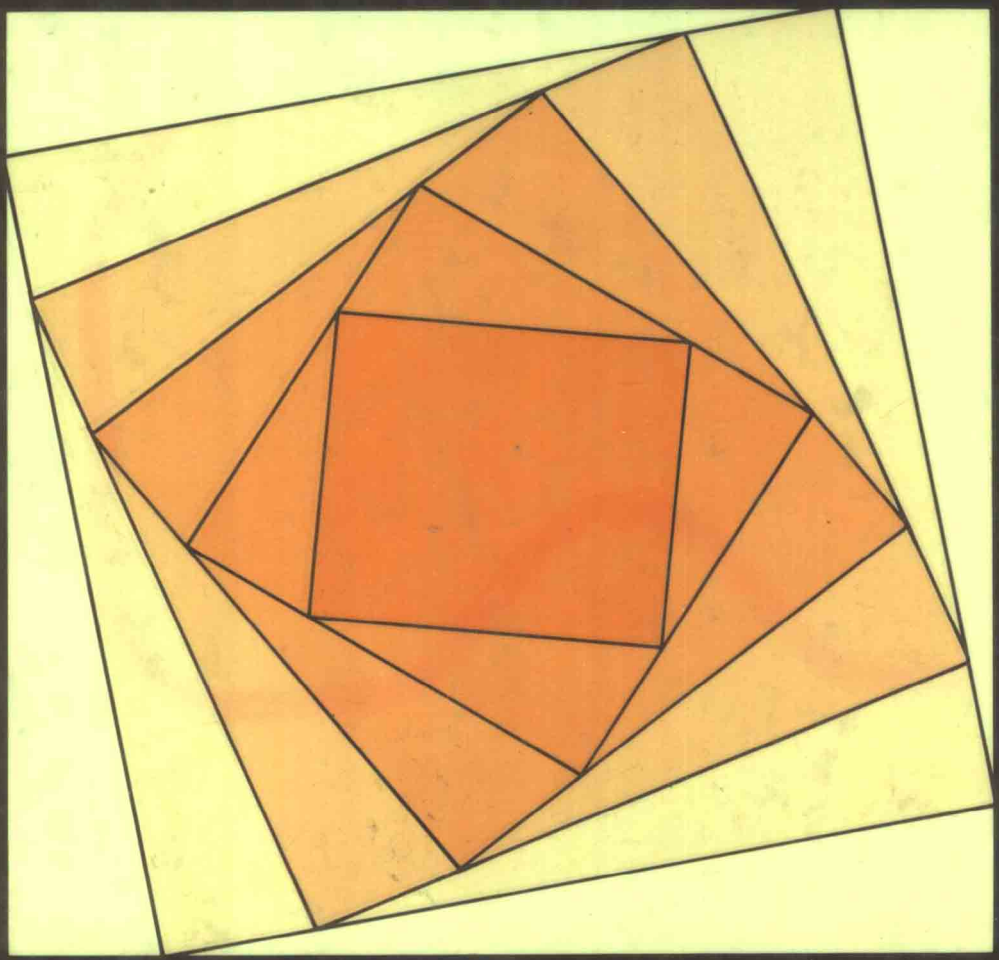
ELEMENTS OF THE THEORY OF COMPUTATION



Harry R. Lewis · Christos H. Papadimitriou

ELEMENTS OF THE THEORY OF COMPUTATION

Harry R. Lewis
Harvard University

Christos H. Papadimitriou
Massachusetts Institute of Technology

PRENTICE HALL, Englewood Cliffs, New Jersey 07632

PREFACE

This book is an introduction, on the undergraduate level, to the classical and contemporary theory of computation. The topics covered are, in a few words, the theory of automata and formal languages, computability by Turing machines and recursive functions, uncomputability, computational complexity, and mathematical logic. The treatment is mathematical but the viewpoint is that of computer science; thus the chapter on context-free languages includes a discussion of parsing, and the chapters on logic establish the soundness and completeness of resolution theorem-proving.

In the undergraduate curriculum, exposure to this subject tends to come late, if at all, and collaterally with courses on the design and analysis of algorithms. It is our view that computer science students should be exposed to this material earlier—as sophomores or juniors—both because of the deeper insights it yields on specific topics in computer science, and because it serves to establish essential mathematical paradigms. But we have found teaching a rigorous undergraduate course on the subject a difficult undertaking because of the mathematical maturity assumed by the more advanced textbooks. Our goal in writing this book has been to make the essentials of the subject accessible to a broad undergraduate audience in a way that is mathematically sound but presupposes no special mathematical experience.

The whole book represents about a year's worth of coursework. We have each taught a one-term course covering much of the material in Chapters 1 through 6, omitting on various occasions and in various combinations the sections on parsing, on recursive functions, and on particular unsolvable decision problems. Other selections are also possible; for example, a course

emphasizing computability and the foundations of mechanical logic might skip quickly over Chapters 1 through 3 and concentrate on Chapters 4, 6, 8, and 9. However it is used, our fervent hope is that the book will contribute to the intellectual development of the next generation of computer scientists by introducing them at an early stage of their education to crisp and methodical thinking about computational problems.

We take this opportunity to thank all from whom we have learned, both teachers and students. Specific thanks go to Larry Denenberg and Aaron Temin for their proofreading of early drafts, and to Michael Kahl and Oded Shmueli for their assistance and advice as teaching assistants. In the spring of 1980 Albert Meyer taught a course at M.I.T. from a draft of this book, and we thank him warmly for his criticisms and corrections. Of course, the blame for any remaining errors rests with us alone. Renate D'Arcangelo typed and illustrated the manuscript with her characteristic but extraordinary perfectionism and rapidity.

CONTENTS

CHAPTER 1

SETS, RELATIONS, AND LANGUAGES

1.1 "IF-THEN" AND ITS RELATIVES

Mathematics deals with true and false statements and the relations between statements. Of course, these statements are *about* objects of one kind or another, and we shall shortly take up the subject matter of the particular branch of mathematics we are studying. But first some remarks are in order about mathematical statements in general.

In mathematics, we often use the English language in ways more precise than those of everyday discourse. Some odd statements may result, but if all the terminology is clearly understood and taken literally, each statement can be seen, without ambiguity, to be either true or false. For example, Sentence (1) should cause no controversy.

The word *watermelon* has more *e*'s than *o*'s. (1)

Neither should Sentence (2).

The word *watermelon* has at least as many *e*'s as *o*'s. (2)

This is patently true, although a bit peculiar in light of the previous statement. It is hard to imagine why one would want to say (2) when one could as easily say (1). That, however, does not affect the *truthfulness* of (2). What about the following sentence?

The word *watermelon* has at least as many *x*'s as *y*'s. (3)

This is another true statement, since zero is at least as big as zero; never mind that one would not ordinarily say such a thing.

The conjunctions *and* and *or* play an important and precise role in the formation of statements. They combine two statements to make a third, which is true or false depending on the truthfulness or falsity of the pieces. In the case of *and*, the compound statement is true if both component statements are true; otherwise the compound statement is false. For example,

the word *watermelon* has more *e*'s than *o*'s and
the word *blueberry* has two consecutive *r*'s (4)

is true since (1) and

the word *blueberry* has two consecutive *r*'s (5)

are both true. In the case of *or*, the compound statement is true if either component statement is true. Thus

the word *blueberry* has two consecutive *r*'s or
the word *peach* is six letters long (6)

is true because (5) is true, in spite of the fact that

the word *peach* is six letters long (7)

is false. Also,

the word *blueberry* has two consecutive *r*'s or
the word *watermelon* has at least as many *e*'s as *o*'s (8)

is true; a combination of statements with the connective *or* is true if one or the other or both of the combined statements is true and false only if both of the statements being combined are false.

Another phrase commonly used as a conjunction is *if . . . then. . . .* In everyday discourse this phrase has overtones of explanation or causality. Such concepts are alien to mathematics, however; we must have a clearer criterion for the truth of an if-then statement. The rule could not be simpler: an if-then statement is true if the first part is false or if the second part is true. By way of shorthand, let us write p and q for the two statements involved. Then *if p then q* can be divided into two cases.

Case 1. Statement p is true. Then in order for the compound statement to be true, q must be true as well.

Case 2. Statement p is false. Then the compound statement is automatically true, regardless of whether q is true.

For example,

if the word *watermelon* has more *e*'s than *o*'s,
then the word *blueberry* has two consecutive *r*'s

is true, since Case 1 applies and q is true. The statement

if the word *blueberry* has two consecutive *r*'s,
then the word *peach* is six letters long

is false, since Case 1 applies and q is false. Finally, *any* statement of the form

if the word *peach* is six letters long, then q

is true, regardless of whether q is true or false, since Case 2 applies. In all situations, to show that *if p then q* is true, there is no need to look for a "meaningful" connection between p and q; one merely verifies that they are related by Case 1 or by Case 2.

Mathematics rarely deals with statements about particular objects, such as the words *watermelon* and *blueberry*. Instead, it tends to deal with general statements about classes of objects. To deal with such generalities, we introduce symbols to stand for the objects being discussed, in the way we have used p and q to stand for statements. For example, suppose x stands for any word. Then the statement

$$\text{if } x \text{ has more } e\text{'s than } o\text{'s, then } x \text{ has at least one } e \tag{9}$$

is true. Arguing very carefully, we would break this statement into two cases. If x does not have more e's than o's, then Case 2 applies and Statement (9) is true. On the other hand, if x does have more e's than o's, then Case 1 applies, and to prove that (9) is true, we must show that x has at least one e. Now x cannot have fewer than zero o's, and since it has more e's than o's, it must have at least as many e's as the next number bigger than zero, that is, at least one e. Thus (9) is true.

When the *if* part of an if-then statement can under no circumstances be true, the compound statement is said to be true **vacuously**. For example, let x be any word, l_1 and l_2 any letters, and n_1 and n_2 any numbers, and consider the statement

$$\begin{aligned}&\text{if } x \text{ has } n_1 \ l_1\text{'s, } n_2 \ l_2\text{'s, and } n_1 < n_2,\\ &\text{then } x \text{ has at least } n_1 + n_2 \text{ letters in all.}\end{aligned} \tag{10}$$

As before, we need consider only the case in which the *if* part is true. But now we must deal with two subcases. If l_1 and l_2 are the same letter, then (10) is vacuously true, since then x cannot have fewer l_1's than l_2's. If l_1 and l_2 are different letters, then x has $n_1 + n_2$ letters which are either l_1's or l_2's, and therefore at least $n_1 + n_2$ letters in all.

Let us go back to Cases 1 and 2 for the truth of an if-then statement. Another way to interpret these cases is to state that *if p then q* is true if it is impossible for p to be true and q to be false simultaneously. One can therefore try to establish a sentence of the form *if p then q* by **contradiction**, that is, by assuming q to be false and p to be true and showing that an inconsistency results. We illustrate this principle by a numerical example. Suppose that x is any number. We might argue as follows to show

$$\text{if } x^2 = 0, \text{ then } x = 0.$$

Suppose that $x^2 = 0$, but $x \neq 0$. Then either $x > 0$ or $x < 0$. But if $x > 0$, then $x^2 > 0$, and if $x < 0$, then $x^2 > 0$. In either case, $x^2 > 0$. This contradicts the assumption that $x^2 = 0$.

In writing mathematics, the phrase

$$p \text{ only if } q$$

means exactly the same thing as

$$\text{if } p, \text{ then } q.$$

Again, we use a numerical example. Let x and y be integers. Then

$$x + y \text{ is odd only if one of } x, y \text{ is odd} \tag{11}$$

means the same thing as

$$\text{if } x + y \text{ is odd, then one of } x, y \text{ is odd}$$

and is a true statement. On the other hand,

$$q \text{ if } p$$

means exactly the same thing as

$$\text{if } p, \text{ then } q.$$

Another way of rephrasing (11) is

$$x \text{ or } y \text{ is odd if } x + y \text{ is odd.}$$

Often *p only if q* (that is, *if p then q*) and *p if q* (that is, *if q then p*) are combined into

$$p \text{ if and only if } q.$$

In order for this statement to be true, p and q must either both be true or both be false. To put it another way, *p if and only if q* means that p and q are true under exactly the same circumstances. To establish that an if-and-only-if statement is true, we usually break it into its two parts and establish each separately. For example, consider

$$x + y \text{ is odd if and only if exactly one† of } x \text{ and } y \text{ is odd.}$$

This can be written in two parts.

(a) If exactly one of x and y is odd, then $x + y$ is odd.

(b) If $x + y$ is odd, then exactly one of x and y is odd.

To establish (a) we may simply write x and y as $2m$ and $2n + 1$ (not necessarily in that order) and note that $2m + 2n + 1$ is odd. To establish (b), it is easiest to argue by contradiction; that is, to assume that $x + y$ is odd but either both or neither of x and y is odd. A contradiction follows immediately.

†*Exactly one* means *one, and not more than one.*

The statement *if q then p* is called the **converse** of the statement *if p then q*. Obviously, the converses of some true statements are true, and the converses of other true statements are false. To argue *p if and only if q*, we may first show *if p then q*, and then show **conversely**, as we shall say, *if q then p*.

1.2 SETS

Mathematics deals with statements about objects. Objects of various kinds have special properties of their own: numbers are even or odd, words are made up of letters, and so on. But some general properties of objects and collections of objects do not depend on what kinds of objects they are; these properties depend only on objects being the same or different from each other, and being grouped together in various ways. The ideas that objects are parts of groups, and that those groups can combine and overlap, have been found to be basic and powerful in many branches of mathematics.

A **set** is a collection of objects. For example, the collection of the four letters a, b, c, and d is a set, which we may name L; we write $L = \{a, b, c, d\}$. The objects comprising a set are called its **elements** or **members**. For example, b is an element of the set L; in symbols, $b \in L$. Sometimes we simply say that b is **in** L, or that L **contains** b. On the other hand, z is not an element of L, and we write $z \notin L$.

In a set we do not distinguish repetitions of the elements. Thus {red, blue, red} is the same set as {red, blue}. Similarly, the order of the elements is immaterial; for example, {3, 1, 9}, {9, 3, 1}, and {1, 3, 9} are the same set. To summarize: *Two sets are equal* (that is, the same) *if and only if they have the same elements.*

The elements of a set need not be related in any way; for example, {3, red, {d, blue}} is a set with three elements, one of which is itself a set. A set may have only one element; it is then called a **singleton**. For example, {1} is the set with 1 as its only element; thus {1} and 1 are quite different. There is also a set with no element at all. Naturally, there can be only one such set: it is called the **empty set**, and is denoted by $\varnothing$. Any set other than the empty set is said to be **nonempty**.

So far we have specified sets by simply listing all their elements, separated by commas and included in braces. Some sets cannot be written in this way, because they are **infinite**. For example, the set $\mathbb{N}$ of natural numbers is infinite; we may suggest its elements by writing $\mathbb{N} = \{0, 1, 2, \ldots\}$, using the three dots and your intuition in place of an infinitely long list. A set that is not infinite is **finite**.†

†This is an informal explanation, since a definition would be beyond the scope of this book.

Another way to specify a set is by referring to other sets and to properties that elements may or may not have. Thus if $I = \{1, 3, 9\}$ and $G = \{3, 9\}$, G may be described as the set of elements of I that are greater than 2. We write this fact as follows.

$$G = \{x: x \in I \text{ and } x \text{ is greater than } 2\}.$$

In general, if a set A has been defined and P is a property that elements of A may or may not have, then we can define a new set

$$B = \{x: x \in A \text{ and } x \text{ has property } P\}.$$

As another example, the set of odd natural numbers is

$$O = \{x: x \in \mathbb{N} \text{ and } x \text{ is not divisible by } 2\}.$$

A set A is a **subset** of a set B—in symbols, $A \subseteq B$—if each element of A is also an element of B. We also say that A **is included in** B. Thus $O \subseteq \mathbb{N}$, since each odd natural number is a natural number. Note that any set is a subset of itself. If A is a subset of B but A is not the same as B, we say that A is a **proper subset** of B and write $A \subsetneq B$. Also note that the empty set is a subset of every set. For if B is any set, then $\varnothing \subseteq B$ vacuously, since each element of $\varnothing$ (of which there are none) is also an element of B.

To prove that two sets A and B are equal, we may prove that $A \subseteq B$ and $B \subseteq A$. Every element of A must then be an element of B and vice versa, so that A and B have the same elements and $A = B$.

Two sets can be combined to form a third by various **set operations**, just as numbers are combined by arithmetic operations such as addition. One set operation is **union**: the union of two sets is that set having as elements the objects that are elements of at least one of the two given sets, and possibly of both. We use the symbol $\cup$ to denote union, so that

$$A \cup B = \{x: x \in A \text{ or } x \in B\}.$$

For example,

$$\{1, 3, 9\} \cup \{3, 5, 7\} = \{1, 3, 5, 7, 9\}.$$

The **intersection** of two sets is the collection of all elements the two sets have in common; that is,

$$A \cap B = \{x: x \in A \text{ and } x \in B\}.$$

For example,

$$\{1, 3, 9\} \cap \{3, 5, 7\} = \{3\}$$

and

$$O \cap \mathbb{N} = O.$$

Finally, the **difference** of two sets A and B, denoted by $A - B$, is the set of all elements of A that are not elements of B.

$$A - B = \{x: x \in A \text{ and } x \notin B\}$$

For example,

$$\{1, 3, 9\} - \{3, 5, 7\} = \{1, 9\}.$$

Certain properties of the set operations follow easily from their definitions. For example, if A, B, and C are sets, the following laws hold.

Idempotency	$A \cup A = A$
	$A \cap A = A$
Commutativity	$A \cup B = B \cup A$
	$A \cap B = B \cap A$
Associativity	$(A \cup B) \cup C = A \cup (B \cup C)$
	$(A \cap B) \cap C = A \cap (B \cap C)$
Distributivity	$A \cup (B \cap C) = (A \cup B) \cap (A \cup C)$
	$A \cap (B \cup C) = (A \cap B) \cup (A \cap C)$
Absorption	$A \cap (A \cup B) = A$
	$A \cup (A \cap B) = A$
DeMorgan's Laws	$A - (B \cup C) = (A - B) \cap (A - C)$
	$A - (B \cap C) = (A - B) \cup (A - C)$

Example 1.2.1

Let us prove the first of DeMorgan's laws. Let

$$L = A - (B \cup C)$$

and

$$R = (A - B) \cap (A - C);$$

we are to show that $L = R$. We do this by showing (a) $L \subseteq R$ and (b) $R \subseteq L$.

(a) Let x be any element of L; then $x \in A$, but $x \notin B$ and $x \notin C$. Hence x is an element of both $A - B$ and $A - C$, and is thus an element of R. Therefore $L \subseteq R$.

(b) Let $x \in R$; then x is an element of both $A - B$ and $A - C$, and is therefore in A but in neither B nor C. Hence $x \in A$ but $x \notin B \cup C$, so $x \in L$. Therefore $R \subseteq L$, and we have established that $L = R$.

Two sets are **disjoint** if they have no element in common, that is, if their intersection is empty.

It is possible to form intersections and unions of more than two sets. If S is any collection of sets, we write $\bigcup S$ for the set whose elements are the elements of the sets in S. For example, if $S = \{\{a, b\}, \{b, c\}, \{c, d\}\}$ then $\bigcup S = \{a, b, c, d\}$; and if $S = \{\{n\} : n \in \mathbb{N}\}$, that is, the collection of all the singleton sets with natural numbers as elements, then $\bigcup S = \mathbb{N}$. In general,

$$\bigcup S = \{x : x \in P \text{ for some set } P \in S\}.$$

Similarly,

$$\bigcap S = \{x : x \in P \text{ for each set } P \in S\}.$$

The collection of all subsets of a set A is itself a set, called the **power set** of A and denoted by 2^A. For example, the subsets of $\{c, d\}$ are $\{c, d\}$ itself, the singletons $\{c\}$ and $\{d\}$, and the empty set $\varnothing$, so

$$2^{\{c,d\}} = \{\varnothing, \{c\}, \{d\}, \{c, d\}\}.$$

A **partition** of a nonempty set A is a subset Π of 2^A such that $\varnothing$ is not an element of Π and such that each element of A is in one and only one set in Π. That is, Π is a partition of A if Π is a set of subsets of A such that

1. each element of Π is nonempty;
2. distinct members of Π are disjoint;
3. $\bigcup \Pi = A$.

For example, $\{\{a, b\}, \{c\}, \{d\}\}$ is a partition of $\{a, b, c, d\}$, but $\{\{a, b, c\}, \{c, d\}\}$ is not. The sets of even and odd natural numbers form a partition of $\mathbb{N}$.

1.3 RELATIONS AND FUNCTIONS

Mathematics deals with statements about objects and the relations between them. It is natural to say, for example, that "less than" is a relation between objects of a certain kind—namely, numbers—which holds between 4 and 7 but not between 4 and itself. But the *general* idea of a relation is, at this point, an intuitive and nonmathematical one; what exactly constitutes a relation? Standard mathematical procedure is to define relations in terms of sets: a relation is a set of objects of a particular kind. The objects that belong to relations are, in essence, the combinations of individuals for which that relation holds in the intuitive sense. So the less-than relation is the set of all pairs of numbers such that the first number is less than the second. Now there is no mystery about less-than as an abstraction; it has been reduced to the set of all its concrete instances.

But we have moved a bit quickly. In a pair that belongs to a relation, we need to be able to distinguish the two parts of the pair, and we have not explained how to do so. We cannot write these pairs as sets, since $\{4, 7\}$ is the same thing as $\{7, 4\}$. It is easiest to introduce a new device for grouping objects called an **ordered pair.**†

We write the ordered pair of two objects a and b as (a, b); a and b are called the *components* of the ordered pair (a, b). The ordered pair (a, b) is not the same as the set $\{a, b\}$. First, the order matters: (a, b) is different from (b, a), whereas $\{a, b\} = \{b, a\}$. Second, the two components of an ordered pair need not be distinct; $(7, 7)$ is a valid ordered pair. Note that two ordered pairs (a, b) and (c, d) are equal only when $a = c$ and $b = d$.

†*True fundamentalists would see the ordered pair* (a, b) *not as a new kind of object, but as identical to* $\{a, \{a, b\}\}$.