First Order Logic

Consider decomposing statements into **objects** & **properties** of objects

if all men are mortal & I am a man, then I am mortal

men: object; mortal: property; man: object; mortal: property

if $\forall x\,(M(x))$ & $y = x$, then $M(y)$

Predicate Symbols

("properties"; give statements true / false value)

$\boxed{=}$ $\quad \forall x, y, z : \; (x = y \;\&\; y = z) \implies x = z$

$\boxed{\leq}$ $\quad \forall x, y : \; (x \leq y \;\&\; y \leq x) \implies x = y$

Ex:

Statement → FOL

Statement: $\boxed{\text{at least 3 people in the room}}$ $\quad$ $\boxed{\text{at most 3 people in the room}}$

$x_1, x_2, \dots$: people

$R(x)$: 'x is in the room'

FOL:

$$\boxed{\begin{array}{l} \exists x_1, x_2, x_3 : \\ R(x_1), R(x_2), R(x_3) \;\wedge\; \neg(x_1 = x_2 = x_3) \end{array}}$$

$$\boxed{\begin{array}{l} \forall x_1, x_2, x_3, x_4 : \qquad \text{2 must be the same} \\ R(x_1) \wedge R(x_2) \wedge R(x_3) \wedge R(x_4) \implies (x_1 = x_2 \vee x_1 = x_3 \vee x_1 = x_4 \vee \dots) \end{array}}$$

Ex: (number theory)

Statement → FOL

Statement: $\boxed{x + y = y + x}$ $\quad$ $\boxed{x \text{ is Prime}}$

$=$ $\quad$ predicate symbols $\quad$ $=$

$f : +$ $\quad$ function-symbols $\quad$ $g : \cdot$

FOL: $\boxed{\forall x, y : \; f(x,y) = f(y,x)}$ $\quad$ $\boxed{\forall y, z \; [\, g(y,z) = x \rightarrow (y = x \vee z = x) \,]}$

Ex: (set theory)

Statement → FOL

Statement: $\boxed{X \subseteq Y}$ $\quad$ $\boxed{X = Y \cup Z}$

predicate symbols : $M(x, y) \equiv x \in y$

FOL: $\boxed{\forall z, \; M(z, x) \implies M(z, y)}$ $\quad$ $\boxed{\forall t, \; (M(t,x) \iff M(t,y) \vee M(t,z))}$

SYNTAX

F.O.L = collection of languages $\begin{cases} L_1 & \text{(number theory)} \\ L_2 & \text{(set theory)} \\ \vdots & \text{(people in the room)} \end{cases}$

Language Independent Symbols (occur in every F.O.A language)

1. Logical Symbols : $($, $)$, $\rightarrow$, $\neg$, $\wedge$, $\vee$, $\forall$, $\exists$
   Shorthand for $\neg \forall \neg$
2. Variables : x_1, x_2, x_3, ...
3. Relation : '$=$'

Language Specific Symbols

1. Constants : $a_0, b_0, a_1, b_1, \ldots$ (set value)
2. Relations : $\leq$, $R(\,)$, $P(\,)$, ... (give the statement a truth value)
3. Functions : $F(\cdot)$, $G(\cdot)$, ... (don't give the statement a truth value)

Vocabulary defines a language

$L = \langle \{\text{constants}\}, \{\text{relations}\}, \{\text{Functions}\} \rangle$

Empty Language $L = \langle \, \rangle$

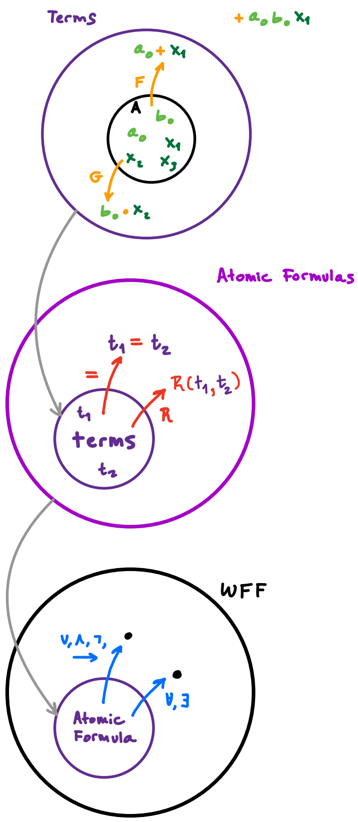
- only language independent symbols
  - terms : $x, y, \ldots$
  - atomic formulas : $x = y, \ldots$
  - WFF : $\forall x \forall y (x = y)$, $\forall x \exists y \neg (x = y)$, ...

Terms (objects of a Language)

Terms = I(x, A, P)

Variables
Constants

Functions



Atomic Formulas terms + relations

Atomic Formulas = I(X , terms , relations)

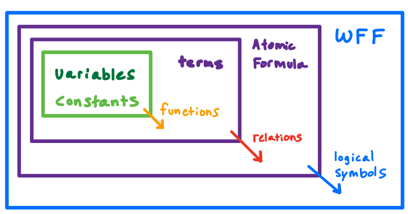
1) $R(t_1,t_2)$

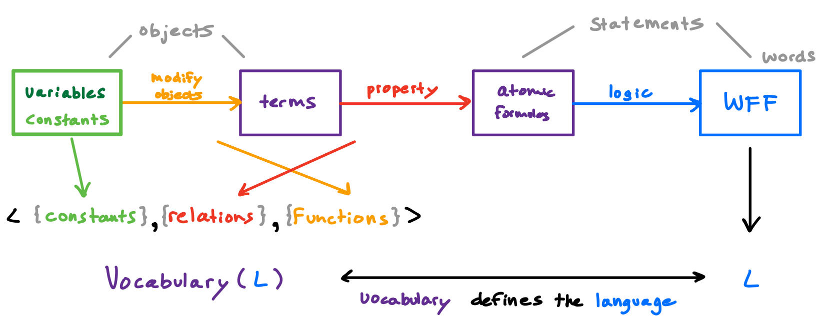
2) $t_1 = t_2$

WFF (words of a FOL)

WFF = I(X, atomic formulas, Logical Symbols)

Summary





EX

$$\underbrace{\forall x\ (\underbrace{\overbrace{F(x,S(y))}^{\text{term}} \overset{\text{relation}}{=} \overbrace{S(F(x,y))}^{\text{term}}}_{\text{atomic Formula}})}_{\text{WFF}}$$

Free/Bound Variables

Free	Bound
Not bound by $\forall, \exists$	"Captured" by $\forall, \exists$

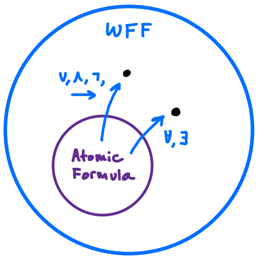
Notation: $\mathrm{Fr}(\overset{\text{WFF}}{\alpha}) = \{\text{free variables in } \alpha\}$

Free

(defined inductively)

For $\alpha \in \text{WFF}$

α	$\mathrm{Fr}(\alpha)$
Atomic	all variables in α
$\beta \to \gamma$ $\beta \wedge \gamma$ $\beta \vee \gamma$	$\mathrm{Fr}(\beta) \cup \mathrm{Fr}(\gamma)$
$\neg\beta$	$\mathrm{Fr}(\beta)$
$\forall x \beta$	$\mathrm{Fr}(\beta) \setminus \{x\}$



Sentence

WFF w/ no free variables

(already have T/F value without an assignment)

Semantics

Structures

Vocabulary
$L = \langle a, R, \bar{F} \rangle$

$\underbrace{a, R, F}_{\text{Symbols (no meaning)}}$

$\longrightarrow$

Structure
$M = \langle U^M, \bar{a}, \bar{R}, \bar{F} \rangle$

$\underbrace{\bar{a}, \bar{R}, \bar{F}}_{\text{Interpretation of Symbols}}$

$U^M \downarrow$ **Universe** Domain of the variables\quantifiers ($\forall, \exists$)

$M \models \alpha$

$M \models \alpha$: The structure <u>satisfies</u> the formula

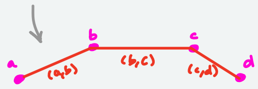
(M = structure, $\models$ = satisfies, α = formula)

EX

$L = \langle \phi, R(\cdot,\cdot), \phi \rangle$

$\alpha = \forall x, \exists y (R(x,y))$

M	Meaning	$M \models \alpha$?
$\langle \mathbb{N}, \leq \rangle$	$\forall x, \exists y \ (x \leq y)$	$M_1 \models \alpha$
$\langle \mathbb{N}, \geq \rangle$	$\forall x, \exists y \ (x \geq y)$	$M_2 \models \alpha$
$\langle \{a,b,c,d\}, \{(a,b),(b,c),(c,d)\} \rangle$	$\forall x, \exists y \ ((x,y))$	$M_3 \not\models \alpha$



EX

$L = \langle a, b, R(\cdot,\cdot), F(\cdot,\cdot), G(\cdot,\cdot) \rangle$

$\alpha = \forall x, \exists y (F(y,y) = x)$

M	Meaning	$M \models \alpha$?
$\langle \mathbb{N}, 0, b, \leq, +, \cdot \rangle$	$\forall x, \exists y (y + y = x)$	$M_1 \not\models \alpha$
$\langle \mathbb{R}, 0, b, \leq, +, \cdot \rangle$	$\forall x, \exists y (y + y = x)$	$M_2 \models \alpha$

If α has free variables, the structure isn't enough.

We need to define T/F for all <u>free variables</u> in α

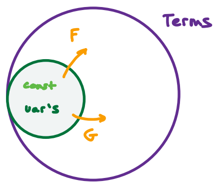
$\boxed{\text{Assignment for } M}$

$\boxed{s}$ s : variables $\longrightarrow U^M$

$\boxed{\bar{s}}$ $\bar{s}$: terms $\longrightarrow U^M$

For $t \in I$ (const's $\cup$ vars , Functions)

t	$\bar{s}(t)$
a	$\bar{a}$
x	$s(x)$
$F(t_1, \dots, t_n)$	$\bar{F}(\bar{s}(t_1), \dots, \bar{s}(t_n))$



EX

$$\alpha = F(G(x), H(y))$$

$$\bar{s}(\alpha) = F(\bar{s}(G(x)), \bar{s}(H(y)))$$

$$G(\bar{s}(x)) \quad H(\bar{s}(y))$$

$$s(x) \quad s(y)$$

$$3 \quad 7$$

$\boxed{M \models_s \alpha}$

For $\alpha \in I$ (Atomic Forms , Logicals)

α	$M \models_s \alpha \iff$
$t_1 = t_2$	$\bar{s}(t_1) = \bar{s}(t_2)$
$R(t_1, \dots, t_n)$	$R(\bar{s}(t_1), \dots, \bar{s}(t_n))$
$\beta \vee \gamma$	$M \models_s \beta \;\vee\; M \models_s \gamma$
$\beta \wedge \gamma$	$M \models_s \beta \;\wedge\; M \models_s \gamma$
$\beta \to \gamma$	$M \models_s \beta \;\to\; M \models_s \gamma$
$\forall x \beta$	$\forall d \in U^M,\ M \models_{s^x_d} \beta$

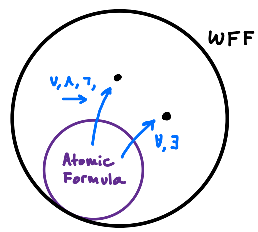
Atomic Formulas

WFF

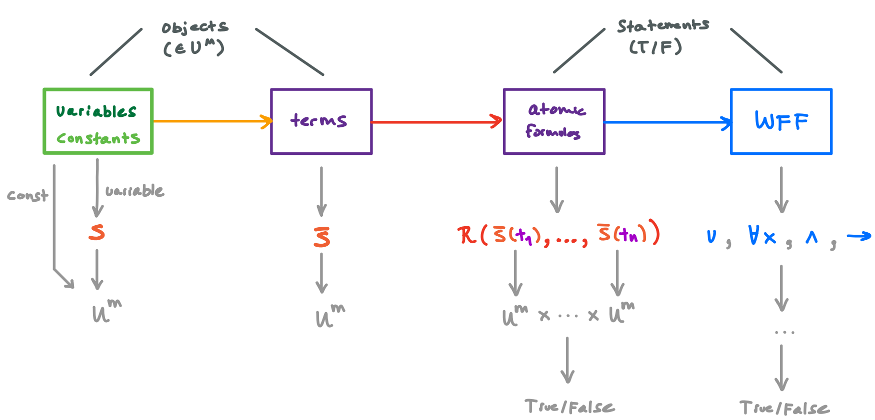
$\equiv \forall d \in U^M,\ M \models_s \beta[{}^x_d]$

For any <u>value</u> in U^M

when we assign x to that value β is satisfied



<u>Summary</u>



$\boxed{\alpha}$

	has free variables	Sentence
meaning of α depends on:	① M ② s for free variables	① M
α is satisfied:	$\boxed{M \models_s \alpha}$	$\boxed{M \models \alpha}$
$\boxed{M \models_{s_1} \alpha \iff M \models_{s_2} \alpha}$	if $\boxed{\forall x \in F_r(\alpha),\ s_1(x) = s_2(x)}$ Two assignments assign the same value to every free variable	Always $\forall s_1, s_2$

Notation: $F_R(\alpha) = \{x_1, \dots, x_k\}$

$$x_1 \to s(x_1), \quad x_k \to s(x_k)$$

$$M \models_s \alpha \iff M \models \alpha[a_1, \dots, a_k]$$

Ex:

$\alpha = \forall x, R(x,y)$ $M = \langle \mathbb{N}, \leq \rangle$	y is free x is bound $\therefore$ only care ab y
$s_1(x) = 3 \quad s_1(y) = 5$	$M \not\models_{s_1} \alpha$
Now consider s_2: $s_2(x) = 7 \quad s_2(y) = 5$	$M \not\models_{s_2} \alpha$ Since $s_1(y) = s_2(y)$

Ex:

$L = \langle a, R(\square,\square) \rangle$
$M = \langle \mathbb{N}, 0, \leq \rangle$
$\alpha = \forall x\, R(a,x)$

$M \models \forall x\, R(a,x)$	$(0 \leq x)$	no assignments are needed
$M \not\models \forall x\, R(x,a)$	$(x \leq 0)$	

Ex:

$\alpha = \forall x, R(x,y) \rightarrow R(x,z)$ $M = \langle \mathbb{N}, \leq \rangle$	$\{y, z\}$ is free x is bound
$s(y) = 5 \quad s(z) = 5$	$M \models_s \alpha$

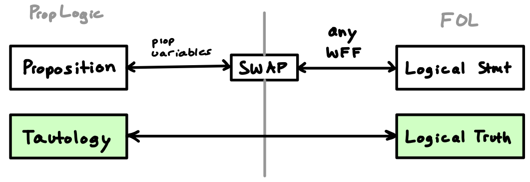
Ex:

$M = \langle \mathbb{N}, \leq \rangle$ $\alpha = \forall x, R(x,y) \rightarrow R(x,z)$	$\alpha[3,5] = \forall x, x \leq 3 \rightarrow x \leq 5$ $M \models \alpha[3,5]$

Ex:

$L = \langle F(\cdot,\cdot) \rangle$ $M = \langle \mathbb{N}, + \rangle$ $\alpha = \exists x, F(x,y) = z$	For what (n,m) does $M \models \alpha[n,m]$ $\{(n,m) : M \models \alpha[n,m]\}$ $= \{(n,m) : n \leq m\}$

Prop Logic $\rightleftharpoons$ FOL



Ex:

prop variables

tautology $((p_1 \to p_2) \to (p_2 \to p_1))$

$p_1 \rightleftharpoons \alpha$
$p_2 \rightleftharpoons \beta$

logical truth $((\alpha \to \beta) \to (\beta \to \alpha))$

any WFF

Ex:

Is $\alpha = \exists x\,(P(x) \to \forall x\, P(x))$ a logical truth

<u>2 Cases:</u>

① $M \models \forall x P(x)$

$\therefore\ \exists x\,(P(x) \to \overset{T}{\forall x P(x)})$

By Truth Table of '$\to$' : $(P(x) \to T)$ is true, $\forall x$

$\therefore\ \alpha$ is always true (in this case)

so $M \models \alpha$

② $M \not\models \forall x P(x)$

$\therefore\ \exists x\,(P(x) \to \overset{F}{\forall x P(x)})$

But $M \not\models \forall x P(x) \implies \forall d \in U^M,\ M \models_{s^x_d} P(x)$

$\implies M \not\models_{s^x_x} P(x)$

$\implies M \not\models P(x)$

$\therefore\ \exists x\,(\underbrace{\overset{F}{P(x)} \to \overset{F}{\forall x P(x)}}_{T})$ By Truth Table of '$\to$'

$\therefore\ \alpha$ is always true (in this case)

so $M \models \alpha$

$M \models \alpha$ (always) $\implies \alpha$ is a logical truth

Semantic Notions

Satisfies

Sentence (α) :

$\exists M : M \models \alpha$

$\boxed{\alpha \text{ is Satisfiable}}$ $\exists M, \exists s : M \models_s \alpha$

Sentence (α) :

$\forall M : M \models S$

$\boxed{\Sigma \text{ is Satisfiable}}$ $\exists M, \exists s : \forall \beta \in \Sigma, M \models_s \beta$

Logical Truth

$\forall M, \forall s : M \models_s \alpha$

Logical Implication

$\boxed{\alpha \models \beta}$ $\forall M, \forall s : \quad M \models_s \alpha \implies M \models_s \beta$

$\boxed{\Sigma \models \beta}$ $\forall M, \forall s : \quad \forall \alpha \in \Sigma, M \models_s \alpha \implies M \models_s \beta$

{WFF} WFF

EX

Σ	$\Sigma \models$
$\{\alpha, \alpha \to \beta\}$	β
$\{\forall x \alpha\}$	α
$\{\forall x\, \alpha, \forall x (\alpha \to \beta)\}$	β

Defines

A WFF α <u>defines</u> a <u>set</u> that will satisfy α :

given: M

Defines a set $\subseteq U^M$

not given: M

Defines a <u>set of structures</u>

Within M

1 free Variable

$Fr(\alpha) = \{x\}$

α **defines** $A = \{a \in U^M : M \models \alpha[a]\}$

What we can assign $Fr(\alpha)$ to make $M \models \alpha$ true

2+ free Variables

$Fr(\alpha) = \{x_1, \dots, x_k\}$

α **defines** $A = \{\underbrace{(a_1, \dots, a_K)}_{K\text{-tople}} \subseteq (U^M)^K : M \models \alpha[a_1, \dots, a_K]\}$

How to | Find A from α

$M = \langle \cdots \rangle$

$\alpha = \cdots$

① "Solve" α ; for what values of x is $\alpha[x]$ true?

How to | Find α from A

$M = \langle \cdots \rangle$

$A = \{\cdots\}$

① Find a property that holds only for all $a \in A$

② Express this property as a formula (α)

1 Free Variable

Ex: Find A from α

$L = \langle F(\square,\square) \rangle$

$\alpha = \exists x\, F(x,x) = y \qquad F_r(\alpha) = y$

Case	M	α	A
1	$\langle \mathbb{R}, \cdot \rangle$	$\alpha = \exists x(x^2 = y)$	$A = \{y : \exists x(x^2 = y)\}$ $= \{y \in \mathbb{R} : y \geq 0\}$ — $\mathbb{R}$ w/ a square root
2	$\langle \mathbb{N}, + \rangle$	$\exists x\,(2x = y)$	$A = \{y : \exists x\,(2x = y)\}$ $= \{\text{even } \mathbb{N}\}$

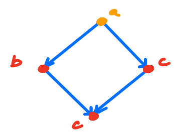
Ex: Find α from α

$L = \langle R(\square,\square) \rangle$

$A = \{a\}$

Find α that defines the set A

① $M = \langle \{\overset{\text{vertex}}{a,b,c,d}\}, \{\overset{\text{edge}}{(a,b),(b,d),(a,c),(c,d)}\} \rangle$



Step 1: Find a property that holds only for $\{a\}$

Property: no incoming edge

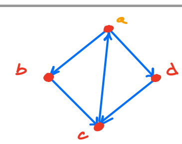
Step 2: Express this property as a formula (α)

$\alpha = \neg \exists x\, R(\underset{\text{from}}{x}, \underset{\text{to}}{y})$

Result:

$\left.\begin{array}{l} \alpha[a] = \neg \exists x\, R(x,a) \\ M \models \alpha[a] \end{array}\right\}$ α defines $A = \{a\}$

② $M' = \langle \{\overset{\text{vertex}}{a,b,c,d}\}, \{\overset{\text{edge}}{(a,b),(b,d),(a,c),(c,d)}\} \rangle$ *



Note: previous property does not hold

Step 1: property: 2 outgoing edges

Step 2: $\alpha = \exists x_1 \exists x_2\, (\neg x_1 = x_2 \wedge R(y,x_1) \wedge R(y,x_2))$

Result:

$\left.\begin{array}{l} \alpha[a] = \alpha = \exists x_1 \exists x_2\, (\neg x_1 = x_2 \wedge R(a,x_1) \wedge R(a,x_2)) \\ M' \models \alpha[a] \end{array}\right\}$ α defines $A = \{a\}$

2+ Free Variables

Ex: Find A from α

$M = \langle \mathbb{N}, \cdot \rangle$

$L = \langle F(\square,\square) \rangle$

$\alpha = \exists x\, F(x,y) = z \qquad F_r(\alpha) = \{y, z\}$

What is the set (A) that α defines in this M?

$A = \{(y,z) : M \models \alpha[y,z]\}$

$= \{(y,z) : \exists x\; xy = z\}$

$= \{(y,z) : \exists x\; x = \frac{z}{y}\}$

$= \{(y,z) : y \text{ divides } z\}$

Defining {Structures}

Given: $F_r(\alpha) = \emptyset$

makes sense only if α has no free variables

$\alpha \xrightarrow{\text{defines}} W = \{M : M \models \alpha\}$

Note:

1. Every $M \in W$ satisfies α
2. Every $M \notin W$ does not satisfy α

Defining {Structures} w/ Σ

Given: $F_r(\alpha) = \emptyset \quad \forall \alpha \in \Sigma$

makes sense only if α has no free variables

$\Sigma \xrightarrow{\text{defines}} W = \{M : M \models \Sigma\}$

Ex: Find W from Σ

$\Sigma = \{\alpha_1, \alpha_2 \dots \alpha_n\}_{n \in \mathbb{N}}$ (infinite set)

$\alpha_1 = \exists x_1 [x_1 \neq x_2 \wedge x_1 \neq x_2 \wedge \dots \wedge x_1 = x_k]$

$\alpha_2 = \exists x_1 \exists x_2 [x_1 \neq x_2 \wedge x_1 \neq x_2 \wedge \dots \wedge x_1 = x_k \wedge x_2 \neq x_1 \wedge x_2 \neq x_2 \wedge \dots \wedge x_2 = x_k]$

$\vdots$

$\alpha_k = \exists x_1 \exists x_2 \dots \exists x_k [x_i \neq x_j : i \neq j] = \alpha_1 \wedge \alpha_2 \wedge \dots \wedge \alpha_{k-1}$

Σ defines $W = \{$ infinite structures $\}$

(M can satisfy all the members of Σ if & only if it is infinite)

because α_n says there are at least n-elements & n can be infinite.

Defining Structures with just a Relation

$L = \langle R(\dots) \rangle$

$\downarrow$

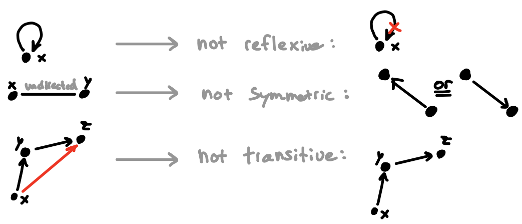
$M = \langle U^M, R^M(\dots) \rangle$

By defining $W = \{M : M \models \alpha\}$, we are essentialy defining:

$W = \{ M :$ M has relation R^M (that has some properties) $\}$

Classifying Relations

Reflexive	$\forall x\, R(x,x)$
Symmetric	$\forall x \forall y\; R(x,y) \to R(y,x)$
Transitive	$\forall x \forall y \forall z\; [R(x,y) \wedge R(y,z) \to R(x,z)]$



Equivalence Relation

- Reflexive
- Symmetric
- Transitive

Ordering

A 2 place relation $(R(\cdot,\cdot))$ that orders elements in U^M

$<$ $\leq$

Strict Order

- not reflexive
- not symmetric
- transitive

Non-Strict Order

- reflexive
- not symmetric
- transitive

Linear every pair of elements is comparable by R

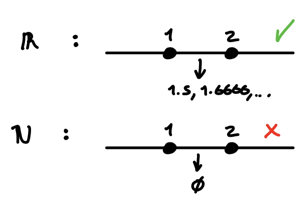
$\forall x \forall y\; (R(x,y) \vee R(y,x))$

Linear + Strict

$\forall x \forall y\; (\neg x = y \to (R(x,y) \vee R(y,x)))$

Dense Between any 2 elements, there's another element

$\forall x \forall y\; [R(x,y) \to \exists z (R(x,z) \vee R(z,y))]$



$L = \langle R(\cdot,\cdot) \rangle$

Example 1

Find Σ that defines : $W = \{ M : R^M$ is a <u>strict order relation</u> of $U^M \}$

<u>Strict order relation</u>

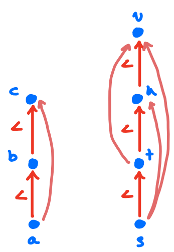
① non-reflexive: $\forall x : \neg R(x,x)$

② non-symetric: $\forall x, \forall y : R(x,y) \rightarrow \neg R(y,x)$

③ Transitivity: $\forall x, \forall y, \forall z : R(x,y) \wedge R(y,z) \rightarrow R(x,z)$

$\Big\}$ $\Sigma = \{ ①, ②, ③ \}$ defines W

<u>ie</u>: $M = \langle \{a,b,c,s,t,u,v\}, \{ab, bc, ac, st, su, sv, tu, tv, uv\} \rangle$



<u>Strict Order</u>:

① $a \nless a$ ✓ $\therefore M \models ①$

② $b < a \longrightarrow a \nless b$ ✓ $\therefore M \models ②$

③ $b < a$ & $c < b \longrightarrow c < a$ ✓ $\therefore M \models ③$

$\Big\}$ $M \models \Sigma$

Example 2

$\Sigma = \{ ①, ②, ③, ④ \}$ defines : $W = \{ M : R^M$ is a <u>linear, strict ordering</u> of $U^M \}$

④ $\downarrow$

$$\forall x, \forall y \; [\underbrace{R(x,y) \vee R(y,x)}_{\text{they're comparable}} \vee x = y]$$

$x=y$: or they're the same (not comparable)

Example 3

$\Sigma = \{ ①, ②, ③, ④, ⑤ \}$ defines : $W = \{ M : R^M$ is a <u>dense, linear, strict ordering</u> of $U^M \}$

⑤ $\downarrow$

$$\forall x \forall y \; [R(x,y) \rightarrow \exists z (R(x,z) \vee R(z,y))]$$

Example 4

What will these formulas say about the ordering?

$\exists x \, [\forall y \, (x = y \vee \underbrace{R(x,y)}_{x<y})]$

"There's a smallest element"

$\forall y \, [\exists x \, (R(x,y))]$

"There's no smallest element"

Defining Structures with just a Function

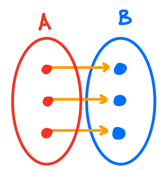
$L = \langle F(\cdot) \rangle$

Example 1

Find Σ that defines : $W = \{ M : F^M$ is $\underline{\text{one-to-one}}$ & $\underline{\text{not onto}} \}$

bijective

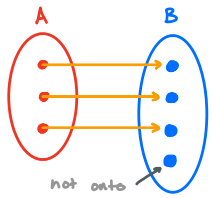
ie : $F : A \to B$



$\underline{\text{one-to-one}}$: F doesn't map different elements to the same value

$\underline{\text{onto}}$: range of $F = B$

$\underline{\text{one-to-one}}$ & $\underline{\text{not onto}}$:



① $\underline{\text{one-to-one}}$: $\forall x \forall y \, [F(x) = F(y) \to x = y]$

$\underline{\text{onto}}$: $\forall y \, \exists x \, [F(x) = y]$

② $\underline{\text{not onto}}$: $\exists y \, \forall x \, [\neg (F(x) = y)]$

$\Sigma = \{ ①, ② \}$ defines W

What structure(s) $M = \langle U^M, F^M \rangle$ satisfy $\Sigma = \{ ①, ② \}$?

$\underline{\text{Ex}}$: $M = \langle \mathbb{N}, x \to x+1 \rangle$

① $\underline{\text{one-to-one}}$: any $\mathbb{N} + 1$ is another unique $\mathbb{N}$

② $\underline{\text{not onto}}$: can't get $F(x) = 0$ for any x

Example 2

Find α that defines $W = \emptyset$

=> no structure satisfies it

=> α is a contradiction

$\underline{\text{ie}}$: $\alpha = \neg \forall x \, (x = x)$

Example 3

Find α that defines $W = \{ \text{all structures} \}$

=> every structure $M = \langle U^M, F^M \rangle$ satisfies it

=> α is a logical truth

$\underline{\text{ie}}$: $\alpha = \forall x \, (x = x)$

Defining $\mathbb{N}$

How do we define $W = \{ M : \text{behaves like } \mathbb{N} \}$

<u>Language for $\mathbb{N}$</u>

$L = \langle \{a, b\}, \{F(\cdot,\cdot), G(\cdot,\cdot), S(\cdot)\} \rangle$

our intentions

$M_{\mathbb{N}} = \langle \{ \{0,1,2,\dots\}, \{0, 1\}, \{+, \times, x \mapsto x+1\} \} \rangle$

STEP 1 Arithmetic

$\Sigma_0 = \{ \text{Axioms (Rules) of arithmetic} \}$ (Basic Properties of natural Numbers)

Includes (but not limited to):

1) $\forall x \forall y [F(x,y) = F(y,x)]$ — addition is commutative : $x+y = y+x$

2) $\forall x \forall y [G(x,y) = G(y,x)]$ — multiplication is commutative : $xy = yx$

3) $\forall x [F(a,x) = x]$ — $0 + x = x$

4) $\forall x \forall y [F(x, S(y)) = S(F(x,y))]$ — $x+(y+1) = (x+y)+1$

5) $\forall x \forall y [G(x, S(y)) = F(G(x,y), x)]$ — $x \cdot (y+1) = xy + x$

6) $\forall x \forall y \forall z [G(z, F(x,y)) = F(G(z,x), G(z,y))]$ — $z \cdot (x+y) = zx + zy$

7) $\forall x (\neg (S(x) = x))$ — Infinite Universe

STEP 2 Induction

key property of $\mathbb{N}$: we can do proof by induction on formulas using $\mathbb{N}$

<u>Claim</u>: $\forall x$: $\alpha[x]$ holds

Induction on $\mathbb{N}$

Base $x = 0$: Does $\alpha(0)$ hold?

Inductive Step $x \geq 0$: Assume $\alpha(x)$ holds. Does $\alpha(x+1)$ hold?

Result: $\alpha(x)$ holds $\forall x$

$\alpha[a] \wedge \forall x\, \alpha[x] \rightarrow \alpha[S(x)] \rightarrow \forall x\, \alpha[x]$

a: 0 $\quad$ $S(x)$: $x+1$

Induction Principle

$$I(\alpha) \;=\; \alpha[a] \wedge \forall x\,[\alpha[x] \to \alpha[s(x)]] \;\to\; \forall x\,\alpha[x]$$

exactly 1 free variable (x)

Note: $M_N \vDash I(\alpha)$ ($I(\alpha)$ is a logical truth for any α)

EX

$\alpha = \exists y\,(F(G(x,x),x) = F(y,y))$

$= \exists y\,(x^2 + x = 2y)$ — in our structure

$=$ "$x^2 + x$ is always even"

$I(\alpha) = \alpha[a] \wedge \forall x\,[\alpha[x] \to \alpha[s(x)]] \to \forall x\,\alpha[x]$

$\alpha[a]$: $\exists y\,(F(G(a,a),a) = F(y,y))$ $\downarrow$ $\exists y\,(0 = 2y)$ $\downarrow$ True

$\alpha[x]$: $\forall x \exists y\,(F(G(x,x),x) = F(y,y))$ $\downarrow$ $\exists y\,(x^2 + x = 2y)$ $\downarrow$ True

$\alpha[s(x)]$: $\exists y\,(F(G(s(x),s(x)),s(x)) = F(y,y))$ $\downarrow$ $\exists y\,((x+1)^2 + (x+1) = 2y)$ $\downarrow$ True

$\forall x\,\alpha[x]$ $\downarrow$ True

True $\to$ True

$\downarrow$

True

EX

$\beta[x] = \exists y\,[F(y, F(y,y)) = x]$

$= \exists y\,[3y = x]$ — in our structure

$=$ " x is divisible by 3"

$I(\beta) = (a \text{ is divisible by } 3) \wedge \forall x\,[(x \text{ is divisible by } 3) \to (x+1 \text{ is divisible by } 3)] \to \forall x\,(x \text{ is divisible by } 3)$

$(a \text{ is divisible by } 3)$ $\downarrow$ True

$(x \text{ is divisible by } 3) \to (x+1 \text{ is divisible by } 3)$:

True $\to$ False

False $\to$ True

$\underbrace{\qquad\qquad}_{\text{False}}$

$\forall x\,(x \text{ is divisible by } 3)$ $\downarrow$ False

False $\to$ False

$\downarrow$

True

$I(\beta)$ is True. Even though $\forall x\,\beta[x]$ is not.

STEP	3	Combine

Peano Arithmetic:

$$PA \;=\; \Sigma_0 \,\cup\, \{I(\alpha) : \alpha \text{ has 1 free variable } x\}$$

Σ_0: Axioms of Arithmetic

$\{I(\alpha)\}$: Induction Principle

PA is the set of Axioms which describes/defines $\mathbb{N}$

you can prove things about natural numbers using PA

Note

PA defines a set of structures which behave 'like' $\mathbb{N}$, not just' our desired M_N

ie: If we make $U^M = \mathbb{N} \cup \mathbb{N} \cup \mathbb{N} \cup \mathbb{N} \cup \mathbb{N}$

Then it's a different structure which still satisfies PA

Defining Within a Structure

(M is given and α has free variables)

$$\alpha[\overbrace{x_1,\dots,x_k}^{\text{Free Variables}}] \xrightarrow{\text{defines}} \underbrace{R^M(\dots)}_{k\text{-place}} \text{ in } M \iff \{s : M \models_s \alpha\} = \{s : R^M(s(x_1),\dots,s(x_k)) \text{ is satisfied}\}$$

EX ADDING Order to M_N w/ a Formula

$$L = \langle \{\overset{0}{a},\overset{1}{b}\}, \{\overset{+}{F(\cdot,\cdot)}, \overset{\times}{G(\cdot,\cdot)}, \overset{x \to x+1}{S(\cdot)}\} \rangle$$

(no order)

↓ define order in M_N w/ a formula

$$\alpha[x,y] \equiv \exists z(\neg(z=a) \land F(x,z)=y)$$

$z \neq 0 \lor x+z=y$

there's a non-zero # z that we can add to x to get y $\longrightarrow x < y$

"defines the order" in $\mathbb{N}$

defines an ordering (set of ordered pairs) in M

$$\{s : M \models_s \alpha[x,y]\} = \{s : s(x) < s(y)\}$$

EX

Find $\alpha[x]$ that defines: $\{r \in \mathbb{R} : r \geq 0\}$ in $M = \langle \mathbb{R}, \{0,1\}, \{+,\times, x \to x+1\}\rangle$

$$\alpha[x] = \exists y(G(y,y) = x)$$

$y^2 = x$

$y = \sqrt{x}$

$\alpha[x]$ defines $\{\text{\#'s with a square root}\} = \{r \in \mathbb{R} : r > 0\}$

EX

Find $\alpha[x]$ that defines $\{2,3\}$ in $M = \langle \mathbb{N}, 0, 1, +, \times, x \to x+1\rangle$

$$\alpha[x] \equiv S(S(b)) = x \quad \land \quad S(S(S(b))) = x$$

Formal Proof System

Formal Theorems

$\{\text{Formal Theorems}\} = I(\underset{\text{WFF}}{X}, \text{Axioms}, \text{M.P})$

$\boxed{\vdash \alpha}$ " α is a formal theorem"

Formal Proof generating sequence in $I(X, A, P)$

Formal Consequences

$\{\text{Formal Consequences of } \Gamma\} = I(\underset{\text{WFF}}{X}, \text{Axioms} \cup \Gamma, \text{M.P})$

$\boxed{\Gamma \vdash \alpha}$ " α is a formal consequence"

Formal Proof From Assumptions generating sequence in $I(X, A, P)$

Axioms

defined inductively

$\{\text{Axioms}\} = I(X, \text{Atomic Axioms}, \{\ \})$

$\left\{ \dfrac{\alpha}{\forall x \alpha} : \text{For all variables } `x` \right\}$

free or bound

If α is an axiom, then :

$\forall x \alpha$ is an axiom
$\forall y \alpha$ is an axiom
$\forall z \alpha$ is an axiom
$\vdots \quad \vdots \quad \vdots$

Atomic Axioms

1	Substitution in a propositional tautology
2	$\forall x \alpha \rightarrow \alpha^x_t$ (given we're allowed)
3	$\forall x(\alpha \rightarrow \beta) \rightarrow (\forall x \alpha \rightarrow \forall x \beta)$
4	$\alpha \rightarrow \forall x \alpha$ (when x does not occur free in α)
5	$x = x$ for every variable x
6	$x = y \rightarrow (\alpha \rightarrow \alpha')$ (α' : replace every x in α w/ y)

Ex : Using M.P

We showed that : $\forall x \, \exists y \, P(x,y) \rightarrow (\exists z \, R(x,z) \rightarrow \forall x \, \exists y \, P(x,y))$ is an axiom

By M.P : $\forall z \, (\forall x \, \exists y \, P(x,y) \rightarrow (\exists z \, R(x,z) \rightarrow \forall x \, \exists y \, P(x,y)))$ is an axiom

EX Formal Proof

<u>prove that:</u> $P(x) \rightarrow \exists y \, P(y)$

$\therefore$ <u>Show that :</u> $\vdash P(x) \rightarrow \exists y \, P(y)$ $\quad \exists \equiv \neg \forall \neg$

$\vdash P(x) \rightarrow \neg \forall y \, (\neg P(y))$

<u>Formal Proof:</u>

1 $\quad \forall y \, (\neg P(y)) \rightarrow \neg P(x)$ $\quad$ (by A-Axiom 2) $\quad \alpha^{y}_{x}$

2 $\quad [\underbrace{\forall y \, (\neg P(y))}_{\alpha} \rightarrow \underbrace{\neg P(x)}_{\neg\beta}] \rightarrow [\underbrace{P(x)}_{\beta} \rightarrow \underbrace{\neg \forall y \, (\neg P(y))}_{\neg\alpha}]$ $\quad$ (by A-axiom #1 : Substitute in prop-tautology)

3 $\quad P(x) \rightarrow \neg \forall y \, (\neg P(y))$ $\quad$ (M.P)

3 Requirements of a F.P.S

1	Soundness	Formal Proof => logical truth
2	Completeness	logical truth => Formal Proof
3	Verifiable	Formal Proof's are verifiable

Our axioms should be enough such that when we combine axioms + M.P, we get a F.P.S that satisfies the above requirements

In a way, our axioms should "capture full meaning of semantics"

Axioms just define formal proofs

Soundness & completeness are properties of the full proof system, not the individual axioms.

1 | Substitution in a propositional tautology

Ex:

$(\neg A \to \neg B) \to (B \to \neg\neg A)$

$(\neg \beta \to \neg \gamma) \to (\gamma \to \neg\neg \beta)$

P.L WFF		FOL WFF
A	$\longrightarrow$	β
B	$\longrightarrow$	γ

How to | check if a WFF "is a" propositional Tautology

1) parse tree (generation sequence)

2) Stop when connectives are exhausted

3) Check by truth table of connectives if it's a tautology

Ex | is α a logical truth?

$\forall x \exists y\, P(x,y) \to (\exists z\, R(x,z) \to \forall x \exists y\, P(x,y))$

$\forall x \exists y\, P(x,y)$ $(\exists z\, R(x,z) \to \forall x \exists y\, P(x,y))$

α

$\exists z\, R(x,z)$ $\forall x \exists y\, P(x,y)$

β α

$\beta \to (\gamma \to \beta) \equiv$ propositional AX I

$\therefore$ α is a type #1 axiom

2	$\forall x \alpha \rightarrow \alpha^x_t$ (when it's allowed)

$\forall x \alpha$ means: * no matter what you substitute for x, α is still true

α^x_t is allowed $\iff$ x doesn't go from free to bound

Note: $\forall x \alpha \rightarrow \alpha^x_x$: substituting x for x is always allowed

Ex : allowed

$$\forall x \overbrace{(R(x,y) \rightarrow R(y,x))}^{\alpha} \longrightarrow (R(z,y) \rightarrow R(y,z)) \quad \alpha^x_z$$

$$\longrightarrow (R(F(z),y) \rightarrow R(y,F(z))) \quad \alpha^x_{F(z)}$$

Ex : not allowed

$$\forall x (\underbrace{\exists y \neg(x=y)}_{\text{can be true}}) \longrightarrow \overbrace{\underbrace{\exists y (\neg(y=y))}_{\text{always false}}}^{\alpha^x_y} \rightarrow \text{can be False}$$

→ by substituting, we turned a free variable (x) into a bound variable (y)

3	$\forall x(\alpha \rightarrow \beta) \rightarrow (\forall x \alpha \rightarrow \forall x \beta)$

Interprets the meaning of : how '$\forall$' interacts with the connective '$\rightarrow$'

4	$\alpha \rightarrow \forall x \alpha$ (when x does not occur free in x)

Interprets the meaning of : '$\forall x\ \alpha$' when : 1) α does not have 'x' or
2) x is not free

↓

it means nothing

ie: $\forall x\ P(y)$ just means $P(y)$

Proving : Axioms are Sound

<u>claim</u>: every axiom is a logical truth $(\forall M \forall s : M \models_s \alpha)$

INDUCTION on $\alpha \in I(\text{atomic-Axioms}, \frac{\alpha}{\forall x})$

Base Case: $\alpha \in$ atomic-Axioms

1 Substitution in a propositional tautology

a tautology is always true.
So α is a logical truth

2 $\alpha = \forall x \beta \to \beta^x_t$, when allowed

<u>Assume</u>: B.w.o.c that ~~this is not a logical truth~~

$\therefore \exists M,s : M \not\models_s (\forall x \beta \to \beta^x_t)$

by the T.T of '$\to$' : $M \models_s \forall x \beta$ & $M \not\models_s \beta^x_t$

by semantics of '$\forall x$' : $M \models_{s^x_t} \beta$

$\equiv$

$M \models_s \beta^x_t$

contradiction!

$\therefore$ this is a logical truth

3 $\forall x (\alpha \to \beta) \to (\forall x \alpha \to \forall x \beta)$

<u>Assume</u>: b.w.o.c ~~this is not a logical truth~~

$\exists M,s : M \not\models_s (\forall x(\alpha \to \beta) \to (\forall x \alpha \to \forall x \beta))$

T.T of '$\to$' : $M \models_s \forall x(\alpha \to \beta)$ $\quad$ $M \not\models_s (\forall x \alpha \to \forall x \beta)$

T.T of '$\to$' : $M \models_s \forall x \alpha$ $\quad$ $M \not\models_s \forall x \beta$

by semantics of '$\forall x$' : $\forall a \in U^M : M \models_{s^a_x} \alpha$ $\quad$ $\exists a \in U^M : M \not\models_{s^a_x} \beta$

T.T of '$\to$' : $M \not\models_{s^a_x} (\alpha \to \beta)$

by semantics of '$\forall x$' : $M \not\models_s \forall x (\alpha \to \beta)$

contradiction

$\therefore$ this is a logical truth

4 $\alpha \to \forall x \alpha$ (when x does not occur free in x)

<u>Assume</u>: x does not occur free in α

<u>Assume</u>: b.w.o.c not a logical truth

$\exists M,s : M \not\models_s (\alpha \to \forall x \alpha)$

by T.T of '$\to$' : $M \models_s \alpha$ $\quad$ $M \not\models_s \forall x \alpha$

by def^n of Semantics : $\exists a \in U^M : M \not\models_{s^a_x} \alpha$

Since x is not free : $M \not\models_s \alpha$

contradiction

$\therefore$ the formula is true

Inductive Step $\frac{\alpha}{\forall x \alpha}$: for every variable 'x'

I.H assume α is a logical truth $(\forall M, \forall s : M \models_s \alpha)$

Let x be an arbitrary variable.

<u>assume</u>: b.w.o.c, ~~$\forall x \alpha$ is not a logical truth~~

$\therefore \exists M,s : M \not\models_s \forall x \alpha$

by Semantics of '$\forall$' : $\exists a \in U^M : M \not\models_{s^x_a} \alpha$

Contradiction

$\therefore \forall x \alpha$ is a logical truth

Soundness Theorem

$\forall \Gamma, \forall \alpha$: $\Gamma \vdash \alpha \Rightarrow \Gamma \models \alpha$

$\Gamma = \emptyset$

$\vdash \alpha$ → provable (Formal Theorem)

$\models \alpha$ → logical truth

Proof:

$\boxed{\text{INDUCTION}}$ on $\alpha \in I(X, \text{axioms} \cup \Gamma, \text{M.P})$

- $\boxed{\text{Base Case}}$
  - $\boxed{1}$ $\alpha \in$ Axioms

    every axiom is a logical truth
  - $\boxed{2}$ $\alpha \in \Gamma$

    Since $\alpha \in \Gamma$: $\Gamma \models \alpha$
- $\boxed{\text{Inductive Step}}$ M.P : $\dfrac{\alpha, \alpha \to \beta}{\beta}$

$\boxed{\text{I.H}}$ assume $\Gamma \models \alpha$ & $\Gamma \models (\alpha \to \beta)$

$\forall M, \forall s : [\forall \gamma \in \Gamma \; M \models_s \gamma] \to [M \models_s \alpha]$

$\forall M, \forall s : [\forall \gamma \in \Gamma \; M \models_s \gamma] \to [M \models_s (\alpha \to \beta)]$

$\to [M \models_s \alpha \to M \models_s \beta]$ by T.T of '$\to$'

$\to M \models_s \beta$ by T.T of '$\to$'

Assume: b.w.o.c that : $\Gamma \not\models \beta$

$\exists M, \exists s : [\forall \gamma \in \Gamma \; M \models_s \gamma] \wedge [M \not\models_s \beta]$

Contradiction

$\therefore \Gamma \models \beta$

Basic Theorems on Formal Proofs

Deduction Theorem $\quad \Gamma \cup \{\alpha\} \vdash \beta \iff \Gamma \vdash (\alpha \to \beta)$

<u>Proof</u>: (by substitution in prop tautology)

Consistency

$$\left.\begin{aligned} \Gamma \text{ is consistent} &\iff \exists \beta \text{ s.t } \Gamma \nvdash \beta \\ &\iff \nexists \alpha \text{ s.t } \Gamma \vdash \alpha \ \& \ \Gamma \vdash \neg\alpha \end{aligned}\right\} \text{equivalent}$$

Summary

SYNTAX	SEMANTICS
WFF	Structures : $\mathcal{M}$
Free, Bound	Assignments : $s, \bar{s}$
Sentence	Structure Satisfies : $\mathcal{M} \models \alpha$ (for a sentence α)
	$\mathcal{M} \models_s \alpha$ (α not a sentence)
	Logical Implication : $\alpha \models \beta$, $\Sigma \models \alpha$
	Satisfiable : Σ, α
	Defines : α defines subset of $U^{\mathcal{M}}$
	α defines $\{\text{structures}\}$
	Σ defines $\{\text{structures}\}$
	subsets $\subseteq U^{\mathcal{M}}$ within $\mathcal{M}$

$$\Sigma \vdash \alpha \rightarrow \Sigma \models \alpha$$

Soundness Theorem

In particular :

$$PA \vdash \alpha \longrightarrow \mathcal{M}_{\mathbb{N}} \models \alpha$$

Axioms for $\mathbb{N}$ — natural #s satisfy α

In math, we often want to show that $\mathbb{N}$ satisfy some property (α)
So we prove the property formally ($PA \vdash \alpha$)