CS 245

Let Σ be a consistent set of formulae in $Form(L)$.

Def. Σ is maximal consistent

if Σ is consistent and

for all $A \in \text{Form}(\mathcal{L})$

if $A \notin \Sigma$ then $\Sigma \cup \{A\}$

is inconsistent.

Given a maximal consistent set Σ^* we can construct a valuation, v, such that for all $A \in Form(L)$, $A^v = \underline{1}$ if and only if $A \in \Sigma^*$.

Fact: If $\Sigma \subseteq Form(L)$ and Σ is consistent then Σ is satisfiable.

Fact: If $\Sigma \subseteq Form(L)$ and $A \in Form(L)$ then if $\Sigma \models A$ then $\Sigma \vdash A$.

Example: Consider a graph

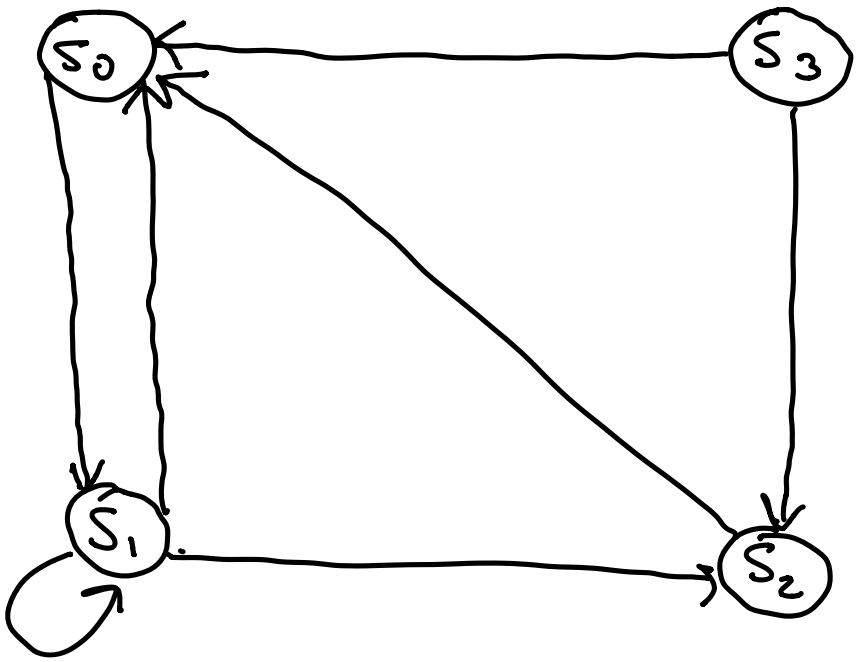
G with a set of states

$S = \{s_0, s_1, s_2, s_3\}$ and an edge

relation, $R = \{(s_0, s_1), (s_1, s_0),$

$(s_1, s_1), (s_1, s_2), (s_2, s_0), (s_3, 0),$

$(s_3, s_2)\}$.



A directed graph.

Notice that a graph like G can be used to represent the behavior of a (finite state) program, or an embedded system or hardware model.

We can then represent statements about graph in first order logic and evaluate those statement with respect to valuations over domains that represent graphs.

For instance, we can write $E(n_0, n_1)$ to represent the statement that there is an edge from the node associated with n_0 to the node associated with n_1.

If we write $\exists x \exists y \, E(x, y)$ then this will evaluate to $\underline{1}$ on graphs with at least one edge.

Can we write formulae that express

- The graph has two vertices.
- The graph has at least one edge from a node to itself.

- The graph contains a node that has no incoming edges.

If we think of the graph as representing the states and transitions of a (finite state) program we can ask questions relating to the correctness of the program.

- Are all states of the program 'good'?

An important question in studing graph theory, and program correctness is the question of reachability.

Given a graph $G = (S, R)$ and nodes $s_0, s_1 \in S$ we say that there is a path from s_0 to s_1 in R if there exists $n \in \mathbb{N}$ such that
- for all $i \in [0..n]$: $t_i \in S$
- for all $j \in [0..n-1]$: $(t_j, t_{j+1}) \in R$
- $s_0 = t_0$
- $s_1 = t_n$

Reachability: given nodes s_0 and s_1 in directed graph G then s_1 is reachable from s_0 if there is a path in G from s_0 to s_1.

Notice that being able to answer the reachability question (i.e. is s_i reachable from s_0) is important in both a graph theoretic sense and a program correctness sense.

For program correctness,
if we could solve the
reachability problem on
program transition graphs
we could ask whether
a 'bad' state is reachable
from an initial 'good' state.

Generalizing from reachability of a single bad state allows other important questions to be asked: are all (reachable) program states 'good'?

- Can a deadlock state be reached?

Can reachability be expressed in first-order logic?

$E(u_0, u_1)$

expresses that u_1 is reachable from u_0 in one transition.

$$\exists x \, (E(u_0, x) \wedge E(x, u_1))$$

Expresses that u_1 is reachable from u_0 by a path of length 2.

So it seems clear that for any finite, fixed, k we can write that u_1 is reachable from u_0 by a path of length k.

$$\exists x_1 \dots x_{k-1} \left(E(u_0, x_1) \wedge \dots \wedge E(x_{k-1}, u_1) \right)$$

However a difficulty arrises from the requirement that u_1 is reachable from u_0 by some path of arbitrary finite (but unbounded) length.

A formula expressing reachability, if it exists, must be of finite length.

Def. A sentence is a formula of first order logic with no free variables.

Compactness: Let Γ be a set of sentences of first order logic. If all finite subsets of Γ are satisfiable then Γ is satisfiable.

Proof idea: Suppose that the finite subsets of Γ are each satisfiable but Γ is not satisfiable.

Then $\Gamma \models A \wedge \neg A$ holds as there is no domain D and valuation v such that $[\![\Gamma]\!]^v = \mathbb{1}$.

From the completeness of ND for first order logic we have $\Gamma \vdash A \wedge \neg A$.

The proof in ND is of finite length using say Δ sentences from Γ.

This implies that $\Delta \vdash A \wedge \neg A$.

From the soundness of ND proofs we have $\Delta \models A \wedge \neg A$.

Since Δ is a finite subset of Γ then Δ is satisfiable by some valuation v under domain D.

Therefore since $\Delta \models A \wedge \neg A$ and $\Delta^v = \underline{1}$ then $(A \wedge \neg A)^v = \underline{1}$, a contradiction.

Fact: (Löwenheim-Skolem Theorem)
Let A be a sentence of first order logic such that for any $n \in \mathbb{N}$, $n \geq 1$, there is a domain D and valuation v, with at least n elements in D, such that $A^v = \mathcal{I}$. Then A has a domain D' and valuation v' such that $A^{v'} = \underline{1}$ and D' has an infinite number of elements.

Proof idea: Consider the formula

$$B_n : \exists x_1 \ldots x_n \bigwedge_{1 \leq i < j \leq n} \neg (x_i \approx x_j)$$

Each sentence, B_n, expresses that a domain satisfying the sentence has at least n elements.

Let $\Gamma = \{A\} \cup \{B_n \mid n \geq 1\}$.

Suppose Δ is a finite subset of Γ.

Consider $k \geq 1$ and $n \leq k$ for all $B_n \in \Delta$. Since Δ is a finite set there is some such k.

By assumption $\{A, B_k\}$ is satisfiable. Since $B_k \to B_n$ for all $n \leq k$ it follows that Δ is satisfiable.

By the compactness result it follows that Γ is satisfiable.

Since the domain D and valuation v exists such that $\Gamma^v = \underline{1}$ then D cannot have a finite number of elements.

Fact: Reachability is not expressible in first order logic.

There is no formula $A(u_0, u_1)$ whose only free variables are u_0 and u_1 and R is its only predict symbol such that $A(u_0, u_1)$ holds in a graph G iff there is a path in the graph from the node associated with u_0 to the node associated with u_1.

Proof idea: Suppose such a formula $A(u_0, u_1)$ existed.

Let c_0 and c_1 be individual symbols.

Let B_n be the formula expressing that there is a path of length n from c_0 to c_1.

B_0 : $c_0 = c_1$

B_1 : $R(c_0, c_1)$

for $n \geq 1$

B_n: $\exists x_1 \ldots \exists_{n-1} (R(c_0, x_1) \wedge R(x_1, x_2) \wedge \ldots \wedge R(x_{n-1}, c_1))$.

Then let $\Delta = \{\neg B_i \mid i \geq 0\} \cup \{A(c_0, c_1)\}$.

The formulae of Δ are all sentences and Δ itself is unsatisfiable.

Δ is unsatisfiable since the $\neg B_i$ say there is no finite path from c_0 to c_1 and $A(c_0, c_1)$ says there is a finite path from c_0 to c_1.

On the other hand every finite subset of Δ is satisfiable. The compactness result says that since every finite subset of Δ is satisfiable then Δ is satisfiable. This is a contradiction, therefore there is no such formula $A(u_1, u_2)$.