Metamathematics

David Marker

Fall 2003

1 Languages and Structures

In mathematical logic, we use first-order languages to describe mathematical structures. Intuitively, a structure is a set that we wish to study equipped with a collection of distinguished functions, relations, and elements. We then choose a language where we can talk about the distinguished functions, relations, and elements and nothing more. For example, when we study the ordered field of real numbers with the exponential function, we study the structure $(\mathbb{R}, +, \cdot, \exp, <, 0, 1)$, where the underlying set is the set of real numbers, and we distinguish the binary functions addition and multiplication, the unary function $x \mapsto e^x$, the binary order relation, and the real numbers 0 and 1. To describe this structure, we would use a language where we have symbols for $+, \cdot, \exp, <, 0, 1$ and can write statements such as $\forall x \forall y \ \exp(x) \cdot \exp(y) = \exp(x + y)$ and $\forall x \ (x > 0 \rightarrow \exists y \ \exp(y) = x)$. We interpret these statements as the assertions "$e^x e^y = e^{x+y}$ for all x and y" and "for all positive x, there is a y such that $e^y = x$."

For another example, we might consider the structure $(\mathbb{N}, +, 0, 1)$ of the natural numbers with addition and distinguished elements 0 and 1. The natural language for studying this structure is the language where we have a binary function symbol for addition and constant symbols for 0 and 1. We would write sentences such as $\forall x \exists y \ (x = y + y \ \vee \ x = y + y + 1)$, which we interpret as the assertion that "every number is either even or 1 plus an even number."

Definition 1.1 A *language* $\mathcal{L}$ is given by specifying the following data:
 i) a set of function symbols $\mathcal{F}$ and positive integers n_f for each $f \in \mathcal{F}$;
 ii) a set of relation symbols $\mathcal{R}$ and positive integers n_R for each $R \in \mathcal{R}$;

iii) a set of constant symbols $\mathcal{C}$.

The numbers n_f and n_R tell us that f is a function of n_f variables and R is an n_R-ary relation.

Any or all of the sets $\mathcal{F}$, $\mathcal{R}$, and $\mathcal{C}$ may be empty. Examples of languages include:

i) the language of rings $\mathcal{L}_{\mathrm{r}} = \{+, -, \cdot, 0, 1\}$, where $+, -$ and $\cdot$ are binary function symbols and 0 and 1 are constants;

ii) the language of ordered rings $\mathcal{L}_{\mathrm{or}} = \mathcal{L}_{\mathrm{r}} \cup \{<\}$, where $<$ is a binary relation symbol;

iii) the language of pure sets $\mathcal{L} = \emptyset$;

iv) the language of graphs is $\mathcal{L} = \{R\}$ where R is a binary relation symbol.

Next, we describe the structures where $\mathcal{L}$ is the appropriate language.

Definition 1.2 An $\mathcal{L}$-*structure* $\mathcal{M}$ is given by the following data:

i) a nonempty set M called the *universe*, *domain*, or *underlying set* of $\mathcal{M}$;

ii) a function $f^{\mathcal{M}} : M^{n_f} \to M$ for each $f \in \mathcal{F}$;

iii) a set $R^{\mathcal{M}} \subseteq M^{n_R}$ for each $R \in \mathcal{R}$;

iv) an element $c^{\mathcal{M}} \in M$ for each $c \in \mathcal{C}$.

We refer to $f^{\mathcal{M}}$, $R^{\mathcal{M}}$, and $c^{\mathcal{M}}$ as the *interpretations* of the symbols f, R, and c. We often write the structure as $\mathcal{M} = (M, f^{\mathcal{M}}, R^{\mathcal{M}}, c^{\mathcal{M}} : f \in \mathcal{F}, R \in \mathcal{R}$, and $c \in \mathcal{C})$. We will use the notation $A, B, M, N, \ldots$ to refer to the underlying sets of the structures $\mathcal{A}, \mathcal{B}, \mathcal{M}, \mathcal{N}, \ldots$.

For example, suppose that we are studying groups. We might use the language $\mathcal{L}_{\mathrm{g}} = \{\cdot, e\}$, where $\cdot$ is a binary function symbol and e is a constant symbol. An $\mathcal{L}_{\mathrm{g}}$-structure $\mathcal{G} = (G, \cdot^{\mathcal{G}}, e^{\mathcal{G}})$ will be a set G equipped with a binary relation $\cdot^{\mathcal{G}}$ and a distinguished element $e^{\mathcal{G}}$. For example, $\mathcal{G} = (\mathbb{R}, \cdot, 1)$ is an $\mathcal{L}_{\mathrm{g}}$-structure where we interpret $\cdot$ as multiplication and e as 1; that is, $\cdot^{\mathcal{G}} = \cdot$ and $e^{\mathcal{G}} = 1$. Also, $\mathcal{N} = (\mathbb{N}, +, 0)$ is an $\mathcal{L}_{\mathrm{g}}$-structure where $\cdot^{\mathcal{N}} = +$ and $e^{\mathcal{G}} = 0$. Of course, $\mathcal{N}$ is not a group, but it is an $\mathcal{L}_{\mathrm{g}}$-structure.

Usually, we will choose languages that closely correspond to the structure that we wish to study. For example, if we want to study the real numbers as an ordered field, we would use the language of ordered rings $\mathcal{L}_{\mathrm{or}}$ and give each symbol its natural interpretation.

Formulas and Terms

We use the language $\mathcal{L}$ to create formulas describing properties of $\mathcal{L}$-structures. Formulas will be strings of symbols built using the symbols of $\mathcal{L}$, variable symbols $v_1, v_2, \ldots$, the equality symbol $=$, the Boolean connectives $\wedge$, $\vee$, and $\neg$, which we read as "and," "or," and "not", the quantifiers $\exists$ and $\forall$, which we read as "there exists" and "for all", and parentheses (,).

Definition 1.3 The set of *$\mathcal{L}$-terms* is the smallest set $\mathcal{T}$ such that
i) $c \in \mathcal{T}$ for each constant symbol $c \in \mathcal{C}$,
ii) each variable symbol $v_i \in \mathcal{T}$ for $i = 1, 2, \ldots$, and
iii) if $t_1, \ldots, t_{n_f} \in \mathcal{T}$ and $f \in \mathcal{F}$, then $f(t_1, \ldots, t_{n_f}) \in \mathcal{T}$.

For example, $\cdot(v_1, -(v_3, 1))$, $\cdot(+(v_1, v_2), +(v_3, 1))$ and $+(1, +(1, +(1, 1)))$ are $\mathcal{L}_{\mathrm{r}}$-terms. For simplicity, we will usually write these terms in the more standard notation $v_1(v_3 - 1)$, $(v_1 + v_2)(v_3 + 1)$, and $1 + (1 + (1 + 1))$ when no confusion arises. In the $\mathcal{L}_{\mathrm{r}}$-structure $(\mathbb{Z}, +, \cdot, 0, 1)$, we think of the term $1 + (1 + (1 + 1))$ as a name for the element 4, while $(v_1 + v_2)(v_3 + 1)$ is a name for the function $(x, y, z) \mapsto (x + y)(z + 1)$. We will see below that we can do something similar for any term in any $\mathcal{L}$-structure.

We are now ready to define $\mathcal{L}$-formulas.

Definition 1.4 We say that ϕ is an *atomic $\mathcal{L}$-formula* if ϕ is either
i) $t_1 = t_2$, where t_1 and t_2 are terms, or
ii) $R(t_1, \ldots, t_{n_R})$, where $R \in \mathcal{R}$ and $t_1, \ldots, t_{n_R}$ are terms.

The set of *$\mathcal{L}$-formulas* is the smallest set $\mathcal{W}$ containing the atomic formulas such that
i) if ϕ is in $\mathcal{W}$, then $\neg\phi$ is in $\mathcal{W}$,
ii) if ϕ and ψ are in $\mathcal{W}$, then $(\phi \wedge \psi)$ and $(\phi \vee \psi)$ are in $\mathcal{W}$, and
iii) if ϕ is in $\mathcal{W}$, then $\exists v_i\ \phi$ and $\forall v_i\ \phi$ are in $\mathcal{W}$.

Here are three examples of $\mathcal{L}_{\mathrm{or}}$-formulas.
- $v_1 = 0 \vee v_1 > 0$.
- $\exists v_2\ v_2 \cdot v_2 = v_1$.
- $\forall v_1\ (v_1 = 0 \vee \exists v_2\ v_2 \cdot v_1 = 1)$.

Intuitively, the first formula asserts that $v_1 \geq 0$, the second asserts that v_1 is a square, and the third asserts that every nonzero element has a multiplicative inverse.

We want to define when a formula is true in a structure. The first example above already illustrates one problem we have to consider. Let $\mathbb{R}$ be the real numbers. Is the formula $v_1 \geq 0$ true? Of course the answer is "it depends". If $v_1 = 2$ then it is true, while if $v_1 = -7$, then it is false. Similarly, in the $\mathcal{L}_{\mathrm{or}}$-structure $(\mathbb{Z}+, -, \cdot, <, 0, 1)$, the second formula would be true if $v_1 = 9$

but false if $v_1 = 8$. It should be clear that to decide if a formula is true or false we need to consider how we interpret the variables.

Definition 1.5 Let $V = \{v_0, v_1, \ldots\}$. If $\mathcal{M}$ is an $\mathcal{L}$- structure, an *assignment* is a function $\sigma : V \to M$.

We start by showing how to evaluate terms. Suppose $\mathcal{M}$ is an $\mathcal{L}$- structure and $\sigma : V \to M$ is an assignment. We inductively define $t^{\mathcal{M}}[\sigma] \in M$ as follows:

i) if $t = c \in \mathcal{C}$ is a constant, then $t^{\mathcal{M}}[\sigma] = c^{\mathcal{M}}$;

ii) if $t = v_i$ is a variable, then $t^{\mathcal{M}}[\sigma] = \sigma(v_i)$;

iii) if $t_1, \ldots, t_m$ are terms, f is an m-ary function symbol and $t = f(t_1, \ldots, t_m)$, then

$$t^{\mathcal{M}}[\sigma] = f^{\mathcal{M}}(t_1^{\mathcal{M}}[\sigma], \ldots, t_m^{\mathcal{M}}[\sigma]).$$

For example, let $\mathcal{L} = \{f, g, c\}$, where f is a unary function symbol, g is a binary function symbol, and c is a constant symbol. We will consider the $\mathcal{L}$-terms $t_1 = g(v_1, c)$, $t_2 = f(g(c, f(v_1)))$, and $t_3 = g(f(g(v_1, v_2)), g(v_1, f(v_2)))$. Let $\mathcal{M}$ be the $\mathcal{L}$-structure $(\mathbb{R}, \exp, +, 1)$; that is, $f^{\mathcal{M}} = \exp$, $g^{\mathcal{M}} = +$, and $c^{\mathcal{M}} = 1$.

Then

$$t_1^{\mathcal{M}}[\sigma] = \sigma(v_1) + 1,$$

$$t_2^{\mathcal{M}}[\sigma] = e^{1+e^{\sigma(v_1)}}, \text{ and}$$

$$t_3^{\mathcal{M}}[\sigma] = e^{\sigma(v_1)+\sigma(v_2)} + (\sigma(v_1) + e^{\sigma(v_2)}).$$

If $\sigma : V \to M$ is an assignment, $v \in V$ and $a \in M$ we let $\sigma[\frac{a}{v}]$ be the assignment

$$\sigma\left[\frac{a}{v}\right](v_i) = \begin{cases} \sigma(v_i) & \text{if } v_i \neq v \\ a & \text{if } v_i = v \end{cases}.$$

Satisfaction

Before defining truth for formulas, we need to illustrate one other important concept.

Definition 1.6 We say that an occurence of a variable v in a formula ϕ is *free* it is not inside a $\exists v$ or $\forall v$ quantifier; otherwise, we say that it is *bound*.

For example in the formula

$$\forall v_2\ (v_0 > 0 \wedge \exists v_1\ v_1 \cdot v_2 = v_0)$$

v_0 occurs freely while v_1 and v_2 are bound. A more complicated example is the formula

$$v_0 > 0 \vee \exists v_0\ v_1 + v_0 = 0.$$

Clearly v_1 occurs freely, but v_0 has both free and bound occurences. The first occurence is free, while the second is bound.

Definition 1.7 Let $\mathcal{M}$ be an $\mathcal{L}$-structure. We inductively define $\mathcal{M} \models_\sigma \phi$ for all $\mathcal{L}$-formulas ϕ and all assignments σ.

i) If ϕ is $t_1 = t_2$, then $\mathcal{M} \models_\sigma \phi$ if $t_1^\mathcal{M}[\sigma] = t_2^\mathcal{M}[\sigma]$.

ii) If ϕ is $R(t_1, \dots, t_{n_R})$, then $\mathcal{M} \models_\sigma \phi$ if $(t_1^\mathcal{M}[\sigma], \dots, t_{n_R}^\mathcal{M}[\sigma]) \in R^\mathcal{M}$.

iii) If ϕ is $\neg\psi$, then $\mathcal{M} \models_\sigma \phi$ if $\mathcal{M} \not\models_\sigma \psi$.

iv) If ϕ is $(\psi \wedge \theta)$, then $\mathcal{M} \models_\sigma \phi$ if $\mathcal{M} \models_\sigma \psi$ and $\mathcal{M} \models_\sigma \theta$.

v) If ϕ is $(\psi \vee \theta)$, then $\mathcal{M} \models_\sigma \phi$ if $\mathcal{M} \models_\sigma \psi$ or $\mathcal{M} \models_\sigma \theta$.

vi) If ϕ is $\exists v_j \psi$, then $\mathcal{M} \models_\sigma \phi$ if there is $a \in M$ such that $\mathcal{M} \models_{\sigma[\frac{a}{v_j}]} \psi$.

vii) If ϕ is $\forall v_j \psi$, then $\mathcal{M} \models_\sigma \phi$ if $\mathcal{M} \models_{\sigma[\frac{a}{v_j}]} \psi$ for all $a \in M$.

If $\mathcal{M} \models_\sigma \phi$ we say that $\mathcal{M}$ with assignment σ *satisfies* ϕ or ϕ is *true* in $\mathcal{M}$ with assignment σ.

Remarks 1.8 • There are a number of useful abbreviations that we will use: $\phi \to \psi$ is an abbreviation for $\neg\phi \vee \psi$, and $\phi \leftrightarrow \psi$ is an abbreviation for $(\phi \to \psi) \wedge (\psi \to \phi)$. In fact, we did not really need to include the symbols $\vee$ and $\forall$. We could have considered $\phi \vee \psi$ as an abbreviation for $\neg(\neg\phi \wedge \neg\psi)$ and $\forall v \phi$ as an abbreviation for $\neg(\exists v \neg\phi)$. Viewing these as abbreviations will be an advantage when we are proving theorems by induction on formulas because it eliminates the $\vee$ and $\forall$ cases.

We also will use the abbreviations $\bigwedge_{i=1}^{n} \psi_i$ and $\bigvee_{i=1}^{n} \psi_i$ for $\psi_1 \wedge \ldots \wedge \psi_n$ and $\psi_1 \vee \ldots \vee \psi_n$, respectively.

• In addition to $v_1, v_2, \dots$, we will use $w, x, y, z, ...$ as variable symbols.

• It is important to note that the quantifiers $\exists$ and $\forall$ range only over elements of the model. For example the statement that an ordering is complete (i.e., every bounded subset has a least upper bound) cannot be expressed as a formula because we cannot quantify over subsets. The fact that we are limited to quantification over elements of the structure is what makes it "first-order" logic.

When proving results about satisfaction in models, we often must do an induction on the construction of formulas. As a first example of this method we show that $\mathcal{M} \models_\sigma \phi$ only depends on the restriction of σ to the variables occuring freely in ϕ.

Lemma 1.9 (Coincedence Lemma) *Suppose $\mathcal{M}$ is an $\mathcal{L}$-structure.*

i) Suppose t is an $\mathcal{L}$-term and $\sigma, \tau : V \to M$ are assignments that agree on all variables occuring in t. Then $t^{\mathcal{M}}[\sigma] = t^{\mathcal{M}}[\tau]$.

ii) Suppose ϕ is an $\mathcal{L}$-formula and $\sigma, \tau : V \to M$ are assignments that agree on all variables occuring freely in ϕ. Then $M \models_\sigma \phi$ if and only if $\mathcal{M} \models_\tau \phi$.

Proof i) We prove this by induction on terms.

If $t = c \in \mathcal{C}$ is a constant, then

$$t^{\mathcal{M}}[\sigma] = c^{\mathcal{M}} = t^{\mathcal{M}}[\tau].$$

If $t = v_i$ is a variable, then

$$t^{\mathcal{M}}[\sigma] = \sigma(v_i) = \tau(v_i) = t^{\mathcal{M}}[\tau].$$

Suppose the lemma is true for $t_1, \ldots, t_m$, f is an m-ary function symbol and $t = f(t_1, \ldots, t_m)$. Then

$$t^{\mathcal{M}}[\sigma] = f^{\mathcal{M}}(t_1^{\mathcal{M}}[\sigma], \ldots, t_m^{\mathcal{M}}[\sigma]) = f^{\mathcal{M}}(t_1^{\mathcal{M}}[\tau], \ldots, t_m^{\mathcal{M}}[\tau]) = t^{M}[\tau].$$

ii) We prove this by induction on formulas.

Suppose ϕ is $t_1 = t_2$ where t_1 and t_2 are $\mathcal{L}$-terms. Then

$$\begin{aligned} \mathcal{M} \models_\sigma \phi &\Leftrightarrow t_1^{\mathcal{M}}[\sigma] = t_2^{\mathcal{M}}[\sigma] \\ &\Leftrightarrow t_1^{\mathcal{M}}[\tau] = t_2^{\mathcal{M}}[\tau] \\ &\Leftrightarrow \mathcal{M} \models_\tau \sigma. \end{aligned}$$

Suppose R is an m-ary relation symbol, $t_1, \ldots, t_m$ are $\mathcal{L}$- terms, and ϕ is $R(t_1, \ldots, t_m)$. Then

$$\begin{aligned} \mathcal{M} \models_\sigma \phi &\Leftrightarrow (t_1^{\mathcal{M}}[\sigma], \ldots, t_m^{\mathcal{M}}[\sigma]) \in R^{\mathcal{M}} \\ &\Leftrightarrow (t_1^{\mathcal{M}}[\tau], \ldots, t_m^{\mathcal{M}}[\tau]) \in R^{\mathcal{M}} \\ &\Leftrightarrow \mathcal{M} \models_\tau \phi. \end{aligned}$$

Suppose the claim is true for ψ and ϕ is $\neg\psi$. Then

$$\begin{array}{rcl}\mathcal{M} \models_\sigma \phi & \Leftrightarrow & \mathcal{M} \not\models_\sigma \psi \\ & \Leftrightarrow & \mathcal{M} \not\models_\tau \psi \\ & \Leftrightarrow & \mathcal{M} \models_\tau \phi.\end{array}$$

Suppose the claim is true for ψ and θ and ϕ is $\psi \wedge \theta$. Then

$$\begin{array}{rcl}\mathcal{M} \models_\sigma \phi & \Leftrightarrow & \mathcal{M} \not\models_\sigma \psi \text{ and } \mathcal{M} \models_\sigma \theta \\ & \Leftrightarrow & \mathcal{M} \not\models_\tau \psi \text{ and } \mathcal{M} \models_\tau \theta \\ & \Leftrightarrow & \mathcal{M} \models_\tau \phi.\end{array}$$

Suppose the claim is true for ψ, ϕ is $\exists v_i \psi$ and $\mathcal{M} \models_\sigma \phi$. Then there is $a \in M$ such that $\mathcal{M} \models_{\sigma[\frac{a}{v_i}]} \psi$. The assignments $\sigma[\frac{a}{v_i}]$ and $\tau[\frac{a}{v_i}]$ agree on all variables, free in ψ. Thus, by induction, $\mathcal{M} \models_{\tau[\frac{a}{v_i}]} \psi$ and $\mathcal{M} \models_\tau \phi$. Symmetricly if $\mathcal{M} \models_\tau \phi$, then $\mathcal{M} \models_\sigma \phi$.

Thus, by induction, $\mathcal{M} \models_\sigma \phi$ if and only if $\mathcal{M} \models_\tau \phi$.

Definition 1.10 We say that an $\mathcal{L}$-formula ϕ is a *sentence* if ϕ has no freely occuring variables.

Corollary 1.11 *Suppose ϕ is an $\mathcal{L}$-sentence and $\mathcal{M}$ is an $\mathcal{L} - structure$. The following are equivalent:*
i) $\mathcal{M} \models_\sigma \phi$ for some assignment σ;
ii) $\mathcal{M} \models_\sigma \phi$ for all assignments σ.

Definition 1.12 If ϕ is a sentence, we write $\mathcal{M} \models \phi$ if $\mathcal{M} \models_\sigma \phi$ for all assignments $\sigma : V \to M$.

Suppose ϕ is a formula with free variables from $v_1, \ldots, v_n$. If $a_1, \ldots, a_n \in M$ we write $\mathcal{M} \models \phi(a_1, \ldots, a_n)$ if $\mathcal{M} \models_\sigma \phi$ whenever σ is an assignment with $\sigma(v_i) = a_i$ for $i = 1, \ldots, n$. By the Coincedence Lemma, this is well defined.

$\mathcal{L}$-embeddings and Substructures

We will also study maps that preserve the interpretation of $\mathcal{L}$.

Definition 1.13 Suppose that $\mathcal{M}$ and $\mathcal{N}$ are $\mathcal{L}$-structures with universes M and N, respectively. An *$\mathcal{L}$-embedding* $\eta : \mathcal{M} \to \mathcal{N}$ is a one-to-one map

$\eta : M \to N$ that preserves the interpretation of all of the symbols of $\mathcal{L}$. More precisely:

i) $\eta(f^{\mathcal{M}}(a_1, \ldots, a_{n_f})) = f^{\mathcal{N}}(\eta(a_1), \ldots, \eta(a_{n_f}))$ for all $f \in \mathcal{F}$ and $a_1, \ldots, a_n \in M$;

ii) $(a_1, \ldots, a_{m_R}) \in R^{\mathcal{M}}$ if and only if $(\eta(a_1), \ldots, \eta(a_{m_R})) \in R^{\mathcal{N}}$ for all $R \in \mathcal{R}$ and $a_1, \ldots, a_{m_j} \in M$;

iii) $\eta(c^{\mathcal{M}}) = c^{\mathcal{N}}$ for $c \in \mathcal{C}$.

A bijective $\mathcal{L}$-embedding is called an *$\mathcal{L}$-isomorphism*. If $M \subseteq N$ and the inclusion map is an $\mathcal{L}$-embedding, we say either that $\mathcal{M}$ is a *substructure* of $\mathcal{N}$ or that $\mathcal{N}$ is an *extension* of $\mathcal{M}$.

For example:

i) $(\mathbb{Z}, +, 0)$ is a substructure of $(\mathbb{R}, +, 0)$.

ii) If $\eta : \mathbb{Z} \to \mathbb{R}$ is the function $\eta(x) = e^x$, then η is an $\mathcal{L}_{\mathrm{g}}$-embedding of $(\mathbb{Z}, +, 0)$ into $(\mathbb{R}, \cdot, 1)$.

The next proposition asserts that if a formula without quantifiers is true in some structure, then it is true in every extension. It is proved by induction on quantifier-free formulas.

Proposition 1.14 *Suppose that $\mathcal{M}$ is a substructure of $\mathcal{N}$, $\overline{a} \in M$, and $\phi(\overline{v})$ is a quantifier-free formula. Then, $\mathcal{M} \models \phi(\overline{a})$ if and only if $\mathcal{N} \models \phi(\overline{a})$.*

Proof

Claim If $t(\overline{v})$ is a term and $\overline{b} \in M$, then $t^{\mathcal{M}}(\overline{b}) = t^{\mathcal{N}}(\overline{b})$. This is proved by induction on terms.

If t is the constant symbol c, then $c^{\mathcal{M}} = c^{\mathcal{N}}$.

If t is the variable v_i, then $t^{\mathcal{M}}(\overline{b}) = b_i = t^{\mathcal{N}}(\overline{b})$.

Suppose that $t = f(t_1, \ldots, t_n)$, where f is an n-ary function symbol, $t_1, \ldots, t_n$ are terms, and $t_i^{\mathcal{M}}(\overline{b}) = t_i^{\mathcal{N}}(\overline{b})$ for $i = 1, \ldots, n$. Because $\mathcal{M} \subseteq \mathcal{N}$, $f^{\mathcal{M}} = f^{\mathcal{N}} | M^n$. Thus,

$$\begin{aligned} t^{\mathcal{M}}(\overline{b}) &= f^{\mathcal{M}}(t_1^{\mathcal{M}}(\overline{b}), \ldots, t_n^{\mathcal{M}}(\overline{b})) \\ &= f^{\mathcal{N}}(t_1^{\mathcal{M}}(\overline{b}), \ldots, t_n^{\mathcal{M}}(\overline{b})) \\ &= f^{\mathcal{N}}(t_1^{\mathcal{N}}(\overline{b}), \ldots, t_n^{\mathcal{N}}(\overline{b})) \\ &= t^{\mathcal{N}}(\overline{b}). \end{aligned}$$

We now prove the proposition by induction on formulas.

If ϕ is $t_1 = t_2$, then

$$\mathcal{M} \models \phi(\overline{a}) \Leftrightarrow t_1^{\mathcal{M}}(\overline{a}) = t_2^{\mathcal{M}}(\overline{a}) \Leftrightarrow t_1^{\mathcal{N}}(\overline{a}) = t_2^{\mathcal{N}}(\overline{a}) \Leftrightarrow \mathcal{N} \models \phi(\overline{a}).$$

If ϕ is $R(t_1, \ldots, t_n)$, where R is an n-ary relation symbol, then

$$\begin{aligned} \mathcal{M} \models \phi(\overline{a}) &\Leftrightarrow (t_1^{\mathcal{M}}(\overline{a}), \ldots, t_n^{\mathcal{M}}(\overline{a})) \in R^{\mathcal{M}} \\ &\Leftrightarrow (t_1^{\mathcal{M}}(\overline{a}), \ldots, t_n^{\mathcal{M}}(\overline{a})) \in R^{\mathcal{N}} \\ &\Leftrightarrow (t_1^{\mathcal{N}}(\overline{a}), \ldots, t_n^{\mathcal{N}}(\overline{a})) \in R^{\mathcal{N}} \\ &\Leftrightarrow \mathcal{N} \models \phi(\overline{a}). \end{aligned}$$

Thus, the proposition is true for all atomic formulas.

Suppose that the proposition is true for ψ and that ϕ is $\neg\psi$. Then,

$$\mathcal{M} \models \neg\phi(\overline{a}) \Leftrightarrow \mathcal{M} \not\models \psi(\overline{a}) \Leftrightarrow \mathcal{N} \not\models \psi(\overline{a}) \Leftrightarrow \mathcal{N} \models \phi(\overline{a}).$$

Finally, suppose that the proposition is true for ψ_0 and ψ_1 and that ϕ is $\psi_0 \wedge \psi_1$. Then,

$$\begin{aligned} \mathcal{M} \models \phi(\overline{a}) &\Leftrightarrow \mathcal{M} \models \psi_0(\overline{a}) \text{ and } \mathcal{M} \models \psi_1(\overline{a}) \\ &\Leftrightarrow \mathcal{N} \models \psi_0(\overline{a}) \text{ and } \mathcal{M} \models \psi_1(\overline{a}) \\ &\Leftrightarrow \mathcal{N} \models \phi(\overline{a}). \end{aligned}$$

We have shown that the proposition holds for all atomic formulas and that if it holds for ϕ and ψ, then it also holds for $\neg\phi$ and $\phi \wedge \psi$. Because the set of quantifier-free formulas is the smallest set of formulas containing the atomic formulas and closed under negation and conjunction, the proposition is true for all quantifier-free formulas.

Elementary Equivalence and Isomorphism

We next consider structures that satisfy the same sentences.

Definition 1.15 We say that two $\mathcal{L}$-structures $\mathcal{M}$ and $\mathcal{N}$ are *elementarily equivalent* and write $\mathcal{M} \equiv \mathcal{N}$ if

$$\mathcal{M} \models \phi \text{ if and only if } \mathcal{N} \models \phi$$

for all $\mathcal{L}$-sentences ϕ.

We let Th($\mathcal{M}$), the *full theory of* $\mathcal{M}$, be the set of $\mathcal{L}$-sentences ϕ such that $\mathcal{M} \models \phi$. It is easy to see that $\mathcal{M} \equiv \mathcal{N}$ if and only if Th($\mathcal{M}$)= Th($\mathcal{N}$).

The *cardinality of* $\mathcal{M}$ is $|M|$, the cardinality of the universe of $\mathcal{M}$. If $\eta : \mathcal{M} \to \mathcal{N}$ is an embedding then the cardinality of $\mathcal{N}$ is at least the cardinality of $\mathcal{M}$.

Our next result shows that Th($\mathcal{M}$) is an isomorphism invariant of $\mathcal{M}$. The proof uses the important technique of "induction on formulas."

Theorem 1.16 *Suppose that $j : \mathcal{M} \to \mathcal{N}$ is an isomorphism. Then, $\mathcal{M} \equiv \mathcal{N}$.*

Proof We show by induction on formulas that $\mathcal{M} \models \phi(a_1, \ldots, a_n)$ if and only if $\mathcal{N} \models \phi(j(a_1), \ldots, j(a_n))$ for all formulas ϕ.

We first must show that terms behave well.

Claim Suppose that t is a term and the free variables in t are from $\overline{v} = (v_1, \ldots, v_n)$. For $\overline{a} = (a_1, \ldots, a_n) \in M$, we let $j(\overline{a})$ denote $(j(a_1), \ldots, j(a_n))$. Then $j(t^{\mathcal{M}}(\overline{a})) = t^{\mathcal{N}}(j(\overline{a}))$.

We prove this by induction on terms.

i) If $t = c$, then $j(t^{\mathcal{M}}(\overline{a})) = j(c^{\mathcal{M}}) = c^{\mathcal{N}} = t^{\mathcal{N}}(j(\overline{a}))$.

ii) If $t = v_i$, then $j(t^{\mathcal{M}}(\overline{a})) = j(a_i) = t^{\mathcal{N}}(j(a_i))$.

iii) If $t = f(t_1, \ldots, t_m)$, then

$$\begin{aligned} j(t^{\mathcal{M}}(\overline{a})) &= j(f^{\mathcal{M}}(t_1^{\mathcal{M}}(\overline{a}), \ldots, t_m^{\mathcal{M}}(\overline{a}))) \\ &= f^{\mathcal{N}}(j(t_1^{\mathcal{M}}(\overline{a})), \ldots, j(t_m^{\mathcal{M}}(\overline{a}))) \\ &= f^{\mathcal{N}}(t_1^{\mathcal{N}}(j(\overline{a})), \ldots, t_m^{\mathcal{N}}(j(\overline{a}))) \\ &= t^{\mathcal{N}}(j(\overline{a})). \end{aligned}$$

We proceed by induction on formulas.

i) If $\phi(\overline{v})$ is $t_1 = t_2$, then

$$\begin{aligned} \mathcal{M} \models \phi(\overline{a}) &\Leftrightarrow t_1^{\mathcal{M}}(\overline{a}) = t_2^{\mathcal{M}}(\overline{a}) \\ &\Leftrightarrow j(t_1^{\mathcal{M}}(\overline{a})) = j(t_2^{\mathcal{M}}(\overline{a})) \text{ because } j \text{ is injective} \\ &\Leftrightarrow t_1^{\mathcal{N}}(j(\overline{a})) = t_2^{\mathcal{N}}(j(\overline{a})) \\ &\Leftrightarrow \mathcal{N} \models \phi(j(\overline{a})). \end{aligned}$$

ii) If $\phi(\overline{v})$ is $R(t_1, \ldots, t_n)$, then

$$\mathcal{M} \models \phi(\overline{a}) \Leftrightarrow (t_1^{\mathcal{M}}(\overline{a}), \ldots, t_n^{\mathcal{M}}(\overline{a})) \in R^{\mathcal{M}}$$

$$\begin{aligned}
&\Leftrightarrow\ (j(t_1^{\mathcal{M}}(\overline{a})),\ldots,j(t_n^{\mathcal{M}}(\overline{a}))) \in R^{\mathcal{N}}\\
&\Leftrightarrow\ (t_1^{\mathcal{N}}(j(\overline{a})),\ldots,t_n^{\mathcal{N}}(j(\overline{a}))) \in R^{\mathcal{N}}\\
&\Leftrightarrow\ \mathcal{N} \models \phi(j(\overline{a})).
\end{aligned}$$

iii) If ϕ is $\neg\psi$, then by induction

$$\mathcal{M} \models \phi(\overline{a}) \Leftrightarrow \mathcal{M} \not\models \psi(\overline{a}) \Leftrightarrow \mathcal{N} \not\models \psi(j(\overline{a})) \Leftrightarrow \mathcal{N} \models \phi(j(\overline{a})).$$

iv) If ϕ is $\psi \wedge \theta$, then

$$\begin{aligned}
\mathcal{M} \models \phi(\overline{a}) &\Leftrightarrow \mathcal{M} \models \psi(\overline{a}) \text{ and } \mathcal{M} \models \theta(\overline{a})\\
&\Leftrightarrow \mathcal{N} \models \psi(j(\overline{a})) \text{ and } \mathcal{N} \models \theta(j(\overline{a})) \Leftrightarrow \mathcal{N} \models \phi(j(\overline{a})).
\end{aligned}$$

v) If $\phi(\overline{v})$ is $\exists w\ \psi(\overline{v}, w)$, then

$$\begin{aligned}
\mathcal{M} \models \phi(\overline{a}) &\Leftrightarrow \mathcal{M} \models \psi(\overline{a}, b) \text{ for some } b \in M\\
&\Leftrightarrow \mathcal{N} \models \psi(j(\overline{a}), c) \text{ for some } c \in N \text{because } j \text{ is onto}\\
&\Leftrightarrow \mathcal{N} \models \phi(j(\overline{a})).
\end{aligned}$$

2 Theories

Let $\mathcal{L}$ be a language. An $\mathcal{L}$-*theory* T is simply a set of $\mathcal{L}$-sentences. We say that $\mathcal{M}$ is a *model* of T and write $\mathcal{M} \models T$ if $\mathcal{M} \models \phi$ for all sentences $\phi \in T$.

The set $T = \{\forall x\ x = 0, \exists x\ x \neq 0\}$ is a theory. Because the two sentences in T are contradictory, there are no models of T. We say that a theory is *satisfiable* if it has a model.

We say that a class of $\mathcal{L}$-structures $\mathcal{K}$ is an *elementary class* if there is an $\mathcal{L}$-theory T such that $\mathcal{K} = \{\mathcal{M} : \mathcal{M} \models T\}$.

One way to get a theory is to take $\mathrm{Th}(\mathcal{M})$, the full theory of an $\mathcal{L}$-structure $\mathcal{M}$. In this case, the elementary class of models of $\mathrm{Th}(\mathcal{M})$ is exactly the class of $\mathcal{L}$-structures elementarily equivalent to $\mathcal{M}$. More typically, we have a class of structures in mind and try to write a set of properties T describing these structures. We call these sentences *axioms* for the elementary class.

We give a few basic examples of theories and elementary classes that we will return to frequently.

Example 2.1 *Infinite Sets*

Let $\mathcal{L} = \emptyset$.

Consider the $\mathcal{L}$-theory where we have, for each n, the sentence ϕ_n given by

$$\exists x_1 \exists x_2 \ldots \exists x_n \bigwedge_{i<j\leq n} x_i \neq x_j.$$

The sentence ϕ_n asserts that there are at least n distinct elements, and an $\mathcal{L}$-structure $\mathcal{M}$ with universe M is a model of T if and only if M is infinite.

Example 2.2 *Linear Orders*

Let $\mathcal{L} = \{<\}$, where $<$ is a binary relation symbol. The class of linear orders is axiomatized by the $\mathcal{L}$-sentences

$\forall x\ \neg(x < x)$,

$\forall x \forall y \forall z\ ((x < y \wedge y < z) \rightarrow x < z)$,

$\forall x \forall y\ (x < y \vee x = y \vee y < x)$.

There are a number of interesting extensions of the theory of linear orders. For example, we could add the sentence

$$\forall x \forall y\ (x < y \rightarrow \exists z\ (x < z \wedge z < y))$$

to get the theory of dense linear orders, or we could instead add the sentence

$$\forall x \exists y\ (x < y \wedge \forall z (x < z \rightarrow (z = y \vee y < z)))$$

to get the theory of linear orders where every element has a unique successor. We could also add sentences that either assert or deny the existence of top or bottom elements.

Example 2.3 *Equivalence Relations*

Let $\mathcal{L} = \{E\}$, where E is a binary relation symbol. The theory of equivalence relations is given by the sentences

$\forall x\ E(x, x)$,

$\forall x \forall y (E(x, y) \rightarrow E(y, x))$,

$\forall x \forall y \forall z ((E(x, y) \wedge E(y, z)) \rightarrow E(x, z))$.

If we added the sentence

$$\forall x \exists y (x \neq y \wedge E(x, y) \wedge \forall z\ (E(x, z) \rightarrow (z = x \vee z = y)))$$

we would have the theory of equivalence relations where every equivalence class has exactly two elements. If instead we added the sentence

$$\exists x \exists y (\neg E(x,y) \wedge \forall z (E(x,z) \vee E(y,z)))$$

and the infinitely many sentences

$$\forall x \exists x_1 \exists x_2 \ldots \exists x_n \left(\bigwedge_{i<j\leq n} x_i \neq x_j \wedge \bigwedge_{i=1}^{n} E(x, x_i) \right)$$

we would axiomatize the class of equivalence relations with exactly two classes, both of which are infinite.

Example 2.4 *Graphs*

Let $\mathcal{L} = \{R\}$ where R is a binary relation. We restrict our attention to irreflexive graphs. These are axiomatized by the two sentences
$\forall x \; \neg R(x,x)$,
$\forall x \forall y \; (R(x,y) \rightarrow R(y,x))$.

Example 2.5 *Groups*

Let $\mathcal{L} = \{\cdot, e\}$, where $\cdot$ is a binary function symbol and e is a constant symbol. We will write $x \cdot y$ rather than $\cdot(x,y)$. The class of groups is axiomatized by
$\forall x \; e \cdot x = x \cdot e = x$,
$\forall x \forall y \forall z \; x \cdot (y \cdot z) = (x \cdot y) \cdot z$,
$\forall x \exists y \; x \cdot y = y \cdot x = e$.
We could also axiomatize the class of Abelian groups by adding

$$\forall x \forall y \; x \cdot y = y \cdot x.$$

Let $\phi_n(x)$ be the $\mathcal{L}$-formula

$$\underbrace{x \cdot x \cdots x}_{n-\text{times}} = e;$$

which asserts that $nx = e$.

We could axiomatize the class of torsion-free groups by adding $\{\forall x \; (x = e \vee \neg\phi_n(x)) : n \geq 2\}$ to the axioms for groups. Alternatively, we could axiomatize the class of groups where every element has order at most N by adding to the axioms for groups the sentence

$$\forall x \bigvee_{n \leq N} \phi_n(x).$$

Note that the same idea will not work to axiomatize the class of torsion groups because the corresponding sentence would be infinitely long. In the next chapter, we will see that the class of torsion groups is not elementary.

Let $\psi_n(x,y)$ be the formula

$$\underbrace{x \cdot x \cdots x}_{n-\text{times}} = y;$$

which asserts that $x^n = y$. We can axiomatize the class of divisible groups by adding the axioms $\{\forall y \exists x \; \psi_n(x,y) : n \geq 2\}$.

It will often be useful to deal with additive groups instead of multiplicative groups. The class of additive groups is the collection structures in the language $\mathcal{L} = \{+, 0\}$, axiomatized as above replacing $\cdot$ by $+$ and e by 0.

Example 2.6 *Ordered Abelian Groups*

Let $\mathcal{L} = \{+, <, 0\}$, where $+$ is a binary function symbol, $<$ is a binary relation symbol, and 0 is a constant symbol. The axioms for ordered groups are

the axioms for additive groups,
the axioms for linear orders, and
$\forall x \forall y \forall z (x < y \rightarrow x + z < y + z)$.

Example 2.7 *Left R-modules*

Let R be a ring with multiplicative identity 1. Let $\mathcal{L} = \{+, 0\} \cup \{r : r \in R\}$ where $+$ is a binary function symbol, 0 is a constant, and r is a unary function symbol for $r \in R$. In an R-module, we will interpret r as scalar multiplication by R. The axioms for left R-modules are

the axioms for additive commutative groups,
$\forall x\ r(x + y) = r(x) + r(y)$ for each $r \in R$,
$\forall x\ (r + s)(x) = r(x) + s(x)$ for each $r, s \in R$,
$\forall x\ r(s(x)) = rs(x)$ for $r, s \in R$,
$\forall x\ 1(x) = x$.

Example 2.8 *Rings and Fields*

Let $\mathcal{L}_{\mathrm{r}}$ be the language of rings $\{+, -, \cdot, 0, 1\}$, where $+$, $-$, and $\cdot$ are binary function symbols and 0 and 1 are constants. The axioms for rings are given by

the axioms for additive commutative groups,
$\forall x \forall y \forall z\ (x - y = z \leftrightarrow x = y + z)$,
$\forall x\ x \cdot 0 = 0$,
$\forall x \forall y \forall z\ (x \cdot (y \cdot z) = (x \cdot y) \cdot z)$,
$\forall x\ x \cdot 1 = 1 \cdot x = x$,
$\forall x \forall y \forall z\ x \cdot (y + z) = (x \cdot y) + (x \cdot z)$,
$\forall x \forall y \forall z\ (x + y) \cdot z = (x \cdot z) + (y \cdot z)$.

The second axiom is only necessary because we include $-$ in the language (this will be useful later). We axiomatize the class of fields by adding the axioms

$\forall x \forall y\ x \cdot y = y \cdot x$,
$\forall x\ (x \neq 0 \rightarrow \exists y\ x \cdot y = 1)$.

We axiomatize the class of algebraically closed fields by adding to the field axioms the sentences

$$\forall a_0 \dots \forall a_{n-1} \exists x \; x^n + \sum_{i=0}^{n-1} a_i x^i = 0$$

for $n = 1, 2, \dots$. Let ACF be the axioms for algebraically closed fields.

Let ψ_p be the $\mathcal{L}_{\mathrm{r}}$-sentence $\forall x \underbrace{x + \dots + x}_{p-\text{times}} = 0$, which asserts that a field has characteristic p. For $p > 0$ a prime, let $\mathrm{ACF}_p = \mathrm{ACF} \cup \{\psi_p\}$ and $\mathrm{ACF}_0 = \mathrm{ACF} \cup \{\neg\psi_p : p > 0\}$, be the theories of algebraically closed fields of characteristic p and characteristic zero, respectively.

Example 2.9 *Ordered Fields*

Let $\mathcal{L}_{\mathrm{or}} = \mathcal{L}_{\mathrm{r}} \cup \{<\}$. The class of ordered fields is axiomatized by the axioms for fields,

the axioms for linear orders,
$\forall x \forall y \forall z \; (x < y \to x + z < y + z)$,
$\forall x \forall y \forall z \; ((x < y \wedge z > 0) \to x \cdot z < y \cdot z)$.

Example 2.10 *Differential Fields*

Let $\mathcal{L} = \mathcal{L}_{\mathrm{r}} \cup \{\delta\}$, where δ is a unary function symbol. The class of differential fields is axiomatized by

the axioms of fields,
$\forall x \forall y \; \delta(x + y) = \delta(x) + \delta(y)$,
$\forall x \forall y \; \delta(x \cdot y) = x \cdot \delta(y) + y \cdot \delta(x)$.

Example 2.11 *Peano Arithmetic*

Let $\mathcal{L} = \{+, \cdot, s, 0\}$, where $+$ and $\cdot$ are binary functions, s is a unary function, and 0 is a constant. We think of s as the successor function $x \mapsto x + 1$. The Peano axioms for arithmetic are the sentences

$\forall x \; s(x) \neq 0$,
$\forall x \; (x \neq 0 \to \exists y \; s(y) = x)$,
$\forall x \; x + 0 = x$,
$\forall x \; \forall y \; x + (s(y)) = s(x + y)$,
$\forall x \;\; x \cdot 0 = 0$,

$\forall x \forall y\ x \cdot s(y) = (x \cdot y) + x$,

and the axioms $\mathrm{Ind}(\phi)$ for each formula $\phi(v, \overline{w})$, where $\mathrm{Ind}(\phi)$ is the sentence

$\forall \overline{w}\ [(\phi(0, \overline{w}) \wedge \forall v\ (\phi(v, \overline{w}) \rightarrow \phi(s(v), \overline{w}))) \rightarrow \forall x\ \phi(x, \overline{w})]$.

The axiom $\mathrm{Ind}(\phi)$ formalizes an instance of induction. It asserts that if $\overline{a} \in M$, $X = \{m \in M : \mathcal{M} \models \phi(m, \overline{a})\}$, $0 \in X$, and $s(m) \in X$ whenever $m \in X$, then $X = M$.

Logical Consequence

Definition 2.12 Let T be an $\mathcal{L}$-theory and ϕ an $\mathcal{L}$-sentence. We say that ϕ is a *logical consequence* of T and write $T \models \phi$ if $\mathcal{M} \models \phi$ whenever $\mathcal{M} \models T$.

We give two examples.

Proposition 2.13 *a) Let $\mathcal{L} = \{+, <, 0\}$ and let T be the theory of ordered Abelian groups. Then, $\forall x(x \neq 0 \rightarrow x + x \neq 0)$ is a logical consequence of T.*

b) Let T be the theory of groups where every element has order 2. Then, $T \not\models \exists x_1 \exists x_2 \exists x_3 (x_1 \neq x_2 \wedge x_2 \neq x_3 \wedge x_1 \neq x_3)$.

Proof

a) Suppose that $\mathcal{M} = (M, +, <, 0)$ is an ordered Abelian group. Let $a \in M \setminus \{0\}$. We must show that $a + a \neq 0$. Because $(M, <)$ is a linear order $a < 0$ or $0 < a$. If $a < 0$, then $a + a < 0 + a = a < 0$. Because $\neg(0 < 0)$, $a + a \neq 0$. If $0 < a$, then $0 < a = 0 + a < a + a$ and again $a + a \neq 0$.

b) Clearly, $\mathbb{Z}/2\mathbb{Z} \models T \wedge \neg \exists x_1 \exists x_2 \exists x_3 (x_1 \neq x_2 \wedge x_2 \neq x_3 \wedge x_1 \neq x_3)$.

In general, to show that $T \models \phi$, we give an informal mathematical proof as above that $\mathcal{M} \models \phi$ whenever $\mathcal{M} \models T$. To show that $T \not\models \phi$, we usually construct a counterexample.

In the next sections we will also need a notion of logical consequence for formulas.

Definition 2.14 If Γ is a set of $\mathcal{L}$-formulas and ϕ is an $\mathcal{L}$-formula, we say that ϕ is a *logical consequnce* of Γ and write $\Gamma \models \phi$ if $\mathcal{M} \models_\sigma \phi$, whenever $\mathcal{M}$ is an $\mathcal{L}$-structure, $\sigma : V \rightarrow M$ is an assignment and $\mathcal{M} \models_\sigma \psi$ for all $\psi \in \Gamma$.

3 Formal Proofs

A priori to show $\Gamma \models \phi$ we must examine all structures $\mathcal{M}$ and all assignments $\sigma : V \to M$ where $\mathcal{M} \models_\sigma \Gamma$ and show that $\mathcal{M} \models_\sigma \phi$. This is in general an impossible task. In mathematics we show that $\Gamma \models \phi$ by giving a proof. In this section we will give one example of a formal proof system. We will write $\Gamma \vdash \phi$ if there is a formal proof of ϕ from Γ. We will demand two properties of our proof system.

- SOUNDNESS: If $\Gamma \vdash \phi$, then $\Gamma \models \phi$.

Thus anything that is provable is a logical consequence.

- COMPLETENESS: If $\Gamma \models \phi$, then $\Gamma \vdash \phi$.

Thus every logical consequence is provable.

Soundness of our system will be routine. Gödel's Completeness theorem will be proved in the next section.

In addition we will demand that proof are finite. Any proof will be a finite collection of symbols. Moreover it should be easy to check that a proported proof is correct.

Our proof system is a variant of the sequent calculus.

Definition 3.1 A *proof* will be a finite sequence of assertions of the form

1. $\Gamma_1 \vdash \phi_1$
2. $\Gamma_2 \vdash \phi_2$

$\vdots \quad \vdots$

n. $\Gamma_n \vdash \phi_n$

where each Γ_i is a **finite** set of formulas (possibly empty), ϕ_i is a formula and each assertion $\Gamma_i \vdash \phi_i$ can be derived from the assertions $\Gamma_1 \vdash \phi_1, \ldots, \Gamma_{i-1} \vdash \phi_{i-1}$ by one of the inference rules that we will shortly describe.

We think of "$\Gamma \vdash \phi$" as the assertion that ϕ is derivable from Γ. We will write $\Gamma, \psi \vdash \phi$ to abbreviate $\Gamma \cup \{\psi\} \vdash \phi$.

Our inference rules will have the form

$$\frac{\Gamma_1 \vdash \phi_1 \;\ldots\; \Gamma_n \vdash \phi_n}{\Delta \vdash \psi.}$$

This means that if have already established $\Gamma_1 \vdash \phi_1, \ldots, \Gamma_n \vdash \phi_n$, the we can conlclude that $\Delta \vdash \psi$.

We begin to give the rules of our calculus.

Structural Rules:
S1. (Assumption) If $\phi \in \Gamma$, then

$$\Gamma \vdash \phi$$

S2. (Monotonicity) If $\Gamma \subseteq \Delta$, then

$$\frac{\Gamma \vdash \phi}{\Delta \vdash \phi}$$

S3. (Proof by cases)

$$\frac{\Gamma, \psi \vdash \phi \qquad \Gamma, \neg\psi \vdash \phi}{\Gamma \vdash \phi}$$

Connective Rules
C1. (Contradiction Rule)

$$\frac{\Gamma, \neg\phi \vdash \psi \qquad \Gamma, \neg\phi \vdash \neg\psi}{\Gamma \vdash \phi}$$

C2. (Left $\vee$-rule)

$$\frac{\Gamma, \phi \vdash \theta \qquad \Gamma, \psi \vdash \theta}{\Gamma, (\phi \vee \psi) \vdash \theta}$$

C3. (Right $\vee$-rules)

$$\frac{\Gamma \vdash \phi}{\Gamma \vdash (\phi \vee \psi)} \qquad \frac{\Gamma \vdash \phi}{\Gamma \vdash (\psi \vee \phi)}$$

Before giving the inference rules for quantifiers and equality we give some sample derivations and prove some useful inference rules which are consequences of the rules above.

Example: $\vdash (\phi \vee \neg\phi)$

1.	$\phi \vdash \phi$	S1
2.	$\phi \vdash (\phi \vee \neg\phi)$	C3
3.	$\neg\phi \vdash \neg\phi$	S1
4.	$\neg\phi \vdash (\phi \vee \neg\phi)$	C3
5.	$\vdash (\phi \vee \neg\phi)$	S3

Example: $\neg\neg\phi \vdash \phi$

1.	$\neg\neg\phi, \neg\phi \vdash \neg\neg\phi$	S1
2.	$\neg\neg\phi, \neg\phi \vdash \neg\phi$	S1
3.	$\neg\neg\phi \vdash \phi$	C1

Lemma 3.2 (Second Contradiction Rule)

$$\frac{\Gamma \vdash \psi \quad \Gamma \vdash \neg\psi}{\Gamma \vdash \phi}$$

Proof

1.	$\Gamma \vdash \psi$	Premise
2.	$\Gamma, \neg\phi \vdash \psi$	S2
3.	$\Gamma \vdash \neg\psi$	Premise
4.	$\Gamma, \neg\phi \vdash \neg\psi$	S2
5.	$\Gamma \vdash \phi$	C1

Lemma 3.3 (Chain Rule)

$$\frac{\Gamma \vdash \phi \quad \Gamma, \phi \vdash \psi}{\Gamma \vdash \psi}$$

Proof

1.	$\Gamma \vdash \phi$	Premise
2.	$\Gamma, \neg\phi \vdash \phi$	S2
3.	$\Gamma, \neg\phi \vdash \neg\phi$	S1
4.	$\Gamma, \neg\phi \vdash \psi$	Apply 3.2 to 2,3
5.	$\Gamma, \phi \vdash \psi$	Premise
6.	$\Gamma \vdash \psi$	apply S3 to 4,5

Having proved the Second Contradiction Rule, we are now free to use it as if it was an inference rules.

Lemma 3.4 (Contraposition)

$$\frac{\Gamma, \phi \vdash \psi}{\Gamma, \neg\psi \vdash \neg\phi}$$

Proof

1.	$\Gamma, \phi \vdash \psi$	Premise
2.	$\Gamma, \neg\psi, \phi \vdash \psi$	S2
3.	$\Gamma, \neg\psi, \phi \vdash \neg\psi$	S1
4.	$\Gamma, \neg\psi, \phi \vdash \neg\phi$	apply 3.2 to 2,3
5.	$\Gamma, \neg\psi, \neg\phi \vdash \neg\phi$	S1
6.	$\Gamma, \neg\psi \vdash \neg\phi$	apply S3 to 4,5

Exercise 3.5 We can similarly prove the following versions of the contraposition law.

$$\frac{\Gamma, \neg\phi \vdash \neg\psi}{\Gamma, \psi \vdash \phi} \qquad \frac{\Gamma, \neg\phi \vdash \psi}{\Gamma, \neg\psi \vdash \phi} \qquad \frac{\Gamma, \phi \vdash \neg\psi}{\Gamma, \psi \vdash \neg\phi}$$

Lemma 3.6 (Modus ponens)

$$\frac{\Gamma \vdash (\phi \rightarrow \psi) \qquad \Gamma \vdash \phi}{\Gamma \vdash \psi}$$

Proof

Recall that $(\phi \rightarrow \psi)$ is an abbreviation for $(\neg\phi \vee \psi)$.

1.	$\Gamma \vdash \phi$	Premise
2.	$\Gamma, \neg\phi \vdash \phi$	S2
3.	$\Gamma, \neg\phi \vdash \neg\phi$	S1
4.	$\Gamma, \neg\phi \vdash \psi$	3.2 applied to 2,3
5.	$\Gamma, \psi \vdash \psi$	S1
6.	$\Gamma, (\neg\phi \vee \psi) \vdash \psi$	C2
7.	$\Gamma \vdash (\neg\phi \vee \psi)$	Premise
8.	$\Gamma \vdash \psi$	3.3 applied to 6,7

<u>**Equality Rules**</u>:

E1.(Reflexivity) Let t be any term.

$$\vdash t = t$$

E2. (Substitution) Let $\phi(v)$ be a formula in which v occurs freely Let t_0, t_1 be terms and let $\phi(t_i)$ be the formula obtained by substituting t_i for all free occurences of$v$ in $\phi(v)$.

$$\frac{\Gamma \vdash \phi(t_0)}{\Gamma, t_0 = t_1 \vdash \phi(t_1)}$$

We give two sample derivations.

Example: $t_0 = t_1 \vdash t_1 = t_0$.

Let $\phi(v)$ be "$v = t_0$".

1.	$\vdash t_0 = t_0$	E1
2.	$t_0 = t_1 \vdash t_0 = t_0$	S2
3.	$t_0 = t_1, t_0 = t_0 \vdash t_1 = t_0$	E2 applied to $\phi(v)$
4.	$t_0 = t_1 \vdash t_1 = t_0$	3.3

Example: $t_0 = t_1, t_1 = t_2 \vdash t_0 = t_2$

Substitute t_2 for t_1 in $t_0 = t_1$.

We conclude our list of inference rules with rules for manipulating quantifiers.

<u>**Quantifier Rules**</u>

Q1. (right $\exists$-introduction) Let $\phi(v)$ be a formula in which v is a free variable (there may be others). Suppose t is a term and $\phi(t)$ is the formula obtained by replacing all free occurences of v by t.

$$\frac{\Gamma \vdash \phi(t)}{\Gamma \vdash \exists v \phi(v)}$$

Q2. (left $\exists$-introduction) Let $\phi(v)$ be a formula in which v is a free variable. Let y be either i) a constant symbol not occuring in Γ or ψ or ii) a variable not occuring freely in Γ or ψ.

$$\frac{\Gamma, \phi(y) \vdash \psi}{\Gamma, \exists v\ \phi(v) \vdash \psi}$$

Q2. expresses the usual way that we prove ψ from $\exists v \phi(v)$. We assume that $\phi(v)$ holds for some v and show that $\phi(v) \vdash \psi$. We then conclude ψ follows from $\exists v\ \phi(v)$.

This completes our list of inference rules. We give one more useful lemma and two sample derivations.

Example: $\vdash \exists x\ x = x$

Let t be a term. Let $\phi(v)$ be $v = v$.

1. $\vdash t = t$ E1
2. $\vdash \exists x\ x = x$ Q1

Lemma 3.7 (Right $\forall$-introduction) *Suppose v does not occur freely in Γ then*

$$\frac{\Gamma \vdash \phi(v)}{\Gamma \vdash \forall v\ \phi(v).}$$

Proof

Let ψ be any sentence. Recall that $\forall v\ \phi(v)$ is an abbreviation for $\neg \exists v\ \neg \phi(v)$.

1.	$\Gamma \vdash \phi(v)$	Premise
2.	$\Gamma, \neg\phi(v) \vdash \phi(v)$	S2
3.	$\Gamma, \neg\phi(v) \vdash \neg\phi(v)$	S1
4.	$\Gamma, \neg\phi(v) \vdash \psi$	apply 3.2 to 2,3
5.	$\Gamma, \exists v \neg\phi(v) \vdash \psi$	Q2
6.	$\Gamma, \neg\psi \vdash \neg\exists v \neg\phi(v)$	apply 3.4 to 5
7.	$\Gamma, \neg\phi(v) \vdash \neg\psi$	apply 3.2 to 2,3
8.	$\Gamma, \exists v \neg\phi(v) \vdash \neg\psi$	Q2
9.	$\Gamma, \psi \vdash \neg\exists v \neg\phi(v)$	apply 3.5 to 8
10.	$\Gamma \vdash \neg\exists v \neg\phi(v)$	by S2 from 6,9

Example: $\exists x \forall y\ \phi(x, y) \vdash \forall y \exists x\ \phi(x, y)$.

1.	$\neg\phi(x, y) \vdash \neg\phi(x, y)$	S1
2.	$\neg\phi(x, y) \vdash \exists y\ \neg\phi(x, y)$	Q1
3.	$\neg\exists y\ \neg\phi(x, y) \vdash \phi(x, y)$	apply 3.5 to 2.
4.	$\neg\exists y\ \neg\phi(x, y) \vdash \exists x \phi(x, y)$	Q1
5.	$\neg\exists y\ \neg\phi(x, y) \vdash \forall y \exists x \phi(x, y)$	3.7
6.	$\exists x \neg\exists y\ \neg\phi(x, y) \vdash \forall y \exists x \phi(x, y)$	Q2

Theorem 3.8 (Soundness Theorem) *Suppose that the assertion $\Gamma \vdash \phi$ can be derived using the inference rules given above. Then $\Gamma \models \phi$.*

Proof

Recall that $\Gamma \models \phi$ if for any $\mathcal{L}$-structure $\mathcal{M}$ and any assignment $\sigma : V \to M$, if $\mathcal{M} \models_\sigma \Gamma$, then $\mathcal{M} \models_\sigma \phi$.

We prove the Soundness Theorem by induction on proofs.

Base cases:

S1. Clearly if $\phi \in \Gamma$, then $\Gamma \models \phi$.

E1. Clearly $\mathcal{M} \models_\sigma t = t$ for any assignment σ.

Inference rules: If we have an inference rule

$$\frac{\Gamma_1 \vdash \phi_1\ \ \ldots\ \ \Gamma_n \vdash \phi_n}{\Delta \vdash \psi}$$

then we must show that if $\Gamma_i \models \phi_i$ for all i, then $\Delta \models \psi$.

This is obvious for S2, C2, C3, E2, and Q1.

S3. Suppose $\Gamma, \phi \models \psi$ and $\Gamma, \neg\phi \models \psi$. If $\mathcal{M} \models \Gamma$, then $\mathcal{M} \models \phi$ or $\mathcal{M} \models \neg\phi$. In either case $\mathcal{M} \models \psi$.

C1. Suppose $\Gamma, \neg\phi \models \psi$ and $\Gamma, \neg\phi \models \neg\psi$. Let $\mathcal{M} \models \Gamma$. Since we can't have $\mathcal{M} \models \psi$ and $\mathcal{M} \models \neg\psi$ we must have $\mathcal{M} \models \phi$.

Q2. This is immediate from lemma 1.2.

Since all of the inference rules preserve truth the soundness theorem holds.

Definition 3.9 Suppose Γ is a (possibly infinite) set of sentences. We say that ϕ is *provable* from Γ if for some finite $\Delta \subseteq \Gamma$ the assertion $\Delta \vdash \phi$ is derivable in our calculus. If ϕ is provable from Γ we write $\Gamma \vdash \phi$.

Corollary 3.10 *If $\Gamma \vdash \phi$, then $\Gamma \models \phi$.*

Proof Let Δ be a finite subset of Γ such that $\Delta \vdash \phi$ is derivable. Then $\Delta \models \phi$. Since any model of Γ is a model of Δ, $\Gamma \models \phi$.

Definition 3.11 : We say that Γ is *consistent* if there is no sentence ϕ such that $\Gamma \vdash \phi$ and $\Gamma \vdash \neg\phi$.

Proposition 3.12 *i) Γ is inconsistent if and only if $\Gamma \vdash \psi$ for every formula ψ.*

ii) If Γ is satisfiable, then Γ is consistent.

iii) If Γ is consistent, then for any formula ϕ either $\Gamma \cup \{\phi\}$ is consistent or $\Gamma \cup \{\neg\phi\}$ is consistent (or both).

iv) If $\Gamma \not\vdash \phi$, then $\Gamma \cup \{\neg\phi\}$ is consistent.

Proof i) If $\Gamma \vdash \phi$ and $\Gamma \vdash \neg\phi$, then $\Gamma \vdash \psi$ by Lemma 3.2. Certainly if every sentence is derivable from Γ, then Γ is inconsistent.

ii) If $\mathcal{A} \models \Gamma$ either $\mathcal{A} \not\models \phi$ or $\mathcal{A} \not\models \neg\phi$. Thus by the Soundness Theorem, $\Gamma \not\vdash \phi$ or $\Gamma \not\vdash \neg\phi$.

iii) Suppose not. Let ψ be any sentence. By i) $\Gamma, \phi \vdash \psi$ and $\Gamma, \neg\phi \vdash \psi$. By S3, $\Gamma \vdash \psi$. Thus Γ is inconsistent.

iv) Suppose $\Gamma \cup \{\neg\phi\}$ is inconsistent. Then $\Gamma \cup \{\neg\phi\} \vdash \phi$. Since $\Gamma \cup \{\phi\} \vdash \phi$, by S3 $\Gamma \vdash \phi$.

In §4 we will prove the converse of 3.12 ii). We will see that this is just a restatement of Gödel's Completeness Theorem.

4 Gödel's Completeness Theorem

In this section we will prove one of the central theorems of mathematical logic

Theorem 4.1 (Gödel's Completeness Theorem) *Let Γ be a set of $\mathcal{L}$-sentences. If $\Gamma \models \phi$ then $\Gamma \vdash \phi$.*

To prove the Completeness Theorem we will infact prove the following converse to 3.12 ii).

(*) If Γ is consistent, then Γ is satisfiable.

Proof (*) $\Rightarrow$ Completeness

Suppose $\Gamma \not\vdash \phi$, then, by 3.12, $\Gamma \cup \{\neg\phi\}$ is consistent. By (*) $\Gamma \cup \{\neg\phi\}$ has a model $\mathcal{M}$. But then $\Gamma \not\models \phi$.

To prove (*) we must actually construct a model of Γ. The method of proof we give here is due to Leon Henkin.

Definition 4.2 We say that a consistent set of $\mathcal{L}$-sentences Σ is *maximal consistent* if for all $\mathcal{L}$-sentences ϕ either $\phi \in \Sigma$ or $\neg\phi \in \Sigma$ (as Σ is consistent exactly one of ϕ and $\neg\phi$ is in Σ).

Lemma 4.3 *i) If Σ is maximal consistent and $\Sigma \vdash \phi$, then $\phi \in \Sigma$.*
ii) If Σ is maxiaml consistent and $\phi \vee \psi \in \Sigma$, then $\phi \in \Sigma$ or $\psi \in \Sigma$.

Proof

i) If not $\neg\phi \in \Sigma$ and Σ is inconsistent.

ii) Otherwise $\neg\phi$ and $\neg\psi$ are both in Σ and hence $\neg(\phi \vee \psi) \in \Sigma$.

Definition 4.4 We say that Σ has the *witness property* if for any $\mathcal{L}$-formula $\phi(v)$, there is a constant c such that

$$\Sigma \vdash (\exists v \phi(v) \ \rightarrow \ \phi(c)).$$

Theories with this property are sometimes called *Henkinized*.

The proof of (*) comes in two steps:

STEP 1. Show that if Γ is consistent, there is $\Sigma \supseteq \Gamma$ which is maximal consistent and Henkinized. (Note: In general we will have to expand the language to get a theory with the witness property.)

STEP 2. Show that if Σ is maximal consistent and has the witness property, then there is a model of Σ.

We will examine STEP 2 first. Let $\mathcal{L}$ denote the language of Σ. Let C be the constants of $\mathcal{L}$. The universe of our model will be equivalence classes of elements of C. If c_1 and c_2 are constants we say that $c_1 E c_2$ iff and only if $c_1 = c_2 \in \Sigma$.

Lemma 4.5 *E is an equivalence relation.*

Proof

Let $c_1, c_2, c_3 \in C$. By E1, E2, and the examples following them

$$\Sigma \vdash c_1 = c_1$$

$$\Sigma, c_1 = c_2 \vdash c_2 = c_1$$

and

$$\Sigma, c_1 = c_2, c_2 = c_3 \vdash c_1 = c_3.$$

Thus, by 4.3, E is an equivalence relation.

For $c \in C$ let $[c]$ denote the equivalence class of c. We now begin to build a structure $\mathcal{A}$ which we call the *canonical structure* for Σ. The underlying set of $\mathcal{A}$ will be

$$A = \{[c] : c \in C\}.$$

The next lemma will allow us to interpret the relation and function symbols of $\mathcal{L}$.

Lemma 4.6 *i) If R is an n-ary relation symbol of $\mathcal{L}$, $c_1, \ldots, c_n, d_1, \ldots, d_n \in C$ and $c_i E d_i$ for all i, then*

$$R(c_1, \ldots, c_n) \in \Sigma \Leftrightarrow R(d_1, \ldots, d_n) \in \Sigma.$$

ii) Let f be an n-ary function symbol of $\mathcal{L}$ and let $c_1, \ldots, c_n \in C$, there is $d \in C$ such that $f(c_1, \ldots, c_n) = d \in \Sigma$.

iii) Let f be an n-ary function symbol of $\mathcal{L}$ and let $c_0, \ldots, c_n, d_0, \ldots, d_n \in C$ such that $c_i E d_i$ for $i \geq 0$, $f(c_1, \ldots, c_n) = c_0 \in \Sigma$ and $f(d_1, \ldots, d_n) = d_0 \in \Sigma$. Then $c_0 = d_0 \in \Sigma$.

Proof

i) By repeated applications of E2,

$$c_1 = d_1, \ldots, c_n = d_n \vdash \ R(c_1, \ldots, c_n) \leftrightarrow R(d_1, \ldots, d_n)$$

ii) By E1

$$\vdash f(c_1, \ldots, c_n) = f(c_1, \ldots, c_n).$$

Thus by Q1

$$\vdash \exists v \ f(c_1, \ldots, c_n) = v.$$

Thus $\exists v \ f(c_1, \ldots, c_n) = v$ is in Σ. Since Σ has the witness proterty, there is a constant symbol d such that $f(c_1, \ldots, c_n) = d \in \Sigma$.

iii) By repeated application of E2,

$$c_1 = d_1, \ldots, c_n = d_n, f(c_1, \ldots, c_n) = c_0 \vdash f(d_1, \ldots, d_n) = c_0$$

Thus $\Sigma \vdash f(d_1, \ldots, d_n) = c_0$ and $\Sigma \vdash f(d_1, \ldots, d_n) = d_0$. By the examples in §3, $\Sigma \vdash c_0 = d_0$.

We can now give the interpretation of $\mathcal{L}$ in $\mathcal{A}$.

- The universe of $\mathcal{A}$ is A.
- For each constant symbol c of $\mathcal{L}$, let $c^{\mathcal{A}} = [c]$.
- If R is an n-ary relation symbol let $R^{\mathcal{A}} \subseteq A^n$ be defined by

$$R^{\mathcal{A}} = \{([c_1], \ldots, [c_n]) \in A^n : R(c_1, \ldots, c_n) \in \Sigma\}.$$

By 4.6 i) $R^{\mathcal{A}}$ is well defined.

- If f is an n-ary function symbol define $f^{\mathcal{A}} : A^n \to A$ by

$$f^{\mathcal{A}}([c_1], \ldots, [c_n]) = d \Leftrightarrow f(c_1, \ldots, c_n) = d \in \Sigma.$$

By 4.6 ii) and iii) $f^{\mathcal{A}}$ is well defined and $f^{\mathcal{A}} : A^n \to A$.

Lemma 4.7 *Suppose $t(v_1, \ldots, v_n)$ is a term (some of the variables may not occur) and $c_0, \ldots, c_n \in C$ such that $t(c_1, \ldots, c_n) = c_0 \in \Sigma$. If σ is an assignment where $\sigma(v_i) = [c_i]$, then $t^{\mathcal{A}}[\sigma] = [c_0]$. Moreover if $d_0, \ldots, d_n \in C$, $t(d_1, \ldots, d_n) = d_0 \in \Sigma$ and $d_i E c_i$ for $i > 0$, then $c_0 E d_0$.*

Proof The moreover is clear since

$$t(c_1,\ldots,c_n)=c_0, t(d_1,\ldots,d_n)=d_0, c_1=d_1,\ldots,c_n=d_n \vdash c_0=d_0$$

so $c_0=d_0\in\Sigma$.

The main assertion is proved by induction on the complexity of t.

If t is a constant symbol c, then $t^{\mathcal{A}}[\sigma]=[c]$. Since $c=c_0\in\Sigma$, $[c]=[c_0]$.

If t is the variable v_i, then $t^{\mathcal{A}}[\sigma]=[c_i]$ and $c_i=c_0\in\Sigma$, thus $[c_0]=t^{\mathcal{A}}[\sigma]$.

Suppose t is $f(t_1,\ldots,t_m)$ and the claim holds for $t_1,\ldots,t_m$. For each i,

$$\exists w\ t_i(c_1,\ldots,c_n)=w\in\Sigma.$$

Thus since Σ has the witness property, for each i there is $b_i\in C$ such that $t_i(c_1,\ldots,c_n)=b_i\in\Sigma$. By our inductive assumption $t_i^{\mathcal{A}}[\sigma]=[b_i]$. Clearly $t(c_1,\ldots,c_n)=f(b_1,\ldots,b_m)\in\Sigma$, thus $f(b_1,\ldots,b_m)=c_0\in\Sigma$. But then

$$t^{\mathcal{A}}[\sigma]=f([b_1],\ldots,[b_m])=[c_0]$$

as desired.

Thus the claim holds for all terms.

Theorem 4.8 *If Σ is a maximal, consistent theory with the witness property and $\mathcal{A}$ is the canonical structure for Σ, then $\mathcal{A}\models\Sigma$.*

Proof

We will prove that for all formulas $\phi(v_1,\ldots,v_n)$ and constants $c_1,\ldots,c_n$,

$$\mathcal{A}\models\phi([c_1],\ldots,[c_n]) \quad \text{if and only if} \quad \phi(c_1,\ldots,c_n)\in\Sigma.$$

This will be proved by induction on the complexity of ϕ.

1) ϕ is $t_1(v_1,\ldots,v_n)=t_2(v_1,\ldots,v_n)$

Since Σ has the witness property there are $d_1,d_2\in C$ such that $t_i(c_1\ldots,c_n)=d_i\in\Sigma$. By Lemma 4.7 $t_i([c_1],\ldots,[c_n])=[d_i]$. Thus

$$\begin{aligned}\mathcal{A}\models t_1([c_1],\ldots,[c_n])=t_2([c_1],\ldots,[c_n]) &\Leftrightarrow [d_1]=[d_2]\\ &\Leftrightarrow t_1(\overline{c})=t_2(\overline{c})\in\Sigma.\end{aligned}$$

2) ϕ is $R(t_1,\ldots,t_m)$ where R is an m-ary relation symbol.

Since Σ has the witness property there are $d_1, \ldots, d_m \in C$ such that $t_i(c_1, \ldots, c_n) = d_i \in \Sigma$. By 4.7, $t_i([c_1], \ldots, [c_n]) = [d_i]$.

$$\begin{aligned} \mathcal{A} \models \phi([c_1], \ldots, [c_n]) &\Leftrightarrow ([d_1], \ldots, [d_m]) \in \widehat{R} \\ &\Leftrightarrow R(d_1, \ldots, d_m) \in \Sigma \\ &\Leftrightarrow R(t_1(\overline{c}), \ldots, t_m(\overline{c})) \in \Sigma. \end{aligned}$$

3) ϕ is $\neg\psi$

Then

$$\begin{aligned} \mathcal{A} \models \phi(\overline{[c]}) &\Leftrightarrow \mathcal{A} \not\models \psi(\overline{[c]}) \\ &\Leftrightarrow \psi(\overline{c}) \notin \Sigma \quad \text{(by induction)} \\ &\Leftrightarrow \phi(\overline{c}) \in \Sigma \text{ since } \Sigma \text{ is maximal.} \end{aligned}$$

4) ϕ is $\psi \vee \theta$

$$\begin{aligned} \mathcal{A} \models \phi(\overline{[c_i]}) &\Leftrightarrow \mathcal{A} \models \psi(\overline{[c_i]}) \vee \mathcal{A} \models \theta(\overline{[c_i]}) \\ &\Leftrightarrow \psi(\overline{c}) \in \Sigma \text{ or } \theta(\overline{c}) \in \Sigma \text{ by induction} \\ &\Leftrightarrow \phi(\overline{c}) \in \Sigma \text{ by 4.3ii).} \end{aligned}$$

5) $\phi(\overline{v})$ is $\exists w\ \psi(w, \overline{v})$

If $\mathcal{A} \models \exists w\ \psi(w, \overline{[c]})$, then there is $d \in C$ such that $A \models \psi([d], \overline{[c]})$. By induction $\psi(d, \overline{c}) \in \Sigma$, and by maximality $\exists w\ \psi(w, \overline{c}) \in \Sigma$.

On the other hand if $\exists w\ \psi(w, \overline{c}) \in \Sigma$, then, since Σ has the witness property, there is $d \in C$, such that $\psi(d, \overline{c}) \in \Sigma$. By induction $\mathcal{A} \models \psi([d], \overline{[c]})$ and $\mathcal{A} \models \phi(\overline{[c]})$.

We have now completed STEP 2. That is, we have shown that if Σ is maximal, consistent theory with the witness property, then there is $\mathcal{A} \models \Sigma$. The completeness theorem will now follow from the following result.

Theorem 4.9 *Let Γ be a consistent $\mathcal{L}$-theory. There is $\mathcal{L}^* \supseteq \mathcal{L}$ and $\Sigma \supseteq \Gamma$ a maximal consistent $\mathcal{L}^*$-theory with the witness property.*

Let $\mathcal{L}_0$=$\mathcal{L}$, let C_0 be the constants of $\mathcal{L}$, and let $\Gamma_0 = \Gamma$. In general let F_n be the set of all $\mathcal{L}_n$-formulas in one free variable v.

Let $\mathcal{L}_{n+1} = \mathcal{L}_n \cup \{c_\phi : \phi(v) \in F_n\}$, where each c_ϕ is a new constant symbol. For $\phi(v) \in \mathbb{F}_n$ let θ_ϕ be the formula

$$(\exists v \phi(v) \ \rightarrow \ \phi(c_\phi)).$$

Let

$$\Gamma_{n+1} = \Gamma_n \cup \{\theta_\phi : \phi \in F_n\}.$$

Let

$$\Gamma^* = \bigcup_{n \geq 0} \Gamma_n$$

and

$$\mathcal{L}^* = \bigcup_{n \geq 0} \mathcal{L}_n.$$

Lemma 4.10 *i) If $\Sigma \supseteq \Gamma^*$ is an $\mathcal{L}^*$-theory, then Σ has the witness property.*
ii) Each Γ_n is consistent.
iii) Γ^* is consistent.

Proof
i) For any $\mathcal{L}^*$ formula $\phi(v)$ in one free variable v, there is an n, such that $\phi(v) \in F_n$. Then $(\exists v \phi(v) \rightarrow \phi(c_\phi)) \in \Gamma_{n+1} \subseteq \Sigma$. Thus Σ has the witness property.

ii) We prove this by induction on n. Since $\Gamma_0 = \Gamma$ it is conistent. Suppose Γ_n is consistent, but Γ_{n+1} is inconsistent. Since the proofs of contradictions are finite, there are $\phi_1, \ldots, \phi_m \in F_n$ such that $\Gamma_n, \theta_{\phi_1}, \ldots, \theta_{\phi_m}$ is inconsistent. By choosing m-minimal we may assume that $\Delta = \Gamma_n, \theta_{\phi_1}, \ldots, \theta_{\phi_{m-1}}$ is consistent. Let $\phi(v)$ be ϕ_m. In particular there is an $\mathcal{L}$-sentence ψ such that

$$\Delta \not\vdash \psi$$

and

$$\Delta, \theta_\phi \vdash \psi.$$

Consider the following proof

1.	$\Delta, \neg\exists v\phi(v) \vdash \neg\exists v\phi(v)$	S1
2.	$\Delta, \neg\exists v\phi(v) \vdash \theta_\phi$	C3 since θ_ϕ is $(\neg\exists v\phi(v) \vee \phi(c_\phi))$
3.	$\Delta, \theta_\phi \vdash \psi$	Premise
4.	$\Delta, \neg\exists v\phi(v), \theta_\phi \vdash \psi$	S2
5.	$\Delta, \neg\exists v\phi(v) \vdash \psi$	apply Lemma 3.3 to 2,4
6.	$\Delta, \phi(c_\phi) \vdash \phi(c_\phi))$	S1
7.	$\Delta, \phi(c_\phi) \vdash \theta_\phi$	C3 since θ_ϕ is $(\neg\exists v\phi(v) \vee \phi(c_\phi))$
8.	$\Delta, \phi(c_\phi), \theta \vdash \phi$	S2 to 2,4
9.	$\Delta, \phi(c_\phi) \vdash \psi$	by Lemma3.3
10.	$\Delta, \exists v\phi(v) \vdash \psi$	Q2 (as c_ϕ does not occur in ψ)
11.	$\Delta \vdash \psi$	S3 applied to 5,10

Thus $\Delta \vdash \psi$, a contradiction.

iii) In general suppose we have consistent theories

$$\Sigma_0 \subseteq \Sigma_1 \subseteq \dots$$

and $\Sigma = \bigcup_n \Sigma_n$. If Σ is inconsistent, there is ϕ such that $\Sigma \vdash \phi \wedge \neg\phi$. Since the proof of $\phi \wedge \neg\phi$ uses only finitely many premises from Σ, there is an n such that $\Sigma_n \vdash \phi \wedge \neg\phi$, a contradiction.

We have one lemma remaining.

Lemma 4.11 *If Δ is a consistent $\mathcal{L}$-theory, there is a maximal consistent $\mathcal{L}$-theory $\Sigma \supseteq \Delta$.*

If we apply Lemma 4.11 to Γ^* from Lemma 4.10 we obtain a maximal consistent $\Sigma \supseteq \Gamma$ with the witness property.

We first prove Lemma 4.11 in the special case that the language $\mathcal{L}$ is countable. We let $\phi_0, \phi_1, \dots$ list all $\mathcal{L}$-sentences. We build a sequence of consistent $\mathcal{L}$-theories

$$\Delta = \Delta_0 \supseteq \Delta_1 \supseteq \Delta_2 \supseteq \dots$$

as follows: We assume that Δ_n is consistent. If $\Delta_n \cup \{\phi_n\}$ is consistent, let $\Delta_{n+1} = \Delta_n \cup \{\phi_n\}$. If not, let $\Delta_{n+1} \cup \{\neg\phi_n\}$. By Lemma 3.12 iii), Δ_n is consistent.

Let $\Sigma = \bigcup_n \Delta_n$. As in Lemma 4.10 iii), Σ is a consistent $\mathcal{L}$-theory. For any ϕ, either ϕ or $\neg\phi$ is in Σ. Thus Σ is maximal consistent.

In the general case when $\mathcal{L}$ is uncountable we need to use Zorn's lemma.

Definition 4.12 Let P be a set and let $<$ be a partial order of P. We say that $X \subseteq P$ is a *chain* if for all $x, y \in X$ $x = y$ or $x < y$ or $x > y$ (ie. $<$ linearly orders X). We say that z is an *upper bound* for X if for all $x \in X$, $x \leq z$. We say that $z \in P$ is *maximal* for $<$ if there is no $z^* \in P$, with $z < z^*$.

Lemma 4.13 (Zorn's Lemma) *Let $(P, <)$ be a partial order such that every chain has an upper bound. Then there is $z \in P$ maximal for $<$.*

Zorn's Lemma is equivalent to the Axiom of Choice.

Proof of Lemma 4.11

Let $P = \{\Gamma \supseteq \Delta : \Gamma \text{ is a consistent } \mathcal{L}\text{-theory}\}$. We order P by $\Gamma_0 < \Gamma_1$ if and only if $\Gamma_0 \subset \Gamma_1$.

Claim If $X \subset P$ is a chain, then X has an upper bound.

Let
$$\Gamma^* = \bigcup_{\Gamma \in X} \Gamma.$$
Clearly for all $\Gamma \in X$, $\Gamma \subseteq \Gamma^*$ thus Γ^* is an upper bound. We need only show that $\Gamma^* \in P$ (ie. Γ^* is consistent).

Suppose Γ^* is inconsistent. Since proofs are finite, there are $\theta_1, \ldots, \theta_m \in \Gamma^*$ such that $\{\theta_1, \ldots, \theta_m\}$ is inconsistent. For each i, there is n_i, such that $\theta_i \in \Gamma_{n_i}$. Since X is a chain, there is $k \leq m$ such that for all i, $\Gamma_{n_i} \subseteq \Gamma_{n_k}$. Thus all $\theta_i \in \Gamma_{n_k}$ and Γ_{n_k} is inconsistent, a contradiction. Hence $\Gamma^* \in P$.

Thus we may apply Zorn's Lemma to obtain $\Sigma \in P$ which is maximal for $<$. Since $\Sigma \in P$, $\Sigma \supseteq \Delta$ and Σ is consistent. Let ϕ be any $\mathcal{L}$-sentence, By 3.12 iii) one of $\Sigma \cup \{\phi\}$ or $\Sigma \cup \{\neg\phi\}$ is consistent. Say $\Sigma \cup \{\phi\}$ is consistent. Then $\phi \in \Sigma$ for otherwise $\Sigma \cup \{\phi\}$ would contradict the maximality of Σ. Thus Σ is maximal.

We can now summarize the proof of the Completeness Theorem. Suppose Γ is a consistent $\mathcal{L}$-theory. By Lemma 4.10 there is $\mathcal{L}^* \supseteq \mathcal{L}$ and $\Gamma^* \supseteq \Gamma$ a consistent $\mathcal{L}^*$-theory such that every $\mathcal{L}^*$-theory extending Γ has the witness property. By Lemma 4.11 there is a maximal consistent $\mathcal{L}^*$-theory $\Sigma \supseteq \Gamma$. By construction Γ has the witness property. By Theorem 4.8 there is $\mathcal{A} \models \Sigma$. Clearly $\mathcal{A} \models \Gamma$.

Our proof gives some information about the size of the model obtained. For $\mathcal{L}$ any language, $|\mathcal{L}|$ is the cardinality of the set of constant, function and relation symbols of $\mathcal{L}$.

Corollary 4.14 *Suppose* Γ *is a consistent* $\mathcal{L}$*-theory. Then* Γ *has a model* $\mathcal{A} = (A, \ldots)$ *with* $|A| \leq |\mathcal{L}| + \aleph_0$.

Proof The model of Γ that we build above as cardinality at most $|C|$, where C is the set of constant symbols of $\mathcal{L}^*$. We argue inductively that $\mathcal{L}_n$ has at most $|\mathcal{L}| + \aleph_0$ constant symbols. This is because $\mathcal{L}_{n+1}$ has at most one new constant symbol for each $\mathcal{L}_n$-formula. In general if a language has κ symbols, there are $\kappa + \aleph_0$ possible formulas (formulas are finite strings of symbols). [Note: Unless κ is finite $\kappa + \aleph_0 = \kappa$.]

5 Basic Model Theory

Our first result is deceptively simple but suprisingly powerful consequence of the Completeness Theorem.

If $\mathcal{L}$ is any language let $||\mathcal{L}||$ denote the cardinality of the set of $\mathcal{L}$-sentences. We know that $||\mathcal{L}|| = \max(|\mathcal{L}|, \aleph_0)$.

Theorem 5.1 (Compactness Theorem) *Suppose* Γ *is a set of sentences and every finite subset of* Γ *is satisfiable. Then* Γ *is satisfiable. Indeed* Γ *has a model of cardinality at most* $||\mathcal{L}||$.

Proof If Γ is not satisfiable, then, by the Completeness Theorem, Γ is inconsistent. Thus for some ϕ, $\Gamma \vdash \phi$ and $\Gamma \vdash \neg\phi$. But then there is a finite $\Delta \subseteq \Gamma$ such that $\Delta \vdash \phi$ and $\Delta \vdash \neg\phi$. By the Soundness Theorem, Δ is not satisfiable.

Corollary 5.2 *Suppose* Γ *has arbitrarily large finite models, then* Γ *has an infinite model.*

Proof Let ϕ_n be the sentence:

$$\exists v_1 \ldots \exists v_n \bigwedge_{i<j\leq n} v_i \neq v_j.$$

Let $\Gamma^* = \Gamma \cup \{\phi_n : n = 1, 2, \ldots\}$. Clearly any model of Γ^* is an infinite model of Γ. If $\Delta \subset \Gamma^*$ is finite, then for some N, $\Delta \subset \Gamma \cup \{\phi_1, \ldots, \phi_N\}$. There is $\mathcal{A} \models \Gamma$ with $|\mathcal{A}| \geq N$, thus $\mathcal{A} \models \Delta$. By the Compactness Theorem, Γ^* has a model.

Corollary 5.3 *Let* $\mathcal{L} = \{+, \cdot, 0, 1, <\}$ *and let* $\mathrm{Th}(\mathbb{N})$*, be the complete theory of the natural numbers. There is* $\mathcal{A} \models \mathrm{Th}(\mathbb{N})$ *with* $a \in \mathcal{A}$ *infinite.*

Proof Let $\mathcal{L}^* = \mathcal{L} \cup \{c\}$, where c is a new constant symbol. Let $\Gamma = \mathrm{Th}(\mathbb{N}) \cup \{c > 0, c > 1, c > 1+1, c > 1+1+1, \ldots\}$. If $\Delta \subset \Gamma$ is finite, then

$$\Delta \subseteq \mathrm{Th}(\mathbb{N}) \cup \{c > 0, \ldots, c > \underbrace{1 + \ldots + 1}_{N-\text{times}}\}$$

for some N. But then we can find a model of Δ by taking the natural numbers and interpreting c as $N+1$. Thus by the Compactness Theorem Γ^* has a model. In this model the interpretation of c is greater that every natural number.

Example: Let $G = (V, E)$ be a graph such that every finite subgraph can be four colored (for example suppose G is a planar graph). We claim that G can be four colored. Let $\mathcal{L} = \{R, B, Y, G\} \cup \{c_v : v \in V\}$. Let Γ be the $\mathcal{L}$-theory with axioms:

i) $\forall x\ [(R(x) \wedge \neg B(x) \wedge \neg Y(x) \wedge \neg G(x)) \vee \ldots \vee (\neg R(x) \wedge \neg B(x) \wedge \neg Y(x) \wedge G(x))]$

ii) if $(v, w) \in E$ add the axiom: $\neg(R(c_v) \wedge R(c_w)) \wedge \ldots \wedge \neg(G(c_v) \wedge G(c_w))$.

If Δ is a finite subset of Γ, let V_Δ be the verticies such that c_v is used in Δ. Since the restriction of G to V_Δ is four colorable, Δ is consistent. Thus Γ is consistent. Let $\mathcal{A} \models \Gamma$.

Color G by coloring v as $\mathcal{A}$ colors c_v.

Theorem 5.4 (Löwenheim–Skolem Theorem) *Suppose* Γ *is an* $\mathcal{L}$*-theory. If* Γ *has an infinite model, then it has a model of cardinality* κ *for every* $\kappa \geq ||\mathcal{L}||$.

Proof Let I be a set of cardinality κ. Let $\mathcal{L}^* = \mathcal{L} \cup \{c_\alpha : \alpha \in I\}$. Let

$$\Gamma^* = \Gamma \cup \{c_\alpha \neq c_\beta : \alpha < \beta\}.$$

If Δ is a finite subset of Γ^*, then in any infinit model $\mathcal{A}$ of Γ we can interpret the constants such that $\mathcal{A} \models \Delta$. Thus Γ has a model of size at most κ. But certainly any model of Γ^* has size at least κ (the map $\alpha \mapsto \widehat{c}_\alpha$ is one to one).

Definition 5.5 A consistent theory Γ is *complete* if $\Gamma \models \phi$ or $\Gamma \models \neg\phi$ for all $\mathcal{L}$-sentences ϕ.

It is easy to see that Γ is complete if and only if $\mathcal{M} \prec \mathcal{N}$ for any $\mathcal{M}, \mathcal{N} \models \Gamma$. If $\mathcal{M}$ is an $\mathcal{L}$-structure, then $\mathrm{Th}(\mathcal{M})$ is a complete theory, but it may be difficult to figure out if $\phi \in \mathrm{Th}(\mathcal{M})$. We will give one useful test to decide if a theory is complete.

Definition 5.6 Γ is κ-categorical if and only if any two models of Γ of cardinality κ are isomorphic.

Let $\mathcal{L} = \{+, 0\}$ be the language of additive groups and let T be the $\mathcal{L}$-theory of torsion-free divisible Abelian groups. The axioms of T are the axioms for Abelian groups together with the axioms

$$\forall x (x \neq 0 \rightarrow \underbrace{x + \ldots + x}_{n-\text{times}} \neq 0)$$

and

$$\forall y \exists x \ \underbrace{x + \ldots + x}_{n-\text{times}} = y$$

for $n = 1, 2, \ldots$.

Proposition 5.7 *The theory of torsion-free divisible Abelian groups is κ-categorical for all $\kappa > \aleph_0$.*

Proof We first argue that models of T are essentially vector spaces over the field of rational numbers $\mathbb{Q}$. Clearly, if V is any vector space over $\mathbb{Q}$, then the underlying additive group of V is a model of T. On the other hand, if $G \models T$, $g \in G$, and $n \in \mathbb{N}$ with $n > 0$, we can find $h \in G$ such that $nh = g$. If $nk = g$, then $n(h - k) = 0$. Because G is torsion-free there is a unique $h \in G$ such that $nh = g$. We call this element g/n. We can view G as a $\mathbb{Q}$-vector space under the action $\frac{m}{n} g = m(g/n)$.

Two $\mathbb{Q}$-vector spaces are isomorphic if and only if they have the same dimension. Thus, models of T are determined up to isomorphism by their dimension. If G has dimension λ, then $|G| = \lambda + \aleph_0$. If κ is uncountable and G has cardinality κ, then G has dimension κ. Thus, for $\kappa > \aleph_0$ any two models of T of cardinality κ are isomorphic.

Note that T is not $\aleph_0$-categorical. Indeed, there are $\aleph_0$ nonisomorphic models corresponding to vector spaces of dimension $1, 2, 3, \ldots$ and $\aleph_0$.

A similar argument applies to the theory of algebraically closed fields. Let ACF_p be the theory of algebraically closed fields of characteristic p, where p is either 0 or a prime number.

Proposition 5.8 ACF_p *is κ-categorical for all uncountable cardinals κ.*

Proof Two algebraically closed fields are isomorphic if and only if they have the same characteristic and transcendence degree (see, for example Lang's *Algebra* X §1). An algebraically closed field of transcendence degree λ has cardinality $\lambda + \aleph_0$. If $\kappa > \aleph_0$, an algebraically closed field of cardinality κ also has transcendence degree κ. Thus, any two algebraically closed fields of the same characteristic and same uncountable cardinality are isomorphic.

We give two simpler examples.

• Let $\mathcal{L}$ be the empty language. Then the theory of an infinite set is κ-categorical for all cardinals κ.

• Let $\mathcal{L} = \{E\}$, where E is a binary relation, and let T be the theory of an equivalence relation with exactly two classes, both of which are infinite. It is easy to see that any two countable models of T are isomorphic. On the other hand, T is not κ-categorical for $\kappa > \aleph_0$. To see this, let $\mathcal{M}_0$ be a model where both classes have cardinality κ, and let $\mathcal{M}_1$ be a model where one class has cardinality κ and the other has cardinality $\aleph_0$. Clearly, $\mathcal{M}_0$ and $\mathcal{M}_1$ are not isomorphic.

Theorem 5.9 (Vaught's Test) *Suppose every model of Γ is infinite, $\kappa \geq ||\mathcal{L}||$ and Γ is κ-categorical. Then Γ is complete.*

Proof Suppose not. Let ϕ be an $\mathcal{L}$-sentence such that $\Gamma \not\models \phi$ and $\Gamma \not\models \neg\phi$. Let $\Gamma_0 = \Gamma \cup \{\phi\}$ and $\Gamma_1 = \Gamma \cup \{\neg\phi\}$. Each Γ_i has a model, thus since Γ has only infinite models, each Γ_i has an infinite model. By the Löwenheim-Skolem theorem there is $\mathcal{A}_i \models \Gamma_i$ where $\mathcal{A}_i$ has cardinality κ. Since Γ is κ-categorical, $\mathcal{A}_0 \cong \mathcal{A}_1$ and hence by 1.16, $\mathcal{A}_0 \prec \mathcal{A}_1$. But $\mathcal{A}_0 \models \phi$ and $\mathcal{A}_1 \models \neg\phi$, a contradiction.

The assumption that T has no finite models is necessary. Suppose that T is the $\{+, 0\}$-theory of Abelian groups, where every element has order 2. In the exercises, we will show that T is κ-categorical for all $\kappa \geq \aleph_0$. However, T is not complete. The sentence $\exists x \exists y \exists z\ (x \neq y \wedge y \neq z \wedge z \neq x)$ is false in the two-element group but true in every other model of T.

Vaught's test implies that all of the categorical theories discussed above are complete. In particular, algebraically closed fields are complete. This result of Tarski has several immediate interesting consequences.

The next definition is, for the moment, imprecise. In later chapters we will make the concepts precise.

Definition 5.10 We say that an $\mathcal{L}$-theory T is *decidable* if there is an algorithm that when given an $\mathcal{L}$-sentence ϕ as input decides whether $T \models \phi$.

Lemma 5.11 *Let T be a recursive complete satisfiable theory in a recursive language $\mathcal{L}$. Then T is decidable.*

Proof Start enumerating all finite sequence of strings of $\mathcal{L}$-symbols. For each one, check to see if it is a derivation in the sequent calculus of $\Delta \vdash \phi$ or $\Delta \vdash \neg\phi$. If it is then check to see if all of the sentences in Δ and in Γ. If so output yes if $\Delta \vdash \phi$ and no if $\Delta \vdash \neg\phi$. If not, for on to the next string. Since Γ is complete, the completeness theorem implies there is a finite $\Delta \subseteq \Gamma$ such that $\Delta \vdash \phi$ or $\Delta \vdash \neg\phi$. Thus our search will halt at some stage.

Informally, to decide whether ϕ is a logical consequence of a complete satisfiable recursive theory T, we begin searching through possible proofs from T until we find either a proof of ϕ or a proof of $\neg\phi$. Because T is satisfiable, we will not find proofs of both. Because T is complete, we will eventually find a proof of one or the other.

Corollary 5.12 *For $p = 0$ or p prime,* ACF_p *is decidable. In particular,* $\mathrm{Th}(\mathbb{C})$*, the first-order theory of the field of complex numbers, is decidable.*

The completeness of ACF_p can also be thought of as a first-order version of the Lefschetz Principle from algebraic geometry.

Corollary 5.13 *Let ϕ be a sentence in the language of rings. The following are equivalent.*

i) ϕ is true in the complex numbers.

ii) ϕ is true in every algebraically closed field of characteristic zero.

iii) ϕ is true in some algebraically closed field of characteristic zero.

iv) There are arbitrarily large primes p such that ϕ is true in some algebraically closed field of characteristic p.

v) There is an m such that for all $p > m$, ϕ is true in all algebraically closed fields of characteristic p.

Proof The equivalence of i)–iii) is just the completeness of ACF_0 and v)$\Rightarrow$ iv) is obvious.

For ii) $\Rightarrow$ v) suppose that $\mathrm{ACF}_0 \models \phi$. There is a finite $\Delta \subset \mathrm{ACF}_0$ such that $\Delta \vdash \phi$. Thus, if we choose p large enough, then $\mathrm{ACF}_p \models \Delta$. Thus, $\mathrm{ACF}_p \models \phi$ for all sufficiently large primes p.

For iv) $\Rightarrow$ ii) suppose $\mathrm{ACF}_0 \not\models \phi$. Because ACF_0 is complete, $\mathrm{ACF}_0 \models \neg\phi$. By the argument above, $\mathrm{ACF}_p \models \neg\phi$ for sufficiently large p; thus, iv) fails.

Ax found the following striking application of Corollary 5.13.

Theorem 5.14 *Every injective polynomial map from $\mathbb{C}^n$ to $\mathbb{C}^n$ is surjective.*

Proof Remarkably, the key to the proof is the simple observation that if k is a finite field, then every injective function $f : k^n \to k^n$ is surjective. From this observation it is easy to show that the same is true for $\mathbb{F}_p^{\mathrm{alg}}$, the algebraic closure of the p-element field.

Claim Every injective polynomial map $f : (\mathbb{F}_p^{\mathrm{alg}})^n \to (\mathbb{F}_p^{\mathrm{alg}})^n$ is surjective.

Suppose not. Let $\overline{a} \in \mathbb{F}_p^{\mathrm{alg}}$ be the coefficients of f and let $\overline{b} \in (\mathbb{F}_p^{\mathrm{alg}})^n$ such that $\overline{b}$ is not in the range of f. Let k be the subfield of $\mathbb{F}_p^{\mathrm{alg}}$ generated by $\overline{a}, \overline{b}$. Then $f|k^n$ is an injective but not surjective polynomial map from k^n into itself. But $\mathbb{F}_p^{\mathrm{alg}} = \bigcup_{n=1}^{\infty} \mathbb{F}_{p^n}$ is a locally finite field. Thus k is finite, a contradiction.

Suppose that the theorem is false. Let $X = (X_1, \ldots, X_n)$. Let $f(X) = (f_1(X), \ldots, f_n(X))$ be a counterexample where each $f_i \in \mathbb{C}[X]$ has degree at most d. There is an $\mathcal{L}$-sentence $\Phi_{n,d}$ such that for K a field, $K \models \Phi_{n,d}$ if and only if every injective polynomial map from K^n to K^n where each coordinate function has degree at most d is surjective. We can quantify over polynomials of degree at most d by quantifying over the coefficients. For example, $\Phi_{2,2}$ is the sentence

$$\forall a_{0,0} \forall a_{0,1} \forall a_{0,2} \forall a_{1,0} \forall a_{1,1} \forall a_{2,0} \forall b_{0,0} \forall b_{0,1} \forall b_{0,2} \forall b_{1,0} \forall b_{1,1} \forall b_{2,0}$$

$$\Big[(\forall x_1 \forall y_1 \forall x_2 \forall y_2 ((\sum a_{i,j} x_1^i y_1^j = \sum a_{i,j} x_2^i y_2^j \wedge \sum b_{i,j} x_1^i y_1^j = \sum b_{i,j} x_2^i y_2^j) \rightarrow$$

$$(x_1 = x_2 \wedge y_1 = y_2))) \rightarrow \forall u \forall v \exists x \exists y \sum a_{i,j} x^i y^j = u \wedge \sum b_{i,j} x^i y^j = v \Big].$$

By the claim $\mathbb{F}_p^{\mathrm{alg}} \models \Phi_{n,d}$ for all primes p. By Corollary 5.13, $\mathbb{C} \models \Phi_{n,d}$, a contradiction.

Back-and-Forth

We give two examples of $\aleph_0$-categorical theories. The proofs use the "back-and-forth" method, a style of argument that has many interesting applications. We start with Cantor's proof that any two countable dense linear orders are isomorphic.

Let $\mathcal{L} = \{<\}$ and let DLO be the theory of dense linear orders without endpoints. DLO is axiomatized by the axioms for linear orders plus the axioms

$$\forall x \forall y\ (x < y \rightarrow \exists z\ x < z < y)$$

and

$$\forall x \exists y \exists z\ y < x < z.$$

Theorem 5.15 *The theory DLO is $\aleph_0$-categorical and complete.*

Proof Let $(A, <)$ and $(B, <)$ be two countable models of DLO. Let $a_0, a_1, a_2, \ldots$ and $b_0, b_1, b_2, \ldots$ be one-to-one enumerations of A and B. We will build a sequence of partial bijections $f_i : A_i \rightarrow B_i$ where $A_i \subset A$ and $B_i \subset B$ are finite such that $f_0 \subseteq f_1 \subseteq \ldots$ and if $x, y \in A_i$ and $x < y$, then $f_i(x) < f_i(y)$. We call f_i a *partial embedding*. We will build these sequences such that $A = \bigcup A_i$ and $B = \bigcup B_i$. In this case, $f = \bigcup f_i$ is the desired isomorphism from $(A, <)$ to $(B, <)$.

At odd stages of the construction we will ensure that $\bigcup A_i = A$, and at even stages we will ensure that $\bigcup B_i = B$.

<u>stage 0</u>: Let $A_0 = B_0 = f_0 = \emptyset$.

<u>stage $n + 1 = 2m + 1$</u>: We will ensure that $a_m \in A_{n+1}$.

If $a_m \in A_n$, then let $A_{n+1} = A_n, B_{n+1} = B_n$ and $f_{n+1} = f_n$. Suppose that $a_m \notin A_n$. To add a_m to the domain of our partial embedding, we must find $b \in B \setminus B_n$ such that

$$\alpha < a_m \Leftrightarrow f_n(\alpha) < b$$

for all $\alpha \in A_n$. In other words, we must find $b \in B$, which is in the image under f_n of the cut of a_m in A_n. Exactly one of the following holds:

i) a_m is greater than every element of A_n, or

ii) a_m is less than every element of A_n, or

iii) there are α and $\beta \in A_n$ such that $\alpha < \beta$, $\gamma \leq \alpha$ or $\gamma \geq \beta$ for all $\gamma \in A_n$ and $\alpha < a_m < \beta$.

In case i) because B_n is finite and $B \models$ DLO, we can find $b \in B$ greater than every element of B_n. Similarly in case ii) we can find $b \in B$ less than every element of B_n. In case iii), because f_n is a partial embedding, $f_n(\alpha) < f_n(\beta)$ and we can choose $b \in B \setminus B_n$ such that $f_n(\alpha) < b < f_n(\beta)$. Note that

$$\alpha < a_m \Leftrightarrow f_n(\alpha) < b$$

for all $\alpha \in A_n$.

In any case, we let $A_{n+1} = A_n \cup \{a_m\}$, $B_{n+1} = B_n \cup \{b\}$, and extend f_n to $f_{n+1} : A_{n+1} \rightarrow B_{n+1}$ by sending a_m to b. This concludes stage n.

stage $n+1 = 2m+2$: We will ensure that $b_m \in B_{n+1}$.

Again, if b_m is already in B_n, then we make no changes and let $A_{n+1} = A_n, B_{n+1} = B_n$ and $f_{n+1} = f_n$. Otherwise, we must find $a \in A$ such that the image of the cut of a in A_n is the cut of b_m in B_n. This is done as in the odd case.

Clearly, at odd stages we have ensured that $\bigcup A_n = A$ and at even stages we have ensured that $\bigcup B_n = B$. Because each f_n is a partial embedding, $f = \bigcup f_n$ is an isomorphism from A onto B.

Because there are no finite dense linear orders, Vaught's test implies that DLO is complete.

The proof of Theorem 5.15 is an example of a *back-and-forth* construction. At odd stages, we go forth trying to extend the domain, whereas at even stages we go back trying to extend the range. We give another example of this method.

The Random Graph

Let $\mathcal{L} = \{R\}$, where R is a binary relation symbol. We will consider an $\mathcal{L}$-theory containing the graph axioms $\forall x\, \neg R(x,x)$ and $\forall x \forall y\, R(x,y) \rightarrow R(y,x)$. Let ψ_n be the "extension axiom"

$$\forall x_1 \ldots \forall x_n \forall y_1 \ldots \forall y_n \left(\bigwedge_{i=1}^{n} \bigwedge_{j=1}^{n} x_i \neq y_j \rightarrow \exists z \bigwedge_{i=1}^{n} (R(x_i,z) \wedge \neg R(y_i,z)) \right).$$

We let T be the theory of graphs where we add $\{\exists x \exists y\, x \neq y\} \cup \{\psi_n : n = 1, 2, \ldots\}$ to the graph axioms. A model of T is a graph where for any finite disjoint sets X and Y we can find a vertex with edges going to every vertex in X and no vertex in Y.

Theorem 5.16 *T is satisfiable and $\aleph_0$-categorical. In particular, T is complete and decidable.*

Proof We first build a countable model of T. Let G_0 be any countable graph.

Claim There is a graph $G_1 \supset G_0$ such that G_1 is countable and if X and Y are disjoint finite subsets of G_0 then there is $z \in G_1$ such that $R(x,z)$ for $x \in X$ and $\neg R(y,z)$ for $y \in Y$.

Let the vertices of G_1 be the vertices of G_0 plus new vertices z_X for each finite $X \subseteq G_0$. The edges of G_1 are the edges of G together with new edges between x and z_X whenever $X \subseteq G_0$ is finite and $x \in X$. Clearly, G_1 is countable and has the desired property.

We iterate this construction to build a sequence of countable graphs $G_0 \subset G_1 \subset \ldots$ such that if X and Y are disjoint finite subsets of G_i, then there is $z \in G_{i+1}$ such that $R(x,z)$ for $x \in X$ and $\neg R(y,z)$ for $y \in Y$. Then, $G = \bigcup G_n$ is a countable model of T.

Next we show that T is $\aleph_0$-categorical. Let G_1 and G_2 be countable models of T. Let $a_0, a_1, \ldots$ list G_1, and let $b_0, b_1, \ldots$ list G_2. We will build a sequence of finite partial one-to-one maps $f_0 \subseteq f_1 \subseteq f_2 \subseteq \ldots$ such that for all x, y in the domain of f_s,

$$G_1 \models R(x,y) \quad \text{if and only if} \quad G_2 \models R(f_s(x), f_s(y)). \qquad (*)$$

Let $f_0 = \emptyset$.

<u>stage $s+1 = 2i+1$</u>: We make sure that a_i is in the domain.

If a_i is in the domain of f_s, let $f_{s+1} = f_s$. If not, let $\alpha_1, \ldots, \alpha_m$ list the domain of f_s and let $X = \{j \leq m : R(\alpha_j, a_i)\}$ and let $Y = \{j \leq m : \neg R(\alpha_j, a_i)\}$. Because $G_2 \models T$, we can find $b \in G_2$ such that $G_2 \models R(f_s(\alpha_j), b)$ for $j \in X$ and $G_2 \models \neg R(f_s(\alpha_j), b)$ for $j \in Y$. Let $f_{s+1} = f_s \cup \{(a_i, b)\}$. By choice of b and induction, f_{s+1} satisfies $(*)$.

<u>stage $s+1 = 2i+2$</u>: By a similar argument, we can ensure that f_{s+1} satisfies $(*)$ and b_i is in the image of f_{s+1}.

Let $f = \bigcup f_s$. We have ensured that f maps G_1 onto G_2. By $(*)$, f is a graph isomorphism. Thus, $G_1 \cong G_2$ and T is $\aleph_0$-categorical.

Because all models of T are infinite, T is complete. Because T is recursively axiomatized, T is decidable.

The theory T is very interesting because it gives us insights into random finite graphs. Let $\mathcal{G}_N$ be the set of all graphs with vertices $\{1, 2, \ldots, N\}$. We consider a probability measure on $\mathcal{G}_N$ where we make all graphs equally likely. This is the same as constructing a random graph where we independently decide whether there is an edge between i and j with probability $\frac{1}{2}$. For any $\mathcal{L}$-sentence ϕ,

$$p_N(\phi) = \frac{|\{G \in \mathcal{G}_N : G \models \phi\}|}{|\mathcal{G}_N|}$$

is the probability that a random element of $\mathcal{G}_N$ satisfies ϕ.

We argue that large graphs are likely to satisfy the extension axioms.

Lemma 5.17 $\lim_{N \to \infty} p_N(\psi_n) = 1$ *for* $n = 1, 2, \ldots$.

Proof Fix n. Let G be a random graph in $\mathcal{G}_N$ where $N > 2n$. Fix $x_1, \ldots, x_n, y_1, \ldots, y_n, z \in G$ distinct. Let q be the probability that

$$\neg\left(\bigwedge_{i=1}^{n}(R(x_i, z) \wedge \neg R(y_i, z))\right).$$

Then $q = 1 - 2^{-2n}$. Because these probabilities are independent, the probability that

$$G \models \neg\exists z \neg\left(\bigwedge_{i=1}^{n}(R(x_i, z) \wedge \neg R(y_i, z))\right)$$

is q^{N-2n}. Let M be the number of pairs of disjoint subsets of G of size n. Thus

$$p_N(\neg\psi_n) \leq Mq^{N-2n} < N^{2n}q^{N-2n}.$$

Because $q < 1$,

$$\lim_{N\to\infty} p_N(\neg\psi_n) = \lim_{N\to\infty} N^{2n}q^N = 0,$$

as desired.

We can now use the fact that T is complete to get a good understanding of the asymptotic properties of random graphs.

Theorem 5.18 (Zero-One Law for Graphs) *For any $\mathcal{L}$-sentence ϕ either $\lim_{N\to\infty} p_N(\phi) = 0$ or $\lim_{N\to\infty} p_N(\phi) = 1$. Moreover, T axiomatizes $\{\phi : \lim_{N\to\infty} p_N(\phi) = 1\}$, the* almost sure theory of graphs. *The almost sure theory of graphs is decidable and complete.*

Proof If $T \models \phi$, then there is n such that if G is a graph and $G \models \psi_n$, then $G \models \phi$. Thus, $p_N(\phi) \geq p_N(\psi_n)$ and by Lemma 5.17, $\lim_{N\to\infty} p_N(\phi) = 1$. On the other hand, if $T \not\models \phi$, then, because T is complete, $T \models \neg\phi$ and $\lim_{N\to\infty} p_N(\neg\phi) = 1$ so $\lim_{N\to\infty} p_N(\phi) = 0$.