Chapter 1

Mathematical argument

Basic mathematical notation and methods of argument are introduced, including a review of the important principle of mathematical induction.

1.1 Logical notation

We shall use some informal logical notation in order to stop our mathematical statements getting out of hand. For statements (or assertions) A and B, we shall commonly use abbreviations like:

- A & B for (A and B), the conjunction of A and B,
- $A \Rightarrow B$ for (A implies B), which means (if A then B), and so is automatically true when A is false,
- $A \iff B$ to mean (A iff B), which abbreviates (A if and only if B), and expresses that A implies B and B implies A.

We shall also make statements by forming disjunctions (A or B), with the self-evident meaning, and negations (not A), sometimes written $\neg A$, which is true iff A is false. There is a tradition to write for instance $7 \not< 5$ instead of $\neg(7 < 5)$, which reflects what we generally say: "7 is not less than 5" rather than "not 7 is less than 5."

The statements may contain variables (or unknowns, or place-holders), as in

$$(x \le 3) \ \&\ (y \le 7)$$

which is true when the variables x and y over integers stand for integers less than or equal to 3 and 7 respectively, and false otherwise. A statement like $P(x, y)$, which involves variables x, y, is called a predicate (or property, or relation, or condition) and it only becomes true or false when the pair x, y stand for particular things.

We use logical quantifiers $\exists$, read "there exists", and $\forall$, read " for all". Then you can read assertions like

$$\exists x.\ P(x)$$

as abbreviating "for some x, $P(x)$" or "there exists x such that $P(x)$", and

$$\forall x.\ P(x)$$

as abbreviating " for all x, $P(x)$" or "for any x, $P(x)$". The statement

$$\exists x, y, \cdots, z.\ P(x, y, \cdots, z)$$

abbreviates

$$\exists x \exists y \cdots \exists z.\ P(x, y, \cdots, z),$$

and

$$\forall x, y, \cdots, z.\ P(x, y, \cdots, z)$$

abbreviates

$$\forall x \forall y \cdots \forall z.\ P(x, y, \cdots, z).$$

Sometimes you'll see a range for the quantification given explicitly as in $\forall x\,(0 < x \leq k).\ P(x)$. Later, we often wish to specify a set X over which a quantified variable ranges. Then one writes $\forall x \in X.\ P(x)$—read "for all x in X, $P(x)$"— instead of $\forall x.\ x \in X \Rightarrow P(x)$, and $\exists x \in X.\ P(x)$ instead of $\exists x.\ x \in X\ \&\ P(x)$.

There is another useful notation associated with quantifiers. Occasionally one wants to say not just that there exists some x satisfying a property $P(x)$ but also that x is the *unique* object satisfying $P(x)$. It is traditional to write

$$\exists! x.\ P(x)$$

as an abbreviation for

$$(\exists x.\ P(x))\ \&\ (\forall y, z.\ P(y)\ \&\ P(z) \Rightarrow y = z)$$

which means that there is some x satisfying the property $P(x)$ and also that if any y, z both satisfy the property they are equal. This expresses that there exists a unique x satisfying $P(x)$.

Occasionally, and largely for abbreviation, we will write *e.g.*, $X =_{def} E$ to mean that X is defined to be E. Similarly, we will sometimes use *e.g.*, $P(x) \Leftrightarrow_{def} A$ in defining a property in terms of an expression A.

Exercise 1.1 What is the difference between $\forall x.(\exists y.P(x,y))$ and $\exists y.(\forall x.P(x,y))$? [You might like to consider $P(x,y)$ to mean "x loves y."] □

1.2 Patterns of proof

There is no magic formula for discovering proofs in anything but the simplest contexts. However often the initial understanding of a problem suggests a general pattern of proof. Patterns of proof like those below appear frequently, often locally as ingredients of a bigger proof, and are often amongst the first things to try. It is perhaps best to tackle this section fairly quickly at a first reading, and revisit it later when you have had more experience in doing proofs.

1.2.1 Chains of implications

To prove an $A \Rightarrow B$ it suffices to show that starting from the assumption A one can prove B. Often a proof of $A \Rightarrow B$ factors into a chain of implications, each one a manageable step:

$$\begin{aligned} A &\Rightarrow A_1 \\ &\Rightarrow \cdots \\ &\Rightarrow A_n \\ &\Rightarrow B\ . \end{aligned}$$

This really stands for

$$A \Rightarrow A_1,\ A_1 \Rightarrow A_2, \cdots, A_n \Rightarrow B\ .$$

One can just as well write "Therefore" (or "$\because$") between the different lines, and this is preferable if the assertions $A_1, \cdots, A_n$ are large.

A bi-implication $A \iff B$ stands for both $A \Rightarrow B$ and $B \Rightarrow A$. One often sees a proof of $A \iff B$ broken down into a chain

$$\begin{aligned} A &\iff A_1 \\ &\iff \cdots \\ &\iff A_n \\ &\iff B\ . \end{aligned}$$

A common mistake is not to check the equivalence in the backwards direction, so that while the implication A_{i-1} to A_i is obvious enough, the reverse implication from A_i to A_{i-1} is unclear, in which case an explanation is needed, or even untrue. Remember, while a proof of $A \iff B$ very often does factor into a proof of $A \Rightarrow B$ and $B \Rightarrow A$, the proof route taken in showing $B \Rightarrow A$ needn't be the reverse of that taken in showing $A \Rightarrow B$.

1.2.2 Proof by contradiction

The method of proof by contradiction was known to the ancients and carries the Latin name *reductio ad absurdum.* Sometimes the only known proof of an assertion A is by contradiction. In a proof by contradiction, to show A, one shows that assuming $\neg A$ leads to a conclusion which is false. We have thus shown $\neg A$ is not the case, so A.

That $\sqrt{2}$ is irrational was a dreadful secret known to the followers of Pythagoras. The proof is a proof by contradiction: Assume, with the aim of obtaining a contradiction, that $\sqrt{2}$ is rational, *i.e.* $\sqrt{2} = a/b$ where a and b are integers with no common prime factors. Then, $2b^2 = a^2$. Therefore 2 divides a, so $a = 2a_0$ for some integer a_0. But then $b^2 = 2a_0^2$. So 2 also divides b—a contradiction.

Beware: a “beginner’s mistake” is an infatuation with proof by contradiction, leading to its use even when a direct proof is at least as easy.

Exercise 1.2 Show for any integer m that $\sqrt{m}$ is rational iff m is a square, *i.e.* $m = a^2$ for some integer a.[1] □

Sometimes one shows $A \Rightarrow B$ by proving its *contrapositive* $\neg B \Rightarrow \neg A$. Showing the soundness of such an argument invokes proof by contradiction. To see that $A \Rightarrow B$ follows from the contrapositive, assume we have $\neg B \Rightarrow \neg A$. We want to show $A \Rightarrow B$. So assume A. Now we use proof by contradiction to deduce B as follows. Assume $\neg B$. Then from $\neg B \Rightarrow \neg A$ we derive $\neg A$. But now we have both A and $\neg A$—a contradiction. Hence B.

1.2.3 Argument by cases

The truth of $(A_1$ or $\cdots$ or $A_k) \Rightarrow C$ certainly requires the truth of $A_1 \Rightarrow C, \ldots,$ and $A_k \Rightarrow C$. Accordingly, most often a proof of $(A_1$ or $\cdots$ or $A_k) \Rightarrow C$ breaks down into k cases, showing $A_1 \Rightarrow C, \ldots,$ and $A_k \Rightarrow C$. An example:

Proposition For all nonnegative integers $a > b$ the difference of squares $a^2 - b^2$ does not give a remainder of 2 when divided by 4.

Proof. We observe that

$$a^2 - b^2 = (a + b)(a - b) \ .$$

Either (i) a and b are both even, (ii) a and b are both odd, or (iii) one of a, b is even and the other odd.[2] We show that in all cases $a^2 - b^2$ does not give remainder 2 on division by 4.

Case (i): both a and b are even. In this case $a^2 - b^2$ is the product of two even numbers so divisible by 4, giving a remainder 0 and not 2.

Case (ii): both a and b are odd. Again $a^2 - b^2$ is the product of two even numbers so divisible by 4.

Case(iii): one of a and b is even and one odd. In this case both $a + b$ and $a - b$ are odd numbers. Their product which equals $a^2 - b^2$ is also odd. If $a^2 - b^2$ gave remainder 2 on division by 4 it would be even—a contradiction. □

1.2.4 Existential properties

To prove $\exists x.\ A(x)$ it suffices to exhibit an object a such that $A(a)$. Often proofs of existentially quantified statements do have this form. We’ll see examples where this is not the case however (as in showing the existence of transcendental numbers). For example, sometimes one can show $\exists x.\ A(x)$ by obtaining a contradiction from its negation *viz.* $\forall x.\ \neg A(x)$ and this need not exhibit an explicit object a such that $A(a)$.

Exercise 1.3 Suppose 99 passengers are assigned to one of two flights, one to Almeria and one to Barcelona. Show one of the flights has at least 50 passengers assigned to it. (Which flight is it?) □

[1] Plato reported that the irrationality of $\sqrt{p}$ was known for primes p up to 17, which suggests that the ancient Greeks didn’t have the general argument. But they didn’t have the benefit of algebra to abbreviate their proofs.

[2] In checking the basic facts about even and odd numbers used in this proof it’s helpful to remember that an even number is one of the form $2k$, for a nonnegative integer k, and that an odd number has the form $2k + 1$, for a nonnegative integer k.

1.2.5 Universal properties

The simplest conceivable way to prove $\forall x.\ A(x)$ is to let x be an arbitrary element and then show $A(x)$. But this only works in the easiest of cases. More often than not the proof requires a knowledge of how the elements x are built up, and this is captured by induction principles. The most well-known such principle is *mathematical induction*, which deserves a section to itself.

1.3 Mathematical induction

We review mathematical induction and some of its applications. Mathematical induction is an important proof technique for establishing a property holds of all nonnegative integers 0, 1, 2, $\ldots$, n, $\ldots$

The principle of mathematical induction
To prove a property $A(x)$ for all nonnegative integers x it suffices to show

- the *basis* $A(0)$, and
- the *induction step*, that $A(n) \Rightarrow A(n+1)$, for all nonnegative integers n.

(The property $A(x)$ is called the *induction hypothesis*.)

A simple example of mathematical induction:

Proposition 1.4 *For all nonnegative integers n*

$$0 + 1 + 2 + 3 + \cdots + n = \frac{n(n+1)}{2} \ .$$

Proof. By mathematical induction, taking as induction hypothesis the property $P(n)$ of a nonnegative integer n that

$$0 + 1 + 2 + 3 + \cdots + n = \frac{n(n+1)}{2} \ .$$

Basis: The sum of the series consisting of just 0 is clearly 0. Also $0(0+1)/2 = 0$. Hence we have established the basis of the induction $P(0)$.

Induction step: Assume $P(n)$ for a nonnegative integer n. Then adding $(n+1)$ to both sides of the corresponding equation yields

$$0 + 1 + 2 + 3 + \cdots + n + (n+1) = \frac{n(n+1)}{2} + (n+1) \ .$$

Now, by simple algebraic manipulation we derive

$$\frac{n(n+1)}{2} + (n+1) = \frac{(n+1)((n+1)+1)}{2} \ .$$

Thus

$$0 + 1 + 2 + 3 + \cdots + n + (n+1) = \frac{(n+1)((n+1)+1)}{2} \ ,$$

and we have established $P(n+1)$. Therefore $P(n) \Rightarrow P(n+1)$, and we have shown the induction step.

By mathematical induction we conclude that $P(n)$ is true for all nonnegative integers. □

The proof above is perhaps overly pedantic, but it does emphasise that, especially in the beginning, it is very important to state the induction hypothesis clearly, and spell out the basis and induction step of proofs by mathematical induction.

There's another well-known way to prove Proposition 1.4 spotted by Gauss in kindergarten. Asked to sum together all numbers from 1 to 100 he didn't go away—presumably the goal in setting the exercise, but replied 5,050, having observed that by aligning two copies of the sum, one in reverse order,

$$\begin{array}{ccccccccc} 1 & + & 2 & + & \cdots & + & 99 & + & 100 \\ 100 & + & 99 & + & \cdots & + & 2 & + & 1 \end{array}$$

each column—and there are 100 of them—summed to 101; so that twice the required sum is 100×101.

Exercise 1.5 Prove that 7 divides $2^{4n+2} + 3^{2n+1}$ for all nonnegative integers n.

We can also use mathematical induction to establish a definition over all the nonnegative integers.

Definition by mathematical induction
To define a function f on all nonnegative integers x it suffices to define

- $f(0)$, the function on 0, and
- $f(n+1)$ in terms of $f(n)$, for all nonnegative integers n.

For example, the factorial function $n! = 1 \cdot 2 \cdots (n-1) \cdot n$ can be defined by the mathematical induction

$$\begin{aligned} &0! = 1 \\ &(n+1)! = n! \cdot (n+1) \ . \end{aligned}$$

Given a series $x_0, x_1, \ldots, x_i, \ldots$ we can define the sum

$$\Sigma_{i=0}^{n} x_i = x_0 + x_1 + \cdots + x_n$$

by mathematical induction:[3]

$$\begin{aligned} &\Sigma_{i=0}^{0} x_i = x_0 \\ &\Sigma_{i=0}^{n+1} x_i = (\Sigma_{i=0}^{n} x_i) + x_{n+1} \ . \end{aligned}$$

Exercise 1.6 Let a and d be real numbers. Prove by mathematical induction that for all nonnegative integers n that

$$a + (a+d) + (a+2d) + \cdots + (a + (n-1)d) + (a+nd) = \frac{(n+1)(2a+nd)}{2} \ .$$

□

Exercise 1.7 Prove by mathematical induction that for all nonnegative integers n that

$$1 + 1/2 + 1/4 + 1/8 + \cdots + 1/2^n = 2 - \frac{1}{2^n} \ .$$

Let a and r be real numbers. Prove by mathematical induction that for all nonnegative integers n that

$$a + a \cdot r + a \cdot r^2 + \cdots + a \cdot r^n = \frac{a(1 - r^{n+1})}{1-r} \ .$$

□

Exercise 1.8 The number of r combinations from $n \geq r$ elements

$${}^{n}C_r =_{def} \frac{n!}{(n-r)!r!}$$

expresses the number of ways of choosing r things from n elements.
(i) Show that

$$\begin{aligned} &{}^{0}C_0 = 1 \\ &{}^{n+1}C_r = \frac{(n+1)}{r} \cdot {}^{n}C_{r-1} \end{aligned}$$

for all nonnegative integers r, n with $r \leq n+1$.

[3] In the exercises it is recommended that you work with the more informal notation $x_0 + x_1 + \cdots + x_n$, and assume obvious properties such as that the sum remains the same under rearrangement of its summands. Such an ‘obvious’ property can be harder to spot, justify and handle with the more formal notation $\Sigma_{i=0}^{n} x_i$.

(ii) Show that

$$^{n+1}C_r =^n C_{r-1} +^n C_r$$

for all nonnegative integers r, n with $0 < r \leq n$.
(iii) Prove by mathematical induction that

$$^nC_0 +^n C_1 + \cdots +^n C_r + \cdots +^n C_n = 2^n$$

for all nonnegative integers n.[4] □

Tower of Hanoi

The tower of Hanoi is a puzzle invented by E. Lucas in 1883. The puzzle starts with a stack of discs arranged from largest on the bottom to smallest on top placed on a peg, together with two empty pegs. The puzzle asks for a method, comprising a sequence of moves, to transfer the stack from one peg to another, where moves are only allowed to place smaller discs, one at a time, on top of larger discs. We describe a method, in fact optimal, which requires $2^n - 1$ moves, starting from a stack of n discs.

Write $T(n)$ for the number of moves the method requires starting from a stack of n discs. When $n = 0$ it suffices to make no moves, and $T(0) = 0$. Consider starting from a stack of $n + 1$ discs. Leaving the largest disc unmoved we can use the method for n discs to transfer the stack of n smaller discs to another peg—this requires $T(n)$ moves. Now we can move the largest disc to the remaining empty peg—this requires 1 move. Using the method for n discs again we can put the stack of n smaller discs back on top of the largest disc—this requires a further $T(n)$ moves. We have succeeded in transferring the stack of $n + 1$ discs to another peg. In total the method uses

$$T(n) + 1 + T(n) = 2 \cdot T(n) + 1$$

moves to transfer $n + 1$ discs to a new peg. Hence,

$$\begin{array}{l} T(0) = 0 \\ T(n+1) = 2 \cdot T(n) + 1 \end{array} .$$

Exercise 1.9 Prove by mathematical induction that $T(n) = 2^n - 1$ for all nonnegative integers n. □

[4] From school you probably know more intuitive ways to establish (i) and (ii) by considering the coefficients of powers of x in $(1 + x)^n$; the *binomial theorem* asserts the equality of combinations ^nC_r and coefficients of x^r.