Hamilton - Logic for Mathematicians
Notes and Solutions

Contents

1 Informal statement calculus **4**
- 1.1 Statements and connectives . . . 4
- 1.2 Truth functions and truth tables . . . 4
- 1.3 Rules for manipulation and substitution . . . 5
- 1.4 Normal forms . . . 11
- 1.5 Adequate sets of connectives . . . 14
- 1.6 Arguments and validity . . . 17

2 Formal statement calculus **19**
- 2.1 The formal system L . . . 19
- 2.2 The Adequacy Theorem for L . . . 26

3 Informal predicate calculus **32**
- 3.1 Predicates and sequences . . . 32
- 3.2 First order languages . . . 33
- 3.3 Interpretations . . . 37
- 3.4 Satisfaction, truth . . . 38

4 Formal predicate calculus **50**
- 4.1 The formal system $K_{\mathscr{L}}$ . . . 50
- 4.2 Equivalence, substitution . . . 59
- 4.3 Prenex Form . . . 64
- 4.4 The Adequacy Theorem for K . . . 72
- 4.5 Models . . . 80

5 Mathematical systems **85**
- 5.1 Introduction . . . 85
- 5.2 First order systems with equality . . . 85
- 5.3 The theory of groups . . . 94
- 5.4 First order arithmetic . . . 99
- 5.5 Formal set theory . . . 100
- 5.6 Consistency and models . . . 102

6 The Gödel Incompleteness Theorem **103**

7 Computability, unsolvability, undecidability **104**

A Additional propositions **105**

B Additional exercises **107**
B.1 Informal statement calculus 107
B.2 Formal statement calculus 107
B.3 Informal predicate calculus 107
B.4 Formal predicate calculus 107

Chapter 1

Informal statement calculus

1.1 Statements and connectives

Solutions to exercises

1. (a) $(D \wedge P) \to T$
   (b) $J \to E$
   (c) $\sim J \to ((S \vee R) \wedge \sim E)$
   (d) $(X \wedge Y) \to \sim Z$
   (e) $M \vee H$
   (f) $(\sim M) \to H$
   (g) $S \leftrightarrow (E \vee O)$
   (h) $X \to (Y \to \sim Z)$

2. (a) The statements (a) and (d) have the same form.
   (b) The statements (d) and (h) have the same meaning ((a) also has the same form as (d), so it could also be interpreted as having the same meaning). The statements (e) and (f) have the same meaning.

1.2 Truth functions and truth tables

Note. For readability of truth tables, the value 1 will be used for T and the value 0 will be used for F. The final operation to be evaluated, which indicates the truth value of the final statement form, will be underlined.

Solutions to exercises

3. Because truth tables are tedious to write, only (a) has been done. The rest are done similarly.

   (a) Observe the truth table below.

$((\sim$	$p)$	$\underline{\wedge}$	$(\sim$	$q))$
0	1	0	0	1
0	1	0	1	0
1	0	0	0	1
1	0	1	1	0

4. When p and q take on particular values, the values of $((\sim p) \vee q)$ and $(p \rightarrow q)$ are identical. This can be shown by constructing truth tables, but that process is omitted here. Similarly, $((\sim p) \rightarrow (q \vee r))$ can be shown to give rise to the same truth function as $((\sim q) \rightarrow ((\sim r) \rightarrow p))$ by constructing truth tables.

5. The statement forms (a), (b), and (d) are tautologies.

6. Because truth tables are tedious to write, only (a) has been done. The rest are done similarly.

   (a) The truth table for $(p \rightarrow q)$ is seen below.

$(p$	$\underline{\rightarrow}$	$q)$
1	1	1
1	0	0
0	1	1
0	1	0

   The truth table for $((\sim q) \rightarrow (\sim p))$ is seen below.

$((\sim$	$q)$	$\underline{\rightarrow}$	$(\sim$	$p))$
0	1	1	0	1
0	1	1	1	0
1	0	0	0	1
1	0	1	1	0

   Notice that when p and q take on the same values in both truth tables, the values underneath the underlined $\rightarrow$, which indicate the final operation to be evaluated, and therefore the truth value of the statement form, are identical. Therefore, the two statement forms are logically equivalent.

7. When p and q are both true, the value $(((\sim p) \rightarrow q) \rightarrow (p \rightarrow (\sim q)))$ is false, so the statement form is not a tautology.

   Let $\mathscr{A} = \mathscr{B} = (p \rightarrow p)$. Notice that this is a tautology, and for that matter, any tautology can be substituted here. The value of $(((\sim \mathscr{A}) \rightarrow \mathscr{B}) \rightarrow (\mathscr{A} \rightarrow (\sim \mathscr{B})))$ can then be seen to be a contradiction by constructing the appropriate truth table or in the same way that the above statement form was seen to be false.

1.3 Rules for manipulation and substitution

Proposition 1.10. If $\mathscr{A}$ and $(\mathscr{A} \rightarrow \mathscr{B})$ are tautologies, then $\mathscr{B}$ is a tautology.

Proof. Suppose for a contradiction that $\mathscr{A}$ and $(\mathscr{A} \to \mathscr{B})$ are tautologies, while $\mathscr{B}$ is not a tautology. Then there is an assignment of truth values to the statement variables of $\mathscr{B}$ such that $\mathscr{B}$ is given the value F, while $\mathscr{A}$, being a tautology is necessarily given the value T. But then $(\mathscr{A} \to \mathscr{B})$ must have the value F, which contradicts it being a tautology. □

Proposition 1.11. Let $\mathscr{A}$ be the statement form in which the statement variables $p_1, p_2, \ldots, p_n$ appear, and let $\mathscr{A}_1, \mathscr{A}_2, \ldots, \mathscr{A}_n$ be any statement forms. If $\mathscr{A}$ is a tautology, then $\mathscr{B}$, the statement form obtained by replacing p_i in $\mathscr{A}$ with $\mathscr{A}_i$, is also a tautology.

Proof. By definition of $\mathscr{B}$, any assignment of truth values to $\mathscr{A}_1, \mathscr{A}_2, \ldots, \mathscr{A}_n$ in $\mathscr{B}$, would result in the same truth value of $\mathscr{A}$ if the same truth values had been assigned to $p_1, p_2, \ldots, p_n$. The truth value of $\mathscr{A}$ is T, and so the truth value of $\mathscr{B}$ must also be T, making it a tautology as well. □

Note. This proof is not entirely rigorous. See the note in Proposition 1.15.
Note. It is important to note that if $\mathscr{A}$ is not a tautology, then $\mathscr{B}$ may not be an equivalent truth function (see Exercise 7). However, if $\mathscr{A}$ is a contradiction, then $\mathscr{B}$ must be a contradiction, and the proof of this is nearly identical.

Proposition 1.12. For any statement forms $\mathscr{A}$ and $\mathscr{B}$, $(\sim (\mathscr{A} \wedge \mathscr{B}))$ is logically equivalent to $((\sim \mathscr{A}) \vee (\sim \mathscr{B}))$, and $(\sim (\mathscr{A} \vee \mathscr{B}))$ is logically equivalent to $((\sim \mathscr{A}) \wedge (\sim \mathscr{B}))$.

Proof. By Example 1.8 in the book or by creating tables, it can be easily seen that

$$(\sim (p \wedge q)) \leftrightarrow ((\sim p) \vee (\sim a)), \text{ and } (\sim (p \vee q)) \leftrightarrow ((\sim p) \wedge (\sim q))$$

is a tautology. By application of Proposition 1.11, we may conclude that if any statement form with p and q substituted for the statement forms $\mathscr{A}$ and $\mathscr{B}$ would be a tautology as well, i.e.,

$$(\sim (\mathscr{A} \wedge \mathscr{B})) \leftrightarrow ((\sim \mathscr{A}) \vee (\sim \mathscr{B})), \text{ and } (\sim (\mathscr{A} \vee \mathscr{B})) \leftrightarrow ((\sim \mathscr{A}) \wedge (\sim \mathscr{A}))$$

is a tautology, and therefore $(\sim (\mathscr{A} \wedge \mathscr{B}))$ is logically equivalent to $((\sim \mathscr{A}) \vee (\sim \mathscr{B}))$, and $(\sim (\mathscr{A} \vee \mathscr{B}))$ is logically equivalent to $((\sim \mathscr{A}) \wedge (\sim \mathscr{B}))$. □

Proposition 1.14. Let $\mathscr{A}$ and $\mathscr{B}$ be logically equivalent statement forms. Let $\mathscr{A}'$ be a statement form in which $\mathscr{A}$ appears. Let $\mathscr{B}'$ be the statement form in which every instance of $\mathscr{A}$ is replaced by $\mathscr{A}'$. The statement forms $\mathscr{A}'$ and $\mathscr{B}'$ are logically equivalent.

Proof. We wish to show that $\mathscr{A}' \leftrightarrow \mathscr{B}'$ is a tautology, which is done by showing that the truth values of $\mathscr{A}'$ and $\mathscr{B}'$ always match under some arbitrary assignment of truth values to any statement variables. Consider the truth value of $\mathscr{A}'$ under some assignment of truth values. The truth value of $\mathscr{B}'$ must be the same, since it differs only in having $\mathscr{B}$ in place of $\mathscr{A}$, and $\mathscr{A}$ and $\mathscr{B}$ are logically equivalent. Therefore, $\mathscr{A}' \leftrightarrow \mathscr{B}$ must be a tautology, and so $\mathscr{A}'$ and $\mathscr{B}'$ must be logically equivalent. □

Note. This proof is not entirely rigorous. See the note in Proposition 1.15.

For the remainder of Chapter 1, a statement form involving only the connectives $\sim$, $\wedge$ and $\vee$ will be called a *restricted statement form*.

Proposition 1.15. Let $\mathscr{A}$ be a restricted form and let $\mathscr{A}'$ be the statement form obtained from $\mathscr{A}$ by interchanging $\wedge$ and $\vee$ and replacing every statement variable p by $(\sim p)$. The statement forms $\mathscr{A}$ and $\mathscr{A}'$ are logically equivalent.

Proof. The proof is by strong induction on n, the number of connectives which appear in $\mathscr{A}$.

(base case) It may be the case that $n = 0$, i.e., $\mathscr{A}$ has no connectives, so $\mathscr{A}$ is p, where p is any statement variable. Then $\mathscr{A}'$ must be $(\sim p)$, which is logically equivalent to $(\sim \mathscr{A})$.

(inductive step) It may be the case that $n > 0$, i.e., $\mathscr{A}$ has one or more connectives. Suppose as an inductive hypothesis that any restricted statement form with fewer than n connectives is equivalent to the statement form obtained by interchanging $\wedge$ and $\vee$ and replacing each statement variable by its negation. Since $\mathscr{A}$ has one or more connectives, there are three cases to consider, based on the final connective in $\mathscr{A}$ to be evaluated.

1. It may be that $\mathscr{A}$ has the form $(\sim \mathscr{B})$, in which case $\mathscr{A}'$ must be $(\sim \mathscr{B}')$, since the only instances of $\wedge$, $\vee$, and any statement variables must necessarily appear in $\mathscr{B}$. By the inductive hypothesis, since $\mathscr{B}$ has fewer than n connectives, $\mathscr{B}'$ is logically equivalent to $(\sim \mathscr{B})$. By Proposition 1.14, $(\sim \mathscr{B}')$ must be logically equivalent to $(\sim (\sim \mathscr{B}))$ which is $(\sim \mathscr{A})$. Since $(\sim \mathscr{B}')$ is $\mathscr{A}'$, we have proved that $\mathscr{A}'$ is logically equivalent to $(\sim \mathscr{A})$, as desired.

2. It may be that $\mathscr{A}$ has the form $(\mathscr{B} \vee \mathscr{C})$. Then $\mathscr{A}'$ must be $(\mathscr{B}' \wedge \mathscr{C}')$. By the induction hypothesis, $\mathscr{B}'$, which must have fewer than n connectives, is logically equivalent to $(\sim \mathscr{B})$. By proposition 1.14, $(\mathscr{B}' \wedge \mathscr{C}')$ must be logically equivalent to $((\sim \mathscr{B}) \wedge \mathscr{C}')$, which must again be equivalent to $((\sim \mathscr{B}) \wedge (\sim \mathscr{C}))$ by the same reasoning applied to $\mathscr{C}'$, which must finally be equivalent to $(\sim (\mathscr{B} \vee \mathscr{C}))$ by Proposition 1.11, and this final statement form is $(\sim \mathscr{A})$, as desired.

3. It may be that $\mathscr{A}$ has the form $(\mathscr{B} \wedge \mathscr{C})$. Then $\mathscr{A}'$ must be $(\mathscr{B}' \vee \mathscr{C}')$. By the induction hypothesis, $\mathscr{B}'$, which must have fewer than n connectives, is logically equivalent to $(\sim \mathscr{B})$. By proposition 1.14, $(\mathscr{B}' \vee \mathscr{C}')$ must be logically equivalent to $((\sim \mathscr{B}) \vee \mathscr{C}')$, which must again be equivalent to $((\sim \mathscr{B}) \vee (\sim \mathscr{C}))$ by the same reasoning applied to $\mathscr{C}'$, which must finally be equivalent to $(\sim (\mathscr{B} \wedge \mathscr{C}))$ by Proposition 1.11, and this final statement form is $(\sim \mathscr{A})$, as desired.

Verifying the desired property for all three cases finishes the inductive step, thereby concluding the induction and the proof. □

Note. Whenever induction appears in the textbook, it is referring to strong induction. The general framework for induction seen in this proof will resemble all other inductive proofs seen throughout the manual. Strictly speaking, strong induction has no base case, but practically speaking, there are usually one or more special values of the number being inducted on which require special attention since they do not rely on the inductive hypothesis. These will be referred to as the base cases.
Note. The proofs of Proposition 1.14 and Proposition 1.10 could have been made rigorous by being done similarly, but an inductive proof would have been unnecessarily lengthy to prove the propositions, which were obvious.

Corollary 1.16. Let $p_1, p_2, \ldots, p_n$ be statement variables.

(i) The statement forms

$$(\sim (p_1 \wedge p_2 \wedge \cdots \wedge p_n)) \text{ and } ((\sim p_1) \vee (\sim p_2) \vee \cdots \vee (\sim p_n))$$

are logically equivalent.

(ii) The statement forms

$$(\sim (p_1 \vee p_2 \vee \cdots \vee p_n)) \text{ and } ((\sim p_1) \wedge (\sim p_2) \wedge \cdots \wedge (\sim p_n))$$

are logically equivalent.

Proof. For (i), let $\mathscr{A}$ be the statement form

$$(p_1 \wedge p_2 \wedge \cdots \wedge p_n).$$

Then interchanging $\wedge$ and $\vee$ and negating each statement variable results in

$$((\sim p_1) \vee (\sim p_2) \vee \cdots \vee (\sim p_n)).$$

By Proposition 1.15, this is equivalent to $(\sim \mathscr{A})$, which is

$$(\sim (p_1 \wedge p_2 \wedge \cdots \wedge p_n)),$$

as desired. Part (ii) is proved in the same way as (i). □

Proposition 1.17 (De Morgan's Laws)**.** Let $\mathscr{A}_1, \mathscr{A}_2, \ldots, \mathscr{A}_n$ be statement forms.

(i) The statement forms

$$(\sim (\mathscr{A}_1 \wedge \mathscr{A}_2 \wedge \cdots \wedge \mathscr{A}_n)) \text{ and } ((\sim \mathscr{A}_1) \vee (\sim \mathscr{A}_2) \vee \cdots \vee (\sim \mathscr{A}_n))$$

are logically equivalent.

(ii) The statement forms

$$(\sim (\mathscr{A}_1 \vee \mathscr{A}_2 \vee \cdots \vee \mathscr{A}_n)) \text{ and } ((\sim \mathscr{A}_1) \wedge (\sim \mathscr{A}_2) \wedge \cdots \wedge (\sim \mathscr{A}_n))$$

are logically equivalent.

Proof. This is an application of Proposition 1.10 to Corollary 1.16. □

Solutions to exercises

8. Since (a) - (d) are proved in the same way, only (a) will be done, and the rest will be omitted.

   (a) Let p, q, r be statement letters. The following truth table demonstrates that $((p \vee (q \vee r)) \leftrightarrow ((p \vee q) \vee r))$ is a tautology.

$((p$	$\vee$	$(q$	$\vee$	$r))$	$\underline{\leftrightarrow}$	$((p$	$\vee$	$q)$	$\vee$	$r))$
1	1	1	1	1	1	1	1	1	1	1
1	1	1	1	0	1	1	1	1	1	0
1	1	0	1	1	1	1	1	0	1	1
1	1	0	0	0	1	1	1	0	1	0
0	1	1	1	1	1	0	1	1	1	1
0	1	1	1	0	1	0	1	1	1	0
0	1	0	1	1	1	0	0	0	1	1
0	0	0	0	0	1	0	0	0	0	0

By proposition 1.10, the statement form $((\mathscr{A} \vee (\mathscr{B} \vee \mathscr{C})) \leftrightarrow ((\mathscr{A} \vee \mathscr{B}) \vee \mathscr{C}))$ is a tautology, where $\mathscr{A}, \mathscr{B}, \mathscr{C}$ are any statement forms. Therefore, $((\mathscr{A} \vee (\mathscr{B} \vee \mathscr{C}))$ is logically equivalent to $((\mathscr{A} \vee \mathscr{B}) \vee \mathscr{C}))$.

9. (a) The statement form $((p \wedge q) \to p)$ can be seen to be a tautology by creating a truth table for it. By Proposition 1.10, $((\mathscr{A} \wedge \mathscr{B}) \to \mathscr{A})$ must be a tautology as well.

   (b) The statement form $((p \wedge q) \to q)$ can be seen to be a tautology by creating a truth table for it. By Proposition 1.10, $((\mathscr{A} \wedge \mathscr{B}) \to \mathscr{B})$ must be a tautology as well.

10. By part (a) of Example 1.4 in the book, it can be seen that $((\sim p) \vee q)$ is logically equivalent to $(p \to q)$, and so $(((\sim p) \vee q) \to (p \to q))$ is a tautology. By Proposition 1.10, for any statements forms $\mathscr{A}$ and $\mathscr{B}$, $(((\sim \mathscr{A}) \vee \mathscr{B}) \to (\mathscr{A} \to \mathscr{B}))$ must be a tautology as well, and so $(((\sim \mathscr{A}) \vee \mathscr{B})$ and $(\mathscr{A} \to \mathscr{B}))$ must be logically equivalent. This equivalence will be referred to as $(\star)$.

    Therefore, the following statement forms must be equivalent by the substitution on the right and Proposition 1.14. Note that $\mathscr{C} \equiv \mathscr{D}$ indicates that the statement forms $\mathscr{C}$ and $\mathscr{D}$ are logically equivalent.

$$\begin{array}{rr}
((p \to q) \to r) & \\
((\sim (p \to q)) \vee r) & ((p \to q) \to r) \equiv ((\sim (p \to q)) \vee r), \text{ by } (\star) \\
((\sim ((\sim p) \vee q)) \vee r) & (p \to q) \equiv ((\sim p) \vee q), \text{ by } (\star)
\end{array}$$

11. Let $\mathscr{A}, \mathscr{B}, \mathscr{C}$ be statement forms. The following equivalences will be used.

    (i) $(\mathscr{A} \vee \mathscr{B})$ is logically equivalent to $(\mathscr{B} \vee \mathscr{A})$.

    (ii) $(\mathscr{A} \to \mathscr{B})$ is logically equivalent to $((\sim \mathscr{A}) \vee \mathscr{B})$.

    (iii) $(\sim (\sim \mathscr{A}))$ is logically equivalent to $\mathscr{A}$.

    (iv) $(\mathscr{A} \to \mathscr{B})$ is logically equivalent to $((\sim \mathscr{B}) \to (\sim \mathscr{A}))$.

    (v) $(\mathscr{A} \vee \mathscr{A})$ is logically equivalent to $\mathscr{A}$.

    In the sub-exercises, successive statement forms are equivalent by substitution via Proposition 1.14 of an equivalent statement form indicated by the braces. The column on the right justifies the equivalence of substituted statement forms.

    (a) The statement form $((\sim (p \vee (\sim q))) \to (q \to r))$ is equivalent to:

$$\begin{array}{rc}
((\sim \underbrace{((\sim q) \vee p)}) \to (q \to r)) & \text{(i)} \\
((\sim \underbrace{(q \to p)}) \to (q \to r)) & \text{(ii)} \\
((\sim (q \to p)) \to \underbrace{((\sim q) \vee r)}) & \text{(ii)}
\end{array}$$

(b) The statement form $((\sim (p \vee (\sim q))) \to (q \to r))$ is equivalent to:

$$
\begin{aligned}
(\underbrace{((\sim p) \wedge (\sim (\sim q)))} \to (q \to r)) &\qquad \text{Proposition 1.17} \\
(((\sim p) \wedge \underbrace{\ q\ }) \to (q \to r)) &\qquad \text{(iii)} \\
(((\sim p) \wedge q) \to \underbrace{((\sim q) \vee r)}) &\qquad \text{(ii)} \\
(((\sim p) \wedge q) \to \underbrace{(\sim (\sim ((\sim q) \vee r)))}) &\qquad \text{(iii)} \\
(((\sim p) \wedge q) \to (\sim \underbrace{((\sim (\sim q)) \wedge (\sim r))})) &\qquad \text{Proposition 1.17} \\
(((\sim p) \wedge q) \to (\sim (\underbrace{\ q\ } \wedge (\sim r)))) &\qquad \text{(iii)}
\end{aligned}
$$

(c) The statement form $((\sim (p \vee (\sim q))) \to (q \to r))$ is equivalent to:

$$
\begin{aligned}
\underbrace{((\sim (q \to r)) \to (\sim (\sim (p \vee (\sim q)))))} &\qquad \text{(iv)} \\
((\sim (q \to r)) \to \underbrace{(p \vee (\sim q))}) &\qquad \text{(iii)} \\
((\sim (q \to r)) \to \underbrace{((\sim q) \vee p)}) &\qquad \text{(i)} \\
((\sim (q \to r)) \to \underbrace{(q \to p)}) &\qquad \text{(ii)} \\
((\sim \underbrace{((\sim q) \vee r)}) \to (q \to p)) &\qquad \text{(ii)}
\end{aligned}
$$

(d) The statement form $((\sim (p \vee (\sim q))) \rightarrow (q \rightarrow r))$ is equivalent to:

$$\underbrace{((\sim ((\sim q) \vee r)) \rightarrow (q \rightarrow p))} \qquad \text{Exercise 11, part (c)}$$

$$(\underbrace{((\sim (\sim q)) \wedge (\sim r))} \rightarrow (q \rightarrow p)) \qquad \text{Proposition 1.17}$$

$$((\underbrace{q} \wedge (\sim r)) \rightarrow (q \rightarrow p)) \qquad \text{(iii)}$$

$$\underbrace{((\sim (q \wedge (\sim r))) \vee (q \rightarrow p))} \qquad \text{(ii)}$$

$$(\underbrace{((\sim q) \vee (\sim (\sim r)))} \vee (q \rightarrow p)) \qquad \text{Proposition 1.17}$$

$$(((\sim q) \vee \underbrace{r}) \vee (q \rightarrow p)) \qquad \text{(iii)}$$

$$(((\sim q) \vee r) \vee \underbrace{((\sim q) \vee p)}) \qquad \text{(ii)}$$

$$(\underbrace{(r \vee (\sim q))} \vee ((\sim q) \vee p)) \qquad \text{(i)}$$

$$\underbrace{(((\sim q) \vee (\sim q)) \vee (p \vee r)))} \qquad \text{associativity and commutativity of } \vee$$

$$(\underbrace{(\sim q)} \vee (p \vee r)) \qquad \text{(v)}$$

$$(q \rightarrow (p \vee r)) \qquad \text{(ii)}$$

Note. In (d), a few tedious steps were skipped when invoking the associativity and commutativity of $\vee$. An inductive proof could be used to prove that any parenthesization of $\mathscr{A}_1 \vee \mathscr{A}_2 \vee \ldots \mathscr{A}_n$ is equivalent to $\mathscr{A}_1 \vee \mathscr{A}_2 \vee \ldots \mathscr{A}_n$ to make the proof more rigorous, but it is more pedantic than necessary.

1.4 Normal forms

Proposition 1.18. Every statement form is equivalent to a restricted statement form.

Proof. Let $\mathscr{A}$ be a statement form in which the statement variables $p_1, \ldots, p_n$ occur. It may be the case that $\mathscr{A}$ is a contradiction, in which case $\mathscr{A}$ is equivalent to

$$((p_1 \wedge (\sim p_1)) \wedge p_2 \wedge \cdots \wedge p_n),$$

a statement form with n statement variables which is a contradiction.

Now if $\mathscr{A}$ is not a contradiction, then consider the 2^n possible assignments of truth values to the statement variables. For each assignment indexed by k, let Q_k be the statement form defined by

$$q_1 \wedge \cdots \wedge q_n,$$

where each q_i is defined as p_i if p_i is true under the particular assignment or $(\sim p_i)$ if p_i is false under the particular assignment.

Notice that, by construction, Q_k is true under the kth assignment. Consider a different assignment of truth values to $p_1, \ldots, p_n$. Then it must assign some statement variable, say p_i, a different truth value. Therefore, by construction, q_i must be either

$(\sim p_i)$ if p_i is true or p_i if p_i is false. In either case q_i be false, and so Q_k must be false under the assignment which is not the kth one.

Therefore, Q_k is true if and only if the assignment of statement variables is the kth one. In other words, there is a one-to-one correspondence between each Q_i and each assignment of truth values to the statement variables.

So let $\{R_1, R_2, \ldots, R_j\}$ be a set such that each element is a distinct Q_i that corresponds to an assignment of truth values which makes $\mathscr{A}$ true. Notice that $\mathscr{A}$ was assumed to not be a contradiction, so the set exists. Consider the statement form $R_1 \vee \cdots \vee R_j$. By construction, it is a restricted statement form and is true only when $\mathscr{A}$ is true, i.e., it is logically equivalent to $\mathscr{A}$, as desired. $\square$

Note. This proposition is slightly different in meaning from the textbook.

A statement form of the form $P_1 \vee \cdots \vee P_n$, where each P_i is $(p_1 \wedge \cdots \wedge p_j)$ for statement variables $p_i, \ldots, p_j$ is said to be in *disjunctive normal form*.

A statement form of the form $P_1 \wedge \cdots \wedge P_n$, where each P_i is $(p_1 \vee \cdots \vee p_j)$ for statement variables $p_i, \ldots, p_j$ is said to be in *conjunctive normal form*.

Note. These definitions are slightly more general than the ones in the textbook. Here, every P_i need not be of a fixed length.

Corollary 1.20. Every statement form which is not a contradiction is equivalent to a statement form in disjunctive normal form.

Proof. Let $\mathscr{A}$ be a statement form. The constructed statement form in Proposition 1.18 is in disjunctive normal form and logically equivalent to $\mathscr{A}$. Therefore, $\mathscr{A}$ is equivalent to a statement form in disjunctive normal form. $\square$

Note. By the definition used in this manual, we need not restrict the statement form to not be a contradiction.

Corollary 1.21. Every statement form which is not a tautology is equivalent to a statement form in conjunctive normal form.

Proof. Let $\mathscr{A}$ be a statement form which is not a tautology in which the statement variables $p_1, \ldots, p_n$ appear. Then $(\sim \mathscr{A})$ is not a contradiction, so it is equivalent to a statement form Q which has the form $(Q_1 \vee \cdots \vee Q_k)$, where each Q_i is of the form $q_1 \wedge \cdots \wedge q_n$, where each q_j is either p_j or $(\sim p_j)$. By Proposition 1.17, $(\sim Q)$ must be

$$((\sim q_1) \wedge \cdots \wedge (\sim q_n))$$

which is logically equivalent to $(\sim (\sim \mathscr{A}))$, which is logically equivalent to $\mathscr{A}$. Now replacing each $(\sim (\sim p_i))$ occurring in $(\sim Q)$ with p_i using Proposition 1.14 yields a statement form in conjunctive normal form which is equivalent to $\mathscr{A}$, as desired. $\square$

Note. By the definition used in this manual, we need not restrict the statement form to not be a tautology.

Solutions to exercises

12. (a) First we find all assignments of truth values such that $(p \leftrightarrow q)$ is true. The only assignments are when p and q are both assigned the value T or both assigned the value F. So continuing in the way described in Proposition 1.18, we see that the statement form

$$(p \wedge q) \vee ((\sim p) \wedge (\sim q))$$

is in disjunctive normal form and logically equivalent to $(p \leftrightarrow q)$.

The remaining sub-exercises are done in the same way.

(b) The statement form

$$\begin{array}{ccccc} (p \wedge q \wedge r) & & & & \vee \\ (p \wedge (\sim q) \wedge r) & \vee & (p \wedge (\sim q) \wedge (\sim r)) & & \vee \\ ((\sim p) \wedge q \wedge r) & \vee & ((\sim p) \wedge q \wedge (\sim r)) & & \vee \\ ((\sim p) \wedge (\sim q) \wedge r) & \vee & ((\sim p) \wedge (\sim q) \wedge (\sim r)) & & \end{array}$$

in disjunctive normal form is logically equivalent to $(p \rightarrow ((\sim q) \vee r))$.

(c) The statement form $((p \wedge q) \vee ((\sim q) \leftrightarrow r))$ is logically equivalent to

$$((\sim p)\wedge(\sim q)\wedge r)\vee((\sim p)\wedge q\wedge(\sim r))\vee(p\wedge(\sim q)\wedge r)\vee(p\wedge q\wedge(\sim r)\vee(p\wedge q\wedge r)),$$

which is in disjunctive normal form.

(d) The statement form $\sim ((p \rightarrow (\sim q)) \rightarrow r)$ is logically equivalent to

$$(((\sim p) \wedge (\sim q) \wedge (\sim r)) \vee (p \wedge (\sim q) \wedge r) \vee (p \wedge (\sim q) \wedge (\sim r))),$$

which is in disjunctive normal form.

(e) The statement form $(((p \rightarrow q) \rightarrow r) \rightarrow s)$ is logically equivalent to

$$\begin{array}{cc} ((\sim p) \wedge (\sim q) \wedge (\sim r) \wedge (\sim s)) & \vee \\ ((\sim p) \wedge (\sim q) \wedge (\sim r) \wedge s) & \vee \\ (p \wedge q \wedge (\sim r) \wedge (\sim s)) & \vee \\ (p \wedge q \wedge (\sim r) \wedge s) & \vee \\ ((\sim p) \wedge q \wedge (\sim r) \wedge s) & \vee \\ ((\sim p) \wedge q \wedge r \wedge s) & \vee \\ ((\sim p) \wedge q \wedge r \wedge (\sim s)) & \vee \\ (p \wedge (\sim q) \wedge r \wedge s) & \vee \\ (p \wedge q \wedge (\sim r) \wedge (\sim s)) & \vee \\ (p \wedge q \wedge (\sim r) \wedge s) & \vee \\ (p \wedge q \wedge r \wedge s) & \end{array}$$

which is in disjunctive normal form.

13. (a) We first negate the statement form to obtain $\sim (((\sim p) \vee q) \rightarrow r)$, and by using the method used in the previous exercise, we find that the statement form

$$(((\sim p) \wedge (\sim q) \wedge (\sim r)) \vee ((\sim p) \wedge q \wedge (\sim r)) \vee (p \wedge q \wedge (\sim r)))$$

is in disjunctive normal form and is logically equivalent. By Proposition 1.17, we negate the above statement form to obtain

$$((p \vee q \vee r) \wedge (p \vee (\sim q) \vee r) \wedge ((\sim p) \vee (\sim q) \vee r)),$$

which is logically equivalent to $(((\sim p) \vee q) \rightarrow r)$ and is in conjunctive normal form, as desired.

The remaining sub-exercises are done similarly.

(b) The statement form $((p \vee (\sim q)) \wedge ((\sim p) \vee q))$ is in conjunctive normal form and is logically equivalent to $(p \leftrightarrow q)$.

(c) The statement form $(\sim ((p \wedge q \wedge r) \vee ((\sim p) \wedge (\sim q) \wedge r)))$ is logically equivalent to the statement form

$$\begin{array}{cc} ((\sim p) \wedge (\sim q) \wedge (\sim r)) & \vee \\ ((\sim p) \wedge q \wedge (\sim r)) & \vee \\ ((\sim p) \wedge q \wedge r) & \vee \\ (p \wedge (\sim q) \wedge (\sim r)) & \vee \\ (p \wedge (\sim q) \wedge r) & \vee \\ (p \wedge q \wedge (\sim r)), & \end{array}$$

which is in disjunctive normal form. Therefore, $(p \wedge q \wedge r) \vee ((\sim p) \wedge (\sim q) \wedge r)$ is logically equivalent, by Proposition 1.17, to

$$\begin{array}{cc} (p \vee q \vee r) & \wedge \\ (p \vee (\sim q) \vee r) & \wedge \\ (p \vee (\sim q) \vee (\sim r)) & \wedge \\ ((\sim p) \vee q \vee r) & \wedge \\ ((\sim p) \vee q \vee (\sim r)) & \wedge \\ ((\sim p) \vee (\sim q) \vee r), & \end{array}$$

which is a statement form in conjunctive normal form, as desired.

(d) The statement form $(((p \rightarrow q) \rightarrow r) \rightarrow s)$ is logically equivalent to

$$\begin{array}{cc} ((\sim p) \vee (\sim q) \vee r \vee (\sim s)) & \wedge \\ ((\sim p) \vee q \vee r \vee (\sim s)) & \wedge \\ (p \vee (\sim q) \vee (\sim r) \vee (\sim s)) & \wedge \\ (p \vee (\sim q) \vee r \vee (\sim s)) & \wedge \\ (p \vee q \vee r \vee (\sim s)), & \end{array}$$

which is a statement form in conjunctive normal form, as desired.

1.5 Adequate sets of connectives

Definition 1.23. An *adequate* set of connectives is a set such that every truth function can be represented by a statement form containing only connectives from that set.

In the last chapter, we have seen that $\{\sim, \vee, \wedge\}$ is an adequate set of connectives. We will use this fact to prove the next proposition.

Proposition 1.24. The sets $\{\sim, \wedge\}$, $\{\sim, \wedge\}$, and $\{\sim, \vee\}$ are adequate sets of connectives.

Proof. The proof is done by showing that any statement form using the connectives in the set $\{\sim, \vee, \wedge\}$ can be formed by using only the connectives in the sets described above. Since the set $\{\sim, \vee, \wedge\}$ is an adequate set of connectives, this method is sufficient to demonstrate that the other sets are adequate.

Let $\mathscr{A}$ and $\mathscr{B}$ be arbitrary statement forms.

Any statement form of the form $\mathscr{A} \vee \mathscr{B}$ can be expressed, via Proposition 1.17, as $((\sim \mathscr{A}) \wedge (\sim \mathscr{B}))$. Therefore, $\{\sim, \wedge\}$ is an adequate set of connectives.

Any statement form of the form $\mathscr{A} \wedge \mathscr{B}$ can be expressed, via Proposition 1.17, as $((\sim \mathscr{A}) \vee (\sim \mathscr{B}))$. Therefore, $\{\sim, \vee\}$ is an adequate set of connectives.

Any statement form of the form $\mathscr{A} \vee \mathscr{B}$ can be expressed as $(\sim \mathscr{A} \rightarrow \mathscr{B})$ and any statement form of the form $\mathscr{A} \wedge \mathscr{B}$ can be expressed as $(\sim (\mathscr{A} \rightarrow (\sim \mathscr{B})))$. These equivalences can be easily verified by constructing truth tables. Therefore, $\{\sim, \rightarrow\}$ is an adequate set of connectives. □

The *Nor* connective, denoted by $\downarrow$ is defined such that $p \downarrow q$ is true if and only if p and q are both false.

The *Nand* connective, denoted by $\uparrow$ is defined such that $p \uparrow q$ is false if and only if p and q are both true. In other words, it indicates that one of its operands is false.
Note. In the book, the symbol | is used for the Nand connective.

Proposition 1.26. The singleton sets $\{\downarrow\}$ and $\{\uparrow\}$ are adequate sets of connectives.

Proof. Let p and q be statement variables.

The statement form $\sim p$ can be represented as $p \downarrow p$, and the statement form $p \wedge q$ can be represented as $(p \downarrow p) \downarrow (q \downarrow q)$. Since the set $\{\sim, \wedge\}$ is an adequate set of connectives, the set $\{\downarrow\}$ must also be an adequate set of connectives.

The statement form $\sim p$ can be represented as $p \uparrow p$, and the statement form $p \vee q$ can be represented as $(p \uparrow p) \uparrow (q \uparrow q)$. Since the set $\{\sim, \vee\}$ is an adequate set of connectives, the set $\{\uparrow\}$ must also be an adequate set of connectives. □

Solutions to exercises

Note. The solutions for exercises 14 through 16 have not been verified and were done quickly. They likely contain mistakes.

14. (a) $(\sim p \vee ((\sim q) \vee r))$
    (b) $((\sim (\sim (p \vee q))) \vee (\sim (r \vee (\sim s))))$
    (c) $((\sim ((\sim p) \vee q)) \vee (\sim ((\sim q) \vee p)))$
15. (a) $(\sim (p \wedge (q \wedge (\sim r))))$
    (b) $(((\sim ((\sim p) \wedge (\sim q))) \wedge (\sim r)) \wedge (\sim ((p \wedge q) \wedge r)))$
    (c) $((\sim (((\sim (p \wedge q)) \wedge (\sim ((\sim q) \wedge (\sim p)))) \wedge (\sim r))) \wedge (\sim (r \wedge (\sim ((\sim (p \wedge q)) \wedge (\sim ((\sim q) \wedge (\sim p))))))))$
16. (a) $((p \rightarrow (\sim q)) \rightarrow (\sim (r \rightarrow (\sim s))))$
    (b) $(\sim ((p \rightarrow q) \rightarrow (\sim (q \rightarrow p))))$

(c) $(\sim((\sim(p \to (\sim q))) \to (\sim r)))$

17. (a) The value of a statement form consisting of only $\wedge$ and $\vee$ when all statement variables take value T must also be T, since $\mathscr{B} \wedge \mathscr{C}$ and $\mathscr{B} \vee \mathscr{C}$ both take value T when arbitrary statement forms $\mathscr{B}$ and $\mathscr{C}$ both take value T.

    Thus, no contradiction can be formed by only the connectives $\wedge$ and $\vee$, so the set $\{\wedge, \vee\}$ is not an adequate set of connectives.

    (b) We will first prove that if $\mathscr{A}$ is a statement form in which only two statement variables p and q appear and consists of only the connectives $\sim$ and $\leftrightarrow$, the value that $\mathscr{A}$ takes when p is true and q is false is the same as the value that it takes when p is false and q is true. The proof is by strong induction on the number of connectives appearing in $\mathscr{A}$.

    (base case) It is impossible for $\mathscr{A}$ to have zero connective. It may be that $\mathscr{A}$ has only one connective, and this connective must necessarily be $\leftrightarrow$, in which case $\mathscr{A}$ is $p \leftrightarrow q$. When p is true and q is false, the value of $\mathscr{A}$ is false, and when p is false and q is true, the value of $\mathscr{A}$ is also false, as desired.

    (inductive step) It may be that $\mathscr{A}$ has n connectives, where $n > 1$. Suppose as an induction hypothesis that any statement form consisting of only the statement variables p and q and fewer than n of the connectives $\sim$ and $\leftrightarrow$ has the above property. There are two cases to check.

    i. It may be that $\mathscr{A}$ is of the form $\sim \mathscr{B}$. If the value that $\mathscr{B}$ takes when p is true and q is false is T, then $\sim \mathscr{B}$ must take value F. By the induction hypothesis, $\mathscr{B}$ must also take the value T when p is false and q is true, and so $\sim \mathscr{B}$ must take value F, as desired. The other case for when $\sim \mathscr{B}$ identically takes the value T under both assignments of p and q can be verified in the same way.

    ii. It may be that $\mathscr{A}$ is of the form $\mathscr{B} \leftrightarrow \mathscr{C}$. The statement forms $\mathscr{B}$ and $\mathscr{C}$ will take certain values when p is true and q is false. By the induction hypothesis, they will take the same values when p is false and q is true. Therefore, the value of $\mathscr{B} \leftrightarrow \mathscr{C}$ will remain constant, as desired.

    Now that the above property has been proved, we may see that any truth function equivalent to the one generated by $p \to q$ can not be represented by a statement form generated by only the connectives $\leftrightarrow$ and $\sim$. For if a statement form were to consist of only p, q, the connectives $\leftrightarrow$ and $\sim$, then by the above proof, either it would take value T with p true and q false, or otherwise it would identically take value F with p false and q true.

    Since the set of connectives $\{\sim, \leftrightarrow\}$ is unable to generate a statement form representing a particular truth function, the set of connectives must not be adequate.

18. $(((p \uparrow p) \uparrow (p \uparrow p)) \uparrow (q \uparrow q))$

19. Let $\star$ be a *singularly adequate* binary connective in the sense that $\{\star\}$ is an adequate set of connectives.

    It must be able to express $\sim p$, where p is a statement variable, in terms of p and $\star$. It may be that when both p and q take value T, $p \star q$ takes value T. But then any contradiction involving p and q cannot be expressed using only $\star$, for the assignment of truth values of T to both p and q would result in the contradiction having a true vale, which would be contradictory. Similarly, if $p \star q$ takes value F when both p and q take value F, then no tautology involving only $\star$ can be expressed.

Thus, a partial truth table for $\star$ can be built.

p	q	$p \star q$
1	1	0
1	0	-
0	1	-
0	0	1

Now suppose that the truth table for $\star$ is either of the ones shown below.

p	q	$p \star q$
1	1	0
1	0	1
0	1	0
0	0	1

p	q	$p \star q$
1	1	0
1	0	0
0	1	1
0	0	1

Then any statement form involving p, q and $\star$ as its sole connective cannot be a tautology, since its truth value when p is true and q is false is different from its value when p is true and q is false [1]. So we may conclude that $\star$ cannot have one of the above truth tables.

On the other hand, the other possible truth tables for $\star$ correspond to $\uparrow$ and $\downarrow$, which are both singularly adequate. So $\star$ must be either $\uparrow$ or $\downarrow$, as desired.

1.6 Arguments and validity

An *argument form* is a finite sequence of statement forms. The last statement form is the called the *conclusion* and the other statement forms are called the *premises*.

Definition 1.28. The argument form $\mathscr{A}_1, \ldots, \mathscr{A}_n \therefore \mathscr{A}$ is *invalid* if it is possible to assign truth values to the statement variables occurring in such a way as to make each of the premises take value T while making the conclusion take value F. Otherwise, the argument form is *valid*.

Proposition 1.32. The argument form $\mathscr{A}_1, \ldots, \mathscr{A}_n \therefore \mathscr{A}$ is valid if and only if the statement form $((\mathscr{A}_1 \wedge \cdots \wedge \mathscr{A}_n) \rightarrow \mathscr{A})$ is a tautology.

[1] This can be made rigorous by a tedious induction similar to one done in part (b) of Exercise 17.

Proof. $\Rightarrow$ Suppose that the argument form $\mathscr{A}_1, \ldots, \mathscr{A}_n \therefore \mathscr{A}$ is valid. For a contradiction, suppose that $((\mathscr{A}_1 \wedge \cdots \wedge \mathscr{A}_n) \to \mathscr{A})$ is not a tautology. This will only occur when there exists some assignment of truth values to the statement variables occurring such that $(\mathscr{A}_1 \wedge \cdots \wedge \mathscr{A}_n)$ takes value T and $\mathscr{A}$ takes value F. This is to say that each $\mathscr{A}_i$ takes value T, while $\mathscr{A}$ takes value F, contradicting the validity of the argument form $\mathscr{A}_1, \ldots, \mathscr{A}_n \therefore \mathscr{A}$.

$\Leftarrow$ Suppose that the statement form $((\mathscr{A}_1 \wedge \cdots \wedge \mathscr{A}_n) \to \mathscr{A})$ is a tautology. For a contradiction, suppose that the argument form $\mathscr{A}_1, \ldots, \mathscr{A}_n \therefore \mathscr{A}$ is invalid. This will only occur when there exists some assignment of truth values to the statement variables occurring such that each $\mathscr{A}_i$ takes value T, while $\mathscr{A}$ takes value F, which is to say that $((\mathscr{A}_1 \wedge \cdots \wedge \mathscr{A}_n)$ is true while $\mathscr{A}$ is false. Then, under this assignment, the statement form $((\mathscr{A}_1 \wedge \cdots \wedge \mathscr{A}_n) \to \mathscr{A})$ must be false, contradicting the fact that it is a tautology. □

Solutions to exercises

20. (a) The corresponding argument form,

$$((\sim F) \to (\sim G)), G \therefore F,$$

is valid.

(b) The corresponding argument form,

$$(C \to (S \vee B)), (\sim B) \therefore ((\sim S) \to (\sim C)),$$

is valid.

(c) The corresponding argument form,

$$(D \to (E \vee (\sim G))), ((\sim O) \vee (\sim E)) \therefore G,$$

is invalid.

(d) The corresponding argument form,

$$(P \to (Q \wedge R \wedge S)), Q, (S \to R) \therefore (S \to P)$$

is invalid.

21. Suppose that $\mathscr{A}_1, \mathscr{A}_2, \ldots, \mathscr{A}_n \therefore \mathscr{A}$ is a valid argument form. Then whenever $\mathscr{A}_1, \mathscr{A}_2, \ldots, \mathscr{A}_n$ are all true, $\mathscr{A}$ is true as well.

Now suppose that $\mathscr{A}_1, \mathscr{A}_2, \ldots, \mathscr{A}_{n-1}$ are all true. It may be that $\mathscr{A}_n$ is true, in which case, by the above, $\mathscr{A}$ is true, so $(\mathscr{A}_n \to \mathscr{A})$ is true. Otherwise, $\mathscr{A}_n$ is false, so $(\mathscr{A}_n \to \mathscr{A})$ is vacuously true.

Therefore, $(\mathscr{A}_n \to \mathscr{A})$ is always true when $\mathscr{A}_1, \mathscr{A}_2, \ldots, \mathscr{A}_{n-1}$ are all true, and so $\mathscr{A}_1, \mathscr{A}_2, \ldots, \mathscr{A}_{n-1} \therefore (\mathscr{A}_n \to \mathscr{A})$ is a valid argument form.

22. Suppose that the premises p and $(p \uparrow (q \uparrow r))$ are true. Then p must be true. For $(p \uparrow (q \uparrow r))$ to be true, $(q \uparrow r)$ must be false, and this only occurs when q and r are both true. Since the conclusion r must be true, the argument form is valid.

Chapter 2

Formal statement calculus

2.1 The formal system L

A *formal system* is a mathematical structure representing a deductive system. It consists of

1. A set of symbols called an *alphabet*.
2. A set of finite strings of these symbols representing the valid sentences in the system. Each string is called a *well-formed formula*, or *wf* for short.

   There is usually a formula, called a *grammar*, for determining which strings are wfs.
3. A subset of the set of wfs representing the axioms.
4. A finite set of *inference rules*, functions which take a set of *wf*s and return a *wf*. The returned *wf* is said to be deduced from the set of *wf*s.

This chapter is devoted to a particular formal system described below.

Definition 2.1. The *formal system L of statement calculus* is defined by the following:

1. The alphabet consists of the symbols $\sim, \rightarrow, ($, and $)$, along with the countably infinite set of symbols $p_1, p_2, p_3, \ldots$.
2. The set of *wf*s is defined recursively by the following rules:
   (a) For any i, p_i is a *wf*.
   (b) If $\mathscr{A}$ and $\mathscr{B}$ are *wf*s, then $(\sim \mathscr{A})$ and $(\mathscr{A} \rightarrow \mathscr{B})$ are *wf*s.
   This rule also defines the semantics of the parentheses, and, because one set of parentheses will always contain only one of $\sim$ or $\rightarrow$ not in parentheses, it also eliminates the need for an order of operations.
   (c) The set of all *wf*s is generated by the above rules.
3. Let $\mathscr{A}, \mathscr{B}, \mathscr{C}$ be *wf*s. All axioms take on one of the following forms:
   (a) Axiom scheme 1 (L1): $(\mathscr{A} \rightarrow (\mathscr{B} \rightarrow \mathscr{A}))$.
   (b) Axiom scheme 2 (L2): $((\mathscr{A} \rightarrow (\mathscr{B} \rightarrow \mathscr{C})) \rightarrow ((\mathscr{A} \rightarrow \mathscr{B}) \rightarrow (\mathscr{A} \rightarrow \mathscr{C})))$.

   (c) Axiom scheme 3 (L3): $(((\sim \mathscr{A}) \to (\sim \mathscr{B})) \to (\mathscr{B} \to \mathscr{A}))$.

4. There is one rule of deduction known as *modus ponens* (MP): from $\mathscr{A}$ and $\mathscr{A} \to \mathscr{B}$, $\mathscr{B}$ is a direct consequence, where $\mathscr{A}, \mathscr{B}$ are any *wf*sof L.

Definition 2.2. A *proof of $\mathscr{A}_n$ in L*, or just a *proof in L*, is a sequence of *wf*s $\mathscr{A}_1, \ldots, \mathscr{A}_n$ such that for any i, $\mathscr{A}_i$ is an axiom of L or $\mathscr{A}_i$ follows from MP and two previous *wf*s in the sequence. The *wf* $\mathscr{A}_n$ is said to be a *theorem of L*.

Instead of using the word theorem to discuss a result about formal system, we will instead use the word *metatheorem* to prevent confusion with the word *theorem* in the sense of the previous definition.

Definition 2.5. Let Γ be a set of *wf*s of L. A proof in L with the members of Γ regarded as additional axioms is called a *deduction from* Γ. The last *wf* in the proof, call it $\mathscr{A}$, is said to be *deducible from* Γ or a *consequence of* Γ and is symbolized by $\Gamma \vdash_L \mathscr{A}$. If $\Gamma = \varnothing$ then we instead write $\vdash_L \mathscr{A}$, which is to say that $\mathscr{A}$ is a theorem of L.

Proposition 2.8 (The Deduction Theorem)**.** If $\Gamma \cup \{\mathscr{A}\} \vdash_L \mathscr{B}$, then $\Gamma \vdash_L (\mathscr{A} \to \mathscr{B})$, where $\mathscr{A}$ and $\mathscr{B}$ are *wf*s of L, and Γ is a set of *wf*s of L (possibly empty).

Proof. The proof is by strong induction on the number of *wf*s in the sequence forming the deduction of $\mathscr{B}$ from $\Gamma \cup \{\mathscr{A}\}$.

(base case) There is only one *wf* in the deduction of $\mathscr{B}$ from $\Gamma \cup \{\mathscr{A}\}$, which is to say that the proof consists of only $\mathscr{B}$, and there are two cases in which this can happen:

1. The *wf* $\mathscr{B}$ is an axiom of L or a member of Γ. In either case the deduction of $\mathscr{A} \to \mathscr{B}$ proceeds as follows:

1	$\mathscr{B}$	$\mathscr{B}$ is an axiom or a member of Γ
2	$(\mathscr{B} \to (\mathscr{A} \to \mathscr{B}))$	(L1)
3	$(\mathscr{A} \to \mathscr{B})$	1, 2, MP

   The above is a deduction of $(\mathscr{A} \to \mathscr{B})$ from Γ.

2. The *wf* $\mathscr{B}$ is $\mathscr{A}$, and so $(\mathscr{A} \to \mathscr{B})$ is $(\mathscr{A} \to \mathscr{A})$.

1	$((\mathscr{A} \to ((\mathscr{A} \to \mathscr{A}) \to \mathscr{A})) \to ((\mathscr{A} \to (\mathscr{A} \to \mathscr{A})) \to (\mathscr{A} \to \mathscr{A})))$	(L2)
2	$(\mathscr{A} \to ((\mathscr{A} \to \mathscr{A}) \to \mathscr{A}))$	(L1)
3	$((\mathscr{A} \to (\mathscr{A} \to \mathscr{A})) \to (\mathscr{A} \to \mathscr{A}))$	1, 2, MP
4	$(\mathscr{A} \to (\mathscr{A} \to \mathscr{A}))$	(L1)
5	$(\mathscr{A} \to \mathscr{A})$	3, 4, MP

   The above is a deduction of $(\mathscr{A} \to \mathscr{B})$ (which is $(\mathscr{A} \to \mathscr{A})$) from Γ. Note that it is also a general theorem of L.

(inductive step) Suppose that for any deduction of $\mathscr{C}$ from $\Gamma \cup \{\mathscr{A}\}$ with up to and including n members, it is possible to deduce $(\mathscr{A} \to \mathscr{B})$ from Γ alone. This is the hypothesis of strong induction.

Additionally suppose that there exists a deduction of $\mathscr{B}$ from $\Gamma \cup \{\mathscr{A}\}$ with $n+1$ members. We now provide a proof that there exists a deduction of $(\mathscr{A} \to \mathscr{B})$ from Γ alone. There are three cases to consider:

1. The *wf* $\mathscr{B}$ is an axiom of L or a member of Γ. A deduction of $(\mathscr{A} \rightarrow \mathscr{B})$ from Γ is shown in case 1 in the base case.

2. The *wf* $\mathscr{B}$ is $\mathscr{A}$. A deduction of $(\mathscr{A} \rightarrow \mathscr{B})$ from Γ is shown in case 2 in the base case.

3. The *wf* $\mathscr{B}$ is obtained applying MP along with two *wf*s, which are necessarily of the form $\mathscr{C}$ and $(\mathscr{C} \rightarrow \mathscr{B})$, where $\mathscr{C}$ is any *wf*. The deduction of $\mathscr{B}$ from $\Gamma \cup \{\mathscr{A}\}$ must be the sequence

$$(\ldots, \mathscr{C}, \ldots, (\mathscr{C} \rightarrow \mathscr{B}), \ldots, \mathscr{B}) \text{ or } (\ldots, (\mathscr{C} \rightarrow \mathscr{B}), \ldots, \mathscr{C}, \ldots, \mathscr{B}),$$

   from which it can be seen that the subsequences $(\ldots, \mathscr{C})$ and $(\ldots, (\mathscr{C} \rightarrow \mathscr{B}))$ are both deductions of $\mathscr{C}$ and $(\mathscr{C} \rightarrow \mathscr{B})$ from $\Gamma \cup \{\mathscr{A}\}$ with n members or less. Therefore, by the hypothesis, $\Gamma \vdash_L (\mathscr{A} \rightarrow \mathscr{C})$ and $\Gamma \vdash_L (\mathscr{A} \rightarrow (\mathscr{C} \rightarrow \mathscr{B}))$, which is to say that $(\mathscr{A} \rightarrow \mathscr{C})$ and $(\mathscr{A} \rightarrow (\mathscr{C} \rightarrow \mathscr{B}))$ are both deducible from Γ alone.

   So appending the proof of $(\mathscr{A} \rightarrow (\mathscr{C} \rightarrow \mathscr{B}))$ to $(\mathscr{A} \rightarrow \mathscr{C})$, yields the sequence

$$(\ldots, (\mathscr{A} \rightarrow \mathscr{C}), \ldots, (\mathscr{A} \rightarrow (\mathscr{C} \rightarrow \mathscr{B}))).$$

   which may have redundant *wf*s, but is nevertheless a valid deduction from Γ. The following proof builds on the sequence.

	$\vdots$	
k	$(\mathscr{A} \rightarrow \mathscr{C})$	deduced from Γ
	$\vdots$	
l	$(\mathscr{A} \rightarrow (\mathscr{C} \rightarrow \mathscr{B}))$	deduced from Γ
l + 1	$((\mathscr{A} \rightarrow (\mathscr{C} \rightarrow \mathscr{B})) \rightarrow ((\mathscr{A} \rightarrow \mathscr{C}) \rightarrow (\mathscr{A} \rightarrow \mathscr{B})))$	(L2)
l + 2	$((\mathscr{A} \rightarrow \mathscr{C}) \rightarrow (\mathscr{A} \rightarrow \mathscr{B}))$	l, l + 1
l + 3	$((\mathscr{A} \rightarrow (\mathscr{C} \rightarrow \mathscr{B})) \rightarrow ((\mathscr{A} \rightarrow \mathscr{C}) \rightarrow (\mathscr{A} \rightarrow \mathscr{B})))$	(L2)

And so in all three cases, $(\mathscr{A} \rightarrow \mathscr{B})$ can be deduced from Γ alone, which concludes the induction. □

Proposition 2.9 (Converse of The Deduction Theorem)**.** If $\Gamma \vdash_L (\mathscr{A} \rightarrow \mathscr{B})$ then $\Gamma \cup \{\mathscr{A}\} \vdash_L \mathscr{B}$, where $\mathscr{A}$ and $\mathscr{B}$ are *wf*s of L and Γ is a (possibly empty) set of *wf*s of L.

Proof. The following is a deduction of $\mathscr{B}$ from $\Gamma \cup \{\mathscr{A}\}$, provided that $\Gamma \vdash_L (\mathscr{A} \rightarrow \mathscr{B})$.

	$\vdots$	
k	$(\mathscr{A} \rightarrow \mathscr{B})$	deduction from Γ
k + 1	$\mathscr{A}$	member of $\Gamma \cup \{\mathscr{A}\}$
k + 2	$\mathscr{B}$	k, k + 1, MP

□

Corollary 2.10 (The Hypothetical Syllogism (HS))**.** For any *wf*s $\mathscr{A}, \mathscr{B}, \mathscr{C}$ of L,

$$\{(\mathscr{A} \rightarrow \mathscr{B}), (\mathscr{B} \rightarrow \mathscr{C})\} \vdash_L (\mathscr{A} \rightarrow \mathscr{C}).$$

Proof. We will first prove $S \vdash_L \mathscr{C}$, where $S = \{(\mathscr{A} \to \mathscr{B}), (\mathscr{B} \to \mathscr{C})\} \cup \{\mathscr{A}\}$.

1	$\mathscr{A} \to \mathscr{B}$	member of S
2	$\mathscr{B} \to \mathscr{C}$	member of S
3	$\mathscr{A}$	member of S
4	$\mathscr{B}$	1, 3, MP
5	$\mathscr{C}$	2, 4, MP

Seeing as though we have proved

$$\{(\mathscr{A} \to \mathscr{B}), (\mathscr{B} \to \mathscr{C})\} \cup \{\mathscr{A}\} \vdash_L \mathscr{C}$$

we may use the deduction theorem to conclude that

$$\{(\mathscr{A} \to \mathscr{B}), (\mathscr{B} \to \mathscr{C})\} \vdash_L (\mathscr{A} \to \mathscr{C}).$$

□

Proposition 2.11. For any *wf*s $\mathscr{A}$ and $\mathscr{B}$ of L, the following are theorems of L.

(a) $((\sim \mathscr{A}) \to (\mathscr{B} \to \mathscr{A}))$

(b) $(((\sim \mathscr{A}) \to \mathscr{A}) \to \mathscr{A})$

Proof. (a)

1	$((\sim \mathscr{B}) \to ((\sim \mathscr{A}) \to (\sim \mathscr{B})))$	(L1)
2	$(((\sim \mathscr{A}) \to (\sim \mathscr{B})) \to (\mathscr{B} \to \mathscr{A}))$	(L3)

Application of HS and the above two lines yields $((\sim \mathscr{B}) \to (\mathscr{B} \to \mathscr{A}))$, as desired.

(b) We will first prove that $\{((\sim \mathscr{A}) \to \mathscr{A})\} \vdash_L \mathscr{A}$.

1	$((\sim \mathscr{A}) \to \mathscr{A})$	assumption
2	$((\sim \mathscr{A}) \to ((\sim (\sim ((\sim \mathscr{A}) \to \mathscr{A}))) \to (\sim \mathscr{A})))$	(L1)
3	$(((\sim (\sim ((\sim \mathscr{A}) \to \mathscr{A}))) \to (\sim \mathscr{A})) \to$ $(\mathscr{A} \to (\sim ((\sim \mathscr{A}) \to \mathscr{A}))))$	(L3)
4	$((\sim \mathscr{A}) \to (\mathscr{A} \to (\sim ((\sim \mathscr{A}) \to \mathscr{A}))))$	2, 3, HS
5	$(((\sim \mathscr{A}) \to (\mathscr{A} \to (\sim ((\sim \mathscr{A}) \to \mathscr{A})))) \to$ $(((\sim \mathscr{A}) \to \mathscr{A}) \to ((\sim \mathscr{A}) \to (\sim ((\sim \mathscr{A}) \to \mathscr{A})))))$	(L2)
6	$(((\sim \mathscr{A}) \to \mathscr{A}) \to ((\sim \mathscr{A}) \to (\sim ((\sim \mathscr{A}) \to \mathscr{A}))))$	4, 5, MP
7	$((\sim \mathscr{A}) \to (\sim ((\sim \mathscr{A}) \to \mathscr{A})))$	1, 6, MP
8	$(((\sim \mathscr{A}) \to (\sim ((\sim \mathscr{A}) \to \mathscr{A}))) \to$ $(((\sim \mathscr{A}) \to \mathscr{A}) \to \mathscr{A}))$	(L3)
9	$(((\sim \mathscr{A}) \to \mathscr{A}) \to \mathscr{A})$	7, 8, MP
10	$\mathscr{A}$	1, 9, MP

By the deduction theorem, we may conclude that $(((\sim \mathscr{A}) \to \mathscr{A}) \to \mathscr{A})$.

□

Note. Because of the use of HS in line 4, which is a metatheorem, the above proof is not technically a proof in L. An actual proof would require a few additional lines.

Solutions to exercises

Note. All formulas are fully parenthesized, so they may look different from how they appear in the book. Additionally, any metatheorems are referenced as if they were rules of deduction, just like in the book.

1. (a)

$$\begin{array}{lrr}
1 & ((\sim p_1 \to \sim p_2) \to (p_2 \to p_1)) & \text{(L3)} \\
2 & (((\sim p_1 \to \sim p_2) \to (p_2 \to p_1)) \to & \\
 & ((p_1 \to p_2) \to ((\sim p_1 \to \sim p_2) \to (p_2 \to p_1)))) & \text{(L1)} \\
3 & ((p_1 \to p_2) \to ((\sim p_1 \to \sim p_2) \to (p_2 \to p_1))) & 1, 2, \text{MP}
\end{array}$$

(b)

$$\begin{array}{lrr}
1 & ((\underbrace{(p_1 \to (p_2 \to p_3))}_{\mathscr{A}} \to (\underbrace{(p_1 \to p_2)}_{\mathscr{B}} \to \underbrace{(p_1 \to p_3)}_{\mathscr{C}})) \to & \\
 & (((p_1 \to (p_2 \to p_3)) \to (p_1 \to p_2)) \to ((p_1 \to (p_2 \to p_3)) \to (p_1 \to p_3)))) & \text{(L2)} \\
2 & ((p_1 \to (p_2 \to p_3)) \to ((p_1 \to p_2) \to (p_1 \to p_3))) & \text{(L2)} \\
3 & (((p_1 \to (p_2 \to p_3)) \to (p_1 \to p_2)) \to ((p_1 \to (p_2 \to p_3)) \to (p_1 \to p_3))) & 1, 2, \text{MP}
\end{array}$$

(c)

$$\begin{array}{lrr}
1 & ((\underbrace{(p_1 \to (p_1 \to p_2))}_{\mathscr{A}} \to (\underbrace{(p_1 \to p_1)}_{\mathscr{B}} \to \underbrace{(p_1 \to p_2)}_{\mathscr{C}})) \to & \\
 & (((p_1 \to (p_1 \to p_2)) \to (p_1 \to p_1)) \to ((p_1 \to (p_1 \to p_2)) \to (p_1 \to p_2)))) & \text{(L2)} \\
2 & ((p_1 \to (p_1 \to p_2)) \to ((p_1 \to p_1) \to (p_1 \to p_2))) & \text{(L2)} \\
3 & (((p_1 \to (p_1 \to p_2)) \to (p_1 \to p_1)) \to ((p_1 \to (p_1 \to p_2)) \to (p_1 \to p_2))) & 1, 2, \text{MP} \\
4 & (p_1 \to ((p_1 \to p_2) \to p_1)) & \text{(L1)} \\
5 & ((p_1 \to ((p_1 \to p_2) \to p_1)) \to ((p_1 \to (p_1 \to p_2)) \to (p_1 \to p_1))) & \text{(L2)} \\
6 & ((p_1 \to (p_1 \to p_2)) \to (p_1 \to p_1)) & 4, 5, \text{MP} \\
7 & ((p_1 \to (p_1 \to p_2)) \to (p_1 \to p_2)) & 3, 6, \text{MP}
\end{array}$$

Lines 1-3 are identical to exercise (b) with p_1 substituted for p_2 and p_2 substituted for p_3.

Lines 4-6 are identical to example 2.4 in the book with $(p_1 \to p_2)$ substituted for p_2.

(d)

$$\begin{array}{lrr}
1 & (p_2 \to (p_1 \to p_2)) & \text{(L1)} \\
2 & (\underbrace{(p_2 \to (p_1 \to p_2))}_{\mathscr{A}} \to (\underbrace{p_1}_{\mathscr{B}} \to \underbrace{(p_2 \to (p_1 \to p_2))}_{\mathscr{A}})) & \text{(L1)} \\
3 & (p_1 \to (p_2 \to (p_1 \to p_2)) & 1, 2, \text{MP}
\end{array}$$

2. (a)

$$\begin{array}{lrr}
1 & (\sim \mathscr{A}) & \text{assumption} \\
2 & (((\sim \mathscr{B}) \to (\sim \mathscr{A})) \to (\mathscr{A} \to \mathscr{B})) & \text{(L3)} \\
3 & ((\sim \mathscr{A}) \to ((\sim \mathscr{B}) \to (\sim \mathscr{A}))) & \text{(L1)} \\
4 & ((\sim \mathscr{B}) \to (\sim \mathscr{A})) & 1, 3, \text{MP} \\
5 & (\mathscr{A} \to \mathscr{B}) & 2, 4, \text{MP}
\end{array}$$

(b)

1	$(\sim (\sim \mathscr{A}))$	assumption
2	$(((\sim \mathscr{A}) \to (\sim (\sim (\sim \mathscr{A})))) \to ((\sim (\sim \mathscr{A})) \to \mathscr{A})$	(L3)
3	$(((\sim (\sim (\sim (\sim \mathscr{A})))) \to (\sim (\sim \mathscr{A}))) \to$ $((\sim \mathscr{A}) \to (\sim (\sim (\sim (\mathscr{A})))))$	(L3)
4	$((\sim (\sim \mathscr{A})) \to ((\sim (\sim (\sim (\sim \mathscr{A})))) \to (\sim (\sim \mathscr{A}))))$	(L1)
5	$((\sim (\sim (\sim (\sim \mathscr{A})))) \to (\sim (\sim \mathscr{A})))$	1, 4, MP
6	$((\sim \mathscr{A}) \to (\sim (\sim (\sim \mathscr{A}))))$	3, 5, MP
7	$((\sim (\sim \mathscr{A})) \to \mathscr{A})$	2, 6, MP
8	$\mathscr{A}$	1, 7, MP

(c)

1	$(\mathscr{A} \to \mathscr{B})$	assumption
2	$(\sim (\mathscr{B} \to \mathscr{C}) \to (\sim \mathscr{A}))$	assumption
3	$(((\sim (\mathscr{B} \to \mathscr{C})) \to (\sim \mathscr{A})) \to (\mathscr{A} \to (\mathscr{B} \to \mathscr{C})))$	(L3)
4	$(\mathscr{A} \to (\mathscr{B} \to \mathscr{C}))$	2, 3, MP
5	$((\mathscr{A} \to (\mathscr{B} \to \mathscr{C})) \to ((\mathscr{A} \to \mathscr{B}) \to (\mathscr{A} \to \mathscr{C})))$	(L2)
6	$((\mathscr{A} \to \mathscr{B}) \to (\mathscr{A} \to \mathscr{C}))$	4, 5, MP
7	$(\mathscr{A} \to \mathscr{C})$	1, 6, MP

(d)

1	$(\mathscr{A} \to (\mathscr{B} \to \mathscr{C}))$	assumption
2	$((\mathscr{A} \to (\mathscr{B} \to \mathscr{C})) \to ((\mathscr{A} \to \mathscr{B}) \to (\mathscr{A} \to \mathscr{C})))$	(L2)
3	$((\mathscr{A} \to \mathscr{B}) \to (\mathscr{A} \to \mathscr{C}))$	1, 2, MP
4	$(\mathscr{B} \to (\mathscr{A} \to \mathscr{B}))$	(L1)
5	$(\mathscr{B} \to (\mathscr{A} \to \mathscr{C}))$	3, 4, HS

3. (a) We apply the deduction theorem to exercise to the result of exercise 2(b) and get $\vdash_L (\sim (\sim \mathscr{A}) \to \mathscr{A})$, which will be referred to as $\star$.

1	$\mathscr{A}$	assumption
2	$(\sim (\sim (\sim \mathscr{A})) \to (\sim \mathscr{A}))$	$\star$
3	$((\sim (\sim (\sim \mathscr{A})) \to (\sim \mathscr{A})) \to (\mathscr{A} \to (\sim (\sim \mathscr{A}))))$	(L3)
4	$(\mathscr{A} \to (\sim (\sim \mathscr{A})))$	2, 3, MP
5	$(\sim (\sim \mathscr{A}))$	1, 4, MP

By the deduction theorem, $\vdash_L (\mathscr{A} \to (\sim (\sim \mathscr{A})))$.

(b) This solution relies on the solutions for 3(a) and 2(b).

1	$(\mathscr{B} \to \mathscr{A})$	assumption
2	$(\mathscr{A} \to (\sim (\sim \mathscr{A})))$	$\star$
3	$((\sim (\sim \mathscr{B})) \to \mathscr{B})$	exercise 3(a)
4	$(\mathscr{B} \to (\sim (\sim \mathscr{A})))$	1, 2, HP
5	$((\sim (\sim \mathscr{B})) \to (\sim (\sim \mathscr{A})))$	3, 4, HP
6	$(((\sim (\sim \mathscr{B})) \to (\sim (\sim \mathscr{A}))) \to ((\sim \mathscr{A}) \to (\sim \mathscr{B})))$	(L3)
7	$((\sim \mathscr{A}) \to (\sim \mathscr{B}))$	5, 6, MP

By the deduction theorem, $\vdash_L ((\mathscr{B} \to \mathscr{A}) \to ((\sim \mathscr{A}) \to (\sim \mathscr{B})))$.

(c)

1	$((\mathscr{A} \to \mathscr{B}) \to \mathscr{A})$	assumption
2	$((\sim \mathscr{A}) \to (\mathscr{A} \to \mathscr{B}))$	Proposition 2.11(a)
3	$(\sim \mathscr{A} \to \mathscr{A})$	1, 2, HS
4	$((\sim \mathscr{A} \to \mathscr{A}) \to \mathscr{A})$	Proposition 2.11(b)
5	$\mathscr{A}$	3, 4, MP

By the deduction theorem, $\vdash_L (((\mathscr{A} \to \mathscr{B}) \to \mathscr{A}) \to \mathscr{A})$.

(d)

1	$(\sim (\mathscr{A} \to \mathscr{B}))$	assumption
2	$((\mathscr{B} \to (\mathscr{A} \to \mathscr{B})) \to (\sim (\mathscr{A} \to \mathscr{B}) \to (\sim \mathscr{B})))$	exercise 3(b)
3	$(\mathscr{B} \to (\mathscr{A} \to \mathscr{B}))$	(L1)
4	$(\sim (\mathscr{A} \to \mathscr{B}) \to (\sim \mathscr{B}))$	2, 3, MP
5	$(\sim \mathscr{B})$	1, 4, MP
6	$(\sim \mathscr{B} \to (\mathscr{B} \to \mathscr{A}))$	Proposition 2.11(a)
7	$(\mathscr{B} \to \mathscr{A})$	5, 6, MP

By the deduction theorem, $\vdash_L ((\sim (\mathscr{A} \to \mathscr{B})) \to (\mathscr{B} \to \mathscr{A}))$.

4. (i)

1	$((\sim \mathscr{A}) \to (\sim \mathscr{B}))$	assumption
2	$((\sim \mathscr{A}) \to \mathscr{B})$	assumption
3	$(((\sim \mathscr{A}) \to (\sim \mathscr{B})) \to (\mathscr{B} \to \mathscr{A}))$	(L3)
4	$(\mathscr{B} \to \mathscr{A})$	1, 3, MP
5	$((\sim \mathscr{A}) \to \mathscr{A})$	2, 4, HS
6	$(((\sim \mathscr{A}) \to \mathscr{A}) \to \mathscr{A})$	2.11(b)
7	$\mathscr{A}$	5, 6, MP

By the deduction theorem, which is valid since its proof relies only on $(L'1)$ and $(L'2)$, $\vdash_{L'} (((\sim \mathscr{A}) \to (\sim \mathscr{B})) \to (((\sim \mathscr{A}) \to \mathscr{B}) \to \mathscr{A}))$.

(ii) We will prove $\{((\sim \mathscr{A}) \to (\sim \mathscr{B})), \mathscr{B}\} \vdash_{L'} \mathscr{A}$

1	$((\sim \mathscr{A}) \to (\sim \mathscr{B}))$	assumption
2	$\mathscr{B}$	assumption
3	$(((\sim \mathscr{A}) \to (\sim \mathscr{B})) \to (((\sim \mathscr{A}) \to \mathscr{B}) \to \mathscr{A}))$	(L'3)
4	$(((\sim \mathscr{A}) \to \mathscr{B}) \to \mathscr{A})$	1, 3, MP
5	$(\mathscr{B} \to ((\sim \mathscr{A}) \to \mathscr{B}))$	(L'2)
6	$((\sim \mathscr{A}) \to \mathscr{B})$	2, 5, MP
7	$\mathscr{A}$	4, 6, MP

By the deduction theorem twice, $\vdash_{L'} (((\sim \mathscr{A}) \to (\sim \mathscr{B})) \to (\mathscr{B} \to \mathscr{A}))$.

Suppose a *wf* is proved in L. By definition, it follows from (L1), (L2), and (L3) and MP. Since (L1), (L2) and MP are properties of L', and since we just proved that $\vdash_{L'}$ (L3), the *wf* can also be proved in L'. The other direction is argued for in the same way, so a *wf* is a theorem in L if and only if it is a theorem in L'.

5. The rule is valid, see example 2.6 (where $\mathscr{A}$ and $\mathscr{B}$ in the exercise appear switched in the example).

2.2 The Adequacy Theorem for L

Definition 2.12. A *valuation* of L is a function v whose domain is the set of *wf*s of L and whose range is the set $\{T, F\}$ such that, for any *wf*s $\mathscr{A}, \mathscr{B}$ of L,

(i) $v(\mathscr{A}) \neq v((\sim \mathscr{A}))$ and

(ii) $v((\mathscr{A} \to \mathscr{B})) = F$ if and only if $v(\mathscr{A}) = T$ and $v(\mathscr{B}) = F$.

This definition formalizes the previous idea of truth functions for statement forms. Note that (i) and (ii) simply define the behavior of the two logic operators in L such that they correspond to the truth tables introduced in the last chapter.

Definition 2.13. A *wf* $\mathscr{A}$ of L is a *tautology* if for every valuation v, $v(\mathscr{A}) = T$. If for every valuation v, $v(\mathscr{A}) = F$, it is a *contradiction*.
Note. The definition of a contradiction isn't in the book, but the term is used later on.

The goal of this chapter is to prove that every *wf* in L is a tautology if and only if it is a theorem in L. One direction can be done immediately.

Proposition 2.14 (The Soundness Theorem)**.** Every theorem of L is a tautology.

Proof. Let $\mathscr{A}$ be a *wf* in L. It is a theorem if and only if it is the last member of a proof in L. The proof is by strong induction on the number of *wf*s in the proof of $\mathscr{A}$.

Suppose that all theorems containing up to n *wf*s in their proofs are tautologies. Now suppose that $\mathscr{A}$ has n *wf*s in its proof. In the proof, any *wf* preceding $\mathscr{A}$ must necessarily be a tautology because it is a theorem with fewer than n *wf*s in its proof. So the only thing to prove is that $\mathscr{A}$ is a tautology, and $\mathscr{A}$ can either be an axiom, in which case it is a tautology (see Exercise 6) or a product of MP and two previous *wf*s. These two *wf*s must necessarily be of the form $\mathscr{B}$ and $(\mathscr{B} \to \mathscr{A})$. By Proposition 1.9 (see the note below), $\mathscr{A}$ must be a tautology. □

Note. Proposition 1.9 is actually not strictly applicable here because it uses the previous informal notion of a tautology. But re-proving it using v would be nearly identical.
Note. A formal system is said to be sound if everything statement that is provable in it is true, and L has this property, as seen from this theorem, hence the name.

Definition 2.15. An *extension of* L is a formal system obtained by altering or enlarging the set of axioms so that all theorems of L remain theorems.
Note. By this definition, L is not an extension on L. Additionally, an extension of L may not actually extend the list of theorems of L.

Definition 2.16. An extension of L or L itself is *consistent* if for no *wf* $\mathscr{A}$ of L are both $\mathscr{A}$ and $(\sim \mathscr{A})$ theorems of the extension.
Note. This definition has been generalized slightly to be defined for L.

Proposition 2.17. L is consistent.

Proof. Suppose that L is not consistent. Then there exists a *wf* $\mathscr{A}$ such that $\mathscr{A}$ and $(\sim \mathscr{A})$ are both theorems of L. Since all theorems of L are tautologies (Proposition 2.14), $\mathscr{A}$ and $(\sim \mathscr{A})$ must be tautologies, meaning that for any valuation v, $v(\mathscr{A}) = v((\sim \mathscr{A})) = T$. But this contradicts v being a valuation (see Definition 2.12(i)). □

Note. Therefore, consistency of L is a consequence of its soundness, Proposition 2.14.

Proposition 2.18. An extension L^* of L is consistent if and only if there is a *wf* which is not a theorem of L^*.

Proof. $\Rightarrow$ Let L^* be consistent. Then, for any *wf* $\mathscr{A}$, either $\mathscr{A}$ or $\sim \mathscr{A}$ is not a theorem.

$\Leftarrow$ For the other direction, we use contrapositive reasoning. Suppose that L^* is not consistent, which is to say that there exists a *wf* $\mathscr{B}$ such that $\mathscr{B}$ and $(\sim \mathscr{B})$ are both theorems of L^*. Now let $\mathscr{A}$ be any *wf* of L^*. Since, by Proposition 2.11(a), $((\sim \mathscr{B}) \to (\mathscr{B} \to \mathscr{A}))$ is a theorem of L, it is a theorem of L^*. So by MP and since $(\sim \mathscr{B})$ is a theorem, $(\mathscr{B} \to \mathscr{A})$ is a theorem. By MP and since $\mathscr{B}$ is a theorem, $\mathscr{A}$ is a theorem. Therefore, there any *wf* $\mathscr{A}$ is a theorem of L^*. □

Note. The above proposition says that in a system with a contradiction in it, that contradiction can be used to vacuously prove anything, so a consistent system need only have one *wf* which is not a theorem.

Adding axioms to L or any of its extension can break its consistency. Consider a *wf* $\mathscr{A}$. Either it is true or false or maybe even both in L^* in the sense that $\vdash_{L^*} \mathscr{A}$ and/or $\vdash_{L^*} (\sim \mathscr{A})$, or it is undecidable in the sense that neither $\vdash_{L^*} \mathscr{A}$ or $\vdash_{L^*} (\sim \mathscr{A})$. In the latter case, would arbitrarily adding $\mathscr{A}$ or $(\sim \mathscr{A})$ break the consistency of L? The answer is no, as the following proposition shows.

Proposition 2.19. Let L^* be a consistent extension of L and let $\mathscr{A}$ be a *wf* of L which is not a theorem of L^*. Then L^{**} also consistent, where L^{**} is the extension of L obtained from L^* by including $(\sim \mathscr{A})$ as an additional axiom.

Proof. Suppose that L^{**} is not consistent. Then there exists some *wf* $\mathscr{B}$ such that both $\mathscr{B}$ and $(\sim \mathscr{B})$ are theorems of L^{**}. Now by Proposition 2.18 (see the note below), $\mathscr{A}$ must be a theorem of L^{**}. But since any theorem of L^{**} is a deduction from $(\sim \mathscr{A})$ in L^*, which is to say that $\{(\sim \mathscr{A})\} \vdash_{L^*} \mathscr{A}$ it follows from the deduction theorem that $\vdash_{L^*} ((\sim \mathscr{A}) \to \mathscr{A})$. From Proposition 2.11(b) and since all theorems of L are theorems of L^*, we have $\vdash_{L^*} ((\sim \mathscr{A}) \to \mathscr{A}) \to \mathscr{A})$, and so $\vdash_{L^*} \mathscr{A}$ by MP. But this contradicts $\mathscr{A}$ not being a theorem of L^*. Therefore, L^{**} must be consistent. □

Note. Proposition 2.18 is not strictly applicable here, but its proof can be easily generalized to L^{**}.
Note. Clearly if $(\sim \mathscr{A})$ is a theorem of L^*, then adding it as an axiom in L^{**} will not break consistency. Only when $\mathscr{A}$ is "neither true nor false" is this theorem interesting.

Definition 2.20. An extension of L is *complete* if for each *wf* $\mathscr{A}$, either $\mathscr{A}$ or $(\sim \mathscr{A})$ is a theorem of the extension.
Note. Completeness is the converse of soundness.

Proposition. The set of *wf*s of L is countable.

Proof. See the appendix. □

Proposition 2.21. Let L^* be a consistent extension of L. Then there is a consistent complete extension of L^*.

Proof. Since the set of all *wf*s of L is countable, let $\mathscr{A}_1, \mathscr{A}_2, \mathscr{A}_3$ be an enumerations of the *wf*s. Define a sequence $J_0, J_1, J_2, \ldots$ by the following rules.

1. If $n = 0$, let J_0 be L^*.

2. If $n > 0$, let J_n be J_{n-1} if $\vdash_{J_{n-1}} \mathscr{A}_n$.

3. If $n > 0$, let J_n be J_{n-1} extended with $(\sim \mathscr{A}_n)$ as an additional axiom if $\mathscr{A}_n$ is not a theorem of J_{n-1}.

Notice that since $J_0 = L^*$ is consistent and every following member of the sequence is either the previous member or a consistent extension by Proposition 2.19, every member of the sequence is consistent.

Now define J to be an extension of L^* such that a *wf* is an axiom of J if and only if it is an axiom of J_n for any n. Notice that by construction of the sequence, for any k, either $\mathscr{A}_k$ or $(\sim \mathscr{A}_k)$ is a theorem of J_k. So J_k or $(\sim J_k)$ must be a theorem of J, which extends J_k. Therefore, J is complete.

Now suppose that J is not consistent. Then there is a *wf* $\mathscr{A}$ such that $\vdash_J \mathscr{A}$ and $\vdash_J (\sim \mathscr{A})$. Now in these proofs, there are a finite number of axioms used, and each axiom must of course appear in the list of all numbered *wf*s. Let $\mathscr{A}_k$ refer to the axiom with the highest index k. So both $\vdash_{J_k} \mathscr{A}_k$ and $\vdash_{J_k} (\sim \mathscr{A}_k)$, contradicting the consistency of J_k. Hence, J must be consistent. □

Note. An extension of L^* is defined in the same way as an extension of L is.
Note. The set of *wf*s is purposely indexed starting from 1 instead of 0 like in the book so that $\mathscr{A}_n$ or $(\sim \mathscr{A}_n)$ is a theorem of $\mathscr{B}_n$.

Proposition 2.22. If L^* is a consistent extension of L then there is a valuation in which each theorem of L^* takes value T.

Proof. Let J be the consistent complete extension of L^* given in the proof of Proposition 2.21. Define v on *wf*s of L by $v(\mathscr{A}) = T$ if $\mathscr{A}$ is a theorem of J and $v(\mathscr{A}) = F$ otherwise.

Now it remains to be shown that v is a valuation consistent with Definition 2.12. Since J is complete, v is defined on all *wf*s. For any $\mathscr{A}$, $v(\mathscr{A}) \neq v((\sim \mathscr{A}))$, since J is consistent. It remains to show that $v(\mathscr{A} \to \mathscr{B}) = F$ if and only if $v(\mathscr{A}) = T$ and $v(\mathscr{B}) = F$.

$\Rightarrow$ Suppose that $v(\mathscr{A} \to \mathscr{B}) = F$ and that either $v(\mathscr{A}) = F$ or $v(\mathscr{B}) = T$. Since J is consistent, $\sim (\mathscr{A} \to \mathscr{B})$ must be a theorem of J and either $(\sim \mathscr{A})$ or $\mathscr{B}$ is also theorem of J. If $(\sim \mathscr{A})$, then

1	$(\sim \mathscr{A})$	assumption
2	$((\sim \mathscr{A}) \to ((\sim \mathscr{B}) \to (\sim \mathscr{A})))$	(L1)
3	$((\sim \mathscr{B}) \to (\sim \mathscr{A}))$	1, 2, MP
4	$(((\sim \mathscr{B}) \to (\sim \mathscr{A})) \to (\mathscr{A} \to \mathscr{B}))$	(L3)
5	$(\mathscr{A} \to \mathscr{B})$	3, 4, MP

or if $\mathscr{B}$, then

1	$\mathscr{B}$	assumption
2	$(\mathscr{B} \to (\mathscr{A} \to \mathscr{B}))$	(L2)
3	$(\mathscr{A} \to \mathscr{B})$	1, 2, MP

and so in either case, $(\mathscr{A} \to \mathscr{B})$ is a theorem of J along with $(\sim (\mathscr{A} \to \mathscr{B}))$, contradicting the consistency of J. Therefore, if $v(\mathscr{A} \to \mathscr{B})$, then $v(\mathscr{A}) = T$ and $v(\mathscr{B}) = F$.

$\Leftarrow$ Suppose that $v(\mathscr{A}) = T, v(\mathscr{B}) = F$ and that $v((\mathscr{A} \to \mathscr{B})) = T$. Then $\mathscr{A}$, $(\sim \mathscr{B})$, and $(\mathscr{A} \to \mathscr{B})$ are theorems of J. Then by MP, $\mathscr{A}$, and $(\mathscr{A} \to \mathscr{B})$, it follows that $\mathscr{B}$ is a theorem of J as well along with $(\sim \mathscr{B})$, contradicting the consistency of J. Therefore, if $v(\mathscr{A}) = T, v(\mathscr{B}) = F$ implies that $v((\mathscr{A} \to \mathscr{B})) = F$.

In conclusion, v is indeed a valuation and so if $\mathscr{A}$ is a theorem of L^*, then it must be a theorem of the extension J, in which case it takes the value T under the valuation v, making v a valuation in which each theorem of L^* takes value T. □

Proposition 2.23 (The Adequacy Theorem for L)**.** If $\mathscr{A}$ is a *wf* of L and $\mathscr{A}$ is a tautology, then $\mathscr{A}$ is a theorem of L.

Proof. Let $\mathscr{A}$ be a tautology and suppose that it is not a theorem of L. Then $(\sim \mathscr{A})$ must be a theorem of the extension L^* by Proposition 2.21. Therefore, by Proposition 2.22, there exists a valuation v in which $v(\sim \mathscr{A}) = T$. But $v(\mathscr{A}) = T$, since $\mathscr{A}$ is a tautology. This contradiction demonstrates that $\mathscr{A}$ must be a theorem of L. □

Proposition 2.24. L is *decidable*, i.e., there is an effective method for deciding, given any *wf* of L, whether it is a theorem of L.

Proof. The effective method of determining whether a *wf* is a tautology is to show that any valuation assigns the *wf* the value of T. If so, then it is a tautology, and by Proposition 2.23, it must be a theorem of L. □

Note. Showing that any valuation assigns the *wf* the value of T can be done by creating truth tables like in the first chapter.

Solutions to exercises

6. The truth tables for each scheme of L are shown below, and since the values for any assignment of T or F to the *wf*s is T, the axioms must all be tautologies.

   For $(L1)$,

$(\mathscr{A}$	$\underline{\to}$	$(\mathscr{B}$	$\to$	$\mathscr{A}))$
1	1	1	1	1
1	1	0	1	1
0	1	1	0	0
0	1	0	1	0

   For $(L2)$,

$((\mathscr{A}$	$\to$	$(\mathscr{B}$	$\to$	$\mathscr{C}))$	$\underline{\to}$	$((\mathscr{A}$	$\to$	$\mathscr{B})$	$\to$	$(\mathscr{A}$	$\to$	$\mathscr{C})))$
1	1	1	1	1	1	1	1	1	1	1	1	1
1	0	1	0	0	1	1	1	1	0	1	0	0
1	1	0	1	1	1	1	0	0	1	1	1	1
1	1	0	1	0	1	1	0	0	1	1	0	0
0	1	1	1	1	1	0	1	1	1	0	1	1
0	1	1	0	0	1	0	1	1	1	1	0	0
0	1	0	1	1	1	0	1	0	1	0	1	1
0	1	0	1	0	1	0	1	0	1	0	1	0

For ($L3$),

$(((\sim$	$\mathscr{A})$	$\rightarrow$	$(\sim$	$\mathscr{B}))$	$\underline{\rightarrow}$	$(\mathscr{B}$	$\rightarrow$	$\mathscr{A}))$
0	1	1	0	1	1	1	1	1
0	1	1	1	0	1	0	1	1
1	0	0	0	1	1	1	0	0
1	0	1	1	0	1	0	1	0

7. Let $\mathscr{A}$ be a *wf* of L and let L^+ be the extension of L obtained by including $\mathscr{A}$ as a new axiom. It is to be proved that the set of theorems of L^+ is different from the set of theorems of L if and only if $\mathscr{A}$ is not a theorem of L.

   $\Rightarrow$ Proceeding by contrapositive, suppose that $\mathscr{A}$ is a theorem of L. Then let $\mathscr{B}$ any theorem of L^+. We will demonstrate that $\mathscr{B}$ is a theorem of L.

   If the proof of $\mathscr{B}$ does not involve the axiom $\mathscr{A}$, then $\mathscr{B}$ is a theorem of L, since L differs from L^+ only in not having $\mathscr{A}$ as an axiom.

   Otherwise, the proof of $\mathscr{B}$ does involve the axiom $\mathscr{A}$, which is to say that $\{\mathscr{A}\} \vdash_L \mathscr{B}$, and by the deduction theorem $\vdash_L (\mathscr{A} \rightarrow \mathscr{B})$. By MP and $\mathscr{A}$ being a theorem in L, $\mathscr{B}$ is a theorem in L.

   Therefore, any theorem in L^+ is a theorem in L.

   $\Leftarrow$ Suppose that $\mathscr{A}$ is not a theorem of L. Then since $\mathscr{A}$ is a theorem of L^+ by virtue of all axioms being theorems, the set of theorems of L^+ must be different from the set of theorems of L^+.

8. Notice that $\mathscr{A}$ is neither a tautology nor a contradiction. Therefore, neither $\mathscr{A}$ nor $(\sim \mathscr{A})$ are theorems of L. Therefore, by the previous exercise, L^+, the extension of L with $\mathscr{A}$ as an axiom, has a larger set of theorems than L, in the sense that more *wf*s are theorems of L^+.

   Now suppose that L^+ is inconsistent. In an inconsistent system, every *wf* is a theorem, so $(\sim \mathscr{A})$ must be a theorem of L^+. But since L^+ is L with $\mathscr{A}$ as an additional axiom, it follows that $\{\mathscr{A}\} \vdash_L (\sim \mathscr{A})$, and by the deduction theorem, $(\mathscr{A} \rightarrow (\sim \mathscr{A}))$ is a theorem of L. But since $(\mathscr{A} \rightarrow (\sim \mathscr{A}))$ is not a tautology, it cannot be a theorem of L. With this contradiction, it is seen that L^+ must be consistent.

9. Suppose that $\mathscr{B}$ is a contradiction as well as a theorem in L^+. For a contradiction, suppose that L^+ is a consistent extension of L. Then by Proposition 2.22, there is a valuation v such that every theorem of L^* takes value T. So $v(\mathscr{B}) = T$, but this contradicts $\mathscr{B}$ being a contradiction.

   *Note.*See the note in Definition 2.13.

10. L^{++} must have the contradiction

$$(((\sim (p_1 \rightarrow p_1)) \rightarrow (p_1 \rightarrow p_1)) \rightarrow ((p_1 \rightarrow p_1) \rightarrow (\sim (p_1 \rightarrow p_1))))$$

   as a theorem, since it is an instance of the given axiom scheme. By the previous exercise, L^{++} cannot be consistent.

11. Let J be a consistent complete extension of L, and let $\mathscr{A}$ be a *wf* of L. Let J^+ be the extension of J obtained by including $\mathscr{A}$ as an additional axiom. It is to be proved that J^+ is consistent if and only if $\mathscr{A}$ is a theorem of J.

    $\Rightarrow$ Suppose that J^+ is consistent. For a contradiction, suppose that $\mathscr{A}$ is not a theorem of J. Then $(\sim \mathscr{A})$ must be a theorem of J, since J is consistent and complete. Since J^+ is an extension of J, $(\sim \mathscr{A})$ must also be a theorem of J^+, which contradicts the consistency of J^+, since $\mathscr{A}$ is an axiom and hence a theorem of J.

    $\Leftarrow$ Suppose that $\mathscr{A}$ is a theorem of J and let $\mathscr{B}$ be any theorem in J^+. We will demonstrate that $\mathscr{B}$ must be a theorem in J.

    If the proof of $\mathscr{B}$ in J^+ does not rely on $\mathscr{A}$, then $\mathscr{B}$ is a theorem of J, since J^+ extends J with only $\mathscr{A}$ as an additional axiom.

    The other possibility is that the proof of $\mathscr{B}$ does involve $\mathscr{A}$, which is to say that $\{\mathscr{A}\} \vdash_J \mathscr{B}$, and so by the deduction theorem $\vdash_J (\mathscr{A} \to \mathscr{B})$. By MP and $\mathscr{A}$ being a theorem in J, $\mathscr{B}$ is a theorem in J. Therefore, any theorem in J^+ is a theorem in J, and since J is consistent, J^+ must be so as well.

12. We will prove this using strong induction on the number of *wf*s in the proof of $\mathscr{A}$.

    Suppose as an induction hypothesis that for any theorem $\mathscr{A}$ in L in which statement letters appear and in which its proof involves less than n *wf*s, $\mathscr{B}$, a *wf* with any *wf*s substituted for the statement letters, is also a theorem of L.

    It may be the case that $\mathscr{A}$ is an instance of an axiom, in which case $\mathscr{B}$ is also an instance of axiom and hence a theorem of L.

    Otherwise, $\mathscr{A}$ proceeds from two prior *wf*s in the proof via MP. These two *wf*s have less than n *wf*s in their proof, and therefore by the induction hypothesis, there exist theorems in L with the same substitutions of *wf*s for the statement letters described above. By MP and these two statements, $\mathscr{B}$ is a theorem of L as well.

    Note. In other words, $\mathscr{B}$ can be proved in an identical manner as $\mathscr{A}$, except by substituting the proper *wf*s for each *wf* in the proof of $\mathscr{A}$.

Chapter 3

Informal predicate calculus

3.1 Predicates and sequences

A warning

The reader of *Logic For Mathematicians* of course already has knowledge of formal mathematics regarding quantified statements. There is a common unspoken convention in math that statements are to quantified implicitly if quantifiers are absent. A statement like $x < y$ might be written to be short for $(\forall x)(\forall y)(x < y)$, where x and y are integers.

But this assumption cannot be held while reading Chapter 3 of the textbook or when studying first-order logic in general. Some strings of symbols, which will later be called *wf*s, are neither true nor false, and the reason for this is the absence of quantifiers. For example, the string $x < y$ is assumed to be indeterminate in the sense that it is neither true nor false, and likewise $(\forall x)x < y$ is also indeterminate. The truth of these formulas depend on how x and y are evaluated ($x = y = 3$ would yield a false evaluation, for example), which is an idea which will be formalized in the last chapter of this section.

We will see later that all *closed formulas*, which refer to formulas where all variables are quantified, are true or false, as expected. However, not all unquantified formulas are indeterminate. Consider $x = x$, which is true, despite the formula having no quantifiers.

Solutions to exercises

1. (a) $\sim (\forall x)(F(x) \rightarrow D(x))$
   (b) $(\exists x)(F(x) \wedge C(x) \wedge (\sim D(x)))$
   (c) $(\exists x)(T(x) \wedge L(x)) \rightarrow (\forall x)(T(x) \rightarrow L(x))$
   (d) $(\forall x)(E(x) \vee O(x))$
   (e) $\sim (\exists x)(E(x) \wedge O(x))$
   (f) $(\exists x)(P(x) \wedge (\forall y)(P(y) \rightarrow H(x,y)))$
   (g) $(\forall x)(E(x) \rightarrow (\forall y)(M(y) \rightarrow H(x,y)))$

2. (a) $\sim (\forall x)(C(x) \rightarrow T(x))$
   $(\exists x)(C(x) \wedge \sim T(x))$

(b) $\sim (\forall x)(P(x) \to (\sim L(x) \wedge \sim S(x)))$
$(\exists x)(P(x) \wedge (L(x) \vee S(x)))$

(c) $(\forall x)(\forall y)((M(x) \wedge E(y)) \to \sim H(x, y))$
$\sim (\exists x)(\exists y)(M(x) \wedge E(y) \wedge H(x, y))$

(d) $(\forall x)(N(x) \vee S(x))$
$\sim (\exists x)((\sim N(x)) \wedge (\sim S(x)))$

3.

3.2 First order languages

Here we will define a mathematical structure which is not a formal system as it has no rules or deductions or axioms. It does have an alphabet, which is specified below. In fact, it may be thought of, structurally speaking, as only an alphabet, a set of symbols.

A *first order language* $\mathscr{L}$ will have as its alphabet of symbols:

- the countably infinite list of *variables* $x_1, x_2, \ldots$
- some or none of the *constants* $a_1, a_2, \ldots$
- some or none of the *predicate letters* $A_1^1, A_2^1, \ldots; A_1^2, A_2^2, \ldots; A_1^3, A_1^3, \ldots; \ldots$
- some or none of the *function letters* $f_1^1, f_2^1, \ldots; f_1^2, f_2^2, \ldots; f_1^3, f_1^3, \ldots; \ldots$
  - the predicate and function letters are countably infinite lists of countably infinite lists
  - the subscripts are used to distinguish different functions of the same arity, while the superscript indicates the arity
  - the function letters are not strictly necessary, as they can be expressed as relations as well, but the redundancy is kept for purposes of intuitive clarity
- the left and right parentheses (and) and the comma , as *punctuation symbols*
- the *connectives* $\sim$ and $\to$
- the quantifier $\forall$
  - the existential quantifier $\exists$ can be expressed in terms of the universal quantifier along with the $\sim$ connective, so it is not included

Note. Two first order languages differ only in the symbols which are in the alphabet, particularly which constants, predicate letters and function letters are included. For example, one first order language might only include a_1 and f_1^1, and another might only include A_1^1.

The alphabet will be part of a formal system described in the next chapter which will make clear the logical rules in a first-order system. Since no rules of deduction or axioms have been specified, studying first order languages, which is the subject of this chapter, will be limited to studying not the valid rules of transformations of strings of symbols that correspond to valid deductions, but rather what the valid strings are and how they are to be interpreted.

Definition 3.6. A *term* in a first order language $\mathscr{L}$ is defined as follows

(i) Variables and individual constants are terms.

(ii) If f_i^n is a function letter in $\mathscr{L}$, and $t_1, \ldots, t_2$ are terms in $\mathscr{L}$, then $f_i^n(t_1, \ldots, t_2)$ is a term in $\mathscr{L}$.

(iii) The set of all terms is generated as in (i) and (ii).

An *atomic formula* in $\mathscr{L}$ is defined by: if A_j^k is a predicate letter in $\mathscr{L}$ and $t_1, \ldots, t_n$ are terms in L, then $A_j^k(t_1, \ldots, t_n)$ is an atomic formula of $\mathscr{L}$.

A *well-formed formula* of $\mathscr{L}$ is defined by:

(i) Every atomic formula of $\mathscr{L}$ is a *wf* of $\mathscr{L}$.

(ii) If $\mathscr{A}$ and $\mathscr{B}$ are *wf*s, so are $(\sim \mathscr{A}), (\mathscr{A} \rightarrow \mathscr{B})$ and $(\forall x_i)\mathscr{A}$, where x_i is any variable.

(iii) The set of all *wf*s of $\mathscr{L}$ is generated as in (i) and (ii)

Terms are to be considered as objects in the language, a *wf* as a statement, and an atomic formula as the most simple kind of statement.

The symbols $\exists, \wedge$ and $\vee$ are treated as shorthand.

- $(\exists x_i)\mathscr{A}$ is an abbreviation for $(\sim ((\forall x_i)(\sim \mathscr{A}))$
- $(\mathscr{A} \wedge \mathscr{B})$ is an abbreviation for $(\sim (\mathscr{A} \rightarrow (\sim \mathscr{B})))$
- $(\mathscr{A} \vee \mathscr{B})$ is an abbreviation for $((\sim \mathscr{A}) \rightarrow \mathscr{B})$

Note. Unlike in chapter 2, this manual will follow the book's style for omitting parentheses. That is, a $\sim$ will be presumed to apply to the shortest possible subsequent *wf*. Also notice that this is how the $\forall$ quantifier is treated, by definition.

Definition 3.8. In the *wf* $(\forall x_i)\mathscr{A}$, we say that $\mathscr{A}$ is the *scope* of the quantifier. When $(\forall x_i)\mathscr{A}$ occurs as a subformula of a *wf* $\mathscr{B}$, the scope of the quantifier $(\forall x_i)$ is said to be $\mathscr{A}$ in $\mathscr{B}$.

A variable x_i in a *wf* is said to be *bound* if it occurs within the scope of a $(\forall x_i)$ in the *wf* or if it is the x_i in a $(\forall x_i)$. A variable which is not bound is said to be *free*.

Note. One point of confusion is that the meaning of a formula $(\forall x_i)\mathscr{A}$ is reliant on its *free* variables, not its bound ones, which might be contrary to one's intuitions about the words *free* and *bound*.

From here on out, if $\mathscr{A}(x_i)$ is a *wf* in which x_i occurs free, then $\mathscr{A}(t)$ will refer to $\mathscr{A}(x_i)$ with all *free* occurrences of x_i replaced with t. So if $\mathscr{A}(x_i)$ is $(\forall x_2)A_1^1(x_i) \rightarrow (\forall x_i)A_1^1(x_i))$, then $\mathscr{A}(t)$ is $(\forall x_2)A_1^1(t) \rightarrow (\forall x_i)A_1^1(x_i))$. We will want to only substitute t for x_i if it does not interact with quantifiers in $\mathscr{A}(x_i)$. In the previous example, x_2 would be a different substitution that any other variable. For this reason, we need the next definition, which is as important as it is confusing. A few equivalent definitions will be provided.

Definition 3.11. Let $\mathscr{A}$ be any *wf* of $\mathscr{L}$. A term t is *free for x_i in $\mathscr{A}$* if x_i does not occur free in $\mathscr{A}$ within the scope of a $(\forall x_j)$, where x_j is any variable occurring in t.

Equivalently, a term t is *free for x_i in $\mathscr{A}$* if substituting t for any free instance of x_i in $\mathscr{A}$ would not introduce any new bound variables.

Equivalently, a term t is *free for x_i in $\mathscr{A}$* if any variable in t is free in $\mathscr{A}$ after substituting it for any free instance of x_i.

An algorithm for determining whether a term t is *free for x_i in $\mathscr{A}$* goes as follows:

1. Find all free instances of x_i in $\mathscr{A}$.
2. For each free instance x_j, repeat the following step:
   (a) For each variable x_k in t, repeat the following steps:
      i. Substitute x_k for x_j.
      ii. If x_k is bound in $\mathscr{A}$, then t is not free for x_i, and terminate the algorithm.
3. Conclude that t is free for x_i.

Note. A term being free for a variable x_i does not necessarily indicate that it may be substituted for that variable, because the variable x_i may be bound. But if x_i only occurs free, then a term being free for it is equivalent to a term being substitutable for it. Therefore "t being free for x_i" can be thought of as "t being substitutable for free instances of x_i."

Note. It is easy to confirm that if x_i occurs only bound in $\mathscr{A}$, then any term is free for it. Also, for any *wf* and any variable x_i, x_i is free for itself in $\mathscr{A}$.

Solutions to exercises

4. The set of terms in a first order language with no function letters is just the set of the variables and the individual constants.

5. The set of terms is $f_1^1(x_1), f_1^1(x_2), f_1^1(x_3), \ldots$.

6. The formulas that are well-formed formulas are (a), (d), (e), (g), and (h).

   Note. The answer key in the book omits (d) as a well-formed formula, but this appears to be wrong.

7. (a) free
   (b) bound, bound
   (c) bound, bound, free
   (d) free, free, free, free

   Since all occurrences of x_2 in the *wf*s are bound, the term $f_1^2(x_1, x_3)$ (and any other term) is free for x_2 in the *wf*s.

8. Suppose that x_j is free for x_i in $\mathscr{A}(x_i)$. Then x_i does not occur free in the scope of a $(\forall x_j)$ in $\mathscr{A}(x_i)$. The goal is to show that x_j does not occur free in the scope of a $(\forall x_i)$ in $\mathscr{A}(x_j)$.

   Now consider an occurrence of an x_j in $\mathscr{A}(x_j)$, which is either (1) a substitution for an x_i in $\mathscr{A}(x_i)$ or (2) not a substitution for an x_i in $\mathscr{A}(x_i)$. If (1), then since x_1

was assumed to occur free in $\mathscr{A}(x_i)$, it must not be in the scope of a $(\forall x_i)$, and so the substituted x_j must also not be in the scope of a $(\forall x_i)$. If (2), then it must occur the same as it does in $\mathscr{A}(x_i)$, a *wf* in which it is assumed to occur bound, and therefore it does not occur free in the scope of a $(\forall x_i)$, or any quantifier for that matter.

Since in both (1) and (2), x_j does not occur free in the scope of a $(\forall x_i)$ in $\mathscr{A}(x_j)$, it can be concluded that x_i is free for x_j in $\mathscr{A}(x_j)$.

Note. The hypothesis that x_j is free for x_i is never used in the proof. It seems that there is either a mistake in the proof or in the exercise. The hint/proof in the back of the book seems to agree with the proof given here.

9. (a) Since $(\forall x_1)$ and $(\forall x_3)$ never occur, $\underline{t \text{ is free for } x_1}$.
   (b) Since x_1 only occurs bound, $\underline{t \text{ is free for } x_1}$.
   (c) Since x_1 occurs free in the scope of a $(\forall x_3)$, $\underline{t \text{ is not free for } x_1}$.
   (d) Since x_1 occurs free in the scope of a $(\forall x_3)$, $\underline{t \text{ is not free for } x_1}$.

10. Here, the (a), (b), (c), and (d) refer to the *wf*s in the exercise 9 and not the terms in exercise 10.

    Note. There is a mistake in the text, the exercise should read "Repeat Exercise 9..." instead of "Repeat Exercise 6...".

    Let $t = x_2$.

    (a) Since x_1 occurs free in the scope of a $(\forall x_2)$, $\underline{t \text{ is not free for } x_1}$.
    (b) Since x_1 only occurs bound, $\underline{t \text{ is free for } x_1}$.
    (c) Since x_1 does not occur in the scope of a $(\forall x_2)$, it does not occur free in it, so $\underline{t \text{ is free for } x_1}$.
    (d) Since x_1 occurs free in the scope of a $(\forall x_2)$, $\underline{t \text{ is not free for } x_1}$.

    Let $t = x_3$.

    (a) Since a $(\forall x_3)$ never occurs, $\underline{t \text{ is free for } x_1}$.
    (b) Since x_1 only occurs bound, $\underline{t \text{ is free for } x_1}$.
    (c) Since x_1 occurs free in the scope of a $(\forall x_3)$, $\underline{t \text{ is not free for } x_1}$.
    (d) Since x_1 occurs free in the scope of a $(\forall x_3)$, $\underline{t \text{ is not free for } x_1}$.

    Let $t = f_1^2(a_1, x_1)$.

    (a) Since a $(\forall x_1)$ never occurs, $\underline{t \text{ is free for } x_1}$.
    (b) Since x_1 only occurs bound, $\underline{t \text{ is free for } x_1}$.
    (c) Since a $(\forall x_1)$ never occurs, $\underline{t \text{ is free for } x_1}$.
    (d) Since a $(\forall x_1)$ never occurs, $\underline{t \text{ is free for } x_1}$.

    Let $f_1^3(x_1, x_2, x_3)$.

    (a) Since x_1 occurs free in the scope of a $(\forall x_2)$, $\underline{t \text{ is not free for } x_1}$.

(b) Since x_1 only occurs bound, $\underline{t \text{ is free for } x_1}$.

(c) Since x_1 occurs free in the scope of a $(\forall x_3)$, $\underline{t \text{ is not free for } x_1}$.

(d) Since x_1 occurs free in the scope of a $(\forall x_2)$ and a $(\forall x_3)$, $\underline{t \text{ is not free for } x_1}$.

3.3 Interpretations

Definition 3.14. An *interpretation* I of $\mathscr{L}$ is

- a non-empty set D_I called the *domain* of I together with a collection
- a collection of distinguished elements $(\overline{a}_1, \overline{a}_2, \dots)$ of D_I
- a collection of functions from D_I to D_I denoted by $(\overline{f}_1^n, i > 0, n > 0)$
- a collection of relations on D_I denoted by $(\overline{A}_1^n, i > 0, n > 0)$

An interpretation allows a *wf* of a first order language to be interpreted as a statement with a truth value, analogous to how a valuation of L allowed a *wf* in L to have a truth value. This concept will be formalized in the coming sections.

Solutions to exercises

11. The interpretation of $\mathscr{A}$ in I is the statement

$$(\forall x_1)(\forall x_2)(x_1 - x_2 < 0 \to x_1 < x_2)$$

which is a true statement in the integers. Consider the same interpretation I with $\overline{f}_1^2(x, y)$ as $x + y$. The interpretation of $\mathscr{A}$ in I is then

$$(\forall x_1)(\forall x_2)(x_1 + x_2 < 0 \to x_1 < x_2)$$

which is false.

12. Let I be the interpretation described above in the previous exercise with the addition of $\overline{f}_1^1, \overline{A}_1^1$ defined by $\overline{f}_1^1(x) = x - 1$ and $\overline{A}_1^1(x)$ if and only if $x > 0$. Then the statement corresponding to the *wf* under I is

$$(\forall x_i)(x_1 > 0 \to x_1 - 1 > 0)$$

which is false.

13. Let I again be the interpretation described in Exercise 11 with $\overline{A}_1^2(x, y)$ as $x < y$. Then the interpretation of the *wf* is

$$(\forall x_1)(x_1 < x_2 \to x_2 < x_1)$$

which is false, since it defies the law of trichotomy, a property of the integers.

3.4 Satisfaction, truth

In this chapter I will be an interpretation of the language $\mathscr{L}$ with notation consistent with Definition 3.14.

In the previous chapter, values of true or false were informally assigned to various *wf*s of $\mathscr{L}$ under some interpretation I. This chapter will formalize this process of evaluating the truth of a *wf*. The process will and must be similar to the informal process of determining the truth value of a *wf*. First, the terms must be assigned to values. A particular assignment is formally known as a *valuation*.

Definition 3.17. A *valuation* in I is a function v from the set of terms of $\mathscr{L}$ to the set domain of I, D_I, with the properties:

(i) $v(a_i) = \overline{a}_i$ for each constant a_i of $\mathscr{L}$.

(ii) $v(f_i^n(t_1, \ldots, t_n)) = f_i^n(v(t_1)), \ldots, v(t_n))$, where f_i^n is any function letter in $\mathscr{L}$, and $t_1, \ldots, t_n$ are any terms of $\mathscr{L}$.

Note. An interpretation will have as many different valuations as there are ways of assigning the variables in $\mathscr{L}$ to elements of D_I.
Note. A term in $\mathscr{L}$ may be a variable, a constant, or a function with terms as its arguments. The variables can be assigned to any elements in D_I and no property is needed to govern the valuation of a variable. By property (i), every valuation assigns constants of $\mathscr{L}$ to its corresponding constant in D_I. Property (ii) guarantees that the valuation of functions in $\mathscr{L}$ behave as expected.

Definition 3.19. Two valuations v and v' are *i-equivalent* if $v(x_j) = v'(x_j)$ for every $j \neq i$.
Note. The purpose of this definition will be better understood after reading further on.

Continuing from where we left off before Definition 3.17, after the terms are assigned values, the *wf*s can be evaluated as true or false, depending on the particular values of the terms. If a particular *wf* is to be interpreted as a true statement when its terms take on some particular values specified by a valuation, the valuation is said to satisfy the *wf*. Since a *wf* in $\mathscr{L}$ was defined recursively, and likewise the definition of satisfaction of a *wf* must also be defined recursively.

Definition 3.20. Let $\mathscr{A}$ be a *wf* of $\mathscr{L}$, and let I be an interpretation of $\mathscr{L}$. A valuation v in I is said to satisfy...

(i) the atomic formula $A_j^n(t_1, \ldots, t_n)$ if $\overline{A}_j^n(v(t_1), \ldots, v(t_n))$ is true in D_I,

(ii) the negation $(\sim \mathscr{B})$ if v does not satisfy $\mathscr{B}$,

(iii) the implication $(\mathscr{B} \rightarrow \mathscr{C})$ if either v satisfies $(\sim \mathscr{B})$ or v satisfies $\mathscr{C}$,

(iv) the quantified *wf* $(\forall x_i)\mathscr{B}$ if all valuations v' which are i-equivalent to v satisfy $\mathscr{B}$.

Note. The first three parts of the definition are straightforward. The last one should be explained further. It states that a valuation satisfies a quantified *wf* if any corresponding interpretation is true when the bound variable takes on any possible value.

Proposition 3.23. Let $\mathscr{A}(x_i)$ be a *wf* of $\mathscr{L}$ in which x_i appears free, and let t be a term free for x_i. Suppose that v is a valuation and v' is the valuation which is i-equivalent to v and has $v'(x_i) = v(t)$. Then v satisfies $\mathscr{A}(t)$ if and only if v' satisfies $\mathscr{A}(x_i)$.
Note. The condition that x_i appears free in $\mathscr{A}(x_i)$ can be relaxed if $\mathscr{A}(t)$ is defined as replacing all bound instances of x_i.

Proof. We will first prove a lemma.

Lemma. Let u be a term in which x_i occurs. Let u' be the term obtained by substituting t for x_i in u. Then $v(u') = v'(u)$.

Proof. The proof is by strong induction on the number of sub-terms in u. Note that this number takes sub-terms of sub-terms into account, so $f_1^2(f_1^2(x_1, x_1), f_1^2(x_1, x_1))$ has four, not two, sub-terms.

Suppose as a hypothesis of strong induction that if a term has fewer than n sub-terms in it, then $v(u') = v'(u)$, where u and u' are defined as above.

(base case) It may be that $n = 1$, in which case $u = x_i$ and $u' = t$. Then $v'(u) = v'(x_i) = v(t) = v(u')$ by construction of v' in the premise.

(inductive step) Otherwise, $n > 1$, and so $u = f_i^k(u_1, \ldots, u_k)$, where $u_1, \ldots, u_k$ are sub-terms that necessarily have fewer than n sub-terms. In the same way that u' was defined for u, define $u_1', \ldots, u_k'$ as the terms obtained by substituting t for x_i in $u_1, \ldots, u_k$. Finally, notice that $u' = f_i^k(u_1', \ldots, u_k')$, so

$$\begin{aligned}
v(u') &= v(f_i^k(u_1', \ldots, u_k')) && \text{definition of } u' \\
&= \overline{f}_i^k(v(u_1'), \ldots, v(u_k')) && \text{Definition 3.17} \\
&= \overline{f}_i^k(v'(u_1), \ldots, v'(u_k)) && \text{Induction hypothesis} \\
&= v'(f_i^k(u_1, \ldots, u_k)) && \text{Definition 3.17} \\
&= v'(u) && \text{Definition of } u
\end{aligned}$$

With this induction complete, we may conclude that $v'(u) = v(u')$ for any u. □

Now we prove the proposition by another strong induction on the number of connectives and quantifiers of $\mathscr{A}(x_i)$.

(base case) It may be that $\mathscr{A}(x_i)$ has non quantifiers and connectives, and so it must be an atomic formula, say $A_i^n(u_1, \ldots, u_n)$. Let $u_1', \ldots, u_n'$ be the terms $u_1, \ldots, u_n$ with t substituted for x_i, so that $\mathscr{A}(t)$ must then be $\mathscr{A}(u_1', \ldots, u_n')$. Then the following are all equivalent.

(a) v satisfies $\mathscr{A}(t)$, by assumption

(b) v satisfies $A_i^n(u_1', \ldots, u_n')$, by definition of $\mathscr{A}(t)$

(c) $A_i^n(v(u_1'), \ldots, v(u_n'))$ is true in I, by Definition 3.20

(d) $A_i^n(v'(u_1), \ldots, v'(u_n))$ is true in I, by the lemma above

(e) v' satisfies $A_i^n(u_1, \ldots, u_n)$, by Definition 3.20

(f) v' satisfies $A_i^n(x_i)$, by Definition 3.20

and the equivalence of (a) and (f) is what we desired to prove.

(inductive step) Otherwise, $\mathscr{A}(x_i)$ has k quantifiers and connectives. Suppose that $\mathscr{B}(x_i)$ has fewer than k quantifiers and connectives. Let w be a valuation and let w' be the valuation which is i-equivalent to w and has $w'(x_i) = w(t)$. Suppose, as an inductive hypothesis, that w satisfies $\mathscr{A}(t)$ if and only if w' satisfies $\mathscr{A}(x_i)$.

There are three cases to check.

1. The *wf* $\mathscr{A}(x_i)$ is $\sim \mathscr{B}(x_i)$, a *wf* with fewer than k quantifiers and connectives. Note that $\mathscr{A}(t)$ is $\sim \mathscr{B}(t)$. The following are equivalent.

   (a) v satisfies $\mathscr{A}(t)$, by assumption

   (b) v satisfies $\sim \mathscr{B}(t)$, by definition of $\mathscr{A}(t)$

   (c) v does not satisfy $\mathscr{B}(t)$, by Definition 3.20

   (d) v' does not satisfy $\mathscr{B}(t)$, by the induction hypothesis

   (e) v' satisfies $\sim \mathscr{B}(t)$, by definition of $\mathscr{A}(t)$

   (f) v' satisfies $\mathscr{A}(x_i)$, by Definition 3.20

   The equivalence between (a) and (f) is what we desired to prove. Note that in (d), we used the equivalent negative form of the inductive hypothesis.

2. The *wf* $\mathscr{A}(x_i)$ is $\mathscr{B}(x_i) \to \mathscr{C}(x_i)$, where both $\mathscr{B}(x_i)$ and $\mathscr{C}(x_i)$ are *wf*s with fewer than k quantifiers and connectives. Note that $\mathscr{B}(t)$ is $\mathscr{B}(t) \to \mathscr{C}(t)$. The following are equivalent.

   (a) v satisfies $\mathscr{A}(t)$, by assumption

   (b) v satisfies $\mathscr{B}(t) \to \mathscr{C}(t)$, by definition of $\mathscr{A}(t)$

   (c) v satisfies $\sim \mathscr{B}(t)$ or v satisfies $\mathscr{C}(t)$, by Definition 3.20

   (d) v' satisfies $\sim \mathscr{B}(t)$ or v satisfies $\mathscr{C}(t)$, by the induction hypothesis

   (e) v' satisfies $\sim \mathscr{B}(t) \to \mathscr{C}(t)$, by Definition 3.20

   (f) v' satisfies $\mathscr{A}(x_i)$, by definition of $\mathscr{A}(x_i)$

3. The *wf* $\mathscr{A}(x_i)$ is $(\forall x_j)\mathscr{B}(x_i)$, where $i \neq j$ because x_i is assumed to occur free in $\mathscr{A}$. Note that $\mathscr{B}(x_i)$ has fewer than k quantifiers and that $\mathscr{A}(t)$ is $(\forall x_j)\mathscr{B}(t)$. Then the following are all equivalent.

   (a) v satisfies $\mathscr{A}(t)$, by assumption

   (b) v satisfies $(\forall x_j)\mathscr{B}(t)$, by definition of $\mathscr{A}(t)$

   (c) any j-equivalent valuation to v satisfies $\mathscr{B}(t)$, by Definition 3.20

   (d) any j-equivalent valuation to v' satisfies $\mathscr{B}(x_i)$, by the induction hypothesis, and the note below

   (e) v' satisfies $(\forall x_j)\mathscr{B}(x_i)$, by Definition 3.20

   (f) v' satisfies $\mathscr{A}(x_i)$, by definition of $\mathscr{A}(x_i)$

Additional detail must be given to show that (c) and (d) are equivalent.

$\Rightarrow$ Suppose that any j-equivalent valuation to v satisfies $\mathscr{B}(t)$. Then let w' be a valuation j-equivalent to v'. Let w be a valuation j-equivalent to v with $w(x_j) = w'(x_j)$ that necessarily satisfies $\mathscr{B}(t)$. By construction, we have that w is i-equivalent to w'. Notice that $v'(x_i) = v'(t)$, so $w'(x_i) = w'(t)$, since w' is j-equivalent to v', and so we may apply the inductive hypothesis. Therefore, w' satisfies $\mathscr{B}(x_i)$.

$\Leftarrow$ Suppose that any j-equivalent valuation to v' satisfies $\mathscr{B}(x_i)$. Then let w be a valuation j-equivalent to v. Let w' be a valuation j-equivalent to v' with $w'(x_j) = w(x_j)$ that necessarily satisfies $\mathscr{B}(x_i)$. By construction, we have that w' is i-equivalent to w. Notice that $v'(x_i) = v'(t)$, so $w'(x_i) = w'(t)$, since w' is j-equivalent to w, and so we may apply the inductive hypothesis. Therefore, w satisfies $\mathscr{B}(t)$.

By verifying all three cases, we have completed the induction. □

Note. In the proof in the book, there is a mistake in Case 1, it should instead read: "$\mathscr{A}(x_i)$ is $\sim \mathscr{B}(x_i)$".

Definition 3.24. A *wf* $\mathscr{A}$ is true in an interpretation I if every valuation in I satisfies $\mathscr{A}$. It is *false* if there is no valuation in I which satisfies $\mathscr{A}$. If $\mathscr{A}$ is true in I, we write $I \models \mathscr{A}$.
Note. By part (ii) of Definition 3.20, if a given *wf* is satisfied by all valuations, then its negation is not satisfied by all valuations and vice versa. So no *wf* can be both true and false.
Note. Some *wf*s can be neither true nor false if there exists a valuation satisfying it and another one satisfying its negation.

Proposition 3.26. If, in an interpretation I, the *wf* $\mathscr{A}$ and $(\mathscr{A} \to \mathscr{B})$ are true, then $\mathscr{B}$ is also true.

Proof. Let v be a valuation in I. The *wf*s $\mathscr{A}$ and $(\mathscr{A} \to \mathscr{B})$ are true in I, which is to say that they are true for any valuation, and thus true for v. Since v satisfies $(\mathscr{A} \to \mathscr{B})$, it either satisfies $\mathscr{B}$ or $(\sim \mathscr{A})$. But it cannot satisfy $(\sim \mathscr{A})$, or else it would not satisfy $\mathscr{A}$. Therefore, it satisfies $\mathscr{B}$. Since v was chosen as an arbitrary valuation, every valuation satisfies $\mathscr{B}$, and so it is true in I. □

Proposition 3.27. Let $\mathscr{A}$ be a *wf* of $\mathscr{L}$, and let I be an interpretation of $\mathscr{L}$. Then $I \models \mathscr{A}$ if and only if $I \models (\forall x_i)\mathscr{A}$, where x_i is any variable.

Proof. $\Rightarrow$ Suppose that $I \models \mathscr{A}$. Let v be any valuation in I and let v' be any i-equivalent valuation to v. Since all valuations satisfy $\mathscr{A}$, v' satisfies $\mathscr{A}$. Therefore, v, which was chosen to be an arbitrary valuation, satisfies $(\forall x_i)\mathscr{A}$, and so all valuations in I satisfy $(\forall x_i)\mathscr{A}$.

$\Leftarrow$ Suppose that $I \models (\forall x_i)\mathscr{A}$. Let v be any valuation in I. Since v is i-equivalent to v, it must satisfy $\mathscr{A}$. Since v was chosen as an arbitrary valuation, all valuations in I satisfy $\mathscr{A}$. □

Corollary 3.28. Let $y_1, \ldots, y_n$ be variables in $\mathscr{L}$, let $\mathscr{A}$ be a *wf* of $\mathscr{L}$, and let I be an interpretation. Then $I \models \mathscr{A}$ if and only if $I \models (\forall y_1) \ldots (\forall y_n)\mathscr{A}$.

Proof. By repeated application of Proposition 3.27. □

The above corollary is significant because it states that implicit quantification of variables is legitimate when a statement of an interpretation is known to be true. For example, $x = x$ as a statement about the integers does not need be quantified because it is known that the statement alone is true. Similarly, if a true statement already has all of its variables quantified, then the quantifiers can be omitted with no loss of meaning. It also implies that adding quantifiers to a false or indeterminate *wf* cannot "upgrade" its truth value so that the new quantified *wf* is true. However, adding quantifiers can turn an indeterminate *wf* into one which is false (there are many examples of this).

Proposition 3.29. In an interpretation I, a valuation v satisfies the formula $(\exists x_i)\mathscr{A}$ if and only if there is at least one valuation v' which is i-equivalent to v and which satisfies $\mathscr{A}$.

Proof. This proof is done by mechanically applying the definitions. Let v be a valuation in an interpretation I.

$\Rightarrow$ Suppose v satisfies the formula $(\exists x_i)\mathscr{A}$, which is to say that v satisfies $\sim (\forall x_i)(\sim \mathscr{A})$, and therefore v does not satisfy $(\forall x_i)(\sim \mathscr{A})$. Therefore there must exist some v' which i-equivalent to v which does not satisfy $\sim \mathscr{A}$, and so this v' must satisfy $\mathscr{A}$.

$\Leftarrow$ Suppose that v' is an i-equivalent valuation to v that satisfies $\mathscr{A}$. Then this v' does not satisfy $(\sim \mathscr{A})$, and so v does not satisfy $(\forall x_i)(\sim \mathscr{A})$, and so v must satisfy $\sim (\forall x_i)(\sim \mathscr{A})$, i.e., v satisfies $(\exists x_i)\mathscr{A}$. □

A *wf* of L and a *wf* of $\mathscr{L}$ are both formed by possibly using the connectives $\sim$ and $\to$. If we take a *wf* $\mathscr{A}$ in L and replace all of its statement letters by the same *wf* in $\mathscr{L}$, the new formula is now a *wf* in $\mathscr{L}$, and we call it a *substitution instance* of $\mathscr{A}$ in $\mathscr{L}$.

Note that a *wf* in $\mathscr{L}$ can be a substitution instance of more than one *wf* in L, depending on how its sub-formulas are replaced. For instance,

$$\underbrace{((\forall x_i)A_1^1(x_1)}_{p_1} \to \underbrace{((\forall x_i)A_1^2(x_1)}_{p_2} \to \underbrace{(\forall x_i)A_1^2(x_1)))}_{p_3}$$

may be considered as a substitution instance of $(p_1 \to (p_2 \to p_3))$. Also,

$$\underbrace{((\forall x_i)A_1^1(x_1)}_{p_1} \to \underbrace{((\forall x_i)A_1^2(x_1) \to (\forall x_i)A_1^2(x_1)))}_{p_2}$$

may be considered as a substitution instance of $(p_1 \to p_2)$.

The use of the term tautology may be expanded to $\mathscr{L}$, and it has the expected property of being true regardless of its valuation in any interpretation.

Definition 3.30. A *wf* $\mathscr{A}$ of $\mathscr{L}$ is a *tautology* if it is a substitution instance in $\mathscr{L}$ of a tautology in L.

Proposition 3.31. A *wf* of $\mathscr{L}$ which is a tautology is true in any interpretation of $\mathscr{L}$.

Proof. Let $\mathscr{A}_{\mathscr{L}}$ be a tautology in $\mathscr{L}$ and let $\mathscr{A}_L$ be its corresponding tautology in L. Then $\mathscr{A}_L$ consists of the statement letters $p_1, \ldots, p_n$ whose replacements in L are the *wf*s that we shall label $\mathscr{A}_1, \ldots, \mathscr{A}_n$.

Now let $v_{\mathscr{L}}$ be a valuation in any interpretation I. The goal is to prove that $v_{\mathscr{L}}$ satisfies $\mathscr{A}_{\mathscr{L}}$.

First notice that $\mathscr{A}_L$ can only be evaluated as true or false if its statement letters have values, and to this end. So let v_L be the valuation in L defined on the statement letters $p_1, \dots, p_n$ in an expected way:

$$v_L(p_i) = \begin{cases} T & \text{if } v_{\mathscr{L}} \text{ satisfies } \mathscr{A}_i \\ F & \text{if } v_{\mathscr{L}} \text{ does not satisfy } \mathscr{A}_i \end{cases}$$

The values of v_L for all other statement letters not appearing in $\mathscr{A}_L$ are arbitrarily set to T so that v_L is indeed a valuation.

Now we will prove that $v_{\mathscr{L}}$ satisfies $\mathscr{A}_{\mathscr{L}}$ if and only if $v_L(\mathscr{A}_L) = T$. From this result, the proof of the proposition will immediately follow. We proceed by strong induction on the number of connectives $\sim$ and $\rightarrow$ in $\mathscr{A}_L$:

Suppose as a hypothesis of string induction that if a *wf* in L has fewer than k connectives, then $v_{\mathscr{L}}$ satisfies the *wf* if and only if the value of v_L when applied to the substitution instance in $\mathscr{L}$ is T.

Now let the number of connectives of $\mathscr{A}_L$ be j. If $j = 0$, then $\mathscr{A}$ consists of a statement letter only, say p. By the definition of v_L, $v_L(p) = T$ if and only if $v_{\mathscr{L}}$ satisfies $\mathscr{A}_{\mathscr{L}}$, as desired. If $j > 0$, then there are two cases two consider:

1. The *wf* $\mathscr{A}_L$ is of the form $\sim \mathscr{B}_L$. Then $\mathscr{A}_{\mathscr{L}}$ is of the form $\sim \mathscr{B}_{\mathscr{L}}$, where $\mathscr{B}_{\mathscr{L}}$ is the substitution instance of $\mathscr{B}_L$. Since $\mathscr{B}_L$ has fewer than j connectives, by the induction hypothesis, v satisfies $\mathscr{B}$ if and only if $v'(\mathscr{B}_{\mathscr{L}}) = T$, which is equivalent to saying that v does not satisfy $\mathscr{B}$ if and only if $v'(\mathscr{B}_{\mathscr{L}}) = F$, which is once again equivalent, by Definition 3.20 (ii) and 2.12 (i) to saying that v satisfies $\mathscr{A}_{\mathscr{L}}$ if and only if $v(\mathscr{A}_L) = T$.

2. The *wf* $\mathscr{A}_L$ of the form $\mathscr{B}_L \rightarrow \mathscr{C}_L$, and so $\mathscr{A}$ is of the form $\mathscr{B}_{\mathscr{L}} \rightarrow \mathscr{C}_{\mathscr{L}}$, where $\mathscr{B}_{\mathscr{L}}$ and $\mathscr{C}_{\mathscr{L}}$ are the substitution instances of $\mathscr{B}_L$ and $\mathscr{C}_L$ respectively. Note that $\mathscr{B}_L$ and $\mathscr{C}_L$ both have fewer than j connectives. The following assertions are all equivalent:

   (a) $v_{\mathscr{L}}$ satisfies $\mathscr{A}_{\mathscr{L}}$

   (b) $v_{\mathscr{L}}$ satisfies $\mathscr{B}_{\mathscr{L}} \rightarrow \mathscr{C}_{\mathscr{L}}$

   (c) either $v_{\mathscr{L}}$ satisfies $\sim \mathscr{B}_{\mathscr{L}}$ or $\mathscr{C}_{\mathscr{L}}$ (by Definition 3.20 (iii))

   (d) either v does not satisfy $\mathscr{B}_{\mathscr{L}}$ or satisfies $\mathscr{C}_{\mathscr{L}}$ (by Definition 3.20 (ii))

   (e) either $v_L(\mathscr{B}_L) = F$ or $v_L(\mathscr{C}_L) = T$ (by the strong induction hypothesis)

   (f) $v_L(\mathscr{B}_L \rightarrow \mathscr{C}_L) = T$ (by Definition 2.12)

   (g) $v_L(\mathscr{A}_L) = T$

   and the equivalence of (a) and (g) is what we desired to prove for this case.

Now with the induction complete, we can prove the original proposition. Recall that $\mathscr{A}_{\mathscr{L}}$ is a tautology in $\mathscr{L}$, $\mathscr{A}_L$ is a tautology in L, and $v_{\mathscr{L}}$ is an arbitrary valuation in an arbitrary interpretation I. From the above, we know that $v_{\mathscr{L}}$ satisfies $\mathscr{A}_{\mathscr{L}}$ if and only if $v_L(\mathscr{A}_L) = T$. But $\mathscr{A}_L$ is a tautology in L, so indeed $v_L(\mathscr{A}_L) = T$, and so $v_{\mathscr{L}}$ satisfies $\mathscr{A}_{\mathscr{L}}$. Thus $\mathscr{A}_{\mathscr{L}}$ is true in any interpretation I. □

Note. This proof is long, but also is mostly just straightforward applications of definition. Its length comes from having to define v_L
Note. The need for strong induction comes from case 2. Normal induction would not be sufficient because both of the *wf*s in L might have fewer than $j-1$ connectives.

As stated in the warning at the beginning of this chapter (in the manual, not the textbook), if a *wf* has all of its variables quantified, then it must be either true or false. We will prove this shortly, but first we introduce a short definition and a proposition.

Definition 3.32. A *wf* $\mathscr{A}$ of $\mathscr{L}$ is said to be *closed* if all variables in $\mathscr{A}$ occur bound.

Proposition 3.33. Let I be an interpretation of $\mathscr{L}$ and let $\mathscr{A}$ be a *wf* of $\mathscr{L}$. If v and w are valuations such that $v(x_i) = w(x_i)$ for every free variable x_i of $\mathscr{A}$, then v satisfies $\mathscr{A}$ if and only if w satisfies $\mathscr{A}$.
Note. This is stating the obvious fact that if two valuations "plug in" the same values for variables, then the resulting truth values will be the same.

Proof. The proof follows from strong induction on the numbers of connectives and quantifiers in $\mathscr{A}$.

As a hypothesis of strong induction, suppose that for any *wf* $\mathscr{A}$ of $\mathscr{L}$ with fewer than n connectives, v satisfies $\mathscr{A}$ if and only if w satisfies $\mathscr{A}$, where v and w are valuations such that $v(x_i) = w(x_i)$ for any x_i of $\mathscr{A}$.

It may be the case that $n = 0$, in which case the *wf* is an atomic formula with j terms of the general form $A_i^j(t_1, \ldots, t_j)$. A term t can either be a constant, in which case $v(t) = w(t)$, since all are defined to have the same values for constants, or the term can be a variable or a function which takes terms. Since v and w agree for variables, since any variable in the atomic formula occurs free, they must also agree for functions (this can be formalized via another induction, but that is tedious). Therefore, for any atomic formula $\mathscr{A}$, v satisfies $\mathscr{A}$ if and only if w satisfies $\mathscr{A}$.

It may be the case that $n > 0$, in which case the inductive hypothesis must be employed to prove the three distinct cases which may occur.

1. The *wf* $\mathscr{A}$ is of the form $\sim \mathscr{B}$. Notice that $\mathscr{B}$ has fewer than n connectives, so v satisfies $\mathscr{B}$ if and only if w satisfies $\mathscr{B}$, which is to say that v does not satisfy $\mathscr{B}$ if and only if w does not satisfy $\mathscr{B}$, which is once again equivalent to stating that v satisfies $\sim \mathscr{B}$ if and only if w satisfies $\sim \mathscr{B}$, by Definition 3.20 (ii). And since $\sim \mathscr{B}$ is $\mathscr{A}$, we have proved the desired property for this case.

2. The *wf* $\mathscr{A}$ is of the form $\mathscr{B} \rightarrow \mathscr{C}$. The following are all equivalent:

   (a) v satisfies $\mathscr{A}$

   (b) v satisfies $\mathscr{B} \rightarrow \mathscr{C}$

   (c) v satisfies $\sim \mathscr{B}$ or v satisfies $\mathscr{C}$, by Definition 3.20 (iii)

   (d) w satisfies $\sim \mathscr{B}$ or w satisfies $\mathscr{C}$, by the induction hypothesis, and the fact that that both $\sim \mathscr{B}$ and $\mathscr{C}$ have fewer than n connectives

   (e) w satisfies $\mathscr{B} \rightarrow \mathscr{C}$, again by definition 3.20 (ii)

   (f) w satisfies $\mathscr{A}$

   and the equivalence between (a) and (f) is what we desired to prove for this case.

3. The *wf* $\mathscr{A}$ is of the form $(\forall x_i)\mathscr{B}$. We are to prove that v satisfies $\mathscr{A}$ if and only if w satisfies $\mathscr{A}$.

   $\Rightarrow$ Suppose that v satisfies $\mathscr{A}$. Then for any i-equivalent valuation to v, v' satisfies $\mathscr{B}$. To show that w satisfies $\mathscr{A}$, which is $(\forall x_i)\mathscr{B}$, we must show that any i-equivalent valuation to w satisfies $\mathscr{B}$. So let w' be i-equivalent to w, and let v' be the particular valuation i-equivalent to v which satisfies $v'(x_i) = w'(x_i)$. Now let y be a free variable of $\mathscr{B}$. There are two cases to consider.

   (a) If $y = x_i$, then $v'(x_i) = w'(x_i)$, since v' was chosen in this way.

   (b) If $y \neq x_i$, then it is a free variable of $\mathscr{A}$, since $\mathscr{B}$ differs from $\mathscr{A}$ in that only x_i may potentially be free in $\mathscr{B}$, and so

$$\begin{aligned} v'(y) &= v(y) && v' \text{ and } v \text{ are } i\text{-equivalent} \\ v(y) &= w(y) && v(x) = w(x) \text{ for any free variable } x \text{ in } \mathscr{A} \\ w(y) &= w'(y) && w' \text{ and } w \text{ are } i\text{-equivalent} \end{aligned}$$

   with the conclusion in this case being that $v'(y) = w'(y)$.

   Therefore, whenever y is a free variable of $\mathscr{B}$, a *wf* with fewer than n connectives, $v'(y) = w'(y)$, and so by the induction hypothesis and since v' satisfies $\mathscr{B}$, w' satisfies $\mathscr{B}$. Since w' was chosen to be an arbitrary i-equivalent valuation to w, it follows that w satisfies $(\forall x_i)\mathscr{B}$, i.e., w satisfies $\mathscr{A}$.

   $\Leftarrow$ This direction is proved in precisely the same way as the above direction except with the occurrences of v and w switched.

With the induction complete, we have proved the proposition. □

Note. In case 3, x_i need not be free in $\mathscr{B}$, in which the quantifier $(\forall x_i)$ appears in $\mathscr{B}$, but in that case x_i would not be considered as a possible free variable y in $\mathscr{B}$, so it would be disregarded.
Note. In case 1, the free variables of $\mathscr{A}$ were the same as the free variables of $\mathscr{B}$. Similarly, in case 2, the free variables of $\mathscr{B}$ and $\mathscr{C}$ were the same as $\mathscr{A}$. Therefore, in both cases, v and w could be applied to the inductive hypothesis regarding $\mathscr{B}$ in case 2 or $\mathscr{B}$ and $\mathscr{C}$ in case 3. In case 3, on the other hand, the free variables of $\mathscr{A}$ and $\mathscr{B}$ differed in that x_i need not have been free in $\mathscr{B}$. Instead, i-equivalent valuations of v and w were shown to agree for any free variable in $\mathscr{B}$ so that the inductive hypothesis could be applied.

Corollary 3.34. If $\mathscr{A}$ is a closed *wf* of $\mathscr{L}$ and I is an interpretation of $\mathscr{L}$, then either $I \models \mathscr{A}$ or $I \models (\sim \mathscr{A})$.

Proof. Let v and w be any valuations. Since $\mathscr{A}$ has no free variables, $v(y) = w(y)$ for any free variable y, vacuously. So v satisfies $\mathscr{A}$ if and only if w satisfies $\mathscr{A}$, by Proposition 3.33. So, either every valuation satisfies $\mathscr{A}$ or every valuation does not satisfy $\mathscr{A}$, which is to say that $\mathscr{A}$ is either true or false in I. So either $I \models \mathscr{A}$ or $I \models (\sim \mathscr{A})$. □

Definition 3.35. A *wf* $\mathscr{A}$ of $\mathscr{L}$ is *logically valid* if $\mathscr{A}$ is true in every interpretation of $\mathscr{L}$ and is *contradictory* if $\mathscr{A}$ is false in every interpretation of $\mathscr{L}$.

These terms are the analogues of tautology and contradiction in L. However, there are more logically valid *wf*s in $\mathscr{L}$ than there are tautologies in $\mathscr{L}$ in the sense that all tautologies in $\mathscr{L}$ are logically valid (Proposition 3.31), but there are some logically valid *wf*s that are not tautologies, i.e., their logical validity comes not from their form involving but $\sim$ and $\rightarrow$ but rather from the relationship between quantifiers and terms. The goal of the next chapter is to find all of these logically valid *wf*s.

Solutions to exercises

14. (a) The corresponding statement in N is $x_1 + x_1 = x_2 \times x_3$. Any valuation v with $v(x_1) = v(x_2) = v(x_3) = 0$ will satisfy the *wf*, and any valuation v with $v(x_1) = v(x_2) = v(x_3) = 1$ will not satisfy the *wf*.

    (b) The corresponding statement in N is $x_1 + 0 = x_2 \rightarrow x_1 + x_2 = x_3$. Any valuation v with $v(x_1) = v(x_2) = v(x_3) = 0$ will satisfy the *wf*, and any valuation v with $v(x_1) = v(x_2) = v(x_3) = 1$ will not satisfy the *wf*.

    (c) The corresponding statement in N is $\sim (x_1x_2 = x_2x_3)$. Any valuation v with $v(x_1) = 0, v(x_2) = v(x_3) = 1$ will satisfy the *wf*, and any valuation v with $v(x_1) = v(x_2) = v(x_3) = 1$ will not satisfy the *wf*.

    (d) The corresponding statement in N is $(\forall x_1)x_1x_2 = x_3$. Any valuation v with $v(x_2) = v(x_3) = 0$ will satisfy the *wf*, and any valuation v with $v(x_2) = v(x_3) = 1$ will not satisfy the *wf*.

    (e) The corresponding statement in N is $((\forall x_1)x_1 \times 0 = x_1) \rightarrow x_1 = x_2$. Since $(\forall x_1)x_1 \times 0 = x_1$ is false in N, any valuation will vacuously satisfy the *wf*, and so no valuation will not satisfy the *wf*.

15. (a) The corresponding statement is $x_1 < 0$. Any valuation v with $v(x_1) = -1$ will satisfy the *wf*, and any valuation v with $v(x_1) = 1$ will not satisfy the *wf*.

    (b) The corresponding statement is $x_1 - x_2 < x_1 \rightarrow 0 < x_1 - x_2$. Any valuation v with $v(x_1) = v(x_2) = 0$ will satisfy the *wf*, and any valuation v with $v(x_1) = v(x_2) = 1$ will not satisfy the *wf*.

    (c) The corresponding statement is $\sim (x_1 < x_1 - (x_1 - x_2))$. Any valuation v with $v(x_1) = v(x_2) = 0$ will satisfy the *wf*, and any valuation v with $v(x_1) = 0, v(x_2) = 1$ will not satisfy the *wf*.

    (d) The corresponding statement is $(\forall x_1)x_1 - x_2 < x_3$, which is false, so no valuation will satisfy the *wf*, and any valuation will not satisfy the *wf*.

    (e) The corresponding statement is $((\forall x_1)x_1 - 0 < x_1) \rightarrow x_1 < x_2$. Since $((\forall x_1)x_1 - 0 < x_1)$ is false, any valuation will vacuously satisfy the *wf*, and no valuation will not satisfy the *wf*.

16. Only the *wf*s (b), (c), and (d) are true in the interpretation.

17. Only the *wf*s (c) and (d) are true in the interpretation.

18. We are to prove that in an interpretation I, a *wf* $(\mathscr{A} \rightarrow \mathscr{B})$ is false if and only if $\mathscr{A}$ is true and $\mathscr{B}$ is false. Let v be a valuation in I. The following are all equivalent statements.

(a) $(\mathscr{A} \to \mathscr{B})$ is false

(b) v does not satisfy $(\mathscr{A} \to \mathscr{B})$, by (a)

(c) v does not satisfy $(\sim \mathscr{A})$ and v does not satisfy $\mathscr{B}$, by Definition 3.20 (iii)

(d) v satisfies $\mathscr{A}$ and v does not satisfy $\mathscr{B}$, by Definition 3.20 (ii)

(e) $\mathscr{A}$ is true and $\mathscr{B}$ is false, by Definition 3.24

Note that (e) is true since v is an arbitrary valuation. The equivalence between (a) and (e) is what we set out to prove.

19. In the following lemma and sub-exercises, let I be any interpretation and let v be any valuation in I.

Lemma. Let $\mathscr{A}$ and $\mathscr{B}$ be *wf*s of $\mathscr{L}$. Let $\star$ be the implication "if v satisfies $\mathscr{A}$, then v satisfies $\mathscr{B}$". If $\star$ is true, then $\mathscr{A} \to \mathscr{B}$ is logically valid.

Proof. Suppose that the implication $\star$ is true. Then there are two cases to consider.

(i) The valuation v satisfies $\mathscr{A}$. By $\star$, v satisfies $\mathscr{B}$, and therefore by Definition 3.20 (iii), v satisfies $\mathscr{A} \to \mathscr{B}$.

(ii) The valuation v does not satisfy $\mathscr{A}$. By Definition 3.20 (ii), v satisfies $\sim \mathscr{A}$. By Definition 3.20 (iii), v satisfies $\mathscr{A} \to \mathscr{B}$.

We have proved that v, an arbitrary valuation in an arbitrary interpretation, always satisfies $\mathscr{A} \to \mathscr{B}$. Therefore, $\mathscr{A} \to \mathscr{B}$ is logically valid. □

Note. This lemma can be more succinctly stated as "if $\mathscr{A}$ being true in any I implies that $\mathscr{B}$ is true in any I, then $\mathscr{A} \to \mathscr{B}$ is logically valid." Also notice that the relationship is an "if and only if", and a little more work could be done to prove the other direction.

This lemma confirms that the logical validity of a *wf* of the form $\mathscr{A} \to \mathscr{B}$ can be proved in the expected way. Using this lemma, we now prove that the *wf*s in (a), (b), (c) and (d) are logically valid.

(a) Suppose that v satisfies $(\exists x_1)(\forall x_2)A_1^2(x_1, x_2)$. By Proposition 3.29, there is a valuation v' which is 1-equivalent to v which satisfies $(\forall x_2)A_1^2(x_1, x_2)$. By Definition 3.20 (iv), any 2-equivalent valuation to v' satisfies $A_1^2(x_1, x_2)$ $(*)$.
Now, let w be 2-equivalent to v. The goal is to show the existence of a valuation which is 1-equivalent to w and satisfies $A_1^2(x_1, x_2)$. So let w' be the valuation which is 2-equivalent to v' with $w'(x_2) = w(x_2)$. By $(*)$, w' satisfies $A_1^2(x_1, x_2)$. Now let x be any element in the domain of w' which is not x_1. There are two cases to consider.

i. It may be that $x = x_2$, in which case, by construction of w', $w'(x) = w(x)$.

ii. Otherwise, $x \neq x_2$. Since w' is 2-equivalent to v', $w'(x) = v'(x)$. Since v' is 1-equivalent to v, and since x is assumed not to be x_1, we have $v'(x) = v(x)$. Since w is 2-equivalent to v, we have $v(x) = w(x)$. Finally, by the chaining the equalities, $w'(x) = v'(x) = v(x) = w(x)$.

Therefore, w' is 1-equivalent to w and satisfies $A_1^2(x_1, x_2)$, and by Proposition 3.29, $(\forall x_2)(\exists x_1)A_1^2(x_1, x_2)$. By the lemma above, we may conclude that $((\exists x_1)(\forall x_2)A_1^2(x_1, x_2) \to (\forall x_2)(\exists x_1)A_1^2(x_1, x_2))$.

Note. In the following sub-exercises for the sake of brevity, the lemma, Definition 3.20, and Proposition 3.29 will not be explicitly referenced when they are used.

(b) We will first demonstrate that if $(\forall x_1)A_1^1(x_1)$ is true in I, then $(\forall x_2)A_1^1(x_2)$ is true in I.

Suppose that v satisfies $(\forall x_1)A_1^1(x_1)$. Then any 1-equivalent valuation to v satisfies $A_1^1(x_1)$. Let v_2 be a 2-equivalent valuation to v. Let v_1 be the 1-equivalent valuation with $v_1(x_1) = v_2(x_2)$, which must necessarily satisfy $A_1^1(x_1)$, which is a *wf* in which x_2 is free for x_1. By Proposition 3.23, v_2 satisfies $A_1^1(x_2)$ if and only if v_1 satisfies $A_1^1(x_1)$. Since v_1 does indeed satisfy $A_1^1(x_1)$, v_2 must satisfy $A_1^1(x_2)$. Therefore, v satisfies $(\forall x_2)A_1^1(x_2)$, as desired.

Now, we will prove that the original *wf* is logically valid. Suppose that v satisfies $(\forall x_1)A_1^1(x_1)$. By the above, we know that v satisfies $(\forall x_2)A_1^1(x_2)$, and therefore it satisfies $((\forall x_1)A_2^1(x_1) \to (\forall x_2)A_1^1(x_2))$, and so we may conclude that $(\forall x_1)A_1^1(x_1) \to ((\forall x_1)A_2^1(x_1) \to (\forall x_2)A_1^1(x_2))$ is logically valid.

(c) Suppose that v satisfies $(\forall x_1)(\mathscr{A} \to \mathscr{B})$. There are two cases to consider.

i. It may be that v satisfies $\sim (\forall x_i)\mathscr{A}$. Then v satisfies $(\forall x_i)\mathscr{A} \to (\forall x_i)\mathscr{B}$.

ii. Otherwise, v satisfies $(\forall x_i)\mathscr{A}$. Now let v' be 1-equivalent to v. It must satisfy $\mathscr{A}$, and therefore it cannot satisfy $\sim \mathscr{A}$. But since v also satisfies $(\forall x_1)(\mathscr{A} \to \mathscr{B})$, v' must satisfy $\mathscr{B}$ if it does not satisfy $\sim \mathscr{A}$. Therefore, v must satisfy $(\forall x_i)\mathscr{B}$, and so v must satisfy $(\forall x_i)\mathscr{A} \to (\forall x_i)\mathscr{B}$.

In both cases, $(\forall x_i)\mathscr{A} \to (\forall x_i)\mathscr{B}$, and so we may conclude that

$$(\forall x_1)(\mathscr{A} \to \mathscr{B}) \to ((\forall x_1)\mathscr{A} \to (\forall x_1)\mathscr{B}).$$

Note. This proof relies on applying Definition 3.20 (iii) repeatedly.

(d) Suppose that v satisfies $(\forall x_1)(\forall x_2)\mathscr{A}$. Then

(i) any valuation v' which is 1-equivalent to v satisfies $(\forall x_2)\mathscr{A}$ and...

(ii) any valuation which is 2-equivalent to v' satisfies $\mathscr{A}$.

Now let w be a valuation which is 2-equivalent to v and let w' be a valuation that is 1-equivalent to w. The goal is to show that w' satisfies $\mathscr{A}$, from which we may deduce that w satisfies $(\forall x_1)\mathscr{A}$ and hence v satisfies $(\forall x_2)(\forall x_1)\mathscr{A}$.

Let v' be a valuation which is 1-equivalent to v with $v'(x_1) = w'(x_1)$. Then by (i), v' satisfies $(\forall x_2)\mathscr{A}$. Now let x be any element in the domain of w' that is not x_2. There are two cases to consider.

(1) It may be that $x = x_1$, in which case, by construction of v', $v'(x) = w'(x)$.

(2) Otherwise, $x \neq x_1$, so

$$\begin{aligned} v'(x) &= v(x), && \text{since } v' \text{ is 1-equivalent to } v \\ v(x) &= w(x), && \text{since } w \text{ is 2-equivalent to } w \\ w(x) &= w'(x), && \text{since } w' \text{ is 1-equivalent to } w \end{aligned}$$

and thus, $v'(x) = w'(x)$ in this case as well.

In both cases, we can see that $v'(x) = w'(x)$, and therefore w' is 2-equivalent to v'. By (ii), we may conclude that w' satisfies $\mathscr{A}$, as desired.

20. One example is $A_1^1(x_1) \to A_1^1(x_1)$. It is not closed, but it is a tautology since it is a substitution instance of $p_1 \to p_1$. Therefore, it is logically valid.

21. Suppose that v is a valuation in an interpretation I that satisfies $\mathscr{A}(t)$. Let v' be i-equivalent to v with $v'(x_i) = v(t)$. By Proposition 3.23, v' must satisfy $\mathscr{A}(x_i)$. By Proposition 3.29, v must satisfy $(\exists x_i)\mathscr{A}(x_i)$. By the lemma in Exercise 19, $\mathscr{A}(t) \to (\exists x_i)\mathscr{A}(x_i)$ is logically valid.

22. Let I be the interpretation with the integers as the domain, $\overline{a}_0 = 0$, the relation $\leq$ as A_1^2, and the relation $= 0$ as A_1^1. Note that A_1^1 does not involve $\overline{a}_0 = 0$, since the relation is just the set $\{(0, 0)\}$. Then the given *wf*s (a) - (d) correspond to the following *wf*s.

    (a) $((\forall x_1)(\exists x_2)\ x_1 \leq x_2) \to ((\exists x_2)(\forall x_1)\ x_1 \leq x_2)$

    (b) $(\forall x_1)(\forall x_2)(x_1 \leq x_2 \to x_2 \leq x_1)$

    (c) $(\forall x_1)(\sim (x_1 = 0)) \to (\sim (x_1 = 0))$

    (d) $(\forall x_1)(x_1 \leq x_1) \to ((\exists x_2)(\forall x_1)\ x_1 \leq x_2)$

    These statements in I are all easily seen to be false, and therefore, none of the *wf*s are logically valid.

23. This follows immediately from Proposition 3.23, since if v satisfies $v(x_i) = v(t)$, then it itself is an i-equivalent valuation v' to v with $v'(x_i) = v(t)$.

    Note. In the textbook, Proposition 3.23 is not proved fully, and the remainder is left as an exercise, but in this manual it is proved fully, so there is no need to elaborate more on it here.

Chapter 4

Formal predicate calculus

4.1 The formal system $K_{\mathscr{L}}$

In the previous chapter, we discussed various *wf*s which were valid in all first-order languages. Depending on the interpretations of the language, the *wf*s could be true or false. Some *wf*s were seen to be true regardless of the interpretation, and these *wf*s were said to be logically valid. In this chapter, we will construct a formal system which will allow deduction of other *wf*s from certain *wf*s. The fundamental property of this system that will be proved is that its theorems are precisely the *wf*s which are logically valid.

Let $\mathscr{L}$ be a first order language. The formal system $K_{\mathscr{L}}$ has, as its alphabet of symbols, the same alphabet of symbols as $\mathscr{L}$.

Let $\mathscr{A}$ and $\mathscr{B}$ be *wf*s of $\mathscr{L}$. The axioms of $K_{\mathscr{L}}$ are given by the following schemes.

- (K1) $(\mathscr{A} \to (\mathscr{B} \to \mathscr{A}))$.
- (K2) $((\mathscr{A} \to (\mathscr{B} \to \mathscr{C})) \to ((\mathscr{A} \to \mathscr{B}) \to (\mathscr{A} \to \mathscr{C})))$.
- (K3) $(((\sim \mathscr{A}) \to (\sim \mathscr{B})) \to (\mathscr{B} \to \mathscr{A}))$.
- (K4) $((\forall x_i)\mathscr{A} \to \mathscr{A})$, if x_i does not occur free in $\mathscr{A}$.
- (K5) $((\forall x_i)\mathscr{A}(x_i) \to \mathscr{A}(t))$, if t is free for x_i in $\mathscr{A}(x_i)$.
- (K6) $((\forall x_i)(\mathscr{A} \to \mathscr{B}) \to (\mathscr{A} \to (\forall x_i)\mathscr{B}))$, if $\mathscr{A}$ contains no free occurrences of x_i.

Note. The reason why the phrase "does not occur free in" is used is because a variable can occur either bound, free, or not occur whatsoever. In other words, "does not occur free in" means that a variable "occurs bound in" or "does not occur whatsoever in".

Note. In (K4) and (K6), it may aid understanding to note that a variable does not occur free in a *wf* if it occurs bound, in which case it can either not occur at all in a *wf*, or it occurs bound already. In both cases, the quantifier is redundant or meaningless. Therefore, (K4) allows the removal of an unnecessary quantifier while (K6) allows the quantifier in an implication to moved to only the consequent of the implication if the quantifier is unnecessary in the hypothesis.

Note. We may immediately deduce that $((\forall x_i)\mathscr{A} \to \mathscr{A})$ for any *wf* $\mathscr{A}$, regardless of whether x_i occurs free in $\mathscr{A}$ or not. For if x_i does not occur free in $\mathscr{A}$, then $((\forall x_i)\mathscr{A} \to \mathscr{A})$ is true by (K4). If x_i occurs free in $\mathscr{A}$, then we may write $\mathscr{A}(x_i)$, and since x_i is free for x_i in $\mathscr{A}(x_i)$, by (K6), we may deduce $((\forall x_i)\mathscr{A}(x_i) \to \mathscr{A}(x_i))$.

The rules of deduction of $K_{\mathscr{L}}$ are:

1. *Modus ponens*, from $\mathscr{A}$ and $(\mathscr{A} \to \mathscr{B})$, deduce $\mathscr{B}$.

2. *Generalization*, from $\mathscr{A}$, deduce $(\forall x_i)\mathscr{A}$, where x_i is any variable.

The second rule may be curious. It states that a quantifier may be added to a *wf* with no consequences in terms of logical deduction. Indeed, if the quantified variable is bound already in $\mathscr{A}$, then the addition of the quantifier will be redundant. But if the variable is free in $\mathscr{A}$, then $\mathscr{A}$ may be neither true nor false in some interpretation, so there may be a valuation in which $\mathscr{A}$ is true but $(\forall x_i)\mathscr{A}$ is false (a concrete example of this will be provided shortly). The consequence of this is that the Deduction Theorem for $\mathscr{L}$ must be restricted slightly, as we will see. However, the theorems of $K_{\mathscr{L}}$ will be shown to be the logically valid *wf*s of $\mathscr{L}$, so this issue will not arise as long as generalization is applied to a *wf* which is theorem of $K_{\mathscr{L}}$.

Definition 4.2. A *proof* in $K_{\mathscr{L}}$ is a sequence of *wf*s such that each *wf* is an axiom of $K_{\mathscr{L}}$ or a deduction from one or more of the previous *wf*s by one of the rules of deduction. A *theorem* of $K_{\mathscr{L}}$ is any *wf* which is the last member of a sequence of a proof in $K_{\mathscr{L}}$.

Let Γ be a set of *wf*s of $K_{\mathscr{L}}$. A *deduction from* Γ is a proof in $K_{\mathscr{L}}$ with any *wf* of Γ permitted as a *wf* in the sequence or proof. A *consequence* of Γ in $K_{\mathscr{L}}$ is the last member of a deduction from Γ.

We write $\Gamma \vdash_{K_{\mathscr{L}}} \mathscr{A}$ to denote that $\mathscr{A}$ is a consequence of Γ, and if Γ is empty, then $\mathscr{A}$ is just a theorem of $K_{\mathscr{L}}$, in which case we write $\vdash_{K_{\mathscr{L}}} \mathscr{A}$.

For the sake of convenience, we will abbreviate $K_{\mathscr{L}}$ to K unless there is reason to specify $\mathscr{L}$. Writing that a *wf* is a *wf* of K is to say that it is a *wf* of the unspecified first-order language associated with K.

Proposition 4.3. If $\mathscr{A}$ is a tautology (see Definition 3.30), then $\mathscr{A}$ is a theorem of K.

Proof. Recall that $\mathscr{A}$ must be a *wf* of $\mathscr{L}$ which is a substitution instance of a tautology in L, which is to say that there must be a $\mathscr{A}_L$ in L which is a tautology such that $\mathscr{A}$ is obtained by substituting the statement variables of L with *wf*s of $\mathscr{L}$. By Proposition 2.23, $\mathscr{A}_L$ must be a theorem of L. Therefore, there exists a proof in L of $\mathscr{A}_L$. In the proof, substitute each statement variable in L with the *wf* which was substituted for that statement variable to obtain $\mathscr{A}$ to obtain a sequence of *wf*s of K.

Consider a *wf* after this substitution. It could have been an axiom in L, in which case the substituted *wf* is an axiom of K since the axioms of L are given in (K1), (K2) and (K3). Otherwise, the *wf* was a result of MP and since MP is a rule of deduction in K, the substituted *wf* could be obtained from two previous *wf*s in the sequence after the substitution. Therefore, the sequence is a valid proof in K, and so $\mathscr{A}$ is a theorem of K. □

*Note.*As usual, this proof could be done via induction. In particular, the last paragraph could be verified in this way.

The converse of this proposition can easily be seen to false. For example, the *wf* $((\forall x_i)\mathscr{A} \to (\exists x_i)\mathscr{A})$ was seen to be logically valid in Example 3.37 for any first-order language $\mathscr{L}$. This *wf* in $K_{\mathscr{L}}$ is a substitution instance of the *wf* $(p_1 \to p_2)$ in L, which is not a tautology of L, and therefore the *wf* in $\mathscr{L}$ is not a tautology in $\mathscr{L}$. Later, we shall see that the theorems of $K_{\mathscr{L}}$ are the logically valid *wf*s of $\mathscr{L}$, and so the given *wf* disproves the converse of the proposition.

We will know prove that K has the basic property of being sound. That is, every theorem is logically valid. We start by proving the property for the axioms.

Proposition 4.4. All axioms of $K_{\mathscr{L}}$ are logically valid.

Proof. Let $\mathscr{C}$ be an axiom of $K_{\mathscr{L}}$. It may be the case that it is an instance of axioms (K1), (K2), or (K3). In this case, $\mathscr{C}$ must be a tautology, as it is a substitution instance of a tautology in L, and by Proposition 4.3, $\mathscr{C}$ must be logically valid. The other possibility is that $\mathscr{C}$ is an instance of the axiom schemes (K4), (K5), or (K6).

We implicitly use the lemma in exercise 19 of Section 3.4 to prove implications. Let v be a valuation in any interpretation of $\mathscr{L}$.

- For (K4), $((\forall x_i)\mathscr{A} \to \mathscr{A})$, suppose that v satisfies $(\forall x_i)\mathscr{A}$. Then any i-equivalent valuation to v satisfies $\mathscr{A}$, so, in particular, v satisfies $\mathscr{A}$. Therefore, (K4), $((\forall x_i)\mathscr{A} \to \mathscr{A})$ is logically valid.

- For (K5), $((\forall x_i)\mathscr{A}(x_i) \to \mathscr{A}(t))$ if t is free for x_i, suppose that v satisfies $(\forall x_i)\mathscr{A}(x_i)$ and that t is a term free for x_i. Then any i-equivalent valuation to v satisfies $\mathscr{A}(x_i)$. In particular, the i-equivalent valuation v' with $v'(x_i) = v(t)$ satisfies $\mathscr{A}(x_i)$, so by Proposition 3.23, v satisfies $\mathscr{A}(t)$. Therefore, (K5), $((\forall x_i)\mathscr{A}(x_i) \to \mathscr{A}(t))$, is logically valid.

- For (K6), $((\forall x_i)(\mathscr{A} \to \mathscr{B}) \to (\mathscr{A} \to (\forall x_i)\mathscr{B}))$ if $\mathscr{A}$ contains no free occurrence of the variable x_i, suppose that v satisfies $(\forall x_i)(\mathscr{A} \to \mathscr{B})$ and that x_i does not occur free in $\mathscr{A}$. Then every i-equivalent valuation to v satisfies $(\mathscr{A} \to \mathscr{B})$, which is to say that it must either not satisfy $\mathscr{A}$ or satisfy $\mathscr{B}$, by Definition 3.20, and we label this statement as $\star$.

  The goal is to show that v satisfies $(\mathscr{A} \to (\forall x_i)\mathscr{B})$, as doing this will demonstrate the logical validity of (K6), so suppose that v satisfies $\mathscr{A}$. Now, let w be an i-equivalent valuation to v. Notice that v satisfies $\mathscr{A}$ by assumption, so by Proposition 3.33 and the fact that x_i does not occur free in $\mathscr{A}$, w must also satisfy $\mathscr{A}$, and so by $\star$, w must satisfy $\mathscr{B}$, which allows us to say that v satisfies $(\forall x_i)\mathscr{B}$. We may conclude that v satisfies $(\mathscr{A} \to (\forall x_i)\mathscr{B})$, as desired.

We have shown that any instance of the axiom schemes of $K_{\mathscr{L}}$ are logically valid, i.e., any axiom of $K_{\mathscr{L}}$ is logically valid. □

Proposition 4.5 (The Soundness Theorem for K)**.** If $\mathscr{A}$ is a theorem of K, then $\mathscr{A}$ is logically valid.

Proof. The proof is by strong induction on n, the number of *wf*s in the sequence consisting of the proof of $\mathscr{A}$. As a hypothesis of strong induction, suppose that any theorem of K with fewer than n *wf*s in its proof is logically valid.

(base case) It may be the case that $n = 1$, which is to say that $\mathscr{A}$ is an axiom of K, and so by the previous proposition, $\mathscr{A}$ is logically valid.

(induction step) Alternatively, $n > 1$. It may still be the case that $\mathscr{A}$ is an axiom of K, in which case it is logically valid. If it is not an axiom, then it follows from one of the two rules of deduction.

1. In the case that $\mathscr{A}$ follows from MP and two *wf*s, one *wf* must necessarily be of the form $\mathscr{B}$ and the other of the form $(\mathscr{B} \to \mathscr{A})$. By the induction hypothesis, both of these *wf*s are logically valid, and so by Remark 3.36(a) (which, in turn, is a consequence of Proposition 3.26), $\mathscr{A}$ must be logically valid.

2. In the case that $\mathscr{A}$ follows from Generalization from a previous *wf* $\mathscr{B}$, $\mathscr{A}$ must necessarily be of the form $(\forall x_i)\mathscr{B}$. Since, by the induction hypothesis, $\mathscr{B}$ is logically valid, $\mathscr{A}$ must be logically valid by Remark 3.36(b) (which, in turn, is a consequence of Proposition 3.26).

We have shown that in both cases when $\mathscr{A}$ follows from a rule of deduction, $\mathscr{A}$ is logically valid, as desired. □

Corollary 4.6. *K* is consistent (for no *wf* $\mathscr{A}$ are both $\mathscr{A}$ and $(\sim \mathscr{A})$) both theorems of *K*).

Proof. For a contradiction, suppose that both $\mathscr{A}$ and $(\sim \mathscr{A})$ are both theorems of *K* for some *wf* $\mathscr{A}$ of *K*. Then $\mathscr{A}$ and $(\sim \mathscr{A})$ are both logically valid, by the above proposition. Hence, in any interpretation, both $\mathscr{A}$ and $(\sim \mathscr{A})$ are true, which contradictions Remark 3.25(c). □

In *L*, we saw that if we could prove $\mathscr{A} \vdash_L \mathscr{B}$, then $\vdash_L (\mathscr{A} \to \mathscr{B})$. This is almost true in $\mathscr{L}$ in the sense that we must restrict the relationship between $\mathscr{A}$ and $\mathscr{B}$ to apply a similar theorem for *K*. In particular, in the deduction of $\mathscr{B}$ from $\mathscr{A}$ must not involve the deduction rule of Generalization. The reason for this is best seen with an example.

Consider $x = 0$ in the integers. It is neither true nor false, since its truth value is dependent on what a valuation assigns to x. Now consider $(\forall x)x = 0$. It is certainly false, since any valuation that does not assign x to 0 will not satisfy $x = 0$. So the implication $x = 0 \to (\forall x)x = 0$ must be false in the interpretation.

Now, notice that $x = 0$ is an interpretation of $A_1^1(x)$, where x is just any variable of some appropriate first order language, and likewise $(\forall x)x = 0$ is an interpretation of $(\forall x)A_1^1(x)$. We know that by Generalization, $A_1^1(x) \vdash_{K_{\mathscr{L}}} (\forall x)A_1^1(x)$, but we have just seen an interpretation where $A_1^1(x) \to (\forall x)A_1^1(x)$ is false, and hence the *wf* is not logically valid, and so it cannot be a theorem of *K*, by Proposition 4.5.

This example shows the issue that can arise when generalizing a statement that is neither true nor false in an interpretation[1]. However, with careful restriction on the *wf*s, we may still use the Deduction Theorem of *L* in an analogous way in *K*.

Proposition 4.8 (The Deduction Theorem for *K*)**.** Let $\mathscr{A}$ and $\mathscr{B}$ be *wf*s of *K* and let Γ be a set of *wf*s of $\mathscr{L}$. If $\Gamma \cup \{\mathscr{A}\} \vdash_K \mathscr{B}$, and this deduction contains no application of Generalization involving a variable free in $\mathscr{A}$, then $\Gamma \vdash_K (\mathscr{A} \to \mathscr{B})$.

Proof. The proof is by induction on the number of *wf*s, n, in the deduction of $\mathscr{B}$. Let $\mathscr{A}'$ and $\mathscr{B}'$ be *wf*s and let Γ' be a set of *wf*s. Suppose, as an induction hypothesis, that whenever $\Gamma' \cup \{\mathscr{A}'\} \vdash_K \mathscr{B}'$, and this deduction has fewer than n *wf*s and has no occurrence of Generalization involving a variables free in $\mathscr{A}'$, it follows that $\Gamma' \vdash_K (\mathscr{A}' \to \mathscr{B}')$.

[1]If the statement is not indeterminate in this sense, then generalization is fine (see the additional exercises section in the appendix of the manual)

(base case) The verification of the base case proceeds in an identical manner as that of the proof of the Deduction Theorem for L. It may be that $n = 1$, in which $\mathscr{B}$ is either an axiom of K, a member of Γ, or $\mathscr{A}$ itself. If $\mathscr{B}$ is an axiom of K, then:

1	$\mathscr{B}$	axiom of K
2	$(\mathscr{B} \to (\mathscr{A} \to \mathscr{B}))$	(K1)
3	$(\mathscr{A} \to \mathscr{B})$	1, 2, MP

If $\mathscr{B}$ is a member of Γ:

1	$\mathscr{B}$	member of Γ
2	$(\mathscr{B} \to (\mathscr{A} \to \mathscr{B}))$	(K1)
3	$(\mathscr{A} \to \mathscr{B})$	1, 2, MP

If $\mathscr{B}$ is $\mathscr{A}$, then $(\mathscr{A} \to \mathscr{B})$ is $(\mathscr{A} \to \mathscr{A})$.

1	$((\mathscr{A} \to ((\mathscr{A} \to \mathscr{A}) \to \mathscr{A})) \to ((\mathscr{A} \to (\mathscr{A} \to \mathscr{A})) \to (\mathscr{A} \to \mathscr{A})))$	(L2)
2	$(\mathscr{A} \to ((\mathscr{A} \to \mathscr{A}) \to \mathscr{A}))$	(L1)
3	$((\mathscr{A} \to (\mathscr{A} \to \mathscr{A})) \to (\mathscr{A} \to \mathscr{A}))$	1, 2, MP
4	$(\mathscr{A} \to (\mathscr{A} \to \mathscr{A}))$	(L1)
5	$(\mathscr{A} \to \mathscr{A})$	3, 4, MP

The above is a deduction of $(\mathscr{A} \to \mathscr{B})$ (which is $(\mathscr{A} \to \mathscr{A})$) from Γ. Note that it is also a general theorem of K.

And so in all three cases, we have formed a deduction of $(\mathscr{A} \to \mathscr{B})$ from Γ, as desired.

(inductive step) Now it may be that $n > 1$. There are a number of cases to verify.

1. It may be that $\mathscr{B}$ is an axiom of K or a member of $\Gamma \cup \{\mathscr{A}\}$, in which case the deductions in the base case serve as the desired deductions.

2. It may be that $\mathscr{B}$ proceeds from MP and two prior *wf*s in the deduction. The two *wf*s must necessarily be of the form $\mathscr{C}$ and $(\mathscr{C} \to \mathscr{B})$, and the subsequences of the deduction of $\mathscr{B}$ that are deductions of $\mathscr{C}$ and $(\mathscr{C} \to \mathscr{B})$ must necessarily have fewer than n *wf*s, in which case, by the induction hypothesis, there exist deductions from Γ of $(\mathscr{A} \to \mathscr{C})$ and $(\mathscr{A} \to (\mathscr{C} \to \mathscr{B}))$.

1	$(\mathscr{A} \to \mathscr{C})$	Induction hypothesis
2	$(\mathscr{A} \to (\mathscr{C} \to \mathscr{B}))$	Induction hypothesis
3	$((\mathscr{A} \to (\mathscr{C} \to \mathscr{B})) \to ((\mathscr{A} \to \mathscr{C}) \to (\mathscr{A} \to \mathscr{B})))$	(K2)
4	$((\mathscr{A} \to \mathscr{C}) \to (\mathscr{A} \to \mathscr{B}))$	2, 3, MP
5	$(\mathscr{A} \to \mathscr{B})$	1, 4, MP

The above is deduction of $(\mathscr{A} \to \mathscr{B})$ from Γ, as desired. The first two lines were shortened ways of expressing that deductions from Γ of $(\mathscr{A} \to \mathscr{C})$ and $(\mathscr{A} \to (\mathscr{C} \to \mathscr{B}))$ exist.

3. The only possible remaining is that $\mathscr{B}$ follows from generalization from some *wf*, $\mathscr{C}$, and so $\mathscr{B}$ is $(\forall x_i)\mathscr{C}$, where x_i is a variable that must necessarily not be free in $\mathscr{A}$. The induction hypothesis may be applied to the deduction of $\mathscr{C}$, so there exists a deduction from Γ of $(\mathscr{A} \to \mathscr{C})$.

1	$(\mathscr{A} \to \mathscr{C})$	Induction hypothesis
2	$(\forall x_i)(\mathscr{A} \to \mathscr{C})$	1, Generalization
3	$((\forall x_i)(\mathscr{A} \to \mathscr{C}) \to (\mathscr{A} \to (\forall x_i)\mathscr{C}))$	(K6)
4	$(\mathscr{A} \to (\forall x_i)\mathscr{C})$	1, 3, MP

Just as in the previous case, the first line is an abbreviation of the deduction of $(\mathscr{A} \to \mathscr{C})$ from Gamma. We have constructed a deduction of $\mathscr{A} \to \mathscr{B}$ from Γ, since $(\mathscr{A} \to (\forall x_i)\mathscr{C})$ is $(\mathscr{A} \to \mathscr{B})$.

In all possible cases, we have constructed a deduction of $(\mathscr{A} \to \mathscr{B})$ from Γ, as desired. □

Corollary 4.9. If $\Gamma \cup \{\mathscr{A}\} \vdash_K \mathscr{B}$ and $\mathscr{A}$ is a closed *wf*, then $\Gamma \vdash_K (\mathscr{A} \to \mathscr{B})$.

Proof. Since $\mathscr{A}$ is closed, it contains no free variables, so by the previous proposition, $\Gamma \vdash_K (\mathscr{A} \to \mathscr{B})$. □

Corollary 4.10. For any *wf*s $\mathscr{A}, \mathscr{B}, \mathscr{C}$ of K,

$$\{(\mathscr{A} \to \mathscr{B}), (\mathscr{B} \to \mathscr{C})\} \vdash_K (\mathscr{A} \to \mathscr{C})$$

Proof. The proof relies only on the Deduction Theorem above and is identical to that of Corollary 2.10. □

Just as in L, the corollary of the Deduction Theorem holds in K.

Proposition 4.11. Let $\mathscr{A}$ and $\mathscr{B}$ are *wf*s of K, and let Γ be a set of *wf*s of K. Then if $\Gamma \vdash_K (\mathscr{A} \to \mathscr{B})$, then $\Gamma \cup \{\mathscr{A}\} \vdash_K \mathscr{B}$.

Proof. The proof is identical to the proof of Proposition 2.9. □

It will often be the case that we would like to apply the deduction theorem to a deduction obtained from the Deduction Theorem. The following corollary will be useful.

Corollary. Let $\mathscr{A}$ and $\mathscr{B}$ be *wf*s of K and let Γ be a set of *wf*s of $\mathscr{L}$. Suppose that $\Gamma \vdash_K (\mathscr{A} \to \mathscr{B})$ is obtained from the fact that $\Gamma \cup \{\mathscr{A}\} \vdash_K \mathscr{B}$ and the Deduction Theorem. The deduction of $\mathscr{A} \to \mathscr{B}$ contains no application of Generalization involving a variable free in $\mathscr{A}$.

Proof. Since the Deduction Theorem was applied to $\Gamma \cup \{\mathscr{A}\}$, we must assume that the deduction obtained contains no instances of Generalization involving a variable free in $\mathscr{A}$. Now consider the deduction $\Gamma \vdash_K \mathscr{A}$. The proof of the Deduction Theorem contains a construction of it. All lines in all deductions do not invoke Generalization except for in Case 3 of the proof in the inductive step or possibly lines obtained from the induction hypothesis. If the line was obtained by the induction hypothesis, we may use similarly use induction to demonstrate that those lines only involved instances of Generalization occurring free in $\mathscr{A}$, although we will not write this out fully. Now it might be the case that a line of the deduction was obtained by Generalization. In particular, line 2 of case 3 of the inductive step was justified by Generalization involving a variable not assumed to be free in $\mathscr{A}$.

Therefore, the deduction of $\Gamma \vdash_K (\mathscr{A} \to \mathscr{B})$ obtained from $\Gamma \cup \{\mathscr{A}\} \vdash_K \mathscr{B}$ contains no instances of Generalization involving a variable free in $\mathscr{A}$. □

The next corollary is used implicitly in the textbook. We will state it clearly here.

Corollary. Let $\mathscr{A}, \mathscr{B}, \mathscr{C}$ be *wf*s of K and let Γ be a set of *wf*s of $\mathscr{L}$. Suppose that $\Gamma \cup \{\mathscr{A}\} \vdash_K (\mathscr{B} \to \mathscr{C})$ is obtained from the fact $\Gamma \cup \{\mathscr{A}, \mathscr{B}\} \vdash_K \mathscr{C}$ using the Deduction Theorem. If $\mathscr{B}$ contains no variables occurring free in $\mathscr{A}$, then $\Gamma \vdash_K \mathscr{A} \to (\mathscr{B} \to \mathscr{C})$.

Proof. The deduction of $\mathscr{B} \to \mathscr{C}$ obtained from the Deduction Theorem contains no applications of Generalization involving a variable occurring free in $\mathscr{B}$, by the above lemma. Therefore, if $\mathscr{B}$ contains no variables occurring free in $\mathscr{A}$, then the deduction of $\mathscr{B} \to \mathscr{C}$ contains no applications of Generalization involving a variable occurring free in $\mathscr{A}$. By the Deduction Theorem, we may conclude that $\Gamma \vdash_K \mathscr{A} \to (\mathscr{B} \to \mathscr{C})$. □

Just as in the textbook, we will not explicitly reference these corollaries when they are used.

Solutions to exercises

1. The following is a proof of $(\forall x_1)(A_1^1(x_1) \to A_1^1(x_1))$.

1	$(A_1^1(x_1) \to A_1^1(x_1))$	tautology
2	$(\forall x_i)(A_1^1(x_1) \to A_1^1(x_1))$	Generalization

2. In (a) of the exercise, x_i must not occur free in $\mathscr{B}$. This is ambiguous in the presentation of the exercise, since the condition is only stated in (b) and the assumption is that the *wf* $\mathscr{B}$ is the same one in $\mathscr{A}$.

   (a) We will first prove a simple lemma.

   Lemma. Let $\mathscr{A}, \mathscr{B}, \mathscr{C}$ be *wf*s of some first order language $\mathscr{L}$. If $\mathscr{A} \vdash_{K_\mathscr{L}} ((\sim \mathscr{C}) \to (\sim \mathscr{B}))$, then $\mathscr{A} \vdash_{K_\mathscr{L}} (\mathscr{B} \to \mathscr{C})$.

   Proof. Suppose that $\mathscr{A} \vdash_{K_\mathscr{L}} ((\sim \mathscr{C}) \to (\sim \mathscr{B}))$. The deduction can be extended in the following way.

	$\vdots$	
k	$((\sim \mathscr{C}) \to (\sim \mathscr{B}))$	deduction from $\mathscr{A}$
k+1	$(((\sim \mathscr{C}) \to (\sim \mathscr{B})) \to (\mathscr{B} \to \mathscr{C}))$	(K3)
k+2	$(\mathscr{B} \to \mathscr{C})$	k, k+1, MP

   The above is a deduction of $(\mathscr{B} \to \mathscr{C})$ from $\mathscr{A}$. □

Now we begin the proof. First we show that $\{(\sim \mathscr{B}), (\forall x_i)\mathscr{A}\} \vdash_{K_{\mathscr{L}}} (\forall x_i)(\sim (\mathscr{A} \to \mathscr{B}))$.

1	$(\sim \mathscr{B})$	assumption
2	$(\forall x_i)\mathscr{A}$	assumption
3	$\mathscr{A}$	Remark 4.1(b)
4	$((\sim \mathscr{B}) \to (\mathscr{A} \to (\sim (\mathscr{A} \to \mathscr{B}))))$	tautology
5	$(\mathscr{A} \to (\sim (\mathscr{A} \to \mathscr{B})))$	1, 4, MP
6	$(\sim (\mathscr{A} \to \mathscr{B}))$	2, 5, MP
7	$(\forall x_i)(\sim (\mathscr{A} \to \mathscr{B}))$	Generalization

By the deduction theorem and the fact that the only instance of generalization in the above deduction involved x_i, a variable not free in $(\forall x_i)\mathscr{A}$, we have

$$(\sim \mathscr{B}) \vdash_{K_{\mathscr{L}}} ((\forall x_i)\mathscr{A} \to (\forall x_i)(\sim (\mathscr{A} \to \mathscr{B}))),$$

and by the lemma,

$$(\sim \mathscr{B}) \vdash_{K_{\mathscr{L}}} ((\sim (\forall x_i)(\sim (\mathscr{A} \to \mathscr{B}))) \to (\sim (\forall x_i)\mathscr{A})),$$

which is, by the definition of the $\exists$ quantifier,

$$(\sim \mathscr{B}) \vdash_{K_{\mathscr{L}}} ((\exists x_i)(\mathscr{A} \to \mathscr{B}) \to (\sim (\forall x_i)\mathscr{A})),$$

and by the converse of the Deduction Theorem, Proposition 4.11,

$$\{(\exists x_i)(\mathscr{A} \to \mathscr{B}), (\sim \mathscr{B})\} \vdash_{K_{\mathscr{L}}} (\sim (\forall x_i)\mathscr{A}),$$

and by the Deduction theorem once again and the fact that x_i does not occur free in $\mathscr{B}$,

$$\{(\exists x_i)(\mathscr{A} \to \mathscr{B})\} \vdash_{K_{\mathscr{L}}} ((\sim \mathscr{B}) \to (\sim (\forall x_i)\mathscr{A})),$$

By the lemma,

$$\{(\exists x_i)(\mathscr{A} \to \mathscr{B})\} \vdash_{K_{\mathscr{L}}} ((\forall x_i)\mathscr{A} \to \mathscr{B}),$$

Finally, by the deduction theorem once again,

$$\vdash_{K_{\mathscr{L}}} ((\exists x_i)(\mathscr{A} \to \mathscr{B}) \to ((\forall x_i)\mathscr{A} \to \mathscr{B})).$$

(b) Observe the following deduction.

1	$(\sim (\forall x_i) \sim \mathscr{A} \to \mathscr{B})$	assumption
2	$\sim \mathscr{B}$	assumption
3	$(\sim (\forall x_i) \sim \mathscr{A} \to \mathscr{B}) \to (\sim \mathscr{B} \to \sim\sim (\forall x_i) \sim \mathscr{A})$	tautology
4	$(\sim \mathscr{B} \to \sim\sim (\forall x_i) \sim \mathscr{A})$	1, 2, MP
5	$\sim\sim (\forall x_i) \sim \mathscr{A}$	2, 4, MP
6	$\sim\sim (\forall x_i) \sim \mathscr{A} \to (\forall x_i) \sim \mathscr{A}$	tautology
7	$(\forall x_i) \sim \mathscr{A}$	5, 6, MP
8	$\sim \mathscr{A}$	Remark 4.1(b)

The above deduction did not invoke Generalization. Therefore, by the Deduction Theorem,

$$((\exists x_i)\mathscr{A} \rightarrow \mathscr{B}) \vdash_{K_{\mathscr{L}}} (\sim \mathscr{B} \rightarrow \sim \mathscr{A}).$$

Note that we used the existential quantifier abbreviation above. Therefore, there exists a deduction from $((\exists x_i)\mathscr{A} \rightarrow \mathscr{B})$ of $(\sim \mathscr{B} \rightarrow \sim \mathscr{A})$ that may be extended in the following way.

	$\vdots$	
k	$(\sim \mathscr{B} \rightarrow \sim \mathscr{A})$	deduction from $((\exists x_i)\mathscr{A} \rightarrow \mathscr{B})$
k+1	$(\sim \mathscr{B} \rightarrow \sim \mathscr{A}) \rightarrow (\mathscr{A} \rightarrow \mathscr{B})$	(K3)
k+2	$(\mathscr{A} \rightarrow \mathscr{B})$	k, k+1, MP
k+3	$(\forall x_i)(\mathscr{A} \rightarrow \mathscr{B})$	Generalization

The above deduction does not involve Generalization involving a variable occurring free in $((\exists x_i)\mathscr{A} \rightarrow \mathscr{B})$, since x_i does not occur free in $\mathscr{B}$. Therefore, by the Deduction Theorem,

$$((\exists x_i)\mathscr{A} \rightarrow \mathscr{B}) \rightarrow (\forall x_i)(\mathscr{A} \rightarrow \mathscr{B})$$

is a theorem of $K_{\mathscr{L}}$.

(c) Observe the following deduction.

1	$(\forall x_i) \sim\sim \mathscr{A}$	assumption
2	$\sim\sim \mathscr{A}$	Remark 4.1(b)
3	$(\sim\sim \mathscr{A} \rightarrow \mathscr{A})$	tautology
4	$\mathscr{A}$	2, 3, MP
5	$(\forall x_i)\mathscr{A}$	Generalization

The only instance of Generalization in the above deduction involves x_i, which is free in $(\forall x_i) \sim\sim \mathscr{A}$. Therefore, by the Deduction Theorem,

$$((\forall x_i) \sim\sim \mathscr{A} \rightarrow (\forall x_i)\mathscr{A})$$

is a theorem of $K_{\mathscr{L}}$, so the proof of the above can be extended in the following way.

	$\vdots$	
k	$((\forall x_i) \sim\sim \mathscr{A} \rightarrow (\forall x_i)\mathscr{A})$	theorem of $K_{\mathscr{L}}$
k+1	$(((\forall x_i) \sim\sim \mathscr{A} \rightarrow (\forall x_i)\mathscr{A}) \rightarrow$ $(\sim (\forall x_i)\mathscr{A} \rightarrow \sim (\forall x_i) \sim\sim \mathscr{A}))$	tautology
k+2	$(\sim (\forall x_i)\mathscr{A} \rightarrow \sim (\forall x_i) \sim\sim \mathscr{A})$	k, k+1, MP

and therefore, the last line is a theorem of $K_{\mathscr{L}}$, and it is, by definition of $\exists$,

$$(\sim (\forall x_i)\mathscr{A} \rightarrow (\exists x_i) \sim \mathscr{A}),$$

as desired.

3. (a) In line 2, Generalization involving x_1 appears, but the variable x_1 occurs free in $(\exists x_2)A_1^2(x_1, x_2)$, so the application of the Deduction Theorem later is invalid. Additionally, in line 3, x_2 is not free for x_1 in $(\exists x_2)A_1^2(x_1, x_2)$, so the instance of axiom scheme (K5) is invalid.

   (b) Consider an interpretation with the domain being the integers and $A_1^2(x_i, x_j)$ indicating that $x_i \neq x_j$. Then the interpretation of the formula given in the exercise is $((\exists x_2)x_1 \neq x_2 \to (\exists x_2)x_2 \neq x_2)$. Let v be any valuation such that $v(x_1) \neq v(x_2)$. This valuation will not satisfy the *wf*, and hence the given formula is not logically valid.

4.2 Equivalence, substitution

Let $\mathscr{A}, \mathscr{B}$ be *wf*s of $\mathscr{L}$. The connective is defined such that $(\mathscr{A} \leftrightarrow \mathscr{B})$ is to stand for

$$\sim ((\mathscr{A} \to \mathscr{B}) \to\sim (\mathscr{B} \to \mathscr{A})).$$

Proposition 4.15. For any *wf*s $\mathscr{A}, \mathscr{B}$ of $\mathscr{L}$, $\vdash_K (\mathscr{A} \leftrightarrow \mathscr{B})$ if and only if $\vdash_K (\mathscr{A} \to \mathscr{B})$ and $\vdash_K (\mathscr{B} \to \mathscr{A})$.

Proof. $\Rightarrow$ Suppose that $\vdash_K (\mathscr{A} \leftrightarrow \mathscr{B})$, i.e. $\vdash_K \star$., where $\star$ is

$$\sim ((\mathscr{A} \to \mathscr{B}) \to\sim (\mathscr{B} \to \mathscr{A})).$$

Then $\star \to (\mathscr{A} \to \mathscr{B})$ and $\star \to (\mathscr{B} \to \mathscr{A})$ are both tautologies (their truth tables will verify this), and so, by MP, both $\vdash_K (\mathscr{A} \to \mathscr{B})$ and $\vdash_K (\mathscr{B} \to \mathscr{A})$.

$\Leftarrow$ Suppose that $\vdash_K (\mathscr{A} \to \mathscr{B})$ and $\vdash_K (\mathscr{B} \to \mathscr{A})$. The *wf*

$$(\mathscr{A} \to \mathscr{B}) \to ((\mathscr{B} \to \mathscr{A}) \to\sim ((\mathscr{A} \to \mathscr{B}) \to\sim (\mathscr{B} \to \mathscr{A})))$$

is a tautology (by its truth table), and by MP, $\vdash_K\sim ((\mathscr{A} \to \mathscr{B}) \to\sim (\mathscr{B} \to \mathscr{A}))$. □

Definition 4.16. If $(\mathscr{A} \leftrightarrow \mathscr{B})$ is a theorem of K, then we say that the *wf*s $\mathscr{A}$ and $\mathscr{B}$ are *provably equivalent*.

Corollary 4.17. Let $\mathscr{A}, \mathscr{B}, \mathscr{C}$ be *wf*s of $\mathscr{L}$. If $\vdash_K (\mathscr{A} \leftrightarrow \mathscr{B})$ and $\vdash_K (\mathscr{B} \leftrightarrow \mathscr{C})$, then $\vdash_K (\mathscr{A} \leftrightarrow \mathscr{C})$.

Proof. By Proposition 4.15, $\vdash_K (\mathscr{A} \leftrightarrow \mathscr{B})$ if and only if $\vdash_K (\mathscr{A} \to \mathscr{B})$ and $\vdash_K (\mathscr{B} \to \mathscr{A})$. Similarly, $\vdash_K (\mathscr{B} \leftrightarrow \mathscr{C})$ if and only if $\vdash_K (\mathscr{B} \to \mathscr{C})$ and $\vdash_K (\mathscr{C} \to \mathscr{B})$. Since both $\vdash_K (\mathscr{A} \to \mathscr{B})$ and $\vdash_K (\mathscr{B} \to \mathscr{C})$, by HP, $\vdash_K (\mathscr{A} \to \mathscr{C})$. Since both $\vdash_K (\mathscr{C} \to \mathscr{B})$ and $\vdash_K (\mathscr{B} \to \mathscr{A})$, by HP, $\vdash_K (\mathscr{C} \to \mathscr{A})$. By Proposition 4.15, $\vdash_K (\mathscr{A} \leftrightarrow \mathscr{C})$. □

Recall that $\mathscr{A}(x_i)$ denotes a *wf* in which x_i occurs free, and $\mathscr{A}(x_j)$ denotes $\mathscr{A}(x_i)$ with every *free* occurrence of x_i substituted with x_j.

Proposition 4.18. If x_i occurs *only free and never bound*[2] in $\mathscr{A}(x_i)$ and x_j is a variable which does not occur, free or bound, in $\mathscr{A}(x_i)$, then

$$\vdash_K ((\forall x_i)\mathscr{A}(x_i) \leftrightarrow (\forall x_j)\mathscr{A}(x_j)).$$

[2]We add this additional restriction to handle the "edge case" in which x_i occurs redundantly bound within $\mathscr{A}(x_i)$.

Proof. First, x_j is free for x_i in $\mathscr{A}(x_i)$, therefore line 2 in the following deduction is valid.

1	$(\forall x_i)\mathscr{A}(x_i)$	assumption
2	$((\forall x_i)\mathscr{A}(x_i) \to \mathscr{A}(x_j))$	(K5)
3	$\mathscr{A}(x_j)$	1, 2, MP
4	$(\forall x_j)\mathscr{A}(x_j)$	Generalization

Hence, since the instance of Generalization in line 4 involved x_j, a variable not free in $(\forall x_i)\mathscr{A}(x_i)$, we may use the Deduction Theorem to obtain

$$\vdash_K ((\forall x_i)\mathscr{A}(x_i) \to (\forall x_j)\mathscr{A}(x_j)).$$

Now, since x_i is free for x_j in $\mathscr{A}(x_j)$, we may use an identical deduction as the one above with x_j and x_i switched.

1	$(\forall x_j)\mathscr{A}(x_j)$	assumption
2	$((\forall x_j)\mathscr{A}(x_j) \to \mathscr{A}(x_i))$	(K5)
3	$\mathscr{A}(x_i)$	1, 2, MP
4	$(\forall x_i)\mathscr{A}(x_i)$	Generalization

By the Deduction Theorem, we obtain the converse of the implication above,

$$\vdash_K ((\forall x_j)\mathscr{A}(x_j) \to (\forall x_i)\mathscr{A}(x_i)),$$

so by Proposition 4.15,

$$\vdash_K ((\forall x_j)\mathscr{A}(x_j) \leftrightarrow (\forall x_i)\mathscr{A}(x_i)),$$

as desired. □

The above proposition makes clear that the name of a bound variable in a *wf* is of no importance to the meaning of the *wf*. The meaning of the *wf* is dependent on its free variables.

Proposition 4.19. Let $\mathscr{A}$ be a *wf* of $\mathscr{L}$ whose n free variables are $x_1, \ldots, x_n$. The *wf* $\mathscr{A}$ is a theorem of K if and only if $(\forall x_1) \ldots (\forall x_n)\mathscr{A}$ is a theorem of K.

Proof. $\Rightarrow$ Suppose that $\vdash_K \mathscr{A}$. We proceed by induction on n. As a hypothesis of induction, suppose that if $\mathscr{B}$ is a *wf* of $\mathscr{L}$ with fewer than n free variables, then if $\mathscr{B}$ is a theorem of K, then $(\forall y_1) \ldots (\forall y_k)\mathscr{B}$ is a theorem of K, where $y_1, \ldots, y_k$ are the free variables of $\mathscr{B}$.

(base case) It may be that $n = 0$, which is to say that $\mathscr{A}$ has no free variables. In this case, $\mathscr{A}$ itself has all of its free variables vacuously quantified.

Alternatively, it may be that $n = 1$, in which case since $\mathscr{A}$ is a theorem of K, by Generalization, $(\forall y_1)\mathscr{A}$ must be a theorem of K as well, where y_1 is the only free variable occurring in $\mathscr{A}$.

(inductive step) It may be that $n > 1$. Since $\mathscr{A}$ is a theorem of K, by Generalization, $(\forall y_n)\mathscr{A}$ is a theorem of K. Notice this *wf* has $y_1, \ldots, y_{n-1}$ as its free variables, so by the induction hypothesis

$$(\forall y_1) \ldots (\forall y_{n-1})(\forall y_n)\mathscr{A}$$

must be a theorem of K, as desired.

$\Leftarrow$ By Remark 4.1(b) or repeated applications of (K5), if $(\forall y_1) \ldots (\forall y_1)\mathscr{A}$ is a theorem of K, then $\mathscr{A}$ must be a theorem of K[3] □

[3] A more complete proof would involve induction in the proof of the other direction of the equivalence.

Definition 4.20. Let $\mathscr{A}$ be a *wf* of $\mathscr{L}$ with $y_1, \ldots, y_n$ as the only variables occurring free in $\mathscr{A}$. The *wf* $(\forall y_1) \ldots (\forall y_n)\mathscr{A}$ is the *universal closure* of $\mathscr{A}$ and is denoted by $\mathscr{A}'$.

It is true that $\vdash_K \mathscr{A}' \to \mathscr{A}$, but $\mathscr{A}$ and $\mathscr{A}'$ are in general not provably equivalent. A counterexample can be found in the example in this manual used to motivate the Deduction Theorem.

Proposition 4.22. Let $\mathscr{A}$ and $\mathscr{B}$ be *wf*s of $\mathscr{L}$, and let $\mathscr{A}_0$ be a *wf* of $\mathscr{L}$ with occurrences of $\mathscr{A}$, and let $\mathscr{B}_0$ be the *wf* $\mathscr{A}_0$ in which all occurrences of $\mathscr{A}$ are replaced with $\mathscr{B}$.

If $\vdash_K (\mathscr{A} \to \mathscr{B})'$, then $\vdash_K (\mathscr{A}_0 \leftrightarrow \mathscr{B}_0)$.

Proof. Let n denote the number of connectives and quantifiers in $\mathscr{A}_0$. We proceed by induction on n.

(hypothesis) Suppose that for any *wf* containing instances of $\mathscr{A}$ and having fewer n connectives and quantifiers, the property above holds for it.

(base case) It may be that $n = 0$, i.e., $\mathscr{A}_0$ has no connectives or quantifiers. Then $\mathscr{A}_0$ is just $\mathscr{A}$, and $\mathscr{B}_0$ is just $\mathscr{B}$. Therefore, $\vdash_K (\mathscr{A} \leftrightarrow \mathscr{B})' \to (\mathscr{A} \leftrightarrow \mathscr{B})$, by repeated applications of Remark 4.1(b), i.e. $\vdash_K (\mathscr{A} \leftrightarrow \mathscr{B})' \to (\mathscr{A}_0 \leftrightarrow \mathscr{B}_0)$, as desired.

(induction step) It may be that $n > 1$, which is to say that more than one connective or quantifier occurs in $\mathscr{A}_0$. There are three cases to consider, each one corresponding to one of the three possible forms that $\mathscr{A}_0$ can take.

1. The *wf* $\mathscr{A}_0$ is $(\sim \mathscr{C}_0)$ and $\mathscr{B}_0$ is $(\sim \mathscr{D}_0)$, where $\mathscr{D}_0$ is the *wf* in which instances of $\mathscr{B}$ in $\mathscr{C}_0$ are substituted for $\mathscr{A}$. The induction hypothesis may be applied to $\mathscr{C}_0$, so

   $$\vdash_K ((\mathscr{A} \leftrightarrow \mathscr{B})' \to (\mathscr{C}_0 \leftrightarrow \mathscr{D}_0)).$$

   Since $(\mathscr{C}_0 \leftrightarrow \mathscr{D}_0) \to (\sim \mathscr{C}_0 \leftrightarrow \sim \mathscr{D}_0)$ is a tautology, it is a theorem of K. By HS,

   $$\vdash_K ((\mathscr{A} \leftrightarrow \mathscr{B})' \to (\sim \mathscr{C}_0 \leftrightarrow \sim \mathscr{D}_0)), \text{ i.e., } \vdash_K ((\mathscr{A} \leftrightarrow \mathscr{B})' \to (\mathscr{A}_0 \leftrightarrow \mathscr{B}_0)),$$

   as desired.

2. The *wf* $\mathscr{A}_0$ is $(\sim \mathscr{C}_0 \to \sim \mathscr{D}_0)$ and $\mathscr{B}_0$ is $(\sim \mathscr{E}_0 \to \sim \mathscr{F}_0)$, where $\mathscr{E}_0$ and $\mathscr{F}_0$ are the *wf*s in which instances of $\mathscr{B}$ are substituted for $\mathscr{A}$ in $\mathscr{C}_0$ and $\mathscr{D}_0$, respectively. The induction hypothesis may be applied to both $\mathscr{C}_0$ and $\mathscr{D}_0$, so

   $$\vdash_K ((\mathscr{A} \leftrightarrow \mathscr{B})' \to (\mathscr{C}_0 \leftrightarrow \mathscr{E}_0)) \text{ and } \vdash_K ((\mathscr{A} \leftrightarrow \mathscr{B})' \to (\mathscr{D}_0 \leftrightarrow \mathscr{F}_0)).$$

   The statement form

   $$(a \to (c \leftrightarrow e)) \to ((a \to (d \leftrightarrow f)) \to (a \to ((c \to d) \leftrightarrow (e \to f)))),$$

   is a tautology. Therefore, (treat a as $(\mathscr{A} \leftrightarrow \mathscr{B})'$) by two applications of MP,

   $$\vdash_K ((\mathscr{A} \leftrightarrow \mathscr{B})' \to ((\mathscr{C}_0 \to \mathscr{D}_0) \leftrightarrow (\mathscr{E}_0 \to \mathscr{F}_0))),$$

   which is to say that

   $$\vdash_K ((\mathscr{A} \leftrightarrow \mathscr{B})' \to (\mathscr{A}_0 \leftrightarrow \mathscr{B}_0)),$$

   as desired.

3. The *wf* $\mathscr{A}_0$ is $(\forall x_i)\mathscr{C}_0$, and $\mathscr{B}_0$ is $(\forall x_i)\mathscr{D}_0$, where $\mathscr{D}_0$ is the *wf* obtained by replacing all instances of $\mathscr{A}$ in $\mathscr{C}_0$ with $\mathscr{B}$. The induction hypothesis may be applied to $\mathscr{C}_0$ to obtain $\vdash_K ((\mathscr{A} \leftrightarrow \mathscr{B})' \to (\mathscr{C}_0 \leftrightarrow \mathscr{D}_0))$. We may continue this deduction in the following way.

$$
\begin{array}{lrr}
 & \vdots & \\
\text{k} & ((\mathscr{A} \leftrightarrow \mathscr{B})' \to (\mathscr{C}_0 \leftrightarrow \mathscr{D}_0)) & \text{Induction hypothesis} \\
\text{k+1} & (\forall x_i)((\mathscr{A} \leftrightarrow \mathscr{B})' \to (\mathscr{C}_0 \leftrightarrow \mathscr{D}_0)) & \text{Generalization} \\
\text{k+2} & (\forall x_i)((\mathscr{A} \leftrightarrow \mathscr{B})' \to (\mathscr{C}_0 \leftrightarrow \mathscr{D}_0)) & \\
 & \to ((\mathscr{A} \leftrightarrow \mathscr{B})' \to (\forall x_i)(\mathscr{C}_0 \leftrightarrow \mathscr{D}_0)) & \text{(K6)} \\
\text{k+3} & ((\mathscr{A} \leftrightarrow \mathscr{B})' \to (\forall x_i)(\mathscr{C}_0 \leftrightarrow \mathscr{D}_0)) & \text{k+1, k+2, MP} \\
\text{k+4} & ((\forall x_i)(\mathscr{C}_0 \leftrightarrow \mathscr{D}_0) \to ((\forall x_i)\mathscr{C}_0 \leftrightarrow (\forall x_i)\mathscr{D}_0)) & \text{Lemma} \\
\text{k+5} & ((\mathscr{A} \leftrightarrow \mathscr{B})' \to ((\forall x_i)\mathscr{C}_0 \leftrightarrow (\forall x_i)\mathscr{D}_0)) & \text{k+3, k+4, HS}
\end{array}
$$

Note that line k+2 is possible by since x_i does not occur free in $(\mathscr{A} \leftrightarrow \mathscr{B})'$, since it is a universal closure, and this is also the reason that proving $\mathscr{A}$ to be provably equivalent to $\mathscr{B}$ is not enough for the proposition. Line k+1 is justified by the following lemma.

Lemma. Let $\mathscr{A}$ and $\mathscr{B}$ be *wf*s of $\mathscr{L}$. Then

$$(\forall x_i)(\mathscr{A} \leftrightarrow \mathscr{B}) \to ((\forall x_i)\mathscr{A} \leftrightarrow (\forall x_i)\mathscr{B})$$

is a theorem of K.

Proof. We claim that

$$\vdash_K (\forall x_i)(\mathscr{A} \to \mathscr{B}) \to ((\forall x_i)\mathscr{A} \to (\forall x_i)\mathscr{B}),$$

and we will prove this in Exercise 4. Additionally, the deduction above contains no instances of generalization involving a variable other than x_i.

$$
\begin{array}{lrr}
1 & (\forall x_i)(\mathscr{A} \leftrightarrow \mathscr{B}) & \text{assumption} \\
2 & (\forall x_i)(\mathscr{A} \to \mathscr{B}) & \text{1, Proposition 4.15} \\
3 & (\forall x_i)(\mathscr{B} \to \mathscr{A}) & \text{1, Proposition 4.15} \\
4 & (\forall x_i)(\mathscr{A} \to \mathscr{B}) \to ((\forall x_i)\mathscr{A} \to (\forall x_i)\mathscr{B}) & \text{above theorem} \\
5 & (\forall x_i)(\mathscr{B} \to \mathscr{A}) \to ((\forall x_i)\mathscr{B} \to (\forall x_i)\mathscr{A}) & \text{above theorem} \\
6 & ((\forall x_i)\mathscr{A} \to (\forall x_i)\mathscr{B}) & \text{2, 4, MP} \\
7 & ((\forall x_i)\mathscr{B} \to (\forall x_i)\mathscr{A}) & \text{3, 5, MP} \\
8 & ((\forall x_i)\mathscr{A} \to (\forall x_i)\mathscr{B}) \to & \\
 & ((\forall x_i)\mathscr{B} \to (\forall x_i)\mathscr{A}) \to ((\forall x_i)\mathscr{A} \leftrightarrow (\forall x_i)\mathscr{B}) & \text{tautology} \\
9 & ((\forall x_i)\mathscr{B} \to (\forall x_i)\mathscr{A}) \to ((\forall x_i)\mathscr{A} \leftrightarrow (\forall x_i)\mathscr{B}) & \text{6, 8, MP} \\
10 & ((\forall x_i)\mathscr{A} \leftrightarrow (\forall x_i)\mathscr{B}) & \text{7, 9, MP}
\end{array}
$$

By the Deduction Theorem,

$$(\forall x_i)(\mathscr{A} \leftrightarrow \mathscr{B}) \leftrightarrow ((\forall x_i)\mathscr{A} \leftrightarrow (\forall x_i)\mathscr{B}),$$

as desired. ◻

To conclude the induction and the proof, we have shown that for any value of n, $\vdash_K (\mathscr{A} \leftrightarrow \mathscr{B})' \rightarrow (\mathscr{A}_0 \leftrightarrow \mathscr{B}_0)$, as desired. □

Now, for the *wf*s $\mathscr{A}, \mathscr{B}$ described above, if $(\mathscr{A} \leftrightarrow \mathscr{B})$ is logically valid, i.e., it is a theorem of K, then its universal closure is also a theorem, so we may freely use the above Proposition. We will refer to this property in the below corollary.

Corollary 4.23. Let $\mathscr{A}, \mathscr{B}, \mathscr{A}_0, \mathscr{B}_0$ be as in Proposition 4.22 above. If $\vdash_K (\mathscr{A} \leftrightarrow \mathscr{B})$, then $\vdash_K (\mathscr{A}_0 \leftrightarrow \mathscr{B}_0)$.

Proof. Suppose that $\vdash_K (\mathscr{A} \leftrightarrow \mathscr{B})$. Then, by Proposition 4.19, $\vdash_K (\mathscr{A} \leftrightarrow \mathscr{B})'$. By Proposition 4.22, $\vdash_K ((\mathscr{A} \leftrightarrow \mathscr{B})' \rightarrow (\mathscr{A}_0 \leftrightarrow \mathscr{B}_0))$. By MP, $\vdash_K (\mathscr{A}_0 \leftrightarrow \mathscr{B}_0)$. □

Corollary 4.24. Let x_i occur free in the *wf* $\mathscr{A}(x_i)$. Let $\mathscr{A}_0$ be a *wf* containing instances of $(\forall x_i)\mathscr{A}(x_i)$ as a subformula. Let $\mathscr{B}_0$ be the *wf* obtained by replacing in $\mathscr{A}_0$ one or more instances of $(\forall x_i)\mathscr{A}(x_i)$ with $(\forall x_j)\mathscr{A}(x_j)$.

If x_j does not occur, free or bound, in $\mathscr{A}(x_i)$, then $\vdash_K (\mathscr{A}_0 \leftrightarrow \mathscr{B}_0)$.

Proof. Since x_j does not occur, free or bound, in $\mathscr{A}_(x_i)$, by Proposition 4.18,

$$\vdash_K ((\forall x_i)\mathscr{A}(x_i) \leftrightarrow (\forall x_i)\mathscr{B}(x_i))$$

Therefore, by Corollary 4.23, $\vdash_K (\mathscr{A}_0 \leftrightarrow \mathscr{B}_0)$. □

Solutions to exercises

4. Observe the following deduction.

1	$(\forall x_i)(\mathscr{A} \rightarrow \mathscr{B})$	assumption
2	$(\forall x_i)\mathscr{A}$	assumption
3	$\mathscr{A} \rightarrow \mathscr{B}$	1, Remark 4.1(b)
4	$\mathscr{A}$	2, Remark 4.1(b)
5	$\mathscr{B}$	3, 4, MP
6	$(\forall x_i)\mathscr{B}$	5, Generalization

Notice that the only instance of Generalization involves x_i, which does not occur free in $(\forall x_i)(\mathscr{A} \rightarrow \mathscr{B})$ and $(\forall x_i)\mathscr{A}$. By applying the Deduction Theorem twice, we conclude that

$$\vdash_K (\forall x_i)(\mathscr{A} \rightarrow \mathscr{B}) \rightarrow ((\forall x_i)\mathscr{A} \rightarrow (\forall x_i)\mathscr{B}),$$

as desired.

5. The *wf* $(\sim\sim (\forall x_i) \sim \mathscr{A}) \leftrightarrow (\forall x_i)(\sim \mathscr{A})$ is a tautology, hence it is a theorem of K. Notice that by the definition of $\exists$, the left-hand side of the $\leftrightarrow$ is $\sim (\exists x_i)\mathscr{A}$, so

$$\vdash_K (\sim (\exists x_i)\mathscr{A}) \leftrightarrow (\forall x_i)(\sim \mathscr{A}),$$

i.e., $(\sim (\exists x_i)\mathscr{A})$ and $(\forall x_i)(\sim \mathscr{A})$ are provably equivalent.

6. (a) Observe the following deduction.

1	$(\forall x_1)(\forall x_2)A_1^2(x_1, x_2)$	assumption
2	$((\forall x_1)(\forall x_2)A_1^2(x_1, x_2) \leftrightarrow (\forall x_1)(\forall x_3)A_1^2(x_1, x_3))$	Proposition 4.18
3	$((\forall x_1)(\forall x_2)A_1^2(x_1, x_2) \leftrightarrow (\forall x_1)(\forall x_3)A_1^2(x_1, x_3)) \rightarrow$ $((\forall x_1)(\forall x_2)A_1^2(x_1, x_2) \rightarrow (\forall x_1)(\forall x_3)A_1^2(x_1, x_3))$	tautology
4	$((\forall x_1)(\forall x_2)A_1^2(x_1, x_2) \rightarrow (\forall x_1)(\forall x_3)A_1^2(x_1, x_3))$	2, 3, MP
5	$(\forall x_1)(\forall x_3)A_1^2(x_1, x_3)$	1, 4, MP

We could continue this deduction in the same way to deduce

$$(\forall x_2)(\forall x_3)A_1^2(x_2, x_3),$$

as desired.

(b) The following is a satisfactory deduction.

1	$(\forall x_1)(\forall x_2)A_1^2(x_1, x_2)$	assumption
2	$((\forall x_1)(\forall x_2)A_1^2(x_1, x_2) \rightarrow (\forall x_2)A_1^2(x_1, x_2))$	Remark 4.1(b)
3	$((\forall x_2)A_1^2(x_1, x_2) \rightarrow A_1^2(x_1, x_1))$	(K5)
4	$((\forall x_1)(\forall x_2)A_1^2(x_1, x_2) \rightarrow A_1^2(x_1, x_1))$	2, 3, HS
5	$A_1^2(x_1, x_1)$	1, 4, MP
6	$(\forall x_1)A_1^2(x_1, x_1)$	5, Generalization

Note that in line 3, we used the fact that x_1 is free for x_2 in $A_1^2(x_1, x_2)$.

7. Since x_j does not occur, free or bound, in $\sim \mathscr{A}(x_i)$, by Proposition 4.18,

$$\vdash_K (\forall x_i)(\sim \mathscr{A}(x_i)) \leftrightarrow (\forall x_j)(\sim \mathscr{A}(x_j)),$$

and since $(\mathscr{C} \leftrightarrow \mathscr{D}) \rightarrow ((\sim \mathscr{D}) \leftrightarrow (\sim \mathscr{C}))$ is a tautology, then by MP and the previously obtained theorem,

$$\vdash_K (\sim (\forall x_i)(\sim \mathscr{A}(x_i))) \leftrightarrow (\sim (\forall x_j)(\sim \mathscr{A}(x_j))), \text{ i.e., } \vdash_K (\exists x_i)\mathscr{A}(x_i) \leftrightarrow (\exists x_j)\mathscr{A}(x_j),$$

as desired.

4.3 Prenex Form

Proposition 4.25. Let $\mathscr{A}$ and $\mathscr{B}$ be *wf*s of $\mathscr{L}$.

1. If x_i does not occur free in $\mathscr{A}$, then

   (a) $\vdash_K ((\forall x_i)(\mathscr{A} \rightarrow \mathscr{B}) \leftrightarrow (\mathscr{A} \rightarrow (\forall x_i)\mathscr{B}))$.

   (b) $\vdash_K ((\exists x_i)(\mathscr{A} \rightarrow \mathscr{B}) \leftrightarrow (\mathscr{A} \rightarrow (\exists x_i)\mathscr{B}))$.

2. If x_i does not occur free in $\mathscr{B}$, then

(a) $\vdash_K ((\forall x_i)(\mathscr{A} \to \mathscr{B}) \leftrightarrow ((\exists x_i)\mathscr{A} \to \mathscr{B}))$.

(b) $\vdash_K ((\exists x_i)(\mathscr{A} \to \mathscr{B}) \leftrightarrow ((\forall x_i)\mathscr{A} \to \mathscr{B}))$.

Proof. A total of eight implications must be proved to be theorems of K.

1. (a) If x_i does not occur free in $\mathscr{A}$, then immediately by (K6) we get

$$\vdash_K ((\forall x_i)(\mathscr{A} \to \mathscr{B}) \to (\mathscr{A} \to (\forall x_i)\mathscr{B})).$$

For the other direction, observe the following deduction.

1	$(\mathscr{A} \to (\forall x_i)\mathscr{B})$	assumption
2	$((\forall x_i)\mathscr{B} \to \mathscr{B})$	Remark 4.1(b)
3	$(\mathscr{A} \to \mathscr{B})$	(1), (2), HS
4	$(\forall x_i)(\mathscr{A} \to \mathscr{B})$	3, Generalization

By the deduction theorem, we obtain

$$\vdash_K ((\mathscr{A} \to (\forall x_i)\mathscr{B}) \to (\forall x_i)(\mathscr{A} \to \mathscr{B})).$$

(b) Observe the following deduction.

1	$(\forall x_i) \sim \mathscr{B}$	assumption
2	$\mathscr{A}$	assumption
3	$\sim \mathscr{B}$	Remark 4.1(b)
4	$\mathscr{A} \to ((\sim \mathscr{B}) \to (\sim (\mathscr{A} \to \mathscr{B})))$	tautology
5	$(\sim \mathscr{B}) \to (\sim (\mathscr{A} \to \mathscr{B}))$	2, 4, MP
6	$\sim (\mathscr{A} \to \mathscr{B})$	3, 5, MP
7	$(\forall x_i) \sim (\mathscr{A} \to \mathscr{B})$	6, Generalization

Since the only usage of Generalization involved x_i, which does not occur free in $\mathscr{A}$, by the Deduction Theorem,

$$(\forall x_i) \sim \mathscr{B} \vdash_K \mathscr{A} \to (\forall x_i) \sim (\mathscr{A} \to \mathscr{B}).$$

Now by using a lemma similar to the one found in exercise 2(a),

$$(\forall x_i) \sim \mathscr{B} \vdash_K (\sim (\forall x_i) \sim (\mathscr{A} \to \mathscr{B})) \to (\sim \mathscr{A}).$$

By the definition of $\exists$,

$$(\forall x_i) \sim \mathscr{B} \vdash_K (\exists x_i)(\mathscr{A} \to \mathscr{B}) \to (\sim \mathscr{A}).$$

By the converse of the Deduction Theorem, Proposition 4.11,

$$\{(\exists x_i)(\mathscr{A} \to \mathscr{B}), (\forall x_i) \sim \mathscr{B}\} \vdash_K (\sim \mathscr{A}).$$

By the Deduction Theorem,

$$(\exists x_i)(\mathscr{A} \to \mathscr{B}) \vdash_K (\forall x_i) \sim \mathscr{B} \to (\sim \mathscr{A}).$$

By using the same lemma,

$$(\exists x_i)(\mathscr{A} \to \mathscr{B}) \vdash_K \sim\sim \mathscr{A} \to (\sim (\forall x_i) \sim \mathscr{B}).$$

By the definition of $\exists$,

$$(\exists x_i)(\mathscr{A} \to \mathscr{B}) \vdash_K \sim\sim \mathscr{A} \to (\exists x_i)\mathscr{B}.$$

Since $\mathscr{A} \to \sim\sim \mathscr{A}$ is a tautology, we may extend by the above deduction using HS to obtain

$$(\exists x_i)(\mathscr{A} \to \mathscr{B}) \vdash_K \mathscr{A} \to (\exists x_i)\mathscr{B}.$$

Finally, by the Deduction Theorem once more,

$$\vdash_K (\exists x_i)(\mathscr{A} \to \mathscr{B}) \to (\mathscr{A} \to (\exists x_i)\mathscr{B}).$$

For the other direction, observe the following deduction.

1	$\sim\sim (\forall x_i) \sim (\mathscr{A} \to \mathscr{B})$	assumption
2	$(\sim\sim (\forall x_i) \sim (\mathscr{A} \to \mathscr{B}) \to (\forall x_i) \sim (\mathscr{A} \to \mathscr{B}))$	tautology
3	$(\forall x_i) \sim (\mathscr{A} \to \mathscr{B})$	1, 2, MP
4	$\sim (\mathscr{A} \to \mathscr{B})$	Remark 4.1(b)
5	$(\sim (\mathscr{A} \to \mathscr{B}) \to \mathscr{A})$	tautology
6	$(\sim (\mathscr{A} \to \mathscr{B}) \to (\sim \mathscr{B}))$	tautology
7	$\mathscr{A}$	4, 5, MP
8	$\sim \mathscr{B}$	4, 6, MP
9	$(\forall x_i)(\sim \mathscr{B})$	8, Generalization
10	$\mathscr{A} \to ((\forall x_i)(\sim \mathscr{B}) \to (\sim (\mathscr{A} \to (\sim (\forall x_i)(\sim \mathscr{B})))))$	tautology
11	$(\forall x_i)(\sim \mathscr{B}) \to (\sim (\mathscr{A} \to (\sim (\forall x_i)(\sim \mathscr{B}))))$	7, 10, MP
12	$(\sim (\mathscr{A} \to (\sim (\forall x_i)(\sim \mathscr{B}))))$	9, 11, MP

Hence, we have shown that,

$$\sim\sim (\forall x_i) \sim (\mathscr{A} \to \mathscr{B}) \vdash_K (\sim (\mathscr{A} \to (\sim (\forall x_i)(\sim \mathscr{B})))),$$

so by the Deduction Theorem,

$$\vdash_K \sim\sim (\forall x_i) \sim (\mathscr{A} \to \mathscr{B}) \to (\sim (\mathscr{A} \to (\sim (\forall x_i)(\sim \mathscr{B})))),$$

and this deduction can be extended by (K3) and MP. Therefore,

$$\vdash_K (\mathscr{A} \to (\sim (\forall x_i) \sim \mathscr{B})) \to (\sim (\forall x_i) \sim (\mathscr{A} \to \mathscr{B})),$$

which, by the definition of $\exists$, is

$$\vdash_K (\mathscr{A} \to (\exists x_i)\mathscr{B}) \to (\exists x_i)(\mathscr{A} \to \mathscr{B}).$$

Note that since we did not use the fact that x_i does not occur free in $\mathscr{A}$, this direction is a general theorem of K.

2. (a) Observe the following deduction.

1	$(\forall x_i)(\mathscr{A} \to \mathscr{B})$	assumption
2	$\sim \mathscr{B}$	assumption
3	$(\mathscr{A} \to \mathscr{B})$	1, Remark 4.1(b)
4	$(\sim \mathscr{B}) \to ((\mathscr{A} \to \mathscr{B}) \to (\sim \mathscr{A}))$	tautology
5	$((\mathscr{A} \to \mathscr{B}) \to (\sim \mathscr{A}))$	2, 4, MP
6	$\sim \mathscr{A}$	3, 5, MP
7	$(\forall x_i) \sim \mathscr{A}$	6, Generalization
8	$((\forall x_i) \sim \mathscr{A}) \to (\sim\sim (\forall x_i) \sim \mathscr{A})$	tautology
9	$(\sim\sim (\forall x_i) \sim \mathscr{A})$	7, 8 MP

And thus, by the definition of $\exists$ and by applying the Deduction Theorem (x_i does not occur free in $(\sim \mathscr{B})$),

$$(\forall x_i)(\mathscr{A} \to \mathscr{B}) \vdash_K (\sim \mathscr{B}) \to\sim (\exists x_i)\mathscr{A},$$

and we can easily extend this deduction using the fact that (K3) to obtain

$$(\forall x_i)(\mathscr{A} \to \mathscr{B}) \vdash_K ((\exists x_i)\mathscr{A} \to \mathscr{B}),$$

and finally by applying the deduction theorem again,

$$\vdash_K (\forall x_i)(\mathscr{A} \to \mathscr{B}) \to ((\exists x_i)\mathscr{A} \to \mathscr{B}).$$

The other direction is

$$\vdash_K ((\exists x_i)\mathscr{A} \to \mathscr{B}) \to (\forall x_i)(\mathscr{A} \to \mathscr{B}),$$

and this was proved in Exercise 2(b).

(b) The proof of

$$\vdash_K (\exists x_i)(\mathscr{A} \to \mathscr{B}) \to ((\forall x_i)\mathscr{A} \to \mathscr{B}),$$

was done in Exercise 2(a). For the other direction, observe the following deduction.

1	$\sim\sim (\forall x_i) \sim (\mathscr{A} \to \mathscr{B})$	assumption
2	$(\sim\sim (\forall x_i) \sim (\mathscr{A} \to \mathscr{B}) \to (\forall x_i) \sim (\mathscr{A} \to \mathscr{B}))$	tautology
3	$(\forall x_i) \sim (\mathscr{A} \to \mathscr{B})$	1, 2, MP
4	$\sim (\mathscr{A} \to \mathscr{B})$	Remark 4.1(b)
5	$(\sim (\mathscr{A} \to \mathscr{B}) \to \mathscr{A})$	tautology
6	$(\sim (\mathscr{A} \to \mathscr{B}) \to (\sim \mathscr{B}))$	tautology
7	$\mathscr{A}$	4, 5, MP
8	$\sim \mathscr{B}$	4, 6, MP
9	$(\forall x_i)\mathscr{A}$	7, Generalization
10	$(\forall x_i)\mathscr{A} \to ((\sim \mathscr{B}) \to (\sim ((\forall x_i)\mathscr{A} \to \mathscr{B})))$	tautology
11	$((\sim \mathscr{B}) \to (\sim ((\forall x_i)\mathscr{A} \to \mathscr{B})))$	9, 10, MP
12	$(\sim ((\forall x_i)\mathscr{A} \to \mathscr{B}))$	8, 11, MP

Hence, we have shown that,

$$\sim\sim (\forall x_i) \sim (\mathscr{A} \to \mathscr{B}) \vdash_K (\sim ((\forall x_i)\mathscr{A} \to \mathscr{B})),$$

so by the Deduction Theorem,

$$\vdash_K \sim\sim (\forall x_i) \sim (\mathscr{A} \to \mathscr{B}) \to (\sim ((\forall x_i)\mathscr{A} \to \mathscr{B})),$$

and this deduction can be extended by (K3) and MP. Therefore,

$$\vdash_K ((\forall x_i)\mathscr{A} \to \mathscr{B}) \to\sim (\forall x_i) \sim (\mathscr{A} \to \mathscr{B}),$$

which, by the definition of $\exists$, is

$$\vdash_K ((\forall x_i)\mathscr{A} \to \mathscr{B}) \to (\exists x_i)(\mathscr{A} \to \mathscr{B}).$$

Note that proof of this direction never used the fact that x_i does not occur free in $\mathscr{B}$, so the *wf* is a general theorem of K.

In all cases, we may apply Proposition 4.15 to show that the *wf*s are provably equivalent. □

Definition 4.27. A *wf* of $\mathscr{L}$ is said to be in *prenex form* if all of its quantifiers appears at the beginning. In other words, it is of the form

$$(Q_1 x_{i_1})(Q_1 x_{i_1}) \ldots (Q_n x_{i_n})\mathscr{B},$$

where each Q_i is a quantifier, and $\mathscr{B}$ is a *wf* with no quantifiers.

The following proposition is not difficult, but requires writing many tedious *wf*s in proper forms so that previous propositions may be applied. It is easier to understand after a few examples of transforming *wf*s to prenex form have been done, and some examples are given in the solutions to the exercises below.

Proposition 4.28. For any *wf* of $\mathscr{L}$, there is a provably equivalent *wf* in prenex form.

Proof. Let $\mathscr{A}$ be a *wf* of $\mathscr{L}$. It must be of the form

$$\mathscr{A}_1 \to \mathscr{A}_2 \to \ldots \to \mathscr{A}_n$$

parenthesized in some way. Suppose that a variable occurs bound in some $\mathscr{A}_i$ while occurring free or bound in some $\mathscr{A}_j$. By Proposition 4.18 and Proposition 4.22, we may obtain a provably equivalent *wf* such that this condition does not occur. By repeated applications of the above to all bound variables satisfying the same condition, we may obtain a *wf* $\mathscr{A}^*$ in which all bound variables are unique to the $\mathscr{A}_i$ in which they occur[4].

Now we prove the proposition by induction on n, the numbers of connectives or quantifiers in $\mathscr{A}^*$ (or $\mathscr{A}$).

(hypothesis) Suppose that for any *wf* which fewer than n connectives or quantifiers, there is a *wf* in prenex form which is provably equivalent.

(base case) It may be that $n = 0$, i.e., $\mathscr{A}$ is an atomic formula. Then it is provably equivalent to itself, a *wf* which is vacuously in prenex form.

(inductive step) It may be that $n > 1$, in which $\mathscr{A}^*$ must take one of the following forms.

[4]This part of the proof is a bit informal, and a more rigorous proof would be done by constructing an algorithm and demonstrating its correctness. Regardless an example of this process will be shown in the solutions to the exercises.

1. The *wf* $\mathscr{A}^*$ is of the form $\sim \mathscr{B}$. In this case, $\mathscr{B}$ contains fewer than n quantifiers and connectives, so $\mathscr{B}$ must be equivalent to $\mathscr{B}^{\text{pre}}$, a *wf* in prenex form. We may write $\mathscr{B}^{\text{pre}}$ as
$$(Q_1 x_{i_1}) \dots (Q_n x_{i_n})\mathscr{C}$$
where $\mathscr{D}$ contains no quantifiers and each Q is a quantifier. By applying the definition of $\exists$ the tautology $\sim\sim \mathscr{A} \leftrightarrow \mathscr{A}$ for any *wf* $\mathscr{A}$ and Proposition 4.22, $\sim \mathscr{B}^{\text{pre}}$ can be seen to be
$$(Q_1^* x_{i_1}) \dots (Q_n^* x_{i_n}) \sim \mathscr{C}$$
where each Q_k^* is the quantifier that Q_k was not. Therefore, $\sim \mathscr{B}^{\text{pre}}$ is also in prenex form. Since $\mathscr{A}$ is provably equivalent to $\mathscr{A}^*$, and $\mathscr{A}^*$ is provably equivalent to $\sim \mathscr{B}^{\text{pre}}$, by Corollary 4.17, we may conclude that $\mathscr{A}$ is provably equivalent to $\sim \mathscr{B}^{\text{pre}}$, a *wf* in prenex form.

2. The *wf* $\mathscr{A}^*$ is of the form $\mathscr{B} \to \mathscr{C}$. Since $\mathscr{B}$ and $\mathscr{C}$ both contain fewer than n connectives and quantifiers, there exists *wf*s $\mathscr{B}^{\text{pre}}$ and $\mathscr{C}^{\text{pre}}$ such that
$$\vdash_K \mathscr{B} \leftrightarrow \mathscr{B}^{\text{pre}} \text{ and } \vdash_K \mathscr{C} \leftrightarrow \mathscr{C}^{\text{pre}}.$$
By Corollary 4.23,
$$\vdash_K (\mathscr{B} \to \mathscr{C}) \leftrightarrow (\mathscr{B}^{\text{pre}} \to \mathscr{C}) \text{ and } \vdash_K (\mathscr{B}^{\text{pre}} \to \mathscr{C}) \leftrightarrow (\mathscr{B}^{\text{pre}} \to \mathscr{C}^{\text{pre}}).$$
By Corollary 4.17,
$$\vdash_K (\mathscr{B} \to \mathscr{C}) \leftrightarrow (\mathscr{B}^{\text{pre}} \to \mathscr{C}^{\text{pre}}) \text{ i.e., } \mathscr{A}^* \leftrightarrow (\mathscr{B}^{\text{pre}} \to \mathscr{C}^{\text{pre}}).$$
By Definition 4.27, $\mathscr{B}_{\text{pre}} \to \mathscr{C}_{\text{pre}}$ is of the form,
$$(Q_1^* x_{i_1}) \dots (Q_n^* x_{i_n})\mathscr{D} \to (R_1^* x_{j_1}) \dots (R_m^* x_{j_m})\mathscr{E},$$
where the symbols are to be interpreted in accordance with Definition 4.27. We may use Proposition 4.25 repeatedly to move all the quantifiers to the beginning, changed if necessary, since the variables occurring in the quantifiers are all different and different from any of the free variables occurring in $\mathscr{D}$ and $\mathscr{E}$. The resulting *wf* is of the form
$$(Q_1^* x_{i_1}) \dots (Q_n^* x_{i_n})(R_1^* x_{j_1}) \dots (R_m^* x_{j_m})(\mathscr{D} \to \mathscr{E}),$$
is in prenex form, and is provably equivalent to $\mathscr{A}$ by repeated applications of Corollary 4.17.

3. The *wf* $\mathscr{A}^*$ is of the form $(\forall x_i)\mathscr{B}$. Since $\mathscr{B}$ has fewer connectives and quantifiers, it is provably equivalent to a *wf* in prenex form, i.e.,
$$\vdash_K (\mathscr{B} \leftrightarrow (Q_1 x_{i_1}) \dots (Q_n x_{i_n})\mathscr{C}),$$
where the symbols are above are defined according to Definition 4.27. By Generalization,
$$\vdash_K (\forall x_i)(\mathscr{B} \leftrightarrow (Q_1 x_{i_1}) \dots (Q_n x_{i_n})\mathscr{C}),$$
and by the lemma which appears in Proposition 4.22,
$$\vdash_K ((\forall x_i)\mathscr{B} \leftrightarrow (\forall x_i)(Q_1 x_{i_1}) \dots (Q_n x_{i_n})\mathscr{C}),$$
and since the left-hand side is $\mathscr{A}$ and the right-hand side is a *wf* in prenex form, we have shown that $\mathscr{A}$ is equivalent to a *wf* in prenex form.

Therefore, for any n, $\mathscr{A}$ is equivalent to a *wf* in prenex form. □

Definition 4.30. Let n be a nonnegative integer.

(i) A *wf* in prenex form is a Π_n*-form* if it starts with a universal quantifier and has $n-1$ alternations of quantifiers.

(ii) A *wf* in prenex form is a Σ_n*-form* if it starts with an existential quantifier and has $n-1$ alternations of quantifiers.

In general, quantifiers are not commutative in the sense that their order of appearance is of no matter to the meaning of a *wf*, although quantifiers of the same type are commutative (see Appendix A).

Using Proposition 4.25, we see that we may pull out quantifiers according to the equivalences of Proposition 4.25, but this does not mean that the quantifiers at the beginning of the prenex form can appear in any order. As an example of this, see the additional exercises in Appendix B.

Solutions to exercises

8. (a) The original *wf* is

$$(\forall x_1)A_1^1(x_1) \rightarrow (\forall x_2)A_1^2(x_1, x_2).$$

First, we change the bound variables so that they do not occur bound in one subformula and free or bound in another. By Proposition 4.22 and 4.18, We obtain the provably equivalent *wf*

$$(\forall x_3)A_1^1(x_3) \rightarrow (\forall x_2)A_1^2(x_1, x_2).$$

We apply Proposition 4.25 1(a) to get the provably equivalent *wf*

$$(\forall x_2)((\forall x_3)A_1^1(x_3) \rightarrow A_1^2(x_1, x_2)).$$

We apply Proposition 4.25 2(b) to get the provably equivalent *wf*

$$(\forall x_2)(\exists x_3)(A_1^1(x_3) \rightarrow A_1^2(x_1, x_2)),$$

which is prenex form.

(b) The original *wf* is

$$(\forall x_1)(A_1^2(x_1, x_2) \rightarrow (\forall x_2)A_1^2(x_1, x_2)).$$

First, we change the bound variables so that they do not occur bound in one subformula and free or bound in another. By Proposition 4.22 and 4.18, We obtain the provably equivalent *wf*

$$(\forall x_1)(A_1^2(x_1, x_2) \rightarrow (\forall x_3)A_1^2(x_1, x_3)).$$

We apply Proposition 4.25 1(a) to get the provably equivalent *wf*

$$(\forall x_1)(\forall x_3)(A_1^2(x_1, x_2) \rightarrow A_1^2(x_1, x_3)),$$

which is in prenex form.

(c) The original *wf* is

$$(\forall x_1)(A_1^1(x_1) \rightarrow A_1^2(x_1, x_2)) \rightarrow ((\exists x_2)A_1^1(x_2) \rightarrow (\exists x_3)A_1^2(x_2, x_3)).$$

First, we change the bound variables so that they do not occur bound in one subformula and free or bound in another. By Proposition 4.22 and 4.18, We obtain the provably equivalent *wf*

$$(\forall x_1)(A_1^1(x_1) \rightarrow A_1^2(x_1, x_2)) \rightarrow ((\exists x_3)A_1^1(x_3) \rightarrow (\exists x_4)A_1^2(x_2, x_4)).$$

We apply Proposition 4.25 1(b) to get the provably equivalent *wf*

$$(\forall x_1)(A_1^1(x_1) \rightarrow A_1^2(x_1, x_2)) \rightarrow (\exists x_4)((\exists x_3)A_1^1(x_3) \rightarrow A_1^2(x_2, x_4)).$$

We apply Proposition 4.25 2(a) to get the provably equivalent *wf*

$$(\forall x_1)(A_1^1(x_1) \rightarrow A_1^2(x_1, x_2)) \rightarrow (\exists x_4)(\forall x_3)(A_1^1(x_3) \rightarrow A_1^2(x_2, x_4)).$$

We apply Proposition 4.25 1(b) to get the provably equivalent *wf*

$$(\exists x_4)((\forall x_1)(A_1^1(x_1) \rightarrow A_1^2(x_1, x_2)) \rightarrow (\forall x_3)(A_1^1(x_3) \rightarrow A_1^2(x_2, x_4))).$$

We apply Proposition 4.25 1(a) to get the provably equivalent *wf*

$$(\exists x_4)(\forall x_3)((\forall x_1)(A_1^1(x_1) \rightarrow A_1^2(x_1, x_2)) \rightarrow (A_1^1(x_3) \rightarrow A_1^2(x_2, x_4))).$$

We apply Proposition 4.25 2(b) to get the provably equivalent *wf*

$$(\exists x_4)(\forall x_3)(\exists x_1)((A_1^1(x_1) \rightarrow A_1^2(x_1, x_2)) \rightarrow (A_1^1(x_3) \rightarrow A_1^2(x_2, x_4))),$$

which is prenex form.

(d) The original *wf* is

$$(\exists x_1)A_1^2(x_1, x_2) \rightarrow (A_1^1(x_1) \rightarrow \sim (\exists x_3)A_1^2(x_1, x_3))$$

First, we change the bound variables so that they do not occur bound in one subformula and free or bound in another. By Proposition 4.22 and 4.18, We obtain the provably equivalent *wf*

$$(\exists x_4)A_1^2(x_4, x_2) \rightarrow (A_1^1(x_1) \rightarrow \sim (\exists x_3)A_1^2(x_1, x_3)).$$

By the definition of $\exists$, Proposition 4.22, and the tautology $\mathscr{A} \leftrightarrow \sim\sim \mathscr{A}$, we obtain the provably equivalent *wf*

$$(\exists x_4)A_1^2(x_4, x_2) \rightarrow (A_1^1(x_1) \rightarrow (\forall x_3) \sim A_1^2(x_1, x_3)).$$

We apply Proposition 4.25 1(a) to get the provably equivalent *wf*

$$(\exists x_4)A_1^2(x_4, x_2) \rightarrow (\forall x_3)(A_1^1(x_1) \rightarrow \sim A_1^2(x_1, x_3)).$$

We apply Proposition 4.25 1(a) to get the provably equivalent *wf*

$$(\forall x_3)((\exists x_4)A_1^2(x_4, x_2) \rightarrow (A_1^1(x_1) \rightarrow \sim A_1^2(x_1, x_3))).$$

We apply Proposition 4.25 2(a) to get the provably equivalent *wf*

$$(\forall x_3)(\forall x_4)(A_1^2(x_4, x_2) \rightarrow (A_1^1(x_1) \rightarrow \sim A_1^2(x_1, x_3))),$$

which is in prenex form.

9. The original *wf* is
$$((\exists x_1)\mathscr{A}(x_1) \to (\exists x_2)\mathscr{B}(x_2)).$$
By applying Proposition 1(b) before applying Proposition 2(a), we obtain the provably equivalent *wf*
$$(\exists x_2)(\forall x_1)(\mathscr{A}(x_1) \to \mathscr{B}(x_2)),$$
which is in Σ_2 form. By applying Proposition 2(a) before applying Proposition 1(b), we obtain the provably equivalent *wf*
$$(\forall x_1)(\exists x_2)(\mathscr{A}(x_1) \to \mathscr{B}(x_2)),$$
which is in Π_2 form.

10. One solution can be obtained by finding a logically valid formula in Σ_2 form such that applying Generalization to it will lead to a provably equivalent formula which is in Π_3 form. So
$$(\exists x_2)(\forall x_1)(A_1^1(x_1, x_2) \to A_1^1(x_1, x_2)) \text{ and } (\forall x_3)(\exists x_2)(\forall x_1)(A_1^1(x_1, x_2) \to A_1^1(x_1, x_2))$$
are formulas in the desired forms which are provably equivalent.

4.4 The Adequacy Theorem for K

As a reminder, the main goal of this chapter is to prove that K is adequate in the sense that any logically valid *wf* of $\mathscr{L}$ is a theorem of K.

Definition 4.32. An *extension of K* is a formal system obtained by altering or enlargin the set of axioms so that all theorems of K remain theorems.

Additionally, given two extensions of K, if one has more theorems than the other, that extension is considered to be larger. The book does not explicate whether K is an extension of K or not, although it seems to imply that K is an extension of K. In this manual, K will be an extension of K.

Definition 4.33. Let $\mathscr{L}$ be a first order language. A *first order system* is an extension of $K_{\mathscr{L}}$.

In other words, a first order system is another way of saying an extension of K.

Definition 4.34. A first order system S is *consistent* if for no *wf* are both $\mathscr{A}$ and $\sim \mathscr{A}$ both theorems of S.

Proposition 4.35. Let S be a consistent first order system. If $\mathscr{A}$ is a closed *wf* which is not a theorem of S, then the extension of S obtained by adding $\sim \mathscr{A}$ as an additional axiom is consistent.

Proof. Let S^* refer to the extension of S described above. Suppose, for a contradiction, that it is not consistent. That is, there exists *wf* $\mathscr{B}$ and $\sim \mathscr{B}$ that are both theorems of S^*. Hence, $(\sim \mathscr{B} \to (\mathscr{B} \to \mathscr{A}))$ is a tautology, so it is a theorem of K, and therefore, it is a theorem of S^*. By two applications of MP, $\mathscr{A}$ must be a theorem of S^*.

There is therefore a proof of $\mathscr{A}$ in S^*. By definition, since S^* is an extension of S with only $\sim \mathscr{A}$ as additional axiom, any proof in S^* is a deduction from $\sim \mathscr{A}$ in S. Hence, $(\sim \mathscr{A}) \vdash_S \mathscr{A}$, and since $\mathscr{A}$ is closed, no application of Generalization in the proof can involve a variable free in $\mathscr{A}$. Therefore, $\vdash_S (\sim \mathscr{A} \rightarrow \mathscr{A})$, by the Deduction Theorem. Using the fact that $(\sim \mathscr{A} \rightarrow \mathscr{A}) \rightarrow \mathscr{A}$ is a tautology and MP, $\mathscr{A}$ must be a theorem of S. But this contradicts the consistency of S.

We may conclude that S^* is consistent. □

Definition 4.36. A first order system S is *complete* if for each *closed wf* $\mathscr{A}$, either $\mathscr{A}$ or $\sim \mathscr{A}$ is a theorem of S.

Note that K is not complete, since any atomic formula with additional quantifiers applied so that it is a closed formula is not a theorem of K.

Proposition 4.37. For any consistent first order system, there exists a complete, consistent extension.

Proof. Let $\mathscr{A}_0, \mathscr{A}_1, \ldots, \ldots$ be an enumeration of the *closed wf*s of $\mathscr{L}$. Define a sequence of extensions of K first by $S_0 = S$. If $n > 0$, then there are two cases:

1. If S_{n-1} contains $\mathscr{A}_n$ as a theorem, then $S_n = S_{n-1}$.
2. If S_{n-1} does not contain $\mathscr{A}_n$ as a theorem, then S_n is S_{n-1} with $\sim \mathscr{A}_n$ as an additional axiom.

By Proposition 4.35 and the fact that S is consistent, S_n for any n is a consistent extension. Now let S_∞ be the extension whose axioms are the *wf*s which are in at least one of the members of the sequence constructed earlier. The extension may be proved to be consistent in the same way that S^* was seen to be consistent in the proof of Proposition 4.35. □

If anything is unclear about the above proof, see Proposition 2.21.

This next theorem is the longest in the book. The reward for completing this proposition will be a short proof of the Adequacy Theorem. The theorem, along with its converse, is also important in its own right, as it reveals many things about first order systems.

Proposition 4.38. Let S be a first order system, i.e., a consistent extension of $K_{\mathscr{L}}$. If S is consistent, then there exists an interpretation in which every theorem of S is true.

Proof. Considering the significant length of this proof, we will split it into sections.

1. Let S^+ be the system S obtained by changing the first order language to $\mathscr{L}^+$, which is identical to $\mathscr{L}$ except with the addition of the infinite sequence of constants $a_0^+, a_1^+, a_2^+, \ldots$[5]. The system S^+ is consistent.

   Suppose for a contradiction that S^+ is not consistent. Then there exists proofs of some *wf*s $\mathscr{A}$ and $\sim \mathscr{A}$. These proofs involve a finite number of the constants $a_0^+, a_1^+, a_2^+, \ldots$. By replacing these constants each with a respective but arbitrary variable which does not appear in the proof, we obtain proofs of $\mathscr{A}$ and $\sim \mathscr{A}$ in S, which contradicts the consistency of S. Hence, S^+ must be consistent.

[5]Note that S^+ is not an extension of S as it was obtained not by extending the axioms of S, but by extending the language of S. It is tempting but invalid to apply previous results in this chapter.

2. In this step, we will construct a sequence of first order systems so that we may produce a consistent and complete system from it. First consider the following *wf* in any first order language with a constant c and a *wf* $\mathscr{A}$ with one free variable.

$$\mathscr{A}(c) \rightarrow (\forall x_i)\mathscr{A}(x_i)$$

   The meaning of this *wf* is that $\mathscr{A}$ is true for the constant c only when $\mathscr{A}$ is true for any variable. We shall construct the sequence of first order systems in such a way that every member of the sequence (except for the first one) has a corresponding axiom with the same meaning.

   We begin by enumerating, in the extended first order language described above, the *wf*s which contain one free variable[6]:

$$\mathscr{F}_0(x_{i_0}), \mathscr{F}_1(x_{i_1}), \mathscr{F}_2(x_{i_2}), \ldots.$$

   Now, we will want to associate a constant from $a_0^+, a_1^+, a_2^+, \ldots$, the ones used to extend $\mathscr{L}$, to each first order system. These constants will altogether form a subsequence $c_0, c_1, c_2, \ldots$ of $a_0^+, a_1^+, a_2^+, \ldots$. We will also restrict the constants so that they appear progressively in the introduced axioms of the first order systems. Therefore, we will restrict each c_n such that c_n is not $c_0, c_1, c_2, \ldots, c_{n-1}$ and does not appear in any $\mathscr{F}_0(x_{i_0}), \mathscr{F}_1(x_{i_1}), \mathscr{F}_2(x_{i_2}), \ldots, \mathscr{F}_2(x_{i_n})$[7].

   We are finally capable of described the sequence of first order systems to be constructed. The first member S_0, is S^+. Every other member S_{n+1} of the sequence is an extension of the previous one with the additional axiom,

$$\mathscr{G}_n, \text{ which is } (\sim (\forall x_{i_n})\mathscr{F}_n(x_{i_n})) \rightarrow (\sim \mathscr{F}_n(c_n)).$$

   Note that $\mathscr{G}_n$ has the same meaning as the *wf* which we previously stated that we would insert a version of as an axiom into each first order system. We choose to insert the contrapositive form only so that later parts of the proof will be slightly shorter.

3. We will next want to prove the consistency of each system in the sequence, and this will be done by induction. Note that, for the first time, we do not use strong induction here.

   (base case) The first member of the sequence, S^+ is consistent. This was proved in step 1.

   (inductive step) Suppose that S_n is consistent. For a contradiction, suppose that S_{n+1} is not consistent. Then there must be a *wf* $\mathscr{A}$ such that both $\mathscr{A}$ and $\sim \mathscr{A}$ are theorems of S_{n+1}.

   Let $\mathscr{B}$ be any *wf*. Since $\mathscr{A} \rightarrow (\sim \mathscr{A} \rightarrow (\sim \mathscr{B}))$ is a tautology, it is a theorem of S_{n+1}, so by two applications of MP, its proof can be extended to yield a proof of $\sim \mathscr{B}$. In particular, $\sim \mathscr{G}_n$ must be a theorem of S_{n+1}. A proof in S_{n+1} is a deduction from $\mathscr{G}_n$ in S_n. Therefore,

$$\mathscr{G}_n \vdash_{S_n} (\sim \mathscr{G}_n).$$

[6]The variables which appear will necessarily not be distinct.

[7]The constant c_0 will vacuously satisfy the first condition and will not appear in $\mathscr{F}_0(x_{i_0})$.

Since this proof involves no instance of Generalization, by the Deduction Theorem[8],

$$\vdash_{S_n} \mathscr{G}_n \to (\sim \mathscr{G}_n).$$

This proof may be extended by MP to yield a proof of $\sim \mathscr{G}_n$, i.e.,

$$\vdash_{S_n} (\sim (\forall x_{i_n})\mathscr{F}_n(x_{i_n})) \to (\sim \mathscr{F}_n(c_n)),$$

In turn, the proofs of the tautologies

$$\vdash_{S_n} ((\sim (\forall x_{i_n})\mathscr{F}_n(x_{i_n}) \to (\sim \mathscr{F}_n(c_n))) \to \mathscr{F}_n(c_n),$$

$$\vdash_{S_n} ((\sim (\forall x_{i_n})\mathscr{F}_n(x_{i_n})) \to (\sim \mathscr{F}_n(c_n))) \to (\sim (\forall x_{i_n})\mathscr{F}_n(x_{i_n})),$$

may be extended by MP to yield proofs of $\mathscr{F}_n(c_n)$ and $(\sim (\forall x_{i_n})\mathscr{F}_n(x_{i_n}))$. In the proof of $\mathscr{F}_n(c_n)$, each occurrence of c_n may be replaced by x, a variable not occurring in the proof, to yield a proof of $(\forall x)\mathscr{F}_n(x)$, since c_n does not occur in any of the axioms of S_n. and by Generalization, we obtain a proof of $(\forall x)\mathscr{F}_n(x)$, a *wf* in which x_{i_n} does not occur whatsoever in. Finally, by Proposition 4.18, we obtain a proof of $(\forall x_{i_n})\mathscr{F}_n(x_{i_n})$. But since its negation $(\forall x_{i_n})\mathscr{F}_n(x_{i_n})$ is also a theorem, we have found a contradiction. Therefore, S_{n+1} must be consistent when S_n is consistent, completing the inductive step.

We may conclude that every system in the sequence is consistent.

4. As we have been constructing in the proofs of Proposition 2.21 and 4.37, let S_∞ be the system whose set of axioms is the infinite union of all axioms of the members of the sequence of first order systems we constructed earlier. Suppose that the system S_∞ is not consistent. Then a contradiction could be derived using finitely many of its axioms. There exists an n large enough such that S_n has all of these axioms, and so the contradiction would exist in S_n, contradicting its consistency. Therefore, S_∞ must be consistent. Therefore, by Proposition 4.37, there exists some system T which is a complete and consistent extension of S_∞.

5. Here, we construct a particular interpretation of $\mathscr{L}^+$, the first order language defined in 1., whose fundamental property will be proved in the next step. The interpretation, which we will call I, is defined by the following.

   (a) The domain of interpretation is the terms (not *wf*s) of $\mathscr{L}^+$ which have no variables, i.e., the terms in which only constants appear. These terms are also known as *closed terms*[9].

   (b) The interpretation of any given predicate letter A_i^n is given by the relation $\bar{A}_i^n$ defined by the following statements in which $d_1, \ldots, d_n$ stand for elements in the domain of interpretation.

      i. $\bar{A}_i^n(d_1, \ldots, d_n)$ is true whenever $\vdash_T A_i^n(d_1, \ldots, d_n)$.

      ii. $\bar{A}_i^n(d_1, \ldots, d_n)$ is false whenever $\vdash_T \sim A_i^n(d_1, \ldots, d_n)$.

[8]The textbook mentions that $\mathscr{G}_n$ is closed here, which is either irrelevant or there is a mistake in this step of the proof.

[9]We refer to the terms without variables as closed because no quantifiers can occur in a term, so all appearances of variables can be thought of as being “free”, so a closed term contains only constants.

For the interpretation I to be valid, each statement letter must have an associated relation. Since each statement letter is a closed *wf*, then since T is consistent, the relation defined above is suitable. This relation is well-defined since T is complete, so indeed each statement letter has an associated relation, as desired.

We must define the interpretations of the constants and the function letters. These interpretations must necessarily be members of the domain, so they must be terms with no variables.

(c) The interpretation of any constant is the constant itself.

(d) The function letter f_n^i is interpreted as the function $\bar{f}_n^i$, which is itself defined by $\bar{f}_n^i(d_1, \ldots, d_n) = f_n^i(d_1, \ldots, d_n)$.
This may be confusing. Recall that, by Definition 3.14 of an interpretation, f_n^i must have a corresponding $\bar{f}_n^i$ which is defined as a function over the domain of interpretation. Therefore, in the particular interpretation that we are constructing, the function $\bar{f}_n^i$ must map some elements $d_1, \ldots, d_n$ in the domain of interpretation to a particular element in the domain of interpretation. Since $d_1, \ldots, d_n$ are closed terms, the term $f_n^i(d_1, \ldots, d_n)$, for any i, is a closed term as well. We choose to use this term as the value that $\bar{f}_n^i$ maps $d_1, \ldots, d_n$ to.

We have now defined an interpretation, I, of $\mathscr{L}^+$.

6. Now, we must prove the following property of I: For any *closed wf* $\mathscr{A}$ of T, $\mathscr{A}$ is a theorem of T is a theorem of T if and only if $\mathscr{A}$ is true in the interpretation I[10]. In symbols,

$$\vdash_T \mathscr{A} \text{ if and only if } I \models \mathscr{A}.$$

The proof is done by strong induction on n, the number of connectives and quantifiers in $\mathscr{A}$.

(hypothesis) Suppose that whenever a *wf* has fewer than n connectives and quantifiers, the *wf* is a theorem of T if and only if it is true in I.

(base case) It may be that $n = 0$, in which case $\mathscr{A}$ has no connectives or quantifiers, i.e., $\mathscr{A}$ is an atomic formula.

$\Rightarrow$ Suppose that $\mathscr{A}$ is a theorem of T. It is an atomic formula, so since it is a theorem of T, by the construction of interpretations of atomic formulas in I (see (b) of step 5), $\mathscr{A}$ is true in I.

$\Leftarrow$ The proof of this direction is the proof of the forward direction reversed. Suppose that $\mathscr{A}$ is true in I. Again, by construction of interpretations of atomic formulas in I, Since $\mathscr{A}$ is an atomic formula, it must be that $\mathscr{A}$ is a theorem of T.

(inductive step) It may be that $n > 0$. The *wf* $\mathscr{A}$ may appear in one of three forms.

(a) It may be that $\mathscr{A}$ is of the form $\sim \mathscr{B}$.

[10] We will only later use the one direction of this biconditional, but in this case the biconditional is easier to prove than either one of the directions individually.

$\Rightarrow$ Suppose that $\mathscr{A}$ is a theorem of T. Then $\sim \mathscr{B}$ is a theorem of T, and since T is consistent, $\mathscr{B}$ must not be a theorem of T. By the induction hypothesis, since $\mathscr{B}$ has fewer than n quantifiers and connectives, $\mathscr{B}$ is not true in I. Since $\mathscr{B}$ is closed, by Corollary 3.34, $\sim \mathscr{B}$ must be true in I, i.e. $\mathscr{A}$ is true in I.

$\Leftarrow$ The proof of this direction is the proof of the forward direction reversed. Suppose that $\mathscr{A}$, which is $\sim \mathscr{B}$, is true in I. Then since $\mathscr{B}$ is closed, $\mathscr{B}$ must not be true in I. By the induction hypothesis, $\mathscr{B}$ is not a theorem of T. Since T is consistent, $\sim \mathscr{B}$ must be a theorem of T, i.e., $\mathscr{A}$ is a theorem of T.

(b) It may be that $\mathscr{A}$ is of the form $\mathscr{B} \to \mathscr{C}$. Note that $\mathscr{B}$ and $\mathscr{C}$ must necessarily both be closed, since $\mathscr{A}$ is closed.

$\Rightarrow$ Suppose that $\mathscr{A}$ is a theorem of T. For a contradiction, suppose that $\mathscr{A}$, which is $\mathscr{B} \to \mathscr{C}$, is not true in I. Then there exists a valuation which satisfies $\mathscr{B}$ and $\sim \mathscr{C}$. Since $\mathscr{B}$ and $\sim \mathscr{C}$ are both closed *wf*s, then, by Proposition 3.33, any other valuation must satisfy $\mathscr{B}$ and $\sim \mathscr{C}$. Therefore, $\mathscr{B}$ is true in I and $\mathscr{C}$ is not true in I[11]. By the induction hypothesis, $\mathscr{B}$ is a theorem of T and $\mathscr{C}$ is not a theorem of T. Since T is consistent, $\sim \mathscr{B}$ must be a theorem of T. Note that $\mathscr{B} \to (\sim \mathscr{C} \to (\sim (\mathscr{B} \to \mathscr{C})))$ is a tautology, so it must be a theorem of T, and its proof can be easily extended by two instances of MP, yielding a proof of $\sim (\mathscr{B} \to \mathscr{C})$ in T, i.e. $\mathscr{A}$ is not a theorem of T. With this contradiction, we may conclude that if $\mathscr{A}$ is a theorem of T, then $\mathscr{A}$ is true in I.

$\Leftarrow$ Suppose that $\mathscr{A}$, which is $\mathscr{B} \to \mathscr{C}$, is true in I. For a contradiction, suppose that $\mathscr{A}$ is not a theorem of T. Then, since T is complete, $\sim (\mathscr{B} \to \mathscr{C})$ is a theorem of T. The *wf*s $\sim (\mathscr{B} \to \mathscr{C}) \to \mathscr{B}$ and $\sim (\mathscr{B} \to \mathscr{C}) \to \sim \mathscr{C}$ are both tautologies, and extending these proofs using MP yields proofs of $\mathscr{B}$ and $\sim \mathscr{C}$ in T. Since T is consistent, $\mathscr{C}$ is not a theorem of T. By the induction hypothesis, $\mathscr{B}$ is true in I and $\mathscr{C}$ is not true in I. Since $\mathscr{C}$ is closed, $\mathscr{C}$ must be false in I by Corollary 3.34 and Remark 3.25(c), and therefore, by Remark 3.25(d), $(\mathscr{B} \to \mathscr{C})$ is false in I, and therefore not true in I. With this contradiction, we may conclude that if $\mathscr{B} \to \mathscr{C}$ is true in I, then $\mathscr{A}$ is a theorem of T.

(c) It may be that $\mathscr{A}$ is of the form $(\forall x_i)\mathscr{B}(x_i)$. Note that $\mathscr{A}$ is closed and $\mathscr{B}(x_i)$ differs from $\mathscr{A}$ only in the appearance of the quantifier $(\forall x_i)$, so all variables other than x_i must not occur free. The variable x_i may be either free or not free in $\mathscr{A}(x_i)$[12], and we will prove the biconditional for these two cases.

i. It may be that x_i occurs free in $\mathscr{B}(x_i)$. Since all variables other than x_i in $\mathscr{B}(x_i)$ are not free, $\mathscr{B}(x_i)$ must have only one free variable. Therefore, it must be one of the *wf*s in the sequence constructed in 2., say $\mathscr{F}_m(x_{i_m})$.

$\Rightarrow$ Suppose that $\mathscr{A}$, which is

$$(\forall x_{i_m})\mathscr{F}_m(x_{i_m}),$$

is true in I. Since (K5) is logically valid,

$$(\forall x_{i_m})\mathscr{F}_m(x_{i_m}) \to \mathscr{F}(c_m)$$

[11]Here, $\mathscr{C}$ was already known to be not truth in I by the fact that some valuation was shown to not satisfy it.

[12]Even though x_i must appear in $\mathscr{B}(x_i)$, x_i can still occur not free in $\mathscr{B}(x_i)$ if it occurs free in one sub-formula but bound in another.

is logically valid, and therefore it is true in every interpretation, namely I, i.e.,

$$(\forall x_{i_m})\mathscr{F}_m(x_{i_m}) \rightarrow \mathscr{F}_m(c_m)$$

is true in I. Since $\mathscr{F}_m(c_m)$ not being true would make

$$(\forall x_{i_m})\mathscr{F}_m(x_{i_m}) \rightarrow \mathscr{F}_m(c_m)$$

false, considering that

$$(\forall x_{i_m})\mathscr{F}_m(x_{i_m})$$

is true, it must be that $\mathscr{F}_m(c_m)$ is true.
For a contradiction, suppose that $\mathscr{A}$ is not a theorem of T. Since T is consistent, $\sim \mathscr{A}$ must be a theorem instead, which is to say that

$$\sim (\forall x_{i_m})\mathscr{F}_m(x_{i_m})$$

is a theorem of T. Recall that T was constructed as an extension of S_∞, a system which has $\mathscr{G}_m$, which is

$$(\sim (\forall x_{i_m})\mathscr{F}_m(x_{i_m})) \rightarrow (\sim \mathscr{F}(c_m)),$$

as an axiom. We may use MP to obtain a proof of $\sim \mathscr{F}(c_m)$, but this contradicts the consistency of T, in light of the fact that $\mathscr{F}(c_m)$ is a theorem of T. With this contradiction, we may conclude that $\mathscr{A}$ is a theorem of T.
$\Leftarrow$ Suppose that $\mathscr{A}$ is a theorem of T, i.e.

$$(\forall x_{i_m})\mathscr{F}_m(x_{i_m})$$

is a theorem of T. For a contradiction, suppose that $\mathscr{A}$ is not true in I. Therefore, there exists a valuation which does not satisfy the above *wf*. By Definition 3.20, there exists a valuation v which does not satisfy $\mathscr{F}_m(x_{i_m})$. By Definition 3.17, the value $d = v(x_{i_m}$ is necessarily a member of the domain of I, and $v(d) = d$, since d is a closed term. Clearly, v is i_m-equivalent to itself and has $v(d) = d = v(x_{i_m})$. Proposition 3.23 states that v satisfies $\mathscr{F}_m(d)$ if and only if v satisfies $\mathscr{F}_m(x_i)$, which it does not, so v does not satisfy $\mathscr{F}_m(d)$. Therefore, $\mathscr{F}_m(d)$ is not true in I. Notice that $\mathscr{F}_m(d)$ is closed since d is a closed term and x_i was assumed to be the only free variable in $\mathscr{F}_m$. Therefore, by Corollary 3.34, $\sim \mathscr{F}_m(d)$ is true in I. But since

$$(\forall x_{i_m})\mathscr{F}_m(x_{i_m})$$

is a theorem of T, by axiom (K5) and MP and the fact that the closed term d is free for x_{i_m}, $\mathscr{F}_m(d)$ is a theorem of T. By the induction hypothesis, $\mathscr{F}_m(d)$ is true in I, contradicting that $\sim \mathscr{F}_m(d)$ is true in I.
With this contradiction, we may conclude that $\mathscr{A}$ is true in I.

ii. It may be that x_i does not occur free in $\mathscr{B}(x_i)$. Since all variables other than x_i do not occur free in it, $\mathscr{B}(x_i)$ must be closed.
$\Rightarrow$ Suppose that $\mathscr{A}$, which is $(\forall x_i)\mathscr{B}(x_i)$, is a theorem of T. By (K4) and MP, $\mathscr{B}(x_i)$ must be a theorem of T, and since it is a closed *wf* with fewer

than n connectives and quantifiers, by the induction hypothesis, it is true in I. By Corollary 3.28, $(\forall x_i)\mathscr{B}(x_i)$, which is $\mathscr{A}$, must be true in I.
$\Leftarrow$ Suppose that $(\forall x_i)\mathscr{B}(x_i)$ is true in I. By Corollary 3.28, $\mathscr{B}(x_i)$ is true in I. It is a closed *wf* with fewer than n connectives and quantifiers, so by the induction hypothesis, $\mathscr{B}(x_i)$ is a theorem of T. Its proof can be extended via Generalization to yield a proof of $(\forall x_i)\mathscr{B}(x_i)$, which is $\mathscr{A}$, in T, i.e. $\mathscr{A}$ is a theorem of T.

7. Finally, we conclude that there exists some interpretation in which every theorem of S is true. Recall that T was obtained from S by enlarging the language and adding new axioms. Therefore, every proof in S is a proof in T, so every theorem of S is a theorem of T. By the previous step, we may further infer that every theorem of S is true in the interpretation I[13].

   Now we obtain the interpretation that we desire by restricting or "shrinking" I so that it is an interpretation of S. We do this by removing the interpretations of the terms containing the constants added to $\mathscr{L}$ to construct $\mathscr{L}^+$. Similarly, the domain becomes the closed terms of $\mathscr{L}$ instead of $\mathscr{L}^+$. As desired, every theorem of S is true in this interpretation[14].

The seven steps above demonstrate that every consistent formal system has an interpretation in which all the theorems of the system are true. □

With this result, the proof of the Adequacy Theorem is brief.

Proposition 4.39 (The Adequacy Theorem for $K_{\mathscr{L}}$)**.** If $\mathscr{A}$ is a logically valid *wf* of $\mathscr{L}$, then $\mathscr{A}$ is a theorem of $K_{\mathscr{L}}$.

Proof. Let $\mathscr{A}$ be a logically valid *wf* of $\mathscr{L}$. The universal closure $\mathscr{A}'$ of $\mathscr{A}$ is necessarily closed. By Corollary 3.28, $\mathscr{A}'$ must be logically valid. For a contradiction, suppose that $\mathscr{A}$ is not a theorem of $K_{\mathscr{L}}$. Then by Proposition 4.19, $\mathscr{A}'$ must not be a theorem also. By Proposition 4.35, including $\sim \mathscr{A}'$ as an axiom of $K_{\mathscr{L}}$ yields a new system $K'_{\mathscr{L}}$, which is consistent. By Proposition 4.38, there is an interpretation in which every theorem of $K'_{\mathscr{L}}$ is true. In particular, $\sim \mathscr{A}'$ is true in this interpretation. Since $\sim \mathscr{A}'$ is true, by Corollary 3.34, $\mathscr{A}'$ is not true. But this contradicts $\mathscr{A}'$ being logically valid, since $\mathscr{A}'$ must be true in any interpretation. We may conclude that $\mathscr{A}$ is a theorem of $K_{\mathscr{L}}$. □

Solutions to exercises

11. Let S be an extension of $K_{\mathscr{L}}$. Suppose that $\mathscr{L}$ is not empty (there exists *wf*s of $\mathscr{L}$)[15].

    $\Rightarrow$ Suppose that S is inconsistent. Then there exists a *wf* $\mathscr{A}$ such that $\mathscr{A}$ and $\sim \mathscr{A}$ are both theorems of S. Since, $\mathscr{A} \to (\sim \mathscr{A} \to \mathscr{B})$ is a tautology for any *wf* $\mathscr{B}$,

[13]Note again that we only used one direction of the biconditional in the previous step, as we said we would. We can now see that the biconditional was easier to prove than either of the directions because, informally speaking, proving both directions in the inductive steps relied on the other directions in the inductive hypotheses.

[14]We could have also constructed this interpretation early on. Then I would have been built by expanding the interpretation.

[15]As per the definition given in the beginning of Section 3.2, we may not assume that $\mathscr{L}$ actually has an *wf*s. To be pedantic, when $\mathscr{L}$ is empty, the biconditional we are to prove is not true.

extending this proof by two applications of MP will prove $\mathscr{B}$. Therefore, any *wf* is a theorem of S.

$\Leftarrow$ Suppose that every *wf* of $\mathscr{L}$ is a theorem of S. Then any *wf* and its negation are both theorems of S, so it is not consistent.

12. Let S be a consistent first order system such that, for every closed *wf* of S, if the system obtained by including $\mathscr{A}$ as an additional axiom is consistent then $\mathscr{A}$ is a theorem of S. For a contradiction, suppose that S is not complete. Then there is a closed *wf* $\mathscr{A}$ such that $\mathscr{A}$ and $\sim \mathscr{A}$ are not theorems of S.

    Since $\mathscr{A}$ is not a theorem, by Proposition 4.35, the extension of S with $\sim \mathscr{A}$ as an additional axiom is consistent. Therefore, $\sim \mathscr{A}$ must be a theorem of S, which is a contradiction[16].

13. Let $\mathscr{B}$ be $\sim \mathscr{A}$. Then $\mathscr{A} \vee \mathscr{B}$ is logically valid, so it is a theorem of $K_{\mathscr{L}}$. But $\mathscr{A}$ and $\mathscr{B}$ cannot both be theorems of $K_{\mathscr{L}}$ or else it would not be consistent. Therefore, the answer to the exercise is negative.

14. No predicate letter is logically valid, since each predicate letter in some interpretation can be interpreted by a relation that assigns false to all of its values. Therefore, by Proposition 4.35, the extension of S obtained by including the negation of any predicate letter is consistent. Since there are infinitely many predicate letters, there are infinitely many consistent extensions of S.

4.5 Models

Definition 4.40. A *model* can describe a set of *wf*s of $\mathscr{L}$ or a first order system.

(i) Let Γ be a set of *wf*s of $\mathscr{L}$. A *model of S* is an interpretation of $\mathscr{L}$ in which each *wf* of Γ is true.

(ii) Let S be a first order system. A *model of S* is an interpretation in which theorem of S is true.

Note that by Proposition 4.38, every consistent first order system has a model. Also, any interpretation of $K_{\mathscr{L}}$ is a model of it for any $\mathscr{L}$. This is because, by the Adequacy Theorem, Proposition 4.39, all theorems of $K_{\mathscr{L}}$ are logically valid, so they are true in all interpretations.

Proposition 4.41. Let S be a first order system, and let I be an interpretation. If every axiom of S is true in I, then I is a model of S.

Proof. We must show that any theorem of S, $\mathscr{A}$, is true in I. The proof is by induction on n, the number of *wf*s in the proof of $\mathscr{A}$.

(hypothesis) Suppose that any theorem with fewer than n *wf*s in its proof is true in I.

(base case) It may be that $n = 1$, which is to say that $\mathscr{A}$ is an axiom of S, therefore it is true in I.

(inductive step) It may be that $n > 1$. There are three cases to consider, each one corresponding to one of the three ways in which $\mathscr{A}$ could be derived in its proof.

[16] The hints in the back of the textbook say to apply Proposition 4.35 twice, but it is only applied once here. There may be a mistake in the textbook or in this text.

1. It may be that $\mathscr{A}$ is an axiom, in which it is true in I.

2. It may be that $\mathscr{A}$ is derived from $\mathscr{B}$ and $\mathscr{B} \to \mathscr{A}$ via MP. Since $\mathscr{B}$ and $\mathscr{B} \to \mathscr{A}$ are true in I by the induction hypothesis, $\mathscr{A}$ is true in I by Proposition 3.26.

3. It may be that $\mathscr{A}$ is derived from $\mathscr{B}$ by Generalization. Since $\mathscr{B}$ is true in I by the induction hypothesis, $(\forall x_i)\mathscr{B}$, which is $\mathscr{A}$, is true in I by Proposition 3.27.

Therefore, for any n, $\mathscr{A}$ is true in I. □

A result of this proposition is that if an interpretation is true for the set of axioms of a first order system, it is true for the first order system.

Proposition 4.42. A first order system is consistent if and only if it has a model.

Proof. Let S be a first order system.

$\Rightarrow$ Suppose that S is consistent. By Proposition 4.38, S has a model.

$\Leftarrow$ Suppose that there exists a model of S. For a contradiction, suppose that S is not consistent. Then there exists a theorem $\mathscr{A}$ in S such that $\mathscr{A}$ and $\sim \mathscr{A}$ are both theorems of S. Then they must be true in I, which is impossible by Remark 3.25(b). Therefore, S must be consistent. □

It is important to note that just because a *wf* is true in a model of some system S does not mean that the *wf* is a theorem of S. This becomes obvious when considering that every interpretation is a model of S, but some interpretations may contain true *wf*s which are logically valid.

In the book, the following basic but unproved proposition is used.

Proposition. Any model of an extension of a first order system is a model of the first order system itself.

Proof. Let S be a consistent first order system with an extension S^+. Let $\mathscr{A}$ be a theorem of S. Since S^+ is an extension of S, $\mathscr{A}$ must be a theorem of S^+, so it must be true in any model of S^+. □

Proposition 4.44. Let S be a consistent first order system. If $\mathscr{A}$ is a closed *wf* which is true in every model of S, then $\mathscr{A}$ is a theorem of S.

Proof. For a contradiction, suppose that $\mathscr{A}$ is not a theorem of S. By Proposition 4.35, the extension with $\sim \mathscr{A}$ as an additional axiom is consistent. By Proposition 4.42, this extension necessarily has a model. This model must necessarily be a model of S. Since $\sim \mathscr{A}$ is a theorem of the extension of S, it must be true in the model, by Definition 4.40. By Corollary 3.34, since $\sim \mathscr{A}$ is true (and closed) in the model, $\mathscr{A}$ must not be true in the model. This contradicts the assumption that $\mathscr{A}$ is true in every model of S, so we may conclude that $\mathscr{A}$ is a theorem of S. □

This next theorem has many paradoxical implications. For now, it will be only stated and proved.

Proposition 4.45 (Löwenheim-Skolem Theorem)**.** If a first order system has a model, then it has a model whose domain is countable.

Proof. Let S be a consistent first order system. As shown in the proof of Proposition 4.38, there exists a model of S whose domain is the set of closed terms of the language of S[17]. The set of *wf*s of S is countable, so for each term, associate the term x uniquely with the *wf* $A_1^1(x)$. This yields a subset of the *wf*s of $\mathscr{L}$ (or possibly $\mathscr{L}$ with the addition of A_1^1), which is countable since the set of *wf*s of $\mathscr{L}$ is countable (see the appendix). □

Proposition 4.46 (The Compactness Theorem)**.** If each finite subset of the set of axioms of a first order system S has a model, then S has a model.

Proof. Suppose that each finite subset of the axioms of S has a model. For a contradiction, suppose that S does not have a model. By Proposition 4.42, S does is not consistent. So there exists some *wf* $\mathscr{A}$ such that $\mathscr{A}$ and $\sim \mathscr{A}$ are both theorems of S. These proofs contain Γ, a finite subset of the axioms in their proofs. Therefore, Γ has a model M.

We will now prove that a theorem $\mathscr{C}$ whose proof has only the axioms in Γ is true in M by induction on n, the number of connectives and quantifiers in $\mathscr{C}$[18].

(hypothesis) Any theorem using the axioms in Γ with fewer than n connectives is true in M.

(base case) It may be that $n = 1$. That is, $\mathscr{C}$ is an axiom of Γ. Therefore, it is true in M, by Definition 4.40.

(inductive step) It may be that $n > 1$. Then there are three cases to consider.

1. It may be that $\mathscr{C}$ is an axiom of Γ. Therefore, it is true in M, by Definition 4.40.

2. It may be that $\mathscr{C}$ is derived via MP and $\mathscr{B}$ and $\mathscr{B} \to \mathscr{C}$. Then $\mathscr{B}$ and $\mathscr{B} \to \mathscr{C}$ are both true in the interpretation M. By Proposition 3.26, $\mathscr{C}$ is true in M.

3. It may be that $\mathscr{C}$ is derived via Generalization from $\mathscr{B}$, which is true in M by the induction hypothesis. Therefore, since $\mathscr{C}$ is of the form $(\forall x_i)\mathscr{B}$, by Proposition 3.27, $\mathscr{C}$ is true in M.

With this induction complete, since $\mathscr{A}$ and $\sim \mathscr{A}$ are theorems whose proofs use only the axioms in Γ, we may conclude that $\mathscr{A}$ and $\sim \mathscr{A}$ are both true in M. This contradicts the fact that both a *wf* and its negation cannot be true in an interpretation (Remark 3.25(c)). With this contradiction, we may conclude that S has a model. □

Note that the converse of this is true. If a first order system has a model, then every theorem is true in the model. Since any axiom is a theorem, it will be true in the model. So the model will also be a model for any finite subset of the axioms.

Corollary 4.47. Let Γ be an infinite set of *wf*s of K. If each finite subset of Γ has a model, then Γ has a model.

Proof. Suppose that each finite subset of Γ has a model. Consider the first order system which extends K by having Γ as its axioms. By Proposition 4.46, Γ has a model. □

[17]The book states that the domain is the set of closed terms of the enlarged language. This does not seem to be necessary.

[18]This proof is nearly identical to that of Proposition 4.41.

The above corollary is equivalent to Proposition 4.46, although proving the other direction would require relaxing the restriction that Γ is an infinite set. We could prove the relaxed version corollary explicitly, and this would be like the proof of Proposition 4.46. Then we would be able to see that Proposition 4.46 follows.

Finally, with models, we can now show that there is another way, other than Proposition 4.37, to construct a complete and consistent first order system from a given consistent first order system.

Proposition. Let S be a first order system. If S has a model, then a complete extension of S shares the same model.

Proof. Since S has a model M, it is consistent by Proposition 4.42. If S is complete, then we can add some theorem of S as an axiom to obtain a complete extension of S which shares the same model. So assume that S is not complete. Then there must exist some closed *wf* $\mathscr{A}$ such that neither $\mathscr{A}$ nor $\mathscr{A}$ is a theorem of S. By Proposition 3.33, in M, this *wf*, since it closed, is either true or false.

Now we define $S(M)$ to be the first order system which is the extension of S obtained by adding all *wf*s of M as axioms. Of course, every axiom of $S(M)$ will be true in M, so M is a model of $S(M)$. Additionally, we can show that the theorems of $S(M)$ are precisely the axioms of $S(M)$. This is because all *wf*s in a proof in $S(M)$ will be true in M because the rules of deduction of $S(M)$ conserve truth[19].

Now $S(M)$ is consistent, since if a *wf* and its negation are both theorems, then they are both true in the model, which is impossible, by Definition 3.20. Also, $S(M)$ is complete, since if $\mathscr{A}$ is a closed *wf*, either $\mathscr{A}$ or $\sim \mathscr{A}$ is true in M, by Corollary 3.34.

Therefore, we have constructed for any first order system S, the system $S(M)$, which is a complete extension of S that shares the same model. □

Solutions to exercises

15. Suppose that $\mathscr{A}$ can be deduced from Γ with n *wf*s in its deduction. We proceed by induction on n to show that $\mathscr{A}$ is true in M.

    (hypothesis) Suppose that any *wf* with fewer than n *wf*s in its proof is true in M.

    (base case) It may be that $n = 0$, $\mathscr{A}$ is an axiom or a member of Γ. If it is an axiom, then it is logically valid, so it is true in M. If it is a member of Γ, then since M is a model of Γ, $\mathscr{A}$ is true in M.

    (inductive step) It may be that $n > 1$.

    (a) It may be that $\mathscr{A}$ is an axiom or a member of Γ. See the base case.
    (b) It may be that $\mathscr{A}$ is deduced by MP. By Proposition 3.26 and the induction hypothesis, $\mathscr{A}$ is true in M.
    (c) It may be that $\mathscr{A}$ is deduced by Generalization. By Proposition 3.26 and the induction hypothesis $\mathscr{A}$ is true in M.

    Note that this proof has been treated tersely because it is so essentially no different from the proofs of Proposition 4.41 and 4.46.

[19] A formal proof of this would be via induction, but we have done this already in Proposition 4.41 and 4.46.

The converse is not true. Let Γ be the logically valid *wf*s of $\mathscr{L}$. Trivially, any interpretation is a model of Γ. Consider any interpretation with a true *wf* which is not logically valid to disprove the other direction of the exercise.

16. Let $\mathscr{A}$ be a closed *wf* true in a model of S. If $\mathscr{A}$ is not a theorem in S, then $\sim \mathscr{A}$ must be a theorem of S, since S is consistent and complete. Therefore, $\sim \mathscr{A}$ must be true in any model of S. But both $\mathscr{A}$ and $\sim \mathscr{A}$ cannot be both true in a model, as this would contradict Remark 3.25(b). So it must be that $\mathscr{A}$ is a theorem of S. Therefore, $\mathscr{A}$ is true in any another model, as desired.

17. It is easy to see that M is also a model for the axioms added to S to obtain S^+. Any theorem of S^+ will be deduction from this set of axioms in S. Hence, by exercise 15, every theorem of S^+ will be true in M, so M is a model for S^+. By Proposition 4.46, S^+ is consistent.

    To see that S^+ need not be complete, let S^+ be S. That is, no atomic formulas of $\mathscr{L}$ are true in M, so no atomic formulas are added as axioms of S. But S is not complete since both $(\forall x_1)A_1^1(x_1)$ and $\sim (\forall x_1)A_1^1(x_1)$ are not logically valid, therefore they are not theorems of S.

18. We will use S^+ to indicate the extension of S.

    By the same reasoning as in the previous exercise, S^+ is consistent. Just as in the previous exercise, to see that S^+ need not be complete, let S^+ be S. That is, no closed atomic formulas of $\mathscr{L}$ or their negations are true in M, so no atomic formulas are added as axioms of S. But S is not complete since both $(\forall x_1)A_1^1(x_1)$ and $\sim (\forall x_1)A_1^1(x_1)$ are not logically valid, therefore they are not theorems of S.

19. An interpretation I of $\mathscr{L}$ is a model if A_I contains all $\bar{a}_i$ such that $A_1^1(a_i)$ is a theorem of S. Therefore, any $\{A_1^1(a_i), \ldots, A_1^1(a_n)\}$ has M_n as a model. Now consider any finite subset of all $A_1^1(a_i)$. Since it is finite, it has a highest indexed a_i, and so the subset has M_n as a model. By Corollary 4.47, S must have a model M in which all $\bar{a}_i \in A_M$ for every i.

Chapter 5

Mathematical systems

5.1 Introduction

From here no out, we will study formal systems. That is, we will study $K_{\mathscr{L}}$ with the addition of some axioms. The six axioms in $K_{\mathscr{L}}$ are called *logical axioms*. The additional axioms in a formal system are known as *proper axioms*.

5.2 First order systems with equality

In all languages that we study in this chapter, = will be the intended interpretation of A_1^2. In a system with A_1^2 interpreted as =, we will include the following as proper axioms.

- (E7) $A_1^2(x_1, x_1)$.
- (E8) $A_1^2(u, v) \to A_1^2(f_i^n(\ldots, u, \ldots), f_1^n(\ldots, v, \ldots))$
- (E9) $A_1^2(u, v) \to (A_i^n(\ldots, u, \ldots) \to A_i^n(\ldots, v, \ldots))$

The axiom (E7) is a single *wf*. The rules (E8) and (E9) are axiom schemes, where u and v are any terms. The function letter f_i^n and the predicate letter A_i^n are to stand for arbitrary functions and statements. The position in which u and v appear in the sequences of terms $\ldots, u, \ldots$ and $\ldots, v, \ldots$ must be the same.

All of these axioms are written with no quantifiers. Whoever, it is easy to prove that they are equivalent to their universal closures, the *wf*s in which all the variables occur bound. Proposition 4.18 can be used to change (E7) to be true for any variable, not just x_1.

The informal intended meaning of (E7) is "anything is equal to itself." The axiom schemes (E8) and (E9) are intended to mean "if two things are equal, then any predicate involving the things are evaluated in the same way[1]", or "equal things may be substituted for each other."

Definition 5.4. The axioms (E7), (E8), and (E9) are called *axioms for equality*. A system which includes the axioms given be these schemes is known as a *first order system with equality*.

[1]This is sometimes called the Identity of Indiscernibles.

Proposition 5.5. A first order system with equality has the following *wf*s as theorems.

(i) $(\forall x_1)A_1^2(x_i, x_i)$.

(ii) $(\forall x_1)(\forall x_2)(A_1^2(x_1, x_2) \to A_1^2(x_2, x_1))$.

(iii) $(\forall x_1)(\forall x_2)(\forall x_3)(A_1^2(x_1, x_2) \to (A_1^2(x_2, x_3) \to A_1^2(x_1, x_3)))$.

Proof. Let S be a first order system with equality. We will prove each assertion in S.

(i) Apply Generalization to (E7).

(ii) The following is a proof of the *wf* in S.

1	$A_1^2(x_1, x_2) \to (A_1^2(x_1, x_1) \to A_1^2(x_2, x_1))$	(E9)
2	$(A_1^2(x_1, x_2) \to (A_1^2(x_1, x_1) \to A_1^2(x_2, x_1))) \to$ $((A_1^2(x_1, x_2) \to (A_1^2(x_1, x_1))) \to (A_1^2(x_1, x_2) \to A_1^2(x_2, x_1)))$	(K2)
3	$((A_1^2(x_1, x_2) \to (A_1^2(x_1, x_1))) \to (A_1^2(x_1, x_2) \to A_1^2(x_2, x_1)))$	1, 2, MP
4	$(A_1^2(x_1, x_1) \to (A_1^2(x_1, x_2) \to A_1^2(x_1, x_1)))$	(K1)
5	$A_1^2(x_1, x_1)$	(E6)
6	$A_1^2(x_1, x_2) \to A_1^2(x_1, x_1)$	5, 6, MP
7	$A_1^2(x_1, x_2) \to A_1^2(x_2, x_1)$	3, 6, MP
8	$(\forall x_1)(\forall x_2)A_1^2(x_1, x_2) \to A_1^2(x_2, x_1)$	7, Generalization

(iii) The following is a proof of the *wf* in S.

1	$A_1^2(x_2, x_1) \to (A_1^2(x_2, x_3) \to A_1^2(x_1, x_3))$	(E9)
2	$A_1^2(x_1, x_2) \to A_1^2(x_2, x_1)$	(ii) above
3	$A_1^2(x_1, x_2) \to (A_1^2(x_2, x_3) \to A_1^2(x_1, x_3))$	1, 2, HS
4	$(\forall x_1)(\forall x_2)A_1^2(x_1, x_2) \to (A_1^2(x_2, x_3) \to A_1^2(x_1, x_3))$	Generalization

Thus (i), (ii), (iii) are theorems of any first order system. □

From this proposition, we can see that any interpretation of A_1^2 in a model must be an equivalence relation, for the three properties verified above correspond to reflexivity, symmetry, and transitivity.

The axioms for equality do not necessarily have to be interpreted by = in a model of equality. As an example, consider addition in the integers modulo 2. Let $\mathscr{L}$ be a language with equality with f_1^2 interpreted as addition modulus 2 and with its domain being the integers. However, let $A_1^2(x_i, x_j)$ be interpreted as $x \equiv y \pmod 2$, where x and y are the interpretations of x_i and x_j. We will verify that this interpretation is a model by verifying the axioms for equality.

1. For (E7), its interpretation is $x \equiv x \pmod 2$, which is true.

2. For (E8), the verification is done in exercise 1.

3. For (E9), their are only two instances of the scheme. The first one is

$$A_1^2(t,u) \to (A_1^2(t,v) \to A_1^2(u,v)),$$

and its interpretation is

$$\text{if } x \equiv y \pmod 2, \text{ then } x \equiv z \pmod 2 \text{ implies } y \equiv z.$$

The second one is

$$A_1^2(t,u) \to (A_1^2(t,v) \to A_1^2(u,v)),$$

and its interpretation is

$$\text{if } x \equiv y \pmod 2, \text{ then } z \equiv x \pmod 2 \text{ implies } y \equiv y.$$

These statements in I are both true.

Seeing as though we have verified the axioms for equality, we have found a model of a first order system with equality in which A_1^2 is not interpreted as =. However, every first order system with equality *can* have a model with this desired property.

Proposition 5.6. If S is a consistent first order system with equality, then S has a model in which the interpretation of A_1^2 is =.

Proof. By Proposition 4.42, since S is consistent, it has a model M. The interpretation $\bar{A}_1^2$ must be an equivalence relation by Proposition 5.4. Denote the equivalence containing x by $[x]$, as usual, where x is some member of the domain of M.

Now we construct an interpretation M^* whose domain is the equivalence classes of the interpretation of A_1^2 in M. Let any constant a_i in the language of S be interpreted in M^* by $[a_i]$.

Now we must define how the function letters of the language S are to be interpreted. Let any function f_i^n be interpreted by $\bar{\bar{f}}_i^n$, which is defined by

$$\bar{\bar{f}}_i^n([\bar{x}_1], \dots, [\bar{x}_n]) = [\bar{f}_i^n(\bar{x}_1, \dots, \bar{x}_n)],$$

Let any predicate letter be interpreted by

$$\bar{\bar{A}}_i^n([\bar{x}_1], \dots, [\bar{x}_n]) \text{ iff } [\bar{\bar{A}}_i^n(\bar{x}_1, \dots, \bar{x}_n)],$$

where $\bar{x}_j$, for any j, stands for any member of the domain of M. Of course, we want $\bar{\bar{A}}_1^2$ to be interpreted by =.

As usual, since the function $\bar{\bar{f}}_i^n$ takes equivalence classes as its arguments, we must verify that we indeed have defined a function. As a reminder, this means that we must verify that if $x = y$, then $f(x) = f(y)$, for any function f and members of its domain x, y.

So let that $\bar{\bar{f}}^n$ is some function of n-places in M^*. Let $\bar{x}_1, \dots, \bar{x}_n$ and $\bar{y}_1, \dots, \bar{y}_n$ be elements in the domain of M. Suppose that

$$[\bar{x}_1, \dots, \bar{x}_n] = [\bar{y}_1, \dots, \bar{y}_n], \text{ i.e., } [\bar{x}_1] = [\bar{y}_1], \dots, [\bar{x}_n] = [\bar{y}_n].$$

By $(E8)$ we know that

$$A_1^2(x_1, x_2) \to A_1^2(\bar{f}^n(\dots, x_1, \dots), \bar{f}^n(\dots, x_2, \dots))$$

is a theorem in S, where f^n is any n-valued function letter in the language of S. Because M is a model of S, the *wf* is true in M. Therefore, in M this is interpreted as

$$\text{if } \bar{A}_1^2(\bar{x}_i, \bar{y}_i) \text{ then, } \bar{A}_1^2(\bar{f}^n(\dots, \bar{x}_i, \dots), \bar{f}^n(\dots, \bar{y}_i, \dots)).$$

In M^*, this is interpreted as

$$\text{if } \bar{\bar{A}}_1^2([\bar{x}_i], [\bar{y}_i]) \text{ then, } \bar{\bar{A}}_1^2([\bar{f}^n(\dots, \bar{x}_i, \dots)], [\bar{f}^n(\dots, \bar{y}_i, \dots)]),$$

which is to say that,

$$\text{if } [\bar{x}_i] = [\bar{y}_i] \text{ then, } [\bar{f}^n(\dots, \bar{x}_i, \dots)] = [\bar{f}^n(\dots, \bar{y}_i, \dots)],$$

since $\bar{\bar{A}}_1^2$ is interpreted as =. Therefore the following implications are all true.

$$\begin{array}{lll} \text{If } [\bar{x}_1] = [\bar{y}_1], & \text{then} & [\bar{f}^n(\bar{x}_1, \bar{x}_2, \dots, \bar{x}_n)] = [\bar{f}^n(\bar{y}_1, \bar{x}_2, \dots, \bar{x}_n)]. \\ \text{If } [\bar{x}_2] = [\bar{y}_2], & \text{then} & [\bar{f}^n(\bar{y}_1, \bar{x}_2, \dots, \bar{x}_n)] = [\bar{f}^n(\bar{y}_1, \bar{y}_2, \dots, \bar{x}_n)]. \\ & \vdots & \\ \text{If } [\bar{x}_n] = [\bar{y}_n], & \text{then} & [\bar{f}^n(\bar{y}_1, \bar{y}_2, \dots, \bar{x}_n)] = [\bar{f}^n(\bar{y}_1, \bar{y}_2, \dots, \bar{y}_n)]. \end{array}$$

All the equalities on the left-hand side are satisfied, so the equalities on the right are true. Using transitivity of equality,

$$[\bar{f}^n(\bar{x}_1, \bar{x}_2, \dots, \bar{x}_n)] = [\bar{f}^n(\bar{y}_1, \bar{y}_2, \dots, \bar{y}_n)],$$

and by definition of $\bar{\bar{f}}^n$,

$$\bar{\bar{f}}^n([\bar{x}_1], [\bar{x}_2], \dots, [\bar{x}_n)]]) = \bar{\bar{f}}^n([\bar{y}_1], [\bar{y}_2], \dots, [\bar{y}_n)]).$$

Therefore, $\bar{\bar{f}}^n$ is well-defined. Using a similar process, we can deduce that any interpretation in M^* of a statement letter in the language of S is well-defined (see Exercise 4). We may conclude that M^* is a model of S in which A_1^2 is interpreted as =. □

Definition 5.7. Let S be a first order system with equality. A *normal model* of S is a model in which A_1^2 is interpreted as =.

For convenience's sake, in any normal model, we will now write $x_i = x_j$ to mean $A_1^2(x_i, x_j)$.

Solutions to exercises

1. Since there is only one 2-placed predicate letter in $\mathscr{L}$, two possible instances of (E8) are
$$A_1^2(x_1, x_2) \to A_1^2(f_1^2(x_1, x_3), f_1^2(x_2, x_3))$$
and
$$A_1^2(x_1, x_2) \to A_1^2(f_1^2(x_3, x_1), f_1^2(x_3, x_2)).$$
Seeing as any three terms t, u, v are free for x_1, x_2, x_3, we may say that use (K5) to say
$$A_1^2(t, u) \to A_1^2(f_1^2(t, u), f_1^2(v, u))$$

and

$$A_1^2(t,u) \to A_1^2(f_1^2(t,u), f_1^2(t,v)),$$

and these are interpreted as

$$\text{if } x_1 \equiv x_3 \pmod 2, \text{ then } x_1 + x_2 \equiv x_3 + x_2 \pmod 2$$

and

$$\text{if } x_2 \equiv x_3 \pmod 2, \text{ then } x_1 + x_2 \equiv x_1 + x_3 \pmod 2,$$

which are both true statements in the interpretation[2].

2. Suppose that there exists some model of S in which $\mathscr{A}$ is not true. Then $\mathscr{A}$ must not be a theorem of S, so by Proposition 4.35, there exists a consistent extension S^* of S in which $\sim \mathscr{A}$ is a theorem. By Proposition 5.6, there exists a normal model M^* of S^*. But a normal model of S^* must also be a normal model of S, since all the theorems of S are theorems of S^*. So $\mathscr{A}$ must be true in M^*. But $\sim \mathscr{A}$ is a theorem of S^*, so it too is true in M^*, which contradicts Definition 3.20. Therefore, $\mathscr{A}$ must be true in all models of S.

3. Let E be the first order system with equality. This exercise is made easier by either proving the statement for x_i or x_j or by proving the *wf*

$$(x_1 = x_2 \to (\mathscr{A}(x_1) \leftrightarrow \mathscr{A}(x_2))$$

instead. We will do this second option. The proof is by induction on n, the number of connectives and quantifiers of $\mathscr{A}(x_1)$.

(hypothesis) Suppose that for any *wf* with fewer than n connectives and quantifiers, if $x_i = x_j$, then the original *wf* is provably equivalent to any identical *wf* with a single free instance of x_1 substituted with x_2.

(base case) It may be that $n = 0$, i.e., $\mathscr{A}(x_1)$ is an atomic formula, $A_i^n(\ldots, x_1, \ldots))$, say. Since there are no quantifiers in the expression, x_2 is free for x_1, and we know by (E7) that

$$\vdash_E x_1 = x_2 \to (A_i^n(\ldots, x_1, \ldots) \to A_i^n(\ldots, x_2, \ldots)).$$

Notice that $A_i^n(\ldots, x_2, \ldots)$ has x_2 substituted for one of the free occurrences of x_1, as desired. We also have

$$\vdash_E x_2 = x_1 \to (A_i^n(\ldots, x_2, \ldots) \to A_i^n(\ldots, x_1, \ldots)).$$

Since = is symmetric (Proposition 5.4), $x_1 = x_2 \to x_2 = x_1$, so by HS,

$$\vdash_E x_1 = x_2 \to (A_i^n(\ldots, x_2, \ldots) \to A_i^n(\ldots, x_1, \ldots)).$$

Therefore,

$$\vdash_E x_1 = x_2 \to (A_i^n(\ldots, x_2, \ldots) \leftrightarrow A_i^n(\ldots, x_1, \ldots)).$$

by MP and the tautology

$$\mathscr{A} \to (\mathscr{B} \to \mathscr{C}) \to ((\mathscr{A} \to (\mathscr{C} \to \mathscr{B})) \to (\mathscr{A} \to (\mathscr{A} \leftrightarrow \mathscr{C}))),$$

where $\mathscr{A}, \mathscr{B}, \mathscr{C}$ are any *wf*s of the language of E.

(inductive step) It may be that $n > 1$. There are three cases to consider.

[2]This exercise is ambiguous in its requirement. In the example, a shorter procedure was used to prove that (E9) was correct in the interpretation, but the suggestions in the back of the textbook suggest something different.

(a) It may be that $\mathscr{A}(x_1)$ is of the form $\sim \mathscr{B}(x_1)$. By the induction hypothesis

$$\vdash_E (x_1 = x_2 \longrightarrow (\mathscr{B}(x_1) \leftrightarrow \mathscr{B}(x_2))),$$

and since $\mathscr{B}(x_1) \leftrightarrow \mathscr{A}(x_2)$ is provably equivalent to $\sim \mathscr{B}(x_1) \leftrightarrow \sim \mathscr{B}(x_2)$, we can easily deduce that

$$\vdash_E (x_1 = x_2 \longrightarrow (\sim \mathscr{B}(x_1) \leftrightarrow \sim \mathscr{B}(x_2))),$$

by Proposition 4.22, i.e.,

$$\vdash_E (x_1 = x_2 \longrightarrow (\mathscr{A}(x_1) \leftrightarrow \mathscr{A}(x_2))).$$

(b) It may be that $\mathscr{A}(x_1)$ is an implication. Therefore, $\mathscr{A}(x_2)$ may appear in one of four forms.

i. It may be that $\mathscr{A}(x_2)$ is $\mathscr{B}(x_2) \longrightarrow \mathscr{C}(x_1)$, i.e., both subformulas contain a free instance of x_1, but $\mathscr{B}(x_2)$ contains the substitution. By the induction hypothesis,

$$\vdash_E x_1 = x_2 \longrightarrow (\mathscr{B}(x_1) \leftrightarrow \mathscr{B}(x_2)),$$

where $\mathscr{B}(x_2)$ is defined just as $\mathscr{A}(x_2)$ was (only one free occurrence of x_1 is replaced). It is easily seen that

$$\vdash_E x_1 = x_2 \longrightarrow ((\mathscr{B}(x_1) \longrightarrow \mathscr{C}(x_1)) \leftrightarrow (\mathscr{B}(x_1) \longrightarrow \mathscr{C}(x_1))),$$

since the right-hand side is a tautology. Therefore, by substitution of provable equivalences,

$$\vdash_E x_1 = x_2 \longrightarrow ((\mathscr{B}(x_1) \longrightarrow \mathscr{C}(x_1)) \leftrightarrow (\mathscr{B}(x_2) \longrightarrow \mathscr{C}(x_1))),$$

i.e.,

$$\vdash_E x_1 = x_2 \longrightarrow (\mathscr{A}(x_1) \leftrightarrow \mathscr{A}(x_2)).$$

ii. It may be that $\mathscr{A}(x_2)$ is $\mathscr{B}(x_2) \longrightarrow \mathscr{C}(x_1)$. This is proved similarly way as the above case. By the inductive hypothesis,

$$\vdash_E x_1 = x_2 \longrightarrow (\mathscr{C}(x_1) \leftrightarrow \mathscr{C}(x_2)).$$

It is easily seen that

$$\vdash_E x_1 = x_2 \longrightarrow ((\mathscr{B}(x_1) \longrightarrow \mathscr{C}(x_1)) \leftrightarrow (\mathscr{B}(x_1) \longrightarrow \mathscr{C}(x_1))).$$

By substitution of provable equivalences,

$$\vdash_E x_1 = x_2 \longrightarrow ((\mathscr{B}(x_1) \longrightarrow \mathscr{C}(x_1)) \leftrightarrow (\mathscr{B}(x_1) \longrightarrow \mathscr{C}(x_2))),$$

i.e.,

$$\vdash_E x_1 = x_2 \longrightarrow (\mathscr{A}(x_1) \leftrightarrow \mathscr{A}(x_2)).$$

iii. The third is $\mathscr{B}(x_2) \longrightarrow \mathscr{C}$. That is, $\mathscr{C}$ does not contain an instance of x_1 (or x_2, for that matter). By the inductive hypothesis

$$\vdash_E x_1 = x_2 \longrightarrow (\mathscr{B}(x_1) \leftrightarrow \mathscr{B}(x_2)).$$

It is easily seen that

$$\vdash_E x_1 = x_2 \to ((\mathscr{B}(x_1) \to \mathscr{C}) \leftrightarrow (\mathscr{B}(x_1) \to \mathscr{C})).$$

By substitution of provable equivalences,

$$\vdash_E x_1 = x_2 \to ((\mathscr{B}(x_1) \to \mathscr{C}) \leftrightarrow (\mathscr{B}(x_2) \to \mathscr{C})),$$

i.e.,

$$\vdash_E x_1 = x_2 \to (\mathscr{A}(x_1) \leftrightarrow \mathscr{A}(x_2)).$$

iv. The third is $\mathscr{B} \to \mathscr{C}(x_2)$. The proof for this case should be obvious at this point.

(c) It may be that $\mathscr{A}(x_1)$ is of the form $(\forall x_i)\mathscr{B}(x_1)$, where x_i is not x_1, since x_1 occurs free in $\mathscr{A}(x_1)$. Likewise, x_i cannot be x_2, or else x_2 would not be free for x_1 in $\mathscr{A}(x_1)$. We want to prove that

$$\vdash_E x_1 = x_2 \to ((\forall x_i)\mathscr{B}(x_1) \leftrightarrow (\forall x_i)\mathscr{B}(x_2)).$$

By the induction hypothesis,

$$\vdash_E x_1 = x_2 \to (\mathscr{B}(x_1) \leftrightarrow \mathscr{B}(x_2)).$$

By Generalization,

$$\vdash_E (\forall x_i)(x_1 = x_2 \to (\mathscr{B}(x_1) \leftrightarrow \mathscr{B}(x_2))).$$

By Exercise 4 from Chapter 4 and MP,

$$\vdash_E (\forall x_i)(x_1 = x_2) \to (\forall x_i)((\mathscr{B}(x_1) \leftrightarrow \mathscr{B}(x_2))).$$

By the lemma used in the proof of Proposition 4.22,

$$\vdash_E (\forall x_i)((\mathscr{B}(x_1) \leftrightarrow \mathscr{B}(x_2))) \to ((\forall x_i)\mathscr{B}(x_1) \leftrightarrow (\forall x_i)\mathscr{B}(x_2)).$$

Recall that x_i cannot be x_1 or x_1. So, by Generalization and the Deduction Theorem,

$$\vdash_E x_1 = x_2 \to (\forall x_i)(x_1 = x_2).$$

By HS,

$$\vdash_E x_1 = x_2 \to ((\forall x_i)\mathscr{B}(x_1) \leftrightarrow (\forall x_i)\mathscr{B}(x_2)),$$

as desired.

Therefore, for any number of connectives and quantifiers in $\mathscr{A}(x_1)$,

$$x_1 = x_2 \to (\mathscr{A}(x_1) \leftrightarrow \mathscr{A}(x_2))$$

is a theorem of E, so, by definition of $\leftrightarrow$,

$$x_1 = x_2 \to (\mathscr{A}(x_1) \to \mathscr{A}(x_2))$$

is a theorem of E.

4. Let $y_1, \ldots, y_n, z_1, \ldots, z_n$ be elements in the domain of M. Suppose that
$$[y_1] = [z_1], \ldots, [y_n] = [z_n].$$
To show that $\bar{\bar{A}}_i^n$ is well-defined, we must show that
$$\bar{\bar{A}}_i^n([y_1], \ldots, [y_n]) \text{ if and only if } \bar{\bar{A}}_i^n([z_1], \ldots, [z_n]),$$
which, by definition of $\bar{\bar{A}}_i^n$, is equivalent to showing that
$$\bar{A}_i^n(y_1, \ldots, y_n) \text{ if and only if } \bar{A}_i^n(z_1, \ldots, z_n).$$
Since M is a model for S, by (E8), the axiom
$$A_1^2(t_1, u_1) \to (A_i^n(t_1, \ldots, t_n) \to A_i^n(u_1, \ldots, t_n))$$
is a theorem of S, so
$$\text{if } \bar{A}_1^2(y_1, z_1), \text{ then } A_i^n(y_1, \ldots, y_n) \text{ implies } A_i^n(z_1, \ldots, y_n).$$
In M^*, this is interpreted as
$$\text{if } y_1 = z_1, \text{ then } \bar{\bar{A}}_i^n([y_1], \ldots, [y_n]) \text{ implies } \bar{\bar{A}}_i^n([z_1], \ldots, [y_n]).$$
Similarly, we can obtain
$$\text{if } y_2 = z_2, \text{ then } \bar{\bar{A}}_i^n([z_1], [y_2], \ldots, [y_n]) \text{ implies } \bar{\bar{A}}_i^n([z_1], [z_2], \ldots, [y_n]),$$
$$\ldots,$$
$$\text{if } y_n = z_n, \text{ then } \bar{\bar{A}}_i^n([z_1], [z_2], \ldots, [y_n]) \text{ implies } \bar{\bar{A}}_i^n([z_1], [z_2], \ldots, [z_n]).$$
Since the hypothesis of all these statements are satisfied, using the transitive property of implication,
$$\bar{\bar{A}}_i^n([y_1], \ldots, [y_n]) \text{ implies } \bar{\bar{A}}_i^n([z_1], \ldots, [z_n]).$$
The other direction can be proved in the same way by using the fact that A_1^2 and equality are symmetric. Therefore,
$$\bar{\bar{A}}_i^n([y_1], \ldots, [y_n]) \text{ if and only if } \bar{\bar{A}}_i^n([z_1], \ldots, [z_n]).$$
as desired.

5. We may express this as
$$(\exists x_i)(\exists x_j)(\mathscr{A}(x_i) \wedge \mathscr{A}(x_j) \wedge (\sim (x_i = x_j)) \wedge (\forall x_k)(\mathscr{A}(x_k) \to (x_k = x_i \vee x_k = x_j))).$$

6. Let E be a first order system with equality. The proof is by induction on n, the number of connectives and quantifiers in $\mathscr{A}(t_1, \ldots, t_k, \ldots, t_n)$.

   (base case) It may be that $n = 0$, in which $\mathscr{A}$ is an atomic formula. Then (E9) provides the desired result.

   (inductive step) It may be that $n > 1$, in which case, there are three cases to verify.

(a) It may be that $\mathscr{A}(t_1, \ldots, t_k, \ldots, t_n)$ is of the form $\sim \mathscr{B}(t_1, \ldots, t_k, \ldots, t_n)$. By reversing the equality and applying the induction hypothesis,

$$\vdash_E u = t_k \to (\mathscr{B}(t_1, \ldots, u, \ldots, t_n) \to \mathscr{B}(t_1, \ldots, t_k, \ldots, t_n)).$$

The following *wf* is a tautology:

$$\vdash_E (\mathscr{B}(t_1, \ldots, u, \ldots, t_n) \to \mathscr{B}(t_1, \ldots, t_k, \ldots, t_n)) \to$$

$$((\sim \mathscr{B}(t_1, \ldots, t_k, \ldots, t_n)) \to (\sim \mathscr{B}(t_1, \ldots, u, \ldots, t_n))).$$

By Proposition 5.4(ii), $t_k = u \to u = t_k$. By HS twice,

$$t_k = u \to ((\sim \mathscr{B}(t_1, \ldots, t_k, \ldots, t_n)) \to (\sim \mathscr{B}(t_1, \ldots, u, \ldots, t_n))),$$

which is to say that

$$\vdash_E t_k = u \to (\mathscr{A}(t_1, \ldots, t_k, \ldots, t_n) \to \mathscr{A}(t_1, \ldots, u, \ldots, t_n)),$$

as desired.

(b) It may be that $\mathscr{A}(t_1, \ldots, t_k, \ldots, t_n)$ is an implication of the form

$$\mathscr{B}(b_1, \ldots, b_{m_1}) \to \mathscr{C}(c_1, \ldots, c_{m_2}),$$

where $b_1, \ldots, b_n$ and $c_1, \ldots, c_n$ combined contain all terms $t_1, \ldots, t_k, \ldots, t_n$. From here, there are two cases. Either

$$\mathscr{A}(t_1, \ldots, u, \ldots, t_n)$$

is of the form

$$\mathscr{B}(b_1, \ldots, u, \ldots, b_{m_1}) \to \mathscr{C}(c_1, \ldots, c_{m_2}),$$

where the substitution of u for t_k occurs in $\mathscr{B}$, or of the form

$$\mathscr{B}(c_1, \ldots, c_{m_2}) \to \mathscr{C}(b_1, \ldots, u, \ldots, b_{m_1}),$$

where the substitution of u for t_k occurs in $\mathscr{C}$. Consider the first case. By the induction hypothesis,

$$\vdash_E t_k = u \to (\mathscr{B}(b_1, \ldots, t_k, \ldots, b_{m_1}) \to \mathscr{B}(b_1, \ldots, u, \ldots, b_{m_1})),$$

and

$$\vdash_E u = t_k \to (\mathscr{B}(b_1, \ldots, u, \ldots, b_{m_1}) \to \mathscr{B}(b_1, \ldots, t_k, \ldots, b_{m_1})),$$

and since $t_k = u \to u = t_k$,

$$\vdash_E u = t_k \to (\mathscr{B}(b_1, \ldots, t_k, \ldots, b_{m_1}) \leftrightarrow \mathscr{B}(b_1, \ldots, u, \ldots, b_{m_1})).$$

The following *wf* is easily seen to be true:

$$\vdash_E u = t_k \to ((\mathscr{B}(b_1, \ldots, t_k, \ldots, b_{m_1}) \to \mathscr{C}(c_1, \ldots, c_{m_2})) \to$$

$$(\mathscr{B}(b_1, \ldots, t_k, \ldots, b_{m_1}) \to \mathscr{C}(c_1, \ldots, c_{m_2}))),$$

by the fact that the right-hand side is a tautology, (K1), and MP. It is easy to construct (but tedious to write out fully) the tautology that allows us to substitute $\mathscr{B}(b_1, \ldots, u, \ldots, b_{m_1})$ for the second instance of $\mathscr{B}(b_1, \ldots, t_k, \ldots, b_{m_1})$ in the *wf* above to obtain

$$\vdash_E u = t_k \to ((\mathscr{B}(b_1, \ldots, t_k, \ldots, b_{m_1}) \to \mathscr{C}(c_1, \ldots, c_{m_2})) \to$$

$$(\mathscr{B}(b_1, \ldots, u, \ldots, b_{m_1}) \to \mathscr{C}(c_1, \ldots, c_{m_2}))),$$

i.e.,

$$\vdash_E u = t_k \to (\mathscr{A}(t_1, \ldots, t_k, \ldots, t_n) \to \mathscr{A}(t_1, \ldots, u, \ldots, t_n)),$$

as desired. The case where the substitution of u for t_k occurs in $\mathscr{C}$ is proved in the same way.

(c) It may be that $\mathscr{A}(t_1, \ldots, t_k, \ldots, t_n)$ is of the form

$$(\forall x_i)\mathscr{B}(t_1, \ldots, t_k, \ldots, t_n).$$

We know that, by the induction hypothesis,

$$\vdash_E t_k = u \to (\mathscr{B}(t_1, \ldots, t_k, \ldots, t_n) \to \mathscr{B}(t_1, \ldots, u, \ldots, t_n)).$$

Note that x_i cannot be any variables appearing free in any of terms $t_1, \ldots, t_n$, or else variables in these terms would not be free in $\mathscr{A}$. Similarly, x_i cannot be u, or else u would not be free for any of the terms $t_1, \ldots, t_n$. Therefore, by Generalization and the Deduction Theorem,

$$\vdash_E \mathscr{B}(t_1, \ldots, t_k, \ldots, t_n) \leftrightarrow (\forall x_i)\mathscr{B}(t_1, \ldots, t_k, \ldots, t_n)$$

and

$$\vdash_E \mathscr{B}(t_1, \ldots, u, \ldots, t_n) \leftrightarrow (\forall x_i)\mathscr{B}(t_1, \ldots, u, \ldots, t_n).$$

By substituting these provable equivalences into the *wf* obtained from the induction hypothesis above (made possible by Proposition 4.22),

$$\vdash_E t_k = u \to ((\forall x_i)\mathscr{B}(t_1, \ldots, t_k, \ldots, t_n) \to (\forall x_i)\mathscr{B}(t_1, \ldots, u, \ldots, t_n)),$$

i.e.,

$$\vdash_E t_k = u \to (\mathscr{A}(t_1, \ldots, t_k, \ldots, t_n) \to \mathscr{A}(t_1, \ldots, u, \ldots, t_n)).$$

By completing the induction, we may conclude that,

$$\vdash_E ((t_k = u) \to (\mathscr{A}(t_1, \ldots, t_k, \ldots, t_n) \to \mathscr{A}(t_1, \ldots, u, \ldots, t_n))).$$

5.3 The theory of groups

Group theory is based on a set of axioms, and these axioms are expressed[3] in a language that we will denote by $\mathscr{L}_G$, which has the following alphabet:

- variables $x_1, x_2, \ldots$

[3]There are other languages which can be used, see the first exercise of this section.

- a single constant a_1, which is to be interpreted as the group identity
- two function symbols, f_1^1, which is to be interpreted as the inverse function, and f_1^2, which is to be interpreted as the group product
- one predicate symbol A_1^2, which is to be interpreted as =
- punctuation marks (,), and ,
- logical symbols $\forall, \sim, \mathscr{A}$

Now define $\mathscr{G}$ to be a first order system with equality whose additional proper axioms are the following.

- (G1) $f_1^2(f_1^2(x_1, x_2), x_3) = f_1^2(x_1, f_1^2(x_2, x_3))$
- (G2) $f_1^2(a_1, x_1) = x_1$
- (G3) $f_1^2(f_1^1(x_1), x_1) = a_1$

These axioms are to be interpreted respectively as the following.

- the group product is associative
- the constant a_1 is a left identity
- every element in the group has a left inverse

Note that there is no need to assert the existence of a_1, the left identity constant, and $f_1^1(x_1)$, left inverse for any x_1. This is because in any model of $\mathscr{G}$, there must exist interpretations of a_1 and f_1^1 which satisfy the properties given by the axioms. Similarly, there is no need to include an axiom for closure of the functions, as these will be interpreted, in some model, as closed functions over the domain of the model.

Any group is a model of $\mathscr{G}$, provided that the zero element, the inverse function, and the product function of the group interpret their respective analogues a_1, f_1^1, and f_1^2 in $\mathscr{G}$. However, there are models of $\mathscr{G}$ which are not groups.

Consider, as an example, the interpretation I of $\mathscr{G}$ in which the following are defined.

- The domain is the set of integers
- $\bar{a}_1$ is 0
- $\bar{f}_1^1(x)$ is $-x$
- $\bar{f}_1^2(x, y)$ is $x + y$
- $\bar{A}_1^2$, or the interpretation of =, is congruence mod m, where m is some fixed positive integer

In the last item, recall that = is shorthand for A_1^2. However, as we see here, = is not interpreted here by = in the interpretation, or equality of integers. In other words, our interpretation cannot be a normal model of $\mathscr{G}$. However, this interpretation is a model of $\mathscr{G}$. The logical axioms (K1) - (K6) are logically valid, and hence true in any interpretation. The axioms for equality (E7), (E8), and (E9) are true, and this is verified just as in Example 5.5. The group axioms remain to be verified.

- (G1) is interpreted as $(x + y) + z \equiv x + (y + z) \pmod{m}$.
- (G2) is interpreted as $0 + x \equiv x \pmod{m}$.
- (G3) is interpreted as $-x + x \equiv 0 \pmod{m}$.

In the interpretation, all of these are true statements, hence the interpretation is a model of G. However, the interpretation is not a group, since it involves congruence instead of equality. However, just as in the proof of Proposition 5.6, we can construct a normal model from the interpretation where the domain consists of the equivalence, or congruence, classes brought about by congruence mod m. Note that this is not some contrived example, for this is the construction of the group $\mathbb{Z}_m$.

Solutions to exercises

7. In a language with no individual constants, (G2) and (G3) may be replaced by

$$(\exists x_1)(\forall x_2)(f_1^2(x_1, x_2) = x_2 \wedge f_1^2(f_1^1(x_2), x_2) = x_1),$$

where the x_1 above is to be interpreted as the group identity.

In a language with no function letters, let $A_1^3(x_1, x_2, x_3)$ be interpreted as $x_1 x_2 = x_3$ so that

$$(\forall x_1)(\forall x_2)(\exists x_3)A_1^3(x_1, x_2, x_3),$$

in other words, a group product always exists for two elements of the group.

(G1) may be replaced by

$$(A_1^3(x_1, x_2, x_4) \wedge A_1^3(x_4, x_3, x_5) \wedge A_1^3(x_2, x_3, x_6) \wedge A_1^3(x_1, x_6, x_7)) \rightarrow x_5 = x_7,$$

where x_4 is meant to be $f_1^2(x_1, x_2)$ in (G1), x_5 is meant to $f_1^2(f_1^2(x_1, x_2), x_3)$, etc.

(G2) may be replaced by

$$(\forall x_1)A_1^3(a_1, x_1, x_1),$$

(G3) may be replaced by

$$(\forall x_1)(\exists x_2)A_1^3(x_1, x_2, a_1).$$

8. A first order system of semigroup theory may be described by simply having (G1) as a sole axiom.

9. Because the axioms (G1), (G2), and (G3) do not include the constant symbols, the interpretations of constants may (and must) be included without altering the theorems which may be proved in the formal system.

10. A language for ring theory is the same as the language for group theory, with the addition of f_2^2 to describe multiplication. The axioms for ring theory are given as follows. The first four describe addition.

   (a) $f_1^2(f_1^2(x_1, x_2), x_3) = f_1^2(x_1, f_1^2(x_2, x_3))$
   (b) $f^2(x_1, x_2) = f^2(x_2, x_1)$
   (c) $f_1^2(a_1, x_1) = x_1$

(d) $f_1^2(f_1^1(x_1), x_1) = a_1$

The next four describe multiplication.

(a) $f_2^2(f_2^2(x_1, x_2), x_3) = f_2^2(x_1, f_2^2(x_2, x_3))$

(b) $f_2^2(a_1, x_1) = x_1$

The next two describe the distributive properties.

(a) $f_2^2(x_1, f_1^2(x_2, x_3)) = f_1^2(f_2^2(x_1, x_2), f_2^2(x_1, x_3))$

(b) $f_2^2(f_1^2(x_1, x_2), x_3) = f_1^2(f_2^2(x_2, x_1), f_2^2(x_3, x_1))$

Constructing an interpretation of this system which is not a ring may be done in the same way as the examples shown in the textbook. That is, by constructing an interpretation in which equality is congruence modulo n, where n is some positive integer. So let the domain of interpretation be the integers. Interpret the symbols in the usual way (f_1^2 corresponds to addition, f_1^1 is the additive inverse, etc.), except let A_1^2 or $=$ in the system be interpreted by congruence modulo n. It is easy to see that all the axioms are satisfied, but the model is not a ring.

However, just as in the previous examples, a ring may easily be constructed by considering equivalence classes mod n.

11. There are two parts to this question.

(a) To construct a first order system whose models are infinite groups, include as an additional axiom schema

$$\underbrace{x_1 + x_1 + \cdots + x_1}_{k \text{ times}} = a_1 \rightarrow x_1 = a_1$$

for all k. That is, include infinitely many axioms of the above instance for each positive integer k. This will guarantee that only 0, the interpretation of a_1, in the model of the group, will have an order. Therefore, each model must have infinitely many elements, except for the trivial group, the group with a singular element, which is a group. To exclude this group, we also include the following axiom.

$$(\exists x_1)(\exists x_2) \sim (x_1 = x_2).$$

This axiom states that there exist at least two distinct elements. Finally, note that the models of this system are certainly not all infinite groups, since there exists groups with infinitely many elements but with some elements having finite order. However, the models of this system will all have infinite order, since the included axioms restrict the possibility of the group having finite order.

(b) The second part of the exercise asks whether it is "possible for a first order system to have as its normal models all *finite groups*?" This may be interpreted as asking to construct a system whose normal models are finite groups, or, alternatively, according to the other interpretation, the set of all possible finite groups. Regarding the first interpretation, it is simple to construct a system whose normal models are only finite groups. Include the additional axiom

$$x_1 = a_1,$$

so that the only normal model up to isomorphism is the trivial group. Regarding the second interpretation, the answer is no, there exists no system whose normal models are the set of all finite groups. Suppose that such a system exists. Then it must have the axioms of the above scheme

$$\underbrace{x_1 + x_1 + \cdots + x_1}_{k \text{ times}} = a_1 \to x_1 = a_1$$

as theorems for all k. By Corollary 4.47, the set of all such *wf* should have a model. By nature of the axiom scheme and the same reasoning as in part (a), the set of all *wf*s must have a normal model which is an infinite group.

12. Recall that a field with characteristic k is a field in which the smallest number that the fields additive identity may be added to itself to reach the multiplicative identity is k. If any sum of the additive identity with itself is never equal to the multiplicative identity, the field has characteristic zero.

    Just as in exercise 10, consider an extension of the system of field theory whose axioms are given by the scheme

$$\underbrace{x_1 + x_1 + \cdots + x_1}_{k \text{ times}} = a_1 \to x_1 = a_1$$

    for all k, where a_1 is interpreted as the unique additive identity, or zero, in the field. The normal models of this system must necessarily be all fields of characteristic zero. So the *wf* $\mathscr{A}$ described in the exercise must be a theorem of this system, hence its proof uses finitely many of these axioms. The axioms of the scheme differ only in their value for k, so let $n+1$ denote the lowest number in the axioms used in the proof of $\mathscr{A}$. By construction, n will necessarily be a positive integer[4] such that $\mathscr{A}$ will be true in all fields of characteristic p, with $p > n$, since systems which have these fields as models will have these axioms in the proof as axioms in the system.

13. Construct an extension of $\mathscr{F}$ called $\mathscr{F}'$ which includes $\mathscr{A}$ as an axiom along with

$$\underbrace{x_1 + x_1 + \cdots + x_1}_{k \text{ times}} = a_1 \to x_1 = a_1$$

    for all k, where a_1 is interpreted as the additive identity in any normal model of the system. Consider a system with any finite subset of the axioms of $\mathscr{F}'$. It contains finitely many instances of the above axiom schema. Denote the highest k occurring in these axioms by n. It must be that there exists a field of characteristic p, with $p > n$, in which $\mathscr{A}$ is true, by assumption. Since, in a field, the minimum

[4] It is well-known that the characteristic of a field must be a prime number if not zero. In fact, we could have specified this in the axiom scheme.

number of times that any element can be added to itself until it reaches 0 will be the characteristic of the field, the field of characteristic p will be a model for the system with the chosen axioms.

Therefore, by Corollary 4.47, since every finite subset of the axioms of $\mathscr{F}$ has a model, $\mathscr{F}$ has a model, and since $\mathscr{A}$ is a theorem of $\mathscr{F}$, it is true in the model. This model may not be a field itself, but a field may be constructed from the model by an argument similar to the one in Proposition 5.6.

5.4 First order arithmetic

The notation we use will be slightly different from that in the textbook. We will use $\mathbb{N}$ to denote the natural numbers as an interpretation of the system we will construct.

Let $\mathscr{L}_N$ refer to the language with the function letters f_1^1, f_1^2, f_2^2 to be interpreted as the successor, sum, product, the constant a_1 to be interpreted as 0, and the predicate symbol A_1^2 for equality. We will use = to stand for A_1^2 just as we did in Chapter 5.2

We will denote by $\mathcal{N}$ the extension of $K_{\mathscr{L}_N}$ obtained by including the axioms of equality introduced in Section 5.2 and the following axioms.

- (N1) $(\forall x_1)(\sim f_1^1(x_1) = a_1)$
- (N2) $(\forall x_1)(\forall x_2)(f_1^1(x_1) = f_1^1(x_2 \rightarrow x_1 = x_2)$
- (N3) $(\forall x_1)f_1^2(x_1, a_1) = x_1$
- (N4) $(\forall x_1)(\forall x_2)f_1^2(x_1, f_1^1(x_2)) = f_1^1(f_1^2(x_1, x_2))$
- (N5) $(\forall x_1)f_2^2(x_1, a_1) = a_1$
- (N6) $(\forall x_1)(\forall x_2)f_2^2(x_1, f_1^1(x_2)) = f_1^2(f_2^2(x_1, x_2), x_1)$
- (N7) $\mathscr{A}(a_1) \rightarrow ((\forall x_1)(\mathscr{A}(x_1) \rightarrow \mathscr{A}(f_1^1(x_2))) \rightarrow (\forall x_1)\mathscr{A}(x_1))$, for each *wf* $\mathscr{A}(x_1)$ of $\mathscr{L}_N$ in which x_1 occurs free

These are to be interpreted by the following statements.

- There exists no number whose successor is zero.
- If two numbers have the same successor, those two numbers are equal.
- The sum of any number and zero is the number.
- The successor of the sum of two numbers is the sum of the successor of the first number and the second numbers.
- The product of any number and zero is zero.
- The product of a number and the successor of another number is the sum of the product of the numbers and the first number.
- If a statement holds for zero and if the fact that a statement holds for one number implies that the statement holds for the next one, then that statement is true for all numbers.

It is worth comparing these axioms to the well-known Peano postulates.

- Zero is a number.
- Every number has a successor which is a natural number.
- The successor of no number is zero.
- If two numbers have the same successor, then those two numbers are the same.
- If any set of numbers contains zero and has the property that if any number is in the set, then the successor of that number is also in the set, then that set contains all numbers.

The essential difference between this set of axioms and the ones for $\mathcal{N}$ is that these axioms rely on some notion of sets. In particular, the final axiom is a predicate over elements in the set of sets of numbers, and this set it is uncountable. On the other hand, (N7) is a predicate over *wf*s of $\mathscr{L}_N$, a set which is countable.

A basic question to ask about $\mathcal{N}$ is whether it is complete. The next chapter will outline a proof that essentially states that if $\mathcal{N}$ is consistent, then it is not complete (and if it is inconsistent, then it is trivially complete), in which case the system may be extended to two consistent systems by separately adding an unprovable *wf* or its negation as axioms, and these two systems will have distinct models[5]. Therefore, $\mathcal{N}$ has more than one model.

Solutions to exercises

14.

5.5 Formal set theory

Let $\mathscr{L}_{ZF}$ be a language with A_1^2 and A_2^2. For any terms u, v, we will write $u = v$ to mean $A_1^2(u, v)$ and $u \in v$ to mean $A_2^2()$. *There are no individual constants and function letters.* Let ZF be an extension of $K_{\mathscr{L}_{ZF}}$ with the axioms of equality[6] introduced in Section 5.2 and the following axioms.

$$(ZF1) \qquad x_1 = x_2 \leftrightarrow (\forall x_3)(x_3 \in x_1 \leftrightarrow x_3 \in x_2)$$

This is the Axiom of Extensionality. It says that two sets are equal if they have the same elements.

$$(ZF2) \qquad (\exists x_1)(\forall x_2) \sim (x_2 \in x_1)$$

This is the Null Set Axiom. It says that there is a set which contains no elements. It can be proved that this set is unique. We will denote it by $\varnothing$.

$$(ZF3) \qquad (\forall x_1)(\forall x_2)(\exists x_3)(\forall x_4)(x_4 \in x_3 \leftrightarrow (x_4 = x_1 \vee x_4 = x_2))$$

[5]The propositions used to justify this sentence should be obvious at this point.
[6]There are no instances of (E8).

This is the Axiom of Pairing. Given any two sets, there is a set whose members are those two sets.

$$(ZF4) \qquad (\forall x_1)(\exists x_2)(\forall x_3)(x_3 \in x_2 \leftrightarrow (\exists x_4)(x_4 \in x_1 \wedge x_3 \in x_4))$$

This is the Axiom of Unions. Given any set (of sets) S, there exists a set whose members are all members of members of S. For example, if $S = \{\{1, 2\}, \{3\}\}$, then there exists a set whose members are $\{1, 2, 3\}$.

$$(ZF5) \qquad (\forall x_1)(\exists x_2)(\forall x_3)(x_3 \in x_2 \leftrightarrow x_2 \subseteq x_1)$$

In the above, the symbol $\subseteq$ is defined such that, for arbitrary variables x_1, x_2 and x_3, $x_1 \subseteq x_2$ stands for $(\forall x_3)(x_3 \in x_1 \to x_3 \in x_2)$. This is the Power Set Axiom. For any set, the power set (the set containing all subsets of a specified set), of that set exists.

$$(ZF6) \quad (\forall x_1)(\exists_1 x_2)\mathscr{A}(x_1, x_2) \to (\forall x_3)(\exists x_4)(\forall x_5)(x_5 \in x_4 \leftrightarrow (\exists x_6)(x_6 \in x_3 \wedge \mathscr{A}(x_6, x_5)))$$

This is the Axiom Scheme of Replacement. Its form is an implication with the hypothesis that $\mathscr{A}$ is a function, since a particular x_2 is *uniquely* associated with any x_1 (note the $\exists_1$ quantifier).

$$(ZF7) \qquad (\forall x_1)(\varnothing \in x_1 \wedge (\forall x_2)(x_2 \in x_1 \to x_2 \cup \{x_2\} \in x_1))$$

This is the Axiom of Infinity. It asserts that there exists a set with a countably infinite number of elements, where, for sets x_1 and x_2, $x_1 \cup x_2$ denotes their union and $\{x_1\}$ denotes the set containing only x_1, which exists because x_1 may be paired with itself to yield $\{x_1, x_1\}$ by the Axiom of Pairing. In particular, the set is

$$\{\{\}, \{\{\}\}, \{\{\}, \{\{\}\}\}, \{\{\}, \{\{\}\}, \{\{\}, \{\{\}\}\}\}, \ldots\},$$

i.e.,

$$\{\varnothing, \{\varnothing\}, \{\varnothing, \{\varnothing\}\}, \{\varnothing, \{\varnothing\}, \{\varnothing, \{\varnothing\}\}\}\}.$$

$$(ZF8) \qquad (\forall x_1)(\sim x_1 = \varnothing \to (\exists x_2)(x_2 \in x_1 \wedge \sim (\exists x_3)(x_3 \in x_2 \wedge x_3 \in x_1)))$$

This is the Axiom of Foundation. It states that every set has an element which is disjoint, i.e. the element shares no elements.

The above axioms specify the modern foundations of set theory. There are two additional axioms that are worth mentioning.

(AC) For any non-empty set (of sets) x, there is a set which contains precisely one element in common with each member with each member of x.

This is the Axiom of Choice. It is equivalent to *Zorn's Lemma*, if each chain in a partially ordered set has an upper bound, then the set has a maximal element, and *The Well-Ordering Principle*, every set can be well-ordered, i.e., there exists an order on any set such that any non-empty subset has a least element according to the order.

(CH) Each subset of real numbers is either countable[7] or has the same cardinality as the set of real numbers.

[7] We use the definition that finite sets are countable.

This is the Continuum Hypothesis. It is equivalent to asserting the nonexistence of a set with cardinality greater than that of the natural numbers but less than that of the real numbers.

Both (AC) and (CH) are optional axioms in ZC. That is, if the system ZC is assumed to be consistent, then the four extensions which individually include (AC), (CH) and their negations are also consistent. Of course, this raises the question of the consistency of ZC, and this is the subject of the following chapter.

Solutions to exercises

15.

5.6 Consistency and models

Chapter 6

The Gödel Incompleteness Theorem

Chapter 7

Computability, unsolvability, undecidability

Appendix A

Additional propositions

This chapter contains proofs of exercises left to the reader in the textbook or otherwise useful propositions.

Proposition A.1. The set of *wf*s of L is countable.

Proposition A.2. Let $\mathscr{A}$ be a *wf* of some first-order language.

1. The *wf* $(\forall x_i)(\forall x_j)\mathscr{A} \leftrightarrow (\forall x_i)(\forall x_j)\mathscr{A}$ is a theorem of $K_{\mathscr{L}}$.

2. The *wf* $(\exists x_i)(\exists x_j)\mathscr{A} \leftrightarrow (\exists x_i)(\exists x_j)\mathscr{A}$ is a theorem of $K_{\mathscr{L}}$.

3. The *wf* $(\forall x_i)(\exists x_j)\mathscr{A} \leftrightarrow (\exists x_i)(\forall x_j)\mathscr{A}$ is not a theorem of $K_{\mathscr{L}}$.

Proof. For 1 and 2, we prove that the *wf*s are theorems of K using the Deduction Theorem. For 3, in light of the Adequacy Theorem for K (Proposition 4.39), we prove that the *wf* is not a theorem of K by finding an interpretation in which the *wf* is not true.

1. Observe the following deduction.

1	$(\forall x_i)(\forall x_j)\mathscr{A}$	assumption
2	$(\forall x_j)\mathscr{A}$	1, Remark 4.1(a)
3	$\mathscr{A}$	2, Remark 4.1(a)
4	$(\forall x_i)\mathscr{A}$	3, Generalization
5	$(\forall x_j)(\forall x_i)\mathscr{A}$	4, Generalization

   By the Deduction Theorem, and since x_i and x_j do not occur free in $(\forall x_i)(\forall x_j)\mathscr{A}$, $(\forall x_i)(\forall x_j)\mathscr{A} \rightarrow (\forall x_j)(\forall x_i)\mathscr{A}$ must be a theorem of K. The other direction is proved in the same way with the positions of the variables flipped. Therefore, by Proposition 4.15, the *wf* $(\forall x_i)(\forall x_j)\mathscr{A} \leftrightarrow (\forall x_i)(\forall x_j)\mathscr{A}$ is a theorem of K.

2. Note that for any *wf* $\mathscr{B}$, we may deduce $\mathscr{B}$ from $\sim\sim \mathscr{B}$ or vice versa by MP and

the fact that $\sim\sim \mathscr{B} \leftrightarrow \mathscr{B}$ is a tautology. Call this property $\star$.

1	$\sim\sim (\forall x_i) \sim\sim (\forall x_j) \sim \mathscr{A}$	assumption
2	$(\forall x_i) \sim\sim (\forall x_j) \sim \mathscr{A}$	$\star$
3	$\sim\sim (\forall x_j) \sim \mathscr{A}$	Remark 4.1(a)
4	$(\forall x_j) \sim \mathscr{A}$	$\star$
5	$\sim \mathscr{A}$	Remark 4.1(a)
6	$(\forall x_i) \sim \mathscr{A}$	5, Generalization
7	$\sim\sim (\forall x_i) \sim \mathscr{A}$	$\star$
8	$(\forall x_j) \sim\sim (\forall x_i) \sim \mathscr{A}$	7, Generalization
9	$\sim\sim (\forall x_j) \sim\sim (\forall x_i) \sim \mathscr{A}$	$\star$

By the Deduction Theorem, and since x_i and x_j do not occur free in the *wf* on line 1,

$$(\sim\sim (\forall x_i) \sim\sim (\forall x_j) \sim \mathscr{A}) \to (\sim\sim (\forall x_j) \sim\sim (\forall x_i) \sim \mathscr{A})$$

must be a theorem of K. By an obvious application of (K3) and MP,

$$(\sim (\forall x_j) \sim\sim (\forall x_i) \sim \mathscr{A}) \to (\sim (\forall x_i) \sim\sim (\forall x_j) \sim \mathscr{A})$$

must be a theorem of K as well. By the definition of $\exists$,

$$(\exists x_j)(\exists x_i)\mathscr{A}) \to (\exists x_i)(\exists x_j)\mathscr{A})$$

must be a theorem of K. The other direction is proved in the same way with the positions of the variables flipped. Therefore, by Proposition 4.15, the *wf*

$$(\exists x_i)(\exists x_j)\mathscr{A} \leftrightarrow (\exists x_i)(\exists x_j)\mathscr{A}$$

is a theorem of K.

3.

$\square$

Proposition A.3. Let $\mathscr{L}$ be a first order language. The set of *wf*s of $\mathscr{L}$ is countable.

Appendix B

Additional exercises

B.1 Informal statement calculus

B.2 Formal statement calculus

B.3 Informal predicate calculus

B.4 Formal predicate calculus

1. Consider the *wf* $(\forall x_1)A_1^1(x_1) \to (\forall x_2)(\exists x_3)A_1^2(x_2, x_3)$. Which *wf*s in prenex form are provably equivalent? For the ones which are provably equivalent, provide a proof. For the ones which are not provably equivalent, provide an interpretation in which the *wf* is false.

   (a) $(\forall x_1)(\forall x_2)(\exists x_3)(A_1^1(x_1) \to A_1^2(x_2, x_3))$

   (b) $(\forall x_1)(\forall x_3)(\exists x_2)(A_1^1(x_1) \to A_1^2(x_2, x_3))$

   (c) $(\forall x_2)(\forall x_1)(\exists x_3)(A_1^1(x_1) \to A_1^2(x_2, x_3))$

   (d) $(\forall x_2)(\forall x_3)(\exists x_1)(A_1^1(x_1) \to A_1^2(x_2, x_3))$

   (e) $(\forall x_3)(\forall x_1)(\exists x_2)(A_1^1(x_1) \to A_1^2(x_2, x_3))$

   (f) $(\forall x_3)(\forall x_2)(\exists x_1)(A_1^1(x_1) \to A_1^2(x_2, x_3))$