Decision Procedures

Jochen Hoenicke

Software Engineering
Albert-Ludwigs-University Freiburg

Winter Term 2015/16

Quantifier-free Theory of Equality

The Theory of Equality T_E

$$\Sigma_E \ : \ \{=,\ a,\ b,\ c,\ \ldots,\ f,\ g,\ h,\ \ldots,\ p,\ q,\ r,\ \ldots\}$$

uninterpreted symbols:

- constants $a, b, c, \ldots$
- functions $f, g, h, \ldots$
- predicates $p, q, r, \ldots$

Axioms of T_E

1. $\forall x.\ x = x$ (reflexivity)
2. $\forall x, y.\ x = y \rightarrow y = x$ (symmetry)
3. $\forall x, y, z.\ x = y \wedge y = z \rightarrow x = z$ (transitivity)

define $=$ to be an equivalence relation.

Axiom schema

4. for each positive integer n and n-ary function symbol f,

$$\forall x_1, \dots, x_n, y_1, \dots, y_n.\ \textstyle\bigwedge_i x_i = y_i \rightarrow f(x_1, \dots, x_n) = f(y_1, \dots, y_n) \qquad \text{(congruence)}$$

5. for each positive integer n and n-ary predicate symbol p,

$$\forall x_1, \dots, x_n, y_1, \dots, y_n.\ \bigwedge_i x_i = y_i \rightarrow (p(x_1, \dots, x_n) \leftrightarrow p(y_1, \dots, y_n)) \qquad \text{(equivalence)}$$

Congruence Closure Algorithm

$F : s_1 = t_1 \land \cdots \land s_m = t_m \land \; s_{m+1} \neq t_{m+1} \land \cdots \land s_n \neq t_n$

The algorithm performs the following steps:

1. Construct the congruence closure $\sim$ of

$$\{s_1 = t_1, \ldots, s_m = t_m\}$$

over the subterm set S_F. Then

$$\sim \models s_1 = t_1 \land \cdots \land s_m = t_m \; .$$

2. If for any $i \in \{m + 1, \ldots, n\}$, $s_i \sim t_i$, return unsatisfiable.
3. Otherwise, $\sim \models F$, so return satisfiable.

How do we actually construct the congruence closure in Step 1?

Congruence Closure Algorithm (Details)

Begin with the finest congruence relation $\sim_0$:

$$\{\{s\} \;:\; s \in S_F\}\ .$$

Each term of S_F is only congruent to itself.

Then, for each $i \in \{1, \dots, m\}$, impose $s_i = t_i$ by merging

$$[s_i]_{\sim_{i-1}} \quad \text{and} \quad [t_i]_{\sim_{i-1}}$$

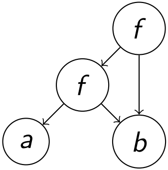
to form a new congruence relation $\sim_i$. To accomplish this merging,

- form the union of $[s_i]_{\sim_{i-1}}$ and $[t_i]_{\sim_{i-1}}$
- propagate any new congruences that arise within this union.

The new relation $\sim_i$ is a congruence relation in which $s_i \sim t_i$.

Efficient data structure for computing the congruence closure.

- Directed Acyclic Graph (DAG) to represent terms.

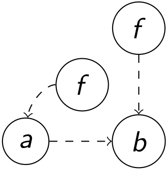


$f(f(a, b), b)$

$f(a, b)$

$a \qquad b$

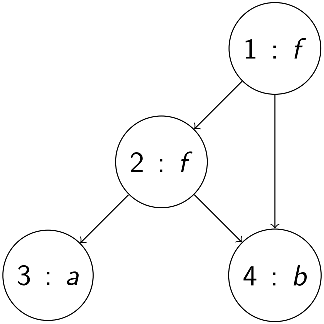
- Union-Find data structure to represent equivalence classes:



For every subterm of the Σ_E-formula F, create

- a node labelled with the function symbols.
- and edges to the argument nodes.

If two subterms are equal, only one node is created.



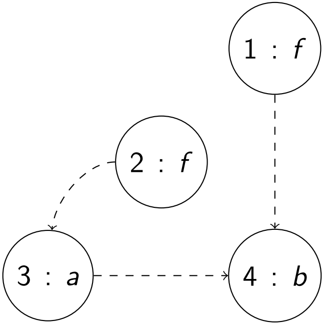
$f(f(a, b), b)$

$f(a, b)$

$a \quad b$

Union-Find Data Structure

Equivalence classes are connected by a tree structure, with arrows pointing to the root node.

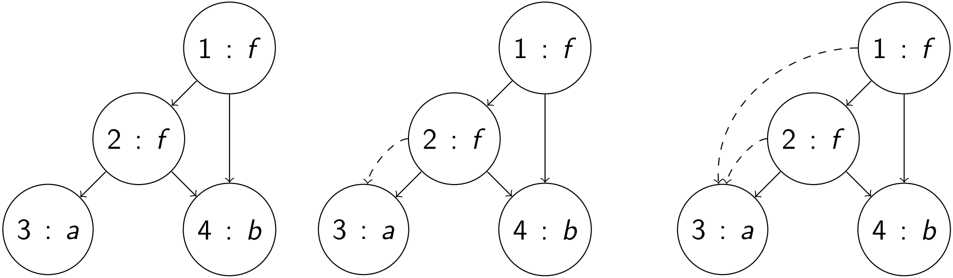


Two operations are defined:

- FIND: Find the representative of an equivalence class by following the edges. $O(\log n)$
- UNION: Merge two classes by connecting the representatives. $O(1)$

Summary of idea

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



Initial DAG

$f(a,b) = a \;\Rightarrow$
$\textsc{merge}\ f(a,b)\ a$

$f(a,b) \sim a,\ \ b \sim b \;\Rightarrow$
$f(f(a,b),b) \sim f(a,b)$
$\textsc{merge}\ f(f(a,b),b)$
$f(a,b)$

$$\left.\begin{array}{r} \textsc{find}\ f(f(a,b),b) = a = \textsc{find}\ a \\ f(f(a,b),b) \neq a \end{array}\right\} \Rightarrow \textbf{Unsatisfiable}$$

DAG representation

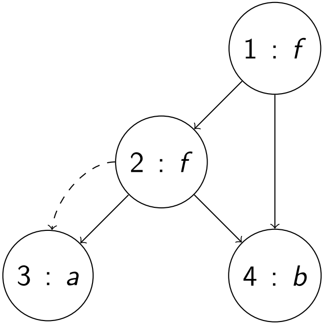
type **node** = {

`id`	:	**id** node's unique identification number
`fn`	:	**string** constant or function name
`args`	:	**id list** list of function arguments
`mutable find`	:	**id** the edge to the representative
`mutable ccpar`	:	**id set** if the node is the representative for its congruence class, then its `ccpar` (congruence closure parents) are all parents of nodes in its congruence class

}

DAG Representation of node 2

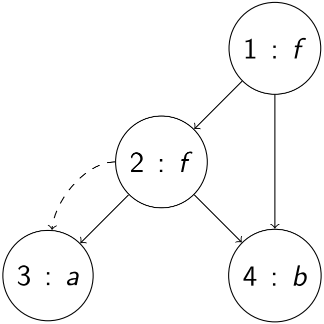
$$
\begin{array}{llll}
\texttt{type } \textbf{node} = \{ & & & \\
\quad \texttt{id} & : & \textbf{id} & \ldots 2 \\
\quad \texttt{fn} & : & \textbf{string} & \ldots f \\
\quad \texttt{args} & : & \textbf{idlist} & \ldots [3, 4] \\
\quad \texttt{mutable find} & : & \textbf{id} & \ldots 3 \\
\quad \texttt{mutable ccpar} & : & \textbf{idset} & \ldots \emptyset \\
\} & & &
\end{array}
$$



DAG Representation of node 3

type **node** = {
- `id` : **id** . . . 3
- `fn` : **string** . . . *a*
- `args` : **idlist** . . . []
- `mutable find` : **id** . . . 3
- `mutable ccpar` : **idset** . . . $\{1, 2\}$

}

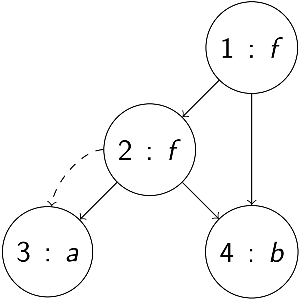


The Implementation: FIND

FIND function

returns the representative of node's congruence class

```
let rec FIND i =
  let n = NODE i in
  if n.find = i then i else FIND n.find
```



Example: $\textsc{find}\ 2 = \textsc{find}\ 3 = 3$

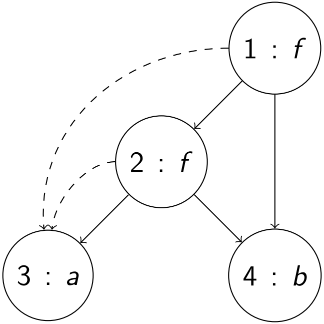
3 is the representative of 2.

UNION function

$$
\begin{aligned}
&\texttt{let}\ \textsc{union}\ i_1\ i_2 = \\
&\quad \texttt{let}\ n_1\ =\ \textsc{node}\ (\textsc{find}\ i_1)\ \texttt{in} \\
&\quad \texttt{let}\ n_2\ =\ \textsc{node}\ (\textsc{find}\ i_2)\ \texttt{in} \\
&\quad n_1.\texttt{find}\ \leftarrow\ n_2.\texttt{find}; \\
&\quad n_2.\texttt{ccpar}\ \leftarrow\ n_1.\texttt{ccpar}\ \cup\ n_2.\texttt{ccpar}; \\
&\quad n_1.\texttt{ccpar}\ \leftarrow\ \emptyset
\end{aligned}
$$

n_2 is the representative of the union class

Example



$\textsc{union}\ 1\ 2 \qquad n_1 = 1 \quad n_2 = 3$

$\quad 1.\mathtt{find} \leftarrow 3$

$\quad 3.\mathtt{ccpar} \leftarrow \{1, 2\}$

$\quad 1.\mathtt{ccpar} \leftarrow \emptyset$

The Implementation: CONGRUENT

CCPAR function

Returns parents of all nodes in i's congruence class

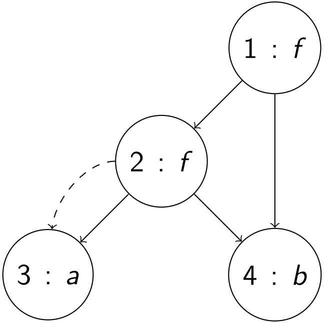
$$\begin{array}{l}\texttt{let}\ \textsc{ccpar}\ i\ =\\ \quad (\textsc{node}\ (\textsc{find}\ i)).\texttt{ccpar}\end{array}$$

CONGRUENT predicate

Test whether i_1 and i_2 are congruent

$$\begin{array}{l}\texttt{let}\ \textsc{congruent}\ i_1\ i_2\ =\\ \quad \texttt{let}\ n_1\ =\ \textsc{node}\ i_1\ \texttt{in}\\ \quad \texttt{let}\ n_2\ =\ \textsc{node}\ i_2\ \texttt{in}\\ \quad n_1.\texttt{fn} = n_2.\texttt{fn}\\ \qquad \wedge |n_1.\texttt{args}| = |n_2.\texttt{args}|\\ \qquad \wedge \forall i \in \{1, \ldots, |n_1.\texttt{args}|\}.\ \textsc{find}\ n_1.\texttt{args}[i] = \textsc{find}\ n_2.\texttt{args}[i]\end{array}$$

Example



Are 1 and 2 congruent?

`fn` fields	— both f
# of arguments	— same
left arguments $f(a, b)$ and a	— both congruent to 3
right arguments b and b	— both 4 (congruent)

Therefore 1 and 2 are congruent.

MERGE function

$$
\begin{array}{l}
\texttt{let rec}\ \textsc{merge}\ i_1\ i_2\ = \\
\quad \texttt{if}\ \textsc{find}\ i_1 \neq \textsc{find}\ i_2\ \texttt{then begin} \\
\quad\quad \texttt{let}\ P_{i_1}\ =\ \textsc{ccpar}\ i_1\ \texttt{in} \\
\quad\quad \texttt{let}\ P_{i_2}\ =\ \textsc{ccpar}\ i_2\ \texttt{in} \\
\quad\quad \textsc{union}\ i_1\ i_2; \\
\quad\quad \texttt{foreach}\ t_1, t_2 \in P_{i_1} \times P_{i_2}\ \texttt{do} \\
\quad\quad\quad \texttt{if}\ \textsc{find}\ t_1 \neq \textsc{find}\ t_2 \wedge \textsc{congruent}\ t_1\ t_2 \\
\quad\quad\quad \texttt{then}\ \textsc{merge}\ t_1\ t_2 \\
\quad\quad \texttt{done} \\
\quad \texttt{end}
\end{array}
$$

P_{i_1} and P_{i_2} store the current values of CCPAR i_1 and CCPAR i_2.

Decision Procedure: T_E-satisfiability

Given Σ_E-formula

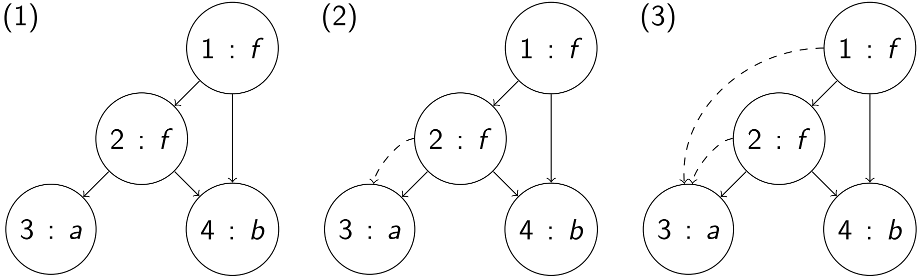
$$F : s_1 = t_1 \wedge \cdots \wedge s_m = t_m \wedge s_{m+1} \neq t_{m+1} \wedge \cdots \wedge s_n \neq t_n ,$$

with subterm set S_F, perform the following steps:

1. Construct the initial DAG for the subterm set S_F.
2. For $i \in \{1, \ldots, m\}$, MERGE s_i t_i.
3. If FIND s_i = FIND t_i for some $i \in \{m+1, \ldots, n\}$, return unsatisfiable.
4. Otherwise (if FIND $s_i \neq$ FIND t_i for all $i \in \{m+1, \ldots, n\}$) return satisfiable.

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

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



(1) Initial DAG

(2) MERGE 2 3
- UNION 2 3
- $P_2 = \{1\}$
- $P_3 = \{2\}$
- CONGRUENT 1 2

(3) MERGE 1 2
- UNION 1 2
- $P_1 = \{\}$
- $P_2 = \{1, 2\}$

FIND $f(f(a,b),b) = a =$ FIND $a \Rightarrow$ **Unsatisfiable**

Given Σ_E-formula

$$F : \ f(a,b) = a \land f(f(a,b),b) \neq a \ .$$

The subterm set is

$$S_F = \{a, \ b, \ f(a,b), \ f(f(a,b),b)\} \ ,$$

resulting in the initial partition

$$(1) \ \{\{a\}, \ \{b\}, \ \{f(a,b)\}, \ \{f(f(a,b),b)\}\}$$

in which each term is its own congruence class. Fig (1).

Final partition

$$(2) \ \{\{a, f(a,b), f(f(a,b),b)\}, \ \{b\}\}$$

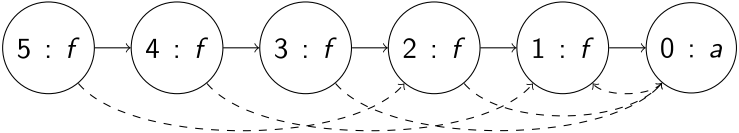
Does

$$(3) \ \{\{a, f(a,b), f(f(a,b),b)\}, \ \{b\}\} \models F \ ?$$

No, as $f(f(a,b),b) \sim a$, but F asserts that $f(f(a,b),b) \neq a$. Hence, F is T_E-unsatisfiable.

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

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



Initial DAG

$$\begin{array}{lllll}
f(f(f(a))) = a & \Rightarrow & \textsc{merge}\ 3\ 0 & P_3 = \{4\} & P_0 = \{1\} \\
 & \Rightarrow & \textsc{merge}\ 4\ 1 & P_4 = \{5\} & P_1 = \{2\} \\
 & \Rightarrow & \textsc{merge}\ 5\ 2 & P_5 = \{\} & P_2 = \{3\}
\end{array}$$

$$\begin{array}{lllll}
f(f(f(f(f(a))))) = a & \Rightarrow & \textsc{merge}\ 5\ 0 & P_5 = \{3\} & P_0 = \{1,4\} \\
 & \Rightarrow & \textsc{merge}\ 3\ 1 & P_3 = \{1,3,4\}, & P_1 = \{2,5\}
\end{array}$$

$\textsc{find}\ f(a) = f(a) = \textsc{find}\ a \Rightarrow$ **Unsatisfiable**

Given Σ_E-formula

$$F : \; f(f(f(a))) = a \wedge f(f(f(f(f(a))))) = a \wedge f(a) \neq a ,$$

which induces the initial partition

1. $\{\{a\}, \{f(a)\}, \{f^2(a)\}, \{f^3(a)\}, \{f^4(a)\}, \{f^5(a)\}\}$.
   The equality $f^3(a) = a$ induces the partition
2. $\{\{a, f^3(a)\}, \{f(a), f^4(a)\}, \{f^2(a), f^5(a)\}\}$.
   The equality $f^5(a) = a$ induces the partition
3. $\{\{a, f(a), f^2(a), f^3(a), f^4(a), f^5(a)\}\}$.
   Now, does

$$\{\{a, f(a), f^2(a), f^3(a), f^4(a), f^5(a)\}\} \models F \; ?$$

No, as $f(a) \sim a$, but F asserts that $f(a) \neq a$. Hence, F is T_E-unsatisfiable.

Theorem (Sound and Complete)

Quantifier-free conjunctive Σ_E-formula F is T_E-satisfiable iff the congruence closure algorithm returns satisfiable.

Proof:

$\Rightarrow$ Let I be a satisfying interpretation.
By induction over the steps of the algorithm one can prove:
Whenever the algorithm merges nodes t_1 and t_2, $I \models t_1 = t_2$ holds.

Since $I \models s_i \neq t_i$ for $i \in \{m+1, \ldots, n\}$ they cannot be merged.

Hence the algorithm returns satisfiable.

Correctness of the Algorithm (2)

Proof:

$\Leftarrow$ Let S denote the nodes of the graph and
Let $[t] := \{t' \mid t \sim t'\}$ denote the congruence class of t and
$S/\!\sim \; := \{[t] \mid t \in S\}$ denote the set of congruence classes.
Show that there is an interpretation I:

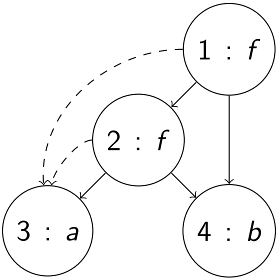
$$D_I = S/\!\sim \cup \{\Omega\}$$

$$\alpha_I[f](v_1, \ldots, v_n) = \begin{cases} [f(t_1, \ldots, t_n)] & v_1 = [t_1], \ldots, v_n = [t_n], \\ & f(t_1, \ldots, t_n) \in S \\ \Omega & \text{otherwise} \end{cases}$$

$$\alpha_I[=](v_1, v_2) = \top \text{ iff } v_1 = v_2$$

I is well-defined!
$\alpha_I[=]$ is a congruence relation,
$I \models F$.

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



$S = \{f(f(a,b),b), f(a,b), a, b\}$
$S/\!\sim\; = \{\{f(f(a,b),b), f(a,b), a\}, \{b\}\} = \{[a],[b]\}$
$D_I = \{[a],[b],\Omega\}$

$\alpha_I[f]$	$[a]$	$[b]$	Ω
$[a]$	Ω	$[a]$	Ω
$[b]$	Ω	Ω	Ω
Ω	Ω	Ω	Ω

$\alpha_I[=]$	$[a]$	$[b]$	Ω
$[a]$	$\top$	$\bot$	$\bot$
$[b]$	$\bot$	$\top$	$\bot$
Ω	$\bot$	$\bot$	$\top$

How to handle predicates?

We can get rid of predicates by

- Introduce fresh constant $\bullet$ corresponding to $\top$.
- Introduce a fresh function f_p for each predicate p.
- Replace $p(t_1, \ldots, t_n)$ with $f_p(t_1, \ldots, t_n) = \bullet$.

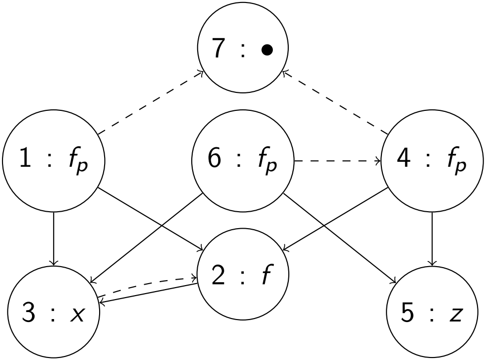
Compare the equivalence axiom for p
with the congruence axiom for f_p.

- $\forall x_1, x_2, y_1, y_2.\ x_1 = y_1 \land x_2 = y_2 \rightarrow p(x_1, x_2) \leftrightarrow p(y_1, y_2)$
- $\forall x_1, x_2, y_1, y_2.\ x_1 = y_1 \land x_2 = y_2 \rightarrow f_p(x_1, x_2) = f_p(y_1, y_2)$

$$x = f(x) \land p(x, f(x)) \land p(f(x), z) \land \neg p(x, z)$$

is rewritten to

$$x = f(x) \land f_p(x, f(x)) = \bullet \land f_p(f(x), z) = \bullet \land f_p(x, z) \neq \bullet$$



FIND $f_p(x, z) = \bullet$

FIND $\bullet = \bullet$

$\Rightarrow$ **Unsatisfiable**

Theory of Lists

Theory of Lists T_{cons}

Σ_{cons} : $\{\text{cons}, \ \text{car}, \ \text{cdr}, \ \text{atom}, \ =\}$

- constructor cons: $\text{cons}(a, b)$ list constructed by prepending a to b
- left projector car: $\text{car}(\text{cons}(a, b)) = a$
- right projector cdr: $\text{cdr}(\text{cons}(a, b)) = b$
- atom: unary predicate

Axioms of T_{cons}

- reflexivity, symmetry, transitivity
- congruence axioms:

$$\forall x_1, x_2, y_1, y_2.\ x_1 = x_2 \ \wedge\ y_1 = y_2 \ \rightarrow\ \text{cons}(x_1, y_1) = \text{cons}(x_2, y_2)$$
$$\forall x, y.\ x = y \ \rightarrow\ \text{car}(x) = \text{car}(y)$$
$$\forall x, y.\ x = y \ \rightarrow\ \text{cdr}(x) = \text{cdr}(y)$$

- equivalence axiom:

$$\forall x, y.\ x = y \ \rightarrow\ (\text{atom}(x) \ \leftrightarrow\ \text{atom}(y))$$

- $\forall x, y.\ \text{car}(\text{cons}(x, y)) = x$ (left projection)
  $\forall x, y.\ \text{cdr}(\text{cons}(x, y)) = y$ (right projection)
  $\forall x.\ \neg\text{atom}(x) \rightarrow \text{cons}(\text{car}(x), \text{cdr}(x)) = x$ (construction)
  $\forall x, y.\ \neg\text{atom}(\text{cons}(x, y))$ (atom)

First simplify the formula:

- Consider only conjunctive $\Sigma_{\text{cons}} \cup \Sigma_{\text{E}}$-formulae.
  Convert non-conjunctive formula to DNF and check each disjunct.
- $\neg\text{atom}(u_i)$ literals are removed:

  $$\text{replace} \quad \neg\text{atom}(u_i) \quad \text{with} \quad u_i = \text{cons}(u_i^1, u_i^2)$$

  by the (construction) axiom.

Result is a conjunctive $\Sigma_{\text{cons}} \cup \Sigma_{\text{E}}$-formula with the literals:

- $s = t$
- $s \neq t$
- $atom(u)$

where s, t, u are $T_{\text{cons}} \cup T_{\text{E}}$-terms.

Algorithm: T_{cons}-Satisfiability (the idea)

$$
\begin{aligned}
F:\quad & \underbrace{s_1 = t_1 \ \wedge\ \cdots\ \wedge\ s_m = t_m}_{\text{generate congruence closure}} \\
\wedge\ & \underbrace{s_{m+1} \neq t_{m+1} \ \wedge\ \cdots\ \wedge\ s_n \neq t_n}_{\text{search for contradiction}} \\
\wedge\ & \underbrace{\mathrm{atom}(u_1) \ \wedge\ \cdots\ \wedge\ \mathrm{atom}(u_\ell)}_{\text{search for contradiction}}
\end{aligned}
$$

where s_i, t_i, and u_i are $T_{\text{cons}} \cup T_{\text{E}}$-terms.

UNI FREIBURG

1. Construct the initial DAG for S_F
2. for each node n with $n.\mathtt{fn} = \text{cons}$
   - add $\text{car}(n)$ and MERGE $\text{car}(n)$ $n.\mathtt{args}[1]$
   - add $\text{cdr}(n)$ and MERGE $\text{cdr}(n)$ $n.\mathtt{args}[2]$

   by axioms (left projection), (right projection)
3. for $1 \leq i \leq m$, MERGE s_i t_i
4. for $m + 1 \leq i \leq n$, if FIND s_i $=$ FIND t_i, return **unsatisfiable**
5. for $1 \leq i \leq \ell$, if $\exists v.$ FIND v $=$ FIND u_i $\wedge$ $v.\mathtt{fn} = \text{cons}$, return **unsatisfiable**
6. Otherwise, return **satisfiable**

Example

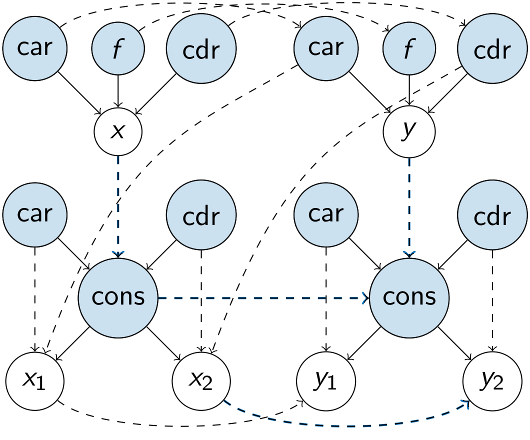
Given $(\Sigma_{\text{cons}} \cup \Sigma_{\text{E}})$-formula

$$F : \quad \begin{array}{c} \text{car}(x) = \text{car}(y) \;\wedge\; \text{cdr}(x) = \text{cdr}(y) \\ \wedge\; \neg\text{atom}(x) \;\wedge\; \neg\text{atom}(y) \;\wedge\; f(x) \neq f(y) \end{array}$$

where the function symbol f is in Σ_{E}

$$F' : \quad \begin{array}{lr} \text{car}(x) = \text{car}(y) \quad \wedge & (1) \\ \text{cdr}(x) = \text{cdr}(y) \quad \wedge & (2) \\ x = \text{cons}(x_1, x_2) \quad \wedge & (3) \\ y = \text{cons}(y_1, y_2) \quad \wedge & (4) \\ f(x) \neq f(y) & (5) \end{array}$$

Example: $\text{car}(x) = \text{car}(y) \land \text{cdr}(x) = \text{cdr}(y) \land$ $x = cons(x_1, x_2) \land y = cons(y_1, y_2) \land f(x) \neq f(y)$



Step 1
Step 2
Step 3 :
$\textsc{merge}$ car(x) car(y)
$\textsc{merge}$ cdr(x) cdr(y)
$\textsc{merge}$ x cons(x_1, x_2)
$\textsc{merge}$ car(x) car(cons(x_1, x_2))
$\textsc{merge}$ cdr(x) cdr(cons(x_1, x_2))
$\textsc{merge}$ y cons(y_1, y_2)
$\textsc{merge}$ car(y) car(cons(y_1, y_2))
$\textsc{merge}$ cdr(y) cdr(cons(y_1, y_2))
$\textsc{merge}$ cons(x_1, x_2) cons(y_1, y_2)
$\textsc{merge}$ $f(x)$ $f(y)$
Step 4 :
$\textsc{find}\ f(x) = \textsc{find}\ f(y)$
$\Rightarrow$ *unsatisfiable*

Theorem (Sound and Complete)

Quantifier-free conjunctive Σ_{cons}-formula F is T_{cons}-satisfiable iff the congruence closure algorithm for T_{cons} returns satisfiable.

Proof:

$\Rightarrow$ Let I be a satisfying interpretation.
By induction over the steps of the algorithm one can prove:
Whenever the algorithm merges nodes t_1 and t_2, $I \models t_1 = t_2$ holds.

Since $I \models s_i \neq t_i$ for $i \in \{m+1, \ldots, n\}$ they cannot be merged.
From $I \models \neg atom(\text{cons}(t_1, t_2))$ and $I \models atom(u_i)$
follows $I \models u_i \neq \text{cons}(t_1, t_2)$ by equivalence axiom.
Thus u_i for $i \in \{1, \ldots, \ell\}$ cannot be merged with a cons node.

Hence the algorithm returns satisfiable.

Correctness of the Algorithm (2)

Proof:

$\Leftarrow$ Let S denote the nodes of the graph and let $S/\sim$ denote the congruence classes computed by the algorithm. Show that there is an interpretation I:

$$
\begin{aligned}
D_I = \ & \{\text{binary trees with leaves labelled with } S/\sim\} \\
& \setminus \{\text{trees with subtree } \begin{smallmatrix} \swarrow & \searrow \\ [t_1] & [t_2] \end{smallmatrix} \text{ with } \mathrm{cons}(t_1, t_2) \in S\}
\end{aligned}
$$

$$
\mathrm{cons}_I(v_1, v_2) = \begin{cases} [cons(t_1, t_2)] & v_1 = [t_1], v_2 = [t_2], \mathrm{cons}(t_1, t_2) \in S \\ \begin{smallmatrix} \swarrow & \searrow \\ v_1 & v_2 \end{smallmatrix} & \text{otherwise} \end{cases}
$$

$$
\mathrm{car}_I(v) = \begin{cases} [car(t)] & \text{if } v = [t], \mathrm{car}(t) \in S \\ v_1 & \text{if } v = \begin{smallmatrix} \swarrow & \searrow \\ v_1 & v_2 \end{smallmatrix} \\ \text{arbitrary} & \text{otherwise} \end{cases}
$$

Correctness of the Algorithm (3)

$$\mathrm{cdr}_I(v) = \begin{cases} [cdr(t)] & \text{if } v = [t], \mathrm{cdr}(t) \in S \\ v_2 & \text{if } v = \begin{array}{cc} \swarrow & \searrow \\ v_1 & v_2 \end{array} \\ \text{arbitrary} & \text{otherwise} \end{cases}$$

$$atom_I(v) = \begin{cases} \text{false} & \text{if } v = [cons(t_1, t_2)] \\ \text{false} & \text{if } v = \begin{array}{cc} \swarrow & \searrow \\ v_1 & v_2 \end{array} \\ \text{true} & \text{otherwise} \end{cases}$$

$$\alpha_I[=](v_1, v_2) = \text{true iff } v_1 = v_2$$

I is well-defined! $\alpha_I[=]$ is obviously a congruence relation.

$\forall x, y.\ \mathrm{car}(\mathrm{cons}(x, y)) = x$ (left projection)

$\forall x, y.\ \mathrm{cdr}(\mathrm{cons}(x, y)) = y$ (right projection)

$\forall x.\ \neg\mathrm{atom}(x) \rightarrow \mathrm{cons}(\mathrm{car}(x), \mathrm{cdr}(x)) = x$ (construction)

$\forall x, y.\ \neg\mathrm{atom}(\mathrm{cons}(x, y))$ (atom)

Example: $\text{car}(x) = \text{car}(y) \land \text{cdr}(x) = \text{cdr}(y) \land$ $x = cons(x_1, x_2) \land y = cons(y_1, y_2)$