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: $T : X' \subseteq X \to \{\mathbf{true}, \mathbf{false}\}$

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

If $\mathit{var}(\varphi) \subseteq X'$, 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.

First-Order Logic with Equality

Vocabulary: $\Sigma = (\Phi, \Pi, r)$:
Φ: function symbols, Π: predicate symbols, r: arity

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

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

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

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

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

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

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

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

$\mathcal{L}(\Sigma)$ = set of formulas of vocabulary $\Sigma = (\Phi, \Pi, r)$

terms: inductive definiton of 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: inductive definiton of formulas

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

More Abbreviations:

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

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

$\mathcal{L}(\Sigma_N)$ Abbreviations:

$$
\begin{array}{lcl}
t_1 \le t_2 & \hookrightarrow & (t_1 = t_2 \ \vee \ t_1 < t_2) \\
1 & \hookrightarrow & \sigma(0) \\
2 & \hookrightarrow & \sigma(1) \\
3 & \hookrightarrow & \sigma(2) \\
t_1 | t_2 & \hookrightarrow & \exists x (t_1 \times x = t_2) \\
\textsf{prime}(t_1) & \hookrightarrow & 1 < t_1 \ \wedge \ \forall x (x | t_1 \to (x = 1 \vee x = t_1))
\end{array}
$$

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. $\forall x \exists y(x < y \ \wedge \ \textsf{prime}(y))$
5. $\forall xy(\sigma(x) = \sigma(y) \ \to \ x = y)$
6. $\forall xy(x < y \ \to \ \sigma(x) \le y)$

$\mathcal{L}(\Sigma_g)$

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

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

Free and Bound Variables

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.

A first-order formula says something about its free variables.

Logical Structures

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

The **interpretation** μ maps each symbol, α of Σ to its **meaning** $\mu(\alpha) = \alpha^{\mathcal{A}}$ in $\mathcal{A}$.

$|\mathcal{A}|$ is the **universe** so $\forall x$ means "for all elements $x \in |\mathcal{A}|$."

$$\begin{array}{rl} \mu : V \longrightarrow |A| & \mu : x \mapsto \mu(x) = x^{\mathcal{A}} \\ \mu : \Phi \longrightarrow \text{total functions on } U^{O(1)} & \mu : f \mapsto \mu(f) = f^{\mathcal{A}} : U^{r(f)} \longrightarrow U \\ \mu : \Pi \longrightarrow \text{relations on } U^{O(1)} & \mu : R \mapsto \mu(R) = R^{\mathcal{A}} \subseteq U^{r(R)} \end{array}$$

Example: A graph, $\mathcal{G} = (\{v_1, \ldots v_n\}, s^{\mathcal{G}}, t^{\mathcal{G}}, E^{\mathcal{G}})$ is a structure of vocabulary Σ_G, i.e, $\mathcal{G} \in \mathrm{STRUC}[\Sigma_G]$.

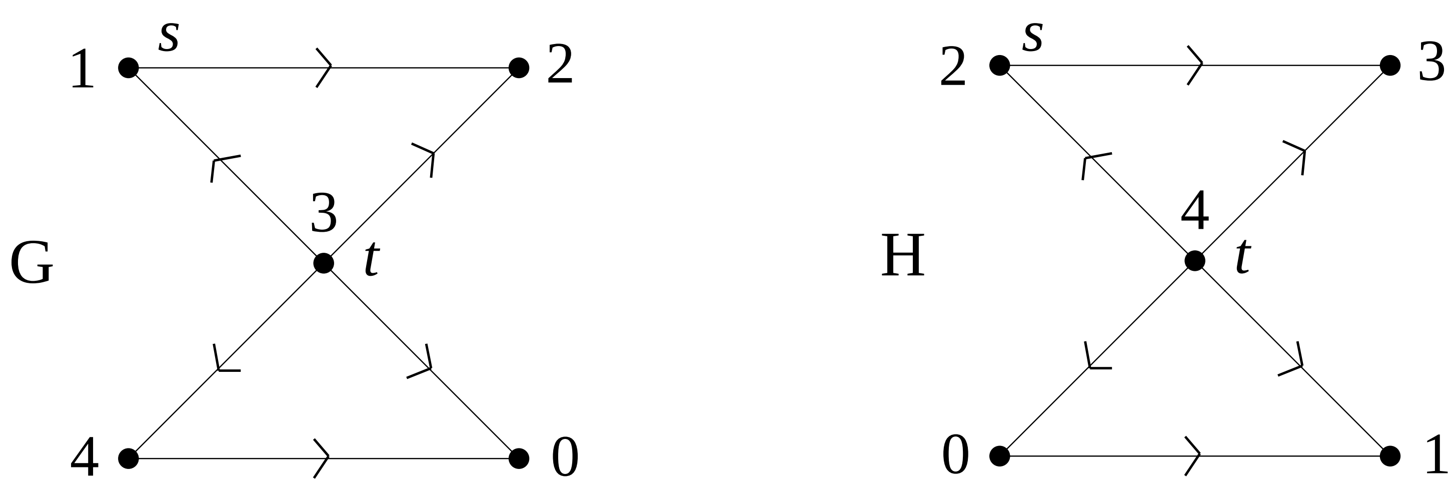
$$s^{\mathcal{G}}, t^{\mathcal{G}} \in \{v_1, \ldots, v_n\};\ E^{\mathcal{G}} \subseteq \{v_1, \ldots, v_n\} \times \{v_1, \ldots, v_n\}$$

$$G = \langle V^G, s^G, t^G, E^G \rangle, H = \langle V^H, s^H, t^H, E^H \rangle \in \text{STRUC}[\Sigma_g]$$

$$s^G = 1, \quad t^G = 3; \qquad s^H = 2, \quad t^H = 4$$

$$V^G = \{0, 1, 2, 3, 4\}; \; E^G = \{(1,2), (3,0), (3,1), (3,2), (3,4), (4,0)\}$$

$$V^H = \{1, 2, 3, 4, 0\}; \; E^H = \{(2,3), (4,1), (4,2), (4,3), (4,0), (0,1)\}$$



$$G \cong H$$

Binary String: $w =$ "01101"

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

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

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

Relational Database

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

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

$$\begin{aligned}
U_0 &= \{\text{Abraham, Isaac, Rebekah, Sarah, } \ldots\} \\
F_0 &= \{\text{Sarah, Rebekah, } \ldots\} \\
P_0 &= \{\langle \text{Abraham,Isaac} \rangle, \langle \text{Sarah,Isaac} \rangle, \ldots\} \\
S_0 &= \{\langle \text{Abraham,Sarah} \rangle, \langle \text{Isaac,Rebekah} \rangle, \ldots\}
\end{aligned}$$

$$\begin{aligned}
\varphi_{sibling}(x, y) \quad &\equiv \quad \exists f, m(x \neq y \land f \neq m \ \land \\
&\qquad P(f, x) \land P(f, y) \land P(m, x) \land P(m, y))
\end{aligned}$$

$$\begin{aligned}
\varphi_{aunt}(x, y) \quad &\equiv \quad \exists p, s(P(p, y) \land \varphi_{sibling}(p, s) \land \\
&\qquad (s = x \lor S(x, s)) \ \land \ F(x))
\end{aligned}$$

$\mathbf{N} = (\mathbf{N}, 0, \sigma, +, \times, \uparrow, <)$, 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

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

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

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