4. PROOFS

§4.1. Writing Proofs

A proof is a *chain of reasoning* that leads from a set of assumptions to a conclusion. There are many proofs in computing science and, of course, mathematics is all theorems and proofs, or so it seems.

The important word here is “chain”. A proof is not just a heap of arguments which make the conclusion seem plausible. A case for the prosecution in a court of law might rely on evidence heaped upon evidence till the scales of justice tip. In a proof, however, we present a chain — an intellectual journey. Whoever takes this journey should find that the truth of what is being proved is inescapable.

Structure is as important in a proof as in a computer program. No trained computer programmer would dream of writing a program by assembling some loosely connected statements in some arbitrary order. Yet that is what the same programmer often does when asked to write a proof.

The structure of a proof must reflect the logical structure of the proposition being proved. If you keep this in mind then many simple proofs just seem to write themselves with little or no imagination required on the part of the prover. In fact this approach is built in to automated theorem-proving software. These programs are not designed to put mathematicians out of a job. A really significant mathematical break-through will always require the mathematical ingenuity of a real mathematician. But there is a growing area of proof of program correctness, whereby a computer program is analysed logically in a mechanical way and a proof that it meets the specifications is generated.

§4.2. Patterns of Proof

IMPLICATION: $p \rightarrow q$

We assume p and then prove q.

$p \rightarrow q$
Suppose p
…………
Therefore q

Example 10: Prove that if n is odd then n^2 is odd.

Proof: Suppose n is odd.
Then $n = 2k + 1$ for some integer k.
Thus $n^2 = (2k + 1)^2 = 4k^2 + 4k + 1 = 2(2k^2 + 2k) + 1$, which is odd.

NEGATION: –p

If the statement of the theorem has a negative form it is usually best to use Proof by Contradiction.

–p
Suppose p.
…………
A contradiction.
Hence –p.

Example 11: Prove that $\sqrt{2}$ is irrational.

Proof: Suppose that $\sqrt{2}$ is rational. Therefore $\sqrt{2} = \frac{m}{n}$ for some integers m, n with $n \neq 0$.

We may suppose without loss of generality (wlog) that m, n have no common factor (i.e. are coprime). Now $m^2 = 2n^2$ and so m is even. Put $m = 2k$. Then $4k^2 = 2n^2$ and so $n^2 = 2k^2$ which implies that n is even. This contradicts the assumption that m, n are coprime.
Hence $\sqrt{2}$ must be irrational.

Example 12: Prove that $\forall x\, \exists y\, [(Px \to -Qy) \to (Qx \to -Px)]$
This is a tautology, in the sense of quantifiers, that is, it is true for all possible predicates P, Q.
Proof: We suppose that the theorem is false and use the Negation Rules.

Suppose $-\forall x\, \exists y\, [(Px \to -Qy) \to (Qx \to -Px)]$.
$\therefore\ \exists x\, -\exists y\, [(Px \to -Qy) \to (Qx \to -Px)]$.
$\therefore\ \exists x\, \forall y\, -[(Px \to -Qy) \to (Qx \to -Px)]$.
$\therefore\ \exists x\, \forall y\, [(Px \to -Qy) \wedge -(Qx \to -Px)]$.
$\therefore\ \exists x\, \forall y\, [(Px \to -Qy) \wedge Qx \wedge --Px)]$.
$\therefore\ \exists x\, \forall y\, [(Px \to -Qy) \wedge Qx \wedge Px)]$.

In particular, taking $y = x$ we get $(Px \to -Qx) \wedge Qx \wedge Px)$ which is a contradiction.
Hence the original proposition is true.

OR: $p \vee q$
The simplest way to prove a "p or q" theorem is to recast it as $-p \to q$. Note that $(p \vee q) \leftrightarrow (-p \to q)$ is a tautology.

Suppose $-p$.
…………..
Therefore q.
Hence $p \vee q$.

Example 13: Prove that there exists an irrational number x such that $x^{\sqrt{2}}$ is rational.
This does not appear to have an obvious "p or q" form. But if we start the proof with "let $x = \sqrt{2}$ or $x = (\sqrt{2})^{\sqrt{2}}$ " then our goal is to prove that for one of these alternatives x is irrational and $x^{\sqrt{2}}$ is rational.
Proof: Suppose $(\sqrt{2})^{\sqrt{2}}$ is rational. Then we have an irrational that becomes rational when raised to the power $\sqrt{2}$. Suppose now that $x = (\sqrt{2})^{\sqrt{2}}$ is irrational. Then $x^{\sqrt{2}} = (\sqrt{2}^{\sqrt{2}})^{\sqrt{2}} = \sqrt{2}^{(\sqrt{2}\sqrt{2})} = (\sqrt{2})^2 = 2$, which is rational.

It is interesting that we can so easily conclude that either $\sqrt{2}$ or $(\sqrt{2})^{\sqrt{2}}$ is a candidate for the above theorem but deciding which one actually is requires a very deep mathematical argument. [In fact $x = (\sqrt{2})^{\sqrt{2}}$ is irrational (hard to prove) and $x^{\sqrt{2}}$ is rational (obvious).]

AND: $p \wedge q$.
This is simply a case of two theorems rolled up into one.

$p \wedge q$
…….
Therefore p.
…….
Therefore q.
Hence $p \wedge q$.

Example 14:

Prove that the sequence given by $u_n = 0$, $u_{n+1} = \sqrt{u_n + 3}$ converges as $n \to \infty$.
We use the theorem that increasing sequences, that are bounded above, converge.
So we must prove that $\forall n[u_{n+1} > u_n] \wedge \exists b\ \forall n[u_n < b]$. We prove each of these statements by induction on n.

$u_{n+1} > u_n$ for all n
We prove this by induction on n. $u_1 = \sqrt{3} > u_0 = 0$ so it holds for $n = 0$.
Suppose it is true for n, that is, $u_{n+1} > u_n$.
Then $u_{n+2}^2 - u_{n+1}^2 = u_{n+1} - u_n > 0$ so $u_{n+2}^2 > u_{n+1}^2$ and hence $u_{n+2} > u_{n+1}$.
(NB $u_n > 0$ for all n.)
Hence it is true for $n + 1$ and so, by induction, it is true for all n.

$u_n < 3$ for all n.
[Why 3? The reason is that when we calculate values of u_n we get the values:

0, 1.73205, 2.17533, 2.27493, 2.29672, ….

It appears that they will never exceed 3, so we try to prove that this guess is indeed correct. We do in fact succeed. But, had u_n eventually become bigger than 3, the proof would obviously break down. In that case we might have tried a larger number as a possible upper bound.]

We prove this by induction on n. $u_0 = 0 < 3$ so it holds for $n = 0$.
Suppose it is true for n, that is, $u_n < 3$.
Then $u_{n+1}^2 = u_n + 3 < 3 + 3 = 6$ so $u_{n+1} < \sqrt{6} < 3$.
Hence it is true for $n + 1$ and so, by induction, it is true for all n.

EQUIVALENCE: $p \leftrightarrow q$
This is essentially an "and" since $p \leftrightarrow q$ is equivalent to $(p \to q) \wedge (q \to p)$.

$p \leftrightarrow q$	
Suppose p. ………… Therefore q.	Now suppose q. ………… Therefore p.
Hence $p \leftrightarrow q$.	

Example 15:

Prove that if p is prime then p divides mn if and only if p divides m or p divides n.
Solution: Suppose that p divides m. Then m = pq for some integer q and so mn = pqn and so p divides mn. Similarly if p divides n. (This is it the easy half of the proof.)
Now suppose that p divides mn and suppose p does not divide m.
(Here we need to prove "p divides m or p divides n" so we use the appropriate pattern of proof.)
So GCD(p, m) = 1. Using a well-known fact about greatest common divisors we can write
1 = ph + mk for some integers h, k.
Hence n = pnh + (mn)k. Since p divides each of these terms, p divides n.

UNIVERSAL QUANTIFIER: $\forall x[Px]$
If we are to prove that something true for all x in S we begin by considering a typical x.

$$\mathbf{\forall x[Px]}$$
$$\text{Let } x \in S.$$
$$\ldots\ldots\ldots\ldots$$
$$\text{Therefore } Px.$$

EXISTENTIAL QUANTIFIER: $\exists x[Px]$

When the proposition to be proved states that something exists with a certain property we need to define, or choose, the x at some stage.

$$\mathbf{\exists x[Px]}$$
$$\text{Let } x = \ldots$$
$$\ldots\ldots\ldots\ldots$$
$$\text{Therefore } Px.$$

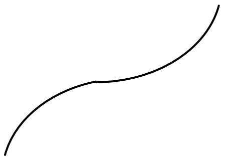
Often the x is not a particular x but rather something chosen with a certain property.

§4.3. The Importance of Definitions

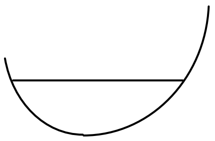
One of the major difficulties students have in writing proofs is not knowing how to handle definitions. The problem arises from the fact that a lecturer, when presenting a new concept, generally begins by stating the formal definition. Because this will seem rather abstract to the student the lecturer then gives several informal versions and a number of illustrative examples. This is good and will improve the student's grasp of the concept. The problem is that all this illustrative stuff tends to overwrite the original formal definition in the student's mind. So when it comes to writing a proof based on that concept, the student encounters difficulty. It is important to remember that:

in writing proofs one should only use formal definitions

A 1-1 (one to one) function is one where different elements have different images or where you do not get a doubling up like you do when you square the numbers –x and +x. If we can graph the function, it is 1-1 if you never have more than one part of the curve at any given level and not 1-1 if there are two or more parts at the same level. For example:



1-1



not 1-1

All this may very well help you to *understand* the concept but try to prove a theorem about 1-1 functions using the above collection of ideas!

The formal, technical, definition of the statement **f is 1-1** is the following:

if f(x) = f(y) then x = y.

Another problem often encountered is the difficulty of adapting a formal definition to the current circumstances and notation. It really is not such a difficult thing but you need to get into the right mind-set. Adapting a definition is simply a symbol substitution exercise. It does not require any intuitive understanding. It is simply an automatic and mindless operation with symbols, and in fact thinking about what the symbols mean only makes the exercise more difficult.

The definition of the 1-1 property can be recast as a rewriting rule:

whenever you encounter the string “□ **is 1-1**” you can replace it by

“if □(x) = □(y) then x = y”.

Here □ can stand for any symbol or collection of symbols that could represent a function.

So if you encounter “g is 1-1” you rewrite it as “if $g(x) = g(y)$ then $x = y$”. The statement “$g\circ f$ is 1-1” becomes “if $g\circ f(x) = g\circ f(y)$ then $x = y$”. We will explain the meaning of the $\circ$ symbol in a later chapter but the important thing to realise is that you do not need to understand the symbols in order to adapt a definition. It is simply a mindless clerical task with symbols. So “$\nabla\clubsuit+$ is 1-1” becomes “if $\nabla\clubsuit+(x) = \nabla\clubsuit+(y)$ then $x = y$”.

Now the statement “if $f(x) = f(y)$ then $x = y$” contains a hidden quantifier. Strictly speaking it should read “for all x and for all y, if $f(x) = f(y)$ then $x = y$”, but we usually leave out the quantifiers in cases like this. We can use any symbol we like for such dummy variables provided they do not have any other meaning. It would not be good to use “if $f(\pi) = f(2)$ then $\pi = 2$” to express the fact that f is 1-1 because the symbols π and 2 cannot be used as variables without some confusion. Also, if x has been used elsewhere, except as a dummy variable, then we cannot use it here. So if the name of a function was T_x we could not write “if $T_x(x) = T_x(y)$ then $x = y$”. We would need to replace the dummy variable x by something else, such as z and so write “if $T_x(z) = T_x(y)$ then $z = y$”.

But it *is* perfectly permissible to use x as a dummy variable several times provided the scope of the associated quantifiers do not overlap.

Another property of functions is the property of being “onto”. Here we are thinking of functions not just as formulas or rules to get $f(x)$ from x. A function $f: S \to T$ is a pair of sets S, T together with a rule. The first set S is called the **domain** of the function and the second set is called its **codomain**. A function is **onto** if every element of the codomain is the image of something in the domain. It is just like a target where every point on the target gets hit by an arrow. The function $f(x) = x^2$ is onto if the codomain is the set of x with $x \geq 0$ but is not onto if we consider f as a function to the set of *all* real numbers.

These analogies and example might help us to grasp the concept but to prove any theorem involving it we need to use the crisp, clear, but somewhat abstract-looking, formal definition.

The formal definition of a function being onto is:

$f:S \to T$ is onto if:

for all t in T there exists s in S such that f(s) = t,

or more briefly

if $\forall t \in T\ \exists s \in S[f(s) = t]$

Here we are using the standard symbols for the quantifiers “for all” and “for some”. Also we are using the symbol “$\in$” to denote that something belongs to (or is an element of) some set. Finally the “such that” serves no purpose except to make the sentence more readable, so we leave it out when writing the statement in symbols.

Example 16:

Let $f:A\to B$ and $g:B\to C$ be functions. Prove that if f is onto and $g \circ f$ is 1-1 then g is 1-1.

Solution: (1) Suppose f is onto and $g \circ f$ is 1-1.

(We must write down our assumptions explicitly in the proof.)

(2) Suppose $g(b) = g(b')$.

(We write this because our goal is to prove that g is 1-1 and that says "if $g(b) = g(b')$ then …")

(3) Since f is onto there exist $a, a' \in A$ such that $f(a) = b$ and $f(a') = b'$.

(We write this because the assumption that f is onto needs elements in B and we now have them.

(4) Hence $g(f(a)) = g(f(a'))$, that is $(g \circ f)(a) = (g \circ f)(a')$.

(We needed to get this so that we could use the assumption that $g \circ f$ is 1-1.

(5) Since $g \circ f$ is 1-1 we conclude that $a = a'$.

(But we are not quite finished.)

(6) Hence $f(a) = f(a')$, that is, $b = b'$.

(This is the conclusion to the statement that g is 1-1.)

(7) Therefore g is 1-1.

Here are some hints for writing proofs.

- Begin by writing down your assumptions.
- Examine the logical structure of the theorem and structure your proof accordingly.
- Keep asking yourself "what does that mean in more primitive terms?"
- Keep asking yourself "what is my current goal?" This changes throughout the proof.
- Use formal definitions.
- Work forward from what you know and back from what you have to prove, till they link up. But when you write the proof it must proceed in the direction from the assumptions to the goal.
- Never write down what you are trying to prove (unless you qualify it by such words as "we shall prove that …")
- Never prove that a statement holds for all x by merely considering one or more particular x's.

The following is a short list of formal definitions from various parts of mathematics written in the form of rewriting rules.

REWRITE …	**AS …**
n is even	there exists $m \in \mathbf{Z}$ such that $n = 2m$
$a \mid b$	$b = aq$ for some $q \in \mathbf{Z}$
p is a positive prime	$p > 1$, and if $p = ab$ for some $a,b \in \mathbf{Z}$ then $a = 1$ or $b = 1$
$S \subseteq T$	if $s \in S$ then $s \in T$
$(f \circ g)(x)$	$f(g(x))$
$f:S\to T$ is 1-1	if $f(x) = f(y)$ then $x = y$
$f:S \to T$ is onto	If $t \in T$ there exists $s \in S$ such that $f(s) = t$
R is transitive	if aRb and bRc then aRc

EXERCISES FOR CHAPTER 4

Exercise 1: Prove that for all a, b $\in$ **Z**, if a | b and b | a^2 then a + b is even.

Exercise 2: Prove that for all positive primes p there exists a positive prime q with
p < q < p! (where p! = p(p − 1)(p − 2). … 3.2.1).
[HINT: Begin with “Let q be a positive prime dividing p! − 1.]

Exercise 3: Prove, without using Venn Diagrams, that if $A \subseteq B \cup C$ then $A - B \subseteq C$.

Exercise 4: Let $g:X\to Y$ and $f:Y\to Z$ be functions. Prove that if $f \circ g$ is 1-1 and g is onto then f is 1-1.

Exercise 5: Let $f:A\to B$ and $g:B\to C$ be functions. Prove that if both f and g are onto then so is $g \circ f$.

Exercise 6: Let $f:A\to B$ and $g:B\to C$ be functions. Define $h = g \circ f$. Prove that if both f and g are 1-1 then so is h.

Exercise 7: Let $f:A\to B$ and $g:B\to C$ be functions. Prove that if $g \circ f$ is onto then so is g.

Exercise 8: Let $f:A\to B$ and $g:B\to C$ be functions. Prove that if $g \circ f$ is onto and g is 1-1 then f is onto.

Exercise 9: Let $f:A\to B$ and $g:B\to C$ be functions. Prove that if $g \circ f$ is 1-1 then so is f.

SOLUTIONS FOR CHAPTER 4

Exercise 1: Suppose a | b and b | a^2.
Then a = kb and b = ha^2 for some h, k $\in$ **Z**.
Hence a = kha^2.
If a ≠ 0 then 1 = kha. Hence a, h, k are all ±1.
Hence b = ±1.
Thus a = b = 1 or a = 1, b = –1 or a = –1, b = 1 or a = b = –1.
Hence a + b = 2, 0 or –2 and so a + b is even.
Suppose now that a = 0. Then b = 0. Hence a + b = 0, which is even.

Exercise 2: Let q be a positive prime dividing p! − 1.
Suppose q ≤ p.
Then q | p! and hence q does not divide p! − 1, a contradiction.
Hence q > p.
Clearly q ≤ p! − 1 < p!.

Exercise 3: Let $x \in A - B$.
$\therefore$ $x \in A$ and $x \notin B$.
Since $x \in A$, $x \in B \cup C$.
$\therefore$ $x \in B$ or $x \in C$.
If $x \in B$ we contradict $x \notin B$.
Hence $x \in C$.

Exercise 4: Suppose $g(x) = g(y)$ for $x, y \in B$.
Since f is onto, $x = f(u)$ for some $u \in A$, and $y = f(v)$ for some $v \in A$.
Thus $g(f(u)) = g(f(v))$, that is, $g \circ f(u) = g \circ f(v)$.
Since $g \circ f$ is 1-1 it follows that $u = v$.
Hence $f(u) = f(v)$, that is, $x = y$.

Exercise 5: Suppose f is onto and g is onto.
Let $c \in C$. Since g is onto, $c = g(b)$ for some $b \in B$.
Since f is onto, $b = f(a)$ for some $a \in A$.
Then $c = g(b) = g(f(a)) = g \circ f(a)$.
Hence $g \circ f$ is onto.

Exercise 6: Suppose f and g are 1-1.
Suppose that $h(x) = h(y)$.
Then $g(f(x)) = g(f(y))$.
Since g is 1-1, $f(x) = f(y)$.
Since f is 1-1, $x = y$.
Hence h is 1-1.

Exercise 7: Suppose $g \circ f$ is onto.
Let $z \in C$.
Then $(g \circ f)(x) = z$ for some $z \in A$.
Thus $g(f(x)) = z$.
Hence g is onto.

Exercise 8: Suppose $g \circ f$ is onto and g is 1-1.
Let $y \in B$.
Then $g(y) \in C$.
Hence, since $g \circ f$ is onto, $(g \circ f)(x) = g(y)$ for some $x \in A$.
Thus $g(f(x)) = g(y)$.
Since g is 1-1, $f(x) = y$.
Thus f is onto.

Exercise 9: Suppose $g \circ f$ is 1-1 and that $f(x) = f(y)$.
Then $g(f(x)) = g(f(y))$, that is $(g \circ f)(x) = (g \circ f)(y)$.
Since $g \circ f$ is 1-1 it follows that $x = y$.