INDISCRETE MATHEMATICS

Prof. Timothy Walsh, Department of Computer Science, UQAM

TABLE OF CONTENTS

INDISCRETE MATHEMATICS

Discrete mathematics isn't prudent mathematics; it deals with the mathematical properties of individual objects that can be counted using integers, like drops of water, as opposed to continuous mathematics, which studies objects that must be measured using real numbers, like the mass of a quantity of water. This monograph contains a collection of humourous illustrations of some of the concepts of discrete mathematics. My goal in writing it is to show that mathematics can be useful even for computer science students and, more incredibly yet, it can even be fun. Hopefully, some of the material contained in this monograph will find its way into lectures delivered by professors other than me.

CHAPTER 1. LOGIC

1.1 What is a proposition?

A *proposition* is either an assertion that is true or an assertion that is false. An assertion whose truth value is indeterminate is not a proposition. For example, "Montreal is the biggest city in Quebec" is a true proposition and "Montreal is the biggest city in Canada" is a false proposition (Toronto's population is now greater than Montreal's). "Do you like Montreal?" is not a proposition because it is not even an assertion, and neither is "Come and live in Montreal!". "Quebec will be part of Canada in five years." is an assertion, but it is not a proposition because its truth value is as yet indeterminate; it is not yet established whether there will be another neverendum referendum in the next five years or, if there is one, which side will cheat enough to win it.

Turning to more mathematical examples, $\frac{1}{2}+\frac{1}{3}=\frac{5}{6}$ is a true proposition. Some students add fractions by adding the numerators and the denominators, thus deriving the false proposition that $\frac{1}{2}+\frac{1}{3}=\frac{2}{5}$. On the other hand, $x \geq y$ is not a proposition because its truth value is indeterminate as long as the values of x and y are unknown. Similarly, it is unknown whether the end justifies the means until we know what end is desired and what means will be used.

1.2 Combining propositions

Logic has some similarities with the algebra you're familiar with: there are constants, variables and operators. But since a proposition must be either true or false, in logic there are only two constants: 0 meaning false and 1 meaning true. A variable represents either a true proposition or a false one. A logical operator that operates on one variable, say p, is defined by determining whether it is true if p is true and whether it is true if p is false. If it operates on two variables, say p and q, it is defined by determining whether it is true or false under each of the four possible conditions (p and q true, p true and q false, p false and q true, p and q both false). This definition can be expressed in tabular form as a *truth table*. Below are the truth tables for the most commonly used logical operators that act on two variables.

Columns 1 and 2 of the truth tables just below list the possible truth values of the two propositions p and q. Suppose that p is the proposition that it is raining and q is the proposition that it is freezing. On the first line it is both raining and freezing; so there will soon be a power outage, causing a subsequent increase in the birth rate. On the second line, it is raining but not

freezing; so we will stay indoors and watch television. On the third line, it is freezing but not raining; so we will go skiing if it snows or skating otherwise. On the fourth line it is neither freezing nor raining; so we will play golf. Under any other condition we will study.

1	2	3	4	5	6	7	8	9
p	q	$p \wedge q$	$p \vee q$	$p \oplus q$	$p \leftrightarrow q$	$p \rightarrow q$	$q \rightarrow p$	$\neg q \rightarrow \neg p$
1	1	1	1	0	1	1	1	1
1	0	0	1	1	0	0	1	0
0	1	0	1	1	0	1	0	1
0	0	0	0	0	1	1	1	1

Column 3 is the truth table for *conjunction*: p and q. It is raining and freezing: very bad weather. Column 4 is the truth table for *disjunction*: p or q. It is either raining or freezing **or both** (*inclusive or*): bad weather. To exclude the possibility that it is both raining and freezing (leaving only moderately bad weather) we use the *exclusive or* (column 5).

Column 7 is the truth table for *implication*: if p, then q. Now let p be the proposition that it is raining and q the proposition that I will take my umbrella. Then the implication means that if it rains, I will take my umbrella. On line 1, it is raining and I took my umbrella; so I told the truth. On line 2, it is raining but I didn't take my umbrella; so I lied and get punished by getting wet. On line 4, it is not raining and I didn't take my umbrella; so I told the truth. On line 3, it isn't raining but I took my umbrella anyway. According to the truth table, I told the truth. How could that be? Well, I didn't say that I would take my umbrella **if and only if** it rains – that is *logical equivalence* or *double implication* (column 6). All I said is that **if** it rains, **then** I will take my umbrella. I didn't say **what** I would do if it **doesn't** rain; so I can take my umbrella or leave it at home and I am telling the truth either way, since the facts do not contradict my claim. Similarly, the NDP isn't lying no matter what they promise to do if they become the government because they will never become the government.

To illustrate the last two columns, let p be the proposition that Paul killed Peter and q the proposition that Peter is dead. The implication $p \rightarrow q$ of column 7 is that if Paul killed Peter, then Peter is dead. The implication $q \rightarrow p$ of column 8 is that if Peter is dead, Paul killed him. The implication $q \rightarrow p$ is called the *converse* of the original implication $p \rightarrow q$. Two propositions are called *logically equivalent* if their truth tables are identical. The converse of an implication is not logically equivalent to the original implication: the truth tables of columns 7 and 8 are not identical, and in particular, on line 3, Peter is dead but not at Paul's hand. In column 9, the symbol $\neg$ is called *negation* : $\neg p$ means not p, which is false if p is true and true if p is false (see the truth table below). The implication $\neg q \rightarrow \neg p$ of column 9 is that if Peter isn't dead, then Paul didn't kill him. The implication $\neg q \rightarrow \neg p$ is called the *contrapositive* of the original implication $p \rightarrow q$ and is logically equivalent to the original implication: the truth tables of columns 7 and 9 are identical. This fact can be expressed as a *logical identity*: $(\neg q \rightarrow \neg p) \leftrightarrow (p \rightarrow q)$.

Other logical identities can be proved using truth tables, for example the laws of complementation: $p \wedge \neg p \leftrightarrow 0$ and $p \vee \neg p \leftrightarrow 1$. Let p be the proposition that it will rain. In the truth tables immediately below, column 3 is the statement that it will rain and it will not rain. This statement is false whether or not it rains, and a weatherman making such a prediction is probably crazy and will certainly get fired. It is an example of a *contradiction*: a proposition that

is false under all circumstances (its truth table has a 0 on every line). Column 4 is the statement that it will rain or it will not rain. This statement is true whether or not it rains and a weatherman making such a prediction is giving no information; he too will get fired and would be well advised to consider a career more suited to his talents, such as politics. It is an example of a *tautology*: a proposition that is true under all circumstances (its truth table has a 1 on every line). A logical identity, then, is by definition a tautology.

p	$\neg p$	$p \wedge \neg p$	$p \vee \neg p$
1	0	0	1
0	1	0	1

Other logical identities you can prove (and I would advise you to do so) are

$\neg(\neg p) \leftrightarrow p$ (double negation),
$p \wedge p \leftrightarrow p$ and $p \vee p \leftrightarrow p$ (idempotence),
$1 \vee p \leftrightarrow 1$ and $0 \wedge p \leftrightarrow 0$ (domination),
$1 \wedge p \leftrightarrow p$ and $0 \vee p \leftrightarrow p$ (identity),
$p \wedge (p \vee q) \leftrightarrow p$ and $p \vee (p \wedge q) \leftrightarrow p$ (absorption),
$p \wedge q \leftrightarrow q \wedge p$ and $p \vee q \leftrightarrow q \vee p$ (commutativity),
$(p \wedge q) \wedge r \leftrightarrow p \wedge (q \wedge r)$ and $(p \vee q) \vee r \leftrightarrow p \vee (q \vee r)$ (associativity),
$p \wedge (q \vee r) \leftrightarrow (p \wedge q) \vee (p \wedge r)$ and $p \vee (q \wedge r) \leftrightarrow (p \vee q) \wedge (p \vee r)$ (distributivity),
$\neg (p \wedge q) = (\neg p) \vee (\neg q)$ and $\neg (p \vee q) = (\neg p) \wedge (\neg q)$ (de Morgan's laws).

How many lines would a truth table have to have to prove the laws of associativity or distributivity? And if there were n different variable names in an identity, how many lines would the truth table need to have?

An assertion expressed by means of the constants 0 and 1, variable names and operators is called a *Boolean expression*, named after the mathematician, philosopher and logician George Boole, who invented the prototype of what is now called Boolean logic. Other logical operators, like implication, double implication and exclusive or are also logical operators, but any proposition can be written as a Boolean expression that uses no logical operators except conjunction, disjunction and negation. Here's how it's done. First you construct a truth table of the proposition (see column 3 of the truth table below). For each line of the truth table for which the proposition is true – that is, where there is a 1 – you write the all the variable names, with a negation sign in front of each variable that is false, and you separate all the variables by the conjuction operator. This conjunction will be true just for that line (see columns 4 and 7 of the truth table below). Finally, you surround each of those conjunctions by parentheses and you separate them by the disjunction operator (see column 8). This expression, which uses no logical operators except conjunction, disjunction and negation, will be true just for those lines for which the original proposition is true; so it is logically equivalent to the proposition.

1	2	3	4	5	6	7	8
p	q	$p \leftrightarrow q$	$p \wedge q$	$\neg p$	$\neg q$	$\neg p \wedge \neg q$	$(p \wedge q) \vee (\neg p \wedge \neg q)$
1	1	1	1	0	0	0	1
1	0	0	0	0	1	0	0
0	1	0	0	1	0	0	0
0	0	1	0	1	1	1	1

Of course you don't have to write all the columns of the above truth table, only the first three; the others were added here to show why the method works. Here's another example to illustrate this point.

p	q	$p \oplus q$
1	1	0
1	0	1
0	1	1
0	0	0

This proposition is true when p is true and q is false and also when p is false and q is true; so it is logically equivalent to $(p \wedge \neg q) \vee (\neg p \wedge q)$.

If more of the lines in the truth table are 1 than 0, there's a way to construct a Boolean expression that has only as many conjunctions are there are zero-lines, and if you are as lazy as most mathematicians, you will certainly want to do so. After constructing the truth table of the proposition, you construct the truth table of the negation of that proposition by changing each 1 to 0 and each 0 to 1 (see column 4 of the truth table below). This table will have fewer ones than zeros; so the Boolean expression for the negation will have fewer conjunctions. You write out that Boolean expression and then you negate it.

p	q	$p \rightarrow q$	$\neg (p \rightarrow q)$
1	1	1	0
1	0	0	1
0	1	1	0
0	0	1	0

The resulting Boolean expression for $\neg (p \rightarrow q)$ is $p \wedge \neg q$; so $p \rightarrow q$ is logically equivalent to $\neg (p \wedge \neg q)$. But of course you will want to shorten your Boolean expression even further, and you can do so using de Morgan's laws, named after their inventor, Augustus de Morgan. Applying one of these laws to $\neg (p \wedge \neg q)$, we obtain the Boolean expression $(\neg p) \vee q$, which is the usual way of expressing $p \rightarrow q$ without using any logical operators except conjunction (not used in this case), disjunction and negation.

The study of the consequences of the above identities is called Boolean algebra. There are some similarities between Boolean algebra and the algebra you're familiar with. If you replace $\wedge$ by $\times$, $\vee$ by $+$ and negation by subtraction from 1 in most of the above identities you get corresponding laws of algebra. There are some exceptions; for example,

$$1 + 1 \neq 1 \text{ and } p + (q \times r) \neq (p + q) \times (p + r).$$

There are other exceptions as well. Can you find them all?

Of course, George Boole didn't take Boolean algebra as far as it has been taken since his time, but they still named that subject after him. They also named a crater on the moon after him although he didn't create it, visit it or even discover it.

1.3 Quantified propositions

The assertion $x \geq 0$ is not a proposition because its truth value is indeterminate as long as the value of x is unknown; such an assertion is called a *propositional function*. One way to turn this propositional function into a proposition is to assign a value to x. For example, if we set $x = 1$, then $x \geq 0$ becomes the true proposition $1 \geq 0$, whereas if we set $x = -1$, then $x \geq 0$ becomes the false proposition $-1 \geq 0$.

Another way to turn that assertion into a proposition is to quantify x – that is, to state that the assertion is true for all x or for at least one x. Suppose we want to say that $x \geq 0$ for all x. To express that assertion in mathematical notation, we take the letter A, the first letter of the word All, and write it upside down. It then becomes the *universal quantifier* $\forall$ and the assertion is written $(\forall x)\ x \geq 0$. Is this assertion true or false? Well, if x can be any integer, then the assertion is false, but if x is restricted to the *natural numbers* (non-negative integers), then the assertion is true. Without determining the possible values x can have, you can't determine whether the assertion is true or false, or even whether it makes any sense: if x is a dog or a cat or an ice cream cone, it can't be compared with 0. For a quantified assertion to be a quantified proposition, you must define a *universe of discourse*, usually denoted by U; then $(\forall x)\ x \geq 0$ means that $x \geq 0$ for all x in U. If U consists of all the intergers, then the assertion is a false proposition, whereas if U consists of the natural numbers, then the assertion is a true proposition.

Similarly, suppose we want to say that there exists an x such that $x \geq 0$. To express that assertion in mathematical notation, we take the letter E, the first letter of the word Exists, and write it backwards. It then becomes the *existential quantifier* $\exists$; the assertion is written $(\exists x)\ x \geq 0$ and it means that there exists an x in U such that $x \geq 0$. If U consists of all the integers, then the assertion is a true proposition; if U consists of the negative integers, then the assertion is a false proposition.

In general, a *predicate* is a statement about one or more *subjects*. The notation for a generic predicate with one subject x is $P(x)$; in our example, $P(x)$ is the predicate $x \geq 0$. A predicate with two subjects x and y is denoted by $P(x,y)$ and predicates with many subjects have similar notations.

The proposition $\exists x \exists y P(x,y)$ means that there exists x in U and there exists y in U such that the predicate $P(x,y)$ is true. Suppose that U consists of all the real numbers. If $P(x,y)$ is the predicate $x + y = -1$, then the proposition $\exists x \exists y P(x,y)$ is true, but if $P(x,y)$ is the predicate $x^2 + y^2 = -1$, then the proposition $\exists x \exists y P(x,y)$ is false.

The proposition $\forall x \forall y P(x,y)$ means that for all x in U and for all y in U the predicate $P(x,y)$ is true. Suppose that U consists of all the real numbers. If $P(x,y)$ is the predicate $x^2 + y^2 \geq 0$, then the proposition $\forall x \forall y P(x,y)$ is true, but if $P(x,y)$ is the predicate $x + y = -1$, then the proposition $\forall x \forall y P(x,y)$ is false.

The proposition $\forall x \exists y P(x,y)$ means that for all x in U there exists a y in U such that $P(x,y)$ is true. Suppose that $P(x,y)$ is the predicate $y > x$. If U consists of all the real numbers, then the proposition $\forall x \exists y P(x,y)$ is true (for all x, let y be $x + 1$), but if U consists of the numbers

1,2,3,4,5, then the proposition is $\forall x \exists y P(x,y)$ is false (if $x = 5$, then there is no y in U that is greater than x).

The proposition $\exists y \forall x P(x,y)$ means that there exists a y in U such that for all x in U the predicate $P(x,y)$ is true. Suppose that $P(x,y)$ is the predicate $x \geq y$. If U consists of all the integers, then the proposition $\exists y \forall x P(x,y)$ is false (for all y, let x be $y - 1$), but if U consists of all the natural numbers, then the proposition $\exists y \forall x P(x,y)$ is true (if $y = 0$, then $x \geq y$ for any natural number x).

The above examples illustrate the way to negate a quantified proposition: you change each $\exists$ to $\forall$, change each $\forall$ to $\exists$ and negate the predicate. For example, the negation of the proposition $\exists y \forall x P(x,y)$ is $\forall y \exists x \neg P(x,y)$. In the above example, the original proposition is that there is an integer y which is greater than equal to every integer x, and this proposition was proved false by using its negation: for every integer y there exists an integer $x = y - 1$ which is less than y.

If you want x and y to belong to different parts of U, you define some predicates that say that a subject has a particular property and then you use another operator, denoted by a colon, which means "such that". For example, if you want to refer to rabbits and foxes, you let U be all the animals and you define the following predicates: $R(x)$ means that x is a rabbit, $F(y)$ means that y is a fox and $C(y,x)$ means that y can catch x. Then the statement "for every rabbit there is a fox that can catch it" is written as $(\forall x : R(x))(\exists y : F(y))C(y,x)$. Its negation – "there is a rabbit that no fox can catch" – is written as $(\exists x : R(x))(\forall y : F(y))\neg C(y,x)$. To negate a proposition of this sort, you don't negate the predicates that describe the subjects: the rabbit doesn't become a non-rabbit and the fox doesn't become a non-fox.

Two quantified propositions are *logically equivalent* if they have the same truth value whatever predicate and whatever universe of discourse we choose, as long as they are the same for both propositions. For example, the propositions $\exists x \exists y P(x,y)$ and $\exists y \exists x P(x,y)$ are logically equivalent: the order in which we take the x and the y is unimportant. For the same reason, the propositions $\forall x \forall y P(x,y)$ and $\forall y \forall x P(x,y)$ are logically equivalent.

Are the propositions $\forall x \exists y P(x,y)$ and $\exists y \forall x P(x,y)$ logically equivalent? We have seen that if $P(x,y)$ is the predicate $y > x$ and U consists of all the real numbers, then $\forall x \exists y P(x,y)$ is true. With the same predicate and universe of discourse, is it true that $\exists y \forall x P(x,y)$? That would mean that there is a real number y that is bigger than all the real numbers including y itself! This proposition is patently false. Wherein lies the difference between these two quantified propositions? With $\forall x \exists y P(x,y)$ there could be **a different *y*** for each x, whereas with $\exists y \forall x P(x,y)$ **the same *y*** has to be used with each x. The difference can be further illustrated by a non-mathematical example. A man says, "I read in the paper that in New York someone gets hit by a car every half hour." His wife says, "Oh, the poor guy!" He means that for every half hour there is a person in New York (a different person for each half hour) who gets hit by a car and she thinks he means that there is a person in New York who gets hit by a car every half hour (the same person for each half hour). Such confusion could be avoided if only everyone spoke the language of quantified propositions!

CHAPTER 2. SETS

2.1 Set definitions

A *set* is a collection of objects, called its *elements*. We express the proposition that the object x is an element of the set S in mathematical shorthand as $x \in S$ and the proposition that x is not an element of S as $x \notin S$. We have already seen sets in Chapter 1: the universe of discourse of a quantified proposition is a set whose elements are the things that the subjects can be. Another example of a set is the set of students in a classroom where I'm teaching you discrete mathematics. All the elements of a set are distinct (you'd find it strange to see a copy of yourself sitting beside you) and two sets are equal if they have the same elements without regard to order (you are not in any order, at least until I have marked your exams).

A set can be defined *explicitly* by listing its elements, separated by commas and surrounded by braces. For example, the set of vowels is {a,e,i,o,u}, the set of natural numbers is {0,1,2,3,…} (the symbol … means "and so on") and the set of integers is {…,-3,-2,-1,0,1,2,3,…}.

Some sets are used so often that they are given names. The set of natural numbers (non-negative integers) is called **N** for **n**atural. The set of integers is called **Z** for the German word **Z**ahlen, which means numbers. The set of rational numbers is called **Q** for **q**uotient because a rational number is the quotient of two integers. The set of real numbers is called **R** for **r**eal. And the empty set, defined explicitly as {}, is called ϕ for reasons I don't know.

A set S can be defined *implicitly* by stating a condition that an object x satisfies if and only if $x \in S$. Implicit definition uses the symbol :, which means "such that". In some textbooks a vertical line | is used to mean "such that", but since a vertical line also means "divides" (the integer d *divides* the integer a if there is an integer q such that $a=qd$), I use : to avoid confusion. For example, the set of even integers is defined implicitly as $\{x \in \mathbf{Z}:2|x\}$, which is at least somewhat less confusing than $\{x \in \mathbf{Z}|2|x\}$.

2.2 Set operators

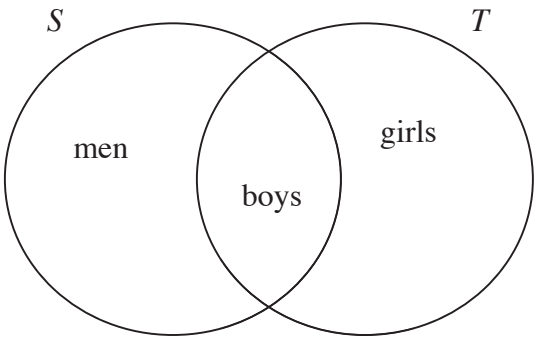
Suppose that S and T are two sets. Other sets can be formed from S and T using *set operators*.

The *union* of S and T is the set of objects that are either in S or in T or in both. It is denoted mathematically by $S \cup T$. The symbol $\cup$ was chosen because it looks like a U, which stands for **u**nion. It is also called "cup" because it looks like one. The above definition of $S \cup T$ is of necessity implicit; it is expressed in mathematical shorthand as $S \cup T = \{x : x \in S \vee x \in T\}$. Note the similarity between the symbol $\cup$, which looks like a U, and the symbol $\vee$, which looks like V, the next letter in the alphabet, obtained from U by using a pencil sharpener.

The *intersection* of S and T, denoted by $S \cap T$, is the set of objects that are in both S and T, so that $S \cap T = \{x : x \in S \wedge x \in T\}$. The symbol $\cap$, sometimes called "cap" because it looks like one, is obtained from $\cup$ by writing it upside down, and the symbol $\wedge$ can be obtained by either turning $\vee$ upside down or applying the pencil sharpener to $\cap$.

For example, if S is the set of human males and T is the set of human children, then $S \cap T$ is the set of boys and $S \cup T$ is the set of people who have time to play video games.

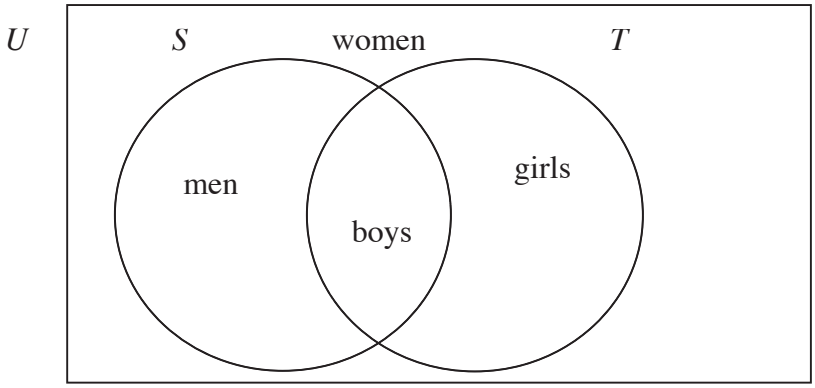
For those who prefer pictures to symbols, these operators can be illustrated using a Venn diagram. In the Venn diagram below, S and T are the interiors of the circles with the corresponding label, $S \cap T$ is the region inside both circles and $S \cup T$ consists of the three regions inside either or both circles.



The *symmetric difference* of S and T, denoted by $S \oplus T$, is the set of objects that are either in S or in T but not in both, so that $S \oplus T = \{x : x \in S \oplus x \in T\}$. Note that the same symbol is used for symmetric difference and exclusive or. In the above example, $S \oplus T$ is the set of men and girls.

The *difference* of T from S, denoted by $S \backslash T$ or $S–T$, is the set of objects that are in S but not in T. In the above example, $S \backslash T$ is the set of men and $T \backslash S$ is the set of girls.

The *complement* of S, denoted by $\overline{S}$ or S^C, is the set of objects that are not in S. In the above example, what is the complement of $S \cup T$? Well, women are not in $S \cup T$ but neither are cats or stars. To define the complement of a set we have to define a *universal set*, denoted by U just like the universe of discourse. Then $\overline{S}$ is equal to $U \backslash S$. In a Venn diagram, U is represented by a rectangle that surrounds all the circles. If we let U be the set of all humans, then $(S \cup T)^C$ is the set of women, as in the Venn diagram below.

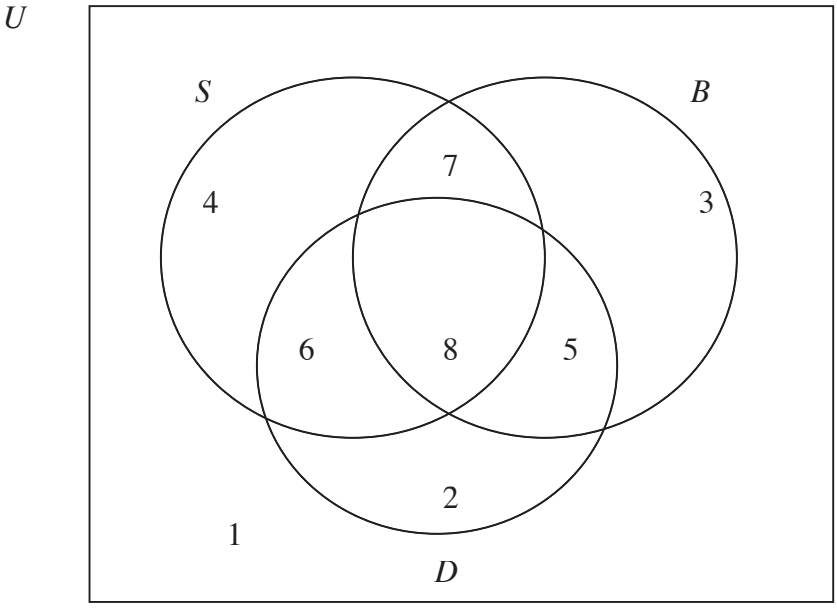


Every logical identity has a corresponding set identity, which you can obtain by changing disjunction to union, conjunction to intersection, negation to complementation, 0 to the empty set and 1 to the universal set. To prove the set identity, all you have to do is prove the corresponding logical identity by using a truth table.

We say that T is a *subset* of S, denoted by $T \subseteq S$, if every element of T is also an element of S. In the above example, the set of boys is a subset of the set of children. We say that S and T are *disjoint* if they have no elements in common – that is, if $S \cap T = \phi$. In the above example, the set of men and the set of women are disjoint – or at least they were before the advent of sex change operations.

Union and intersection can be defined on more than two sets. The union of several sets is the set of objects that are in at least one of those sets and the intersection of several sets is the set of objects that are in all of those sets. The following example illustrates the union and intersection of three sets.

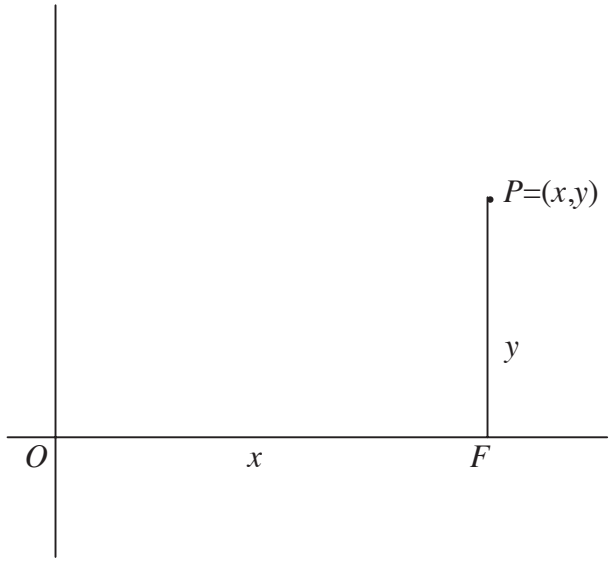
In a certain high school in the United States, the graduating class has 36 students of which 25 smoke, 23 drink booze, 21 take drugs, 15 smoke and drink, 14 smoke and take drugs, 13 drink and take drugs, and 8 smoke, drink and take drugs. How many of them have none of these vices and are therefore considered dorks by the rest of the class? To shorten the notation for the number of elements in a set S, we denote it by $\#(S)$. If we let U, the universal set, be the set of students in the graduating class, S be the set of students who smoke, B the set of those who drink booze and D be the set of those who take drugs, then $\#(U)=36$, $\#(S)=25$, $\#(B)=23$, $\#(D)=21$, $\#(S \cap B)=15$, $\#(S \cap D)=14$, $\#(B \cap D)=13$, $\#(S \cap B \cap D)=8$ and we want to find $\#((S \cup B \cup D)^C)$. The easiest way to solve such a problem is by means of a Venn diagram. A Venn diagram of three sets will have 8 regions representing 8 disjoint subsets of U. Using the fact that if S and T are disjoint, then $\#(S \cup T) = \#(S) + \#(T)$, we can calculate the number of elements in each of these subsets and write it in the corresponding region; the number in the region outside of all 3 circles will be the answer to the problem (see the Venn diagram below).



Other examples of the same type are easy to construct. A certain number of aristocrats pay $1000 each to come to an exclusive dinner. Three anarchists break windows and throw paint at the fan. Some of the aristocrats are splattered with yellow paint, some with red paint, some with blue paint, and some with various combinations of colours. How many of them are spared because they are already so drunk that they are under the table? Of a certain number of music students, some can sing, some can play an instrument, some can compose music and some have various combinations of these talents. How many of them have no musical talent and are thus reduced to becoming music critics? Of a certain number of lawyers, some lie, some cheat, some steal and some commit various combinations of these sins. How many of them are honest? None of them (phi on them all)! As an example using four sets, the Sorting Hat sorts the first-year Hogwarts students into their favourite house among those for which they are eligible. Of a certain number of first-years, some are eligible for Gryffindor, some for Hufflepuff, some for Ravenclaw, some for Slytherin, and some for each of the various combinations of houses. How many are squibs, eligible for none of the houses, and are sent back to King's Cross Station on the Hogwarts Express to attend a Muggle school? As you can see, by changing the number and definition of the sets and the number of elements in each of them and their various intersections, I can formulate a different exam question every session!

2.3 Cartesian product of sets and the power set

The famous mathematician and philosopher René Descartes invented a way of expressing the points in a plane algebraically. Draw a horizontal line, called the *x-axis*, and a vertical line, called the *y-axis*; the point of intersection of these two axes is called the *origin O*. Given a point *P* on the plane, draw a vertical line through *P* and call *F* the point of intersection of this line and the *x*-axis. Then the signed distance from *O* to *F* is called the *abscissa*, denoted by *x*, which is positive if *F* is to the right of *O* and negative if *F* is to the left of *O*, and the signed distance from *F* to *P* is called the *ordinate*, denoted by *y*, which is positive if *P* is above *F* and negative if *P* is below *F* (see the diagram below). Then *P* is identified by the ordered pair (*x*,*y*), its *co-ordinates*.



Since x can be any number in $\mathbf{R}$, the set of real numbers, and y can also be any number in $\mathbf{R}$, the whole plane is represented by the set of ordered pairs $\{(x,y) : x \in \mathbf{R} \wedge y \in \mathbf{R}\}$. In honour of Descartes, we call this set the *Cartesian product* of $\mathbf{R}$ by $\mathbf{R}$ and denote it by $\mathbf{R}\times\mathbf{R}$.

Similarly, any point P on the surface of the Earth can be represented by two co-ordinates. One of these is the *latitude*, which is the number of degrees that P is north (positive) or south (negative) of the equator. To define the other co-ordinate, the *longitude*, we use the Greenwich meridian, a circle passing through the two poles and a designated spot in England. Let O be the point south of Greenwich where this meridian intersects the equator. Draw a meridian through P and the two poles and let F be the point nearest to P where this meridian intersects the equator. Then the *longitude* of P is the number of degrees that F is east (positive) or west (negative) of O. The latitude can have any value between –90 and 90, inclusive; the set of these values is denoted by [-90,90]. The longitude can have any value between –180, exclusive, and 180, inclusive; the set of these values is denoted by]-180,180]. Then P is represented by the ordered pair (x,y), where x is the latitude and y is the longitude, and the surface of the Earth is represented by the set $\{(x,y) : x \in]-180,180] \wedge y \in [-90,90]\} =]-180,180]\times[-90,90]$.

Generalizing from these two examples, if S and T are two arbitrary sets, then the Cartesian product $S\times T$ is the set $\{(x,y) : x \in S \wedge y \in T\}$. For example, if S=$\{a,b,c\}$ and T=$\{0,1\}$, then $S\times T$=$\{(a,0),(a,1),(b,0),(b,1),(c,0),(c,1)\}$. It is easy to see that $\#(S\times T)=\#(S)\times\#(T)$; the symbol $\times$ was probably chosen for the Cartesian product because it looks nice when used twice in the above equation.

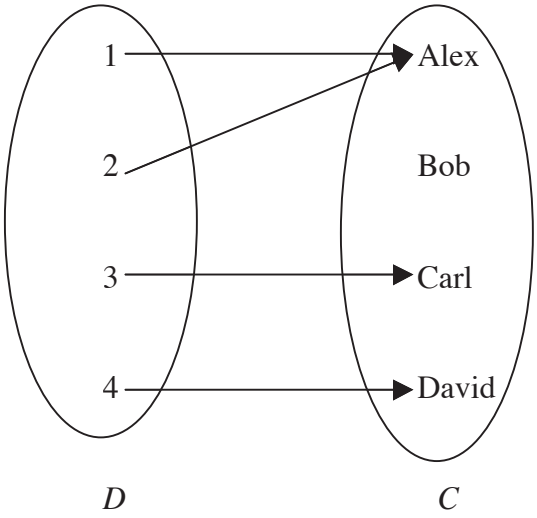
Like union and intersection, the Cartesian product can be generalized to more than two sets. Three-dimensional space can be represented by the Cartesian product $\mathbf{R}\times\mathbf{R}\times\mathbf{R}$, the three co–ordinates being east-west, north-south and up-down (or else left-right, up-down and near-far if you are watching a 3D movie, except that the last co-ordinate must be positive), and altitude above or below sea level can be added to latitude and longitude for expressing points on or near the surface of the Earth. The altitude of a fixed point on the surface of the Earth is expected to decrease, in some cases to negative values, as a result of global warming.

The *power set* of a set S, denoted by $P(S)$, is the set of all subsets of S. For example, if the set S is $\{0,1,2\}$, then $P(S) = \{\{2,1,0\}, \{2,1\}, \{2,0\}, \{2\}, \{1,0\}, \{1\}, \{0\}, \{\}\}$. If you represent a subset T of $\{0,1,2\}$ as a word $b_2b_1b_0$, where $b_i = 1$ if $i \in T$ and 0 otherwise, and write these words one under the other in the order in which the subsets appear above, then $P(S)$ looks like the first three columns of the 8-line truth table for the propositions $2\in T$, $1\in T$ and $0\in T$. Try it! More generally, a *binary string of length n* – a string of n 1s and 0s, called *binary digits* or *bits* – represents a subset of a set with n elements $\{x_1, \cdots, x_n\}$: the ith bit of the string is 1 if x_i is in the subset and 0 otherwise. The number of subsets T of a set with n elements is 2^n because for each element x_i of S there are two possiblities: either x_i is in T or it isn't. In some textbooks $P(S)$ is denoted by 2^S (the **power** set 2^S is the S^{th} **power** of 2). This notation allows mathematicians to write the elegant equation $\#\left(2^S\right) = 2^{\#(S)}$. Mathematicians place a high value on elegance.

CHAPTER 3. FUNCTIONS

3.1 Definitions.

I won't tell you yet what a function **is**; for the moment I'll just tell you what a function **does**. Given two sets D and C, a function f from D to C, denoted by $f:D\to C$, associates to each element $x\in D$ exactly one element $y=f(x)\in C$. The set D is called the *domain* of f and the set C is called the *codomain* of f. The element $y=f(x)$ is called the *image* of x under f and x is called a *preimage* of y under f. For example, suppose that $D=\{1,2,3,4\}$, $C=\{\text{Alex,Bob,Carl,David}\}$, $f(1)=\text{Alex}$, $f(2)=\text{Alex}$, $f(3)=\text{Carl}$ and $f(4)=\text{David}$ (see the diagram below). Each element $x\in C$ has exactly one image, but one element $\text{Alex}\in C$ has two preimages, 1 and 2, and another element $\text{Bob}\in C$ has none.

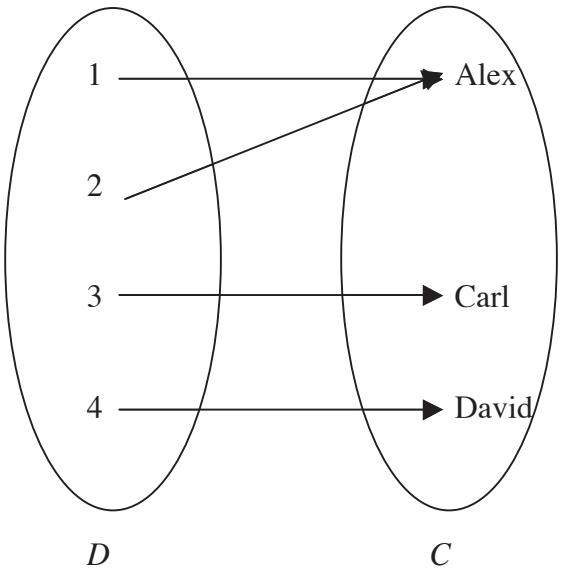


A function from D to C

The *range* of a function is the set of elements of C that have at least one preimage. In the above example, the range of the function f is {Alex, Carl, David}.

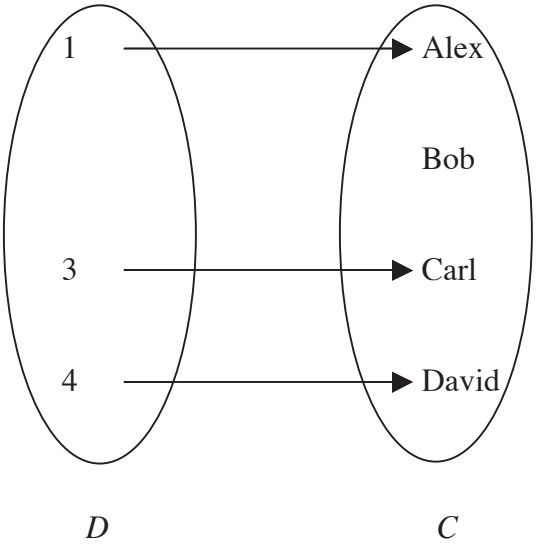
Suppose you are distributing candies to children. All the candies must be given away (or else the children will call you a pig) and no candy can be given to more than one child (because the candies are too hard to be cut and letting more than one child share a candy would be unsanitary); so the child to which each candy is given constitutes a function from the set D of candies to the set C of children. The above distribution is grossly unfair because Alex gets two candies and Bob doesn't get any. This example illustrates two properties of functions, which between them make a distribution fair.

A function $f:D\to C$ is called *onto* or *surjective* if every element of C has at least one preimage (in our model, if each child gets at least one candy). Any function can made onto by reducing the codomain so that it is equal to the range of the function. In the above example, if Bob kicks you and runs away crying, the codomain is now equal to {Alex, Carl, David}, the range of f, so that every remaining child gets at least one candy (see the illustration below).



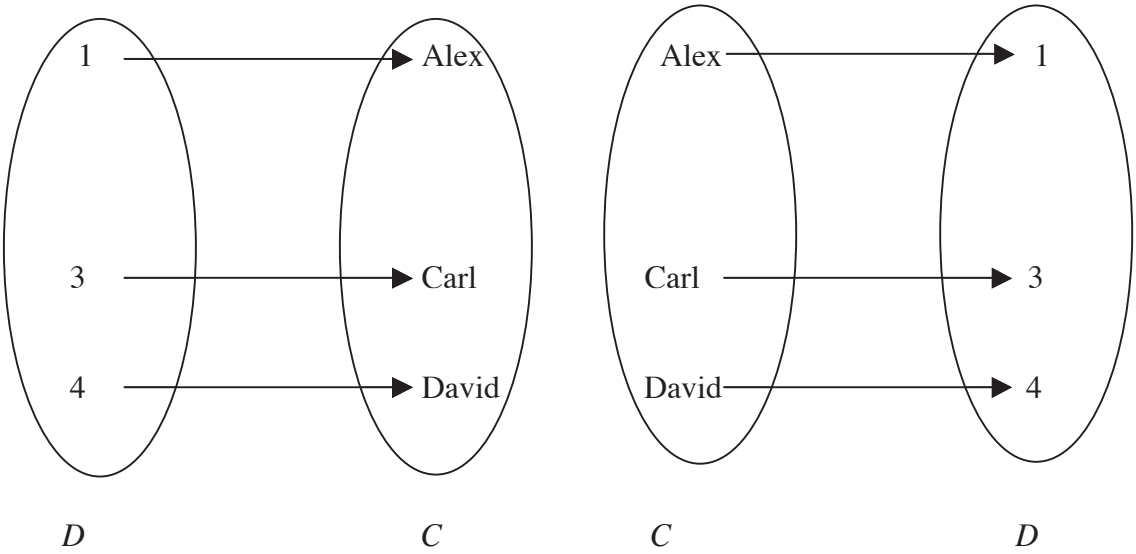
The function is now surjective.

A function is called *one-to-one* or *injective* if no element of *C* has more than one preimage or, equivalently, if no two elements of *D* have the same image (in our model, if no child gets more than one candy). Any function can be made one-to-one by choosing, for each element *y* of *C* that has more than one preimage, one of its preimages and deleting all the other preimages of *y* from *D*. In the above example, starting from the original function, you can grab candy number 2 back from Alex and eat it yourself. The domain is now {1, 3, 4} and every child now gets at most one candy (see the illustration below).



The original function is now injective.

A function that is both one-to-one and onto is called a *one-to-one correspondence* or *bijective*, so that every element of *C* has exactly one preimage (in our model, each child gets exactly one candy). Any function can be made bijective by making it both injective and surjective in either order (see the left illustration below).

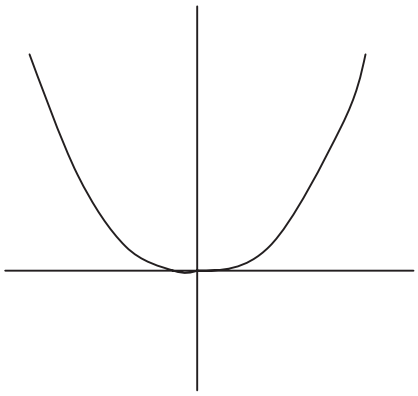


A one-to-one correspondence and its inverse

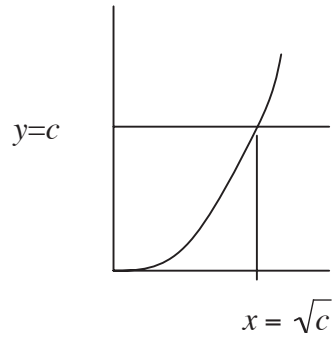
Since every element in *C* has exactly one preimage under *f*, we can define a function from *C* to *D* that associates to every element in *C* its unique preimage in *D* (see the right illustration above). This function is called the *inverse* of *f* and is denoted by f^{-1}. In our model, the image of each child in *C* under f^{-1} is the one candy he gets to eat.

3.2 Functions of real variables: powers, roots, exponentials and logarithms

As an example in which the domain and the codomain are infinite, let $f:\mathbf{R}\to\mathbf{R}$ be the function defined by $f(x) = x^2$ (see the left diagram below). This function is not surjective because the negative numbers have no preimage (the square of a real number cannot be negative) and it is not injective either because, for example, $f(1) = f(-1) = 1$. It can be made both surjective and injective by changing both the domain and the codomain to $\mathbf{R}^{\geq 0}$, the set of non-negative real numbers (see the right diagram below).



neither injective nor surjective



bijective

How do we know that the function is injective? As you can see from the diagram, it is *strictly increasing*: that is, the bigger x gets, the bigger x^2 gets. Why does that fact imply that a function is injective? Well, if two members of the domain are distinct, then one of them is bigger than the other. Call the bigger one b and the smaller one s. Since f is strictly increasing, $f(b) > f(s)$; so the images of b and s are unequal. And how do we know that this particular function is strictly increasing? Well, if you know calculus, you can find the derivative of this function, which is $2x$, which is positive everywhere in the domain except at $x = 0$, and there is a theorem that says that in this case a function is strictly increasing. Of course, this problem can be solved without calculus; so here goes. If we multiply the inequality $b > s$ by b, which is positive because $b > s \geq 0$, we get $b^2 > bs$. And if we multiply the same inequality by s, which is non-negative, we get $bs \geq s^2$. Since bs is at least as big as s^2 and b^2 is bigger than bs, b^2 must be bigger than s^2.

This is one of many examples of problems that can be solved with or without calculus but the solution without calculus is more difficult. The word *calculus* is a medical term meaning a stone, and stones can be very useful, as the following bit of history will show. Before people became hunters, they were scavengers. When they came upon the corpse of an animal that had been killed by a predator, they usually found that all the meat left by the predator had been picked clean by other scavengers, like hyenas and vultures. There is some nourishment in bone marrow, and the people cracked the bones with their teeth to get to the marrow. Unfortunately, sometimes they cracked their teeth as well. Eventually they discovered that they could break the bones without cracking their teeth by using a stone. If you don't want to learn calculus, you will make the solution of some problems so difficult that you may crack your teeth on them.

Returning to the function $f(x) = x^2$, how do we know that it is surjective? Given a real non-negative number c, is there always a real non-negative number x such that $f(x) = c$? If $c = 0$, then c has a preimage $x = 0$. Suppose that $c > 0$. The curve of the equation $y = x^2$ is below the line $y = c$ for $x = 0$ and above the line for big enough x. Since the function $f(x) = x^2$ is continuous, the curve can't jump over the line; so it must intersect the line at some positive real value of x, which is the preimage of c (see the diagram above). This is a consequence of a theorem of real analysis called the intermediate value theorem. If you try to prove that the

function $f(x) = x^2$ from the non-negative reals to the non-negative reals is surjective without using that theorem, you will surely crack your teeth.

Since this function is both injective and surjective, it has an inverse: $f^{-1}(x) = \sqrt{x}$, the (positive) *square root* of x. Similarly, we can define $\sqrt[n]{x}$, the nth root of x, to be the inverse of the function $f(x) = x^n$, again from the non-negative reals to the non-negative reals.

Another example is the *exponential* function $f:\mathbf{R}\to\mathbf{R}$ defined by $f(x) = b^x$, where b is some real number greater than 1. To define this function, we first define it for non-negative integers x: $b^0 = 1$, and for any $x > 0$, $b^x = b \times b \times ... \times b$ (x factors). It is easy to prove that for non-negative integers the exponential function satisfies the equations

$$b^{x+y} = b^x \times b^y \tag{3.2.1}$$

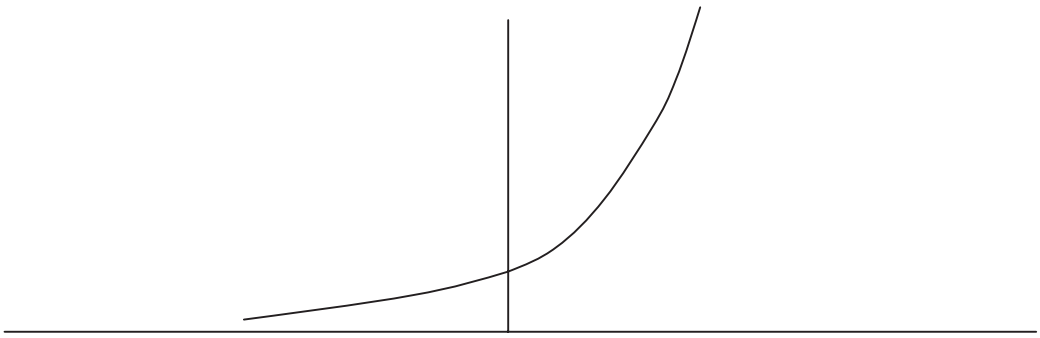
and

$$b^{xy} = \left(b^x\right)^y. \tag{3.2.2}$$

To prove (3.2.1) we note that both sides are equal to $x + y$ factors of b and to prove (3.2.2) we note that both sides are equal to xy factors of b.

We extend this definition to any integer x by stating that $b^{-x} = 1/b^x$. This is the only definition that makes (3.2.1) hold when $x + y = 0$. We further extend it to the rationals m/n, where $n > 0$, with the equation $b^{m/n} = \sqrt[n]{b^m}$. This is the only definition that makes (3.2.2) hold when x is the non-zero integer m and $y = 1/m$. Finally, we extend it to any real number x by defining $f(x)$ to be the limit of $f(q)$ as the rational number q tends to x. I invite you to prove that (3.2.1) and (3.2.2) hold for any real x and y, or at least for any rational x and y.

This function is not surjective, because $b^x > 0$ for any real x; so we restrict the codomain to $\mathbf{R}^{>0}$, the set of positive real numbers (see the diagram below).



This function is strictly increasing: if $g > s$, then $g - s > 0$, so that $b^{g-s} > 1$, and since $b^s > 0$, $b^g - b^s = b^s(b^{g-s} - 1) > 0$ so that $b^g > b^s$; so it is injective. And it is also surjective: if

c is any positive real number, then by making x small enough we can make $f(x) < c$, and by making x big enough we can make $f(x) > c$, so that there is some x for which $f(x) = c$. Therefore this function has an inverse $f^{-1} : \mathbf{R}^{>0} \to \mathbf{R}$, which we call $\log_b x$, the *logarithm* of x in base b.

From (3.2.1) and (3.2.2) it is not difficult to prove the following equations:

$$\log_b(mn) = \log_b(m) + \log_b(n) \tag{3.2.3}$$

$$\log_b(m^n) = n \times \log_b(m) \tag{3.2.4}$$

$$\log_b(n) = \frac{\log_c(n)}{\log_c(b)}\ , \tag{3.2.5}$$

where c is any real number greater than 1. These proofs too are left as exercises.

Logarithms were introduced by John Napier early in the 17th century as a means to simplify calculations. Navigators need to be able to do arithmetic, but in those days many of them were unable to multiply or divide large numbers; they could only add and subtract them. A table of logarithms in base 10 (common logarithms) and another table of exponentials in base 10 enabled them to multiply and divide the numbers they needed to navigate using (3.2.3). Of course they knew nothing of logarithms, but they didn't need to; all they needed to know was that you look up the numbers you want to multiply in a table called a table of logs, add the entries in that table and look up the sum in another table, called a table of antilogs. For example, to 5 decimal places, $\log_{10} 2 = 0.30103$ and $\log_{10} 3 = 0.47712$. The navigator would read these numbers in the table of logarithms, add them and get 0.77815. The entry for that number in the table of antilogs is $10^{0.47721} = 6.00000$, which would allow the navigator to multiply 2 by 3.

One day a naturalist who, like Harry Potter, can talk to snakes, was walking through a forest when he heard two snakes crying. He asked them why they were crying and they said, "We can't have any children! You see, we can't multiply because we're only adders." He left them and returned home, feeling sad. The next day there was a hurricane in which the naturalist dared not venture, but the day after that, the hurricane had passed; so the naturalist returned to the spot in the forest where he had met the crying snakes. Some of the trees had been blown down by the hurricane. Under one of them he found the two snakes surrounded by little snakes and smiling. He asked them how they had managed to multiply and they said, "We used the logs."

Of course, if you know how to multiply, it is easier to do so than to look up logarithms in a table, but logarithms are still useful – for calculating powers using (3.2.4) when the exponent is not a small integer. And you don't need a table of logarithms or exponentials either. In any calculus textbook you can find a formula for calculating logarithms in base $e = 2.718281828\ldots$ (natural logarithms , sometimes denoted by ln):

$$\log_e(1 + x) = x - \frac{x^2}{2} + \frac{x^3}{3} - \frac{x^4}{4} + \ldots \tag{3.2.6}$$

and another formula for calculating exponentials in the same base:

$$e^x = 1 + x + \frac{x^2}{2!} + \frac{x^3}{3!} + \frac{x^4}{4!} + \ldots \ . \qquad (3.2.7)$$

This is how a computer or a hand-held calculator calcuates powers. Of course, x has to be small for these series to converge quickly, but the computer stores floating-point numbers as an integral power of 2 (the exponent is the *characteristic* c) multiplied by a number between 1/2 and 1 (the *mantissa* m) and a sign. To calculate $e^{m\times 2^c}$ you first calculate e^m from (3.2.7) – that series converges quickly for x between 1/2 and 1 – and then square it c times. And $\log_e\left(m \times 2^c\right) = \log_e(m) - c \times \log_e(1/2)$; if $1 + x$ lies between 1/2 and 1, then x lies between –1/2 and 0, and for these numbers (3.2.6) converges quickly.

And to change from base e to any other base, the computer uses (3.2.5).

Engineers use logarithms in base 10 because they need 10 fingers to build bridges. Computer scientists use logarithms in base 2 because they need 2 fingers to type on a keyboard. And mathematicians use logarithms in base e because that's the number of fingers they need to hold a pen.

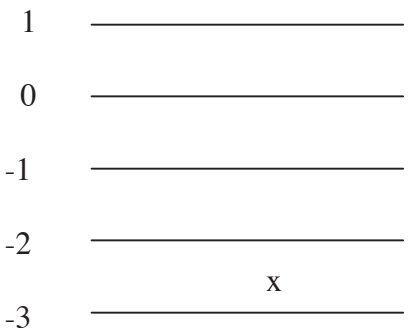
By this time (if not sooner), you have probably asked yourself why I would be so mean as to introduce indiscrete subjects like functions of a real variable such as powers, roots, exponentials and logarithms in a monograph about discrete mathematics. Well, as computer scientists, you will be writing programs, and as good computer scientists you will want to write programs that the computer will execute fast. In general, the more data you feed to a program, the longer it takes the program to run (for example, it takes longer to search a big array than a little one); so that the execution time is a function of the data size and we need to study functions to be able to predict the execution time of programs given the data size. Some programs run in a time proportional to the data size n, some in time proportional to some power or root of n, or an exponential function like 2^n or even $\log_2 n$, and if different programs that solve the same problem have different running times for the same n, you need to know which of these programs has the smallest running time for big n. The size of functions of n for large n is the subject of a later chapter. For the moment, trust me: you will find it useful to know the contents of this one.

3.3 Some special functions

Given any set S, the *identity function* on S, denoted by ι_S, is defined by $\iota_S(x) = x \ \forall x \in S$. This function is clearly bijective and it is its own inverse.

Another pair of functions we will need are $\lfloor x \rfloor$ = floor(x) and $\lceil x \rceil$ = ceiling(x), whose domain is $\mathbf{R}$ and whose codomain is $\mathbf{Z}$. We define $\lfloor x \rfloor$ to be the largest integer $n \le x$ and we define $\lceil x \rceil$ to be the smallest integer $n \ge x$. For example, $\lfloor 2.6 \rfloor = 2$ and $\lceil 2.6 \rceil = 3$. So what are $\lfloor -2.6 \rfloor$ and $\lceil -2.6 \rceil$? A fly 0.6 of the way from the ceiling to the floor in a room three levels below street level is at a height of –2.6 (see the diagram below). The floor is at level –3 and the ceiling is at level –2; so it is reasonable to define floor(–2.6) to be –3 and ceiling(–2.6) to be –2. "Less than" means "more negative", not "closer to 0". Some compilers compute the integer part of a real number by rounding towards 0. A possible explanation is that on the surface of the Earth,

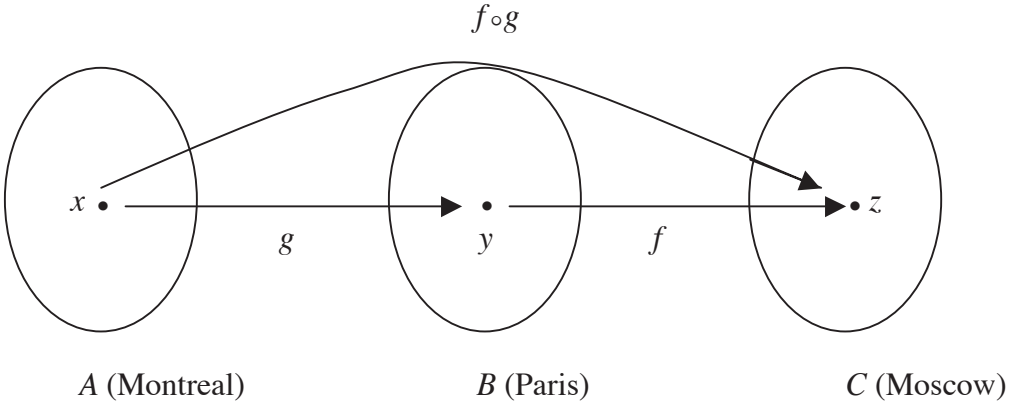
down means the opposite direction in Australia from what it means in North America; so maybe the people who write those compilers are Australian.



The ceiling function is often illustrated using boring examples like asking how many cans of paint have to be bought in order to paint a room of given dimensions. Here is a more indiscrete example. A certain female vampire needs to drink five litres of blood per week to survive. Since she doesn't like to kill people, she instead keeps a harem of men and asks them to donate as much blood as they can. If each of her men can donate half a litre of blood every four days, what is the minimum number of men she has to keep in her harem to survive forever? The demand divided by the supply per man is not an integer (calculating the exact ratio is left as an exercise), but since a fraction of a man could supply blood only temporarily, the number of men must be rounded up to the nearest integer using the ceiling function.

3.4 The composition of functions

Let g be a function from A to B and f be a function from B to C. Then $f \circ g$, the *composition* of g by f, is the function from A to C that takes every element x in A into $f(g(x))$, which is in C (see the diagram below).

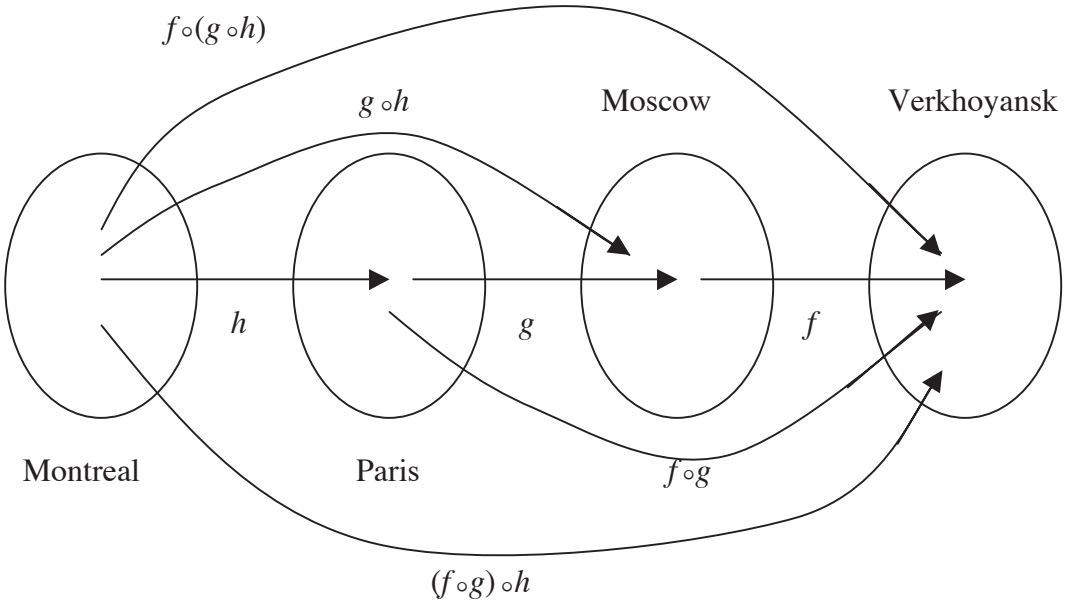


If A is Montreal, B is Paris and C is Moscow, g an Air Canada flight from Montreal to Paris and f an Air France flight from Paris to Moscow, then $f \circ g$ is a flight from Montreal to Moscow with a stopover in Paris.

Is it always true that $f \circ g = g \circ f$? Well, in the above example, $g \circ f$ isn't even defined: when you've applied f you have taken the Air France flight from Paris to Moscow; so you can't apply g, which takes the Air Canada flight from Montreal to Paris, because you're in Moscow instead

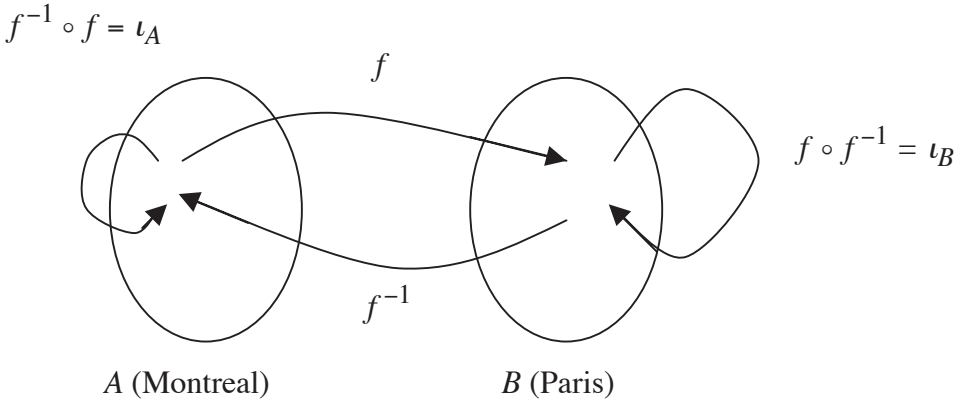
of Montreal! And even if $f \circ g$ and $g \circ f$ are both defined, they are not always equal. If $f : \mathbf{R} \to \mathbf{R}$ and $g : \mathbf{R} \to \mathbf{R}$ are defined by $f(x) = x + 1$ and $g(x) = x^2$, then $(f \circ g)(x) = f(g(x)) = f(x^2) = x^2 + 1$ and $(g \circ f)(x) = g(f(x)) = g(x+1) = (x+1)^2 = x^2 + 2x + 1$.

Is it always true that $(f \circ g) \circ h = f \circ (g \circ h)$? In the diagram below, h is the Air Canada flight from Montreal to Paris, g is the Air France flight from Paris to Moscow, and f is the Aeroflot flight that goes from Moscow to Verkhoyansk - if you're lucky. If you apply $(f \circ g) \circ h$, you fly to Paris and stay there overnight, and the next day you fly to Moscow and transfer directly to the flight to Verkhoyansk. If you apply $f \circ (g \circ h)$, you fly to Paris and transfer directly to the flight to Moscow, stay there overnight, and the next day you fly to Verkhoyansk. You'll probably get more enjoyment from a night in Paris than from a night in Mosocw, but your final destination will be the same: Verkhoyansk, which has the coldest winters in the Northern hemisphere (the average January temperature is -50 degrees Celsius and the record is near -70). With functions, what counts is the final destination; so yes, $(f \circ g) \circ h = f \circ (g \circ h)$.

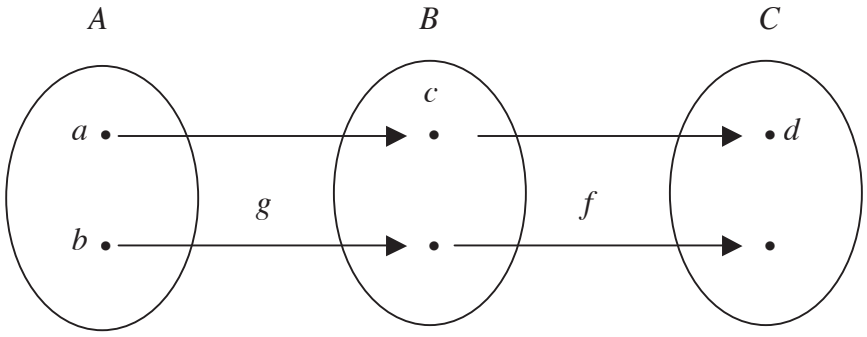


Having introduced the inverse of bijective functions and the composition of two functions, let's combine these two concepts in two different ways.

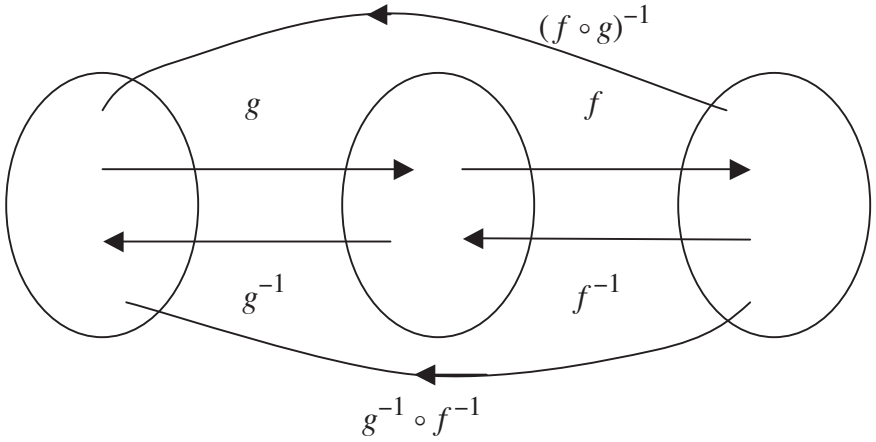
First, suppose that $f : A \to B$ is a bijective function so that it has an inverse $f^{-1} : B \to A$. What is the function $f \circ f^{-1}$? Suppose that f takes you from Montreal to Paris. Then f^{-1} takes you from Paris to Montreal. So $f \circ f^{-1}$ would have to take you from where you are now to where you are now. But where is that, Montreal or Paris? Since you first apply f^{-1}, you would have to be in Paris, so that $f \circ f^{-1}$ takes you from Paris to Paris. In general, $f \circ f^{-1} = \iota_B$ and $f^{-1} \circ f = \iota_A$ (see the diagram below).



Now suppose that g is a bijective function from A to B and f is a bijective function from B to C. Is $f \circ g: A \to C$ necessarily bijective? First we show that since f and g are injective, $f \circ g$ must be injective (see the diagram below). If a and b are two distinct elements of A, then since g is injective, g must take them into two distinct elements of B, and since f is injective, f must take those elements of B into two distinct elements of C, so that $f \circ g$ is indeed injective. From the same diagram, we see that $f \circ g$ is surjective. Let d be any element of C. Then since f is surjective, d has a preimage c in B, and since g is surjective, c has a preimage a in A. Since $f \circ g$ takes a into d, d has a preimage a in A, so that $f \circ g$ is indeed surjective.



Since $f \circ g$ is both injective and surjective, it is bijective; so it has an inverse $(f \circ g)^{-1}$. Is this inverse equal to $f^{-1} \circ g^{-1}$ or $g^{-1} \circ f^{-1}$? From the diagram below, you can see that $(f \circ g)^{-1} = g^{-1} \circ f^{-1}$.



This may seem counter-intuitive, but it shouldn't be. If you do one thing and then a second thing, to restore the original situation you first have to undo the second thing and then the first thing. For example, if you first fly from Montreal to Paris and then from Paris to Moscow, then to get back to Montreal you first have to fly from Moscow back to Paris and then from Paris to Montreal. If you put a briefcase on a table and then put a book on top of the briefcase, to lift them both off the table one at a time you first have to take the book off the briefcase and then take the briefcase off the table. When you get dressed you first put on your socks and then your shoes, and when you get undressed you first take off your shoes and then your socks. I could give other examples of the same type, but that would be too indiscrete even for me.

CHAPTER 4. MATHEMATICAL INDUCTION

Induction is the process of generalizing from observations. Here is a mathematical example of this process. Take the number 41. It's a *prime* – that is, the only positive divisors of 41 are 1 and 41. Now add 2 to 41 and you get 43, another prime. Now add 4 to 43 and you get 47, another prime. Add 6, 8, and then 10, and you get 53, 61, 71, all primes. There were those who, like some programmers who think that their program works for all inputs if it works for the inputs they tested it on, concluded that all the numbers obtained this way are primes. In fact, the first 40 numbers you obtain are indeed primes, but not the 41st. The process of generalizing from observation does not always lead to a correct conclusion, and if your program gives the wrong answer for the input the user enters and he complains to your boss, you could get fired.

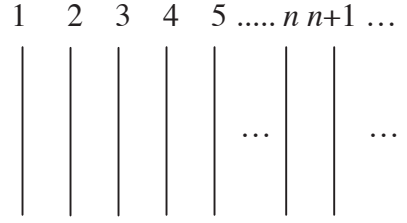
Here is another example. Suppose your teacher gives you a detention and tells you that you have to sit at your desk until you have added all the numbers from 1 to 100, and that if you get the wrong answer, you will get a detention every day for a week. You add the numbers one at a time: starting with 1, you add 2 and get 3, add 3 and get 6, add 4 and get 10, add 5 and get 15, add 6 and get 21, add 7 and get 28, add 8 and get 36, add 9 and get 45, add 10 and get 55, add 11 and get bored; so you look for a shortcut. You divide each current sum by the number n you just added and make a table of values (see the table below). Comparing this quotient with n, you see that it is equal to $(n+1)/2$ for each n from 1 to 10.

n	1	2	3	4	5	6	7	8	9	10
$1 + 2 + \ldots + n$	1	3	6	10	15	21	28	36	45	55
$(1 + 2 + \ldots + n)/n$	1	1.5	2	2.5	3	3.5	4	4.5	5	5.5
$(n + 1)/2$	1	1.5	2	2.5	3	3.5	4	4.5	5	5.5

Generalizing from these observations, you conclude that $1 + 2 + \ldots + n = n(n+1)/2$. If your conjecture is correct, then the sum you have to calculate is just $100 \times 101/2 = 50 \times 101 = 5050$, which is a good deal easier than adding all 100 numbers. But, since you want to be sure to avoid getting more detentions, you ought to prove your conjecture before handing in your answer.

Section 4.1 Standard induction

Mathematical induction is a way to prove that a mathematical proposition is correct. To understand the principle behind mathematical induction, imagine some dominos standing in a row, as in the illustration below. What will happen if you push the leftmost domino to the right? Any child knows the answer: all the dominos will fall to the right.



Now let $p(n)$ be the proposition that domino number n will fall to the right. The proposition $p(1)$ says that the first domino will fall to the right. The proof? You push it. For each integer $n \geq 1$, the implication $p(n) \rightarrow p(n+1)$ says that if domino number n falls to the

right, then domino number $n + 1$ will fall to the right. The proof? If domino number n falls to the right, it will push domino number $n + 1$, making that domino fall to the right as well. The conclusion? All the dominos will fall to the right.

In general, let $p(n)$ be any proposition about a positive integer n. Suppose that $p(1)$ is true, and that for any integer n, $p(n) \rightarrow p(n+1)$. Since $p(1)$ is true and $p(1) \rightarrow p(2)$, $p(2)$ must be true. Since $p(2)$ is true and $p(2) \rightarrow p(3)$, $p(3)$ must be true, and so on. It follows that $p(n)$ is true for every positive integer n. The process of proving that $p(1)$ is true is called the *basic step*. The process of proving that $p(n) \rightarrow p(n+1)$ is true for every positive integer n is called the *induction step*. The two steps together constitute mathematical induction.

As an example, we will prove that $1 + 2 + 3 + \ldots + n = n(n+1)/2$ by mathematical induction.

Basic step: $n = 1$. With $n = 1$, the left side of the equation is 1 and the right side is $1 \times 2/2 = 1$; so the equation holds for $n = 1$.

Induction step: We need to prove that for every positive integer n, if the equation holds for n, then it will hold when n is replaced by $n + 1$. One way to prove the implication $p \rightarrow q$ is the so-called *direct proof*: you assume that p is true and you deduce that q is true. In this case, we assume that the equation holds for n (the *induction hypothesis*) and that $n \geq 1$, and we deduce that the equation holds when n is replaced by $n + 1$. Suppose that $n \geq 1$ and that

$$1 + 2 + 3 + \ldots + n = n(n+1)/2.$$

Required to prove: $1 + 2 + 3 + \ldots + n + (n+1) = (n+1)(n+2)/2$.

By the induction hypothesis, we can replace $1 + 2 + 3 + \ldots + n$ in the left side of the equation by $n(n+1)/2$; the left side then becomes $n(n+1)/2 + (n+1)$. Taking $(n+1)/2$ as a common factor, we get $[(n+1)/2](n+2)$, which is equal to the right side of the equation. By the principle of mathematical induction, the equation holds for every positive integer n, but since that kind of conclusion holds for every induction proof, you don't need to write it. Just write QED, which is a pedantic way of saying "end of proof".

The basic step isn't always $n = 1$. It could be any integer, just as the numerical labels on the dominos in the above diagram could start with 1 or with 0 or with any other integer. In the following example, which will be useful in a later chapter, we will prove that $2^n \geq n$ for any integer $n \geq 0$. This example will show why it is necessary to assume, in addition to the induction hypothesis, that n is at least as big as the number used for the basic step.

Basic step: $n = 0$. With $n = 0$, the left side of the inequality is 1, the right side is 0 and $1 \geq 0$,

Induction step. Suppose that $n \geq 0$ and that $2^n \geq n$. Required to prove: $2^{n+1} \geq n+1$. Since the right side of that new inequality is n plus something, and the induction hypothesis states that $2^n \geq n$, it would be useful to express the left side, which is 2^{n+1}, as 2^n + something. Well, 2^{n+1} is two times 2^n; so it's $2^n + 2^n$, and you need to prove that $2^n + 2^n \geq n + 1$. Now the

induction hypothesis states that $2^n \geq n$ and **since $n \geq 0$** (that other assumption) you can conclude that $2^n \geq 1$. Adding those two inequalities, you get $2^n + 2^n \geq n + 1$, QED.

As an exercise, try to prove by induction that that for any positive integer n, $n(n+1)(n+2)$ is a multiple of 6.

One of the criticisms that is sometimes made of mathematical induction is that it uses circular reasoning: you're assuming what you're trying to prove. Here is an example of circular reasoning that occurs rather often in the real world. John has an enemy who goes around saying, "John is a scoundrel (or some other, less printable name). When he says he isn't a scoundrel, he's lying. All liars are scoundrels. Therefore, John is a scoundrel." In this case it is easy to see the flaw in the logic, but if you dare to point it out to the malicious gossip, he will go around saying nasty things about you! The enemies of mathematical induction claim that you're assuming that $p(n)$ is true for all n in order to prove that $p(n)$ is true for all n. In fact, you're assuming that $p(n)$ is true in order to prove that $p(n)$ implies $p(n+1)$; so the claim of circularity is false.

Another, more legitimate criticism of mathematical induction is that it can't give you anything new; it just lets you prove things that you have to derive by other means. For example, not too many people could guess at the formula for $1 + 2 + \ldots + n$ by examining the first few values, and in fact the first derivation of this formula, or rather of the value of $1 + 2 + \ldots + 100$, was not obtained using mathematical induction.

The great mathematician Karl Friedrich Gauss obtained a great many results in mathematics, but the one of which he was the most proud was the one he discovered when he was only ten years old. According to legend, his whole class was given a detention and required to calculate $1 + 2 + 3 + \ldots + 100$. All the other pupils worked for the better part of an hour and they all got different answers, all of them wrong. Little Karl got the right answer in only two minutes, handed it in to the teacher, and then ran out of the classroom as fast as he could before his classmates could catch him and beat him up. Here is his calculation. $1 + 100 = 101$, $2 + 99 = 101$, $3 + 98 = 101$, … , $50 + 51 = 101$. Adding up these 50 equations, he got $1 + 2 + 3 + \ldots + 99 + 100 = 50 \times 101 = 5050$.

This method can be generalized to obtain the formula for $1 + 2 + \ldots + n$.
Let $S = 1 + 2 + \ldots + (n\text{-}1) + n$. Writing the same list of numbers backwards, we get
$S = n + (n\text{-}1) + \ldots + 2 + 1$. Adding these two equations, we get
$2S = (n+1) + (n+1) + \ldots + (n+1) + (n+1) = n(n+1)$ because there are n copies of $n + 1$.
Dividing by 2, we get $S = n(n+1)/2$.

When I was considerably older than 10 (more than 3 times as old, I admit to my shame), I found another proof of the same formula. The proof is certainly not original, but the story behind it is. I taught mathematics for two years at the University of Bordeaux, and during my stay in France I noticed that when French people enter a room, each Frenchman who enters the room shakes hands with every other Frenchman who is already in the room. Now suppose that $n + 1$ Frenchman enter a room one at a time. The second Frenchman to enter the room shakes hands with 1 other Frenchman, the first one to enter. The third Frenchman shakes hands with 2 others, the fourth with 3 others and so on until the n+1st Frenchman shakes hands with n others. The total number of handshakes is $1 + 2 + 3 + \ldots + n$. Now let's count the handshakes in a different way. Each of the $n + 1$ Frenchmen shakes hands with n others, but the product $n(n+1)$ counts

each handshake twice (Pierre with Paul and Paul with Pierre); so the total number of handshakes is $n(n+1)/2$.

Before returning to Canada, I took a trip to a few countries and decided to try the same experiment in each of them. The British refused to shake hands because they were afraid of getting germs. The Americans too were reluctant to do so, but they agreed when I offered them enough money. The Germans were very co-operative: they organized a tournament. The Russians would have liked to do the same thing, but they were too drunk; so I conducted a statistical experiment with them: what is the probability that two Russians will succeed in shaking hands if each of them sees two images of the other one? Back in Canada, all went well until two hockey players found themselves face to face, and instead of shaking hands they came out fighting. I separated them, and then the whole crowd jumped on me to punish me for having spoiled the pleasure they were getting from watching the fight. I managed to escape, but I decided to stop the experiment. It was too dangerous.

Getting serious (for the moment), there are conjectures for which mathematical induction is the best proof. If you don't believe me, try to prove that $2^n \geq n$ for any integer $n \geq 0$ without using mathematical induction. I guarantee that there will be an induction hidden behind whatever proof you come up with.

Returning to the first problem of this section, would it have been necessary to test all the numbers $41, 41 + 2 = 43, 43 + 4 = 47$, etc. to discover that one of them wasn't a prime? The first number in this sequence is 41. The second one is $41 + 2$. The third one is $41 + 2 + 4$. The fourth one is $41 + 2 + 4 + 6$. Examining these sums, we can see that the nth one is $41 + 2(1+2+3+\ldots+(n-1))$. Now we have already seen several proofs of the equation $1 + 2 + 3 + \ldots + n = n(n+1)/2$. Substituting $n - 1$ for n in this equation, we find that $1 + 2 + 3 + \ldots + (n-1) = n(n-1)/2$. Substituting that formula into the one for the nth term in the sequence of so-called primes, we get $41 + n(n-1)$. If $n = 41$, we get $41 + 41\times40 = 41(1+40) = 41\times41$, which is not a prime. Those who thought that their sequence of numbers consists entirely of primes could have figured out that they were wrong - if only they had been as smart as Gauss was when he was ten years old!

Section 4.2 Generalized induction

With standard induction, you go from a smaller number n to a bigger number $n + 1$. There are some problems for which you have to go from a smaller number n to a bigger number that isn't $n + 1$. In that case you need to use a generalized form of induction where the induction step is proving that if $p(m)$ is true for every $m < n$, then $p(n)$ is also true. Look at the dominos at the beginning of section 4.1 and imagine that every domino is heavier than its neighbour to the left so that it takes the combined weight of all the dominos to its left to knock it over. If you push the first domino to the right, it will knock over the second one. The combined weight of the first and second dominos will knock over the third one. Then the combined weight of the first three dominos will knock over the fourth one, and so on, so that all the dominos will fall to the right.

Here is an example of a theorem that needs generalized induction to prove: **every positive integer is either 1, a prime or the product of primes**. For example, 24 is a product of primes: $24 = 2\times2\times2\times3$.

Basic step: $n = 1$. That was one of the choices.

Induction step: Suppose that $n > 1$ and that every positive integer $m < n$ is either 1, a prime or a product of primes. Required to prove: n is either a prime or a product of primes (we can eliminate the possibility that $n = 1$ because we already supposed that $n > 1$). If n is a prime, we are done: that was one of the choices. Suppose that n is not a prime. Then, by definition, n has a positive divisor d that is neither 1 nor n; so $1 < d < n$. By the induction hypothesis, d is either a prime or a product of primes. Let $q = n/d$ be the quotient of this division. Since $1 < d$, $q < n$, and since $d < n$, $q > 1$. By the induction hypothesis, q too is either a prime or a product of primes. Since $q = n/d$, $n = dq$. Then n is the product of primes: all the prime factors of d and all the prime factors of q (QED). For example, let $n = 24$. If $d = 2$, then $q = 12$. Now 2 is a prime and $12 = 2\times2\times3$; so $24 = 2\times(2\times2\times3)$, a product of primes. If $d = 4 = 2\times2$, then $q = 6 = 2\times3$ and $24 = (2\times2)\times(2\times3)$, a product of primes.

Just as with standard induction, the basic step doesn't have to be $n = 1$, and, unlike standard induction, the basic step doesn't have to consist of a single number: you may have to push over a few dominos by hand to get them to knock over the rest of them. For example, consider the famous *Fibonacci numbers*, defined as follows:

$$f(0) = 0, f(1) = 1; f(n) = f(n\text{-}1) + f(n\text{-}2) \text{ if } n \geq 2.$$

Note that the formula for $f(n)$ contains terms of the form f(a number smaller than n). This is called a *recursive definition* of a function; this topic will be studied in more detail in Section 7.1. To study the properties of a recursively defined function you have to start by constructing a table of the first few values of the function (see the table below).

n	0	1	2	3	4	5	6	7	8	9	10	11	12
$f(n)$	0	1	1	2	3	5	8	13	21	34	55	89	144

By examining the table, you can observe that for every $n \geq 2$, $f(n+1) \geq (3/2)\times f(n)$, and since $f(2) = 1$, it would be reasonable to conjecture that $f(n) \geq (3/2)^{n-2}$ for every integer $n \geq 2$. Since the formula for $f(n)$ contains $f(n\text{-}2)$ as well as $f(n\text{-}1)$, you can't prove that conjecture by standard induction; you need to use generalized induction. Since the conjecture supposes that $n \geq 2$, the basic step has to include $n = 2$, but it can't consist only of $n = 2$. Suppose you try to start the induction step with $n = 3$. The formula for $f(3)$ contains $n = 1$ and we're assuming that $n \geq 2$; so you need to include $n = 3$ in the basic step and start the induction step with $n = 4$.

Basic step: $n = 2$ and $n = 3$. With $n = 2$, $f(n) = f(2) = 1$ and $(3/2)^{n-2} = (3/2)^0 = 1$, and $1 \geq 1$. With $n = 3$, $f(n) = f(3) = 2$ and $(3/2)^{n-2} = (3/2)^1 = 1.5$, and $2 \geq 1.5$.

Induction step: Suppose that $n \geq 4$ and that $f(m) \geq (3/2)^{m-2}$ for every integer m such that $2 \leq m < n$ (we have assumed that $m \geq 2$ because that's where the conjectured inequality starts – we push over dominos 2 and 3 by hand; so we can't suppose that the weight of dominos 0 and 1 will help to push the other dominos over). Required to prove: $f(n) \geq (3/2)^{n-2}$.

From the formula, $f(n) = f(n\text{-}1) + f(n\text{-}2)$, and we can use the induction hypothesis to get inequalities for $f(n\text{-}1)$ and $f(n\text{-}2)$. Since $n \geq 4$, $2 \leq n\text{-}1 < n$ and $2 \leq n - 2 < n$; so the induction

hypothesis applies to n - 1 and n - 2. Specializing the induction hypothesis to n - 1 and n - 2, we find that $f(n\text{-}1) \geq (3/2)^{n-3}$ and $f(n\text{-}2) \geq (3/2)^{n-4}$. Adding these two inequalities, we find that

$$f(n) = f(n\text{-}1) + f(n\text{-}2) \geq (3/2)^{n-3} + (3/2)^{n-4}.$$

The two terms on the right side of the above inequality have a common factor, which we take out and get $(3/2)^{n-4}((3/2)+1)$. We know, therefore, that $f(n) \geq (3/2)^{n-4}((3/2)+1)$ and we want to prove that $f(n) \geq (3/2)^{n-2}$. Now $(3/2)^{n-2}$ also contains a factor of $(3/2)^{n-4}$; so we take that one out too: $(3/2)^{n-2} = (3/2)^{n-4}(3/2)^2$. Now all we have to prove is that

$$(3/2)^{n-4}((3/2)+1) \geq (3/2)^{n-4}(3/2)^2;$$

since $f(n) \geq (3/2)^{n-4}((3/2)+1)$, this will prove that $f(n) \geq (3/2)^{n-4}(3/2)^2$ as required. To prove that $(3/2)^{n-4}((3/2)+1) \geq (3/2)^{n-4}(3/2)^2$ it is sufficient to prove that $((3/2)+1) \geq (3/2)^2$. The left side of that inequality is 2.5 and the right side is 2.25; so that inequality holds and the conjecture is proved, QED.

Can we do any better than $(3/2)^{n-2}$? Well, the only part of the induction step that used the particular value of 3/2 was the inequality $((3/2)+1) \geq (3/2)^2$. What is the biggest number that we can substitute for 3/2 and still have that inequality hold? That's the number x that satisfies the equation $x+1 = x^2$, derived from the inequality by replacing 3/2 by x and $\geq$ by $=$. This is a quadratic equation and its two roots are $(1+\sqrt{5})/2$ and $(1-\sqrt{5})/2$. We choose the bigger root $(1+\sqrt{5})/2$, which is between 1.61 and 1.62. This number was called the Golden Ratio by the ancient Greeks because they thought that it was the most pleasing ratio of the width to the height of a building, and they built a lot of buildings to that specification. We can now substitute $(1+\sqrt{5})/2$ for 3/2 everywhere in the proof and we will have proved that $f(n) \geq \left((1+\sqrt{5})/2\right)^{n-2}$ for every integer $n \geq 2$.

As an exercise, try to prove by generalized induction that if the price of mailing a letter is at least 12 cents, you can pay the exact price using only 3-cent stamps and 7-cent stamps. And then try to generalize this assertion by proving that if $m > 0$ and $n > 0$ have no positive divisors in common except 1 and the price is at least $(m\text{-}1)(n\text{-}1)$ cents, then you can pay the exact price using only m-cent stamps and n-cent stamps, but you can't pay exactly $(m\text{-}1)(n\text{-}1) - 1$ cents.

Section 4.3 Proving that the smallest exception isn't

Another form of mathematical induction uses the fact that **if $p(n)$ isn't true for every positive integer n, then there must be a smallest positive integer n for which $p(n)$ is false**. You prove that for every exception there must be a smaller one; this contradiction proves that there can be no exceptions. To illustrate this method of proof we return to the fact (which is a fact because we proved it in the preceding section) that every positive integer is either 1, a prime or a product of primes. What we didn't yet prove is that there is only one way to express a positive integer as a product of primes. Of course, you may say, there is more than one way; after all, $6 = 2\times3 = 3\times2$. But suppose we insist that the prime factors be written in increasing

order. Does this guarantee that there is only one way to decompose a positive integer into prime factors?

There once was a lunatic who thought otherwise. He had learned in school that a kilogram is 1000 grams and that a kilometer is 1000 meters. One day he read that a kilobyte is 2^{10} bytes and concluded that $2^{10} = 1000$. Since he knew that 1000 is divisible by 5, he decided that there were two distinct ways to decompose 1000 into prime factors. He bought a program that decomposes a positive integer into prime factors, entered 1000 into the program, and got $2^3 5^3$; so he concluded that $2^{10} = 2^3 5^3$. He decided that it would be more impressive if he found a smaller number that could be decomposed into prime factors in two different ways; so he set about trying to find one. Noticing that each of the factorizations of 1000 has 3 factors of 2, he canceled them from both of these factorizations and got $2^7 = 5^3$. Now the smallest factor in each of these factorizations was different (2 in one case and 5 in the other), but this did not dissuade him from seeking to diminish the number further. He replaced the 5 in the right factorization by 2, subtracted the resulting number from both sides of the equation and got $2^7 - 2 \times 5^2 = 5^3 - 2 \times 5^2$. The left side of this equation has a common factor 2 and the right side has a common factor 5^2; he took out each of these common factors and got $2(2^6 - 5^2) = 5^2(5 - 2)$. He then used his computer to evaluate the other factor on both sides of the equation and got $2 \times 39 = 5^2 \times 3$. He entered 39 and 3 into his prime factorization program and got $2 \times 3 \times 13 = 3 \times 5^2$, a number smaller than $2^7 = 5^3$ with two distinct decompositions into prime factors. Dizzy with success, he continued this process until he had proved that 2 = 1. He substracted 1 from each side to get 1 = 0 and then multiplied each side by x and concluded that $x = 0$ for every real number x. He wrote up his result in an article and submitted it to a journal for publication.

The referee rejected the article but did not ignore it. He realized that the lunatic's construction could be generalized to obtain a simpler proof of the unicity of prime factorization than any he had seen in the literature. Being a scoundrel, he wrote up his result as an article and submitted it for publication without giving any credit to the lunatic. Here is his article.

A SIMPLE PROOF OF THE UNICITY OF PRIME FACTORIZATION
by Samuel Oliver Brown

It is a well-known fact that **any positive integer can be factorized into prime factors in exactly one way if we insist that the factors be written in increasing order**. Here is a proof of this theorem that is simpler than any of the others in the literature.

It can be easily proved by generalized induction that any positive integer can be written as a product of primes: none of them if the number is 1, one of them if it's a prime and more than one if it's composite. We now prove that this factorization is unique. If there were an exception, then let n be the smallest positive integer with two distinct prime factorizations. We will show that there must be a positive integer smaller than n that also has two distinct prime factorizations.

We first note that n cannot be 1, because any other factorization of 1 would have to be a prime, which is bigger than 1, or the product of primes, which is also bigger than 1. We also note that n cannot be a prime, because n cannot be expressed as two different primes, and the product

of primes is not a prime. Therefore, n must be composite, and any decomposition of n must have at least two prime factors.

Let $p_1p_2...p_i$ and $q_1q_2...q_j$ be two distinct prime factorizations of n, where $p_1 \le p_2 \le ... \le p_i$ and $q_1 \le q_2 \le ... \le q_j$. There are two cases to consider.

Case 1: $p_1 = q_1$. In this case, we have the two distinct prime factorizations $p_2...p_i$ and $q_2...q_j$ of the number $n / p_1 < n$.

Case 2: $p_1 \neq q_1$. In this case, without loss of generality we can assume that $p_1 < q_1$; otherwise we relabel the factors by exchanging the letters p and q. Now let m be the number $p_1 q_2...q_j$ obtained by replacing q_1 by p_1 in the factorization $q_1q_2...q_j$ of n. Then, since $p_1 < q_1$, $m < n$, and since $m > 0$, $n - m$ is a positive integer which is less than n. We prove that $n - m$ also has two distinct prime factorizations. Subtracting the factorization of m from each of the two distinct factorizations of n, we obtain the equation

$$p_1p_2...p_i - p_1 q_2...q_j = q_1q_2...q_j - p_1 q_2...q_j .$$

Now the two terms on the left side of this equation have a common factor p_1; so it can be written as $p_1(p_2...p_i - q_2...q_j)$. The number $p_2...p_i - q_2...q_j$ is a positive integer $(n-m)/ p_1$; so it can be factorized into primes. When p_1 is appended as a prime factor, we have a factorization of $n - m$ that contains the prime factor p_1.

The two terms on the right side of the same equation have a common factor $q_2...q_j$; so it can be written as $(q_1 - p_1)(q_2...q_j)$. The number $q_1 - p_1$ is a positive integer because $p_1 < q_1$; so it can be factorized into primes. None of these primes can be p_1 because p_1 does not divide $q_1 - p_1$; otherwise q_1 would be the sum of two multiples of p_1 and, therefore also a multiple of p_1, which is impossible because q_1 is a prime which is greater than p_1. Also, none of the factors $q_2,...,q_j$ can be equal to p_1 because $p_1 < q_1 \le q_2 \le ... \le q_j$. Therefore, when the factors $q_2,...,q_j$ are appended to the prime factorization of $q_1 - p_1$ we get a factorization of $n - m$ that does not contain the prime factor p_1.

We thus have two distinct prime factorizations of $n - m$, one with p_1 and the other without p_1. This proves that there is no smallest exception to the unicity of prime factorization and, therefore, no exception, QED.

This article was accepted for publication; so the mathematical community got a simpler proof of the theorem thanks to the existence of lunatics and scoundrels in the world. Actually, I discovered this proof, and it was simpler than any of the proofs in the one number theory book I had read. Not being a lunatic, however, I didn't submit my proof for publication, which turned out to be very fortunate because I found the same proof in the next number theory book I read!