Lecture 14

Monday, March 9, 2020 4:56 PM

- Announcement regarding Wed / Friday
- Demo of Z3
- Theory of Equality with Uninterpreted Fns.

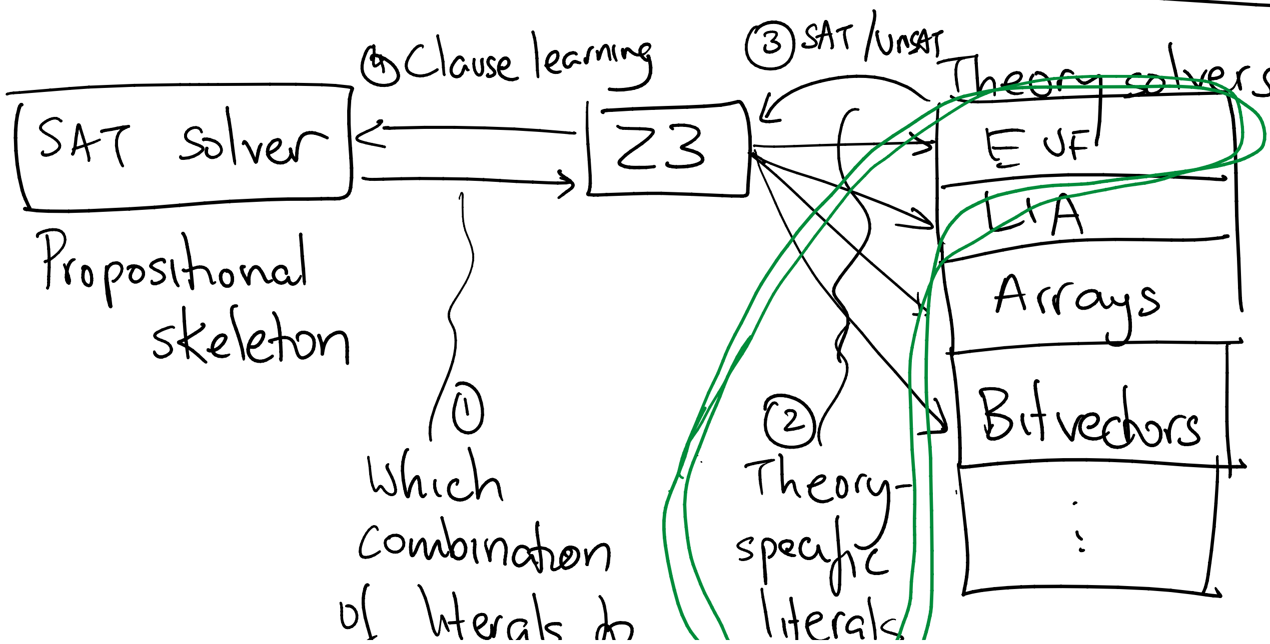
EUF

Other theories: LIA, LRA

AUFLIA, AUFBV, ...

- Theory combination / Nelson-Oppen Proc.

Stably infinite



combination of literals to satisfy

specific literals

Deciding EUF : Congruence Closure

Input: Set of EUF literals, φ

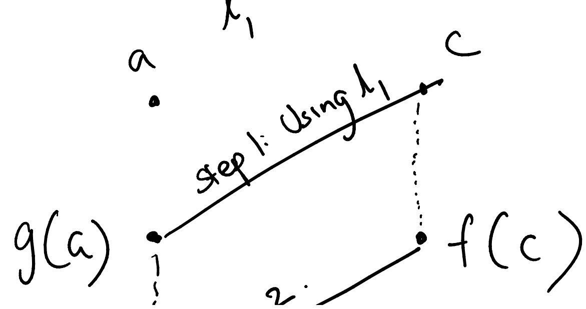
l_1 and l_2 and ... and l_k

$$\text{Literal}, l ::= t == t' \mid t \neq t'$$

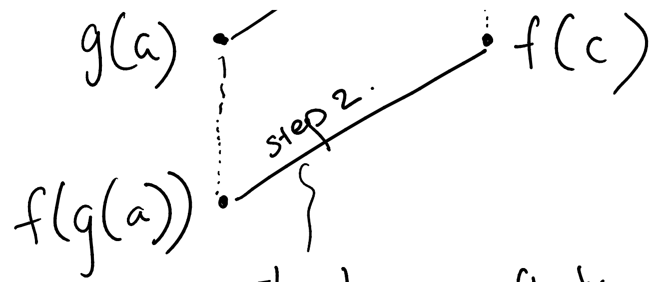
$$\text{Term}, t ::= v \ (\text{Variable}) \mid f(t)$$

Output: Satisfying interpretation of φ, if it exists.

Example①: $\underbrace{g(a) == c}_{l_1}$ and $\underbrace{f(g(a)) \neq f(c)}_{l_2}$.



Step 1, 2, ...: Draw as many lines



This line conflicts with the requirement that $f(g(a)) \neq f(c)$. Therefore unsat.

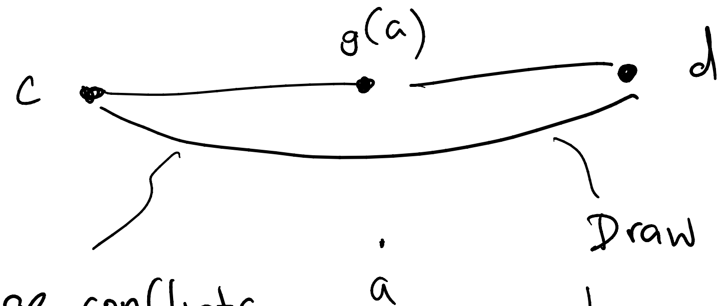
as many lines as possible.

Step n+1: Examine inequality constraints

Example 2: $l_1: g(a) == c$ and

$l_2: g(a) == d$ and

$l_3: c \neq d$.



This edge conflicts with the requirement that $c \neq d$.

Draw c — d shortcut because of c — g(a) and g(a) — d edges

Algorithm: ① Draw graph G with node for each term appearing in φ.

node for each term appearing in φ.

② For every equality constraint $t_1 == t_2$ in φ, draw $t_1 — t_2$ edge in G.

③ Till fixpoint, do:

- If there is an edge $t — t'$ s.t. for some fn. f, both $f(t)$ and $f(t')$ are nodes of G, then draw edge $f(t) — f(t')$.

- If there are two edges
$$t — t' — t''$$
then add the shortcut
$$t — t''.$$

④ Now look at each inequality constraint

$t \neq t'$ in φ.

If we have drawn an edge

t —— t' in G

then return false

5. Return true.

Conjecture: Congruence Closure (φ) = true

iff φ is satisfiable.

Proof Case 1: $\Rightarrow$

Case 2: $\Leftarrow$ (Straightforward)

TST: φ is satisfiable $\Rightarrow$ $CC(\varphi)$ = true

- We will show: $CC(\varphi)$ = false $\Rightarrow$ φ is unsat.

- We will show: $CC(\varphi) = \text{false} \Rightarrow \varphi$ is unsat.
- Observe that whenever $CC(\varphi)$ returns false, we have discovered a conflict in φ.

Case 1:

TST: If $CC(\varphi) = \text{true}$, then φ is satisfiable

Chelsea's suggestion:

- Find SCCs of G.
- Assign distinct value to each SCC. All variables share that value.

- Assumes ability to invent new values.
- Assumes (crucially) that T is infinite.

(Note to self: Turn this into a HW problem).

<u>Theorem</u>: If domain of variables is infinite, then $cc(\varphi) = \text{true}$ iff φ is satisfiable.