

G22.2390-001 Logic in Computer Science
Fall 2009
Lecture 6

Review

Last time

- Proofs
- A Deductive Calculus
- Deduction Rules
- Soundness

Outline

- solution for Exercise 6, p. 99
- 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 and Completeness

Soundness Theorem

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

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 Σ .

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

1. For each n -ary predicate symbol $P \in \Sigma$ and each n -tuple $\langle a_1, \dots, a_n \rangle$ of elements of $\text{dom}(\mathcal{A})$,

$$\langle a_1, \dots, a_n \rangle \in P^{\mathcal{A}} \text{ iff } \langle h(a_1), \dots, h(a_n) \rangle \in P^{\mathcal{B}}.$$

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

$$h(f^{\mathcal{A}}(a_1, \dots, a_n)) = f^{\mathcal{B}}(h(a_1), \dots, h(a_n)).$$

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

Some versions of this theorem only require (1) to hold for the “only if” direction.

The above definition is then called a *strong homomorphism*.

A homomorphism which is injective (one-to-one) is an *embedding*.

An embedding which is surjective (onto) is an *isomorphism*.

A homomorphism of $\mathcal{A}$ into $\mathcal{A}$ is called an *endomorphism* of $\mathcal{A}$.

An isomorphism of $\mathcal{A}$ to $\mathcal{A}$ is called an *automorphism* of $\mathcal{A}$.

Example

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

Define $h : \mathcal{N} \rightarrow \{0, 1\}$ 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 $i : \text{dom}(\mathcal{A}) \rightarrow \text{dom}(\mathcal{B})$ 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 homomorphism from $\mathcal{A}$ to $\mathcal{B}$, and let s map the set of variables into $\text{dom}(\mathcal{A})$.

1. For any term t , $h(\bar{s}(t)) = \overline{h \circ s}(t)$, where $\bar{s}$ is computed in $\mathcal{A}$, and $\overline{h \circ s}(t)$ is computed in $\mathcal{B}$.
2. For any quantifier-free formula α not containing the equality symbol,
 $\models_{\mathcal{A}} \alpha[s]$ iff $\models_{\mathcal{B}} \alpha[h \circ s]$.
3. If h is an embedding, then the above holds even if α contains the equality symbol.
4. If h is surjective (onto), then the above holds even if α contains quantifiers.

Proof of Homomorphism Theorem

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

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

This follows from a simple inductive argument on t .

2. For any quantifier-free formula α not containing the equality symbol,

$$\models_{\mathcal{A}} \alpha[s] \text{ iff } \models_{\mathcal{B}} \alpha[h \circ s].$$

For an atomic formula, we have:

$$\begin{aligned} \models_{\mathcal{A}} Pt[s] &\Leftrightarrow \bar{s}(t) \in P^{\mathcal{A}} \\ &\Leftrightarrow h(\bar{s}(t)) \in P^{\mathcal{B}} && \text{defn. of homomorphism} \\ &\Leftrightarrow \overline{h \circ s}(t) \in P^{\mathcal{B}} && \text{by (1)} \\ &\Leftrightarrow \models_{\mathcal{B}} Pt[h \circ s] \end{aligned}$$

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

Proof of Homomorphism Theorem

3. If h is an embedding, then for any quantifier-free formula α ,

$$\models_{\mathcal{A}} \alpha[s] \text{ iff } \models_{\mathcal{B}} \alpha[h \circ s].$$

The argument for atomic formulas without equality is as above. For an equality, we have:

$$\begin{aligned} \models_{\mathcal{A}} u = t[s] &\Leftrightarrow \bar{s}(u) = \bar{s}(t) \\ &\Leftrightarrow h(\bar{s}(u)) = h(\bar{s}(t)) && h \text{ is 1-1.} \\ &\Leftrightarrow \overline{h \circ s}(u) = \overline{h \circ s}(t) && \text{by (1)} \\ &\Leftrightarrow \models_{\mathcal{B}} u = t[h \circ s] \end{aligned}$$

As before, the more general case then follows by induction on $\neg$ and $\rightarrow$.

4. If h is surjective (onto), then the above statements hold even for formulas with quantifiers.

In addition to the arguments given above, we must show an additional inductive case: if α has the property that for every s , $\models_{\mathcal{A}} \alpha[s]$ iff $\models_{\mathcal{B}} \alpha[h \circ s]$, then $\forall x \alpha$ has this same property.

Thus, we must show that for every s , $\models_{\mathcal{A}} \forall x \alpha[s]$ iff $\models_{\mathcal{B}} \forall x \alpha[h \circ s]$.

Proof of Homomorphism Theorem

We must show that for every s , $\models_{\mathcal{A}} \forall x \alpha[s]$ iff $\models_{\mathcal{B}} \forall x \alpha[h \circ s]$.

We start with the if direction. Suppose $a \in \text{dom}(\mathcal{A})$.

$$\begin{aligned} \models_{\mathcal{B}} \forall x \alpha[h \circ s] &\Rightarrow \models_{\mathcal{B}} \alpha[(h \circ s)(x|h(a))] && \text{semantics of } \forall \\ &\Leftrightarrow \models_{\mathcal{B}} \alpha[h \circ (s(x|a))] && (h \circ s)(x|h(a)) = h \circ (s(x|a)) \\ &\Leftrightarrow \models_{\mathcal{A}} \alpha[s(x|a)] && \text{ind. hypothesis} \end{aligned}$$

Since a was chosen arbitrarily, it follows that $\models_{\mathcal{A}} \forall x \alpha[s]$.

For the other direction, suppose $\not\models_{\mathcal{B}} \forall x \alpha[h \circ s]$:

$$\begin{aligned} \not\models_{\mathcal{B}} \forall x \alpha[h \circ s] &\Rightarrow \models_{\mathcal{B}} \neg \alpha[(h \circ s)(x|b)] && \text{for some } b \in \text{dom}(\mathcal{B}) \\ &\Rightarrow \models_{\mathcal{B}} \neg \alpha[(h \circ s)(x|h(a))] && h \text{ is onto} \\ &\Leftrightarrow \models_{\mathcal{B}} \neg \alpha[h \circ (s(x|a))] && (h \circ s)(x|h(a)) = h \circ (s(x|a)) \\ &\Leftrightarrow \models_{\mathcal{A}} \neg \alpha[s(x|a)] && \text{ind. hypothesis} \\ &\Rightarrow \not\models_{\mathcal{A}} \forall x \alpha[s] && \text{semantics of } \forall \end{aligned}$$

□

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 $a_1, \dots, a_n \in \text{dom}(\mathcal{A})$,

$$\langle a_1, \dots, a_n \rangle \in R \text{ iff } \langle h(a_1), \dots, h(a_n) \rangle \in R.$$

Proof

Let ϕ be the formula which defines R in $\mathcal{A}$. By the homomorphism theorem,

$$\models_{\mathcal{A}} \phi[s] \text{ iff } \models_{\mathcal{A}} \phi[h \circ s].$$

It follows that

$$\models_{\mathcal{A}} \phi[[a_1, \dots, a_n]] \text{ iff } \models_{\mathcal{A}} \phi[[h(a_1), \dots, h(a_n)]],$$

and thus

$$\langle a_1, \dots, a_n \rangle \in R \text{ iff } \langle h(a_1), \dots, h(a_n) \rangle \in R.$$

□

Undefinable 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.

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.