

$\{P\} S \{Q\} \longrightarrow \text{verify} \longrightarrow \text{yes/no}$

Satisfiability formula  
in  
Boolean logic  $\longrightarrow \text{yes/no}$

propositional

Atoms :  $T, \perp, P, Q, R, S, \dots$

$\nearrow$   
true

$\nearrow$   
false

$\nearrow$   
NOT  
NEG

Literals : variable or its negation, e.g.  $P$  or  $\neg P$

Formula  $F ::= \text{literal}$

$| \neg F$

(NOT, negation)

$| F \wedge F$

(AND, conjunction)

$| F \vee F$

(OR, disjunction)

E.g.  $P \wedge \neg Q$

implication  $| F_1 \Rightarrow F_2$

$\neg F_1 \vee F_2$

bi-implication  $| F_1 \Leftrightarrow F_2$

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

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

How many interpretations are there?

$2^{\text{Var}}$

$P \Rightarrow Q \equiv \neg P \vee Q$		
P	Q	$\neg P \vee Q$
$\perp$	$\perp$	T
$\perp$	T	T
T	$\perp$	$\perp$
T	T	T

$I \models F$  if  $F$  evaluates to  $\perp$  under  $I$   
 *$I$  is a model of  $F$*

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

e.g.  $F \triangleq (p \wedge q) \Rightarrow (p \vee \neg q)$   
 $I = \{p \mapsto \perp, q \mapsto \perp\}$

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

$$\perp \Rightarrow (\perp \vee \neg \perp)$$

$$\equiv \top$$

$$\therefore I \models F$$

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.

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

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

conj

$$\frac{I \models F \wedge G}{I \models F \quad I \models G}$$

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

disj

$$\frac{I \models F \vee G}{I \models F \quad \text{OR} \quad I \models G}$$

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

impl.

$$\frac{I \models F \Rightarrow G}{I \models \neg F \quad \text{OR} \quad I \models G}$$

$$\frac{\neg F \vee G}{I \not\models F \Rightarrow G}$$
$$\frac{}{I \models F \quad I \not\models G}$$

$$\{\} \models \top$$

contradiction

$$\frac{I \models F \quad I \not\models F}{I \models \perp}$$

$$\{\} \models P \Rightarrow P$$

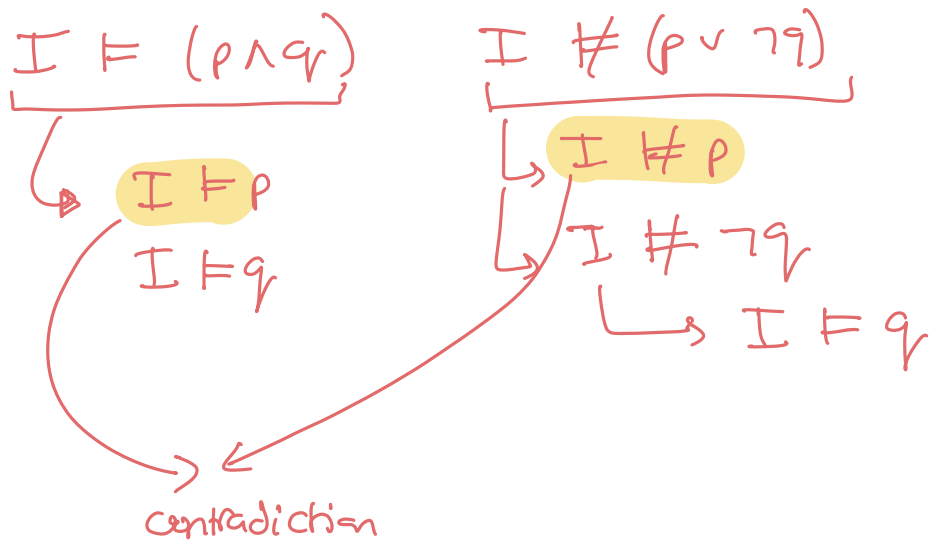
assume  $F$  is VALID

$$\begin{array}{c} \text{---} \\ \text{---} \\ \text{---} \\ \downarrow \\ I \models F \end{array}$$

e.g.

$$I \not\models (P \wedge Q) \Rightarrow (P \vee \neg Q)$$

this means



∴ 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)

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

DeMorgan

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

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

### ② DNF disjunctive normal form

$$\begin{aligned} \text{e.g.} \quad & (p \wedge q \wedge \neg r) \\ & \vee (\neg p \wedge \neg q \wedge \neg r) \\ & \vee (p \wedge q \wedge r) \\ & \vdots \end{aligned}$$

$$F \longrightarrow \text{DNF}$$

### ③ Conjunctive normal form (CNF)

$$\begin{aligned} \text{e.g.} \quad & (p \vee q \vee r) \\ & \wedge (p \vee \neg q \vee r) \\ & \wedge \vdots \end{aligned}$$

we can distribute  $\vee$  over  $\wedge$  } may cause an exponential explosion!

$$\begin{aligned} & r \vee (p \wedge q) \\ & (r \vee p) \wedge (r \vee q) \end{aligned}$$

## Tseitin's transformation

$F \longrightarrow F'$  in CNF

ideally

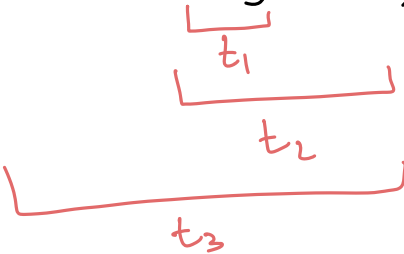
$$F \equiv F'$$

### 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

---

```
def f(x, y, z):  
    return (x + (2*y + 3))
```



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

SSA form

$$F \triangleq (p \wedge q) \vee (q \wedge \neg r \wedge s)$$

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

$$\begin{aligned}
 F'_1 &\triangleq t_1 \iff (p \wedge q) \\
 F'_2 &\triangleq t_2 \iff (q \wedge \neg r) \\
 F'_3 &\triangleq t_3 \iff (t_2 \wedge s) \\
 F'_4 &\triangleq t_4 \iff (t_1 \vee t_3) \\
 F' &= F'_1 \wedge F'_2 \wedge F'_3 \wedge F'_4 \wedge t_4
 \end{aligned}$$

① for every subformula  $F_i$  create new variable  $t_i$

② for every  $F_i$ ,

$$F'_i \triangleq t_i \iff (l_i \circ l'_i)$$

$\uparrow \quad \quad \uparrow$   
 $\text{LHS of } F_i \quad \quad \text{RHS of } F_i$