Proofs

What is the meaning of the following statement?:

$$\Gamma \models \phi$$

In propositional logic, it means that every truth assignment which makes every formula in Γ true also makes ϕ true.

In first-order logic, it means that every model and variable assignment which makes every formula in Γ true also makes ϕ true.

How do we demonstrate or convince a skeptic of these facts?

In propositional logic, a skeptic could use a truth table to check whether $\Gamma \models \phi$.

In first-order logic, no such method exists: we cannot, in general, enumerate all possible models and variable assignments.

Instead, we rely on the notion of a formal mathematical proof.

What is a Proof?

A *proof* is a convincing argument made up of a finite sequence of fixed indisputable steps.

Mathematicians, including the author of the textbook, rely on proofs to convince their audience of the mathematical truth of a proposition.

For the most part, proofs are arguments *about* mathematical objects, but are not mathematical objects themselves. Let's call these "informal" proofs.

In logic, because part of our purpose is to study proofs themselves, we will define proofs that are themselves mathematical objects. We refer to such proofs as *formal proofs* or *deductions*.

Deductions are built from *axioms*, facts which we accept without proof, *assumptions*, facts assumed to be true for the purpose of the deduction, and *rules of inference*, an agreed-upon set of rules for creating new facts from old. Any fact that can be derived in this manner is a (formal) *theorem*.

A particular choice of axioms and rules of inference is often referred to as a *calculus*.

Proofs

Note that because a proof is finite and each step conforms to a pre-determined set of rules, the question of whether a given sequence of steps is a valid proof is decidable.

Thus, a proof is an effective mechanism for convincing a skeptic.

The interplay of formal and informal proofs is a potential source of confusion, especially since we often use informal proofs to prove things about formal proofs! To avoid confusion, remember:

- An informal proof is a convincing argument *about* mathematical objects.
- A formal proof or deduction is a mathematical object *itself*: a sequence of theorems obtained using a specific set of axioms, assumptions, and rules of inference.

We will have more to say about the relationship between formal and informal proofs later in the semester.

Remember that an "informal" proof must still be convincing!

A Deductive Calculus for First-Order Logic

A calculus whose axioms are valid first-order formulas and whose rules of inference preserve first-order validity can be used to derive theorems which are valid first-order formulas.

There are many possible choices for axioms and rules of inference.

We present a calculus for first-order logic with an infinite number of axioms, which we will denote as Λ, and which uses only a single rule of inference, known as *modus ponens*.

This rule states that given formulas α and $\alpha \to \beta$ we may infer β.

Rules of inference are often written in the following format with the given formulas above and the deduced formula below:

$$\frac{\alpha, \alpha \to \beta}{\beta}.$$

A Deductive Calculus

A *deduction of* ϕ *from* Γ is a sequence $\langle \alpha_0, \ldots, \alpha_n \rangle$ of formulas such that $\alpha_n = \phi$ and for each $i \leq n$ either

- α_i is in $\Gamma \cup \Lambda$, or
- for some j and k less than i, α_i is obtained by modus ponens from α_j and α_k (i.e. $\alpha_k = \alpha_j \rightarrow \alpha_i$).

If such a deduction exists, we say that ϕ is *deducible* from Γ or that ϕ is a *theorem* of Γ, and we write $\Gamma \vdash \phi$.

The set of theorems of Γ is the set generated from $\Gamma \cup \Lambda$ by modus ponens.

Note that although this is a well-defined inductive definition, the set is not freely generated.

A set of formulas Δ is *closed under modus ponens* iff whenever α and $\alpha \rightarrow \beta$ are in Δ, so is β.

Our definition of deduction gives rise to the following induction principle.

Induction Principle

Suppose that S is a set of wffs that includes $\Gamma \cup \Lambda$ and is closed under modus ponens. Then S contains every theorem of Γ.

Axioms

A *wff* ϕ is a *generalization* of ψ iff for some variables $x_1, \ldots, x_n$, where $n \geq 0$, we have $\phi = \forall x_1 \ \cdots \forall x_n \ \psi$.

The axioms Λ are made up of all generalizations of *wffs* of the following forms, where x and y are variables and α and β are *wffs*.

1. Tautologies
2. $\forall x\, \alpha \to \alpha_t^x$, where t is substitutable for x in α;
3. $\forall x\, (\alpha \to \beta) \to (\forall x\, \alpha \to \forall x\, \beta)$;
4. $\alpha \to \forall x\, \alpha$, where x does not occur free in α;
5. $x = x$;
6. $x = y \to (\alpha \to \alpha')$, where α is atomic and α' is obtained from α by replacing x in zero or more places by y.

Note that the axioms depend on the definition of a well-formed formula which requires that a language be specified. The last two items are only included if the language includes equality.

Tautologies

Axiom group 1 consists of *tautologies*. These are the *wffs* obtainable from tautologies of propositional logic by replacing each propositional symbol by a *wff* of the first-order language.

For example, consider the propositional tautology

$$(A \to \neg B) \to (B \to \neg A).$$

A corresponding axiom is the formula

$$\forall x\, [(\forall y\, \neg Py \to \neg Px) \to (Px \to \neg \forall y\, \neg Py)].$$

There is a more direct way to view the relationship of first-order and propositional logic.

A first-order formula is *prime* if it is atomic or of the form $\forall x\, \alpha$.

First-order formulas correspond exactly to propositional logic formulas in which the set of propositional symbols is taken to be all prime first-order formulas.

By viewing first-order formulas as instances of propositional logic formulas, all propositional notions are also defined for first-order formulas.

Thus, the notions of *tautology*, *tautological consequence*, and *tautological implication* are thus directly applicable to first-order formulas.

Theorem

If Γ tautologically implies ϕ, then Γ logically implies ϕ.

Note that the converse fails.

Theorem

$\Gamma \vdash \phi$ iff $\Gamma \cup \Lambda$ tautologically implies ϕ.

Proof

$\Rightarrow$: Follows from the fact that modus ponens is propositionally valid.

$\Leftarrow$: By the compactness theorem for propositional logic, there is a finite subset $\Delta = \{\delta_1, \ldots, \delta_m\}$ of $\Gamma \cup \Lambda$ which tautologically implies ϕ. Thus, $\delta_1 \rightarrow \ldots \rightarrow \delta_m \rightarrow \phi$ is a tautology and hence is in Λ. By applying modus ponens m times, we obtain ϕ.

Substitution

The second axiom group contains formulas of the form $\forall\, x\ \alpha \rightarrow \alpha_t^x$.

The notation α_t^x denotes the expression obtained from α by replacing x, wherever it occurs free in α, by the term t.

We must also impose the restriction that t be *substitutable* for x in α. Informally, t is substitutable for x in α if no variables from t become bound when the substitution is made. Formally, this is defined as follows.

- For atomic α, t is substitutable for x in α.
- t is substitutable for x in $(\neg\alpha)$ iff it is substitutable for x in α, and t is substitutable for x in $(\alpha \rightarrow \beta)$ iff it is substitutable for x in both α and β.
- t is substitutable for x in $\forall\, y\ \alpha$ iff either
  - x does not occur free in $\forall\, y\ \alpha$, or
  - y does not occur in t and t is substitutable for x in α.

Example

For convenience, we repeat the first three axiom groups here:

1. Tautologies
2. $\forall x\, \alpha \to \alpha_t^x$, where t is substitutable for x in α;
3. $\forall x\, (\alpha \to \beta) \to (\forall x\, \alpha \to \forall x\, \beta)$;

We will give a deduction of: $\vdash \forall x\, (Px \to \exists y\, Py)$.

1.	$\forall x\, [(\forall y\, \neg Py \to \neg Px) \to (Px \to \neg \forall y\, \neg Py)]$	Tautology
2.	$(1) \to [\forall x\, (\forall y\, \neg Py \to \neg Px) \to \forall x\, (Px \to \neg \forall y\, \neg Py)]$	Axiom group 3
3.	$\forall x\, (\forall y\, \neg Py \to \neg Px) \to \forall x\, (Px \to \neg \forall y\, \neg Py)$	MP(1, 2)
4.	$\forall x\, (\forall y\, \neg Py \to \neg Px)$	Axiom group 2
5.	$\forall x\, (Px \to \neg \forall y\, \neg Py)$	MP(4, 3)

Reasoning About Deductions

Recall that our goal is to have a method to convince skeptics that $\Gamma \vdash \phi$.

If we can get the skeptic to believe in our deductive system (we'll tackle that issue shortly when we discuss *soundness*), then all we have to do is give a deduction of ϕ from Γ.

However, as you might imagine from the previous example, a deduction can be tedious and lengthy. For this reason, we introduce a number of shortcuts which can be used to show that $\Gamma \vdash \phi$ without giving an explicit deduction.

In each case we will have to justify that the given shortcut or rule is just as good as giving a deduction.

Generalization Theorem

Theorem

If $\Gamma \vdash \phi$ and x *does not occur free in any formula in* Γ, then $\Gamma \vdash \forall x\, \phi$.

Proof

It suffices to show that the set $\{\phi \mid \Gamma \vdash \forall x\, \phi\}$ includes $\Gamma \cup \Lambda$ and is closed under modus ponens.

- Suppose $\phi \in \Gamma$. Then x does not occur free in ϕ. Thus $\phi \rightarrow \forall x\, \phi$ is in axiom group 4, and it follows that $\Gamma \vdash \forall x\, \phi$.
- Suppose $\phi \in \Lambda$. Then $\forall x\, \phi$ is also an axiom, so $\Gamma \vdash \forall x\, \phi$.
- Suppose $\Gamma \vdash \forall x\, \psi$ and $\Gamma \vdash \forall x\, (\psi \rightarrow \phi)$. Using axiom group 3, we obtain $\Gamma \vdash \forall x\, \psi \rightarrow \forall x\, \phi$, and thus $\Gamma \vdash \forall x\, \phi$.

Theorem (rule T)

If $\Gamma \vdash \alpha_1, \ldots, \Gamma \vdash \alpha_n$ and $\{\alpha_1, \ldots, \alpha_n\}$ tautologically implies β, then $\Gamma \vdash \beta$.

Proof

Apply modus ponens n times to $\alpha_1 \rightarrow \cdots \rightarrow \alpha_n \rightarrow \beta$, which is a tautology.

Deduction Theorem

Theorem

If $\Gamma \cup \{\gamma\} \vdash \phi$ then $\Gamma \vdash (\gamma \rightarrow \phi)$.

Proof

$\Gamma \cup \{\gamma\} \vdash \phi$ iff $\Gamma \cup \{\gamma\} \cup \Lambda$ tautologically implies ϕ
iff $\Gamma \cup \Lambda$ tautologically implies $\gamma \rightarrow \phi$
iff $\Gamma \vdash (\gamma \rightarrow \phi)$.

Corollary (contraposition)

$\Gamma \cup \{\phi\} \vdash \neg\psi$ iff $\Gamma \cup \{\psi\} \vdash \neg\phi$.

A set of formulas is *inconsistent* iff for some *wff* β, both β and $\neg\beta$ are theorems of the set.

Corollary (reductio ad absurdum)

If $\Gamma \cup \{\phi\}$ is inconsistent, then $\Gamma \vdash \neg\phi$.

Example

Often it is easiest to work backward. Consider showing that

$$\vdash \exists x \forall y \phi \rightarrow \forall y \exists x \phi.$$

By the deduction theorem, it suffices to show that

$$\exists x \forall y \phi \vdash \forall y \exists x \phi.$$

By the generalization theorem, it suffices to show that

$$\exists x \forall y \phi \vdash \exists x \phi,$$

which is equivalent to

$$\neg\forall x \neg\forall y \phi \vdash \neg\forall x \neg\phi.$$

By contraposition, it thus suffices to show that

$$\forall x \neg\phi \vdash \forall x \neg\forall y \phi.$$

And again, by generalization, it suffices to show that

$$\forall x \neg\phi \vdash \neg\forall y \phi.$$

To show

$$\forall x \neg\phi \vdash \neg\forall y \phi,$$

it suffices (by reductio ad absurdum) to show that

$$\forall x \neg\phi, \forall y \phi$$

is inconsistent.

But this is easy to see, since

$$\forall x \neg\phi \vdash \neg\phi \text{ and}$$
$$\forall y \phi \vdash \phi.$$

Generalization on Constants

Theorem

Suppose $\Gamma \vdash \phi$ and c is a constant symbol which does not occur in Γ. Then there is a variable y which does not occur in Γ such that $\Gamma \vdash \forall\, y\ \phi_y^c$. Furthermore, there is a deduction of $\forall\, y\ \phi_y^c$ in which c does not occur.

Proof

Let $\langle \alpha_0, \ldots, \alpha_n \rangle$ be a deduction of ϕ from Γ. Let y be a variable which does not occur in any α_i. We claim that $\langle (\alpha_0)_y^c, \ldots, (\alpha_n)_y^c \rangle$ is a deduction from Γ of ϕ_y^c.

- Case 1: $\alpha_k \in \Gamma$. Then c does not occur in α_k, so $(\alpha_k)_y^c = \alpha_k$, which is in Γ.
- Case 2: $\alpha_k \in \Lambda$. A careful examination of the axioms reveals that if $\alpha_k \in \Lambda$, then $(\alpha_k)_y^c$ must also be in Λ.
- Case 3: α_k is obtained by modus ponens from α_i and α_j. It follows that $(\alpha_k)_y^c$ is obtained by modus ponens from $(\alpha_i)_y^c$ and $(\alpha_j)_y^c$.

It follows from the generalization theorem that there is a deduction of $\forall\, y\ \phi_y^c$, and it is not hard to see that c does not occur in the deduction.

Corollaries

Corollary

If $\Gamma \vdash \phi_c^x$, where c does not occur in Γ or in ϕ, then $\Gamma \vdash \forall\, x\ \phi$, and there is a deduction in which c does not occur.

Corollary (rule EI)

If $\Gamma \cup \{\phi_c^x\} \vdash \psi$ and c does not occur in any of Γ, ϕ, or ψ, then $\Gamma \cup \{\exists\, x\ \phi\} \vdash \psi$, and there is a deduction in which c does not occur.

Proof

By contraposition, we have $\Gamma \cup \{\neg\psi\} \vdash \neg\phi_c^x$.

By the above corollary, it follows that $\Gamma \cup \{\neg\psi\} \vdash \forall\, x\ \neg\phi$.

Applying contraposition again, yields $\Gamma \cup \{\exists\, x\ \phi\} \vdash \psi$.

Alphabetic Variants

An *alphabetic variant* of a formula ϕ is a formula ϕ' obtained by renaming some of the bound variables of ϕ. This is useful when we want to substitute t into ϕ, but t is not substitutable.

Theorem (Existence of Alphabetic Variants)

Let ϕ be a formula, t a term, and x a variable. Then there exists ϕ' such that

1. $\phi \vdash \phi'$ and $\phi' \vdash \phi$; and
2. t is substitutable for x in ϕ'.

Proof

We construct ϕ' by recursion on ϕ.

- If ϕ is atomic, $\phi' = \phi$
- $(\neg\phi)' = (\neg\phi')$ and $(\phi \to \psi)' = (\phi' \to \psi')$
- $(\forall\, y\ \phi)' = \forall\, z\ (\phi')^y_z$, where z does not appear in ϕ' or t or x.

It is not hard to show that the two conditions are satisfied by this definition.

Equality

Assuming the language includes equality, the following are the standard set of common facts about equality. Their proofs are straightforward.

1. Reflexivity: $\vdash \forall\, x\ x = x$.
2. Symmetry: $\vdash \forall\, x \forall\, y\ (x = y \to y = x)$.
3. Transitivity: $\vdash \forall\, x \forall\, y \forall\, z\ (x = y \to y = z \to x = z)$.
4. Substitutivity in predicates: if P is an n-place predicate symbol, then $\vdash \forall\, x_1 \ldots \forall\, x_n \forall\, y_1 \ldots \forall\, y_n\ (x_1 = y_1 \to \ldots \to x_n = y_n \to Px_1 \ldots x_n \to Py_1 \ldots y_n)$.
5. Substitutivity in functions: if f is an n-place function symbol, then $\vdash \forall\, x_1 \ldots \forall\, x_n \forall\, y_1 \ldots \forall\, y_n\ (x_1 = y_1 \to \ldots \to x_n = y_n \to fx_1 \ldots x_n = fy_1 \ldots y_n)$.

Syntactic strategies

Often, a strategy for showing the existence of a deduction can be chosen by looking at the syntax of the formula to be deduced.

- Suppose $\phi = (\psi \to \theta)$. Then it is sufficient (and always possible) to show that $\Gamma \cup \{\psi\} \vdash \theta$
- Suppose that ϕ is $\forall\, x\ \psi$. If x does not occur free in Γ, then it will suffice to show that $\Gamma \vdash \psi$. If x does occur free in Γ, then an alphabetic variant can be constructed where x is renamed to a variable that doesn't occur free in Γ.
- Suppose ϕ is the negation of another formula.
  - If $\phi = \neg(\psi \to \theta)$, then it suffices (by rule T) to show that $\Gamma \vdash \psi$ and $\Gamma \vdash \neg\theta$.
  - If $\phi = \neg\neg\psi$, then it suffices to show $\Gamma \vdash \psi$.
  - If $\phi = \neg\forall\, x\ \psi$, then it suffices to show that $\Gamma \vdash \neg\psi^x_t$, where t is substitutable for x in ψ. Unfortunately, this is not always possible.

As an example of when the last strategy fails, consider $\neg\forall\, x\ \neg(Px \to \forall\, y\ Py)$. It is true that $\vdash \neg\forall\, x\ \neg(Px \to \forall\, y\ Py)$, but for every term t, $\nvdash (Pt \to \forall\, y\ Py)$.

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 ϕ deducible from Γ is logically implied by Γ.

- Case 1: if ϕ 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 ϕ is obtained by modus ponens from ψ 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 $\Gamma \models \phi$.

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* ϕ, then for any model M and variable assignment s, $\models_M \phi^x_t[s]$ iff $\models_M \phi[s(x|\overline{s}(t))]$.

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 ϕ.

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

Assume $\models_M \forall x\, \alpha[s]$. We must show that $\models_M \alpha^x_t[s]$. We know from $\models_M \forall x\, \alpha[s]$ that for any $d \in \mathit{dom}(M)$, $\models_M \alpha[s(x|d)]$. In particular, if we let $d = \overline{s}(t)$, then we have $\models_M \alpha[s(x|\overline{s}(t))]$. But by the substitution lemma, this implies that $\models_M \alpha^x_t[s]$.

Soundness Corollaries

Corollary

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

Corollary

If ϕ' is an alphabetic variant of ϕ, then ϕ and ϕ' are logically equivalent.

Recall that a set Γ is *consistent* iff there is no formula ϕ such that both $\Gamma \vdash \phi$ and $\Gamma \vdash \neg\phi$.

Define Γ to be *satisfiable* iff there is some model M and variable assignment s such that $\models_M \Gamma[s]$.

Corollary

If Γ is satisfiable, then Γ 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.

The proof of the completeness theorem is the focus of the next lecture.

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 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 $h : dom(\mathcal{A}) \longrightarrow dom(\mathcal{B})$ 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 $dom(\mathcal{A})$,
   $\langle a_1, \ldots, a_n \rangle \in P^{\mathcal{A}}$ iff $\langle h(a_1), \ldots, h(a_n) \rangle \in P^{\mathcal{B}}$.
2. For each n-ary function symbol $f \in \Sigma$ and each n-tuple $\langle a_1, \ldots, a_n \rangle$ of elements of $dom(\mathcal{A})$,
   $h(f^{\mathcal{A}}(a_1, \ldots, a_n)) = f^{\mathcal{B}}(h(a_1), \ldots, h(a_n))$.
3. For each constant symbol $c \in \Sigma$, $h(c^{\mathcal{A}}) = c^{\mathcal{B}}$.

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 $h : \mathcal{N} \to \{0,1\}$ 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 $dom(\mathcal{A}) \subseteq dom(\mathcal{B})$ and the identity map $i : dom(\mathcal{A}) \to dom(\mathcal{B})$ 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 $dom(\mathcal{A})$.

1. For any term t, $h(\overline{s}(t)) = \overline{h \circ s}(t)$, where $\overline{s}$ 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 $dom(\mathcal{A})$.

1. For any term t, $h(\overline{s}(t)) = \overline{h \circ s}(t)$, where $\overline{s}$ 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,
   $\models_{\mathcal{A}} \alpha[s]$ iff $\models_{\mathcal{B}} \alpha[h \circ s]$.

   For an atomic formula, we have:

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

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

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

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

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

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

   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 $\models_{\mathcal{B}} \forall x\, \alpha[h \circ s]$.

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 $a \in \mathit{dom}(\mathcal{A})$.

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

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

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

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

□

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 $dom(\mathcal{A})$ definable in $\mathcal{A}$, then for any $a_1, \ldots, a_n \in dom(\mathcal{A})$,

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

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

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

and thus

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

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.