CHAPTER 4

SOME METHODS OF PROOF

In all sciences, general theories usually arise from a number of observations. In the experimental sciences, the validity of the theories can only be tested by carefully devised experiments and by making further observations. In mathematics, however, we seek to justify our theories by giving a logical argument to show they are true. In computer science, too, we must be able to prove that a program will do what we claim it will. In this chapter, we consider two types of statement that arise in mathematics and some methods of proof: *direct* proof, the use of *counter-example,* proof by *contradiction* and the method of proof by *mathematical induct ion.*

Quantifiers

In mathematics, we often claim that a statement is true for *all* members of a given set; in this case, we usually use phrases such as "for all", "for every", or "for any", called universal quantifiers.

Example 4.1 In the following statements, *universal* quantifiers are used.

(a) *For any* real number x, $|x+1|= | x | +1$.
(b) The formula $u_n=n_2+n+41$ gives a prime number, *for all* $n \geq 0$.
(c) $1+2+. . .+n = n(n+1)/2$, *for every* positive integer *n.*

On the other hand, we may claim that we can find *at least one* member of the set for which the statement is true; in this case, phrases such as "we can find a", "there exists a", "for some", called existential quantifiers, are often used.

Example 4.1. (continued) In these statements, *existential* quantifiers are used.

(d) *There exists a* real number x such that $|x|=5$ and $|x|=6$.
(e) The formula $u_n=n^2+n+41$ gives a prime number, *for some integer n.*

Some of these statements may be true and some may be false. Before we try to prove or disprove any of these statements, make quite sure you understand exactly what each is claiming. Compare (b) with (e), for example: to prove that (b) is true, we would need to show that n^2+n+41 is a prime number *whatever non-negative integer value is given to n;* whereas to prove that (e) is true, we need only find *one* value of *n* for which n^2+n+41 is a prime number.

Exercise 4.1. Find the value of n^2+n+41, for n=0,1,.. . ,10. For which of these values of *n* is n^2+n+41 prime?

In answering Exercise 11.1, you will have shown that (e) is true since, for example, $u_0=41$ which is prime. Similarly, to prove that the statement (d) is true, we only need to find *one* example of a real number x for which $| x | =5$ and $|x]=6$. In fact any real number *x* such that $5< x <6$ will do, so we could choose x=5.2, for example.

We now consider the statements (a) to (c) which contain *universal* quantifiers.

Exercise 4.2. Experiment with the statement (a) in Example 4.1 and see whether you believe it is true or false. Can you see *why?*

In answering Exercise 4.2, you should have found that $|x+1|=| x | + 1$ for several different values of x. So, in order to *prove* statement (a), is it sufficient to say, "Statement (a) is true because, for example, when x=2.36, then [x+1] =[3.36]=3, |2.36| =2 and so $|x+1| = |x | + 1$

The answer, sadly, is NO, this is *not* a proof of (a) for the following reason. All we have done above is to demonstrate that the statement is true for *one* real number x and the inference that it is therefore true for *all* real numbers has not been justified. Even if we had demonstrated that $|x+1|=| x | +1$ is true for a million values of x, nothing that we had done would answer the question, "How do you know that there

is not a number that you have not tested for which the statement is false?" That there *might* be such a number Is demonstrated by considering Example 4.1(b).

In answering Exercise 4.1, you should have found that the numbers given by $u = n^2+n+41$ are prime for n=O,1,. . .,1O, and it is an interesting fact that u~ continues to be prime for n=11,12,...,39; but then $u_{40}=41^2$ (and you can easily see that u_{41} is also divisible by 41). So although statement (b) is true in a large number of successive cases, it is never—the—less *not* true for all integers $n \geq O$.

Thus we must look for a reasoning method to prove a statement is true "for all" members of a given set (unless the set is finite and so small that we can give a demonstration for *every* member of it). We shall consider some different methods of proof we might use below.

However, we can prove that a statement is *not* true *for all* members of a given set by finding just *one* member of the set for which the assertion is false; this is called giving a counter-example. Thus, we may conclude that statement (b) is false because we have found a counter—example: U4c~ is *not* prime.

Exercise 4.3.

Prove each of the following statements is *false* by giving a *counter-example.*

(a) Suppose that *a,b* are integers such that $a>b$, then $a^2>b^2$.
(b) Formual $a \in Z$ and all $x \in R$, $|a - x]=| a] - |x]$.

Direct proof

We have seen that it is necessary to give a reasoning proof of statement (a) of Example 4.1.

Example 4.2 We prove that *for any* real number x, $|x +1| = |x]+1$.

Proof. Suppose that |x]=n, where *n* is an integer.
Then from the definition of |x], we know that $n < n+1$.
Adding 1 to each side of these inequalities gives $n+1 \leq x+1 \leq n+2$.
But this means that $| x +1| = n+1=| x |+1$, as required.

The proof of statement (a) given in Example 4.2 is an example of a direct proof by inference. In such a proof, we start with a statement p that we know to be true. Now suppose that we also know that the truth of statement p implies the truth of a second statement q.

Then we may infer that the statement q is also true. If we know further that the truth of statement q implies the truth of a third statement *r,* then we may infer that the statement *r* is true as well. In this way, we can infer the truth of a succession of statements, culminating in the required conclusion.

Exercise 4.4. Give a *direct* proof of each of the following statements.

(a) The sum of two odd integers is an even integer.
(b) The square of an odd integer is odd.

Hint: Remember that an odd number a can be written in the form a=2r+1.

In contrast, the methods of proof described below are called indirect.
Proof by contradiction

This method of proof is often useful when we want to show that a given item (or items) *fails* to satisfy a certain condition.

Example 4.3 We prove that it is not possible to find integers a and *b* such that $a+b$ is even and $a-b$ is odd.

Proof. We start by supposing that this statement is *false;* that is, we suppose we *can* find integers *a,b* such that $a+b$ is even and $a-b$ is odd. *Recollect that an even integer is one that can be written in the form 2m and an odd integer is one that can be written as* 2n+1, *for some in,* $n \in Z$. Thus we can find an integer **in** such that $a+b = 2$ m, and an integer *n* such that $a - b = 2n+1$. Adding these two equations,

we get

$$2a = 2(m+n)+1.$$

Now the left hand side of this equation represents an *even* integer, while the right hand side is an *odd* integer. But this is clearly impossible. So the hypothesis that we can find such integers *a,b* has led to a false conclusion. Hence the hypothesis must be false. So we conclude that there are no integers *a,b* such that *a+b* is even and *a-b* is odd.

Proof by induction

A technique that is often useful in proving results for all positive integers *n"* is called the Principle of Induction. It is based on the following fundamental property of the integers.

Suppose that S is a subset of Z~ *and that we have the following information about S:*

(i) $1 \in S$**;**

(ii) *whenever the integers* 1,2,... ,*k* π *S, then* k+1 $\in$ *S also.*

Then we may conclude that S = Z^+

To see why this is true, we note first that $1 \in S$ by (1), and since $1 \in S$, then $2 \in S$ by (ii). But since $1,2 \in S$, then $3 \in S$ by (ii) again; similarly, since $1,2,3 \in S$, then $4 \in S$ by (ii) ... and so on. Thus the two conditions together show that $Z \subseteq S$**.** But we are told that S *fX*HZ^+ and hence S= Z^+.

Now suppose that we wish to prove that a certain result is true "for all $n \in Z^+$". Let *S* be the subset of Z^+ for which the result holds.

To prove that $S=Z^+$ we must show that the conditions (i) and (ii) above are satisfied by S. We can do this if we can establish the following THREE steps.

1. *(Base case)* Give a verification that the result is true when n=1 so that $1 \in S$.
2. *(Induction hypothesis)* We suppose that the result is true for all the integers 1,2,... ,*k* (for some integer $k \geq 1$).
3. *(Induction step)* Using the hypothesis that the result is true when n=1,2 *k,* we prove that the result also holds when *n=k+1.*

Example **4.4** Consider the sequence 2,5,8,11,14 We saw in section 3A that the recurrence relation for this sequence is *u~~1=u~+3.* So starting from the initial term $u_1=2$, we can calculate successively:

$u_2 = u_1 + 3 = + 3(1),$

$u_3 = u_2 + 3 = u_1 + 3 + 3 = u_1 + 3(2),$

$u_4 = u_3 + 3 = u_1 + 3 + 3 + 3 = u_1 + 3(3)$**,**

and it would be reasonable to guess that a formula that would give us the value of *u~* directly in terms of *n* might be

$u_n = u_1+3(n-1) = 2+3(n-1) = 3n - 1,$

for all $n \in Z^+$ We can use the Principle of Induction to prove that this guess is correct.

(Base case) The formula is correct when *n=1* , since $3(1) - 1 = 2 = u_1$.

(Induction hypothesis) Suppose that $u_n=3n-1$ is true for *n=1,2,3,...,k.* Thus in particular we know that $u_k = 3k - 1$

(Induction step) We prove that $u_n=3n-1$ is also true when n_{k+1}. To do this, we must calculate the value of

u_{k+1} from u_k (using (1) the recurrence relation and (2) the induction hypothesis) and check that the result agrees with the formula, i.e. we check that we get $\mathbf{U}_{k+1}=3(k+1) - 1$.

So (1) putting *n=k* in the recurrence relation, gives

$$u_{k+1} = u_k+3$$

and (2) using the induction hypothesis to substitute for U_k, gives $U_{k+1} = (3k - 1)+3 =$ **3k+2**

But the formula gives $u_{k+1} = 3(k+1) - 1 = 3k+2$.

Thus the formula holds when *n=k+1* and hence it holds for all $n \geq 1$ by induction. •

Exercise **4.5.** A sequence is determined by the recurrence relation $u_{n+1}=2u_n - 1$ and initial term $u_1=3$. Use the recurrence relation to evaluate the next three terms of the sequence. Prove by induction that $u_n=2^n+1$, for all $n \in Z^+$

Example **4.5.** Induction gives a method of proving statement (c) of Example 4.1. Let T_n denote the sum of the first *n* integers, so that $T = 1+2+. . . +n$. We prove by induction that $T~=n(n+1)/2$, for all $n \geq 1$.

(Base case) The formula gives $T_1=1(1+1)/2=1$, so the formula holds when *n=1*.
(Induction hypothesis) Suppose that $T_n=n(n+1)/2$, for n = 1,2,... ,k; then in particular we know that $T_k=k(k+1)/2$.

(Induction step) We prove that that $T_n=n(n + l)/2$ is also true when n=k+1*;* that is, we find T_{k+1} from T_k and check that the result agrees with the the formula. Now T_k=l+2 + 3 ….+k+ (k+1) and T_{k+1}=1+2+3+.. .+*k÷(k+1),* so

$$T_{k+1}= T_k + (k+1).$$

Using the induction hypothesis to substitute for T_k gives

$$\begin{aligned} T_{k+1} &= k(k+l)/2 + (k+1) \\ &= (k+1)(k/2 + 1) \\ &= (k+1)(k+2)/2. \end{aligned}$$

But putting nk+1 in the formula gives $T_{k+l}=(k+1)(k+2)/2$. Thus the formula also holds for n = k+1 and hence it holds for all $n \geq 1$, by induction.

Example 4.5
Illustrates that induction is a useful method for verifying a formula for the SUM of a finite number of terms of a sequence, because it is very easy to obtain the relation between Sn and Sn+1. For, suppose $S= u_1+u_2+...+u_n$. Then $S_{k+l}=(u_1 + u_2+...+u_n)+u_{n+1}$. Hence

$$Sn+1 = Sn + u_{n+1}$$

Example 4.6. Let Sn denote the sum of the squares of the first *n* integers, so that $Sn=1^2+2^2+...+n^2$. We shall prove by induction that Sn is given by the formula: Sn = n(n+l)(2n+l)/6, for all $n \geq 1$.

(Base case) When n=1, $S_1=1^2$. The formula gives $S_1=1(1+l)(2+1)/6=l$. Hence the formula holds when n1.

(Induction hypothesis) Suppose Sn=n(n+1)(2n+1)/6 is true for n= 1 , 2, . . . , *k;* then, in particular, we know that Sk =*k(k+1)* (2k+l)/6.

(Induction step) We prove that the formula also holds for n= k+1*;* that is, we calculate Sk+1 from Sk and check that the result agrees with the formula. From the recurrence relation we have

$$Sk+l = Sk + (k+1)^2.$$

Using the induction hypothesis to substitute for Sk gives $Sk+l = k(k+l)(2k+1)/6 + (k+l)^2$

$$\begin{aligned} &= (k+1)[k(2k÷1)/6 + (k+l)] \\ &= \textit{(k+1)[2k}^2 \textit{ + 7k + 6]/6} \\ &= (k+1)(k+2)(2k+3)/6. \end{aligned}$$

But putting n=k + 1 in the formula gives Sk+1 =(k+1)(k+2)(2k+3)/6. Thus the formula also holds for n=k+l and hence it holds for all $n \geq 1$, by induction. .

Exercise 4.6. Let S_n denote the sum of the first *n odd* integers. Calculate the values of S_1,S_2 S_5 and guess a formula for S_n,. How can you express the nth odd integer in terms of *n?* Prove your formula for S_n, is correct by induction.
We can use induction to prove results "for all *n* n_0", for any integer rl_0; the base case is then n=ri0 and the rest of the proof follows as above. Notice that your base case is always the least value of n for which the statement is true. In the following example, this least value of n is n=O.

Exercise 4.7

Let $S_n = F_0+F_1+F_2+.. .+ F_n$, $n \geq 0$, denote the sum of the first n+ l Fibonacci numbers. Tabulate the value of S_n against n for n=0,1,. . . ,9. Find a connection between S_n and F_{n+2} that is true when $n \leq 9$. Prove that this connection is true for all $n \in N$, by induction.

Example 4.7.
A sequence is determined by the recurrence relation $u_n = 4u_{n-1}- 3u_{n-2}$ and the initial terms $u_0=0$, $u_1=2$. We shall prove that $u_n=3^n - 1$

Exercise 4.8.
Use the recurrence relation to calculate the next three terms of the sequence. Verify that the suggested formula for u~ gives the correct value for u_0, u_1, u_2, u_3, u_4.

Example 4.7 (continued). Notice that we could not calculate u_2 and subsequent terms of this sequence unless we had been given the values of TWO initial terms. Thus for the base case, we must verify the formula is correct for BOTH u_0 and u_1. Also, note that the recurrence relation connects u_n with *two* previous terms, not *just* with u_{n-1}

(Base cases) When n = 0, the formula $u_n=3^n -1$ gives $u_0=3°-1 =0$; and when n=1, it gives $u_1=3^1-1 =2$. Hence it holds for n=0 and n=1

(Induction hypothesis) Suppose the formula $u_n =3^n - 1$ holds for n=0 ,l,2,.. . ,k-1 (note that for algebraic convenience, we go just to k- 1 this time).

(Induct ion step) We prove the formula also holds for n_k. From the recurrence relation, we have

$$u_k = 4 u_{k-1} – 3u_{k-2}$$

By the induction hypothesis, the result is true when n=k-1 and n=k-2.
Hence $u_k = 3^{k-1}$_- l and $u_{k-2}= 3^{k-2}- 1$
Substituting in the recurrence relation gives

$u_k = 4(3^{k-1}- 1)- 3(3^{k-2}- 1)- 4(3^{k-1}- 1) – 4 – 3^{k-1}+3 = (4 - 1)3^{k-1}-1= 3^k - 1.$

Thus the formula also holds when $n=k$ and hence holds for all $n \in N$ by induction. .

Exercise *4.9.* A sequence is 'determined by the recurrence relation $u_n =3u_{n-1}-2u_{n-2}$ and initial terms $u_0=O$, $u_1= 1$. Prove by induction that $u_n =2^n - 1$, for all $n \in N$.

Recurrence relations often arise from practical problems. Here is a simple example.

Example 4.8. Suppose that each of the *n* terminals in an electronic circuit are connected to each of the others. Denote the number of interconnections by u_n. (a) We find a recurrence relation connecting u_{n+1} with u; (b) we prove by induction that $u_n =n(n-1)/2$.

(a) To find the recurrence relation, we consider how many extra connections must be formed when we add the *(n+1)th* terminal and connect it to each of the existing *n* terminals. Clearly just *n* new connections are needed. So $u_{n+1}=u_n + n$.

(b) We now prove that u~$=n(n-1)/2$.

(Base case) When n=1, no interconnections need to be made, so $u_1=O$. But the formula gives $u_1=1(1-1)/2=0$, so the formula holds for n=1. *(Induction hypothesis)* Suppose $u_n=n(n- 1)/2$ holds for n=1 , 2,. . . , *k;* then in particular we know that $u_k=k(k-1)/2$.

(Induction step) We use the recurrence relation that we found in (a) to find from u_k and check this gives the same result as predicted by the formula when n=k+1 Now

$u_{k+1}= u_k+k$, by the recurrence relation,
$= k(k-1)/2 + k$, from the induction hypothesis,
$=k[(k—1)/2 + 1]$
$=k(k+1)/2.$

But the formula gives $u_{k+1}= (k+1)k/2$. Thus the formula also holds for n= k+1 and hence holds for all $n \geq 1$, by induction. .

Exercise 4.9. There is an old puzzle known as the *Tower of Hanoi.* It consists of a board with 3 pegs and a number of circular rings of different diameters. At the start of the puzzle the rings are stacked on one of the pegs in order of size, with the ring of greatest diameter at the bottom of the stack, as shown in Fig.4.1 below in the case where there are 4 rings. The puzzle is to determine the least number of moves required to transfer the whole stack, one ring at a time, from one peg to another in such a way that no ring is ever placed on top of a smaller one. All three pegs may be used to hold rings during the

transfer.

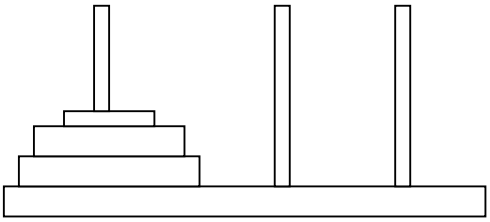

Fig 4.1

(a) Find the solution in the cases when there are 1, 2 and 3 rings respectively. When you know the solution for 3 rings, can you deduce the solution for *4* rings?

(b) Let u_n denote the minimum number of moves necessary to transfer a pile of n rings from one peg to one of the others. Explain why $u_{n+1} = 2u_n + 1$. Tabulate the value of u_n against n for n=0,1,. . . ,6. Guess a formula for u_n and prove your guess is correct by induction.