Lecture 13

Wednesday, March 4, 2020 5:03 PM

- Recap of last class
  - Finished discussion of SAT solvers

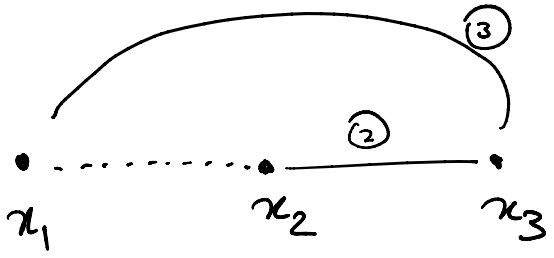
    Convert arbitrary SAT instances to CNF-SAT

    Simple algorithms for CNF-SAT
      - DPLL / Unit propagation
      - Clause learning
      - Decision heuristics + restart strategies
  - Introduced the problem of SMT.

    Satisfiability modulo theory

Ex: $\exists x_1\ x_2\ x_3 \quad \underbrace{x_1 \neq x_2}_{①} \quad \underbrace{x_2 = x_3}_{②} \quad \underbrace{x_3 = x_1}_{③}$

This is unsat.



②, ③ $\Rightarrow x_1 = x_2$

x_1 x_2 x_3 ⟶ Contradicts (1)

Ex: $\exists a\ b\ c\ d, f\ g$ s.t.

$g(a) = c$ and

$(f(g(a)) \neq f(c)$ or $g(a) = d)$ and

$c \neq d$

Is unsatisfiable.

α and

$(\beta$ or $\gamma)$ and

δ

SAT: Why not $\{\alpha, \beta, \delta\}$

T-solver: No. $\overline{\alpha \wedge \beta \wedge \delta}$.

SAT: OK, how about $\{\alpha, \gamma, \delta\}$

T-solver: No, $\overline{\alpha \wedge \delta \wedge \delta}$

SAT: OK, then unsat.

- Today's plan
  - Discuss SMT in more detail.

Theory solvers

- Equality with uninterpreted fns
- Difference logic / Linear (integer) arithmetic
- Arrays (McCarthy's theory)
- Bitvectors
- Strings

Strings

- How to combine SAT solvers with theory solvers
  - DPLL(T)
  - Combining theories: Nelson-Oppen procedure

Ex: $\underbrace{x \geq y+5}_{①}$ and $y+6 \geq x$ and $y \geq x$

This is unsatisfiable for $x, y \in \mathbb{Z}$.

There are algorithms to decide if a formula in LIA / LRA is decidable.

IA with multiplication is undecidable

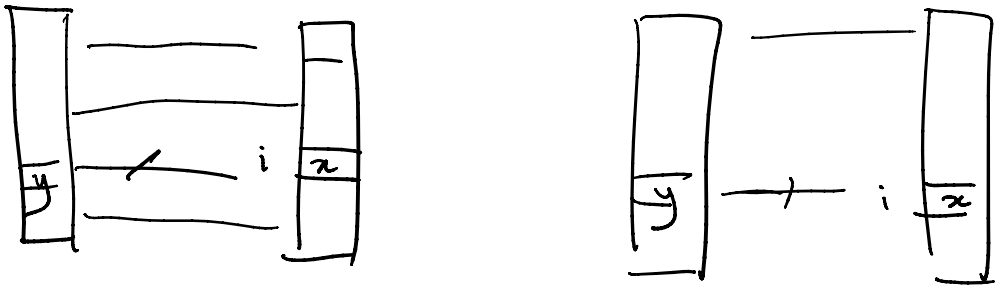
Theory of arrays

`a[i] := v;`	`assume (i ≠ j); old_aj = a[j]` `a[i] := v;`

```
a[i] := v;
assert(a[j] = old_aj)
```

---

a write(a, i, x) b write(b, i, x)



$a = b$ and $write(a, i, x) \neq b$

$\Rightarrow b[i] \neq x$

$a[i] \neq x$

Difference logic

Variables assume integer values.

Each literal is of the form $x - y \leq c$

Ex: $x - y < 3 \iff x - y \leq 2$

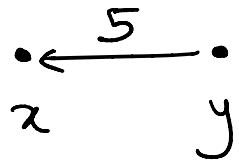
$x - y = 3 \iff (x - y \leq 3 \text{ and } y - x \leq -3)$

$x - y > 3 \iff y - x < -3 \iff y - x \leq -4$

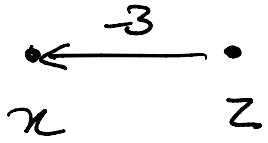
$x - y \geq 3 \iff y - x \leq -3$

Ex (from CB 24)

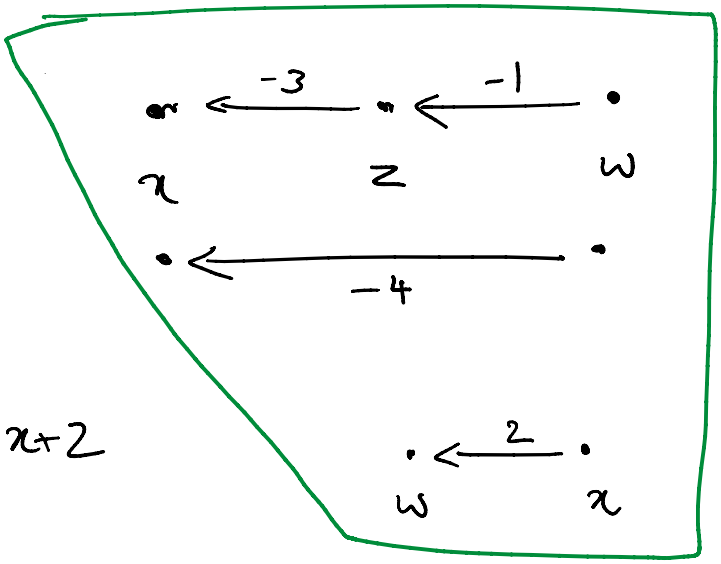
$x - y \leq 5 \iff x \leq y + 5$



$x - z \leq -3 \iff x \leq z - 3$



$z - w \leq -1 \iff z \leq w - 1$



$w - x \leq 2 \iff w \leq x + 2$

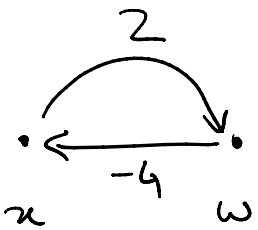
$x - w \leq -4$

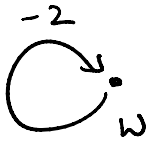
$x - w \leq -4$

$w - x \leq 2$

$-2 \leq x - w$

$-2 \leq -4$





$w \leq w - 2$

$0 \leq -2$

Sara's argument : Unsatisfiable because $-2 \nleq -4$

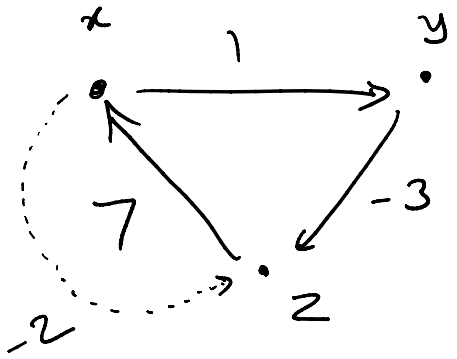
CB's argument: Unsatisfiable because negative weight path from $w \to w$

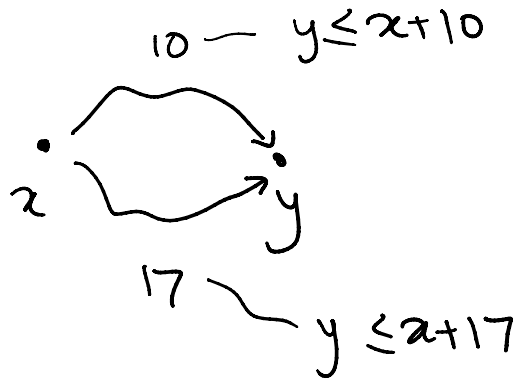
Theorem: Given a conjunction of difference logic literals φ:

① If negative weight cycle occurs in the corresponding weighted graph, then φ is unsatisfiable.

② If no negative weight cycle occurs, then φ is satisfiable.

Ex for (2)





Arbitrarily fix $x = 0$.

Find shortest path from x to v, $\forall$ variables v.

$y \leq x+1$ $\quad \pi_v$ with weight c_v.

Set $v \mapsto c$.

$x = 0$; $y = 1$; $z = -2$

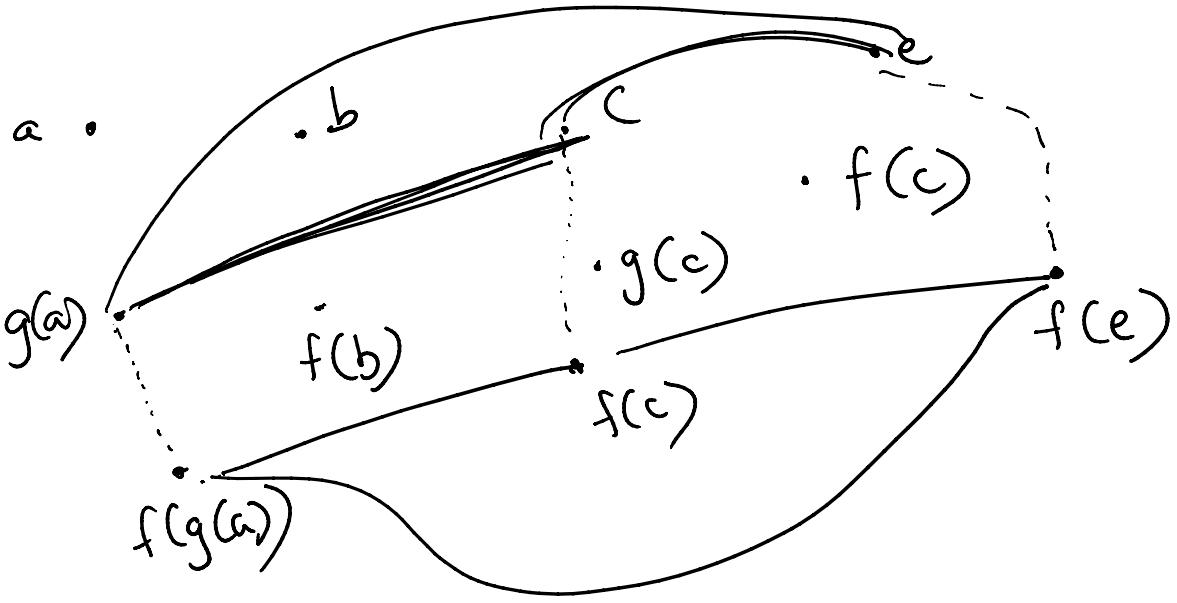
Solvers for Equality with Uninterpreted Fns (EUF)

(CB Slide 30)

- Example from beginning of class

- SAT solver proposes $\{\alpha, \beta, \delta\}$

$g(a) = c \quad f(g(a)) \neq f(c) \quad c \neq d \quad c = e$



Given : Conjunction of EUF literals, φ.

- Term, $t ::= v \mid f(t)$
- Literals, $l ::= t_1 = t_2 \mid t_1 \neq t_2$
- $\varphi ::= l_1$ and l_2 and ... and l_k.

To find : Is φ satisfiable?

Construction : ① Build graph with vertex for each term t in φ

② If there is a literal $t_1 = t_2$ in φ then draw an edge $t_1 — t_2$.

③ If there are two edges $t_1 — t_2 — t_3$, then draw the shortcut $t_1 — t_3$.

④ If there is an edge $t_1 — t_2$ and both $f(t_1)$ & $f(t_2)$ occur in the graph, then draw

$$f(t_1) — f(t_2).$$

(Repeat ②, ③, ④ until fixpoint)

⑤ For each literal $t_1 \neq t_2$ look for the $t_1 — t_2$ edge.

If it exists, report unsat.

⑥ (If we have reached here) φ is satisfiable.

Proposition: If ——————

then algorithm returns sat iff

φ is satisfiable.