Logic and Mechanized Reasoning

Congruence Closure

Marijn J.H. Heule

Carnegie Mellon University

Second Midterm Exam

Second midterm on Monday, March 25, during class time.

- last name starts with A-H are in room GHC 4301
- last name starts with K-Z are in room NSH 1305

The exam will cover:

- DP and DPLL, following the slides from the 2/12 lecture
- Sections 8.2, 8.3, and 8.4 in the textbook
- Chapters 9-12 in the textbook
- Construct unifiers of terms by hand, but not the algorithm

Extra OH before the exam:

- Joseph, Friday, 12-1, in Baker Hall 139
- Alex, Sunday, 4-5 in Baker Hall 139.

Introduction

Data Structures

Example Runs

Proofs

Extensions

Ground Terms

Letters early in the alphabet refer to constants, e.g. a, b, c

- Constants can be seen as 0-arity functions

Small letters starting with f refer to functions, e.g. f, g, h

Capital letters refer to relations, e.g. P, Q, R

No variables in ground terms

- Usually letters late in the alphabet, e.g. x, y, z

Motivation

Consider the following equations and disequations:

1. $f(a,a) = b$
2. $g(c,a) = c$
3. $g(c,f(a,a)) = f(g(c,a),g(c,a))$
4. $f(c,c) \neq g(c,b)$

Are they satisfiable?

Motivation

Consider the following equations and disequations:

1. $f(a,a) = b$
2. $g(c,a) = c$
3. $g(c,f(a,a)) = f(g(c,a),g(c,a))$
4. $f(c,c) \neq g(c,b)$

Are they satisfiable?

We can derive the following

5. $g(c,f(a,a)) = g(c,b)$ from 1.

Motivation

Consider the following equations and disequations:

1. $f(a,a) = b$
2. $g(c,a) = c$
3. $g(c,f(a,a)) = f(g(c,a),g(c,a))$
4. $f(c,c) \neq g(c,b)$

Are they satisfiable?

We can derive the following

5. $g(c,f(a,a)) = g(c,b)$ from 1.
6. $f(g(c,a),g(c,a)) = f(c,c)$ from 2.

Motivation

Consider the following equations and disequations:

1. $f(a,a) = b$
2. $g(c,a) = c$
3. $g(c,f(a,a)) = f(g(c,a),g(c,a))$
4. $f(c,c) \neq g(c,b)$

Are they satisfiable?

We can derive the following

5. $g(c,f(a,a)) = g(c,b)$ from 1.
6. $f(g(c,a),g(c,a)) = f(c,c)$ from 2.
7. $f(c,c) = g(c,b)$ from 3, 5, and 6.

Examples

Reasoning about equality is important

- Interesting problems combine equations with disequations

Examples

Reasoning about equality is important

- Interesting problems combine equations with disequations

A couple of examples. Which are satisfiable?

- $f(a) = f(b) \wedge a \neq b$

Examples

Reasoning about equality is important

- Interesting problems combine equations with disequations

A couple of examples. Which are satisfiable?

- $f(a) = f(b) \wedge a \neq b$
  satisfiable
- $f(a) = a \wedge f(f(a)) \neq a$

Examples

Reasoning about equality is important

- Interesting problems combine equations with disequations

A couple of examples. Which are satisfiable?

- $f(a) = f(b) \wedge a \neq b$
  satisfiable
- $f(a) = a \wedge f(f(a)) \neq a$
  unsatisfiable
- $f(f(f(a))) = a \wedge f(f(f(f(f(a))))) = a \wedge f(a) \neq a$

Examples

Reasoning about equality is important

- Interesting problems combine equations with disequations

A couple of examples. Which are satisfiable?

- $f(a) = f(b) \wedge a \neq b$
  satisfiable
- $f(a) = a \wedge f(f(a)) \neq a$
  unsatisfiable
- $f(f(f(a))) = a \wedge f(f(f(f(f(a))))) = a \wedge f(a) \neq a$
  unsatisfiable

Decidable

Theorem

The question as to whether a finite set of ground equations and disequations is satisfiable is decidable.

The idea behind the proof is to use a saturation argument:

- Start from the equations in question
- Derive new equations until no more equations are derivable
- Unsatisfiable, if an equation contradicts a disequation
- Otherwise satisfiable

Derivation Rules

- Reflexivity

$$t = t$$

- Symmetry

$$\frac{s = t}{t = s}$$

- Transitivity of equality

$$\frac{r = s \qquad s = t}{r = t}$$

- Congruence

$$\frac{s_1 = t_1 \qquad \ldots \qquad s_n = t_n}{f(s_1, \ldots, s_n) = f(t_1, \ldots, t_n)}$$

Avoiding Infinite Loops

Consider an equational problem with $a = f(a)$

We can derive infinitely many new equations:

$$\dfrac{\dfrac{\dfrac{\dfrac{\dfrac{a = f(a)}{f(a) = f(f(a))}}{f(f(a)) = f(f(f(a)))}}{f(f(f(a))) = f(f(f(f(a))))}}{f(f(f(f(a)))) = f(f(f(f(f(a)))))}}{\cdots}$$

Avoiding Infinite Loops

Consider an equational problem with $a = f(a)$

We can derive infinitely many new equations:

$$\begin{array}{c} a = f(a) \\ \hline f(a) = f(f(a)) \\ \hline f(f(a)) = f(f(f(a))) \\ \hline f(f(f(a))) = f(f(f(f(a)))) \\ \hline f(f(f(f(a)))) = f(f(f(f(f(a))))) \\ \hline \cdots \end{array}$$

We only need to consider the terms in the original problem!

Congruence Closure

Lemma (Congruence Closure)

Let Γ consist of a set of equations and disequations. Let S be the set of subterms of all the terms occurring in Γ. Let Γ' be the set of all equations between elements of S that can be derived from the equations in Γ using the derivation rules. Then Γ is satisfiable if and only if no disequation in Γ is the negation of an equation in Γ'.

Congruence Closure Proof

UNSAT direction of the lemma is easy

- The equational rules preserve truth in any model
- Deriving a contradiction implies unsatisfiable

Congruence Closure Proof

UNSAT direction of the lemma is easy

- The equational rules preserve truth in any model
- Deriving a contradiction implies unsatisfiable

SAT direction of the lemma

- Let S denote the set of all subterms in the formula
- Algorithm terminates because finite number of terms
- Let $t \equiv s$ denote that t is equivalent to s
- For each element t we have an equivalence class

$$[t] = \{s \in S \mid s \equiv t\}$$

- After termination, construct a model as follows

$$f^{\mathfrak{M}}([t_1], \ldots, [t_n]) = \begin{cases} [f(t_1, \ldots, t_n)] & \text{if } f(t_1, \ldots, t_n) \text{ is in } S \\ \star & \text{otherwise} \end{cases}$$

High-Level Algorithm

- Given a set of equations and disequations, construct the set of all subterms.
- Merge subterms that are equal due to equations
- Keep merging based on the congruence rule

High-Level Algorithm

- Given a set of equations and disequations, construct the set of all subterms.
- Merge subterms that are equal due to equations
- Keep merging based on the congruence rule

Example

$$f(a,b) = a \ \wedge \ f(f(a,b),b) \neq a$$

- Set of all subterms $=$

High-Level Algorithm

- Given a set of equations and disequations, construct the set of all subterms.
- Merge subterms that are equal due to equations
- Keep merging based on the congruence rule

Example

$$f(a,b) = a \ \wedge \ f(f(a,b),b) \neq a$$

- Set of all subterms $= \{\{a\},\{b\},\{f(a,b)\},\{f(f(a,b),b)\}\}$
- Merge subterms $=$

High-Level Algorithm

- Given a set of equations and disequations, construct the set of all subterms.
- Merge subterms that are equal due to equations
- Keep merging based on the congruence rule

Example

$$f(a,b) = a \ \wedge \ f(f(a,b),b) \neq a$$

- Set of all subterms $= \{\{a\},\{b\},\{f(a,b)\},\{f(f(a,b),b)\}\}$
- Merge subterms $= \{\{a,f(a,b)\},\{b\},\{f(f(a,b),b)\}\}$
- Which two terms can be merge using the congruence rule?

High-Level Algorithm

- Given a set of equations and disequations, construct the set of all subterms.
- Merge subterms that are equal due to equations
- Keep merging based on the congruence rule

Example

$$f(a,b) = a \ \wedge \ f(f(a,b),b) \neq a$$

- Set of all subterms $= \{\{a\},\{b\},\{f(a,b)\},\{f(f(a,b),b)\}\}$
- Merge subterms $= \{\{a,f(a,b)\},\{b\},\{f(f(a,b),b)\}\}$
- Which two terms can be merge using the congruence rule?

$$\frac{f(a,b) = a \qquad b = b}{f(f(a,b),b) = f(a,b)}$$

High-Level Algorithm

- Given a set of equations and disequations, construct the set of all subterms.
- Merge subterms that are equal due to equations
- Keep merging based on the congruence rule

Example

$$f(a,b) = a \ \wedge \ f(f(a,b),b) \neq a$$

- Set of all subterms $= \{\{a\},\{b\},\{f(a,b)\},\{f(f(a,b),b)\}\}$
- Merge subterms $= \{\{a, f(a,b)\},\{b\},\{f(f(a,b),b)\}\}$
- Which two terms can be merge using the congruence rule?

$$\frac{f(a,b) = a \qquad b = b}{f(f(a,b),b) = f(a,b)}$$

- Unsatisfiable because a and $f(f(a,b),b)$ in the same set

Larger Example

Example

$$f^3(a) = a \ \wedge \ f^5(a) = a \ \wedge \ f(a) \neq a$$

- Initial set of congruence classes:

Larger Example

Example

$$f^3(a) = a \land f^5(a) = a \land f(a) \neq a$$

- Initial set of congruence classes:

$$\{\{a\},\{f(a)\},\{f^2(a)\},\{f^3(a)\},\{f^4(a)\},\{f^5(a)\}\}$$

- Merge classes using equalities:

Larger Example

Example

$$f^3(a) = a \ \wedge \ f^5(a) = a \ \wedge \ f(a) \neq a$$

- Initial set of congruence classes:

$$\big\{\{a\},\{f(a)\},\{f^2(a)\},\{f^3(a)\},\{f^4(a)\},\{f^5(a)\}\big\}$$

- Merge classes using equalities:

$$\big\{\{a,f^3(a),f^5(a)\},\{f(a)\},\{f^2(a)\},\{f^4(a)\}\big\}$$

- Which terms can be merged using the congruence rule?

Larger Example

Example

$$f^3(a) = a \land f^5(a) = a \land f(a) \neq a$$

- Initial set of congruence classes:

$$\{\{a\},\{f(a)\},\{f^2(a)\},\{f^3(a)\},\{f^4(a)\},\{f^5(a)\}\}$$

- Merge classes using equalities:

$$\{\{a, f^3(a), f^5(a)\},\{f(a)\},\{f^2(a)\},\{f^4(a)\}\}$$

- Which terms can be merged using the congruence rule?

$$\frac{a = f^3(a)}{f(a) = f^4(a)}$$

Larger Example

Example

$$f^3(a) = a \ \wedge \ f^5(a) = a \ \wedge \ f(a) \neq a$$

- Initial set of congruence classes:

$$\big\{\{a\},\{f(a)\},\{f^2(a)\},\{f^3(a)\},\{f^4(a)\},\{f^5(a)\}\big\}$$

- Merge classes using equalities:

$$\big\{\{a, f^3(a), f^5(a)\},\{f(a)\},\{f^2(a)\},\{f^4(a)\}\big\}$$

- Which terms can be merged using the congruence rule?

$$\frac{a = f^3(a)}{f(a) = f^4(a)} \qquad \frac{f(a) = f^4(a)}{f^2(a) = f^5(a)}$$

Larger Example

Example

$$f^3(a) = a \ \wedge \ f^5(a) = a \ \wedge \ f(a) \neq a$$

- Initial set of congruence classes:

$$\{\{a\}, \{f(a)\}, \{f^2(a)\}, \{f^3(a)\}, \{f^4(a)\}, \{f^5(a)\}\}$$

- Merge classes using equalities:

$$\{\{a, f^3(a), f^5(a)\}, \{f(a)\}, \{f^2(a)\}, \{f^4(a)\}\}$$

- Which terms can be merged using the congruence rule?

$$\frac{a = f^3(a)}{f(a) = f^4(a)} \quad \frac{f(a) = f^4(a)}{f^2(a) = f^5(a)} \quad \{\{a, f^2(a), f^3(a), f^5(a)\}, \{f(a), f^4(a)\}\}$$

- Which terms can be merged using the congruence rule?

Larger Example

Example

$$f^3(a) = a \ \wedge \ f^5(a) = a \ \wedge \ f(a) \neq a$$

- Initial set of congruence classes:

$$\big\{\{a\},\{f(a)\},\{f^2(a)\},\{f^3(a)\},\{f^4(a)\},\{f^5(a)\}\big\}$$

- Merge classes using equalities:

$$\big\{\{a,f^3(a),f^5(a)\},\{f(a)\},\{f^2(a)\},\{f^4(a)\}\big\}$$

- Which terms can be merged using the congruence rule?

$$\frac{a = f^3(a)}{f(a) = f^4(a)} \quad \frac{f(a) = f^4(a)}{f^2(a) = f^5(a)} \quad \big\{\{a,f^2(a),f^3(a),f^5(a)\},\{f(a),f^4(a)\}\big\}$$

- Which terms can be merged using the congruence rule?

$$\frac{a = f^2(a)}{f(a) = f^3(a)}$$

Larger Example

Example

$$f^3(a) = a \ \land \ f^5(a) = a \ \land \ f(a) \neq a$$

- Initial set of congruence classes:

$$\{\{a\},\{f(a)\},\{f^2(a)\},\{f^3(a)\},\{f^4(a)\},\{f^5(a)\}\}$$

- Merge classes using equalities:

$$\{\{a,f^3(a),f^5(a)\},\{f(a)\},\{f^2(a)\},\{f^4(a)\}\}$$

- Which terms can be merged using the congruence rule?

$$\frac{a = f^3(a)}{f(a) = f^4(a)} \quad \frac{f(a) = f^4(a)}{f^2(a) = f^5(a)} \quad \{\{a,f^2(a),f^3(a),f^5(a)\},\{f(a),f^4(a)\}\}$$

- Which terms can be merged using the congruence rule?

$$\frac{a = f^2(a)}{f(a) = f^3(a)} \quad \{\{a,f(a),f^2(a),f^3(a),f^4(a),f^5(a)\}\}$$

Union-Find

High-level of Union-Find:

- Each element has a (pointer to its) parent
- An element is the representative of an equivalence class if it is equal to its parent
- Find e returns the representative of element e
- Union $e\ f$, merges the equivalences classes of e and f

Union-Find

High-level of Union-Find:

- Each element has a (pointer to its) parent
- An element is the representative of an equivalence class if it is equal to its parent
- Find e returns the representative of element e
- Union $e\,f$, merges the equivalences classes of e and f

Find e

- if ($e.\texttt{parent} = e$) return e
- else return Find $e.\texttt{parent}$

Union-Find

High-level of Union-Find:

- Each element has a (pointer to its) parent
- An element is the representative of an equivalence class if it is equal to its parent
- Find e returns the representative of element e
- Union $e\,f$, merges the equivalences classes of e and f

Find e

- if ($e.\texttt{parent} = e$) return e
- else return Find $e.\texttt{parent}$

Union $e\,f$

- if (Find $e \neq$ Find f) Merge $e\,f$

Union-Find Optimizations

Path compression: Update the paths to the representative

Find e

- if ($e.\texttt{parent} \neq e$) $e.\texttt{parent} :=$ Find $e.\texttt{parent}$
- return $e.\texttt{parent}$

Two heuristics of selecting the new representative:

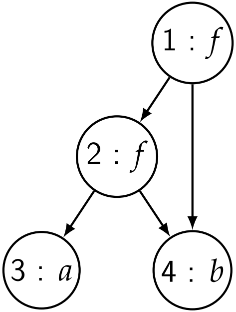
- Rank Length of the longest path
- Tree Size of the tree

Implemented in Lean: DisjointSet

Subterm Set as Directed Acyclic Graph

To compute congruence closure efficiently, we will represent the subterm set of the formula as a Directed Acyclic Graph

- Each node corresponds to a subterm and has unique id
- Edges point from function symbol to arguments
- What subterm does node labeled 1 represent?

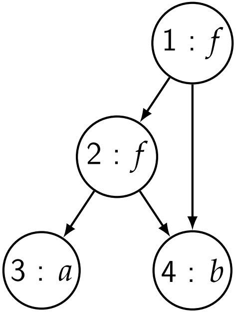


Subterm Set as Directed Acyclic Graph

To compute congruence closure efficiently, we will represent the subterm set of the formula as a Directed Acyclic Graph

- Each node corresponds to a subterm and has unique id
- Edges point from function symbol to arguments
- What subterm does node labeled 1 represent?

$$f(f(a,b),b)$$

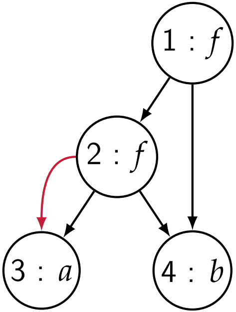


Representatives and Predecessors

Each equivalence class has a single representative / root

The set of predecessors is stored only with the representative

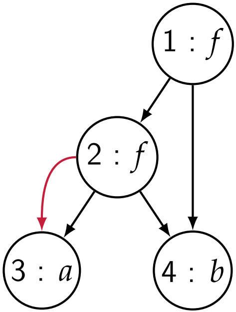
- Initially each node is its own representative
- When two equivalence classes are merged, their set of predecessors is merged as well
- In the image $f(a)$ and a are merged (denoted by red edge)
- Their set of predecessorsis $\{f(a,b), f(f(a,b),b)\}$



Small Example

Example

$$f(a,b) = a \land f(f(a,b),b) \neq a$$

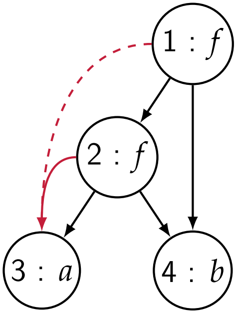


- Construct initial DAG
- Process equality $f(a,b) = a$ denoted by red edges
- Are the predecessors $f(a,b) = a$ and $f(f(a,b),b)$ congruent?

Small Example

Example

$$f(a,b) = a \wedge f(f(a,b),b) \neq a$$

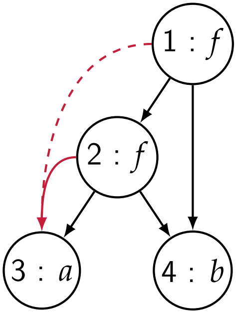


- Construct initial DAG
- Process equality $f(a,b) = a$ denoted by red edges
- Are the predecessors $f(a,b) = a$ and $f(f(a,b),b)$ congruent?
- Yes, so $a = f(f(a,b),b)$

Small Example

Example

$$f(a,b) = a \land f(f(a,b),b) \neq a$$



- Construct initial DAG
- Process equality $f(a,b) = a$ denoted by red edges
- Are the predecessors $f(a,b) = a$ and $f(f(a,b),b)$ congruent?
- Yes, so $a = f(f(a,b),b)$

Formula is unsatisfiable because a and $f(f(a,b),b)$ are in the same equivalence class

Example Unsatisfiable Run

Example

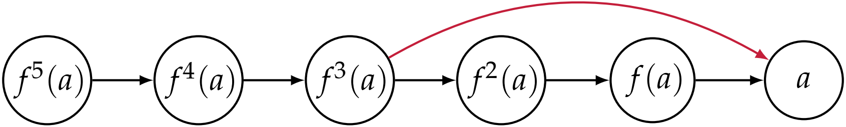
$$f^3(a) = a \;\wedge\; f^5(a) = a \;\wedge\; f(a) \neq a$$

$$f^5(a) \to f^4(a) \to f^3(a) \to f^2(a) \to f(a) \to a$$

Example Unsatisfiable Run

Example

$$f^3(a) = a \ \wedge \ f^5(a) = a \ \wedge \ f(a) \neq a$$

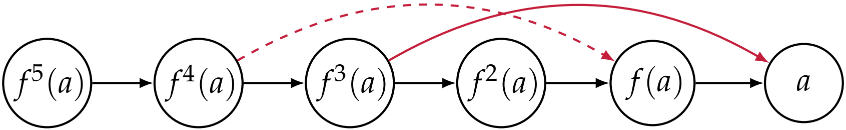


- Process $f^3(a) = (a)$

Example Unsatisfiable Run

Example

$$f^3(a) = a \ \wedge \ f^5(a) = a \ \wedge \ f(a) \neq a$$

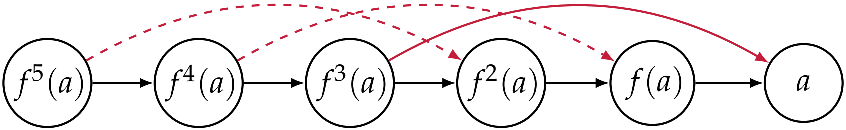


- Process $f^3(a) = (a)$

Example Unsatisfiable Run

Example

$$f^3(a) = a \ \wedge \ f^5(a) = a \ \wedge \ f(a) \neq a$$

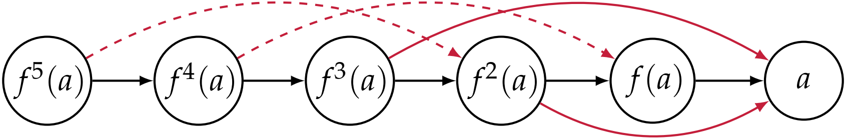


- Process $f^3(a) = (a)$

Example Unsatisfiable Run

Example

$$f^3(a) = a \ \wedge \ f^5(a) = a \ \wedge \ f(a) \neq a$$

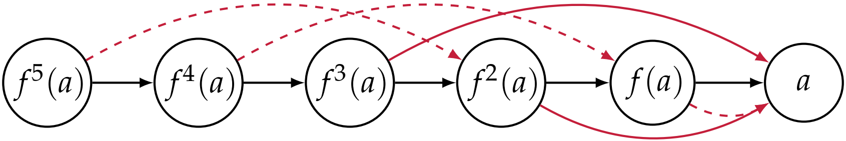


- Process $f^3(a) = (a)$
- Process $f^5(a) = (a)$

Example Unsatisfiable Run

Example

$$f^3(a) = a \ \wedge \ f^5(a) = a \ \wedge \ f(a) \neq a$$

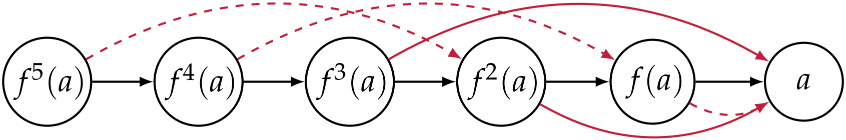


- Process $f^3(a) = (a)$
- Process $f^5(a) = (a)$

Example Unsatisfiable Run

Example

$$f^3(a) = a \ \wedge \ f^5(a) = a \ \wedge \ f(a) \neq a$$



- Process $f^3(a) = (a)$
- Process $f^5(a) = (a)$
- Unsatisfiable

Example Satisfiable Run

Example

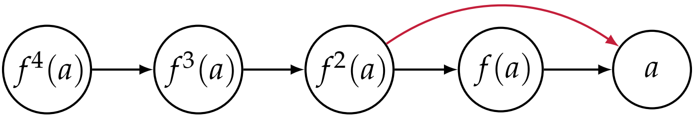
$$f^2(a) = a \ \wedge \ f^4(a) = a \ \wedge \ f(a) \neq a \ \wedge \ f(a) \neq b$$

$$f^4(a) \longrightarrow f^3(a) \longrightarrow f^2(a) \longrightarrow f(a) \longrightarrow a$$

Example Satisfiable Run

Example

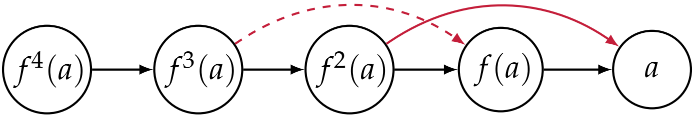
$$f^2(a) = a \ \wedge \ f^4(a) = a \ \wedge \ f(a) \neq a \ \wedge \ f(a) \neq b$$



Example Satisfiable Run

Example

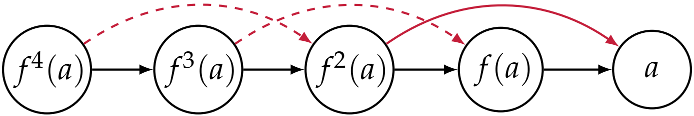
$$f^2(a) = a \;\wedge\; f^4(a) = a \;\wedge\; f(a) \neq a \;\wedge\; f(a) \neq b$$



Example Satisfiable Run

Example

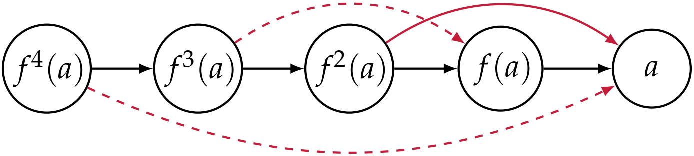
$$f^2(a) = a \ \wedge\ f^4(a) = a \ \wedge\ f(a) \neq a \ \wedge\ f(a) \neq b$$



Example Satisfiable Run

Example

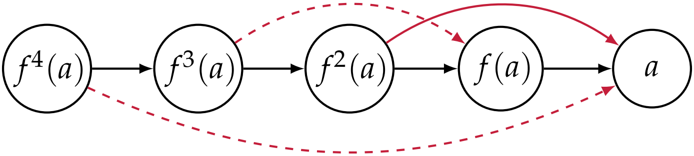
$$f^2(a) = a \ \wedge \ f^4(a) = a \ \wedge \ f(a) \neq a \ \wedge \ f(a) \neq b$$



Example Satisfiable Run

Example

$$f^2(a) = a \ \wedge \ f^4(a) = a \ \wedge \ f(a) \neq a \ \wedge \ f(a) \neq b$$



Equivalence classes:

- $[a] = \{a, f^2(a), f^4(a)\}$
- $[f(a)] = \{f(a), f^3(a)\}$
- $[b] = \{b\}$
- No contradiction, thus satisfiable

Small Refutation Proof

Example

$$f(a,b) = a \land f(f(a,b),b) \neq a$$

$$\cfrac{\cfrac{\cfrac{f(a,b) = a \qquad b = b}{}}{}}{\bot}$$

Small Refutation Proof

Example

$$f(a,b) = a \;\wedge\; f(f(a,b),b) \neq a$$

$$\dfrac{\dfrac{\dfrac{f(a,b) = a \qquad b = b}{f(f(a,b),b) = f(a,b)}}{\qquad}\qquad}{\bot}$$

Small Refutation Proof

Example

$$f(a,b) = a \ \wedge\ f(f(a,b),b) \neq a$$

$$\dfrac{\dfrac{f(a,b) = a \qquad b = b}{f(f(a,b),b) = f(a,b)} \qquad f(a,b) = a}{\qquad}$$

$$\dfrac{\qquad\qquad}{\bot}$$

Small Refutation Proof

Example

$$f(a,b) = a \ \wedge \ f(f(a,b),b) \neq a$$

$$\dfrac{\dfrac{\dfrac{f(a,b) = a \qquad b = b}{f(f(a,b),b) = f(a,b)} \qquad f(a,b) = a}{f(f(a,b),b) = a} \qquad f(f(a,b),b) \neq a}{\bot}$$

Small Refutation Proof

Example

$$f(a,b) = a \ \wedge \ f(f(a,b),b) \neq a$$

$$\cfrac{\cfrac{\cfrac{f(a,b) = a \qquad b = b}{f(f(a,b),b) = f(a,b)} \qquad f(a,b) = a}{f(f(a,b),b) = a} \qquad f(f(a,b),b) \neq a}{\bot}$$

Larger Refutation Proof

Example

$$f^3(a) = a \;\wedge\; f^5(a) = a \;\wedge\; f(a) \neq a$$

$$\dfrac{\dfrac{\dfrac{\dfrac{\dfrac{\dfrac{\dfrac{\dfrac{\dfrac{f^3(a) = a}{f^4(a) = f(a)}}{f^5(a) = f^2(a)}}{f^2(a) = f^5(a)} \qquad f^5(a) = a}{f^2(a) = a}}{f^3(a) = f(a)}}{f(a) = f^3(a)} \qquad f^3(a) = a}{f(a) = a} \qquad f(a) \neq a}{\bot}$$

Model for Satisfiable Run

Example

$$f^2(a) = a \ \wedge \ f^4(a) = a \ \wedge \ f(a) \neq a \ \wedge \ f(a) \neq b$$

Congruence classes:

- $[a] = \{a, f^2(a), f^4(a)\}$
- $[f(a)] = \{f(a), f^3(a)\}$
- $[b] = \{b\}$

Model:

- $f^{\mathfrak{M}}([a]) = [f(a)]$
- $f^{\mathfrak{M}}([f(a)]) = [a]$
- $f^{\mathfrak{M}}([b]) = \star$
- $f^{\mathfrak{M}}(\star) = \star$

Model for Satisfiable Run

Example

$$f^2(a) = a \ \wedge \ f^4(a) = a \ \wedge \ f(a) \neq a \ \wedge \ f(a) \neq b$$

Congruence classes:

- $[a] = \{a, f^2(a), f^4(a)\}$
- $[f(a)] = \{f(a), f^3(a)\}$
- $[b] = \{b\}$

Model:

- $f^{\mathfrak{M}}([a]) = [f(a)]$
- $f^{\mathfrak{M}}([f(a)]) = [a]$
- $f^{\mathfrak{M}}([b]) = \star$
- $f^{\mathfrak{M}}(\star) = \star$

Introduction

Data Structures

Example Runs

Proofs

Extensions

Equality Reasoning with Relations

So far we only considered formulas with functions

We can include relations using the following rule

$$\frac{s_1 = t_1 \qquad \ldots \qquad s_n = t_n \qquad R(s_1, \ldots, s_n)}{R(t_1, \ldots, t_n)}$$

If the algorithm terminates without contradiction

- $R^{\mathfrak{M}}([t_1], \ldots, [t_n])$ holds iff $R(t_1, \ldots, t_n)$ is a consequence

Validity of Universally Quantified Formulas

Throughout the lecture we didn't use variables

The same techniques can be used to checked the validity of

- $\forall x_1, \ldots x_n.\ P[x_1, \ldots, x_n]$
- where $P[x_1, \ldots, x_n]$ doesn't include any relations besides $=$

The method works as follows

- Replace variables $x_1, \ldots, x_n$ by constants $c_1, \ldots, c_n$
- Turn $\neg P[c_1, \ldots, c_n]$ into a DNF formula $D[c_1, \ldots, c_n]$
- Each D_i is a disjunction of equations and disequations
- $\forall x_1, \ldots x_n.\ P[x_1, \ldots, x_n]$ is valid if D is unsatisfiable

Validity of Universally Quantified Formulas Example

Example

$$\forall x_1, x_2.\ x_1 \neq x_2 \vee f(x_1) = f(x_2)$$

Replace the variables with constants and negate the formula

$$c_1 = c_2 \wedge f(c_1) \neq f(c_2)$$

Is this formula satisfiable?

Validity of Universally Quantified Formulas Example

Example

$$\forall x_1, x_2.\ x_1 \neq x_2 \vee f(x_1) = f(x_2)$$

Replace the variables with constants and negate the formula

$$c_1 = c_2 \wedge f(c_1) \neq f(c_2)$$

Is this formula satisfiable? No, thus for original one is valid