

# Chapter 3

## Propositional Logic: Deductive Systems

The concept of deducing theorems from a set of axioms and rules of inference is very old and is familiar to every high-school student who has studied Euclidean geometry. Modern mathematics is expressed in a style of reasoning that is not far removed from the reasoning used by Greek mathematicians. This style can be characterized as ‘formalized informal reasoning’, meaning that while the proofs are expressed in natural language rather than in a formal system, there are conventions among mathematicians as to the forms of reasoning that are allowed. The deductive systems studied in this chapter were developed in an attempt to formalize mathematical reasoning.

We present two deductive systems for propositional logic. The second one  $\mathcal{H}$  will be familiar because it is a formalization of step-by-step proofs in mathematics: It contains a set of three axioms and one rule of inference; proofs are constructed as a sequence of formulas, each of which is either an axiom (or a formula that has been previously proved) or a derivation of a formula from previous formulas in the sequence using the rule of inference. The system  $\mathcal{G}$  will be less familiar because it has one axiom and many rules of inference, but we present it first because it is almost trivial to prove the soundness and completeness of  $\mathcal{G}$  from its relationship with semantic tableaux. The proof of the soundness and completeness of  $\mathcal{H}$  is then relatively easy to show by using  $\mathcal{G}$ . The chapter concludes with three short sections: the definition of an important property called *consistency*, a generalization to infinite sets of formulas, and a survey of other deductive systems for propositional logic.

### 3.1 Why Deductive Proofs?

Let  $U = \{A_1, \dots, A_n\}$ . Theorem 2.50 showed that  $U \models A$  if and only if  $\models A_1 \wedge \dots \wedge A_n \rightarrow A$ . Therefore, if  $U$  is a set of axioms, we can use the completeness of the method of semantic tableaux to determine if  $A$  follows from  $U$  (see Sect. 2.5.4 for precise definitions). Why would we want to go through the trouble of searching for a mathematical proof when we can easily compute if a formula is valid?

There are several problems with a purely semantical approach:

- The set of axioms may be infinite. For example, the axiom of induction in arithmetic is really an infinite set of axioms, one for each property to be proved. For semantic tableaux in propositional logic, the only formulas that appear in the tableaux are subformulas of the formula being checked or their negations, and there are only a finite number of such formulas.
- Very few logics have decision procedures like propositional logic.
- A decision procedure may not give insight into the relationship between the axioms and the theorem. For example, in proofs of theorems about prime numbers, we would want to know exactly where primality is used (Velleman, 2006, Sect. 3.7). This understanding can also help us propose other formulas that might be theorems.
- A decision procedure produces a ‘yes/no’ answer, so it is difficult to recognize intermediate results (lemmas). Clearly, the millions of mathematical theorems in existence could not have been inferred directly from axioms.

**Definition 3.1** A *deductive system* is a set of formulas called *axioms* and a set of *rules of inference*. A *proof* in a deductive system is a sequence of formulas  $S = \{A_1, \dots, A_n\}$  such that each formula  $A_i$  is either an axiom or it can be inferred from previous formulas of the sequence  $A_{j_1}, \dots, A_{j_k}$ , where  $j_1 < \dots < j_k < i$ , using a rule of inference. For  $A_n$ , the last formula in the sequence, we say that  $A_n$  is a *theorem*, the sequence  $S$  is a *proof* of  $A_n$ , and  $A_n$  is *provable*, denoted  $\vdash A_n$ . If  $\vdash A$ , then  $A$  may be used like an axiom in a subsequent proof. ■

The deductive approach can overcome the problems described above:

- There may be an infinite number of axioms, but only a finite number will appear in any proof.
- Although a proof is not a decision procedure, it can be mechanically *checked*; that is, given a sequence of formulas, a syntax-based algorithm can easily check whether the sequence is a proof as defined above.
- The proof of a formula clearly shows which axioms, theorems and rules are used and for what purposes.
- Once a theorem has been proved, it can be used in proofs like an axiom.

Deductive proofs are not generated by decision procedures because the formulas that appear in a proof are not limited to subformulas of the theorem and because there is no algorithm telling us how to generate the next formula in the sequence forming a proof. Nevertheless, algorithms and heuristics can be used to build software systems called *automatic theorem provers* which search for proofs. In Chap. 4, we will study a deductive system that has been successfully used in automatic theorem provers. Another promising approach is to use a *proof assistant* which performs administrative tasks such as proof checking, bookkeeping and cataloging previously proved theorems, but a person guides the search by suggesting lemmas that are likely to lead to a proof.

$\alpha$	$\alpha_1$	$\alpha_2$	$\beta$	$\beta_1$	$\beta_2$
$\neg\neg A$	$A$				
$\neg(A_1 \wedge A_2)$	$\neg A_1$	$\neg A_2$	$B_1 \wedge B_2$	$B_1$	$B_2$
$A_1 \vee A_2$	$A_1$	$A_2$	$\neg(B_1 \vee B_2)$	$\neg B_1$	$\neg B_2$
$A_1 \rightarrow A_2$	$\neg A_1$	$A_2$	$\neg(B_1 \rightarrow B_2)$	$B_1$	$\neg B_2$
$A_1 \uparrow A_2$	$\neg A_1$	$\neg A_2$	$\neg(B_1 \uparrow B_2)$	$B_1$	$B_2$
$\neg(A_1 \downarrow A_2)$	$A_1$	$A_2$	$B_1 \downarrow B_2$	$\neg B_1$	$\neg B_2$
$\neg(A_1 \leftrightarrow A_2)$	$\neg(A_1 \rightarrow A_2)$	$\neg(A_2 \rightarrow A_1)$	$B_1 \leftrightarrow B_2$	$B_1 \rightarrow B_2$	$B_2 \rightarrow B_1$
$A_1 \oplus A_2$	$\neg(A_1 \rightarrow A_2)$	$\neg(A_2 \rightarrow A_1)$	$\neg(B_1 \oplus B_2)$	$B_1 \rightarrow B_2$	$B_2 \rightarrow B_1$

**Fig. 3.1** Classification of  $\alpha$ - and  $\beta$ -formulas

## 3.2 Gentzen System $\mathcal{G}$

The first deductive system that we study is based on a system proposed by Gerhard Gentzen in the 1930s. The system itself will seem unfamiliar because it has one type of axiom and many rules of inference, unlike familiar mathematical theories which have multiple axioms and only a few rules of inference. Furthermore, deductions in the system can be naturally represented as trees rather in the linear format characteristic of mathematical proofs. However, it is this property that makes it easy to relate Gentzen systems to semantic tableaux.

**Definition 3.2** (Gentzen system  $\mathcal{G}$ ) An *axiom* of  $\mathcal{G}$  is a set of literals  $U$  containing a complementary pair. *Rule of inference* are used to infer a set of formulas  $U$  from one or two other sets of formulas  $U_1$  and  $U_2$ ; there are two types of rules, defined with reference to Fig. 3.1:

- Let  $\{\alpha_1, \alpha_2\} \subseteq U_1$  and let  $U'_1 = U_1 - \{\alpha_1, \alpha_2\}$ . Then  $U = U'_1 \cup \{\alpha\}$  can be inferred.
- Let  $\{\beta_1\} \subseteq U_1$ ,  $\{\beta_2\} \subseteq U_2$  and let  $U'_1 = U_1 - \{\beta_1\}$ ,  $U'_2 = U_2 - \{\beta_2\}$ . Then  $U = U'_1 \cup U'_2 \cup \{\beta\}$  can be inferred.

The set or sets of formulas  $U_1, U_2$  are the *premises* and set of formulas  $U$  that is inferred is the *conclusion*. A set of formulas  $U$  that is an axiom or a conclusion is said to be *proved*, denoted  $\vdash U$ . The following notation is used for rules of inference:

$$\frac{\vdash U'_1 \cup \{\alpha_1, \alpha_2\}}{\vdash U'_1 \cup \{\alpha\}} \quad \frac{\vdash U'_1 \cup \{\beta_1\} \quad \vdash U'_2 \cup \{\beta_2\}}{\vdash U'_1 \cup U'_2 \cup \{\beta\}}.$$

Braces can be omitted with the understanding that a sequence of formulas is to be interpreted as a set (with no duplicates). ■

*Example 3.3* The following set of formulas is an axiom because it contains the complementary pair  $\{r, \neg r\}$ :

$$\vdash p \wedge q, q, r, \neg r, q \vee \neg r.$$

The disjunction rule for  $A_1 = q$ ,  $A_2 = \neg r$  can be used to deduce:

$$\frac{\vdash p \wedge q, q, r, \neg r, q \vee \neg r}{\vdash p \wedge q, r, q \vee \neg r, q \vee \neg r}.$$

Removing the duplicate formula  $q \vee \neg r$  gives:

$$\frac{\vdash p \wedge q, q, r, \neg r, q \vee \neg r}{\vdash p \wedge q, r, q \vee \neg r}.$$

Note that the premises  $\{q, \neg r\}$  are no longer elements of the conclusion. ■

A proof can be written as a sequence of sets of formulas, which are numbered for convenient reference. On the right of each line is its *justification*: either the set of formulas is an axiom, or it is the conclusion of a rule of inference applied to a set or sets of formulas earlier in the sequence. A rule of inference is identified by the rule used for the  $\alpha$ - or  $\beta$ -formula on the principal operator of the conclusion and by the number or numbers of the lines containing the premises.

*Example 3.4* Prove  $\vdash (p \vee q) \rightarrow (q \vee p)$  in  $\mathcal{L}$ .

*Proof*

- |   |                         |
|---|-------------------------|
| 1. $\vdash \neg p, q, p$                      | Axiom                   |
| 2. $\vdash \neg q, q, p$                      | Axiom                   |
| 3. $\vdash \neg(p \vee q), q, p$              | $\beta \vee, 1, 2$      |
| 4. $\vdash \neg(p \vee q), (q \vee p)$        | $\alpha \vee, 3$        |
| 5. $\vdash (p \vee q) \rightarrow (q \vee p)$ | $\alpha \rightarrow, 4$ |
- 

*Example 3.5* Prove  $\vdash p \vee (q \wedge r) \rightarrow (p \vee q) \wedge (p \vee r)$  in  $\mathcal{L}$ .

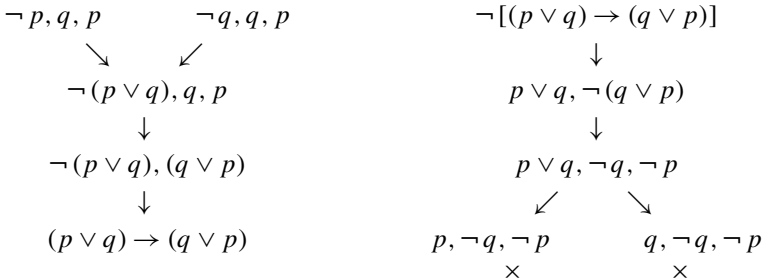
*Proof*

- |   |                          |
|---|--------------------------|
| 1. $\vdash \neg p, p, q$  | Axiom                    |
| 2. $\vdash \neg p, (p \vee q)$  | $\alpha \vee, 1$         |
| 3. $\vdash \neg p, p, r$  | Axiom                    |
| 4. $\vdash \neg p, (p \vee r)$  | $\alpha \vee, 3$         |
| 5. $\vdash \neg p, (p \vee q) \wedge (p \vee r)$                          | $\beta \wedge, 2, 4$     |
|   |                          |
| 6. $\vdash \neg q, \neg r, p, q$  | Axiom                    |
| 7. $\vdash \neg q, \neg r, (p \vee q)$                                    | $\alpha \vee, 6$         |
| 8. $\vdash \neg q, \neg r, p, r$  | Axiom                    |
| 9. $\vdash \neg q, \neg r, (p \vee r)$                                    | $\alpha \vee, 8$         |
| 10. $\vdash \neg q, \neg r, (p \vee q) \wedge (p \vee r)$                 | $\beta \wedge, 7, 9$     |
| 11. $\vdash \neg(q \wedge r), (p \vee q) \wedge (p \vee r)$               | $\alpha \wedge, 10$      |
|   |                          |
| 12. $\vdash \neg(p \vee (q \wedge r)), (p \vee q) \wedge (p \vee r)$      | $\beta \vee, 5, 11$      |
| 13. $\vdash p \vee (q \wedge r) \rightarrow (p \vee q) \wedge (p \vee r)$ | $\alpha \rightarrow, 12$ |
-

### 3.2.1 The Relationship Between $\mathcal{G}$ and Semantic Tableaux

It might seem that we have been rather clever to arrange all the inferences in these proofs so that everything comes out exactly right in the end. In fact, no cleverness was required. Let us rearrange the Gentzen proof into a tree format rather than a linear sequence of sets of formulas. Let the axioms be the leaves of the tree, and let the inference rules define the interior nodes. The root at the bottom will be labeled with the formula that is proved.

The proof from Example 3.4 is displayed in tree form on the left below:



If this looks familiar, it should. The semantic tableau on the right results from turning the derivation in  $\mathcal{G}$  upside down and replacing each formula in the labels on the nodes by its complement (Definition 2.57).

A set of formulas labeling a node in a semantic tableau is an *implicit conjunction*, that is, all the formulas in the set must evaluate to true for the set to be true. By taking complements, a set of formulas labeling a node in a derivation in  $\mathcal{G}$  is an *implicit disjunction*.

An axiom in  $\mathcal{G}$  is valid: Since it contains a complementary pair of literals, as a disjunction it is:

$$\dots \vee p \vee \dots \vee \neg p \vee \dots,$$

which is valid.

Consider a rule applied to obtain an  $\alpha$ -formula, for example,  $A_1 \vee A_2$ ; when the rule is written using disjunctions it becomes:

$$\frac{\vdash \bigvee U'_1 \vee A_1 \vee A_2}{\vdash \bigvee U'_1 \vee (A_1 \vee A_2)},$$

and this is a valid inference in propositional logic that follows immediately from associativity.

Similarly, when a rule is applied to obtain a  $\beta$ -formula, we have:

$$\frac{\vdash \bigvee U'_1 \vee B_1 \qquad \vdash \bigvee U'_2 \vee B_2}{\vdash \bigvee U'_1 \vee \bigvee U'_2 \vee (B_1 \wedge B_2)},$$

which follows by the distribution of disjunction over conjunction. This inference simply says that if we can prove both  $B_1$  and  $B_2$  then we can prove  $B_1 \wedge B_2$ .

The relationship between semantic tableaux and Gentzen systems is formalized in the following theorem.

**Theorem 3.6** *Let  $A$  be a formula in propositional logic. Then  $\vdash A$  in  $\mathcal{G}$  if and only if there is a closed semantic tableau for  $\neg A$ .*

This follows immediately from a more general theorem on sets of formulas.

**Theorem 3.7** *Let  $U$  be a set of formulas and let  $\bar{U}$  be the set of complements of formulas in  $U$ . Then  $\vdash U$  in  $\mathcal{G}$  if and only if there is a closed semantic tableau for  $\bar{U}$ .*

*Proof* Let  $\mathcal{T}$  be a closed semantic tableau for  $\bar{U}$ . We prove  $\vdash U$  by induction on  $h$ , the height of  $\mathcal{T}$ . The other direction is left as an exercise.

If  $h = 0$ , then  $\mathcal{T}$  consists of a single node labeled by  $\bar{U}$ . By assumption,  $\mathcal{T}$  is closed, so it contains a complementary pair of literals  $\{p, \neg p\}$ , that is,  $\bar{U} = \bar{U}' \cup \{p, \neg p\}$ . Obviously,  $U = U' \cup \{\neg p, p\}$  is an axiom in  $\mathcal{G}$ , hence  $\vdash U$ .

If  $h > 0$ , then some tableau rule was used on an  $\alpha$ - or  $\beta$ -formula at the root of  $\mathcal{T}$  on a formula  $\bar{\phi} \in \bar{U}$ , that is,  $\bar{U} = \bar{U}' \cup \{\bar{\phi}\}$ . The proof proceeds by cases, where you must be careful to distinguish between applications of the tableau rules and applications of the Gentzen rules of the same name.

**Case 1:**  $\bar{\phi}$  is an  $\alpha$ -formula (such as  $\neg(A_1 \vee A_2)$ ). The tableau rule created a child node labeled by the set of formulas  $\bar{U}' \cup \{\neg A_1, \neg A_2\}$ . By assumption, the subtree rooted at this node is a closed tableau, so by the inductive hypothesis,  $\vdash U' \cup \{A_1, A_2\}$ . Using the appropriate rule of inference from  $\mathcal{G}$ , we obtain  $\vdash U' \cup \{A_1 \vee A_2\}$ , that is,  $\vdash U' \cup \{\phi\}$ , which is  $\vdash U$ .

**Case 2:**  $\bar{\phi}$  is a  $\beta$ -formula (such as  $\neg(B_1 \wedge B_2)$ ). The tableau rule created two child nodes labeled by the sets of formulas  $\bar{U}' \cup \{\neg B_1\}$  and  $\bar{U}' \cup \{\neg B_2\}$ . By assumption, the subtrees rooted at this node are closed, so by the inductive hypothesis  $\vdash U' \cup \{B_1\}$  and  $\vdash U' \cup \{B_2\}$ . Using the appropriate rule of inference from  $\mathcal{G}$ , we obtain  $\vdash U' \cup \{B_1 \wedge B_2\}$ , that is,  $\vdash U' \cup \{\phi\}$ , which is  $\vdash U$ . ■

**Theorem 3.8** (Soundness and completeness of  $\mathcal{G}$ )

$\models A$  if and only if  $\vdash A$  in  $\mathcal{G}$ .

*Proof*  $A$  is valid iff  $\neg A$  is unsatisfiable iff there is a closed semantic tableau for  $\neg A$  iff there is a proof of  $A$  in  $\mathcal{G}$ . ■

The proof is very simple because we did all the hard work in the proof of the soundness and completeness of tableaux.

The Gentzen system  $\mathcal{G}$  described in this section is not very useful; other versions (surveyed in Sect. 3.9) are more convenient for proving theorems and are closer to Gentzen's original formulation. We introduced  $\mathcal{G}$  as a theoretical stepping stone to Hilbert systems which we now describe.

### 3.3 Hilbert System $\mathcal{H}$

In Gentzen systems there is one axiom and many rules of inference, while in a Hilbert system there are several axioms but only one rule of inference. In this section, we define the deductive system  $\mathcal{H}$  and use it to prove many theorems. Actually, only one theorem (Theorem 3.10) will be proved directly from the axioms and the rule of inference; practical use of the system depends on the use of derived rules, especially the deduction rule.

**Notation:** Capital letters  $A, B, C, \dots$  represent arbitrary formulas in propositional logic. For example, the notation  $\vdash A \rightarrow A$  means: for *any* formula  $A$  of propositional logic, the formula  $A \rightarrow A$  can be proved.

**Definition 3.9** (Deductive system  $\mathcal{H}$ ) The *axioms* of  $\mathcal{H}$  are:

**Axiom 1**  $\vdash (A \rightarrow (B \rightarrow A)),$

**Axiom 2**  $\vdash (A \rightarrow (B \rightarrow C)) \rightarrow ((A \rightarrow B) \rightarrow (A \rightarrow C)),$

**Axiom 3**  $\vdash (\neg B \rightarrow \neg A) \rightarrow (A \rightarrow B).$

The *rule of inference* is **modus ponens** (MP for short):

$$\frac{\vdash A \quad \vdash A \rightarrow B}{\vdash B}.$$

In words: the formula  $B$  can be inferred from  $A$  and  $A \rightarrow B$ .

The terminology used for  $\mathcal{G}$ —*premises, conclusion, theorem, proved*— carries over to  $\mathcal{H}$ , as does the symbol  $\vdash$  meaning that a formula is proved. ■

**Theorem 3.10**  $\vdash A \rightarrow A.$

*Proof*

1.  $\vdash (A \rightarrow ((A \rightarrow A) \rightarrow A)) \rightarrow ((A \rightarrow (A \rightarrow A)) \rightarrow (A \rightarrow A))$  Axiom 2
2.  $\vdash A \rightarrow ((A \rightarrow A) \rightarrow A)$  Axiom 1
3.  $\vdash (A \rightarrow (A \rightarrow A)) \rightarrow (A \rightarrow A)$  MP 1, 2
4.  $\vdash A \rightarrow (A \rightarrow A)$  Axiom 1
5.  $\vdash A \rightarrow A$  MP 3, 4

■

When an axiom is given as the justification, identify which formulas are substituted for the formulas  $A, B, C$  in the definition of the axioms above.

#### 3.3.1 Axiom Schemes and Theorem Schemes \*

As we noted above, a capital letter can be replaced by any formula of propositional logic, so, strictly speaking,  $\vdash A \rightarrow (B \rightarrow A)$  is not an axiom, and similarly,  $\vdash A \rightarrow A$

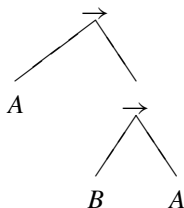
is not a theorem. A more precise terminology would be to say that  $\vdash A \rightarrow (B \rightarrow A)$  is an *axiom scheme* that is a shorthand for an infinite number of axioms obtained by replacing the ‘variables’  $A$  and  $B$  with actual formulas, for example:

$$\overbrace{((p \vee \neg q) \leftrightarrow r)}^A \rightarrow ( \overbrace{\neg(q \wedge \neg r)}^B \rightarrow \overbrace{((p \vee \neg q) \leftrightarrow r)}^A ).$$

Similarly,  $\vdash A \rightarrow A$  is a *theorem scheme* that is a shorthand for an infinite number of theorems that can be proved in  $\mathcal{H}$ , including, for example:

$$\vdash ((p \vee \neg q) \leftrightarrow r) \rightarrow ((p \vee \neg q) \leftrightarrow r).$$

We will not retain this precision in our presentation because it will always clear if a given formula is an instance of a particular axiom scheme or theorem scheme. For example, a formula  $\phi$  is an instance of Axiom 1 if it is of the form:



where there are subtrees for the formulas represented by  $A$  and  $B$ . There is a simple and efficient algorithm that checks if  $\phi$  is of this form and if the two subtrees  $A$  are identical.

### 3.3.2 The Deduction Rule

The proof of Theorem 3.10 is rather complicated for such a trivial formula. In order to formalize the powerful methods of inference used in mathematics, we introduce new rules of inference called *derived rules*. The most important derived rule is the *deduction rule*. Suppose that you want to prove  $A \rightarrow B$ . Assume that  $A$  has already been proved and use it in the proof of  $B$ . This is not a proof of  $B$  unless  $A$  is an axiom or theorem that has been previously proved, in which case it can be used directly in the proof. However, we claim that the proof can be mechanically transformed into a proof of  $A \rightarrow B$ .

*Example 3.11* The deduction rule is used frequently in mathematics. Suppose that you want to prove that *the sum of any two odd integer numbers is even*, expressed formally as:

$$\text{odd}(x) \wedge \text{odd}(y) \rightarrow \text{even}(x + y),$$

for every  $x$  and  $y$ . To prove this formula, let us *assume* the formula  $\text{odd}(x) \wedge \text{odd}(y)$  as if it were an additional axiom. We have available all the theorems we have already



deduced about odd numbers, in particular, the theorem that any odd number can be expressed as  $2k + 1$ . Computing:

$$x + y = 2k_1 + 1 + 2k_2 + 1 = 2(k_1 + k_2 + 1),$$

we obtain that  $x + y$  is a multiple of 2, that is, *even*( $x + y$ ). The theorem now follows from the deduction rule which *discharges* the assumption. ■

To express the deduction rule, we extend the definition of *proof*.

**Definition 3.12** Let  $U$  be a set of formulas and  $A$  a formula. The notation  $U \vdash A$  means that the formulas in  $U$  are *assumptions* in the proof of  $A$ . A *proof* is a sequence of lines  $U_i \vdash \phi_i$ , such that for each  $i$ ,  $U_i \subseteq U$ , and  $\phi_i$  is an axiom, a previously proved theorem, a member of  $U_i$  or can be derived by *MP* from previous lines  $U_{i'} \vdash \phi_{i'}$ ,  $U_{i''} \vdash \phi_{i''}$ , where  $i', i'' < i$ . ■

**Rule 3.13** (Deduction rule)

$$\frac{U \cup \{A\} \vdash B}{U \vdash A \rightarrow B}.$$

We must show that this derived rule is *sound*, that is, that the use of the derived rule does not increase the set of provable theorems in  $\mathcal{H}$ . This is done by showing how to transform any proof using the rule into one that does not use the rule. Therefore, in principle, any proof that uses the derived rule could be transformed to one that uses only the three axioms and *MP*.

**Theorem 3.14** (Deduction theorem) *The deduction rule is a sound derived rule.*

*Proof* We show by induction on the length  $n$  of the proof of  $U \cup \{A\} \vdash B$  how to obtain a proof of  $U \vdash A \rightarrow B$  that does not use the deduction rule.

For  $n = 1$ ,  $B$  is proved in one step, so  $B$  must be either an element of  $U \cup \{A\}$  or an axiom of  $\mathcal{H}$  or a previously proved theorem:

- If  $B$  is  $A$ , then  $\vdash A \rightarrow A$  by Theorem 3.10, so certainly  $U \vdash A \rightarrow A$ .
- Otherwise ( $B$  is an axiom or a previously proved theorem), here is a proof of  $U \cup \{A\} \vdash B$  that does not use the deduction rule or the assumption  $A$ :
 

1.	$U \vdash B$	Axiom or theorem
2.	$U \vdash B \rightarrow (A \rightarrow B)$	Axiom 1
3.	$U \vdash A \rightarrow B$	MP 1, 2

If  $n > 1$ , the last step in the proof of  $U \cup \{A\} \vdash B$  is either a one-step inference of  $B$  or an inference of  $B$  using *MP*. In the first case, the result holds by the proof for  $n = 1$ . Otherwise, *MP* was used, so there is a formula  $C$  and lines  $i, j < n$  in the proof such that line  $i$  in the proof is  $U \cup \{A\} \vdash C$  and line  $j$  is  $U \cup \{A\} \vdash C \rightarrow B$ . By the inductive hypothesis,  $U \vdash A \rightarrow C$  and  $U \vdash A \rightarrow (C \rightarrow B)$ . A proof of  $U \vdash A \rightarrow B$  is given by:

- |    |  |                      |
|----|--|----------------------|
| 1. | $U \vdash A \rightarrow C$   | Inductive hypothesis |
| 2. | $U \vdash A \rightarrow (C \rightarrow B)$   | Inductive hypothesis |
| 3. | $U \vdash (A \rightarrow (C \rightarrow B)) \rightarrow ((A \rightarrow C) \rightarrow (A \rightarrow B))$ | Axiom 2              |
| 4. | $U \vdash (A \rightarrow C) \rightarrow (A \rightarrow B)$   | MP 2, 3              |
| 5. | $U \vdash A \rightarrow B$   | MP 1, 4              |

■

### 3.4 Derived Rules in $\mathcal{H}$

The general form of a derived rule will be one of:

$$\frac{U \vdash \phi_1}{U \vdash \phi}, \quad \frac{U \vdash \phi_1 \quad U \vdash \phi_2}{U \vdash \phi}.$$

The first form is justified by proving the formula  $U \vdash \phi_1 \rightarrow \phi$  and the second by  $U \vdash \phi_1 \rightarrow (\phi_2 \rightarrow \phi)$ ; the formula  $U \vdash \phi$  that is the conclusion of the rule follows immediately by one or two applications of *MP*. For example, from Axiom 3 we immediately have the following rule:

**Rule 3.15** (Contrapositive rule)

$$\frac{U \vdash \neg B \rightarrow \neg A}{U \vdash A \rightarrow B}.$$

The contrapositive is used extensively in mathematics. We showed the completeness of the method of semantic tableaux by proving: *If a tableau is open, the formula is satisfiable*, which is the contrapositive of the theorem that we wanted to prove: *If a formula is unsatisfiable (not satisfiable), the tableau is closed (not open)*.

**Theorem 3.16**  $\vdash (A \rightarrow B) \rightarrow [(B \rightarrow C) \rightarrow (A \rightarrow C)]$ .

*Proof*

- |    |  |             |
|----|--|-------------|
| 1. | $\{A \rightarrow B, B \rightarrow C, A\} \vdash A$                                       | Assumption  |
| 2. | $\{A \rightarrow B, B \rightarrow C, A\} \vdash A \rightarrow B$                         | Assumption  |
| 3. | $\{A \rightarrow B, B \rightarrow C, A\} \vdash B$                                       | MP 1, 2     |
| 4. | $\{A \rightarrow B, B \rightarrow C, A\} \vdash B \rightarrow C$                         | Assumption  |
| 5. | $\{A \rightarrow B, B \rightarrow C, A\} \vdash C$                                       | MP 3, 4     |
| 6. | $\{A \rightarrow B, B \rightarrow C\} \vdash A \rightarrow C$                            | Deduction 5 |
| 7. | $\{A \rightarrow B\} \vdash [(B \rightarrow C) \rightarrow (A \rightarrow C)]$           | Deduction 6 |
| 8. | $\vdash (A \rightarrow B) \rightarrow [(B \rightarrow C) \rightarrow (A \rightarrow C)]$ | Deduction 7 |

■

**Rule 3.17** (Transitivity rule)

$$\frac{U \vdash A \rightarrow B \quad U \vdash B \rightarrow C}{U \vdash A \rightarrow C}.$$

The transitivity rule justifies the step-by-step development of a mathematical theorem  $\vdash A \rightarrow C$  through a series of *lemmas*. The antecedent  $A$  of the theorem is used to prove a lemma  $\vdash A \rightarrow B_1$  whose consequent is used to prove the next lemma  $\vdash B_1 \rightarrow B_2$  and so on until the consequent of the theorem appears as  $\vdash B_n \rightarrow C$ . Repeated use of the transitivity rule enables us to deduce  $\vdash A \rightarrow C$ .

**Theorem 3.18**  $\vdash [A \rightarrow (B \rightarrow C)] \rightarrow [B \rightarrow (A \rightarrow C)]$ .*Proof*

- |    |  |             |
|----|--|-------------|
| 1. | $\{A \rightarrow (B \rightarrow C), B, A\} \vdash A$                                     | Assumption  |
| 2. | $\{A \rightarrow (B \rightarrow C), B, A\} \vdash A \rightarrow (B \rightarrow C)$       | Assumption  |
| 3. | $\{A \rightarrow (B \rightarrow C), B, A\} \vdash B \rightarrow C$                       | MP 1, 2     |
| 4. | $\{A \rightarrow (B \rightarrow C), B, A\} \vdash B$                                     | Assumption  |
| 5. | $\{A \rightarrow (B \rightarrow C), B, A\} \vdash C$                                     | MP 3, 4     |
| 6. | $\{A \rightarrow (B \rightarrow C), B\} \vdash A \rightarrow C$                          | Deduction 5 |
| 7. | $\{A \rightarrow (B \rightarrow C)\} \vdash B \rightarrow (A \rightarrow C)$             | Deduction 6 |
| 8. | $\vdash [A \rightarrow (B \rightarrow C)] \rightarrow [B \rightarrow (A \rightarrow C)]$ | Deduction 7 |

■

**Rule 3.19** (Exchange of antecedent rule)

$$\frac{U \vdash A \rightarrow (B \rightarrow C)}{U \vdash B \rightarrow (A \rightarrow C)}.$$

Exchanging the antecedent simply means that it doesn't matter in which order we use the lemmas necessary in a proof.

**Theorem 3.20**  $\vdash \neg A \rightarrow (A \rightarrow B)$ .*Proof*

- |    |   |             |
|----|---|-------------|
| 1. | $\{\neg A\} \vdash \neg A \rightarrow (\neg B \rightarrow \neg A)$            | Axiom 1     |
| 2. | $\{\neg A\} \vdash \neg A$  | Assumption  |
| 3. | $\{\neg A\} \vdash \neg B \rightarrow \neg A$                                 | MP 1, 2     |
| 4. | $\{\neg A\} \vdash (\neg B \rightarrow \neg A) \rightarrow (A \rightarrow B)$ | Axiom 3     |
| 5. | $\{\neg A\} \vdash A \rightarrow B$   | MP 3, 4     |
| 6. | $\vdash \neg A \rightarrow (A \rightarrow B)$                                 | Deduction 5 |

■

**Theorem 3.21**  $\vdash A \rightarrow (\neg A \rightarrow B)$ .*Proof*

- |    |   |              |
|----|---|--------------|
| 1. | $\vdash \neg A \rightarrow (A \rightarrow B)$ | Theorem 3.20 |
| 2. | $\vdash A \rightarrow (\neg A \rightarrow B)$ | Exchange 1   |

■

These two theorems are of major theoretical importance. They say that if you can prove some formula  $A$  and its negation  $\neg A$ , then you can prove *any* formula  $B$ ! If you can prove any formula then there are no unprovable formulas so the concept of proof becomes meaningless.

**Theorem 3.22**  $\vdash \neg\neg A \rightarrow A$ .

*Proof*

- |   |                  |
|---|------------------|
| 1. $\{\neg\neg A\} \vdash \neg\neg A \rightarrow (\neg\neg\neg\neg A \rightarrow \neg\neg A)$ | Axiom 1          |
| 2. $\{\neg\neg A\} \vdash \neg\neg A$   | Assumption       |
| 3. $\{\neg\neg A\} \vdash \neg\neg\neg\neg A \rightarrow \neg\neg A$                          | MP 1, 2          |
| 4. $\{\neg\neg A\} \vdash \neg A \rightarrow \neg\neg\neg A$                                  | Contrapositive 3 |
| 5. $\{\neg\neg A\} \vdash \neg\neg A \rightarrow A$   | Contrapositive 4 |
| 6. $\{\neg\neg A\} \vdash A$  | MP 2, 5          |
| 7. $\vdash \neg\neg A \rightarrow A$  | Deduction 6      |

■

**Theorem 3.23**  $\vdash A \rightarrow \neg\neg A$ .

*Proof*

- |   |                  |
|---|------------------|
| 1. $\vdash \neg\neg\neg A \rightarrow \neg A$ | Theorem 3.22     |
| 2. $\vdash A \rightarrow \neg\neg A$          | Contrapositive 1 |

■

**Rule 3.24** (Double negation rule)

$$\frac{U \vdash \neg\neg A}{U \vdash A}, \quad \frac{U \vdash A}{U \vdash \neg\neg A}.$$

Double negation is a very intuitive rule. We expect that ‘it is raining’ and ‘it is not true that it is not raining’ will have the same truth value, and that the second formula can be simplified to the first. Nevertheless, some logicians reject the rule because it is not constructive. Suppose that we can prove for some number  $n$ , ‘it is not true that  $n$  is prime’ which is the same as ‘it is not true that  $n$  is not composite’. This double negation could be reduced by the rule to ‘ $n$  is composite’, but we have not actually demonstrated any factors of  $n$ .

**Theorem 3.25**  $\vdash (A \rightarrow B) \rightarrow (\neg B \rightarrow \neg A)$ .

*Proof*

- |   |                   |
|---|-------------------|
| 1. $\{A \rightarrow B\} \vdash A \rightarrow B$                       | Assumption        |
| 2. $\{A \rightarrow B\} \vdash \neg\neg A \rightarrow A$              | Theorem 3.22      |
| 3. $\{A \rightarrow B\} \vdash \neg\neg A \rightarrow B$              | Transitivity 2, 1 |
| 4. $\{A \rightarrow B\} \vdash B \rightarrow \neg\neg B$              | Theorem 3.23      |
| 5. $\{A \rightarrow B\} \vdash \neg\neg A \rightarrow \neg\neg B$     | Transitivity 3, 4 |
| 6. $\{A \rightarrow B\} \vdash \neg B \rightarrow \neg A$             | Contrapositive 5  |
| 7. $\vdash (A \rightarrow B) \rightarrow (\neg B \rightarrow \neg A)$ | Deduction 6       |

■

**Rule 3.26** (Contrapositive rule)

$$\frac{U \vdash A \rightarrow B}{U \vdash \neg B \rightarrow \neg A}.$$

This is the other direction of the contrapositive rule shown earlier.

Recall from Sect. 2.3.3 the definition of the logical constants *true* as an abbreviation for  $p \vee \neg p$  and *false* as an abbreviation for  $p \wedge \neg p$ . These can be expressed using implication and negation alone as  $p \rightarrow p$  and  $\neg(p \rightarrow p)$ .

**Theorem 3.27**

$$\begin{aligned} &\vdash \textit{true}, \\ &\vdash \neg \textit{false}. \end{aligned}$$

*Proof*  $\vdash \textit{true}$  is an instance of Theorem 3.10.  $\vdash \neg \textit{false}$ , which is  $\vdash \neg \neg(p \rightarrow p)$ , follows by double negation. ■

**Theorem 3.28**  $\vdash (\neg A \rightarrow \textit{false}) \rightarrow A$ .

*Proof*

- |   |                   |
|---|-------------------|
| 1. $\{\neg A \rightarrow \textit{false}\} \vdash \neg A \rightarrow \textit{false}$           | Assumption        |
| 2. $\{\neg A \rightarrow \textit{false}\} \vdash \neg \textit{false} \rightarrow \neg \neg A$ | Contrapositive    |
| 3. $\{\neg A \rightarrow \textit{false}\} \vdash \neg \textit{false}$                         | Theorem 3.27      |
| 4. $\{\neg A \rightarrow \textit{false}\} \vdash \neg \neg A$                                 | MP 2, 3           |
| 5. $\{\neg A \rightarrow \textit{false}\} \vdash A$   | Double negation 4 |
| 6. $\vdash (\neg A \rightarrow \textit{false}) \rightarrow A$                                 | Deduction 5       |
- 

**Rule 3.29** (Reductio ad absurdum)

$$\frac{U \vdash \neg A \rightarrow \textit{false}}{U \vdash A}.$$

Reductio ad absurdum is a very useful rule in mathematics: Assume the negation of what you wish to prove and show that it leads to a contradiction. This rule is also controversial because proving that  $\neg A$  leads to a contradiction provides no reason that directly justifies  $A$ .

Here is an example of the use of this rule:

**Theorem 3.30**  $\vdash (A \rightarrow \neg A) \rightarrow \neg A$ .

*Proof*

- |   |                        |
|---|------------------------|
| 1. $\{A \rightarrow \neg A, \neg \neg A\} \vdash \neg \neg A$                                     | Assumption             |
| 2. $\{A \rightarrow \neg A, \neg \neg A\} \vdash A$   | Double negation 1      |
| 3. $\{A \rightarrow \neg A, \neg \neg A\} \vdash A \rightarrow \neg A$                            | Assumption             |
| 4. $\{A \rightarrow \neg A, \neg \neg A\} \vdash \neg A$  | MP 2, 3                |
| 5. $\{A \rightarrow \neg A, \neg \neg A\} \vdash A \rightarrow (\neg A \rightarrow \text{false})$ | Theorem 3.21           |
| 6. $\{A \rightarrow \neg A, \neg \neg A\} \vdash \neg A \rightarrow \text{false}$                 | MP 2, 5                |
| 7. $\{A \rightarrow \neg A, \neg \neg A\} \vdash \text{false}$                                    | MP 4, 6                |
| 8. $\{A \rightarrow \neg A\} \vdash \neg \neg A \rightarrow \text{false}$                         | Deduction 7            |
| 9. $\{A \rightarrow \neg A\} \vdash \neg A$   | Reductio ad absurdum 8 |
| 10. $\vdash (A \rightarrow \neg A) \rightarrow \neg A$  | Deduction 9            |

■

We leave the proof of the following theorem as an exercise.

**Theorem 3.31**  $\vdash (\neg A \rightarrow A) \rightarrow A$ .

These two theorems may seem strange, but they can be understood on the semantic level. For the implication of Theorem 3.31 to be false, the antecedent  $\neg A \rightarrow A$  must be true and the consequent  $A$  false. But if  $A$  is false, then so is  $\neg A \rightarrow A \equiv A \vee A$ , so the formula is true.

### 3.5 Theorems for Other Operators

So far we have worked with only negation and implication as operators. These two operators are adequate for defining all others (Sect. 2.4), so we can use these definitions to prove theorems using other operators. Recall that  $A \wedge B$  is defined as  $\neg(A \rightarrow \neg B)$ , and  $A \vee B$  is defined as  $\neg A \rightarrow B$ .

**Theorem 3.32**  $\vdash A \rightarrow (B \rightarrow (A \wedge B))$ .

*Proof*

- |     |   |                        |
|-----|---|------------------------|
| 1.  | $\{A, B\} \vdash (A \rightarrow \neg B) \rightarrow (A \rightarrow \neg B)$ | Theorem 3.10           |
| 2.  | $\{A, B\} \vdash A \rightarrow ((A \rightarrow \neg B) \rightarrow \neg B)$ | Exchange 1             |
| 3.  | $\{A, B\} \vdash A$   | Assumption             |
| 4.  | $\{A, B\} \vdash (A \rightarrow \neg B) \rightarrow \neg B$                 | MP 2, 3                |
| 5.  | $\{A, B\} \vdash \neg \neg B \rightarrow \neg (A \rightarrow \neg B)$       | Contrapositive 4       |
| 6.  | $\{A, B\} \vdash B$   | Assumption             |
| 7.  | $\{A, B\} \vdash \neg \neg B$   | Double negation 6      |
| 8.  | $\{A, B\} \vdash \neg (A \rightarrow \neg B)$                               | MP 5, 7                |
| 9.  | $\{A\} \vdash B \rightarrow \neg (A \rightarrow \neg B)$                    | Deduction 8            |
| 10. | $\vdash A \rightarrow (B \rightarrow \neg (A \rightarrow \neg B))$          | Deduction 9            |
| 11. | $\vdash A \rightarrow (B \rightarrow (A \wedge B))$                         | Definition of $\wedge$ |

■

**Theorem 3.33** (Commutativity)  $\vdash A \vee B \leftrightarrow B \vee A$ .

*Proof*

- |    |  |                   |
|----|--|-------------------|
| 1. | $\{\neg A \rightarrow B, \neg B\} \vdash \neg A \rightarrow B$           | Assumption        |
| 2. | $\{\neg A \rightarrow B, \neg B\} \vdash \neg B \rightarrow \neg \neg A$ | Contrapositive 1  |
| 3. | $\{\neg A \rightarrow B, \neg B\} \vdash \neg B$                         | Assumption        |
| 4. | $\{\neg A \rightarrow B, \neg B\} \vdash \neg \neg A$                    | MP 2, 3           |
| 5. | $\{\neg A \rightarrow B, \neg B\} \vdash A$                              | Double negation 4 |
| 6. | $\{\neg A \rightarrow B\} \vdash \neg B \rightarrow A$                   | Deduction 5       |
| 7. | $\vdash (\neg A \rightarrow B) \rightarrow (\neg B \rightarrow A)$       | Deduction 6       |
| 8. | $\vdash A \vee B \rightarrow B \vee A$                                   | Def. of $\vee$    |

The other direction is similar.

■

The proofs of the following theorems are left as exercises.

**Theorem 3.34** (Weakening)

- $$\begin{aligned} &\vdash A \rightarrow A \vee B, \\ &\vdash B \rightarrow A \vee B, \\ &\vdash (A \rightarrow B) \rightarrow ((C \vee A) \rightarrow (C \vee B)). \end{aligned}$$

**Theorem 3.35** (Associativity)

$$\vdash A \vee (B \vee C) \leftrightarrow (A \vee B) \vee C.$$

**Theorem 3.36** (Distributivity)

- $$\begin{aligned} &\vdash A \vee (B \wedge C) \leftrightarrow (A \vee B) \wedge (A \vee C), \\ &\vdash A \wedge (B \vee C) \leftrightarrow (A \wedge B) \vee (A \wedge C). \end{aligned}$$

### 3.6 Soundness and Completeness of $\mathcal{H}$

We now prove the soundness and completeness of the Hilbert system  $\mathcal{H}$ . As usual, soundness is easy to prove. Proving completeness will not be too difficult because we already know that the Gentzen system  $\mathcal{G}$  is complete so it is sufficient to show how to transform any proof in  $\mathcal{G}$  into a proof in  $\mathcal{H}$ .

**Theorem 3.37** *The Hilbert system  $\mathcal{H}$  is sound: If  $\vdash A$  then  $\models A$ .*

*Proof* The proof is by structural induction. First we show that the axioms are valid, and then we show that *MP* preserves validity. Here are closed semantic tableaux for the negations of Axioms 1 and 3:

$$\begin{array}{c}
 \neg[A \rightarrow (B \rightarrow A)] \\
 \downarrow \\
 A, \neg(B \rightarrow A) \\
 \downarrow \\
 A, B, \neg A \\
 \times
 \end{array}
 \qquad
 \begin{array}{c}
 \neg[(\neg B \rightarrow \neg A) \rightarrow (A \rightarrow B)] \\
 \downarrow \\
 \neg B \rightarrow \neg A, \neg(A \rightarrow B) \\
 \downarrow \\
 \neg B \rightarrow \neg A, A, \neg B \\
 \swarrow \quad \searrow \\
 \neg\neg B, A, \neg B \qquad \neg A, A, \neg B \\
 \downarrow \qquad \qquad \times \\
 B, A, \neg B \\
 \times
 \end{array}$$

The construction of a tableau for the negation of Axiom 2 is left as an exercise.

Suppose that *MP* were not sound. There would be a set of formulas  $\{A, A \rightarrow B, B\}$  such that  $A$  and  $A \rightarrow B$  are valid, but  $B$  is not valid. Since  $B$  is not valid, there is an interpretation  $\mathcal{I}$  such that  $v_{\mathcal{I}}(B) = F$ . Since  $A$  and  $A \rightarrow B$  are valid, for any interpretation, in particular for  $\mathcal{I}$ ,  $v_{\mathcal{I}}(A) = v_{\mathcal{I}}(A \rightarrow B) = T$ . By definition of  $v_{\mathcal{I}}$  for implication,  $v_{\mathcal{I}}(B) = T$ , contradicting  $v_{\mathcal{I}}(B) = F$ . ■

There is no circularity in the final sentence of the proof: We are not using the syntactical proof rule *MP*, but, rather, the semantic definition of truth value in the presence of the implication operator.

**Theorem 3.38** *The Hilbert system  $\mathcal{H}$  is complete: If  $\models A$  then  $\vdash A$ .*

By the completeness of the Gentzen system  $\mathcal{G}$  (Theorem 3.8), if  $\models A$ , then  $\vdash A$  in  $\mathcal{G}$ . The proof of the theorem showed how to construct the proof of  $A$  by first constructing a semantic tableau for  $\neg A$ ; the tableau is guaranteed to close since  $A$  is valid. The completeness of  $\mathcal{H}$  is proved by showing how to transform a proof in  $\mathcal{G}$  into a proof in  $\mathcal{H}$ . Note that all three steps can be carried out algorithmically: Given an arbitrary valid formula in propositional logic, a computer can generate its proof.



We need a more general result because a proof in  $\mathcal{G}$  is a sequence of *sets* of formulas, while a proof in  $\mathcal{H}$  is a sequence of formulas.

**Theorem 3.39** *If  $\vdash U$  in  $\mathcal{G}$ , then  $\vdash \bigvee U$  in  $\mathcal{H}$ .*

The difficulty arises from the clash of the data structures used:  $U$  is a set while  $\bigvee U$  is a single formula. To see why this is a problem, consider the base case of the induction. The set  $\{\neg p, p\}$  is an axiom in  $\mathcal{G}$  and we immediately have  $\vdash \neg p \vee p$  in  $\mathcal{H}$  since this is simply  $\vdash p \rightarrow p$ . But if the axiom in  $\mathcal{G}$  is  $\{q, \neg p, r, p, s\}$ , we can't immediately conclude that  $\vdash q \vee \neg p \vee r \vee p \vee s$  in  $\mathcal{H}$ .

**Lemma 3.40** *If  $U' \subseteq U$  and  $\vdash \bigvee U'$  in  $\mathcal{H}$  then  $\vdash \bigvee U$  in  $\mathcal{H}$ .*

*Proof* The proof is by induction using weakening, commutativity and associativity of disjunction (Theorems 3.34–3.35). We give the outline here and leave it as an exercise to fill in the details.

Suppose we have a proof of  $\bigvee U'$ . By repeated application of Theorem 3.34, we can transform this into a proof of  $\bigvee U''$ , where  $U''$  is a permutation of the elements of  $U$ . By repeated applications of commutativity and associativity, we can move the elements of  $U''$  to their proper places. ■

*Example 3.41* Let  $U' = \{A, C\} \subset \{A, B, C\} = U$  and suppose we have a proof of  $\vdash \bigvee U' = A \vee C$ . This can be transformed into a proof of  $\vdash \bigvee U = A \vee (B \vee C)$  as follows, where Theorems 3.34–3.35 are used as derived rules:

- |   |                  |
|---|------------------|
| 1. $\vdash A \vee C$  | Assumption       |
| 2. $\vdash (A \vee C) \vee B$                               | Weakening, 1     |
| 3. $\vdash A \vee (C \vee B)$                               | Associativity, 2 |
| 4. $\vdash (C \vee B) \rightarrow (B \vee C)$               | Commutativity    |
| 5. $\vdash A \vee (C \vee B) \rightarrow A \vee (B \vee C)$ | Weakening, 4     |
| 6. $\vdash A \vee (B \vee C)$                               | MP 3, 5          |
- 

*Proof of Theorem 3.39* The proof is by induction on the structure of the proof in  $\mathcal{G}$ . If  $U$  is an axiom, it contains a pair of complementary literals and  $\vdash \neg p \vee p$  can be proved in  $\mathcal{H}$ . By Lemma 3.40, this can be transformed into a proof of  $\bigvee U$ .

Otherwise, the last step in the proof of  $U$  in  $\mathcal{G}$  is the application of a rule to an  $\alpha$ - or  $\beta$ -formula. As usual, we will use disjunction and conjunction as representatives of  $\alpha$ - and  $\beta$ -formulas.

**Case 1:** A rule in  $\mathcal{G}$  was applied to obtain an  $\alpha$ -formula  $\vdash U_1 \cup \{A_1 \vee A_2\}$  from  $\vdash U_1 \cup \{A_1, A_2\}$ . By the inductive hypothesis,  $\vdash ((\bigvee U_1) \vee A_1) \vee A_2$  in  $\mathcal{H}$  from which we infer  $\vdash \bigvee U_1 \vee (A_1 \vee A_2)$  by associativity.

**Case 2:** A rule in  $\mathcal{G}$  was applied to obtain a  $\beta$ -formula  $\vdash U_1 \cup U_2 \cup \{A_1 \wedge A_2\}$  from  $\vdash U_1 \cup \{A_1\}$  and  $\vdash U_2 \cup \{A_2\}$ . By the inductive hypothesis,  $\vdash (\bigvee U_1) \vee A_1$  and  $\vdash (\bigvee U_2) \vee A_2$  in  $\mathcal{H}$ . We leave it to the reader to justify each step of the following deduction of  $\vdash \bigvee U_1 \vee \bigvee U_2 \vee (A_1 \wedge A_2)$ :

1.  $\vdash \bigvee U_1 \vee A_1$
2.  $\vdash \neg \bigvee U_1 \rightarrow A_1$
3.  $\vdash A_1 \rightarrow (A_2 \rightarrow (A_1 \wedge A_2))$
4.  $\vdash \neg \bigvee U_1 \rightarrow (A_2 \rightarrow (A_1 \wedge A_2))$
5.  $\vdash A_2 \rightarrow (\neg \bigvee U_1 \rightarrow (A_1 \wedge A_2))$
6.  $\vdash \bigvee U_2 \vee A_2$
7.  $\vdash \neg \bigvee U_2 \rightarrow A_2$
8.  $\vdash \neg \bigvee U_2 \rightarrow (\neg \bigvee U_1 \rightarrow (A_1 \wedge A_2))$
9.  $\vdash \bigvee U_1 \vee \bigvee U_2 \vee (A_1 \wedge A_2)$

■

*Proof of Theorem 3.38* If  $\models A$  then  $\vdash A$  in  $\mathcal{G}$  by Theorem 3.8. By the remark at the end of Definition 3.2,  $\vdash A$  is an abbreviation for  $\vdash \{A\}$ . By Theorem 3.39,  $\vdash \bigvee \{A\}$  in  $\mathcal{H}$ . Since  $A$  is a single formula,  $\vdash A$  in  $\mathcal{H}$ . ■

### 3.7 Consistency

What would mathematics be like if both  $1 + 1 = 2$  and  $\neg(1 + 1 = 2) \equiv 1 + 1 \neq 2$  could be proven? An inconsistent deductive system is useless, because *all* formulas are provable and the concept of proof becomes meaningless.

**Definition 3.42** A set of formulas  $U$  is *inconsistent* iff for some formula  $A$ , both  $U \vdash A$  and  $U \vdash \neg A$ .  $U$  is *consistent* iff it is not inconsistent. A deductive system is *inconsistent* iff it contains an inconsistent set of formulas. ■

**Theorem 3.43**  $U$  is inconsistent iff for all  $A$ ,  $U \vdash A$ .

*Proof* Let  $A$  be an arbitrary formula. If  $U$  is inconsistent, for some formula  $B$ ,  $U \vdash B$  and  $U \vdash \neg B$ . By Theorem 3.21,  $\vdash B \rightarrow (\neg B \rightarrow A)$ . Using *MP* twice,  $U \vdash A$ . The converse is trivial. ■

**Corollary 3.44**  $U$  is consistent if and only if for some  $A$ ,  $U \not\vdash A$ .

If a deductive system is sound, then  $\vdash A$  implies  $\models A$ , and, conversely,  $\not\models A$  implies  $\not\vdash A$ . Therefore, if there is even a single falsifiable formula  $A$  in a sound system, the system must be consistent! Since  $\not\models \text{false}$  (where *false* is an abbreviation for  $\neg(p \rightarrow p)$ ), by the soundness of  $\mathcal{H}$ ,  $\not\vdash \text{false}$ . By Corollary 3.44,  $\mathcal{H}$  is consistent.

The following theorem is another way of characterizing inconsistency.

**Theorem 3.45**  $U \vdash A$  if and only if  $U \cup \{\neg A\}$  is inconsistent.

*Proof* If  $U \vdash A$ , obviously  $U \cup \{\neg A\} \vdash A$ , since the extra assumption will not be used in the proof.  $U \cup \{\neg A\} \vdash \neg A$  because  $\neg A$  is an assumption. By Definition 3.42,  $U \cup \{\neg A\}$  is inconsistent.

Conversely, if  $U \cup \{\neg A\}$  is inconsistent, then  $U \cup \{\neg A\} \vdash A$  by Theorem 3.43. By the deduction theorem,  $U \vdash \neg A \rightarrow A$ , and  $U \vdash A$  follows by *MP* from  $\vdash (\neg A \rightarrow A) \rightarrow A$  (Theorem 3.31). ■

### 3.8 Strong Completeness and Compactness \*

The construction of a semantic tableau can be generalized to an infinite set of formulas  $S = \{A_1, A_2, \dots\}$ . The label of the root is  $\{A_1\}$ . Whenever a rule is applied to a leaf of depth  $n$ ,  $A_{n+1}$  will be added to the label(s) of its child(ren) in addition to the  $\alpha_i$  or  $\beta_i$ .

**Theorem 3.46** A set of formulas  $S = \{A_1, A_2, \dots\}$  is unsatisfiable if and only if a semantic tableau for  $S$  closes.

*Proof* Here is an outline of the proof that is given in detail in Smullyan (1968, Chap. III).

If the tableau closes, there is only a finite subset  $S_0 \subset S$  of formulas on each closed branch, and  $S_0$  is unsatisfiable. By a generalization of Theorem 2.46 to an infinite set of formulas, it follows that  $S = S_0 \cup (S - S_0)$  is unsatisfiable.

Conversely, if the tableau is open, it can be shown that there must be an infinite branch containing all formulas in  $S$ , and the union of formulas in the labels of nodes on the branch forms a Hintikka set, from which a satisfying interpretation can be found. ■

The completeness of propositional logic now generalizes to:

**Theorem 3.47** (Strong completeness) Let  $U$  be a finite or countably infinite set of formulas and let  $A$  be a formula. If  $U \models A$  then  $U \vdash A$ .

The same construction proves the following important theorem.

**Theorem 3.48** (Compactness) Let  $S$  be a countably infinite set of formulas, and suppose that every finite subset of  $S$  is satisfiable. Then  $S$  is satisfiable.

*Proof* Suppose that  $S$  were unsatisfiable. Then a semantic tableau for  $S$  must close. There are only a finite number of formulas labeling nodes on each closed branch. Each such set of formulas is a finite unsatisfiable subset of  $S$ , contradicting the assumption that all finite subsets are satisfiable. ■

### 3.9 Variant Forms of the Deductive Systems \*

$\mathcal{G}$  and  $\mathcal{H}$ , the deductive systems that we presented in detail, are two of many possible deductive systems for propositional logic. Different systems are obtained by changing the operators, the axioms or the representations of proofs. In propositional logic, all these systems are equivalent in the sense that they are sound and complete. In this section, we survey some of these variants.

#### 3.9.1 Hilbert Systems

Hilbert systems almost invariably have *MP* as the only rule. They differ in the choice of primitive operators and axioms. For example,  $\mathcal{H}'$  is an Hilbert system where Axiom 3 is replaced by:

$$\text{Axiom } 3' \quad \vdash (\neg B \rightarrow \neg A) \rightarrow ((\neg B \rightarrow A) \rightarrow B).$$

**Theorem 3.49**  $\mathcal{H}$  and  $\mathcal{H}'$  are equivalent in the sense that a proof in one system can be transformed into a proof in the other.

*Proof* We prove Axiom 3' in  $\mathcal{H}$ . It follows that any proof in  $\mathcal{H}'$  can be transformed into a proof in  $\mathcal{H}$ , by starting with this proof of the new axiom and using it as a previously proved theorem.

- |  |                  |
|--|------------------|
| 1. $\{\neg B \rightarrow \neg A, \neg B \rightarrow A, \neg B\} \vdash \neg B$                       | Assumption       |
| 2. $\{\neg B \rightarrow \neg A, \neg B \rightarrow A, \neg B\} \vdash \neg B \rightarrow A$         | Assumption       |
| 3. $\{\neg B \rightarrow \neg A, \neg B \rightarrow A, \neg B\} \vdash A$                            | MP 1, 2          |
| 4. $\{\neg B \rightarrow \neg A, \neg B \rightarrow A, \neg B\} \vdash \neg B \rightarrow \neg A$    | Assumption       |
| 5. $\{\neg B \rightarrow \neg A, \neg B \rightarrow A, \neg B\} \vdash A \rightarrow B$              | Contrapositive 4 |
| 6. $\{\neg B \rightarrow \neg A, \neg B \rightarrow A, \neg B\} \vdash B$                            | MP 3, 5          |
| 7. $\{\neg B \rightarrow \neg A, \neg B \rightarrow A\} \vdash \neg B \rightarrow B$                 | Deduction 7      |
| 8. $\{\neg B \rightarrow \neg A, \neg B \rightarrow A\} \vdash (\neg B \rightarrow B) \rightarrow B$ | Theorem 3.31     |
| 9. $\{\neg B \rightarrow \neg A, \neg B \rightarrow A\} \vdash B$                                    | MP 8, 9          |
| 10. $\{\neg B \rightarrow \neg A\} \vdash (\neg B \rightarrow A) \rightarrow B$                      | Deduction 9      |
| 11. $\vdash (\neg B \rightarrow \neg A) \rightarrow ((\neg B \rightarrow A) \rightarrow B)$          | Deduction 10     |

The use of the deduction theorem is legal because its proof in  $\mathcal{H}$  does not use Axiom 3, so the identical proof can be done in  $\mathcal{H}'$ .

We leave it as an exercise to prove Axiom 3 in  $\mathcal{H}'$ . ■

Either conjunction or disjunction may replace implication as the binary operator in the formulation of a Hilbert system. Implication can then be defined by  $\neg(A \wedge \neg B)$  or  $\neg A \vee B$ , respectively, and *MP* is still the only inference rule. For disjunction, a set of axioms is:

- Axiom 1**  $\vdash A \vee A \rightarrow A,$   
**Axiom 2**  $\vdash A \rightarrow A \vee B,$   
**Axiom 3**  $\vdash A \vee B \rightarrow B \vee A,$   
**Axiom 4**  $\vdash (B \rightarrow C) \rightarrow (A \vee B \rightarrow A \vee C).$

The steps needed to show the equivalence of this system with  $\mathcal{H}$  are given in Mendelson (2009, Exercise 1.54).

Finally, Meredith's axiom:

$$\vdash ((A \rightarrow B) \rightarrow (\neg C \rightarrow \neg D)) \rightarrow C \rightarrow E \rightarrow [(E \rightarrow A) \rightarrow (D \rightarrow A)],$$

together with *MP* as the rule of inference is a complete deductive system for propositional logic. Adventurous readers are invited to prove the axioms of  $\mathcal{H}$  from Meredith's axiom following the 37-step plan given in Monk (1976, Exercise 8.50).

### 3.9.2 Gentzen Systems

$\mathcal{G}$  was constructed in order to simplify the theoretical treatment by using a notation that is identical to that of semantic tableaux. We now present a deductive system similar to the one that Gentzen originally proposed; this system is taken from Smullyan (1968, Chap. XI).

**Definition 3.50** If  $U$  and  $V$  are (possibly empty) sets of formulas, then  $U \Rightarrow V$  is a *sequent*. ■

Intuitively, a sequent represents 'provable from' in the sense that the formulas in  $U$  are assumptions for the set of formulas  $V$  that are to be proved. The symbol  $\Rightarrow$  is similar to the symbol  $\vdash$  in Hilbert systems, except that  $\Rightarrow$  is part of the object language of the deductive system being formalized, while  $\vdash$  is a metalanguage notation used to reason about deductive systems.

**Definition 3.51** Axioms in the Gentzen sequent system  $\mathcal{S}$  are sequents of the form:

$$U \cup \{A\} \Rightarrow V \cup \{A\}.$$

The rules of inference are shown in Fig. 3.2. ■

The semantics of the sequent system  $\mathcal{S}$  are defined as follows:

**Definition 3.52** Let  $S = U \Rightarrow V$  be a sequent where  $U = \{U_1, \dots, U_n\}$  and  $V = \{V_1, \dots, V_m\}$ , and let  $\mathcal{I}$  be an interpretation for  $U \cup V$ . Then  $v_{\mathcal{I}}(S) = T$  if and only if  $v_{\mathcal{I}}(U_1) = \dots = v_{\mathcal{I}}(U_n) = T$  implies that for some  $i$ ,  $v_{\mathcal{I}}(V_i) = T$ . ■

This definition relates sequents to formulas: Given an interpretation  $\mathcal{I}$  for  $U \cup V$ ,  $v_{\mathcal{I}}(U \Rightarrow V) = T$  if and only if  $v_{\mathcal{I}}(\bigwedge U \rightarrow \bigvee V) = T$ .

<i>op</i>	Introduction into consequent	Introduction into antecedent
$\wedge$	$\frac{U \Rightarrow V \cup \{A\} \quad U \Rightarrow V \cup \{B\}}{U \Rightarrow V \cup \{A \wedge B\}}$	$\frac{U \cup \{A, B\} \Rightarrow V}{U \cup \{A \wedge B\} \Rightarrow V}$
$\vee$	$\frac{U \Rightarrow V \cup \{A, B\}}{U \Rightarrow V \cup \{A \vee B\}}$	$\frac{U \cup \{A\} \Rightarrow V \quad U \cup \{B\} \Rightarrow V}{U \cup \{A \vee B\} \Rightarrow V}$
$\rightarrow$	$\frac{U \cup \{A\} \Rightarrow V \cup \{B\}}{U \Rightarrow V \cup \{A \rightarrow B\}}$	$\frac{U \Rightarrow V \cup \{A\} \quad U \cup \{B\} \Rightarrow V}{U \cup \{A \rightarrow B\} \Rightarrow V}$
$\neg$	$\frac{U \cup \{A\} \Rightarrow V}{U \Rightarrow V \cup \{\neg A\}}$	$\frac{U \Rightarrow V \cup \{A\}}{U \cup \{\neg A\} \Rightarrow V}$

Fig. 3.2 Rules of inference for sequents

### 3.9.3 Natural Deduction

The advantage of working with sequents is that the deduction theorem is a rule of inference: introduction into the consequent of  $\rightarrow$ . The convenience of Gentzen systems is apparent when proofs are presented in a format called *natural deduction* that emphasizes the role of assumptions.

Look at the proof of Theorem 3.30, for example. The assumptions are dragged along throughout the entire deduction, even though each is used only twice, once as an assumption and once in the deduction rule. The way we reason in mathematics is to set out the assumptions once when they are first needed and then to *discharge* them by using the deduction rule. A natural deduction proof of Theorem 3.30 is shown in Fig. 3.3.

The boxes indicate the scope of assumptions. Just as in programming where local variables in procedures can only be used within the procedure and disappear when the procedure is left, an assumption can only be used within the scope of its box, and once it is discharged by using it in a deduction, it is no longer available.

### 3.9.4 Subformula Property

**Definition 3.53** A deductive system has the *subformula property* iff any formula appearing in a proof of  $A$  is either a subformula of  $A$  or the negation of a subformula of  $A$ . ■

The systems  $\mathcal{G}$  and  $\mathcal{S}$  have the subformula property while  $\mathcal{H}$  does not. For example, in the proof of the theorem of double negation  $\vdash \neg\neg A \rightarrow A$ , the formula  $\vdash \neg\neg\neg\neg A \rightarrow \neg\neg A$  appeared even though it is obviously not a subformula of the theorem.

Gentzen proposed his deductive system in order to obtain a system with the subformula property. Then he defined the system  $\mathcal{S}'$  by adding an additional rule of inference, the *cut rule*:

$$\frac{U, A \Rightarrow V \quad U \Rightarrow V, A}{U \Rightarrow V}$$

1.	$A \rightarrow \neg A$	Assumption																		
<table style="width: 100%; border-collapse: collapse;"> <tr> <td style="padding: 5px;">2.</td> <td style="padding: 5px;"><math>\neg \neg A</math></td> <td style="padding: 5px; text-align: right;">Assumption</td> </tr> <tr> <td style="padding: 5px;">3.</td> <td style="padding: 5px;"><math>A</math></td> <td style="padding: 5px; text-align: right;">Double negation 2</td> </tr> <tr> <td style="padding: 5px;">4.</td> <td style="padding: 5px;"><math>\neg A</math></td> <td style="padding: 5px; text-align: right;">MP 1, 3</td> </tr> <tr> <td style="padding: 5px;">5.</td> <td style="padding: 5px;"><math>A \rightarrow (\neg A \rightarrow \text{false})</math></td> <td style="padding: 5px; text-align: right;">Theorem 3.21</td> </tr> <tr> <td style="padding: 5px;">6.</td> <td style="padding: 5px;"><math>\neg A \rightarrow \text{false}</math></td> <td style="padding: 5px; text-align: right;">MP 3, 5</td> </tr> <tr> <td style="padding: 5px;">7.</td> <td style="padding: 5px;"><math>\text{false}</math></td> <td style="padding: 5px; text-align: right;">MP 4, 6</td> </tr> </table>			2.	$\neg \neg A$	Assumption	3.	$A$	Double negation 2	4.	$\neg A$	MP 1, 3	5.	$A \rightarrow (\neg A \rightarrow \text{false})$	Theorem 3.21	6.	$\neg A \rightarrow \text{false}$	MP 3, 5	7.	$\text{false}$	MP 4, 6
2.	$\neg \neg A$	Assumption																		
3.	$A$	Double negation 2																		
4.	$\neg A$	MP 1, 3																		
5.	$A \rightarrow (\neg A \rightarrow \text{false})$	Theorem 3.21																		
6.	$\neg A \rightarrow \text{false}$	MP 3, 5																		
7.	$\text{false}$	MP 4, 6																		
8.	$\neg \neg A \rightarrow \text{false}$	Deduction 2, 7																		
9.	$\neg A$	Reductio ad absurdum 8																		
10.	$(A \rightarrow \neg A) \rightarrow \neg A$	Deduction 1, 9																		

**Fig. 3.3** A natural deduction proof

to the system  $\mathcal{S}$  and showed that proofs in  $\mathcal{S}'$  can be mechanically transformed into proofs in  $\mathcal{S}$ . See Smullyan (1968, Chap. XII) for a proof of the following theorem.

**Theorem 3.54** (Gentzen’s Hauptsatz) *Any proof in  $\mathcal{S}'$  can be transformed into a proof in  $\mathcal{S}$  not using the cut rule.*

### 3.10 Summary

Deductive systems were developed to formalize mathematical reasoning. The structure of Hilbert systems such as  $\mathcal{H}$  imitates the style of mathematical theories: a small number of axioms, *modus ponens* as the sole rule of inference and proofs as linear sequences of formulas. The problem with Hilbert systems is that they offer no guidance on how to find a proof of a formula. Gentzen systems such as  $\mathcal{G}$  (and variants that use sequents or natural deduction) facilitate finding proofs because all formulas that appear are subformulas of the formula to be proved or their negations.

Both the deductive systems  $\mathcal{G}$  and  $\mathcal{H}$  are sound and complete. Completeness of  $\mathcal{G}$  follows directly from the completeness of the method of semantic tableaux as a decision procedure for satisfiability and validity in propositional logic. However, the method of semantic tableaux is not very efficient. Our task in the next chapters is to study more efficient algorithms for satisfiability and validity.

### 3.11 Further Reading

Our presentation is based upon Smullyan (1968) who showed how Gentzen systems are closely related to tableaux. The deductive system  $\mathcal{H}$  is from Mendelson (2009); he develops the theory of  $\mathcal{H}$  (and later its generalization to first-order logic) without recourse to tableaux. Huth and Ryan (2004) base their presentation of logic on natural deduction. Velleman (2006) will help you learn how to prove theorems in mathematics.

### 3.12 Exercises

3.1 Prove in  $\mathcal{G}$ :

$$\begin{aligned} &\vdash (A \rightarrow B) \rightarrow (\neg B \rightarrow \neg A), \\ &\vdash (A \rightarrow B) \rightarrow ((\neg A \rightarrow B) \rightarrow B), \\ &\vdash ((A \rightarrow B) \rightarrow A) \rightarrow A. \end{aligned}$$

3.2 Prove that if  $\vdash U$  in  $\mathcal{G}$  then there is a closed semantic tableau for  $\bar{U}$  (the forward direction of Theorem 3.7).

3.3 Prove the derived rule *modus tollens*:

$$\frac{\vdash \neg B \quad \vdash A \rightarrow B}{\vdash \neg A}.$$

3.4 Give proofs in  $\mathcal{G}$  for each of the three axioms of  $\mathcal{H}$ .

3.5 Prove  $\vdash (\neg A \rightarrow A) \rightarrow A$  (Theorem 3.31) in  $\mathcal{H}$ .

3.6 Prove  $\vdash (A \rightarrow B) \vee (B \rightarrow C)$  in  $\mathcal{H}$ .

3.7 Prove  $\vdash ((A \rightarrow B) \rightarrow A) \rightarrow A$  in  $\mathcal{H}$ .

3.8 Prove  $\{\neg A\} \vdash (\neg B \rightarrow A) \rightarrow B$  in  $\mathcal{H}$ .

3.9 Prove Theorem 3.34 in  $\mathcal{H}$ :

$$\begin{aligned} &\vdash A \rightarrow A \vee B, \\ &\vdash B \rightarrow A \vee B, \\ &\vdash (A \rightarrow B) \rightarrow ((C \vee A) \rightarrow (C \vee B)). \end{aligned}$$

3.10 Prove Theorem 3.35 in  $\mathcal{H}$ :

$$\vdash A \vee (B \vee C) \leftrightarrow (A \vee B) \vee C.$$

3.11 Prove Theorem 3.36 in  $\mathcal{H}$ :

$$\begin{aligned} &\vdash A \vee (B \wedge C) \leftrightarrow (A \vee B) \wedge (A \vee C), \\ &\vdash A \wedge (B \vee C) \leftrightarrow (A \wedge B) \vee (A \wedge C). \end{aligned}$$

3.12 Prove that Axiom 2 of  $\mathcal{H}$  is valid by constructing a semantic tableau for its negation.

3.13 Complete the proof that if  $U' \subseteq U$  and  $\vdash \bigvee U'$  then  $\vdash \bigvee U$  (Lemma 3.40).

3.14 Prove the last two formulas of Exercise 3.1 in  $\mathcal{H}$ .



**3.15** \* Prove Axiom 3 of  $\mathcal{H}$  in  $\mathcal{H}'$ .

**3.16** \* Prove that the Gentzen sequent system  $\mathcal{S}$  is sound and complete.

**3.17** \* Prove that a set of formulas  $U$  is inconsistent if and only if there is a finite set of formulas  $\{A_1, \dots, A_n\} \subseteq U$  such that  $\vdash \neg A_1 \vee \dots \vee \neg A_n$ .

**3.18** A set of formulas  $U$  is *maximally consistent* iff every proper superset of  $U$  is not consistent. Let  $S$  be a countable, consistent set of formulas. Prove:

1. Every finite subset of  $S$  is satisfiable.
2. For every formula  $A$ , at least one of  $S \cup \{A\}$ ,  $S \cup \{\neg A\}$  is consistent.
3.  $S$  can be extended to a maximally consistent set.

## References

- M. Huth and M.D. Ryan. *Logic in Computer Science: Modelling and Reasoning about Systems (Second Edition)*. Cambridge University Press, 2004.
- E. Mendelson. *Introduction to Mathematical Logic (Fifth Edition)*. Chapman & Hall/CRC, 2009.
- J.D. Monk. *Mathematical Logic*. Springer, 1976.
- R.M. Smullyan. *First-Order Logic*. Springer-Verlag, 1968. Reprinted by Dover, 1995.
- D.J. Velleman. *How to Prove It: A Structured Approach (Second Edition)*. Cambridge University Press, 2006.