Foundations of Computer Science Comp109

University of Liverpool
Boris Konev
konev@liverpool.ac.uk
http://www.csc.liv.ac.uk/~konev/COMP109

Part 1. Number Systems and Proof Techniques

Comp109 Foundations of Computer Science

Reading

- S. Epp. *Discrete Mathematics with Applications*
  Chapter 4, Sections 5.2 and 5.3.
- E. Bloch. *Proofs and Fundamentals*
  Chapter 2, Section 6.3.
- K. Rosen. *Discrete Mathematics and Its Applications*
  Section 5.1.

Contents

What is a number?

The natural numbers

$$0, 1, 2, 3, \ldots$$

Key property: Any natural number can be obtained from 0 by applying the operation $S(n) = n + 1$ some number times.

Examples: $S(0) = 1$.

$S(S(0)) = 2$.

$S(S(S(0))) = 3$.

Prime numbers

A prime number is a integer greater than 1 which has exactly two divisors that are positive integers: 1 and itself.

$$2, 3, 5, 7, 11, 13, 17, 19, 23, 29, 31, 37, 41, 43, \ldots$$

Every natural number greater than 1 can be written as a unique product of prime numbers.

Examples: $6 = 2 \times 3$. $15 = 3 \times 5$. $1400 = 2^3 \times 5^2 \times 7$.

Example: prime and composite numbers

1. Is 1 prime?
2. Is every integer greater than 1 either prime or composite?
3. Write the first six prime numbers.
4. Write the first six composite numbers.

Beyond naturals

The Integers $\ldots, -2, -1, 0, 1, 2, \ldots$

The Rational Numbers all numbers that can be written as $\dfrac{m}{n}$ where m and n are integers and n is not 0.

Reminder: Algebraic manipulation

Solving and computing

Mathematics underpins STEM subjects. In many cases, we are concerned with solving and computing

The quadratic equation $2x^2 + 6x + 7 = 0$ has roots α and β.

Write down the value of $\alpha + \beta$ and the value of $\alpha\beta$.

Complete the table of values for $y = 3 - x^2$

x	−3	−2	−1	0	1	2	3
y		−1	2		2		−6

Work out $\frac{1}{3} \times \frac{1}{5}$

Find the general solution, in degrees, of the equation

$$2\sin(3x + 45°) = 1$$

5 miles = 8 kilometres

Which is longer, 26 miles or 45 km?

Statements

Which of the following are true?

- "26 miles is longer than 45 km."
- An integer doubled is larger than the integer.
- The sum of any two odd numbers is even.

The moral of the story

- We can't believe a statement just because it appears to be true.

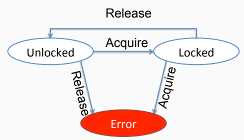
We need a proof that the statement is true or a proof that it is false.

Do we care?

Example: Drivers behaviour[1]

```
do {
    KeAcquireSpinLock();
    nPacketsOld = nPackets;
    if (request) {
        request = request->Next;
        KeReleaseSpinLock();
        nPackets++;
    }
} while (nPackets != nPacketsOld);
KeReleaseSpinLock();
```

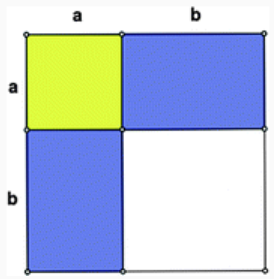
Does this code obey the locking rules?



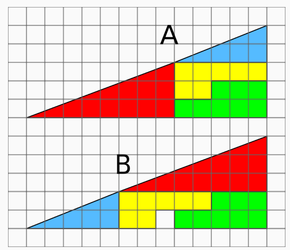
You don't need to understand the actual code!

[1] from Microsoft presentations on Static Driver Verifier (part of Visual Studio)

Historical detour: Visual proofs



Visual proof of $(a + b)^2 = a^2 + 2ab + b^2$



Visual "proof" of 32.5 = 31.5

Proofs

- A mathematical proof is as a **carefully reasoned argument** to convince a sceptical listener (often yourself) that a given statement is true.
- Both discovery and proof are integral parts of problem solving. When you think you have discovered that a certain statement is true, try to figure out why it is true.
- If you succeed, you will know that your discovery is genuine. Even if you fail, the process of trying will give you insight into the nature of the problem and may lead to the discovery that the statement is false.

Example: Odd and even numbers

Definition

An integer n is **even** if, and only if, n equals twice some integer.
An integer n is **odd** if, and only if, n equals twice some integer plus 1.

Symbolically, if n is an integer, then

n is even $\Leftrightarrow \exists$ an integer k such that $n = 2k$.
n is odd $\Leftrightarrow \exists$ an integer k such that $n = 2k + 1$.

Notice the use of $\Leftrightarrow$ $\exists$ $\forall$.

Example: Properties of odd and even numbers

Use the definitions of even and odd to justify your answers to the following questions.

Definition

n is even $\Leftrightarrow \exists$ an integer k such that $n = 2k$.
n is odd $\Leftrightarrow \exists$ an integer k such that $n = 2k + 1$.

1. Is 0 even?
2. Is 301 odd?

Example: Properties of odd and even numbers

Definition

n is even $\Leftrightarrow \exists$ an integer k such that $n = 2k$.
n is odd $\Leftrightarrow \exists$ an integer k such that $n = 2k + 1$.

3. If a and b are integers, is $6a^2b$ even?
4. If a and b are integers, is $10a + 8b + 1$ odd?
5. Is every integer either even or odd?

Existence proofs

Statements of the form $\exists x\ Q(x)$

Examples:

1. Prove the following: $\exists$ an even integer n that can be written in two ways as a sum of two prime numbers.
2. Suppose that r and s are integers. Prove the following: $\exists$ an integer k such that $22r + 18s = 2k$.

Constructive proof

- One way to prove
$$\exists x\ Q(x)$$
is to find an x in that makes $Q(x)$ true.

Proving universal statements

The vast majority of mathematical statements to be proved are universal. In discussing how to prove such statements, it is helpful to imagine them in a standard form:
$$\forall x \text{ if } P(x) \text{ then } Q(x)$$

For example,

- If a and b are integers then $6a^2b$ is even.

Proving universal statements: The method of exhaustion

Some theorems can be proved by examining relatively small number of examples.

- Prove that $(n + 1)^3 \geq 3^n$ if n is a positive integer with $n \leq 4$.
  - $n = 1$
  - $n = 2$
  - $n = 3$
  - $n = 4$
- Prove for every natural number n with $n < 40$ that $n^2 + n + 41$ is prime.

Motivating example: "Mathematical trick"

Pick any number, add 5, multiply by 4, subtract 6, divide by 2, and subtract twice the original number. The answer is 7.

Step	Visual Result	Algebraic Result
Pick a number.	□	x
Add 5.	□|||||	$x + 5$
Multiply by 4.	□||||| □||||| □||||| □|||||	$(x + 5) \cdot 4 = 4x + 20$
Subtract 6.	□|| □|| □||||| □|||||	$(4x + 20) - 6 = 4x + 14$
Divide by 2.	□|| □|||||	$\frac{4x + 14}{2} = 2x + 7$
Subtract twice the original number.	|| |||||	$(2x + 7) - 2x = 7$

Generalising from the Generic Particular

The most powerful technique for proving a universal statement is one that works regardless of the choice of values for x.

To show that every x satisfies a certain property, suppose x is a particular but arbitrarily chosen and show that x satisfies the property.

Method of direct proof

- Express the statement to be proved in the form
$$\text{"}\forall x, \text{ if } P(x) \text{ then } Q(x).\text{"}$$
(This step is often done mentally.)
- Start the proof by supposing x is a particular but arbitrarily chosen element for which the hypothesis $P(x)$ is true.
(This step is often abbreviated "Suppose P(x).")
- Show that the conclusion $Q(x)$ is true by using definitions, previously established results, and the rules for logical inference.

Prove that the sum of any two even integers is even

Prove that every integer is rational

Prove that the sum of any two rational numbers is rational

Prove that the product of any two rational numbers is rational

Prove that the double of a rational number is rational

Prove for all integers n, if n is even then n^2 is even

Prove by cases: Combine generic particulars and proof by exhaustion

Statement: For all integers n, $n^2 + n$ is even

Case 1: n is even

Case 2: n is odd

How about

Prove for all integers m and n, if $m^2 = n^2$ then $m = n$?

Disproving universal statements by counterexample

To disprove a statement means to show that it is false. Consider the question of disproving a statement of the form

$$\forall x, \text{ if } P(x) \text{ then } Q(x).$$

Showing that this statement is false is equivalent to showing that its negation is true. The negation of the statement is existential:

$$\exists x \text{ such that } P(x) \text{ and not } Q(x).$$

Is it true that for every positive integer n, $n^2 \geq 2n$?

Indirect proofs

- In a direct proof you start with the hypothesis of a statement and make one deduction after another until you reach the conclusion.
- Indirect proofs are more roundabout. One kind of indirect proof, argument by contradiction, is based on the fact that either a statement is true or it is false but not both.
- So if you can show that the assumption that a given statement is not true leads logically to a contradiction, impossibility, or absurdity, then that assumption must be false: and, hence, the given statement must be true.

Motivating example: Trial and error

5	3			7				
6			1	9	5			
	9	8					6	
8				6				3
4			8		3			1
7				2				6
	6					2	8	
			4	1	9			5
				8			7	9

Use proof by contradiction to show that there is no greatest integer

Use proof by contradiction to show that there is no smallest positive rational number

Use proof by contradiction to show that no integer can be both even and odd

Use proof by contradiction to show that there is no greatest prime number

Let $f(x) = 2x + 5$. Prove that if $x \neq y$ then $f(x) \neq f(y)$

Direct proof

Proof by contradiction

When to use indirect proof

- Many theorems can be proved either way. Usually, however, when both types of proof are possible, indirect proof is clumsier than direct proof.
- In the absence of obvious clues suggesting indirect argument, try first to prove a statement directly. Then, if that does not succeed, look for a counterexample.
- If the search for a counterexample is unsuccessful, look for a proof by contradiction

The real numbers

All (decimal) numbers — distances to points on a number line.

Examples.

- -3.0
- 0
- 1.6
- $\pi = 3.14159\ldots$

A real number that is not rational is called irrational.

But are there any irrational numbers?

Proving that $\sqrt{2}$ is not a rational number

Proof by contradiction.

- If $\sqrt{2}$ were rational then we could write it as $\sqrt{2} = x/y$ where x and y are integers and y is not 0.
- By repeatedly cancelling common factors, we can make sure that x and y have no common factors so they are not both even.
- Then $2 = x^2/y^2$ so $x^2 = 2y^2$ so x^2 is even. This means x is even, because the square of any odd number is odd.

the proof continued

- Let $x = 2w$ for some integer w.
- Then $x^2 = 4w^2$ so $4w^2 = 2y^2$ so $y^2 = 2w^2$ so y^2 is even so y is even.
- This contradicts the fact that x and y are not both even, so our original assumption, that $\sqrt{2}$ is rational, must have been wrong.

Prove that $1 + 3\sqrt{2}$ is irrational

Mathematical induction

- Mathematical induction is one of the more *recently* developed techniques of proof in the history of mathematics.
- It is used to check conjectures about the outcomes of processes that occur repeatedly and according to definite patterns.
- In general, mathematical induction is a method for proving that a property defined for integers n is true for all values of n that are greater than or equal to some initial integer

Example: Domino effect

One domino for each natural number, arranged in order.

- I will push domino 0 (the one at the front of the picture) towards the others.
- For every natural number m, if the m'th domino falls, then the $(m+1)$st domino will fall.

Conclude: All of the Dominoes will fall.

Proving by induction that a property holds for every natural number n

- Prove that the property holds for the natural number $n = 0$.
- Prove that if the property holds for $n = m$ (for any natural number m) then it holds for $n = m + 1$.

The validity of proof by mathematical induction is generally taken as an axiom. That is why it is referred to as the principle of mathematical induction rather than as a theorem.

A proof of a property by induction looks like this

Base Case: Show that the property holds for $n = 0$.

Inductive Step: Assume that the property holds for $n = m$. Show that it holds for $n = m + 1$.

Conclusion: You can now conclude that the property holds for every natural number n.

Example: Proof by induction

For every natural number n,

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

Base Case: Take $n = 0$. The left-hand-side and the right-hand-side are both 0 so they are equal.

Inductive Step: Assume that the property holds for $n = m$, so

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

Now consider $n = m + 1$. We must show that

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

Proof continued

Since

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

$$\begin{aligned} 0 + 1 + \cdots + m + (m+1) &= \frac{m(m+1)}{2} + m + 1 \\ &= \frac{m(m+1) + 2(m+1)}{2} \\ &= \frac{(m+1)(m+2)}{2} \end{aligned}$$

Other starting values

Suppose you want to prove a statement not for all natural numbers, but for all integers greater than or equal to some particular natural number b

Base Case: Show that the property holds for $n = b$.

Inductive Step: Assume that the property holds for $n = m$ for any $m \geq b$. Show that it holds for $n = m + 1$.

Conclusion: You can now conclude that the property holds for every integer $n \geq b$.

Example: Proof by induction

For all integers $n \geq 8$, n¢ can be obtained using 3¢ and 5¢ coins.

Base Case: For $n = 8$, 8¢ = 3¢ + 5¢.

Inductive Step: Suppose that m¢ can be obtained using 3¢ and 5¢ coins for any $m \geq 8$. We must show that $(m + 1)$¢ can be obtained using 3¢ and 5¢ coins.

Consider cases

- There is a 5¢ coin among those used to make up the m¢.
  - Replace the 5¢ coin with two 3¢ coins. We obtain $(m + 1)$¢.
- There is no 5¢ coin among those used to make up the m¢.
  - There are three 3¢ coins ($m \geq 8$).
    - Replace the three 3¢ coins with two 5¢ coins

Example: Proof by induction

For every integer $n \geq 3$, $4^n > 2^{n+2}$.

Base Case: Take $n = 3$. Then $4^n = 4^3 = 64$. Also, $2^{n+2} = 2^5 = 32$. So $4^n > 2^{n+2}$.

Inductive Step: For any $m \geq 3$, assume that the statement $4^m > 2^{m+2}$ is true. (This is called the "inductive hypothesis".) Now consider $n = m + 1$. We must show that $4^{m+1} > 2^{(m+1)+2} = 2^{m+3}$.

Here is the calculation. $4^{m+1} = 4 \times 4^m$. But by the inductive hypothesis, $4 \times 4^m > 4 \times 2^{m+2}$. Finally,

$$4 \times 2^{m+2} > 2 \times 2^{m+2} = 2^{m+3}.$$

Using induction to show that a program is correct

What does the following program do?

```
i = 0
M = 0
mylist = [1, 2, 6, 3, 4, 5]
while i < len(mylist):
      M = max(M, mylist[i])
      i = i + 1
print M
```


Using induction to show that a program is correct

```
i = 0
M = 0
mylist = [1, 2, 6, 3, 4, 5]
while i < len(mylist):
      M = max(M, mylist[i])
      i = i + 1
print M
```

Property: After the statement M = max(M , mylist[i]) gets executed, the value of M is max(mylist[0],...,mylist[i]).

Proof by induction

Property: After the statement M = max(M, mylist[i]) gets executed, the value of M is max(mylist[0],...,mylist[i]).

Base Case: Take i=0. Before the statement, M=0, so the statement assigns M to be the maximum of 0 and mylist[0], which is mylist[0].

Inductive Step: Assume that the statement is true for i=m for some m≥ 0. Now consider i=m+1. The statement assigns M to be the maximum of mylist[m+1] and max(mylist[0],...,mylist[m]), so after the statement, M is max(mylist[0],...,mylist[m+1]).

Strong induction

- Prove that the property holds for the natural number $n = 0$.
- Prove that **if** the property holds for $n = 0, 2, \ldots, m$ (and not just for m!) **then** it holds for $n = m + 1$.

Can also be used to prove a property for all integers greater than or equal to some particular natural number b

Example: Proof by strong induction

Every natural number $n \geq 2$, is a prime or a product of primes.

Base Case: Take $n = 2$. Then n is a prime number.

Inductive Step: Assume that the property holds for $n = m$ so *every* number i s.t. $2 \leq i \leq m$ is a prime or a produce of primes. Now consider $n = m + 1$.

Example: Number of multiplications

For any integer $n \geq 1$, if $x_1, x_2, \ldots, x_n$ are n numbers, then no matter how the parentheses are inserted into their product, the number of multiplications used to compute the product is $n - 1$.

Bad proofs: Arguing from example

An incorrect "proof" of the fact that the sum of any two even integers is even.

This is true because if $m = 14$ and $n = 6$, which are both even, then $m + n = 20$, which is also even.

Bad proofs: Using the same letter to mean two different things

Consider the following "proof" fragment:

Suppose m and n are any odd integers. Then by definition of odd, $m = 2k + 1$ and $n = 2k + 1$ for some integer k.

Bad proofs: Jumping to a conclusion

To jump to a conclusion means to allege the truth of something without giving an adequate reason.

Suppose m and n are any even integers. By definition of even, $m = 2r$ and $n = 2s$ for some integers r and s. Then $m + n = 2r + 2s$. So $m + n$ is even.

Bad proofs: Circular reasoning

To engage in circular reasoning means to assume what is to be proved.

Suppose m and n are any odd integers. When any odd integers are multiplied, their product is odd. Hence mn is odd.

Bad proofs: Confusion between what is known and what is still to be shown

Suppose m and n are any odd integers. We must show that mn is odd. This means that there exists an integer s such that

$$mn = 2s + 1.$$

Also by definition of odd, there exist integers a and b such that

$$m = 2a + 1 \text{ and } n = 2b + 1.$$

Then

$$mn = (2a + 1)(2b + 1) = 2s + 1.$$

So, since s is an integer, mn is odd by definition of odd.

Good proofs in practice[2]

State your game plan.

A good proof begins by explaining the general line of reasoning, for example, "We use case analysis" or "We argue by contradiction."

[2] *Mathematics for Computer Science* by E. Lehman, F. T. Leighton, and A. R. Meyer.

Good proofs in Practice

Keep a linear flow.

Sometimes proofs are written like mathematical mosaics, with juicy titbits of independent reasoning sprinkled throughout. This is not good. The steps of an argument should follow one another in an intelligible order.

Good proofs in practice

A proof is an essay, not a calculation.

Many students initially write proofs the way they compute integrals. The result is a long sequence of expressions without explanation, making it very hard to follow. This is bad. A good proof usually looks like an essay with some equations thrown in. Use complete sentences.

Good proofs in practice

Structure your proof

- Theorem—A very important true statement.
- Proposition—A less important but still interesting statement.
- Lemma—A true statement used to prove other statements.
- Corollary—A simple consequence of a theorem or a proposition.

Finish

> *At some point in a proof, you'll have established all the essential facts you need. Resist the temptation to quit and leave the reader to draw the "obvious" conclusion. Instead, tie everything together yourself and explain why the original claim follows.*