$\{P\}\ S\ \{Q\} \longrightarrow$ verify $\longrightarrow$ yes/No

Satisfiability: formula in Boolean logic $\longrightarrow$ yes/No

---

propositional

Atoms : $\top$, $\bot$, p, q, r, s, ...

($\top$: true, $\bot$: false)

Literals : variable or its negation , e.g. p or $\neg p$ (NOT NEG)

Formula $F ::=$ literal

$\mid \neg F$ (NOT, negation)

$\mid F \wedge F$ (AND , conjunction)

$\mid F \vee F$ (OR , disjunction)

E.g. $p \wedge \neg q$

implication $\mid F_1 \Rightarrow F_2$ $\qquad \neg F_1 \vee F_2$

bi-implication $\mid F_1 \Leftrightarrow F_2$ $\qquad (F_1 \Rightarrow F_2) \wedge (F_2 \Rightarrow F_1)$

An interpretation I is a map from variables to $\{\top, \bot\}$

How many interpretations are there?

$$2^{|var|}$$

$p \Rightarrow q \equiv \neg p \vee q$

p	q	$\neg p \vee q$
$\bot$	$\bot$	$\top$
$\bot$	$\top$	$\top$
$\top$	$\bot$	$\bot$
$\top$	$\top$	$\top$

$I \models F$ iff F evaluates to $\top$ under I

I is a model of F

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

e.g. $F \triangleq (p \wedge q) \Rightarrow (p \vee \neg q)$

$I = \{p \mapsto \bot, q \mapsto \bot\}$

$(\bot \wedge \bot) \Rightarrow (\bot \vee \neg \bot)$

$\bot \Rightarrow (\bot \vee \neg \bot)$

$\equiv \top$

$\therefore I \models F$

Satisfiability (SAT)

F is satisfiable iff there is an $I \models F$

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

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

1. Truth table (brute force)
2. SAT solvers
3. deductive proofs

semantic argument method

neg.

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

conj

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

disj

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

impl.

$$\frac{I \models F \Longrightarrow G}{I \models \neg F \quad \text{OR} \quad I \models G} \qquad \frac{I \not\models \overbrace{F \Longrightarrow G}^{\neg F \vee G}}{I \models F \quad I \not\models G}$$

contradiction

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

$\{\} \models \top$

$\{\} \models p \Rightarrow p$

assume F is VALID

$\rightsquigarrow$

$I \not\models F$

e.g. $I \not\models (p \wedge q) \Longrightarrow (p \vee \neg q)$

this means

$I \models (p \wedge q)$ $\quad$ $I \not\models (p \vee \neg q)$

$I \models p$

$I \models q$

$I \not\models p$

$I \not\models \neg q$

$I \models q$

contradiction

$\therefore$ there does not exist $I \not\models (p \wedge q) \Rightarrow (p \vee \neg q)$

So the formula is VALID

Two formulas are equivalent $F_1 \equiv F_2$

iff for all I, $I \models F_1$ iff $I \models F_2$

given a VALID solver, how can we show $F_1 \equiv F_2$

$F_1 \equiv F_2$ iff $F_1 \Leftrightarrow F_2$ is VALID

$(F_1 \Rightarrow F_2) \wedge (F_2 \Rightarrow F_1)$

Normal forms

① Negation normal form (NNF)

$$-(x+y) \longrightarrow -x-y$$

DeMorgan

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

$$\neg\neg F \longrightarrow F$$

② DNF disjunctive normal form

E.g.

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

$$F \longrightarrow DNF$$

③ Conjunctive normal form (CNF)

E.g.

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

we can distribute $\vee$ over $\wedge$

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

may cause an exponential explosion!

Tseitin's transformation

$$F \longrightarrow F' \text{ in CNF}$$

ideally

$$F \equiv F'$$

properties

1. if F' is UNSAT then F is UNSAT
2. any model of F' is a model of F if we disregard additional variables

$$\text{def } f(x, y, z):$$
$$\qquad \text{return } \underbrace{(x + \underbrace{(\underbrace{2*y}_{t_1} + 3)}_{t_2})}_{t_3}$$

$\downarrow$

```
def f'(x, y, z)
    t1 = 2*y
    t2 = t1 + 3
    t3 = t2 + x
    return t3
```

$\boxed{\text{SSA form}}$

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

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

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

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

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

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

1. for every subformula F_i create new variable t_i

2. for every F_i,

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

l_i: LHS of F_i

$\circ$: $\wedge, \vee$

l_i': RHS of F_i