Intro to Mathematical Reasoning (Math 300)

Supplement 3. **Proving universal statements** [1]

These notes supplement sections 1.9-1.14 of the text.

1 Theorems and conjectures

As mathematicians and students of mathematics, it is our job to separate those mathematical statements that are true from those that are false. The method that mathematicians use to verify that a statement is true is called *deductive proof*. Roughly speaking, a deductive proof is a *step by step* argument that uses *known facts* and applies *valid rules of deduction* to build to a desired conclusion.

Mathematicians use the words *Theorem*, *Proposition*, *Lemma*, and *Corollary* to refer to mathematical statements that are known to be true because a proof has been given. There is no precise distinction among these terms but here is a guideline for their meaning:

- The words "theorem", "proposition", and "corollary" refer to proved mathematical statements that are interesting in their own right. The word "theorem" tends to be used for statements that are most interesting and/or harder to prove. The word "proposition" is used for statements that are less interesting and/or easier to prove. If a mathematical statement is proved as an easy consequence of a previously proved statement, we say that statement is a "corollary" of the previous statement.
- The word "lemma" refers to a proved mathematical statement that is mainly of interest because it is a step in the proof of a theorem or proposition.

A statement that a mathematician *believes* to be true, but for which no proof is known is called a *conjecture*. For example, one of the most famous conjectures in mathematics is *Goldbach's conjecture*:

> Every even number greater than 2 can be expressed as the sum of two primes.

It has been verified by computer that every even number between 4 and 4×10^{14} can be expressed as the sum of two primes. However, no one knows whether this is true of all even numbers.

2 Why do we need rules for mathematical proof?

As you will learn, to be valid, a mathematical proof must be constructed in accordance with certain rules. Early in the course, most beginning students will find that the proofs they submit are often rejected as *faulty* because they fail to follow these rules. Before discussing what these rules are, it is important to understand why there are rules for mathematical proof.

In any activity, certain occurences are recognized as disasters. In rock climbing, falling off a rock face from 100 feet without being secured to the rock by a rope is a disaster. In mathematics,

[1] Version 2/4/04.

the biggest disaster that can happen is *to declare that a mathematical statement has been proved to be true, when actually the mathematical statement is false.* It is a mathematical disaster because it undermines our search for mathematical truth, and it is a personal disaster because it can be quite embarassing. In some circumstances, it can also be disastrous on a practical level: if a mistaken theorem is used to plan the orbit of a satellite, the satellite may crash or be lost in space.

The rules for mathematical proof are designed to prevent this disaster from occuring; if you follow the rules *it is impossible to accidentally give a proof of a false statement.*

A proposed proof that does not follow the rules for mathematical proof is called a *faulty proof.* A proof can be faulty even if the statement it is trying to prove is true. Such proofs are not permitted because they use arguments that could be used to prove false statements.

3 Formal and informal proof

There are different styles of mathematical proof, from strictly formal proofs to informal. In *strictly formal proofs*, the rules are very clear and precise. Formal proofs are written symbolically rather than in English. These proofs are the least prone to error but they are also very hard to work with because the symbolic language they use is very hard to read. Also, strictly formal proofs, even of very simple statements, tend to be extremely long. We will not learn how to do formal proofs in this course.

Because strictly formal proofs are so tedious, mathematicians rarely write them. Instead, they write informal proofs, which are written in some "natural" language (which, for us, is English) augmented with mathematical terminology and symbols. *These are the kinds of proofs you will learn to do in this course.* Informal proofs written in English should consist of complete sentences and follow the the usual grammatical rules of English, In addition, there are the rules for making proper mathematical deductions. Unfortunately, the rules for informal proof are harder to specify than for formal proofs. In this supplement and the next two, many of the rules will be explained. Writing informal proofs is learned largely from examples, and many examples will be given.

4 What known facts can be used in our proofs?

As stated above, a proof is a a *step by step* argument that uses *known facts* and applies *valid rules of deduction* to build to the desired conclusion.

In formal mathematical proofs, the known facts are completely specified and are called *axioms.* Any fact which is not an axiom must be proved. For example, the axioms for working with real numbers are given (in English, not symbolically) on pages 180, 183 and 187 of the text. In principle it is possible to prove all known results about the real numbers from these axioms.

However, there are many basic facts that are not axioms. Here are some examples:

- $47 + 28 = 75$.
- For all real numbers x, $x \times 0 = 0$.
- For all real numbers x, y, if $xy = 0$ then $x = 0$ or $y = 0$.
- For all real numbers x, y, $(-x) \times y = x \times (-y)$.

- For all real numbers x, y, $(x+y)^2 = x^2 + 2xy + y^2$.

If required to work only from the axioms, these statements must all be proved. Proving these statements is tedious and time consuming and some are rather tricky. Later when we get to chapter 8, we will spend some time showing how to prove statements like these from the axioms.

But for most of the course, we want to assume these basic facts and others like them. Unfortunately, it is not so easy to clearly specify what known facts you are allowed to use, and which you aren't. The best we can do at this point is to give some guidelines. Here are facts you may use in your proofs about real numbers (unless otherwise instructed).

- All axioms and theorems stated in sections 8.1,8.2 and 8.3.
- *Arithmetic facts.* Arithmetic facts involving exact calculations with specific integers and rational numbers that you could do by hand such as "$\frac{2}{3} + \frac{1}{5} = \frac{13}{15}$", "$453 - 28 = 425$", "$3^5 = 243$", and "52 is not a multiple of 7".
- *Basic laws of algebra.* Any computation involving addition, subtraction, multiplication and division that can be justified by applying the commutative, distributive and associative laws of arithmetic. For example, you may say that the statement "For all real numbers a,b, $(a+b) \times (a+b) = a^2 + 2ab + b^2$." is true by the basic laws of algebra because the left hand side can be transformed into the right hand side by applying the commutative, distributive and associative laws. Facts involving division may require some care to ensure that you don't divide by 0.
- Basic facts about inequalities such as: "for all real numbers a, b, c, if $b \geq c$ then $a+b \geq a+c$." Some but not all of these facts are given as theorems in section 8.3. Again these facts require care in applying them. For example, it is not true that "for all real numbers a, b, c, if $b \geq c$ then $ab \geq ac$" because there are counterexamples. It is true that "for all real numbers a, b, c, if $b \geq c$ and $a \geq 0$ then $ab \geq ac$."

There is a basic principle that is used all the time, that is so obvious that it is often not mentioned. This is the *substitution principle*: Whenever y and z are numbers (or other mathematical objects) and it is known that $y = z$, if we are given a true statement about y then we may substitute z for A in the statement to get a new true statement. When we say that something is true "by substitution" we mean that we are using this principle.

Here are some examples of facts that, at this point in the course, *can not* be taken as known facts for your proofs:

- Facts involving square roots, cube roots and higher roots of real numbers. For example, you may not assume the fact that every nonnegative real number has a square root.
- Facts involving prime numbers, divisibility, etc. (such as the fact that every positive integer greater than 1 can be written as the product of prime numbers).
- Facts involving calculus.

At different points in the course, the facts we will take as known facts may change. For example, when we are proving statements about the integers (rather than about the real numbers), involving concepts like prime numbers, divisor, etc. then we will consider that basic facts about addition, subtraction and multiplication are known, but not basic facts about division.

5 Proving Existential Statements

(This section supplements section 1.9 in the book.)

A statement of the form "$\exists x$ such that $P(x)$" simply says that there is at least one value of x that makes $P(x)$ true. So to prove this, you need only produce one example of a value a for which $P(a)$ is true, and then give a proof of the fact that $P(a)$ is true. (As always, the word "value" does not always mean "number" but refers to whatever type of mathematical object, such as number, set, function, etc., that x is supposed to be.)

Disproving a universal statement is the same as *proving* an existential statement. To disprove "$\forall x, Q(x)$" is the same as proving its negation "$\sim \forall x, Q(x)$" which is equivalent to proving the existential statement "$\exists x, \sim Q(x)$".

We've already seen examples of proving existential statements, since in handout 1 and homework 1 we disproved some universal statements. Here's one more example:

> **Theorem.** There exist integers a, b, c such that no one is a multiple of the other, but the product of any two is a multiple of the third.

Proof. Choose $a = 6$, $b = 15$ and $c = 10$. 6 is not a multiple of 10 or of 15, 10 is not a multiple of 6 or of 15 and 15 is not a multiple of 10 or 6. $6 \times 10 = 60$ is equal to 4×15 and so is a multiple of 15, 6×15 is equal to 9×10 and so is a multiple of 10, and 10×15 is equal to 25×6 and so is a multiple of 6. $\square$.

The symbol "$\square$" is a common way to indicate that your proof is ended. An alternative is to use the Latin abbreviation "QED" for "quod erat demonstrandum" which means "that which was to be proven".

6 Proving Universal Statements

(Note: this section supplements sections 1.10, 1.12, 1.13 and 1.14 in the book. In sections 1.12, 1.13 and 1.14 the book talks about how to prove "statements" of the form "if $A(x)$ then $B(x)$". As we have already discussed, in such statements there is a quantifier that has been omitted, and the sentence really means "for all x, if $A(x)$ then $B(x)$.")

We have just seen that to prove an existential statement involves producing and verifying one example of the associated predicate. How do we go about proving a universal statement? A universal statement has the form "For all x that satisfies the hypothesis $H(x)$, the conclusion $C(x)$ must also be true." As we've said before, a single universal statement summarizes many (often infinitely many) different statements, one for each value of x that makes $H(x)$ true. Somehow, we must prove that $C(x)$ holds, knowing that $H(x)$ is true but not knowing what x is.

If we can show that there are only a few possible values of x that make $H(x)$ true, then we can just check each one to see if $C(x)$ is true. For example here's a proof of:

> Every positive integer less than 5 is a root of the polynomial p defined by $p(x) = x^4 - 10x^3 + 35x^2 - 50x + 24$.

Proof. The only positive integers less than 5 are 1,2,3 and 4. By elementary arithmetic, we check $p(1) = 1-10+35-50+24 = 0$, $p(2) = 16-80+140-100+24 = 0$, $p(3) = 81-270+315-150+24 = 0$,

and $p(4) = 256 - 640 + 560 - 200 + 24 = 0$, so $1, 2, 3$ and 4 are all roots of p. Therefore every positive integer less than 5 is a root of $x^4 - 10x^3 + 35x^2 - 50x + 24$. □

However if we can't easily check all of the values that make $H(x)$ true, then it is often not clear how to prove the statement. Trying a few values for x that satisfy $H(x)$ and checking that they satisfy $C(x)$ is a useful way to gain understanding about what the universal statement means, but it does not prove the statement.

There are a few methods for proving a universal statement. The most important is a method that we'll call the

Arbitrary Value method.[2]

Here's the idea. We start by imagining that someone else has chosen an arbitrary value for x that makes $H(x)$ true. We don't know the value so we give it a letter name, such as a. We then use the fact that $H(a)$ is true to build a chain of deductions that leads to $C(a)$. Each step of the proof must be true regardless what the unknown value a is.

This is all very vague. How to we build this "chain of deductions"? What is a "chain of deductions" anyway? As usual, it's helpful to look at an example.

Example. Consider the universal statement:

Theorem. The product of any two real numbers is at most the square of their average.

Proof. First, we rewrite the statement to be proved using variables and quantifiers: For all real numbers x and y, $xy \leq \left(\frac{x+y}{2}\right)^2$.

Let r and s be arbitrary real numbers. We will show that $rs \leq (\frac{r+s}{2})^2$. To do this, we will show that $(\frac{r+s}{2})^2 - rs \leq 0$.

By definition of "squared", $(\frac{r+s}{2})^2 = (\frac{r+s}{2}) \times (\frac{r+s}{2})$. We now apply basic laws of algebra for real numbers to say that $(\frac{r+s}{2}) \times (\frac{r+s}{2}) = \frac{1}{4}(r^2 + 2rs + s^2)$. Subtracting rs from both sides we have: $(\frac{r+s}{2}) \times (\frac{r+s}{2}) - rs = \frac{1}{4}(r^2 + 2rs + s^2) - rs$. By the basic laws of algebra, the right hand side of this equation is equal to $(\frac{r-s}{2})^2$, and so, by substitution, $(\frac{r+s}{2})^2 - rs = (\frac{r-s}{2})^2$. Since the square of any real number is greater than or equal to 0, we have that $(\frac{r-s}{2})^2 \geq 0$ and so, by substitution, $(\frac{r+s}{2})^2 - rs \geq 0$. Adding rs to both sides, we conclude that $(\frac{r+s}{2})^2 \geq rs$.

Since r and s were arbitrary real numbers, we conclude that for all real numbers x and y $(\frac{x+y}{2})^2 \geq xy$. □

Let's discuss this proof in detail.

1. The first thing we do is to reformulate the statement to be proved using variables and quantifiers, so that the logical structure of the statement is clear. Here we are proving a universal statement whose hypothesis is "x and y are real numbers" and whose conclusion is "$xy \leq (\frac{x+y}{2})^2$".

[2]This method is a standard method of mathematical proof, but the name "arbitrary value method" is not a standard term in mathematics. We will use this name in these notes, but students should not expect to see this name elsewhere, and should not expect people outside the course to know what the "arbitrary value method" means.

2. Next, we begin the arbitrary value method. The first sentence, "Let r and s be arbitrary real numbers." is a mathematician's way of saying:

   > I am going to use the arbitrary value method to prove this statement. In this proof, r represents an arbitrary value for x and s represents an arbitrary value for y.

3. We then say clearly what we need to show: $rs \leq (\frac{r+s}{2})^2$. We then explain our overall strategy: "we will show that $(\frac{r+s}{2})^2 - rs \geq 0$."

4. So far, what we have done can be thought of us "setting up" the proof. Next comes the main part of the proof, which proceeds step by step to demonstrate that, whatever two numbers r and s are chosen, the desired conclusion holds. Each step consists of building on what has been established, and using known facts to draw a new conclusion until we reach our goal. Each step of the proof is justified by stating what general facts we are using.

5. The final paragraph summarizes by saying that since we accomplished what is needed for the arbitrary value method, the universal statement is proved.

Example. *Uniqueness theorems.* Sometimes, a given statement does not look like a universal statement but is equivalent to a universal statement. Section 1.10 in the book discusses "uniqueness theorems". Example 1.10.1 in the book presents one such statement.

> **Proposition.** There is a unique real number that is a root of the equation $x^3 + 37 = 0$.

Proving this statement requires proving two things, which normally must be proved separately. The first is to show that there is *at least one* solution to the given equation and the second is to show that there is *at most one* solution to the equation.

Showing that there is at least one solution means proving the existential statement:

> There exists a unique real number that is a root of the equation $x^3 + 37 = 0$.

To prove this, we would use the usual method by which we prove existential statements. However, by the rules we follow the following *is not an acceptable proof*:

> Let x be the cube root of -37. Then $x^3 = -37$ so $x^3 + 37 = 0$.

Why not? Because the first step assumes that there is a cube root of -37. While it is true that there is a cube root of -37, we said earlier that in this course the basic facts about square roots, cube roots and higher roots are not assumed to be known. So for this proof, we would have to prove that there is a cube root of -37. This is not so easy, and requires use of the completeness axiom presented in Section 8.4. This is a relatively difficult concept that will either be discussed later in this course, or in 311.

So we are not ready to prove the first part. Even though we can't yet prove the first part, we can still try to prove the second part, which is a separate statement. This part says: "There is at most one solution to the equation $x^3 + 37 = 0$"; in other words, this equation either has no solutions or it has precisely one solution.

Can this statement be classfied as existential or universal? Since the statement starts with "There is" we might think that it is existential. But an existential statement is one that can be written in the form "$\exists x$ such that $P(x)$." There is no statement equivalent to the given statement that has this form. On the other hand, we can reword the statement as "There do not exist numbers x and y satisfying $x^3 + 37 = 0$ and $y^3 + 37 - 0$ such that $x \neq y$.", which is *the negation of an existential statement* and is therefore equivalent to a universal statement. One way to write this universal statement is:

For all real numbers x, y, if $x^3 + 37 = 0$ and $y^3 + 37 = 0$ then $x = y$.

Now, the book gives a proof which looks something like this:

Proof. Let a and b be real numbers satisfying $a^3 + 37 = 0$ and $b^3 + 37 = 0$. Then $a^3 + 37 = b^3 + 37$ so $a^3 = b^3$. Since each real number has a unique cube root, a must equal b. □

Actually, there is a small error in the book, and "+" and "-" are confused. This error is easily corrected, but, from our point of view, there is a more serious problem with the proof, namely, that the proof is incomplete. The last sentence relies on a true statement that is not one of our known facts: "Each real number has a unique cube root." To make the proof complete we would have to justify this statement, and the book does not do this.

Here is a complete proof of the statement.

Proof. Let a and b be real numbers satisfying $a^3 + 37 = 0$ and $b^3 + 37 = 0$. We will show that $a = b$. By the hypothesis we have $a^3 + 37 = b^3 + 37$ so $a^3 = b^3$. Therefore $a^3 - b^3 = 0$. To finish the proof, we will show that $a = b$.

By basic laws of algebra, $a^3 - b^3 = (a - b)(a^2 + ab + b^2)$. Since $a^3 - b^3 = 0$, we have $0 = (a - b)(a^2 + ab + b^2)$. For the product of two numbers to be 0, at least one of them must be 0, so $a - b = 0$ or $a^2 + ab + b^2 = 0$. There are two possibilities, either $a^2 + ab + b^2 \neq 0$ or $a^2 + ab + b^2 = 0$. We will now show that in either case, $a = b$.

First consider the possibility that $a^2 + ab + b^2 \neq 0$. Then since we know that $a - b = 0$ or $a^2 + ab + b^2 = 0$, we conclude $a - b = 0$ so $a = b$.

Now consider the possibility that $a^2 + ab + b^2 = 0$. Subtracting ab from both sides, we have $a^2 + b^2 = -ab$. Since $a^2 \geq 0$ and $b^2 \geq 0$ we have $a^2 + b^2 \geq 0$ and so $-ab \geq 0$. By the basic laws of algebra, $a^2 + ab + b^2 = (a + b)^2 - ab$. Since $(a + b)^2 \geq 0$ and $-ab \geq 0$ and their sum is 0 we must have both $(a + b)^2 = 0$ and $-ab = 0$. The first condition implies $a + b = 0$ which implies $a = -b$. Substituting this into the second condition gives $b^2 = 0$ so $b = 0$ and since $a = -b$ then a is also 0. Therefore $a = b$.

Thus we have shown that $a = b$ in both cases. We therefore conclude that for all real numbers x, y, $x^3 + 37 = 0$ and $y^3 + 37 = 0$ implies $x = y$. □.

7 Universal-Existential statements

The statement "Every real number has a cube root" when carefully written using variables and quantifiers says:

For all real numbers x, there exists a real number y such that $y^3 = x$.

This statement is a universal statement because it has the form "For all x satisfying the hypothesis $H(x)$, x satisfies the conclusion $C(x)$." Here $H(x)$ is simply "x is a real number". The conclusion is somewhat complicated: "There exists a real number y such that $y^3 = x$". Here the conclusion is an existential predicate with x as free variable and a new bound variable y.

A universal statement whose conclusion is an existential predicate is called a "universal-existential" statement. The form of such a statement is:

For all x satisfying $H(x)$, there exists a y such that x and y together satisfy $Q(x, y)$.

In a universal-existential statement the variable (or variables) that are universally quantified can be thought of as the *input variable* (or variables) and the variable (or variables) that are existentially quantified can be thought of as the *output variables.* The statement above can be thought of as:

If you give me any input x that satisfies $H(x)$, I can find an output y such that $Q(x, y)$ is satisfied.

As is discussed on page 13 of the book, the order of the quantifiers matters, there is a big difference between a statement of the above form, and an *existential-universal* statement which has the form: "There exists y such that for all x satisfying $H(x)$, x and y together satisfy $Q(x, y)$."

Since a universal-existential statement is a kind of universal statement, we use the arbitrary value method to prove it. Let's see an example of a simple proof of such a statement.

Example. Prove: For all real numbers x, if $x < 2$ then there is a real number z such that $x < z$ and $z < 2$.

Here the hypothesis is "x is a real number satisfying $x < 2$." The conclusion is "There is a real number z such that $x < z$ and $z < 2$."

Intuitively, the statement says that if you give me a number x that is less than 2, I can find a bigger number that is still less than 2. Like many of the things we will prove in this course, this result seems obvious, but since we are learning to write proofs, "seems obvious" is not enough.

Before actually writing the proof, let's plan out how we will do the proof. Since this is a universal statement, we will try to prove this by the arbitrary value method. So let a be an arbitrary real number less than 2.

Now we want to show "There is a real number z such that $a < z$ and $z < 2$". This is an existential predicate that depends on the value of a. As with the proof of an existential statement we will try to do this by giving instructions for choosing the output z and then verifying that if z is chosen according to the instructions, then the conclusion holds. The difficulty here is that we don't know what a is. We want to pick z to be a *little bit bigger* than a. But it won't work to say: Choose z to be $a + .0000001$. (Why not?)

What we need to do is to give instructions for choosing z that depend on a. The difference between 2 and a is $2 - a$. If we add half of that difference to a, then we would expect the result to be bigger than a and smaller than 2. So $a + (2 - a)/2$, which simplies to $(a + 2)/2$ seems like a good choice for z.

Now that we think we know how to give instructions for picking z, we can try to write a proof.

Proof. Let a be an arbitrary real number satisfying $a < 2$. We will show that there exists a real number z such that $a < z$ and $z < 2$. Let $b = (a + 2)/2$. We show that b satisfies $a < b$ and $b < 2$.

Since $a < 2$, we can add a to both sides to get $a + a < a + 2$ and multiply both sides by $1/2$ to get $a < (a + 2)/2$. Since the expression on the right is b, we have $a < b$.

Also, since $a < 2$, we have $a + 2 < 4$ and so $(a + 2)/2 < 2$ and thus $b < 2$. We have thus shown that $a < b$ and $b < 2$. Since a was an arbitrary number less than 2, we conclude that for all real numbers x satisfying $x < 2$, there is a real number z such that $x < z$ and $z < 2$. □

Here are some additional remarks about the proof.

- The most important thing to realize about the proof of a universal-existential statement is that your job is to explain how, given as input a value a that satisfies the hypothesis, it is possible to select an output such that a and your selected output satisfy the conclusion. For this, you must (1) give precise instructions for selecting the output, and (2) carefully prove that a and and the number given by your instructions satisfy the conclusion.

- When doing universal-existential proofs, it is usually not at all obvious how to construct the output from the input. It often requires considerable thought and ingenuity. Once you think you know how to choose the output, you should try to prove it. If the proof succeeds, great! If not, then you may have to try another way to choose the output.

- Whenever you are proving the existence of something, there may be more than one choice that satisfies the required conditions. That is true here also. In this case, there are other ways to select the output. Consider the exercise below.

Exercise. Redo the above proof with output chosen to be $(2a + 6)/5$ instead of $(a + 2)/2$. Can you make the proof work with $(3a + 6)/5$ instead of $(a + 2)/2$?

Example. Here's a similar but more difficult example. Prove: For any positive real number x such that $x^2 < 2$ there is a real number w such that $x < w$ and $w^2 < 2$.

As before, we begin by planning out the proof. Using the arbitrary value method, we'll let a be an arbitrary positive real number satisfying $a^2 < 2$. This tells us that $a < \sqrt{2}$. By an argument similar to the previous proof, we should be able to prove that there is a number z such that $a < z$ and $z < \sqrt{2}$, and we should be able to deduce from this that $z^2 < 2$.

But there is a problem with this approach. The argument is correct, it is incomplete because it uses a fact that we have not yet proved: that 2 has a square root. Since we don't yet know how to prove that 2 has a square root, we must prove our statement without referring to $\sqrt{2}$.

We are given as input positive real number a that satisfies $a^2 < 2$. We are looking for a number w that is bigger than a and satisfies $w^2 < 2$. As in the previous proof we want to choose w to be "a little bit bigger" than a, but our proof must give precise instructions for choosing such a w. A good way to think about this is to think of w as a plus a small amount, and give that small amount a name. It is common to use the Greek letter ε for numbers that we think of as relatively small so let's think of w as $a + \varepsilon$. So we want to choose ε to satisfy the two requirements (i) $\varepsilon > 0$ and (ii) $(a+\varepsilon)^2 < 2$. The second requirement can be rewritten as $(2a+\varepsilon)\varepsilon < 2-a^2$, so we have to choose ε to be small enough to guarantee that the left hand side is at most the positive number $2-a^2$. Now

since $a^2 < 2$ we can deduce that $a < 2$ so for any choice of ε, $(2a+\varepsilon)\varepsilon < (4+\varepsilon)\varepsilon$. Provided that we choose $\varepsilon \leq 1$ this will be at most 5ε. So if we choose $\varepsilon = (2-a^2)/5$, then $(2a+\varepsilon)\varepsilon \leq 5\varepsilon \leq 2-a^2$ as needed.

Now that we have a good guess for how to define the output from the input, we are ready to try to write our proof.

Proof. Let a be an arbitrary positive real number that satisfies $a^2 < 2$. Our goal is to show that there is a number w such that $w > a$ and $w^2 < 2$. This is the same as showing that there is a positive number ε such that $(a+\varepsilon)^2 < 2$, since if we can find such a ε then $a+\varepsilon > a$ and $(a+\varepsilon)^2 < 2$.

Let us define $\varepsilon = (2-a^2)/5$. Since $2-a^2 > 0$, this is positive. We need to show that $(a+\varepsilon)^2$ is less than 2.

We have:

$$(a+\varepsilon)^2 = a^2 + (2a+\varepsilon)\varepsilon.$$

Now, we must have $a < 2$, since if $a \geq 2$ then $a^2 \geq 4$ which contradicts $a^2 < 2$. Also, $\varepsilon < 1$ since $\varepsilon = (2-a^2)/5 \leq 2/5$. Since $\varepsilon > 0$ we have that $(2a+\varepsilon)\varepsilon < 5\varepsilon$ and so:

$$(a+\varepsilon)^2 < a^2 + 5\varepsilon = a^2 + 5\frac{2-a^2}{5} = 2.$$

Thus $a + (2-a^2)/5 > a$ and $(a+(2-a^2)/5)^2 < 2$, and this demonstrates that there exists a number w such that $w > a$ and $w^2 < 2$. Since a was an arbitrary real number satisfying the hypothesis, we conclude that for every positive real number x such that $x^2 < 2$ there is a real number w such that $x < w$ and $w^2 < 2$. □

Example. Often, it is not obvious that a statement is a universal-existential statement. Let us consider the statement:

For all odd integers a and b, $a+b$ is even.

As we all know, this is a true universal statement. Let's see how we would go about proving it. First let's note that the hypothesis is "a and b are each odd integers" and the conclusion is "$a+b$ is even". Now the conclusion $a+b$ is even means "There exists an integer k such that $a+b=2k$." So the conclusion is an existential predicate. So this is equivalent to a universal-existential statement.

In the proof, we use the following definition of *odd*. An integer n is said to be odd provided that there is an integer d such that $n = 2d+1$.

Proof. Let v and w be arbitrary odd integers. We will show that $v+w$ must be even. By the definition of even, to show $v+w$ is even we must show that there exists an integer k such that $v+w=2k$.

Since v is odd, by definition of odd, there is an integer, which we will call s, such that $v = 2s+1$. Similarly, w is odd, so there is an integer, which we will call t, such that $w = 2t+1$. Then

$$v+w = (2s+1)+(2t+1) = 2s+2t+2 = 2(s+t+1).$$

Since s, t and 1 are integers, their sum $s+t+1$ is also an integer. Therefore we have shown that $v+w$ is 2 times some integer, namely $s+t+1$ and therefore $v+w$ is even.

8 Testing a proof using trial values

When solving mathematical problems, we all know the importance of checking your work for errors. Checking proofs is similarly important.

If we have a proof of a universal statement that uses the arbitrary value method, then one of the most useful ways to check for obvious errors is by using *trial values*. Here's how this works. Suppose we are proving a statement of the form, "For all x satisfying the hypothesis $H(x)$, x must satisfy the conclusion $C(x)$." To use the arbitrary value method and start with something like "Let a be an arbitrary number satisfying $H(a)$. We wlll prove $C(a)$." To test our proof, we select a *specific value* for a that satisfies $H(a)$ and then substitute that value for a in the main part of the proof. If our proof is correct then it should provide a proof that $C(a)$ holds for the specific value of a we selected.

Let's try this method on the last proof we did. Here we started by letting v and w be arbitrary odd integers. So let's use the trial values $v = 37$ and $w = 15$. Let's rewrite the main part of the proof with this substitution:

> We will show that $37 + 15$ must be even. By the definition of even, to show $37 + 15$ is even we must show that there exists an integer k such that $37 + 15 = 2k$. We will now give instructions for finding a value for k that satisfies the required conditions.
>
> 37 is odd and the definition of odd tells us that there is an integer, which we will call s, such that $37 = 2s + 1$. Similarly, 15 is odd, so there is an integer, which we will call t, such that $15 = 2t + 1$. Then
>
> $$37 + 15 = (2s + 1) + (2t + 1) = 2s + 2t + 2 = 2(s + t + 1).$$
>
> Since s, t and 1 are integers, their sum $s + t + 1$ is also an integer.

After this substitution, the proof still makes grammatical sense. Now, let's see if all the steps are correct.

First s is selected so that $2s+1 = 37$. We can select s to be 18, which is an integer as required. Next t is selected so that $2t+1 = 15$. Here we can select t to be 7, which is an integer as required. Next we take $s + t + 1$ which is 26, as our value of k and we check that $2k = v + w$. Since 2×26 does equal $37 + 15$, the proof passes our test.

Checking your proof using trial values is a good way to catch errors. Sometimes, are you substitute trial values you see that the result does not make sense, or that there is an obvious error (see the next example). If the proof passes your test, this does not guarantee that the proof is correct, but it provides you with additional confidence of its correctness. You should get in the habit of testing your proofs on at least one (and possibly) more trial values.

Example. Let's return to an earlier example.

> Prove: For all real numbers x, if $x < 2$ then there is a real number z such that $x < z$ and $z < 2$.

Here is a faulty proof.

Proposed proof. Let a be an arbitrary real number satisfying $a < 2$. We will show that there is a real number z such that $a < z$ and $z < 2$. We select z to be $a + .00001$.

Since $.00001 > 0$, $a + .00001 > a$. Since $a < 2$ and .00001 is a very small number $a + .00001$ is still less than 2.

Therefore $a < a + .00001$ and $a + .00001 < 2$. Since a was an arbitrary number less than 2, we conclude that for all real numbers x satisfying $x < 2$, there is a real number z such that $x < z$ and $z < 2$. □

If we use trial values to test this proof, we might try $a = 1.99$. Our instructions say to choose $z = 1.99001$ which does satisfy $1.99 < 1.99001$ and $1.99001 < 2$.

But, if we try $a = 1.999999$ then $a + .00001 = 2.000009$ which is bigger than 2. So the proof must be faulty, which means that there must be some error in reasoning. In this case, the error is fairly obvious: just because .00001 is a very small number we can't be sure that $a + .00001$ will be less than 2, because $2 - a$ might be even less than .00001.

9 The arbitrary value method and the textbook

The proofs in the textbook seem to have a different format than those in these notes and students may wonder: "Which way am I supposed to do proofs–the way they are done in the book or the way they are done in the notes."

The first thing to realize is that the differences between the proofs and those in the notes are minor. While the textbook does not actually talk about the arbitrary value method, it does use the method.

The differences in the proofs here and those in the book are primarily in the language used to get the proof started. In these notes we use a consistent format for setting up a proof by the arbitrary value method. This consistent format, while not essential, is useful for getting your proof started correctly and it is strongly recommended that you use it.

Let's look at an example of how to modify a proof in the book into the format recommended here. At the top of page 33 is a proof that "if x is an even integer then x^2 is an even integer." As we have discussed, this is a universal statement which is more properly stated as: "For all integers x, if x is even then x^2 is even." The proof given in the book uses the arbitrary value method. Here's the suggested way to write this proof:

Proof.

Let a be an arbitrary even integer. We will show a^2 is even. Since a is even, by the definition of even, there is an integer that we will call y such that $a = 2y$. We must show that there is an integer w such that $a^2 = 2w$. Since $a = 2y$ we have $a^2 = (2y)^2 = 2(2y^2)$. Now $2y^2$ is an integer since y is an integer and the product of integers is an integer. Therefore there is an integer w, namely $w = 2y^2$, such that $a^2 = 2w$ and so a^2 is even.

Since a was an arbitrary even integer, we conclude that for all integers x, if x is even then x^2 is even. □

The main difference between this proof and the one in the book is that we start our proof by introducing a new letter a to represent an arbitrary even integer. While it is not "wrong" to use the same letter x that is used in the statement of the theorem, it can lead to confusion, so it is

recommended that, for now, you use a different letter for the "arbitrary value".

Another difference is that we conclude our proofs with a sentence that summarizes what we have proved.

Let's look at another example. On page 35, the author uses "proof by contradiction" to prove "If $a > 0$ then $1/a > 0$." Again, the initial quantifier "For all real numbers a" is missing and we insert it. Here, you should think of this proof as using the arbitrary value method, combined with proof by contradiction. Here is a modified version of the proof.

Proof. Let c be an arbitrary positive real number. We will show that $1/c$ is positive. We will prove this by contradiction. Assume for contradiction that $1/c \leq 0$. Since $1/c \leq 0$ there is some nonnegative number b so that $1/a + b = 0$. Multiplying both sides of this equality by a we get $1 + ab = 0$ which implies $ab = -1$. Since $a > 0$ and $b \geq 0$ we have $ab \geq 0$. But then substituting -1 for ab we get $-1 \geq 0$ which is false, so we have the desired contradiction. Therefore our assumption that $1/c \leq 0$ must be false, and so $1/c > 0$.

Since c was an arbitrary positive real number, we conclude that for all real numbers a, if $a > 0$ then $1/a > 0$.