The Science of Proof: Mathematical Reasoning and Its Limitations

William G. Faris
University of Arizona

Contents

Preface

The book you are reading began as notes for a one-semester undergraduate course in mathematical logic. The students in such a course have ordinarily already taken a course in which they have explicit training in constructing proofs. They also tend to have experiences in courses in algebra or analysis where rigorous proofs are an important part of the content. However, the material in this book may well be of wider interest. A considerable number of professional mathematicians do not know explicit rules for constructing proofs; even fewer know the implications of these rules for our understanding of mathematics. The author would argue that every mathematician should pay serious attention to this subject.

The book is organized in four parts. The material in Chapters 1 through 6 is the practical story about proof construction. The following Chapters 7 through 9 attempt to explain proofs from a more theoretical point of view. Chapters 10 through 12 describe the extent to which the theorems and proofs of mathematics characterize mathematical reality; the answer given by model theory is there is fundamental ambiguity. The remaining chapters are supplementary material: background results in Chapters 13 through 15, a new topic sketched in Chapter 16.

The thesis of this book is that there is a science of proof. Mathematics prides itself on making its assumptions explicit, but most mathematicians learn to construct proofs in an unsystematic way, by example. This is in spite of the known fact that there is an organized way of creating proofs using only a limited number of proof techniques. This is not only true as a theoretical matter, but in actual mathematical practice.

Relatively few mathematics texts present a systematic exposition of rules for proof. However it is common for logic texts written by philosophers to introduce a subject called *natural deduction*. This is a set of rules that comes rather close to those that mathematicians use in practice. Of course mathematicians justifiably tend to skip over the more trivial steps in logical reasoning. Some less obvious techniques, such as the use of "arbitrary variables," are nicely captured by natural deduction.

Even using natural deduction it is possible to make stupid attempts at proof construction, such as going around in a circle of statements. One natural question is whether it is possible to construct proofs in a way that actually leads to progress. It will be shown that there are a small number of natural deduction *proof templates* that accomplish this. These work quite well in practice for the simple proofs that are often used as exercises for beginning students.

The templates for natural deduction have a somewhat clumsy structure. The reason for this may be traced back to the fact that at each stage in reasoning there may be a number of hypotheses in force, but at the particular stage there is only a single conclusion. There are alternatives to natural deduction for which at each stage there can be multiple hypotheses and multiple (alternative) conclusions. *Gentzen deduction* is of this nature. See Kleene's book [6] for a treatment. (The tableau framework [17] is similar; it is basically a more efficient packaging of Gentzen deduction.) In Gentzen deduction it is immediately clear what needs to be done at each stage of proof construction.

There is a translation between natural deduction with templates and Gentzen deduction. In Gentzen deduction one allows multiple alternate conclusions. In natural deduction with templates there is only one conclusion at a time; possible alternative conclusions are replaced by negated hypotheses. This seems like a small distinction, but the two approaches appear quite different. At a deeper level they are the same.

In this book we present the translation of natural deduction templates to Gentzen deduction. We use natural deduction for practical reasoning and Gentzen deduction for theoretical understanding. The fundamental theoretical result is the classic *Gödel completeness theorem.* (We shall see that this might be better called the Gödel "semantic completeness" theorem.) In the framework of proof theory, this theorem says that there is a systematic way of attempting to construct proofs. If there is a proof, then the method is guaranteed to construct it. If there is no proof, then the method produces a counterexample.

It might seem that this might make mathematics a trivial enterprise, but this is not at all the case. The problem is that the construction of a counterexample is in most cases an infinite process. In a practical instance of proof construction, at a given stage one may not know whether one is on the way to a proof, or whether one is working at the never-ending task of constructing the counterexample. This deep problem arises from the fact that there can be a never-ending sequence of "arbitrary variables" with ever more complex properties.

In this context, it is a remarkable fact that each proof, once accomplished, is finite. This fact, combined with the Gödel completeness theorem, leads to another classic result called the *compactness theorem.* It turns out that the compactness theorem has strikingly negative implications for our hope of understanding the mathematical universe. This issue is the beginning of the subject of *model theory.* In this book we treat model theory at a very elementary level. Nevertheless, we shall see in an explicit way that any mathematical theory that treats infinite mathematical objects will have *non-standard models.* These are interpretations that are essentially different from the original interpretation that we were trying to specify. In other words, in mathematics we almost never know what we are talking about. This is a fundamental problem of semantics.

There is a more positive aspect to the existence of non-standard models. Some mathematicians have proposed a program of non-standard mathematics, in which mathematical reasoning is enriched by acknowledging additional properties that arise in such models. Thus there is non-standard arithmetic and even non-standard analysis. Non-standard analysis turns out to be a possible framework for introducing infinitesimals, which then leads to a particularly elementary approach to calculus. The approach developed by Nelson [10, 11] gives an accessible introduction to this circle of ideas.

> It is worth making a few comments about a topic that is not included in this book. There is an extremely famous result called the *Gödel incompleteness theorem*. The meaning of the word "complete" in this context is quite different. It refers to the difficult of finding an effective set of axioms for a theory that settles all questions about the theory. (For this reason the result might better be called the Gödel "syntatic incompleteness" theorem.) This theory applies in particular to the theory of the natural number system. The description of what is meant by an effective set of axioms and the developments needed to prove the Gödel incompleteness theorem are somewhat complicated. They are not treated in this book.
>
> The Gödel incompleteness theorem is said to have dramatic implications for mathematics, and this is in fact the case. However, the author believes that the result that follows from the Gödel completeness theorem and the compactness theorem, while quite different, is even more devastating. There is an artificial device for defining a set of axioms that settles all questions about the theory of some infinite mathematical object, such as the natural number system. One can just take as axioms all true statements. So it is always possible to have a complete theory in this syntactic sense, at least in principle. However, a complete theory of the natural numbers will still have non-standard models. In other words, even the collection of all true statements about the natural numbers cannot characterize the natural number system. The natural numbers go on and on, but just how they do it is a mystery.

The origin of this book was the proof theory part; the model theory part was added later. It arose from my desire to understand the natural mathematical structure of logical reasoning. When I was a student at the University of Washington I attended lectures of Paul Halmos on algebraic logic, and I found this the beginning of a coherent account [5]. More clarification came from a series of conversations with William Lawvere, when we were both visiting the Institut des Hautes Etudes Scientifiques. He pointed out that commonly used patterns of logical inference are adjoint functors in the sense of category theory. At some point he mentioned the text by Kleene [6] and the Gentzen calculus explained there. I was pleased by Gentzen's idea of systematically eliminating logical operations in an attempt to produce a proof, and I decided to base a logic course on this approach. The Gentzen calculus turns reasoning into something akin to manipulating inequalities, and this is not how we reason in practice. So I also taught natural deduction, which is closer to the the way we construct proofs in mathematics. I also introduced that templates for natural deduction that channel it into a framework that is guaranteed to produce a proof (if one exists). These templates seem not to be widely known, but the world would surely be a better place if every mathematician were aware of their existence.

> It seems appropriate to dedicate this book to Edward Nelson (1932–2014). He contributed to analysis, probability, mathematical physics, non-standard mathematics, and logic. In every field in which he worked he dealt with the most important and fundamental issues. His insights will be prized as long as there is a world of mathematics and mathematicians.

Chapter 1

Introduction

1.1 Introduction

Mathematics is different from other sciences. The distinction is expressed in the following passage by James Glimm [4].

> There is an absolute nature to truth in mathematics, which is unmatched in any other branch of knowledge. A theorem, once proven, requires independent checking but not repetition or independent derivation to be accepted as correct. In contrast, experiments in physics must be repeated to be regarded as confirmed. In medicine, the number of independent confirmations required is much higher. Truth in mathematics is totally dependent on pure thought, with no component of data to be added. This is unique. Associated with truth in mathematics is an absolute certainty in its validity.
>
> Why does this matter, and why does it go beyond a cultural oddity of our profession? The answer is that mathematics is deeply embedded in the reasoning used within many branches of knowledge. That reasoning often involves conjectures, assumptions, intuition. But whatever aspect has been reduced to mathematics has an absolute validity. As in other subjects search for truth, the mathematical components embedded in their search are like the boulders in the stream, providing a solid footing on which to cross from one side to the other.

A mathematical result has added value when it is accompanied by a mathematical proof. This does not mean that it is superfluous to draw an illuminating picture or present a striking application. However, in this book the focus is on proof.

Most mathematicians have some idea of how to construct a proof and check its validity, but the process is learned by experience. The thesis of this book is that there is a science of proof (proof theory) that should be known to mathematicians. In simple cases it can even help in creating proofs. Proofs are not only a source of certainty; they also have useful internal structure.

In every branch of applied mathematics a theory is created to understand a given subject matter. Proof theory is no different; logic is applied to understand what mathematicians are attempting when they construct proofs. The logical tools also have broader implications. It turns out that mathematical proof, while indeed giving a kind of certainty, is an imperfect description of mathematical reality. This appears in the last part of the book (model theory).

The book treats the following topics:

1. The syntax and semantics of logic (chapters 2,3,4)

2. Natural deduction with templates (chapters 5,6)

3. Gentzen deduction and the Gödel completeness theorem (chapters 7,8,9)

4. Model theory (chapters 10,11,12)

5. Mathematical background (chapters 13,14,15)

The appendix (chapter 16) is a brief introduction to intuitionistic logic.

1.2 Syntax and semantics

In mathematical logic there is a distinction between *syntax* and *semantics*. Syntax is the study of the formal structure of the language. The formation of sentences and the structure of proofs are part of syntax. Semantics is about possible interpretations of sentences of the language and about the truth of sentences in an interpretation. Syntax is about language, and semantics is about content.

The word semantics is used rather generally to refer to meaning. Thus a sentence like "Rover swims" might refer to the ability of a certain dog named Rover. To grasp this sort of meaning requires a knowledge of the world, including animals and bodies of water. On the other hand, we might only care that the sentence "Rover swims" is true. In other words, there is some object (named Rover) that belongs to some set (of swimming dogs). The kind of object and the identity of the set may be irrelevant. This kind of semantics might be called *truth semantics*. It is a much less informative kind of semantics.

The semantics studied in mathematical logic is truth semantics. Even this is an interesting subject. This is not completely obvious at first, since a sentence like "Rover swims" is rather trivial from the point of truth semantics. Either Rover belongs to the set of swimmers, or Rover does not belong to the set of swimmers. So the sentence is either true or false. The chapter on property logic presents a complete analysis of the truth semantics of this kind of sentence.

The situation is entirely different when there is a relation in the story. The truth semantics of sentences involving even a single relation can be rich enough to be worth serious study. In general, no complete analysis is possible. For a start, the truth of a small number of appropriately chosen sentences may imply that there are infinitely many objects under discussion. This fact is familiar in contexts such as the sentence "Every event is caused by some other event". Take this sentence together with sentences that assert that "causes" is irreflexive and transitive. (See the next section for such sentences.) If these sentences are true, then it follows logically that there is no first cause.

1.3 Syntax constrains semantics

Here is an example of how syntax constrains semantics. It is the same example with the relation "causes", but now we use the symbol $<$. Consider the three sentences.

$\forall x\, \exists y\, y < x$

$\forall x\, \neg\, x < x$

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

These have clear meanings in the theory of causation. The first says that every x is caused by some y. The second says that it is never the case that x causes x. The third says that if y causes x and z causes y, then z (indirectly) causes x.

If these three sentences have an interpretation in some domain of objects (events), then it follows that there are infinitely many objects. In other words, there is no first cause. This is an example where simple syntax (three sentences) has profound semantic implications.

It also shows how convenient it is to use truth semantics. One does not need a deeper knowledge of the nature of events or the meaning of causation. In fact, these are notoriously difficult issues in philosophy. All one needs to ask is what happens when three axioms are true.

1.4 Language and metalanguage

In order to give understand logic and proof, it is useful to focus on a precisely specified language. This is called the *object language*, and it is the intended object of study. For example, we could have a language that is intended to describe certain aspects of natural numbers. It could have property symbols "even" and "odd". A typical sentence might be

$$\neg \exists n\, (n \text{ even} \wedge n \text{ odd})$$

This is intended to say that there does not exist a number that is both even and odd. Another sentence is

$$\forall n\, (\neg n \text{ even} \vee \neg n \text{ odd})$$

This is intended to mean that every number is not even or not odd.

We can now discuss properties of these sentences. For instance, we could say that they are logically equivalent. That is, without knowing anything about "even" and "odd" other than that they express properties of some kind of objects, the two sentences are both true or both false.

In the intended interpretation of the sentences, in which the objects are natural numbers and the properties are the usual properties of evenness and oddness, the sentences are both true. The fact that the sentences are logically equivalent gives us the possibility of transforming such sentences one into another in other contexts. For instance, we might be talking about some group of people. Perhaps in this context "even" means "even-tempered" and "odd" means "non-conformist". Then the truth or falsity of the individual sentences is not so clear, but they are true or false together.

There is a syntactical discussion about the formal relation of these sentences. There is also a semantic discussion about the implications of this relation for truth. These discussions are in the *metalanguage*, the language that is used to discuss the object language. In this case, the metalanguage is English, but in the following it will usually also have a component of mathematical jargon. We could say that

$$\neg\exists n\,(A \wedge B)$$

is logically equivalent to

$$\forall n\,(\neg A \vee \neg B)$$

Here A, B are variables that stand for formulas involving n. The A, B variables are not part of the language, but are part of the metalanguage. Such expressions involve a confusing mixture of object language and metalanguage to which the reader must remain alert.

In the translation from English to mathematical logic one drops the word "is". Instead of writing "n is even", one just writes "n even". It might seem shocking that this word is superfluous, but this is a matter of context, as will now be demonstrated.

In the following discussion, the object language will be Russian, and the metalanguage will be English. In English one would write, "Every happy family is similar to every other happy family." In Russian one would write the equivalent of "Every happy family similar to every other happy family." This is completely natural in the Russian language.

Here is a translation (by Constance Garnett) of the famous opening sentences of Anna Karenina.

> Happy families are all alike; every unhappy family is unhappy in its own way.
>
> Everything was in confusion in the Oblonskys' house. The wife had discovered that the husband was carrying on an intrigue with a French girl, who had been a governess in their family, and she had announced to her husband that she could not go on living in the same house with him.

The word "is" (with various variations) occurs a number of times in the translated passage. In the original Russian it is omitted, at least in the present tense.

Another feature of Russian is that there are no articles. In place of “the wife” and “a French girl” the Russian form would be “wife” and ”French girl”. However, it would be a mistake to think that the Russian language is relatively impoverished. On the contrary, it has a rich internal structure of its own, a structure that is not preserved in the process of translation to English.

The object language of mathematical logic is designed to be simple and explicit. It is our good fortune that it is so primitive; we have at least some hope of understanding it.

Chapter 2

Propositional logic

2.1 Syntax of propositional logic

Propositional logic is logic that describes how to combine sentences. The symbols that represent sentences of propositional logic will be called formulas.

Here is the syntax of propositional logic. There are *atomic formulas* denoted $P, Q, R, \ldots$. They are combined by *connectives* $\wedge$, $\vee$, $\Rightarrow$, $\neg$ to form more complicated *formulas*. (One could just as well use the more familiar connectives "and", "or", "implies", "not". These are the intended meanings of the symbols.) Here are the rules for generating these formulas:

And If A, B are formulas, then $(A \wedge B)$ is a formula.

Or If A, B are formulas, then $(A \vee B)$ is a formula.

Implies If A, B are formulas, then $(A \Rightarrow B)$ is a formula.

Not If A, B are formulas, then $\neg A$ is a formula.

This particular list of connectives is chosen for later convenience. There is something unnatural about having three binary operations and only one unary operation. This could be avoided by the following device. Introduce an atomic sentence $\perp$ that is always to be interpreted as false. Then one could take $\neg A$ as an abbreviation of $(A \Rightarrow \perp)$.

Sometimes people introduce other connectives. One that is frequently useful is *equivalent*. In this treatment we treat this as an abbreviation; in fact $(A \Leftrightarrow B)$ is taken as a shorter version of $((A \Rightarrow B) \wedge (B \Rightarrow A))$.

Example: The implication $(Q \Rightarrow (P \wedge (P \Rightarrow Q)))$ is a formula. So is the implication $(\neg(P \wedge Q) \Rightarrow \neg P)$.

Example: The expression $(Q \Rightarrow (P \Rightarrow Q \wedge P))$ is not a formula. However $(Q \Rightarrow (P \Rightarrow (Q \wedge P)))$ $(Q \Rightarrow ((P \Rightarrow Q) \wedge P))$ are both formulas.

The word "formula" in logic is used in more general contexts, such as the logic of properties or the logic of relations. In these contexts a sentence is a special kind of formula such that in a given interpretation it is either true or false. In propositional logic a formula is always a sentence, so this may also be called the logic of sentences.

Convention 2.1 *In writing a formula, omit the outermost parentheses. Restore them when the formula becomes part of another formula.*

This convention is just a convenient abbreviation. Thus the formula $Q \Rightarrow (P \wedge (P \Rightarrow Q))$ is an abbreviation for the formula $(Q \Rightarrow (P \wedge (P \Rightarrow Q)))$. On the other hand, its negation must be written as $\neg(Q \Rightarrow (P \wedge (P \Rightarrow Q)))$.

2.2 Lore of connectives

The connectives $\wedge$, $\vee$, $\neg$ are sometimes called *conjunction*, *disjunction*, *negation*.

The *implication* $A \Rightarrow B$ is also written

if A, then B

A only if B

B if A.

The *converse* of the implication $A \Rightarrow B$ is the implication $B \Rightarrow A$. The *contrapositive* of the implication $A \Rightarrow B$ is the implication $\neg B \Rightarrow \neg A$.

The equivalence $A \Leftrightarrow B$ is also written

A if and only if B.

Warning: In mathematical practice, when A is defined by B, the definition is usually written in the form A if B. It has the logical force of $A \Leftrightarrow B$.

2.3 Semantics of propositional logic

Here is the semantics of propositional logic. Since the only syntactic objects are sentences, the semantics is rather degenerate: in an interpretation every sentence is either false or true.

A *propositional interpretation* is specified by attaching to each atomic sentence a truth value, false or true. For example, one could attach to P the value true and to Q the value false.

The next thing is to determine the truth value for compound formulas. In logic the word "or" is used in the inclusive sense, so that an "or" formula is true when either one or the other or both of the constituents are true. (Some treatments of logic also introduce an "exclusive or", but we shall not need that.)

And $(A \wedge B)$ is true when A is true and B is true, otherwise false.

Or $(A \vee B)$ is true when A is true or B is true, otherwise false.

Implies $(A \Rightarrow B)$ is true when A is false or B is true, otherwise false.

Not $\neg A$ is true when A is false, otherwise false.

It is easy to see that $(A \Leftrightarrow B)$ is true when A, B are both true or both false, otherwise false.

Example: With the interpretation in which P is true and Q is false, the formula $Q \Rightarrow (P \wedge (P \Rightarrow Q))$ is true. On the other hand, the formula $\neg(P \wedge Q) \Rightarrow \neg P$ is false.

2.4 Interpretation of formulas

Sometimes it is helpful to have a somewhat more mathematical description of the semantics. For convenience we use the symbols 0 and 1 to denote falsity and truth. A *propositional interpretation* is specified by attaching to each atomic sentence a truth value 0 or 1. For example, one could attach to P the value 1 and to Q the value 0. If we write $\mathcal{P}$ for the set of atomic sentences, then the interpretation is specified by a function $\phi : \mathcal{P} \to \{0, 1\}$. So in the example the function ϕ is chosen so that $\phi[P] = 1$ and $\phi[Q] = 0$.

Proposition 2.2 *If there are k atomic sentences, then there are 2^k interpretations.*

In principle the number of atomic sentences could be very large, but in a given argument it may be that a relatively small number of them actually occur. So we may often think of the set $\mathcal{P}$ of atomic sentences as having k elements, where k is not particularly large. In that case we can do logical calculations by examining all 2^k possibilities.

In this more sophisticated notation the truth value for a compound formula is determined as follows.

And $\phi[(A \wedge B)] = \min[\phi[A], \phi[B]]$.

Or $\phi[(A \vee B)] = \max[\phi[A], \phi[B]]$.

Implies $\phi[(A \Rightarrow B)] = \max[(1 - \phi[A]), \phi[B]]$.

Not $\phi[\neg A] = 1 - [\phi[A]]$.

The essential property of implication is that $\phi[(A \Rightarrow B)] = 1$ precisely when $\phi[A] \leq \phi[B]$. The convention for the symbol $\perp$ is that $\phi[\perp] = 0$, so $\phi[\neg A] = \phi[(A \Rightarrow \perp)]$.

For equivalence the important thing is that $\phi[A \Leftrightarrow B] = 1$ precisely when $\phi[A] = \phi[B]$. For instance, we could express $\phi[(A \Leftrightarrow B)] = 1 - (\phi[A] - \phi[B])^2$.

Example: With the interpretation in which P is true and Q is false, the sentence $Q \Rightarrow (P \wedge (P \Rightarrow Q))$ is true. The sentence $\neg(P \wedge Q) \Rightarrow \neg P$ is false.

The first calculation is easy, all one needs is the value $\phi[Q] = 0$. The result is $\phi[Q \Rightarrow (P \wedge (P \Rightarrow Q))] = \max[1 - 0, \phi[P \Rightarrow (P \Rightarrow Q)] = 1$.

The second calculation is more intricate. Compute $\phi[\neg(P \wedge Q) \Rightarrow \neg P] = \max[1 - \phi[P \wedge Q], 1 - \phi[P]]$. Since $\phi[P] = 1$ we have $\phi(P \wedge Q) = \min[1, 0] = 0$. So this is $\max[0, 0] = 0$.

2.5 Tree structure of formulas

Another way to think of a formula of propositional logic is as a rooted tree. The original formula is the root, and the successors are the constituent formulas. The immediate successors are defined by the last logical operation that was used.

In the following discussion the propositional connectives are $\wedge, \vee, \Rightarrow$, and $\neg$. As usual, we omit writing outermost parentheses.

Example: Take the formula $Q \Rightarrow (P \wedge (P \Rightarrow Q))$. This is the root. The last operation used to construct was the first implication, so the immediate successors of the root are Q and $P \wedge (P \Rightarrow Q)$. The Q is an end element, but $P \wedge (P \Rightarrow Q)$ is a conjunction. Its immediate successors are P and $P \Rightarrow Q$. Finally, the implication $P \Rightarrow Q$ has two immediate successors P, Q.

Example: Consider $\neg(P \wedge Q) \Rightarrow \neg P$. This is an implication. The immediate successors are the negations $\neg(P \wedge Q)$ and $\neg P$. The first of these has immediate successors the conjunction $P \wedge Q$ and finally P, Q. The second has immediate successor P.

These trees have been constructed so that the end elements are atomic sentences. This gives a nice way of describing the truth value of the root formula in an interpretation. The idea is to start with the end elements, whose truth values are given. Then work toward the root, finding the truth value of each element from the truth value of its immediate successors.

Each formula of propositional logic is either atomic or is a formula corresponding to one of the connectives. The connective is the last one that was used to construct the formula. So even if a formula is very complicated, then it makes sense to say that the formula is a conjunction or disjunction or implication or negation.

2.6 Logical implication

To know whether a formula is true or false, one needs to know the truth or falsity of the constituent atomic sentences. In a specific situation one would need some empirical data to get this information. However, in logic one looks for results that do not depend on the state of the world. This leads to another kind of semantics, the semantics of *logical implication*.

If A, C are formulas, then the logical implication $A \models C$ means that for every interpretation in which A is true it is also the case that C is true. There is also a more general notion in which several hypotheses lead logically to a certain conclusion. Thus, if A, B, C are formulas, then the logical implication $A, B \models C$ means that in every interpretation in which A, B are both true, it is also the case that C is true. (The observant reader will notice that the comma plays a role rather similar to that of the "and" conjunction. This is often the case in mathematics.) The other extreme is when there are no hypotheses. In this case it is conventional to write $\models B$ to mean that B is true in every interpretation.

Example: Take $P, P \Rightarrow Q \models Q$. If Q is true, then there is no problem. If P is false, then there is also no problem. The only issue is when P is true and Q is false. But then $P \Rightarrow Q$ is false, so again there is no problem.

Example: Take $\models P \vee \neg P$. There are only two possible interpretations of P, and $P \vee \neg P$ is true in each of them.

There is an interesting relation between logical implication and implication: $A \models B$ is equivalent to $\models A \Rightarrow B$.

There is another related concept. The logical equivalence $A \equiv B$ means that in every interpretation ϕ we have that A is true if and only if B is true. It is not hard to see that $A \equiv B$ is equivalent to $\models A \Leftrightarrow B$.

Example: It would be incorrect to say that $P \wedge (P \Rightarrow Q)$ is logically equivalent to Q. For instance, if we take an interpretation in which P is false and Q is true, then $P \wedge (P \Rightarrow Q)$ is false and the Q is true. On the other hand, it is true that $\neg(P \vee Q) \equiv (\neg P \wedge \neg Q)$.

One way to check a logical implication is semantically, examining all possible interpretations, but this is tedious. There are, however, general syntactic principles, such as the following:

$A, A \Rightarrow B \models B$.

This rule is called *modus ponens*. This is Latin for "mode of putting." Say that $A \Rightarrow B$ is known. The most straightforward way to draw a conclusion is to put down A. In that case B follows logically.

Such a general principle can have powerful consequences. For instance, one consequence is that $(P \vee Q) \wedge ((P \vee Q) \Rightarrow (R \wedge \neg S)) \models R \wedge \neg S$. If we wanted to check this by looking at all interpretations of atomic sentences, then one would have to attach to each of P, Q, R, S a truth value 0 or 1, and there would be $2^4 = 16$ such interpretations.

Here are some famous logical equivalences in propositional logic:

The law of *double negation* states that

$$\neg\neg A \equiv A. \tag{2.1}$$

De Morgan's laws for connectives state that

$$\neg(A \wedge B) \equiv \neg A \vee \neg B \tag{2.2}$$

and that

$$\neg(A \vee B) \equiv \neg A \wedge \neg B. \tag{2.3}$$

Implication may be defined in terms of other connectives by

$$A \Rightarrow B \equiv \neg A \vee B. \tag{2.4}$$

An implication is logically equivalent to its contrapositive, that is,

$$A \Rightarrow B \equiv \neg B \Rightarrow \neg A. \tag{2.5}$$

Problems

1. Find the formation tree of $((P \Rightarrow Q) \wedge (Q \Rightarrow \neg P)) \Rightarrow (P \vee Q)$. What kind of sentence is it?

2. Find the truth value of the preceding sentence when P has value 0 and Q has value 1. Also, find the truth value of the preceding sentence when P has value 0 and Q has value 0.

3. Find the truth value of $(P \Rightarrow R) \Rightarrow ((P \Rightarrow Q) \wedge (Q \Rightarrow R))$ for each of the eight truth valuations.

4. By examining each of the eight truth valuations, prove that it is the case that $\models ((P \Rightarrow Q) \wedge (Q \Rightarrow R)) \Rightarrow (P \Rightarrow R)$.

5. Is it true that $\neg(P \wedge Q) \models \neg P \vee \neg Q$? Prove that your answer is correct.

6. Is it true that $\neg(P \wedge Q) \models \neg P \wedge \neg Q$? Prove that your answer is correct.

7. Is it the case that $P \vee Q, P \Rightarrow \neg R, Q \Rightarrow \neg R \models \neg R$. Give a proof.

8. Is the following reasoning logically valid. Either I'll try this problem or I'll go have a coffee. If I try I won't get it. But if I go have a coffee then I certainly won't get it. So I won't get it.

9. Is it the case that $(P \vee Q) \Rightarrow R, \neg P, \neg Q \models \neg R$. Give a proof.

10. How about the following reasoning? *If logic is part of mathematics or part of philosophy, then it is a scientific field. But logic is not part of mathematics, neither is it part of philosophy. So it is not a scientific field.*

Chapter 3

Property logic

3.1 Syntax of property logic

The basic ideas of propositional logic are rather simple. The formulas are sentences, and all one has to do is to attach to each atomic sentence a truth value, and the rest is determined.

In property logic a formula has a more complex structure. An atomic formula has a subject and a predicate. As a start, consider the case when the subject is a variable. Thus a typical atomic formula might be "x happy", which says that an unspecified individual is happy. Consider a population (say of people) and an interpretation of the predicate "happy". It is not immediately clear whether this formula should be true or false in this interpretation, since this would seem to depend on which individual in the population is denoted by x. A slightly more complicated formula is $\forall x\, x$ happy. This is says that everyone is happy. In a given interpretation this formula is either true or false. It is true if everyone in the population is happy, and it is false if there is an unhappy individual.

A peculiarity of this example is that the truth or falsity of $\forall x\, x$ happy does not depend on any information about x. The x in such a context is called a bound variable. This usage of bound variables in sentences is unusual in English, but it is rather standard in mathematics. In English the closest equivalent might be "For every individual under consideration, that individual is happy." More likely we would say "Everyone is happy".

In property logic we have a choice of language. It is determined by a list of property symbols $p, q, r, \ldots$. For instance, we could tell a story about a population of individuals who could each be describes as happy, rich, or wise.

In logic it is customary to have variables such as x, y, z that are allowed to stand for various objects. For at least certain aspects of property logic it is possible to get by with only one variable x. Then an atomic formula is of the form $x\,p$, where p is a property symbol.

We may combine formulas with the same propositional connectives as before. However now we may make new formulas with quantifiers.

All If A is a formula, then $\forall x\, A$ is a formula.

Exists If A is a formula, then $\exists x\, A$ is a formula.

Example: Take A to be the sentence x happy. Then $\forall x\, x$ happy is also a formula. It says that everyone is happy.

Example: A quantifier may be placed in front of a formula to make a new formula. Thus $\forall x\, 2 + x = 5$ is a formula, one that in the usual mathematical interpretation would be regarded as false. On the other hand, $\forall x\, 2 + z = 5$ is a legitimate but rather odd formula. It turns out to be logically equivalent to the formula $2 + z = 5$ without the quantifier. Such a formula is true or false depending on what value is assigned to z.

Example: For a more complicated case, take B to be the formula x happy $\wedge$ $\neg x$ rich. (Here again the convention is that the outermost parentheses are omitted.) Then $\exists x\, B$ is the formula $\exists x\, (x$ happy $\wedge \neg x$ rich). This is the classic but improbable story about an individual who is happy but poor. Notice that it is important that we restore the parentheses. Otherwise, we would get a different formula: $\exists x\, x$ happy $\wedge \neg x$ rich. This would say that there is a happy individual, and, furthermore, somebody called x is poor. Yet another variation is $\exists x\, x$ happy $\wedge\, \exists x\, \neg x$ rich. (Again outermost parentheses are omitted.) This says that there is a happy individual and there is also a poor individual. They may or may not be the same.

Example: How about the formulas $\exists x\, \exists x\, (x$ happy$\wedge\neg x$ rich) and $\exists x\, (\exists x\, x$ happy$\wedge$ $\exists x\, x$ rich)? They both seem odd, but such formulas are allowed by the rules. The initial existential quantifier is superfluous in both examples. On the other hand, $\exists x\, (\exists x\, x$ happy $\wedge\, x$ rich) is logically equivalent to $\exists x\, x$ happy $\wedge\, \exists x\, x$ rich.

It may seem odd to have a formula where the same variable is used both as a free variable and as a bound variable, as in $\exists x\, x$ happy $\wedge\, x$ rich. While the formula is legitimate, it would certainly be more clear to write this in the equivalent form $\exists y\, y$ happy $\wedge\, x$ rich. One way out would be to use two alphabets, one for free variables and one for bound variables. But this is not usual mathematical practice. The present convention at least has the nice feature that the rules for formation of formulas are simple and uniform.

A final important observation is that each formula of property logic has a tree structure. The original formula is the root. The immediate successors of a formula on the tree are obtained by using the appropriate formation rule to decompose the formula into parts. The end points of the tree are the atomic formulas.

3.2 Lore of quantifiers

The quantifiers $\forall$ and $\exists$ are often called the *universal quantifier* and *existential quantifier*.

Here are various equivalent ways of expressing the same mathematical ideas. The universal quantified formula $\forall x\, A$ could also be written

for all x A

for each x A

for every x A.

The existential quantified formula $\exists x\, A$ may be expressed by

there exists x with A

for some x A.

Warning: It is wise to avoid the expression

for any x A.

The English word "any" does not serve as a quantifier, even in mathematics. It does have a legitimate use, but this is complicated enough to deserve an extended discussion. This will be given in a later section.

3.3 Semantics of property logic

The semantics of property logic is still comparatively simple. The fundamental notion is a *domain*, which is a non-empty set. The domain could consist of people or experimental outcomes or of natural numbers. These are the objects that one intends to talk about.

One way to define an interpretation is to have each property symbol determine a subset of D. Thus, if p, q, r are property symbols, then there are three corresponding subsets of D. Depending on the interpretation they may overlap in various ways.

Sometimes in future work it will be convenient replace a subset of D by its indicator function. This is the function defined on D with values in the set $\{0, 1\}$ that has the value 1 on the subset and 0 on its complement. Clearly, there is a one-to-one correspondence between subsets of D and functions from D to $\{0, 1\}$. Which representation is used is a matter of convenience.

For the moment, define the interpretation of a property symbol p to be a subset of D. A property symbol by itself is not a formula, so this is only a start on the project of interpreting formulas.

Consider an atomic formula such as $x\, p$. This says that x has property p, but what is x? It is possible to assign x to stand for various elements of D, and the truth of $x\, p$ may depend on the assignment. Thus

$x\, p$ is true for an assignment to variable x of the value d provided that d is in the subset corresponding to p in the interpretation.

Example: As an example, take the formula x happy. Suppose the domain D has five individual. Call them a, b, c, d, e. Suppose a, b, d are the happy individuals. Then x happy is true for an assignment to x of one of the values

a, b, d, and x happy is otherwise false. Suppose a, b, e are the rich individuals. Then x happy $\wedge \neg x$ rich is true when the assignment to x has value d and is otherwise false.

Now consider a formula $\forall x\, A$. This formula is true in an interpretation if and only if A is true for every assignment to x of an element of D. For instance, $\forall x\,(x$ happy $\wedge \neg x$ rich) is false in the above interpretation.

Similarly, consider a formula $\exists x\, A$. This formula is true in an interpretation if and only if A is true for some assignment to x of an element of D. For instance, $\exists x\,(x$ happy $\wedge \neg x$ rich) is true in the above interpretation.

3.4 Logical implication

As before, we write $A, B \models C$ to mean that for every interpretation (and every assignment to x of an element of the domain), if A, B are true, then C is also true.

To prove a logical implication like this, it would seem that one needs to examine all interpretations. However, it turns out that one only needs to examine types of interpretations. Say, for instance, that one has a atomic property symbols $p_1, \ldots, p_k$. For each point in the domain D, there is a propositional interpretation which is a list of k zeros and ones. The *type* of the interpretation is the set of all such propositional interpretations that occur. Since D is non-empty, this set must be non-empty. (This notion of "type" is perhaps not standard terminology, but it is convenient for our purposes.) It turns out that the type of the interpretation is the only information that is needed to check truth in property logic.

There are 2^k propositional interpretations. Write $n = 2^k$. Then there are $2^n - 1$ non-empty subsets. So the number of types to be checked is

$$N(k) = 2^n - 1, \tag{3.1}$$

where $n = 2^k$.

For $k = 1$ there are three types of interpretations. They are $\{0, 1\}, \{0\}, \{1\}$. Thus p_1 is sometimes true and sometimes false, or p_1 is always false, or p_1 is always true. These are the only possibilities.

For $k = 2$ there are $2^4 - 1 = 15$ types of interpretations. They are listed here:

$$\begin{array}{cccccc}
\{00,01,10,11\} & & & & & \\
\{01,10,11\} & \{00,10,11\} & \{00,01,11\} & \{00,01,10\} & & \\
\{00,01\} & \{00,10\} & \{00,11\} & \{01,10\} & \{01,11\} & \{10,11\} \\
\{00\} & \{01\} & \{10\} & \{11\} & &
\end{array} \tag{3.2}$$

Checking truth in 15 cases is tedious but routine. It is often easy to find shortcuts.

Example: Take the assertion that $\forall x\,(p(x) \wedge q(x)) \models \forall x\, p(x)$. The left hand side is true in just one type of interpretation, namely $\{11\}$. The right hand side is true in three types of interpretations, namely $\{10, 11\}, \{10\}, \{11\}$. However, the interpretation that makes the left hand side true is included among the interpretations that make the right hand side true, and this is sufficient to prove the logical implication.

For $k = 3$ (the case of the Aristotelian syllogism) there are $2^8 - 1 = 255$ types of interpretations. In this case using the classification into types may be a silly way to proceed, but it should work in principle. In practice one uses the method of Venn diagrams. This simply means that one sketches the subsets and uses the hypotheses to rule out certain cases. Then one checks that the remaining cases force the conclusion to be true.

3.5 The syllogism

The logic of Aristotle ruled for almost two thousand years. Particular emphasis was placed on sentences of the following forms.

A $\forall x\,(x\,s \Rightarrow x\,p)$

I $\exists x\,(x\,s \wedge x\,p)$

E $\forall x\,(x\,s \Rightarrow \neg x\,p)$

O $\exists x\,(x\,s \wedge \neg x\,p)$

These are universal and existentially quantified sentences concerning property p (or its negation) with restrictions imposed by the property s. The implication goes with the universal quantifier, and the conjunction goes with the existential quantifier. This is the standard pattern for restrictions.

Note that $O \equiv \neg A$ and $E \equiv \neg I$. Furthermore, I and E are symmetric in the two properties.

The triumph of Aristotelian logic was the list of syllogisms. These are inferences where two sentences of this general type imply a third such sentence. For instance, a syllogism with the name Ferio states that the hypothesis $\forall x\,(x\,m \Rightarrow \neg x\,p)$ together with the hypothesis $\exists x\,(x\,s \wedge x\,m)$ logically implies the conclusion $\exists x\,(x\,s \wedge \neg x\,p)$.

There are quite a number of such syllogisms, so it is useful to have an abbreviated way of writing them. For instance, for Ferio we could write $mEp, sIm \models sOp$. Certain of the syllogisms require an extra hypothesis of the form $\exists x\, x\, m$. This will be abbreviated by $\exists m$.

There is a list of syllogisms in Table 1. They are classified into four figures, according to the pattern in which the properties occur. Within each figure each syllogism has a name that is intended to help recall the kind of sentence that occurs. For instance, for Ferio the vowels e,i,o indicate the structure E,I,O of the three sentences.

These syllogisms may all be proved semantically in a simple way. Take again

1	Barbara		mAp	sAm	sAp
1	Celarent		mEp	sAm	sEp
1	Darii		mAp	sIm	sIp
1	Ferio		mEp	sIm	sOp
2	Cesare		pEm	sAm	sEp
2	Camestres		pAm	sEm	sEp
2	Festino		pEm	sIm	sOp
2	Baroco		pAm	sOm	sOp
3	Darapti	∃ m	mAp	mAs	sIp
3	Disamis		mIp	mAs	sIp
3	Datisi		mAp	mIs	sIp
3	Felapton	∃ m	mEp	mAs	sOp
3	Bocardo		mOp	mAs	sOp
3	Ferison		mEp	mIs	sOp
4	Bramantip	∃ p	pAm	mAs	sIp
4	Camenes		pAm	mEs	sEp
4	Dimaris		pIm	mAs	sIp
4	Fesapo	∃ m	pEm	mAs	sOp
4	Fresison		pEm	mIs	sOp

Table 3.1: Aristotelian syllogisms

the example of Ferio. Suppose that $\forall x\,(x\,m \Rightarrow \neg x\,p)$ and $\exists x\,(x\,s \wedge x\,m)$ are both true. Then there is an element of the domain that makes both s and m true. However every element of the domain for which m is true is also an element of the domain for which p is false. So the element of the domain that makes s and m true also makes s true and p false. This implies that $\exists x\,(x\,s \wedge \neg x\,p)$ is true.

On the other hand, not every triple of sentences gives a logical implication. Take, for instance, the example that might be called anti-Ferio, in which the hypotheses are the same, but the conclusion is to be $\exists x\,(x\,s \wedge x\,p)$. In other words, the pattern is mEp, SIm, sIp. A counterexample may be constructed by taking a domain with exactly one element, for which s, m are both true, but p is false.

Aristotle's theory of syllogisms is very special. The modern theory presented in the following chapters is much more general and powerful, and now the only role that the Aristotelian theory plays is historical.

3.6 Constants

Property logic as presented above is rather limited, in that the language is built out of property symbols that serve as verbs, but there are no proper nouns. It is easy to augment the language to include proper nouns. In logic these are called constants. For instance, the language could have constants a, b, c. If the language is talking about people, the constants could be Alice, Bob, Carol.

The only syntactic change is that there is a new way of forming sentences. If a is a constant, and p is a property symbol, then $a\,p$ is a sentence. For instance, if "Alice" is a proper noun of the language, and "rich" is a property that individuals may or may not have, then "Alice rich" is the statement that the individual named Alice is indeed rich.

There is also a semantic change. In an interpretation in domain D, each property symbol is interpreted as a subset of D. Each constant is interpreted as an element of D. So $a\,p$ is true when the object denoted by a belongs to the subset designated by p.

Again there is a classification of interpretations into types. Say that we have property symbols $p_1, \ldots, p_k$ and constant symbols $a_1, \ldots, a_m$. There are $n = 2^k$ possible propositional interpretations of $p_1, \ldots, p_k$. The number of property interpretations for which i of these propositional interpretations occur is the number of i element subsets $\binom{n}{i}$. In such a situation there are i^m essentially different ways of interpreting the constants. So the total number of property plus constant interpretations is

$$N(k, m) = \sum_{i=1}^{n} i^m \binom{n}{i}, \tag{3.3}$$

where $n = 2^k$.

As a special case, take the case $m = 1$ of one constant symbol. Then each property interpretation corresponds to a subset together with a designated element. Alternatively, one can think of such a property interpretation as consisting of the element indexed by the subset. In other words, it is the disjoint union of the elements. The total number is

$$N(k, 1) = \sum_{i=1}^{n} i \binom{n}{i} = n2^{n-1}, \tag{3.4}$$

with $n = 2^k$. One way to verify this formula is to note that for each of the n elements there are 2^{n-1} subsets with this element in it.

As an example, take $k = 2$ and $m = 1$. Then $N(2, 1) = 32$. A classic application is the inference: All men are mortal, Socrates is a man $\models$ Socrates is mortal. The domain is presumably men (humans) and gods. The 32 interpretations of the two property symbols and the one constant correspond to the 32 elements in the disjoint union of the sets in (3.2).

The first premise says that the subset of men is included in the subset of mortals. This excludes the possibility that there is an 10 element in the domain. So the 12 remaining interpretations correspond to the elements of the disjoint union of $\{00, 01, 11\}, \{00, 01\}, \{00, 11\}, \{01, 11\}, \{00\}, \{01\}, \{11\}$. The second premise says that the individual called Socrates belongs to the subset of men. This narrows it down to the four configurations where Socrates has the 11 place in $\{00, 01, 11\}, \{00, 11\}, \{01, 11\}, \{11\}$. In all cases Socrates is mortal.

Problems

1. Find the formation tree of the sentence (1) $\forall x\,(x \text{ rich} \Rightarrow x \text{ happy})$.
2. Find the formation tree of the sentence (2) $\forall x\, x \text{ rich} \Rightarrow \forall x\, x \text{ happy}$.
3. Find an interpretation in which (1) is true and (2) is true.
4. Find an interpretation in which (1) is false and (2) is true.
5. Find an interpretation in which (1) is false and (2) is false.
6. Show that $\exists x\, x \text{ rich}, \forall x\,(x \text{ rich} \Rightarrow x \text{ happy}) \models \exists x\, x \text{ happy}$ is true.
7. Show that $\exists x\, x \text{ happy}, \forall x\,(x \text{ rich} \Rightarrow x \text{ happy}) \models \exists x\, x \text{ rich}$ is not true.

Chapter 4

Predicate logic

4.1 Syntax of predicate logic

Propositional logic is the logic of combining sentences. The only semantic notion is that of a sentence being true or false.

Property logic is the logic of sentences with subjects and verbs. The verbs express properties. The semantic notion in this case is that of a subset of a domain set.

Relational logic is the logic of subjects and verbs and objects. In this kind of logic formulas may describe the relation between two objects. Thus "Tony loves Maria" is a formula that describes a relation between two people. Similarly, $5 < 2$ is a formula that describes a relation between two numbers. Both these sentences happen to be false: the first one in the interpretation of West Side Story, the second one in the interpretation of natural numbers. Nevertheless, they are legitimate logical expressions. The relevant semantic notion is the notion of relation on a domain set.

The general notion of *predicate logic* includes these various kinds of logic. A specification of an object language includes a choice of certain *predicate symbols*. A zero-place predicate symbol is a propositional symbol. A one-place predicate symbol is a property symbol. A two-place predicate symbol is a relation symbol. In principle one could allow three-place predicate symbols and so on, but these are rare in mathematics. Once there is at least one two-place predicate symbol, then logic becomes non-trivial.

Example: One useful 0-place symbol is $\bot$, which is interpreted as always false. Here is a 1-place symbol in arithmetic: even. For a 2-place symbol take: $<$.

The other ingredient in the language is a set V of *variables* $x, y, z, x', y', z', \ldots$. Ordinarily we think of this as an infinite list, though in any one argument we are likely to use only finitely many variables.

4.2 Terms

It is possible to do logic and even substantial mathematics in a system where the only terms are variables. However it is often convenient to allow more complicated terms. These are constructed from a new set of *function symbols*. These may be 0-place function symbols, or constants. These stand for objects in some set. Or they may be 1-place functions symbols. These express functions from some set to itself, that is, with one input and one output. Or they may be 2-place function symbols. These express functions with two inputs and one output.

Example: Here are symbols that occur in arithmetic. Constant symbol: 8. 1-place function symbol: square. 2-place function symbol: +.

Once the function symbols have been specified, then one can form *terms*. An *atomic term* is a variable or a constant symbol. These are the building blocks for general terms, according to the following scheme.

Variable Each variable is a term.

Constant Each constant symbol is a term.

Function symbol: 1 input If t is a term, and f is a 1-place function symbol, then $f(t)$ is a term.

Function symbol: 2 inputs If s and t are terms, and g is a 2-place function symbol, then $g(s, t)$ or $(s\, g\, t)$ is a term.

Example: In an language with constant terms $1, 2, 3$ and 2-place function symbol + the expression $(x + 2)$ is a term, and the expression $(3 + (x + 2))$ is a term.

Convention 4.1 *Omit outer parentheses used with a two-place function symbol* $(s\, g\, t)$*. That is, in this context* $s\, g\, t$ *abbreviates* $(s\, g\, t)$*. Restore the parentheses when such a term is used as part of another term.*

Example: With this convention $x + 2$ abbreviates $(x + 2)$, while $3 + (x + 2)$ abbreviates $(3 + (x + 2))$.

Once the terms have been specified, then the *atomic formulas* are determined.

Propositional formula A propositional symbol is an atomic formula.

Property formula If p is a property symbol, and t is a term, then $t\, p$ is an atomic formula.

Relational formula If s and t are terms, and r is a relation symbol, then $s\,r\,t$ is an atomic formula.

Example: The relational formula $(x+2) < 3$ is an atomic formula. This could be abbreviated $x + 2 < 3$.

4.3 Formulas

Finally there are logical symbols. Each of $\wedge$, $\vee$, $\Rightarrow$, $\neg$ is a logical *connective*. The $\forall$, $\exists$ are each a *quantifier*. Once the atomic formulas are specified, then the other *formulas* are obtained by logical operations. For instance $\exists x\, x + 2 < 3$ is an existential formula.

And If A and B are formulas, then so is $(A \wedge B)$.

Or If A and B are formulas, then so is $(A \vee B)$.

Implies If A and B are formulas, the so is $(A \Rightarrow B)$.

Not If A is a formula, then so is $\neg A$.

All If x is a variable and A is a formula, then so is $\forall x\, A$.

Exists If x is a variable and A is a formula, then so is $\exists x\, A$.

In writing a formula, we often omit the outermost parentheses. However this is just an abbreviation. The parentheses must be restored when the formula is part of another formula.

4.4 Free and bound variables

In a formula each occurrence of a variable is either free or bound. The occurrence of a variable x is *bound* if it is in a subformula of the form $\forall x\, B$ or $\exists x\, B$. (In mathematics there are other operations, such as the set builder construction, that produce bound variables.) If the occurrence is not bound, then it is *free*. A formula with no free occurrences of variables is called a *sentence*.

In general, a bound variable may be replaced by a new bound variable without changing the meaning of the formula. Thus, for instance, suppose that there are free occurrences of the variable y in formula B. Suppose that y' is a variable that does not occur in the formula, and let C be the result of replacing the free occurrences of y by y'. Then $\forall y\, B$ should have $\forall y'\, C$ as a logical equivalent.

Example: Let the formula be $\exists y\, x < y$. This says that there is a number greater than x. In this formula x is free and y is bound. The formula $\exists y'\, x < y'$ has the same meaning. In this formula x is free and y' is bound. On the other hand, the formula $\exists y\, x' < y$ has a different meaning. This formula says that there is a number greater than x'. Finally, the sentence $\forall x\, \exists y\, x < y$ says that for every number there is a bigger number.

We wish to define *careful substitution* of a term t for the free occurrences of a variable x in A. The resulting formula will be denoted $A_x(t)$ There is no particular problem in defining substitution in the case when the term t has no variables that already occur in A. The care is needed when there is a subformula in which y is a bound variable and when the term t contains the variable y. Then mere substitution might produce an unwanted situation in which the y in the term t becomes a bound variable. So one first makes a change of bound variable in the subformula. Now the subformula contains a bound variable y' that cannot be confused with y. Then one substitutes t for the free occurrences of x in the modified formula. Then y will be a free variable after the substitution, as desired.

Example: Let the formula be $\exists y\, x < y$. Say that one wished to substitute $y+1$ for the free occurrences of x. This should say that there is a number greater than $y + 1$. It would be wrong to make the careless substitution $\exists y\, y + 1 < y$. This statement is not only false, but worse, it does not have the intended meaning. The careful substitution proceeds by first changing the original formula to $\exists y'\, x < y'$. The careful substitution then produces $\exists y'\, y + 1 < y'$. This says that there is a number greater than $y + 1$, as desired. The sentence that says that for every number there is one that exceeds it by more than 1 is then $\forall y\, \exists y'\, y + 1 < y'$.

The general rule is that if y is a variable with bound occurrences in the formula, and one wants to substitute a term t containing y for the free occurrences of x in the formula, then one should change the bound occurrences of y to bound occurrences of a new variable y' before the substitution. This gives the kind of careful substitution that preserves the intended meaning.

It might be convenient to have two lists of variables, with the variables in one list only used as free variables, and with the variables in the other list only used as bound variables. For instance, one could take Latin letters for free variables and Greek letters for bound variables. There would never be any issue about careful substitution. One could substitute $y + 1$ for x in $\exists \beta\, x < \beta$ to get $\exists \beta\, y + 1 < \beta$. The sentence described in the example would then be $\forall \alpha\, \exists \beta\, \alpha + 1 < \beta$. It would be tempting to adopt such a system for formulating results of logic. For better or worse, it is not the custom in mathematics.

4.5 Restricted variables

Often a quantifier has a restriction. Let C be a formula that places a restriction on the variable x. (Thus C could be a formula like $x > 0$.) The restricted universal quantifier is $\forall x\, (C \Rightarrow A)$. The restricted existential quantifier is $\exists x\, (C \wedge A)$.

It is common to have implicit restrictions. For example, say that the context of a discussion is real numbers x. There may be an implicit restriction $x \in \mathbb{R}$. Since the entire discussion is about real numbers, it may not be necessary to make this explicit in each formula. This, instead of $\forall x\,(x \in \mathbb{R} \Rightarrow x^2 \geq 0)$ one would write just $\forall x\, x^2 \geq 0$.

Sometimes restrictions are indicated by use of special letters for the variables. Often i, j, k, l, m, n are used for integers. Instead of saying that m is odd if and only if $\exists y\,(y \in \mathbf{N} \wedge m = 2y + 1)$ one would just write that m is odd if and only if $\exists k\, m = 2k + 1$.

The letters ϵ, δ are used for strictly positive real numbers. The corresponding restrictions are $\epsilon > 0$ and $\delta > 0$. Instead of writing $\forall x\,(x > 0 \Rightarrow \exists y\,(y > 0 \wedge y < x))$ one would write $\forall \epsilon \exists \delta\, \delta < \epsilon$.

Other common restrictions are to use f, g, h for functions or to indicate sets by capital letters. Reasoning with restricted variables should work smoothly, provided that one keeps the restriction in mind at the appropriate stages of the argument.

4.6 Semantics of predicate logic

The semantics of predicate logic is not difficult but can be frustrating to grasp. Here is a quotation from a book on model theory [12] that captures the dilemma.

> One of the author's worst fears, ever since he has been teaching elementary logic, has been of portraying model theorists as simple-minded. "Not-f" is true if and only if f is not true, "there exists x such that f" is true if and only if there exists an x such that f, etc.... Do we go through this complicated formalism just to duplicate common sense? Yet even the definition of truth necessarily involves such complexity; in particular, we have to convince ourselves that to determine the truth or falsity of a sentence, we need to consider subformulas that are not sentences.

The symbols of predicate logic may have many interpretations. Each propositional symbol may be treated as true or false. Each property symbol may be treated as a subset of the domain D. Each relational symbol may be treated as a relation between the elements of domain D (a set of ordered pairs).

When a formula has free variables, then the truth value of the formula also depends on a variable assignment. This is an assignment to each variable of an element of the domain D. The truth value only depends on the assignments to the variables that occur free in the formula. The extreme case is that of a sentence, a formula with no free variables. Then the truth value is independent of the variable assignment.

Here is an informal description of the case when the only terms are variables.

And $(A \wedge B)$ is true when A is true and B is true, otherwise false.

Or $(A \vee B)$ is true when A is true or B is true, otherwise false.

Implies $(A \Rightarrow B)$ is true when A is false or B is true, otherwise false.

Not $\neg A$ is true when A is false, otherwise false.

All $\forall x\, A$ is true (for a given variable assignment) if A is true for all possible reassignments to the variable x.

Exists $\exists x\, A$ is true (for a given variable assignment) if A is true for some possible reassignment to the variable x.

4.7 Interpretation of formulas

This section is a more technical description of interpretation of formulas. Let D be a non-empty set (the domain). An *interpretation* attaches to each propositional symbol P a truth value $\phi[P]$ in $\{0, 1\}$. An interpretation attaches to each property symbol p a function $\phi[P]$ from D to $\{0, 1\}$. An interpretation attaches to each relational symbol P a function $\phi[P]$ from $D \times D$ to $\{0, 1\}$.

Let V be the set of variables. A *variable assignment* is a function α from V to D. If α is a variable assignment, x is a variable, and d is an element of the domain D, then α_x^d is a new variable assignment, defined by

$$\begin{aligned} \alpha_x^d(x) &= d \\ \alpha_x^d(y) &= \alpha(y) \text{ if } y \neq x. \end{aligned} \tag{4.1}$$

In other words, one switches the assignment of x to d while leaving the assignments of all other variables alone.

The *interpretation* $\phi[A]$ of a formula A is a function whose input is a variable assignment α and whose output is a truth value $\phi[A](\alpha)$ in $\{0, 1\}$. Here are the interpretations of atomic formulas formed using variables.

Propositional formula $\phi[P](\alpha) = \phi[P]$.

Property formula $\phi[x\, p](\alpha) = \phi[p](\alpha(x))$.

Relational formula $\phi[x\, r\, y] = \phi[r](\alpha(x), \alpha(y))$.
formula.

Here are the interpretations of formulas defined by connectives and quantifiers.

And $\phi[(A \wedge B)](\alpha) = \min[\phi[A](\alpha), \phi[B](\alpha)]$.

Or $\phi[(A \vee B)](\alpha) = \max[\phi[A](\alpha), \phi[B](\alpha)]$.

Implies $\phi[(A \Rightarrow B)](\alpha) = \max[1 - \phi[A](\alpha), \phi[B](\alpha)]$.

Not $\phi[\neg A](\alpha) = 1 - \phi[A](\alpha)$.

All $\phi[\forall x\, A](\alpha) = \min_d \phi[A](\alpha_x^d)$

Exists $\phi[\exists x\, A](\alpha) = \max_d \phi[A](\alpha_x^d)$

The only definitions in the above lists that are not routine are the last two, involving the interpretations of universal and existential formulas. To interpret such a formula for a given variable assignment it is necessary to interpret another formula with many different variable assignments.

It turns out that if a formula is a sentence, then the truth value of the formula does not depend on the variable assignment.

Example: Take the formula $m < n$ with the interpretation that m, n are natural numbers and $<$ is the usual "less than" relation. (The symbol $<$ in the object language denotes the relation $<$ for natural numbers.) The formula $m < n$ is true for variable assignment α if $\alpha(m) < \alpha(n)$. The formula $\exists n\, m < n$ is true for all variable assignments. The sentence $\forall m\, \exists n\, m < n$ is true for all variable assignments. The formula $\exists m\, m < n$ is true for variable assignments α with $\alpha(n) \neq 0$. The sentence $\forall n\, \exists m\, m < n$ is false.

4.8 Interpretation of terms

This section is a rather dull technical distribution of the interpretation of terms constructed from function symbols and of formulas built from terms. This is a process that proceeds in stages.

The first stage is the *interpretation* of a function symbol as a function, according to the following scheme.

Constant $\phi[c]$ is an element of D.

Function symbol: 1 input $\phi[f]$ is a function from D to D.

Function symbol: 2 input $\phi[g]$ is a function from $D \times D$ to D.

The second stage is the *interpretation* $\phi[t]$ of a term t. The result is a function whose input is a variable assignment α and whose output is an element $\phi[t](\alpha)$ in D.

Variable $\phi[x](\alpha) = \alpha(x)$

Constants $\phi[c](\alpha) = \phi[c]$

Function: 1 input $\phi[f(t)](\alpha) = \phi[f](\phi[t](\alpha))$.

Function: 2 inputs $\phi[g(s,t)](\alpha) = \phi[g](\phi[s](\alpha), \phi[t](\alpha))$.

The description above uses prefix notation for defining a 2 input term. With infix notation $(s\, g\, t)$ the interpretation is the same: $\phi[(s\, g\, t)](\alpha) = \phi[g](\phi[s](\alpha), \phi[t](\alpha))$.

The third stage is the interpretation of predicate symbols, which we have seen before. The fourth stage is the interpretation of atomic formulas formed from predicate symbols and terms.

Propositional formula $\phi[P](\alpha) = \phi[P]$.

Property formula $\phi[t\,p](\alpha) = \phi[p](\phi[t](\alpha))$.

Relational formula $\phi[s\,r\,t](\alpha) = \phi[r](\phi[s](\alpha), \phi[t](\alpha))$.

The fifth and final stage is the interpretation of general formulas built using connectives and quantifiers. This follows the same plan as in the previous section.

4.9 Tree structure of terms and formulas

Each formula has a tree structure. The formula itself is the root. For each formula on the tree, the immediate successor formulas are determined by the logical type of the formula. The end points are the atomic formulas. The truth of a formula in a given interpretation as a function of the variable assignment is determined by the truth of the atomic formulas in the interpretation as functions of the variable assignment.

Each term also has a tree structure. The term itself is the root. A term is created by a function symbol together with appropriate terms that serve as symbolic inputs to the function. For each term on the tree, the immediate successor terms are these input terms. The end points are atomic terms, that is, variables and constants. The interpretation of a term in a given interpretation with a given variable assignment is determined by the interpretations of the function symbols (including constants) together with the variable assignment.

The truth of an atomic formula for a given interpretation and variable assignment is determined by the interpretation of the predicate symbol together with the interpretation of the terms in the atomic formula with this variable assignment.

These syntactic trees are rather simple. However the semantics is complicated, because of the fact that the fact that the truth of a quantified formula with a given variable assignment may depend on the truth of constituent formulas with other variable assignments. In other words, it is necessary to understand truth of formulas as functions of variable assignments.

4.10 Logical implication

Let U be a set of formulas, and let C be a formula. Then U *logically implies* C in the semantic sense provided that in every interpretation (and every variable assignment) the truth of all the formulas in U implies the truth of the formula C. In this case we may also say more informally that U *gives* C. The most common symbolic notation for this is $U \models C$. If the members of U are $H_1, \ldots, H_k$, then this is often written in the following form:

$$H_1, \ldots, H_k \models C \tag{4.2}$$

There are interesting special cases. The logical implication $H \models C$ is a relation between two formulas. The logical implication $\models C$ says that C is true in every interpretation (and with every variable assignment). In this case C is said to be *valid*. Notice that $H \models C$ is the same as saying that $H \Rightarrow C$ is valid.

There is also a notion of logical equivalence. We write $A \equiv B$ to mean $A \models B$ and $B \models A$. Notice that $A \equiv B$ is the same as saying that $A \Leftrightarrow B$ is valid.

Here are some useful logical equivalences. *De Morgan's laws for quantifiers* state that

$$\neg\forall x\, A \equiv \exists x\, \neg A \tag{4.3}$$

and

$$\neg\exists x\, A \equiv \forall x\, \neg A. \tag{4.4}$$

Since $\neg(C \Rightarrow A) \equiv (C \wedge \neg A)$ and $\neg(C \wedge A) \equiv (C \Rightarrow \neg A)$, De Morgan's laws continue to work with restricted quantifiers.

An important special case of logical implication is $U \models \bot$. In this case the set U is *unsatisfiable*. There is no interpretation ϕ and variable assignment that makes all the formulas true.

The opposite situation is when there is an interpretation (and variable assignment) that makes all the formulas in U true. In that case U is said to be *satisfiable*. Say that U is a set of sentences and ϕ is an interpretation that makes all the formulas in U true. Then U is satisfied by ϕ. In another terminology, ϕ is a *model* of U. In this account the relation ϕ models U is denoted $\phi \Vvdash U$.

Remark: In model theory it is common to use the symbol $\models$ with a double meaning, to denote semantic logical implication and also to denote the modeling relation that we have called $\Vvdash$. It may seem an excess of caution to introduce the new symbol $\Vvdash$, but it avoids notational awkwardness later on in the treatment of Gentzen deduction.

Problems

1. Consider the formula A: $\forall x\, x$ loves y. Find the result $A_y(z)$ of carefully substituting z for the free occurrences of y in A.

2. Find the result $A_x(z)$ of carefully substituting z for the free occurrences of x in A.

3. Find the result $A_y(x)$ of carefully substituting x for the free occurrences of y in A.

4. Find the result $A_x(y)$ of carefully substituting y for the free occurrences of x in A.

5. Find the formula $\exists y\, A$ and describe the free variables in this formula.

6. Find the formula $\exists y\, A_y(z)$ and describe the free variables in this formula.
7. Find the formula $\exists y\, A_x(z)$ and describe the free variables in this formula.
8. Find the formula $\exists y\, A_y(x)$ and describe the free variables in this formula.
9. Consider the sentences:

   $\forall x \exists y\, x$ loves y

   $\forall x\, \neg x$ loves x

   $\forall x \forall y\, (x$ loves $y \Rightarrow \neg y$ loves $x)$

   Find the smallest number k such that there is a model of these sentences with k elements. Describe the structure of a model with k elements.
10. Prove or disprove:

$$\forall w\, \neg w < w, \forall p \forall q\, (p < q \Rightarrow \neg q < p), \forall u \exists v\, u < v \models \bot$$

Chapter 5

Natural deduction

5.1 Natural deduction principles

The formalization of logic that corresponds most closely to the practice of mathematical proof is *natural deduction*. Natural deduction proofs are constructed so that they may be read from the top down. On the other hand, to construct a natural deduction proof, it is often helpful to work from the top down and the bottom up and try to meet in the middle.

In natural deduction each **Suppose** introduces a new hypothesis to the set of hypotheses. Each matching **Thus** removes the hypothesis. Each line is a claim that the formula on this line follows logically from the hypotheses above that have been introduced by a **Suppose** and not yet eliminated by a matching **Thus** .

Example: If one knows the algebraic fact $\forall x\,(x > 0 \Rightarrow x + 1 > 0)$, then one is forced by pure logic to accept that $\forall y\,(y > 0 \Rightarrow (y + 1) + 1 > 0)$. Here is the argument, showing every logical step. For clarity outermost parentheses are omitted, both in formulas and in terms.

Suppose $\forall x(x > 0 \Rightarrow x + 1 > 0)$
    Suppose $z > 0$
    $z > 0 \Rightarrow z + 1 > 0$
    $z + 1 > 0$
    $z + 1 > 0 \Rightarrow (z + 1) + 1 > 0$
    $(z + 1) + 1 > 0$
Thus $z > 0 \Rightarrow (z + 1) + 1 > 0$
$\forall y\,(y > 0 \Rightarrow (y + 1) + 1 > 0$

The indentation makes the hypotheses in force at each stage quite clear. On the other hand, the proof could also be written in narrative form. It could go like this.

Suppose that for all x, if $x > 0$ then $x + 1 > 0$. **Suppose** $z > 0$. By specializing the hypothesis, obtain that if $z > 0$, then $z + 1 > 0$. It follows that $z + 1 > 0$. By specializing the hypothesis again, obtain that if $z + 1 > 0$, then $(z + 1) + 1 > 0$. It follows that $(z + 1) + 1 > 0$. **Thus** if $z > 0$, then $(z + 1) + 1 > 0$. Since z is arbitrary, conclude that for all y, if $y > 0$, then $(y + 1) + 1 > 0$).

Mathematicians usually write in narrative form, but it is useful to practice proofs in outline form, with proper indentation to show the subarguments.

The only axiom for natural deduction is that if A is among the hypotheses, then A is also a conclusion. Here is an example that uses this *repetition* rule explicitly.

        Suppose Q
                Suppose P
                Q
        Thus $P \Rightarrow Q$
Thus $Q \Rightarrow (P \Rightarrow Q)$

In natural deduction there is only one axiom pattern, the one that says that every formula is a consequence of itself. However there are a number of patterns of inference, given by a rather long set of rules. The nice thing is that these rules are on the whole rather close to those used in mathematical practice.

There is one headache in formulating natural deduction. In addition to the formulas of the object language, one needs a method of indicating what temporary hypotheses are in force at a given stage of the argument. There are many ways of doing this, and the use of **Suppose** and **Thus** pairs are just one possible mechanism. The reason they are used here is that they suggest what one might say in mathematical practice. Logicians have invented all sorts of alternatives, some of them quite at variance with mathematical practice. For instance, they might require that a subargument be placed in a box. Or they might number every hypothesis and at each line give a list of the numbers of the hypotheses that are in force. Or they might write the entire proof as a tree.

It is sometimes required that every line of the proof be accompanied by a justification. This is tedious and ultimately unnecessary, but it is a good idea for beginners to do something like this.

5.2 Rules for natural deduction

There are systematic rules for logical deduction. This section presents these rules. There are twelve rules that occur in pairs, plus a proof by contradiction rule that does not fall into the same pattern.

In each of the paired rules there is a connective or quantifier that is the center of attention. It may be in the hypothesis or in the conclusion, and this explains the pairing. Each rule shows how to reduce an argument involving this logical operation to one without the logical operation. To accomplish this, the rule needs to be used just once, except for the "all in hypothesis" and "exists in conclusion" rules. If it were not for this exception, mathematics would be simple indeed.

Natural deduction also makes use of a *transitivity* rule. Say that certain hypotheses lead to a formula B. Say that in addition these hypotheses, together with B as an additional hypothesis, lead to conclusion C. Then the original hypotheses lead to C. The transitivity rule is very powerful; it allows the use of a formula B that plays the role of a lemma. On the other hand, it may be difficult to find the correct intermediate formula B. The attempt in the following is to try to restrict the use of this rule, in order to avoid or postpone guessing. This can be helpful in simple cases. In real mathematics, however, it is difficult to get by without deeper insight, and finding the correct lemma may be a crucial step.

Here are the natural deduction rules for the logical operations $\wedge$, $\forall$, $\Rightarrow$, $\neg$, and the falsity symbol $\perp$. The rules for $\vee$ and $\exists$ are treated in the following section. Most of these rules gives a practical method for using a hypothesis or for proving a conclusion that works in all circumstances. The exceptions are noted, but the templates of the following chapter provide recipes for these cases too.

In the statement of a rule, the last line is the conclusion. (Exception: In the rule for using "and in hypothesis" it is convenient to draw two conclusions at once.) In some of the rules there is a temporary hypothesis indicated by **Suppose** . This must lead logically to a certain conclusion. The removal of this temporary hypothesis is indicated by **Thus** .

In the natural deduction rules there is a crucial concept of "arbitrary variable." Roughly speaking, at a given stage in a proof a variable is arbitrary if it does not occur as a free variable in any hypothesis (supposition) that is in force at that stage in the proof. Thus if we can start with $x > 1$ and other hypotheses not involving x and derive $\sqrt{x} > 1$, then the x in $\sqrt{x} > 1$ is not arbitrary. But if we only have the other hypotheses, then the x in $x > 1 \Rightarrow \sqrt{x} > 1$ is arbitrary. This is what allows us to generalize to $\forall x\,(x > 1 \Rightarrow \sqrt{x} > 1)$.

And in hypothesis

$A \wedge B$
A
B

And in conclusion

A

B
$A \wedge B$

All in hypothesis (specialization)

$\forall x\, A$
$A_x(t)$

Note: This rule may be used repeatedly with various terms.

All in conclusion (arbitrary variable for generalization)

If z is a variable that does not occur free in a hypothesis in force or in $\forall x\, A$, then

$A_x(z)$
$\forall x\, A$

Note: The restriction on the variable is usually signalled by an expression such as "since z is arbitrary, conclude $\forall x\, A$."

Implication in hypothesis (modus ponens) See template.

$A \Rightarrow B$

A
B

Implication in conclusion

Suppose A

B
Thus $A \Rightarrow B$

The operation of negation $\neg A$ is regarded as an abbreviation for $A \Rightarrow \bot$. Thus we have the following two specializations of the implication rules.

Not in hypothesis See template.

$\neg A$

A
$\bot$

Not in conclusion

Suppose A

$\bot$
Thus $\neg A$

Contradiction

Suppose $\neg C$

$\bot$
Thus C

A contradiction is a formula or set of formulas that leads logically to $\perp$. The rule for proving a negated conclusion says that if supposing A gives a contradiction, then $\neg A$ follows logically. With this rule, the conclusion is always a negation.

Proof by contradiction says that if supposing $\neg C$ gives a contradiction, then C follows logically. This is a famous law with a special status. The other laws start with a hypothesis with a certain logical form, or with a conclusion with a certain logical form. These laws thus occur in pairs. By contrast, in proof by contradiction one is heading for a conclusion C. Nothing is assumed about the logical form of C; it could be an atomic formula. (In a typical situation there is a negated hypothesis $\neg A$, where A can have a complicated logical form, and the goal is to prove C. To do this, temporarily suppose $\neg C$ and attempt to derive A. If this succeeds, then $\neg A$ leads to C.)

Mathematicians sometimes feel that there is something artificial about proof by contradiction and that it should be avoided or postponed. However it or something like it is an essential part of classical logic. Its role will be clarified by the later discussion of Gentzen deduction, which is a form of logical deduction that allows multiple alternative conclusions. In Gentzen deduction the rules occur in pairs; proof by contradiction is not needed.

Intuitionistic logic is a natural and beautiful generalization of classical logic. In intuitionistic logic proof by contradiction is replaced by a weaker rule that says that from $\perp$ one can deduce C. If one has intuitionistic logic in mind, then it is worth trying to avoid proof by contradiction. (Intuitionistic logic is briefly discussed in an appendix.)

5.3 Additional rules for or and exists

So far there are no rules for $A \vee B$ and for $\exists x\, A$. Classical logic could dispense with such rules, because $A \vee B$ could always be replaced by $\neg(\neg A \wedge \neg B)$ and $\exists x\, A$ could be replaced by $\neg \forall x\, \neg A$. Such a replacement is clumsy and is not common practice. Also, it would not work in intuitionistic logic. The following section gives additional rules that explicitly deal with $A \vee B$ and with $\exists x\, A$.

Or in hypothesis (cases)

$A \vee B$

  Suppose A

  C

  Instead suppose B

  C

Thus C

Or in conclusion See template.

A
$A \vee B$

together with

B
$A \vee B$

Exists in hypothesis (arbitrary variable for temporary name)

If z is a variable that does not occur free in a hypothesis in force, in $\exists x\, A$, or in C, then

$\exists x\, A$

  Suppose $A_x(z)$

  C

Thus C

Exists in conclusion See template.

$A(t)$
$\exists x\, A(x)$

The only rule that seems strange to a mathematician is the rule for an existential hypothesis. However it is worth the effort to understand it before taking shortcuts.

In using this rule the restriction on the variable could be signalled by an expression such as "since z is arbitrary, conclude C on the basis of the existential hypothesis $\exists x\, A$." The idea is that if the existential hypothesis is true, then since z is arbitrary the condition on it is true for at least one value of z. So if one can reason from this to a conclusion not depending on z, then one did not need to know what this value might be. So the same conclusion follows from the existential hypothesis alone. The assumption on z did not really matter.

The rule is quite parallel to the rule of proof by cases, the "or in hypothesis" rule. For that rule, if one knows $A \vee B$ is true, then one knows that at least one of the two cases A, B is true. If one can reason from this to a conclusion not depending on which case is true, then it did not matter whether it was A or B that was true. The same conclusion follows from the disjunction alone.

Mathematicians tend not to use this version of the rule in practice. They simply suppose that some convenient variable may be used as a name for the thing that exists. They reason with this name up to a point at which they get a conclusion that no longer mentions it. At this point they conveniently forget the temporary supposition. Logicians have attempted to formulate rules for forgetfulness, but this turns out to be a nuisance. The issue will be discussed later on.

5.4 Examples

A natural deduction proof consists of a list of formulas of the object language. These are augmented with **Suppose** and **Thus** expressions that indicate when hypotheses are introduced or are no longer in force. Other expositions of natural deduction may use somewhat different ways of indicating precisely which hypotheses are needed to obtain a given formula, but the basic device is always the same.

Someone first learning natural deduction may find it useful to annotate each line that does not have a **Suppose** with an indication of which logical rule was used to justify this line as a new conclusion. Such indications are provided in this section, but they are not needed as part of the proof. After all, in principle one could examine all previous conclusions and all possible rules to see if there is a justification.

With experience one should be able to provide natural deduction proofs that are easy to read without such annotations. Even then, it is a considerable kindness to the reader to adopt a convention where **Suppose** — **Thus** pairs are indicated visually by indentation.

Example: Here is a natural deduction proof of the fact that $\neg\exists x\, x$ standard logically implies $\forall x\, \neg x$ standard.

Suppose $\neg\exists x\, x$ standard	
Suppose w standard	
$\exists x\, x$ standard	exists in conclusion
$\perp$	not in hypothesis
Thus $\neg w$ standard	not in conclusion
$\forall x\, \neg x$ standard	all in conclusion

Example: Here is a natural deduction proof of the fact that $\forall x\, \neg x$ standard leads to $\neg\exists x\, x$ standard.

Suppose $\forall x\, \neg x$ standard	
Suppose $\exists x\, x$ standard	
Suppose z standard	
$\neg z$ standard	all in hypothesis
$\perp$	not in hypothesis
Thus $\perp$	exists in hypothesis
Thus $\neg\exists x\, x$ standard	not in conclusion

Example: Here is a degenerate example: a standard gives $a > 0 \Rightarrow a$ standard.

Suppose a standard	
Suppose $a > 0$	
a standard	repeat
Thus $a > 0 \Rightarrow a$ standard	implication in conclusion

Here is another possible style for the notation that indicates which rule is used. The rule for "and in hypothesis" is indicated $\wedge \longrightarrow$; while "and in conclusion" is $\longrightarrow \wedge$. Analogous notation is used for the other pairs. The contradiction rule could be indicated by $\neg\neg \longrightarrow$, since one can think of it in two stages, going from $\neg C$ to $\neg\neg C$ and then to C.

Example:

Here is a proof of the syllogism Baroco.

Suppose $\forall x\,(x\,p \Rightarrow x\,m)$			
Suppose $\exists x\,(x\,s \wedge \neg x\,m)$			
	Suppose $z\,s \wedge \neg z\,m$		
	$z\,s$		$\wedge \longrightarrow$
	$\neg z\,m$		$\wedge \longrightarrow$
	$z\,p \Rightarrow z\,m$		$\forall \longrightarrow$
		Suppose $z\,p$	
		$z\,m$	$\Rightarrow\longrightarrow$
		$\bot$	$\neg \longrightarrow$
	Thus $\neg z\,p$		$\longrightarrow \neg$
	$z\,s \wedge \neg z\,p$		$\longrightarrow \wedge$
	$\exists x(x\,s \wedge \neg x\,p)$		$\longrightarrow \exists$
Thus $\exists x\,(x\,s \wedge \neg x\,p)$			$\exists \longrightarrow$

5.5 Strategies for natural deduction

A natural deduction proof is read from top down. However it is often discovered by working simultaneously from the top and the bottom, until a meeting in the middle. The discoverer obscures the origin of the proof by presenting it from the top down. This is convincing but not illuminating.

Example: Here is a natural deduction proof that $\forall x\,(x \text{ rich} \Rightarrow x \text{ happy})$ leads to $\forall x\,(\neg x \text{ happy} \Rightarrow \neg x \text{ rich})$.

Suppose $\forall x\,(x \text{ rich} \Rightarrow x \text{ happy})$		
	Suppose $\neg w$ happy	
		Suppose w rich
		w rich $\Rightarrow$ w happy
		w happy
		$\bot$
	Thus $\neg w$ rich	
Thus $\neg w$ happy $\Rightarrow \neg w$ rich		
$\forall x\,(\neg x \text{ happy} \Rightarrow \neg x \text{ rich})$		

There are 3 **Suppose** lines and 2 **Thus** lines. Each **Thus** removes a **Suppose** . Since $3 - 2 = 1$, the bottom line follows from the top line alone.

Here is how to construct the proof. Start from the bottom up. To prove the general conclusion, prove the implication for an arbitrary variable. To prove the implication, make a supposition. This reduces the problem to proving a negation. Make a supposition without the negation and try to get a contradiction. To accomplish this, specialize the hypothesis and use modus ponens.

Here is the same proof in narrative form.

Suppose $\forall x\,(x \text{ rich} \Rightarrow x \text{ happy})$. **Suppose** $\neg w$ happy. **Suppose** w rich. Specializing the hypothesis gives w rich $\Rightarrow$ w happy. So w happy. This gives a false conclusion $\bot$. **Thus** $\neg w$ rich. **Thus** $\neg w$ happy $\Rightarrow \neg w$ rich. Since w is arbitrary $\forall x\,(\neg x$ happy $\Rightarrow \neg x$ rich)

Example: Here is a natural deduction proof of the fact that $\exists x\,(x$ happy $\wedge$ x rich) logically implies that $\exists x\, x$ happy $\wedge\, \exists x\, x$ rich.

Suppose $\exists x\,(x$ happy $\wedge$ x rich)
    Suppose z happy $\wedge$ z rich
    z happy
    z rich
    $\exists x\, x$ happy
    $\exists x\, x$ rich
    $\exists x\, x$ happy $\wedge\, \exists x\, x$ rich
Thus $\exists x\, x$ happy $\wedge\, \exists x\, x$ rich

Here is the same proof in narrative form.

Suppose $\exists x\,(x$ happy $\wedge\, x$ rich). **Suppose** z happy $\wedge\, z$ rich. Then z happy and hence $\exists x\, x$ happy. Similarly, z rich and hence $\exists x\, x$ rich. It follows that $\exists x\, x$ happy$\wedge\exists x\, x$ rich. **Thus** , since z is an arbitrary name, the same conclusion holds on the basis of the original supposition of existence.

Example: We could try to reason in the other direction, from the existence of a happy individual and the existence of a rich individual to the existence of a happy, rich individual. What goes wrong?

Suppose $\exists x\, x$ happy$\wedge\exists x\, x$ rich. Then $\exists x\, x$ happy, $\exists x\, x$ rich. **Suppose** z happy. **Suppose** w rich. Then z happy $\wedge$ w rich. This approach does not work.

Here is another attempt at the other direction.

Suppose $\exists x\, x$ happy$\wedge\exists x\, x$ rich. Then $\exists x\, x$ happy, $\exists x\, x$ rich. **Suppose** z happy. **Suppose** z rich. Then z happy$\wedge z$ rich. So $\exists x\,(x$ happy$\wedge x$ rich). So this proves the conclusion, but we needed two temporary hypotheses on z. However we cannot conclude that we no longer need the last temporary hypothesis z rich, but only need $\exists x\, x$ rich. The problem is that we have temporarily supposed also that z happy, and so z is not an arbitrary name for the rich individual. All this proves is that one can deduce logically from z happy, z rich that $\exists x\,(x$ happy$\wedge\, x$ rich). So this approach also does not work.

Example: Here is a natural deduction proof that $\exists y \forall x\, x \leq y$ gives $\forall x \exists y\, x \leq y$.

Suppose $\exists y \forall x\, x \leq y$
    Suppose $\forall x\, x \leq y'$
    $x' \leq y'$
    $\exists y\, x' \leq y$
Thus $\exists y\, x' \leq y$
$\forall x \exists y\, x \leq y$

Here is the same proof in narrative form.

Suppose $\exists y \forall x\, x \leq y$. **Suppose** y' satisfies $\forall x\, x \leq y'$. In particular, $x' \leq y'$. Therefore $\exists y\, x' \leq y$. **Thus** , since y' is just an arbitrary name, this same conclusion follows on the basis of the original existential supposition. Finally, since x' is arbitrary, conclude that $\forall x \exists y\, x \leq y$.

A useful strategy for natural deduction is to begin with writing the hypotheses at the top and the conclusion at the bottom. Then work toward the middle. Try to use the "all in conclusion" rule and the "exists in hypothesis" rule early in this process of proof construction. This introduces new "arbitrary" variables. Then use the "all in hypothesis" rule and the "exists in conclusion" rule with terms formed from these variables. It is reasonable to use these latter rules later in the proof construction process. They may need to be used repeatedly.

Example: Here is a proof that if everyone loves someone, and love is reciprocal, then everyone belongs to a loving pair.

Suppose $\forall x\, \exists y\, x$ loves y
Suppose $\forall x\, \forall y\, (x$ loves $y \Rightarrow y$ loves $x)$
$\exists y\, z$ loves y
  Suppose z loves w
  $\forall y\, (z$ loves $y \Rightarrow y$ loves $z)$
  z loves $w \Rightarrow w$ loves z
  w loves z
  z loves $w \wedge w$ loves z
  $\exists y\, (z$ loves $y \wedge y$ loves $z)$
Thus $\exists y\, (z$ loves $y \wedge y$ loves $z)$
$\forall x\, \exists y\, (x$ loves $y \wedge y$ loves $x)$

The idea of the proof is the following. Everyone loves someone, so z loves someone. Suppose that z loves w. It follows from the assumptions that w loves z. So z loves w and w loves z. Therefore there is someone who z loves and who loves z. This was deduced from the additional supposition that z loves w. However w is arbitrary, so it is free to stand for the individual z loves. So all we really need is that z loves someone to conclude that there is someone whom z loves and who loves z. Since z is arbitrary, it is free to stand for anyone. This shows that there is a loving pair.

5.6 The soundness theorem

The expression $U \models C$ was defined to mean that for every interpretation (and variable assignment), if all the formulas in U are true, then C is true. This is a semantic notion. Let U be a finite set of formulas. If there is a natural deduction proof starting with the hypotheses in U and concluding with C, then we write $U \vdash C$ and say that U *logically implies* C in the syntactic sense. We may also say less formally that that U *gives* C. This is a syntactic notion.

Again there are important special cases of this notion. If $U \vdash \perp$, then U is said to be a *contradiction* or to be *inconsistent.* In the opposite situation the terminology is that U is *consistent.*

The *soundness theorem* says that if $U \vdash C$, then $U \models C$. In other words, it says that the syntactic notion of derivation via natural deduction has consequences for the semantic notion of logical consequence. In particular, if U is a contradiction, then U is unsatisfiable. This proof of this theorem is comes from the fact that the rules of natural deduction were designed at the outset to be rules that lead to logical consequence. It is a rather unexciting result.

The *completeness theorem* due to Gödel is considerably deeper. This theorem says that if $U \models C$, then $U \vdash C$. In other words, the rules of natural deduction are powerful enough to completely characterize logical consequence. The proof and full consequences of the completeness theorem will be the subject of considerable later discussion. A particular case, already highly interesting, is that if U is consistent, then U is satisfiable.

The Gödel completeness theorem is a theorem that says that syntax has implications for semantics. Syntactic logical deduction is *semantically complete* in the sense that it encompasses semantic logical deduction. The Gödel completeness theorem could well be called the *semantic completeness theorem.*

5.7 Lore of free variables

In statements of mathematical theorems it is common to have implicit universal quantifiers. For example, say that we are dealing with real numbers. Instead of stating the theorem that

$$\forall x \forall y \, 2xy \leq x^2 + y^2$$

one simply claims that

$$2uv \leq u^2 + v^2.$$

Clearly the second statement is a specialization of the first statement. But it seems to talk about u and v, and it is not clear why this might apply for someone who wants to conclude something about p and q, such as $2pq \leq p^2 + q^2$. Why is this permissible?

The answer is that the two displayed statements are logically equivalent, provided that there is no hypothesis in force that mentions the variables u or v. Then given the second statement and the fact that the variables in it are arbitrary, the first statement is a valid generalization.

A special case of this type of statement is an *identity* A typical example is

$$(u - v)^2 = u^2 + 2uv + v^2.$$

This is a general equality, but the universal quantifiers are implicit.

This should be contrasted with the situation in *equation solving.* Here is an example. Suppose general principles $\forall z \, (z^2 = 0 \Rightarrow z = 0)$ and $\forall x \forall y \, (x - y = 0 \Rightarrow x = y)$. If the equation is $(u - v)^2 = 0$ we can apply these principles to conclude that $u-v=0$ and hence $u=v$. However $u=v$ cannot be generalized, because it depends on an assumption about u and v. On the other hand, we can conclude

$$(u-v)^2 = 0 \Rightarrow u = v,$$

as a statement subject to universal quantification. In equation solving it is the implication that is general.

There is no similar principle for existential quantifiers. The statement

$$\exists x\, x^2 = x$$

is a theorem about real numbers, while the statement

$$u^2 = u$$

is a condition that is true for $u = 0$ or $u = 1$ and false for all other real numbers. It is certainly not a theorem about real numbers. It might occur in a context where there is a hypothesis that $u = 0$ or $u = 1$ in force, but then it would be incorrect to generalize.

One cannot be careless about inner quantifiers, even if they are universal. Thus there is a theorem

$$\exists x\, x < y.$$

This could be interpreted as saying that for each arbitrary y there is a number that is smaller than y. Contrast this with the statement

$$\exists x \forall y\, x < y$$

with an inner universal quantifier. This is clearly false for the real number system.

Here is a caution for mathematicians. There is no problem with expressions of the form $\forall x\, A$ or "for all x A" or "for every x A" or "for each x A". These are all universal quantifiers. There is also no problem with expressions of the form $\exists x\, A$ or "for some x A" or "there exists x with A". These are all existential quantifiers. The trap to avoid is expressions of the form "for any x A." The word "any" does not function as a quantifier in the usual way.

For example, if one says "z is special if and only if for any singular x it is the case that x is tied to z", it is not clear which quantifier on x might be intended.

The correct usage of the word "any" in mathematical contexts is to indicate a free variable. Consider the following sentences:

Anything is special.

Anything special is exceptional.

There is not anything that is special.

If anything is special, then the conclusion follows.

If the hypothesis is satisfied, then anything is special.

These would be translated as follows:

x special

x special $\Rightarrow$ x exceptional

$\neg$ x special
x special $\Rightarrow$ conclusion
hypothesis $\Rightarrow$ x special

In the typical situation when there is no assumption that specifies x, these are logically equivalent to the universally quantified sentences:
$\forall x$ x special
$\forall x$ (x special $\Rightarrow$ x exceptional)
$\forall x$ $\neg$ x special
$\forall x$ (x special $\Rightarrow$ conclusion)
$\forall x$ (hypothesis $\Rightarrow$ x special)

These in turn are logically equivalent to:
$\forall x$ x special
$\forall x$ (x special $\Rightarrow$ x exceptional)
$\neg$ $\exists x$ x special
$\exists x$ x special $\Rightarrow$ conclusion
hypothesis $\Rightarrow$ $\forall x$ x special

Now return to the first, confusing example. Assuming that there are no conditions imposed on z or x, this is
z special $\Leftrightarrow$ x tied to z

A little thought will establish that this is equivalent to the conjunction of the following two sentences:
z special $\Rightarrow$ $\forall x$ x tied to z
$\exists x$ x tied to z $\Rightarrow$ z special

In this example the word "any" is functioning both as a universal quantifier and as an existential quantifier. This explains why the sentence is so confusing.

Warning to mathematicians: avoid thinking of "any" as a quantifier. Use "all, every" or "exists, some" in statements of theorems. Since theorems have no free variables, this should suffice in all cases.

5.8 Equality

One way to introduce equality is to add axioms of the form

$$\forall x\, x = x$$

and

$$\forall x\, \forall y\, (x = y \Rightarrow (A_z(x) \Rightarrow A_z(y)).$$

The last axioms is actually a list of infinitely many axioms, one for each formula A.

One consequence of these axioms is

$$\forall x\, \forall y\, (x = y \Rightarrow y = x).$$

This may be proved as follows. Suppose $x = y$. Let A be the formula $z = x$. Then $x = y \Rightarrow (x = x \Rightarrow y = x)$. Then $x = x \Rightarrow y = x$. But we always have $x = x$, so $y = x$. Thus $x = y \Rightarrow y = x$.

Another consequence of these axioms is

$$\forall x\, \forall y\, \forall z\, ((x = y \wedge y = z) \Rightarrow x = z)).$$

This may be proved as follows. Suppose $x = y \wedge y = z$. Then $x = y$ and also $y = z$. Let A be the formula $x = w$ and substitute this time for w. Then $y = z \Rightarrow (x = y \Rightarrow x = z)$. Then $x = y \Rightarrow x = z$. Then $x = z$. Thus $(x = y \wedge y = z) \Rightarrow x = z$.

These deductions show that equality is an equivalence relation. It does not follow that equality is interpreted as actual equality. However, it is possible to modify the definition of interpretation to require that equality is interpreted as actual equality. The completeness theorem continues to hold with this revised definition.

Since equality is so fundamental in logic, it may be more natural to think of new rules of inference instead of axioms. In natural deduction the rules would be:

Equality in conclusion

$t = t$

Equality in hypothesis

$s = t$

$A_z(s)$
$A_z(t)$

Problems

The problems here are to be done using natural deduction. Indent. Justify every logical step. Each step involves precisely one logical operation. The logical operation must correspond to the logical type of the formula.

1. Prove that $P \Rightarrow (Q \wedge R) \vdash P \Rightarrow R$.
2. Prove that $P \Rightarrow Q, \neg(P \wedge Q) \vdash \neg P$.
3. Prove that $P \Rightarrow Q, R \Rightarrow \neg Q, P \wedge R \vdash \bot$.
4. Prove that

$$\forall x\, (x \text{ rich} \Rightarrow x \text{ happy}) \vdash \forall x\, x \text{ rich} \Rightarrow \forall x\, x \text{ happy}.$$

5. Prove that

$$\forall z\, z^2 \geq 0, \forall x \forall y\, ((x-y)^2 \geq 0 \Rightarrow 2\cdot(x\cdot y) \leq x^2+y^2) \vdash \forall x \forall y\, 2\cdot(x\cdot y) \leq x^2+y^2.$$

Chapter 6

Natural deduction templates

6.1 Templates

Constructing natural deduction proofs seems to require ingenuity. This is certainly true in complicated situations, but in most examples from elementary logic there is a systematic procedure that makes proof construction rather straightforward. This procedure is to write the hypotheses at the top and the conclusions at the bottom. Then one tries to fill in the middle, working inward. At each stage, the procedure is dictated by picking one of the connectives or quantifiers, in hypothesis or conclusion, and applying the appropriate rule.

In some instances the rules as presented before show how to proceed. But some of these rules leave too much freedom. This section presents templates that show how to use the contradiction rule to remove the imperfections of these excessively flexible rules. These templates are sometimes less convenient, but they always work to produce a proof, if one exists.

The Gödel completeness theorem says that given a set of hypotheses and a conclusion, then either there is a proof using the natural deduction rules, or there is an interpretation in which the hypotheses are all true and the conclusion is false. Furthermore, in the case when there is a proof, it may be constructed via these templates. This will be demonstrated in a later chapter, after the development of Gentzen deduction.

Why does this theorem not make mathematics trivial? The problem is that if there is no proof, then the unsuccessful search for one may not terminate. The problem is with the rule for "all in hypothesis". This may be specialized in more than one way, and there is no upper bound to the number of unsuccessful attempts.

Implication in hypothesis template This template reduces the task of using the hypothesis $A \Rightarrow B$ to obtain C to two tasks: Use $\neg C$ to derive A, use B to derive C.

$A \Rightarrow B$

  Suppose $\neg C$

  A

  B

  C

  $\bot$

Thus C

Negation in hypothesis template This template reduces the task of using the hypothesis $\neg A$ to obtain C to a seemingly equivalent task: Use $\neg C$ to derive A. This reduction is particularly useful when some other rule can be used to derive A.

$\neg A$

  Suppose $\neg C$

  A

  $\bot$

Thus C

Note: The role of this rule to make use of a negated hypothesis $\neg A$. When the conclusion C has no useful logical structure, but A does, then the rule effectively switches A for C.

Or in conclusion template This template reduces the task of proving $A \vee B$ to the task of reasoning from $\neg A \wedge \neg B$ to a contradiction.

Suppose $\neg(A \vee B)$
    Suppose A
    $A \vee B$
    $\perp$
Thus $\neg A$
    Suppose B
    $A \vee B$
    $\perp$
Thus $\neg B$
$\neg A \wedge \neg B$

$\perp$
Thus $A \vee B$

Exists in conclusion template This template reduces the task of proving $\exists x\, A$ to the task of reasoning from $\forall x\, \neg A$ to a contradiction.

Suppose $\neg \exists x\, A$
    Suppose A
    $\exists x\, A$
    $\perp$
Thus $\neg A$
$\forall x\, \neg A$

$\perp$
Thus $\exists x\, A$

Problems

The problems are to be done using natural deduction. Indent.

1. Show that
$$A \Rightarrow (B \lor C), B \Rightarrow \neg A, D \Rightarrow \neg C \vdash A \Rightarrow \neg D.$$

2. Show that
$$P \lor Q, \neg Q \lor R \vdash P \lor R.$$

3. Show that from the hypotheses n odd $\Rightarrow n^2$ odd, n odd$\lor n$ even, $\neg(n^2$ odd$\land$ n^2 even) it may be proved by natural deduction that n^2 even $\Rightarrow n$ even.

4. Show that
$$\forall x\, x \text{ happy} \vdash \neg\exists x \neg\, x \text{ happy}.$$

5. Show that
$$\forall x \exists y\, (x \text{ likes } y \Rightarrow x \text{ adores } y) \vdash \exists x \forall y\, x \text{ likes } y \Rightarrow \exists x \exists y\, x \text{ adores } y.$$

6. Here is a mathematical argument that shows that there is no largest prime number. Assume that there were a largest prime number. Call it a. Then a is prime, and for every number j with $a < j$, j is not prime. However, for every number m, there is a number k that divides m and is prime. Hence there is a number k that divides $a! + 1$ and is prime. Call it b. Now every number $k > 1$ that divides $n! + 1$ must satisfy $n < k$. (Otherwise it would have a remainder of 1.) Hence $a < b$. But then b is not prime. This is a contradiction.

   Use natural deduction to prove that
$$\forall m \exists k\, (k \text{ prime} \land k \text{ divides } m)$$
$$\forall n \forall k\, (k \text{ divides } n! + 1 \Rightarrow n < k)$$
   logically imply
$$\neg\exists n\, (n \text{ prime} \land \forall j\, (n < j \Rightarrow \neg\, j \text{ prime})).$$

6.2 Supplement: Short-cut existential hypotheses rule

The one rule of natural deduction that seems unnatural to a mathematician is the rule for an existential hypothesis. The official rule is to suppose that an object denoted by a new free variable exists and satisfies the appropriate condition. One reasons to a conclusion that does not mention this variable. Then one can obtain the same conclusion without the supposition.

Mathematical practice is somewhat different. One makes the supposition that an object denoted by a new free variable exists and satisfies the appropriate conclusion. One reasons to a conclusion that does not mention this variable. However one does not explicitly state that the supposition is not needed. One simply forgets about it.

There have been many attempts to formalize this procedure, and it is a notorious topic in discussions of natural deduction. Here we give a rough way to deal with this issue. The proposed rule is as follows.

If z is a variable that does not occur free in a hypothesis in force, in $\exists x\, A$, or in C, then

$\exists x\, A$

Let $A_x(z)$

C

From this point on treat C as a consequence of the existential hypothesis without the temporary supposition $A_x(z)$ or its temporary consequences.

The safe course is to take z to be a variable that is used as a temporary name in this context, but which occurs nowhere else in the argument.

Example: Here is a natural deduction proof of the fact that $\exists x\,(x \text{ happy} \wedge x \text{ rich})$ logically implies that $\exists x\, x \text{ happy} \wedge \exists x\, x \text{ rich}$.

Suppose $\exists x\,(x \text{ happy} \wedge x \text{ rich})$

Let z happy $\wedge$ z rich

z happy

z rich

$\exists x\, x$ happy

$\exists x\, x$ rich

$\exists x\, x \text{ happy} \wedge \exists x\, x \text{ rich}$

Here is the same proof in narrative form.

Suppose $\exists x\,(x \text{ happy} \wedge x \text{ rich})$. **Let** z happy $\wedge$ z rich. Then z happy and hence $\exists x\, x$ happy. Similarly, z rich and hence $\exists x\, x$ rich. It follows that $\exists x\, x \text{ happy} \wedge \exists x\, x \text{ rich}$.

Example: We could try to reason in the other direction, from the existence of a happy individual and the existence of a rich individual to the existence of a happy, rich individual? What goes wrong?

Suppose $\exists x\, x \text{ happy} \wedge \exists x\, x \text{ rich}$. Then $\exists x\, x$ happy, $\exists x\, x$ rich. **Let** z happy. **Let** w rich. Then z happy $\wedge$ w rich. This approach does not work.

Here is another attempt at the other direction.

Suppose $\exists x\, x \text{ happy} \wedge \exists x\, x \text{ rich}$. Then $\exists x\, x$ happy, $\exists x\, x$ rich. **Let** z happy. **Let** z rich. Then z happy $\wedge$ z rich. So $\exists x\,(x \text{ happy} \wedge x \text{ rich})$. This seems to proves the conclusion, but it does not. The problem is that we have temporarily supposed also that z happy, and so z is not an arbitrary name for the rich individual. All this proves is that one can deduce logically from z happy, z rich that $\exists x\,(x \text{ happy} \wedge x \text{ rich})$. So this approach also does not work.

Example: Here is a natural deduction proof that $\exists y \forall x\, x \leq y$ gives $\forall x \exists y\, x \leq y$.

Suppose $\exists y \forall x\, x \leq y$
Let $\forall x\, x \leq y'$
$x' \leq y'$
$\exists y\, x' \leq y$
$\forall x \exists y\, x \leq y$

Here is the same proof in narrative form.

Suppose $\exists y \forall x\, x \leq y$. **Let** y' satisfy $\forall x\, x \leq y'$. In particular, $x' \leq y'$. Therefore $\exists y\, x' \leq y$. Since x' is arbitrary, conclude that $\forall x \exists y\, x \leq y$.

6.3 Supplement: Short-cut templates

Here are short-cut templates for natural deduction. While sometimes it is straightforward to obtain a disjunction or an existentially quantified formula in a conclusion, in general it can be a nuisance. These templates reduce such problems to problems without the offending connective or quantifier. The price is a negated hypothesis, which is still something of a bother. These templates might seem like a cheat—essentially they are an appeal to de Morgan's laws—but they can be convenient.

Or in conclusion template Replace $A \vee B$ in a conclusion by $\neg(\neg A \wedge \neg B)$. Thus the template is

$\neg(\neg A \wedge \neg B)$
$A \vee B$

Exists in conclusion template Replace $\exists x\, A$ in a conclusion by $\neg(\forall x\, \neg A)$. Thus the template is

$\neg(\forall x\, \neg A)$
$\exists x\, A$

6.4 Supplement: Relaxed natural deduction

Mathematicians ordinarily do not care to put in all logical steps explicitly, as would be required by the natural deduction rules. However there is a more relaxed version of natural deduction that might be realistic in some contexts. This version omits certain trivial logical steps. Here is an outline of how it goes.

And The rules for eliminating "and" from a hypothesis and for introducing "and" in the conclusion are regarded as obvious.

All The rule for using $\forall x\, A$ in a hypothesis by replacing it with $A_x(t)$ is regarded as obvious. The rule for introducing $\forall x\, A$ in a conclusion by first proving $A_x(z)$ is indicated more explicitly, by some such phrase as "since z is arbitrary", which means that at this stage z does not occur as a free variable in any hypothesis in force.

Implies The rule for using $\Rightarrow$ in a hypothesis is regarded as obvious. The rule for introducing $\Rightarrow$ in a conclusion requires special comment. At an earlier stage there was a **Suppose** A. After some logical reasoning there is a conclusion B. Then the removal of the supposition and the introduction of the implication is indicated by **Thus** $A \Rightarrow B$.

Not The rule for using $\neg$ in a hypothesis is regarded as obvious. The rule for introducing $\neg$ in a conclusion requires special comment. At an earlier stage there was a **Suppose** A. After some logical reasoning there is a false conclusion $\perp$. Then the removal of the supposition and the introduction of the negation is indicated by **Thus** $\neg A$.

Contradiction The rule for proof by contradiction requires special comment. At an earlier stage there was a **Suppose** $\neg A$. After some logical reasoning there is a false conclusion $\perp$. Then the removal of the supposition and the introduction of the conclusion is indicated by **Thus** A.

Or The rule for using $\vee$ in a hypothesis is proof by cases. Start with $A \vee B$. **Suppose** A and reason to conclusion C. **Instead suppose** B and reason to the same conclusion C. **Thus** C. The rule for starting with A (or with B) and introducing $A \vee B$ in the conclusion is regarded as obvious.

Exists Mathematicians tend to be somewhat casual about $\exists x\, A$ in a hypothesis. The technique is to **Let** $A_x(z)$. Thus z is a variable that may be used as a temporary name for the object that has been supposed to exist. (The safe course is to take a variable that will be used only in this context.) Then the reasoning leads to a conclusion C that does not mention z. The conclusion actually holds as a consequence of the existential hypothesis, since it did not depend on the assumption about z. The rule for starting with $A_x(t)$ and introducing $\exists x\, A$ is regarded as obvious.

Rules for equality (everything is equal to itself, equals may be substituted) are also used without comment.

Chapter 7

Gentzen Deduction

7.1 Sequents

Gentzen deduction is a transparent formulation of logical reasoning. The rules are symmetric and easy to recall. Working with it resembles systematic manipulation of mathematical inequalities. The drawback is that one has to repeatedly write the same formulas.

Gentzen deduction works with sequents. A *sequent* is an ordered pair U, V of sets of formulas. In most practical reasoning each of these sets is a finite set. For theoretical purposes it is useful to allow the possibility that these sets are countably infinite. A sequent is written

$$U \longrightarrow V \tag{7.1}$$

with an arrow separating the two sets. The formulas in U are hypotheses; the formulas in V are alternative conclusions. In an interpretation a sequent $U \longrightarrow V$ is true if the truth of all the formulas in U implies the truth of some formula in V. Equivalently, in an interpretation a sequent $U \longrightarrow V$ is false if all the formulas in U are true and all the formulas in V are false. In our terminology each formula in U is a *hypothesis*, and each formula in V is an *alternative conclusion*. There is no claim that this terminology is standard, but it is reasonably close to what mathematicians might use.

It is common to use an abbreviated notation for sequents. If $U = \{A, B\}$ and $V = \{C, D, E\}$, then $U \longrightarrow V$ is written

$$A, B \longrightarrow C, D, E \tag{7.2}$$

This is true in an interpretation if when A, B are both true, then at least one of C, D, E is true. If the set of hypotheses is empty, then we would write something like

$$\longrightarrow C, D, E \tag{7.3}$$

This is true in an interpretation if at least one of C, D, E is true. Similarly, if the set of conclusions is empty, then the corresponding expression might be

$$A, B \longrightarrow \tag{7.4}$$

This is true in an interpretation if A, B are not both true.

Write $\sim V$ for the set of negations of the formulas in V. Then to say that $U \longrightarrow V$ is false in an interpretation is the same as saying that all the formulas in $U, \sim V$ are true in the interpretation. In this case we may also say that the combined set of formulas $U, \sim V$ is *satisfied* in the interpretation.

There are two situations of particular interest. One is when $U \longrightarrow V$ is true in every interpretation (and for every variable assignment). In this case we say that the sequent is *valid*. Equivalently, we have a *semantic logical implication* $U \models V$. It is important to understand that in Gentzen calculus to say that U logically implies V means that the truth of *all* formulas in U implies the truth of *some* formula in V.

The other situation is when there is some interpretation (and variable assignment) such that $U \longrightarrow V$ is false. In this case we say that the sequent $U \longrightarrow V$ is *falsifiable*. Another way of saying this is that the set of formulas $U, \sim V$ is *satisfiable*.

There is an important special case in which the set of alternative conclusions is empty. For simplicity consider the case when all formulas in U are sentences. Then $U \longrightarrow$ is false in the interpretation ϕ if the formulas in U are all true in the interpretation ϕ. In this case we say that U is satisfied by ϕ. Alternatively, we say that ϕ is a model for U. There is a special notation for this, in which we write $\phi \Vert\!\models U$ to indicate that ϕ models U.

To continue this line of thought, if $U \longrightarrow$ is valid, that is, if $U \models$ is true, then U is unsatisfiable, that is, U has no model. On the other hand, if $U \longrightarrow$ is falsifiable, then U is satisfiable, that is, it has a model.

7.2 Gentzen rules

The syntactic notion of derivation is given by the notion of *Gentzen rule*. The specific list of Gentzen rules is given below. Each rule has a sequent or pair of sequents above the line, and a sequent below the line. A sequent above the line will be called a *premise*. In our terminology the sequent below the line is called a *consequent*. (This terminology is not standard, but it seems reasonable in this context.) The rule is designed so that if the premises above the line are valid, then the consequent below the line is valid. Equivalently, if the consequent below the line is falsifiable, then at least one of the premises above the line is falsifiable.

A *Gentzen tree* is a rooted binary tree of sequents in which the immediate successors of each sequent, if they exists, are given by applying one of the rules. In the application of the rule the consequent is below the line, and the immediate successor premisses are above the line. A Gentzen tree is allowed to be infinite.

The basic axiom scheme of the Gentzen calculus is $U, A \longrightarrow A, V$. A sequent is *closed* if it is of this form, that is, has a formula repeated in hypotheses and conclusion. A branch of a Gentzen tree is *closed* if there is a closed sequent in the set. Otherwise it is *open*. A Gentzen tree is *closed* if every branch is closed.

A *Gentzen proof* is a closed Gentzen tree. The notation $U \vdash V$ means that there is a Gentzen proof with $U \longrightarrow V$ as the root. In this case we say that U *logically implies* V in the syntactic sense.

Each Gentzen rule reduces exactly one formula in the consequent. With the four connectives and two quantifiers there are twelve rules. They may be paired in a natural way, according to whether the relevant logical operation is in the hypothesis part or the conclusion part of the sequent.

A deeper analysis of the rules classifies them into α, β, γ, and δ rules. The α and β rules treat connectives; the γ and δ rules are corresponding rules for quantifiers.

Each α rule reduces the consequent to a single premise. Each β rule reduces the consequent to a pair of premises. There is one exception: the rule for a negated hypothesis is a special case of the rule for an implication in the hypothesis, so it is natural to regard it as a β rule.

Each γ rule reduces the consequent to a single premise. The quantifier is repeated in the premise, so the rule may be used repeatedly with various terms. Each δ rule reduces the consequent to a premise with an arbitrary free variable.

α rules: $\wedge \longrightarrow$, $\longrightarrow \vee$, $\longrightarrow \Rightarrow$, $\longrightarrow \neg$

$$\frac{U, A, B \longrightarrow V}{U, A \wedge B \longrightarrow V}$$

$$\frac{U \longrightarrow A, B, V}{U \longrightarrow A \vee B, V}$$

$$\frac{U, A \longrightarrow B, V}{U \longrightarrow A \Rightarrow B, V}$$

$$\frac{U, A \longrightarrow V}{U \longrightarrow \neg A, V}$$

β rules: $\longrightarrow \wedge$, $\vee \longrightarrow$, $\Rightarrow \longrightarrow$, $\neg \longrightarrow$

$$\frac{U \longrightarrow A, V \mid U \longrightarrow B, V}{U \longrightarrow A \wedge B, V}$$

$$\frac{U, A \longrightarrow V \mid U, B \longrightarrow V}{U, A \vee B \longrightarrow V}$$

$$\frac{U \longrightarrow A, V \mid U, B \longrightarrow V}{U, A \Rightarrow B \longrightarrow V}$$

$$\frac{U \longrightarrow A, V}{U, \neg A \longrightarrow V}$$

γ rules: $\forall \longrightarrow$, $\longrightarrow \exists$

$$\frac{U, \forall x\, A, A_x(t) \longrightarrow V}{U, \forall x\, A \longrightarrow V}$$

$$\frac{U \longrightarrow A_x(t), \exists x\, A, V}{U \longrightarrow \exists x\, A, V}$$

δ rules: $\longrightarrow \forall$, $\exists \longrightarrow$
If z is a variable that does not occur free in U, V, or $\forall x\, A$, then

$$\frac{U \longrightarrow A_x(z), V}{U \longrightarrow \forall x\, A, V}$$

$$\frac{U, A_x(z) \longrightarrow V}{U, \exists x\, A \longrightarrow V}$$

Here is a scheme for remembering the four patterns. Since the only effect of a rule is to perform a reduction on one formula in the consequent, the scheme only describes what is done to this formula. The relevant formula is called $\alpha, \beta, \gamma, \delta$ according to its logical type and its position in hypothesis or conclusion.

α rules: $\wedge \longrightarrow$, $\longrightarrow \vee$, $\longrightarrow \Rightarrow$, $\longrightarrow \neg$

If the sequent with α_1, α_2 is valid, then the sequent with α is valid.

$$\frac{\alpha_1, \alpha_2}{\alpha}$$

β rules: $\longrightarrow \wedge$, $\vee \longrightarrow$, $\Rightarrow \longrightarrow$, $\neg \longrightarrow$

If the sequents with β_1 and β_2 are both valid, then the sequent with β is valid.

$$\frac{\beta_1 \mid \beta_2}{\beta}$$

γ rules: $\forall \longrightarrow$, $\longrightarrow \exists$

If the sequent with $\gamma(t)$ is valid, then the sequent with γ is valid. The repetition of γ is to allow the rule to be applied repeatedly with various terms.

$$\frac{\gamma, \gamma(t)}{\gamma}$$

δ rules: $\longrightarrow \forall$, $\exists \longrightarrow$

Suppose z is a new variable. If the sequent with $\delta(z)$ is valid, then so is the sequent with δ.

$$\frac{\delta(z)}{\delta}$$

When a rule is used only one formula is affected. The other formulas are simply recopied. This suggests that a more economical notation might be found in which one only notes the formulas that change from step to step. The *tableau* method is based on this idea. A useful reference for the tableau method is the book [17]. The lecture notes [16] give a particularly readable account.

7.3 Examples

In building a Gentzen tree, it is important to try as far as possible to use the δ rules before using the γ rules. Generally new variables are introduced by the δ rules and subsequently, higher up on the tree, used by the γ rules. The difficulty in logical deduction is due to the γ rules. The reason is that the γ rules may need to be used repeatedly. There is no upper limit to the terms that one might have to try.

A Gentzen proof is usually discovered by working bottom up. However a Gentzen proof can be read either bottom up or top down.

Example: Here is a Gentzen proof of the syntactic logical implication $\exists x\,(x \text{ happy} \wedge x \text{ rich}) \vdash \exists x\, x \text{ happy} \wedge \exists x\, x \text{ rich}$.

z happy, z rich $\longrightarrow z$ happy, $\exists x\, x$ happy $\mid z$ happy, z rich $\longrightarrow z$ rich, $\exists x\, x$ rich
z happy, z rich $\longrightarrow \exists x\, x$ happy $\mid z$ happy, z rich $\longrightarrow \exists x\, x$ rich
z happy, z rich $\longrightarrow \exists x\, x$ happy $\wedge \exists x\, x$ rich
z happy $\wedge\, z$ rich $\longrightarrow \exists x\, x$ happy $\wedge \exists x\, x$ rich
$\exists x\,(x$ happy $\wedge\, x$ rich$) \longrightarrow \exists x\, x$ happy $\wedge \exists x\, x$ rich

Example: Here is a Gentzen proof of $\exists y \forall x\, x \leq y \vdash \forall x \exists y\, x \leq y$.
$\forall x\, x \leq y', x' \leq y' \longrightarrow x' \leq y', \exists y\, x' \leq y$
$\forall x\, x \leq y', x' \leq y' \longrightarrow \exists y\, x' \leq y$
$\forall x\, x \leq y' \longrightarrow \exists y\, x' \leq y$
$\exists y \forall x\, x \leq y \longrightarrow \exists y\, x' \leq y$
$\exists y \forall x\, x \leq y \longrightarrow \forall x \exists y\, x \leq y$

7.4 The soundness theorem

The method is based on the following semantic observations. Consider a fixed interpretation and variable assignment.

α **formulas** If $A \wedge B$ is true, then A, B are both true. If $A \vee B$ is false, then A, B are both false. If $A \Rightarrow B$ is false, then A is true and B is false. If $\neg A$ is false, then A is true.

β **formulas** If $A \wedge B$ is false, then either A or B is false. If $A \vee B$ is true, then either A is true or B is true. If $A \Rightarrow B$ is true, then A is false or B is true. If $\neg A$ is true, then A is false.

γ **formulas** If $\forall x\, A$ is true, then $A_x(z)$ is true for every reassignment of z. If $\exists x\, A$ is false, then $A_x(z)$ is false for every reassignment of z.

δ **formulas** If $\forall x\, A$ is false, then $A_x(z)$ is false for some reassignment of z. If $\exists x\, A$ is true, then $A_x(z)$ is true for some reassignment of z.

These observations may be summarized as follows.

- If the sequent with α is falsified, then the sequent with α_1, α_2 is falsified.
- If the sequent with β is falsified, then either the sequent with β_1 is falsified, or the sequent with β_2 is falsified.
- If the sequent with γ is falsified, then for each reassignment of z the sequent with $\gamma(z)$ is falsified.
- If the sequent with δ is falsified, then for some reassignment of z the sequent with $\delta(z)$ is falsified.

These arguments show that each of the Gentzen rules preserves validity. This is a routine observation for the α and β rules involving only connectives, but the quantifier rules deserve comment.

If the sequent with γ is false in some interpretation and variable assignment, then the sequent with $\gamma(t)$ is false with this interpretation and variable assignment. This shows that if the sequent with $\gamma(t)$ is valid, then the sequence with γ is valid.

If the sequent with δ is false in some interpretation and variable assignment, then there is some reassignment to z that makes the sequent with $\delta(z)$ false with this interpretation and new variable assignment. This shows that if the sequent with $\delta(z)$ is valid, then the sequent with δ is valid.

Recall that a Gentzen proof is a closed Gentzen tree. We write $U \vdash V$ if there is a Gentzen proof with root $U \longrightarrow V$.

Proposition 7.1 (Finiteness of proofs) *If there is a Gentzen proof of $U \vdash V$, then there is a Gentzen proof of $U \vdash V$ with a finite Gentzen tree.*

Proof: Consider the Gentzen proof tree. Every branch has a least closed sequent. The sequents that are below these least closed sequents form a Gentzen proof tree. In this tree every branch is finite. By König's lemma the entire tree is finite. □

Theorem 7.2 (Soundness theorem) *If $U \vdash V$, then $U \models V$.*

Proof: Consider a finite Gentzen proof tree with a closed sequent at each end point. Each closed sequent is automatically valid. Since the Gentzen rules preserve validity, it follows that every sequent in the tree is valid. □

7.5 The cut rule

The *cut rule* is a statement of transitivity. It says that

$$\frac{U \longrightarrow A, V \mid S, A \longrightarrow W}{U, S \longrightarrow V, W}$$

Start with hypotheses U, S. First use U to prove a lemma A, possibly with alternatives V. Then use S together with A to conduct an independent derivation of alternative conclusions W. The cut rule says that U, S leads to alternative conclusions V, W without having to mention the lemma.

Example: The cut rule says that it is not necessary to write the entire proof in one uninterrupted chain of reasoning. Say for instance that U is a collection of sentences in a calculus book (and $V = \emptyset$). Say that from U one can prove the lemma A stating that $\forall x > 0\,(x \text{ irrational} \Rightarrow \sqrt{x} \text{ irrational})$. Then it is easy to construct a separate proof that the conjunction S stating that $\pi > 0, \pi$ irrational together with A leads to the conclusion W stating that $\sqrt{\pi}$ irrational. The cut rule says that it then follows that U together with $\pi > 0, \pi$ irrational leads logically to $\sqrt{\pi}$ irrational. In short, the cut rule says that one can rely on previously proved lemmas.

The cut rule is very powerful, and it can shorten proofs. However it takes imagination to use it—one has to guess the right lemma. It is remarkable that one can dispense with the cut rule and get the same logical implications. In fact, Gentzen showed that cuts may be eliminated by a systematic process. (There is a corresponding process of normalization in natural deduction.) There are a number of books on proof theory. The book by [19] is a good reference. Other useful books include [18, 2, 9]. See [13] for a focus on natural deduction.

Problems

All the problems except the last are to be done using Gentzen deduction. Each step involves precisely one logical operation. The logical operation must correspond to the logical type of the formula.

1. Show that from the hypotheses $P \Rightarrow Q$, $P \vee R$, $\neg(Q \wedge S)$ it may be proved by Gentzen deduction that $S \Rightarrow R$.
2. Show that from the hypotheses $P \Rightarrow Q$, $P \vee R$, $\neg(Q \wedge S)$ it there is no proof by Gentzen deduction that $R \Rightarrow S$. Use a branch of the failed proof to construct a truth-value assignment in which the hypotheses are all true, but the conclusion is false.
3. Show that
$$P \vee Q, \neg Q \vee R \vdash P \vee R.$$
4. Show by using Gentzen deduction that
$$P \vee Q, \neg Q \vee R \vdash P \wedge R$$
is false. Find a branch that closes in atomic formulas but not in an axiom. Use this branch to construct an example that shows that
$$P \vee Q, \neg Q \vee R \models P \wedge R$$
is false.
5. It is a well-known mathematical fact that $\sqrt{2}$ is irrational. In fact, if it were rational, so that $\sqrt{2} = m/n$, then we would have $2n^2 = m^2$. Thus m^2 would have an even number of factors of 2, while $2n^2$ would have an odd number of factors of two. This would be a contradiction.

   Use natural deduction to show that
$$\forall i\, i^2 \text{ even-twos}$$
and
$$\forall j\, (j \text{ even-twos} \Rightarrow \neg\, 2 \cdot j \text{ even-twos})$$
give
$$\neg \exists m \exists n\, 2 \cdot n^2 = m^2.$$

7.6 Appendix: Adjointness

This appendix is an attempt to exhibit a deeper structure to the Gentzen rules. The idea is that an operation on one side of a sequent corresponds to another operation on the other side of a sequent. One such operation is said to be adjoint to the other operation.

$\wedge$ Conjunction in conclusion is right adjoint to constant hypothesis.

$$\frac{\substack{U \longrightarrow A, V \\ U \longrightarrow B, V}}{U \longrightarrow A \wedge B, V}$$

$\vee$ Disjunction in hypothesis is left adjoint to constant conclusion.

$$\frac{\substack{U, A \longrightarrow V \\ U, B \longrightarrow V}}{U, A \vee B \longrightarrow V}$$

$\forall$ The universal quantifier in conclusion is right adjoint to constant hypothesis.

$$\frac{U \longrightarrow A_x(z), V}{U \longrightarrow \forall x\, A, V}$$

$\exists$ The existential quantifier in hypothesis is left adjoint to constant conclusion.

$$\frac{U, A_x(z) \longrightarrow V}{U, \exists x\, A \longrightarrow V}$$

$A \Rightarrow$ Implication in conclusion is right adjoint to conjunction with hypothesis.

$$\frac{U, A \longrightarrow B, V}{U \longrightarrow A \Rightarrow B, V}$$

$A \Rightarrow$ Implication in hypothesis is left adjoint to disjunction with constant conclusion.

$$\frac{\substack{U \longrightarrow A, V \\ U, B \longrightarrow V}}{U, A \Rightarrow B \longrightarrow V}$$

There is no special name for the operation in logic corresponding to a left adjoint for disjunction with B in conclusion. The natural operation would seem to be the one that sends A to $A \wedge \neg B$. Then $U, A \longrightarrow B, V$ would transform to $U, A \wedge \neg B \longrightarrow V$. This certainly works in classical logic, but there is no standard symbol for this excision operation. One could propose $A \setminus B$.

There is an explanation for this lack of symmetry. Intuitionistic logic is a beautiful and natural extension of classical logic. (See the appendix on intuitionistic logic.) In this logic proof by contradiction is not allowed. Only some rules of classical logic apply, and there is a particular problem with disjunctions in the conclusion. As a result, intuitionistic logic has less symmetry than classical logic. A tendency to think in the framework of intuitionistic logic may have affected the traditions of classical logic.

There are two reasons why this might happen. One is that people may unconsciously slip into thinking in the intuitionistic framework. Intuitionistic logic is about stages of development, and this dynamic way of thinking is in some ways more natural than the static formulation of classical logic.

The other reason is that inference is ordinarily conducted in a framework similar to natural deduction. Natural deduction is similar to Gentzen deduction, but the symmetry is less apparent. The main difference is that there are typically several hypotheses in force, but at any one point there is only one conclusion. While in a Gentzen proof alternative conclusions are allowed, in a natural deduction argument one uses proof by contradiction to replace conclusion C by hypothesis $\neg C$. In natural deduction there is a willingness to argue using intuitionistic rules as far as possible and adopt proof by contradiction only as a last resort. So in this context intuitionistic logic affects the spirit of classical logic, if not the substance.

Chapter 8

The completeness theorem

8.1 The satisfaction theorem

This section presents a method for attempting to prove that a sequent $U \longrightarrow V$ is falsifiable, that is, that $U, \sim V$ is satisfiable. The discussion is in the context of a language with predicate symbols but no function symbols. This is merely for technical convenience.

The method is based on the following semantic observations. Consider a fixed interpretation and variable assignment.

α **formulas** If formula A, B are both true, then $A \wedge B$ is true. If a formulas A, B are both false, then $A \vee B$ is false. If A is true and B is false, then $A \Rightarrow B$ is false. If A is true, then $\neg A$ is false.

β **formulas** If either formula A or formula B is false, then formula $A \wedge B$ is false. If either formula A or formula B is true, the formula $A \vee B$ is true. If formula A is false or formula B is true, then $A \Rightarrow B$ is true. If formula A is false, then $\neg A$ is true.

γ **formulas** If $A_x(z)$ is true for every reassignment of z, then $\forall x A$ is true. If $A_z(z)$ is false for every reassignment of z, then $\exists x A$ is false.

δ **formulas** If $A_x(z)$ is false for some reassignment of z, then $\forall x A$ is false. If $A_x(z)$ is true for some reassignment of z, then $\exists x A$ is true.

These observations may be summarized as follows.

- If the sequent with α_1, α_2 is falsified, then the sequent with α is falsified.
- If either the sequent with β_1 is falsified, or the sequent with β_2 is falsified, then the sequent with β is falsified.
- If for each reassignment of z the sequent with $\gamma(z)$ is falsified , then the sequent with γ is falsified.

- If for some reassignment of z the sequent with $\delta(z)$ is falsified, then the sequent with δ is falsified.

Now return to syntax. A branch of a Gentzen tree is a *complete branch* if it has the following properties.

- For every α formula in a sequent on the branch the corresponding rule is used for some successor sequent on the branch.
- For every β formula in a sequent on the branch the corresponding rule is used for some successor sequent on the branch with either β_1 or β_2.
- For every γ formula in a sequent on the branch the corresponding rule is used in successor sequents for all free variables that occur on the branch. (It is assumed that there is at least one such free variable.)
- For every δ formula in a sequent on the branch the corresponding rule is used for some successor sequent on the branch with a new free variable.

The completeness condition is stronger than it first appears. When a γ rule is used with a variable, the result may well be a δ formula. When a δ rule is subsequently used, it requires a new free variable. It is necessary to use the γ with this free variable as well.

Theorem 8.1 (Satisfaction theorem) *Suppose a Gentzen tree has a complete open branch. Then there is an interpretation that falsifies each sequent in the branch.*

Proof: The syntax is used to define the semantics. That is, the domain of the interpretation consists of the free variables that occur anywhere along the branch. Define the variable assignment that assigns to each variable the same variable regarded as an element of the domain. Define the interpretation of the predicate symbols so that in each sequent along the branch the atomic formulas among the hypotheses are true. All other atomic formulas are false. Since the branch is open, this makes the atomic formulas among the conclusions false.

Other formulas along the branch are built up in stages from atomic formulas. Since the search is complete, the semantic observations above may be reformulated as follows.

- If a sequent with α_1, α_2 is falsified, then the sequent with α is falsified.
- If either a sequent with β_1 is falsified, or a sequent with β_2 is falsified, then the sequent with β is falsified.
- If the sequents with $\gamma(z)$ are falsified for each free variable that occurs on the branch, then the sequent with γ is falsified.
- If the sequents with δ_1, δ_2 are falsified for some free variable z that occurs on the branch, then the sequent with δ is falsified.

From this we conclude that the sequents on the branch are all falsified in this interpretation. □

Example: Here is a complete open branch that shows that the semantic logical implication $\exists x\, x$ happy $\wedge\, \exists x\, x$ rich $\models \exists x(x$ happy $\wedge\, x$ rich$)$ is false.

y happy, z rich $\longrightarrow z$ happy, y rich, $\exists x\,(x$ happy $\wedge\, x$ rich$)$
y happy, z rich $\longrightarrow z$ happy, y happy $\wedge\, y$ rich, $\exists x\,(x$ happy $\wedge\, x$ rich$)$
y happy, z rich $\longrightarrow z$ happy, $\exists x\,(x$ happy $\wedge\, x$ rich$)$
y happy, z rich $\longrightarrow z$ happy $\wedge\, z$ rich, $\exists x\,(x$ happy $\wedge\, x$ rich$)$
y happy, z rich $\longrightarrow \exists x\,(x$ happy $\wedge\, x$ rich$)$
y happy, $\exists x\, x$ rich $\longrightarrow \exists x\,(x$ happy $\wedge\, x$ rich$)$
$\exists x\, x$ happy, $\exists x\, x$ rich $\longrightarrow \exists x\,(x$ happy $\wedge\, x$ rich$)$
$\exists x\, x$ happy $\wedge\, \exists x\, x$ rich $\longrightarrow \exists x\,(x$ happy $\wedge\, x$ rich$)$

This shows that the domain consists of y, z. The individual y is happy but not rich, while the individual z is rich but not happy.

Example: Here is a complete open branch that shows that $\forall x \exists y\, x < y$ is satisfiable. We show only the lower part of the infinite search.

$\forall x \exists y\, x < y, x_0 < x_1, x_1 < x_2, x_2 < x_3 \longrightarrow$
$\forall x \exists y\, x < y, x_0 < x_1, x_1 < x_2, \exists y\, x_2 < y \longrightarrow$
$\forall x \exists y\, x < y, x_0 < x_1, x_1 < x_2 \longrightarrow$
$\forall x \exists y\, x < y, x_0 < x_1, \exists y\, x_1 < y \longrightarrow$
$\forall x \exists y\, x < y, x_0 < x_1 \longrightarrow$
$\forall x \exists y\, x < y, \exists y\, x_0 < y \longrightarrow$
$\forall x \exists y\, x < y \longrightarrow$

The domain of the interpretation is $x_0, x_1, x_2, x_2, \ldots$. The formulas $x_0 < x_1, x_1 < x_2, x_2 < x_3, \ldots$ are all true.

8.2 The Gödel completeness theorem

A complete Gentzen tree is a Gentzen tree such that every open branch is complete.

Lemma 8.2 (Completeness lemma) *For every sequent there is a complete Gentzen tree with that sequent as root.*

The idea of the proof is to start with the sequent and construct a Gentzen tree with that sequent as root. The problem is that this is an infinite process. Each γ formula can be used with infinitely many variables. Even if the initial supply of variables in finite, it may turn out that infinitely many δ formulas are uncovered along the way, and this creates an infinite supply of variables.

If one starts with a γ formula and then tries to use it with infinitely many variables, this will construct a tree with a single branch that ignores all other formulas. So this strategy is futile. A better strategy is to limit the use of a γ

formula to finitely many variables at the time. The following construction may not be particularly efficient, but it works.

Proof: Let $x_1, x_2, x_3, \ldots$ be an infinite list of variables. The first m variables in the list are the free variables that occur in the formulas in the sequent. Some of the variables after the first m may be used as new variables in applications of δ rules.

The construction is in stages. Start at stage 0 with the original sequent at the root. Say that a finite tree has been constructed up to stage $n - 1$. Each end point of that finite tree is a sequent. For each such sequent make a finite extension of the tree to obtain stage n. This is done in steps as follows.

- Consider the γ formulas in the sequent. For each such formula use the γ rule with each of the variables $x_1, x_1, \ldots, x_n$. The result is a finite linear extension of the tree.

- For each end point of this extended tree consider the α formulas in the sequent that were copied. For each such formula use the α rule. The result is a further finite linear extension of the tree.

- For each end point of this extended tree consider the δ formulas that were copied. For each such formula use the δ rule. Again the result is a finite linear extension of the tree.

- For each end point of this extended tree consider the β formulas that were copied. For each such formula use the β rule in each branch into which the formula is copied. This gives finite extension of the tree.

The final Gentzen tree is obtained by taking the union of all these finite trees. Various γ formulas are uncovered at various stages of this process. However once a γ formula appears, it continues higher in the tree. Thus in this construction every branch with a γ formula is infinite. Furthermore, each γ formula is used further out on the tree with every variable on the list. Each α, β, or δ formula is also used somewhere further out on the tree. It follows that the Gentzen tree is complete. □

Theorem 8.3 (Gödel completeness theorem) *If $U \models V$, then $U \vdash V$.*

Proof: Consider the sequent $U \longrightarrow V$. By the completeness lemma there is a complete Gentzen tree with $U \longrightarrow V$ as the root. Suppose that $U \vdash V$ is false. Then the Gentzen tree cannot be closed. So it has at least one open branch. By the satisfaction theorem this gives an interpretation that falsifies each sequent in the branch. In particular, it falsifies $U \longrightarrow V$. Thus $U \models V$ is false. □

Theorem 8.4 (Löwenheim-Skolem theorem) *If U is satisfiable, then U is satisfiable in some countable domain.*

Proof: If U is satisfiable, then $U \models$ is false. By the soundness theorem $U \vdash$ is false. But then by the proof of the completeness theorem, U is satisfiable in some countable domain, namely a set of terms in the language. □

The significance of the Löwenheim-Skolem Theorem is profound. Consider a theory that purports to describe properties of the set $\mathbb{R}$ of real numbers. The set of real numbers is uncountable. Yet the theory has another model with a countable domain.

Remark: The completeness theorem continues to hold when the language is allowed to have terms formed using function symbols. See for instance [6].

Remark: The Löwenheim-Skolem theorem continues to hold when the language is allowed to have terms formed from function symbols.

Remark: Suppose that the language has an equality relation =. It is easy to see that in every interpretation the equality relation = is interpreted as an equivalence relation on the domain. Define an *equality interpretation* to be an interpretation for which the equality relation = is interpreted as actual equality. Define a new relation of semantic consequence $\models$ where interpretations are replaces by equality interpretations. With this new relation the completeness theorem continues to hold, that is, $U \models V$ implies $U \vdash V$. Also the Löwenheim-Skolem theorem continues to hold. That is, if $U \vdash$ is false, then U is satisfiable with an equality interpretation in a countable domain.

Problems

1. Consider the hypotheses $\forall x\,(x \text{ happy} \Rightarrow x \text{ rich})$, $\exists x\,(x \text{ happy} \land x \text{ wise})$. The conclusion is $\exists x\,(x \text{ rich} \land x \text{ wise})$. Find a Gentzen proof.

2. Consider the hypotheses $\forall x\,(x \text{ rich} \Rightarrow x \text{ happy})$, $\exists x\, x \text{ rich}$, $\exists x\,(x \text{ happy} \land x \text{ wise})$. The conclusion is $\exists x\,(x \text{ rich} \land x \text{ wise})$. Attempt a Gentzen proof. If the proof fails, use this proof attempt to construct a domain and an interpretation of the three predicate symbols that makes the hypotheses true and the conclusion false.

3. If X is a set, then $P(X)$ is the set of all subsets of X. If X is finite with n elements, then $P(X)$ is finite with 2^n elements. A famous theorem of Cantor states that there is no function f from X to $P(X)$ that is onto $P(X)$. Thus in some sense there are more elements in $P(X)$ than in X. This is obvious when X is finite, but the interesting case is when X is infinite.

   Here is an outline of a proof. Consider an arbitrary function f from X to $P(X)$. We want to show that there exists a set V such that for each

x in X we have $f(x) \neq V$. Consider the condition that $x \notin f(x)$. This condition defines a set. That is, there exists a set U such that for all x, $x \in U$ is equivalent to $x \notin f(x)$. Call this set S. Let p be arbitrary. Suppose $f(p) = S$. Suppose $p \in S$. Then $p \notin f(p)$, that is, $p \notin S$. This is a contradiction. Thus $p \notin S$. Then $p \in f(p)$, that is, $p \in S$. This is a contradiction. Thus $f(p) \neq S$. Since this is true for arbitrary p, it follows that for each x in X we have $f(x) \neq S$. Thus there is a set that is not in the range of f.

Prove using natural deduction that from

$$\exists U \, \forall x \, ((x \in U \Rightarrow \neg x \in f(x)) \wedge (\neg x \in f(x) \Rightarrow x \in U))$$

one can conclude that

$$\exists V \, \forall x \, \neg f(x) = V.$$

Chapter 9

The compactness theorem

9.1 Infinite sequents

A *countable sequent* is a pair $U \longrightarrow V$, where U is a countable set of formulas, and V is another countable set of formulas. The theory of countable sequents parallels the theory of finite sequents.

In particular, the semantic notions are essentially the same. For instance, if $U \longrightarrow V$ is a countable sequent, then $U \models V$ means that for every interpretation (and for every variable assignment), if all the formulas in U are true, then some formula in V is true. The syntactic notions are also very similar. Thus, if $U \longrightarrow V$ is a countable sequent, then $U \models V$ means that there is a closed Gentzen tree with the sequent as root. Again there is a soundness theorem.

Lemma 9.1 (Completeness lemma for countable infinite sequents) *For every sequent there is a complete Gentzen tree with that sequent as root.*

Proof: Let $x_1, x_2, x_3, \ldots$ be an infinite list of variables. There could be infinitely many free variables in the original sequent, so to make sure to get them all, alternate these original free variables with new variables to be used with δ rules. Also, enumerate the formulas in the sequent.

The construction is in stages. Start at stage 0 with the original sequent at the root. Say that a finite tree has been constructed up to stage $n-1$ using the rules only with successors of the first $n-1$ formulas in the enumeration. Each end point of that finite tree is a sequent. For each such sequent make a finite extension of the tree to obtain stage n. In this stage the rules are only applied to successors of the first $n-1$ formulas in the enumeration or to the nth formula in the enumeration.

- Consider the γ formulas among these formulas. For each such formula use the γ rule with each of the variables $x_1, x_1, \ldots, x_n$. The result is a finite linear extension of the tree.

- For each end point of this extended tree consider the α formulas among these formula that occur in the sequents that were copied. For each such formula use the α rule. The result is a further finite linear extension of the tree.
- For each end point of this extended tree consider the δ formulas among these formula that were copied. For each such formula use the δ rule. Again the result is a finite linear extension of the tree.
- For each end point of this extended tree consider the β formulas among these formulas that were copied. For each such formula use the β rule in each branch into which the formula is copied. This gives finite extension of the tree.

The final Gentzen tree is obtained by taking the union of all these finite trees. □

Theorem 9.2 (Gödel completeness theorem for countably infinite sequents) *Consider a countable sequent $U \longrightarrow V$. If $U \models V$, then $U \vdash V$.*

Proof: The proof is as before. □

9.2 Compactness

Proposition 9.3 (Syntactic compactness theorem) *Consider a countable sequent $U \longrightarrow V$. If $U \vdash V$, then there are finite subsets U_0 and V_0 of U and V such that $U_0 \vdash V_0$.*

Proof: Consider the Gentzen proof tree for $U \vdash V$. Every branch has a least closed sequent. The sequents that are below these least closed sequents form a Gentzen proof tree. In this tree every branch is finite. By König's lemma the entire tree is finite. In particular, there are only many finitely many applications of Gentzen rules in the construction of this finite tree and the production of the closed sequents at the end points of this tree. Also, there are only finitely many formulas in the original sequent to which the rules have been applied. If the other formulas are deleted from all the sequents, then the resulting tree is a closed tree with a finite sequent $U_0 \vdash V_0$ at the root. □

Theorem 9.4 (Semantic compactness theorem) *If $U \models V$, then there are finite subsets U_0 and V_0 of U and V such that $U_0 \models V_0$.*

Proof: This follows from the syntactic compactness theorem, the completeness theorem, and the soundness theorem. □

The following corollary is the usual statement of the *compactness theorem*.

Corollary 9.5 *If for all finite subsets U_0 of U the set U_0 is satisfiable, then the set U is satisfiable.*

The significance of the compactness Theorem is profound. Consider a theory that purports to describe properties of the natural numbers. Let c be a new constant symbol. Consider the axioms $c > 0, c > 1, c > 2, c > 3, \ldots$. Every finite subset has a model. By the Compactness Theorem, the whole collection has a model. Thus there is a model of the theory in which there are non-standard natural numbers.

Remark: The completeness and compactness theorems for countably infinite sequents continue to hold when the language is allowed to have terms formed using function symbols.

Remark: The Löwenheim-Skolem theorem holds for countably infinite sequents with a language that is allowed to have terms formed from function symbols.

Remark: Up to now we have been assuming that there are finitely many or at most countably many predicate symbols and function symbols. The completeness and compactness theorems hold even more generally. The language can have uncountably many constant symbols. For instance, one could imagine a constant symbol naming each real number. Such symbols could not be written in any reasonable way, but perhaps one could take the symbol to be the real number itself. Furthermore, the theorems hold when the sequents themselves are uncountable. In the real number example there could be a hypothesized property that holds for each real number, producing uncountably many formulas. These generalizations of the theorems are standard results in mathematical logic that are useful in theoretical investigations of models. A straightforward proof of this version of the compactness theorem may be found in [16].

Problems

1. Often quantifiers are restricted by some condition such as $\forall \epsilon\, (\epsilon > 0 \Rightarrow x\, p)$ or $\exists \epsilon\, (\epsilon > 0 \wedge x\, q)$. The implication restriction goes with the universal quantifier, while the conjunction restriction goes with the existential quantifier. Show by natural deduction that
$$\neg\forall \epsilon\, (\epsilon > 0 \Rightarrow \epsilon\, p) \vdash \exists \epsilon\, (\epsilon > 0 \wedge \neg \epsilon\, p).$$
2. Show by Gentzen deduction that
$$\neg\forall \epsilon\, (\epsilon > 0 \Rightarrow \epsilon\, p) \vdash \exists \epsilon\, (\epsilon > 0 \wedge \neg \epsilon\, p).$$
3. Use the failure of a Gentzen deduction to construct an interpretation that shows that
$$\neg\forall \epsilon\, (\epsilon > 0 \wedge \epsilon\, p) \models \exists \epsilon\, (\epsilon > 0 \wedge \neg \epsilon\, p)$$

is false. Specify domain (variables introduced by δ rules) and interpretations of p, $>$, and 0. (There can be more than one such interpretation.)

4. Here is an argument that if f and g are continuous functions, then the composite function $g \circ f$ defined by $(g \circ f)(x) = g(f(x))$ is a continuous function.

   Assume that f and g are continuous. Consider an arbitrary point a' and an arbitrary $\epsilon' > 0$. Since g is continuous at $f(a')$, there exists a $\delta > 0$ such that for all y the condition $|y - f(a')| < \delta$ implies that $|g(y) - g(f(a'))| < \epsilon'$. Call it δ_1. Since f is continuous at a', there exists a $\delta > 0$ such that for all x the condition $|x - a'| < \delta$ implies $|f(x) - f(a')| < \delta_1$. Call it δ_2. Consider an arbitrary x'. Suppose $|x' - a'| < \delta_2$. Then $|f(x') - f(a')| < \delta_1$. Hence $|g(f(x')) - g(f(a'))| < \epsilon'$. Thus $|x' - a'| < \delta_2$ implies $|g(f(x')) - g(f(a'))| < \epsilon'$. Since x' is arbitrary, this shows that for all x we have the implication $|x - a'| < \delta_2$ implies $|g(f(x)) - g(f(a'))| < \epsilon'$. It follows that there exists $\delta > 0$ such that all x we have the implication $|x - a'| < \delta$ implies $|g(f(x)) - g(f(a'))| < \epsilon'$. Since ϵ' is arbitrary, the composite function $g \circ f$ is continuous at a'. Since a' is arbitrary, the composite function $g \circ f$ is continuous.

   In the following proof the restrictions that $\epsilon > 0$ and $\delta > 0$ are implicit. They are understood because this is a convention associated with the use of the variables ϵ and δ.

   Prove using natural deduction that from

$$\forall a \forall \epsilon \exists \delta \forall x \, (|x - a| < \delta \Rightarrow |f(x) - f(a)| < \epsilon)$$

   and

$$\forall b \forall \epsilon \exists \delta \forall y \, (|y - b| < \delta \Rightarrow |g(y) - g(b)| < \epsilon)$$

   one can conclude that

$$\forall a \forall \epsilon \exists \delta \forall x \, (|x - a| < \delta \Rightarrow |g(f(x)) - g(f(a))| < \epsilon).$$

9.3 Appendix: Translating Gentzen deduction to natural deduction

In the Gentzen calculus presented above, at each stage there can be multiple simultaneous hypotheses and multiple alternative conclusions. In natural deduction, at a given stage there are multiple hypotheses, but a single conclusion.

The following observations will explain the relation between the two systems. The Gentzen rule for $\neg$ in hypothesis has a special case

$$\frac{U \longrightarrow A}{U, \neg A \longrightarrow}$$

If we run this rule backward, we get a special case of the proof by contradiction rule

$$\frac{U, \neg C \longrightarrow}{U \longrightarrow C}$$

These rules can be used together to reduce a negated hypothesis $\neg A$ with conclusion C to a negated hypothesis $\neg C$ with conclusion A.

Here is a method of converting a Gentzen proof of $U \vdash C$ to a natural deduction proof of $U \vdash C$. The idea is clear: replace multiple conclusions with negated hypotheses; swap them back and forth as needed.

- Use de Morgan's laws to eliminate $\vee$ and $\exists$ in conclusion.
- Avoid multiple conclusions. Prepare by replacing conclusion C by hypothesis $\neg C$ with empty conclusion.
- Work on negated hypotheses. Reduce a negated hypothesis $\neg A$ with conclusion C to negated hypothesis $\neg C$ with conclusion A.
- Avoid empty conclusions. Replace them by $\perp$.
- Write the resulting tree of sequents with single conclusions. Convert to natural deduction with templates.

Example: Consider $P \vee Q, \neg Q \vee R, \neg R \vdash P$. Here is a Gentzen tree after the transformation to single conclusions.

$$Q, R, \neg P \longrightarrow R$$
$$Q, \neg R, \neg P \longrightarrow Q \qquad Q, \neg R, R, \neg P \longrightarrow \perp$$
$$Q, Q \Rightarrow R, \neg R, \neg P \longrightarrow \perp$$
$$P, Q \Rightarrow R, \neg R \longrightarrow P \qquad Q, Q \Rightarrow R, \neg R \longrightarrow P$$
$$P \vee Q, Q \Rightarrow R, \neg R \longrightarrow P$$

The proof branches once, then the right side branches again. Here is the corresponding natural deduction proof.

Suppose $P \vee Q$
Suppose $Q \Rightarrow R$
Suppose $\neg R$
    Suppose P
    P
    Instead suppose Q
        Suppose $\neg P$
        Q
        R
        $\perp$
    Thus P
Thus P

The first $P \vee Q$ branch is to the parts from P to P and from Q to P. The second $Q \Rightarrow R$ branch is to the parts from $\neg P$ to Q and from R to $\perp$

Chapter 10

Theories

10.1 Theories and models

From now on the setting is a logical language with specified predicate and function symbols. A *sentence* is a formula in this language without free variables. Its truth value depends on an interpretation of the predicate symbols and function symbols, but not on a variable assignment.

An *axiom set* is a set U of sentences. A *theory* T is a set of sentences closed under logical implication. The axiom set U is an axiom set for the theory T if T consists of all the logical consequences of U.

A theory is *consistent* if there is no sentence such that $A, \neg A$ are both in the theory. This is a syntactic notion.

A theory is *complete* if for every sentence A, either A or $\neg A$ is in the theory. This is a syntactic notion of completeness. To emphasize this, it might be useful to say that the theory is *syntactically complete.* This notion should not confused with semantic completeness.

Consider an interpretation M of the language. This consists of a non-empty domain and of an interpretation of each predicate symbol and function symbol by a predicate or function associated with the domain. If each sentence of U is true in the interpretation M, we say that M is a *model* of U. When M models U we write $M \Vdash\!\!= U$. If U is an axiom set for the theory T, then $M \Vdash\!\!= U$ if and only if $M \Vdash\!\!= T$.

If M is an interpretation, then $\mathrm{Th}(M)$, the theory of M, is the set of all sentences true in M. Thus $\mathrm{Th}(M)$ is always consistent and complete, and $M \Vdash\!\!= \mathrm{Th}(M)$.

The soundness theorem says that if a theory has a model, then it is consistent. The semantic completeness theorem says that if a theory is consistent, then it has a countable model. (The word complete in this context refers to a semantic result, the existence of a model. It has no relation to the syntactic notion of complete theory.)

In the subsequent treatment of theories and models the notion of equality plays an essential role. It is assumed that the language has a relation symbol $=$ and that the usual reasoning with equality is valid. This is enough to ensure that in every model the relation symbol $=$ is interpreted as an equivalence theorem. The interpretation is an *equality interpretation* if the relation symbol $=$ is interpreted as actual equality. Throughout the discussion the notion of interpretation will be taken in this sense, that is, interpretation will mean equality interpretation. Fortunately, the semantic completeness theorem and its consequences remain true in this context.

Let M_1 and M_2 be two models. We say that M_1 is *isomorphic* to M_2 if there is a bijection γ from the domain of M_1 to the domain of M_2 such that each predicate in M_1 is true precisely when the corresponding predicate in M_2 is true, and each function in M_1 is taken to the corresponding function in M_2. Thus for a relation r

$$xR_1y \text{ if and only if } \gamma(x)R_2\gamma(y)$$

and for a 1-place function f

$$\gamma(f_1(x)) = f_2(\gamma(x)).$$

Isomorphic models have the same true sentences. That is, if M_1 is isomorphic to M_2, then $\mathrm{Th}(M_1) = \mathrm{Th}(M_2)$.

A theory is *categorial* if each every pair of models are isomorphic. It would be nice to have categorial theories in mathematics, since they would uniquely characterize the subject matter. It turns out, however, that this condition is very strong; one can hope for a categorial theory only for finite models.

10.2 Theory of a mathematical structure

Given a mathematical structure M, the theory $T = \mathrm{Th}(M)$ consists of all sentences that are true in this model. This is always a complete theory. In the following we want to look at five such theories.

1. The theory of successor. This is a theory where the only non-logical symbols are a constant symbol 0 and a 1-place function symbol s. Each atomic sentence is an equality. It is the theory of all sentences that are true in the model where the domain is $\mathbf{N}$ and 0 is zero and s is the operation of adding one.

2. The theory of dense linear order without minimum or maximum. This is a theory where the only non-logical symbol is $<$. Each atomic sentence is an equality or an inequality. It is the theory of all sentences that are true in the model where the domain is $\mathbf{Q}$ and $<$ is the usual inequality.

3. The theory of discrete linear order with minimum but no maximum. This is a theory where the only non-logical symbols are a constant symbol 0 and a relation symbol $<$. Each atomic sentence is an equality or an inequality.

It is the theory of all sentences that are true in the model where the domain is **N** and $<$ is the usual inequality and 0 is the minimal element.

4. The theory of addition. This is a theory where the only non-logical symbols are constant symbols 0 and 1 and a two-place function symbol $+$. Each atomic sentence is an equality. It is the theory of all sentences that are true in the model where the domain is $\mathbb{N}$ and $+$ is usual addition.

5. The theory of addition and multiplication. This is a theory where the only non-logical symbols are constant symbol 0 and 1 and two-place function symbols $+$ and $\cdot$. Each atomic sentence is an equality. It is the theory of all sentences that are true in the model where the domain is $\mathbb{N}$ and $+$ and $\cdot$ are the usual addition and multiplication.

Problems

1. Say that a language has variables $z_1, z_2, z_3, \ldots$ and a single constant symbol 0 and a single 1-place function symbol s.

   a. Describe all terms in the language.

   b. Prove that the set of terms in the language is countable by describing a one-to-one correspondence between the set of natural numbers $\mathbf{N} = \{0, 1, 2, 3, \ldots\}$ and the set of terms.

2. If a theory has only one model (up to isomorphism), then it is said to be categorical. Show that if a theory is categorical, then it is complete. Hint: Assume the theory has only one model. Suppose the theory T is not complete. Then there is a sentence A such that $T \vdash \neg A$ is false and $T \vdash A$ is false. First show that $T, A \vdash \bot$ is false and that $T, \neg A \vdash \bot$ is false. Is there a way to establish that T, A and $T, \neg A$ each have models?

Chapter 11

Complete theories

11.1 The theory of successor

The language of the theory has a single constant symbol 0 and a single 1-place function symbol s.

We begin with the following axiom.

1. $\forall x\, \forall y\, (sx = sy \Rightarrow x = y)$

This axiom says that s is an injective function. There are many non-isomorphic models for this axiom. Consider an arbitrary number of disjoint copies of $\mathbf{N}$ and $\mathbf{Z}$ and $\mathbf{Z}_n$ for various $n \geq 1$. (You can label them in order to make sure there are no overlaps in the different copies.) In each copy take s to be interpreted as adding one. (In $\mathbf{Z}_n$ we add one modulo n.) This gives an injective function.

2. $\forall x\, \neg sx = 0$

3. $\forall y\, (\neg y = 0 \Rightarrow \exists x\, sx = y)$

These next two axioms say that the range of s omits a single element 0. Thus the only models are the ones where there is precisely one copy of $\mathbf{N}$.

4. An infinite sequence of axioms $\forall x\, \neg sx = x$,$\forall x\, \neg ssx = x$, $\forall x\, \neg sssx = x$, and so on.

These axioms rule out any other possibility other than $\mathbf{N}$ together with a number of copies of $\mathbf{Z}$, at least up to isomorphism. Recall that two models M_1 and M_2 are isomorphic if there is a bijection $\gamma : D_1 \to D_2$ of the domains such that the two constants 0_1 and 0_2 are related by $\gamma(0_1) = 0_2$ and such that the two functions are related by $\gamma(s_1(d)) = s_2(\gamma(d))$ for all d in D_1.

Theorem 11.1 *Every countable model of the theory of successor (axioms 1 through 4) is isomorphic to* $\mathbf{N}$ *together with some countable number of copies of* $\mathbf{Z}$.

We call the model **N** together with 0 and s the standard model. All other models are regarded as non-standard models. Thus each non-standard model is a disjoint union of **N** together with some number of copies of **Z**. Two such models are isomorphic if and only if they have the same number of copies of **Z**.

This usage is considerably more general. Say that we have a theory (preferably a complete theory). Then there may be an *intended model*, the system that we are attempting to describe. A model other than the intended model would be called *non-standard*.

Say that in the present instance we wanted to recognize non-standard models. We could extend the language to have a sequence of new constants $c_1, c_2, c_3, \ldots$. We could then add an infinite set of axioms:

5. $\neg c_i = 0, \neg c_i = s0, \neg c_i = ss0, \neg c_i = sss0, \ldots$ together with $\neg c_i = c_j, \neg c_i = sc_j, \neg c_i = ssc_j, \neg c_i = sssc_j, \ldots$.

These axioms say that the $c_1, c_2, c_3, \ldots$ denote elements that are not standard and also that different constants c_1, c_2, c_3 belong to different copies of the integers.

Theorem 11.2 *Every countable model of the theory of successor with named constants (axioms 1 through 5) has the property that the 0 and s parts of the model (axioms 1 through 4) are isomorphic to* **N** *together with countably infinitely many copies of* **Z**.

Proof: The extended theory with axioms 1 through 5 not only describes each standard natural number in **N** but also describes each non-standard natural number in countably many disjoint copies of **Z**. Each of the non-standard natural numbers in these copies may be described by a condition such as $ss \cdots ssc_i = x$ or $x = ss \cdots ssc_i$. There could be other non-standard natural numbers that have no description, but that does not change the fact that there are a countable infinite number of copies of **Z**. □

Theorem 11.3 *The theory of successor (axioms 1 through 4) is a complete theory. It is the theory of* **N** *together with 0 and s.*

Proof: Let T be the theory in the language of 0 and s generated by axioms 1 through 4. It is consistent, since all the sentences in the theory are true. Suppose it is not complete. Then there is a sentence A in this language such that neither $\neg A$ nor A is in the theory. Let T^+ be the T together with A, and let T^- be T together with $\neg A$. These theories are each consistent. By the semantic completeness theorem they have countable models M^+ and M^-. Let $\hat{T}^+$ and $\hat{T}^-$ be the same theories in an extended language with extra constants $c_1, c_2, c_3, \ldots$. Enumerate all the axioms 1 through 5 in some order. Let $\hat{T}^+_n$ and $\hat{T}^-_n$ be the theories with the first n axioms. These theories have countable models $\hat{M}^+_n$ and $\hat{M}^-_n$. For each n such a model is obtained by taking 0 and s interpreted as in M^+ and M^-. The interpretation of the finitely many constants mentioned by the axioms may denote large standard natural numbers separated by large amounts (depending on n).

By the compactness theorem, $\hat{T}^+_\infty$ and $\hat{T}^-_\infty$ have countable models $\hat{M}^+_\infty$ and $\hat{M}^-_\infty$. These theories describe non-standard natural numbers in countably infinite many different copies of **Z**. In particular, the theories T^+ and T^- in the original language have models M^+_∞ and M^-_∞ with countably infinite many copies of **Z**. These models are isomorphic. But A is true in one model and $\neg A$ is true in the other model. Since isomorphic models have the same true sentences, this is a contradiction. □

11.2 The theory of dense linear order

A theory of linear order has the following axioms:

1. $\forall x\, \forall y\, \forall z\, ((x < y \land y < z) \Rightarrow x < z)$ (transitivity)

2. $\forall x\, \neg x < x$ (non-reflexivity)

3. $\forall x\, \forall y (\neg x = y \Rightarrow (x < y \lor y < x))$ (linear ordering)

Dense linear order is described by the following axiom:

4. $\forall x\, \forall z (x < z \Rightarrow \exists y\, (x < y \land y < z))$ (density)

No maximum and no minimum are expressed by:

5. $\forall x \exists y\, x < y$ (no max)

6. $\forall y \exists x\, x < y$ (no min)

Theorem 11.4 (Cantor theorem on dense linear order) *Let A and B be two sets, each with a dense linear order $<$ with no maximum or minimum elements. If A and B are each countable, then there is an isomorphism f from A to B. That is, there is a bijection $f : A \to B$ that is strictly increasing. Thus for all x and y in A we have $x < y$ in A if and only if $f(x) < f(y)$ in B.*

Proof: Since A is countable, we can let $a_0, a_1, a_2, a_3, \ldots$ be an enumeration of A. Similarly, since B is countable, we can let $b_0, b_1, b_2, b_3, \ldots$ be an enumeration of A. Let $A_n = \{a_0, a_1, a_2, \ldots, a_n\}$ and let $B_n = \{b_0, b_1, b_2, \ldots, b_n\}$.

For each n we shall define finite sets D_n and R_n and a function $f_n : D_n \to R_n$. They shall have the following properties:

$A_n \subseteq D_n$

$B_n \subseteq R_n$

$f_n : D_n \to R_n$ is a bijection that is strictly increasing.

Furthermore, we shall have that $D_n \subseteq D_{n+1}$ and $R_n \subseteq R_{n+1}$ and f_{n+1} agrees with f_n on D_n.

We start by setting $D_0 = A_0$ and $R_0 = B_0$ and defining $f_0(a_0) = b_0$.

To continue, we use induction. We assume that we have $f_n : D_n \to R_n$. The goal is to construct the next $f_{n+1} : D_{n+1} \to R_{n+1}$. This is done in two steps, by a back and forth method.

The forth part is to define sets D'_{n+1} and R'_{n+1} and a strictly increasing bijection $f'_{n+1} : D'_{n+1} \to R'_{n+1}$ extending f_n. If a_{n+1} is in D_n, then $D'_{n+1} = D_n$ and $R'_{n+1} = R_n$ and $f'_{n+1} = f_n$. Otherwise, we take D'_{n+1} to consist of D_n together with a_{n+1}. The function f'_{n+1} is defined by taking $f'_{n+1}(a_{n+1}) = r_{n+1}$, where r_{n+1} is chosen so that the function f'_{n+1} is increasing. The hypothesis that B has a dense linear order without maximum or minimum ensures that the inequalities that say that this function is increasing may always be solved. Then R'_{n+1} is taken to be R_n together with r_{n+1}.

The back part is to define sets D_{n+1} and R_{n+1} and a strictly increasing bijection $f_{n+1} : D_{n+1} \to R_{n+1}$ extending f'_{n+1}. If b_{n+1} is in R'_{n+1}, then $D_{n+1} = D'_{n+1}$ and $R_{n+1} = R'_{n+1}$ and $f_{n+1} = f'_{n+1}$. Otherwise, we take R_{n+1} to consist of R'_{n+1} together with b_{n+1}. The function f_{n+1} is defined by taking $f_{n+1}(d_{n+1}) = b_{n+1}$, where d_{n+1} is chosen so that the function f_{n+1} is increasing. Again the hypothesis on A ensures that this may always be done. Then D_{n+1} is taken to be D'_{n+1} together with d_{n+1}.

To conclude the proof, note that the union of the D_n is all of A, and the union of the R_n is all of B. Let $f : A \to B$ be the common extension of all the f_n. Then f is the desired isomorphism. □

The Cantor theorem just proved has an important consequence. A theory is *categorical for countable models* if each two countable models are isomorphic.

Theorem 11.5 *The theory of dense linear order without max or min is categorical for countable models.*

The obvious countable model is $\mathbf{Q}$ with the usual order $<$. Notice that there are uncountable models. The most obvious example is $\mathbf{R}$ with the usual order $<$. The following theorem is relevant to this example. Its proof is a problem in this chapter.

Theorem 11.6 *A theory that is categorical for countable models is complete.*

Corollary 11.7 *The theory of dense linear order without max or min is complete. It is the theory of* $\mathbf{Q}$ *with the relation* $<$.

11.3 The theory of discrete linear order

A theory of linear order has the following axioms.

1. $\forall x\, \forall y\, \forall z\, ((x < y \wedge y < z) \Rightarrow x < z)$ (transitivity)
2. $\forall x\, \neg x < x$ (non-reflexivity)
3. $\forall x\, \forall y (\neg x = y \Rightarrow (x < y \vee y < x))$ (linear order)

To get a theory of discrete linear order with min but no max, take the following axioms.

4. $\forall x\, \neg x < 0$ (min)

5. $\forall x\, \exists y\, (x < y \wedge \neg \exists w\, (x < w \wedge w < y))$ (successor)

6. $\forall y\, (\neg y = 0 \Rightarrow \exists x\, (x < y \wedge \neg \exists w\, (x < w \wedge w < y)))$ (predecessor)

Each model of this theory is of the form $\mathbf{N}$ followed by $\mathbf{Z} \times C$ with the lexicographic order. Here C is some linearly ordered set. The lexicographic order is defined by $\langle m, s\rangle < \langle n, t\rangle$ in $\mathbf{Z} \times C$ if and only if either $s < t$ or else $s = t$ and $m < n$.

There is a countable model that is universal in the sense that every countable model is isomorphic to part of it. This universal model is $\mathbf{N}$ followed by $\mathbf{Z} \times \mathbf{Q}$.

It may be shown that the theory of discrete linear order with min but no max is complete. It is the theory of $\mathbf{N}$ with the usual 0 and the relation $<$.

11.4 The theory of addition

The language of the theory of addition has constant symbols 0 and 1 and a two-place function symbol $+$. One possible set of axioms is the following:

1. $\forall x \forall y\, x + y = y + x$ (commutative law)

2. $\forall x \forall y \forall z\, (x + y) + z = x + (y + z)$ (associative law)

3. $\forall x\, x + 0 = 0$ (additive identity)

4. $\forall x\, \neg x + 1 = x$

5. $\forall x \forall y\, (x + y = 1 \Rightarrow (x = 0 \vee x = 1))$

6. $\forall x \forall y \exists z\, (x = y + z \vee y = x + z)$

7. $\forall x \forall y \forall u \forall v ((x = y + u \wedge y = x + v) \Rightarrow x = y))$

If we define

$$\forall x \forall y\, (x \leq y \leftrightarrow \exists z\, x + z = y)$$

then the last three axiom take forms that are more transparent.

5. $\forall x\, (x \leq 1 \Rightarrow (x = 0 \vee x = 1))$.

6. $\forall x \forall y\, (x \leq y \vee y \leq x)$

7. $\forall x \forall y\, ((y \leq x \wedge x \leq y) \Rightarrow x = y)$

It may be shown that if we define

$$\forall x\, sx = x + 1$$

then the theory of the successor is included in the theory of the sum. Similarly, it may be shown that if we define

$$\forall x\, (x < y \leftrightarrow \exists z\, (\neg z = 0 \wedge x + z = y))$$

then the theory of discrete linear order is also included.

The theory is completed by an infinite sequence of axioms:

8. $\forall x \exists y\, (x = y + y \vee x = y + y + 1)$
   $\forall x \exists y\, (x = y + y + y \vee x = y + y + 1 \vee x = y + y + y + 1 + 1)$
   and so on.

These axioms say that every number is either even or odd, every number is either a multiple of three, a multiple of three with a remainder of one, or a multiple of three with a remainder of two, and so on.

It may be shown that this theory is a complete theory. It is the theory of $\mathbb{N}$ with 0, 1, and +. There are many countable models of the theory, and they are too complicated to describe in totality. However it is possible to see what the order $<$ must be in a countable model. The order must be either isomorphic to that of $\mathbf{N}$, or it must be isomorphic to that of $\mathbf{N}$ followed by $\mathbf{Z} \times \mathbf{Q}$. The latter is the universal countable model of discrete order.

An example of a countable non-standard model is to take all the elements $\langle m, t \rangle$ in $\mathbf{Z} \times \mathbf{Q}$ with $\langle 0, 0 \rangle \leq \langle m, t \rangle$ in the lexicographic ordering. The zero element is $\langle 0, 0 \rangle$ and the one element is $\langle 1, 0 \rangle$. Addition is defined by $\langle m, t \rangle + \langle m', t' \rangle = \langle m + m', t + t' \rangle$. This has the order structure described above. The elements of the form $\langle m, 0 \rangle$ with $0 \leq m$ are order isomorphic to $\mathbf{N}$, while the elements of the form $\langle m, t \rangle$ with $0 < t$ are order isomorphic to $\mathbf{Z} \times \mathbf{Q}$.

Problems

1. Consider the following set of hypotheses for a theory: $\forall x\, \neg\, sx = x$, $\forall x\, \neg\, ssx = x$, $\forall x\, sssx = x$. These are hypotheses for the theory of a function with period three. Note that in this theory the only relation symbol is $=$ and the only function symbol is s.

   Recall that a model for a theory given by axioms is an interpretation in which all the axioms (and their consequences) are true. Throughout we consider models in which the $=$ relation symbol is interpreted as equality. Also recall that the Gödel semantic completeness theorem is true for such models: Every consistent theory has a countable model. (The proof involves an extra construction in which an equivalence relation on the original domain is replaced by equality on a smaller domain.) An example of a model of the above theory is where the domain is three points $D = \{d_1, d_2, d_3\}$ and the function symbol s is represented as the function f with $f(d_1) = d_2$, $f(d_2) = d_3$, and $f(d_3) = d_1$.

   a. Describe all models of the theory of a function with period three.

   b. In these models must the function be an injection?

   c. Must it be onto D?

   d. What is the smallest model?

   Hint: Consider a function f of period three with domain D. All one knows about such a function is that for all d in D we have $f(d) \neq d$, $f(f(d)) \neq d$, and $f(f(f(d))) = d$. Take an element in D and describe what happens when one repeatedly applies f. Take another element and do the same thing. What pattern emerges? If D is finite, what can you say about the number of points in D?

2. Show that the theory of a function with period three is not complete. (Hint: Find a closed sentence that is true in the smallest model but is not true in all other models.)

3. Find an additional axiom that makes the theory of a function with period three categorical.

4. If a theory has only one countable model (up to isomorphism), then it is said to be categorical for countable models. Show that if a theory is categorical for countable models, then it is complete.

Chapter 12

Incomplete theories

12.1 Decidable and enumerable sets

This chapter is an overview of results involving computability. It makes no claim to rigor or to full coverage of the topics. At best it is an orientation that may lead the reader to other accounts.

Let S be a countable infinite set, such as the set of natural numbers, or a set of character strings. In any case we assume that there is a computer program that translates between S and $\mathbb{N}$. Let S' be another such set. A function $f : S \to S'$ is said to be *computable* if there is a computer program (in some reasonable programming language) that defines f. That is, the program has an input that belongs to S. It defines a calculation that terminates with an output in S'. The mapping between the input and the output is the function.

If U is a subset of S, then U is said to be *decidable* if its indicator function $1_U : S \to \{0, 1\}$ is computable. Here as usual the indicator function 1_U is defined so that $1_U(s) = 1$ if s is in U and $1_U(s) = 0$ if s is not in U.

Proposition 12.1 *If U is finite, then U is decidable.*

Proof: If U is finite, then there is a list $s_1, \ldots, s_n$ of the elements of U. The computer program checks an arbitrary input to see if it is one of these. If so, the program outputs 1. Otherwise, it outputs 0. □

Proposition 12.2 *If U is decidable, then its complement $S \setminus U$ in S is decidable.*

Proof: If χ is the indicator function of U, then χ is computable. If s is an arbitrary input, then $1 - \chi(s)$ is 1 if s is in the complement of U, and is 0 if s is not in the complement of U. □

If U is a subset of S, then U is said to be *effectively enumerable* if it is empty or if there is a computable function $f : \mathbb{N} \to S$ such that U is the range of f. In the following we may for brevity refer to such a set as *enumerable.*

Proposition 12.3 *If U is decidable, then U is enumerable.*

Proof: Suppose U is decidable. Then there is a computable function $\chi : S \to \{0, 1\}$ such that χ is 1 on each element of S and 0 on each element of S. If U is finite, then U is enumerable. Otherwise let $g : \mathbb{N} \to S$ be a computable bijection. Set $k = 0$ and $m = 0$. While $m \leq n$ replace m by $m + \chi(g(k))$ and k by $k + 1$. At the end of this loop the value of k is the number of elements of U that were encountered. Set $f(n) = g(k - 1)$. $\square$

Proposition 12.4 *If U and its complement $S \setminus U$ in S are enumerable, then U is decidable.*

Proof: Let $f : \mathbb{N} \to S$ be a computable function that enumerates U. Let $g : \mathbb{N} \to S$ be a computable function that enumerates $S \setminus U$. Suppose that both U and $S \setminus U$ are non-empty. For each s in S, define $\chi(s)$ as follows. Set n to have the value 0. While both $f(n) \neq s$ and $g(n) \neq s$, replace n by $n+1$. At the end of this loop, either $f(n) = s$ or $g(n) = s$, but not both. If $f(n) = s$ then $\chi(s) = 1$, else $\chi(s) = 0$. $\square$

Remark: If $f : S \to S'$ is a function, then the graph of f is a subset of the Cartesian product $S \times S'$. It is natural to ask what happens if the function is thought of in this way as a subset. Here is the answer.

If $f : S \to S'$ is a function, then f is computable if and only if the graph of f is decidable if and only if the graph of f is enumerable.

Here is the proof. Suppose f is computable. Define χ by $\chi(s, s') = 1$ if $f(s) = s'$. So the graph of f is decidable. Suppose the graph of f is decidable. Then the graph of f is enumerable. Suppose the graph of f is enumerable. Let g enumerate the graph of f. Let s be in S. Set $m = 0$. While $m \neq (s, f(s))$ replace m by $m + 1$. Then $f(s)$ is the second component of $g(m)$. So f is computable.

Theorem 12.5 (Church's theorem) *Consider predicate logic with at least one non-logical relation symbol. Then the set of valid sentences (sentences that are true in every interpretation) is enumerable, but not decidable.*

Church's theorem may be thought of as a result for a theory with no axioms. The proof of Church's theorem will not be attempted here.

Recall that a theory T may be defined by giving an axiom set U. Then T consists of all logical consequences of U. If the axiom set is decidable, then this allows a computer program to check whether a purported proof is a proof. If the axiom set U is decidable, then U is also enumerable.

Theorem 12.6 *If a theory T has an enumerable axiom set U, then the theory T itself is enumerable.*

Proof: Enumerate the axiom set and enumerate the sentences. For each n, consider all proofs using only the first n sentences and depending on the first n axioms. There are only finitely many such proofs. By increasing n one gets an enumeration of all proofs. In particular, one gets an enumeration of all consequences of the axioms. $\square$

Theorem 12.7 (Craig) *If a theory T has an enumerable axiom set U, then it has a decidable axiom set V.*

Proof: Let $A_0, A_1, A_2, A_3, \ldots,$ be an enumeration of U. Let $V = A_0 \wedge A_1, (A_0 \wedge A_1) \wedge A_2, ((A_0 \wedge A_1) \wedge A_2) \wedge A_3, \ldots$. It is clear that U and V define the same theory T. Let C be a sentence. If C is not a conjunction, then it is not in V. If C is a k-fold iterated conjunction, then to check whether or not C is in V, one only has to check whether C is one of the first k in the listing of V. □

Theorem 12.8 (Turing) *If a theory T is enumerable and complete, then T is decidable.*

Proof: If the theory T is enumerable, then the negations $\sim T$ of the sentences in the theory are enumerable. If the theory is complete, then the set $\sim T$ is the complement T^c of the set of sentences in the theory. But if the set and its complement are enumerable, then the set is decidable. □

From the above results we see that there are the three following possibilities for a theory T. For a complete theory the second possibility is excluded.

1. T is decidable.
2. T is not decidable, but it has an axiom set U that is decidable. In that case T is enumerable.
3. T is not enumerable.

The theories we have examined up to now fall into the first category. Most realistic theories in mathematics are in the second category. There are also theories in the third category, but they have more theoretical than practical importance.

12.2 The theory of addition and multiplication

We formulate arithmetic in a language with constant symbols 0 and 1 and with two-place function symbols $+$ and $\cdot$. The intended model is the natural numbers $\mathbb{N}$ with ordinary addition and multiplication.

Theorem 12.9 (Gödel incompleteness theorem) *If an axiom set U for arithmetic is enumerable, then the resulting theory T is not complete.*

This famous result is purely syntactic, and so it might well be called the *syntactic incompleteness theorem.* A proof may be found in [14]. There is a decidable axiom set U for arithmetic that generates a theory T known as Peano arithmetic. By the Gödel incompleteness theorem, Peano arithmetic is incomplete. It is known that Peano arithmetic is enumerable, but not decidable.

Corollary 12.10 *The theory* $T = \mathrm{Th}(\mathbb{N})$ *of all true statements of arithmetic in the language with 0, 1, + and · is complete, but not enumerable.*

Proof: The theory of all true statements of arithmetic is complete. Suppose it were enumerable. By the Gödel incompleteness theorem, the theory would not be complete. This is a contradiction. □

The fact that the theory T of all true statements of arithmetic is not enumerable and has no decidable axiom set means that it is very difficulty to know the theory entirely. Still, it is a complete theory. Furthermore, the natural numbers are a model, that is, $\mathbb{N} \Vdash\!\!= T$. Does that mean that it uniquely defines the number system $\mathbb{N}$? The answer is no.

Theorem 12.11 *The theory* T *of all true statements of arithmetic has non-standard models* $\mathbb{N}^*$ *such that* $\mathbb{N}^* \Vdash\!\!= T$.

Proof: Let T be the theory of all true sentences of arithmetic. Consider an extended language with a new constant symbol c. Let T_∞ be T together with the axioms $\neg c = 0, \neg c = 1, \neg c = 1 + 1, \neg c = 1 + 1 + 1, \cdots$. Enumerate the axioms of T_∞. Let T_n be the first n axioms. Then T_n has a model, namely the standard model $\mathbb{N}$. Hence by the compactness theorem T_∞ has a model. This model must be non-standard. □

The countable non-standard models of the theory of arithmetic are extraordinarily complicated. A useful reference for model theory is the book [12].

Problems

1. Consider the theory of a dense linear order with greatest element and with least element. Is this theory categorical for countable models? Prove that your answer is correct.

2. Is it categorical? Prove that your answer is correct.

3. Is it complete? Prove that your answer is correct.

4. Consider a logical language with relation symbols $\Vdash\!\!=$, $\vdash$, and $\cong$. Suppose that it also has a one-place function symbol $\sim$ and a two-place function symbol &.

   Consider the following hypotheses:

   $$\forall M \forall B (M \Vdash\!\!= T \& B \Rightarrow M \Vdash\!\!= T)$$

   and

   $$\forall M \forall B (M \Vdash\!\!= T \& B \Rightarrow M \Vdash\!\!= B)$$

   and

   $$\forall M \forall C \, \neg (M \Vdash\!\!= C \wedge M \Vdash\!\!= \sim C)$$

   and

   $$\forall M \forall N (M \cong N \Rightarrow \forall A (M \Vdash\!\!= A \Rightarrow N \Vdash\!\!= A))$$

and

$$\forall C\,(\neg T \vdash C \Rightarrow \exists M\; M \Vvdash T \& \sim C)$$

Use natural deduction to show that

$$\forall M \forall N\,((M \Vvdash T \wedge N \Vvdash T) \Rightarrow M \cong N) \Rightarrow \forall A\,(T \vdash A \vee T \vdash \sim A)$$

Chapter 13

Sets and Cardinal Number

13.1 Sets

The purpose of this chapter is to record terminology about sets and functions and numbers and to establish basic facts about infinite cardinal numbers.

It is natural to begin with sets. If A is a set, the expression

$$t \in A \tag{13.1}$$

can be read simply "t in A". Alternatives are "t is a member of A, or "t is an element of A", or "t belongs to A", or "t is in A". The expression $\neg t \in A$ is often abbreviated $t \notin A$ and read "t not in A".

If A and B are sets, the expression

$$A \subseteq B \tag{13.2}$$

is defined in terms of membership by

$$\forall t\,(t \in A \Rightarrow t \in B). \tag{13.3}$$

This can be read simply "A subset B." Alternatives are "A is included in B" or "A is a subset of B". It may be safer to avoid such phrases as "t is contained in A" or "A is contained in B", since here practice is ambiguous. Perhaps the latter is more common.

The *axiom of extensionality* says that a set is determined by its members. In other words, if $A \subseteq B$ and $B \subseteq A$, then $A = B$. Thus, if A is the set consisting of the digits that occur at least once in my car's license plate 5373, and if B is the set consisting of the odd one digit prime numbers, then $A = B$ is the same three element set. All that matters are that its members are the numbers 7,3,5.

Consider an arbitrary condition $p(x)$ expressed in the language of set theory. If B is a set, then the subset $S \subseteq B$ consisting of elements in B that satisfy that condition is denoted by

$$S = \{x \in B \mid p(x)\} \tag{13.4}$$

and is characterized by the condition that for all y

$$y \in S \Leftrightarrow (y \in B \wedge p(y))). \tag{13.5}$$

The *intersection* $A \cap B$ is characterized by saying that for all x

$$x \in A \cap B \Leftrightarrow (x \in A \wedge A \in B). \tag{13.6}$$

The *union* $A \cup B$ is characterized by saying that for all x

$$x \in A \cup B \Leftrightarrow (x \in A \vee x \in B). \tag{13.7}$$

The *relative complement* $X \setminus A$ is characterized by saying that for all x

$$x \in X \setminus A \Leftrightarrow (x \in X \wedge x \notin A). \tag{13.8}$$

Sometimes when the set X is understood the *complement* $X \setminus A$ of A is denoted A^c.

If $\Gamma \neq \emptyset$ is a set of sets, then the *intersection* $\bigcap \Gamma$ is defined by requiring that for all x

$$x \in \bigcap \Gamma \Leftrightarrow \forall A\, (A \in \Gamma \Rightarrow x \in A) \tag{13.9}$$

If Γ is a set of sets, then the *union* $\bigcup \Gamma$ is defined by requiring that for all x

$$x \in \bigcup \Gamma \Leftrightarrow \exists A\, (A \in \Gamma \wedge x \in A)) \tag{13.10}$$

There is a peculiarity in the definition of $\bigcap \Gamma$ when $\Gamma = \emptyset$. If there is a context where X is a set and every set in Γ is a subset of X, then we can define

$$\bigcap \Gamma = \{x \in X \mid \forall A\, (A \in \Gamma \Rightarrow x \in A)\}. \tag{13.11}$$

If $\Gamma \neq \emptyset$, then this definition is independent of X and is equivalent to the previous definition. On the other hand, by this definition $\bigcap \emptyset = X$. This might seem strange, since the left hand side does not depend on X. However in most contexts there is a natural choice of X, and this is the definition that is appropriate to such contexts.

The constructions $A \cap B$, $A \cup B$, $\bigcap \Gamma$, $\bigcup \Gamma$, and $X \setminus A$ are means of producing objects that have a special relationship to the corresponding logical operations $\wedge, \vee, \forall, \exists, \neg$. A look at the definitions makes this apparent.

Two sets A, B are *disjoint* if $A \cap B = \emptyset$. More generally, a set Γ of subsets of X is disjoint if for each A in Γ and $B \in \Gamma$ with $A \neq B$ we have $A \cap B = \emptyset$. A *partition* of X is a set Γ of subsets of X such that Γ is disjoint and $\emptyset \notin \Gamma$ and $\bigcup \Gamma = X$.

13.2 Ordered pairs and Cartesian product

The simplest set is the *empty set* $\emptyset$. Then there are sets with one element a; such a set is denoted $\{a\}$. Next there are sets $\{a, b\}$; such a set has one element if $a = b$ and two elements if $a \neq b$. A two element set $\{a, b\}$ is a *pair*.

There is also a very important *ordered pair* construction. If a, b are objects, then there is an object $\langle a, b\rangle$. This ordered pair has the following fundamental property: For all a, b, p, q we have

$$\langle a, b\rangle = \langle p, q\rangle \Leftrightarrow (a = p \wedge b = q). \tag{13.12}$$

If $y = \langle a, b\rangle$ is an ordered pair, then the first coordinates of y is a and the second coordinate of y is b.

There are also ordered triples and so on. The ordered triple $\langle a, b, c\rangle$ is equal to the ordered triple $\langle p, q, r\rangle$ precisely when $a = p$ and $b = q$ and $c = r$. If $z = \langle a, b, c\rangle$ is an ordered triple, then the coordinates of z are a, b and c. The ordered n-tuple construction has similar properties.

There are degenerate cases. There is an ordered 1-tuple $\langle a\rangle$. If $x = \langle a\rangle$, then its only coordinate is a. Furthermore, there is an ordered 0-tuple $\langle\ \rangle = \emptyset$.

Corresponding to these constructions there is a set construction called *Cartesian product*. If A, B are sets, then $A \times B$ is the set of all ordered pairs $\langle a, b\rangle$ with $a \in A$ and $b \in B$.

One can also construct Cartesian products with more factors. Thus $A \times B \times C$ consists of all ordered triples $\langle a, b, c\rangle$ with $a \in A$ and $b \in B$ and $c \in C$.

The Cartesian product with only one factor is the set whose elements are the $\langle a\rangle$ with $a \in A$. There is a natural correspondence between this somewhat trivial product and the set A itself. The correspondence associates to each $\langle a\rangle$ the corresponding coordinate a. The Cartesian product with zero factors is a set $\{\emptyset\}$ with precisely one element $\emptyset$.

There is a notion of sum of sets that is dual to the notion of product of sets. This is the *disjoint union* of two sets. The idea is to attach labels to the elements of A and B. Thus, for example, for each element a of A consider the ordered pair $\langle 0, a\rangle$, while for each element b of B consider the ordered pair $\langle 1, b\rangle$. Even if there are elements common to A and B, their tagged versions will be distinct. Thus the sets $\{0\} \times A$ and $\{1\} \times B$ are disjoint. The disjoint union of A and B is the set

$$A + B = \{0\} \times A \cup \{1\} \times B. \tag{13.13}$$

One can also construct disjoint unions with more summands in the obvious way.

13.3 Relations

A *relation* R between sets A and B is a subset of $A \times B$. In this context one often writes xRy instead of $\langle x, y\rangle \in R$ and says that x is related to y by the relation R. A relation between A and A is called a relation on the set A.

There are two common ways of picturing a relation R between A and B. The first is the *graph* of the relation. This is the subset of the product space $A \times B$ consisting of the points $\langle x, y\rangle$ in R. In the special case of a relation on A, the elements $\langle x, x\rangle$ belong to the *diagonal*. This diagonal corresponds to the *identity relation* on A.

The other picture is the *cograph* of the relation. In the case of a relation R between A and B, draw the disjoint union $A + B$. For each $\langle x, y\rangle$ in R sketch an arrow from the tagged x to the tagged y. In the special case of a relation on A, it is sufficient to draw A. Then for each $\langle x, y\rangle$ in R sketch an arrow from x to y. The elements on the diagonal correspond to arrows from x to itself.

Consider a relation R on A. The relation R is *reflexive* if for each x in A we have xRx. For a reflexive relation the diagonal is a subset of the graph. The cograph of a relation known to be reflexive may be sketched omitting the arrows from a point to itself, since their inclusion is automatic.

The relation R is *symmetric* if for each x and y in A we have that xRy implies yRx. For a symmetric relation the graph is symmetric across the diagonal. The cograph of a relation known to be reflexive may be sketched using lines instead of arrows.

The relation R is *transitive* if for each x, y, z in A the conjunction xRy, yRz implies xRz. The transitivity condition may be checked in the cograph by following along the arrows.

A relation that is reflexive, symmetric, and transitive (RST) is called an *equivalence relation.*

Theorem 13.1 *Consider a set A. Let Γ be a partition of A. Then there is a corresponding equivalence relation E, such that $\langle x, y\rangle \in E$ if and only if for some subset U in Γ both x in U and y in U. Conversely, for every equivalence relation E on A there is a unique partition Γ of A that gives rise to the relation in this way.*

The sets in the partition defined by the equivalence relation are called the *equivalence classes* of the relation. The partition of A defined by an equivalence relation E is called the *quotient* and is denoted A/E.

A relation R on A is *antisymmetric* if for each x, y in A the conjunction xRy, yRx implies $x = y$. A *ordering* of A is a relation that is reflexive, antisymmetric, and transitive (RAT). Ordered sets will merit further study.

13.4 Functions

A *function* $f : A \to B$ with *domain* A and *target* (or *codomain*) B assigns to each element x of A a unique element $f(x)$ of B. The *graph* of a function is the subset of the Cartesian product $A \times B$ consisting of all ordered pairs $\langle x, y\rangle$ with $x \in A$ and $y = f(x)$.

Sometimes a function is regarded as being identical with its graph as a subset of the Cartesian product. On the other hand, there is something to be said for a point of view that makes the notion of function as fundamental as the notion of set. In that perspective, each function from A to B has a graph that is a subset of $A \times B$. The function is an operation with an input and output, and the graph is a set that describes the function.

There is a useful function builder notation that corresponds to the set builder notation. Say that it is known that for every x in A there is another corresponding object $\phi(x)$ in B. The notation is

$$f = \{x \mapsto \phi(x) : A \to B\}. \tag{13.14}$$

As a graph this is defined by

$$f = \{\langle x, \phi(x)\rangle \in A \times B \mid x \in A\}. \tag{13.15}$$

This is an explicit definition of a function from A to B. It could be abbreviated as $\{x \mapsto \phi(x)\}$ when the restrictions on x and $\phi(x)$ are clear. The variables in such an expression are of course bound variables. For instance, the squaring function $u \mapsto u^2$ is the same as the squaring function $t \mapsto t^2$.

There are other binding operations in mathematics. The integral of the function $t \mapsto t^2$ from 1 to 2 is

$$\int_1^2 t^2\,dt = \frac{7}{3}.$$

The variable of integration t is a bound variable.

There is a general framework for bound variables in which the fundamental notion is the function builder notation. The set builder and even the quantifiers are then special cases. It is called *lambda calculus* and is usually presented in somewhat unfamiliar notation. It has even been proposed as a framework for mathematics in place of set theory [1].

The set of values $f(x)$ for x in A is called the *range* of f or the *image* of A under f. In general for $S \subseteq A$ the set $f[S]$ of values $f(x)$ in B for x in A is called the *image* of S under f. On the other hand, for $T \subseteq B$ the set $f^{-1}[T]$ consisting of all x in A with $f(x)$ in T is the *inverse image* of T under f. In this context the notation f^{-1} does not imply that f has an inverse function.

The function is *injective* (or one-to-one) if $f(x)$ uniquely determines x, and it is *surjective* (or onto) if each element of B is an $f(x)$ for some x, that is, the range is equal to the target. The function is *bijective* if it is both injective and surjective. In that case it has an *inverse function* $f^{-1} : B \to A$.

If $f : A \to B$ and $g : B \to C$ are functions, then the *composition* $g \circ f : A \to C$ is defined by $(g \circ f)(x) = g(f(x))$ for all x in A.

Say that $r : A \to B$ and $s : B \to A$ are functions and that $r \circ s = I_B$, the identity function on B. That is, say that $r(s(b)) = b$ for all b in B. In this situation r is a *left inverse* of s and s is a *right inverse* of r.

Theorem 13.2 *If r has a right inverse, then r is a surjection.*

Theorem 13.3 *If s has a left inverse, then s is an injection.*

Theorem 13.4 *Suppose $s : B \to A$ is an injection. Assume that $B \neq \emptyset$. Then there exists a function $r : A \to B$ that is a left inverse to s.*

Proof: Since B is not empty, there is an element $b \in B$. For each $y = s(x)$ in the range of s define $r(y) = x$. For each y not in the range of s define $r(y) = b$. □

Theorem 13.5 *Suppose $r : A \to B$ is a surjection. Then there is a function s that is a right inverse to r.*

Proof: For every b in N there is a set of x with $r(x) = b$, and since r is a surjection, each such set is non-empty. The function s makes a choice $s(b)$ of an element in each set. □

13.5 Cartesian powers

The set of all subsets of A is called the *power set* of A and is denoted $P(A)$. Thus $S \in P(A)$ is equivalent to $S \subseteq A$.

The set of all functions from A to B is denoted B^A and is called a *Cartesian power*. If we think of n as the set $\{1, \ldots, n\}$, then $\mathbb{R}^n$ is a Cartesian power.

Write $2 = \{0, 1\}$. Each element of 2^A is the *indicator function* of a subset of A. There is a natural bijective correspondence between the 2^A and $P(A)$. If χ is an element of 2^A, then $\chi^{-1}[1]$ is a subset of A. On the other hand, if X is a subset of A, then the indicator function 1_X that is 1 on X and 0 on $A \setminus X$ is an element of 2^A. (Sometimes an indicator function is called a characteristic function, but this term has other uses.)

13.6 Number systems

This section is a quick review of the number systems commonly used in mathematics. Here is a list.

- The set $\mathbb{N} = \{0, 1, 2, 3, \ldots\}$ is the set of all *natural numbers*. It is used to count finite sets. For each finite set there is an associated natural number that describes how many elements are in the set. For the empty set $\emptyset$ the associated number is of course 0. It is sometimes useful to consider the set of natural numbers with zero removed. In this following we denote this set by $\mathbb{N}_+ = \{1, 2, 3, \ldots\}$.

- The set $\mathbb{Z} = \{\ldots, -3, -2, -1, 0, 1, 2, 3, \ldots\}$ is the set of all *integers*. The name for this set comes from the German word *zahlen*, meaning numbers.

- The set $\mathbb{Q}$ of *rational numbers* consists of all quotients of integers, where the denominator is not allowed to be zero.

- The set $\mathbb{R}$ is the set of *real numbers*. The transition from $\mathbb{Q}$ to $\mathbb{R}$ is the transition from algebra to analysis. The result is that it is possible to solve equations by approximation rather than by algebraic means.

- The set $\mathbb{C}$ is the set of all *complex numbers*. Each complex number is of the form $a + bi$, where a, b are real numbers, and $i^2 = -1$.

- The set $\mathbb{H}$ is the set of all *quaternions*. Each quaternion is of the form $t + ai + bj + ck$, where t, a, b, c are real numbers. Here $i^2 = -1, j^2 = -1, k^2 = -1$, $ij = k$, $jk = i$, $ki = j$, $ji = -k$, $kj = -i$, $ik = -j$. A pure quaternion is one of the form $ai + bj + ck$. The product of two pure quaternions is $(ai + bj + ck)(a'i + b'j + c'k) = -(aa' + bb' + cc') + (bc' - cb')i + (ca' - ac')j + (ab' - ba')k$. Thus quaternion multiplication includes both the dot product and the cross product in a single operation. The letter H in the notation is used in honor of Hamilton, who discovered these numbers.

In summary, the number systems of mathematics are $\mathbb{N}, \mathbb{Z}, \mathbb{Q}, \mathbb{R}, \mathbb{C}, \mathbb{H}$. The systems $\mathbb{N}, \mathbb{Z}, \mathbb{Q}, \mathbb{R}$ each have a natural linear order, and there are natural order preserving injective functions from $\mathbb{N}$ to $\mathbb{Z}$, from $\mathbb{Z}$ to $\mathbb{Q}$, and from $\mathbb{Q}$ to $\mathbb{R}$. The natural algebraic operations in $\mathbb{N}$ are addition and multiplication. In $\mathbb{Z}$ they are addition, subtraction, and multiplication. In $\mathbb{Q}, \mathbb{R}, \mathbb{C}, \mathbb{H}$ they are addition, subtraction, multiplication, and division by non-zero numbers. In $\mathbb{H}$ the multiplication and division are non-commutative. The number systems $\mathbb{R}, \mathbb{C}, \mathbb{H}$ have the completeness property, and so they are particularly useful for analysis.

13.7 Cardinality and Cantor's theorem on power sets

Say that a set A is *countable* if A is empty or if there is a surjection $f : \mathbb{N} \to A$.

Theorem 13.6 *If A is countable, then there is an injection from $A \to \mathbb{N}$.*

Proof: This can be proved without the axiom of choice. For each $a \in A$, define $g(a)$ to be the least element of $\mathbb{N}$ such that $f(g(a)) = a$. Then g is the required injection. □

There are sets that are not countable. For instance, $P(\mathbb{N})$ is such a set. This follows from the following theorem of Cantor.

Theorem 13.7 (Cantor) *Let X be a set. There is no surjection from X to $P(X)$.*

The proof that follows is a diagonal argument. Suppose that $f : X \to P(X)$. Form an array of ordered pairs $\langle a, b \rangle$ with a, b in X. One can ask whether $b \in f(a)$ or $b \notin f(a)$. The trick is to look at the diagonal $a = b$ and construct the set of all a where $a \notin f(a)$.

Proof: Assume that $f : X \to P(X)$. Let $S = \{x \in X \mid x \notin f(x)\}$. Suppose that S were in the range of f. Then there would be a point a in X with $f(a) = S$. Suppose that $a \in S$. Then $a \notin f(a)$. But this means that $a \notin S$.

This is a contradiction. Thus $a \notin S$. This means $a \notin f(a)$. Hence $a \in S$. This is a contradiction. Thus S is not in the range of f. □

One idea of Cantor was to associate to each set A, finite or infinite, a *cardinal number* $\#A$. Each number in $\mathbb{N}$ is a *finite cardinal number*. If there is a bijection between two sets, then they have the same cardinal number. If there is no bijection, then the cardinal numbers are different. That is, the statement $\#A = \#B$ is equivalent to saying that there is a bijection from A to B.

The two most important infinite cardinal numbers are $\omega_0 = \#\mathbb{N}$ and $c = \#P(\mathbb{N})$. The Cantor theorem shows that these are different cardinal numbers. The cardinal number ω_0 is the smallest infinite cardinal number; sometimes it is called the *countable infinite cardinal number*. The countable cardinal numbers are the natural numbers together with ω_0.

13.8 Bernstein's theorem for sets

If there is an injection $f : A \to B$, then it is natural to say that $\#A \leq \#B$. Thus, for example, it is easy to see that $\omega_0 \leq c$. In fact, by Cantor's theorem $\omega_0 < c$. The following theorem is proved in the problems.

Theorem 13.8 (Bernstein) *If there is an injection $f : A \to B$ and there is an injection $g : B \to A$, then there is a bijection $h : A \to B$.*

It follows from Bernstein's theorem that $\#A \leq \#B$ and $\#B \leq \#A$ together imply that $\#A = \#B$. This result gives a way of calculating the cardinalities of familiar sets.

Theorem 13.9 *The set $\mathbb{N}^2 = \mathbb{N} \times \mathbb{N}$ has cardinality ω_0.*

Proof: It is sufficient to count $\mathbb{N}^2$ via a bijection $f : \mathbb{N} \to \mathbb{N}^2$. Think of $\mathbb{N}^2$ as arranged in rows and columns. It would be futile to try to count the rows in order, and it would be equally futile to try to count the columns in order. But a limited search does what is wanted. For each $n = 0, 1, 2, 3, \ldots$ consider the set A_n consisting of the $2n + 1$ ordered pairs $\langle i, j \rangle$ with $\max(i, j) = n$. It is sufficient to count these in order. □

Corollary 13.10 *A countable union of countable sets is countable.*

Proof: Let Γ be a countable collection of countable sets. Then there exists a surjection $u : \mathbb{N} \to \Gamma$. For each $S \in \Gamma$ choose a function that assigns to each S in Γ a surjection $v_S : \mathbb{N} \to S$. Let $w(m, n) = v_{u(m)}(n)$. Then v is a surjection from $\mathbb{N}^2$ to $\bigcup \Gamma$. It is a surjection because each element q of $\bigcup \Gamma$ is an element of some S in Γ. There is an m such that $u(m) = S$. Furthermore, there is an n such that $v_S(n) = q$. It follows that $w(m, n) = q$. However once we have the surjection $w : \mathbb{N}^2 \to \bigcup \Gamma$ we also have a surjection $\mathbb{N} \to \mathbb{N}^2 \to \bigcup \Gamma$. □

Theorem 13.11 *The set $\mathbb{Z}$ of integers has cardinality ω_0.*

Proof: There is an obvious injection from $\mathbb{N}$ to $\mathbb{Z}$. On the other hand, there is also a surjection $(m, n) \mapsto m - n$ from $\mathbb{N}^2$ to $\mathbb{Z}$. There is a bijection from $\mathbb{N}$ to $\mathbb{N}^2$ and hence a surjection from $\mathbb{N}$ to $\mathbb{Z}$. Therefore there is an injection from $\mathbb{Z}$ to $\mathbb{N}$. This proves that $\#\mathbb{Z} = \omega_0$. □

Theorem 13.12 *The set $\mathbb{Q}$ of rational numbers has cardinality ω_0.*

Proof: There is an obvious injection from $\mathbb{Z}$ to $\mathbb{Q}$. On the other hand, there is also a surjection from $\mathbb{Z}^2$ to $\mathbb{Q}$ given by $(m, n) \mapsto m/n$ when $n \neq 0$ and $(m, 0) \mapsto 0$. There is a bijection from $\mathbb{Z}$ to $\mathbb{Z}^2$. (Why?) Therefore there is a surjection from $\mathbb{Z}$ to $\mathbb{Q}$. It follows that there is an injection from $\mathbb{Q}$ to $\mathbb{Z}$. (Why?) This proves that $\#\mathbb{Q} = \omega_0$. □

Theorem 13.13 *The set $\mathbb{R}$ of real numbers has cardinality c.*

Proof: First we give an injection $f : \mathbb{R} \to P(\mathbb{Q})$. In fact, we let $f(x) = \{q \in \mathbb{Q} \mid q \leq x\}$. This maps each real number x to a set of rational numbers. If $x < y$ are distinct real numbers, then there is a rational number r with $x < r < y$. This is enough to establish that f is an injection. From this it follows that there is an injection from $\mathbb{R}$ to $P(\mathbb{N})$.

Recall that there is a natural bijection between $P(\mathbb{N})$ (all sets of natural numbers) and $2^{\mathbb{N}}$ (all sequences of zeros and ones). For the other direction, we give an injection $g : 2^{\mathbb{N}} \to \mathbb{R}$. Let

$$g(s) = \sum_{n=0}^{\infty} \frac{2s_n}{3^{n+1}}. \tag{13.16}$$

This maps $2^{\mathbb{N}}$ as an injection with range equal to the Cantor middle third set. This completes the proof that $\#\mathbb{R} = c$. □

Theorem 13.14 *The set $\mathbb{R}^{\mathbb{N}}$ of infinite sequences of real numbers has cardinality c.*

Proof: Map $\mathbb{R}^{\mathbb{N}}$ to $(2^{\mathbb{N}})^{\mathbb{N}}$ to $2^{\mathbb{N} \times \mathbb{N}}$ to $2^{\mathbb{N}}$. □

The cardinal number c is also called the *cardinality of the continuum*, since $c = \#\mathbb{R}$. The *continuum hypothesis* is that there are no cardinal numbers strictly larger than ω_0 and strictly smaller then c. It was shown in remarkable work by Gödel and even more remarkable work by Cohen that it is impossible to determine whether the continuum hypothesis is true or false on the basis of the usual principles of set theory.

Problems

Let A be a set and let $f : A \to A$ be a function. An orbit is a set of points obtained in the following way. Start with a point a in A. The orbit of a is the smallest set with the following three properties. First, a is in A. Second, if x is in the orbit, then $f(x)$ is also in the orbit. Third, if $f(x)$ is in the orbit, then x is also in the orbit.

Theorem 1. Let A be a set and let $f : A \to A$ be a bijection. Then A is the disjoint union of orbits with the following structure. The action on each orbit is either isomorphic to the shift on $\mathbf{Z}_n$ for some $n \geq 1$ or to the shift on $\mathbf{Z}$.

Theorem 2. Let A be a set and let $f : A \to A$ be an injection. Then A is the disjoint union of orbits with the following structure. The action on each orbit is either isomorphic to the shift on $\mathbf{Z}_n$ for some $n \geq 1$ or to the shift on $\mathbf{Z}$ or to the shift on $\mathbf{N}$.

1. My social security number is 539681742. This defines a function defined on 123456789. It is a bijection from a nine point set to itself. What are the orbits? How many are they? How many points in each orbit?

2. Let $f : \mathbb{R} \to \mathbb{R}$ be defined by $f(x) = x+1$. What are the orbits? How many are they (cardinal number)? How many points in each orbit (cardinal number)?

3. Let $f : \mathbb{R} \to \mathbb{R}$ be defined by $f(x) = 2\arctan(x)$. (Recall that the derivative of $f(x)$ is $f'(x) = 2/(1 + x^2) > 0$, so f is strictly increasing.) What is the range of f? How many points are there in the range of f (cardinal number)? What are the orbits? How many are there (cardinal number)? How many points in each orbit (cardinal number)? Hint: It may help to use a calculator or draw graphs.

4. Let $f : A \to A$ be an injection with range $R \subseteq A$. Let R' be a set with $R \subseteq R' \subseteq A$. Show that there is an injection $j : A \to A$ with range R'. Hint: Use Theorem 2.

5. Bernstein's theorem. Let $g : A \to B$ be an injection, and let $h : B \to A$ be an injection. Prove that there is a bijection $k : A \to B$. Hint: Use the result of the previous problem.

Chapter 14

Ordered sets

14.1 Ordered sets and linearly ordered sets

The purpose of this chapter is to review terminology for ordered sets [15]. This will help distinguish concepts that could easily be confused, such as maximal element and greatest element.

An *pre-ordered set* is a set W and a binary relation $\leq$ that is a subset of $W \times W$. The pre-order relation $\leq$ must satisfy the first two of the following properties:

1. $\forall p\, p \leq p$ (reflexivity)
2. $\forall p\, \forall q\, \forall r\, ((p \leq q \land q \leq r) \Rightarrow p \leq r)$ (transitivity)
3. $\forall p\, \forall q\, ((p \leq q \land q \leq p) \Rightarrow p = q)$ (antisymmetry)

If it also satisfies the third property, then it is an *ordered set*. An ordered set is often called a *partially ordered set* or a *poset*. In an ordered set we write $p < q$ if $p \leq q$ and $p \neq q$. Once we have one ordered set, we have many related order sets, since each subset of an ordered set is an ordered set in a natural way.

In an ordered set we say that p, q are *comparable* if $p \leq q$ or $q \leq p$. An ordered set is *linearly ordered* (or *totally ordered*) if each two points are comparable. (Sometime a linearly ordered set is also called a *chain*.)

Here is another equivalent definition of ordered set. The axioms are

1. $\forall p\, \neg p < p$ (irreflexivity)
2. $\forall p\, \forall q\, \forall r\, ((p < q \land q < r) \Rightarrow p < r)$ (transitivity)

The asymmetry property $\forall p \forall q\, \neg(p < q \land q < p)$ is a consequence of these two axioms. The relation between these two notions is that $p \leq q$ is equivalent to $p < q$ or $p = q$, while $p < q$ is equivalent to $p \leq q$ and $p \neq q$.

For each $m \in \mathbb{N}$ there is a finite linearly ordered set with m elements. These all look the same. They may be realized as $\{0, 1, 2, \ldots, m-1\}$ or as $\{1, 2, 3, \ldots, m\}$.

Infinite linearly ordered sets are more interesting. Standard examples are obtained by looking at the ordering of number systems. Thus we shall denote by **N** a set that is ordered in the same way as $\mathbb{N}$ or $\mathbb{N}_+$. Thus it has a discrete linear order with a least element but no greatest element. Similarly, **Z** is a set ordered the same way as the integers. It has a discrete linear order but without either greatest or least element. The set **Q** is ordered like the rationals. It is a countable densely ordered set with no greatest or least element. Finally, **R** is a set ordered like the reals. It is an uncountable densely ordered set with no greatest or least element.

Examples:

1. The ordered sets **N**, **Z**, **Q**, and **R** are linearly ordered sets.
2. Let I be a set and let W be an ordered set. Then W^I with the pointwise ordering is an ordered set.
3. In particular, $\mathbf{R}^I$, the set of all real functions on I, is an ordered set.
4. In particular, $\mathbf{R}^n$ is an ordered set.
5. If X is a set, the power set $P(X)$ with the subset relation is an ordered set.
6. Since $2 = \{0, 1\}$ is an ordered set, the set 2^X with pointwise ordering is an ordered set. (This is the previous example in a different form.)

14.2 Greatest and least; maximal and minimal

Let W be an ordered set. An element p of W is the *least* element of W if $\forall r \in W\, p \leq r$. An element q of W is the *greatest* element of W if $\forall r \in W\, r \leq q$.

An element p of W is a *minimal* element of W if $\forall r \in W\, (r \leq p \Rightarrow r = p)$. An element q of W is a *maximal* element of W if $\forall r \in W\, (q \leq r \Rightarrow r = q)$.

Theorem 14.1 *If p is the least element of W, then p is a minimal element of W. If q is the greatest element of W, then a is a maximal element of W.*

In a linearly ordered set a minimal element is the least element and a maximal element is the greatest element.

If W is an ordered set, and $S \subseteq W$, then S may also be regarded as an ordered set. There are various constructions that produce subsets. One is the closed interval construction, for which $[a, b]$ is the set of r with $a \leq r \leq b$. In this case a is a least element and b is a greatest element of $[a, b]$.

Chapter 15

Rooted Trees

15.1 Rooted tree concepts

A *rooted tree* is an ordered set with a least element r (the root) such that for each t in the set the interval $[r, t]$ is a finite linearly ordered set. If $s < t$ in the rooted tree, then we say that s precedes t and that t is a successor of s. It is clear that the root precedes each other element of the rooted tree. The interval $[r, t]$ consists of t and its predecessors.

It follows from this definition that each element of the rooted tree, other than the root, has a unique immediate predecessor. On the other hand, each element may have a number of immediate successors. If an element has no successors, then it is a maximal element. It this context a maximal element may also be called an *end element*. Another term for a maximal element is *leaf*. A finite rooted tree will have maximal elements, but an infinite rooted tree need not have maximal elements.

A rooted tree has a recursive structure. It may be thought of as a root element, together with a collection (possibly empty) of new rooted trees. These new rooted trees have roots that are the immediate successors of the root of the original rooted tree.

The notion of rooted tree occurs in set theory, in graph theory, and in computer science. Because it occurs in so many domains there are multiple variants of terminology. The reader should always check to see what terms are being used in a given context. While drawing a rooted tree it might seem natural to place the root at the bottom, but the opposite convention is also common.

15.2 König's lemma

A rooted tree is *binary* if each element has zero, one, or two successors. A rooted tree is *finitely generated* if each point has at most finitely many immediate successors. A rooted tree is *countably generated* if each point has at most countably many immediate successors.

A *branch* of a rooted tree is a maximal linearly ordered subset. A branch is either finite running from the root to an end point, or it is ordered like the natural numbers starting from the root. It is possible to have an infinite rooted tree with only finite branches. *König's lemma* gives a condition that rules this out.

Theorem 15.1 (König's lemma) *If a rooted tree is finitely generated, then if each branch is finite, the rooted tree is finite.*

Proof: Consider a finitely generated rooted tree. Suppose it is infinite. Define a branch inductively as follows. Start with the root. There are infinitely many elements above the root. Having reached an element with infinitely many elements above it, look at the finitely many trees rooted in the immediate successors of this element. At least one of these must be infinite. Choose such an infinite tree. Its root is the next element, and it continues to have infinitely many elements above it. This inductive construction produces an infinite branch. □

15.3 Search of a rooted tree

A *search* of a rooted tree is a sequence (finite or infinite) of distinct points in the rooted tree that starts at the root and such that no point on the rooted tree is in the sequence before its immediate predecessor is in the sequence. The range of a search is a subtree of the original rooted tree. The search provides an increasing function from this subtree to a linearly ordered set. The search is complete if it succeeds in searching the entire rooted tree.

Consider a rooted tree. There are two obvious kinds of searches.

A *depth-first search* may be conducted by the following procedure. Start with the root. When the search reaches a certain point on the rooted tree, then search in turn each of the subtrees corresponding to immediate successors. This kind of search is complete when the rooted tree is finite.

A *breadth-first search* may be conducted as follows. Start with the root at level 0. Then search all points at level n before searching all points at level $n+1$. This kind of search is complete when the rooted tree is finitely generated.

Example: Consider the rooted tree consisting of words on an alphabet with two letters, 0 and 1. A depth-first search would start with the root (the empty word) and then continue with 0, 00, 000, 0000, and so on. It would never get to 1. On the other hand, a breadth-first search would start with the root, the continue with 0,1, 00,01,10,11, 000, 001,010,011,100,101, 110,111, and so on. The breadth-first search is complete. In particular, the rooted tree has countably many points. Notice, however, that the number of branches is uncountable. This is because each branch is given by an infinite sequence of 0's and 1's, and there are uncountably many such infinite sequences.

If a rooted tree is countably generated, then the situation is more complicated. Arrange the immediate successors of each element in a sequence starting with 0. Start with the root at stage 0. Say that the search has been conducted through stage n. At stage $n+1$ search all the remaining points at level $\leq n+1$ that are $\leq n+1$ in the appropriate sequences. This might be called a *limited search*.

Example: Consider the rooted tree consisting of words on an alphabet $0, 1, 2, 3, 4, \ldots$ that is countably infinite. The breadth-first search would start with the root (the empty word) and then continue with $0, 1, 2, 3, 4, \ldots$ and never get to 00. The limited search is more complicated. At stage 0 it counts the root. At stage 1 it counts 1. At stage 2 it counts 11,12, 2, 21, 22. At stage 3 it counts 111,112,113,121,122,123,13,131,132,133,211,212,213 and then 23,231,232,233 and finally 3,31,311,312,313,32,321,322,323,33,331,332,333. The words get longer, and they use more letters, but in a limited way. The limited search is complete. In particular, this rooted tree has countably many points.

Chapter 16

Appendix: Intuitionistic logic

16.1 Propositional logic

This chapter is a brief sketch of intuitionistic logic, designed to point out the contrast with classical logic. Intuitionistic logic is more general; while many of the rules of classical logic continue to hold, some rules fail in interesting ways. This puts classical logic in a richer context. Some references are [20, 3, 8]

Intuitionistic logic arose from an idea in philosophy of mathematics called intuitionism. This is sometimes regarded as a form of constructivism. However, there is another view of intuitionistic logic: it is a logic of evolution. The truth value of a sentence evolves as a function of time. If it is false at one time, it may be true at a later time. Once it becomes true, then it remains true in the future.

The notion of time is convenient in explaining the theory, but the formulation is considerably more general. There is a fixed partially ordered set $\mathcal{T}$. Each t in $\mathcal{T}$ is thought of as a time, or more generally, as a stage of development.

First consider propositional logic in the framework of intuitionism. The truth of a sentence is an increasing function of time. Thus if $t \leq t'$, and a sentence A is true at time t, then it is true at t'.

Example: A rather simple example is the linearly ordered set $\{1, 2, 3, \ldots, m\}$ with m stages of development. The possible sets on which a sentence can be true are of the form $\{k, \ldots, m\}$ with $1 \leq k \leq m$ together with the empty set $\emptyset$. There are $m + 1$ possible truth values, corresponding to these truth sets.

The simplest non-trivial case is when $m = 2$. In this case the possible truth sets are $\{0, 1\}$, $\{1\}$, and $\emptyset$. These correspond to always true, eventually (but not always) true, and never true.

Example: Another example has a first stage that may develop in one of two ways. Thus there is a stage t and two later stages with $t < t'$ and $t < t''$. The stages t', t'' are not comparable. There are five possible truth sets: all three stages, both future stages t, t', the future stage t' alone, the future stage t'' alone, and no stages.

The semantics of intuitionistic logic is called *Kripke semantics*. Here are the rules for the connectives.

- $A \wedge B$ is true at t iff A true at t and B true at t.
- $A \vee B$ is true at t iff A true at t or B true at t.
- $A \Rightarrow B$ is true at t iff for all t' with $t \leq t'$, A true at t' implies B true at t'.

The third definition is crucial. To say that the formula $A \Rightarrow B$ is true at some time is a promise about the future; it says that by the time A becomes true B will also come true. In particular, $A \Rightarrow B$ may be false at time t even if A is false at time t.

Define $\neg A$ to be $A \Rightarrow \perp$.

- $\perp$ is never true at t.
- $\neg A$ is true at t iff for all t' with $t \leq t'$, A is not true at t'.

Thus negation is also about the future. To say that $\neg A$ is true at some time is to say that A will never become true in the future. In other words, in intuitionistic logic $\neg$ means *never*.

- $\neg A$ false at s iff there exists s' with $s \leq s'$ with A true at s'.
- $\neg\neg A$ true at t iff for all t' with $t \leq t'$ there exists t'' with $t' \leq t''$ such that A is true at t''.

In simple language, $\neg\neg A$ is true at a time means that A will *eventually* be true in every future.

In intuitionistic logic the logical implication $A \models C$ means that if A is true at t, then also C is true at t. In particular, $\models C$ means that C is true for all t.

There are theorems of classical logic that are not true for intuitionistic logic. For instance, it is possible that $A \vee \neg A$ is not true for some t. This is because A could be false for this t, but true for some $t' > t$. So at time t it is neither the case that A is true nor that A will never be true.

Here are some theorems of intuitionistic logic.

- $A \models \neg\neg A$
- $\neg A \vee B \models A \Rightarrow B$
- $A \Rightarrow B \models \neg B \Rightarrow \neg A$

- $A \vee B \models \neg(\neg A \wedge \neg B)$
- $\neg A \vee \neg B \models \neg(A \wedge B)$

There are counterexamples for the inferences going the other way. For instance, take the case when there are two time instants $t < t'$, A, B both false at t, true at t'.

- $\neg\neg A$ is true at t, while A is not true at t
- $A \Rightarrow B$ is true at t, while $\neg A \vee B$ is not true at t
- $\neg(\neg A \wedge \neg B)$ is true at t, while $\neg A \vee \neg B$ is not true at t

Another interesting example is when $t < t'$, A is true at t, B is false at t but true at t'.

- $\neg B \Rightarrow \neg A$ is true at t, but $A \Rightarrow B$ is false at t

Here is a more complicated situation. Say that there is a present t and two different futures, t' and t'', so that $t < t'$ and $t < t''$. Say that A is true only at t' and B is true only at t''. The following example provides a pair of sentences that distinguish the two possible worlds.

- $\neg(A \wedge B)$ is true at t, but $\neg A \vee \neg B$ is not true at t.

The rules of natural deduction for intuitionistic logic are the same as for classical logic, except that the law of contradiction is replaced by the weaker law that says that from $\perp$ one can deduce an arbitrary formula. Alternatively, there is an intuitionistic version of Gentzen deduction where the special feature is that a sequent can have only one conclusion. Either formulation defines the notion of derivability $A \vdash B$. As before there is a soundness theorem that says that $A \vdash B$ implies $A \models B$ and a completeness theorem that says that $A \models B$ implies $A \vdash B$.

Example: Here is a typical natural deduction proof. It shows that in intuitionistic logic $\neg B \Rightarrow \neg A \vdash \neg\neg A \Rightarrow \neg\neg B$

Suppose $\neg B \Rightarrow \neg A$
  Suppose $\neg\neg A$
    Suppose $\neg B$
    $\neg A$
    $\perp$
  Thus $\neg\neg B$
Thus $\neg\neg A \Rightarrow \neg\neg B$

Example: Say that one wanted to deduce that $\neg B \Rightarrow \neg A$ leads to $A \Rightarrow B$. The obvious strategy is to suppose A. Then suppose $\neg B$. Then one gets $\neg A$ and then $\bot$. However there is no contradiction rule to remove the last supposition and get B.

16.2 Predicate logic

Intuitionistic logic also works for predicate logic. In an interpretation there is a domain $D(t)$ for each t. It is required that $t \leq t'$ implies $D(t) \subseteq D(t')$. Objects can come into existence, but they can never vanish.

- $\forall x\, A(x)$ is true at t iff for all t' with $t \leq t'$ and for every element of $D(t')$, the formula A is true at t' when x is assigned to that element.
- $\exists x\, A(x)$ is true at t iff for some element of $D(t)$, the formula A is true at t when x is assigned to that element.

The universal statement is about everything that will come to exist in the future. The existential statement also has implications for the future, since if something exists at time t it will automatically continue to exist at all times t' with $t \leq t'$.

Example: Here is a failure of one of de Morgan's laws. It is possible that $\neg\forall x\, \neg A$ is true at some instant when $\exists x\, A$ is false. As an instance, take A to be $x^2 + 1 = 0$. Take $D(\text{now}) = \mathbb{R}$, $D(\text{later}) = \mathbb{C}$. Then $\exists x\, x^2 + 1$ is false now, since the equation has no real solutions. On the other hand, $\forall x\, \neg x^2 + 1 = 0$ is always false, since complex solutions later on cannot be excluded. Thus $\neg\forall x\, \neg x^2 + 1 = 0$ is true now.

Sometimes it is said that intuitionistic logic is related to constructive methods in mathematics. This at first seems reasonable, since various assertions become more and more true with time, and occasionally new objects pop into existence. On the other hand, there is a problem with this claim. An intuitionistic statement such as $A \Rightarrow B$ is a promise about the future: B will be true by the time A is true. However it does not come equipped with a mechanism to show why this comes about. So the connection with constructive methods is far from clear.

Intuitionistic logic is a logic of systems that are undergoing some kind of development. It arises in set theory in situations involving forcing, and it is basic in topos theory [7]. Furthermore, Gödel discovered a method of translating classical logic into intuitionistic logic. It follows that all results of classical logic can also be derived in the intuitionistic framework. The logician trained in intuitionistic logic has a more powerful tool than the classical logician.

In addition, intuitionistic logic explains a quirk of mathematical practice. Mathematicians often find proofs by contradiction awkward or even unnatural. From the point of intuitionistic logic it is quite natural to avoid proofs by contradiction. In fact, they are not valid, for the simple reason that a sentence that is eventually true is not guaranteed to be true now. The intuitionistic spirit is congenial, even when it is not recognized.

Bibliography

[1] Peter B. Andrews, *An introduction to mathematical logic and type theory: To truth through proof*, Academic Press, Orlando, FL, 1986.

[2] Samuel R. Buss (ed.), *Handbook of proof theory*, Studies in Logic and the Foundations of Mathematics, no. 137, North-Holland, Amsterdam, 1998.

[3] Melvin Chris Fitting (ed.), *Intuitionistic logic, model theory, and forcing*, Studies in Logic and the Foundations of Mathematics, North-Holland, Amsterdam, 1969.

[4] James Glimm, *Reflections and perspectives*, Bulletin of the American Mathematical Society (New Series) **47** (2010), 127–136.

[5] Paul Halmos, *Algebraic logic*, Chelsea, New York, NY, 1962.

[6] Stephen Cole Kleene, *Mathematical logic*, Dover Publications, Mineola, NY, 2002.

[7] Saunders MacLane and Ieke Moerdijk, *Sheaves in geometry and logic: A first introduction to topos theory*, Springer, New York, NY, 1992.

[8] Grigori Mints, *A short introduction to intuitionistic logic*, Kluwer/Plenum, New York, NY, 2000.

[9] Sara Negri and Jan von Plato, *Structural proof theory*, Cambridge University Press, Cambridge, 2001.

[10] Edward Nelson, *Internal set theory: A new approach to non-standard analysis*, Bulletin of the American Mathematical Society **83** (1977), 1165–1198.

[11] ______, *Radically elementary probability theory*, Annals of Mathematics Studies 117, Princeton University Press, Princeton, NJ, 1987.

[12] Bruno Poizat, *A course in model theory: An introduction to contemporary mathematical logic*, Springer, New York, NY, 2000.

[13] Dag Prawitz, *Natural deduction: A proof-theoretical study*, Dover Publications, Mineola, NY, 2006.

[14] Wolfgang Rautenberg, *A concise introduction to mathematical logic*, third ed., Springer, New York, NY, 2010.

[15] Bernd S. W. Schröder, *Ordered sets: An introduction*, Birkhäuser, Boston, 2003.

[16] Stephen G. Simpson, *Mathematical logic*, Lecture notes, Department of Mathematics, Pennsylvania State University, 2008.

[17] Raymond M. Smullyan, *First-order logic*, Dover Publications, New York, NY, 1995.

[18] Gaisi Takeuti, *Proof theory*, second ed., Studies in Logic and the Foundations of Mathematics, no. 81, North-Holland, Amsterdam, 1987.

[19] A. S. Troelstra and H. Schwichtenberg, *Basic proof theory*, second ed., Cambridge Tracts in Theoretical Computer Science, no. 43, Cambridge University Press, Cambridge, 2000.

[20] Dirk van Dalen, *Logic and structure*, third ed., Springer, New York, NY, 1994.

Notation

Object language symbols	
$\wedge$	and
$\vee$	or
$\Rightarrow$	implies
$\perp$	false statement
$\neg$	not ($\Rightarrow \perp$)
$\forall$	for all
$\exists$	for some, there exists
Metalanguage symbols	
$\sim$	negation (set of formulas)
$\longrightarrow$	sequent implication
$\models$	logically implies (semantic)
$\vdash$	logically implies (syntactic)
$\Vdash$	models
$\cong$	isomorphic
Sets	
$\in$	in
$\subseteq$	subset
$\emptyset$	empty set
$\cap$	intersection (of two sets)
$\cup$	union (of two sets)
$\setminus$	relative complement (of two sets)
$\bigcap$	intersection (of collection of sets)
$\bigcup$	union (of collection of sets)
$\{\ ,\ \}$	unordered pair
$\langle\ ,\ \rangle$	ordered pair
$\times$	Cartesian product (of two sets)
$+$	disjoint union construction (two sets)
P	power set (all subsets of set)
$/$	quotient (of set by equivalence relation)

Number systems

$\mathbb{N}$	natural numbers starting at 0
$\mathbb{N}_+$	natural numbers starting at 1
$\mathbb{Z}$	integers
$\mathbb{Z}_n$	integers modulo n
$\mathbb{Q}$	rational numbers
$\mathbb{R}$	real numbers
$\mathbb{C}$	complex numbers
$\mathbb{H}$	quaternions

Cardinalities

ω_0	countable infinite cardinality
c	cardinality of the continuuum, 2^{ω_0}

Ordered sets

$\leq$	generic order relation
$<$	strict order relation
$\mathbf{N}$	set ordered like $\mathbb{N}$ or $\mathbb{N}_+$
$\mathbf{Z}$	set ordered like $\mathbb{Z}$
$\mathbf{Q}$	set ordered like $\mathbb{Q}$
$\mathbf{R}$	set ordered like $\mathbb{R}$

Index