Foundations of Computer Science Comp109

University of Liverpool
Boris Konev
konev@liverpool.ac.uk

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

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: $S(0) = 1$.

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

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

Beyond naturals: Integers

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

> *God made the integers, all else is the work of man*
>
> (Leopold Kronecker)

Beyond integers: Rationals and Reals

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

The Real Numbers all (decimal) numbers — distances to points on a number line.

Mathematical proof

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

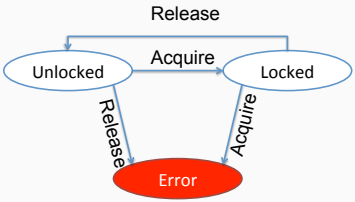
- We can't believe a statement just because it appears to be true.

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

Example: Drivers behaviour[1]

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

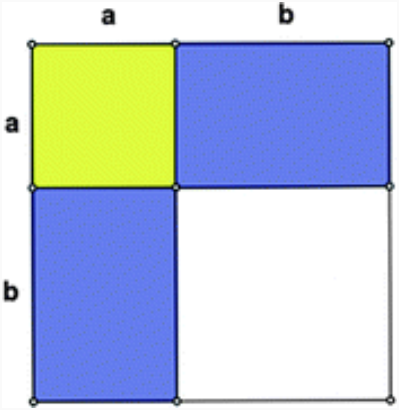
Does this code obey the locking rules?



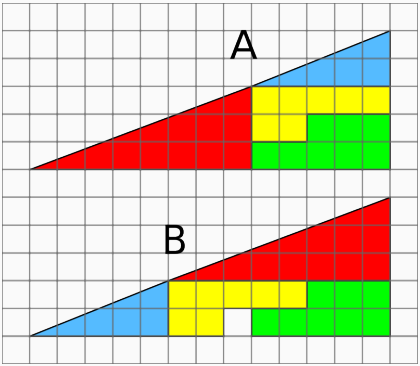
You don't need to understand the actual code!

[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: Properties of odd and even numbers

1. Is 0 even?
2. Is -301 odd?
3. Is the sum of any two odd numbers even?
4. Is every number either even or odd?

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 $\Leftrightarrow$ $\exists$ $\forall$.

Using the definition to justify an answer

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?

More examples

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?

Proving existential statements

Existential statements

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

- The easiest way to prove

  $$\exists x\, Q(x)$$

  is to find an x that makes $Q(x)$ true.

Examples of constructive proof

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 $22r + 18s = 2k$.

More than one variable

$\exists x\ Q(x)$

- there $\exists$ integers m and n such that $m > 1$, $n > 1$ and $\frac{1}{m} + \frac{1}{n}$ is an integer

Proving universal statements

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.

Generalising from the Generic Particular

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

Proof

Suppose that m and n are particular but arbitrarily chosen even integers.
Since m is even, by definition of even, $m = 2k$, for some integer k.
Since n is even, by definition of even, $n = 2l$, for some integer l.
Substituting into $m + n$ we obtain $m + n = 2k + 2l = 2(k + l)$. As $k + l$ is an integer, by definition of even, $m + n$ is even.

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

Proof

Suppose that n is a particular but arbitrarily chosen even integer.
Since n is even, by definition of even, $n = 2k$, for some integer k.
Substituting into n^2 we obtain $n^2 = (2k)^2 = 4k^2 = 2(2k^2)$. As $2k^2$ is an integer, by definition of even, n^2 is even.

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

No, this statement is not true. 1 is an integer, so for $n = 1$, $n^2 = 1$ and $2n = 2$. Obviously, $1 \ngeq 2$.

The statement becomes true if we additionally require n to be greater than or equal to 2.

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 this true?

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

This statement is not true. For $m = -2$ and $n = 2$ we have $m^2 = (-2)^2 = 4 = (2)^2 = n^2$, however, $-2 \neq 2$.
The statement becomes true for natural m, n.

Goldbach's conjecture

Every even integer greater than 2 is the sum of two primes.
(Christian Goldbach (1690–1764))

- $4 =$
- $6 =$
- $8 =$
- $10 =$
- $12 =$
- ...
- up to 10^{17}

Fermat's last theorem

No three positive integers a, b, and c satisfy the equation

$$a^n + b^n = c^n$$

for any integer value of n greater than 2.

- Conjectured around 1637 by Pierre de Fermat (1607-1665)
- Proved 1995 by Andrew Wiles

More examples of direct proof

Prove that every integer is rational

Proof

Suppose that m is a particular but arbitrarily chosen integer.
Consider $r = \frac{m}{1}$.
By definition, r is a rational number and obviously $r = m$. Hence every integer is rational.

Prove that the sum of any two rational numbers is rational

Proof

Suppose that r and s are particular but arbitrarily chosen rational numbers.
By definition of a rational number $r = \frac{k}{l}$, where k and l are integers and $l \neq 0$.
By definition of a rational number $s = \frac{m}{n}$, where m and n are integers and $n \neq 0$.
Then $r + s = \frac{k}{l} + \frac{m}{n} = \frac{k \cdot n + l \cdot m}{l \cdot n}$.
By properties of integers, $k \cdot n + l \cdot m$ and $l \cdot n$ are integers, and as $l \neq 0$ and $n \neq 0$ we have $l \cdot n \neq 0$.
So by definition of rational, $r + s = \frac{k \cdot n + l \cdot m}{l \cdot n}$ is rational.

Prove that the product of any two rational numbers is rational

Proof

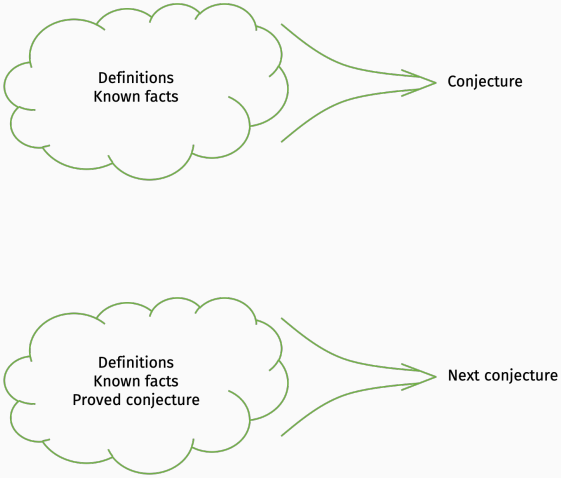
Suppose that r and s are particular but arbitrarily chosen rational numbers.
By definition of a rational number $r = \frac{k}{l}$, where k and l are integers and $l \neq 0$.
By definition of a rational number $s = \frac{m}{n}$, where m and n are integers and $n \neq 0$.
Then $r \cdots = \frac{k}{l} \cdot \frac{m}{n} = \frac{k \cdot m}{l \cdot n}$.
By properties of integers, $k \cdot m$ and $l \cdot n$ are integers, and as $l \neq 0$ and $n \neq 0$ we have $l \cdot n \neq 0$.
So by definition of rational, $r \cdots = \frac{k \cdot m}{l \cdot n}$ is rational.

Prove that the double of a rational number is rational

Proof

Suppose that r is a particular but arbitrarily chosen rational number.
As every integer is a rational number, 2 is rational.
Applying the result on the previous slide we conclude that $2 \cdot r$ is rational.

Mathematical discovery



Proof by cases

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

By definition of even, $n = 2k$ for some integer k. Then $n^2 + n = (2k)^2 + 2k = 4k^2 + 2k = 2(2k^2 + k)$. By Definition of even, $n^2 + n$ is even.

Case 2: n is odd

By definition of odd, $n = 2l + 1$ for some integer l. Then $n^2 + n = (2l + 1)^2 + (2l + 1) = 4l^2 + 4l + 1 + 2l + 1 = 4l^2 + 6l + 2 = 2(2l^2 + 3l + 1)$. By Definition of even, $n^2 + n$ is even.

Prove that the product of any two consecutive integers is even

Proof

Suppose that two particular but arbitrarily chosen consecutive integers are given. Call them m and $m+1$.
We proceed by considering cases.

- Case 1 m is odd.

  By definition of odd, $m = 2k+1$ for some integer k. Then $m \cdot (m+1) = (2k+1) \cdot ((2k+1+1)) = (2k+1) \cdot (2k+2) = (2k+1) \cdot (2 \cdot (k+1)) = 2 \cdot ((2k+1) \cdot (k+1))$. As $(2k+1) \cdot (k+1)$ is an integer, $m \cdot (m+1)$ is even by definition of even

- Case 2 m is even.

  By definition of even, $m = 2l$ for some integer l. Then $m \cdot (m+1) = (2l) \cdot (2l+1) = 2l \cdot (2l+1)$. As $l \cdot (2l+1)$ is an integer, $m \cdot (m+1)$ is even by definition of even

Thus regardless of which case actually occurs, the product of the particular m and $m+1$ is even. As m is chosen arbitrarily, the product of any two consecutive integers is always even.

The square of any integer is of the form $3k$ or $3k+1$

Proof

We require the following property of integers: every integer can be represented as one of $3l$, $3l+1$ or $3l+2$. We do not prove this property, however, its truth can be seen from exploring remainders of division of l by 3.

Suppose that n is a particular by arbitrarily chosen integer.

Consider cases.

Case 1 $n = 3l$, for some integer l. Then $n^2 = (3l)^2 = 3(3l^2)$, so n is of the form $3k$ for $k = 3l^2$.

Case 2 $n = 3l + 1$, for some integer l. Then $n^2 = (3l+1)^2 = 9l^2 + 6l + 1 = 3(3l^2 + 2) + 1$, so n is of the form $3k+1$ for $k = 3l^2 + 2$.

Case 3 $n = 3l + 2$, for some integer l. Then $n^2 = (3l+2)^2 = 9l^2 + 12l + 4 = 9l^2 + 12l + 3 + 1 = 3(3l^2 + 6l + 1) + 1$, so n is of the form $3k+1$ for $k = 3l^2 + 6l + 1$.

Regardless of which case actually occurs, the square of any integer is of the form $3k$ or $3k+1$.

Indirect proofs

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

Motivating example: Proof beyond a reasonable doubt

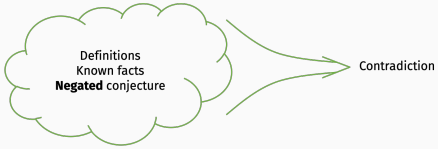
Proving that a defendant is guilty.

- Is it conceivable that the defendant is not guilty?
  - Is being not guilty compatible with the presented evidence?
  - If not, the defendant must be guilty

Direct proof vs proof by contradiction

- Direct proof:

- Proof by contradiction:



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

Proof

Suppose for a proof by contradiction that the is the greatest integer N. Consider $N + 1$. The sum of integers is an integer and $N + 1 > N$, a contradiction. Therefore, there is no greatest integer.

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

Proof

Suppose for a proof by contradiction that some integer n is both even and odd.

By definition of even, $n = 2k$, for some integer k.

By definition of odd, $n = 2l + 1$, for some integer l.

Then, $2k = n = 2l + 1$, so $1 = 2l - 2k = 2(l - k)$, so 1 is even, a contradiction.

Therefore, no integer can be both even and odd.

Show for any integer m, if m^2 is even then m is even

Proof

Suppose for a proof by contradiction that there exists an integer m such that m^2 is even but m is not. As every number is either even or odd, m must be odd. Then $m = 2l + 1$, for some integer l.

Then $m^2 = (2l + 1)^2 = 4l^2 + 2l + 1 = 2(2l^l + l) + 1$ and so m^2 is odd by definition of odd, which is a contradiction.

Therefore, for any integer m, if m^2 is even then m is even.

Proof by contraposition

To prove

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

it suffices to prove

$$\forall x \text{ if } \textbf{not } Q(x) \text{ then } \textbf{not } P(x)$$

Two classic results

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

Proof

Suppose for a proof by contradiction that there exists a greatest prime number. Then we can enumerate all prime numbers, $p_1, p_2, p_3, \ldots, p_N$, where $p_1 = 2$, $p_2 = 3$, $p_3 = 5$ etc and p_N being the greatest prime number. So that there are no prime numbers except $p_1, \ldots, p_N$. Consider $P = p_1 \cdot p_2 \cdot \cdots \cdot p_N + 1$.

Every number is either prime or composite.

Consider cases.

Case 1 P is prime. Since P is larger than any of $p_1, \ldots, p_N$, this contradicts the fact that P_N is the largest prime number

[1] Known to Euclid 300BC

proof continued

Case 2 P is composite. Then P must have a factor other than 1 and P itself.

By repeatedly factorising the factor it can be seen that P must have a prime factor. Since $p_1, \ldots, p_N$ is the list of all primes, one of them must divide P; let this prime be p_i. So, P can be written as $p_i \cdot k$ for some integer k.

On the other hand, p_i is one of $p_1, \ldots, p_N$ so $p_1 \cdot \cdots \cdot p_N$ can be written as $p_i \cdot l$ for some integer l.

By rearranging terms, $P - p_1, \ldots, p_N = 1$. By substitution, $p_i \cdot k - p_i \cdot l = 1$ or $p_i(k - l) = 1$, which means 1 is divisible by a prime number p_i, a contradiction.

Regardless which case takes place, we derive a contradiction. Therefore, there is no greatest prime number.

Recall: 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?

Prove 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.
- 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.

[1] Known to Pythagoras 300BC

proof continued

Indirect proof of an existential statement

Prove that there exist irrational numbers q and r such that q^r is rational.

Proof

The number $\sqrt{2}^{\sqrt{2}}$, as any other real number, is either rational or irrational. Consider cases

Case 1 $\sqrt{2}^{\sqrt{2}}$ is irrational. Then $q = \sqrt{2}^{\sqrt{2}}$ and $r = \sqrt{2}$ and we are done.

Case 2 $\sqrt{2}^{\sqrt{2}}$ is rational. Then $q = \sqrt{2}^{\sqrt{2}}$ and $r = \sqrt{2}$. Notice that $q^r = (\sqrt{2}^{\sqrt{2}})^{\sqrt{2}} = \sqrt{2}^{(\sqrt{2}\cdot\sqrt{2})} = \sqrt{2}^2 = 2$, so we are done.

In both cases we can demonstrate the existence of irrational q, r such that q^r is rational, but this proof does not tell us which case holds.

(In fact, $\sqrt{2}^{\sqrt{2}}$ is irrational, but this requires deeper mathematics)

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

Mathematical induction

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

Generic particular vs induction for universal statements

- Generalisation from the generic particular:
  "Suppose that x is a particular but arbitrarily chosen ..."
  ..."property holds for this x"...
  "...then the property holds for all x"

- Induction
  Some kind of a process that goes over the elements of a set

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 some initial value (e.g. $n = 0$).
- **Prove** that if the property holds for m (for any natural number m) then it holds for $m + 1$.

A proof of a property by induction looks like this

We prove the statement by mathematical induction on n.

Base Case: Show that the property holds for some initial value (e.g. $n = 0$).

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

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

Carl Friedrich Gauss (1777-1855)

$$1 + \cdots + 100 = 5050$$

$$1 + 2 + \cdots + 100 = (1 + 100) + (2 + 99) + \cdots + (50 + 51) = 50 \cdot 101 = 5050$$

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 m, so

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

Proof continued

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

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

Since

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

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

$1+3+\cdots+(2n+1)=(n+1)^2$ for every natural number n

Base Case:

Take $n=0$. The left-hand-side and the right-hand-side are both 1 so they are equal.

Inductive Step:

Assume that the property holds for m, so $1+3+\cdots+(2m+1)=(m+1)^2$.

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

$$1+3+\cdots+(2m+1)+(2(m+1)+1)=((m+1)+1)^2.$$

Since

$$1+3+\cdots+(2m+1)=(m+1)^2,$$

$$\begin{aligned}1+3+\cdots+(2m+1)+(2(m+1)+1) &= (m+1)^2+2(m+1)+1\\ &= ((m+1)+1)^2\end{aligned}$$

Proof continued

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

Base Case: For $n = 8$

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

Proving properties of programs

Using induction to show that a program is correct

What does the following program do?

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

Using induction to show that a program is correct

```
mylist = [1, 2, 6, 3, 5, 6]
i = 0
M = mylist[0]
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=mylist[0], so the statement assigns M to be the maximum of mylist[0] and mylist[0], which is mylist[0].

Inductive Step: Assume that the statement is true for i=m for some $m \geq 0$. 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]).

Computing $1 * 2 * \cdots * n$

```
def f(n):
    f = 1
    for i in range(n):
        f = f*(i+1)
    return f
```

```
def g(n):
    if (n==1):
        return 1
    return g(n-1)*n
```

Prove by induction that $g(n) = 1 * 2 * \cdots * n$

Base case: for $n = 1$ the function immediately returns 1. So $g(1) = 1$, as required.

Induction step: suppose that g correctly computes $1 * 2 * \cdots * m$ for some m. We need to show that the result of computation $g(m + 1)$ is correct. By definition of g, $g(m + 1) = g((m + 1) - 1) * (m + 1) = g(m) * (m + 1)$. By induction hypothesis, $g(m) = 1 * 2 * \cdots * m$, so $g(m + 1) = 1 * 2 * \cdots * m * (m + 1)$ as required.

Strong induction

Strong induction

- Prove that the property holds for the natural number $n = 0$.
- Prove that **if** the property holds for $n = 0, 1, \ldots, m$ (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 m so *every* number i s.t. $2 \leq i \leq m$ is a prime or a product of primes. Now consider $m + 1$.

Consider cases

Case 1 $m + 1$ is prime. There is nothing to prove in this case.

Case 2 $m + 1$ is composite. Then $m + 1$ has a factor k different from 1 and $m + 1$ itself. Let $m + 1 = k \cdot l$. Clearly, l is also different from 1 and $m + 1$. So, k and l are integers s.t. $2 \leq k \leq m$ and $2 \leq l \leq m$. By induction hypothesis, k and l are primes or products of primes. Then $k \cdots l$ is a product of primes.

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 $n - 1$.

We prove the statement by strong induction.

base case For $n = 1$ the sequence contains just one number and the number of multiplications needed is 0. In other words, the number of multiplications is $n - 1$ (as $n = 1$).

induction step Suppose that the statement holds for m, that is, for every sequence of i numbers, where $2 \leq q \leq m$ it takes $m - 1$ multiplications to compute the product of $x_1, \ldots, x_m$.

Now consider $n = m + 1$. Let $x_1, \ldots, x_{m+1}$ be the numbers we want to multiply. Suppose that we group them with paranthesis so that there are l numbers in the first group and $m + 1 - l$ in the second:

$$(x_1, x_2, \ldots, x_l) \cdot (x_{l+1}, \ldots, x_{m+1}) .$$

Proof continued

By induction hypothesis, it takes $l-1$ multiplications to compute the product of $x_1,\ldots, x_l$ and $(m+1-l)-1$ multiplications to compute the product of $x_{l+1},\ldots, x_{m+1}$. It takes one more multiplication to multiply these products. Overall, it takes $l-1+(m+1-l)-1+1 = l-1+m+1-l-1+1 = m$ multiplicaitons. As $n = m+1$, $m = n-1$ and so it takes $n-1$ multiplications. Thus, no matter how the parantheses are inserted, the number of multiplications is $n-1$.

Common mistakes

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

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

Then

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

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

Good practice

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.

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.*