$A \Rightarrow B \vee \forall x\ \exists y : (P(x) \rightarrow Q(x,y) \wedge R(y))\ M \models A \vee M \models_v B \Leftrightarrow [\![A]\!]^M = \mathbf{1} \vee [\![B]\!]^M_v = \mathbf{1}, \exists M : \langle \{q_0, q_1\}, \{0, 1\}, q_0, \tau \rangle \vdash S_0, \Gamma \vdash_{\mathcal{N}} B \rightarrow B, \forall x : x = x \vee \bot$

Mathematical Logic
– an Introduction

Michał Walicki

$A \Rightarrow B \vee \forall x\ \exists y : (P(x) \rightarrow Q(x,y) \wedge R(y))\ M \models A \vee M \models_v B \Leftrightarrow [\![A]\!]^M = \mathbf{1} \vee [\![B]\!]^M_v = \mathbf{1}, \exists M : \langle \{q_0, q_1\}, \{0, 1\}, q_0, \tau \rangle \vdash S_0, \Gamma \vdash_{\mathcal{N}} B \rightarrow B, \forall x : x = x \vee \bot$

Contents

The History of Logic

The term "logic" may be, very roughly and vaguely, associated with something like "correct thinking". Aristotle defined a syllogism as "discourse in which, certain things being stated something other than what is stated follows of necessity from their being so." And, in fact, this intuition not only lies at its origin, ca. 500 BC, but has been the main force motivating its development since that time until the last century.

There was a medieval tradition according to which the Greek philosopher Parmenides (5th century BC) invented logic while living on a rock in Egypt. The story is pure legend, but it does reflect the fact that Parmenides was the first philosopher to use an extended argument for his views, rather than merely proposing a vision of reality. But using arguments is not the same as studying them, and Parmenides never systematically formulated or studied principles of argumentation in their own right. Indeed, there is no evidence that he was even aware of the implicit rules of inference used in presenting his doctrine.

Perhaps Parmenides' use of argument was inspired by the practice of early Greek mathematics among the Pythagoreans. Thus it is significant that Parmenides is reported to have had a Pythagorean teacher. But the history of Pythagoreanism in this early period is shrouded in mystery, and it is hard to separate fact from legend.

We will sketch the development of logic along the three axes which reflect the three main domains of the field.

1. The foremost is the interest in correctness of reasoning which involves study of correct arguments, their *form* or *pattern* and he possibilities of *manipulating* such forms in order to arrive at new correct arguments.

The other two aspects are very intimately connected with this one.

2. In order to construct valid *forms* of arguments one has to know what such forms can be built from, that is, determine the ultimate "building blocks". In particular, one has to ask the questions about the meaning of such building blocks, of various terms and categories of terms and, furthermore, of their combinations.

3. Finally, there is the question of how to *represent* these *patterns*. Although apparently of secondary importance, it is the answer to this question which can be, to a high degree, considered the beginning of modern mathematical logic.

The first three sections sketch the development along the respective lines until Renessance. In section D, we indicate the development in modern era, with particular emphasis on the last two centuries. Section E indicates some basic aspects of modern mathematical logic and its relations to computers.

A. Logic – *patterns* of reasoning

A.1. Reductio ad absurdum

If Parmenides was not aware of general rules underlying his arguments, the same perhaps is not true for his disciple Zeno of Elea (5th century BC). Parmenides taught that there is no real change in the world and that all thing remain, eventually, the same one being. In the defense of this heavily criticized thesis, Zeno designed a series of ingenious arguments, known under the name *"Zeno's paradoxes"*, which demonstrated that the contrary assumption must lead to absurd. Some of the most known is the story of

> *Achilles and tortoise*
> *who compete in a race. Tortoise, being a slower runner, starts some time t before Achilles. In this time t, the tortoise will go some way w towards the goal. Now Achilles starts running but in order to take over the tortoise he has to first run the way w which will take him some time $t1$. In this time, tortoise will again walk some*

> *distance $w1$ away from the point w and closer to the goal. Then again, Achilles must first run the way $w1$ in order to catch the tortoise, but this will in the same time walk some distance $w2$ away. In short, Achilles will never catch the tortoise, which is obviously absurd. Roughly, this means that the thesis that the two are really changing their positions cannot be true.*

The point of the story is not what is possibly wrong with this way of thinking but that *the same form of reasoning* was applied by Zeno in many other stories: *assuming a thesis T, we can analyze it and arrive at a conclusion C; but C turns out to be absurd – therefore T cannot be true.* This pattern has been given the name *"reductio ad absurdum"* and is still frequently used in both informal and formal arguments.

A.2. Aristotle

Various ways of arguing in political and philosophical debates were advanced by various thinkers. *Sophists*, often discredited by the "serious" philosophers, certainly deserve the credit for promoting the idea of "correct arguing" no matter what the argument is concerned with. Horrified by the immorality of sophists' arguing, Plato attempted to combat them by plunging into ethical and methaphisical discussions and claiming that these indeed had a strong methodological logic – the logic of discourse, "dialectic". In terms of development of modern logic there is, however, close to nothing one can learn from that. The development of "correct reasoning" culminated in ancient Greece with Aristotle's (384-322 BC) teaching of *categorical forms* and *syllogisms*.

A.2.1. Categorical forms

Most of Aristotle's logic was concerned with certain kinds of propositions that can be analyzed as consisting of five basic building blocks: (1) usually a quantifier ("every", "some", or the universal negative quantifier "no"), (2) a subject, (3) a copula, (4) perhaps a negation ("not"), (5) a predicate. Propositions analyzable in this way were later called "categorical propositions" and fall into one or another of the following forms:

	(quantifier)	**subject**	**copula**	**(negation)**	**predicate**	
	Every, Some, No	β	is	not	an α	
1.	Every	β	is		an α	: Universal affirmative
2.	Every	β	is	not	an α	: Universal negative
3.	Some	β	is		an α	: Particular affirmative
4.	Some	β	is	not	an α	: Particular negative
5.		x	is		an α	: Singualr affirmative
		Socrates	is		a man	
6.		x	is	not	an α	: Singular negative

A.2.2. Conversions

Sometimes Aristotle adopted alternative but equivalent formulations. Instead of saying, for example, "Every β is an α", he would say, "α belongs to every β" or "α is predicated of every β." More significantly, he might use *equivalent* formulations, for example, instead of 2,he might say "No β is an α."

1. "Every β is an α"	is equivalent to	"α belongs to every β", or
	is equivalent to	"α is predicated of every β."
2. "Every β is not an α"	is equivalent to	"No β is an α."

Aristotle formulated several rules later known collectively as the theory of *conversion*. To "convert" a proposition in this sense is to interchange its subject and predicate. Aristotle observed that propositions of forms 2 and 3 can be validly converted in this way: if" no β is an α", then so too "no α is a β", and if "some β is an α", then so too some "α is a β". In later terminology, such propositions were said to be converted "simply" (simpliciter). But propositions of form 1 cannot be converted in this way; if "every β is an α", it does not follow that "every α is a β". It does follow, however, that "some α is a β". Such propositions, which can be converted provided that not only are their subjects and predicates interchanged but also the universal quantifier is weakened to a particular quantifier "some", were later said to be converted "accidentally" (per accidens). Propositions of form 4 cannot be converted at all; from the fact that some animal is not a dog, it does not follow that some dog is not an animal. Aristotle used these laws of conversion to reduce other syllogisms to syllogisms in the first figure, as described below.

Conversions represent the first form of *formal manipulation*. They provide the rules for:

> *how to replace occurrence of one (categorical) form of a statement by another – without affecting the proposition!*

What does "affecting the proposition" mean is another subtle matter. The whole point of such a manipulation is that one, in one sense or another, changes the concrete appearance of a sentence, without changing its value. In Aristotle this meant simply that the pairs he determined could be exchanged. The intuition might have been that they "essentially mean the same". In a more abstract, and later formulation, one would say that "not to affect a proposition" is "not to change its truth value" – either both are were false or both are true. Thus one obtains the idea that

> *Two statements are equivalent (interchangeable) if they have the same truth value.*

This wasn't exactly the point of Aristotle's but we may ascribe him a lot of intuition in this direction. From now on, this will be a constantly recurring theme in logic. Looking at propositions as thus determining a truth value gives rise to some questions. (And sever problems, as we will see.) Since we allow using some "placeholders" – *variables* – a proposition need not to have a unique truth value. "All α are β" depends on what we substitute for α and β. Considering however possibly other forms of statements, we can think that a proposition P may be:

1. a tautology – P is always, no matter what we choose to substitute for the "placeholders", true; (In particular, a proposition without any "placeholders", e.g., "all animals are animals", may be a tautology.)
2. a contradiction – P is never true;
3. contingent – th$P$ is sometimes true and sometimes false; ("all α are β" is true, for instance, if we substitute "animals" for both α and β, while it is false if we substitute "birds" for α and "pigeons" for β).

A.2.3. Syllogisms

Aristotle defined a syllogism as a

> *"discourse in which, certain things being stated something other than what is stated follows of necessity from their being so."*

But in practice he confined the term to arguments containing two premises and a conclusion, each of which is a categorical proposition. The subject and predicate of the conclusion each occur in one of the premises, together with a third term (the middle) that is found in both premises but not in the conclusion. A syllogism thus argues that because α and γ are related in certain ways to β (the middle) in the premises, they are related in a certain way to one another in the conclusion.

The predicate of the conclusion is called the major term, and the premise in which it occurs is called the major premise. The subject of the conclusion is called the minor term and the premise in which it occurs is called the minor premise. This way of describing major and minor terms conforms to Aristotle's actual practice and was proposed as a definition by the 6th-century Greek commentator John Philoponus. But in one passage Aristotle put it differently: the minor term is said to be "included" in the middle and the middle "included" in the major term. This remark, which appears to have been intended to apply only to the first figure (see below), has caused much confusion among some of Aristotle's commentators, who interpreted it as applying to all three figures.

Aristotle distinguished three different "figures" of syllogisms, according to how the middle is related to the other two terms in the premises. In one passage, he says that if one wants to prove α of γ syllogistically, one finds a middle term β such that either

1. α is predicated of β and β of γ (i.e., β is α and γ is β), or
2. β is predicated of both α and γ (i.e., α is β and γ is β), or else
3. both α and γ are predicated of β (i.e., β is α and β is γ).

All syllogisms must, according to Aristotle, fall into one or another of these figures.

Each of these figures can be combined with various categorical forms, yielding a large taxonomy of possible syllogisms. Aristotle identified 19 among them which were *valid* ("universally correct"). The following is an example of a syllogism of figure 1 and categorical forms 3,1,3. "**Women**" is here the middle term.

Some	of my Friends	are	**Women**.
Every	**Women**	is	Unreliable.
Some	of my Friends	are	Unreliable.

The table below gives examples of syllogisms of all three figures with middle term in **bold face** – the last one is not valid!

figure 1:	[F is **W**]	[**W** is U]	[F is U]	
3,1,3	Some [F is W]	Every [W is U]	Some [F is U]	
1,1,1	Every [F is W]	Every [W is U]	Every [F is U]	
figure 2:	[M is **W**]	[U is **W**]	[M is U]	
2,1,2	No [M is W]	Every [U is W]	no [M is U]	
figure 3:	[**W** is U]	[**W** is N]	[N is U]	
1,1,3	Every [W is U]	Every [W is N]	Some [N is U]	
1,1,1	Every [W is U]	Every [W is N]	Every [N is U]	–

Validity of an argument means here that

> *no matter what concrete terms we substitute for α, β, γ, if only the premises are true then also the conclusion is guaranteed to be true.*

Again we see that the idea is "truth preservation in the reasoning process". An obvious, yet nonetheless *crucially* important, assumption is the so called "contradiction principle":

> *For any proposition P it is never the case that both P and not-P are true.*

This principle seemed (and to many still seems) intuitively obvious enough to accept it without any discussion. Also, if it were violated, there would be little point in constructing such "truth preserving" arguments.

A.3. Other patterns and later developments

Aristotle's syllogisms dominated logic until late Middle Ages. A lot of variations were invented, as well as ways of reducing some valid patterns into others (cf. A.2.2). The claim that

> *all valid arguments can be obtained by conversion and, possibly indirect proof (reductio ad absurdum) from the three figures*

has been challenged and discussed ad nauseum.

Early developments (already in Aristotle) attempted to extend the syllogisms to *modalities*, i.e., by considering instead of the *categorical forms* as above, the propositions of the form "it is possible/necessary that some α are β". Early followers of Aristotle (Theophrastus of Eresus (371-286), the school of Megarians with Euclid (430-360), Diodorus Cronus (4th century BC)) elaborated on the modal syllogisms and introduced another form of a proposition, the conditional

"if (α is β) then (γ is δ)".

These were further developed by Stoics who also made another significant step. Instead of considering logic or "patterns of terms" where α, β, etc. are placeholders for "some objects", they started to investigate logic, or "patterns of propositions". Such patterns would use the variables standing for propositions instead of terms. For instance,

from two propositions: "the first" and "the second",
we may form new propositions, e.g., "the first or the second", or "if the first then the second".

The terms "the first", "the second" were used by Stoics as *variables* instead of α, β, etc. The truth of such compound propositions may be determined from the truth of their constituents. We thus get new patterns of arguments. The Stoics gave the following list of five *patterns*

If 1 then 2;	*but 1;*	*therefore 2.*
If 1 then 2;	*but not 2;*	*therefore not 1.*
Not both 1 and 2;	*but 1;*	*therefore not 2.*
Either 1 or 2;	*but 1;*	*therefore not 2.*
Either 1 or 2;	*but not 2;*	*therefore 1.*

Chrysippus (c.279-208 BC) derived many other schemata. Stoics claimed (wrongly, as it seems) that all valid arguments could be derived from these *patterns*. At the time, the two approaches seemed different and a lot of discussions centered around the question which is "the right one". Although Stoic's "propositional patterns" had fallen in oblivion for a long time, they re-emerged as the basic tools of modern mathematical *propositional logic*.

Medieval logic was dominated by Aristotlean syllogisms elaborating on them but without contributing significantly to this aspect of reasoning. However, scholasticism developed very sophisticated theories concerning other central aspects of logic.

B. Logic – a language *about* something

The *pattern* of a valid argument is the first and through the centuries fundamental issue in the study of logic. But there were (and are) a lot of related issues. For instance, the two statements

1. "all horses are animals", and
2. "all birds can fly"

are not exactly of the same form. More precisely, this depends on what a *form* is. The first says that one class (horses) is included in another (animals), while the second that all members of a class (birds) have some property (can fly). Is this grammatical difference essential or not? Or else, can it be covered by one and the same *pattern* or not? Can we replace a *noun* by an *adjective* in a valid *pattern* and still obtain a valid *pattern* or not? In fact, the first categorical form subsumes both above sentences, i.e., from the point of view of our logic, they are considered as having *the same form*.

This kind of questions indicate, however, that *forms* of statements and *patterns* of reasoning, like syllogisms, require further analysis of "what can be plugged where" which, in turn, depends on which words or phrases can be considered as "having similar function", perhaps even as "having the same meaning". What are the objects referred to by various kinds of words? What are the objects referred to by the propositions.

B.1. Early semantic observations and problems

Certain particular teachings of the sophists and rhetoricians are significant for the early history of (this aspect of) logic. For example, the arch-sophists Protagoras (500 BC) is reported to have been the first to distinguish different kinds of sentences: questions, answers, prayers, and injunctions. Prodicus appears to have maintained that no two words can mean exactly the same thing. Accordingly, he devoted much attention to carefully distinguishing and defining the meanings of apparent synonyms, including many ethical terms.

As described in A.2.1, the *categorical forms*, too, were classified according to such organizing principles.

Since logic studies statements, their form as well as patterns in which they can be arranged to form valid arguments, one of the basic questions concerns the meaning of a proposition. As we indicated earlier, two propositions can be considered equivalent if they have the same truth value. This indicates another, beside the *contradiction*, principle, namely

> **The principle of "excluded middle"**
> *Each proposition P is either true or false.*

There is surprisingly much to say *against* this apparently simple claim. There are modal statements (see B.4) which do not seem to have any definite truth value. Among many early counter-examples, there is the most famous one, produced by the Megarians, which is still disturbing and discussed by modern logicians:

> **The "liar paradox"**
> *The sentence "This sentence is false" does not seem to have any content – it is false if and only if it is true!*

Such paradoxes indicated the need for closer analysis of fundamental notions of the logical enterprise.

B.2. The Scholastic theory of *supposition*

The character and meaning of various "building blocks" of a logical language were thoroughly investigated by the Scholastics. The theory of *supposition* was meant to answer the question:

> "To what does a given occurrence of a term refer in a given proposition?"

Roughly, one distinguished three kinds of supposition:

1. personal: In the sentence "Every horse is an animal", the term "horse" refers to individual horses.
2. simple: In the sentence "Horse is a species", the term "horse" refers to a universal (concept).
3. material: In the sense "Horse is a monosyllable", the term "horse" refers to the spoken or written word.

We can notice here the distinction based on the fundamental duality of *individuals* and *universals* which had been one of the most debated issues in Scholasticism. The third point indicates the important development, namely, the increasing attention paid to the *language* as such which slowly becomes the object of study.

B.3. *Intension* vs. *extension*

In addition to supposition and its satellite theories, several logicians during the 14th century developed a sophisticated theory of *connotation*. The term "black" does not merely *denote* all the black things – it also *connotes* the quality, *blackness*, which all such things possess. This has become one of the central distinctions in the later development of logic and in the discussions about the entities referred to by the words we are using. One begun to call *connotation "intension"* – saying "black" I *intend blackness*. *Denotation* is closer to *"extension"* – the collection of all the objects referred to by the term "black". One has arrived at the understanding of a term which can be represented pictorially as

$$\begin{tikzcd}
 & \text{term} \arrow[dl, "\text{intends}"'] \arrow[dr, "\text{refers to}"] & \\
\text{intension} \arrow[rr, "\text{can be ascribed to}"'] & & \text{extension}
\end{tikzcd}$$

The crux of many problems is that different *intensions* may refer to (denote) the same *extension*. The "Morning Star" and the "Evening Star" have different *intensions* and for centuries were considered to refer to two different stars. As it turned out, these are actually two appearances of one and the same planet Venus, i.e., the two terms have the same *extension*.

One might expect logic to be occupied with *concepts*, that is *connotations* – after all, it tries to capture correct reasoning. Many attempts have been made to design a "universal language of thought" in which one could speak directly about the *concepts* and their interrelations. Unfortunately, the concept of *concept* is not that obvious and one had to wait a while until a somehow tractable way of speaking of/modeling/representing concepts become available. The emergence of modern mathematical logic coincides with the successful coupling of logical language with the precise statement of its meaning in terms of *extension*. This by no means solved all the problems and modern logic still has branches of *intensional logic* – we will return to this point later on.

B.4. Modalities

Also these disputes started with Aristotle. In chapter 9 of *De Interpretatione*, he discusses the assertion

> *"There will be a sea battle tomorrow".*

The problem with this assertion is that, at the moment when it is made, it does not seem to have any definite truth value – whether it is true or false will become clear tomorrow but until then it is possible that it will be the one as well the other. This is another example (besides the "liar paradox") indicating that adopting the principle of "excluded middle", i.e., considering the propositions as having always only one of two possible truth values, may be insufficient.

Medieval logicians continued the tradition of modal syllogistic inherited from Aristotle. In addition, modal factors were incorporated into the theory of supposition. But the most important developments in modal logic occurred in three other contexts:

1. whether propositions about future contingent events are *now* true or false (the question raised by Aristotle),
2. whether a *future* contingent event can be known in advance, and
3. whether God (who, the tradition says, cannot be acted upon causally) can know future contingent events.

All these issues link *logical modality* with *time*. Thus, Peter Aureoli (c. 1280-1322) held that if something is in fact P (P is some predicate) but can be not-P, then it is capable of changing from being P to being not-P.

However here, as in the case of categorical propositions, important issues could hardly be settled before one had a clearer idea as to what kind of objects or state of affairs *modalities* are supposed to describe. Duns Scotus in the late 13th century was the first to sever the link between time and modality. He proposed a notion of possibility that was not linked with time but based purely on the notion of *semantic consistency*. This radically new conception had a tremendous influence on later generations down to the 20th century. Shortly afterward, Ockham developed an influential theory of modality and time that reconciles the claim that every proposition is either true or false with the claim that certain propositions about the future are genuinely contingent.

Duns Scotus' ideas were revived in the 20th century. Starting with the work of Jan Lukasiewicz who, once again, studied Aristotle's example and introduced *3-valued logic* – a proposition may be true, or false, or else it may have the third, "undetermined" truth value.

C. Logic – a *symbolic* language

Logic's preoccupation with concepts and reasoning begun gradually to put more and more severe demands on the appropriate and precise representation of the used terms. We saw that syllogisms used fixed *forms* of categorical statements with *variables* – α, β, etc. – which represented arbitrary terms (or objects). Use of *variables* was indisputable contribution of Aristotle to the logical, and more generally mathematical notation. We also saw that Stoics introduced analogous variables standing for propositions. Such notational tricks facilitated more concise, more general and more precise statement of various logical facts.

Following the Scholastic discussions of *connotations* vs. *denotations*, logicians of the 16th century felt the increased need for a more general logical language. One of the goals was the development of an ideal logical language that naturally expressed ideal thought and was more precise than natural language. An important motivation underlying the attempts in this direction was the idea of *manipulation*, in fact, *symbolic* or even *mechanical manipulation* of arguments represented in such a language. Aristotelian logic had seen itself as a tool for training "natural" abilities at reasoning. Now one would like to develop methods of thinking that would accelerate or improve human thought or would even allow its replacement by mechanical devices.

Among the initial attempts was the work of Spanish soldier, priest and mystic Ramon Lull (1235-1315) who tried to symbolize concepts and derive propositions from various combinations of possibilities. The work of some of his followers, Juan Vives (1492-1540) and Johann Alsted (1588-1683) represents perhaps the first systematic effort at a logical symbolism.

Some philosophical ideas in this direction occurred within the "Port-Royal Logic" – a group of anticlerical Jansenists located in Port-Royal outside Paris, whose most prominent member was Blaise Pascal. They elaborated on the Scholastical distinction *comprehension* vs. *extension*. Most importantly, Pascal introduced the distinction between *real* and *nominal* definitions. *Real* definitions were descriptive and stated the essential properties in a concept, while *nominal* definitions were creative and stipulated the conventions by which a linguistic term was to be used. Although the Port-Royal logic itself contained no symbolism, the philosophical foundation for using symbols by nominal definitions was nevertheless laid.

C.1. The *"universally characteristic language"*

Lingua characteristica universalis was Gottfried Leibniz' ideal that would, first, notationally represent concepts by displaying the more basic concepts of which they were composed, and second, naturally represent (in the manner of graphs or pictures, "iconically") the concept in a way that could be easily grasped by readers, no matter what their native tongue. Leibniz studied and was impressed by the method of the Egyptians and Chinese in using picturelike expressions for concepts. The goal of a universal language had already been suggested by Descartes for mathematics as a "universal mathematics"; it had also been discussed extensively by the English philologist George Dalgarno (c. 1626-87) and, for mathematical language and communication, by the French algebraist François Viète (1540-1603).

C.1.1. *"Calculus of reason"*

Another and distinct goal Leibniz proposed for logic was a "calculus of reason" (*calculus ratiocinator*). This would naturally first require a symbolism but would then

> *involve explicit manipulations of the symbols according to established rules by which either new truths could be discovered or proposed conclusions could be checked to see if they could indeed be derived from the premises.*

Reasoning could then take place in the way large sums are done – that is, mechanically or algorithmically – and thus not be subject to individual mistakes and failures of ingenuity. Such derivations could be checked by others or performed by machines, a possibility that Leibniz seriously contemplated. Leibniz' suggestion that machines could be constructed to draw valid inferences or to check the deductions of others was followed up by Charles Babbage, William Stanley Jevons, and Charles Sanders Peirce and his student Allan Marquand in the 19th century, and with wide success on modern computers after World War II.

The symbolic calculus that Leibniz devised seems to have been more of a calculus of reason than a "characteristic" language. It was motivated by his view that most concepts were "composite": they were collections or conjunctions of other more basic concepts. Symbols (letters, lines, or circles) were then used to stand for concepts and their relationships. This resulted in what is *intensional* rather than an *extensional* logic – one whose terms stand for properties or concepts rather than for the things having these properties. Leibniz' basic notion of the *truth of a judgment* was that

the concepts making up the predicate were "included in" the concept of the subject

For instance, the judgment 'A zebra is striped and a mammal.' is true because the concepts forming the predicate 'striped-and-mammal' are, in fact, "included in" the concept (all possible predicates) of the subject 'zebra'.

What Leibniz symbolized as "$A \infty B$", or what we might write as "$A = B$" was that all the concepts making up concept A also are contained in concept B, and vice versa.

Leibniz used two further notions to expand the basic logical calculus. In his notation, "$A \oplus B \infty C$" indicates that the concepts in A and those in B wholly constitute those in C. We might write this as "$A + B = C$" or "$A \cup B = C$" – if we keep in mind that A, B, and C stand for concepts or properties, not for individual things. Leibniz also used the juxtaposition of terms in the following way: "$AB \infty C$," which we might write as "$A \times B = C$" or "$A \cap B = C$", signifies in his system that all the concepts in both A and B wholly constitute the concept C.

A universal affirmative judgment, such as "All A's are B's," becomes in Leibniz' notation "$A \infty AB$". This equation states that the concepts included in the concepts of both A and B are the same as those in A.

A syllogism: "All A's are B's; all B's are C's; therefore all A's are C's,"
becomes the sequence of equations : $A = AB$; $B = BC$; *therefore* $A = AC$

Notice, that this conclusion can be derived from the premises by two simple algebraic substitutions and the associativity of logical multiplication.

$$
\begin{array}{rrl|rl}
 & 1. & A = AB & & \text{Every } A \text{ is } B \\
 & 2. & B = BC & & \text{Every } B \text{ is } C \\
(1+2) & & A = ABC & & \\
\hline
(1) & & A = AC & \text{therefore :} & \text{Every } A \text{ is } C
\end{array}
$$

Leibniz' interpretation of particular and negative statements was more problematic. Although he later seemed to prefer an algebraic, equational symbolic logic, he experimented with many alternative techniques, including graphs.

As with many early symbolic logics, including many developed in the 19th century, Leibniz' system had difficulties with particular and negative statements, and it included little discussion of propositional logic and no formal treatment of quantified relational statements. (Leibniz later became keenly aware of the importance of relations and relational inferences.) Although Leibniz might seem to deserve to be credited with great originality in his symbolic logic – especially in his equational, algebraic logic – it turns out that such insights were relatively common to mathematicians of the 17th and 18th centuries who had a knowledge of traditional syllogistic logic. In 1685 Jakob Bernoulli published a pamphlet on the parallels of logic and algebra and gave some algebraic renderings of categorical statements. Later the symbolic work of Lambert, Ploucquet, Euler, and even Boole – all apparently uninfluenced by Leibniz' or even Bernoulli's work – seems to show the extent to which these ideas were apparent to the best mathematical minds of the day.

D. 19th and 20th Century – Mathematical Logic

Leibniz' system and calculus mark the appearance of formalized, symbolic language which is prone to mathematical (either algebraic or other) manipulation. A bit ironically, emergence of *mathematical logic* marks also this logic's, if not a divorce then at least separation from philosophy. Of course, the discussions of logic have continued both among logicians and philosophers but from now on these groups form two increasingly distinct camps. Not all questions of philosophical logic are important for mathematicians and most of results of mathematical logic has rather technical character which is not always of interest for philosophers. (There are, of course, exceptions like, for instance, the extremist camp of *analytical philosophers* who in the beginning of 20th century attempted to design a philosophy based exclusively on the principles of mathematical logic.)

In this short presentation we have to ignore some developments which did take place between 17th and 19th century. It was only in the last century that the substantial contributions were made which created modern logic. The first issue concerned the *intentional* vs. *extensional* dispute – the work of George Boole, based on purely *extensional* interpretation was a real break-through. It did not settle the issue once and for all – for instance Frege, "the father of first-order logic" was still in favor of concepts and *intensions*; and in modern logic there is still a branch of *"intensional logic"*. However, Boole's approach was so convincingly precise and intuitive that it was later taken up and become the basis of modern – *extensional* or *set theoretical* – semantics.

D.1. George Boole

The two most important contributors to British logic in the first half of the 19th century were undoubtedly George Boole and Augustus De Morgan. Their work took place against a more general background of logical work in English by figures such as Whately, George Bentham, Sir William Hamilton, and others. Although Boole cannot be credited with the very first symbolic logic, he was the first major formulator of a *symbolic extensional logic* that is familiar today as a logic or algebra of classes. (A correspondent of Lambert, Georg von Holland, had experimented with an extensional theory, and in 1839 the English writer Thomas Solly presented an extensional logic in *A Syllabus of Logic*, though not an algebraic one.)

Boole published two major works, *The Mathematical Analysis of Logic* in 1847 and *An Investigation of the Laws of Thought* in 1854. It was the first of these two works that had the deeper impact on his contemporaries and on the history of logic. *The Mathematical Analysis of Logic* arose as the result of two broad streams of influence. The first was the English logic-textbook tradition. The second was the rapid growth in the early 19th century of sophisticated discussions of algebra and anticipations of nonstandard algebras. The British mathematicians D.F. Gregory and George Peacock were major figures in this theoretical appreciation of algebra. Such conceptions gradually evolved into "nonstandard" abstract algebras such as quaternions, vectors, linear algebra, and Boolean algebra itself.

Boole used capital letters to stand for the *extensions* of terms; they are referred to (in 1854) as classes of "things" but should not be understood as modern sets. Nevertheless, this extensional perspective made the Boolean algebra a very intuitive and simple structure which, at the same time, seems to capture many essential intuitions.

The universal class or term – which he called simply "the Universe" – was represented by the numeral "1", and the empty class by "0". The juxtaposition of terms (for example, "AB") created a term referring to the *intersection* of two classes or terms. The addition sign signified the *non-overlapping union*; that is, "$A + B$" referred to the entities in A or in B; in cases where the extensions of terms A and B overlapped, the expression was held to be "undefined." For designating a proper subclass of a class A, Boole used the notation "vA". Finally, he used subtraction to indicate the removing of terms from classes. For example, "$1 - x$" would indicate what one would obtain by removing the elements of x from the universal class – that is, obtaining the *complement* of x (relative to the universe, 1).

Basic equations included:

$$
\begin{array}{lllll}
 & 1A = A & 0A = 0 & AB = BA & AA = A \\
\text{for } A = 0 : A + 1 = 1 & A + 0 = A & A + B = B + A & A(BC) = (AB)C & \text{(associativity)} \\
 & A(B + C) = AB + AC & A + (BC) = (A + B)(A + C) & & \text{(distributivity)}
\end{array}
$$

Boole offered a relatively systematic, but not rigorously axiomatic, presentation. For a universal affirmative statement such as "All A's are B's," Boole used three alternative notations: $A = AB$ (somewhat in the manner of Leibniz), $A(1 - B) = 0$, or $A = vB$ (the class of A's is equal to some proper subclass of the B's). The first and second interpretations allowed one to derive syllogisms by algebraic substitution; the latter required manipulation of subclass ("v") symbols.

In contrast to earlier symbolisms, Boole's was extensively developed, with a thorough exploration of a large number of equations and techniques. The formal logic was separately applied to the interpretation of *propositional logic*, which became an interpretation of the class or term logic – with terms standing for occasions or times rather than for concrete individual things. Following the English textbook tradition, deductive logic is but one half of the subject matter of the book, with inductive logic and probability theory constituting the other half of both his 1847 and 1854 works.

Seen in historical perspective, Boole's logic was a remarkably smooth bend of the new "algebraic" perspective and the English-logic textbook tradition. His 1847 work begins with a slogan that could have served as the motto of abstract algebra:

> *". . . the validity of the processes of analysis does not depend upon the interpretation of the symbols which are employed, but solely upon the laws of combination."*

D.1.1. Further developments of Boole's algebra; De Morgan

Modifications to Boole's system were swift in coming: in the 1860s Peirce and Jevons both proposed replacing Boole's "+" with a simple inclusive union or summation: the expression "$A+B$" was to be interpreted as designating the class of things in A, in B, or in both. This results in accepting the equation "$1 + 1 = 1$", which is certainly not true of the ordinary numerical algebra and at which Boole apparently balked.

Interestingly, one defect in Boole's theory, its failure to detail relational inferences, was dealt with almost simultaneously with the publication of his first major work. In 1847 Augustus De Morgan published his *Formal Logic; or, the Calculus of Inference, Necessary and Probable.* Unlike Boole and most other logicians in the United Kingdom, De Morgan knew the medieval theory of logic and semantics and also knew the Continental, Leibnizian symbolic tradition of Lambert, Ploucquet, and Gergonne. The symbolic system that De Morgan introduced in his work and used in subsequent publications is, however, clumsy and does not show the appreciation of abstract algebras that Boole's did. De Morgan did introduce the enormously influential notion of a

> *possibly arbitrary and stipulated "universe of discourse"*

that was used by later Booleans. (Boole's original universe referred simply to "all things.") This view influenced 20th-century logical semantics.

The notion of a stipulated "universe of discourse" means that, instead of talking about "The Universe", one can choose this universe depending on the context, i.e., "1" may sometimes stand for "the universe of all animals", and in other for merely two-element set, say "the true" and "the false". In the former case, the syllogism "All A's are B's; all B's are C's; therefore all A's are C's" is derivable from the equational axioms in the same way as Leibniz did it: from "$A = AB$ and $B = BC$" the conclusion "$A = AC$" follows by substitution

In the latter case, the equations of Boolean algebra yield the *laws of propositional logic* where "$A + B$" is taken to mean disjunction "A or B", and juxtaposition "AB" conjunction "A and B". Negation of A is simply its complement $1 - A$, which may also be written as $\overline{A}$.

De Morgan is known to all the students of elementary logic through the so called 'De Morgan laws': $\overline{AB} = \overline{A} + \overline{B}$ and, dually, $(\overline{A})(\overline{B}) = \overline{A+B}$. Using these laws, as well as some additional, today standard, facts, like $\overline{B}B = 0$, $\overline{\overline{B}} = B$, we can derive the following reformulation of the reduction ad absurdum "If every A is B then every not-B is not-A":

$$
\begin{array}{llllll}
A = AB \;\; / -AB & \rightarrow \;\; A - AB = 0 & \rightarrow & A(1-B) = 0 & \rightarrow & A\overline{B} = 0 \text{ /De Morgan} \\
& \rightarrow \;\; \overline{A} + B = 1 \; / \cdot \overline{B} & \rightarrow & \overline{B}(\overline{A} + B) = \overline{B} & \rightarrow & (\overline{B})(\overline{A}) + \overline{B}B = \overline{B} \\
& & \rightarrow & (\overline{B})(\overline{A}) + 0 = \overline{B} & \rightarrow & (\overline{B})(\overline{A}) = \overline{B} \\
\hline
& & & & \rightarrow & \overline{B} = (\overline{B})(\overline{A})
\end{array}
$$

I.e., "Every A is B" implies that "every $\overline{B}$ is $\overline{A}$", i.e., "every not-B is not-A". Or: if "A implies B" then "if B is absurd (false) then so is A".

De Morgan's other essays on logic were published in a series of papers from 1846 to 1862 (and an unpublished essay of 1868) entitled simply *On the Syllogism.* The first series of four papers found its way into the middle of the Formal Logic of 1847. The second series, published in 1850, is of considerable significance in the history of logic, for it marks the first extensive discussion of quantified relations since late medieval logic and Jung's massive *Logica hamburgensis* of 1638. In fact, De Morgan made the point, later to be exhaustively repeated by Peirce and implicitly endorsed by Frege, that *relational inferences* are the core of mathematical inference and scientific reasoning of all sorts; relational inferences are thus not just one type of reasoning but rather are the most important type of deductive reasoning. Often attributed to De Morgan – not precisely correctly but in the right spirit – was the observation that all of Aristotelian logic was helpless to show the validity of the inference,

"All horses are animals; therefore, every head of a horse is the head of an animal."

The title of this series of papers, De Morgan's devotion to the history of logic, his reluctance to mathematize logic in any serious way, and even his clumsy notation – apparently designed to represent the traditional theory of the syllogism – show De Morgan to be a deeply traditional logician.

D.2. Gottlob Frege

In 1879 the young German mathematician Gottlob Frege – whose mathematical speciality, like Boole's, had actually been calculus – published perhaps the finest single book on symbolic logic in the 19th century, *Begriffsschrift* ("Conceptual Notation"). The title was taken from Trendelenburg's translation of Leibniz' notion of a *characteristic language*. Frege's small volume is a rigorous presentation of what would now be called the first-order predicate logic. It contains a careful use of *quantifiers* and *predicates* (although predicates are described as functions, suggestive of the technique of Lambert). It shows no trace of the influence of Boole and little trace of the older German tradition of symbolic logic. One might surmise that Frege was familiar with Trendelenburg's discussion of Leibniz, had probably encountered works by Drobisch and Hermann Grassmann, and possibly had a passing familiarity with the works of Boole and Lambert, but was otherwise ignorant of the history of logic. He later characterized his system as inspired by Leibniz' goal of a *characteristic language* but not of a *calculus of reason*. Frege's notation was unique and problematically two-dimensional; this alone caused it to be little read.

Frege was well aware of the importance of functions in mathematics, and these form the basis of his notation for predicates; he never showed an awareness of the work of De Morgan and Peirce on relations or of older medieval treatments. The work was reviewed (by Schröder, among others), but never very positively, and the reviews always chided him for his failure to acknowledge the Boolean and older German symbolic tradition; reviews written by philosophers chided him for various sins against reigning idealist dogmas. Frege stubbornly ignored the critiques of his notation and persisted in publishing all his later works using it, including his little-read magnum opus, *Grundgesetze der Arithmetik* (1893-1903; "The Basic Laws of Arithmetic").

Although notationally cumbersome, Frege's system contained precise and adequate (in the sense, "adopted later") treatment of several basic notions. The universal affirmative "All A's are B's" meant for Frege that the concept A *implies* the concept B, or that "to be A implies also to be B". Moreover, this applies to arbitrary x which happens to be A. Thus the statement becomes: "$\forall x : A(x) \rightarrow B(x)$", where the quantifier $\forall x$ stands for "for all x" and the arrow "$\rightarrow$" for implication. The analysis of this, and one other statement, can be represented as follows:

Every	horse	is	an animal	Some	animals	are	horses
Every x	which is a horse	is	an animal	Some x's	which are animals	are	horses
Every x	if it is a horse	then	it is an animal	Some x's	are animals	and	horses
$\forall x :$	$H(x)$	$\rightarrow$	$A(x)$	$\exists x :$	$A(x)$	&	$H(x)$

This was not the way Frege would *write* it but this was the way he would *put* it and *think* of it and this is his main contribution. The syllogism "All A's are B's; all B's are C's; therefore: all A's are C's" will be written today in first-order logic as:

$$[\ (\forall x : A(x) \rightarrow B(x))\ \&\ (\forall x : B(x) \rightarrow C(x))\ ]\ \rightarrow\ (\forall x : A(x) \rightarrow C(x))$$

and will be read as: "If any x which is A is also B, and any x which is B is also C; then any x which is A is also C". For instance:

Every pony is a horse;	and	Every horse is an animal;	Hence:	Every pony is an animal.
$(\forall x : P(x) \rightarrow H(x))$	&	$(\forall x : H(x) \rightarrow A(x))$	$\rightarrow$	$(\forall x : P(x) \rightarrow A(x))$
Hugo is a horse;	and	Every horse is an animal;	Hence:	Hugo is an animal.
$H(Hugo)$	&	$(\forall x : H(x) \rightarrow A(x))$		
		$H(Hugo) \rightarrow A(Hugo)$	$\rightarrow$	$A(Hugo)$

The relational arguments, like the one about horse-heads and animal-heads, can be derived after we have represented the involved statements as follows:

1.	y is a head of some horse	=	there is	a horse	and	y is its head
		=	there is an x	which is a horse	and	y is the head of x
		=	$\exists x :$	$H(x)$	&	$Hd(y,x)$
2.	y is a head of some animal	=	$\exists x :$	$A(x)$	&	$Hd(y,x)$

Now, "All horses are animals; therefore: Every horse-head is an animal-head." will be given the following form and treatement (very informally):

$$\begin{array}{rcrcl}
\forall x : H(x) \rightarrow A(x) \quad \text{hence} & \forall y : & \exists x : H(x)\ \&\ Hd(y,x) & \rightarrow & \exists z : A(z)\ \&\ Hd(y,z) \\
\text{take an arbitrary horse} - \text{head } a : & & \exists x : H(x)\ \&\ Hd(a,x) & \rightarrow & \exists z : A(z)\ \&\ Hd(a,z) \\
\text{then there is a horse } h : & & H(h)\ \&\ Hd(a,h) & \rightarrow & \exists z : A(z)\ \&\ Hd(a,z) \\
\text{but } h \text{ is an animal,} & & & \text{so} & A(h)\ \&\ Hd(a,h)
\end{array}$$

Frege's first writings after the *Begriffsschrift* were bitter attacks on Boolean methods (showing no awareness of the improvements by Peirce, Jevons, Schröder, and others) and a defense of his own system. His main complaint against Boole was the artificiality of mimicking notation better suited for numerical analysis rather than developing a notation for logical analysis alone. This work was followed by the *Die Grundlagen der Arithmetik* (1884; "The Foundations of Arithmetic") and then by a series of extremely important papers on precise mathematical and logical topics. After 1879 Frege carefully developed his position that *all of mathematics could be derived from, or reduced to, basic "logical" laws – a position later to be known as logicism in the philosophy of mathematics.*

His view paralleled similar ideas about the reducibility of mathematics to *set theory* from roughly the same time – although Frege always stressed that his was an *intensional* logic of concepts, not of *extensions* and classes. His views are often marked by hostility to British extensional logic and to the general English-speaking tendencies toward nominalism and empiricism that he found in authors such as J.S. Mill. Frege's work was much admired in the period 1900-10 by Bertrand Russell who promoted Frege's logicist research program – first in the *Introduction to Mathematical Logic* (1903), and then with Alfred North Whitehead, in *Principia Mathematica* (1910-13) – but who used a Peirce-Schröder-Peano system of notation rather than Frege's; Russell's development of relations and functions was very similar to Schröder's and Peirce's. Nevertheless, Russell's formulation of what is now called the "set-theoretic" paradoxes was taken by Frege himself, perhaps too readily, as a shattering blow to his goal of founding mathematics and science in an intensional, "conceptual" logic.

Almost all progress in symbolic logic in the first half of the 20th century was accomplished using set theories and extensional logics and thus mainly relied upon work by Peirce, Schröder, Peano, and Georg Cantor. Frege's care and rigour were, however, admired by many German logicians and mathematicians, including David Hilbert and Ludwig Wittgenstein. Although he did not formulate his theories in an axiomatic form, Frege's derivations were so careful and painstaking that he is sometimes regarded as a founder of this axiomatic tradition in logic. Since the 1960s Frege's works have been translated extensively into English and reprinted in German, and they have had an enormous impact on a new generation of mathematical and philosophical logicians.

D.3. Set theory

A development in Germany originally completely distinct from logic but later to merge with it was Georg Cantor's development of *set theory*. As mentioned before, the *extensional* view of concepts began gradually winning the stage with advance of Boolean algebra. Eventually, even Frege's analyses become incorporated and merged with the set theoretical approach to the semantics of logical formalism.

In work originating from discussions on the foundations of the infinitesimal and derivative calculus by Baron Augustin-Louis Cauchy and Karl Weierstrass, Cantor and Richard Dedekind developed methods of dealing with the large, and in fact infinite, sets of the integers and points on the real number line. Although the Booleans had used the notion of a class, they rarely developed tools for dealing with infinite classes, and no one systematically considered the possibility of classes whose elements were themselves classes, which is a crucial feature of Cantorian set theory. The conception of "real" or "closed" infinities of things, as opposed to infinite possibilities, was a medieval problem that had also troubled 19th-century German mathematicians, especially the great Carl Friedrich Gauss. The Bohemian mathematician and priest Bernhard Bolzano emphasized the difficulties posed by infinities in his *Paradoxien des Unendlichen* (1851; "Paradoxes of the Infinite"); in 1837 he had written an anti-Kantian and pro-Leibnizian nonsymbolic logic that was later widely studied. First Dedekind, then Cantor used Bolzano's tool of measuring sets by *one-to-one mappings*;

Two sets are "equinumerous" iff there is one-to-one mapping between them

Using this technique, Dedekind gave in *Was sind und was sollen die Zahlen?* (1888; "What Are and Should Be the Numbers?") a precise definition of an infinite set.

A set is infinite if and only if
the whole set can be put into one-to-one correspondence with a proper part of the set.

De Morgan and Peirce had earlier given quite different but technically correct characterizations of infinite domains; these were not especially useful in set theory and went unnoticed in the German mathematical world.

An example of an infinite set is the set of all natural numbers, N (for instance, the set N_0, i.e., natural numbers without 0, can be easily shown to be in a one-to-one correspondence with N.) A set A is said to be *"countable"* iff it is *equinumerous* with N. One of the main results of Cantor was demonstration that there are uncountable infinite sets, in fact, sets "arbitrarily infinite". (For instance, the set R of real numbers was shown by Cantor to "have more elements" than N.)

Although Cantor developed the basic outlines of a set theory, especially in his treatment of infinite sets and the real number line, he did not worry about rigorous foundations for such a theory – thus, for example, he did not give axioms of set theory – nor about the precise conditions governing the concept of a set and the formation of sets. Although there are some hints in Cantor's writing of an awareness of problems in this area (such as hints of what later came to be known as the class/set distinction), these difficulties were forcefully posed by the paradoxes of Russell and the Italian mathematician Cesare Burali-Forti and were first overcome in what has come to be known as Zermelo-Fraenkel set theory.

D.4. 20th century logic

In 1900 logic was poised on the brink of the most active period in its history. The late 19th-century work of Frege, Peano, and Cantor, as well as Peirce's and Schröder's extensions of Boole's insights, had broken new ground, raised considerable interest, established international lines of communication, and formed a new alliance between logic and mathematics. Five projects internal to late 19th-century logic coalesced in the early 20th century, especially in works such as Russell and Whitehead's *Principia Mathematica*. These were

1. the development of a consistent set or property theory (originating in the work of Cantor and Frege),
2. the application of the axiomatic method (including non-symbolically),
3. the development of quantificational logic,
4. the use of logic to understand mathematical objects
5. and the nature of mathematical proof

. The five projects were unified by a general effort to use symbolic techniques, sometimes called mathematical, or formal, techniques. Logic became increasingly "mathematical," then, in two senses.

- First, it attempted to use symbolic methods like those that had come to dominate mathematics.
- Second, an often dominant purpose of logic came to be its use as a tool for understanding the nature of mathematics – such as in defining mathematical concepts, precisely characterizing mathematical systems, or describing the nature of ideal mathematical proof.

D.4.1. Logic and philosophy of mathematics

An outgrowth of the theory of Russell and Whitehead, and of most modern set theories, was a better articulation of a philosophy of mathematics known as *"logicism"*: that operations and objects spoken about in mathematics are really purely logical constructions. This has focused increased attention on what exactly "pure" logic is and whether, for example, set theory is really logic in a narrow sense. There seems little doubt that set theory is not "just" logic in the way in which, for example, Frege viewed logic – i.e., as a formal theory of functions and properties. Because set theory engenders a large number of interestingly distinct kinds of nonphysical, nonperceived abstract objects, it has also been regarded by some philosophers and logicians as suspiciously (or endearingly) Platonistic. Others, such as Quine, have "pragmatically" endorsed set theory as a convenient way – perhaps the only such way – of organizing the whole world around us, especially if this world contains the richness of transfinite mathematics.

For most of the first half of the 20th century, new work in logic saw logic's goal as being primarily to provide a foundation for, or at least to play an organizing role in, mathematics. Even for those researchers who did not endorse the logicist program, logic's goal was closely allied with techniques and goals in mathematics, such as giving an account of formal systems (*"formalism"*) or of the ideal nature of nonempirical proof and demonstration. Interest in the logicist and formalist program waned after Gödel's demonstration that logic could not provide exactly the sort of foundation for mathematics or account of its formal systems that had been sought. Namely, Gödel proved a mathematical theorem which interpreted in a natural language says something like:

> **Gödel's incompleteness theorem**
>
> *Any logical theory, satisfying reasonable and rather weak conditions, cannot be consistent and, at the same time, prove all its logical consequences.*

Thus mathematics could not be reduced to a *provably complete* and *consistent* logical theory. An interesting fact is that what Gödel did in the proof of this theorem was to construct a sentence which looked very much like the *Liar paradox*. He showed that in any formal theory satisfying his conditions one can write the sentence *"I am not provable in this theory"*, which cannot be provable unless the theory is inconsistent. In spite of this negative result, logic has still remained closely allied with mathematical foundations and principles.

Traditionally, logic had set itself the task of understanding valid arguments of all sorts, not just mathematical ones. It had developed the concepts and operations needed for describing concepts, propositions, and arguments – especially in terms of *patterns*, or "logical forms" – insofar as such tools could conceivably affect the assessment of any argument's quality or ideal persuasiveness. It is this general ideal that many logicians have developed and endorsed, and that some, such as Hegel, have rejected as impossible or useless. For the first decades of the 20th century, logic threatened to become exclusively preoccupied with a new and historically somewhat foreign role of serving in the analysis of arguments in only one field of study, mathematics. The philosophical-linguistic task of developing tools for analyzing statements and arguments that can be expressed in some natural language about some field of inquiry, or even for analyzing propositions as they are actually (and perhaps necessarily) thought or conceived by human beings, was almost completely lost. There were scattered efforts to eliminate this gap by reducing basic principles in all disciplines – including physics, biology, and even music – to axioms, particularly axioms in set theory or first-order logic. But these attempts, beyond showing that it could be done, did not seem especially enlightening. Thus, such efforts, at their zenith in the 1950s and '60s, had all but disappeared in the '70s: one did not better and more usefully understand an atom or a plant by being told it was a certain kind of set.

E. Modern Mathematical Logic

Already Euclid, also Aristotle were well aware of the notion of a rigorous logical theory, in the sense of a specification, often axiomatic, of theorems of a theory. In fact, one might feel tempted to credit the crises in geometry of the 19th century for focusing on the need for very careful presentations of these theories and other aspects of formal systems.

As one should know, Euclid designed his *Elements* around 10 axioms and postulates which one could not resist accepting as obvious. From the assumption of their truth, he deduced some 465 theorems. The famous postulate of the parallels was

> **The fifth postulate**
>
> *If a straight line falling on thwo straight lines makes the interior angles on the same side less than the two right angles, the two straight lines, if produced indefinitely, meet on that side on which the angles are less than the two right angles.*

With time one begun to point out that the fifth postulate (even if reformulated) was somehow less intuitive and more complicated than others (e.g., "an interval can be prolonged indefinitely", "all right angles are equal"). Through hundreds of years mathematicians had unsuccessfully attempted to derive the fifth postulate from the others until, in the 19th century, they started to reach the conclusion that it must be *independent* from the rest. This meant that one might as well drop it!

That was done independently by Hungarian Bólayi and Russian Lobaczewsky in 1832. What was left was *another axiomatic system*, the first system of non-Euclidean geometry.

The discovery unveiled some importance of admitting the possibility of manipulating the axioms which, perhaps, need not be given by God and intuition but may be chosen with some freedom. Dropping the fifth postulate raised the question about what these new (sub)set of axioms possibly describe. New models were created which satisfied all the axioms but the fifth. This was the first exercise in what later became called *"model theory"*.

E.1. Formal logical systems: syntax.

Although set theory and the type theory of Russell and Whitehead were considered to be "logic" for the purposes of the logicist program, a narrower sense of logic re-emerged in the mid-20th century as what is usually called the "underlying logic" of these systems: whatever concerns only rules for propositional connectives, quantifiers, and nonspecific terms for individuals and predicates. (An interesting issue is whether the privileged relation of identity, typically denoted by the symbol "=", is a part of logic: most researchers have assumed that it is.) In the early 20th century and especially after Tarski's work in the 1920s and '30s, a formal logical system was regarded as being composed of three parts, all of which could be rigorously described:

1. the syntax (or notation);
2. the rules of inference (or the *patterns* of reasoning);
3. the semantics (or the meaning of the syntactic symbols).

One of the fundamental contributions of Tarski was his analysis of the concept of 'truth' which, in the above three-fold setting is given a precise treatement as a

relation between syntax (linguistic expressions) and semantics (contexts, world).

The Euclidean, and then non-Euclidean geometry where, as a matter of fact, built as axiomatic-deductive systems (point 2.). The other two aspects of a formal system identified by Tarski were present too, but much less emphasized: notation was very informal, relying often on drawings; the semantics was rather intuitiv and obvious. Tarski's work initiated rigorous study of all three aspects.

(1) First, there is the notation:

the rules of formation for terms and for well-formed formulas in the logical system.

This theory of notation itself became subject to exacting treatment in the concatenation theory, or theory of strings, of Tarski, and in the work of the American Alonzo Church. For instance:

- *an alphabet* Σ *- a set of symbols*

1. *all symbols from* Σ *belong to* L
2. *if* A, B *belong to* L*, then* $A \to B$ *and* $A\&B$ *and* $\overline{A}$ *belong to* L

E.g., given $\Sigma = \{a, b, c\}$*, we may see that*

a, b, c belongs to L
$a \to b$ belongs to L
$\overline{a \to b}$ belongs to L
$c\&(a \to b)$ belongs to L
$\overline{c\&(a \to b)}$ ... belongs to L

Previously, notation was often a haphazard affair in which it was unclear what could be formulated or asserted in a logical theory and whether expressions were finite or were schemata standing for infinitely long wffs (well formed formulas). Issues that arose out of notational questions include definability of one wff by another (addressed in Beth's and Craig's theorems, and in other results), creativity, and replaceability, as well as the expressive power and complexity of different logical languages.

(2) The second part of a logical system consists of

> *the axioms and rules of inference, or*
> *other ways of identifying what counts as a theorem.*

This is what is usually meant by the logical "theory" proper: a (typically recursive) description of the theorems of the theory, including axioms and every wff derivable from axioms by admitted rules. Using the language L, one migh, for instance, define the following theory:

Axioms:

$$\begin{array}{rl} i) & a \\ ii) & a \to b \\ iii) & c \to \overline{a} \\ iv) & A \to \overline{\overline{A}} \qquad \overline{\overline{A}} \to A \end{array}$$

Rules:

$$1)\ \frac{A \to B\ ;\ B \to C}{A \to C} \qquad \left(\frac{\text{if } A \text{ then } B;\ \text{if } B \text{ then } C}{\text{if } A \text{ then } C}\right)$$

$$2)\ \frac{A \to B\ ;\ A}{B} \qquad \left(\frac{\text{if } A \text{ then } B\ ;\ \text{but } A}{B}\right)$$

$$3)\ \frac{A \to B\ ;\ \overline{B}}{\overline{A}} \qquad \left(\frac{\text{if } A \text{ then } B\ ;\ \text{but not } B}{\text{not } A}\right)$$

a derivation:

$$\dfrac{c \to \overline{a} \qquad \dfrac{a \to \overline{\overline{a}}\ ;\ a}{\overline{\overline{a}}}}{\overline{c}}$$

Although the axiomatic method of characterizing such theories with axioms or postulates or both and a small number of rules of inference had a very old history (going back to Euclid or further), two new methods arose in the 1930s and '40s.

1. First, in 1934, there was the German mathematician Gerhard Gentzen's method of succinct Sequenzen (rules of consequents), which were especially useful for deriving metalogical decidability results. This method originated with Paul Hertz in 1932, and a related method was described by Stanisław Jaśkowski in 1934.
2. Next to appear was the similarly axiomless method of "natural deduction," which used only rules of inference; it originated in a suggestion by Russell in 1925 but was developed by Quine and the American logicians Frederick Fitch and George David Wharton Berry. The natural deduction technique is widely used in the teaching of logic, although it makes the demonstration of metalogical results somewhat difficult, partly because historically these arose in axiomatic and consequent formulations.

A formal description of a language, together with a specification of a theory's theorems (derivable propositions), are often called the "syntax" of the theory. (This is somewhat misleading when one compares the practice in linguistics, which would limit syntax to the narrower issue of grammaticality.) The term "calculus" is sometimes chosen to emphasize the purely syntactic, uninterpreted nature of a formal theory.

(3) The last component of a logical system is the semantics for such a theory and language:

> *a declaration of what the terms of a theory refer to, and how the basic operations and connectives are to be interpreted in a domain of discourse, including truth conditions for wffs in this domain.*

Consider, as an example the following rule

$$\frac{A \to B \ \ ; \ \ B \to C}{A \to C}$$

It is merely a "piece of text" and its symbols allow almost unlimited interpretations. We may, for instance, take A, B, C to be (some particular) propositions and $\to$ an implication, but also the former to be sets and the latter set-inclusion.

If	it's nice	then	we'll go		a	$\subseteq$	b
If	we go	then	we'll see a movie	or	b	$\subseteq$	c
If	it's nice	then	we'll see a movie		a	$\subseteq$	c

A specification of a domain of objects (De Morgan's "universe of discourse"), and of rules for interpreting the symbols of a logical language in this domain such that all the theorems of the logical theory are true is then said to be a "model" of the theory (or sometimes, less carefully, an "interpretation" of the theory). We devote next subsection exclusively to this aspect.

E.2. Formal semantics

What is known as formal semantics, or model theory, has a more complicated history than does logical syntax; indeed, one could say that the history of the emergence of semantic conceptions of logic in the late 19th and early 20th centuries is poorly understood even today. Certainly, Frege's notion that propositions refer to (German: bedeuten) "The True" or "The False" – and this for complex propositions as a function of the truth values of simple propositions – counts as semantics. As we mentioned earlier, this has often been the intuition since Aristotle, although modal propositions and paradoxes like the "liar paradox" pose some problems for this understanding. Nevertheless, this view dominates most of the logic, in particular such basic fields as propositional and fist order logic. Also, earlier medieval theories of supposition incorporated useful semantic observations. So, too, do Boolean techniques of letters taking or referring to the values 1 and 0 that are seen from Boole through Peirce and Schröder. Both Peirce and Schröder occasionally gave brief demonstrations of the independence of certain logical postulates using models in which some postulates were true, but not others. This was also the technique used by the inventors of non-Euclidean geometry.

The first clear and significant general result in model theory is usually accepted to be a result discovered by Löwenheim in 1915 and strengthened in work by Skolem from the 1920s.

Löwenheim-Skolem theorem
A theory that has a model at all has a countable model.

That is to say, if there exists some model of a theory (i.e., an application of it to some domain of objects), then there is sure to be one with a domain no larger than the natural numbers. Although Löwenheim and Skolem understood their results perfectly well, they did not explicitly use the modern language of "theories" being true in "models." The Löwenheim-Skolem theorem is in some ways a shocking result, since it implies that any consistent formal theory of anything – no matter how hard it tries to address the phenomena unique to a field such as biology, physics, or even sets or just real numbers – can just as well be understood from its formalisms alone as being about natural numbers.

Consistency

The second major result in formal semantics, Gödel's completeness theorem of 1930, required even for its description, let alone its proof, more careful development of precise concepts about logical systems – metalogical concepts – than existed in earlier decades. One question for all logicians since Boole, and certainly since Frege, had been:

Is the theory consistent? In its purely syntactic analysis, this amounts to the question: Is a contradictory sentence (of the form "A and not-A") a theorem?

In its semantic analysis, it is equivalent to the question:

Does the theory have a model at all?

For a logical theory, consistency means that a contradictory theorem cannot be derived in the theory. But since logic was intended to be a theory of necessarily true statements, the goal was stronger: a theory is Post-consistent (named for the Polish-American logician Emil Post) if every theorem is valid – that is, if no theorem is a contradictory or a contingent statement. (In nonclassical logical systems, one may define many other interestingly distinct notions of consistency; these notions were not distinguished until the 1930s.) Consistency was quickly acknowledged as a desired feature of formal systems: it was widely and correctly assumed that various earlier theories of propositional and first-order logic were consistent. Zermelo was, as has been observed, concerned with demonstrating that ZF was consistent; Hilbert had even observed that there was no proof that the Peano postulates were consistent. These questions received an answer that was not what was hoped for in a later result – Gödel's incompleteness theorem. A clear proof of the consistency of propositional logic was first given by Post in 1921. Its tardiness in the history of symbolic logic is a commentary not so much on the difficulty of the problem as it is on the slow emergence of the semantic and syntactic notions necessary to characterize consistency precisely. The first clear proof of the consistency of the first-order predicate logic is found in the work of Hilbert and Wilhelm Ackermann from 1928. Here the problem was not only the precise awareness of consistency as a property of formal theories but also of a rigorous statement of first-order predicate logic as a formal theory.

Completeness

In 1928 Hilbert and Ackermann also posed the question of whether a logical system, and, in particular, first-order predicate logic, was (as it is now called) *"complete"*. This is the question of

whether every valid proposition – that is, every proposition that is true in all intended models – is provable in the theory.

In other words, does the formal theory describe all the noncontingent truths of a subject matter? Although some sort of completeness had clearly been a guiding principle of formal logical theories dating back to Boole, and even to Aristotle (and to Euclid in geometry) – otherwise they would not have sought numerous axioms or postulates, risking nonindependence and even inconsistency – earlier writers seemed to have lacked the semantic terminology to specify what their theory was about and wherein "aboutness" consists. Specifically, they lacked a precise notion of a proposition being *"valid"*, – that is, "true in all (intended) models" – and hence lacked a way of precisely characterizing completeness. Even the language of Hilbert and Ackermann from 1928 is not perfectly clear by modern standards.

Gödel proved the completeness of first-order predicate logic in his doctoral dissertation of 1930; Post had shown the completeness of propositional logic in 1921. In many ways, however, explicit consideration of issues in semantics, along with the development of many of the concepts now widely used in formal semantics and model theory (including the term metalanguage), first appeared in a paper by Alfred Tarski, *The Concept of Truth in Formalized Languages*, published in Polish in 1933; it became widely known through a German translation of 1936. Although the theory of truth Tarski advocated has had a complex and debated legacy, there is little doubt that the concepts there (and in later papers from the 1930s) developed for discussing what it is for a sentence to be "true in" a model marked the beginning of model theory in its modern phase. Although the outlines of how to model propositional logic had been clear to the Booleans and to Frege, one of Tarski's most important contributions was an application of his general theory of semantics in a proposal for the semantics of the first-order predicate logic (now termed the set-theoretic, or Tarskian, interpretation).

Tarski's techniques and language for precisely discussing semantic concepts, as well as properties of formal systems described using his concepts – such as consistency, completeness, and independence – rapidly and almost imperceptibly entered the literature in the late 1930s and after. This influence accelerated with the publication of many of his works in German and then in English, and with his move to the United States in 1939.

E.3. Computability and Decidability

An underlying theme of the whole development we have sketched were the attempts to *formalize* logical reasoning, hopefully, to the level at which it can be performed mechanically. The idea of "mechanical reasoning" was contemplated by Leibniz. Also in 17th century, Pascal designed a machine – a kind of calculator – which could perform arithmetical operations (and was used by his father in his shop). In the 20th century the questions about computability were raised by the logicians. The answers led to what is today called "informational revolution" centering around the design and use of computers.

Computability

What does it mean that something can be computed mechanically*?*

In the 1930s this question acquired much more precise meaning than ever before. In the proof of incompleteness theorem Gödel introduced special schemata for, so called *"recursive functions"* working on natural numbers. Some time later Church proposed the thesis

Church thesis

A function is computable if and only if it can be defined using only recursive functions.

This may sound astonishing – why just recursive function are to have such a special significance? The answer comes from the work of Alan Turing who introduced "devices" which came to be known as *Turing machines*. Although defined as conceptual entities, one could easily imagine that such devices could be actually built as physical machines performing exactly the operations suggested by Turing. The machines could, for instance, recognize whether a string had some specific form and, generally, compute functions. In fact, the functions which could be computed on Turing machines were shown to be exactly the recursive functions!

Church thesis remains still *only* a thesis. Nevertheless, so far nobody has proposed a notion of computability which would exceed the capacities of Turing machines (and hence of recursive functions). A modern computer, with all its sophistication and high level tools is, at the bottom, *nothing more* than a Turing machine! Thus, logical results, in particular the negative theorems stating the limitations of logical formalism (like Gödel's incompleteness theorem) determine also the ultimate limits of computers' capabilities.

Decidability

By the 1930s almost all work in the foundations of mathematics and in symbolic logic was being done in a standard first-order predicate logic, often extended with axioms or axiom schemata of set- or type-theory. This underlying logic consisted of a theory of "classical" truth functional connectives, such as "and", "not" and "if . . . then" (propositional logic) and first-order quantification permitting propositions that "all" and "at least one" individual satisfy a certain formula. Only gradually in the 1920s and '30s did a conception of a "first-order" logic, and of alternatives, arise – and then without a name.

Formal theories can be classified according to their *"expressive power"*, depending on the language (notation) as well as reasoning system (inference rules) they are using. Propositional logic allows merely manipulation of simple propositions combined with operators like "or", "and". First-order theories allow explicit reference to, and quantification over, individuals, such as numbers or sets, but not quantification over (and hence rules for manipulating) properties of these individuals. For instance, the statement "for all x: if x is A then x is B" is first-order, but "for all P and

R and x: if x is P then x is R" is not (it is second-order because it involves quantification over predicate-variables P and R). Similarly, the fifth postulate of Euclid is a schema or second-order formulation, rather than being strictly in the finitely axiomatizable first-order language that was once preferred.

The question "why should one bother with less expressive formalisms, when more expressive ones are available?" may in this context seem quite natural. The answer lies in the fact that increasing expressive power of a formalisms clashes with another desired feature, namely:

> **decidability**
> *there exists a finite mechanical procedure for determining whether a proposition is, or is not, a theorem of the theory.*

This property took on added interest after World War II with the advent of electronic computers, since modern computers can actually apply algorithms to determine whether a given proposition is, or is not, a theorem, whereas some algorithms had only been shown theoretically to exist. The problems which can be effectively solved by Turing machines (and hence computers) are among the decidable problems.

The decidability of propositional logic, through the use of truth tables, was known to Frege and Peirce; a proof of its decidability is attributable to Jan Lukasiewicz and Emil Post independently in 1921. Löwenheim showed in 1915 that first-order predicate logic with only single-place predicates was decidable and that the full theory was decidable if the first-order predicate calculus with only two-place predicates was decidable; further developments were made by Skolem, Heinrich Behmann, Jacques Herbrand, and Quine. Herbrand showed the existence of an algorithm which, if a theorem of the first-order predicate logic is valid, will determine it to be so; the difficulty, then, was in designing an algorithm that in a finite amount of time would determine that propositions were invalid. As early as the 1880s, Peirce seemed to be aware that the propositional logic was decidable but that the full first-order predicate logic with relations was undecidable. The proof that first-order predicate logic (in any general formulation) was *undecidable* was first shown definitively by Alan Turing and Alonzo Church independently in 1936. Together with Gödel's (second) incompleteness theorem and the earlier Löwenheim-Skolem theorem, the Church-Turing theorem of the undecidability of the first-order predicate logic is one of the most important, even if "negative", results of 20th-century logic. Among the consequences of these negative results are simple facts about limits of modern computers: it is impossible to design a computer and write a computer program which, given an arbitrary first-order theory T and some formula f, is guaranteed to give an answer "Yes" if f is a theorem of T and "No" if it is not.

Bibliography

General and introductory texts

1. D.GABBAY and F. GUENTHNER (eds.), Handbook of Philosophical Logic, 4 vol. (1983-89).
2. GERALD J. MASSEY, Understanding Symbolic Logic (1970).
3. THIERRY SCHEURER, Foundations of Computing, Addison-Wesley (1994).
4. V.SPERSCHNEIDER, G.ANTONIOU, Logic: A Foundatiuon for Computer Science, Addison-Wesley (1991).
5. WILLARD V. QUINE, Methods of Logic, Harvard University Press, 1st. ed. (1950, reprinted 1982).
6. JENS ERIK FENSTAD, DAG NORMANN, Algorithms and Logic, Matematisk Institutt, Universitetet i Oslo (1984).
7. GERALD J. MASSEY, Understanding Symbolic Logic (1970).
8. ELLIOTT MENDELSON, Introduction to Mathematical Logic, 3rd ed. (1987).

9. CHIN-LIANG CHANG, RICHARD CHAR-TUNG LEE, Symbolic Logic and Mechanical Theorem Proving, Academic Press Inc. (1973).
10. R.D.DOWSING, V.J.RAYWARD-SMITH, C.D.WALTER, A First Course in Formal Logic and its Applications in Computer Science, Alfred Waller Ltd. 2nd ed. (1994).
11. RAMIN YASID, Logic and Programming in Logic, Immediate Publishing (1997).
12. ROBERT E. BUTTS and JAAKKO HINTIKKA, Logic, Foundations of Mathematics, and Computability Theory (1977), a collection of conference papers.

History of logic

1. WILLIAM KNEALE and MARTHA KNEALE, The Development of Logic (1962, reprinted 1984).
2. The Encyclopedia of Philosophy, ed. by PAUL EDWARDS, 8 vol. (1967).
3. New Catholic Encyclopedia, 18 vol. (1967-89).
4. I.M. BOCHEŃSKI, Ancient Formal Logic (1951, reprinted 1968).

On Aristotle:

5. JAN LUKASIEWICZ, Aristotle's Syllogistic from the Standpoint of Modern Formal Logic, 2nd ed., enlarged (1957, reprinted 1987).
6. GÜNTHER PATZIG, Aristotle's Theory of the Syllogism (1968; originally published in German, 2nd ed., 1959).
7. OTTO A. BIRD, Syllogistic and Its Extensions (1964).
8. STORRS McCALL, Aristotle's Modal Syllogisms (1963).
9. I.M. BOCHEŃSKI, La Logique de Theophraste (1947, reprinted 1987).

On Stoics:

10. BENSON MATES, Stoic Logic (1953, reprinted 1973).
11. MICHAEL FREDE, Die stoische Logik (1974).

Medieval logic:

12. NORMAN KRETZMANN, ANTHONY KENNY, and JAN PINBORG (eds.), The Cambridge History of Later Medieval Philosophy: From the Rediscovery of Aristotle to the Disintegration of Scholasticism, 1100-1600 (1982).
13. NORMAN KRETZMANN and ELEONORE STUMP (eds.), Logic and the Philosophy of Language (1988).
14. For Boethius, see: MARGARET GIBSON (ed.), Boethius, His Life, Thought, and Influence (1981).

Arabic logic:

15. NICHOLAS RESCHER, The Development of Arabic Logic (1964).
16. L.M. DE RIJK, Logica Modernorum: A Contribution to the History of Early Terminist Logic, 2 vol. in 3 (1962-1967).
17. NORMAN KRETZMANN (ed.), Meaning and Inference in Medieval Philosophy (1988).

Surveys of modern logic:

18. WILHELM RISSE, Die Logik der Neuzeit, 2 vol. (1964-70).
19. ROBERT ADAMSON, A Short History of Logic (1911, reprinted 1965).
20. C.I. LEWIS, A Survey of Symbolic Logic (1918, reissued 1960).
21. JÖRGEN JRGENSEN, A Treatise of Formal Logic: Its Evolution and Main Branches with Its Relations to Mathematics and Philosophy, 3 vol. (1931, reissued 1962).

22. ALONZO CHURCH, Introduction to Mathematical Logic (1956).
23. I.M. BOCHEŃSKI, A History of Formal Logic, 2nd ed. (1970; originally published in German, 1962).
24. HEINRICH SCHOLZ, Concise History of Logic (1961; originally published in German, 1959).
25. ALICE M. HILTON, Logic, Computing Machines, and Automation (1963);
26. N.I. STYAZHKIN, History of Mathematical Logic from Leibniz to Peano (1969; originally published in Russian, 1964);
27. CARL B. BOYER, A History of Mathematics, 2nd ed., rev. by UTA C. MERZBACH (1991);
28. E.M. BARTH, The Logic of the Articles in Traditional Philosophy: A Contribution to the Study of Conceptual Structures (1974; originally published in Dutch, 1971);
29. MARTIN GARDNER, Logic Machines and Diagrams, 2nd ed. (1982); and
30. E.J. ASHWORTH, Studies in Post-Medieval Semantics (1985).

Developments in the science of logic in the 20th century are reflected mostly in periodical literature.

31. WARREN D. GOLDFARB, "Logic in the Twenties: The Nature of the Quantifier," The Journal of Symbolic Logic 44:351-368 (September 1979);
32. R.L. VAUGHT, "Model Theory Before 1945," and C.C. CHANG, "Model Theory 1945-1971," both in LEON HENKIN et al. (eds.), Proceedings of the Tarski Symposium (1974), pp. 153-172 and 173-186, respectively; and
33. IAN HACKING, "What is Logic?" The Journal of Philosophy 76:285-319 (June 1979).
34. Other journals devoted to the subject include History and Philosophy of Logic (biannual); Notre Dame Journal of Formal Logic (quarterly); and Modern Logic (quarterly).

Formal logic

1. MICHAEL DUMMETT, Elements of Intuitionism (1977), offers a clear presentation of the philosophic approach that demands constructibility in logical proofs.
2. G.E. HUGHES and M.J. CRESSWELL, An Introduction to Modal Logic (1968, reprinted 1989), treats operators acting on sentences in first-order logic (or predicate calculus) so that, instead of being interpreted as statements of fact, they become necessarily or possibly true or true at all or some times in the past, or they denote obligatory or permissible actions, and so on.
3. JON BARWISE et al. (eds.), Handbook of Mathematical Logic (1977), provides a technical survey of work in the foundations of mathematics (set theory) and in proof theory (theories with infinitely long expressions).
4. ELLIOTT MENDELSON, Introduction to Mathematical Logic, 3rd ed. (1987), is the standard text; and
5. G. KREISEL and J.L. KRIVINE, Elements of Mathematical Logic: Model Theory (1967, reprinted 1971; originally published in French, 1967), covers all standard topics at an advanced level.
6. A.S. TROELSTRA, Choice Sequences: A Chapter of Intuitionistic Mathematics (1977), offers an advanced analysis of the philosophical position regarding what are legitimate proofs and logical truths; and
7. A.S. TROELSTRA and D. VAN DALEN, Constructivism in Mathematics, 2 vol. (1988), applies intuitionist strictures to the problem of the foundations of mathematics.

Metalogic

1. JON BARWISE and S. FEFERMAN (eds.), Model-Theoretic Logics (1985), emphasizes semantics of models.
2. J.L. BELL and A.B. SLOMSON, Models and Ultraproducts: An Introduction, 3rd rev. ed. (1974), explores technical semantics.
3. RICHARD MONTAGUE, Formal Philosophy: Selected Papers of Richard Montague, ed. by RICHMOND H. THOMASON (1974), uses modern logic to deal with the semantics of natural languages.
4. MARTIN DAVIS, Computability and Unsolvability (1958, reprinted with a new preface and appendix, 1982), is an early classic on important work arising from Gödel's theorem, and the same author's The Undecidable: Basic Papers on Undecidable Propositions, Unsolvable Problems, and Computable Functions (1965), is a collection of seminal papers on issues of computability.
5. ROLF HERKEN (ed.), The Universal Turing Machine: A Half-Century Survey (1988), takes a look at where Gödel's theorem on undecidable sentences has led researchers.
6. HANS HERMES, Enumerability, Decidability, Computability, 2nd rev. ed. (1969, originally published in German, 1961), offers an excellent mathematical introduction to the theory of computability and Turing machines.
7. A classic treatment of computability is presented in HARTLEY ROGERS, JR., Theory of Recursive Functions and Effective Computability (1967, reissued 1987).
8. M.E. SZABO, Algebra of Proofs (1978), is an advanced treatment of syntactical proof theory.
9. P.T. JOHNSTONE, Topos Theory (1977), explores the theory of structures that can serve as interpretations of various theories stated in predicate calculus.
10. H.J. KEISLER, "Logic with the Quantifier 'There Exist Uncountably Many'," Annals of Mathematical Logic 1:1-93 (January 1970), reports on a seminal investigation that opened the way for Barwise (1977), cited earlier, and
11. CAROL RUTH KARP, Language with Expressions of Infinite Length (1964), which expands the syntax of the language of predicate calculus so that expressions of infinite length can be constructed.
12. C.C. CHANG and H.J. KEISLER, Model Theory, 3rd rev. ed. (1990), is the single most important text on semantics.
13. F.W. LAWVERE, C. MAURER, and G.C. WRAITH (eds.), Model Theory and Topoi (1975), is an advanced, mathematically sophisticated treatment of the semantics of theories expressed in predicate calculus with identity.
14. MICHAEL MAKKAI and GONZALO REYES, First Order Categorical Logic: Model-Theoretical Methods in the Theory of Topoi and Related Categories (1977), analyzes the semantics of theories expressed in predicate calculus.
15. SAHARON SHELAH, "Stability, the F.C.P., and Superstability: Model-Theoretic Properties of Formulas in First Order Theory," Annals of Mathematical Logic 3:271-362 (October 1971), explores advanced semantics.

Applied logic

1. Applications of logic in unexpected areas of philosophy are studied in EVANDRO AGAZZI (ed.), Modern Logic–A Survey: Historical, Philosophical, and Mathematical Aspects of Modern Logic and Its Applications (1981).
2. WILLIAM L. HARPER, ROBERT STALNAKER, and GLENN PEARCE (eds.), IFs: Conditionals, Belief, Decision, Chance, and Time (1981), surveys hypothetical reasoning and inductive reasoning.

3. On the applied logic in philosophy of language, see EDWARD L. KEENAN (ed.), Formal Semantics of Natural Language (1975);
4. JOHAN VAN BENTHEM, Language in Action: Categories, Lambdas, and Dynamic Logic (1991), also discussing the temporal stages in the working out of computer programs, and the same author's Essays in Logical Semantics (1986), emphasizing grammars of natural languages.
5. DAVID HAREL, First-Order Dynamic Logic (1979); and J.W. LLOYD, Foundations of Logic Programming, 2nd extended ed. (1987), study the logic of computer programming.
6. Important topics in artificial intelligence, or computer reasoning, are studied in PETER GOERDENFORS, Knowledge in Flux: Modeling the Dynamics of Epistemic States (1988), including the problem of changing one's premises during the course of an argument.
7. For more on nonmonotonic logic, see JOHN McCARTHY, "Circumscription: A Form of Non-Monotonic Reasoning," Artificial Intelligence 13(1-2):27-39 (April 1980);
8. DREW McDERMOTT and JON DOYLE, "Non-Monotonic Logic I," Artificial Intelligence 13(1-2):41-72 (April 1980);
9. DREW McDERMOTT, "Nonmonotonic Logic II: Nonmonotonic Modal Theories," Journal of the Association for Computing Machinery 29(1):33-57 (January 1982); and
10. YOAV SHOHAM, Reasoning About Change: Time and Causation from the Standpoint of Artificial Intelligence (1988).

Chapter 1

Sets, Functions, Relations

- Sets and Functions
  - Set building operations
  - Some equational laws
- Relations and Sets with Structures
  - Properties of relations
  - Ordering relations
- Infinities
  - Countability vs. uncountability

1: Sets and Functions

◇ a Background Story ◇

A set is an arbitrary collection of arbitrary objects, called its members. One should take these two occurrences of "arbitrary" seriously. Firstly, sets may be finite, e.g., the set C of cars on the parking lot outside the building, or infinite, e.g. the set N of numbers greater than 5.

Secondly, any objects can be members of sets. We can talk about sets of cars, blood-cells, numbers, Roman emperors, etc. We can also talk about the set X whose elements are: my car, your mother and number 6. (Not that such a set necessarily is useful for any purpose, but it is possible to collect these various elements into one set.) In particular sets themselves can be members of other sets. I can, for instance, form the set whose elements are: my favorite pen, my four best friends and the set N*. This set will have 6 elements, even though the set N itself is infinite.*

A set with only one element is called a singleton*, e.g., the set containing only planet Earth. There is one special and very important set – the* empty *set – which has no members. If it seems startling, you may think of the set of all square circles or all numbers x such that $x < x$. This set is mainly a mathematical convenience – defining a set by describing the properties of its members in an involved way, we may not know from the very begining what its members are. Eventually, we may find that no such objects exist, that is, that we defined an empty set. It also makes many formulations simpler since, without the assumption of its existence, one would often had to take special precautions for the case a set happened to contain no elements.*

It may be legitimate to speak about a set even if we do not know exactly its members. The set of people born in 1964 may be hard to determine exactly but it is a well defined object because, at least in principle, we can determine membership of any object in this set. Similarly, we will say that the set R of red objects is well defined even if we certainly do not know all its members. But confronted with a new object, we can determine if it belongs to R or not (assuming, that we do not dispute the meaning of the word "red"*.)*

There are four basic means of specifying a set.

1. *If a set is finite and small, we may list all its elements, e.g., $S = \{1, 2, 3, 4\}$ is a set with four elements.*

2. A set can be specified by determining a property which makes objects qualify as its elements. The set R of red objects is specified in this way. The set S can be described as 'the set of natural numbers greater than 0 and less than 5'.

3. A set may be obtained from other sets. For instance, given the set S and the set $S' = \{3, 4, 5, 6\}$ we can form a new set $S'' = \{3, 4\}$ which is the *intersection* of S and S'. Given the sets of odd $\{1, 3, 5, 7, 9...\}$ and even numbers $\{0, 2, 4, 6, 8...\}$ we can form a new set $\mathbf{N}$ by taking their *union*.

4. Finally, a set can be determined by describing the rules by which its elements may be generated. For instance, the set $\mathbf{N}$ of natural numbers $\{0, 1, 2, 3, 4, ...\}$ can be described as follows: 0 belongs to $\mathbf{N}$ and if n belongs to $\mathbf{N}$, then also $n + 1$ belongs to $\mathbf{N}$ and, finally, nothing else belongs to $\mathbf{N}$.

In this chapter we will use mainly the first three ways of describing sets. In particular, we will use various set building operations as in point 3. In the later chapters, we will constantly encouter sets described by the last method. One important point is that the properties of a set are entirely independent from the way the set is described. Whether we just say 'the set of natural numbers' or the set $\mathbf{N}$ as defined in point 2. or 4., we get the same set. Another thing is that *studying and proving* properties of a set may be easier when the set is described in one way rather than another.

$\diamond$ ——————————————————————— $\diamond$

Definition 1.1 Given some sets S and T we write:

$x \in S$	- x is a member (element) of S	
$S \subseteq T$	- S is a subset of T	for all x : if $x \in S$ then $x \in T$
$S \subset T$	- $S \subseteq T$ and $S \neq T$	for all x : if $x \in S$ then $x \in T$ and there is an $x : x \in T$ and $x \notin S$
Set building operations :		
$\emptyset$	- empty set	for any $x : x \notin \emptyset$
$S \cup T$	- union of S and T	$x \in S \cup T$ iff $x \in S$ or $x \in T$
$S \cap T$	- intersection of S and T	$x \in S \cap T$ iff $x \in S$ and $x \in T$
$S \setminus T$	- difference of S and T	$x \in S \setminus T$ iff $x \in S$ and $x \notin T$
S'	- complement of S; assuming a universe U of all elements $S' = U \setminus S$	
$S \times T$	- Cartesian product of S and T	$x \in S \times T$ iff $x = \langle s, t \rangle$ and $s \in S$ and $t \in T$
$\wp(S)$	- the power set of S	$x \in \wp(S)$ iff $x \subseteq S$
$\{x \in S : \mathsf{Prop}(x)\}$	- set of those $x \in S$ which have the specified property Prop	

Remark.
Notice that sets may be members of other sets. For instance $\{\emptyset\}$ is the set with one element – which is the empty set $\emptyset$. In fact, $\{\emptyset\} = \wp(\emptyset)$. It is different from the set $\emptyset$ which has no elements. $\{\{a, b\}, a\}$ is a set with two elements: a and the set $\{a, b\}$. Also $\{a, \{a\}\}$ has two different elements: a and $\{a\}$.
In particular, the power set will contain many sets as elements: $\wp(\{a, \{a, b\}\}) = \{\emptyset, \{a\}, \{\{a, b\}\}, \{a, \{a, b\}\}\}$.

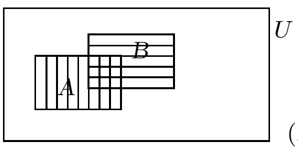
In the definition of Cartesian product, we used the notation $\langle s, t \rangle$ to denote an *ordered* pair whose first element is s and second t. In set theory, all possible objects are modelled as sets. An ordered pair $\langle s, t \rangle$ is then represented as the set with two elements – both being sets – $\{\{s\}, \{s, t\}\}$. Why not $\{\{s\}, \{t\}\}$ or, even simpler, $\{s, t\}$? Because elements of a set are not ordered. Thus $\{s, t\}$ and $\{t, s\}$ denote the same set. Also, $\{\{s\}, \{t\}\}$ and $\{\{t\}, \{s\}\}$ denote the same set (but different from the set $\{s, t\}$). In ordered pairs, on the other hand, the order does matter – $\langle s, t \rangle$ and $\langle t, s \rangle$ are different pairs. This ordering is captured by the representation $\{\{s\}, \{s, t\}\}$. We have here a set with two elements $\{A, B\}$ where $A = \{s\}$ and $B = \{s, t\}$. The relationship between these two elements tells us which is the first and which the second: $A \subset B$ identifies the member of A as the first element of the pair, and then the element of $B \setminus A$ as the second one. Thus $\langle s,t\rangle = \{\{s\},\{s,t\}\} \neq \{\{t\},\{s,t\}\} = \langle t,s\rangle$. $\square$

The set operations $\cup$, $\cap$, $'$ and $\setminus$ obey some well known laws:

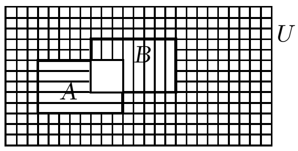
1. Idempotency
$$\begin{aligned} A\cup A &= A \\ A\cap A &= A \end{aligned}$$
2. Associativity
$$\begin{aligned} (A\cup B)\cup C &= A\cup(B\cup C) \\ (A\cap B)\cap C &= A\cap(B\cap C) \end{aligned}$$
3. Commutativity
$$\begin{aligned} A\cup B &= B\cup A \\ A\cap B &= B\cap A \end{aligned}$$
4. Distributivity
$$\begin{aligned} A\cup(B\cap C) &= (A\cup B)\cap(A\cup C) \\ A\cap(B\cup C) &= (A\cap B)\cup(A\cap C) \end{aligned}$$
5. DeMorgan
$$\begin{aligned} (A\cup B)' &= A'\cap B' \\ (A\cap B)' &= A'\cup B' \end{aligned}$$
6. Complement
$$\begin{aligned} A\cap A' &= \emptyset \\ A\setminus B &= A\cap B' \end{aligned}$$
7. Emptyset
$$\emptyset\cup A = A \qquad\qquad \emptyset\cap A = \emptyset$$
8. Consistency principles

   a) $A\subseteq B$ iff $A\cup B = B$ b) $A\subseteq B$ iff $A\cap B = A$

Remark 1.2 **[Venn's diagrams]**
It is very common to represent sets and set relations by means of Venn's diagrams – overlapping figures, typically, circles or rectangles. On the the left in the figure below, we have two sets A and B in some universe U. Their intersection $A\cap B$ is marked as the area belonging to both by both vertical and horisontal lines. If we take A to represent Armenians and B bachelors, the darkest region in the middle represents Armenian bachelors. The region covered by only vertical, but not horisontal, lines is the set difference $A\setminus B$ – Armenians who are not bachelors. The whole region covered by either vertical or horisontal lines represents all those who are either Armenian or are bachelors.



$(A\cup B)' = A'\cap B'$



Now, the white region is the complement of the set $A\cup B$ (in the universe U) – all those who are neither Armenians nor bachelors. The diagram to the right is essentially the same but was constructed in a different way. Here, the region covered with vertical lines is the complement of A – all non-Armenians. The region covered with horisontal lines represents all non-bachelors. The region covered with *both* horisontal and vertical lines is the intersection of these two complements – all those who are neither Armenians nor bachelors. The two diagrams illustrate the first DeMorgan law since the white area on the left, $(A\cup B)'$, is exactly the same as the area covered with both horisontal and vertical lines on the right, $A'\cap B'$. $\square$

Definition 1.3 Given two sets S and T, a *function* f from S to T, $f : S\to T$, is a subset of $S\times T$ such that

- whenever $\langle s,t\rangle\in f$ and $\langle s,t'\rangle\in f$, then $t = t'$, and
- for each $s\in S$ there is some $t\in T$ such that $\langle s,t\rangle\in f$.

A subset of $S\times T$ that satisfies the first condition above but not necessarily the second, is called a *partial* function from S to T.

For a function $f : S\to T$, the set S is called the *source* or *domain* of the function, and the set T its *target* or *codomain*.

The second point of this definition means that function is *total* – for each argument (element $s\in S$), the function has some value, i.e., an element $t\in T$ such that $\langle s,t\rangle\in f$. Sometimes this requirement is dropped and one speaks about *partial functions* which may have no value for some arguments but we will be for the most concerned with total functions.

Example 1.4
Let $\mathbf{N}$ denote the set of natural numbers $\{0, 1, 2, 3, ...\}$. The mapping $f : \mathbf{N} \to \mathbf{N}$ defined by $f(n) = 2n$ is a function. It is the set of all pairs $f = \{\langle n, 2n\rangle : n \in \mathbf{N}\}$. If we let M denote the set of all people, then the set of all pairs $father = \{\langle m, m\text{'s father}\rangle : m \in M\}$ is a function assigning to each person his/her father. A mapping '*children*', assigning to each person his/her children is not a function $M \to M$ for two reasons. For the first, a person may have no children, while saying "function" we mean a total function. For the second, a person may have more than one child. These problems may be overcome if we considered it instead as a function $M \to \wp(M)$ assigning to each person the set (possibly empty) of all his/her children. □

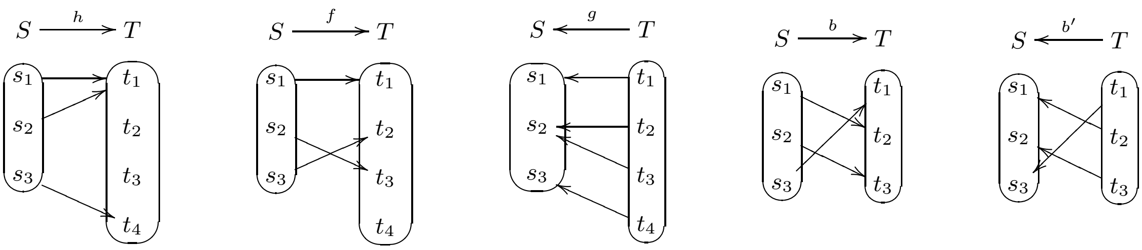
Notice that although intuitively we think of a function as a mapping assigning to each argument some value, the definition states that it is actually a set (a subset of $S \times T$ is a set.) The restrictions put on this set are exactly what makes it possible to think of this set as a mapping. Nevertheless, functions – being sets – can be elements of other sets. We may encounter situations involving sets of functions, e.g. the set T^S of all functions from set S to set T, which is just the set of all subsets of $S \times T$, each satisfying the conditions of the definition 1.3.

Notation.
A function f associates with each element $s \in S$ a *unique* element $t \in T$. We write this t as $f(s)$ – the value of f at point s.
When S is finite (and small) we may sometimes write a function as a set $\{\langle s_1, t_1\rangle, \langle s_2, t_2\rangle, ..., \langle s_n, t_n\rangle\}$ or else as $\{s_1 \mapsto t_1, s_2 \mapsto t_2, ..., s_n \mapsto t_n\}$.
If f is given then by $f[s \mapsto p]$ we denote the function f' which is the same as f for all arguments $x \neq s : f'(x) = f(x)$, while $f'(s) = p$. □

Definition 1.5 A function $f : S \to T$ is
injective iff whenever $f(s) = f(s')$ then $s = s'$;
surjective iff for all $t \in T$ there exists an $s \in S$ such that $f(s) = t$;
bijective, or a **set-isomorphism**, iff it is both injective and surjective.

Injectivity means that no two distinct elements from the source set are mapped to the same element in the target set; surjectivity that each element in the target is an image of some element from the source.

Example 1.6
The function $father : M \to M$ is injective – everybody has exactly one (biological) father, but it is not surjective – not everybody is a father of somebody. The following drawing gives some examples:



Here h is neither injective nor surjective, f is injective but not surjective, $g : T \to S$ is surjective but not injective. b and b' are both injective and surjective, i.e, bijective. □

Soon we will see the particular importance of bijections. There may exist several different set-isomorphisms between two sets S and T. If there is at least one set-isomorphism, we say that the two sets are isomorphic and write $S \rightleftharpoons T$. The following lemma gives another criterion for a function to be a bijection.

Lemma 1.7 $f : S \to T$ is a set-isomorphism if and only if there is an *inverse* function $f^{-1} : T \to S$, such that for all $s \in S : f^{-1}(f(s)) = s$ and for all $t \in T : f(f^{-1}(t)) = t$.

Proof We have to show two implications:

only if) If f is iso, we can define f^{-1} simply as the set of pairs $f^{-1} \stackrel{\text{def}}{=} \{\langle t, s\rangle : t = f(s)\}$.

if) We show this contrapositively. Assume that there is an inverse f^{-1} while f is not injective, i.e., there are $s \neq s' : f(s) = f(s') = t$. Then $s = f^{-1}(f(s)) = f^{-1}(t) = f^{-1}(f(s')) = s'$. But this contradicts the assumption $s \neq s'$, so f must be injective.
Now assume that f is not surjective, i.e., there is a t such that for all $s \in S : f(s) \neq t$. Then for some $s \in S : f^{-1}(t) = s$, and so $f(s) = f(f^{-1}(t)) = t$, contradicting the assumption.
QED (1.7)

In the example 1.6 both b and b' were bijective. In fact, they acted as mutual inverses satisfying the conditions of the above lemma: for each $s \in S; b'(b(s)) = s$ and for each $t \in T : b(b'(t)) = t$.

Definition 1.8 For any set A, the *characteristic function* of A, denoted f_A, is the function

$$\{\langle x, \mathbf{1}\rangle \mid x \in A\} \ \cup \ \{\langle x, \mathbf{0}\rangle \mid x \in A'\}.$$

Hence $f_A(x) = \mathbf{1}$ iff $x \in A$. Note that f_A is a function from U to $\{\mathbf{1}, \mathbf{0}\}$, where U is the actual universe (of sets) and $\{\mathbf{1}, \mathbf{0}\}$ is a set with exactly two elements.

Let $f_\_ : \wp(U) \to 2^U$ denote the function sending each subset A of U to its characteristic function f_A (the notation 2^U stands for the set of all functions from U to a two-element set, e.g., to $\{\mathbf{1}, \mathbf{0}\}$).

It is clear that if $A \neq B$ then $f_A \neq f_B$. The first inequality means that there is an x such that either $x \in A \setminus B$ or $x \in B \setminus A$. In either case we will have that $f_A(x) \neq f_B(x)$. Thus $f_\_$ is injective.

On the other hand, every function $f \in 2^U$ is the characteristic function of some subset of U, namely, of the set $A_f = \{x \in U : f(x) = \mathbf{1}\}$. That is, $f_\_$ is surjective. Together, these two facts mean that we have a set-isomorphism $f_\_ : \wp(U) \rightleftharpoons 2^U$.

2: Relations

Definition 1.9 A *binary relation* R between sets S and T is a subset $R \subseteq S \times T$.
A *binary relation on a set* S is a subset of $S \times S$, and an n-ary relation on S is a subset of $S_1 \times S_2 \times ... \times S_n$, where each $S_i = S$.

Comment.
The definition 1.9 makes *any* subset of $S \times T$ a relation. The definition 1.3 of function, on the other hand, reuired this set to satisfy some additional properties. Thus, it is clear, that a function is a special case of relation, namely, a relation which relates each element of S with exactly one element of T.
Binary relations are sets of *ordered* pairs, i.e., $\langle s, t\rangle \neq \langle t, s\rangle$ – if $s \in S$ and $t \in T$, then the former belongs to $S \times T$ and the latter to $T \times S$, which are different sets. For sets, there is no ordering and thus $\{s, t\} = \{t, s\}$.
We often write the fact that s and t stand in a relation R, $\langle s, t\rangle \in R$, as sRt or as $R(s, t)$.

In general, relations may have arbitrary arities, for instance a subset $R \subseteq S \times T \times U$ is a ternary relation, etc. As a particular case, a *unary* relation on S is simply a subset $R \subseteq S$. In the following we are speaking only about binary relations (unless explicitly stated otherwise). □

Example 1.10
Functions, so to speak, map elements of one set onto the elements of another set (possibly the same). Relations *relate* some elements of one set with some elements of another. Recall the problem from example 1.4 with treating *children* as a function $M \to M$. This problem is overcome by treating *children* as a binary relation on the set M of all people. Thus $children(p, c)$ holds if an only if c is a child of p. Explicitly, this relation is $children = \{\langle p, c\rangle : p, c \in M$ and c is a child of $p\}$. □

Definition 1.11 Given two relations $R \subseteq S \times T$ and $P \subseteq T \times U$, their *composition* is the relation $R \circ P \subseteq S \times U$, defined as the set of pairs $\{\langle s, u\rangle \in S \times U : \text{there is a } t \in T \text{ with } R(s,t) \text{ and } P(t,u)\}$.

As functions are special cases of relations, we may also form the composition $g \circ f$ of functions $g : S \to T$ and $f : T \to U$. It is easy to see that $g \circ f$ will be a function from S to U. Note that $(g \circ f)(s)$ is equal to $f(g(s))$. (Some authors interpret $(g \circ f)(s)$ as $g(f(s))$.)

Definition 1.12 A relation $R \subseteq S \times S$ is :

connected	iff	for all pairs of distinct $s, t \in S : R(s,t)$ or $R(t,s)$		
reflexive	iff	for all $s \in S : R(s,s)$		
irreflexive	iff	for no $s \in S : R(s,s)$		
transitive	iff	whenever $R(s_1, s_2)$ and $R(s_2, s_3)$	then	$R(s_1, s_3)$
symmetric	iff	whenever $R(s,t)$	then	$R(t,s)$
asymmetric	iff	whenever $R(s,t)$	then	it is not the case that $R(t,s)$
antisymmetric	iff	whenever both $R(s,t)$ and $R(t,s)$	then	$s = t$
equivalence	iff	it is reflexive, transitive and symmetric.		

Numerous connections hold between these properties: every irreflexive, transitive relation is also asymmetric, and every asymmetric relation is also antisymmetric. Note also that just one relation is both connected, symmetric and reflexive, namely the universal relation $S \times S$ itself.

The most common (and smallest) example of equivalence is the *identity* relation $id_S = \{\langle s, s\rangle : s \in S\}$. The relation $\rightleftharpoons$ – existence of a set-isomorphism – is also an equivalence relation on any set (collection) of sets. An equivalence relation $\sim$ on a set S allows us to *partition* S into disjoint *equivalence classes* $[s] = \{s' \in S : s' \sim s\}$.

Given a relation $R \subseteq S \times S$, we can form its *closure* with respect to one or more of these properties. For example, the *reflexive closure* of R, written $\underline{R}$, is the relation $R \cup id_S$. (It may very well happen that R already is reflexive, $R = \underline{R}$, but then we do have that $\underline{R} = \underline{\underline{R}}$.) The *transitive closure* of R, written R^+, can be thought of as the infinite union

$$R \cup (R \circ R) \cup (R \circ R \circ R) \cup (R \circ R \circ R \circ R) \cup (R \circ R \circ R \circ R \circ R) \cup \ldots$$

This could also be defined as the least relation R^+ such that $R^+ = R \cup (R^+ \circ R)$.

3: Ordering Relations

Of particular importance are the *ordering* relations which we will use extensively in chapter 2 and later. Often we assume an implicit set S and talk only about relation R. However, it is important to realize that when we are talking about a relation R, we are actually considering a *set with structure*, namely a pair $\langle S, R\rangle$.

Definition 1.13 $\langle S, R\rangle$ is a *quasiorder* (or *preorder*), QO, iff R is
transitive : $R(x,y) \wedge R(y,z) \to R(x,z)$
reflexive : $R(x,x)$

Definition 1.14 $\langle S, R\rangle$ is a *weak partial order*, wPO, iff R is
a quasiorder : $R(x,y) \wedge R(y,z) \to R(x,z)$
: $R(x,x)$
antisymmetric : $R(x,y) \wedge R(y,x) \to x = y$

$\langle S, R\rangle$ is a *strict partial order*, sPO, iff R is
transitive : $R(x,y) \wedge R(y,z) \to R(x,z)$
irreflexive : $\neg R(x,x)$

A *total order*, TO, is a partial order which is connected : $x \neq y \to R(x,y) \vee R(y,x)$

Notation.
Obviously, given a wPO, we can trivially construct its strict version and vice versa. We will therefore

often say "partial order" without specifying which one we have in mind. Similarly, saying PO we will mean, ambiguously, one of the two. Making a wPO irreflexive will automatically turn it into an sPO, and vice versa.
Instead of writing $R(x, y)$ for a PO, we will use the infix notation $x \leq y$ for a wPO, and $x < y$ for the corresponding *sPO*. In other words, $x \leq y$ means $x < y$ or $x = y$, and $x < y$ means $x \leq y$ and $x \neq y$. □

A QO may allow loops, for instance the situations like $R(a_1, a_2)$, $R(a_2, a_3)$, $R(a_3, a_1)$ for distinct a_1, a_2, a_3. PO's forbid such situations: by applications of transitivity we have

- $R(a_2, a_1)$ as well as $R(a_1, a_2)$, which for wPO's imply $a_1 = a_2$.
- $R(a_1, a_1)$, which is impossible for sPO's.

Example 1.15
Consider the set of all people and their age.

1. The relation 'x is older than y' is an sPO on the set of all people : it is transitive, irreflexive (nobody is older than himself) and asymmetric: if 'x is older than y' then 'y is not older than x'.
2. The relation 'x is not younger than y' is a QO. It is not a wPO since it is not antisymmetric. (There are different people of the same age.)

The weak version of the relation in 1. is the relation 'x is older than y or x, y is the same person', which is clearly different from the relation in 2.
The relation in 1. is not a TO – of two *different* persons there may be none who is older than the other. □

Example 1.16
Given a set of symbols, for instance $\Sigma = \{a, b, c\}$, the set Σ^* contains all *finite* strings over Σ, e.g., a, aa, $abba$, $aaabbababab$, ... There are various natural ways of ordering Σ^*. Let $s, p \in \Sigma^*$

1. Define $s \prec_Q p$ iff $length(s) < length(p)$. This gives an sPO. The weak relation $s \preceq_Q p$ iff $length(s) \leq length(p)$ will be a QO but not a wPO since now any subset containing strings of equal length will form a loop.
2. Define $s \prec_P p$ iff s is a prefix of p. (Prefix is an initial segment.) We now obtain a wPO because any string is its own prefix and if both s is a prefix of p and p is a prefix of s the two must be the same string. This is not, however, a TO : neither of the strings a and bc is a prefix of the other.
3. Suppose that the set Σ is totally ordered, for instance, let Σ be the Latin alphabet with the standard ordering $a \prec b \prec c \prec d$.... We may then define the *lexicographic* TO on Σ^* as follows:
   $s \prec_L p$ iff either s is a prefix of p or else the two have a longest common prefix u (possibly empty) such that $s = uv$, $t = uw$ and $head(v) \prec head(w)$, where *head* is the first symbol of the argument string. This defines the usual ordering used, for instance, in dictionaries.

□

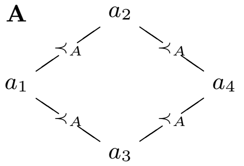
The following notions will not be used extensively, but it is often important to realize that the functions between ordered sets should consider not only the elements of the sets but also the relation between these elements.

Definition 1.17 Given two orderings (of any kind) $P = \langle S_1, R_1 \rangle$ and $Q = \langle S_2, R_2 \rangle$, a *homomorphism* $h : P \to Q$ is an *order preserving* function, i.e., a function $h : S_1 \to S_2$ such that $R_1(x, y)$ implies $R_2(h(x), h(y))$.
An *order-isomorphism* is a set-isomorphism $h : S_1 \rightleftharpoons S_2$ such that both h and h^{-1} are homomorphisms.

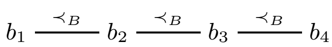
Thus, an order-isomorphism is a set-isomorphism which, in addition, preserves the structure of the isomorphic relations. One often encounters two ordered sets which are set-isomorphic but not order-isomorphic.

Example 1.18
Given two 4-element sets A and B, consider two sPO's $\mathbf{A} = \langle A, \prec_A \rangle$ and $\mathbf{B} = \langle B, \prec_B \rangle$ as shown below:

A



B



	$f(\_)$	$h_1(\_)$	$h_2(\_)$
a_1	b_2	b_1	b_2
a_2	b_1	b_2	b_3
a_3	b_4	b_3	b_3
a_4	b_3	b_4	b_4

Any injective $f : A \to B$ is also a bijection, i.e., $A \rightleftharpoons B$. However, a homomorphism $h : \mathbf{A} \to \mathbf{B}$ must also satisfy the additional condition, e.g., $a_1 \prec_A a_2$ requires that also $h(a_1) \prec_B h(a_2)$. Thus, for instance, f from the table is not a homomorphism $\mathbf{A} \to \mathbf{B}$ while h_1 and h_2 are.

Now, although the underlying sets A and B are isomorphic, there is no *order-isomorphism* between $\mathbf{A} = \langle A, \prec_A \rangle$ and $\mathbf{B} = \langle B, \prec_B \rangle$ because there is no *homomorphism* from the latter to the former. $\mathbf{B}$ is connected, i.e., a total order while $\mathbf{A}$ is not – any homomorphism would have to preserve the relation $\prec_B$ between arbitrary two elements of B, but in A there is no relation $\prec_A$ between a_2 and a_3. □

4: Infinities

◇———— a Background Story ————◇

Imagine a primitive shepherd who possesses no idea of number or counting – when releasing his sheep from the cottage in the morning he wants to find the means of figuring out if, when he collects them in the evening, all are back or, perhaps, some are missing.

He can, and most probably did, proceed as follows. Find a stick and let the sheep leave one by one. Each time a sheep passes through the gate, make a mark – something like / – on the stick. When all the sheep have left, there will be as many marks on the stick as there were sheep. On their return, do the same: let them go through the gate one by one. For each sheep, erase one mark – e.g., set a \ making one / into ×. When all the sheep are inside, check if there are any /-marks left. If no, i.e., there are only × on the stick, then everything is ok – as many sheep returned home as had left in the morning. If yes, then some sheep are missing.

Notice, that the shepherd still does not know "how many" sheep he has – he still does not have the idea of a number. But, perhaps a bit paradoxically, he has the idea of two equal numbers*! This idea is captured by the correspondance, in fact, several functions: the first is a morning-function m which for each sheep from the set S_M of all sheep, assigns a new / on the stick – all the marks obtained in the morning form a set M. The other, evening-function e, assigns to each returning sheep (from the set of returning sheep S_E) another mark \. Superimposing the evening marks \ onto the morning marks /, i.e., forming ×-marks, amounts to comparing the number of elements in the sets M and E by means of a function c assigning to each returning sheep marked by \, a morning sheep /.*

S_M	$\overset{m}{\leftrightarrow}$	M	$\overset{c}{\leftrightarrow}$	E	$\overset{e}{\leftrightarrow}$	S_E
	$\to$	/	×	\	$\leftarrow$	
	$\to$	/	×	\	$\leftarrow$	
	$\to$	/	×	\	$\leftarrow$	
	…					

In fact, this simple procedure may be considered as a basis of counting – comparing the number of elements in various sets. In order to assuring that two sets, like S_M and M, have equal number of we have to insist on some properties of the involved function m. Each sheep must be given a mark (m must be total) and for two distinct sheep we have to make two distinct marks (m must be injective). The third required property – that of surjectivity – follows automatically in the above procedure, since the target set M is formed only along as we mark the sheep. In short, the shepherd knows that there are as many *sheep* as *the morning marks on the stick because he has a bijective function between the respective sets. For the same reason, he knows that the sets of returning sheep and evening marks have the same number of elements and, finally, establishing a bijection between the sets M and E, he rests satisfied. (Violating a bit the profiles of the involved functions, we may say that the composite function $e \circ c \circ m : S_E \to E \to M \to S_M$ turns out to be bijective.)*

You can now easily imagine what is going on when the shepherd discovers that some sheep are missing in the evening. He is left with some /-marks which cannot be converted into $\times$-marks. The function $c : E \to M$ is injective but not surjective. This means that the set E has strictly fewer elements than the set M.

These ideas do not express immediately the concept of a number as we are used to it. (They can be used to do that.) But they do express our intuition about one number being equal to, smaller or greater than another number. What is, perhaps, most surprising is that they work equally well when the involved sets are infinite, thus allowing us to compare "the number of elements" in various infinite sets.

◇―――――――――――――――――――――――――――――――――――◇

In this section, we consider only sets and set functions, in particular, set-isomorphisms.

Definition 1.19 Two sets S and T have *equal cardinality* iff they are set-isomorphic $S \rightleftharpoons T$.
The *cardinality* of a set S, $|S|$, is the equivalence class $[S] = \{T : T \rightleftharpoons S\}$.

This is not an entirely precise definition of cardinality which, as a matter of fact, is the *number associated with* such an equivalence class. The point is that it denotes the intuitive idea of *the number of elements* in the set – all set-isomorphic sets have the same number of elements.

Definition 1.20 $|S| \leq |T|$ iff there exists an injective function $f : S \to T$.

It can be shown that this definition is consistent, i.e., that if $|S_1| = |S_2|$ and $|T_1| = |T_2|$ then there exists an injective function $f_1 : S_1 \to T_1$ iff there exists an injective function $f_2 : S_2 \to T_2$. A set S has cardinality stricly less than a set T, $|S| < |T|$, iff there exists an injective function $f : S \to T$ *but there exists no* such surjective function.

Example 1.21
$|\emptyset| = 0$, $|\{\emptyset\}| = 1$, $|\{\{\emptyset\}\}| = 1$, $|\{\emptyset, \{\emptyset\}\}| = 2$.
$|\{a, b, c\}| = |\{\bullet, \#, +\}| = |\{0, 1, 2\}| = 3$.
For finite sets, all operations from Definition 1.1 yield sets with possibly different cardinality:

$$\begin{array}{rrcl}
1. & |\{a,b\} \cup \{a,c,d\}| = |\{a,b,c,d\}| & |S \cup T| & \geq & |S| \\
2. & |\{a,b\} \cap \{a,c,d\}| = |\{a\}| & |S \cap T| & \leq & |S| \\
3. & |\{a,b\} \setminus \{a,c,d\}| = |\{b\}| & |S \setminus T| & \leq & |S| \\
4. & |\{a,b\} \times \{a,d\}| = |\{\langle a,a\rangle, \langle a,d\rangle, \langle b,a\rangle \langle b,d\rangle\}| & |S \times T| & = & |S| * |T| \\
5. & |\wp(\{a,b\})| = |\{\emptyset, \{a\}, \{b\}, \{a,b\}\}| & |\wp(S)| & > & |S|
\end{array}$$

□

From certain assumptions ("axioms") about sets it can be proven that the relation $\leq$ on cardinalities has the properties of a weak TO, i.e., it is reflexive (obvious), transitive (fairly obvious), antisymmetric (not so obvious) and total (less obvious). As an example of how intricate reasoning may be needed to establish such "not quite but almost obvious" facts, we show that $\leq$ is antisymmetric.

Theorem 1.22 [Schröder and Bernstein] For arbitrary sets X, Y, if there are injections $i : X \to Y$ and $j : Y \to X$, then there is a bijection $f : X \to Y$ (i.e., if $|X| \leq |Y|$ and $|Y| \leq |X|$ then $|X| = |Y|$).

Proof If the injection $i : X \to Y$ is surjective, i.e., $i(X) = Y$, then i is a bijection and we are done. Otherwise, we have $Y_0 = Y \setminus i(X) \neq \emptyset$ and we apply j and i repeatitively as follows

$$\begin{array}{ll}
Y_0 = Y \setminus i(X) & X_0 = j(Y_0) \\
Y_{n+1} = i(X_n) & X_{n+1} = j(Y_{n+1}) \\
Y^* = \bigcup_{n=0}^{\omega} Y_n & X^* = \bigcup_{n=0}^{\omega} X_n
\end{array}
\qquad \textit{i.e.} \qquad
\begin{tikzcd}
Y_0 \arrow[dr, "j"] & Y_1 \arrow[dr, "j"] & Y_2 \arrow[dr, "j"] & {} \arrow[dr, dotted, "j"] & \ldots \; Y^* \\
X \arrow[u, "i"] & X_0 \arrow[u, "i"] & X_1 \arrow[u, "i"] & X_2 \arrow[u, dotted, "i"] & \ldots \; X^*
\end{tikzcd}$$

Thus we can divide both sets into disjoint components as in the diagram below.

$$\begin{tikzcd} Y \arrow[d, shift right, "j"'] & = & Y^* \arrow[d, Leftrightarrow, "j"] & \cup & (Y \setminus Y^*) \arrow[d, Leftrightarrow, "i"'] \\ X \arrow[u, shift right, "i"'] & = & X^* & \cup & (X \setminus X^*) \end{tikzcd}$$

We show that the respective restrictions of j and i are bijections. First, $j : Y^* \to X^*$ is a bijection (it is injective, and the following equation shows that it is surjective):

$$j(Y^*) = j(\bigcup_{n=0}^{\omega} Y_n) = \bigcup_{n=0}^{\omega} j(Y_n) = \bigcup_{n=0}^{\omega} X_n = X^*$$

By lemma 1.7, $j^- : X^* \to Y^*$, defined by $j^-(x) = y : j(y) = x$ is a bijection too. Furthermore:

$$i(X^*) = i(\bigcup_{n=0}^{\omega} X_n) = \bigcup_{n=0}^{\omega} i(X_n) = \bigcup_{n=0}^{\omega} Y_{n+1} = \bigcup_{n=1}^{\omega} Y_n = Y^* \setminus Y_0. \tag{1.23}$$

Now, the first of the following equalities holds since i is injective, the second by (1.23) and since $i(X) = Y \setminus Y_0$ (definition of Y_0), and the last since $Y_0 \subseteq Y^*$:

$$i(X \setminus X^*) = i(X) \setminus i(X^*) = (Y \setminus Y_0) \setminus (Y^* \setminus Y_0) = Y \setminus Y^*,$$

i.e., $i : (X \setminus X^*) \to (Y \setminus Y^*)$ is a bijection. We obtain a bijection $f : X \to Y$ defind by

$$f(x) = \begin{cases} i(x) & if\ x \in X \setminus X^* \\ j^-(x) & if\ x \in X^* \end{cases}$$

QED (1.22)

A more abstract proof.
The construction of the sets X^* and Y^* in the above proof can be subsumed under a more abstract formulation implied by the Claims 1. and 2. below. In particular, Claim 1. has a very general form.

Claim 1. For any set X, if $h : \wp(X) \to \wp(X)$ is monotonic, i.e. such that, whenever $A \subseteq B \subseteq X$ then $h(A) \subseteq h(B)$; then there is a set $T \subseteq X : h(T) = T$.

We show that $T = \bigcup\{A \subseteq X : A \subseteq h(A)\}$.

a) $T \subseteq h(T)$: for for each $t \in T$ there is an $A : t \in A \subseteq T$ and $A \subseteq h(A)$. But then $A \subseteq T$ implies $h(A) \subseteq h(T)$, and so $t \in h(T)$.

b) $h(T) \subseteq T$: from a) $T \subseteq h(T)$, so $h(T) \subseteq h(h(T))$ which means that $h(T) \subseteq T$ by definition of T.

Claim 2. Given injections i, j define $\_^* : \wp(X) \to \wp(X)$ by $A^* = X \setminus j(Y \setminus i(A))$. If $A \subseteq B \subseteq X$ then $A^* \subseteq B^*$.
Follows trivially from injectivity of i and j. $A \subseteq B$, so $i(A) \subseteq i(B)$, so $Y \setminus i(A) \supseteq Y \setminus i(B)$, so $j(Y \setminus i(A)) \supseteq j(Y \setminus i(B))$, and hence $X \setminus j(Y \setminus i(A)) \subseteq X \setminus j(Y \setminus i(B))$.

3. Claims 1 and 2 imply that there is a $T \subseteq X$ such that $T = T^*$, i.e., $T = X \setminus j(Y \setminus i(T))$. Then $f : X \to Y$ defined by $f(x) = \begin{cases} i(x) & \text{if } x \in T \\ j^{-1}(x) & \text{if } x \notin T \end{cases}$ is a bijection. We have $X = j(Y \setminus i(T)) \cup T$ and $Y = (Y \setminus i(T)) \cup i(T)$, and obviously j^{-1} is a bijection between $j(Y \setminus i(T))$ and $Y \setminus i(T)$, while i is a bijection between T and $i(T)$. □

Each finite set has a cardinality which is a natural number. The apparently empty Definition 1.19 becomes more significant when we look at the infinite sets.

Definition 1.24 A set S is *infinite* iff there exists a proper subset $T \subset S$ such that $S \rightleftharpoons T$.

Example 1.25
For simplicity, let us consider the set of natural numbers, $\mathbf{N}$. We denote its cardinality $|\mathbf{N}| \stackrel{\text{def}}{=} \aleph_0$. (Sometimes it is also written ω, although axiomatic set theory usually distinguishes between the *cardinal*

number $\aleph_0$ and the *ordinal number* ω. Ordinal number is a more fine-grained notion than cardinal number, but we shall not worry about this here.) We have, for instance, that $|\mathbf{N}| = |\mathbf{N} \setminus \{0\}|$ by the simple bijection:

$$\begin{array}{cccccc} \{ & 0 & 1 & 2 & 3 & ... \\ & \updownarrow & \updownarrow & \updownarrow & \updownarrow & ... \\ \{ & 1 & 2 & 3 & 4 & ... \end{array}$$

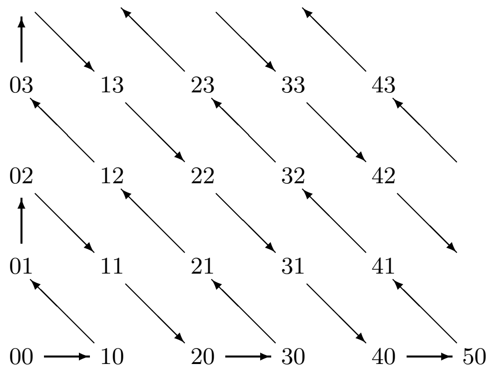
In fact, the cardinality of $\mathbf{N}$ is the same as the cardinality of the even natural numbers! It is easy to see that the pair of functions $f(n) = 2n$ and $f^{-1}(2n) = n$ is a bijection:

$$\begin{array}{ccccccccc} & \{ & 0 & 1 & 2 & 3 & 4 & 5 & ... \\ f\downarrow & & \updownarrow & \updownarrow & \updownarrow & \updownarrow & \updownarrow & \updownarrow & \uparrow f^{-1} \\ & \{ & 0 & 2 & 4 & 6 & 8 & 10 & ... \end{array}$$

In fact, when $|S| = |T| = \aleph_0$ and $|P| = n < \aleph_0$, we have

1. $|S \cup T| = \aleph_0$
3. $|S \setminus P| = \aleph_0$
4. $|S \times T| = \aleph_0$

We illustrate a possible set-isomorphisms $\mathbf{N} \rightleftharpoons \mathbf{N} \times \mathbf{N}$ below:



□

A set-isomorphism $S \rightleftharpoons \mathbf{N}$ amounts to an *enumeration* of the elements of S. Thus, if $|S| \leq \aleph_0$ we say that S is *enumerable* or *countable*; in case of equality, we say that it is countably infinite. Now, the question "are there any uncountable sets?" was answered by the founder of modern set theory, Georg Cantor

Theorem 1.26 For any set $A : |A| < |\wp(A)|$.

Proof The construction applied here shows that the contrary assumption – $A \rightleftharpoons \wp(A)$ – leads to a contradiction. Obviously,

$$(1.27) \qquad |A| \leq |\wp(A)|$$

since the inclusion defined by $f(a) = \{a\}$ is an injective function $f : A \to \wp(A)$.
So, assume that the equality holds in (1.27), i.e., that there is a corresponding $F : A \to \wp(A)$ which is both injective and surjective. Define the subset of A by $B \stackrel{\text{def}}{=} \{a \in A : a \notin F(a)\}$. Since $B \subseteq A$, so $B \in \wp(A)$ and, since F is surjective, there is a $b \in A$ such that $F(b) = B$. Is b in B or not? Each of the two possible answers yields a contradiction:

1. $b \in F(b)$ means $b \in \{a \in A : a \notin F(a)\}$, which means $b \notin F(b)$
2. $b \notin F(b)$ means $b \notin \{a \in A : a \notin F(a)\}$, which means $b \in F(b)$.

QED (1.26)

Corollary 1.28 For each cardinal number λ there is a cardinal number $\kappa > \lambda$.
In particular, $\aleph_0 = |\mathbf{N}| < |\wp(\mathbf{N})| < |\wp(\wp(\mathbf{N}))| < ...$

Theorem 1.26 proves that there exist uncountable sets, but are they of any interest? Another theorem of Cantor shows that such sets have been around in mathematics for quite a while.

Theorem 1.29 The set $\mathbf{R}$ of real numbers is uncountable.

Proof Since $\mathbf{N} \subset \mathbf{R}$, we know that $|\mathbf{N}| \leq |\mathbf{R}|$. The *diagonalisation* technique introduced here by Cantor, reduces the assumption that $|\mathbf{N}| = |\mathbf{R}|$ ad absurdum. If $\mathbf{R} \rightleftharpoons \mathbf{N}$ then, certainly, we can enumerate any subset of $\mathbf{R}$. Consider only the closed interval $[0,1] \subset \mathbf{R}$. If it is countable, we can list all its members, writing them in decimal expansion (each r_{ij} is a digit):

$$\begin{array}{rlllllll}
n_1 = & 0. & \mathbf{r_{11}} & r_{12} & r_{13} & r_{14} & r_{15} & r_{16} & \ldots. \\
n_2 = & 0. & r_{21} & \mathbf{r_{22}} & r_{23} & r_{24} & r_{25} & r_{26} & \ldots. \\
n_3 = & 0. & r_{31} & r_{32} & \mathbf{r_{33}} & r_{34} & r_{35} & r_{36} & \ldots. \\
n_4 = & 0. & r_{41} & r_{42} & r_{43} & \mathbf{r_{44}} & r_{45} & r_{46} & \ldots. \\
n_5 = & 0. & r_{51} & r_{52} & r_{53} & r_{54} & \mathbf{r_{55}} & r_{56} & \ldots. \\
n_6 = & 0. & r_{61} & r_{62} & r_{63} & r_{64} & r_{65} & \mathbf{r_{66}} & \ldots. \\
\vdots & & & & & & & &
\end{array}$$

Form a new real number r by replacing each r_{ii} (marked with **bold**) with another digit, for instance, let $r = 0.r_1r_2r_3r_4...$, where $r_i = \begin{cases} r_{ii}+1 & \text{if } r_{ii} < 9 \\ 0 & \text{if } r_{ii} = 9 \end{cases}$.
Then r cannot be any of the enumerated numbers $n_1, n_2, n_3, ...$ For each number n_i in this list has a digit r_{ii} at its i-th position which is different from the digit r_i at the i-th position in r. **QED** (1.29)

"Sets" which are not Sets

In Definition 1.1 we introduced several set building operations. The power set operation $\wp(\_)$ has proven particularly powerful. However, the most peculiar one is the *comprehension* operation, namely, the one allowing us to form a set of elements satisfying some property $\{x : \mathrm{Prop}(x)\}$. Although apparently very natural, its unrestricted use leads to severe problems.

Russell's Paradox
Define U as the set $\{x : x \notin x\}$. Now the question is: Is $U \in U$? Each possible answer leads to absurdity:

1. $U \in U$ means that U is one of x in U, i.e., $U \in \{x : x \notin x\}$, so $U \notin U$
2. $U \notin U$ means that $U \in \{x : x \notin x\}$, so $U \in U$.

□

The problem arises because in the definition of U we did not specify what kind of x's we are gathering. Among many solutions to this paradox, the most commonly accepted is to exclude such definitions by requiring that x's which are to satisfy a given property when collected into a new set must already belong to some other set. This is the formulation we used in Definition 1.1, where we said that if S is a set then $\{x \in S : \mathrm{Prop}(x)\}$ is a set too. The "definition" of $U = \{x : x \notin x\}$ does not conform to this format and hence is not considered a valid description of a set.

Exercises (week 1)

EXERCISE 1.1+ Given the following sets

$S1 = \{\{\emptyset\}, A, \{A\}\}$	$S6 = \emptyset$
$S2 = A$	$S7 = \{\emptyset\}$
$S3 = \{A\}$	$S8 = \{\{\emptyset\}\}$
$S4 = \{\{A\}\}$	$S9 = \{\emptyset, \{\emptyset\}\}$
$S5 = \{A, \{A\}\}$	

Of the sets S1-S9, which

- are members of S1 ?
- are subsets of S1 ?
- are members of S9 ?
- are subsets of S9 ?
- are members of S4 ?
- are subsets of S4 ?

EXERCISE 1.2+ Let $A = \{a, b, c\},\ B = \{c, d\},\ C = \{d, e, f\}$.

1. Write the sets: $A \cup B$, $A \cap B$, $A \cup (B \cap C)$
2. Is a a member of $\{A, B\}$, of $A \cup B$?
3. Write the sets $A \times B$ and $B \times A$.

EXERCISE 1.3 Using the set theoretic equalities (page 29), show that:

1. $A \cap (B \setminus A) = \emptyset$
2. $((A \cup C) \cap (B \cup C')) \subseteq (A \cup B)$

   (Show first some lemmas:

   - $A \cap B \subseteq A$
   - if $A \subseteq B$ then $A \subseteq B \cup C$
   - if $A_1 \subseteq X$ and $A_2 \subseteq X$ then $A_1 \cup A_2 \subseteq X$

   Expand then the expression $(A \cup C) \cap (B \cup C')$ to one of the form $X_1 \cup X_2 \cup X_3 \cup X_4$, show that each $X_i \subseteq A \cup B$ and use the last lemma.)

EXERCISE 1.4+ Let $S = \{0, 1, 2\}$ and $T = \{0, 1, \{0, 1\}\}$. Construct $\wp(S)$ and $\wp(T)$.

EXERCISE 1.5 Let $S = \{5, 10, 15, 20, 25, ...\}$ and $T = \{3, 4, 7, 8, 11, 12, 15, 16, 19, 20, ...\}$.

1. Specify each of these sets by defining the properties P_S and P_T such that $S = \{x \in \mathbf{N} : P_S(x)\}$ and $T = \{x \in \mathbf{N} : P_T(x)\}$
2. For each of these sets specify two other properties P_{S1}, P_{S2} and P_{T1}, P_{T2}, such that $S = \{x \in \mathbf{N} : P_{S1}(x)\} \cup \{x \in \mathbf{N} : P_{S2}(x)\}$ and similarly for T.

EXERCISE 1.6 Construct examples of injective (but not surjective) and surjective (but not injective) functions $S \to T$, which do not induce the inverse function in the way a bijection does (Lemma 1.7).

EXERCISE 1.7 Prove the claims cited below definition 1.12, that

1. Every sPO (irreflexive, transitive relation) is asymmetric.
2. Every asymmetric relation is antisymmetric.
3. If R is connected, symmetric and reflexive, then $R(s, t)$ for every pair s, t. What about a relation that is both connected, symmetric and transitive? In what way does this depend on the cardinality of S?

<u>EXERCISE 1.8</u>$^{+}$ Let C be a collection of sets. Show that equality $=$ and existence of set-isomorphism $\rightleftharpoons$ are equivalence relations on $C \times C$ as claimed under Definition 1.12. Give an example of two sets S and T such that $S \rightleftharpoons T$ but $S \neq T$ (they are set-isomorphic but not equal).

<u>EXERCISE 1.9</u>$^{+}$ If $|S| = n$ for some natural number n, what will be the cardinality of $\wp(S)$?

<u>EXERCISE 1.10</u>$^{+}$ Given an arbitrary (non-empty) collection of sets C. Show that

1. the inclusion relation $\subseteq$ is a wPO on C
2. $\subset$ is its strict version
3. $\subseteq$ is not (necessarily) a TO on C.

<u>EXERCISE 1.11</u> Let A be a countable set. Show that A has countably many *finite* subsets.

1. Show first that for any $n \in \mathbf{N}$, the set A^n of finite subsets of A with exactly n elements is countable.
2. Using a technique similar to the one from the drawing in example 1.25 on page 37, show that the union $\bigcup_{n \in \mathbf{N}} A^n$ of all these sets is countable.

Chapter 2

Induction

- Well-founded Orderings
  - General notion of Inductive proof
- Inductive Definitions
  - Structural Induction

1: Well-Founded Orderings

a Background Story

Ancients had many ideas about the basic structure and limits of the world. According to one of them our world – the earth – rested on a huge tortoise. The tortoise itself couldn't just be suspended in a vacuum – it stood on the backs of several elephants. The elephants stood all on a huge disk which, in turn, was perhaps resting on the backs of some camels. And camels? Well, the story obviously had to stop somewhere because, as we notice, one could produce new sub-levels of animals resting on other objects resting on yet other animals, resting on ... indefinitely. The idea is not well founded because such a hierarchy has no well defined begining, it hangs in a vacuum. Any attempt to provide the last, the most fundamental level is immediately met with the question "And what is beyond that?"

The same problem of the lacking foundation can be encoutered when one tries to think about the begining of time. When was it? Physicists may say that it was Big Bang. But then one immediately asks "OK, but what was before?". Some early opponents of the Biblical story of creation of the world – and thus, of time as well – asked "What did God do before *He created time?". St. Augustine, realising the need for a definite answer which, however, couldn't be given in the same spirit as the question, answered "He prepared the hell for those asking such questions."*

One should be wary here of the distinction between the begining and the end, or else, between moving backward and forward. For sure, we imagine that things, the world may continue to exist indefinitely in the future – this idea does not cause much trouble. But our intuition is uneasy with things which do not have any begining, with chains of events extending indefinitely backwards, whether it is a backward movement along the dimension of time or causality.

Such non well founded *chains are hard to imagine and even harder to do anything with – all our thinking, activity, constructions have to start from some begining. Having an idea of a begining, one will often be able to develop it into a description of the ensuing process. One will typically say: since the begining was so-and-so, such-and-such had to follow since it is implied by the properties of the begining. Then, the properties of this second stage, imply some more, and so on. But having nothing to start with, we are left without foundation to perform any intelligible acts.*

Mathematics has no problems with chains extending infinitely in both directions. Yet, it has a particular liking for chains which do have a begining, for orderings which are well-founded. As with our intuition and activity otherwise, the possibility of ordering a set in a way which identifies its least, first, starting elements, gives a mathematician a lot of powerful tools. We will study in this chapter some fundamental tools of this kind. As we will see later, almost all our presentation will be based on well-founded orderings.

Definition 2.1 Let $\langle S, \leq \rangle$ be a PO and $T \subseteq S$.

- $x \in T$ is a *minimal element* of T iff there is no element smaller than x, i.e., for no $y \in T : y < x$
- $\langle S, \leq \rangle$ is *well-founded* iff each non-empty $T \subseteq S$ has a minimal element.

The set of natural numbers with the standard ordering $\langle \mathbf{N}, \leq \rangle$ is well-founded, but the set of all integers with the natural extension of this ordering $\langle \mathbf{Z}, \leq \rangle$ is not – the subset of all negative integers does not have a $\leq$-minimal element. Intuitively, well-foundedness means that the ordering has a "basis", a set of minimal "starting points". This is captured by the following lemma.

Lemma 2.2 A PO $\langle S, \leq \rangle$ is well-founded iff there is no infinite decreasing sequence, i.e., no sequence $\{a_n\}_{n \in \mathbf{N}}$ of elements of S such that $a_n > a_{n+1}$.

Proof $\Leftarrow$) If $\langle S, \leq \rangle$ is not well-founded, then let $T \subseteq S$ be a subset without a minimal element. Let $a_1 \in T$ – since it is not minimal, we can find $a_2 \in T$ such that $a_1 > a_2$. Again, a_2 is not minimal, so we can find $a_3 \in T$ such that $a_2 > a_3$. Continuing this process we obtain an infinite descending sequence $a_1 > a_2 > a_3 > ....$

$\Rightarrow$) Suppose that there is such a sequence $a_1 > a_2 > a_3 > ....$ Then, obviously, the set $\{a_n : n \in \mathbf{N}\} \subseteq S$ has no minimal element.

QED (2.2)

Example 2.3
Consider again the orderings on finite strings as defined in example 1.16.

1. The relation $\prec_Q$ is a well-founded sPO; there is no way to construct an infinite sequence of strings with ever decreasing lengths!
2. The relation $\prec_P$ is a well-founded PO : any subset of strings will contain element(s) such that none of their prefixes (except the strings themselves) are in the set. For instance, a and bc are $\prec_P$-minimal elements in $S = \{ab, abc, a, bcaa, bca, bc\}$.
3. The relation $\prec_L$ is not well-founded, since there exist infinite descending sequences like

$$\ldots \prec_L \; aaaab \; \prec_L \; aaab \; \prec_L \; aab \; \prec_L \; ab \; \prec_L \; b.$$

   In order to construct any such descending sequence, however, there is a need to introduce ever longer strings as we proceed towards infinity. Hence the alternative ordering below is also of interest.
4. The relation $\prec_Q$ was defined in example 1.16. Now define $s \prec_{L'} p$ iff $s \prec_Q p$ or ($length(s) = length(p)$ and $s \prec_L p$). Hence sequences are ordered primarily by length, secondarily by the previous lexicographic order. The ordering $\prec_{L'}$ is indeed well-founded and, in addition, connected, i.e., a well-founded TO.

□

Definition 2.4 $\langle S, \leq \rangle$ is a well-ordering, WO, iff it is a TO and is well-founded.

Notice that well-founded ordering is *not* the same as well-ordering. The former can still be a PO which is not a TO. The requirement that a WO $= \langle S, \leq \rangle$ is a TO implies that each (sub)set of S has not only a minimal element but also a *unique* minimal element.

Example 2.5
The set of natural numbers with the "less than" relation, $\langle \mathbf{N}, < \rangle$, is an sPO. It is also a TO (one of two distinct natural numbers must be smaller than the other) and well-founded (any non-empty set of natural numbers contains a least element). □

Although sets like $\mathbf{N}$ or $\mathbf{Z}$ have the natural orderings, these are not the only possible orderings of these sets. In particular, for a given set S there may be several different ways of imposing a well-founded ordering on it.

Example 2.6
The set of integers, $\langle \mathbf{Z}, < \rangle$, is a TO but not well-founded – negative numbers have no minimal element.

That $<$ and $\leq$ fail to be WO on $\mathbf{Z}$ does not mean that $\mathbf{Z}$ cannot be made into a WO. One has to come up with another ordering. For instance, let $|x|$ for an $x \in \mathbf{Z}$ denote the absolute value of x (i.e., $|x| = x$ if

$x \geq 0$ and $|x| = -x$ if $x < 0$.) Say that $x \prec y$ if either $|x| < |y|$ or ($|x| = |y|$ and $x < y$). This means that we order $\mathbf{Z}$ as $0 \prec -1 \prec 1 \prec -2 \prec 2$.... This $\prec$ is clearly a WO on $\mathbf{Z}$.

Of course, there may be many different WO's on a given set. Another WO on $\mathbf{Z}$ could be obtained by swapping the positive and negative integers with the same absolute values, i.e., $0 \prec' 1 \prec' -1 \prec' 2 \prec' -2$....

□

1.1: Inductive Proofs on Well-founded Orderings

Well-founded orderings play a central role in many contexts because they allow one to apply a particularly convenient proof technique – proof by induction – which we now proceed to study.

◇ A Background Story ◇

Given some set S, a very typical problem is to show that all elements of S satisfy some property, call it P, i.e., to show that for all $x \in S : P(x)$. How one can try to prove such a fact depends on how the set S is described.

A special case is when S is finite and has only few elements – in this case, we can just start proving $P(x)$ for each x separately.

A more common situation is that S has infinitely many elements. Let $S = \{2i : i \in \mathbf{Z}\}$ and show that each $x \in S$ is an even number. Well, this is trivial by the way we have defined the set. Let x be an arbitrary element of S. Then, by definition of S, there is some $i \in \mathbf{Z}$ such that $x = 2i$. But this means precisely that x is an even number and, since x was assumed arbitrary, the claim holds for all $x \in S$.

Of course, in most situations, the relation between the definition of S and the property we want to prove isn't that simple. Then the question arises: "How to ensure that we check the property for all *elements of S and that we can do it in finite time (since otherwise we would never finish our proof)?" The idea of proof by induction answers this question in a particular way. It tells us that we have to find some well-founded ordering of the elements of S and then proceed in a prescribed fashion: one shows the statement for the minimal elements and then proceeds to greater elements in the ordering. The trick is that the strategy ensures that only finitely many steps of the proof are needed in order to conclude that the statement holds for* all *elements of S.*

The inductive proof strategy is not guaranteed to work in all cases and, particularly, it depends heavily on the choice of the ordering. It is, nevertheless, a very powerfull proof technique which will be of crucial importance for all the rest of the material we will study.

◇ ◇

The most general and abstract statement of the inductive proof strategy is as follows.

Theorem 2.7 Let $\langle S, \leq \rangle$ be a well-founded ordering and $T \subseteq S$.
Assume the following condition: for all $y \in S$: if (for all $x \in S : x < y \to x \in T$) then $y \in T$.
Then $T = S$.

Proof Assume that T satisfies the condition but $T \neq S$, i.e., $S \setminus T \neq \emptyset$. Since S is well-founded, $S \setminus T$ must have a minimal element y. Since y is minimal in $S \setminus T$, any $x < y$ must be in T. But then the condition implies $y \in T$. This is a contradiction – we cannot have both $y \in T$ and $y \in S \setminus T$ – showing that $T = S$. **QED** (2.7)

This theorem of *induction* is the basis for the following proof strategy for showing properties of sets on which some well-founded ordering has been defined.

Idea 2.8 **[Inductive proof]** Let $\langle S, \leq \rangle$ be well-founded and P be a predicate. Suppose we want to prove that each element $x \in S$ has the property P – that $P(x)$ holds for all $x \in S$. I.e., we want to prove that the sets $T = \{x \in S : P(x)\}$ and S are equal. Proceed as follows:

Induction :: Let x be an arbitrary element of S, and assume that for all $y < x : P(y)$ holds. Prove that this implies that also $P(x)$ holds.

Closure :: If you managed to show this, you may conclude $S = T$, i.e., $P(x)$ holds for all $x \in S$.

Observe that the hypothesis in the INDUCTION step, called the *induction hypothesis*, IH, allows us to assume $P(y)$ for all $y < x$. Since we are working with a well-founded ordering, there are some minimal elements x for which no such y exists. For these minimal x's, we then have no hypothesis and simply have to show that the claim $P(x)$ holds for them without any assumptions. This part of the proof is called the BASIS of induction.

Example 2.9
Consider the natural numbers greater than 1, i.e. the set $\mathbf{N}_2 = \{n \in \mathbf{N} : n \geq 2\}$. We want to prove the *prime number theorem*: for each $n \in \mathbf{N}_2 : P(n)$, where $P(n)$ stands for 'n is a product of prime numbers'. First we have to decide which well-founded ordering on $\mathbf{N}_2$ to use – the most obvious first choice is to try the natural ordering $<$, that is, we prove the statement on the well-founded ordering $\langle \mathbf{N}_2, < \rangle$:

BASIS :: Since 2 – the minimal element in $\mathbf{N}_2$ – is a prime number, we have $P(2)$.

INDUCTION :: So let $n > 2$ and assume IH: that $P(k)$ holds for every $k < n$. If n is prime, $P(n)$ holds trivially. So, finally, assume that n is a non-prime number greater than 2. Then $n = x * y$ for some $2 \leq x, y < n$. By IH, $P(x)$ and $P(y)$, i.e., x and y are products of primes. Hence, n is a product of primes.

CLOSURE :: So $P(n)$ for all $n \in \mathbf{N}_2$.

□

Example 2.10
For any number $x \neq 1$ and for any $n \in \mathbf{N}$, we want to show: $1 + x + x^2 + ... + x^n = \frac{x^{n+1}-1}{x-1}$. There are two different sets involved (of x's and of n's), so we first try the easiest way – we attempt induction on the well-founded ordering $\langle \mathbf{N}, < \rangle$, which is simply called "induction on n":

BASIS :: For $n = 0$, we have $1 = \frac{x-1}{x-1} = 1$.

INDUCTION :: Let $n' > 0$ be arbitrary, i.e., $n' = n + 1$. We expand the left hand side of the equality:

$$\begin{array}{rcl} 1 + x + x^2 + ... + x^n + x^{n+1} & = & (1 + x + x^2 + ... + x^n) + x^{n+1} \\ \text{(by IH since } n < n' = n+1) & = & \dfrac{x^{n+1} - 1}{x - 1} + x^{n+1} \\ & = & \dfrac{x^{n+1} - 1 + (x-1)x^{n+1}}{x - 1} = \dfrac{x^{n+1+1} - 1}{x - 1} \end{array}$$

Notice that here we have used much weaker IH – the hypothesis that the claim holds for $n = n' - 1$ (implied by IH) is sufficient to establish the induction step. CLOSURE yields the claim *for all* $n \in \mathbf{N}$. □

The proof rule from the idea 2.8 used in the above examples may be written more succinctly as

$$\frac{\forall x(\forall y(y < x \rightarrow P(y)) \rightarrow P(x))}{\forall x P(x)} \tag{2.11}$$

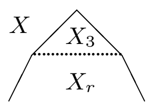
where "$\forall x$" is short for "for all $x \in \mathbf{N}_2$" (in 2.9), resp. "for all $x \in \mathbf{N}$" (in 2.10) and the horizontal line indicates that the sentence below can be inferred from the sentence above.

Example 2.12
A *convex n-gon* is a polygon with n sides and where each interior angle is less than 180°. A triangle is a convex 3-gon and, as you should know from the basic geometry, the sum of the interior angles of a triangle is 180°. Now, show by induction that the sum of interior angles of any convex n-gon is $(n-2)180°$.

The first question is: induction *on what*? Here it seems natural to try induction on n, i.e., on the number of sides. (That is, we consider a well-founded ordering on n-gons in which $X < Y$ iff X has fewer sides than Y.)

The basis case is: let X be an arbitrary triangle, i.e., 3-gon. We use the known result that the sum of interior angles of any triangle is indeed 180°.

For the induction step: let $n > 3$ be arbitrary number and X an arbitrary convex n-gon. Selecting two vertices with one common neighbour vertex between them, we can always divide X into a triangle X_3 and $(n-1)$-gon X_r, as indicated by the dotted line on the drawing below.



X_r has one side less than X so, by induction hypothesis, we have that the sum of its angles is $(n-3)180°$. Also by IH, the sum of angles in X_3 is $180°$. At the same time, the sum of the angles in the whole X is simply the sum of angles in X_3 and X_r. Thus it equals $(n-3)180° + 180° = (n-2)180°$ and the proof is complete. $\square$

The simplicity of the above examples is due to not only the fact that the problems are easy but also that the ordering to be used is very easy to identify. In general, however, there may be different orderings on a given set and then the first question about inductive proof concerns the choice of appropriate ordering.

Example 2.13

We want to prove that for all integers $z \in \mathbf{Z} : \begin{cases} 1+3+5+...+(2z-1) = z^2 & if\ z > 0 \\ (-1)+(-3)+(-5)+...+(2z+1) = -(z^2) & if\ z < 0 \end{cases}$.

We will show examples of two proofs using different orderings.

1. For the first, this looks like two different statements, so we may try to prove them separately for positive and negative integers. Let's do it:

Basis :: For $z = 1$, we have $1 = 1^2$.

Induction :: Let $z' > 1$ be arbitrary, i.e., $z' = z+1$ for some $z > 0$.

$$\begin{array}{rcl} 1+3+...+(2z'-1) & = & 1+3+...+(2z-1)+(2(z+1)-1) \\ \text{(by IH since } z < z' = z+1) & = & z^2+2z+1 \ = \ (z+1)^2 \ = \ (z')^2 \end{array}$$

The proof for $z < 0$ is entirely analogous, but now we have to reverse the ordering: we start with $z = -1$ and proceed along the negative integers only considering $z \prec z'$ iff $|z| < |z'|$, where $|z|$ denotes the absolute value of z (i.e., $|z| = -z$ for $z < 0$). Thus, for $z, z' < 0$, we have actually that $z \prec z'$ iff $z > z'$.

Basis :: For $z = -1$, we have $-1 = -(-1)^2$.

Induction :: Let $z' < -1$ be arbitrary, i.e., $z' = z-1$ for some $z < 0$.

$$\begin{array}{rcl} -1-3+...+(2z'+1) & = & -1-3+...+(2z+1)+(2(z-1)+1) \\ \text{(by IH since } z \prec z') & = & -|z|^2-2|z|-1 \\ & = & -(|z|^2+2|z|+1) \ = \ -(|z|+1)^2 \ = \ -(z-1)^2 \ = \ -(z')^2 \end{array}$$

The second part of the proof makes it clear that the well-founded ordering on the whole $\mathbf{Z}$ we have been using was not the usual $<$. We have, in a sense, ordered both segments of positive and negative numbers independently in the following way (the arrow $x \rightarrow y$ indicates the ordering $x \prec y$):

$$1 \longrightarrow 2 \longrightarrow 3 \longrightarrow 4 \longrightarrow 5 \longrightarrow \cdots$$

$$-1 \longrightarrow -2 \longrightarrow -3 \longrightarrow -4 \longrightarrow -5 \longrightarrow \cdots$$

The upper part coincides with the typically used ordering $<$ but the lower one was the matter of more specific choice.

Notice that the above ordering is different from another, natural one, which orders two integers $z \prec' z'$ iff $|z| < |z'|$. This ordering (shown below) makes, for instance, $3 \prec' -4$ and $-4 \prec' 5$. The ordering above did not relate any pair of positive and negative intergers with each other.

$$\begin{tikzcd} 1 \arrow[r] \arrow[dr] & 2 \arrow[r] \arrow[dr] & 3 \arrow[r] \arrow[dr] & 4 \arrow[r] \arrow[dr] & 5 \arrow[r] \arrow[dr] & \cdots \\ -1 \arrow[r] \arrow[ur] & -2 \arrow[r] \arrow[ur] & -3 \arrow[r] \arrow[ur] & -4 \arrow[r] \arrow[ur] & -5 \arrow[r] \arrow[ur] & \cdots \end{tikzcd}$$

2. Looking again at the problem, we can see that it can be stated a bit differently. We have to show that for all $z \in \mathbf{Z} : \begin{cases} 1+3+5+...+(2z-1) = z^2 & if\ z > 0 \\ -(1+3+5+...+(2|z|-1)) = -(z^2) & if\ z < 0 \end{cases}$.

Thus formulated, it becomes obvious that we only have one statement to prove: we show the first claim (in the same way as we did it in point 1.) and then apply trivial arithmetics to conclude from $x = y$ that also $-x = -y$.

This, indeed, is a smarter way to prove the claim. Is it induction? Yes it is. We prove it first for all positive integers. Then, we take an arbitrary negative integer z and observe (assume induction hypothesis!)

that we have already proved $1 + 3 + ... + (2|z| - 1) = |z|^2$. The well-founded ordering on $\mathbf{Z}$ we are using in this case orders first all positive integers along $<$ (for proving the first part of the claim) and then, for any $z < 0$, puts z after $|z|$ but unrelated to other $n > |z| > 0$ – the induction hypothesis for proving the claim for such a $z < 0$ is, namely, that the claim holds for $|z|$. The ordering is shown on the left:

$$\begin{tikzcd} 1 \arrow[r]\arrow[d] & 2 \arrow[r]\arrow[d] & 3 \arrow[r]\arrow[d] & 4 \arrow[r]\arrow[d] & 5 \arrow[r]\arrow[d] & \cdots \\ -1 & -2 & -3 & -4 & -5 & \cdots \end{tikzcd}$$

$$\begin{tikzcd} & & & & & & -1 \\ & & & & & & -2 \\ 1 \arrow[r] & 2 \arrow[r] & 3 \arrow[r] & 4 \arrow[r] & 5 \arrow[r] & \cdots \arrow[ur]\arrow[uur]\arrow[r]\arrow[dr]\arrow[ddr] & -3 \\ & & & & & & -4 \\ & & & & & & \cdots \end{tikzcd}$$

As a matter of fact, the structure of this proof allows us to view the used ordering in yet another way. We first prove the claim for *all* positive integers. Thus, when proving it for an arbitrary negative integer $z < 0$, we can assume the stronger statement than the one we are actually using, i.e., that the claim holds for *all* positive integers. This ordering puts all negative integers after all positive ones as shown on the right in the figure above.

Notice that *none* of the orderings we encountered in this example was total. □

2: Inductive Definitions

We have introduced the *general* idea of inductive proof over an *arbitrary* well-founded ordering defined on an arbitrary set. The idea of induction – a kind of stepwise construction of the whole from a "basis" by repetitive applications of given rules – can be applied not only for constructing proofs but also for constructing, that is defining, sets. We now illustrate this technique of *definition by induction* and then (subsection 2.3) proceed to show how it gives rise to the possibility of using a special case of the inductive proof strategy on sets defined in this way.

◇——— A Background Story ———◇

Suppose I make a simple statement, for instance, (1) 'John is a nice person'. Its truth may be debatable – some people may think that, on the contrary, he is not nice at all. Pointing this out, they might say – "No, he is not, you only think that he is". So, to make my statemet less definite I might instead say (2) 'I think that 'John is a nice person''. In the philosophical tradition one would say that (2) expresses a reflection over (1) – it expresses the act of reflecting over the first statement. But now, (2) is a new statement, and so I can reflect over it again: (3) 'I think that 'I think that 'John is nice'''. It isn't perhaps obvious why I should make this kind of statement, but I certainly can make it and, with some effort, perhaps even attach some meaning to it. Then, I can just continue: (4) 'I think that (3)', (5) 'I think that (4)', etc. The further (or higher) we go, the less idea we have what one might possibly intend with such expressions. Philosophers used to spend time analysing their possible meaning – the possible meaning of such repetitive acts of reflection over reflection over reflection ... over something. In general, they agree that such an infinite regress does not yield anything intuitively meaningful and should be avoided.

In terms of the normal language usage, we hardly ever attempt to carry such a process beyond the level (2) – the statements at the higher levels do not make any meaningful contribution to a conversation. Yet they are possible for purely linguistic reasons – each statement obtained in this way is grammatically correct. And what is 'this way'? Simply:

Basis :: Start with some statement, e.g., (1) 'John is nice'.

Step :: Whenever you have produced some statement (n) – at first, it is just (1), but after a few steps, you have some higher statement (n) – you may produce a new statement by prepending (n) with 'I think that ...'. Thus you obtain a new, (n+1), statement 'I think that (n)'.

Anything you obtain according to this rule, happens to be grammatically correct and the whole infinite chain of such statements consitutes what philosophers call an infinite regress.

The crucial point here is that we do not start with some set which we analyse, for instance, by looking for some ordering on it. We are defining a new set *– the set of statements* $\{(1), (2), (3), ...\}$ *– in a very particular way. We are applying the idea of induction – stepwise construction from a "basis" – not for proving properties of a given set with some well-founded ordering but for defining a new set.*

◇————————————————————————————————————◇

One may often encounter sets described by means of abbreviations like $E = \{0, 2, 4, 6, 8, ...\}$ or $T = \{1, 4, 7, 10, 13, 16, ...\}$. The abbreviation ... indicates that the author assumes that you have figured out what the subsequent elements will be – and that there will be infinitely many of them. It is assumed that you have figured out *the rule* by which to generate all the elements. The same sets may be defined more precisely with the explicit reference to the respective rule:

(2.14) $$E = \{2 * n : n \in \mathbf{N}\} \text{ and } T = \{3 * n + 1 : n \in \mathbf{N}\}$$

Another way to describe these two rules is as follows. The set E is defined by:

Basis :: $0 \in E$ and,
Step :: whenever an $x \in E$, then also $x + 2 \in E$.
Closure :: Nothing else belongs to E.

The other set is defined similarly:

Basis :: $1 \in T$ and,
Step :: whenever an $x \in T$, then also $x + 3 \in T$.
Closure :: Nothing else belongs to T.

Here we are not so much defining the whole set by one static formula (as we did in (2.14)), as we are specifying the rules for *generating new* elements from some elements which we have already included in the set. Not all formulae (static rules, as those used in (2.14)) allow equivalent formulation in terms of such generation rules. Yet, quite many sets of interest can be defined by means of such generation rules – quite many sets can be introduced by means of *inductive definitions*. Inductively defined sets will play a central role in all the subsequent chapters.

Idea 2.15 [Inductive definition of a set] An *inductive definition* of a set S consists of

Basis :: List some (at least one) elements $B \subseteq S$.
Induction :: Give one or more rules to construct new elements of S from already existing elements.
Closure :: State that S consists exactly of the elements obtained by the basis and induction steps. (This is typically assumed rather than stated explicitly.)

Example 2.16
The finite strings Σ^* over an alphabet Σ from Example 1.16, can be defined inductively, staring with the empty string, ϵ, i.e., the string of length 0, as follows:

Basis :: $\epsilon \in \Sigma^*$
Induction :: if $s \in \Sigma^*$ then $xs \in \Sigma^*$ for all $x \in \Sigma$

Constructors are the empty string ϵ and the operations prepending an element in front of a string $x\_$, for all $x \in \Sigma$. Notice that 1-element strings like x will be here represented as $x\epsilon$. □

Example 2.17
The finite non-empty strings Σ^+ over alphabet Σ are defined by starting with a different basis.

Basis :: $x \in \Sigma^+$ for all $x \in \Sigma$
Induction :: if $s \in \Sigma^+$ then $xs \in \Sigma^+$ for all $x \in \Sigma$

□

Often, one is not interested in all possible strings over a given alphabet but only in some subsets. Such subsets are called *languages* and, typically, are defined by induction.

Example 2.18
Define the set of strings $\mathbf{N}$ over $\Sigma = \{0, s\}$:

BASIS :: $0 \in \mathbf{N}$
INDUCTION :: If $n \in \mathbf{N}$ then $sn \in \mathbf{N}$

This language is the basis of the formal definition of natural numbers. The constructors are 0 and the operation of appending the symbol 's' to the left. (The 's' signifies the "successor" function corresponding to $n+1$.) Notice that we do not obtain the set $\{0, 1, 2, 3...\}$ but $\{0, s0, ss0, sss0...\}$, which is a kind of unary representation of natural numbers. Notice that, for instance, the strings $00s, s0s0 \notin \mathbf{N}$, i.e., $\mathbf{N} \neq \Sigma^*$. □

Example 2.19

1. Let $\Sigma = \{a, b\}$ and let us define the language $L \subseteq \Sigma^*$ consisting only of the strings starting with a number of a's followed by the equal number of b's, i.e., $\{a^n b^n : n \in \mathbf{N}\}$.

   BASIS :: $\epsilon \in L$
   INDUCTION :: if $s \in L$ then $asb \in L$

   Constructors of L are ϵ and the operation adding an a in the beginning and a b at the end of a string $s \in L$.
2. Here is a more complicated language over $\Sigma = \{a, b, c, (,), \neg, \rightarrow\}$ with two rules of generation.

   BASIS :: $a, b, c \in L$
   INDUCTION :: if $s \in L$ then $\neg s \in L$
   if $s, r \in L$ then $(s \rightarrow r) \in L$

   By the closure property, we can see that, for instance, '(' $\notin L$ and $(\neg b) \notin L$.

□

In the examples from section 1 we saw that a given set may be *endowed* with various well-founded orderings. Having succeded in this, we can than use a powerful technique of proof by induction according to theorem 2.7. The usefulness of inductive *definitions* is related to the fact that such an ordering may be obtained for free – the resulting set obtains implicitly a well-founded ordering induced by the very definition as follows.[1]

Idea 2.20 [Induced wf Order] For an inductively defined set S, define a function $f : S \rightarrow \mathbf{N}$ as follows:

BASIS :: Let $S_0 = B$ and for all $b \in S_0 : f(b) \stackrel{\text{def}}{=} 0$.
INDUCTION :: Given S_i, let S_{i+1} be the union of S_i and all the elements $x \in S \setminus S_i$ which can be obtained according to one of the rules from some elements $y_1, \ldots, y_n$ of S_i. For each such new $x \in S_{i+1} \setminus S_i$, let $f(x) \stackrel{\text{def}}{=} i + 1$.
CLOSURE :: The actual ordering is then $x \prec y$ iff $f(x) < f(y)$.

The function f is essentially counting the minimal number of steps – consecutive applications of the rules allowed by the induction step of Definition 2.15 – needed to obtain a given element of the inductive set.

Example 2.21
Refer to Example 2.16. Since the induction step amounts there to increasing the length of a string by 1, following the above idea, we would obtain the ordering on strings $s \prec p$ iff $length(s) < length(p)$. □

[1] In fact, an inductive definition imposes at least two such orderings of interest, but here we consider just one.

2.1: "1-1" Definitions

A common feature of the above examples of inductively defined sets is the impossibility of deriving an element in more than one way. For instance, according to example 2.17 the only way to derive the string abc is to start with a and then add b and c to the right in sequence. One apparently tiny modification to the example changes this state of affairs:

Example 2.22
The finite non-empty strings over alphabet Σ can also be defined inductively as follows.

Basis :: $x \in \Sigma^+$ for all $x \in \Sigma$

Induction :: if $s \in \Sigma^+$ and $p \in \Sigma^+$ then $sp \in \Sigma^+$

□

According to this example, abc can be derived by concatenating either a and bc, or ab and c. We often say that the former definitions are 1-1, while the latter is not. Given a 1-1 inductive definition of a set S, there is an easy way to define new functions on S – again by induction.

Idea 2.23 [Inductive function definition] Suppose S is defined inductively from basis B and a certain set of construction rules. To define a function f on elements of S do the following:

Basis :: Identify the value $f(x)$ for each x in B.

Induction :: For each way an $x \in S$ can be constructed from one or more $y_1, \ldots, y_n \in S$, show how to obtain $f(x)$ from the values $f(y_1), \ldots, f(y_n)$.

Closure :: If you managed to do this, then the closure property of S guarantees that f is defined for all elements of S.

The next few examples illustrate this method.

Example 2.24
We define the *length* function on finite strings by induction on the definition in example 2.16 as follows:

Basis :: $length(\epsilon) = 0$

Induction :: $length(xs) = length(s) + 1$

□

Example 2.25
In Example 2.16 strings were defined by a left append (prepend) operation which we wrote as juxtaposition xs. A corresponding right append operation can be now defined inductively.

Basis :: $\epsilon \vdash y = y\epsilon$

Induction :: $xs \vdash y = x(s \vdash y)$

and the operation of reversing a string:

Basis :: $\epsilon^R = \epsilon$

Induction :: $(xs)^R = s^R \vdash x$

□

The right append operation $\vdash$ does not quite fit the format of idea 2.23 since it takes two arguments – a symbol as well as a string. It is possible to give a more general version that covers such cases as well, but we shall not do so here. The definition below also apparently goes beyond the format of idea 2.23, but in order to make it fit we merely have to think of addition, for instance in $m+n$, as an application of the one-argument function *add* n to the argument m.

Example 2.26
Using the definition of $\mathbf{N}$ from Example 2.18, we can define the plus operation for all $n, m \in \mathbf{N}$:

Basis :: $0 + n = n$

Induction :: $s(m) + n = s(m + n)$

It is not immediate that this is the usual plus - we cannot see, for example, that $n+m = m+n$. We shall see in an exercise that this is actually the case.
We can use this definition to calculate the sum of two arbitrary natural numbers represented as elements of $\mathbf{N}$. For instance, $2+3$ would be processed as follows:

$$ss0 + sss0 \mapsto s(s0 + sss0) \mapsto ss(0 + sss0) \mapsto ss(sss0) = sssss0 \qquad \Box$$

Note carefully that the method of inductive function definition 2.23 is guaranteed to work only when the set is given by a 1-1 definition. Imagine that we tried to define a version of the length function in example 2.24 by induction on the definition in example 2.22 as follows: $len(x) = 1$ for $x \in \Sigma$, while $len(ps) = len(p) + 1$. This would provide us with alternative (and hence mutually contradictive) values for $len(abc)$, depending on which way we choose to derive abc. Note also that the two equations $len(x) = 1$ and $len(ps) = len(p) + len(s)$ provide a working definition, but in this case it takes some reasoning to check that this is indeed the case.

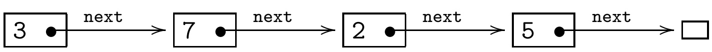
2.2: Inductive Definitions and Recursive Programming

If you are not familiar with the basics of programming you may skip this subsection and go directly to subsection 2.3. Here we do not introduce any new concepts but merely illustrate the relation between the two areas from the title.

All basic structures known from computer science are defined inductively – any instance of a `List`, `Stack`, `Tree`, etc., is generated in finitely many steps by applying some basic constructor operations. These operations themselves may vary from one programming language to another, or from one application to another, but they always capture the inductive structure of these data types. We give here but two simple examples which illustrate the inductive nature of two basic data structures and show how this leads to the elegant technique of recursive programming.

1. Lists
A `List` (to simplify matters, we assume that we store only integeres as data elements) is a sequence of 0 or more integers. The idea of a 'sequence' or, more generally, of a linked structure is captured by pointers between objects storing data. Thus, one would define objects of the form given on the left – the list $3, 7, 2, 5$ would then contain 4 `List` objects (plus additional `null` object at the end) and look as shown on the right:

```
List
  int x;
  List next;
```



The declaration of the `List` objects tells us that a `List` is:

1. either a `null` object (which is a default, always possible value for ponters)
2. or an integer (stored in the current `List` object) followed by another `List` object.

But this is exactly an inductive definition, namely, the one from example 2.17, the only difference being that of the language used.

1a. From inductive definition to recursion
This is also a 1-1 definition and thus gives rise to natural recursive programming over lists. The idea of recursive programming is to traverse a structure in the order opposite to the way we imagine it built along its inductive definition. We start at some point of the structure and proceed to its subparts until we reach the basis case. For instance, the function computing length of a list is programmed recursively to the left:

```
int length(List L)
  IF (L is null) return 0;
  ELSE return (1 + length(L.next));
```

```
int sum(List L)
  IF (L is null) return 0;
  ELSE return (L.x + sum(L.next));
```

It should be easy to see that the pseudo-code on the left is nothing more than the inductive definition of the function from example 2.24. Instead of the mathematical formulation used there, it uses the operational language of programming to specify:

1. the value of the function in the basis case (which also terminates the recursion) and then
2. the way to compute the value in the non-basis case from the value for some subcase which brings recursion “closer to” the basis.

The same schema is applied in the function to the right which computes the sum of all integers in the list.

1b. Equality of Lists

Inductive 1-1 definition of a set (here of the set of `List` objects given by their declaration) gives also rise to the obvious recursive function for comparing objects for equality. Two lists are equal iff

i) they have the same structure (i.e., the same number of elements) and

ii) respective elements in both lists are equal

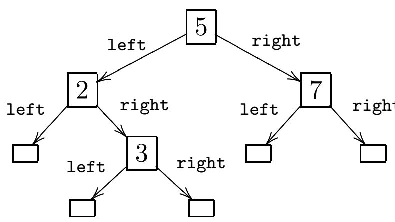
The corresponding pseudo-code for recursive function definition is as follows. The first two lines check point i) and ensure termination upon reaching the basis case. The third line checks point ii). If everything is ok so far, the recursion proceeds to check the rest of the lists:

```
boolean equal(List L, R)
  IF (L is null AND R is null) return TRUE;
  ELSE IF (L is null OR R is null) return FALSE;
  ELSE IF (L.x ≠ R.x) return FALSE;
  ELSE return equal(L.next, R.next);
```

2. Trees

Another very common data structure is binary tree `BT`. (Again, we simplify presentation by assuming that we only store integers as data.) Unlike in a list, each node (except the `null` ones) has two successors (called “children”) left and right:

```
BT
  int x;
  BT left;
  BT right;
```



The inductive definition says that a binary tree `BT` is

1. either a `null` object
2. or an integer (stored in the current `BT` object) with two pointers (`left` and `right`) to other (always distinct) `BT` objects.

2a. From inductive definition to recursion

To compute the sum of integers stored in a given tree, we have to compute the sums stored in its left and right subtrees and add to the them the value stored at the current node itself. The recursive function reflecting the inductive definition is as follows:

```
int sum(BT T)
  IF (T is null) return 0;
  ELSE (sum(T.left) + T.x + sum(T.right));
```

Again, the first line detects the basis case, while the second one computes the sum in the non-basic case by descending recursively down the tree structure.

2b. Equality of Binary Trees

Using the *operational* intuition of inductive generation might suggest that the definition of binary tree is not 1-1. To generate the tree from the example drawing, we might first generate its left subtree and then the right one, or else other way around. The sequence of steps leading to the construction of the whole tree would not be unique.

However, this operational intuition, relaying on the *temporal ordering* of construction steps is not what matters for a definition to be 1-1. There is *only one logical* way to obtain this tree: we must have *both* its left *and* its right subtree, and *only then* we can make this tree. That is, there are *unique* elements (left and right subtree, and the integer to be stored in the root node itself) and the *unique* rule to be applied (put left subtree to the left, right to the right, and the integer in the node). The definition is 1-1.

Consequently, equality of binary trees follows naturally: two trees are equal iff

i) they have the same structure and

ii) respective elements stored at respective nodes in both trees are equal

Having the same structure amounts here to the following condition: trees $T1$ and $T2$ have the same structure iff:

- both are `null` or
- $T1 = (L1, x1, R1)$, $T2 = (L2, x2, R2)$, i.e., neither is `null`, and *both* $L1, L2$ have the same structure *and* $R1, R2$ have the same structure.

This is clearly an inductive definition of 'having the same structure', and we thus obtain the recursive pseudo-code for checking equality of two binary trees:

```
boolean equal(BT T1,T2)
  IF (T1 is null AND T2 is null) return TRUE;
  ELSE IF (T1 is null OR T2 is null) return FALSE;
  ELSE IF (T1.x ≠ T2.x) return FALSE;
  ELSE return ( equal(T1.left, T2.left) AND equal(T1.right,T2.right) );
```

We now end this programming excursion and return to the proof strategy arising from inductive definitions of sets which will be of crucial importance in later chapters.

2.3: Proofs by Structural Induction

Since, according to Idea 2.20, an inductive definition of a set induces a well-founded ordering, it allows us to perform inductive proofs of the properties of this set. This is called proof by *structural induction* – the word "structural" indicating that the proof, so to speak, reflects or proceeds along the structure of the set imposed by its inductive definition. In contrast to the definitions of functions on inductive sets 2.23, this proof strategy works for all inductively defined sets, regardless of whether the definitions are 1-1.

Proof by structural induction is just a special case of the inductive proof Idea 2.8. Simply, because any inductive definition of a set induces a well-founded ordering on this set according to the Idea 2.20. Using this ordering leads to the following proof strategy:

Idea 2.27 [Proof by Structural Induction] Suppose S is defined inductively from basis B and a certain set of construction rules. Suppose we want to prove that each element $x \in S$ has the property P – that $P(x)$ holds for all $x \in S$. Proceed as follows:

Basis :: Show that $P(x)$ holds for all $x \in B$.

Induction :: For each way an $x \in S$ can be constructed from one or more $y_1, \ldots, y_n \in S$, show that the induction hypothesis : $P(y_1), \ldots, P(y_n)$ implies $P(x)$.

Closure :: If you managed to show this, then the closure property of S allows you to conclude that $P(x)$ holds for all $x \in S$.

It is straightforward to infer the proof rule in idea 2.27 from the one in idea 2.8. We assume that 2.8 holds. Then, assuming Basis and Induction step of 2.27, we merely need to prove the Induction step in idea 2.8. So let x be an arbitrary member of S and assume the IH that $P(y)$ holds for all $y \prec x$. There are two possible cases: Either $f(x) = 0$, in which case $x \in S_0 = B$, and $P(x)$ follows from the Basis part of idea 2.27. Otherwise $x \in S_{i+1} \setminus S_i$ for some $i \in \mathbf{N}$. Then x can be obtained from some $y_1, \ldots, y_n \in S_i$. Since these are all less than x in the sense of $\prec$, by the IH $P(y_1)$ and ... and $P(y_n)$. But then $P(x)$ follows from the Induction part of idea 2.27, and the argument is complete.

The great advantage of inductively defined sets is that, in order to prove their properties, one need not to inquire into the details of the induced well-founded ordering but merely has to follow the steps of the definition (as described in idea 2.27).

Example 2.28

The set of natural numbers was defined inductively in example 2.18. The induced well-founded ordering will say that $s^n 0 \prec s^m 0$ iff $n < m$. Thus, writing the natural numbers in the usual way $0, 1, 2, 3, \ldots$, and replacing sn by $n+1$, the induced ordering is the standard ordering $<$ – the structural induction on this set will be the usual mathematical induction. That is:

Basis :: Show that $P(0)$ holds.

Induction :: Assuming the induction hypothesis $P(n)$, show that it implies also $P(n+1)$.

It is the most common form of induction used in mathematics. As a matter of fact, the proof in example 2.10 used precisely this form of induction, what was observed there as a "weaker induction hypothesis" (than the one allowed by the general formulation from idea 2.8).

Using structural induction, we show that for all $n \in \mathbf{N} : 1 + 2 + ... + n + (n+1) = \dfrac{(n+1)(n+2)}{2}$.

Basis :: $n = 0 : (0+1) = 1 = \dfrac{(0+1)(0+2)}{2}$

Induction :: Assume the identity $1 + 2 + ... + n + (n+1) = \dfrac{(n+1)(n+2)}{2}$.

Then $1 + 2 + ... + (n+1) + (n+2) = \dfrac{(n+1)(n+2)}{2} + (n+2) = \dfrac{(n+2)(n+3)}{2}$. □

The proof rule for natural numbers used above can be written more succinctly as follows.

$$\frac{P(0)\ \&\ \forall x(P(x) \to P(x+1))}{\forall x P(x)} \tag{2.29}$$

Note that this rule can be sometimes more cumbersome to use than the rule (2.11). To see this, try to use it to prove the prime number theorem which was shown in example 2.9 using the general induction schema for natural numbers (i.e., the rule (2.11)). The difference between the two concerns, actually, only the "easiness" of carrying out the proof – as you are asked to show in exercise 2.8, the two proof rules have the same power.

Example 2.30

Define the set U inductively:

Basis :: $\emptyset \in U$

Induction :: if $S \in U$ then $\wp(S) \in U$.

and show that for all $S \in U : S \notin S$. What is the ordering $\prec$ induced on the set U by this definition? Well, $\emptyset$ is the least element and then, for any set S we have that $S < \wp(S)$. $\prec$ is the transitive closure of this relation $<$. The nice thing about structural induction is that one actually need not have a full insight into the structure of the induced ordering but merely has to follow the inductive definition of the set.

Basis :: Since, for all $X : X \notin \emptyset$ so, in particular, $\emptyset \notin \emptyset$.

Induction :: Assume IH : $S \notin S$. Contrapositively, assume that $\wp(S) \in \wp(S)$. This means that $\wp(S) \subseteq S$. On the other hand, $S \in \wp(S)$. But since $X \subseteq Y$ iff for all $x : x \in X \Rightarrow x \in Y$, we thus obtain that $S \in \wp(S)\ \&\ \wp(S) \subseteq S \Rightarrow S \in S$, contradiciting IH. □

Example 2.31
Show that the set L defined in Example 2.19.1 is actually the set $T = \{a^n b^n : n \in \mathbf{N}\}$.
1. We show first the inclusion $L \subseteq T$ by structural induction on L.

BASIS :: $\epsilon = a^0 b^0$.

INDUCTION :: Assume that $s \in L$ satisfies the property, i.e., $s = a^n b^n$ for some $n \in \mathbf{N}$. The string produced from s by the rule will then be $asb = aa^n b^n b = a^{n+1} b^{n+1}$. Hence all the strings of L have the required form and $L \subseteq \{a^n b^n : n \in \mathbf{N}\}$.

Notice again that we did not ask about the precise nature of the induced ordering but merely followed the steps of the inductive definition of L in carrying out this proof. (The induced ordering $\prec$ on L is given by: $a^n b^n \prec a^m b^m$ iff $n < m$.)

2. On the other hand, any element of $\{a^n b^n : n \in \mathbf{N}\}$ can be generated in n steps according to the L's construction rule. This is shown by induction on n, that is, on the natural ordering $\langle \mathbf{N}, < \rangle$:

BASIS :: For $n = 0$, we have $a^0 b^0 = \epsilon \in L$.

INDUNCTION :: If IH : $a^n b^n \in L$, then $aa^n b^n b = a^{n+1} b^{n+1} \in L$ by the induction step of definition of L.

Hence $\{a^n b^n : n \in \mathbf{N}\} \subseteq L$. □

Example 2.32
Recall the language L defined in Example 2.19.2. Define the subset S of L :

BASIS :: $B = \{a, b, \neg c, (a \to (b \to c)), (c \to b)\} \subset S$

INDUCTION :: if $s \in S$ and $(s \to t) \in S$ then $t \in S$
if $\neg t \in S$ and $(s \to t) \in S$ then $\neg s \in S$

We show that $S = B \cup \{(b \to c), \neg b, c\}$ constructing S step by step:

$S_0 =$ $B = \{a, b, \neg c, (a \to (b \to c)), (c \to b)\}$

$S_1 =$ $S_0 \cup \{(b \to c)\}$, taking a for s and $(b \to c)$ for t and applying the first rule
$= \{a, b, \neg c, (a \to (b \to c)), (c \to b), (b \to c)\}$

$S_2 =$ $S_1 \cup \{\neg b, c\}$ taking b for s and c for t and applying both rules
$= \{a, b, \neg c, (a \to (b \to c)), (c \to b), (b \to c), \neg b, c\}$

$S =$ Every application of a rule to some new combination of strings now yields a string which is already in S_2. Since no new strings can be produced, the process stops here and we obtain $S = S_2$.

□

We will encounter many examples of inductive proofs in the rest of the course. In fact, the most important sets we will consider will be defined inductively and most proofs of their properties will use structural induction.

3: Transfinite Induction

As a final example, we give an inductive definition of an important set of ordinals (called also "ordinal numbers" though, as a matter of fact, they are sets), and show inductively some properties of this set. The example shows that induction is by no means restricted to finitely generated elements. It can be carried over to sets of arbitrary cardinality. Although the principle is the same as before, emphasising the context, one calls it "transfinite induction".

Example 2.33
Define inductively the collection of ordinals $\mathbf{O}$:

BASIS :: $\varnothing \in \mathbf{O}$

INDUCTION :: 1) if $x \in \mathbf{O}$ then $x^+ = x \cup \{x\} \in \mathbf{O}$ – "successor" of an ordinal is an ordinal
2) if $x_i \in \mathbf{O}$ then $\bigcup x_i \in \mathbf{O}$ – arbitrary (possibly infinite) union of ordinals is an ordinal

We show a few simple facts about $\mathbf{O}$ using structural induction.

A) For all $x \in \mathbf{O} : y \in x \Rightarrow y \subset x$.

BASIS :: there is no $y \in \varnothing$ (nor any $y \subset \varnothing$, i.e., no $y \subseteq \varnothing$ and $y \neq \varnothing$), so this follows trivially.

Ind :: 1) From IH : $y \in x \Rightarrow y \subset x$ show that $y \in x^+ \Rightarrow y \subset x^+$. $y \in x^+$ means that either a) $y \in x$, from which, by IH, we get $y \subset x$ and thus $y \subset x \cup \{x\}$, or b) $y = x$, and then $y \subseteq x$ but $y \neq x \cup \{x\}$, i.e., $y \subset x \cup \{x\}$.
2) IH : for all $x_i : y \in x_i \Rightarrow y \subset x_i$. If $y \in \bigcup x_i$, then there is some $k : y \in x_k$ and, by IH, $y \subset x_k$. But then $y \subset \bigcup x_i$.

B) For all $x \in \mathbf{O} : y \in x \Rightarrow y \in \mathbf{O}$ (each element of an ordinal is itself an ordinal)

Basis :: Since there is no $y \in \emptyset$, this follows trivially.

Ind :: Let $x \in \mathbf{O}$ and 1) assume IH : $y \in x \Rightarrow y \in \mathbf{O}$. If $y \in x \cup \{x\}$ then either $y \in x$ and by IH $y \in \mathbf{O}$, or else $y = x$ but $x \in \mathbf{O}$.
2) IH : for all $x_i : y \in x_i \Rightarrow y \in \mathbf{O}$. If $y \in \bigcup x_i$, then there is some x_k for which $y \in x_k$. Then, by IH, $y \in \mathbf{O}$.

Notice that the second rule in the definition of **O** enables one to construct elements of **O** without any immediate predecessor! In the above proofs, the case 1) was treated by a simple induction assuming the claim about the immediate predecessor. The case 2), however, required the stronger version assuming the claim for all ordinals x_i involved in forming the new ordinal by union. In fact, this step amounts to transfinite induction – what we have proven holds for the set **O** whose small, initial segment is shown below. ω is the first such *limit* ordinal (with no immediate predecessor), $\omega + \omega = 2\omega$ the second, etc.

$$\overbrace{\overbrace{\emptyset \quad \{\emptyset\} \quad \{\emptyset,\{\emptyset\}\} \quad \{\emptyset,\{\emptyset\},\{\emptyset,\{\emptyset\}\}\}}^{\omega} \quad \dots \quad \omega \quad \{\omega,\{\omega\}\} \quad \{\omega,\{\omega\},\{\omega,\{\omega\}\}\} \quad \dots}^{\omega+\omega} \quad 2\omega \quad \{2\omega,\{2\omega\}\} \quad \dots$$

Typically, one uses a more familiar notation :

$$0 \quad 1 \quad 2 \quad 3 \quad \dots \quad \omega \quad \omega+1 \quad \omega+2 \quad \dots \quad 2\omega \quad 2\omega+1 \quad \dots$$

and the sequence of ordinals is continued indefinitely:

$$\begin{array}{l} 0,1,2,3,4,5,\dots\omega,\omega+1,\omega+2,\dots\omega+\omega = \\ \quad 2\omega,2\omega+1,2\omega+2,\dots 3\omega,3\omega+1,\dots 4\omega,4\omega+1,\dots\omega*\omega = \\ \quad\quad \omega^2,\omega^2+1,\dots\omega^3,\omega^3+1,\dots\omega^4,\omega^4+1,\dots \\ \quad\quad\quad \omega^\omega,\omega^\omega+1,\dots\omega^{2\omega},\dots\omega^{3\omega},\dots\omega^{\omega*\omega},\dots\omega^{(\omega^3)},\dots\omega^{(\omega^\omega)},\dots \\ \quad\quad\quad\quad\quad\quad\quad\quad \dots \end{array}$$

Ordinals play the central role in set theory, providing the paradigm for well-orderings (total well-founded orderings). Notice that this means that we may have several ordinals of the same cardinality (the concept of ordinal number includes ordering, that of a cardinal number does not). For instance, the ordinals ω, $\omega + 1$ and $1 + \omega$, can be easily seen to have the same cardinality:

$$\begin{array}{rl} \omega = & \quad 0 < 1 < 2 < 3 < 4 < 5 < \dots \\ \omega + 1 = & \quad 0 < 1 < 2 < 3 < 4 < 5 < \dots < \omega \\ 1 + \omega = & \bullet < 0 < 1 < 2 < 3 < 4 < 5 < \dots \end{array}$$

The functions $f : \omega + 1 \to \omega$ defined by $f(\omega) = \bullet$ and $f(n) = n$ and $g : 1 + \omega \to \omega$ defined by $g(\bullet) = 0$ and $g(n) = n + 1$ are obviously bijections, i.e., set-isomorphisms. g is, in addition order-isomorphism, since it satisfies for all elements $x, y \in 1 + \omega : x < y \Rightarrow g(x) < g(y)$. This means that these two ordinals represent essentially the same ordering. However, f does not preserve the ordering, since it maps the greatest element ω of the ordering $\omega + 1$ onto the smallest element $\bullet$ of the ordering $1 + \omega$. These two ordinals, although of the same cardinality ω, represent different ways of ordering all ω elements. The first makes first an infinite sequence and then adds a maximal element at the end of it. The second makes an infinite sequence and adds a new minimal element in front of it. Thus the former does possess a maximal element while the latter does not. □

Exercises (week 2)

EXERCISE 2.1 Given the following inductively defined set $S \subset \mathbf{N} \times \mathbf{N}$:

BASIS :: $\langle 0, 0 \rangle \in S$
INDUCTION :: If $\langle n, m \rangle \in S$ then $\langle s(n), m \rangle \in S$ and $\langle s(n), s(m) \rangle \in S$

Determine the property P which allows you to describe the set S as a set of the form $\{\langle n, m \rangle : P(n, m)\}$.
Describe those elements of S which can be derived in more than one way.

EXERCISE 2.2$^+$ Let $\Sigma = \{a, b, c\}$, $\Gamma = \{\neg, \rightarrow, (,)\}$ and define the language WFF^Σ over $\Sigma \cup \Gamma$ inductively as follows:

BASIS :: If $A \in \Sigma$ then $A \in \mathsf{WFF}^\Sigma$
INDUCTION :: If $A, B \in \mathsf{WFF}^\Sigma$ then $\neg A \in \mathsf{WFF}^\Sigma$ and $(A \rightarrow B) \in \mathsf{WFF}^\Sigma$.

1. Which of the following strings belong to WFF^Σ :
   $a \rightarrow (b \rightarrow c),\ (a \rightarrow \neg b) \rightarrow c,\ a \rightarrow b \rightarrow c,\ \neg(a \rightarrow b),\ (\neg a \rightarrow b),\ \neg a \rightarrow b$?
2. Replace Σ with $\Delta = \{*, \#\}$ and use the analogous definition of WFF^Δ. Which strings are in WFF^Δ :
   $*\#,\ \neg *,\ \neg(\#\#),\ (* \rightarrow \#),\ * \rightarrow \#,\ * \leftarrow \#$?

EXERCISE 2.3 Describe the ordering induced on the Σ^+ of example 2.22 by the definitions of idea 2.20.

EXERCISE 2.4$^+$ Use induction on $\mathbf{N}$ to prove the following equations for all $1 \leq n \in \mathbf{N}$

1. $1 + 2 + ... + n = \dfrac{n(n+1)}{2}$
2. $(1 + 2 + ... + n)^2 = 1^3 + 2^3 + ... + n^3$
   (In the induction step expand the expression $((1 + 2 + ... + n) + (n + 1))^2$ and use 1.)

EXERCISE 2.5$^+$ Use induction to prove that a finite set with n elements has 2^n subsets (cf. exercise 1.9).

EXERCISE 2.6 Using the definition of strings Σ^* from example 2.16 as a schema for structural induction, show that the reverse operation from example 2.25 is idempotent, i.e., $(s^R)^R = s$. (Show first, by structural induction on s, the lemma: for all $y \in \Sigma, s \in \Sigma^* : (y \dashv s)^R = s^R y$.)

EXERCISE 2.7 Show that the operation $+$ on $\mathbf{N}$, defined in example 2.26, is commutative, i.e., that the identity $n + m = m + n$ holds for all $n, m \in \mathbf{N}$. This requires a *nested* induction, i.e.,

- the basis: for all $m \in \mathbf{N}$, $0 + m = m + 0$, and
- the induction: for all $m \in \mathbf{N}$, $s(n) + m = m + s(n)$, given that for all $m \in \mathbf{N}$, $n + m = m + n$

can themselves be proved only by the use of induction (on m).

EXERCISE 2.8 We have seen two different proof rules for induction on natural numbers – one (2.11) in example 2.9 and another (2.29) in example 2.28. Show that each can be derived from the other. Begin by stating clearly what exactly you are asked to prove!
(One part of this proof follows trivially from the general argument after Idea 2.27.)