G22.3033-002 Logic in Computer Science
Lecture 6
Review

Last time

- A Deductive Calculus
Outline

- Soundness
- Homomorphisms
- Completeness

Sources:

Sections 2.2 and 2.5 of Enderton.
**Soundness and Completeness**

An important question for any calculus is its relationship to the semantic notion of validity.

If only valid formulas are deducible, then the calculus is said to be *sound*.

If all valid formulas are deducible, then the calculus is said to be *complete*.

The existence of a sound and complete calculus for first-order logic is an important result which demonstrates that it is a reasonable model of mathematical thinking.
Soundness

Soundness Theorem

If $\Gamma \vdash \phi$, then $\Gamma \models \phi$.

Proof

The idea of the proof is that the logical axioms are logically valid, and that modus ponens preserves logical implications.

We first assume the axioms are valid and prove by induction that any formula $\phi$ deducible from $\Gamma$ is logically implied by $\Gamma$.

- Case 1: if $\phi$ is a logical axiom, then by our assumption, $\models \phi$, and thus $\Gamma \models \phi$.

- Case 2: If $\phi \in \Gamma$, then clearly $\Gamma \models \phi$.

- Case 3: If $\phi$ is obtained by modus ponens from $\psi$ and $\psi \rightarrow \phi$, then by the inductive hypothesis, $\Gamma \models \psi$ and $\Gamma \models (\psi \rightarrow \phi)$. It follows by the definition of $\models$ for $\rightarrow$ that $\Gamma \models \phi$. 
Soundness

It remains to show that the axioms are valid. We will consider only Axiom Group 2 (the others are straightforward). First a lemma.

Substitution Lemma

If the term $t$ is substitutable for the variable $x$ in the wff $\phi$, then for any model $M$ and variable assignment $\rho$, $M \models_\rho \phi^x_t$ iff $M \models_\rho (x|\bar{\rho}(t)) \phi$.

This lemma states that if we replace a variable $x$ with a term $t$, the semantics are the same as if the variable assignment is modified so that $x$ takes on the same value as the term $t$.

The proof is by induction on $\phi$.

Now, consider Axiom Group 2: $\forall x \alpha \rightarrow \alpha^x_t$, where $t$ is substitutable for $x$ in $\alpha$.

Assume $M \models_\rho \forall x \alpha$. We must show that $M \models_\rho \alpha^x_t$. We know from $M \models_\rho \forall x \alpha$ that for any $d \in \text{dom}(M)$, $M \models_\rho (x|d) \alpha$. In particular, if we let $d = \bar{\rho}(t)$, then we have $M \models_\rho (x|\bar{\rho}(t)) \alpha$. But by the substitution lemma, this implies that $M \models_\rho \alpha^x_t$. 
Soundness Corollaries

Corollary
If $\vdash (\phi \leftrightarrow \psi)$, then $\phi$ and $\psi$ are logically equivalent.

Corollary
If $\phi'$ is an alphabetic variant of $\phi$, then $\phi$ and $\phi'$ are logically equivalent.

Recall that a set $\Gamma$ is consistent iff there is no formula $\phi$ such that both $\Gamma \vdash \phi$ and $\Gamma \vdash \neg \phi$. Define $\Gamma$ to be satisfiable iff there is some model $M$ and variable assignment $\rho$ such that $M \models_{\rho} \Gamma$.

Corollary
If $\Gamma$ is satisfiable, then $\Gamma$ is consistent.
Completeness

Completeness Theorem (Gödel, 1930)

If $\Gamma \models \phi$, then $\Gamma \vdash \phi$.

This is equivalent to the following statement: any consistent set of formulas is satisfiable.
Homomorphisms

Suppose that \( \mathcal{A} \) and \( \mathcal{B} \) are models over the same signature \( \Sigma \).

A \textit{homomorphism} \( h \) of \( \mathcal{A} \) into \( \mathcal{B} \) is a function \( h : \text{dom}(\mathcal{A}) \to \text{dom}(\mathcal{B}) \) such that

1. For each \( n \)-ary predicate symbol \( P \in \Sigma \) and each \( n \)-tuple \( \langle a_1, \ldots, a_n \rangle \) of elements of \( \text{dom}(\mathcal{A}) \),
   
   \[
   \text{if } \langle a_1, \ldots, a_n \rangle \in P^\mathcal{A}, \text{ then } \langle h(a_1), \ldots, h(a_n) \rangle \in P^\mathcal{B}.
   \]

2. For each \( n \)-ary function symbol \( f \in \Sigma \) and each \( n \)-tuple \( \langle a_1, \ldots, a_n \rangle \) of elements of \( \text{dom}(\mathcal{A}) \),

   \[
   h(f^\mathcal{A}(a_1, \ldots, a_n)) = f^\mathcal{B}(h(a_1), \ldots, h(a_n)).
   \]

3. For each constant symbol \( c \in \Sigma \), \( h(c^\mathcal{A}) = c^\mathcal{B} \).

If (1) also holds in reverse, then \( h \) is a \textit{strong homomorphism} (this is what the book calls a homomorphism).

A strong homomorphism which is injective (one-to-one) is an \textit{embedding}.

An embedding which is surjective (onto) is an \textit{isomorphism}.

A homomorphism of \( \mathcal{A} \) into \( \mathcal{A} \) is called an \textit{endomorphism} of \( \mathcal{A} \).

An isomorphism of \( \mathcal{A} \) to \( \mathcal{A} \) is called an \textit{automorphism} of \( \mathcal{A} \).
Example

Let $\mathcal{A} = (\mathcal{N}, +, \times)$, and let $\mathcal{B} = (\{0, 1\}, +[2], \times)$.

Define $h : \mathcal{N} \to \{0, 1\}$ by: $h(n) = \begin{cases} 0 & \text{if } n \text{ is even} \\ 1 & \text{if } n \text{ is odd} \end{cases}$

Then $h$ is a homomorphism.

Proof

The proof is by cases. For example, suppose $a, b \in \mathcal{N}$ and both are odd.

Then $a + b$ is even, so $h(a + b) = 0$. Similarly, $h(a) = h(b) = 1$, so $h(a) +[2] h(b) = 0$.

Also, $a \times b$ is odd, so $h(a \times b) = 1$. Similarly, $h(a) \times h(b) = 1$.

The other cases are similar.
Substructures and Extensions

Let $\mathcal{P}$ be the set of positive integers.

Then there is an isomorphism $h$ from $(\mathcal{P}, <)$ to $(\mathcal{N}, <)$ defined by $h(n) = n - 1$.

Note also that the identity map is an embedding of $(\mathcal{P}, <)$ into $(\mathcal{N}, <)$.

Because of this, we say that $(\mathcal{P}, <)$ is a substructure of $(\mathcal{N}, <)$.

More generally, if $\mathcal{A}$ and $\mathcal{B}$ are models with $\text{dom}(\mathcal{A}) \subseteq \text{dom}(\mathcal{B})$ and the identity map $i : \text{dom}(\mathcal{A}) \to \text{dom}(\mathcal{B})$ is an embedding, then we say that $\mathcal{B}$ is an extension of $\mathcal{A}$ and that $\mathcal{A}$ is a substructure of $\mathcal{B}$.
Homomorphism Theorem

Let $h$ be a strong homomorphism from $\mathcal{A}$ to $\mathcal{B}$, and let $\rho$ map the set of variables into $\text{dom}(\mathcal{A})$.

1. For any term $t$, $h(\overline{\rho}(t)) = \overline{h \circ \rho}(t)$, where $\overline{\rho}$ is computed in $\mathcal{A}$, and $\overline{h \circ \rho}(t)$ is computed in $\mathcal{B}$.

2. For any quantifier-free formula $\alpha$ not containing the equality symbol,
   
   $\mathcal{A} \models_{\rho} \alpha$ iff $\mathcal{B} \models_{h \circ \rho} \alpha$.

3. If $h$ is an embedding, then the above holds even if $\alpha$ contains the equality symbol.

4. If $h$ is surjective (onto), then the above holds even if $\alpha$ contains quantifiers.
Proof of Homomorphism Theorem

1. This follows from a simple inductive argument on $t$.

2. For an atomic formula, we have

$$
\mathcal{A} \models_{\rho} Pt \iff \bar{\rho}(t) \in P^A \\
\iff h(\bar{\rho}(t)) \in P^B \quad \text{defn. of strong homomorphism}
$$

$$
\iff \overline{h \circ \rho(t)} \in P^B \\
\iff \mathcal{B} \models_{h \circ \rho} Pt
$$

The more general case follows by induction on $\neg$ and $\rightarrow$.

3. Same argument as above, except that $P$ is replaced by $=$, and the justification in the second step is replaced with the fact that $h$ is one-to-one.

4. The intuition is that if $h$ is onto, then each $b \in \mathcal{B}$ corresponds to some $h(a)$, so if something holds for everything in $\mathcal{A}$ it will also hold for everything in $\mathcal{B}$.
Automorphism Corollary

As a corollary of the homomorphism theorem, we have the following:

**Theorem**

An automorphism must preserve definable relations: if \( h \) is an automorphism of \( \mathcal{A} \), and \( R \) is an \( n \)-ary relation on \( \text{dom}(\mathcal{A}) \) definable in \( \mathcal{A} \), then for any \( a_1, \ldots, a_n \in \text{dom}(\mathcal{A}) \),

\[
\langle a_1, \ldots, a_n \rangle \in R \iff \langle h(a_1), \ldots, h(a_n) \rangle \in R.
\]

**Proof**

Let \( \phi \) be the formula which defines \( R \) in \( \mathcal{A} \). By the homomorphism theorem,

\[
\mathcal{A} \models_\rho \phi \iff \mathcal{A} \models_{h \circ \rho} \phi.
\]

It follows that

\[
\mathcal{A} \models \phi[[a_1, \ldots, a_n]] \iff \mathcal{A} \models \phi[[h(a_1), \ldots, h(a_n)]]
\]

and thus

\[
\langle a_1, \ldots, a_n \rangle \in R \iff \langle h(a_1), \ldots, h(a_n) \rangle \in R.
\]
Undeniable Relations

We can sometimes use this corollary to show that a given relation is *not* definable.

Consider the model \((\mathcal{R}, <)\) consisting of the set of real numbers with its usual ordering. We will show that the set \(\mathcal{N}\) of natural numbers is not definable in this model.

An automorphism of this model is any bijection from \(\mathcal{R}\) to \(\mathcal{R}\) which is strictly increasing:

\[ a < b \text{ iff } h(a) < h(b). \]

One such function is \(h(a) = a^3\).

Now, if \(\mathcal{N}\) were definable then by the above corollary we would have \(a \in \mathcal{N}\) iff \(a^3 \in \mathcal{N}\) which is clearly untrue.
Definability of a Class of Structures

A *theory* is a set of sentences. For a given signature $\Sigma$, a $\Sigma$-theory is a set of sentences, each of which is a $\Sigma$-formula.

If $\mathcal{K}$ is a class of models with signature $\Sigma$, we say that a $\Sigma$-theory $T$ *axiomatizes* $\mathcal{K}$ or is a *set of axioms* for $\mathcal{K}$ if $\mathcal{K}$ is the class of all models of $T$.

For an arbitrary $\Sigma$-theory $T$, let $\text{Mod}T$ be the class of all models of $T$ (over signature $\Sigma$).

A class $\mathcal{K}$ of models is *first-order definable*, also known as an *elementary class* (EC), iff $\mathcal{K} = \text{Mod}\tau$ for some sentence $\tau$.

A class $\mathcal{K}$ of models is *first-order axiomatizable*, or *generalized first-order definable*, also known as an *elementary class in the wider sense* (EC$_\Delta$), iff $\mathcal{K} = \text{Mod}T$ for some set of sentences $T$. 
Example

Consider a signature \((P)\) with a single binary predicate symbol \(P\).

A model \((A, R)\) is an ordered set iff \(R\) is transitive and satisfies the trichotomy condition (which states that for any \(a, b \in A\) exactly one of \(\langle a, b \rangle \in R\), \(a = b\), \(\langle b, a \rangle \in R\) holds).

This can be written as a first-order sentence as follows:

\[
\forall x \forall y \forall z \left( Pxy \rightarrow Pyz \rightarrow Pxz \right) \land \\
\forall x \forall y \left( Pxy \lor x = y \rightarrow Pyx \right) \land \\
\forall x \forall y \left( Pxy \rightarrow \neg Pyx \right).
\]

Because these can be translated into a sentence, the class of (nonempty) ordered sets is first-order definable.
Example

Consider a signature \((\circ)\) with a single binary function symbol \(\circ\).

The class of all groups is defined by the following sentence:

\[
\forall x \forall y \forall z \ (x \circ (y \circ z) = (x \circ y) \circ z) \land \\
\forall x \forall y \exists z \ (x \circ z = y) \land \\
\forall x \forall y \exists z \ (z \circ x = y).
\]

The class of all \textit{infinite} groups is first-order axiomatizable. To see this, let

\[
\lambda_2 = \exists x \exists y \ x \neq y,
\]

\[
\lambda_3 = \exists x \exists y \exists z \ (x \neq y \land x \neq z \land y \neq z),
\]

\[\ldots\]

\[
\lambda_n = \text{there are at least } n \text{ distinct objects}
\]

Then the class of infinite groups is axiomatized by the sentence for groups together with the set of sentences \(\{\lambda_2, \lambda_3, \ldots\}\).

The class of infinite groups is \textit{not} first-order definable.
Completeness

Completeness Theorem (Gödel, 1930)

If $\Gamma \models \phi$, then $\Gamma \vdash \phi$.

This is equivalent to the following statement: any consistent set of formulas is satisfiable.