

601 Lecture 12: Recall From Last Time

First-Order Logic with Equality

Vocabulary: $\Sigma = (\Phi, \Pi, r)$:

function symbols, predicate symbols, arity function, “=” $\in \Pi$.

terms, atomic formulas, formulas: $\mathcal{L}(\Sigma)$

Structure of vocabulary Σ :

$$\mathcal{A} = (U, \mu) \in \text{STRUC}[\Sigma]; \quad U = |\mathcal{A}| \neq \emptyset$$

$$\mu : V \rightarrow |A| : \quad \mu : x \mapsto x^{\mathcal{A}}$$

$$\mu : \Phi \rightarrow \text{total functions on } U^{O(1)}$$

$$\mu : f \mapsto f^{\mathcal{A}} : U^{r(f)} \rightarrow U$$

$$\mu : \Pi \rightarrow \text{relations on } U^{O(1)}$$

$$\mu : R \mapsto R^{\mathcal{A}} \subseteq U^{r(R)}$$

Tarski's Inductive Definition of Truth

$\mathcal{A} = (|\mathcal{A}|, \mu)$ μ defined on variables, $\mu : x \mapsto x^{\mathcal{A}}$.

Extend $\mu : \text{terms} \rightarrow |\mathcal{A}|$
inductively: $f_j(t_1, \dots, t_{r(f_j)})^{\mathcal{A}} = f_j^{\mathcal{A}}(t_1^{\mathcal{A}}, \dots, t_{r(f_j)}^{\mathcal{A}})$

$$\mathcal{A} \models t_1 = t_2 \Leftrightarrow t_1^{\mathcal{A}} = t_2^{\mathcal{A}}$$

$$\mathcal{A} \models R_j(t_1, \dots, t_{r(R_j)}) \Leftrightarrow \langle t_1^{\mathcal{A}}, \dots, t_{r(R_j)}^{\mathcal{A}} \rangle \in R_j^{\mathcal{A}}$$

$$\mathcal{A} \models \neg\varphi \Leftrightarrow \mathcal{A} \not\models \varphi$$

$$\mathcal{A} \models \varphi \vee \psi \Leftrightarrow \mathcal{A} \models \varphi \text{ or } \mathcal{A} \models \psi$$

$$\mathcal{A} \models \forall x(\varphi) \Leftrightarrow \text{for all } a \in |\mathcal{A}| \ (\mathcal{A}, a/x) \models \varphi$$

where

$$y^{(\mathcal{A}, a/x)} = \begin{cases} y^{\mathcal{A}} & \text{if } y \neq x \\ a & \text{if } y = x \end{cases}$$

Example: Does $\mathbf{Z}/3\mathbf{Z} \models \forall u(u = 0 \vee (\exists v)(u \times v = 1))$?

$$\mathbf{Z}/3\mathbf{Z} \models \forall u(u = 0 \vee \exists v(u \times v = 1))$$

$$\Leftrightarrow \text{forall } a \in \{0, 1, 2\} (\mathbf{Z}/3\mathbf{Z}, a/u) \models (u = 0 \vee \exists v(u \times v = 1))$$

$$(\mathbf{Z}/3\mathbf{Z}, 0/u) \models u = 0$$

$$\Leftrightarrow 0 = 0$$

$$(\mathbf{Z}/3\mathbf{Z}, 1/u) \models \exists v(u \times v = 1)$$

$$\Leftrightarrow \text{exists } b \in \{0, 1, 2\} (\mathbf{Z}/3\mathbf{Z}, 1/u, b/v) \models (u \times v = 1)$$

$$(\mathbf{Z}/3\mathbf{Z}, 1/u, 1/v) \models (u \times v = 1)$$

$$(\mathbf{Z}/3\mathbf{Z}, 2/u) \models (\exists v)(u \times v = 1)$$

Prop: $\mathcal{A} \models \varphi \wedge \psi \iff \mathcal{A} \models \varphi \text{ and } \mathcal{A} \models \psi$

Proof:

$$\mathcal{A} \models \varphi \wedge \psi$$

$$\iff \mathcal{A} \models \neg(\neg\varphi \vee \neg\psi)$$

$$\iff \text{not } \mathcal{A} \models \neg\varphi \vee \neg\psi$$

$$\iff \text{not } \left[(\mathcal{A} \models \neg\varphi) \text{ or } (\mathcal{A} \models \neg\psi) \right]$$

$$\iff \mathcal{A} \not\models \neg\varphi \text{ and } \mathcal{A} \not\models \neg\psi$$

$$\iff \mathcal{A} \models \varphi \text{ and } \mathcal{A} \models \psi$$



Prop: $\mathcal{A} \models \exists x(\varphi) \iff \text{exists } a \in |\mathcal{A}|(\mathcal{A}, a/x) \models \varphi$

Proof:

$$\mathcal{A} \models \exists x(\varphi)$$

$$\Leftrightarrow \mathcal{A} \models \neg \forall x(\neg \varphi)$$

$$\Leftrightarrow \mathcal{A} \not\models \forall x(\neg \varphi)$$

$$\Leftrightarrow \text{not for all } a \in |\mathcal{A}|(\mathcal{A}, a/x) \models \neg \varphi$$

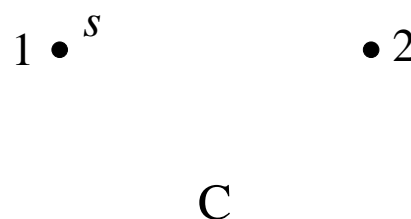
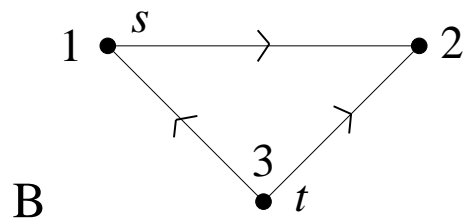
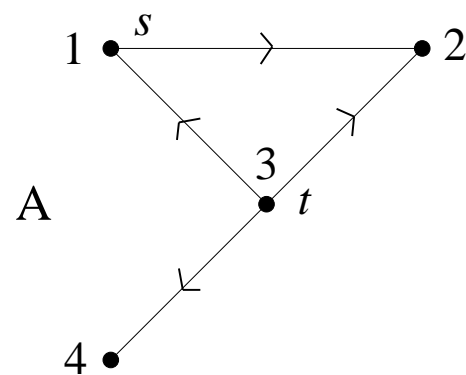
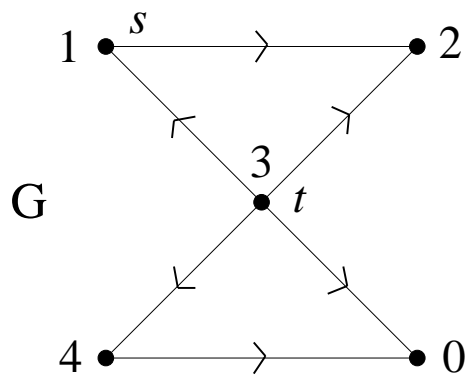
$$\Leftrightarrow \text{for some } a \in |\mathcal{A}|(\mathcal{A}, a/x) \not\models \neg \varphi$$

$$\Leftrightarrow \text{for some } a \in |\mathcal{A}|(\mathcal{A}, a/x) \models \varphi$$



Def: Let $\mathcal{A}, \mathcal{B} \in \text{STRUC}[\Sigma]$, $\Sigma = (\Phi, \Pi, r)$. \mathcal{A} is a **substructure** of \mathcal{B} , ($\mathcal{A} \leq \mathcal{B}$), iff:

1. $|\mathcal{A}| \subseteq |\mathcal{B}|$
2. for all $f \in \Phi$, $f^{\mathcal{A}} = f^{\mathcal{B}} \cap |\mathcal{A}|^{r(f)+1}$
3. for all $R \in \Pi$, $R^{\mathcal{A}} = R^{\mathcal{B}} \cap |\mathcal{A}|^{r(R)}$



A and B but not C are substructures of G.

Def: Let $\mathcal{A}, \mathcal{B} \in \text{STRUC}[\Sigma]$.

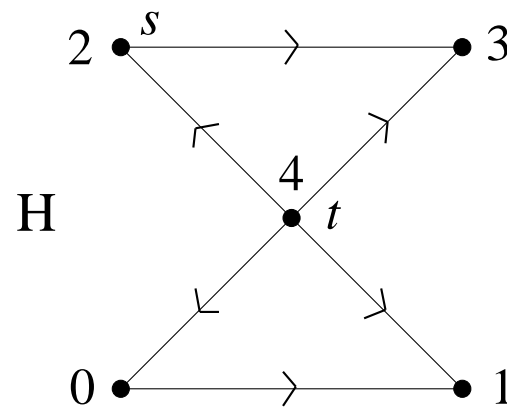
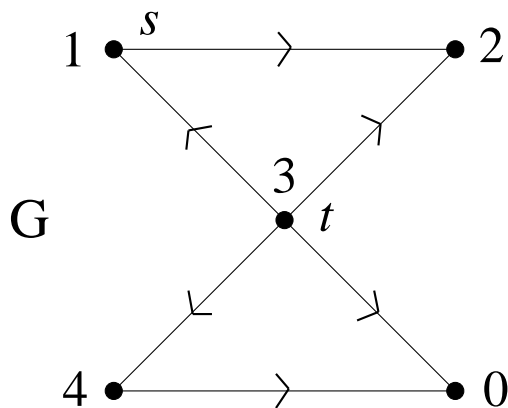
\mathcal{A} is **isomorphic** to \mathcal{B} ($\mathcal{A} \cong \mathcal{B}$) iff exists $\eta : |\mathcal{A}| \xrightarrow[\text{onto}]{1:1} |\mathcal{B}|$,

1. For every $R \in \Pi$, tuple $e_1, \dots, e_{r(R)} \in |\mathcal{A}|$

$$(\langle e_1, \dots, e_{r(R)} \rangle \in R^{\mathcal{A}}) \Leftrightarrow (\langle \eta(e_1), \dots, \eta(e_{r(R)}) \rangle \in R^{\mathcal{B}})$$

2. For every $f \in \Phi$, tuple $e_1, \dots, e_{r(f)} \in |\mathcal{A}|$,

$$\eta(f^{\mathcal{A}}(e_1, \dots, e_{r(f)})) = f^{\mathcal{B}}(\eta(e_1), \dots, \eta(e_{r(f)}))$$



Only names are changed; all structure is preserved.

Def: Let $\mathcal{A}, \mathcal{B} \in \text{STRUC}[\Sigma]$. We say that

\mathcal{A} and \mathcal{B} are **elementarily equivalent** ($\mathcal{A} \equiv \mathcal{B}$) iff

for all sentences $\varphi \in \mathcal{L}(\Sigma)$,

$$\mathcal{A} \models \varphi \quad \Leftrightarrow \quad \mathcal{B} \models \varphi$$

Prop: If $\mathcal{A} \cong \mathcal{B}$ then $\mathcal{A} \equiv \mathcal{B}$.

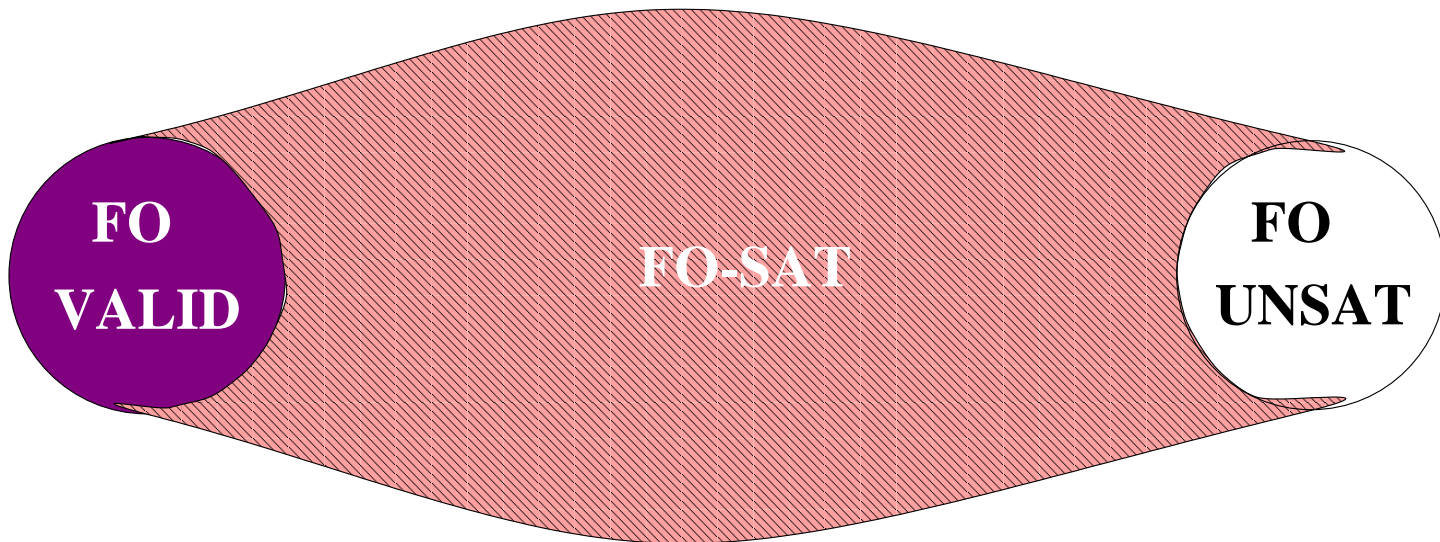
Proof: exercise

First-Order Validity

$\varphi \in \mathcal{L}(\Sigma)$ is **satisfiable** iff exists $\mathcal{A} \in \text{STRUC}[\Sigma]$, $\mathcal{A} \models \varphi$.

φ is **valid** ($\models \varphi$) iff for all $\mathcal{A} \in \text{STRUC}[\Sigma]$, $\mathcal{A} \models \varphi$.

$\Gamma \subseteq \mathcal{L}(\Sigma)$ **semantically implies** $\varphi \in \mathcal{L}(\Sigma)$ ($\Gamma \models \varphi$)
iff for all $\mathcal{A} \in \text{STRUC}[\Sigma]$, $\mathcal{A} \models \Gamma \Rightarrow \mathcal{A} \models \varphi$.



$$\mathbf{FO-VALID} = \{\varphi \mid \models \varphi\}$$

Prop: Let $f(\varphi) = \neg\varphi$.

Then, $f : \mathbf{FO-VALID} \leq \mathbf{FO-UNSAT}$ and

$$f : \mathbf{FO-UNSAT} \leq \mathbf{FO-VALID}$$

Prop: $\{\psi\} \models \varphi \Leftrightarrow \models (\psi \rightarrow \varphi) \Leftrightarrow \models (\neg\psi \vee \varphi)$

Proof: exercise.

Axioms and Proof Rules à la Papadimitriou

We will present a simple set of axioms and proof rules as in Papadimitriou. Advantages: concept of proof very simple, **only one proof rule**.

Other equivalent systems include:

- **Natural deduction**, which has many natural proof rules and **no axioms**!
- **Resolution**, which is used in many automatic proof systems

Notation: “ $\Gamma \vdash \varphi$ ” is read, “ Γ proves φ ”, and means,
“There is a first-order proof of φ assuming Γ .”

Modus Ponens (M.P.) $\frac{\Gamma \vdash \varphi \rightarrow \psi, \Gamma \vdash \varphi}{\Gamma \vdash \psi}$ “mode that affirms”

Prop: Modus Ponens preserves truth, validity, and semantic implication, we’ll just say, “**preserves truth**,” in future:

if $\mathcal{A} \models \varphi \rightarrow \psi$ **and** $\mathcal{A} \models \varphi$ **then** $\mathcal{A} \models \psi$.

if $\Gamma \models \varphi \rightarrow \psi$ **and** $\Gamma \models \varphi$ **then** $\Gamma \models \psi$.

Proof: Suppose $\Gamma \models \varphi$ and $\Gamma \models \varphi \rightarrow \psi$.

Let \mathcal{A} be arbitrary such that $\mathcal{A} \models \Gamma$.

$\mathcal{A} \models \varphi, \mathcal{A} \models \neg\varphi \vee \psi$

$\mathcal{A} \models \psi$

$\Gamma \models \psi$



$\forall x(\varphi)$ is called a **generalization** of φ .

Prop: If $\models \varphi$, then $\models \forall x(\varphi)$.

Proof: Assume that $\models \varphi$ where $\varphi \in \mathcal{L}(\Sigma)$.

Let $\mathcal{A} \in \text{STRUC}[\Sigma]$ be arbitrary.

Let $a \in |\mathcal{A}|$ be arbitrary; $(\mathcal{A}, a/x) \in \text{STRUC}[\Sigma]$

$(\mathcal{A}, a/x) \models \varphi$

for all $a \in |\mathcal{A}|$, $(\mathcal{A}, a/x) \models \varphi$

$\mathcal{A} \models \forall x(\varphi)$

$\models \forall x(\varphi)$



Papadimitriou's First-Order Axioms

all generalizations of the following:

AX0: Tautologies on **at most three boolean variables**, with first-order formula substituted for the variables, e.g.,

1. $x_1 \rightarrow x_1$

2. $x_1 \rightarrow (x_1 \vee x_2)$

3. $x_1 \vee \neg x_1$

4. $x_1 \rightarrow (\neg x_1 \rightarrow x_2)$

1. $\forall u \exists v (E(u, v)) \rightarrow \forall u \exists v (E(u, v))$

2. $\forall z (z < z + z) \rightarrow (\forall z (z < z + z) \vee (\forall y) (y < z))$

3. $\exists z (R(z)) \vee \neg \exists z (R(z))$

4. $\text{prime}(17) \rightarrow (\neg \text{prime}(17) \rightarrow 0 \neq 0)$

Prop: All members of AX0 are valid.

Proof: The meaning of boolean connectives to valuations of boolean formulas is

identical to that in Tarski's definition of truth.

Therefore if φ is a tautology, then $\mathcal{A} \models \varphi$.

Therefore, all tautologies are valid.

Therefore, all generalizations of tautologies are valid. □

Equality Axioms

all generalizations of the following

AX1a $t = t$, for any term t

AX1b $(t_1 = t'_1 \wedge \dots \wedge t_k = t'_k) \rightarrow f(t_1, \dots, t_k) = f(t'_1, \dots, t'_k)$
for terms t_1, \dots, t'_k , $f \in \Phi$, $r(f) = k$

Ax1c

$(t_1 = t'_1 \wedge \dots \wedge t_k = t'_k) \rightarrow (R(t_1, \dots, t_k) \rightarrow R(t'_1, \dots, t'_k))$
for terms t_1, \dots, t'_k , $R \in \Pi$, $r(R) = k$

Prop: Every instance of AX1 is valid.

Proof: Because “=” is interpreted as “identically equal”. \square

Def: Term t is **substitutable** for variable x in φ iff no free occurrence of x in φ is within the scope of a quantifier for a variable z occurring in t . (no capturing occurs when we substitute t for x in φ .)

$\varphi[x \leftarrow t]$ is the result of substituting t for all free occurrences of x in φ .

We never use this expression unless t is substitutable for x in φ .

$$\alpha \equiv \exists y(y < x)$$

$$\alpha[x \leftarrow z + 1] \equiv \exists y(y < z + 1)$$

$$\alpha[x \leftarrow f(u) + v] \equiv \exists y(y < f(u) + v)$$

$$\alpha' \equiv \exists y(y < y)$$

$z + 1, u, f(u), f(u) + v$ are substitutable for x in α .
 $y, y + 1$ are not substitutable for x in α or φ .

$$\alpha \equiv \text{“}x \text{ is not the least element”}$$

$$\alpha[x \leftarrow z + 1] \equiv \text{“}z + 1 \text{ is not the least element”}$$

all generalizations of the following

AX2: $\forall x(\varphi) \rightarrow \varphi[x \leftarrow t]$, x a variable, t a term, t substitutable for x in φ .

Prop: Every instance of AX2 is valid.

Proof: Let $\forall x(\varphi) \rightarrow \varphi[x \leftarrow t] \in \text{AX2}$.



Lemma: Let $\mathcal{A}, \mathcal{A}'$ be identical except for how they interpret some variables not free in φ . Then,

$$\mathcal{A} \models \varphi \quad \Leftrightarrow \quad \mathcal{A}' \models \varphi$$

Proof: Hw6: By induction on φ .

Base cases: $\varphi \equiv R(t_1, \dots, t_k)$; $\varphi \equiv t_1 = t_2$:

[Here you should show by induction on each term that $t_i^{\mathcal{A}} = t_i^{\mathcal{A}'}$.]

Inductive case 1: $\varphi \equiv \neg\psi$

Inductive case 2: $\varphi \equiv (\alpha \vee \beta)$

Inductive case 3: $\varphi \equiv \forall x(\psi)$

[Take some care here.]



all generalizations of the following

AX3: $\varphi \rightarrow \forall x(\varphi)$, where x does not occur freely in φ .

Prop: Every instance of AX3 is valid.

Proof: Let $\varphi \rightarrow \forall x(\varphi) \in \text{AX3}$.

Let $\mathcal{A} \in \text{STRUC}[\Sigma]$ be arbitrary.

Suppose $\mathcal{A} \models \varphi$

$$\mathcal{A} \models \forall x(\varphi) \quad \Leftrightarrow \quad (\text{for all } a \in |\mathcal{A}|)(\mathcal{A}, a/x) \models \varphi$$

By the Lemma on Slide 20, $\mathcal{A} \models \forall x(\varphi)$



all generalizations of the following

AX4: $\forall x(\varphi \rightarrow \psi) \rightarrow (\forall x(\varphi) \rightarrow \forall x(\psi))$

Prop: Every instance of AX4 is valid.

Proof:

$$\forall x(\varphi \rightarrow \psi) \rightarrow (\forall x(\varphi) \rightarrow \forall x(\psi)) \in \text{AX4}$$

Suppose $\mathcal{A} \models \forall x(\varphi \rightarrow \psi)$.

