Recall From Last Time

Boolean variables: $X = \{x_1, x_2, x_3, \ldots\}$

Boolean expressions:

- literals: x_i, $\neg x_i$, $\top$, $\bot$
- $(\alpha \vee \beta)$, $\neg\alpha$, for α, β Boolean exp's.

Truth assignment: $T : X' \subseteq X \to \{\textbf{true}, \textbf{false}\}$

$$X(\varphi) \quad = \quad \{x_i \in X \mid x_i \text{ occurs in } \varphi\}$$

If $X(\varphi) \subseteq X'$, then T is *appropriate* to φ. T assigns truth value to φ: $T \models \varphi$ or $T \models \neg\varphi$.

Facts:

1. SAT and Circuit-SAT are NP-complete.
2. Horn-SAT and CVP are P-complete:
3. 2-SAT is is NL-complete:

Boolean circuits provide another model of computation analogous to Turing machine, lambda calculus, etc.

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

Φ: function symbols,

Π: predicate symbols, “=” $\in \Pi$, not mentioned

r: arity function, $r(=) = 2$.

Variables: $V = \{x, y, z, x_1, y_1, z_1, \ldots\}$

Number Theory: $\Sigma_N = (\Phi_N, \Pi_N, r_N)$

$$\Phi_N \quad = \quad \{0,\ \sigma,\ +,\ \times,\ \uparrow\}$$

$$r_N(0) = 0, r_N(\sigma) = 1, r_N(+) = r_N(\times) = r_N(\uparrow) = 2$$

$$\Pi_N \quad = \quad \{=,\ <\}, \qquad r_N(=) \ = \ r_N(<) \ = \ 2$$

Graph Theory: $\Sigma_G = (\Phi_g, \Pi_g, r_g)$

$$\Phi_g \quad = \quad \{s, t\}, \qquad r_g(s) \ = \ r_g(t) \ = \ 0$$

$$\Pi_g \quad = \quad \{=,\ E\}, \qquad r_g(=) \ = \ r_g(E) \ = \ 2$$

Tarski's World: $\Sigma_T = (\Phi_T, \Pi_T, r_T)$

$$\Phi_T = \{a, b, c, d, e, f\}$$

Π_T = { Tet, Cube, Dodec, Small, Medium, Large, SameSize, SameShape, Larger, Smaller, SameCol, SameRow, Adjoins, LeftOf, RightOf, FrontOf, BackOf, Between }

$$r(a) = r(b) = r(c) = r(d) = r(e) = r(f) = 0$$

$$\begin{aligned} r(\text{Tet}) &= r(\text{Cube}) = r(\text{Dodec}) = r(\text{Small}) \\ &= r(\text{Medium}) = r(\text{Large}) = 1 \end{aligned}$$

$$\begin{aligned} r(\text{SameSize}) &= r(\text{SameShape}) = r(\text{Larger}) = r(\text{Smaller}) \\ &= r(\text{SameCol}) = r(\text{SameRow}) = r(\text{Adjoins}) \\ &= r(\text{LeftOf}) = r(\text{RightOf}) = r(\text{BackOf}) = 2 \end{aligned}$$

$$r(\text{Between}) = 3$$

terms:

1. variables: $x, y, z, \ldots$
2. constants: $c \in \Phi$, $r(c) = 0$
3. $f(t_1, \ldots, t_k)$, where $t_1, \ldots, t_k$ are terms, $f \in \Phi$, $r(f) = k$

atomic formulas: $R(t_1, \ldots, t_k)$, where $t_1, \ldots, t_k$ terms, $R \in \Pi$, $r(R) = k$

formulas:

1. atomic formulas
2. $\neg A$, $(A \vee B)$, where A, B are formulas
3. $(\forall x A)$, where A is a formula

$\mathcal{L}(\Sigma)$ = set of first-order formulas of vocabulary Σ

Abbreviations: (in addition to: $\wedge, \rightarrow, \leftrightarrow$)

$$(\exists x A) \quad \hookrightarrow \quad \neg(\forall x \neg A)$$

$$t_1 \neq t_2 \quad \hookrightarrow \quad \neg t_1 = t_2$$

Abbreviations:

$$t_1 \le t_2 \hookrightarrow (t_1 = t_2 \ \vee \ t_1 < t_2)$$

$$1 \hookrightarrow \sigma(0)$$

$$2 \hookrightarrow \sigma(1)$$

$$3 \hookrightarrow \sigma(2)$$

$$t_1 | t_2 \hookrightarrow (\exists x)(t_1 \times x = t_2)$$

$$\text{prime}(t_1) \hookrightarrow 1 < t_1 \ \wedge \ (\forall x)(x | t_1 \to (x = 1 \vee x = t_1))$$

1. $(\forall x)(x + 0 = x)$
2. $(\exists y)(y + y = x)$
3. $(\forall xy)(x \le y \ \leftrightarrow \ (\exists z)(x + z = y))$
4. $(\forall x)(\exists y)(x < y \ \wedge \ \text{prime}(y))$
5. $(\forall xy)(\sigma(x) = \sigma(y) \ \to \ x = y)$
6. $(\forall xy)(x < y \ \to \ \sigma(x) \le y)$

1. $(\forall xy)(E(x,y) \rightarrow E(y,x))$

2. $(\forall x)(\neg E(x,x))$

3. $(\forall x)(\exists y)(E(x,y) \vee E(y,x))$

4. $(\forall x)(\neg E(x,s))$

5. $(\exists yz)(y \neq z \wedge E(x,y) \wedge E(x,z))$

6. $$(\forall y_1 y_2 y_3)((E(x,y_1) \wedge E(x,y_2) \wedge E(x,y_3)) \rightarrow (y_1 = y_2 \vee y_1 = y_3 \vee y_2 = y_3))$$

An occurrence of a variable x is *bound* iff it occurs within the scope of a quantifier, $(\forall x)$ or $(\exists x)$. Otherwise the occurrence is *free*.

1. $(\exists yz)(y \neq z \wedge E(x,y) \wedge E(x,z))$
2. $(\forall z)(z + x = z)$
3. $(\forall y)(y + x = y)$
4. $(\forall x)(x + x = x)$
5. $x \neq y \;\wedge\; (\exists y)(y < x)$

Bound variables are dummy variables – you can change their names without affecting the meaning.

A first-order formula says something *about* its free variables. You cannot determine the meaning of the formula without knowing the values of the free variables.

A *structure* — also called a *model* — of a vocabulary $\Sigma = (\Phi, \Pi, r)$ is a pair $\mathcal{A} = (U, \mu)$ such that:

$$U = |\mathcal{A}| \neq \emptyset$$

$$\begin{aligned} \mu : \; V &\to U \\ x &\mapsto x^{\mathcal{A}} \end{aligned}$$

$$\begin{aligned} \mu : \; \Phi &\to \text{ total functions on } U^{O(1)} \\ \mu : \; f &\mapsto f^{\mathcal{A}} : U^{r(f)} \to U \end{aligned}$$

$$\begin{aligned} \mu : \; \Pi &\to \text{ relations on } U^{O(1)} \\ \mu : \; R &\mapsto R^{\mathcal{A}} \subseteq U^{r(R)} \end{aligned}$$

How's That Again?

We specify the *universe, variable values, functions,* and *relations* by finite lookup tables. This is the information we need to decide whether a formula is true or false.

Example: Any world, $\mathcal{W}$, for Tarski's World is is structure of vocabulary Σ_T, i.e, $\mathcal{W} \in \text{STRUC}[\Sigma_T]$.

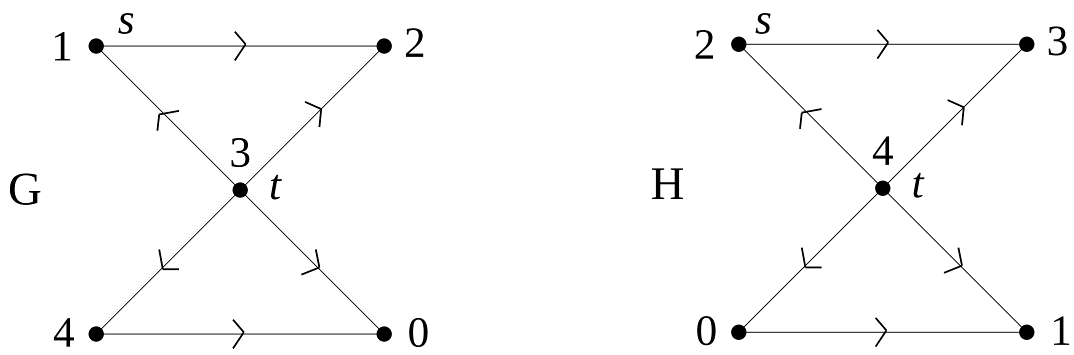


Figure 11.1: Graphs G and H

$$G = \langle V^G, 1, 3, E^G \rangle \ \in \ \text{STRUC}[\Sigma_g]$$

$$\begin{aligned} V^G &= \{0,1,2,3,4\} \\ E^G &= \{(1,2),(3,0),(3,1),(3,2),(3,4),(4,0)\} \end{aligned}$$

is a structure of vocabulary Σ_g, consisting of a directed graph with two specified vertices s and t. G has five vertices and six edges. (See Figure 11.1 which shows G as well as another graph H which is isomorphic but not equal to G.)

Binary String: $w =$ "01101".

$\mathcal{A}_w = \langle\{0,1,\ldots,4\},<,\{1,2,4\}\rangle \in$ STRUC$[\Sigma_s]$

$$\begin{aligned}\Sigma_s &= (\emptyset, \{=,<,S\}, \{\langle =,2\rangle, \langle <,2\rangle, \langle S,1\rangle\}) \\ &= (;<^2, S^1)\end{aligned}$$

1. $(\exists x)(\forall y)(y \leq x \ \wedge \ S(x))$
2. $(\forall xy)((x < y \wedge \neg S(x) \wedge \neg S(y)) \rightarrow (\exists z)(x < z < y))$

sentence = formula with no free variables

$$\Sigma_{gen} \quad = \quad (; F^1, P^2, S^2)$$

$$\mathcal{B}_0 = \langle U_0, F_0, P_0, S_0 \rangle \in \text{STRUC}[\Sigma_{gen}]$$

$$U_0 \;=\; \{\text{Abraham, Isaac, Rebekah, Sarah, } \ldots\}$$

$$F_0 \;=\; \{\text{Sarah, Rebekah, } \ldots\}$$

$$P_0 \;=\; \{\langle\text{Abraham,Isaac}\rangle, \langle\text{Sarah,Isaac}\rangle, \ldots\}$$

$$S_0 \;=\; \{\langle\text{Abraham,Sarah}\rangle, \langle\text{Isaac,Rebekah}\rangle, \ldots\}$$

$$\begin{aligned}\varphi_{sibling}(x,y) \;\equiv\; & (\exists fm)(x \neq y \wedge f \neq m \;\wedge \\ & P(f,x) \wedge P(f,y) \wedge P(m,x) \wedge P(m,y))\end{aligned}$$

$$\begin{aligned}\varphi_{aunt}(x,y) \;\equiv\; & (\exists ps(P(p,y) \wedge \varphi_{sibling}(p,s) \wedge \\ & (s = x \vee S(x,s))) \;\wedge\; F(x)\end{aligned}$$

$\mathbf{N} = (\mathbf{N}, 0, \sigma, +, \times, \uparrow, <)$, the standard model of the naturals

$\mathbf{Z}/p\mathbf{Z} = (\{0, 1, \ldots, p-1\}, 0, +1_p, +_p, \times_p, \uparrow_p, \emptyset)$, p prime

$\mathbf{N}, \mathbf{Z}/p\mathbf{Z} \in \text{STRUC}[\Sigma_N]$

$$\text{MultInverses} \quad \equiv \quad (\forall u)(u = 0 \vee (\exists v)(u \times v = 1))$$

$$\mathbf{N} \models \neg\text{MultInverses}; \qquad \mathbf{Z}/p\mathbf{Z} \models \text{MultInverses}$$

Extend the function μ : terms $\rightarrow |\mathcal{A}|$, (already defined on variables and constants).

$$\mu(f_j(t_1, \ldots, t_{r(f_j)})) \quad = \quad f_j^{\mathcal{A}}(\mu(t_1), \ldots, \mu(t_{r(f_j)}))$$

Now every term has a meaning.

Tarski's Inductive Definition of Truth:

$$\begin{aligned}
(|\mathcal{A}|, \mu) \models t_1 = t_2 \;&\Leftrightarrow\; \mu(t_1) = \mu(t_2) \\
(|\mathcal{A}|, \mu) \models R_j(t_1, \ldots, t_{r(R_j)}) \;&\Leftrightarrow\; \langle \mu(t_1), \ldots, \mu(t_{r(R_j)}) \rangle \in R_j^{\mathcal{A}} \\
(|\mathcal{A}|, \mu) \models \neg\varphi \;&\Leftrightarrow\; (|\mathcal{A}|, \mu) \not\models \varphi \\
(|\mathcal{A}|, \mu) \models \varphi \vee \psi \;&\Leftrightarrow\; (|\mathcal{A}|, \mu) \models \varphi \text{ or } (|\mathcal{A}|, \mu) \models \psi \\
(|\mathcal{A}|, \mu) \models (\forall x)\varphi \;&\Leftrightarrow\; (\text{for all } a \in |\mathcal{A}|)(|\mathcal{A}|, \mu, a/x) \models
\end{aligned}$$

where $$(\mu, a/x)(y) \;=\; \begin{cases} \mu(y) & \text{if } y \neq x \\ a & \text{if } y = x \end{cases}$$

Play Tarski's Truth Game!!!

world: $\mathcal{W}$; sentence: φ; players: A, B

A asserts that $\mathcal{W} \models \varphi$; B denies that $\mathcal{W} \models \varphi$.

The game rules depend inductively on the formula φ:

φ is atomic: A wins iff $\mathcal{W} \models \varphi$.

$\varphi \equiv \alpha \vee \beta$: A asserts $\mathcal{W} \models \alpha$ or A asserts $\mathcal{W} \models \beta$.

$\varphi \equiv \alpha \wedge \beta$: B denies $\mathcal{W} \models \alpha$ or B denies $\mathcal{W} \models \beta$.

$\varphi \equiv \neg\alpha$: A and B switch rôles, and B asserts $\mathcal{W} \models \alpha$.

$\varphi \equiv \exists x(\psi)$: A chooses an element from $|\mathcal{W}|$, assigning it a name n. A asserts that $\mathcal{W}' \models \psi[x \leftarrow n]$.

$\varphi \equiv \forall x(\psi)$: B chooses an element from $|\mathcal{W}|$, assigning it a name n. B denies that $\mathcal{W}' \models \psi[x \leftarrow n]$.

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

$$\mathbf{Z}/3\mathbf{Z}, \mu_0 \models (\forall u)(u = 0 \vee (\exists v)(u \times v = 1))$$

$$\Leftrightarrow \text{(forall } a \in \{0, 1, 2\})$$
$$(\mathbf{Z}/3\mathbf{Z}, \mu_0, a/u) \models (u = 0 \vee (\exists v)(u \times v = 1))$$

$$(\mathbf{Z}/3\mathbf{Z}, \mu_0, 0/u) \models u = 0$$

$$\Leftrightarrow (\mu_0, 0/u)(u) = (\mu_0, 0/u)(0)$$

$$\Leftrightarrow 0 = 0$$

$$(\mathbf{Z}/3\mathbf{Z}, \mu_0, 1/u) \models (\exists v)(u \times v = 1)$$

$$\Leftrightarrow \text{(exists } b \in \{0, 1, 2\})(\mathbf{Z}/3\mathbf{Z}, \mu_0, 1/u, b/v) \models (u \times v = 1)$$

$$(\mathbf{Z}/3\mathbf{Z}, \mu_0, 1/u, 1/v) \models (u \times v = 1)$$

Similarly,

$$(\mathbf{Z}/3\mathbf{Z}, \mu_0, 2/u) \models (\exists v)(u \times v = 1)$$

Proposition 11.2

$(|\mathcal{A}|, \mu) \models \varphi \wedge \psi \quad \Leftrightarrow \quad (|\mathcal{A}|, \mu) \models \varphi$ *and* $(|\mathcal{A}|, \mu) \models \psi$

Proof:

$$
\begin{aligned}
& (|\mathcal{A}|, \mu) \models \varphi \wedge \psi \\
\Leftrightarrow\ & (|\mathcal{A}|, \mu) \models \neg(\neg\varphi \vee \neg\psi) \\
\Leftrightarrow\ & \text{not } (|\mathcal{A}|, \mu) \models \neg\varphi \vee \neg\psi \\
\Leftrightarrow\ & \text{not } [((|\mathcal{A}|, \mu) \models \neg\varphi) \text{ or } ((|\mathcal{A}|, \mu) \models \neg\psi)] \\
\Leftrightarrow\ & (|\mathcal{A}|, \mu) \not\models \neg\varphi \text{ and } (|\mathcal{A}|, \mu) \not\models \neg\psi \\
\Leftrightarrow\ & (|\mathcal{A}|, \mu) \models \varphi \text{ and } (|\mathcal{A}|, \mu) \models \psi
\end{aligned}
$$

♠

Proposition 11.3

$$(|\mathcal{A}|, \mu) \models (\exists x)\varphi \quad \Leftrightarrow \quad (\textit{exists } a \in |\mathcal{A}|)(|\mathcal{A}|, \mu, a/x) \models \varphi$$

Proof:

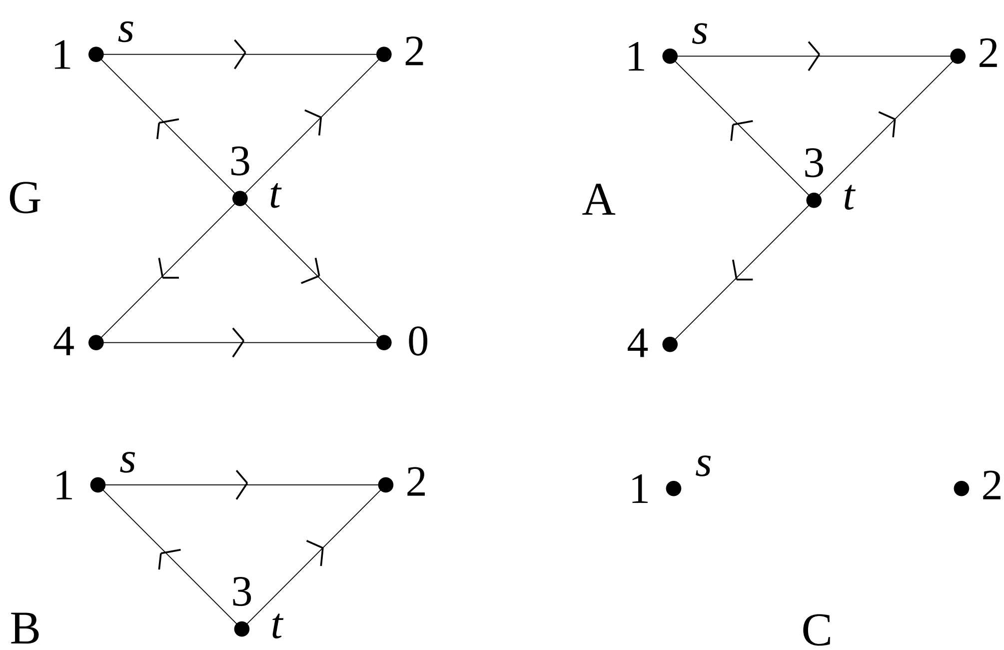
$$\begin{aligned}
& (|\mathcal{A}|, \mu) \models (\exists x)\varphi \\
\Leftrightarrow\ & (|\mathcal{A}|, \mu) \models \neg(\forall x)\neg\varphi \\
\Leftrightarrow\ & (|\mathcal{A}|, \mu) \not\models (\forall x)\neg\varphi \\
\Leftrightarrow\ & \text{not (for all } a \in |\mathcal{A}|)(|\mathcal{A}|, \mu, a/x) \models \neg\varphi \\
\Leftrightarrow\ & (\text{for some } a \in |\mathcal{A}|)(|\mathcal{A}|, \mu, a/x) \not\models \neg\varphi \\
\Leftrightarrow\ & (\text{for some } a \in |\mathcal{A}|)(|\mathcal{A}|, \mu, a/x) \models \varphi
\end{aligned}$$

♠

Definition 11.4 $\mathcal{A}$, $\mathcal{B} \in \mathrm{STRUC}[\Sigma]$, $\Sigma = (\Phi, \Pi, r)$

$\mathcal{A}$ is a *substructure* of $\mathcal{B}$, ($\mathcal{A} \leq \mathcal{B}$), iff:

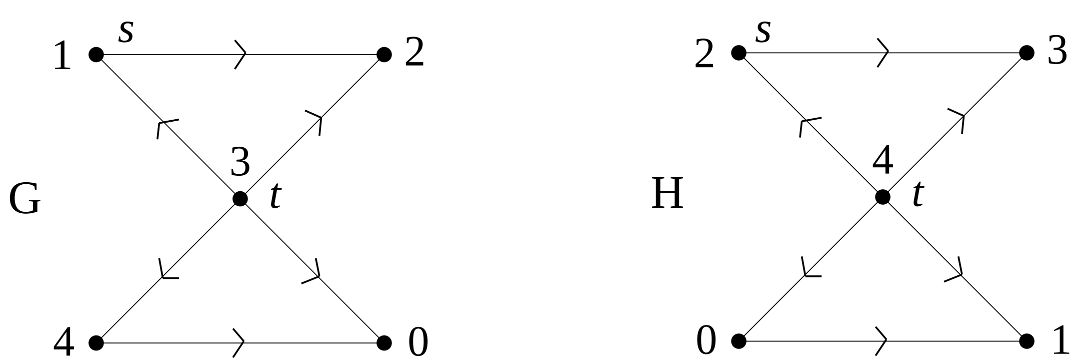
1. $|\mathcal{A}| \subseteq |\mathcal{B}|$
2. For $f \in \Phi$, $f^{\mathcal{A}} = f^{\mathcal{B}} \cap |\mathcal{A}|^{r(f)+1}$
3. For $R \in \Pi$, $R^{\mathcal{A}} = R^{\mathcal{B}} \cap |\mathcal{A}|^{r(R)}$



A and B but not C are substructures of G.

Definition 11.5 $\mathcal{A}, \mathcal{B} \in$ STRUC$[\Sigma]$. $\mathcal{A}$ is *isomorphic* to $\mathcal{B}$ ($\mathcal{A} \cong \mathcal{B}$) iff exists $\eta : |\mathcal{A}| \to |\mathcal{B}|$,

1. η is 1:1 and onto.
2. For every $R \in \Pi$, tuple $e_1, \ldots, e_{r(R)} \in |\mathcal{A}|$
$$(\langle e_1, \ldots, e_{r(R)} \rangle \in R^{\mathcal{A}}) \quad \leftrightarrow \quad (\langle \eta(e_1), \ldots, \eta(e_{r(R)}) \rangle \in R^{\mathcal{B}})$$
3. For every $f \in \Phi$, tuple $e_1, \ldots, e_{r(f)} \in |\mathcal{A}|$,
$$\eta(f^{\mathcal{A}}(e_1, \ldots, e_{r(f)})) \quad = \quad f^{\mathcal{B}}(\eta(e_1), \ldots, \eta(e_{r(f)}))$$



An isomorphism changes only the names of the elements of the universe. All the symbols of Σ are preserved.

Definition 11.6 Let $\mathcal{A}, \mathcal{B} \in$ STRUC$[\Sigma]$. We say that $\mathcal{A}$ and $\mathcal{B}$ are *elementarily equivalent* ($\mathcal{A} \equiv \mathcal{B}$) iff for all sentences $\varphi \in \mathcal{L}(\Sigma)$, $A \models \varphi \quad \Leftrightarrow \quad B \models \varphi$. ♠

Proposition 11.7 *If $\mathcal{A} \cong \mathcal{B}$ then $\mathcal{A} \equiv \mathcal{B}$.*