Chapter 7

First Order Reasoning

To be is to be the value of a bound variable –W.V. Quine [69].

To be or not to be. That is not a question, but a tautology. –Hans Reichenbach[72]

7.1 First Order Semantics

First order languages have denumerable many individual variables 'x_1', 'x_2', 'x_3', ... the first three of which are customarily abbreviated as 'x', 'y', and 'z'. This allows for strings of quantifiers to occur in formulas, and for formulas with nested quantifications, or quantifications within quantifications.

In most cases of interest, first order languages are are not monadic and often have individual constants in their alphabets. It is also convenient to distinguish between individual *constants* and individual *parameters* and between *formulas* and *sentences*. A *parameter* of a first order language L in a language L' is a *constant* of L', where L' has the same alphabet as L except, perhaps for constants which L does not have. A *formula* of L (in L') is then a *sentence* of L', which is also a sentence of L provided that it contains no parameters. In constructing formulas, we never allow one quantifier within another quantification of the same variable. This eliminates certain trivial but annoying problems involving "collisions of quantifiers" or the "capture" of variables by quantifiers.

Each instance $X[\mu/u]$ (where μ is a constant or parameter) of the existential or universal quantification $\forall u\ X(u)$ or $\exists u\ X(u)$ is an immediate subformula of each of these quantifications. Hence subformula trees for first order formulas are not in general finitely generated.

A *truth value assignment* of a first order language L is much like a `TVA` (page 71) of a zero order language, in that the truth value of any sentence is determined by the truth values given to its atomic subformulas. The difference is that you need to add new constants to L, resulting in a new language L', in which any constants not in L are *parameters* of L. This assures that the denoting function

$d : C^{L'} \to \{0, 1\}$ is *onto*. A formula of a first order language L, in which the only constants are L-constants, is a *sentence* of L. Thus a *sentence* of L' is a *formula* of L, which is a *sentence* of L if it is parameter-free.

So given an elementary structure Σ, the truth value of truth functional compounds of formulas of L, and of quantifications of L-formulas arises in a natural way. In particular, the universal quantification $\forall u\ X(u)$ (where u is any variable) is true in Σ `iff` the L'-sentence $X[p/u]$ is true for every constant p of L', while the existential quantification $\exists u\ X(u)$ is true `iff` $X[p/u]$ is true for at least one constant p of L'.

Game trees for formulas are constructed in the usual way, but in general they are not finitely generated.

7.1.1 First Order Languages and Multiple Quantification: Sentences, Interpretations and Truth

We now turn to first order languages which have denumerably many individual variables,

$$x_1,\ x_2,\ x_3,\ \dots \tag{7.1}$$

and so also denumerably many quantifiers $\forall u$ and $\exists u$, two for each variable u. This allows nested quantifications, such as sentences like:

$$\forall x\Big(\exists y(Cy \wedge xDy) \Rightarrow \exists y(Fy \wedge xDy)\Big)\ , \tag{7.2}$$

which might symbolize 'all who draw circles draw figures'. It was recognized in the middle ages that this follows from 'all circles are figures', but this simple fact cannot be proved by Aristotelian syllogisms, or in uniform monadic first order logic, because neither system can deal with inferences involving relations.

If L' is a first order language, whose set of non- logical symbols includes that of the first order language L, then L' is an **extension** of L. If L' is also similar to L, so that L and L' have the same relation symbols, and all L-constants are L'-constants, then we say that L' is a **constant extension** of L. Any individual constants of L' which L lacks are called **parameters** of L (*in* L'), or simply *parameters*, if the context is clear or doesn't matter. We call a constant of L' an **individual symbol** of L (in L'). So an individual symbol of L is a constant or a parameter of L.

Let L' be a constant extension of L, and let R be one of their n-ary relation symbols. Then for any individual symbols $\mu_1, \dots, \mu_n$ of L, $R\mu_1, \dots, \mu_n$ is an **atomic formula** of L. If all of the individual symbols are individual constants of L, then $R\mu_1, \dots, \mu_n$ is an **atomic sentence** of L. Of course in either case, $R\mu_1, \dots, \mu_n$ is an *atomic sentence* of L'.

Let μ be an individual symbol, and $X(\mu)$ an arbitrary formula. If the variable u does *not* occur in $X(\mu)$, then we write $X(u)$ for the expression obtained from $X(\mu)$ by replacing *one or more* occurrences of μ in X by u. Thus $X(\mu)$ results from $X(u)$ by replacing *all* occurrences of u in $X(u)$ by μ, in other words by *substituting* μ for u in $X(u)$. So we sometimes write $X[\mu/u]$ instead of $X(\mu)$ to emphasize that we are indeed *substituting* μ for u in X.

Every atomic formula is therefore a formula, as is any truth functional combination of formulas. Moreover, $Qu\ X(u)$, where Q is a quantifier symbol and $X(\mu)$ is a formula in which u does not occur, is itself a formula, and the **scope** of the quantifier Qu in the formula $Qu\ X(u)$ is the entire formula. Every occurrence of u in $X(u)$ is **free**, while all occurrences of u in the formula $Qu\ X(u)$ are **bound**. A formula which contains no parameters is a **sentence**.

If $X(\mu)$ is a sentence, then $X(u)$ is a ***u*-formula** which is an **open sentence**, and if u is x_1, we call it a **1-formula**. More generally, if the individual variables $u_1, \ldots, u_n$ do not occur in the sentence $X(\mu_1, \ldots, \mu_n)$, then $X(u_1, \ldots, u_n)$, that is, $X[u_1/\mu_1, \ldots, \mu/u_n]$ is an *open sentence*, and if each $u_1, \ldots, u_n$ is 'x_1',…,'x_n', then $X(x_1, \ldots, x_n)$ is an **n-formula**.

The **universal closure** of $X(u)$ is symbolized: $\forall u\ X(u)$, while $\exists u\ X(u)$ is its **existential closure**. Extending, for $X(u_1, \ldots, u_n)$ we then have its,

Universal Closure	$\forall u_1, \ldots, \forall u_n\ X(u_1, \ldots, u_n)$,
Existential Closure	$\exists u_1, \ldots, \exists u_n\ X(u_1, \ldots, u_n)$.

If $1 \leq i \leq n$, all occurrences of the variables $u_1, \ldots, u_n$, are **free** in the open sentence $X(u_1, \ldots, u_n)$, and all occurrences of these variables except u_i are free while u_i is bound in $Qu_i\ X(u_1, \ldots, u_n)$.

To summarize: let u be any variable and μ any individual symbol. Then the following rules are **formation rules** for formulas of L:

1. Any atomic formula is a formula.

2. Any truth functional compound of formulas is a formula.

3. If $X(u)$ is a u-formula, then the universal and existential closures of $X(u)$ are formulas.

A formula of L which contains no parameters is a **sentence** of L.

Valuations in first order languages, as in zero order languages and first order monadic languages, are determined by their elementary structures, which provide interpretations for their sentences.

For instance, suppose L has one relation symbol 'R', which is a binary relation symbol, and two individual constants 'c' and 'd'. Suppose that $\mathbf{Q}$ is an elementary structure of L, the domain Q of which is the set `Rat` of rational numbers (which like $\frac{1}{2}$ or 2 but unlike π or $\sqrt{2}$ can be expressed as a fraction), and that in $\mathbf{Q}$, 'c' denotes 0 and 'd' denotes 1, and 'R' is to be interpreted as '$<$', so that its extension is $\{\langle x, y\rangle \in \mathtt{Rat} : x < y\}$.

Because every member of Q needs a name in $\mathbf{Q}$, while so far only 0 and 1 have names (which are 'c' and 'd'), we take a constant extension L' of $\mathbf{Q}$, the **language** of $\mathbf{Q}$, which has enough constants to provide a name for each member q of Q. The exact choice of a denoting function to provide for a name for every member of Q (and whether it allows more than one name for some members) is arbitrary as long as 'c' denotes 0 and 'd' denotes 1: it has no effect on the truth value in $\mathbf{Q}$ of ***L*-sentences**, but only on formulas which are not sentences.

Thus for most purposes, it will suffice to specify an elementary structure by providing its domain, and stating what the non-logical symbols are to stand for. In this case, we may write:

(i) $Q = \texttt{Rat}$,

(ii) $c = 0, \quad d = 1$,

(iii) xRy `iff` $x < y$.

Here (*iii*) is a defining condition for R which says that for each a and b in Q, $\mathbf{a}R\mathbf{b}$ is true `iff` $a < b$ (where $d(\mathbf{a}) = a$ and $d(\mathbf{b}) = b$, i.e. $\mathbf{a}$ is a name of a and $\mathbf{b}$ is a name of b). Statements (*ii*) and (*iii*) together determine a `TVA` $\sigma : Af \to \{0, 1\}$, which assigns a truth value to every atomic formula of L, which in turn yields a valuation which assigns a truth value to every formula of L. For (iii) determines the extension of $|R|$ of R in $\mathbf{Q}$, namely $\{\langle x, y\rangle \in \texttt{Rat} : x < y\}$, which in turn determines the truth value of (in $\mathbf{Q}$) of every atomic formula of L: for all rational numbers a and b, $\mathbf{a}R\mathbf{b}$ is true (in $\mathbf{Q}$) `iff` $\langle a, b\rangle \in |R|$.

For instance 'cRd' is true because $0 < 1$, as is the sentence '$\exists x(cRx \wedge xRd)$' because for some q in Q, '$cR\mathbf{q} \wedge \mathbf{q}Rd$' is true. In general, then, $\forall u\ X(u)$ is true in $\mathbf{Q}$ `iff` for all q in Q, $X(\mathbf{q})$ is true, and $\exists u\ X(u)$ is true `iff` for some q in Q, $X(\mathbf{q})$ is true. Note that truth may depend on the choice of domain. For instance, without altering (*ii*) or (*iii*), given another elementary structure $\mathbf{Q}'$ with $Q' = N$, so (*i*) becomes,

(i') $Q' = N$,

then '$\exists x(cRx \wedge xRd)$' would be false (in $\mathbf{Q}'$), for there is no natural number n between such that $0 < n < 1$.

PROBLEMS

1. (a) Is '$\exists x \forall y\ yRx$' true in $\mathbf{Q}$? Why or why not?
   (b) Is '$\forall x \exists y\ xRy$' true in $\mathbf{Q}'$? Explain.
   (c) Is '$\forall x \forall y\ \big(xRy \Rightarrow \exists z(xRz \wedge zRy)\big)$' true in $\mathbf{Q}$? Why or why not?
2. Show that no variable can occur both free and bound in any open sentence.

7.1.2 Elementary and Higher Order Structures*

In the previous section, we gave specific examples of the way in which an elementary structure $\mathbf{D}$ of a first order language L determines a valuation of L. We now give a general definition of a valuation of L determined by $\mathbf{D}$. Let

$$D^\star = D \cup D^2 \cup D^3 \cup \ldots = \bigcup_{i \in N^+} D^i \ . \tag{7.3}$$

Also let Ω be the set of relation symbols of L. Then an elementary structure $\mathbf{D}$ of L consists of:

*This part may be skipped without loss of continuity.

(i) A nonempty set D, which is the **domain** of **D**

(ii) A function $g : C^{:} \to D$, and a function $d : C^{L'} \to D$ which extends g, and maps D *onto* D, where L' is a constant extension of L. Any L'-constant c is a name of $d(c)$.

(iii) A function $e : \Omega \to \mathbf{P}(D^\star)$, which assigns an extension $e(R) = |R|$ to every n-ary relation R, where $|R| \subseteq D^n$.

Any right inverse $m : C^{L'} \to D$ of d gives a name $m(a)$ to each a in d, so that $dm(a) = a$. We will usually write **a** or m_a for $m(a)$. **D** also determines a unique `TVA` $\sigma : Af \to \{0, 1\}$ of L: for any n-ary relation symbol R and L'-constants $c_1, \ldots, c_n$,

$$\sigma(Rc_1, \ldots, c_n) = c_{|R|}(d(c_1), \ldots, d(c_n)) \ , \tag{7.4}$$

where $c_{|R|} : D^n \to \{0, 1\}$ is the characteristic function of $|R|$. Then σ has a unique extension which is a **Boolean valuation** and also a **first order valuation** of L in the sense that it obeys these conditions:

$$\tau\big(\forall u\ X(u)\big) \quad = \quad 1 \texttt{ iff } \tau\big(X(a)\big) = 1 \text{ , for all } a \text{ in } D \tag{7.5}$$

$$\tau\big(\exists u\ X(u)\big) \quad = \quad 1 \texttt{ iff } \tau\big(X(a)\big) = 1 \text{ , for some } a \text{ in } D \tag{7.6}$$

If $\tau(Y) = 1$ we also say that Y is **true** (in **D**). Thus,

$$\forall u\ X(u) \quad \text{is true } \texttt{iff} \quad \text{for each } a \text{ in } D,\ X(a) \text{ is true.} \tag{7.7}$$

$$\exists u\ X(u) \quad \text{is true } \texttt{iff} \quad \text{for some } a \text{ in } D,\ X(a) \text{ is true.} \tag{7.8}$$

In the other direction, each truth value assignment σ determines a unique extension for every n-ary relation symbol of:

$$L : |R| = \{\langle a_1, \ldots, a_n\rangle \in D^n : \sigma(R\mathbf{a_1}, \ldots, \mathbf{a_n}) = 1\} \ . \tag{7.9}$$

A "second order" language, by contrast has in addition "second order" variables which range over n-ary relations on the first order domain, a "third order" language has "third order variables" and so on. A "type theory of order omega" has variables of all positive integral order. Valuations of these higher order languages cannot be determined by elementary structures, but require higher order structures, with a separate domain for variables of each order to range over. We will discuss this further in Chapter 8.

EXAMPLE

Let $\mathbf{A} = \langle N^+, L', J, m\rangle$ be an elementary structure of the language L, which has no individual constants, and a single binary relation symbol R. The language L' of **A** is a constant extension of L, which has the individual constants ' a_1 ', ' a_2 ', ' a_3 ', ..., which denote the nonzero natural numbers $1, 2, 3, \ldots$ The denoting function d of this structure sends each constant a_n to the nonzero natural number n. Its inverse d^{-1} exists (since it's one-to-one), and sends each n to

a_n, which we may also write as $\mathbf{n}$, *the* name of n. If $\forall x\ F(x)$ is an L-formula, then it is true `iff` for every n in N^+, $F(\mathbf{n})$ is true, while $\exists x\ F(x)$ is true `iff` for some n in N^+, $F(\mathbf{n})$ is true. Then each of the following L-sentences is true in $\mathbf{A}$:

$$\forall x\ \ -xRx\ , \tag{7.10}$$

$$\forall x \forall y \forall z\ (xRy \wedge yRz \Rightarrow xRz)\ , \tag{7.11}$$

$$\forall x \exists y\ xRy\ . \tag{7.12}$$

For let $|R| = \{\langle x, y\rangle \in (N^+)^2 : x < y\}$. Then the first sentence is true, since no natural number is less than itself, and the second sentence is true since for all natural numbers k, m and n, the L-formula,

$$\mathbf{k} < \mathbf{m} \wedge \mathbf{m} < \mathbf{n} \Rightarrow \mathbf{k} < \mathbf{m} \tag{7.13}$$

is true. Finally, the third sentence is true, for there is no largest natural number.

PROBLEMS

1. (a) Show that ‘ $\exists x\ Fx \Rightarrow \forall x\ Fx$ ’ is true in all structures, the domain of which has a single element.
   (b) Show that this sentence is not true in all structures with a two-element domain.

7.1.3 Models of Sets of Sentences: Some Examples

The structure **I satisfies** a set Γ of sentences `iff` every sentence in Γ is true in $\mathbf{I}$, in which case it is a **model** of Γ. A model $\mathbf{H}$ of Γ with $H \subseteq I$, in which the extension in $\mathbf{H}$ of each relation symbol is a subset of its extension in $\mathbf{I}$ is a **submodel** of $\mathbf{I}$. We have $\Gamma \models X$ `iff` X is true in every model of Γ, that is, the set $\Gamma, -X$ has no model. We say that X and Y are **semantically equivalent** and we write $X \equiv Y$ `iff` both $X \models Y$ and $Y \models X$. The set of true L'-sentences is the **theory** $T_{\mathbf{I}}$ of $\mathbf{I}$.

A structure $\mathbf{D}$, the only nonlogical symbol of which is a binary relation symbol, say ‘R’, is an **ordering** (or **order**) on D. R is then the **ordering relation** of $\mathbf{D}$ and is a **relation on** D.

For instance, let the binary relation symbol ‘ E ’ be the only non-logical symbol of L. Then any model $\mathbf{P}$ of the following set,

`Pre`
$$\forall x\ xEx\ ,$$
$$\forall x \forall y \forall z\ (xEy \wedge yEz \Rightarrow xEz)\ ,$$

of sentences is a **pre-order** on P. The first formula (7.1.3) says that E is **reflexive** in P, while the second one (7.1.3) says that E is **transitive** in P. We say that E is **symmetric** in P `iff` the sentence,

$$\forall x \forall y\ (xEy \Rightarrow yEx)\ , \tag{7.14}$$

holds. The pre-order **P** is said to be an **equivalence relation** `iff` E is symmetric in P.

For example, defining mEn `iff` m and n are both even or both odd, i.e. $(m-n)$ is even, E is an equivalence relation on the set of integers.

We say E is **Euclidean** on P `iff` for all x, y and z in P,

$$xEy \wedge xEz \ \Rightarrow \ yEz \ , \tag{7.15}$$

holds. It is not difficult to show that E is reflexive and Euclidean on P `iff` **P** is an equivalence relation.

If **P** is an equivalence relation, then E divides A into **equivalence classes**, where a and b belong to the same equivalence class `iff` aEb is true in **P**. We also write $[a]_E$ for the class of all elements b of A such that bEa, i.e. bEa holds.

Any two distinct equivalence classes are disjoint. For if c belongs to two equivalence classes, say $[a]_E$ and $[b]_E$, then both cEb and cEa, and so by the Euclidean property, bEa. So suppose that x is an arbitrary element of $[a]_E$. Then xEa, and since also bEa, we have by symmetry aEb. Then by transitivity, xEb, so that $x \in [b]_E$. Thus $[a]_E \subseteq [b]_E$. By a similar argument, $[b]_E \subseteq [a]_E$ and so by extensionality, $[a]_E = [b]_E$.

For example, if E is an equivalence relation on the set of integers, where as above mEn `iff` $(m-n)$ is even, then E divides the set of integers into two equivalence classes: the set of even integers and the set of odd integers.

On the other hand, any model **M** of the following set,

`Sp`
$$\forall x \ -(xPx) \ ,$$
$$\forall x \forall y \forall z \ (xPy \wedge yPz \Rightarrow xPz) \ ,$$

of sentences is a **strict partial order**. The first sentence says that the extension P of 'P'in **M** is **irreflexive** in M. We sometimes write $<$ instead of P for the relation symbol of a strict partial order.

The set Q of rational numbers, and the set Z of integers are both strict partial orders with respect to the relation P when mPn `iff` $m<n$ for all m and n in Q or Z as the case may be (where $m<n$ `iff` m is less than n in the usual arithmetical sense). That is, Q and Z are the underlying sets of the strict partial orders **Q** and **Z** respectively, which in turn are models of `Sp`. Moreover, **Z** is a submodel of **Q**.

Or let **A** be a strict partial order on $A = \{1,2,3,6\}$, with the graph,

$$\{\langle 1,2\rangle, \langle 1,3\rangle, \langle 2,6\rangle, \langle 3,6\rangle, \langle 1,6\rangle\} \ , \tag{7.16}$$

which we may display geometrically by the *directed graph* diagram of figure 7.1. Note that for all x and y in A, xPy, i.e. $x \to y$ `iff` x is a proper divisor of y.

Now if $X(u)$ and $X(w)$ are respectively $u-$ and $w-$formulas (where $X(w)$ is $X(u)[w/u]$, the result of substituting w for u in $X(u)$), then $Qu\ X(u)$ is semantically equivalent to $Qw\ X(w)$.

Moreover, if a formula starts with a string of universal or existential quantifiers, the scopes of which extend to the end, the order in which they occur is

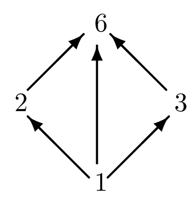


Figure 7.1: Directed Graph of Strict Partial Order on $A = \{1, 2, 3, 6\}$

immaterial. For example,

$$\forall x \forall y(xPy \Rightarrow -yPx) \equiv \forall y \forall x(xPy \Rightarrow -yPx) \ . \qquad (7.17)$$

On the other hand, the order of the initial quantifiers does matter if some are universal and others existential. It would be a fallacy, for example, to conclude from the assumption that everything has a cause, that something causes everything, or to infer from the proposition that every set belongs to some set, that there is a set to which every set belongs.

For an arithmetical example, let mPn hold for all integers m and n `iff` $m > n$, ' $\forall x \exists y\ xPy$ ' is true in the domain of integers, for example, because there is no least integer, while ' $\exists y \forall x\ xPy$ ' is certainly false, since there is no integer less than every integer (including itself). Or take any domain with more than one element. Then ' $\forall x \exists y(x = y)$ ' is true, while ' $\exists y \forall x(x = y)$ ' is false.

There is also a time-worn ordinary language example. Suppose the domain is the set of people in some community, and for any two people x and y, let ' xRy ' hold `iff` x loves y. Then everybody loves somebody if it happens to be a community of narcissists, while 'somebody is loved by everybody' need not be true, if that community has more than one person.

In general, however, ordinary language examples such as the one above don't work very well as counter-examples to invalid arguments. You can always have anything you like in your domain. If you have only natural numbers in it, the properties you need are clear and precise, though unexciting.

PROBLEMS

1. Let Z be the set of integers, and for any integers m and n, let mEn hold `iff` $(m-n)$ is even. What are the equivalence classes into which E divides Z?

2. Show that every reflexive, symmetric and transitive relation E is Euclidean.

3. Show that the ordering relation P of any strict partial order is **asymmetric** in the sense that the sentence ' $\forall x\, \forall y\ (xPy \Rightarrow -yPx)$ ' holds in any strict partial order.

4. Show that any transitive asymmetric relation P is irreflexive.

5. Which (if any) of the structures $\mathbf{Q}$ and $\mathbf{Q}'$ discussed in section 7.1.1 (page 154) are strict partial orders? Explain.

7.1.4 First Order Games*

First order games are played in the same way as the Boolean games of section **??** (page **??**), except that the game trees and the corresponding valuation trees are not always finitely generated, because not all first order subformula trees are finitely generated. (As our examples involve statements about numbers, we write ‘ $\bot$ ’ for the Boolean constant ‘0’ and ‘ $\top$ ’ for the Boolean constant ‘1’).

In addition to the Boolean rules of play, we add two first order rules:

$R\forall$ If the coin is on $\forall$, Nature chooses which point to move it to one step down.

$R\exists$ If the coin is on $\exists$, you choose which point to move it to one step down.

As in Boolean logic, the presence or absence of a winning strategy depends on whether the sentence which produced the game tree and the corresponding valuation tree is true or false in the truth value assignment provided. Any structure of a given first order language which contains the sentence in question determines such a truth value assignment.

By way of illustration, take a first order language L, the alphabet of which consists of ‘F’ and ‘G’ alone. These two non-logical symbols are to denote the “less than” and the “less than or equal to” relations between positive integers. Language L has no constants.

We consider a structure of L in an extension L' of L, the domain of which is the set of positive integers. Then L' itself has denumerably many constants: ‘a_1’, ‘a_2’, ‘a_3’,... which are to denote 1, 2, 3, ...

In this structure, ‘ $\forall x \exists y\ xFy$ ’ is true, while ‘ $\exists y \forall x\ xGy$ ’ is false. The game tree for ‘ $\forall x \exists y\ xFy$ ’ is displayed in Figure 7.2 and the corresponding valuation tree in Figure 7.3. You have a winning strategy for this game, because while at the start of the game it’s Nature’s move, every point to which Nature chooses to move is an ‘ $\exists$ ’ which is safe: it’s your move, and there is always a ‘ $\top$ ’ below you to which you can move and win.

In contrast, let us consider the game tree for ‘ $\exists y \forall x\ xGy$ ’ and the corresponding valuation (Figures 7.4 and 7.5 respectively). Here the tables are turned. Although you have the first move, you have no winning strategy. No matter which move you make, every point to which you choose to move is an ‘ $\forall$ ’ which is unsafe: it’s Nature’s move, and there is always a ‘ $\bot$ ’ below her to which she can move and win (so you lose).

*This part may be skipped without loss of continuity.

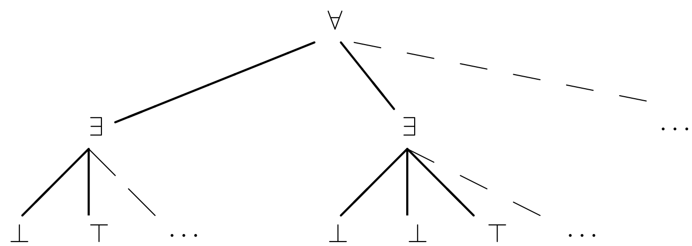


Figure 7.2: Game Tree for ‘ $\forall x \exists y\ xFy$ ’

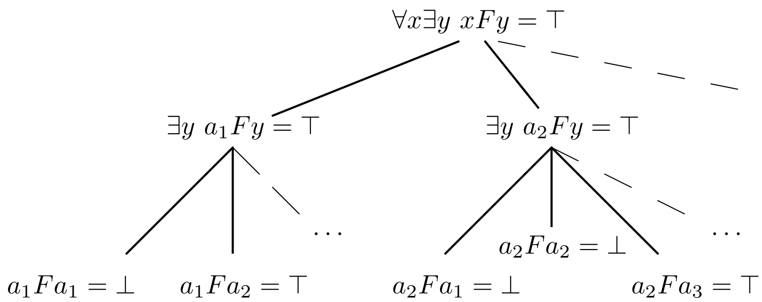


Figure 7.3: Valuation Tree for ‘ $\forall x \exists y\ xFy$ ’

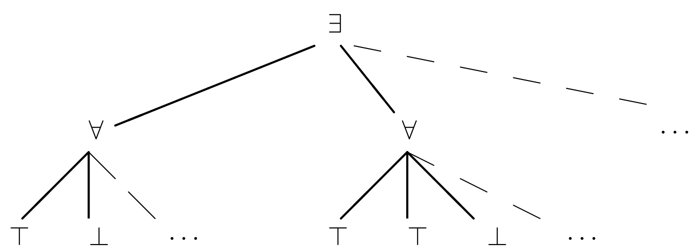


Figure 7.4: Game Tree for ‘ $\exists y \forall x\ xGy$ ’

7.2 Methods of First Order Logic I: Truth Trees

All the Boolean rules for constructing truth trees continue to hold for first order truth trees. There are two additional rules for universal and existential quantifications, and two others for their negations.

A universal quantification $\forall u\ X(u)$ or the negation $-\exists u\ X(u)$ is *fulfilled* if for any constant or parameter μ in its path, $X(\mu)$ or $-X(\mu)$ is also in the path, as the case may be. To fulfill an existential quantification $\exists u X(u)$ or a negated universal quantification $-\forall X(u)$, an instance $X(p)$ or $-X(p)$ (as the case may

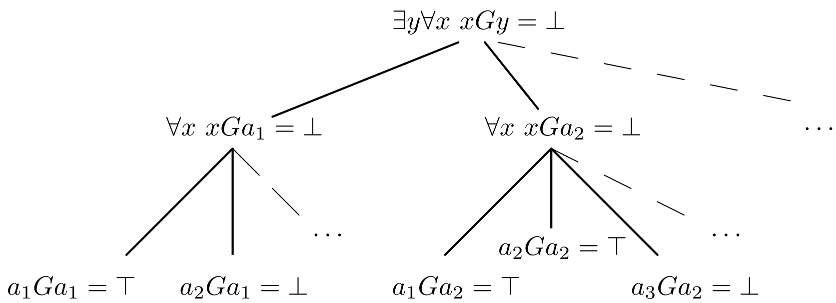


Figure 7.5: Valuation Tree for ‘ $\exists y \forall x\ xGy$ ’

be) must be added to the path, where p is a parameter not previously in the path. Since p is new, if the path subsequently closes, this cannot be due to the particular choice of p.

An open path is *completed* when every formula in the path which is not an atomic formula or its negation, is fulfilled. Any truth value assignment which makes true any atomic formula in a completed open path and makes false any atomic formula whose negation is in the path then satisfies the entire path.

7.2.1 First Order Truth Trees

In constructing first order truth trees, we retain all the rules for connectives, and add one for the existential and one for the negated universal quantifier, and one rule for the universal and one rule for the negated existential quantifier. Each application of these rules is subject to certain restrictions, which we now explain.

Let's first explain the rules which apply to formulas of the form $\exists u\ X(u)$ and $-\forall u\ X(u)$, which behave similarly, since $\exists u\ X(u)$ is true ($-\forall u\ X(u)$ is true) in a valuation if for at least one individual parameter p, $X(p)$ is also true ($-X(p)$ is also true).

In fact, the formulas $-\forall u\ X(u)$ and $\exists u\ -X(u)$ are semantically equivalent, for in any given structure $\mathbf{D}$, not every a in the domain D has (the property expressed by) X, `iff` at least one a in D does not have X, so that,

$$-\forall u\ X(u) \equiv \exists u\ -X(u)\ . \tag{7.18}$$

It is also evident if there is no a in D that has X `iff` no a in D has X, that is,

$$-\exists u\ X(u) \equiv \forall u\ -X(u)\ . \tag{7.19}$$

Indeed, if at least one a in D has X, then not all a in D lack X.

On negating both sides of (7.18) and substituting $-X(u)$ for $X(u)$, we also find,

$$\forall u\ X(u) \equiv -\exists u\ X(u)\ , \tag{7.20}$$

and dually,

$$\exists u\ X(u) \equiv -\forall u\ X(u)\ , \tag{7.21}$$

so that universal and existential quantification are interdefinable, just as conjunction and disjunction are, and (7.18) and (7.19) are first order analogs of DeMorgan's laws.

In the interest of brevity and clarity, therefore, we extend Smullyan's unified notation introduced in Chapter 4, to include quantifications and their negations. We will write δ for any formula $\exists u\ X(u)$ or $-\forall u\ X(u)$ and $\delta(p)$ for any instance or **component** of δ, respectively $X(p)$ or $-X(p)$, where p is any parameter.

The formulas $\forall u\ X(u)$ and $-\exists u\ X(u)$ also behave similarly, and we write γ for any formula $\forall u\ X(u)$ or $-\exists u\ X(u)$, and $\gamma(\mu)$ for any instance or **component** $X(\mu)$ or $-X(\mu)$ of γ, where μ is an individual symbol.

The rules for constructing first order truth trees are then the same as those for constructing Boolean and zero order truth trees together with two new rules, one of which applies to δ formulas and the other to γ formulas.

We first consider the δ-rule. If δ occurs in an open path, we may add $\delta(p)$ to the end of every open path in which δ occurs, thereby fulfilling the formula, and we may star it. But on *one* condition: the individual *parameter* p does *not* occur in the tree before $\delta(p)$ was added to the path.

Why not? Because a structure $\mathbf{D}$ of L satisfies δ `iff` for at least one element a of the domain of $\mathbf{D}$, such that the individual symbol μ denotes a, $\delta(\mu)$ is true in . For example, suppose that the domain of $\mathbf{D}$ is the set of natural numbers and let the formula 'En' be true in $\mathbf{D}$ `iff` n is an even number. Then $\exists x\ Ex$ is true, because at least one number is even, for example 2 is even, making $E\mathbf{2}$ true (where $\mathbf{2}$ denotes 2), although some numbers are not even, for example 3, so that $E\mathbf{3}$ is false.

So it's quite possible that one structure satisfies an open path which contains a formula $\delta(p)$ as well as δ, because for one individual parameter p, $\delta(p)$ is true, while for another individual parameter q, $\delta(q)$ is false. If, then, we were to add $X(p)$ $(-X(p))$ to a path containing $\exists u\ X$ $(-\forall u\ X)$ which already contains $-X(p)$ $(X(p))$, we would have closed a path we shouldn't have closed.

On the other hand, if p is an individual parameter new to the tree, and we add $\delta(p)$ to every open path which contains δ, if any of these paths later close, it would have closed no matter what individual parameter we had used in place of p, since the path's closing at some stage after adding $\delta(p)$ cannot have depended on our choice of individual parameter, since p was new to the tree when we added $\delta(p)$ to it. So any formula δ is fulfilled by adding $\delta(p)$ to every open path which contains δ, provided that p does not occur (in any formula in) the tree before δ was fulfilled.

But by the γ-rule, we may add $\gamma(\mu)$ to the end of any open path in which γ occurs without any restriction. For that very reason, we do not consider γ fulfilled, and do not star it. Instead, we call an open path π **completed** `iff` all α, β and δ formulas in π have been fulfilled, *and* for every individual symbol μ and every formula γ in π, $\gamma(\mu)$ is also in π. And as in Boolean logic, any closed path is also completed, and a tree is **completed** `iff` all paths through it are completed.

We summarize our above discussion of the first order tree rules by the following diagram, in which The formula(s) below the three dots are to be added to the end of every *open* path, in which the premise occurs, but subject to the proviso that p is a new parameter.

$$\begin{array}{lll} \gamma & \delta & \star \\ . & . & \\ . & . & \\ . & . & \\ \gamma(\mu) & \delta(p) & \text{If } p \text{ is a new parameter,} \end{array}$$

that is, the parameter p does not occur in any formula in the path above $\delta(p)$. Let's illustrate how to use these rules to construct first order truth trees to check for validity. Here, for example, is a truth tree to prove the validity of the inference of $\exists x\ Fx$ from $\forall x\ Fx$:

$$\begin{array}{rl} \forall x & Fx \\ -\exists x & Fx \\ & Fa \\ & -Fa \\ & \perp \end{array}$$

Next we show that the formula,

$$\forall x(Px \Rightarrow Qx) \Rightarrow \Big(\forall x(Qx \Rightarrow -Rx) \Rightarrow \forall x(Px \Rightarrow -Rx)\Big)\ , \tag{7.22}$$

is **universally valid**–true in every first order valuation. Universal validity is the first order generalization of tautologousness. We must construct a closed tree from the negation of the above formula, displayed in Figure (7.6).

In Figure (7.6) we adopted a time-saving procedure, not required by the tree rules, of always applying the appropriate rule to all formulas of the form δ as soon as possible. If, for example, we had added $Pb \Rightarrow Qb$ to the path before fulfilling $-\forall x(Px \Rightarrow -Rx)$, and adding $-(Pa \Rightarrow -Ra)$ to the path, where 'a' is a *new* parameter, we'd have to turn around and add $Pa \Rightarrow Qa$, because the introduction of $-Pa$ on the left will close the path, while the introduction of $-Pb$ would not.

Another example: let's construct a truth tree proof that $\exists y\forall x\ xRy \vdash \forall x\exists y\ xRy$:

$$\begin{array}{rll} \exists y\forall x & xRy & \star \\ -\forall xy\exists x & xRy & \star \\ -\exists y & aLy & \\ \forall x & xRb & \\ & aRb & \\ & -(aRb) & \\ & \perp & \end{array}$$

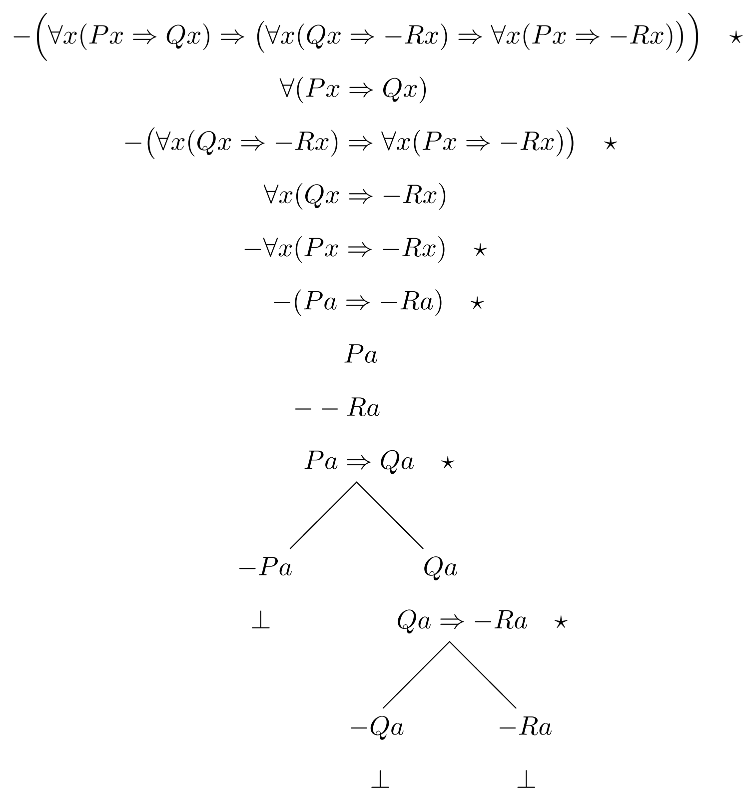


Figure 7.6: Closed tree constructed from sentence
$-(\forall x(Px \Rightarrow Qx) \Rightarrow (\forall x(Qx \Rightarrow -Rx) \Rightarrow \forall x(Px \Rightarrow -Rx)))$

The entailment doesn't hold in the reverse direction, because the set $\forall x \exists y\ xRy$, $-\exists y \forall x = xRy$ is satisfiable, for example in any domain with more than one element in which for any members a and b, aRb is to be true `iff` $a = b$. But every *completed* tree constructed from this set is infinite. In fact, every completed tree constructed from the first mentioned formula in this set is infinite.

Let's show this by starting a tree from the formula $\forall x \exists y\ xRy$, which is satisfiable in the domain having a single element–just take xRy to hold `iff` $x = y$. The initial formula of this tree is of course the formula itself:

$$\forall x \exists y\ xRy \tag{7.23}$$

The tree is not completed, because this formula is not a literal, so the γ-rule applies. No individual symbol occurs in the path, which in this case consists of ' $\forall x \exists y\ xRy$ ' alone. So choose any parameter, say a_1 and apply the γ-rule, adding ' $\exists y\ a_1 Ry$ ',

$$\text{STEP 1: } \left\{ \begin{array}{ll} \forall x \exists y & xRy \\ \exists y & a_1 Ry \end{array} \right. \tag{7.24}$$

and the tree is still not completed, because the bottom formula is not a literal. So we apply the δ-rule to the last formula:

$$\text{STEP 2:} \begin{cases} \forall x \exists y & xRy \\ \exists y & a_1Ry \;\star \\ & a_1Ra_2 \end{cases} \tag{7.25}$$

Of course, '$\forall x \exists y\ xRy$' is still not fulfilled, because the instance '$\exists y\ ya_2$' is not in the path. So we add it:

$$\text{STEP 3:} \begin{cases} \forall x \exists y & xRy \\ \exists y & a_1Ry \;\star \\ & a_1Ra_2 \\ \exists y & a_2Ry \;\star \end{cases} \tag{7.26}$$

It is now clear that the tree is not completed at STEP 1, STEP 2, STEP 3, STEP 4,. . . ,STEP n,. . . but if for every n, STEP n is executed–all of these steps are executed, we have an open path which is infinite.

It is also completed, because every non-literal in the path is fulfilled. Thus '$\forall x \exists y\ xRy$' is fulfilled, because for every parameter a_n $(n = 1, 2, \ldots)$, the instance $\exists y\ a_nRy$ of '$\forall x \exists y\ xRy$' is in the path, so that '$\forall x \exists y\ xRy$' is now fulfilled, and each of these instances has also been fulfilled. Yet at no *step* in the construction of the tree has the top formula been fulfilled.

So while every tree constructed from a finite set of Boolean formula can be completed in a finite number of steps, $\forall x \exists y\ xRy$ is a first order sentence from which no finite completed tree can be constructed, yet it has a model with a one-element domain.

But there are also finite sets of first order sentences which cannot be satisfied in *any* finite domain, but can be satisfied in an infinite domain, so that all trees constructed from any such set *must* have an infinite path[1].

Every open path π in a completed tree constructed from a set Γ of formulas of a language L determines models $\mathbf{M}$ of Γ, in a constant extension L' of L, the constants of which are the individual symbols of L which occur in π. M may be any set for which a surjection $d : C^{L'} \to M$ exists, that is, M has no more members than the set $C^{L'}$ of constants of L'. Thus M can be $C^{L'}$, with each L'-constant denoting itself. Now let σ assign 1 to every L'-atomic formula in π, and 0 to every L'-atomic formula whose negation is in π. If F is an L'-atomic formula such that neither F nor $-F$ is in π, then σ may arbitrarily assign either 0 or 1 to π. Then σ is a truth value assignment of L', which determines the extensions of its relation symbols in the usual way.

[1]One such set consists of the sentences $\forall x \exists y\ xRy$, $\forall x\ -xRx$, and $\forall x \forall y \forall z (xRy \wedge yRz \Rightarrow xRz)$, any model of which is a strict partial order. It cannot have any finite models. For a *path* in such a model is a finite sequence of elements $a_1, \ldots, a_k$ such that $a_1Ra_2, a_2Ra_3, \ldots, a_{k-1}Ra_k$. No two elements a_i and a_j (where $i < j$) are equal, for if $a_iRa_{i+1}, \ldots, a_{j-1}Ra_j$, then by transitivity a_iRa_j, and so a_ia_i, which violates irreflexivity. But then since the path is finite, it must have an end, so that $\forall x \exists y\ xRy$ is not true. One infinite model is the set of natural numbers, in which $\mathbf{m}R\mathbf{n}$ is true `iff` $m < n$.

Every element of M is named in $\mathbf{M}$ by at least one individual symbol of L. A sentence γ of L' is true in M `iff` for every constant $\mathbf{c}$ of L', $\gamma(\mathbf{c})$ is true. Equivalently, γ is true `iff` for all c in M, $\gamma(\mathbf{c})$ is true (where $\mathbf{c}$ denotes c). Thus in $\mathbf{M}$, every sentence γ in π is true, along with all its first order descendants $\gamma(\mathbf{c})$. Dually, δ is true `iff` for some c in M, $\delta(\mathbf{c})$ is true.

The denoting function of $\mathbf{M}$ is not necessarily injective: distinct constants of L' need not denote distinct members of M. Thus consider the infinite tree constructed from the L-formula $\forall x \exists y\ xRy$, where L has the binary relation symbol R but no individual constants constants:

$$\begin{array}{rll} \forall x \exists y & xRy & \\ \exists y & a_1 Ry & \star \\ & a_1 Ry & \\ \exists y & a_2 Ry & \star \\ & \vdots & \end{array}$$

If $M = \{0\}$, then $|R|$ must be $\{0\}$, and every L-parameter whether $a_1, a_2, \ldots$ and so on must denote 0, the single member of M. On the other hand, if $M = N^+$ (where as usual N^+ is the set of positive integers), then we might let $a_1 = 1, a_2 = 2, \ldots$ and so on. In the first case $\mathbf{M}$ has a one-element domain, and so is finite, while in the second case $\mathbf{M}$ has a denumerable domain.

PROBLEMS

1. (a) Find an infinite model for the set

$$\forall x\ xEx$$
$$\forall x \forall y \forall z\ (xEy \wedge xEz \Rightarrow xEz)$$

   (b) Find a finite model for the above set.

   (c) Let E be defined as in (a). It divides the set Z of integers into two equivalence classes,

$$\begin{array}{rcl} V & = & \{\ldots, -4, -2, 0, 2, 4, \ldots\}\ , \\ D & = & \{\ldots, -3, -1, 1, 3, \ldots\}\ , \end{array}$$

   the set of even and odd numbers respectively. Find an infinite model of the set of sentences given in (a), and also a model, the domain of which is $\{0, 1\}$.

2. Call an ordering relation R **serial** `iff` '$\forall x \exists y\ xRy$' holds. Show that no ordering relation of a finite strict partial order can be serial, but that there are infinite strict partial orders which are serial.

3. Use truth trees to verify the following assertions:

$$\begin{array}{rcl}
\forall x(\exists y\ Fx,y \Rightarrow Gx) & \models & \forall x \forall y(Fx,y \Rightarrow Gx) \\
\forall x \forall y(Gx \Rightarrow Fx,y) & \models & \forall x(\exists y\ Fx,y \Rightarrow Gx) \\
\forall x \forall y(Gx \Rightarrow Fx,y) & \models & \forall x(Gx \Rightarrow \forall y\ Fx,y) \\
\forall x \exists y(Gx \Rightarrow Fx,y) & \models & \forall x(Gx \Rightarrow \exists y\ Fx,y)
\end{array}$$

4. Show that every uniform monadic first order logic is **decidable**, in the sense that one can determine by a mechanical procedure whether any given sentence of the language is universally valid. (Hint: note that any truth tree constructed from a uniform monadic sentence can be completed in a finite number of steps).

5. Show that every monadic first order logic is decidable. (Hint: note that $QxQy(Fx \star Gy) \equiv Qx\ Fx \star Qy\ Gy$, where Q is a quantifier symbol and $\star$ is a binary connective).

7.3 Methods of First Order Logic II: Natural Deduction

In addition to the Boolean rules, first order natural deduction systems have two rules for universal and two rules for existential quantifications. **Universal instantiation** (`UI`) allows you to infer any instance $X(\mu)$ (where μ is a constant or parameter) of the universal quantification $\forall u\ X(u)$, while **existential generalization** (`EG`) allows you to infer the existential quantification $\exists u\ X(u)$ from any instance of it.

While you can't infer a general from a particular, you can infer a universal quantification from a given set Γ of assumptions, provided that every instance of it is derivable from Γ. And this condition is met if you can infer an instance $X[p/u]$ of $u\ X(u)$ from Γ, where p is a parameter which does not occur in Γ. The rule **universal generalization** (`UG`) permits the inference of $u\ X(u)$ from $X[p/u]$, provided that $X[p/u]$ is unenclosed and p is a parameter which does not occur in any undischarged assumption. `UG` is therefore not truth preserving. None the less, if $\Gamma \models X(p)$ (where p does not occur in Γ), then $\Gamma \models \forall u\ X(u)$.

Similarly, you cannot infer any particular instance of an existential quantification $\exists u\ X(u)$ from $\exists u\ X(u)$ itself, since it may well be false while $\exists u\ X(u)$ is true. But if $\exists u\ X(u)$ is true, *some* instance must be true. So if you add as a hypothesis the instance $X[p/u]$, where p is a parameter which has not previously occurred in the proof, and you subsequently deduce a formula Y in which p does not occur, then you may infer Y from $\exists u\ X(u)$ and Y by `EI` (so `EI`: *existential instantiation*, is trivially truth preserving) *and* discharge the hypothesis $X[p/u]$, since the validity of the derivation of Y cannot have depended on the choice of p : if $\Gamma, X[p/u] \models Y$ (where p does not occur in Γ or in Y), then $\Gamma \models Y$.

7.3.1 Natural Deduction in First Order Logic: Formal Proofs

In a first order natural deduction system, we retain all the Boolean rules, which govern connectives, and add two rules for the universal and two for the existential quantifier.

The first rule is **universal instantiation** or `UI`. It lets you infer an **instance** $X(\mu)$ of a **generality** or universal quantification $\forall u\ X(u)$ from the generality itself. `UI` is truth preserving for $\forall u\ X(u) \models X(\mu)$.

Caution: `UI` does *not* allow you to infer ‘ $-Fa$ ’ from ‘ $-\forall x\ Fx$ ’, because ‘ $-\forall x\ Fx$ ’ is not a generality but the negation of one. Nor can you infer ‘ $(Fs \Rightarrow Gs) \Rightarrow (Hs \Rightarrow Is)$ ’ from ‘ $\forall x(Fx \Rightarrow Gx) \Rightarrow \forall x(Hx \Rightarrow Ix)$ ’ by `UI`, because the latter formula is not a generality either, but a conditional whose antecedent and consequent are both generalities.

The second rule, a rather weak form of generalization is called (in analogy to universal generalization which we discuss next), **existential generalization** or `EG`: it allows you to infer a from a particular *instance* $X(\mu)$ of $\exists u\ X(u)$ (which does *not* contain u), the formula $\exists u\ X(u)$ itself (which *may* contain μ). Like `UI`, `EG` is truth preserving: $X(\mu) \models \exists u\ X(u)$.

We display these two proper first order rules thus,

`UI`	`EG`
$\forall u\ X(u)$	$X(\mu)$
$\vdots$	$\vdots$
$X(\mu)$	$\exists u\ X(u)$

In uniform first order logic, μ would always be an individual parameter, because uniform languages don't have constants. Thus `UI` and `EG` are always used in an auxiliary way in a proof of a uniform sentence from uniform sentences: the consequence of an application of `UI` can never be the conclusion of such a proof, nor can the premise of an application of `EG` be an assumption. Indeed, it is quite common, when deducing a first order sentence from a set of sentences, whether uniform or not, for some steps in the proof to be formulas which are not sentences. The following three-step proof of ‘ $\exists x\ Fx$ ’ from ‘ $\forall x\ Fx$ ’ may serve as an example:

			REM
——	1	$\forall x\ Fx$	
	2	Fa	1, `UI`
	3	$\exists x\ Fx$	2, `EG`

While `UI` allows the inference from a generalization a particular instance of it, **universal generalization**, or `UG`, goes in the opposite direction. As is well known, you can't infer a generalization from any particular instance of it. But if you can deduce a "generic" instance of a generalization from a set Γ of assumptions–that is, an instance $X(p)$ of the formula $\forall u\ X[u/p]$ (so u does *not* occur in $X(p)$), such that the parameter p does not occur in Γ (and by construction *not* in $\forall u\ X[u/p]$ either), then you may infer $\forall u\ X[u/p]$.

By calling $X(p)$ a "generic" instance of $\forall u\ X[u/p]$, we mean that there is nothing special about it: the deduction of $X(p)$ from Γ could not have depended on the choice of p, since p did not occur in Γ. So we could have used any other individual symbol μ instead, and just as well have deduced $X[\mu/p]$ from Γ. So if $\mathbf{M}$ is a model of Γ, then:

(1) `If` p `does not occur in` Γ `and each instance` $X[\mu/p]$ `of` $\forall u\ X[u/p]$ `is true in` $\mathbf{M}$`, then so is` $\forall u\ X[u/p]$.

`UG`

.

.

.

$X(p)$

$\forall u\ X[u/p]$

The step to the last line is legitimate provided that the parameter p does not occur in any *undischarged* assumption. `UG` is not truth preserving, since $X(p) \not\models \forall u\ X[u/p]$, but by (1) above, If $\Gamma \models X(p)$, then $\Gamma \models \forall u\ X(u)$.

As an example of the use of `UG`, we prove a fundamental derived rule, which we call $-\mathbf{E}$ and says that $\forall u\ -X(u)$ is derivable from $-\exists u\ X(u)$, where $X(u)$ is a 1-formula. One instance of $-\mathbf{E}$ allows you to derive ' $\forall x\ -Fx$ ' from ' $-\exists x\ Fx$ '; you can't get any simpler than that. A convenient auxiliary rule, which we'll call $-\mathbf{E}(\mu)$ is that $-\exists u\ X(u) \vdash -X(\mu)$, a proof of which is the first five lines of the proof below. $X(u)$ is any open formula $X[u/p]$ (where u does not occur in the formula X), to assure that p does not occur in $X[u/p]$ so that the application of `UG` to $-X(p)$ at line 5 is legitimate. On the right, we provide a parallel proof using specific formulas:

			REM
—	1	$-\exists u\ X[u/p]$	
┌	2	$X(p)$	
│	3	$\exists u\ X[u/p]$	2, `EG`
└	4	$\bot$	1,3 `PC`
	5	$-X(p)$	4, `IPC`
	6	$\forall u\ -X[u/p]$	5, `UG`

			REM
—	1	$-\exists x\ Fx$	
┌	2	Fa	
│	3	$\exists x\ Fx$	2, `EG`
└	4	$\bot$	1,3 `PC`
	5	$-Fa$	4, `IPC`
	6	$\forall x\ -Fx$	5, `UG`

We may use $-\mathbf{E}(\mu)$ to prove the dual of $-\mathbf{E}$, which enables us to derive $\exists u\ -X(u)$ from $-\forall u\ X(u)$. We call it $-\mathbf{U}$, and continue to give on the right a proof of a specific case of the derived rule proved on the left:

		REM
1	$-\forall u\ X[u/p]$	
2	$-\exists u\ -X[u/p]$	
3	$--X(p)$	2, $-\mathbf{E}(\mu)$
4	$X(p)$	3, `BDN`
5	$\forall u\ X[u/p]$	4, `UG`
6	$\bot$	1,5 `PC`
7	$\exists u\ -X[u/p]$	6, `BPC`

		REM
1	$-\forall x\ Fx$	
2	$-\exists x\ -Fx$	
3	$--Fa$	2, $-\mathbf{E}(\mu)$
4	Fa	3, `BDN`
5	$\forall x\ Fx$	4, `UG`
6	$\bot$	1,5 `PCD`
7	$\exists x\ -Fx$	6, `BPC`

Then we have **Existential Instantiation** or `EI`. Although we can't derive any instance $X(p)$ of a formula $\exists u\ X[u/p]$, we know that if $\exists X[u/p]$ is true, then *some* instance of it is true. For instance, from $\exists x(Px \wedge Ix)$, (say some presidents are intellectual), $Pw \wedge IW$ (i.e. in particular, w is an intellectual president) does not follow.

So we argue as follows: let's suppose that the instance $X(p)$ of $\exists u\ X[u/p]$ holds, where u occurs in $X[u/p]$, so that p occurs in $X(p)$ because $X(p)$ is the result of substituting p for u in $X[u/p]$.

And let's further suppose that the parameter p does not occur in any formula in the proof above X, and that when we *assume* X, by introducing it as a new assumption or hypothesis, we are able to deduce a conclusion Y which also does not contain p. Then we conclude that Y follows, since the fact that we were able to derive it could not have been due to our choice of p in the instance $X(p)$ of $\exists u\ X[u/p]$ we chose to assume as our hypothesis, since p was new to the proof and does not occur in Y. Therefore we could have deduced Y no matter what instance of $\exists u\ X[u/p]$ we assumed, and so Y follows from the original assumptions, and we may discharge $X(p)$:

`EI`

$\exists u \; X[u/p]$

.

.

.

$X(p)$

.

.

.

Y

Y

where the parameter p does not occur in Y or in any undischarged assumption, (nor, by construction, can it occur in $\exists u \; X[u/p])^2$.

Failure to observe this proviso may result in fallacy, as in the following derivation:

		REM
1	$\exists x(Px \wedge Ix)$	
2	$Pw \wedge Iw$	
3	$Fa \wedge Ga$	2, `EI` (fallaciously)

Now let's give an example of a deduction which is not fallacious–all the rules are correctly applied. We give a proof of $\exists x(Fx \wedge Hx)$ from $\exists x(Fx \wedge Gx)$, $\forall x(Gx \Rightarrow Hx)$:

[2] That is, p does not occur in Y or in any assumption undischarged at the line at which `EI` is applied, which is the first line at which Y occurs in the above diagram.

		REM
1	$\exists x(Fx \wedge Gx)$	
2	$\forall x(Gx \Rightarrow Hx)$	
3	$Fa \wedge Ga$	
4	Fa	3, `SIMP`
5	Ga	3, `SIMP`
6	$Ga \Rightarrow Ha$	2, `UI`
7	Ha	$5, 6$ `MP`
8	$Fa \wedge Ha$	$4, 7$ `ADJ`
9	$\exists x(Fx \wedge Hx)$	8, `EG`
10	$\exists x(Fx \wedge Hx)$	$1, 9$ `EI`

We may use `EI` to obtain converses of the $-\mathbf{E}$ and $-\mathbf{U}$ rules, which we call the $\mathbf{E}-$ and $\mathbf{U}-$ rules. We also refer collectively to all four as the $\mathbf{Q} - rules$.

Using `EI`, we may prove $\mathbf{U}-$, which allows us to derive $-\exists u\ X(u)$ from $\forall u\ -X(u)$:

		REM
1	$\forall u\ -X[u/p]$	
2	$\exists u\ X[u/p]$	
3	$X(p)$	
4	$-X(p)$	1, `UI`
5	$\bot$	$3, 4$ `PC`
6	$\bot$	$2, 5$ `EI`
7	$-\exists u\ X[u/p]$	6, `IPC`

		REM
1	$\forall x\ -Fx$	
2	$\exists x\ Fx$	
3	Fa	
4	$-Fa$	1, `UI`
5	$\bot$	$3, 4$ `PC`
6	$\bot$	$2, 5$ `EI`
7	$-\exists x\ Fx$	6, `IPC`

Observe that the application of `EI` at line 6 is legitimate because p does not occur in $\bot$, nor can any individual symbol, since $\bot$ is a Boolean constant.

Also using `EI`, we may prove $\mathbf{E}-$, which says that $\exists u\ -X[u/p] \vdash -\forall u\ X[u/p]$:

		REM
1	$\exists u\ -X[u/p]$	
2	$\forall u\ X[u/p]$	
3	$-X(p)$	
4	$X(p)$	2, `UI`
5	$\bot$	3, 4 `PC`
6	$\bot$	1, 5 `EI`
7	$-\forall u\ X[u/p]$	6, `IPC`

		REM
1	$\exists x\ -Fx$	
2	$\forall x\ Fx$	
3	$-Fa$	
4	Fa	2, `UI`
5	$\bot$	3, 4 `PC`
6	$\bot$	1, 5 `EI`
7	$-\forall x\ Fx$	6, `IPC`

And one final example: $\exists y \forall x\ xRy \vdash \forall x \exists y\ xRy$.

			REM
1	$\exists y \forall x$	xRy	
2	$\forall x$	xRb	
3		aRb	2, `UI`
4	$\exists y$	aRy	3, `EG`
5	$\forall x \exists y$	xRy	4, `UG`
6	$\forall x \exists y$	xRy	1, 5 `EI`

PROBLEMS

1. Provide formal proofs for the following assertions:

$$\begin{array}{rcl}
\forall x(\exists y\ Fx,y \Rightarrow Gx) & \vdash & \forall x \forall y(Fx,y \Rightarrow Gx) \\
\forall x \forall y(Gx \Rightarrow Fx,y) & \vdash & \forall x(\exists y Fx,y \Rightarrow Gx) \\
\forall x \forall y(Gx \Rightarrow Fx,y) & \vdash & \forall x(Gx \Rightarrow \forall y\ Fx,y) \\
\forall x \exists y(Gx \Rightarrow Fx,y) & \vdash & \forall x(Gx \Rightarrow \exists y\ Fx,y)
\end{array}$$

7.3.2 The Basic Problems of First Order Logic

You can *attack* the satisfiability problem in first order logic by truth trees or proof trees, just as you would in propositional and zero order logic: a set of formulas is satisfiable `iff` it does not close, and an argument is valid `iff` there is a proof of the conclusion from its set of assumptions. But *deciding* whether a set is satisfiable or an argument valid is another matter.

For although the satisfiability problem for finite sets of formulas is *intractable* in Boolean logic–no practical method is known for finding a solution in most cases, because the number of steps required may double with each new atomic formula involved–at least an **algorithm** or **decision procedure** exists for solving it.

In the next chapter, we shall find that in first order logic, this is no longer true: you can't program a computer, even one with an infinite memory (or one with a finite memory which you can always upgrade by adding more space), so that it will always decide whether the set is satisfiable, no matter how long it takes. Thus there is no way, in general, of deciding whether a truth tree under construction will close or not. If you find a closed tree, you have solved the problem. But at any stage, there is not always a way of determining whether it will or will not eventually close.

As we shall see in 7.5.2, an argument is provable `iff` it's valid. Therefore, there is no algorithm for deciding whether a given argument is provable either, that is, whether there is a proof of the conclusion from the assumptions. If we find a proof or a counter-example, we have our answer. But there is no algorithm for finding counter-examples to an argument (if any exist). There is an algorithm for finding a proof of X from Γ if there are any, for any closed truth tree can be converted into a proof. If $\Gamma, -X$ closes, a proof of X from Γ can be found, given a closed tree $\mathbf{T}$ constructed from $\Gamma, -X$. And if $\mathbf{T}$ exists, it can be found in finitely many steps.

Uniform monadic first order logic, however, *is* decidable, for any tree constructed from a finite set U of uniform sentences can always be completed in a finite number of steps, since U can contain only a finite number of δ-formulas, each instance of which is quantifier-free. As a result, the δ rule can be applied only a finite number of times. Thus if you construct a tree from a finite set of uniform sentences and do not apply any γ-rules until all α and β-rules have been applied, followed by all applications of δ-rules, the tree *will* be completed in finitely many steps.

PROBLEMS

1. Outline a decision procedure for Aristotelian or categorical syllogisms.

7.4 First Order Theories

A *first order theory* of a first order language L may be identified with the set T of its *theorems*, which follow from some subset of T, which we may identify with its axioms. Equivalently, T is any set of sentences of L, each member X of which is deducible from T, i.e. $T \vdash X$.

A *first order theory with functions and equality* is a first order theory of a first order language L which has function symbols, and the equality sign ' $=$ ', which we take to be a *logical* symbol. As such, there are certain rules governing equality, which say that everything is equal to itself, and that if $p = q$, then any property (definable in the theory) which p has, q must have as well. That is, for any formula X of L, the formula $X(p) \Leftrightarrow X(q)$ is derivable from $p = q$. The converse, that $p = q$ is derivable from $X(p) \Leftrightarrow X(q)$, is a weaker case of Leibniz' principle of the identity of **indiscernibles**, but is not a truth of first order logic. But the equality sign always denotes the identity relation $\{\langle x, y\rangle \in D^2 : x = y\}$ on the domain D of any structure $\mathbf{D}$ of a first order language with equality. Thus $p = q$ is true in $\mathbf{D}$ `iff` $d(p) = d(q)$.

Any first order theory with functions and equality can be recast as a first order theory without functions and equality, along the lines sketched in 6.1.2, but generally at the expense of simplicity of expression. Not very many interesting first order theories are first order theories without functions and equality (or recast first order theories with functions and equality).

In 7.4.3 (page 183), we present some important examples of first order theories with functions and equality, along with their models. There are five sets of examples, which you may find helpful depending on your interests. Of these, 2 (Arithmetics, page 183), 3 (Orders, page 186) and 6 (Semirings, page 189) are important in various parts of the next chapter, and the remaining three provide some additional insight into trees, into the relation between the inversion complementation and duality relations on Boolean lattices, and into valid Aristotelian syllogisms defined in terms of semigroup identities. The examples you will find most helpful will of course depend on your interests.

In detail, those discussed in 2 (Arithmetics), the first set of examples, discuss various theories of a language M with equality, with the constant '0' with addition, multiplication, exponentiation and the successor function $'$, where the successor a' of a is $a + 1$. The *standard* model $\mathbf{N}$ of M has its domain the set of natural numbers, where the addition and multiplication signs denote addition and multiplication of natural numbers, and $a\hat{\ }b$ denotes a^b. The theories discussed in 1 (page 183) are called **arithmetics**, and are *sound* in the sense that $\mathbf{N}$ is a model of all of them. Thus they are all *subtheories* of $T_{\mathbf{N}}$, the theory of $\mathbf{N}$. Arithmetics are especially important in our discussion of Gödel's incompleteness results, which are arguably the most important development in the foundations of mathematics during the twentieth century. We discuss them in section 8.5 (page 233).

In 2 (Arithmetics, page 183), the second set of examples, we discuss lattices and Boolean algebras, both of which are models of the first order theory of lattices. In section **??** (*Classical Math and Loss of Certainty*, page **??**) of the next chapter, we discuss them in relation to Boolean entailment, and their connection to projective geometries and to zero dimensional compact topological spaces.

In 3 (Orders, page 186), we discuss **groups** in connection with permutation groups (groups of *permutations* of a given set under composition) and the group under composition of the identity, inversion, complementation and duality operations on Boolean vectors.

In 4 (page 187), we discuss **semigroups** in connection with categorical syllogisms. The set of expressions also forms a semigroup with respect to the concatenation or juxtaposition operation. This comes up in section 8.5.2, in connection with Gödel numbering, a device which Gödel first used to talk about arithmetics within the language of arithmetic.

And finally in 6 (page 189), we discuss rings, fields and ordered fields. Boolean algebras can also be taken to be special sorts of rings, while fields play a role in characterizing the rational, real and complex number systems, which are central to the calculus. Problems with the foundations of the calculus which appeared in the late eighteenth and early nineteenth centuries, motivated exact definitions of the real and complex numbers in terms of rational numbers, which in turn were reduced to integers, which were reduced to the natural numbers, within a set-theoretical framework, which we explore in section 8.3.3. Given these definitions, the rational, and real and become ordered fields, while the system of integers so defined is an ordered ring, but not a field, while the complex number system is an unordered field (as is the two-element Boolean ring).

7.4.1 First Order Theories

The Egyptians and the Babylonians knew of special instances of the theorem of Pythagoras, but Pythagoras or members of his school were the first to assert it in all its generality, and to *prove* it. The Pythagoreans and the Athenian geometers stated and proved many other geometric facts, but Euclid was the first to show that all of these could be deduced from a few simple assumptions, which he called *axioms* or *postulates* (if they applied to geometry alone). He may therefore be credited with making geometry a *theory*, although not all of his axioms and postulates or the *theorems* he deduced from them, can be formalized in first order logic.

A **first order theory** of a first order language L is a nonempty set T of sentences of L which is **closed under logical consequence**: if the sentence X is in T and $T \vdash Y$, then Y is in T. In other words, T is a *theory* `iff` the set of all sentences X such that $T \vdash X$ is T itself. A first order theory is sometimes called an **elementary theory**.

Every member X of T is called **theorem** of T, and is *provable* in T, so we may write $T \vdash X$ or else $\vdash_T X$. Thus X is **unprovable** in T `iff` it is not provable in T, and is **disprovable** `iff` $-X$ is provable. Any subset A of T (not necessarily a theory), from which every theorem of T is provable, is an **axiomatization** of T. The members of A are **axioms**. Thus for any axiomatization A of T and sentence X, if $A \vdash X$ then X is in T. Of course, T is an axiomatization of itself and is infinite. If it has a finite axiomatization, it is said to be **finitely axiomatizable**. Any theory of L which contains T is called an **extension** of T, and T is a **subtheory** of any of its extensions[3].

A first order theory T of L is **inconsistent** `iff` all sentences of L are theorems, or equivalently by the spread rule, '$\perp$' (or $X \wedge -X$) is a theorem of T.

[3]Euclid, and many modern authors as well, identify a theory with its particular axiomatization; we do not do so, because it complicates somewhat the definition of extensions of a theory. And unlike Euclid, the modern practice is not to distinguish between axioms and postulates.

We say T is **consistent** `iff` it is not inconsistent. We say T is **complete** `iff` every sentence of L is **decidable** in T, i.e. it is either provable or disprovable in T.

For instance, the first order theory of a language with only one nonlogical symbol, the unary relation symbol 'F', axiomatized by $\{$ '$\forall x\ Fx$'$\}$ is complete, but the theory axiomatized by $\{$ '$\exists x\ Fx$'$\}$ is incomplete.

Let FO_L consist of those sentences of L which are theorems of logic. It is a first order theory, since it is closed under logical consequence and is called the **first order logic** of L. Since every sentence in FO_L is a logical consequence of every set of sentences of L, it is a subset of every theory of L. Thus it has an empty axiomatization $Ax = \emptyset$.

A theory may not be finitely axiomatizable, but there may still be a mechanical procedure, or some computer program (however inefficient) to determine invariably (for a given axiomatization) whether a given sentence is an axiom or not. Such an axiomatization is a **decidable set of sentences**. (Note the distinction between a decidable *set* of sentences and a sentence *decidable in a theory*). We call any theory with a decidable axiomatization **formalizable**. Of course, any finitely axiomatizable theory is formalizable, but as we shall see in Chapter 8, not all theories are formalizable, and not all theories, and not even all finitely axiomatizable theories, are decidable.

PROBLEMS

1. Find an axiomatization for a first order theory of equivalence relations and for strict partial orders.

2. Find another axiomatization for each of these theories.

3. Find a consistent first order theory with no finite model.

4. Find a first order theory which is satisfiable in all (structures with) one-element domains, but not in all domains with more than one element.

5. Based on what was said in the last paragraph of this section, show that not all first order theories are finitely axiomatizable.

6. Show that the theory of any elementary structure **D** is indeed a first order theory of the language L' of **D**.

As is well known, Euclid neglected to make all of his assumptions explicit, a defect remedied by Hilbert in his **Foundations of Geometry**[37]. Thus Euclid proved as a *theorem* what should have been taken as a *postulate* which he implicitly used, equivalent to the proposition that all lines are continuous, which is now called *Pasch's axiom* (see footnote page 26). Hilbert's axiomatization is not a first order theory however, since in addition to individual variables, some axioms contain variables which range over sets. Tarski constructed a much weaker first order version.

7.4.2 Introducing Functions and Equality: First Order Theories with Equality

Although as we have remarked in section 6.1.2, function symbols such as the plus sign aren't strictly needed to express mathematical propositions involving, say, the notion of addition, since we can always write 'Px, y, z' for '$x + y = z$', and we don't need to have the equals sign with special logical properties either, for we can introduce a binary relation sign and postulate the needed properties, for example the universal closures of the following open sentences:

$$
\begin{aligned}
& xEx \ , && (7.27)\\
xEy \ &\Rightarrow \ (xEz \Rightarrow yEz) \ , && (7.28)\\
xEx_1 \ &\Rightarrow \ (Px, y, z \Rightarrow Px_1, y, z) \ , && (7.29)\\
yEy_1 \ &\Rightarrow \ (Px, y, z \Rightarrow Px, y_1, z) \ , && (7.30)\\
zEz_1 \ &\Rightarrow \ (Px, y, z \Rightarrow Px, y, z_1) \ , && (7.31)\\
Px, y, z \ &\Rightarrow \ (Px, y, z_1 \Rightarrow zEz_1) \ . && (7.32)
\end{aligned}
$$

But if you ever actually want to derive consequences from given set of sentences involving addition, instead of merely theorizing about the set, it is certainly more convenient and perspicuous to introduce the plus sign, and instead of postulating the properties of equality piecemeal for each predicate P, to have equality already endowed with the needed logical properties, which Euclid called "axioms" instead of "postulates".

A **first order language** L **with equality** has at least one relation symbol, one of which is the equals sign, and may also have one or more function symbols. A **term** of L is any individual symbol, or any expression $f(t_1, \dots, t_n)$, where f is an n-ary function symbol and $t_1, \dots$ and t_n are terms. If $\star$ is a 2-ary function symbol, we generally write the term in "operator notation" instead of "functional notation". That is, we write $t_1 \star t_2$ instead of $\star(t_1, t_2)$. A theory of a first order language with equality is a **first order theory with equality**.

In a structure **D** with domain I of a first order language L with equality, we extend j so that every n-ary function symbol f has an extension $j(f)$, which we may take to be a function $F : I^n \to I$. We also extend the denoting function of **I** from the set of individual symbols of L onto I, to a function $d : Tm^{L'} \to I$ where $Tm^{L'}$ is the set of terms of L', so

$$d\big(f(t_1, \dots, t_n)\big) = F\big(d(t_1), \dots, d(t_n)\big) \ . \qquad (7.33)$$

Let **H** and **I** be models of Γ, such that $H \subseteq I$ and the extension of every relation of **H** is a subset of its extension in **I**. And suppose that whenever F and G are the extensions in **I** of the n-ary function symbols f and g, then their extensions in **I** are respectively $F|I^n$ and $G|I^n$. Then **H** is a **submodel** of **I**.

A **normal** structure of a first order language with equality must make true every atomic formula $t_1 = t_2$, where t_1 and t_2 are terms, if $d(t_1) = d(t_2)$, and make it false if $d(t_1) \neq d(t_2)$. Thus $t = t$ must always be true, while if $t_1 = t_2$ is true, then the truth value of any formula $X(t_1)$ must be the same as the truth value of $X(t_2)$, where $X(t_2)$ results from $X(t_1)$ by replacing one or more occurrences of t_1 in $X(t_1)$ (if any) by t_2.

We will be concerned only with normal structures. Thus the following two natural deduction rules in first order languages with functions and equality preserve truth and are therefore sound. They are **reflexivity of equality** (`RFE`) and **substitutivity of equality** (`SBE`),

RFE `You may introduce any formula` $t = t$ `at any step, which is` *not* `counted as an assumption.`

SBE `In the natural deduction system, from` $t_1 = t_2$ `and` $X(t_1)$`, you may infer` $X(t_2)$`, provided that both` $t_1 = t_2$ `and` $X(t_1)$ `are unenclosed at this step of the proof.`

For instance, if we define $1 + 1$ to be 2, $2 + 1$ to be 3 and $3 + 1$ to be 4, thus taking '2' to be an abbreviation for '$1 + 1$', '3' to be an abbreviation for '$(1 + 1) + 1$' and '4' to be an abbreviation for '$((1 + 1) + 1) + 1$', and we assume that addition is **associative**, that is,

$$k + (m + n) = (k + m) + n \ , \tag{7.34}$$

for all numbers k, m and n, it follows that $2 + 2 = 4$, for, using Leibniz' proof of this, we have,

$$\begin{array}{rcll} 2+2 & = & 2+2 & \textbf{RFE} \\ & = & 2+(1+1) & \text{By definition} \\ & = & (2+1)+1 & \text{By associativity} \\ & = & 3+1 & \text{By definition} \\ & = & 4 & \text{By definition} \end{array} \tag{7.35}$$

We can also give a formal proof of this *informal* one, to show that from $\forall x \forall y \forall z(x + (y + z) = (x + y) + z)$, together with $1 + 1 = 2$, $2 + 1 = 3$, and $3 + 1 = 4$, we may derive $2 + 2 = 4$:

			REM
——	1	$\forall x \forall y \forall z \Big(x + (y + z) = (x + y) + z \Big)$	
——	2	$1 + 1 = 2$	
——	3	$2 + 1 = 3$	
——	4	$3 + 1 = 4$	
	5	$\forall y \forall z \Big(2 + (y + z) = (2 + y) + z \Big)$	1, `UI`
	6	$\forall z \Big(2 + (1 + z) = (2 + 1) + z \Big)$	5, `UI`
	7	$2 + (1 + 1) = (2 + 1) + 1$	6, `UI`
	8	$2 + 2 = (2 + 1) + 1$	2, 7 `SE`
	9	$2 + 2 = 3 + 1$	3, 8 `SE`
	10	$2 + 2 = 4$	4, 9 `SE`

Truth trees in first order languages with equality have these rules for truth trees:

CL≠ `Close any path in which the formula` $t \neq t$ `occurs.`

SBE `If` $t_1 = t_2$ `and` $X(t_1)$ `both occur in an open path, you may add` $X(t_2)$ `to the end, and` $X(t_1)$ `is not fulfilled until this is done in all possible ways.`

With these two tree rules in hand, we may also get a closed truth tree from the sentences on lines 1-4 in the formal proof above, with the addition of '$2 + 2 \neq 4$':

$$
\begin{array}{rcl}
\forall x \forall y \forall z \Big(x + (y + z) & = & (x + y) + z \Big) \\
1 + 1 & = & 2 \\
2 + 1 & = & 3 \\
3 + 1 & = & 4 \\
2 + 2 & \neq & 4 \\
\forall y \forall z \Big(2 + (y + z) & = & (2 + y) + z \Big) \\
\forall z \Big(2 + (1 + z) & = & (2 + 1) + z \Big) \\
2 + (1 + 1) & = & (2 + 1) + 1 \\
2 + 2 & = & (2 + 1) + 1 \\
2 + 2 & = & 3 + 1 \\
2 + 2 & = & 4 \\
 & \perp &
\end{array}
$$

PROBLEMS

1. Find a first order theory with equality, all normal models of which have a unit domain.

2. Find a first order theory with equality which has no finite normal models.

7.4.3 Some First Order Theories with Functions and Equality

Below we discuss some first order theories with equality which are especially important in the next chapter:

1. Trees

Here is one way of defining a tree: Let L be a first order language with equality which has one constant 'r', and one binary relation symbol 'P'. As axioms, we have the set `Te` of universal closures of the following open sentences:

$$Px, y \wedge Px, z \quad \Rightarrow \quad y = z \tag{7.36}$$
$$x \neq r \quad \Leftrightarrow \quad \exists y \; Px, y \tag{7.37}$$

Any model $\mathbf{T}$ of `Te` may be called a **tree**, the **origin** of which is r, its sole distinguished element. Suppose $|P|$ is the graph of a function $p : T - \{r\} \to T$, so that p is undefined at the origin r, and Px, y holds `iff` $x \neq r$ and $p(x) = y$. We say that y is a **successor** of x `iff` Px, y holds, and that x is the **predecessor** of y. An element of T is a **junction** `iff` it has more than one successor, and an **end** `iff` it has none.

The only trees we consider are **stratisfiable**, in the sense that any subset Q of T which contains r and contains all successors of any member of Q, contains all members of T, so that $Q = T$. Stratisfiability so defined is not a first order concept. But a stratisfiable tree with no junctions may be called a **sequence**, which is **infinite** `iff` it has no end. We may then define the **natural number sequence** to be an infinite sequence with origin 0.

In any infinite sequence, the predecessor function is a one-to-one correspondence from $T - \{r\}$ to T, and its inverse $s : T \to T - \{r\}$ is therefore a one-to-one correspondence from T to $T - \{r\}$. We may then define any nonzero natural number to be,

$$s^n(0) = \underbrace{ss...s0}_{n \ times} \ . \tag{7.38}$$

2. Arithmetics

Let M be a first order language with equality, the nonlogical symbols of which are the addition sign '+', the multiplication sign '$\cdot$', the exponentiation sign '$\hat{}$' (where we may abbreviate $t\hat{}r$ informally as t_r), the successor sign $'$ the relation sign '$\leq$' and the constant '0'. In the sequel, it will be convenient to write n' for $s(n)$, n'' for ssn, and so on, for all n in N. The terms,

$$0,\ 0',\ 0'',\ \ldots \tag{7.39}$$

are called **numerals** of N and we write informally $\mathbf{0}, \mathbf{1}, \mathbf{2}, \ldots$ for these terms.

The **standard** structure $\mathbf{N}$ of M is a normal M-structure which has as its domain the set N of natural numbers, and has one distinguished element, 0. The language of $\mathbf{N}$ is M itself, and the name $\mathbf{n}$ (in $\mathbf{N}$) of each n in N is the numeral $\mathbf{n}$, which denotes n. If r is any M-term,

$$d(r') = d(r) + 1\ , \tag{7.40}$$

and if t is an M-term,

$$d(r+t) = d(r) + d(t)\ , \tag{7.41}$$
$$d(r \cdot t) = d(r) \cdot d(t)\ , \tag{7.42}$$
$$d(r\hat{\ }t) = d(r)^{d(t)}\ , \tag{7.43}$$

and $r \leq t$ is true (in $\mathbf{N}$) `iff` $d(r) \leq d(t)$. Let k, n and p be any natural numbers. **Minimal arithmetic with exponentiation** E_0E is a theory of M. It will be of some use in the next chapter. One of its axiomatizations consists of all sentences of the following form, one for each $k \leq 0$:

$$\forall x\big(x \leq k \Leftrightarrow (x = 0 \wedge \ldots \wedge x = k)\big) \tag{7.44}$$

together with all sentences of the following forms *which are true in* $\mathbf{N}$:

$\mathbf{k}+\mathbf{n}=\mathbf{p}$	for all $k,n,p \in N$ such that	$k+n=p$
$\mathbf{k}\cdot\mathbf{n}=\mathbf{p}$	for all $k,n,p \in N$ such that	$k\cdot n=p$
$\mathbf{k}\hat{\ }\mathbf{n}=\mathbf{p}$	for all $k,n,p \in N$ such that	$k^n=p$
$\mathbf{k}\neq\mathbf{n}$	for all $k,n \in N$ such that	$k\neq n$

Hence E_0 is formalizable theory, for the process of substituting a specific numeral for $\mathbf{k}$ in either of the first two schemes yields an axiom, and each axiom which is a true instance of one of the next four schemes can be shown to be true by calculation.

We call any extension of E_0 an **elementary arithmetic** (with exponentiation). There are two other elementary arithmetics that are of particular importance in the next chapter. The first of these is **Robinson's arithmetic with exponetiation** or `RE`, which is formalizable, for it has a finite axiomatization[4]:

$$\forall x \forall y(x' = y' \Rightarrow x = y) \quad , \tag{7.45}$$
$$\forall x(x' \neq 0) \quad , \tag{7.46}$$
$$\forall x(x + 0 = x) \quad , \tag{7.47}$$

[4]Robinson's arithmetic with exponentiation `RE` is known to be an extension of E_0 (see, e.g. Smullyan[89]), and is therefore an elementary arithmetic.

$$\forall x\forall y\big(x + y' = (x + y)'\big) \quad , \tag{7.48}$$
$$\forall x(x \cdot 0 = 0) \quad , \tag{7.49}$$
$$\forall x\forall y(x \cdot y' = \big(x\cdot) + x\big) \quad , \tag{7.50}$$
$$\forall x(x^0 = \mathbf{1}) \quad , \tag{7.51}$$
$$\forall x\forall y(x^{y'} = x^y \cdot x) \quad , \tag{7.52}$$
$$\forall x(x \leq 0 \Leftrightarrow x = 0) \quad , \tag{7.53}$$
$$\forall x\forall y(x \leq y' \Leftrightarrow x \leq y \vee x = y') \quad , \tag{7.54}$$
$$\forall x\forall y(x \leq x \vee y \leq x) \quad , \tag{7.55}$$
$$\forall x(x \neq 0 \Rightarrow \exists y\ x = y') \ . \tag{7.56}$$

The other one is **Peano arithmetic with exponentiation** or `PE`, and is an elementary form of Peano's postulates. Unlike `RE`, it is not is not finitely axiomatizable. To get an axiomatization of `PE`, replace the last of the above axioms for `RE` by an infinite set of axioms, all of which are instances of the following **induction schemes**, $N_1, \ldots, N_k, \ldots$, one for each $k \geq 1$:

$$S(0) \wedge \forall x_1(S(x_1) \Rightarrow S(x_1')) \Rightarrow \forall x_1\ S(x_1) \quad , \tag{7.57}$$
$$\forall x_1 \ldots \forall x_{k-1}\big(S[0/x_k] \wedge \forall x_k(\Rightarrow S[x_k'/x_k]) \Rightarrow \forall x_1 \ldots \forall x_k\ S\big) \quad , \tag{7.58}$$

from which an axiom results when a k-formula is substituted for S. Using these induction schemes, we may show that `PE` is an extension of `RE`, by proving in `PE` the last axiom of `RE` by induction. Here we take k to be 1 and substitute the 1-formula $x \neq 0 \Rightarrow \exists y\ x = y'$ for S in N_1 (taking x to be x_1 and y to be x_2).

The sentence $S(0)$ is $0 \neq 0 \Rightarrow \exists y\ 0 = y'$, and is called the **base** of the induction. As is often the case, the base is easy to prove, even trivial. Here $S(0)$ is provable in `PE` without appeal to any axiom of `PE`, because it is a truth of logic, for by **RFE** the negation of its antecedent $0 \neq 0$ is a truth of logic, and so $S(0)$ follows truth functionally from $0 \neq 0$.

Next, assume the **inductive hypothesis** $S(n)$, where we may take n to be a parameter,

$$n \neq 0 \Rightarrow \exists y(y' = n) \ . \tag{7.59}$$

To complete the proof, it suffices to infer $S(n')$, or

$$n' \neq 0 \Rightarrow \exists y(y' = n') \ , \tag{7.60}$$

from the inductive hypothesis. This is provable in `PE` (page **??**) from the inductive hypothesis, indeed in from FOm (the first order logic for M) alone, since by `RFE`, $n' = n'$ and therefore by `EG` (page **??**), $\exists y(y' = n')$, which truth functionally implies equation (7.60) above. So by `CP` (page 41), equation (7.59) implies (7.60), i.e. $S(n) \Rightarrow S(n')$, and by `UG` (page **??**), $\forall x(S(x) \Rightarrow S(x'))$. Having thus proved both $S(0)$ and $\forall x(S(x) \Rightarrow S(x'))$, $N - 1$ yields $\forall x\ S(x)$, here $\forall x(x \neq 0 \Rightarrow \exists y\ x = y')$.

`PE` is **sound**, in the sense that $\mathbf{N}$ is a model of `PE`, the **standard model**. Then $\mathbf{N}$ is a submodel of every model of `PE` and is a model of every subtheory of PE, including E_0. We call any *sound* elementary arithmetic an **arithmetic**. The arithmetic which includes all others is $T_{\mathbf{N}}$, the **theory** of **N**, the set of all M-sentences true in **N**. The only submodel of PE is **N** itself.

3. Orders

Let **P** be a pre-order, so that R is a relation which is reflexive and transitive in P. If R is also **antisymmetric** in **P**, so that the sentence

$$\forall x \forall y (xRy \wedge yRx \Rightarrow x = y) \ , \tag{7.61}$$

is true in **P**, then **P** is a **partial order**. When **P** is a partial order, it is customary to write $a \leq b$ instead of aRb. We may also write $a < b$ for $a \leq b \wedge a \neq b$. A partial order in which $\forall x \forall y (x \leq y \vee y \leq x)$ holds is a **linear order**. A **strict linear order** is a strict partial order in which given any two distinct elements a and b, either $a < b$ or $b < a$.

A **lower** (**upper**) **bound** of the subset $\{x, y\}$ of P is an element b of P such that $b \leq x$ and $b \leq y (x \leq bandy \leq b)$. Then b is a **greatest lower bound** (**least upper bound**) of the pair $\{x, y\}$ of elements of **P** iff for every z in P, if z is a lower bound of $\{x, y\}$, then $z \leq b$ (if z is an upper bound of $\{x, y\}$, then $b \leq z$). Clearly, if a greatest lower bound b (least upper bound b) of $\{x, y\}$ exists, it is unique, for if b and b' are both greatest lower bounds (least upper bounds) of $\{x, y\}$, then $b \leq b'$ and $b' \leq b$, so that by virtue of the antisymmetry of $\leq$, $b = b'$. The greatest lower bound of $\{x, y\}$ is also called the **meet**, **infimum** or g.l.b., while the greatest lower bound may be called the **join**, **supremum** or the l.u.b.

A **lattice L** is any model of the **theory of lattices**, and is a partial order in which any pair $\{x, y\}$ of elements has both a greatest lower bound and a least upper bound. We may axiomatize it in a first order language that has a binary relation symbol ‘ $\leq$ ’, the equality sign, and two binary function symbols ‘$\wedge$’ and ‘$\vee$’, where $x \wedge y$ and $x \vee y$ are, respectively, the greatest lower bounds and least upper bounds of $\{x, y\}$. Thus the conditions,

- If $z \leq x$ and $z \leq y$, then $z \leq x \wedge y$,
- If $x \leq z$ and $y \leq z$, then $x \vee y \leq z$,

hold for all x, y, z, in L. In any lattice, $\wedge$ and $\vee$ are **idempotent**, **commutative** and **associative** operations,

$$\text{Idempotent} \equiv \begin{cases} x = x \wedge x & , \\ x = x \vee x & ; \end{cases} \tag{7.62}$$

$$\text{Commutative} \equiv \begin{cases} x \wedge y = y \wedge x & , \\ x \vee y = y \vee x & ; \end{cases} \tag{7.63}$$

$$\text{Associative} \equiv \begin{cases} x \wedge (y \wedge z) = (x \wedge y) \wedge z & , \\ x \vee (y \vee z) = (x \vee y) \vee z & . \end{cases} \tag{7.64}$$

If in addition, we have,

$$\text{Distributive} \equiv \begin{cases} x \wedge (y \vee z) = (x \wedge y) \vee (x \wedge z) & , \\ x \vee (y \wedge z) = (x \vee y) \wedge (x \vee z) & , \end{cases} \tag{7.65}$$

for all x, y, and z in L, then **L** is **distributive**, and is **bounded** `iff` there are elements 0 and 1 such that $0 \leq x \leq 1$ for all x. If a is in L and the set of equations,

$$a \wedge y = 0 \, , \tag{7.66}$$

$$a \vee y = 1 \, , \tag{7.67}$$

has a solution in y, it is unique if **L** is distributive. It is then called the **complement** $-a$ of a. If every x in **L** has a complement $-x$, then **L** is a **complemented lattice**. A distributive complemented lattice is a **Boolean lattice**, or a **Boolean algebra**. The power set of any set is a Boolean lattice with respect to set inclusion, intersection, union and complementation.

4. Semigroups

The **theory of semigroups** is a first order theory with equality with a binary function symbol '$\circ$' which denotes an associative operation. Its single axiom is,

$$\forall x \forall y \forall z \big(x \circ (y \circ z) = (x \circ y) \circ z \big) \; . \tag{7.68}$$

Any model of this axiom is a **semigroup**. We sometimes omit '$\circ$' altogether and write, for example, 'xy' instead of '$x \circ y$'. A semigroup **S** is **commutative** `iff` $x \circ y = y \circ x$ for all elements x and y. We sometimes use the plus sign for the semigroup operation symbol '$\circ$' when the semigroup is commutative and call it an **additive semigroup**; if we use the multiplication sign '$\cdot$' or no sign at all instead, we call it a **multiplicative semigroup**. A multiplicative semigroup that has an element 0, such that for every element x, we have $x \cdot 0 = 0 \cdot x = 0$ is a **semigroup with zero**.

The theory of Aristotelian syllogisms can be translated into the theory of commutative semigroups with zero: write $xy = x$ for "all x's are y's", $xy = 0$ for "no x's are y's", $xy \neq 0$ for "some x's are y's" and $xy \neq x$ for "some x's are not y's". Then, for example, the argument `FERIO` "some x's are y's, no y's are z's, $\therefore$ some x's are not z's" becomes $x \cdot y \neq 0, y \cdot z = 0 \therefore x \cdot z \neq x$ and can be proved thus: assume the conclusion is false, so that $x \cdot z = x$. Then

$$x \cdot y = (x \cdot z) \cdot y = x \cdot (z \cdot y) = x \cdot (y \cdot z) = 0 \; , \tag{7.69}$$

a contradiction. And `BARBARA`,

$$x \cdot y = x, \quad y \cdot z = y, \; \therefore x \cdot z = x \; , \tag{7.70}$$

has this proof:

$$x \cdot y = x \cdot (y \cdot z) = (c \cdot y) \cdot z = x \cdot z \; . \tag{7.71}$$

A set G of elements of a semigroup **S** is a **set of generators** of **S** `iff` every element of **S** can be written in the form $a_1, \ldots, a_n$, where each of the a_i, $1 \le i \le n$, are in G. For instance, the set of prime numbers is a set of generators for the multiplicative group $\mathbf{Z}^{>2}$ of integers greater than 2.

If every element of **S** can be written uniquely in the form $a_1, \ldots, a_n$, so that if $a_1, \ldots, a_n = b_1, \ldots b_n$, then $a_1 = b_1$ and ... and $a_n = b_n$, then **S** is a **S** is a **free semigroup**, and G is its set of **free generators**. Then any function $g : G \to S$ can be extended uniquely to a function $h : S \to T$ such that $h(st) = h(s) \circ h(t)$ (where $\circ$ is the semigroup operation of the semigroup **T**). All elements of **S**, such as $a_1, \ldots, a_n$ are called **expressions**, and the semigroup operation of **S** is called **concatenation**, and h is a **substitution**.

A semigroup which has an element e called the **semigroup identity** such that for every element x,

$$x \circ e = e \circ x = x, \tag{7.72}$$

is called a **monoid**. We write ‘ 1 ’ for the semigroup identity of a multiplicative monoid, and ‘ 0 ’ for the semigroup identity of an additive semigroup.

5. Groups

The **theory of groups** is a theory with equality which in addition to the equals sign has a 2-ary function symbol ‘$\circ$’ for the **group operation**, a 1-ary function symbol ‘$^{-1}$’ for the **group inverse** and the constant ‘e’ for the **group identity**. We have these axioms:

$$\forall x \forall y \forall z \Big(x \circ (y \circ z) = (x \circ y) \circ z \Big) \quad , \tag{7.73}$$

$$\forall x (x \circ e = x) \quad , \tag{7.74}$$

$$\forall x (x \circ x^{-1} = e) \quad . \tag{7.75}$$

Any model of this set of axioms is a **group**. It is a monoid every element of which has an inverse. The group identity of an additive group is 0, and the group identity of a multiplicative group is 1. The group inverse of an additive group is $-x$, while the group inverse of a multiplicative group is $1/x$.

The set of integers is a group with respect to addition, and is an additive group, while the set of positive rational numbers is a multiplicative group. The set $\{0, 1\}$ is also a group with respect to *algebraic* or `mod` 2 addition (see Chapter 2, section 2.3.2, page 39).

The functions $\mathbf{1}$, $-$, ¡ and $\star$ which send respectively each Boolean 4-vector V to V, $-V$, ¡V and $\star V$, forms a group with respect to composition. The set of all permutations of any nonempty set is a group with respect to composition, and is not necessarily commutative. The smallest noncommutative “permutation group” is the set of all permutations (there are six of them) of a three-element set.

6. Semirings

The **theory of semirings** is a first order theory with equality which in addition to the equals sign has two binary function symbols ‘ + ’ and ‘ · ’. The axioms are the universal closures of:

$$x + (y + z) = (x + y) + z \,, \tag{7.76}$$

$$x \cdot (y \cdot z) = (x \cdot y) \cdot z \,, \tag{7.77}$$

$$x + y = y + x \,, \tag{7.78}$$

$$x \cdot (y + z) = (x \cdot y) + (x \cdot z) \,, \tag{7.79}$$

$$(y + z) \cdot x = (y \cdot x) + (z \cdot x) \,. \tag{7.80}$$

Thus a semiring is a commutative semigroup with respect to addition and a semigroup with respect to multiplication, in which the left and right distributive laws for addition and multiplication hold. A semiring is **commutative** if it is a commutative semigroup with respect to multiplication. If it has an element 1 such that $x \cdot 1 = x = 1 \cdot x$, it is a **semiring with unit**, and if it is a semigroup with zero $x + 0 = 0$ and $x \cdot 0 = 0 \cdot x = 0$ it is a **semiring with zero**.

The set Z of integers and the set N of natural numbers are commutative semirings with respect to addition and multiplication, and both are semirings with unit and zero. The set $\{0, 1\}$ is a semiring with unit and zero with respect to logical addition and multiplication.

A commutatuve semiring **S** with zero and unit which is a group with respect to addition is a **ring**. A commutative ring with unit, in which either $x = 0$ or $y = 0$ whenever $x \cdot y = 0$ is an **integral domain**. It is **ordered** if its set S of elements can be divided into three mutually disjoint subsets G, $\{0\}$ and P. Here each element of G has the form $-x$ (where $x + -x = 0$), for some x in P, and P is **closed** under addition and multiplication: both the sum and product of any two elements of P are in P.

Let P be called the set of **positive elements** and G the set of **negative elements** of S, and we may define $x < y$ `iff` $y - x$ is positive. Note that no ordered ring has a largest element x, for since 1 is positive, $x + 1 > x$.

The ring **Z** of integers is an ordered integral domain, and Z a strict linear order with respect to $<$. Moreover, the relation $<$ has the following property: every non-empty subset of P has a least element. We say that $<$ **well-orders** P. But it does not well-order Z, for instance ¡ does not well-order G, for there is no least negative integer.

The **induction principle** also holds for P in this sense: every subset of P which contains 0 and contains for every member x of P also $x + 1$, contains all members of P. For suppose instead that A is a subset of P which contains 0 and contains for every member x of A its successor $x + 1$, but that it does not contain all members of P, so that $P - A$ is not empty, and since $<$ well-orders P, $P - A$ has a least element n. Then $n - 1$ is in P, and therefore so is n, a contradiction.

A ring in which $x \cdot x = 1$ is a **Boolean ring**. In a Boolean ring with unit, we may write $-x$ for $1 + x$, $x \wedge y$ for $x \cdot y$, and $x \vee y$ for $x + y + (x \cdot y)$. A Boolean ring with unit then contains the identities of Boolean algebra.

An integral domain, the nonzero elements of which form a commutative multiplicative group, is a **field**. The real number system `Re` is a field, as is the set $\{0, 1\}$ of truth values with respect to Boolean multiplication and algebraic addition. We see that `Re` is also an **ordered field**, since it is an ordered integral domain.

PROBLEMS

1. Show that equality is symmetric and transitive.

2. Find a set of sentences that has no infinite normal model. (Hint: let E_2 be the formula $\exists x \exists y\ x \neq y$, let E_3 be the formula $\exists x \exists y \exists z (x \neq y \wedge y \neq z \wedge x \neq z)$, etc.).

3. Let $p : N \to \{0, 1\}$ be the characteristic function of the set of positive (i.e. non-zero) natural numbers, so that $p(n) = 1$ if n is positive and $p(n) = 0$ otherwise. Note that $p(x \cdot y) = p(x) \wedge p(y)$ and $p(x + y) = p(x) \vee p(y)$, and that `PE` is a commutative semiring with respect to addition and multiplication. Conclude that the two-element Boolean algebra $\mathbf{B}_2$ is a commutative semiring with respect to logical addition and logical multiplication. (Hint: let $p' = p|\{0, 1\}$ and observe that $p'(x) = x$).

4. Which of the above theories have finite models and which do not. If the theory has no finite models, explain why. If it has a finite model, provide one.

7.5 Reasoning about First Order Reasoning

In this part, we show that an argument is provable `iff` it is valid: $\Gamma \vdash X$ `iff` $\Gamma \vdash X$. One immediate consequence of this result are the *compactness theorem*, which says that any unsatisfiable set has a finite unsatisfiable subset (equivalently, if all finite subsets of Γ are satisfiable, so is Γ). Another is the *Löwenheim-Skolem theorem*, according to which every satisfiable set of sentences (in a language without equality) has a denumerable model. These results can also be proved from their zero order counterparts.

7.5.1 The First Order Soundness Theorem*

For the sake of definiteness, we state our results in the rest of the chapter for **full** first order logics FO_L without functions and equality. Here we take L to be any first order language without functions and equality, which has denumerably many relation symbols of every arity, and L' to be a constant extension of L, which has denumerably many constants not in L, so that L has denumerably many parameters (in L'). This involves no loss of generality, for the extension

*This part may be skipped without loss of continuity.

of the results which apply to full first order logics to first order logics with functions and equality is fairly straightforward.

Our proof of the Boolean soundness theorem used the fact that $\alpha_1, \alpha_2 \vdash \alpha$and that $\beta_1 \vdash \beta$ and $\beta_2 \vdash \beta$. But while $\delta(p) \vdash \delta$, if Γ is the set of all consequences of γ in a **Hitikka set**, it is not the case that $\Gamma \vdash \gamma$. So we'll proceed in another way.

We first note that the following **derivability condition** for assumptions of formal arguments holds:

DCD $\qquad \Gamma, X \vdash X$.

It simply says that a formula X is provable from any set of assumptions to which it belongs. The corresponding **soundness** condition for assumptions in formal arguments is the scheme:

SCD $\qquad \Gamma, X \models X$,

all instances of which are clearly true.

Now every rule of inference has its own **derivability condition** for extending proofs. Suppose that in a formal proof, the formula P appears at a certain step, so that $\Gamma \vdash P$, where Γ contains all the assumptions undischarged at this step, and subsequently Q is inferred from P by a one premise proper rule so that $P \mapsto Q$ and consequently $\Gamma \vdash Q$. Thus the derivability condition for a single premise proper rule has the form,

DCP1 $\qquad$ If $\Gamma \vdash P$, then $\Gamma \vdash Q$.

To get the corresponding **soundness condition** for any rule, just change each single turnstile '$\vdash$' into a double turnstile '$\models$'. So the soundness condition for a single premise *proper* rule will be,

SCP1 $\qquad$ If $\Gamma \models P$, then $\Gamma \models Q$.

The rule is then **sound** `iff` all instances of the soundness condition are true.

Next, suppose that Q is inferred from P_1 and P_2 by an application of a two-premise proper rule, so that $P_1, P_2 \mapsto Q$. Then by essentially the same argument, the derivability condition and the corresponding soundness condition for *two- premise* proper rules will be respectively:

DCP2 $\qquad$ If $\Gamma_1 \vdash P_1$, then $\Gamma_2 \vdash P_2$, then $\Gamma_1 \cup \Gamma_2 \vdash Q$,

SCP2 $\qquad$ If $\Gamma_1 \models P_1$, then $\Gamma_2 \models P_2$, then $\Gamma_1 \cup \Gamma_2 \vdash Q$.

It follows that,

PRSnd `Every proper rule which preserves truth is sound.`

`Proof` Suppose that $\Gamma \models p$ and that $P \mapsto Q$ by a single premise proper rule `R1` which preserves truth. Then $P \models Q$ (since `R1` preserves truth) and so $\Gamma \models Q$. Thus `R1` is sound.

Next suppose that $\Gamma_1 \models P_1$ and $\Gamma 2 \models P_2$, and that Q can be inferred from P_1 and Q_1, by a two-premise rule `R2`, so that $P_1, P_2 \mapsto Q$. By assumption `R2` preserves truth, and so $P_1, P_2 \models Q$. Then by supposition, $\Gamma_1 \cup \Gamma_2 \models Q$. Thus `R2` is sound as well.■

Corollary: `SIMP, ADD, ADJ, DS, MP, UI, and EG are all sound.`

If in a first order language with functions and equality we require all structures to be normal, `RFE` and `SBE` are likewise sound, since they preserve truth.

`CP` and `BPC` are single premise improper rules, which say that if the premise P of an application is derivable from then the consequence Q of that application is derivable from $\Gamma - \{H\}$, where H is the hypothesis. The derivability condition for these two rules therefore has the form,

DCI1 If $\Gamma \vdash P$, then $\Gamma - \{H\} \vdash Q$,

while the corresponding soundness condition will be,

SCI1 If $\Gamma \models P$, then $\Gamma - \{H\} \models Q$.

The soundness condition for `CP` is,

SCCP If $\Gamma \models Y$, then $\Gamma - \{X\} \models X \Rightarrow Y$.

We now demonstrate,

CPSnd `CP is sound.`

`Proof:` To show that `CP`, it will be helpful to divide the derivability condition for `CP`, which corresponds to `SCCP`, into proper and improper parts, by requiring that $\Gamma - \{X\} = \Gamma$, that is, $X \notin \Gamma$. The two parts are:

$$\begin{aligned} \text{If } \Gamma \vdash Y, &\quad \text{then} \quad \Gamma \vdash X \Rightarrow Y. \\ \text{If } \Gamma, X \vdash Y, &\quad \text{then} \quad \Gamma \vdash X \Rightarrow Y. \end{aligned}$$

By **PRSnd**, the proper part is sound, since it is truth preserving: $Y \models X \Rightarrow Y$. The corresponding soundness condition for the improper part is,

$$\text{If } \Gamma, X \models Y, \text{ then } \Gamma \models X \Rightarrow Y.$$

So suppose that $\Gamma, X \models Y$. Then $\Gamma, X, -Y$ is unsatisfiable. Then so is $\Gamma, -(X \Rightarrow Y)$, for any valuation which satisfies $\Gamma, -(X \Rightarrow Y)$ must also satisfy $\Gamma, X, -Y$. Therefore $\Gamma \models X \Rightarrow Y$.■

BPCSnd `BPC is sound.`

`Proof:` The proper part of the derivability condition for `BPC` is $\bot \vdash X$, and is truth preserving since $\bot \models X$ and therefore sound. The soundness condition corresponding to the improper part is:

$$\text{If } \Gamma, -X \models \bot \text{ then } \Gamma \models X \ .$$

So suppose $\Gamma, -X \models \bot$. Then $\Gamma, -X$ is unsatisfiable, and so $\Gamma \models X$.■

The two remaining rules yet to be proved sound are `UG` and `EI`. Note `UG` is a single premise proper rule which does *not* preserve truth. Its soundness condition comes with a proviso: the parameter p mentioned in the soundness condition is not to occur in $\Gamma, \forall u\ X(u)$. Subject to that proviso, the condition is:

$$\text{If } \Gamma \models X(p) \text{ then } \Gamma \models \forall u\ X(u) \ . \tag{7.81}$$

To prove soundness, we must first show that a systematic completed tree can be constructed from any countable set Γ of first order formulas, and that Γ does not close if it's satisfiable. And we want to extend Hintikka's lemma[38] to the first order case. We use the superscript '^{1}' in the abbreviated names of Hintikka's Lemma, the soundness and completeness theorems and related results, to indicate that they are for first order logic, rather than for zero order or Boolean logic.

We construct a **systematic tree** from Γ in the same way as in Boolean logic with this addition (suggested in Smullyan (1968)[85]): when you apply the γ-rule to a formula γ, adding the instance $\gamma(\mu)$ to the end of every open path in which γ occurs, take γ to be **fulfilled**, and add another occurrence of γ to the bottom of every path π *not completed*, which ends with the new occurrence of $\gamma(\mu)$. In a language with functions and equality, add the following restriction: (suggested in Jeffrey (1991)[39]) to the γ-rule: at the n^{th} stage in the construction, apply the γ-rule, `RFE` and `SBE` only to formulas containing terms with less than n function symbols.

For instance, here is a systematic tree constructed from the formula '$\forall x \exists y\ xRy$':

$$\begin{array}{rl}
\forall x \exists y & xRy \ \star \\
\exists y & a_1Ry \ \star \\
\forall x \exists y & xRy \ \star \\
 & a_1Ra_2 \\
\exists y & a_2Ry \ \star \\
\forall x \exists y & xRy \ \star \\
 & a_2Ra_3 \\
 & \vdots
\end{array}$$

It is a completed tree constructed from $\forall x \exists y\ xRy$, with a single path through it, in which every non-literal has been fulfilled. Thus in a systematic tree constructed from Γ, an open path contains all formulas in Γ and is **completed** `iff` every non-literal it contains has been fulfilled. Thus, as in Boolean logic,

$\mathbf{TR}^1_\infty$ `A systematic completed tree can be constructed from any countable set` Γ `of first order formulas.`

Of course there are completed trees which are not systematic and are generally shorter. An infinite tree need not be systematic, whereas a systematic tree is always completed, finite or not and one constructed from Γ always *exists*. So $\mathbf{TR}^1_\infty$ is of theoretical importance in proving results, rather than of practical importance in solving problems. Proofs of propositions actually actually presented are almost always informal.

Now the γ-rule is downward correct for satisfiability, because any structure **D** which makes γ true must also make $\gamma(\mu)$ true, because $\gamma \models \gamma(\mu)$, and any logical consequence of a true formula must likewise be true. Therefore,

SAT `If` Γ, γ `is satisfiable, so is` $\Gamma, \gamma, \gamma(\mu)$`.`

On the other hand, $\delta(p)$ is not a logical consequence of δ, and so the L'-structure **D** might satisfy a path π that contains an unfulfilled formula δ and yet not satisfy $\pi, \delta(p)$. But since **D** makes δ true, there must be *some* element a of D other than p such that **D** satisfies $\delta(\mathbf{a})$, and since p is a new parameter, it does not occur in π. So let $\mathbf{D}'$ be the L'-structure, a "p-variant" of **D** which is like **D**–its domain and language is the same as that of **D** and it has the same denotation function, *except* that in $\mathbf{D}'$, p denotes a. Thus $\mathbf{D}'$ satisfies $\pi, \delta(p)$. And so the δ-rule is also downward correct for *satisfiability*, if not for truth in a given structure:

$\mathbf{SAT}_\delta$ `If` Γ, δ `is satisfiable, so is` $\Gamma, \delta(p)$`, where` p `does not occur in` $\Gamma, \delta(p)$`.`

Corollary 1 ($\mathbf{SAT}^1$): `The` γ `and` δ`-rules are downward correct for satisfiability.`

Corollary 2 ($\mathbf{T}_S AT$): `No countable satisfiable set closes.`

The γ and δ rules are also upward correct for truth in a given structure **D**. For clearly, if $\delta(p)$ is true in **D**, so is δ. Moreover, if in a given completed open path π all instances $\gamma(\mu)$ in π of the formula γ in π are true, so is γ, *provided that* all members of the domain of **D** are named by individual symbols in π. Hintikka's lemma for first order logic now follows:

$\mathbf{HL}^1$ `Every open path through a completed tree is satisfiable.`

It is immediate from $\mathbf{T}_\infty$ and Hintikka's lemma that,

$\mathbf{T}^1_{UNS}$ `Every unsatisfiable set of formulas closes.`

`Proof:` For if Γ does not close, then by $\mathbf{T}_\infty$ it is contained in an open path of a completed tree and by Hintikka's lemma is satisfiable.■

We may now prove,

UGSnd `UG is sound.`

`Proof:` Suppose that $\Gamma \models X(p)$, where p does not occur in $\forall u\ X(u)$ or in any formula in Γ. By $\mathbf{T}^1_{UNS}$, since by supposition $\Gamma \models X(p)$, the set $\Gamma, -X(p)$ closes and so $\Gamma, -\forall u\ X(u)$ closes. So by $\mathbf{SAT}^1$, $\Gamma, -\forall u\ X(u)$ is unsatisfiable, and thus $\Gamma \models \forall u\ X(u)$.■

The soundness condition for `EI` also comes with a proviso: p is not to occur in $\Gamma, \exists u\ X(u), Y$. With that restriction, the soundness condition for `EI` is:

$$\text{If } \Gamma \models \exists u\ X(u) \text{ and } \Gamma, X(p) \models Y, \text{ then } \Gamma \models y\ .$$

EISnd `EI is sound.`

`Proof;` Suppose that $\Gamma \models \exists u\ X(u)$ and $\Gamma, X(p) \models Y$. Then $\Gamma, -Y \models -X(p)$. Since `UG` is sound, $\Gamma, -Y \models \forall u\ -X(u)$. So $\Gamma, \exists u\ X(u) \models Y$, and thus (by the soundness condition of `CP`, $\Gamma \models \exists u\ X(u) \Rightarrow Y$. But also by our supposition, $\Gamma \models \exists u\ X(u)$, and so $\Gamma \models Y$.■

Corollary: `All the natural deduction rules are sound.`

Now that we have shown that all the natural deduction rules are sound, we want to prove that the natural deduction *system* is sound, in the sense that every provable argument is valid. This is a consequence of the soundness of the natural deduction rules and of the nature of formal proofs. The first n steps of any formal proof is a proof of X_n, the formula at the n^{th} step, from Γ_n, where Γ_n is the set of assumptions which are *undischarged* at the n^{th} step. This makes the assertion $\Gamma_n \vdash X_n$ true. Because the rules are sound, the corresponding assertion $\Gamma_n \models X_n$ will likewise be true.

We demonstrate this by showing how to transform any formal proof that $\Gamma \vdash X$ into a proof that $\Gamma \models X$. At the n^{th} step, replace X_n by the assertion that $\Gamma_n \models X_n$. If X_n is an assumption introduced at the n^{th} step, then X_n will be in Γ_n, and so the assertion $\Gamma_n \models X_n$ will be an instance of `SCD`, and so obviously true. On the other hand, if X_n is the consequence of an inference rule `Rl`, then X_n follows by `Rl` from the premise X_k or follows by `Rl` from the premises X_k and X_m. So $\Gamma_n \models X_n$ will follow from $\Gamma_k \models X_k$, or from $\Gamma_k \models X_k$ and $\Gamma_m \models X_m$, together with the appropriate *soundness condition* for `Rl`.

To see how this works, we offer a proof of the validity of the argument $\exists y \forall x\ xRy \therefore \forall x \exists y\ xRy$, the provability of which was demonstrated in section 7.3.1 by a formal proof. The inference rule `Rl` mentioned in the remarks in the central column at the n^{th} step refers not to `Rl` alone, but also to the appropriate *soundness condition* that with `Rl` justifies $\Gamma_n \models X_n$. In steps opposite an assumption bar, Γ_n is an instance of the soundness condition `SCD` for introducing assumptions:

				REM
1	$\exists y \forall x$	xRy	SCD	$\exists y \forall x\ xRy \models \exists y \forall x\ xRy$
2	$\forall x$	xRb	SCD	$\exists y \forall x\ xRy,\ \forall x\ xRb \models \forall x\ xRb$
3		aRb	2, UI	$\exists y \forall x\ xRy,\ \forall x\ xRb \models aRb$
4	$\exists y$	aRy	3, EG	$\exists y \forall x\ xRy,\ \forall x\ xRb \models \exists y\ aRy$
5	$\forall x \exists y$	xRy	4, UG	$\exists y \forall x\ xRy,\ \forall x\ xRb \models \forall x \exists y\ xRy$
6	$\forall x \exists y$	xRy	1, 5 EI	$\exists y \forall x\ xRy \models \forall x \exists y\ xRy$

The weak and strong soundness theorems now follow:

WST^1 `If` $\Gamma_0 \vdash X$, `then` $\Gamma_0 \models X$.

`Proof:` Assume the hypothesis. Then there is a proof of X from Γ_0, a subset Γ_0' of which is the set of its undischarged assumptions. Since the inference rules are sound, given a proof of x from Γ_0, a proof of the assertion $\Gamma_0' \models X$ can be found by the procedure just outlined. It is then immediate that $\Gamma_0 \models X$.■

Corollary WST$'^0$: `Every finite satisfiable set is consistent.`

ST^1 `If` $\Gamma \vdash X$, `then` $\Gamma \models X$.

`Proof:` Assume the hypothesis. Then there is a proof of X from a *finite* subset Γ_0 of Γ, for every proof has a finite number of steps. So by **WST^1**, $\Gamma_0 \models X$. It is then immediate that $\Gamma \models X$.■

Corollary ST$'^1$: `Every satisfiable set is consistent.`

PROBLEMS

1. Prove the Corollary to **ST$'^1$**.

7.5.2 The Completeness Theorem for First Order Natural Deduction, and related results*

The proofs of completeness theorems for first order logic are similar in principle to those for Boolean logic. Since the natural deduction and truth tree rules for first order logic contain those for Boolean logic, we simply extend the proofs to take into account the new first order rules. First, γ is downward correct for consistency, since $\gamma \vdash \gamma(\mu)$:

CON `If` Γ, γ `is consistent, so is` $\Gamma, \gamma, \gamma(\mu)$.

*This part may be skipped without loss of continuity.

$\mathbf{CON}_\delta$ `If` Γ, δ `is consistent, so is` $\Gamma, \delta(p)$ `where` p `does not occur in` $\Gamma, \delta(p)$.

`Proof:` For if Γ, δ is consistent but $-\Gamma, \delta, \delta(p) \vdash \perp$ where p does not occur in $\Gamma, \delta, \perp$, then by `EI`, $\Gamma, \delta \vdash \perp$, a contradiction.■

From the downward correctness of the tree rules for satisfiability and consistency, it follows at once that,

$\mathbf{T}_{CON}$ `No countable consistent set closes.`

We now turn to the completeness theorem, which we prove in a form due to Henkin[36], using the downward correctness of the natural deduction rules for consistency, and Hintikka's Lemma[38]:

$\mathbf{CT}'^1$ `Every consistent set of formulas has a model.`

`Proof:` If Γ is consistent, it does not close, and so by $\mathbf{T}_\infty$ is contained in an open path of a completed tree and by Hintikka's lemma, has a model.■

Corollary 1: `If` $\Gamma \models X$, `then` $\Gamma \vdash X$.

Corollary 2: $\Gamma \models X$, `iff` $\Gamma \vdash X$.

Corollary 3 $\mathbf{CAPT}^1$: `Every unsatisfiable set of sentences has a finite unsatisfiable subset.`

`Proof:` Let Γ be unsatisfiable. Then it is inconsistent, and so some finite subset Γ_0 is inconsistent, since all proofs are finite in length. Then by $\mathbf{WST}^1$, Γ_0 is unsatisfiable.■

Corollary 4 $\mathbf{CAPT}'^1$: `If every finite subset of` Γ `has a model, then` Γ `has a model.`

Instead of deriving the compactness theorem from the completeness theorem, we can of course first prove the weak completeness theorem for first order logic, and then use the compactness theorem to obtain the completeness theorem. We need two derived first order rules:

RG $\gamma \vdash \gamma(\mu)$,

RD `If` $\Gamma_0, \delta, \delta(p) \vdash \perp$, `where` p `does not occur in` Γ_0, δ, `then` $\Gamma, \delta \vdash \perp$.

With these in hand, we can transform a closed tree constructed from Γ_0 into a proof of a contradiction from Γ_0 in the first order natural deduction system, bearing in mind that `RA`, `RB`, `RG` and `RD` are derived rules. Thus every finite set which closes is inconsistent.

On the other hand, any unsatisfiable set Γ closes, lest by $\mathbf{TR}^1_\infty$ some completed tree constructed from Γ have an open path which by $\mathbf{HL}^1$ is satisfiable.

Then every finite unsatisfiable set is inconsistent, and $\mathbf{WCT}^1$ follows by contraposition. And since every unsatisfiable set closes, so does some finite subset, which by is then inconsistent and so by $\mathbf{WST}^1$ is unsatisfiable, which establishes $\mathbf{CAPT}^1$.

Then $\mathbf{CT}^1$ follows, for suppose that *Gamma* is unsatisfiable. Then by the compactness theorem, so is some finite subset Γ_0. Then by $\mathbf{WCT}^1$, Γ_0 is inconsistent, and therefore so is Γ.

As a corollary to the completeness theorem for first order logic, we may observe that any open path π through a completed tree constructed from a satisfiable set Γ contains only a countable number of individual symbols. Thus there is a model $\mathbf{M}^1$ of π, and so of Γ, in which every element of M is named by an individual symbol in π, so that M is countable. This proves the **Löwenheim-Skolem theorem**:

$\mathbf{LST}^1$ `If` Γ `has a model, it has a countable model.`

The compactness theorem and the Löwenheim-Skolem theorem have some surprising implications for first order logic. For instance, the standard model $\mathbf{N}$ of `PE` is not the only model. Let M' be a constant extension of the language of which `PE` is a theory and $\mathbf{N}$ a structure, and let M' be a constant extension of M, containing the constant c. To the axioms of `PE`, add the axioms,

$$\begin{array}{ccc} 0 & < & c \\ 1 & < & c \\ 2 & < & c \\ & \vdots & \end{array}$$

(here $\mathbf{n} < c$ is an abbreviation for $\mathbf{n} \leq c \wedge n \neq c$) and let $\mathtt{PE}^\infty$ be the M' theory, axiomatized by the set $Ax_{\mathtt{PE}}$ of axioms given in section 7.3.2, together with the set Γ of sentences listed above. Thus $\mathtt{PE}^\infty$ is axiomatized by the set $Ax_{\mathtt{PE}} \cup \Gamma$.

Every finite subset of $Ax_{\mathtt{PE}} \cup \Gamma$ is satisfiable, for let $\mathbf{N}'$ be an M'-structure which is a model of `PE`, and let S_0 be a finite subset of $Ax_{\mathtt{PE}} \cup \Gamma$. We may assume that S_0 contains some sentences $\mathbf{k} < c$ in Γ. Let m be the largest number such that $\mathbf{m} < c$ is in S_0, and let c denote $m+1$ in $\mathbf{N}'$. Then $\mathbf{N}'$ is a model of S_0. Thus every finite subset of $Ax_{\mathtt{PE}} \cup \Gamma$ is satisfiable, and so by the compactness theorem, it has a model $\mathbf{N}^\infty$ which is thus a model of $\mathtt{PE}^\infty$. In $\mathbf{N}^\infty$, c denotes an "infinite" number, which exceeds each n in $\mathbf{N}$, or every *standard* natural number, for $\mathtt{PE}^\infty$ contains $\mathbf{n} < c$.

We discuss more such examples in the next chapter, and their significance for the philosophy and foundations of mathematics.

PROBLEMS

1. Find a set Γ of sentences, every finite subset of which has a finite normal model, whereas Γ itself has no infinite normal model.

7.5.3 Deriving the First Order Completeness Theorem from the Boolean Completeness Theorem, and the Löwenheim-Skolem and First Order Compactness Theorems from the Boolean Compactness Theorems*

The methods of proof of the completeness theorems used in the last section for first order logic were essentially the same as those employed to prove their Boolean counterparts. They involved the existence of systematic trees, the downward correctness of the tree rules for consistency, and their upward correctness for truth. But it is of some interest that the results themselves are derivable from the corresponding results for *Boolean* logic, and so also zero order logic, which differs from Boolean logic only in notation.

A finite set of L-formulas is **regular** `iff` its being so can be deduced from these rules:

`Reg`^{0} $\emptyset$ `is regular.`

`Reg` `If` R_0 `is regular, so is` $R_0, \gamma \Rightarrow \Gamma(\mu)$.

`Reg`$^\delta$ `If` R_0 `is regular, so is` $R_0, \delta \Rightarrow \delta(p)$, `where` p `is a parameter which does not occur in` R_0, δ.

We also call an infinite set of L-formulas **regular** `iff` all of its finite subsets are regular. We note that,

REG `If` R `is a regular set and` Γ `is a satisfiable set of formulas which contains no parameter` p `such that` $\delta \Rightarrow \delta(p)$ `is in` R, `then` $R \cup \Gamma$ `is satisfiable.`

`Proof:` Since $\gamma \Rightarrow \gamma(\mu)$ is universally valid, $\Gamma, \gamma \Rightarrow \gamma)\mu)$ is satisfiable.

To show that $\Gamma, \delta \Rightarrow \delta(p)$ is also satisfiable, suppose instead that it's unsatisfiable. Then so are the sets $\Gamma, -\delta$ and $\Gamma, \delta(p)$ (for if either were satisfiable, $\Gamma, \delta \Rightarrow \delta(p)$ would be satisfiable too). Now by hypothesis, p does not occur in Γ. Therefore, Γ, δ is unsatisfiable, for otherwise by downward correctness, if Γ, δ is satisfiable, $\Gamma, \delta, \delta(p)$ is also satisfiable, as is $\Gamma, \delta(p)$, a contradiction. But then both Γ, δ and $\Gamma, -\delta$ are unsatisfiable, so Γ is unsatisfiable, contrary to hypothesis.■

A **Boolean atom** of L is any atomic L-formula, or any L- formula $Qu\ X(u)$ which is either a universal or existential quantification. A **Boolean valuation** τ of L assigns arbitrary truth values to Boolean atoms, while satisfying the usual requirements:

$-$ $$\tau(-X) = -\tau(X) \quad ,$$

$\wedge$ $$\tau(X \wedge Y) = \tau(X) \wedge \tau(Y) \quad ,$$

*This part may be skipped without loss of continuity.

$\vee \qquad \tau(X \vee Y) = \tau(X) \vee \tau(Y)$,

$\Rightarrow \qquad \tau(X \Rightarrow Y) = \tau(X) \Rightarrow \tau(Y)$,

so that any assignment of truth values to the Boolean atoms of L determines a unique Boolean valuation. We say that a set Γ of L-formulas is **truth functionally satisfiable** `iff` some Boolean valuation satisfies Γ, and **truth functionally unsatisfiable** otherwise.

Any first order valuation of L is of course a Boolean valuation, but the converse is not necessarily true. However, the following proposition provides sufficient conditions for a Boolean valuation to be a first order valuation:

BV Suppose that τ is a Boolean valuation such that for all L-formulas γ and δ.

(g) If τ satisfies γ, then for every individual symbol μ, τ satisfies $\gamma(\mu)$.

(d) If τ satisfies δ, for some parameter p, τ satisfies $\delta(p)$. Then τ is a first order valuation.

`Proof:` It will suffice to take γ to be a formula $\forall u\ X(u)$, and δ to have the form $\exists u\ X(u)$. To show that τ is a first order valuation, we must show that the converses of (g) and (d) also hold.

So first assume that for every individual symbol μ, τ satisfies $X(\mu)$. Then τ satisfies $\forall u\ X(u)$. For suppose not. Then τ satisfies $-\forall u\ X(u)$ (since τ is a Boolean valuation), and so by (d), for some parameter p, τ satisfies $-X(p)$, contrary to assumption.

Similarly, assume that for some parameter p, τ satisfies $X(p)$. Then τ satisfies $\exists u\ X(u)$. For suppose not. Then τ satisfies $-\exists u\ X(u)$, and so by (g), τ satisfies $-X(\mu)$ for every individual symbol μ, including p, contrary to assumption.■

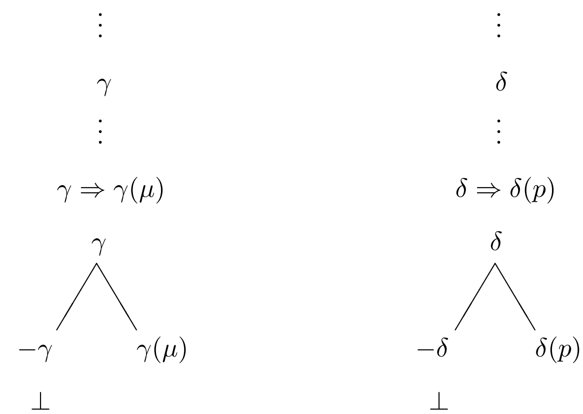
An **associate** R_0 of a finite set Γ_0 of formulas is a finite regular set such that $\Gamma_0 \cup R_0$ is truth functionally unsatisfiable.

We first prove the following lemma:

Lemma Every finite unsatisfiable set Γ_0 has an associate R_0.

`Proof:` By $\mathtt{T}_{UNS}$, let $\mathbf{T}$ be a closed tree constructed from Γ_0. Then R_0 is the set of all formulas of the form $\gamma \Rightarrow \gamma(\mu)$ where γ is the premise and $\gamma(\mu)$ the consequence of an application of the γ-rule in $\mathbf{T}$, and all formulas of the form $\delta \Rightarrow \delta(p)$ where δ is the premise and $\delta(p)$ the consequence of an application of the δ-rule.

To show that R_0 is indeed an associate of Γ_0, we must prove that $\Gamma_0 \cup R_0$ is truth functionally unsatisfiable. To do this, we change **T** to a tree **R** constructed from $\Gamma_0 \cup R_0$. In **T**, for every consequence $\gamma(\mu)$ of a γ-rule with premise γ, insert the formula $\gamma \Rightarrow \gamma(\mu)$ in R_0 immediately above it, and similarly for immediately above every consequence $\delta(p)$ of an application of a δ-rule with premise δ, insert the formula $\delta \Rightarrow \delta(p)$ in R_0. In either case apply the β-rule to the conditional thus inserted, so that we have replaced each application of a γ or δ-rule by an application of a β-rule, as in the following forms:



Then **R** is a closed tree constructed from $\Gamma_0 \cup R_0$ using only the α and β-rules. Since these rules are downward correct for truth-functional satisfiability, no tree constructed from a truth-functionally satisfiable set closes. Therefore, $\Gamma_0 \cup R_0$ is truth functionally unsatisfiable.■

The weak completeness theorem $\mathbf{WCT}^1$ for first order logic is the proposition that every universally valid sentence of L is a theorem of $\texttt{FO}_L$. It is a consequence of the weak completeness theorem $\mathbf{WCT}^0$ for the zero order language with the same nonlogical symbols as L, and says that every tautology of L is a theorem of logic.

Corollary: $\mathbf{WCT}^1$ `is derivable from` $\mathbf{WCT}^0$.

`Proof` : Suppose that X is a universally valid first order formula, so that no first order valuation satisfies $-X$, and let $R_0 = \{Y_1, Y_2, \ldots, Y_n\}$ be an associate of $\{-X\}$. Then $Y_1 \wedge Y_2 \wedge \ldots \wedge Y_n \Rightarrow X$ is a tautology, and so also is,

$$Y_1 \Rightarrow (Y_2 \Rightarrow \ldots \Rightarrow (Y_n \Rightarrow X) \ldots).$$

Then by the weak completeness theorem of *zero order* logic,

$$\vdash Y_1 \Rightarrow (Y_2 \Rightarrow \ldots \Rightarrow (Y_n \Rightarrow X\Big]$$

where we we have written] for) . . .).

We want to show that X is a theorem of first order logic, that is, $\vdash X$ in the first order natural deduction system. Our strategy is to show that in *first order logic*,

(1) If $\vdash Y_1 \Rightarrow (Y_2 \Rightarrow \ldots \Rightarrow (Y_n \Rightarrow X\Big]$, then $\vdash Y_2 \Rightarrow \ldots \Rightarrow Y_n \Rightarrow X]$.

(2) If $\vdash Y_2 \Rightarrow (Y_3 \Rightarrow \ldots \Rightarrow (Y_n \Rightarrow X\Big]$, then $\vdash Y_3 \Rightarrow \ldots \Rightarrow Y_n \Rightarrow X]$.

.

.

.

(n) If $\vdash Y_n \Rightarrow X$, then $\vdash X$.

(n+1) $\vdash X$

where $\{Y_n\}$, $\{Y_n, Y_{n-1}\}$,. . . , $\{Y_n, Y_{n-1}, \ldots, Y_1\} = R_0$ are all regular sets, so that p_n does not occur in the antecedent of Y_n, and if Y_i is $\delta_i \Rightarrow \delta(p_i)$ $(i \leq 2 \leq n)$, then the parameter p_i does not occur in $\{Y_n, \ldots, Y_{i+1}, \delta\}$.

Of course, if Y_1 happens to be $\gamma \Rightarrow \gamma(\mu)$, it is already a theorem of first order logic, so that the passage to,

$$\vdash Y_2 \Rightarrow \ldots \Rightarrow (Y_n \Rightarrow X] \ ,$$

is immediate. On the other hand, if Y_1 is $\delta \Rightarrow \delta(p)$ (where by hypothesis p does not occur in $\{\delta, Y_2, \ldots, Y_n\} = Z_1$), then Y_1 is not a theorem of logic.

So we must prove in general that,

$$\text{If } \vdash (\delta \Rightarrow \delta(p)) \Rightarrow Z, \text{ then } \vdash Z \ ,$$

provided that p does not occur in δ or in Z.

For this it will suffice to show that,

$$\text{if } \vdash (\exists u\ X(u/p) \Rightarrow X) \Rightarrow Z, \text{ then } \vdash Z \ , \tag{7.82}$$

(recall that by definition, p does *not* occur in $X(u/p)$). Indeed, suppose that $\vdash (\exists u\ X(u/p) \Rightarrow X) \Rightarrow Z$. To the end of a proof of,

$$(\exists u\ X(u/p) \Rightarrow X) \Rightarrow Z$$

(which of course has no undischarged assumptions), add a new hypothesis $-\exists u\ X(u/p)$. Then by zero order logic `PMI` (page **??**), we have

$\exists u\ X(u/p) \Rightarrow X$, from which Z follows by MP (page 41). So by CP (page 41),

$$\vdash\ -\exists u\ X(u/p) \Rightarrow Z\ . \tag{7.83}$$

Now take X rather than $-\exists u\ X(u/p)$ as a hypothesis. Then by CP, $\exists u\ X(u/p) \Rightarrow X$ follows, and again we infer Z, so that by CP (page 41) (discharging X), we have $\vdash X \Rightarrow Z$, so that $-Z \vdash -X$. Because p does not occur in Z, by UG (page **??**) we have $-Z \vdash \forall u\ -X(u/p)$, and by CP, $\vdash\ -Z \Rightarrow \forall u\ -X(u/p)$. Then by contraposition and the equivalence of $\forall u\ X(u/p)$ to $-\exists u\ -X(u/p)$,

$$\vdash\ \exists u\ X(u/p) \Rightarrow Z\ . \tag{7.84}$$

From equation (7.83) and (7.84), it follows at once (by SC (page **??**) and the law of the excluded middle) that $\vdash\ Z$. Thus by application of steps (1)-$(n+1)$ above (page 202) we deduce from the fact that in zero order logic $R_0 \vdash\ X$, the statement that $\vdash\ X$ in first order logic. Thus from the weak completeness theorem for *zero order logic*, we derive the weak completeness theorem for *first order logic*.■

The completeness theorem for first order logic is immediate from the weak completeness and compactness theorems for first order logic. We can also deduce the compactness theorem for first order logic, along with the Löwenheim-Skolem theorem, from the compactness theorem for *zero order* logic.

We do this by "magic". Using Smullyan's terminology[5], M is a **magic set** `iff` it is an infinite regular set, consisting of all L-formulas of the form $\gamma \Rightarrow \gamma(\mu)$ and for each δ-formula of L, a formula of the form $\delta \Rightarrow \delta(p)$.

MC: `We may construct a magic set` M `in the following way:`

`Proof:` First let G be the set of all L-formulas of the form $\gamma \Rightarrow \gamma(\mu)$. Now let $\mathbf{b} = b_1, b_2, \ldots$ be the sequence of all parameters of L (recall that there are denumerably many) and let $\mathbf{d} = \delta_1, \delta_2, \ldots$ be the sequence of all δ-formulas of L. We construct a sequence $\mathbf{d}^{\Rightarrow}$ of formulas of the form $\delta \Rightarrow \delta(p)$ in the following way: Let p_1 be the first parameter in the sequence b which does not occur in δ_1. Then the first term in $d^{\Rightarrow}$ is $\delta_1 \Rightarrow \delta_1(p_1)$. Next, let p_2 be the first parameter in b which occurs neither in $\delta_1 \Rightarrow \delta_1(p_1)$ nor in

[5]Smullyan's terminology (in Smullyan (1968)[85]) reflects his interest in magic; he was an accomplished amateur magician.

But we depart from Smullyan and reverse his order of definition: while he first defines a magic set to have certain "magic" properties, and later pulls the rabbit out of the hat, we produce the rabbit first and then show that it is a rabbit.

This may take the "magic" out of magic sets, but then they're not really *that* magic: in one way or other, something like magic sets appear, explicitly or not, in most modern "Henkin style" first order completeness and compactness proofs.

But the properties of "magic" sets are often taken almost for granted, and are rarely discussed as carefully as Smullyan does, and we indebted to him for this discussion of the subject.

δ_2. The second member of $d^{\Rightarrow}$ is then $\delta_2 \Rightarrow \delta_2(p_2)$. And so on. Then $d^{\Rightarrow}$ is,

$$\delta_1 \Rightarrow \delta_1(p_1), \quad \delta_2 \Rightarrow \delta_2(p_2), \quad \ldots$$

Then let D be the set of all terms of $d^{\Rightarrow}$, and let $M = G \cup D$, and M is a magic set as promised.■

M `Magic sets have two important properties:`

M_1 `Every Boolean valuation of a magic set` M `which satisfies` M `is a first order valuation.`

M_2 `Let` Γ_0 `be a finite set of sentences and` M_0 `a finite subset of a magic set` M. `If` Γ_0 `is first order satisfiable, so is` $\Gamma_0 \cup M_0$.

`Proof` : To show that M_1 holds, suppose that τ is a Boolean valuation which satisfies $M = G \cup D$. We use **BV** to prove that τ is a first order valuation, by showing that τ satisfies the hypotheses (`g`) and (`d`) of **BV**.

First suppose that τ satisfies γ. Because τ satisfies the formula $\gamma \Rightarrow \gamma(\mu)$, since it is already in G, τ satisfies $\gamma(\mu)$ for every individual symbol μ (because τ is a Boolean valuation). Thus if τ satisfies γ, then for every individual symbol μ, τ satisfies $\gamma(\mu)$, which is (`g`).

As for (`d`), let τ satisfy δ. Since there is a parameter p such that $\delta \Rightarrow \delta(p)$ is in D, τ satisfies $\delta \Rightarrow \delta(p)$ and so also satisfies $\delta(p)$ for some parameter p (since τ is Boolean).

M_2 is an immediate consequence of **REG**, given that Γ_0 is a set of *sentences* and thus parameter-free, and M_0 is regular since M is regular.■

An immediate consequence of M_1 and M_2 is the following proposition:

SAT `Let` Γ `be a truth functionally satisfiable set of sentences which contains a magic set` M. `Then` Γ `is first order satisfiable in a countable domain.`

`Proof` : Let τ be a Boolean valuation which satisfies Γ. Then τ also satisfies M. So by M_1, τ is a first order valuation which satisfies Γ. Since L has denumerably many parameters, there is a model of Γ which determines τ in which each member of its domain D is named by a parameter, so D is countable.■

We next derive the compactness theorem and the Löwenheim-Skolem theorem for first order logic from the compactness theorem for *zero order* logic.

Corollary 1: `The first order compactness theorem is derivable from the zero order compactness theorem.`

`Proof(Smullyan)` : Let Γ be a set of sentences, every finite subset of which is satisfiable. We must show that Γ is satisfiable.

Suppose the M is a magic set, and that M_0 and Γ_0 are finite subsets of M and Γ, respectively. Then by M_2, $M_0 \cup \Gamma_0$, which is an arbitrary finite subset of $M \cup \Gamma$, is satisfiable. Thus every finite subset of $M \cup \Gamma$ is satisfiable, and so also truth functionally satisfiable. Therefore by the compactness theorem for *zero order logic*, $M \cup \Gamma$ is *truth functionally* satisfiable, and so by M_1, is first-order satisfiable.■

Corollary 2: `The Löwenheim-Skolem theorem is derivable from the zero order compactness theorem.`

`Proof` : By the proof of Corollary 1, since $M \cup \Gamma$ is first order satisfiable, it follows that by **SAT**, Γ has countable model.■