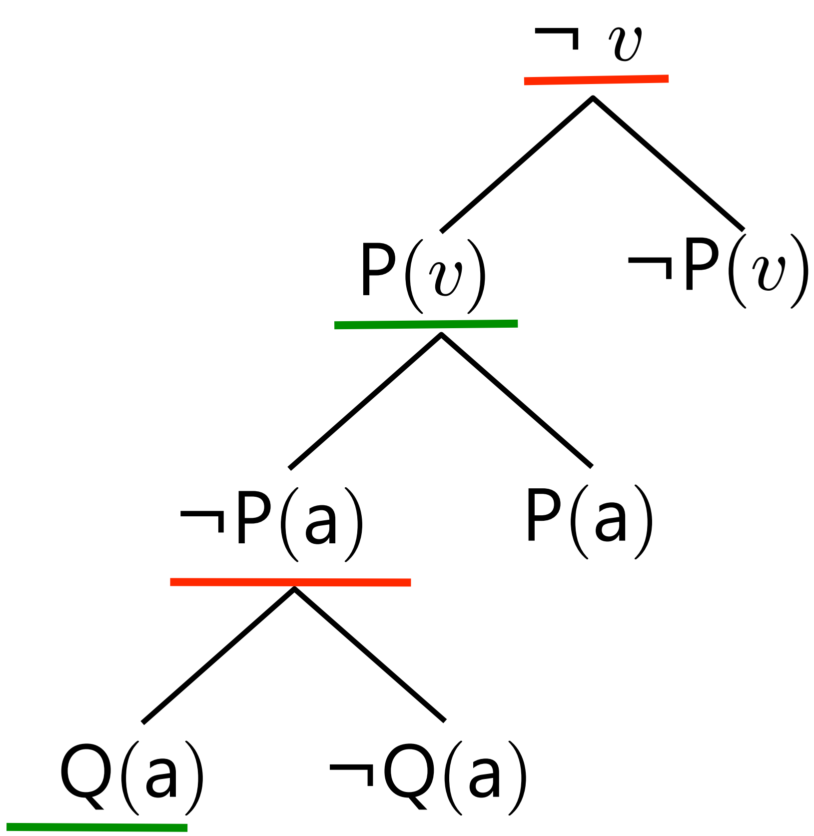
False: $\neg\mathsf{P}(\mathsf{a}),\ \neg\mathsf{Q}(\mathsf{b})$

$$\{\neg v, \mathsf{P}(v), \neg\mathsf{P}(\mathsf{a})\} \overset{?}{\models} \mathsf{P}(x) \vee \mathsf{Q}(x) \quad ✗ \quad \xrightarrow{\text{Context Unifier}} \quad \mathsf{P}(\mathsf{a}) \vee \mathsf{Q}(\mathsf{a})$$

$$\{\neg v, \mathsf{P}(v), \neg\mathsf{P}(\mathsf{a}), \mathsf{Q}(\mathsf{a})\} \overset{?}{\models} \mathsf{P}(x) \vee \mathsf{Q}(x)$$

Split

Inference Rule: Split



Branch: $\{\neg v, \mathsf{P}(v), \neg\mathsf{P}(\mathsf{a})\}$

True: $\mathsf{P}(\mathsf{b})$

False: $\neg\mathsf{P}(\mathsf{a}),\ \neg\mathsf{Q}(\mathsf{a}),\ \neg\mathsf{Q}(\mathsf{b})$

Branch: $\{\neg v, \mathsf{P}(v), \neg\mathsf{P}(\mathsf{a}), \mathsf{Q}(\mathsf{a})\}$

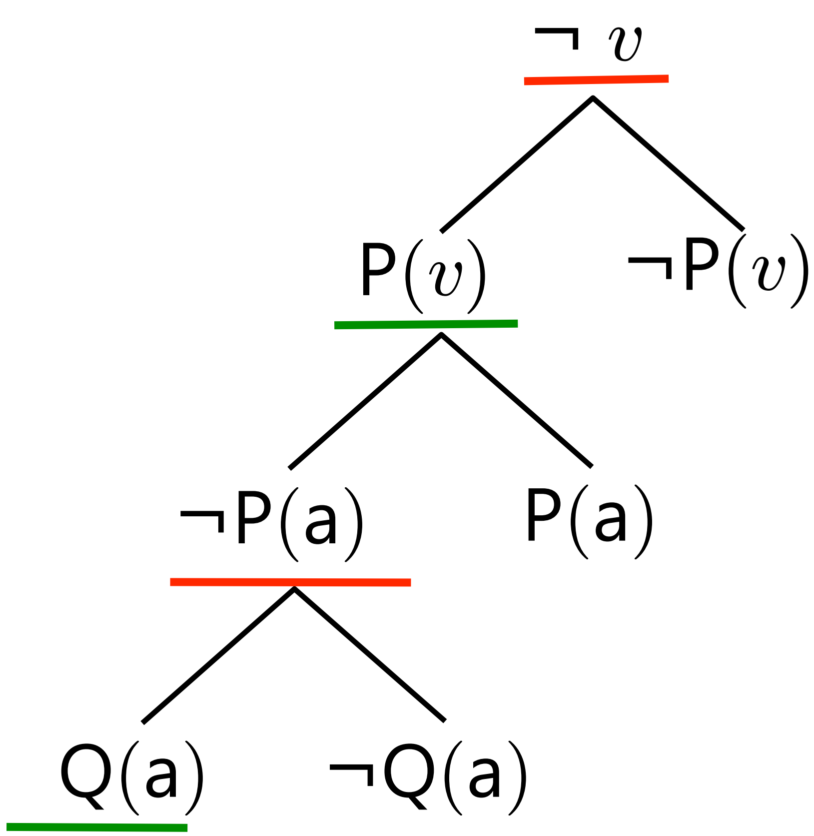
True: $\mathsf{P}(\mathsf{b}),\ \mathsf{Q}(\mathsf{a})$

False: $\neg\mathsf{P}(\mathsf{a}),\ \neg\mathsf{Q}(\mathsf{b})$

$$\{\neg v, \mathsf{P}(v), \neg\mathsf{P}(\mathsf{a})\} \overset{?}{\models} \mathsf{P}(x) \vee \mathsf{Q}(x) \quad ✗ \quad \xrightarrow{\text{Context Unifier}} \quad \frac{\mathsf{P}(\mathsf{a}) \vee \mathsf{Q}(\mathsf{a})}{\text{Split}}$$

$$\{\neg v, \mathsf{P}(v), \neg\mathsf{P}(\mathsf{a}), \mathsf{Q}(\mathsf{a})\} \overset{?}{\models} \mathsf{P}(x) \vee \mathsf{Q}(x) \quad ✓$$

Inference Rule: Split



Branch: $\{\neg v, \mathsf{P}(v), \neg\mathsf{P}(\mathsf{a})\}$

True: $\mathsf{P}(\mathsf{b})$

False: $\neg\mathsf{P}(\mathsf{a})$, $\neg\mathsf{Q}(\mathsf{a})$, $\neg\mathsf{Q}(\mathsf{b})$

Branch: $\{\neg v, \mathsf{P}(v), \neg\mathsf{P}(\mathsf{a}), \mathsf{Q}(\mathsf{a})\}$

True: $\mathsf{P}(\mathsf{b})$, $\mathsf{Q}(\mathsf{a})$

False: $\neg\mathsf{P}(\mathsf{a})$, $\neg\mathsf{Q}(\mathsf{b})$

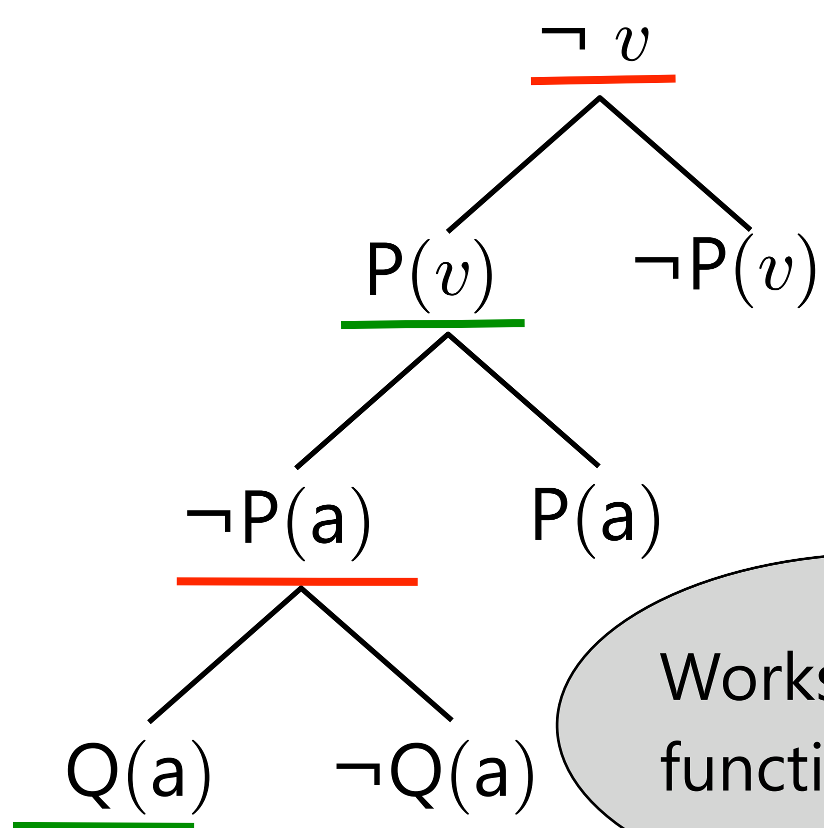
$$\{\neg v, \mathsf{P}(v), \neg\mathsf{P}(\mathsf{a})\} \overset{?}{\models} \mathsf{P}(x) \vee \mathsf{Q}(x) \quad ✗ \quad \xrightarrow{\text{Context Unifier}} \quad \mathsf{P}(\mathsf{a}) \vee \mathsf{Q}(\mathsf{a})$$

$$\{\neg v, \mathsf{P}(v), \neg\mathsf{P}(\mathsf{a}), \mathsf{Q}(\mathsf{a})\} \overset{?}{\models} \mathsf{P}(x) \vee \mathsf{Q}(x) \quad ✓$$

Split

Split - detect falsified instances and repair interpretation
Additional rules: Close, Assert, Compact, Resolve, Subsume

Inference Rule: Split



Works also with function symbols

Branch: $\{\neg v, \mathsf{P}(v), \neg\mathsf{P}(\mathsf{a})\}$

True: $\mathsf{P}(\mathsf{b})$

False: $\neg\mathsf{P}(\mathsf{a})$, $\neg\mathsf{Q}(\mathsf{a})$, $\neg\mathsf{Q}(\mathsf{b})$

Branch: $\{\neg v, \mathsf{P}(v), \neg\mathsf{P}(\mathsf{a}), \mathsf{Q}(\mathsf{a})\}$

True: $\mathsf{P}(\mathsf{b})$, $\mathsf{Q}(\mathsf{a})$

False: $\neg\mathsf{P}(\mathsf{a})$, $\neg\mathsf{Q}(\mathsf{b})$

$$\{\neg v, \mathsf{P}(v), \neg\mathsf{P}(\mathsf{a})\} \overset{?}{\models} \mathsf{P}(x) \vee \mathsf{Q}(x) \quad ✗ \quad \xrightarrow{\text{Context Unifier}} \quad \dfrac{\mathsf{P}(\mathsf{a}) \vee \mathsf{Q}(\mathsf{a})}{\text{Split}}$$

$$\{\neg v, \mathsf{P}(v), \neg\mathsf{P}(\mathsf{a}), \mathsf{Q}(\mathsf{a})\} \overset{?}{\models} \mathsf{P}(x) \vee \mathsf{Q}(x) \quad ✓$$

Split - detect falsified instances and repair interpretation

Additional rules: Close, Assert, Compact, Resolve, Subsume

ME - Achievements so far

- **FDPLL** [CADE-17]
  - Basic ideas, predecessor of ME
- **ME Calculus** [CADE-19, AI Journal]
  - Proper treatment of universal variables and unit propagation
  - Semantically justified redundancy criteria
- **ME+Equality** [CADE-20]
  - Superposition inference rules, currently being implemented
- **ME+Lemmas** [LPAR 2006]
- **Darwin prover** [JAIT 2006]
  `http://combination.cs.uiowa.edu/Darwin/`
  - Won CASC-J3 and CASC-21 EPR division
- **FM-Darwin**: finite model computation [JAL 2007]

Adding Integer Arithmetic to ME

Issues

- Define the input language
- Generalize semantic trees
- Branch closure (soundness aspect)
- Model construction (completeness aspect)
- Inference rules
- Properties

Adding Integer Arithmetic to ME

Issues

- Define the input language
- Generalize semantic trees
- Branch closure (soundness aspect)
- Model construction (completeness aspect)
- Inference rules
- Properties

Discuss these issues in the following

Input Language

- Constraint clauses $C \leftarrow c$, where C is a "normalized" clause, e.g.

$$\mathsf{P}(x_1, x_2) \vee \neg \mathsf{Q}(x_2, x_3) \leftarrow \exists y\ 2 \leq y \wedge y < a + x_1 \wedge x_2 = x_3$$

  where P, Q, ... are free predicate symbols

- Constraints c generated by the syntax

$$\begin{array}{lcl} n & ::= & \text{non-negative integer constants } 0, 1, 2, \ldots \\ a & ::= & \text{free constants ("parameters") a, b, } \ldots \\ x & ::= & \text{variables } x, y, \ldots \\ t & ::= & n \mid a \mid x \mid t_1 + t_2 \\ l & ::= & \top \mid \bot \mid t_1 \leq t_2 \mid t_1 < t_2 \\ c & ::= & l \mid c_1 \wedge c_2 \mid \exists x\ c \end{array}$$

  Interpreted over $\mathbb{N}$ (Literals $t_1 = t_2$ and $\neg l$ can be represented)

- Domain declaration a : $[n_1 \mathinner{..} n_2]$, for every input parameter a

Generalized Semantic Trees

Generalized Semantic Trees

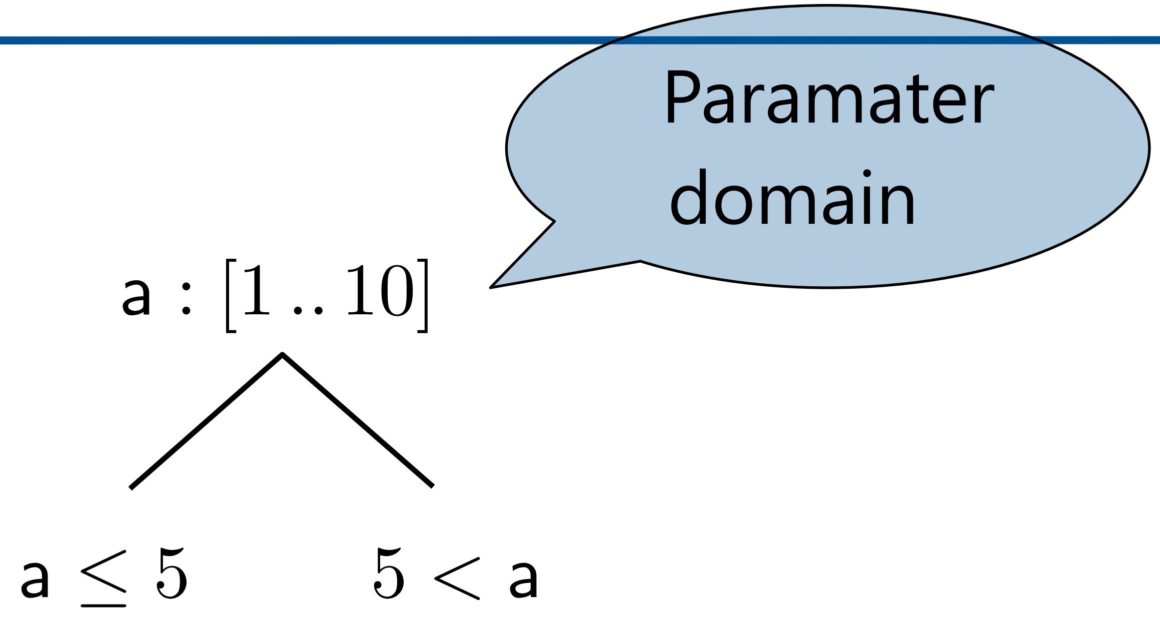
$\mathsf{a} : [1\,..\,10]$

Generalized Semantic Trees

Paramater domain

a : $[1\,..\,10]$

Generalized Semantic Trees



Generalized Semantic Trees

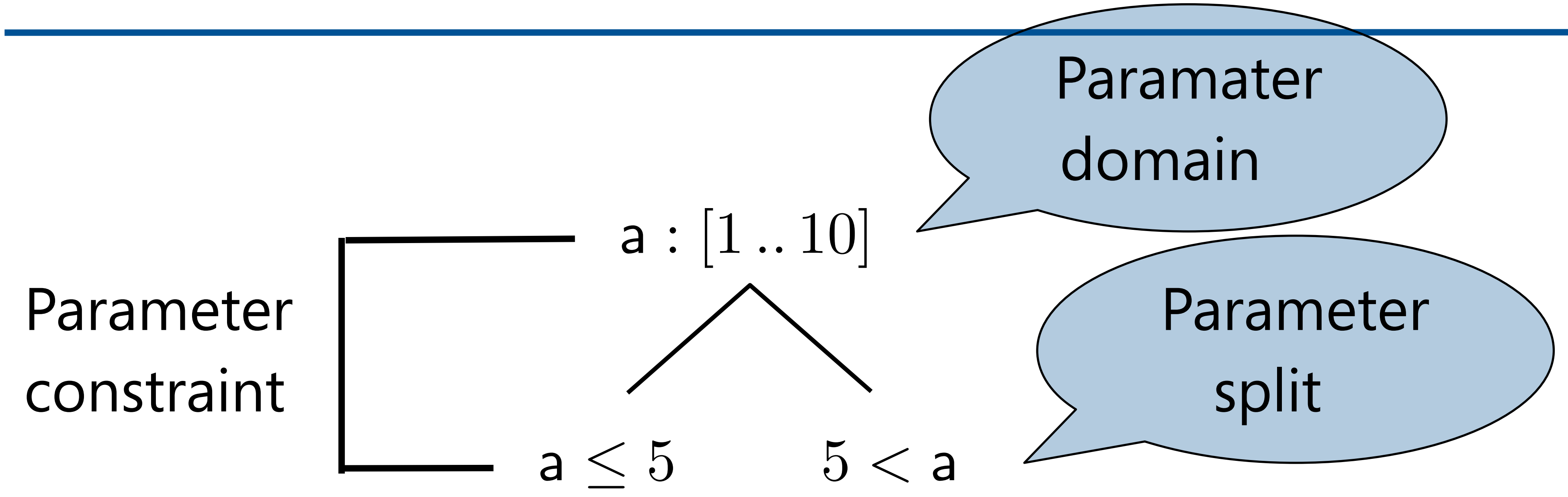
$\mathsf{a} : [1\,..\,10]$

Paramater domain

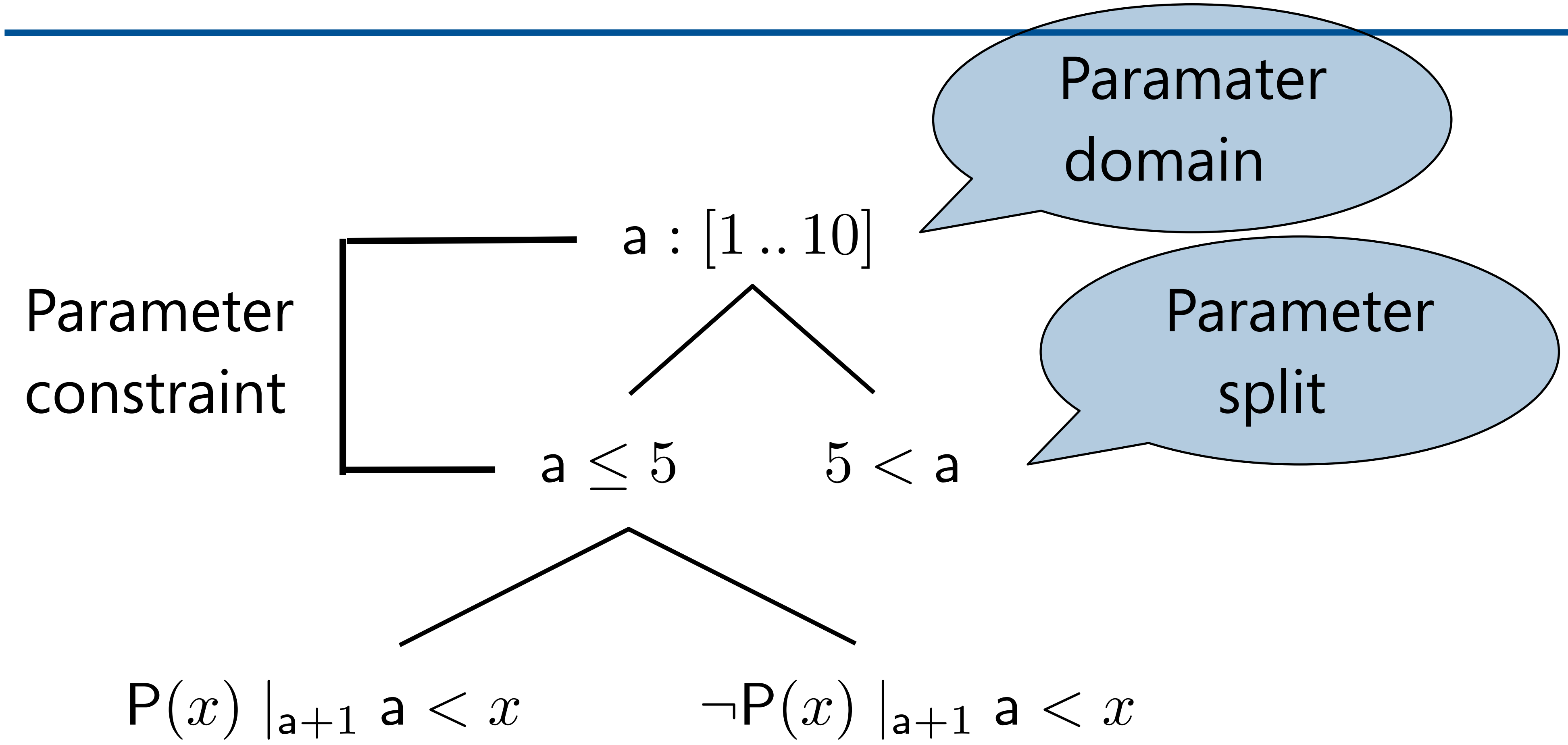
$\mathsf{a} \leq 5$ $\qquad$ $5 < \mathsf{a}$

Parameter split

Generalized Semantic Trees



Generalized Semantic Trees



Generalized Semantic Trees

Paramater domain

$\mathsf{a} : [1 \mathinner{..} 10]$

Parameter constraint

Parameter split

$\mathsf{a} \leq 5$ $\quad\quad 5 < \mathsf{a}$

Branch literal

$\mathsf{P}(x) \mid_{\mathsf{a}+1} \mathsf{a} < x$ $\quad\quad \neg\mathsf{P}(x) \mid_{\mathsf{a}+1} \mathsf{a} < x$

Generalized Semantic Trees

Paramater domain

$a : [1\,..\,10]$

Parameter constraint

Parameter split

$a \leq 5$ $\qquad$ $5 < a$

Branch literal

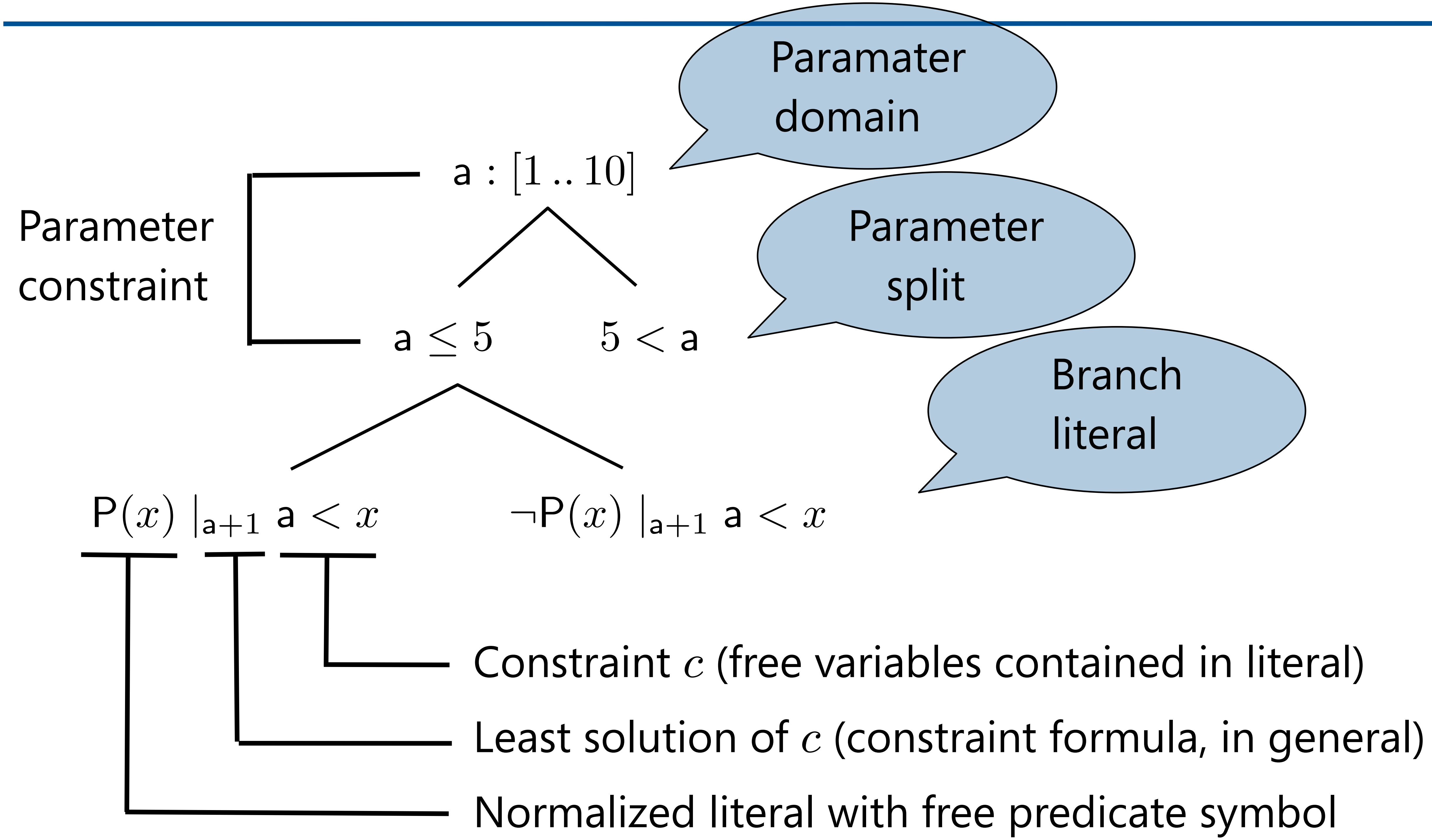
$P(x) \mid_{a+1} a < x$ $\qquad$ $\neg P(x) \mid_{a+1} a < x$

Constraint c (free variables contained in literal)

Least solution of c (constraint formula, in general)

Normalized literal with free predicate symbol

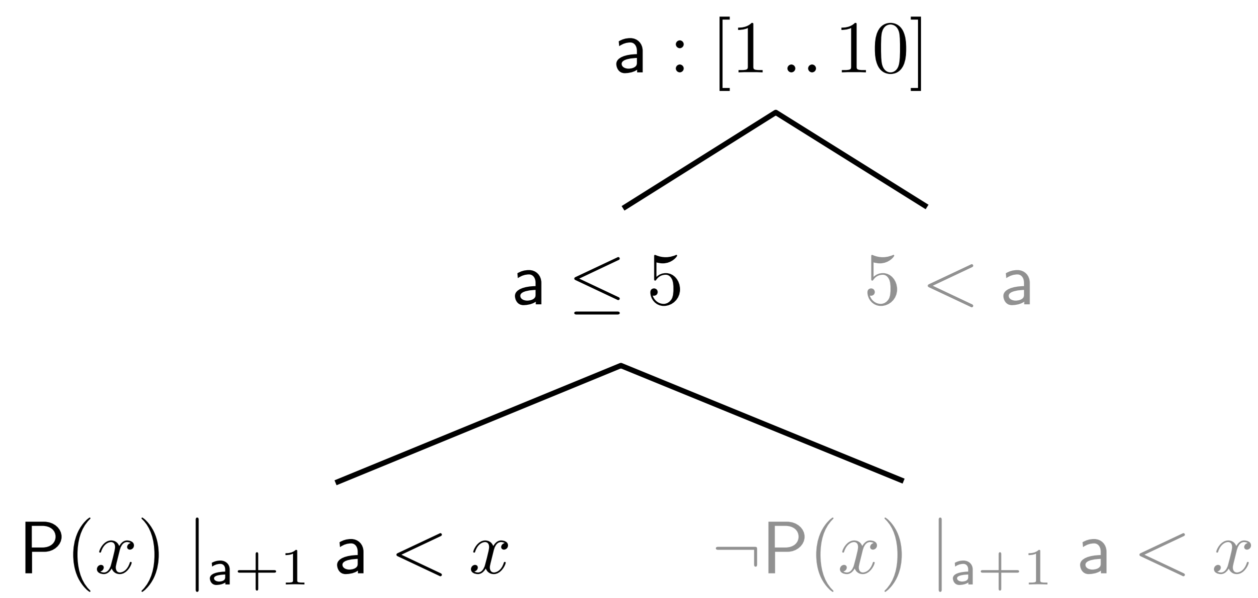
Generalized Semantic Trees



What is the meaning of a branch literal (model construction)?

Model Construction

$$a = 4 : \quad \begin{array}{c} I \\ \hline P(5) \\ P(6) \\ P(7) \\ \vdots \end{array}$$



Interpretations represented by a branch

1. Let α: a → ℕ be an assignment consistent with parameter constraints: ℕ,α ⊨ a : [1 .. 10] ∧ a ≤ 5

2. For all σ: x → ℕ: if ℕ,α ⊨ (a<x)σ then P(xσ) → true "by default"

> A branch literal specifies a truth value for all its ground instances satisfying the constraint, unless there is a branch literal specifying the opposite truth value and that has a greater lower bound.

Model Construction

$$\mathsf{a} : [1 \,..\, 10]$$

$$\mathsf{a} \leq 5 \qquad\qquad 5 < \mathsf{a}$$

$$\mathsf{P}(x) \mid_{\mathsf{a}+1} \mathsf{a} < x \qquad\qquad \neg\mathsf{P}(x) \mid_{\mathsf{a}+1} \mathsf{a} < x$$

Important invariants, maintained by the calculus

For every parameter assignment that satisfies the parameter constraints:

1. The constraint c of any branch literal $\mathsf{L} \mid_t \ c$ is solvable
   i.e. $\mathsf{a} : [1 \,..\, 10] \wedge \mathsf{a} \leq 5 \ \models \ \exists x \ \mathsf{a} < x$ (no junk)

2. No complementary branch literal $\neg\mathsf{L} \mid_t \ c$ has the same lower bound:
   if $\neg\mathsf{P}(x) \mid_t \ c$ in branch then $\mathsf{a} : [1 \,..\, 10] \wedge \mathsf{a} \leq 5 \ \models t \neq \mathsf{a}+1$

(no confusion)

Inference Rule - Split

Inference Rule - Split

$$\mathsf{a} : [1\,..\,10]$$

$$\mathsf{P}(x) \;|_{\mathsf{a}+1}\; \mathsf{a} < x \qquad \neg\mathsf{P}(x) \;|_{\mathsf{a}+1}\; \mathsf{a} < x$$

Inference Rule - Split

$$\frac{I}{\begin{array}{c} P(a+1) \\ P(a+2) \\ P(a+3) \\ \vdots \end{array}}$$

$$\mathsf{a} : [1 \,..\, 10]$$

$$\mathsf{P}(x) \mid_{\mathsf{a}+1} \mathsf{a} < x \qquad \neg \mathsf{P}(x) \mid_{\mathsf{a}+1} \mathsf{a} < x$$

Inference Rule - Split

$$\boxed{\neg P(x) \leftarrow a + 2 < x}$$

$$\begin{array}{c} \neg P(a+3) \\ \neg P(a+4) \\ \neg P(a+5) \\ \vdots \end{array}$$

$$\frac{I}{\begin{array}{c} P(a+1) \\ P(a+2) \\ P(a+3) \\ \vdots \end{array}}$$

$$\mathsf{a} : [1 \mathinner{..} 10]$$

$$\mathsf{P}(x) \;|_{\mathsf{a}+1}\; \mathsf{a} < x \qquad \neg\mathsf{P}(x) \;|_{\mathsf{a}+1}\; \mathsf{a} < x$$

Inference Rule - Split

$$\boxed{\neg P(x) \leftarrow a + 2 < x}$$

$$\neg P(a+3)$$
$$\neg P(a+4)$$
$$\neg P(a+5)$$
$$\vdots$$

$$\frac{I}{\begin{array}{c} P(a+1) \\ P(a+2) \\ P(a+3) \\ \vdots \end{array}}$$

$\mathsf{a} : [1\,..\,10]$

$\mathsf{P}(x) \mid_{\mathsf{a}+1} \mathsf{a} < x$ $\qquad$ $\neg\mathsf{P}(x) \mid_{\mathsf{a}+1} \mathsf{a} < x$

Repair interpretation

Inference Rule - Split

$$\boxed{\neg P(x) \leftarrow a + 2 < x}$$

$$\neg P(a+3)$$
$$\neg P(a+4)$$
$$\neg P(a+5)$$
$$\vdots$$

$$\frac{I}{P(a+1)}$$
$$P(a+2)$$
$$P(a+3)$$
$$\vdots$$

$\mathsf{a} : [1\,..\,10]$

$\mathsf{P}(x) \;|_{\mathsf{a}+1}\; \mathsf{a} < x$ $\quad$ $\neg\mathsf{P}(x) \;|_{\mathsf{a}+1}\; \mathsf{a} < x$

Repair interpretation

Context unifier $\quad \mathsf{a} < x \wedge \mathsf{a} + 2 < x$

Inference Rule - Split

$\boxed{\neg P(x) \leftarrow a + 2 < x}$

$$\begin{array}{c} \neg P(a+3) \\ \neg P(a+4) \\ \neg P(a+5) \\ \vdots \end{array}$$

$$\begin{array}{c} I \\ \hline P(a+1) \\ P(a+2) \\ P(a+3) \\ \vdots \end{array}$$

$\mathsf{a} : [1\,..\,10]$

$\mathsf{P}(x) \mid_{\mathsf{a}+1} \mathsf{a} < x$ $\qquad$ $\neg\mathsf{P}(x) \mid_{\mathsf{a}+1} \mathsf{a} < x$

Repair interpretation

Context unifier $\quad \mathsf{a} < x \wedge \mathsf{a} + 2 < x$

Equivalently $\quad \mathsf{a} + 2 < x$

Inference Rule - Split

$$\boxed{\neg P(x) \leftarrow a + 2 < x}$$

$$\begin{array}{c} \neg P(a+3) \\ \neg P(a+4) \\ \neg P(a+5) \\ \vdots \end{array} \qquad \begin{array}{c} I \\ \hline P(a+1) \\ P(a+2) \\ P(a+3) \\ \vdots \end{array}$$

$\mathsf{a} : [1\,..\,10]$

$\mathsf{P}(x) \mid_{\mathsf{a}+1} \mathsf{a} < x$ $\qquad \neg\mathsf{P}(x) \mid_{\mathsf{a}+1} \mathsf{a} < x$

Repair interpretation

Context unifier $\quad \mathsf{a} < x \wedge \mathsf{a} + 2 < x$

Equivalently $\quad \mathsf{a} + 2 < x$

Split candidate $\quad \neg P(x) \mid_{\mathsf{a}+3} \mathsf{a} + 2 < x$

Inference Rule - Split

$$\boxed{\neg P(x) \leftarrow a + 2 < x}$$

$$\neg P(a+3)$$
$$\neg P(a+4)$$
$$\neg P(a+5)$$
$$\vdots$$

$$\frac{I}{P(a+1)}$$
$$P(a+2)$$
$$P(a+3)$$
$$\vdots$$

$$\mathsf{a} : [1 \mathinner{..} 10]$$

$$\mathsf{P}(x) \;|_{\mathsf{a}+1}\; \mathsf{a} < x \qquad \neg\mathsf{P}(x) \;|_{\mathsf{a}+1}\; \mathsf{a} < x$$

Repair interpretation

Context unifier $\mathsf{a} < x \wedge \mathsf{a} + 2 < x$

Equivalently $\mathsf{a} + 2 < x$

Split candidate $\neg P(x) \;|_{\mathsf{a}+3}\; \mathsf{a} + 2 < x$

No junk: $\mathsf{a} : [1 \mathinner{..} 10] \models \exists x\, \mathsf{a} + 2 < x$

Inference Rule - Split

$$\boxed{\neg P(x) \leftarrow a + 2 < x}$$

$$\begin{array}{c} \neg P(a+3) \\ \neg P(a+4) \\ \neg P(a+5) \\ \vdots \end{array} \qquad \begin{array}{c} I \\ \hline P(a+1) \\ P(a+2) \\ P(a+3) \\ \vdots \end{array}$$

$\mathsf{a} : [1 \,..\, 10]$

$\mathsf{P}(x) \mid_{\mathsf{a}+1} \mathsf{a} < x \qquad \neg\mathsf{P}(x) \mid_{\mathsf{a}+1} \mathsf{a} < x$

Repair interpretation

Context unifier $\mathsf{a} < x \wedge \mathsf{a} + 2 < x$

Equivalently $\mathsf{a} + 2 < x$

Split candidate $\neg P(x) \mid_{\mathsf{a}+3} \mathsf{a} + 2 < x$

No junk: $\mathsf{a} : [1 \,..\, 10] \models \exists x \; \mathsf{a} + 2 < x$

No confusion: $\mathsf{a} : [1 \,..\, 10] \models \mathsf{a} + 3 \neq \mathsf{a} + 1$

Inference Rule - Split

$$\boxed{\neg P(x) \leftarrow a + 2 < x}$$

$$\begin{array}{c} \neg P(a+3) \\ \neg P(a+4) \\ \neg P(a+5) \\ \vdots \end{array}$$

$$\begin{array}{c} I \\ \hline P(a+1) \\ P(a+2) \\ P(a+3) \\ \vdots \end{array}$$

$$\mathsf{a} : [1 \mathinner{..} 10]$$

$$\mathsf{P}(x) \mid_{\mathsf{a}+1} \mathsf{a} < x \qquad \neg\mathsf{P}(x) \mid_{\mathsf{a}+1} \mathsf{a} < x$$

Repair interpretation

Context unifier $\mathsf{a} < x \land \mathsf{a} + 2 < x$

Equivalently $\mathsf{a} + 2 < x$

Split candidate $\neg P(x) \mid_{\mathsf{a}+3} \mathsf{a} + 2 < x$

No junk: $\mathsf{a} : [1 \mathinner{..} 10] \models \exists x\ \mathsf{a} + 2 < x$

No confusion: $\mathsf{a} : [1 \mathinner{..} 10] \models \mathsf{a} + 3 \neq \mathsf{a} + 1$

$\Rightarrow$ Split is applicable

Inference Rule - Split

$$\boxed{\neg P(x) \leftarrow a + 2 < x}$$

$$\neg P(a+3) \quad \neg P(a+4) \quad \neg P(a+5) \quad \vdots$$

$$\frac{I}{P(a+1) \quad P(a+2) \quad P(a+3) \quad \vdots}$$

$\mathsf{a} : [1\,..\,10]$

$\mathsf{P}(x) \mid_{\mathsf{a}+1} \mathsf{a} < x$ $\qquad$ $\neg\mathsf{P}(x) \mid_{\mathsf{a}+1} \mathsf{a} < x$

$\neg\mathsf{P}(x) \mid_{\mathsf{a}+3} \mathsf{a} + 2 < x$ $\qquad$ $\mathsf{P}(x) \mid_{\mathsf{a}+3} \mathsf{a} + 2 < x$

Repair interpretation

Context unifier $\mathsf{a} < x \wedge \mathsf{a} + 2 < x$

Equivalently $\mathsf{a} + 2 < x$

Split candidate $\neg P(x) \mid_{\mathsf{a}+3} \mathsf{a} + 2 < x$

No junk: $\mathsf{a} : [1\,..\,10] \models \exists x\ \mathsf{a} + 2 < x$

No confusion: $\mathsf{a} : [1\,..\,10] \models \mathsf{a} + 3 \neq \mathsf{a} + 1$

$\Rightarrow$ Split is applicable

Inference Rule - Split

$$\boxed{\neg P(x) \leftarrow a + 2 < x}$$

$$\neg P(a+3)$$
$$\neg P(a+4)$$
$$\neg P(a+5)$$
$$\vdots$$

$$\frac{I}{P(a+1)}$$
$$P(a+2)$$
$$P(a+3)$$
$$\vdots$$

$\mathsf{a} : [1 \,..\, 10]$

$\mathsf{P}(x) \mid_{\mathsf{a}+1} \mathsf{a} < x$ $\quad$ $\neg\mathsf{P}(x) \mid_{\mathsf{a}+1} \mathsf{a} < x$

$\neg\mathsf{P}(x) \mid_{\mathsf{a}+3} \mathsf{a} + 2 < x$ $\quad$ $\mathsf{P}(x) \mid_{\mathsf{a}+3} \mathsf{a} + 2 < x$

$$\frac{I}{P(a+1)}$$
$$P(a+2)$$
$$\neg P(a+3)$$
$$\neg P(a+4)$$
$$\vdots$$

Repair interpretation

Context unifier $\mathsf{a} < x \wedge \mathsf{a} + 2 < x$

Equivalently $\mathsf{a} + 2 < x$

Split candidate $\neg P(x) \mid_{\mathsf{a}+3} \mathsf{a} + 2 < x$

No junk: $\mathsf{a} : [1 \,..\, 10] \models \exists x \; \mathsf{a} + 2 < x$

No confusion: $\mathsf{a} : [1 \,..\, 10] \models \mathsf{a} + 3 \neq \mathsf{a} + 1$

$\Rightarrow$ Split is applicable

Inference Rule - Close

Inference Rule - Close

$$\mathsf{a} : [1 \mathinner{..} 10]$$

$$\mathsf{P}(x) \mid_{\mathsf{a}+1} \mathsf{a} < x \qquad \neg\mathsf{P}(x) \mid_{\mathsf{a}+1} \mathsf{a} < x$$

Inference Rule - Close

$$\frac{I}{\begin{array}{c} P(a+1) \\ P(a+2) \\ P(a+3) \\ \vdots \end{array}}$$

$$\mathsf{a} : [1 \mathinner{..} 10]$$

$$\mathsf{P}(x) \mid_{\mathsf{a}+1} \mathsf{a} < x \qquad \neg\mathsf{P}(x) \mid_{\mathsf{a}+1} \mathsf{a} < x$$

Inference Rule - Close

$$\boxed{\neg P(x) \leftarrow x = a + 1}$$

$$\neg P(a+1)$$

$$\frac{I}{\begin{array}{c} P(a+1) \\ P(a+2) \\ P(a+3) \\ \vdots \end{array}}$$

$$\mathsf{a} : [1 \mathinner{..} 10]$$

$$\mathsf{P}(x) \mid_{\mathsf{a}+1} \mathsf{a} < x \qquad \neg\mathsf{P}(x) \mid_{\mathsf{a}+1} \mathsf{a} < x$$

Inference Rule - Close

$$\boxed{\neg P(x) \leftarrow x = a + 1}$$

$$\neg P(a+1)$$

$$\frac{I}{\begin{array}{c} P(a+1) \\ P(a+2) \\ P(a+3) \\ \vdots \end{array}}$$

$\mathsf{a} : [1 \mathinner{..} 10]$

$\mathsf{P}(x) \mid_{\mathsf{a}+1} \mathsf{a} < x$ $\qquad$ $\neg\mathsf{P}(x) \mid_{\mathsf{a}+1} \mathsf{a} < x$

To close use least solution:

$\mathsf{a} : [1 \mathinner{..} 10]$

$\mathsf{P}(\mathsf{a}+1)$ $\qquad$ $\neg\mathsf{P}(\mathsf{a}+1)$

Inference Rule - Close

$$\boxed{\neg P(x) \leftarrow x = a + 1}$$

$$\neg P(a+1)$$

$$\frac{I}{\begin{array}{c} P(a+1) \\ P(a+2) \\ P(a+3) \\ \vdots \end{array}}$$

$\mathsf{a} : [1\,..\,10]$

$\mathsf{P}(x) \mid_{\mathsf{a}+1} \mathsf{a} < x$ $\qquad$ $\neg\mathsf{P}(x) \mid_{\mathsf{a}+1} \mathsf{a} < x$

Abandon interpretation

To close use least solution:

$\mathsf{a} : [1\,..\,10]$

$\mathsf{P}(\mathsf{a}+1)$ $\qquad$ $\neg\mathsf{P}(\mathsf{a}+1)$

Inference Rule - Close

$$\boxed{\neg P(x) \leftarrow x = a + 1}$$

$$\neg P(a+1)$$

$$\frac{I}{\begin{array}{c} P(a+1) \\ P(a+2) \\ P(a+3) \\ \vdots \end{array}}$$

$\mathsf{a} : [1\,..\,10]$

$\mathsf{P}(x) \mid_{\mathsf{a}+1} \mathsf{a} < x$ $\quad$ $\neg\mathsf{P}(x) \mid_{\mathsf{a}+1} \mathsf{a} < x$

Abandon interpretation

Context unifier $\quad \mathsf{a} < x \wedge x = \mathsf{a} + 1$

To close use least solution:

$\mathsf{a} : [1\,..\,10]$

$\mathsf{P}(\mathsf{a}+1)$ $\quad$ $\neg\mathsf{P}(\mathsf{a}+1)$

Inference Rule - Close

$$\boxed{\neg P(x) \leftarrow x = a + 1}$$

$$\neg P(a+1)$$

$$\frac{I}{\begin{array}{c} P(a+1) \\ P(a+2) \\ P(a+3) \\ \vdots \end{array}}$$

$\mathsf{a} : [1 \mathinner{..} 10]$

$\mathsf{P}(x) \mid_{\mathsf{a}+1} \mathsf{a} < x$ $\qquad$ $\neg\mathsf{P}(x) \mid_{\mathsf{a}+1} \mathsf{a} < x$

Abandon interpretation

Context unifier $\quad \mathsf{a} < x \land x = \mathsf{a} + 1$

Equivalently $\quad x = \mathsf{a} + 1$

To close use least solution:

$\mathsf{a} : [1 \mathinner{..} 10]$

$\mathsf{P}(\mathsf{a}+1)$ $\qquad$ $\neg\mathsf{P}(\mathsf{a}+1)$

Inference Rule - Close

$$\boxed{\neg P(x) \leftarrow x = a + 1}$$

$$\neg P(a+1)$$

$$\frac{I}{\begin{array}{c} P(a+1) \\ P(a+2) \\ P(a+3) \\ \vdots \end{array}}$$

$\mathsf{a} : [1 \mathinner{..} 10]$

$\mathsf{P}(x) \mid_{\mathsf{a}+1} \mathsf{a} < x$ $\qquad$ $\neg\mathsf{P}(x) \mid_{\mathsf{a}+1} \mathsf{a} < x$

Abandon interpretation

Context unifier $\mathsf{a} < x \wedge x = \mathsf{a} + 1$

Equivalently $x = \mathsf{a} + 1$

Split candidate $\neg P(x) \mid_{\mathsf{a}+1} x = \mathsf{a} + 1$

To close use least solution:

$\mathsf{a} : [1 \mathinner{..} 10]$

$\mathsf{P}(\mathsf{a}+1)$ $\qquad$ $\neg\mathsf{P}(\mathsf{a}+1)$

Inference Rule - Close

$$\boxed{\neg P(x) \leftarrow x = a + 1}$$

$$\neg P(a+1)$$

$$\frac{I}{\begin{array}{c} P(a+1) \\ P(a+2) \\ P(a+3) \\ \vdots \end{array}}$$

$\mathsf{a} : [1\,..\,10]$

$\mathsf{P}(x) \mid_{\mathsf{a}+1} \mathsf{a} < x$ $\qquad$ $\neg\mathsf{P}(x) \mid_{\mathsf{a}+1} \mathsf{a} < x$

Abandon interpretation

Context unifier $\quad \mathsf{a} < x \wedge x = \mathsf{a} + 1$

Equivalently $\quad x = \mathsf{a} + 1$

Split candidate $\quad \neg P(x) \mid_{\mathsf{a}+1} x = \mathsf{a} + 1$

No junk: $\quad \mathsf{a} : [1\,..\,10] \models \exists x\; x = \mathsf{a} + 1$

To close use least solution:

$\mathsf{a} : [1\,..\,10]$

$\mathsf{P}(\mathsf{a}+1)$ $\qquad$ $\neg\mathsf{P}(\mathsf{a}+1)$

Inference Rule - Close

$$\boxed{\neg P(x) \leftarrow x = a + 1}$$

$$\neg P(a+1)$$

$$\frac{I}{\begin{array}{c} P(a+1) \\ P(a+2) \\ P(a+3) \\ \vdots \end{array}}$$

$\mathsf{a} : [1\,..\,10]$

$\mathsf{P}(x) \mid_{\mathsf{a}+1} \mathsf{a} < x$ $\qquad$ $\neg\mathsf{P}(x) \mid_{\mathsf{a}+1} \mathsf{a} < x$

Abandon interpretation

Context unifier $\mathsf{a} < x \wedge x = \mathsf{a} + 1$

Equivalently $x = \mathsf{a} + 1$

Split candidate $\neg P(x) \mid_{\mathsf{a}+1} x = \mathsf{a} + 1$

No junk: $\mathsf{a} : [1\,..\,10] \models \exists x\ x = \mathsf{a} + 1$

confusion: $\mathsf{a} : [1\,..\,10] \not\models \mathsf{a} + 1 \neq \mathsf{a} + 1$

To close use least solution:

$\mathsf{a} : [1\,..\,10]$

$\mathsf{P}(\mathsf{a}+1)$ $\qquad$ $\neg\mathsf{P}(\mathsf{a}+1)$

Inference Rule - Close

$$\boxed{\neg P(x) \leftarrow x = a + 1}$$

$$\neg P(a+1)$$

$$\frac{I}{\begin{array}{c} P(a+1) \\ P(a+2) \\ P(a+3) \\ \vdots \end{array}}$$

$\mathsf{a} : [1\,..\,10]$

$\mathsf{P}(x) \mid_{\mathsf{a}+1} \mathsf{a} < x$ $\quad$ $\neg\mathsf{P}(x) \mid_{\mathsf{a}+1} \mathsf{a} < x$

Abandon interpretation

Context unifier $\quad \mathsf{a} < x \wedge x = \mathsf{a} + 1$

Equivalently $\quad x = \mathsf{a} + 1$

Split candidate $\quad \neg P(x) \mid_{\mathsf{a}+1} x = \mathsf{a} + 1$

No junk: $\quad \mathsf{a} : [1\,..\,10] \models \exists x\; x = \mathsf{a} + 1$

confusion: $\quad \mathsf{a} : [1\,..\,10] \not\models \mathsf{a} + 1 \neq \mathsf{a} + 1$

Even more $\quad \mathsf{a} : [1\,..\,10] \models \mathsf{a} + 1 = \mathsf{a} + 1$

To close use least solution:

$\mathsf{a} : [1\,..\,10]$

$\mathsf{P}(\mathsf{a}+1)$ $\quad$ $\neg\mathsf{P}(\mathsf{a}+1)$

Inference Rule - Close

$$\boxed{\neg P(x) \leftarrow x = a + 1}$$

$$\neg P(a+1)$$

$$\frac{I}{\begin{array}{c} P(a+1) \\ P(a+2) \\ P(a+3) \\ \vdots \end{array}}$$

$\mathsf{a} : [1\,..\,10]$

$\mathsf{P}(x) \;|_{\mathsf{a}+1}\; \mathsf{a} < x$ $\qquad$ $\neg\mathsf{P}(x) \;|_{\mathsf{a}+1}\; \mathsf{a} < x$

Abandon interpretation

Context unifier $\quad \mathsf{a} < x \wedge x = \mathsf{a} + 1$

Equivalently $\quad x = \mathsf{a} + 1$

Split candidate $\quad \neg P(x) \;|_{\mathsf{a}+1}\; x = \mathsf{a} + 1$

No junk: $\quad \mathsf{a} : [1\,..\,10] \models \exists x\; x = \mathsf{a} + 1$

confusion: $\quad \mathsf{a} : [1\,..\,10] \not\models \mathsf{a} + 1 \neq \mathsf{a} + 1$

Even more $\quad \mathsf{a} : [1\,..\,10] \models \mathsf{a} + 1 = \mathsf{a} + 1$ $\quad \Rightarrow$ Close is applicable

To close use least solution:

$\mathsf{a} : [1\,..\,10]$

$\mathsf{P}(\mathsf{a} + 1)$ $\qquad$ $\neg\mathsf{P}(\mathsf{a} + 1)$

Inference Rule - Close

$\boxed{\neg P(x) \leftarrow x = a + 1}$

$\neg P(a+1)$

$$\frac{I}{\begin{array}{c} P(a+1) \\ P(a+2) \\ P(a+3) \\ \vdots \end{array}}$$

$\mathsf{a} : [1\,..\,10]$

$\mathsf{P}(x) \mid_{\mathsf{a}+1} \mathsf{a} < x$ $\qquad$ $\neg\mathsf{P}(x) \mid_{\mathsf{a}+1} \mathsf{a} < x$

Abandon interpretation

Context unifier $\mathsf{a} < x \wedge x = \mathsf{a} + 1$

Equivalently $x = \mathsf{a} + 1$

Split candidate $\neg P(x) \mid_{\mathsf{a}+1} x = \mathsf{a} + 1$

No junk: $\mathsf{a} : [1\,..\,10] \models \exists x\; x = \mathsf{a} + 1$

confusion: $\mathsf{a} : [1\,..\,10] \not\models \mathsf{a} + 1 \neq \mathsf{a} + 1$

Even more $\mathsf{a} : [1\,..\,10] \models \mathsf{a} + 1 = \mathsf{a} + 1$ $\Rightarrow$ Close is applicable

To close use least solution:

$\mathsf{a} : [1\,..\,10]$

$\mathsf{P}(\mathsf{a}+1)$ $\qquad$ $\neg\mathsf{P}(\mathsf{a}+1)$

*

Inference Rule - Close

$$\boxed{\neg P(x) \leftarrow x = a + 1}$$

$$\neg P(a+1)$$

$$\frac{I}{\begin{array}{c} P(a+1) \\ P(a+2) \\ P(a+3) \\ \vdots \end{array}}$$

a : $[1 \mathinner{..} 10]$

P(x) $|_{\mathsf{a}+1}$ a $< x$ $\neg$P(x) $|_{\mathsf{a}+1}$ a $< x$

*

Abandon interpretation

Context unifier   a $< x \wedge x =$ a $+ 1$

Equivalently $x =$ a $+ 1$

Split candidate $\neg P(x)$ $|_{\mathsf{a}+1}$ $x =$ a $+ 1$

No junk: a : $[1 \mathinner{..} 10] \models \exists x\ x =$ a $+ 1$

confusion: a : $[1 \mathinner{..} 10] \not\models$ a $+ 1 \neq$ a $+ 1$

Even more   a : $[1 \mathinner{..} 10] \models$ a $+ 1 =$ a $+ 1$ $\Rightarrow$ Close is applicable

To close use least solution:

a : $[1 \mathinner{..} 10]$

P(a $+ 1$) $\neg$P(a $+ 1$)

*

Inference Rule - Parameter Split

Inference Rule - Parameter Split

$$\mathsf{a} : [1 \mathinner{..} 10]$$

$$\mathsf{P}(x) \;|_{\mathsf{a}+1}\; \mathsf{a} < x \qquad \neg\mathsf{P}(x) \;|_{\mathsf{a}+1}\; \mathsf{a} < x$$

Inference Rule - Parameter Split

$$\frac{I}{\begin{array}{c} P(a+1) \\ P(a+2) \\ P(a+3) \\ \vdots \end{array}}$$

$$\mathsf{a} : [1\,..\,10]$$

$$\mathsf{P}(x) \;|_{\mathsf{a}+1}\; \mathsf{a} < x \qquad \neg\mathsf{P}(x) \;|_{\mathsf{a}+1}\; \mathsf{a} < x$$

Inference Rule - Parameter Split

$$\boxed{\neg P(x) \leftarrow x = 6}$$

$\neg P(6)$

$$\frac{I}{\begin{array}{c} P(a+1) \\ P(a+2) \\ P(a+3) \\ \vdots \end{array}}$$

$\mathsf{a} : [1 \mathinner{..} 10]$

$\mathsf{P}(x) \mid_{\mathsf{a}+1} \mathsf{a} < x$ $\quad$ $\neg\mathsf{P}(x) \mid_{\mathsf{a}+1} \mathsf{a} < x$

Inference Rule - Parameter Split

$$\boxed{\neg P(x) \leftarrow x = 6}$$

$\neg P(6)$

$$\frac{I}{\begin{array}{c}P(a+1)\\ P(a+2)\\ P(a+3)\\ \vdots\end{array}}$$

$$\mathsf{a} : [1 \mathinner{..} 10]$$

$\mathsf{P}(x) \mid_{\mathsf{a}+1} \mathsf{a} < x$ $\qquad$ $\neg\mathsf{P}(x) \mid_{\mathsf{a}+1} \mathsf{a} < x$

Split domain of parameter

Inference Rule - Parameter Split

$$\boxed{\neg P(x) \leftarrow x = 6}$$

$\neg P(6)$

$$\frac{I}{\begin{array}{c} P(a+1) \\ P(a+2) \\ P(a+3) \\ \vdots \end{array}}$$

$\mathsf{a} : [1 \,..\, 10]$

$\mathsf{P}(x) \mid_{\mathsf{a}+1} \mathsf{a} < x$ $\qquad$ $\neg\mathsf{P}(x) \mid_{\mathsf{a}+1} \mathsf{a} < x$

Split domain of parameter

Context unifier $\quad \mathsf{a} < x \wedge x = 6$

Inference Rule - Parameter Split

$\boxed{\neg P(x) \leftarrow x = 6}$

$\neg P(6)$

$$\frac{I}{\begin{array}{c} P(a+1) \\ P(a+2) \\ P(a+3) \\ \vdots \end{array}}$$

a : $[1 \,..\, 10]$

P(x) $|_{\text{a}+1}$ a $< x$ $\qquad$ $\neg$P(x) $|_{\text{a}+1}$ a $< x$

Split domain of parameter

Context unifier $\quad$ a $< x \wedge x = 6$

Split candidate $\quad$ $\neg P(x) \mid_6$ a $< x \wedge x = 6$

Inference Rule - Parameter Split

$\boxed{\neg P(x) \leftarrow x = 6}$

$\neg P(6)$

$$\frac{I}{\begin{array}{c} P(a+1) \\ P(a+2) \\ P(a+3) \\ \vdots \end{array}}$$

$\mathsf{a} : [1 \mathinner{..} 10]$

$\mathsf{P}(x) \mid_{\mathsf{a}+1} \mathsf{a} < x \qquad \neg\mathsf{P}(x) \mid_{\mathsf{a}+1} \mathsf{a} < x$

Split domain of parameter

Context unifier $\mathsf{a} < x \wedge x = 6$

Split candidate $\neg P(x) \mid_6 \mathsf{a} < x \wedge x = 6$

junk: $\mathsf{a} : [1 \mathinner{..} 10] \not\models \exists x\, \mathsf{a} < x \wedge x = 6$

Inference Rule - Parameter Split

$$\boxed{\neg P(x) \leftarrow x = 6}$$

$$\neg P(6)$$

$$\frac{I}{\begin{array}{c}P(a+1)\\P(a+2)\\P(a+3)\\\vdots\end{array}}$$

$$\mathsf{a} : [1\,..\,10]$$

$$\mathsf{P}(x)\ |_{\mathsf{a}+1}\ \mathsf{a} < x \qquad \neg\mathsf{P}(x)\ |_{\mathsf{a}+1}\ \mathsf{a} < x$$

Split domain of parameter

Context unifier $\mathsf{a} < x \wedge x = 6$

Split candidate $\neg P(x)\ |_6\ \mathsf{a} < x \wedge x = 6$

junk: $\mathsf{a} : [1\,..\,10] \not\models \exists x\ \mathsf{a} < x \wedge x = 6$

Equivalently $\mathsf{a} : [1\,..\,10] \not\models \mathsf{a} < 6$

Inference Rule - Parameter Split

$$\boxed{\neg P(x) \leftarrow x = 6}$$

$\neg P(6)$

$$\frac{I}{\begin{array}{c} P(a+1) \\ P(a+2) \\ P(a+3) \\ \vdots \end{array}}$$

$\mathsf{a} : [1 \,..\, 10]$

$\mathsf{P}(x) \mid_{\mathsf{a}+1} \mathsf{a} < x$ $\quad$ $\neg\mathsf{P}(x) \mid_{\mathsf{a}+1} \mathsf{a} < x$

Split domain of parameter

Context unifier $\quad \mathsf{a} < x \wedge x = 6$

Split candidate $\quad \neg P(x) \mid_6 \mathsf{a} < x \wedge x = 6$

junk: $\quad \mathsf{a} : [1 \,..\, 10] \not\models \exists x\ \mathsf{a} < x \wedge x = 6$

Equivalently $\quad \mathsf{a} : [1 \,..\, 10] \not\models \mathsf{a} < 6$

And also $\quad \mathsf{a} : [1 \,..\, 10] \not\models \neg(\mathsf{a} < 6)$

Inference Rule - Parameter Split

$$\boxed{\neg P(x) \leftarrow x = 6}$$

$$\neg P(6)$$

$$\frac{I}{\begin{array}{c} P(a+1) \\ P(a+2) \\ P(a+3) \\ \vdots \end{array}}$$

$\mathsf{a} : [1\,..\,10]$

$\mathsf{P}(x) \mid_{\mathsf{a}+1} \mathsf{a} < x$ $\qquad$ $\neg\mathsf{P}(x) \mid_{\mathsf{a}+1} \mathsf{a} < x$

Split domain of parameter

Context unifier $\quad \mathsf{a} < x \land x = 6$

Split candidate $\quad \neg P(x) \mid_6 \mathsf{a} < x \land x = 6$

junk: $\quad \mathsf{a} : [1\,..\,10] \not\models \exists x\, \mathsf{a} < x \land x = 6$

Equivalently $\quad \mathsf{a} : [1\,..\,10] \not\models \mathsf{a} < 6$

And also $\quad \mathsf{a} : [1\,..\,10] \not\models \neg(\mathsf{a} < 6)$

$\Rightarrow$ Parameter Split is applicable

Inference Rule - Parameter Split

$$\boxed{\neg P(x) \leftarrow x = 6}$$

$\neg P(6)$

$$\frac{I}{\begin{array}{c} P(a+1) \\ P(a+2) \\ P(a+3) \\ \vdots \end{array}}$$

a : $[1 \mathinner{..} 10]$

P(x) $|_{\mathsf{a}+1}$ a $< x$ $\qquad$ $\neg$P(x) $|_{\mathsf{a}+1}$ a $< x$

$\neg(a < 6)$ $\qquad$ $a < 6$

Split domain of parameter

Context unifier $\quad$ a $< x \wedge x = 6$

Split candidate $\quad$ $\neg P(x)$ $|_6$ a $< x \wedge x = 6$

junk: $\quad$ a : $[1 \mathinner{..} 10] \not\models \exists x$ a $< x \wedge x = 6$

Equivalently $\quad$ a : $[1 \mathinner{..} 10] \not\models$ a < 6

And also $\quad$ a : $[1 \mathinner{..} 10] \not\models \neg($a $< 6)$

$\Rightarrow$ Parameter Split is applicable

Inference Rule - Parameter Split

$$\boxed{\neg P(x) \leftarrow x = 6}$$

$\neg P(6)$

$$\frac{I}{\begin{array}{c} P(a+1) \\ P(a+2) \\ P(a+3) \\ \vdots \end{array}}$$

$\mathsf{a} : [1 \mathinner{..} 10]$

$\mathsf{P}(x) \mid_{\mathsf{a}+1} \mathsf{a} < x$ $\quad \neg\mathsf{P}(x) \mid_{\mathsf{a}+1} \mathsf{a} < x$

$\neg(a < 6)$ $\quad a < 6$

Model

Split domain of parameter

Context unifier $\quad \mathsf{a} < x \wedge x = 6$

Split candidate $\quad \neg P(x) \mid_6 \mathsf{a} < x \wedge x = 6$

junk: $\quad \mathsf{a} : [1 \mathinner{..} 10] \not\models \exists x\, \mathsf{a} < x \wedge x = 6$

Equivalently $\quad \mathsf{a} : [1 \mathinner{..} 10] \not\models \mathsf{a} < 6$

And also $\quad \mathsf{a} : [1 \mathinner{..} 10] \not\models \neg(\mathsf{a} < 6)$

$\Rightarrow$ Parameter Split is applicable

Inference Rule - Parameter Split

$$\boxed{\neg P(x) \leftarrow x = 6}$$

$\neg P(6)$

$$\frac{I}{\begin{array}{c} P(a+1) \\ P(a+2) \\ P(a+3) \\ \vdots \end{array}}$$

$\mathsf{a} : [1 \mathinner{..} 10]$

$\mathsf{P}(x) \mid_{\mathsf{a}+1} \mathsf{a} < x$ $\quad$ $\neg\mathsf{P}(x) \mid_{\mathsf{a}+1} \mathsf{a} < x$

$\neg(a < 6)$ $\quad$ $a < 6$

Model

$\mathsf{a} + 1 = 6$ $\quad$ $\neg(\mathsf{a} + 1 = 6)$

* $\quad$ ...

Split domain of parameter

Context unifier $\quad \mathsf{a} < x \wedge x = 6$

Split candidate $\quad \neg P(x) \mid_6 \mathsf{a} < x \wedge x = 6$

junk: $\quad \mathsf{a} : [1 \mathinner{..} 10] \not\models \exists x\, \mathsf{a} < x \wedge x = 6$

Equivalently $\quad \mathsf{a} : [1 \mathinner{..} 10] \not\models \mathsf{a} < 6$

And also $\quad \mathsf{a} : [1 \mathinner{..} 10] \not\models \neg(\mathsf{a} < 6)$

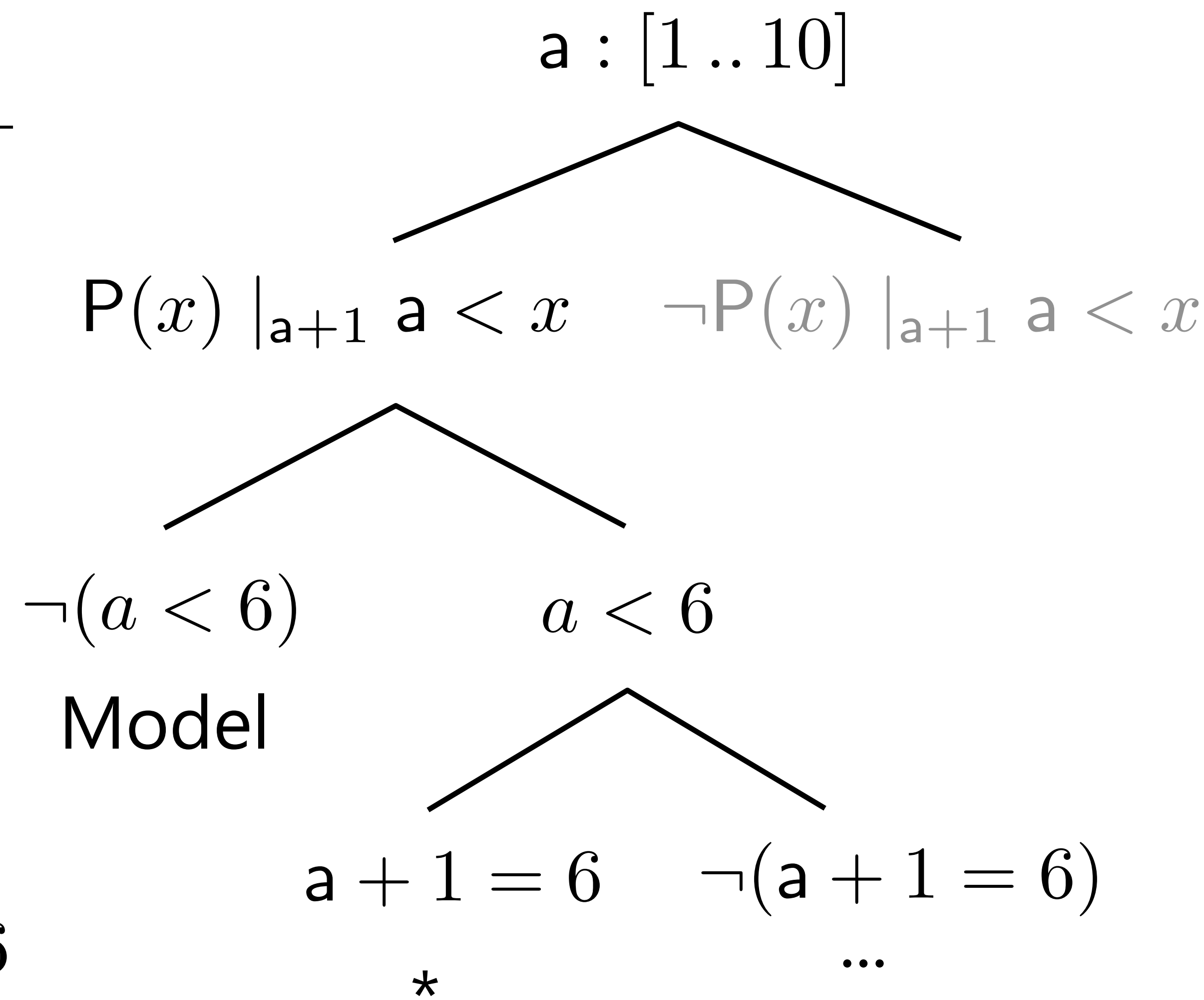
$\Rightarrow$ Parameter Split is applicable

Inference Rule - Parameter Split

$\boxed{\neg P(x) \leftarrow x = 6}$

$\neg P(6)$

$$\frac{I}{\begin{array}{c} P(a+1) \\ P(a+2) \\ P(a+3) \\ \vdots \end{array}}$$



Split domain of parameter

Context unifier a $< x \wedge x = 6$

Split candidate $\neg P(x)\ |_6$ a $< x \wedge x = 6$

junk: a : $[1\,..\,10] \not\models \exists x$ a $< x \wedge x = 6$

Equivalently a : $[1\,..\,10] \not\models$ a < 6

And also a : $[1\,..\,10] \not\models \neg($a $< 6)$

$\Rightarrow$ Parameter Split is applicable

Demand driven
Avoid disjunction

Completeness

Theorem: an exhausted open limit branch provides a model for the input clause set

Proof idea:

- Chose any α: a → $\mathbb{N}$ consistently with limit branch
- Let I be the induced interpretation
- By contradiction assume I,α ⊭ $(C \leftarrow c)$σ
  for some clause $C \leftarrow c$ and some σ: $x \rightarrow \mathbb{N}$
- Analyse candidate context unifier responsible for falsifying $(C \leftarrow c)$σ
  1. Junk situation is impossible -
     Parameter Split would have eliminated it
  2. Confusion situation is impossible -
     Close or Parameter Split would have eliminated it
  3. Close is not applicable because branch open
  4. Split was applied so that the context unifier doesn't falsify $(C \leftarrow c)$σ

Not a Decision Procedure

- ME(LIA) does not provide a decision procedure
  - There are clause sets that don't admit finite model representation with contexts

$P(0)$
$\neg P(1)$
$P(x) \leftrightarrow P(x+2)$

- Enforce termination by finite range restriction for free variables
  - Application e.g. arrays:

Unfolding into disjunctions "by demand" only

Totality axiom for select_{a1} function relationalized:

$\forall i : [1 \mathinner{..} 10]\ \exists v : [1 \mathinner{..} 20]\ \text{select\_a1}(i, v)$

becomes

$$\mathsf{v}_1 : [1 \mathinner{..} 20] \qquad \text{select\_a1}(i, v) \leftarrow i = 1 \land v = \mathsf{v}_1$$

$$\vdots$$

$$\mathsf{v}_{10} : [1 \mathinner{..} 20] \qquad \text{select\_a1}(i, v) \leftarrow i = 10 \land v = \mathsf{v}_{10}$$

Limitations

- There is no complete calculus possible if free constants have unbounded domain, I.e. for "declarations" a : [0 .. ∞]
  - Can express domain emptyness problem of 2-register machines
  - Can express multiplication

P(0)
P(x+1) ← P(x)
¬P(a)

- Ignore the problem?
  - Still sound, lose completeness in general
  - Still decision procedure for ground case (?)
    (no free variables in clauses, as in DPLL(LIA+UIF)
- Build in induction?

Conclusions

Practicality issues

- Sound and complete thanks to native quantifier treatment
- Avoids expanding finite domains into disjunctions
- Counterexample finding:
  - Use finite range for free variables
  - "Unprovable" answer then is more "informative" than "unprovability" answer in system based on instantiation heuristics

Extensions

- Universal literals
- Unit propagation and related inference rules