program $\longrightarrow$ turn this into a formula or constraint system

property $\longrightarrow$

$\{P\}\ S\ \{Q\}$

$$\min \quad x+y$$
$$\text{s.t.} \quad x+y \geq 10$$

---

propositional logic $\quad (p \wedge q \wedge \neg s) \Rightarrow r$

Atoms $\boxed{\top \quad \bot}$ OR $p, q, r, s \ldots$

t f

true false

1 0

Literals atom or its negation p, $\neg q$

not

Formula F is either a literal

or $\neg F_1$

or $F_1 \wedge F_2$ (conjunction, AND)

or $F_1 \vee F_2$ (disjunction)

or $F_1 \Longrightarrow F_2 \qquad \neg F_1 \vee F_2$

or $F_1 \Longleftrightarrow F_2 \qquad ((F_1 \Rightarrow F_2) \wedge (F_2 \Rightarrow F_1))$

An interpretation I is a map from variables to $\{T, \perp\}$

a formula has 2^n interpretations where n is the number of variables

$I \models F$ if F evaluates to T under I

I is a "model" of F

$I \not\models F$ if F evaluates to $\perp$ under I

E.g. $F \triangleq (p \wedge q) \Longrightarrow (p \vee \neg q)$

$\equiv \qquad I = \{p \mapsto \perp,\ q \mapsto \perp\}$

$$\underbrace{(\perp \wedge \perp)} \Longrightarrow (\perp \vee \neg \perp)$$

$$\perp \Longrightarrow T \equiv \neg \perp \vee T$$

$$\equiv T$$

Satisfiability and validity

F is satisfiable (SAT) iff there is $I \models F$

F is valid (VALID) iff for all I, $I \models F$

F is VALID iff $\neg F$ is unsatisfiable (UNSAT)

① Truth table

② Binary decision diagrams (BDDs)

③ SAT solvers

④ deductive proof

semantic argument method

<u>neg</u>

$$\frac{I \models \neg F}{I \not\models F} \qquad \frac{I \not\models \neg F}{I \models F}$$

<u>conj</u>

$$\frac{I \models F \wedge G}{I \models F \qquad I \models G} \qquad \frac{I \not\models F \wedge G}{I \not\models F \ \underline{\text{OR}}\ I \not\models G}$$

<u>disj</u>

$$\frac{I \models F \vee G}{I \models F \ \text{OR}\ I \models G} \qquad \frac{I \not\models F \vee G}{I \not\models F \qquad I \not\models G}$$

<u>impl</u>

$$\neg F \vee G$$

$$\frac{I \models F \Rightarrow G}{I \models \neg F \ \text{OR}\ I \models G} \qquad \frac{I \not\models F \Rightarrow G}{I \models F \qquad I \not\models G}$$

<u>contradiction</u>

$$\frac{I \models F \qquad I \not\models F}{I \models \bot}$$

assume F is VALID

$\rightsquigarrow$

$I \not\models F$

$I \not\models (p \land q) \implies (p \lor \neg q)$

$I \models p \land q$ $\quad$ $I \not\models p \lor \neg q$

$I \models p$ $\quad$ $I \models q$ $\quad$ $I \not\models p$ $\quad$ $I \not\models \neg q$

Contradiction

no I exists therefore formula is VALID

Two formulas are equivalent $F_1 \equiv F_2$

iff forall I, $I \models F_1$ iff $I \models F_2$

$\boxed{F_1 \equiv F_2 \quad \text{iff} \quad F_1 \iff F_2 \text{ is VALID}}$

$\bot \iff \bot$ is VALID

$\top \iff \top$ is VALID

Normal forms

Negation Normal form (NNF)

Disjunctive Normal form (DNF)

Conjunctive Normal form (CNF)

NNF $-(x+y) = -x-y$

DNF

$$(p \wedge q \wedge \neg r)$$
$$\vee (\neg p \wedge q \wedge \neg r)$$
$$\vee \vdots$$
$$\vee$$
$$\vee$$

CNF

$(p \vee q \vee r)$ clause

$\wedge (\neg p \vee q \vee r)$

$\wedge$ ...

$\wedge$ ...

e.g. $r \vee (p \wedge q)$

distribute $\vee$ over $\wedge$

$(r \vee p) \wedge (r \vee q)$

Tseitin's transformation

$$F \xrightarrow{\text{translate}} F' \text{ is in CNF}$$

properties:

① if F' is UNSAT then F is UNSAT

② Any model of F' is a model of F if we disregard the additional variables

Intuition

def $f(x, y, z)$

  return $\underbrace{x + (\underbrace{\underbrace{2*y}_{t_1} + 3}_{t_2})}_{t_3}$

$$\downarrow$$

def $f(x, y, z)$

  $t_1 = 2*y$

  $t_2 = t_1 + 3$

  $t_3 = t_2 + x$

  return t_3

$$F \triangleq \underbrace{\underbrace{(p \wedge q)}_{F_1} \vee (\underbrace{\underbrace{q \wedge \neg r}_{F_2} \wedge s}_{F_3})}_{F_4 = F_1 \vee F_3}$$

① for every F_j create a new variable t_j

② for every F_i (starting with most-deeply nested)

$$F_i' \triangleq t_i \Longleftrightarrow (l_i \circ l_i')$$

LHS of F_i $\wedge, \vee$ RHS of F_i

$F_1' \triangleq t_1 \Leftrightarrow (p \wedge q)$

$F_2' \triangleq t_2 \Leftrightarrow (q \wedge \neg r)$

$F_3' \triangleq t_3 \Leftrightarrow (t_2 \wedge s)$

$F_4' \triangleq t_4 \Leftrightarrow (t_3 \vee t_1)$

use De Morgan's laws

$$F' = t_4 \land F_1' \land F_2' \land F_3' \land F_4'$$