$\{P\}\ S\ \{Q\} \longrightarrow \varphi \longrightarrow \text{SAT} \longrightarrow$ yes

$\text{SAT} \longrightarrow$ No

propositional

FIRST-ORDER LOGIC

function relation relation

$$\exists y.\ \forall x.\quad x + y > 0 \ \wedge\ x > 5$$

existential quantifier universal

a language of FOL is $L(C, F, R)$

const functions relations

<u>Basic term</u>: either a constant $(c \in C)$ or a variable, $x, y, z, \ldots$

<u>Composite terms</u>: $f \in F$

$f(t_1, t_2, \ldots, t_k)$

f has arity k

<u>formulas</u>:

- atomic predicate $p(t_1, \ldots, t_n)$
  $p \in R$ where p has arity n

  e.g. older(x, y)

- $F_1 \wedge F_2$, $F_1 \vee F_2$, $\neg F_1$

- given variable x, $\underbrace{\exists x. F}_{\text{scope of } x}$ $\underbrace{\forall x. F}_{\text{scope of } x}$ | analogy $\lambda x. t$

E.g. $\forall y. ((\forall x. p(x)) \implies q(x, y))$

free variable

a formula is closed iff it doesn't have free variables

sentence

ground formula — has no variables

$p(0, 1)$

E.g. $\forall x. \exists y. \text{friend}(x, y)$

$\exists x. \forall y. \text{friend}(x, y)$

Semantics

① universe $\mathcal{U}$: a non-empty set of objects

$\mathcal{U} = \mathbb{Z}$

$\mathcal{U} = \mathbb{Z} \cup \mathbb{C}$

$\mathcal{U} = \{\square, \triangle, \bigcirc\}$

② An interpretation I is a mapping from C, F, R to objects from $\mathcal{U}$

I maps $c \in C$ to $\mathcal{U}$, i.e. $I(c) \in \mathcal{U}$

I maps $f \in F$ to $I(f) \in \mathcal{U}^n \to \mathcal{U}$

where f has arity n

I maps $p \in R$ to $I(p) \subseteq \mathcal{U}^k$

where p has arity k

E.g. $C = \{a, b, c\}$

$F = \{f\}$ binary

$R = \{p\}$ ternary

Universe $\mathcal{U} = \{1, 2, 3\}$

interpretation $I(a) = 1$, $I(b) = 2$, $I(c) = 3$

$I(f) = \{1 \mapsto 2, 2 \mapsto 3, 3 \mapsto 1\}$

$I(p) = \{(1,2,3), (3,2,1)\}$

Structure $S = (\underbrace{\mathcal{U}}_{\text{universe}}, \underbrace{I}_{\text{interp}})$

a variable assignment σ is a map from variables to elements of $\mathcal{U}$

A formula F is SAT iff there is a structure S and σ s.t. $S, \sigma \models F$

e.g. $\forall x. \exists y. \ p(x,y)$

$U = \mathbb{Z}$

$I(p) = \{(x,y) \mid x+y>0\}$

$S = (U, I)$ $\qquad S \models \forall x. \exists y. \ p(x,y)$

$U = \{0\}$

$I(p) = \{(0,0)\}$

$U = \{0\}$

$I(p) = \{\ \}$ $\qquad (U, I) \not\models \forall x. \exists y. \ p(x,y)$

e.g. $\forall x. \left(p(x,x) \Rightarrow \exists y. \ p(x,y)\right)$

$U = \mathbb{Z}$

$I(p) = \{(x,y) \mid x+y>0\}$

consider $a \in U$

if $p(a,a)$ is false

if $p(a,a)$ is true this means $\exists y. p(a,y)$

FOL theories

a theory T

① $\Sigma_T = (C_T, F_T, R_T)$

② axioms A_T : a set of sentences in Σ_T

e.g.

$\Sigma_T = (\emptyset, \emptyset, \{taller\})$

axiom: $\forall x, y.\ taller(x, y) \implies \neg taller(y, x)$

$U = \{A, B\}$

$I(taller) = \{(A, B)\}$

$(U, I) \models$ axiom

(U, I) is a T-model

$T_=$ theory of equality

$$\Sigma_= = \{ =, \dots \}$$

predicate

axioms $A_=$

$$\forall x.\ x = x$$

$$\forall x, y\ \ x = y \implies y = x$$

$$\forall x, y, z.\ x = y \wedge x = z \implies y = z$$

e.g. $U = \{ \circ, \bullet \}$

$$I(=) = \{ (\circ,\circ), (\bullet,\bullet) \}$$

$$I(=) = \{ (\circ,\circ), (\bullet,\bullet), (\circ,\bullet), (\bullet,\circ) \}$$

T_{PA}

$$\Sigma_{PA} = \{ 0, 1, +, \cdot, = \}$$

axioms $\forall x.\ \neg(x + 1 = 0)$

$$\forall x.\ x + 0 = x$$

$$\forall x, y.\ x + 1 = y + 1 \implies x = y$$

$$\forall x, y.\ x + (y + 1) = (x + y) + 1$$

$$\forall x, y.\ x \cdot (y + 1) = x \cdot y + x$$

+ infinite set of axioms to define induction

Presburger arithmetic (throw away multiplication)

Theory of arrays

$$a[i]$$

$$a(i \leftarrow v)$$

$$a(2 \leftarrow 5)[2] = 5$$

$$\forall a, i, j \,.\; i = j \Longrightarrow a[i] = a[j]$$

$$\forall a, v, i, j \,.\; i = j \Longrightarrow a(i \leftarrow v)[j] = v$$

$$\forall a, v, i, j \;\; i \neq j \Longrightarrow a(i \leftarrow v)[j] = a[j]$$