Herbrand Theorem, Equality, and Compactness

The Herbrand Theorem

We now consider a complete method for proving the unsatisfiability of sets of first-order sentences which is an alternative to LK. This forms the basis of the resolution proof method for the predicate calculus, which is used extensively by automated theorem provers. (See pp 6-9 for propositional resolution.)

Definitions (quantifier-free, $\forall$-sentence, ground instance): A formula A is *quantifier-free* if A has no occurrence of either of the quantifiers $\forall$ or $\exists$. A $\forall$-sentence is a sentence of the form $\forall x_1 ... \forall x_k B$ where $k \geq 0$ and B is a quantifier-free formula. A *ground instance* of this sentence is a sentence of the form $B(t_1/x_1)(t_2/x_2)...(t_k/x_k)$, where $t_1, ..., t_k$ are ground terms (i.e. terms with no variables) from the underlying language.

Notice that a ground instance of a $\forall$-sentence A is a logical consequence of A. Therefore if a set Φ_0 of ground instances of A is unsatisfiable, then A is unsatisfiable.

Definition: An $\mathcal{L}$-*truth assignment* (or just *truth assignment*) is a map

$$\tau : \{\mathcal{L} - \text{atomic formulas}\} \rightarrow \{T, F\}$$

We extend τ to the set of all quantifier-free $\mathcal{L}$-formulas by applying the usual rules for propositional connectives (see page 3).

The above definition of truth assignment is the same as in the propositional calculus, except now we take the set of atoms to be the set of $\mathcal{L}$-atomic formulas. Thus we say that a set Φ_0 of quantifier-free formulas is *propositionally unsatisfiable* if no truth assignment satisfies every member of Φ_0. Note that this is different from simply saying that Φ_0 is *unsatisfiable*, by which we mean that there is no structure $\mathcal{M}$ and object assignment σ which satisfies Φ_0 (see page 23).

Lemma: If a set Φ_0 of quantifier-free sentences is propositionally unsatisfiable, then Φ_0 is unsatisfiable (in the first-order sense).

The converse of the Lemmas is also true, provided that Φ_0 does not contain $=$. This follows from the Herbrand Theorem below.

Proof of Lemma: We prove the contrapositive: Suppose that Φ_0 is satisfiable, and let $\mathcal{M}$ be a structure and σ an object assignment such that $\mathcal{M}$ satisfies Φ_0 under σ. Then $\mathcal{M}$ and σ induce a truth assignment τ by the definition $B^\tau = T$ iff $\mathcal{M} \models B[\sigma]$, where B is an atomic formula. Then $B^\tau = T$ iff $\mathcal{M} \models B[\sigma]$ for each quantifier-free sentence B, so τ satisfies Φ_0. $\square$

We can now state our simplified proof method, which applies to sets of $\forall$-sentences without $=$: Simply take ground instances of sentences in Φ until a propositionally unsatisfiable set Φ_0 is found. The method does not specify how to check for propositional unsatisfiability: any method (such as truth tables) for that will do. Notice that by propositional compactness, it's sufficient to consider finite sets Φ_0 of ground instances. The Herbrand theorem states that this method is sound and complete.

Herbrand Theorem: Let $\mathcal{L}$ be a first-order language without $=$ and with at least one constant symbol, and let Φ be a set of $\forall-\mathcal{L}$-sentences. Then Φ is unsatisfiable iff some finite set Φ_0 of $\mathcal{L}$-ground instances of sentences in Φ is propositionally unsatisfiable.

Herbrand with Equality: The above theorem holds when the language $\mathcal{L}$ includes $=$, provided Φ includes the equality axioms $\mathcal{E}_{\mathcal{L}}$ for $\mathcal{L}$ (next section, page 44).

We suppose that $\mathcal{L}$ does not contain $=$ for the remainder of this section.

Notation: c, d, e stand for constant symbols.

Example: Let
$$\Phi = \{\forall x(Px \supset Pfx), Pc, \neg Pffc\}.$$
Then the set $\mathcal{H}$ of ground terms is $\{c, fc, ffc, ...\}$. We can take the set Φ_0 of ground instances to be
$$\Phi_0 = \{(Pc \supset Pfc), (Pfc \supset Pffc), Pc, \neg Pffc\}.$$
Then Φ_0 is propositionally unsatisfiable, so Φ is unsatisfiable.

Proof (Soundness direction of Herbrand Theorem): We've already proved this: If Φ_0 is propositionally unsatisfiable, then by the above lemma, Φ_0 is unsatisfiable, and hence Φ is unsatisfiable (because each ground instance is a logical consequence of Φ).

Proof (Completeness direction of Herbrand Theorem): We prove the contrapositive: If every finite set of ground instances of Φ is propositionally satisfiable, then Φ is satisfiable.

Let Φ_0 be the set of *all* ground instances of Φ (using ground terms from $\mathcal{L}$). Assuming that every finite subset of Φ_0 is propositionally satisfiable, it follows from the propositional compactness theorem (page 15, Form 3) that the entire set Φ_0 is propositionally satisfiable. Let τ be a truth assignment which satisfies Φ_0. We use τ to construct an $\mathcal{L}$-structure $\mathcal{M}$ which satisfies Φ. We use a term model, similar to that used in the proof of the Completeness Lemma (see page 32).

Let the universe M of $\mathcal{M}$ be the set $\mathcal{H}$ of all ground $\mathcal{L}$-terms.

For each n-ary function symbol f define
$$f^{\mathcal{M}}(t_1, ..., t_n) = ft_1...t_n.$$

(In particular, $c^{\mathcal{M}} = c$ for each constant c, and it follows by induction that $t^{\mathcal{M}} = t$ for each ground term t.)

For each n-ary predicate symbol P of $\mathcal{L}$, define

$$P^{\mathcal{M}} = \{\langle t_1, ..., t_n \rangle : (Pt_1...t_n)^\tau = T\}$$

This completes the specification of $\mathcal{M}$. It follows easily by structural induction that $\mathcal{M} \models B$ iff $B^\tau = T$ for each quantifier-free $\mathcal{L}$-sentence B. Thus $\mathcal{M} \models B$ for every ground instance B of any sentence in Φ. Since every member of Φ is a $\forall$-sentence, and since the elements of the universe are precisely the ground terms, it follows that $\mathcal{M}$ satisfies every member of Φ. (A formal proof would use the Basic Semantic Definition (page 22) and the Substitution Theorem (page 26)). $\Box$

Exercise 1 *Fill in the details in the above argument.*

Exercise 2 *Prove that a satisfiable set of $\forall$ sentences without $=$ and without function symbols except the constants $c_1, ..., c_n$ for $n \geq 1$ has a model with exactly n elements in the universe. Give an example with one binary predicate symbol P showing that $n-1$ elements would not suffice in general. (Hint: Think of P as $<$.)*

We show how to generalize the above method, by adding equality axioms, to the case in which $\mathcal{L}$ has $=$ in the next section. We now show how to generalize the method to arbitrary sentences without equality.

Prenex Form

Definition: We say that a formula A is in *prenex form* if A has the form $Q_1x_1...Q_nx_nB$, where each Q_i is either $\forall$ or $\exists$, and B is a quantifier-free formula.

Theorem: There is a simple procedure which, given a formula A, produces an equivalent formula A' in prenex form.

Proof: First rename all quantified variables in A so that they are all distinct (see page 27). Now move all quantifiers out past the connectives $\wedge, \vee, \neg$ by repeated use of the equivalences below. (Recall that by the Replacement Theorem, page 27, we can replace a subformula in A by an equivalent formula and the result is equivalent to A.)

In each of the following equivalences, we must assume that x does not occur free in C.

$(\forall xB \wedge C) \Longleftrightarrow \forall x(B \wedge C)$
$(\forall xB \vee C) \Longleftrightarrow \forall x(B \vee C)$
$\neg\forall xB \Longleftrightarrow \exists x\neg B$
$(\exists xB \wedge C) \Longleftrightarrow \exists x(B \wedge C)$
$(\exists xB \vee C) \Longleftrightarrow \exists x(B \vee C)$
$\neg\exists xB \Longleftrightarrow \forall x\neg B$
$\Box$

Skolem Functions: To explain how to apply the Herbrand Theorem to a sentence A that is not universal, it is convenient (but not absolutely necessary) to first put A in prenex form. Then we get rid of the existential quantifiers by replacing each existentially quantified variable y by a function symbol $f_y(x_1, ..., x_k)$, where $x_1, ..., x_k$ are the universally quantified variables preceding y in the prefix. The function symbol f_y is called a *Skolem function.*

The simplest case is when the existential quantifier has no universal quantifier in front of it: say A is $\exists yB$, where now B can be any formula. Then we replace y by a new constant c.

Lemma: $\exists yB$ is satisfiable iff $B(c/y)$ is satisfiable, provided c does not occur in B. More generally, if Φ is a set of formulas, then $\{\exists yB\} \cup \Phi$ is satisfiable iff $\{B(c/y)\} \cup \Phi$ is satisfiable, provided that c does not occur in B, nor in any formula in Φ.

Proof: If $\mathcal{M} \models (\{B(c/y)\} \cup \Phi)[\sigma]$, then also $\mathcal{M} \models (\{\exists yB\} \cup \Phi)[\sigma]$, since $c^{\mathcal{M}}[\sigma]$ satisfies the existential quantifier in $\exists yB$. Conversely, if $\mathcal{M} \models (\{\exists yB\} \cup \Phi)[\sigma]$, then we can change $\mathcal{M}$ to $\mathcal{M}'$ by setting $c^{\mathcal{M}'}$ equal to an element in M satisfying the existential quantifier in $\exists yB$. Then $\mathcal{M}' \models B(c/y)$, and also $\mathcal{M}' \models \Phi[\sigma]$, because c does not occur in Φ. $\Box$

Now consider the case $\forall x \exists yB$. If this holds in a structure, then for each value of x we can choose a value $f(x)$ for y making B true.

Lemma: $\forall x \exists yB$ is satisfiable iff $\forall xB(fx/y)$ is satisfiable, provided f is a unary function symbol which does not occur in B. More generally, if Φ is a set of formulas, then $\{\forall x \exists yB\} \cup \Phi$ is satisfiable iff $\{\forall xB(fx/y)\} \cup \Phi$ is satisfiable, provided that f does not occur in B, nor in any formula in Φ.

Proof: Formalize the argument preceding the Lemma. $\Box$

More generally, we construct the *functional form* of a prenex formula A by removing each existential quantifier $\exists y$ in the prefix and replacing y in the formula by $f_y x_1 ... x_k$, where f_y is a new function symbol, and $x_1, ..., x_k$ are the universally quantified variables that precede the quantifier $\exists y$ in the prefix.

Important: To form the functional forms of a set of sentences, it is necessary to make every Skolem function symbol introduced distinct from all Skolem function symbols in all other formulas.

Theorem: A set Φ of sentences is satisfiable iff the set of functional forms of sentences in Φ is satisfiable.

Our more general proof method applies to an arbitrary set Φ of sentences without equality. We first put each sentence of Φ in prenex form, then in functional form, and then apply the Herbrand Theorem. It can be made to apply to sentence with $=$ by including the equality axioms E1,...,E5 (below) in Φ.

Example: We can use this method to show that the set

$$\{(\forall xPx \vee \forall xQx), \neg\forall xPx, \neg\forall xQx\}$$

is unsatisfiable. The prenex form of the first sentence is $\forall x\forall y(Px \vee Qy)$. The prenex forms of the last two sentences are $\exists x\neg Px$ and $\exists x\neg Qx$, respectively. Their functional forms are $\neg Pc$ and $\neg Qd$ (we must plug in distinct constants for the distinct existential quantifiers). Thus we are to show that the set

$$\{\forall x\forall y(Px \vee Qy), \neg Pc, \neg Qd\}$$

is unsatisfiable. By the Herbrand Theorem, it suffices to find a set of ground instances which is propositionally unsatisfiable. In fact, the last two formulas are already ground instances, and we need only take one ground instance of the first formula. Thus the propositionally unsatisfiable set of ground instances is

$$\{(Pc \vee Qd), \neg Pc, \neg Qd\}.$$

We can check that this set is propositionally unsatisfiable by checking that each of the four truth assignments to the two atomic formulas Pc, Qd falsifies at least one of the three above formulas.

Equality Axioms

Definition: A *weak* $\mathcal{L}$-structure $\mathcal{M}$ is an $\mathcal{L}$-structure in which we drop the requirement that $=^{\mathcal{M}}$ is the equality relation (i.e. $=^{\mathcal{M}}$ can be any binary relation on M.)

Are there sentences $\mathcal{E}$ (axioms for equality) such that if $\mathcal{M}$ is any (proper) structure (i.e. $=^{\mathcal{M}}$ is the equality relation) then $\mathcal{M}$ satisfies $\mathcal{E}$ and every weak structure $\mathcal{M}'$ such that $\mathcal{M}'$ satisfies $\mathcal{E}$ must be a proper structure (i.e. $=^{\mathcal{M}'}$ is equality)?

No such set $\mathcal{E}$ of axioms exists. The reason is that if $\mathcal{M}$ is any (proper) structure with universe M, and $m \in M$ and $m' \notin M$ then we can define $M' = M \cup \{m'\}$ and define $(m, m') \in =^{\mathcal{M}'}$ and let $\mathcal{M}'$ be the same as $\mathcal{M}$ except it has universe M' and $\mathcal{M}'$ on m' acts like $\mathcal{M}$ on m. Then for all formulas A and all object assignments σ, $\mathcal{M} \models A[\sigma]$ iff $\mathcal{M}' \models A[\sigma]$, but $\mathcal{M}'$ is not a proper structure. (In general, we can always inflate a point in a model to a set of points, if $=$ is not present.)

Exercise 3 *Show that for every integer $k \geq 1$ there is a sentence φ with vocabulary $\{;=\}$ for which the following holds: φ is satisfied by a structure with universe M iff M has exactly k elements.*

Exercise 4 *In contrast to the above, show that if Φ is any satisfiable set of first order sentences* not *involving $=$, then Φ has a model with an infinite universe. Use the idea of "inflating" a point, discussed in the preceding paragraph.*

Example: The sentence

$$A =_{syn} \quad \forall x\forall y(x = y)$$

has a model $\mathcal{M}_1$ consisting of one element, and in fact every model (in our sense) of this sentence must have a universe of a single element. But now let M be *any* nonempty set (possibly infinite), and define the weak model $\mathcal{M}_{all}$ with universe M such that $=^{\mathcal{M}_{all}}$ is $M \times M$ (i.e.$=^{\mathcal{M}_{all}}$ holds for all pairs of elements of M.) Note that $\mathcal{M}_{all} \models A$. We claim that if $\mathcal{E}$ is any set of equality axioms (by which we mean any set of valid formulas with vocabulary $\mathcal{L}$ consisting of $=$ alone) then $\mathcal{M}_{all} \models \mathcal{E}[\sigma]$ for any σ. This is because $\mathcal{M}_1 \models \mathcal{E}$ (because $\mathcal{E}$ consists of valid formulas) and by structural induction on B, it is easy to see that any formula B involving only $=$ is satisfied by $\mathcal{M}_{all}$ iff it is satisfied by $\mathcal{M}_1$, (no matter what object assignments σ are chosen).

Nevertheless every language $\mathcal{L}$ has a standard set $\mathcal{E}_{\mathcal{L}}$ of equality axioms which satisfies the Equality Theorem below.

Equality Axioms of $\mathcal{L}$ ($\mathcal{E}_{\mathcal{L}}$)

E1: $\forall x(x = x)$ (reflexivity)
E2: $\forall x \forall y(x = y \supset y = x)$ (symmetry)
E3: $\forall x \forall y \forall z((x = y \wedge y = z) \supset x = z)$ (transitivity)
E4: $\forall x_1 ... \forall x_n \forall y_1 ... \forall y_n(x_1 = y_1 \wedge ... \wedge x_n = y_n) \supset f x_1 ... x_n = f y_1 ... y_n$ for each $n \geq 1$ and each n-ary function symbol f in $\mathcal{L}$.
E5: $\forall x_1 ... \forall x_n \forall y_1 ... \forall y_n(x_1 = y_1 \wedge ... \wedge x_n = y_n) \supset (P x_1 ... x_n \supset P y_1 ... y_n)$ for each $n \geq 1$ and each n-ary predicate symbol P in $\mathcal{L}$ other than $=$.

Axioms E1,E2, E3 assert that $=$ is an equivalence relation. Axiom E4 asserts that functions respect the equivalence classes, and Axiom E5 asserts that predicates respect equivalence classes. Together the axioms assert that $=$ is a congruence relation with respect to the function and predicate symbols.

Remark: The Equality Axioms are valid sentences.

Definition: A set Φ of formulas is *weakly satisfiable* iff Φ is satisfied by some weak structure (i.e. a structure that treats $=$ as an any binary predicate symbol) under some object assignment σ.

Equality Theorem: Let Φ be any set of $\mathcal{L}$-formulas. Then Φ is satisfiable iff $\Phi \cup \mathcal{E}_{\mathcal{L}}$ is weakly satisfiable.

Let us define $\Phi \models_w A$ to mean that for every weak $\mathcal{L}$-structure $\mathcal{M}$ and every object assignment σ, if $\mathcal{M} \models \Phi[\sigma]$ then $\mathcal{M} \models A[\sigma]$ (i.e. $\Phi \cup \{\neg A\}$ is not weakly satisfiable).

Corollary 1: $\Phi \models A$ iff $\Phi \cup \mathcal{E}_{\mathcal{L}} \models_w A$.

Corollary 2: $\forall \Phi \models A$ iff A has an $LK - \Psi$ proof, where $\Psi = \Phi \cup \mathcal{E}_{\mathcal{L}}$.

Corollary 1 follows immediately from the Equality Theorem and the observation that $\Phi \models A$ iff $\Phi \cup \{\neg A\}$ is unsatisfiable.

Corollary 2 follows from Corollary 1 and the derivational completeness of LK (see the theorem page 32), where in applying that theorem we treat $=$ as just another binary relation (so we can assume $\mathcal{L}$ does not have the official equality symbol).

Proof of Equality Theorem: The ONLY IF ($\Longrightarrow$) direction is obvious, because every structure $\mathcal{M}$ must interpret $=$ as true equality, and hence $\mathcal{M}$ satisfies the equality axioms $\mathcal{E}_\mathcal{L}$.

For the IF ($\Longleftarrow$) direction, suppose that $\mathcal{M}$ is a weak $\mathcal{L}$-structure with universe M, such that $\mathcal{M}$ satisfies $\Phi \cup \mathcal{E}_\mathcal{L}$ under some object assignment σ. Our job is to construct a proper structure $\hat{\mathcal{M}}$ and object assignment $\hat{\sigma}$ such that $\hat{\mathcal{M}}$ satisfies Φ under $\hat{\sigma}$.

Denote $=^\mathcal{M}$ by $\sim$. In general $\sim$ is not the equality relation, but it does satisfy the equality axioms E1,...,E5, so it is an equivalence relation on M. If $u \in M$, then we use the notation $[u]$ for the equivalence class of u. Thus

$$[u] = \{v \in M | v \sim u\}$$

Note the following properties of $\sim$ and $[u]$:
(i) $u \sim v$ iff $[u] = [v]$.
(ii) $u \not\sim v$ iff $[u] \cap [v] = \varnothing$.

We define the elements of the universe $\hat{M}$ of $\hat{\mathcal{M}}$ to be the equivalence classes of $\sim$. Each relation $P^\mathcal{M}$ induces a relation $P^{\hat{\mathcal{M}}}$ on $\hat{M}$ and each function $f^\mathcal{M}$ induces a function $f^{\hat{\mathcal{M}}}$ on $\hat{M}$. Specifically, for every variable x, every $\mathcal{L}$-function symbol f, and every $\mathcal{L}$-predicate symbol P,

$$f^{\hat{\mathcal{M}}}([u_1], ..., [u_n]) = [f^\mathcal{M}(u_1, ..., u_n)] \tag{1}$$

$$< [u_1], ..., [u_n] > \in P^{\hat{\mathcal{M}}} \text{ iff } < u_1, ..., u_n > \in P^\mathcal{M} \tag{2}$$

It is important to check that (1) and (2) give consistent definitions of $f^{\hat{\mathcal{M}}}$ and $P^{\hat{\mathcal{M}}}$, independent of the choices of the representatives $u_1, ..., u_n$ for the equivalence classes $[u_1], ..., [u_n]$. This consistency follows from equality axioms E4 and E5 and (i) above.

Now define the object assignment $\hat{\sigma}$ on $\hat{\mathcal{M}}$ by

$$\hat{\sigma}(x) = [\sigma(x)] \tag{3}$$

for each variable x.

Lemma 1: $t^{\hat{\mathcal{M}}}[\hat{\sigma}] = [t^\mathcal{M}[\sigma]]$ for each $\mathcal{L}$-term t.

Proof: Structural induction on terms. The base case is (3), and the induction step uses (1) and the Basic Semantic Definition.

Lemma 2: For every formula A and object assignment σ,

$$\hat{\mathcal{M}} \models A[\hat{\sigma}] \text{ iff } \mathcal{M} \models A[\sigma]$$

Proof: Structural induction on formulas A. The base case (A is atomic) follows from (2) and Lemma 1, and the Basic Semantic Definition. The induction step follows from the Basic Semantic Definition.

This completes the proof of the Equality Theorem.

Equality Axioms for LK

For the purpose of using an LK proof to establish $\Phi \models A$, we can replace the standard equality axioms E1,...,E5 by the following simpler sequents, where we include an instance of the sequent for all $\mathcal{L}$-terms t, u, v, t_i, u_i:

EL1: $\rightarrow t = t$
EL2: $t = u \rightarrow u = t$
EL3: $t = u, u = v \rightarrow t = v$
EL4: $t_1 = u_1, ..., t_n = u_n \rightarrow ft_1...t_n = fu_1...u_n$, for each f in $\mathcal{L}$
EL5: $t_1 = u_1, ..., t_n = u_n, Pt_1...t_n \rightarrow Pu_1...u_n$, for each P in $\mathcal{L}$ (Here P is not $=$)

The fact that these sequents suffice for LK proofs involving equality follows from the Equality Theorem and the Derivational Completeness Theorem (page 32). Note that it is not necessary to put in universal quantifiers in these equality axioms because quantifiers can be introduced as needed by the rule $\forall$-**right**. In fact, we do not need EL1,...,EL5 for all terms t, u, v, t_i, u_i, but only for variables. The reason for including all terms is that it makes it unnecessary to introduce these quantifiers (unless the quantified axioms are subformulas of the conclusion), as indicated by Anchored Completeness with Equality below.

Revised Definition: If Φ is a set of $\mathcal{L}$-formulas, where $\mathcal{L}$ includes $=$, then by an $LK - \Phi$ proof we now mean an $LK - \Psi$ proof in the sense of the earlier definition, page 31, where Ψ is Φ together with all instances of the equality axioms EL1,...,EL5. If Φ is empty, we simply refer to an LK-proof (but allow axioms EL1,...,EL5).

Example

Let the vocabulary $\mathcal{L} = [0, s, +; =]$. Let the set Φ of axioms consist of all term substitution instances of the formulas

$$x + 0 = x$$
$$(x + sy) = s(x + y)$$

(as in the Anchored Completeness Theorem page 37). We want to find an $LK - \Phi$ proof of $0 + s0 = s0$. We need the following two instances of equality axioms:

$$EL3: \quad 0 + s0 = s(0 + 0), s(0 + 0) = s0 \;\rightarrow\; 0 + s0 = s0$$
$$EL4: \quad 0 + 0 = 0 \;\rightarrow\; s(0 + 0) = s0$$

Here is the $LK - \Phi$ proof, where the unlabelled leaves are axioms in Φ:

$$\dfrac{\dfrac{EL3 \qquad \rightarrow 0 + s0 = s(0 + 0)}{s(0 + 0) = s0 \rightarrow 0 + s0 = s0}\,\text{cut} \qquad \dfrac{EL4 \qquad \rightarrow 0 + 0 = 0}{\rightarrow s(0 + 0) = s0}\,\text{cut}}{\rightarrow 0 + s0 = s0}\,\text{cut}$$

From the above discussion, we have

Revised Derivational Soundness and Completeness of LK: For any set Φ of formulas and formula A,

$$\forall\Phi \models A \text{ iff } \rightarrow A \text{ has an } LK - \Phi \text{ proof}$$

Notation: $\Phi \vdash A$ means that there is an $LK - \Phi$ proof of $\rightarrow A$.

Recall that if Φ is a set of sentences, then $\forall\Phi$ is the same as Φ. Therefore

$$\Phi \models A \text{ iff } \Phi \vdash A, \quad \text{if } \Phi \text{ is a set of sentences}$$

Exercise 5 *Give an LK proof of the sequent $A \rightarrow B$, where* [10]

$A =_{syn} \forall x \exists y\ x = fy$
$B =_{syn} \forall x \exists y\ x = ffy$

Start by giving the specific instances of the LK equality axioms EL1,...,EL5 that you need in your proof.

You may use abbreviations for formulas in your proof. You do not need to indicate weakinings or exchanges.

Exercise 6 *Consider the following formulas over the vocabulary $\mathcal{L}_A = [0, s, +, \cdot; =]$:*

Q1: $x + 0 = x$
Q2: $x + sy = s(x + y)$
Q3: $x \cdot 0 = 0$
Q4: $x \cdot sy = (x \cdot y) + x$

Let Φ be the set of ground substitution instances of {Q1,Q2,Q3,Q4}, where a ground substitution instance of A is the result of substituting ground terms for all free variables in A. (Here a ground term *is a term over $\mathcal{L}_A$ with no variables.)*

An example of a sentence in Φ obtained from Q2 is $s0 + s0 = s(s0 + 0)$.

Let $A =_{syn} s0 \cdot s0 = s0$.

You are to give an **LK**-Φ *proof of A.*

Do this as follows:
First list all sentences in Φ that you will need in your LK proof.

Now list all instances *of the LK equality axioms $EL1, \cdots, EL5$ given on page 45 that you will need for the proof. The instances should be specific; for example an instance of $EL1$ is $\rightarrow ss0 = ss0$.*

Now give the required **LK**-Φ *proof, using names for all of the above sentences. You may break the tree into pieces for readability if you wish. (Note that no variables appear in your proof, so you will not need any quantifier rules.)*

We can strengthen the derivational completeness theorem as follows:

Anchored Completeness with Equality: Suppose that Φ is a set of formulas (possibly with $=$) closed under substitution of terms for variables, and $\Gamma \rightarrow \Delta$ is a logical consequence of $\forall\Phi$. Then there is $LK - \Phi$ proof of $\Gamma \rightarrow \Delta$ in which every cut formula is either in Φ or it is an equation of the form $t = u$, for some terms t, u.

This follows from a slight strengthening of the Anchored Completeness Theorem on page 37, together with the Equality Theorem (and the Revised Definition above). Note that we have only proved this for the countable case, although it holds in general.

Major Corollaries of Completeness

First recall that a set S is *countable* if there is a map from $\mathbb{N}$ onto S. In other words, S is countable if its members can be placed into a list $S = \{s_0, s_1, s_2, ...\}$. We allow repetitions, so that all finite sets are countable.

(1) **Lowenheim-Skolem Theorem:** If a set Φ of sentences from a countable language is satisfiable, then Φ is satisfiable in a countable universe.

Proof: Suppose that Φ is a satisfiable set of sentences. We apply the proof of the Completeness Lemma (page 32), treating $=$ as any binary relation, replacing Φ by $\Phi' = \Phi \cup \mathcal{E}_{\mathcal{L}}$, and taking $\Gamma \rightarrow \Delta$ to be the empty sequent (always false). In this case $\Gamma \rightarrow \Delta$ is not a logical consequence of Φ', so the proof constructs a structure $\mathcal{M}$ satisfying Φ' (see page 35). This structure has a countable universe M consisting of all the $\mathcal{L}$-terms. By the proof of the Equality Theorem, we can pass to equivalence classes and construct a countable structure $\hat{\mathcal{M}}$ which satisfies Φ (and interprets $=$ as true equality). $\square$

As an application of the above theorem, we conclude that no countable set of first-order sentences can characterize the real numbers. This is because if the field of real numbers forms a model for the sentences, then there will also be a countable model for the sentences. But the countable model cannot be isomorphic to the field of reals, because there are uncountably many real numbers.

"Skolem's Paradox": The set of real numbers can be characterized as an ordered field such that every bounded nonempty set of elements has a least upper bound. These conditions can be stated as first-order sentences in the language of set theory. But according to the Lowenheim/Skolem Theorem, these sentences have a countable model even though the set of real numbers is uncountable. The paradox is resolved by realizing that it is impossible to have first-order axioms for set theory which enforce the condition that all models must include all sets. Nevertheless, there are axioms of set theory called ZFC (Zermelo-Fraenkel with the axiom of choice) which apparently suffice for formalizing all proofs in (ordinary) existing mathematics.

(2) **First-Order Compactness Theorem:** An infinite set Φ of (first-order) formulas is unsatisfiable iff some finite subset is unsatisfiable. (See also the three alternative forms, page 15.)

Proof: The direction $\Longleftarrow$ is obvious, so we prove the direction $\Longrightarrow$. Assume that Φ is unsatisfiable. Then according to Corollary 1 of the Equality Theorem (page 44) it follows that $\Phi \cup \mathcal{E}_\mathcal{L}$ does not even have a weak $\mathcal{L}$ model (take A to be any unsatisfiable formula). Hence we can apply the Completeness Lemma (page 32), since we may treat $=$ like any binary predicate symbol, and take Γ and Δ empty (the empty sequent is unsatisfiable) to conclude that there is a finite subset Γ' of $\Phi \cup \mathcal{E}_\mathcal{L}$ such that $\Gamma' \to$ has an LK proof. By soundness of LK we conclude that Γ' does not have a weak model. Hence $\Phi_0 \cup \mathcal{E}_\mathcal{L}$ does not have a weak model, where $\Phi_0 = \Gamma' \cap \Phi$. Hence again by Corollary 1 of the Equality Theorem, it follows that Φ_0 is unsatisfiable. $\Box$

(3) **Theorem**: Suppose $\mathcal{L}$ has only finitely many function and predicate symbols. Then the set of valid $\mathcal{L}$-sentences is recursively enumerable. Similarly for the set of unsatisfiable $\mathcal{L}$-sentences.

Concerning the third corollary, a set is *recursively enumerable* if there is an algorithm for enumerating its members. (This idea will be defined later in these notes.) To enumerate the valid formulas, enumerate finite LK proofs. To enumerate the unsatisfiable formulas, note that A is unsatisfiable iff $\neg A$ is valid.

Definition: A set Φ of sentences is *decidable* if there is an algorithm which, given a sentence B, determines whether B is in Φ.

Again this notion will be defined formally later.

Later we will show that if $\mathcal{L}$ is the language $\mathcal{L}_A$ of arithmetic, then the set of valid $\mathcal{L}$-sentences is not decidable. In fact, this is true of every language $\mathcal{L}$ which contains at least one binary predicate symbol other than $=$.

Exercise 7 *(Countable Vaught's Test, an application of Lowenheim-Skolem): A set Φ of $\mathcal{L}$-sentences is said to be* complete *if for every $\mathcal{L}$-sentence A, either $\Phi \models A$ or $\Phi \models \neg A$. Prove that if $\mathcal{L}$ is a countable language and Φ is a set of $\mathcal{L}$-sentences such that any two countable models of Φ are isomorphic, then Φ is complete. (Use the fact that if $\mathcal{M}$ and $\mathcal{M}'$ are isomorphic structures, then $\mathcal{M} \models A$ iff $\mathcal{M}' \models A$, for any sentence A.)*

Exercise 8 *The following set Φ of sentences comprise the axioms for a dense linear order with first element 0 and last element 1, over the language $\mathcal{L} = [0, 1\ ;\ <, =]$.*

$0 < 1$
$\forall x \neg x < x$ *(irreflexive)*
$\forall x \forall y \forall z((x < y \wedge y < z) \supset x < z)$ *(transitive)*
$\forall x \forall y(x < y \vee x = y \vee y < x)$ *(linear)*
$\forall x \forall y \exists z(x < y \supset (x < z \wedge z < y))$ *(dense)*
$\forall x(0 = x \vee 0 < x)$
$\forall x(x = 1 \vee x < 1)$

Note that the structure $\mathbb{Q}[0, 1]$ whose universe is the closed interval [0,1] of rational numbers, with $0, 1, <$ getting their standard meanings, is a countable model for Φ.

a) Prove that any two countable models of Φ are isomorphic (i.e. have an order preserving bijection between them). Hint: Enumerate each of the models $u_1, u_2, \ldots$ without repetition and after initializing the bijection ψ, successively define $\psi(u_1), \psi(u_2), \ldots$.

b) Let $\mathbb{Q}[0,1]$ be the $\mathcal{L}$-structure defined above. Prove that for every $\mathcal{L}$ sentence A, $\mathbb{Q}[0,1] \models A$ iff $\Phi \models A$. (Use Exercise 7.)

Exercise 9 *(Application of compactness). Show that if a set Φ of sentences has arbitrarily large finite models, then Φ has an infinite model. (Hint: For each n construct a sentence A_n which is satisfiable in any universe with n or more elements but not satisfiable in any universe with fewer than n elements.)*

Exercise 10 *(Application of compactness). Let A be first-order sentence over the language $\mathcal{L} = [;R,=]$ where R is a binary predicate symbol. Suppose that for each $n \geq 3$, A has a model consisting of a directed cycle with n nodes, where R represents the edge relation of a directed graph. Prove that A has a model $\mathcal{M}$ whose universe M includes an infinite path; i.e. a set of distinct elements $v_0, v_1, \ldots$ such that $R^{\mathcal{M}}(v_i, v_{i+1})$ holds for all $i \geq 0$.*

Exercise 11 *(Application of compactness). A set Φ of $\mathcal{L}$-sentences is said to be* finitely axiomatizable *if there is a finite set Γ of $\mathcal{L}$-sentences such that Φ and Γ have the same set of models. (Note that Γ is not necessarily a subset of Φ.) Prove that if $\Phi = \{A_1, A_2, \ldots\}$ and for all sufficiently large i*

$$\{A_1, \ldots, A_{i-1}\} \not\models A_i$$

then Φ is not finitely axiomatizable. (Note that it is NOT enough to show that for all i, $\{A_1, \ldots, A_i\}$ does not axiomatize Φ.)

Exercise 12 *(Application to algebraic fields). Let $\mathcal{L}$ be the language $[0,1,+,\cdot]$ and let Φ_1 be the axioms for a field expressed as $\mathcal{L}$-sentences ($0 \neq 1$, $+$ and $\cdot$ are commutative and associative, $x \cdot (y+z) = x \cdot y + x \cdot z$, $0 + x = x, 1 \cdot x = x$, all elements have additive inverses and nonzero elements have multiplicative inverses). Let $p_1, p_2, \ldots$ be the sequence of prime numbers, and let $\hat{p_i}$ stand for the term $((..(1+1)+1\ldots+1)$ with p_i 1's. Let*

$$\Phi_2 = \{\hat{p_1} \neq 0, \hat{p_2} \neq 0, \ldots\}$$

Thus the models of $\Phi_1 \cup \Phi_2$ are precisely the fields of characteristic 0. Use Exercise 11 to prove that $\Phi_1 \cup \Phi_2$ is not finitely axiomatizable.

Nonstandard Models of Arithmetic

Let $\mathcal{L}_s$ (the language of successor) be the language $[0, s; =]$. The *standard model* $\underline{\mathbb{N}}_s$ for $\mathcal{L}_s$ has universe $\mathbb{N}$, and 0 and s get their standard meanings (zero and successor).

Let $Th(s)$ (theory of successor) be the set of all sentences of $\mathcal{L}_s$ which are true in the standard model. It turns out that there is a simple (but infinite) complete set of axioms for $Th(s)$, namely the set Ψ_s:

S1) $\forall x(sx \neq 0)$ (zero has no predecessor)
S2) $\forall x \forall y(sx = sy \supset x = y)$ (successor is one-one)
S3) $\forall x(x = 0 \vee \exists y(x = sy))$ (every nonzero element has a predecessor)

S4) $\forall x(sx \neq x)$
S5) $\forall x(ssx \neq x)$
S6) $\forall x(sssx \neq x)$
.
.
.

The axioms S4, S5, ... assert that successor cannot form a finite loop.

Obviously each of the above sentences is true in the standard model. It is not obvious, but true that every sentence true in the standard model is a logical consequence of this set Ψ_s of axioms. Thus $Th(s)$ is precisely the set of sentences which are logical consequences of Ψ_s. This is a so-called *complete theory*, meaning that for every $\mathcal{L}_s$ sentence A, either $A \in Th(s)$ or $\neg A \in Th(s)$ (i.e. either $\Psi_s \models A$ or $\Psi_s \models \neg A$).

Exercise 13 *(Application of compactness) Use Exercise 11 to show that $Th(s)$ is not finitely axiomatizable.*

Later we will show that in general, if the set of sentences true in some structure has a nice axiomatization such as Ψ_s, then this set is decidable. Thus $Th(s)$ forms a decidable set of sentences.

A *nonstandard* model of $Th(s)$ is any model of $Th(s)$ which is not isomorphic to (i.e. is not a renaming of) the standard model $\underline{\mathbb{N}}$. It is possible to give a complete characterization of all of these nonstandard models.

For each set I (I is an "index" set) we construct a model $\mathcal{M}_I$ of $Th(s)$ as follows. Let the universe M be $\mathbb{N} \cup (I \times \mathbb{Z})$, where $\mathbb{Z}$ is the set of integers. Then define $0^{\mathcal{M}}$ to be the zero in $\mathbb{N}$. Also, $s^{\mathcal{M}}$ is the successor function in $\mathbb{N}$, and in $I \times \mathbb{Z}$ we define $s(< x, n >) =< x, n+1 >$.

It is easy to see that every axiom in Ψ_s is true in the structure $\mathcal{M}_I$. Hence by the discussion above, every sentence true in the standard model is also true in $\mathcal{M}_I$.

It is not too hard to see that every model of Ψ_s (and hence every model of $Th(s)$) is isomorphic to $\mathcal{M}_I$ for some index set I. To see this, let $\mathcal{M}$ be such a model. Divide the universe M into equivalence classes, using the equivalence relation: two elements are equivalent if one can be obtained from the other by finitely many applications of the successor function $s^{\mathcal{M}}$. Then the equivalence class that contains the element $0^{\mathcal{M}}$ must be isomorphic to $\mathbb{N}$, and every other equivalence class is isomorphic to $\mathbb{Z}$. Thus the index set I is the set of equivalence classes, other than the one containing $0^{\mathcal{M}}$.

Presburger Arithmetic: Let $\mathcal{L}_+$ (the language of addition) be the language $[0, s, +; =]$. Let $\mathbb{N}_+$ be the standard model for $\mathcal{L}_+$, and let $Th(+)$ be the set of all sentences of $\mathcal{L}_+$ which are true in the standard model. In 1928, Presburger showed in his PhD thesis that $Th(+)$ is a decidable set, and has a nice axiomatization.

An example of a nonstandard model for $Th(+)$ can be obtained by the ring $\mathbb{Q}[x]$ of polynomials with rational number coefficients. Let the universe M consist of zero, together with all polynomials in $\mathbb{Q}[x]$ with both a positive leading coefficient and an integer constant term. Define $+$ as polynomial addition, and successor as $+1$. The result is a nonstandard model for Presburger Arithmetic. (All sentences in the language $\mathcal{L}_+$ which are true in the standard model are also true in this structure.)

True Arithmetic Recall that $\mathcal{L}_A = [0, s, +, \cdot\ ; =]$ is the language of addition and multiplication, and $\underline{\mathbb{N}}$ is its standard model. Let **TA** (True Arithmetic) be the set of all $\mathcal{L}_A$-sentences which are true in the standard model. It follows from Gödel's incompleteness theorem (later in the course) that **TA** is undecidable, and does not have any decidable set of axioms. **TA** does have nonstandard models, but no "nice" nonstandard models. In fact, it has been shown that in any nonstandard model for **TA**, the interpretations of $+$ and $\cdot$ cannot be computable functions.

Theorem: (Application of compactness) **TA** has a nonstandard model.

Proof: Let c be any constant symbol (not in $\mathcal{L}_A$), and let Ψ be the infinite set of sentences

$$\Psi = \{c \neq 0, c \neq s0, c \neq ss0, ...\}$$

It is easy to see that every finite subset of $\mathbf{TA} \cup \Psi$ is satisfiable, since the standard model, with c interpreted as some large integer, will satisfy the finite set. Therefore, by the compactness theorem, $\mathbf{TA} \cup \Psi$ has a model $\mathcal{M}$. But this model cannot be isomorphic to the standard model, since the element which interprets c must satisfy all sentences in Ψ, and therefore cannot be a standard natural number. $\Box$

Exercise 14 *Although the language $\mathcal{L}_A = [0, s, +, \cdot\ ; =]$ does not include the order relation $\leq$, we can define $a \leq b$ as follows:*

$$a \leq b \leftrightarrow \exists x(a + x = b)$$

Under this definition, every model of **TA** *is a totally ordered set, since the properties of a total order (namely $\leq$ is reflexive, semi-antisymmetric, transitive, and any two elements are comparable) can all be expressed by first-order formulas in the vocabulary $\mathcal{L}_A$, and all must be true in the model. Prove that every countable nonstandard model of* **TA** *is order-isomorphic to*

$$\mathbb{N} \oplus \mathbb{Q} \times \mathbb{Z}$$

i.e. it begins with a copy of $\mathbb{N}$, and is followed by copies of $\mathbb{Z}$ which are densely ordered. (See the discussion following Exercise 13.)

Exercise 15 *Suppose that $\mathcal{L}$ is a language which includes an infinite list $c_1, c_2, \ldots$ of constant symbols. Let Γ be the set of sentences*

$$\Gamma = \{c_i \neq c_j \mid i, j \in \mathbb{N}, i < j\}$$

Let A be a sentence such that $\Gamma \models A$. Prove that A has a model with a finite universe.