CS389L: Automated Logical Reasoning

Lecture 16: Decision Procedures for Combination Theories

Işıl Dillig

Motivation

- So far, learned about decision procedures for useful theories
- Examples: Theory of equality with uninterpreted functions, theory of rationals, theory of integers
- But in many cases, we need to decide satisfiability of formulas involving multiple theories
- Example: $1 \leq x \wedge x \leq 2 \wedge f(x) \neq f(1) \wedge f(x) \neq f(2)$
- This formula does not belong to any individual theory
- But it does belong, for instance, to combination of $T_=$ and $T_{\mathbb{Z}}$

Overview

- Recall: Given two theories T_1 and T_2 that have the $=$ predicate, we define a combined theory $T_1 \cup T_2$
- Signature of $T_1 \cup T_2$: $\Sigma_1 \cup \Sigma_2$
- Axioms of $T_1 \cup T_2$: $A_1 \cup A_2$
- Given decision procedures for quantifier-free T_1 and T_2, we want a decision procedure to decide satisfiability of formulas in qff $T_1 \cup T_2$

Nelson-Oppen Overview

Σ_1-theory T_1
$\boxed{P_1}$ for T_1-satisfiability

Σ_2-theory T_2
$\boxed{P_2}$ for T_2-satisfiability

Nelson-Oppen

$\boxed{P}$ for $(T_1 \cup T_2)$-satisfiability

- Also allows combining arbitrary number of theories
- For instance, to combine T_1, T_2, T_3, first combine T_1, T_2
- Then, combine $T_1 \cup T_2$ and T_3 again using Nelson-Oppen

Restrictions of Nelson-Oppen

- Nelson-Oppen method imposes the following restrictions:
  1. Only allows combining quantifier-free fragments
  2. Only allows combining formulas without disjunctions, but not a major limitation because can convert to DNF
  3. Signatures can only share equality: $\Sigma_1 \cap \Sigma_2 = \{=\}$
  4. Theories T_1 and T_2 must be stably infinite
- Theory T is stably infinite iff every satisfiable qff formula is satisfiable in a universe of discourse with infinite cardinality

Example of Non-Stably Infinite Theory

$$\begin{array}{ll} \text{Signature}: & \{a, b, =\} \\ \text{Axiom}: & \forall x.\ x = a \vee x = b \end{array}$$

- Axiom says that any object in the universe of discourse must be equal to either a or b
- Now consider U containing more than 2 distinct elements
- Then, there is at least one element that is not equal to a or b
- Thus, any U with more than 2 elements violates axiom
- Hence, theory only has finite models, and is not stably infinite

Examples of Stably Infinite Theories

- Fortunately, almost any theory of interest is stably infinite
- All theories we discussed, $T_=$, $T_\mathbb{Q}$, $T_\mathbb{Z}$, T_A, are stably infinite
- Which of these theories can we combine using Nelson-Oppen?
  1. $T_=$ and $T_\mathbb{Q}$?
  2. $T_=$ and $T_\mathbb{Z}$?
  3. T_A and $T_\mathbb{Z}$?
  4. $T_\mathbb{Q}$ and $T_\mathbb{Z}$?

Nelson-Oppen Overview

- Nelson-Oppen method has conceptually two-different phases:
  1. Purification: Seperate formula F in $T_1 \cup T_2$ into two formulas F_1 in T_1 and F_2 in T_2
  2. Equality propagation: Propagate all relevant equalities between theories
- Purification step is always the same for any arbitrary theory
- But equality propagation is different between convex and non-convex theories

Purification Overview

- Given formula F in $T_1 \cup T_2$, goal of purification is to separate F into formulas F_1 and F_2 such that:
  1. F_1 belongs only to T_1 (is "pure")
  2. F_2 belong only to T_2 (is "pure")
  3. $F_1 \wedge F_2$ is equisatisfiable as F
- Resulting formula after purification is not equivalent, but this is good enough

How To Purify

- To purify formula F, exhaustively apply the following:
  1. Consider term $f(\ldots, t_i, \ldots)$. If $f \in \Sigma_i$ but t_i is not a term in T_i, replace t_i with fresh variable z and conjoin $z = t_i$
  2. Consider predicate $p(\ldots, t_i, \ldots)$. If $p \in \Sigma_i$ but t_i is not a term in T_i, replace t_i with fresh variable w and conjoin $w = t_i$
- After this procedure, we can write F as $F_1 \wedge F_2$, where each F_i is pure

Purification Example 1

- Consider $T_= \cup T_\mathbb{Q}$ formula $x \leq f(x) + 1$
- Is this formula already pure?
- Since $f(x)$ is not in $T_\mathbb{Q}$, replace with new variable y and add equality constraint $y = f(x)$
- Thus, formula after purification:

$$\underbrace{x \leq y + 1}_{T_\mathbb{Q}} \wedge \underbrace{y = f(x)}_{T_=}$$

Purification Example II

- Consider following $\Sigma_= \cup \Sigma_\mathbb{Z}$ formula:

$$f(x + g(y)) \leq g(a) + f(b)$$

- Easiest to purify "inside out"
- Is the term $x + g(y)$ pure?
- How do we purify it?
- Resulting formula:

$$f(x + z_1) \leq g(a) + f(b) \wedge z_1 = g(y)$$

Purification Example II, cont

$$f(x+z_1) \leq g(a) + f(b) \wedge z_1 = g(y)$$

- Is $f(x+z_1)$ pure?
- How do we purify?
- Resulting formula:

$$f(z_2) \leq g(a) + f(b) \wedge z_1 = g(y) \wedge z_2 = x + z_1$$

- Is formula purified now? no

Purification Example II, cont

$$f(z_2) \leq g(a) + f(b) \wedge z_1 = g(y) \wedge z_2 = x + z_1$$

- How do we purify?
- Resulting formula:

$$f(z_2) \leq z_3 + z_4 \wedge z_1 = g(y) \wedge z_2 = x + z_1 \wedge z_3 = g(a) \wedge z_4 = f(b)$$

- Is formula purified now?

Purification Example II, cont

$$f(z_2) \leq z_3 + z_4 \ \wedge z_1 = g(y) \wedge z_2 = x + z_1 \ \wedge z_3 = g(a) \wedge z_4 = f(b)$$

- How do we purify?
- Resulting formula:

$$z_5 \leq z_3 + z_4 \wedge z_1 = g(y) \wedge z_2 = x + z_1 \wedge \\ z_3 = g(a) \wedge z_4 = f(b) \wedge z_5 = f(z_2)$$

- Is formula purified now?

Shared vs. Unshared Variables

- After purification, we have decomposed a formula F into two pure formulas F_1 and F_2
- If x occurs in both F_1 and F_2, x is called shared variable
- If y occurs only in F_1 or only in F_2, it is called unshared variable
- Consider the following purified formula:

$$\underbrace{w_1 = x + y \wedge y = 1 \wedge w_2 = 2}_{T_{\mathbb{Z}}} \ \wedge \ \underbrace{w_1 = f(x) \wedge f(x) \neq f(w_2)}_{T_{=}}$$

- Which variables are shared? w_1, x, w_2
- Which variables are unshared? y

Two Phases of Nelson-Oppen

- Recall: Nelson-Oppen method has two different phases:
  1. Purification: Seperate formula F in $T_1 \cup T_2$ into two formulas F_1 in T_1 and F_2 in T_2
  2. Equality propagation: Propagate all relevant equalities between theories
- Talk about second phase next
- But this phase is different for convex vs. non-convex theories

Convex Theories

- Theory T is called convex if for every conjunctive formula F:
  - If $F \Rightarrow \bigvee_{i=1}^{n} x_i = y_i$ for finite n
  - Then, $F \Rightarrow x_i = y_i$ for some $i \in [1, n]$
- Thus, in convex theory, if F implies disjunction of equalities, F also implies at least one of these equalities on its own
- If a theory does not satisfy this condition, it is called non-convex

Examples of Convex and Non-Convex Theories

- Example: Consider formula $1 \leq x \wedge x \leq 2$ in $T_{\mathbb{Z}}$
- Does it imply $x = 1 \vee x = 2$?
- Does it imply $x = 1$?
- Does it imply $x = 2$?
- Is $T_{\mathbb{Z}}$ convex?
- However, theory of rationals $T_{\mathbb{Q}}$ is convex
- Theory of equality $T_=$ is also convex
- Combining decision procedures for two convex theories is easier and more efficient

Nelson-Oppen Method for Convex Theories

- Given formula F in $T_1 \cup T_2$ (T_1, T_2 convex), want to decide if F is satisfiable
- First, purify F into F_1 and F_2
- Run decision procedures for T_1, T_2 to decide sat. of F_1, F_2
- If either is unsat, F is unsatisfiable.

Nelson-Oppen Method for Convex Theories

- If both are SAT, this does not mean F is sat
- Example:
$$\underbrace{x + y = 2 \wedge x = 1}_{T_{\mathbb{Z}}} \wedge \underbrace{f(x) \neq f(y)}_{T_=}$$
- Here, F_1 and F_2 are individually sat, but their combination is unsat b/c $T_{\mathbb{Z}}$ implies $x = y$
- In the case where F_1 and F_2 are sat, theories have to exchange all implied equalities
- Why only equalities?

Nelson-Oppen Method for Convex Theories

- For each pair of shared variables x, y, determine if:
  1. $F_1 \Rightarrow x = y$
  2. $F_2 \Rightarrow x = y$
- If (1) holds but not (2), conjoin $x = y$ with F_2
- If (2) holds but not (1), conjoin $x = y$ with F_1
- Let F_1' and F_2' denote new formulas
- Check satisfiability of F_1' and F_2'
- Repeat until either formula becomes unsat or no new equalities can be inferred

Example

- Use Nelson-Oppen to decide sat of following $T_= \cup T_{\mathbb{Q}}$ formula:
$$f(f(x) - f(y)) \neq f(z) \;\wedge\; x \leq y \;\wedge\; y + z \leq x \;\wedge\; 0 \leq z$$
- First, we need to purify:
  - Replace $f(x)$ with new variable w_1
  - Replace $f(y)$ with new variable w_2
  - $f(x) - f(y)$ is now replaced with $w_1 - w_2$ and we conjoin
$$w_1 = f(x) \wedge w_2 = f(y)$$
  - First literal is now $f(w_1 - w_2) \neq f(z)$; still not pure!
  - Replace $w_1 - w_2$ with w_3 and add equality $w_3 = w_1 - w_2$

Example, cont

- Purified formula is $F_1 \wedge F_2$ where:
$$F_1: \quad w_1 = f(x) \wedge w_2 = f(y) \wedge f(w_3) \neq f(z)$$
$$F_2: \quad w_3 = w_1 - w_2 \;\wedge\; x \leq y \;\wedge\; y + z \leq x \;\wedge\; 0 \leq z$$
- Which variables are shared?
- Check sat of F_1. Is it SAT?
- Check sat of F_2. Is it SAT?
- Now, for each pair of shared variable x_i, x_j, we query whether F_1 or F_2 imply $x_i = x_j$

Example, cont

$$F_1: \quad w_1 = f(x) \wedge w_2 = f(y) \wedge f(w_3) \neq f(z)$$
$$F_2: \quad w_3 = w_1 - w_2 \ \wedge \ x \leq y \ \wedge \ y + z \leq x \ \wedge \ 0 \leq z$$

- Consider the query $x = y$ – is it implied by either F_1 or F_2?
- $y + z \leq x \wedge 0 \leq z$ imply $0 \leq z \leq x - y$, i.e., $y \leq x$
- Since we also have $x \leq y$, $T_{\mathbb{Q}}$ implies $x = y$
- Now, propagate this to $T_=$, so F_1' becomes:

$$F_1': w_1 = f(x) \wedge w_2 = f(y) \wedge f(w_3) \neq f(z) \wedge x = y$$

- Check sat of F_1'. Is it SAT? yes
- Are we done? no

Example, cont

$$F_1: \quad w_1 = f(x) \wedge w_2 = f(y) \wedge f(w_3) \neq f(z) \wedge x = y$$
$$F_2: \quad w_3 = w_1 - w_2 \ \wedge \ x \leq y \ \wedge \ y + z \leq x \ \wedge \ 0 \leq z$$

- Since F_1 changed, need to check if it implies any new equality
- Does it imply a new equality? yes, $w_1 = w_2$
- Now, we add $w_1 = w_2$ to F_2:

$$F_2: w_3 = w_1 - w_2 \ \wedge \ x \leq y \ \wedge \ y + z \leq x \ \wedge \ 0 \leq z \ \wedge \ w_1 = w_2$$

- We recheck sat of F_2. Is it SAT? yes
- Still not done b/c need to check if F_2 implies any new equalities

Example, cont

$$F_1: \quad w_1 = f(x) \wedge w_2 = f(y) \wedge f(w_3) \neq f(z) \wedge x = y$$
$$F_2: \quad w_3 = w_1 - w_2 \ \wedge \ x \leq y \ \wedge \ y + z \leq x \ \wedge \ 0 \leq z \ \wedge \ w_1 = w_2$$

- Consider the query $w_3 = z$?
- $w_3 = w_1 - w_2$ and $w_1 = w_2$ imply $w_3 = 0$
- Since $x = y$, $y + z \leq x$ implies $z \leq 0$
- Since $z \leq 0$ and $0 \leq z$, we have $z = 0$
- Thus, $T_{\mathbb{Q}}$ answer "yes" for query $w_3 = z$

Example, cont

- Now, propagate $w_3 = z$ to F_1:

$$F_1: w_1 = f(x) \wedge w_2 = f(y) \wedge f(w_3) \neq f(z) \wedge x = y \ \wedge w_3 = z$$

- Is this sat?
- No, because $w_3 = z$ implies $f(w_3) = f(z)$
- This contradicts $f(w_3) \neq f(z)$
- Thus, original formula is UNSAT

Non-Convex Theories

- Unfortunately, technique discussed so far does not work for non-convex theories
- Consider the following $T_{\mathbb{Z}} \cup T_=$ formula:

$$1 \leq x \wedge x \leq 2 \wedge f(x) \neq f(1) \wedge f(x) \neq f(2)$$

- Is this formula SAT? no
- Let's see what happens if we use technique described so far
- If we purify, we get the following formulas:

$$F_1: \quad f(x) \neq f(w_1) \wedge f(x) \neq f(w_2)$$
$$F_2: \quad 1 \leq x \wedge x \leq 2 \wedge w_1 = 1 \wedge w_2 = 2$$

Example, cont

$$F_1: \quad f(x) \neq f(w_1) \wedge f(x) \neq f(w_2)$$
$$F_2: \quad 1 \leq x \wedge x \leq 2 \wedge w_1 = 1 \wedge w_2 = 2$$

- Is F_1 SAT? yes
- Is F_2 SAT? yes
- Does F_1 imply new equalities? no
- Does F_2 imply new equalities? no
- Thus technique discussed so far returns sat, although formula in unsat

Nelson-Oppen with Non-Convex Theories

- Problem is that in non-convex theories, a formula might imply a disjunction of equalities, but not any individual equality
- We also have to query and propagate disjunctions of equalities
- But how do you propagate disjunctions, since we only allow conjunctive formula?
- If answer to query $\bigvee_{i=1}^{n} x_i = y_i$ is yes, create n subproblems where we propagate $x_i = y_i$ in i'th subproblem
- If there is any subproblem that is satisfiable, original formula is satisfiable
- If every subproblem is unsatisfiable, then original formula is unsatisfiable

Example

- Consider $T_= \cup T_\mathbb{Z}$ formula:

$$1 \leq x \land x \leq 2 \land f(x) \neq f(1) \land f(x) \neq f(2)$$

- After purification, we get:

$$\begin{array}{ll} F_1: & f(x) \neq f(w_1) \land f(x) \neq f(w_2) \\ F_2: & 1 \leq x \land x \leq 2 \land w_1 = 1 \land w_2 = 2 \end{array}$$

- Does F_2 imply any disjunction of equalities?

Example, cont

- Now, we create two subproblems, one where we propagate $x = w_1$ and $x = w_2$
- First subproblem:

$$\begin{array}{ll} F_1: & f(x) \neq f(w_1) \land f(x) \neq f(w_2) \land x = w_1 \\ F_2: & 1 \leq x \land x \leq 2 \land w_1 = 1 \land w_2 = 2 \end{array}$$

- Is this satisfiable?
-

Example, cont

- Second subproblem:

$$\begin{array}{ll} F_1: & f(x) \neq f(w_1) \land f(x) \neq f(w_2) \land x = w_2 \\ F_2: & 1 \leq x \land x \leq 2 \land w_1 = 1 \land w_2 = 2 \end{array}$$

- Is this satisfiable?
-
- Since neither subproblem is satisfiable, Nelson-Oppen returns unsat for original formula

Example II

- Consider the following $T_= \cup T_\mathbb{Z}$ formula:

$$1 \leq x \land x \leq 3 \land f(x) \neq f(1) \land f(x) \neq f(3) \land f(1) \neq f(2)$$

- Formulas after purification:

$$\begin{array}{ll} F_1: & f(x) \neq f(w_1) \land f(x) \neq f(w_3) \land f(w_1) \neq f(w_2) \\ F_2: & 1 \leq x \land x \leq 3 \land w_1 = 1 \land w_2 = 2 \land w_3 = 3 \end{array}$$

- Consider the query $x = w_1 \lor x = w_2 \lor x = w_3$
- Does either formula imply this query?

Example II, cont

- First subproblem:

$$\begin{array}{ll} F_1: & f(x) \neq f(w_1) \land f(x) \neq f(w_3) \land f(w_1) \neq f(w_2) \land x = w_1 \\ F_2: & 1 \leq x \land x \leq 3 \land w_1 = 1 \land w_2 = 2 \land w_3 = 3 \end{array}$$

- Is this satisfiable?
- Second subproblem:

$$\begin{array}{ll} F_1: & f(x) \neq f(w_1) \land f(x) \neq f(w_3) \land f(w_1) \neq f(w_2) \land x = w_2 \\ F_2: & 1 \leq x \land x \leq 3 \land w_1 = 1 \land w_2 = 2 \land w_3 = 3 \end{array}$$

- Is this satisfiable?

Example II, cont

Second subproblem:

$$F_1: \quad f(x) \neq f(w_1) \wedge f(x) \neq f(w_3) \wedge f(w_1) \neq f(w_2) \wedge x = w_2$$
$$F_2: \quad 1 \leq x \wedge x \leq 3 \wedge w_1 = 1 \wedge w_2 = 2 \wedge w_3 = 3$$

- So it's satisfiable, are we done?
- Are there any new implied equalities or disjunctions of equalities?
- Thus, second subproblem is satisfiable
- Do we need to check third subproblem? No
- Thus, original formula is satisfiable

Nelson-Oppen for Convex vs. Non-Convex Theories

- Nelson-Oppen method is much more efficient for convex theories than for non-convex theories
- In convex theories:
  1. need to issue one query for each pair of shared variables
  2. If decision procedures for T_1 and T_2 have polynomial time complexity, combination using Nelson-Oppen also has polynomial complexity
- In non-convex theories:
  1. need to consider disjunctions of equalities between each pair of shared variables
  2. If decision procedures for T_1 and T_2 have NP time complexity, combination using Nelson-Oppen also has NP time complexity

Summary

- Nelson-Oppen method gives a sound and complete decision procedure for combination theories
- However, it only works for quantifier-free theories that are infinitely stable
- Not a severe restriction because most theories of interest are infinitely stable
- Next lecture: How to decide satisfiability in first-order theories without converting to DNF