Durham University

Maths for Computer Science
Calculus

Prof. Magnus Bordewich

Proof

Direct Proof

Start with **hypotheses** or **premises**.

Make logical steps from the hypothesis by applying:

- axioms
- rules of inference (e.g. 1st order logic)
- previous theorems

Reach desired conclusion.

Example:

For $n \in \mathbb{N}$, if n^2 is even, then n is even.

Proof:

Let the prime factorization of n be $n = p_1 p_2 \dots p_k$.

Then $n^2 = p_1^2 p_2^2 \dots p_k^2$.

Since n^2 is even, one of p_i must be 2.

Hence n is also even.

Durham University

Proof by Contradiction

Theorem: $\boldsymbol{p}$

Proof:

- **Assume $\boldsymbol{not\ p}$**
- Show that $not\ p \Rightarrow q$, where q is known to be false.
- If $not\ p \Rightarrow q$, then it cannot be the case that $not\ p$ holds.
- Therefore p.

Theorem: $\sqrt{2} \notin \mathbb{Q}$

Proof:

- **Assume $\sqrt{2} \in \mathbb{Q}$**, i.e. $\sqrt{2} = \frac{m}{n}$, where $\frac{m}{n}$ is a simplified fraction.
- Then $\frac{m^2}{n^2} = 2$, so $m^2 = 2n^2$ and m therefore must be even.
- Let $m = 2k$. Then $4k^2 = 2n^2$, and $2k^2 = n^2$, so n is also even.
- Hence $\frac{m}{n}$ is not a simplified fraction, which contradicts our assumption.
- Since this contradiction followed logically from our assumption, it must be that our assumption is wrong! I.e. $\sqrt{2} \notin \mathbb{Q}$.
- So in fact $\mathbb{Q} \subset \mathbb{R}$.

Theorem: $\mathbb{R}$ is uncountable

Proof: (Cantor's Diagonalization argument)

- Assume for contradiction that there is a bijection f between $\mathbb{R}$ and $\mathbb{N}$.
- Consider all the elements of $\mathbb{R}$ between 0 and 1 listed in order of increasing f.
  - 0.5647388294856378393948573738 94…
  - 0.01100245678394655388485764535462…
  - 0.12500000000450000000000000000…
  - Etc.
- Create a new number $0.x_1x_2x_3x_4$ ... where the digit x_i is 5 if the i^{th} digit of the i^{th} number in the list is not a 5, and 4 if i^{th} digit of the i^{th} number is 5.
- 0.454…. This new number differs from every number in the list but is a real number – a contradiction. Hence our assumption must be wrong, i.e. there is no bijection.

Mathematical proof

Theorem: If **hypotheses** then **conclusion**.

The proof of a statement uses only these components:

- the **hypotheses** of the theorem (that is, the things assumed to be true in the theorem)
- **axioms** known to be true
- previously proved **theorems**
- **rules of inference** (that is, allowable rules that can be used to infer new mathematical statements from existing ones).

Mathematical proof

We have seen a two types of proof so far:

- Direct proofs
- Proof by contradiction

There are other proof types too:

- Proof by contraposition
- Proof by case analysis
- Proof by induction

Durham University

Proof by contraposition

Theorem: If hypotheses then conclusion.

Proof by contraposition: Not conclusion ⇒ not hypotheses

Example: If n is an integer and $3n + 2$ is odd then n is odd.

Proof: Assume the negation of what we want to prove; that is, assume that n is even. So, $n = 2k$, for some integer k.

Thus, $3n + 2 = 6k + 2$ is even.

Hence, if n is even then $3n + 2$ is even ⇒ if $3n + 2$ is odd then n is odd.

Proof by case analysis

Theorem: If hypotheses then conclusion.

Proof by case analysis: One of a), b), c) must occur. If a) … proof of conclusion, if b)… proof of conclusion, and if c) … proof of conclusion. Hence conclusion!

Example: If n is a natural number then $\sum_{i=1}^{n} i = \frac{n(n+1)}{2}$.

Proof: Either a) n is even or b) n is odd.

a) If $n = 2k$,

then $\sum_{i=1}^{n} i = \sum_{i=1}^{k} i + \sum_{i=k+1}^{2k} i = \sum_{i=1}^{k} i + (2k + 1 - i) = k(2k + 1) = \frac{n(n+1)}{2}$.

a) b) If $n = 2k + 1$,

then $\sum_{i=1}^{n} i = \sum_{i=1}^{k} i + (k + 1) + \sum_{i=k+2}^{2k+1} i = \sum_{i=1}^{k} (2k + 2) + (k + 1)$

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

Proof by induction

Theorem: Statement $S(n)$ holds for all integers $n \geq j$, for a fixed integer j.

Proof by induction:

1) **Base case**: Check that $S(j)$; If this is not the case,

then the statement cannot be true. If $S(j)$ is true, then proceed to Step 2.

2) **Induction Step**: Prove the following conditional statement.
If $S(n)$ holds for a fixed value $n \geq j$ *(Ind. Hypothesis)* then $S(n+1)$ also holds.

The two steps together then imply that $S(n)$ holds for $n = j$ by 1), for $n = j + 1$ by 2), for $n = j + 2$ by 2), … and so on, so it holds for all $n \geq j$.

Example: Proving $\forall \mathrm{n} \in \mathbb{N}, n \leq 2^n$ by induction

Theorem: $n \leq 2^n$ for all $n \geq 0$.

Proof by induction:

1) **Base case**: If $n = 0$, then $2^n = 1$, so $n \leq 2^n$ holds.
2) **Induction Step**: Let $k \geq 1$ be an integer. The inductive hypothesis is that the statement holds for $n = k$, that is, $k \leq 2^k$.
   Now suppose $n = k + 1$. Then
   $$n = k + 1 \leq 2^k + 1 \leq 2^k + 2^k = 2^{k+1} = 2^n$$
   The first inequality above is by the inductive assumption.

Since the statement is valid for $n = 0$, and it is valid for $n = k + 1$ if it is valid for $n = k$, we conclude that it is valid for all non-negative integers n.

Example: Insertion sort

Insertion sort:

Given an unordered array of n numbers A

Insertion(A):

if $n \leq 1$

  return A

else

  L = Insertion($A[0{:}\, n-2]$)

  L = L append $A[n-1]$

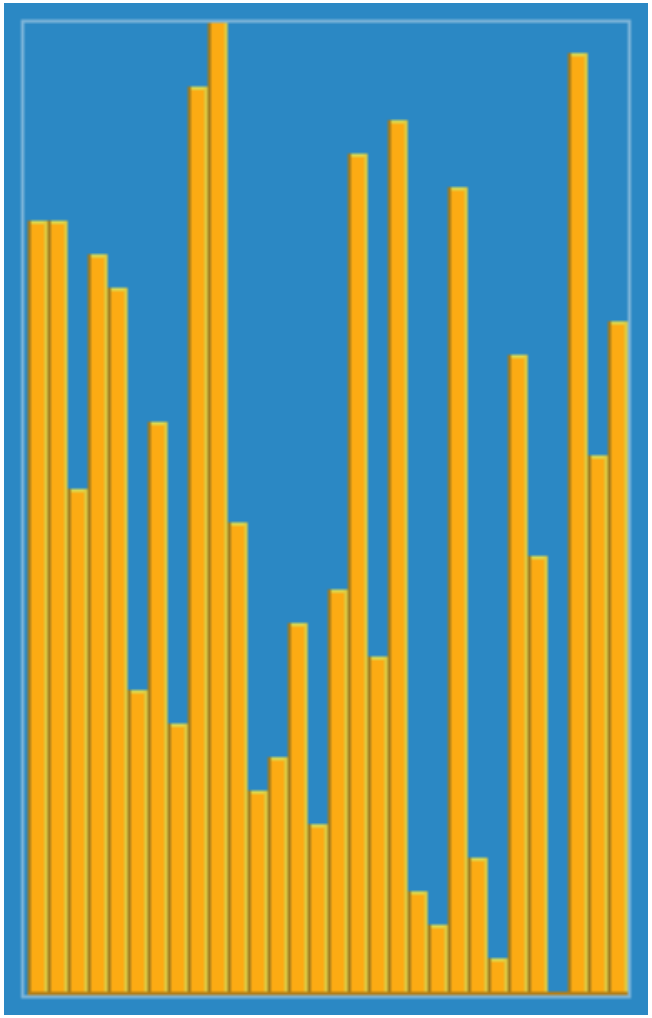
  $j = n - 1$

  while $j > 0$ **and** $L[j-1] > L[j]$

    swap $L[j-1], L[j]$

    $j = j - 1$

  return L



Source: Simpsons contributor
https://commons.wikimedia.org/wiki/File:Insertion_sort.gif

Durham University

Example: Insertion sort

Insertion sort is correct

Statement: For all $n \in \mathbb{N}$, if $|A| = n$, **Insertion sort** returns the correctly sorted list.

Proof by induction:

Base case: If $|\mathrm{A}| = 1$, then we return A, which is sorted.

Induction step: Suppose Insertion(A) is sorted for all sets A such that $|A| = k$. Consider a set A such that $|A| = k + 1$.

Let $B = A \setminus A[n-1]$, then $|B| = k$, and by hypothesis Insertion(B) is correctly sorted.

The final element $A[n-1]$ is appended then moves down until it reaches a point t where $B[t-1] \leq A[n-1] < B[t+1]$.

Since $B[0{:}\, t-1]$ and $B[t+1{:}\, n-1]$ where already sorted, B is still sorted, and the inductive step holds.

Therefore, by induction, the statement holds for all $n \in \mathbb{N}$.

Durham University

Variations on induction

Standard induction:

Base case: $S(0)$ holds

Inductive step: $S(n) \Rightarrow S(n+1)$, for $n \geq 0$.

Variant:

Base case: $S(0), S(1), S(2)$ hold

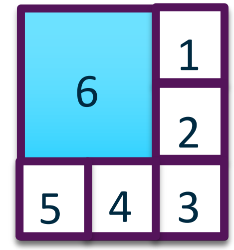
Inductive step: $S(n) \Rightarrow S(n+3)$, for $n \geq 0$.

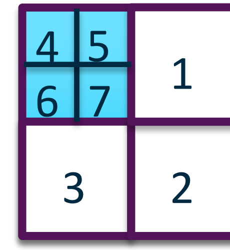
Strong induction:

Base case: $S(0)$ holds

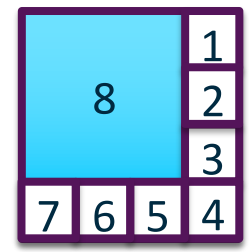
Inductive step: $\forall k, 0 \leq \mathrm{k} \leq \mathrm{n}, S(k) \Rightarrow S(n+1)$, for $n \geq 0$.

Variations on induction: step size



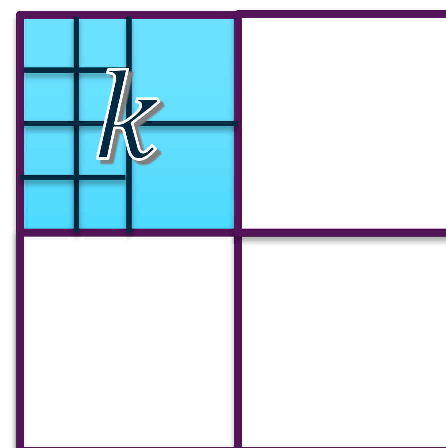


Theorem: For any $n \in \mathbb{N}, n \geq 6$, it is possible to subdivide a square in n smaller squares.



Proof:

The inductive step is easy if we jump in 3s!



Ind. Step: Assume true for $n = k \geq 6$.

Subdivide a square into quarters.

Subdivide one quarter into k smaller squares.

Square is now sub divided into $k + 3$ squares.

Triangulations

3D geometric models are usually built out of polygons. In order to computationally process a complicated surface, the polygons are **triangulated**:

- A **polygon** is a closed geometric figure formed by a sequence of line segments $s_1 \dots, s_n$ called sides, meeting at vertices.
- A polygon is **simple** if no two non-consecutive sides intersect.
- A **diagonal** is a line segment connecting two non-consecutive vertices. An **interior diagonal** is one that lies entirely inside the polygon.
- A **triangulation** is the repeated addition of interior diagonals until all remaining polygons are triangles.

Durham University

Triangulations

There are many possible triangulations of a polygon. Do they all have the same size?

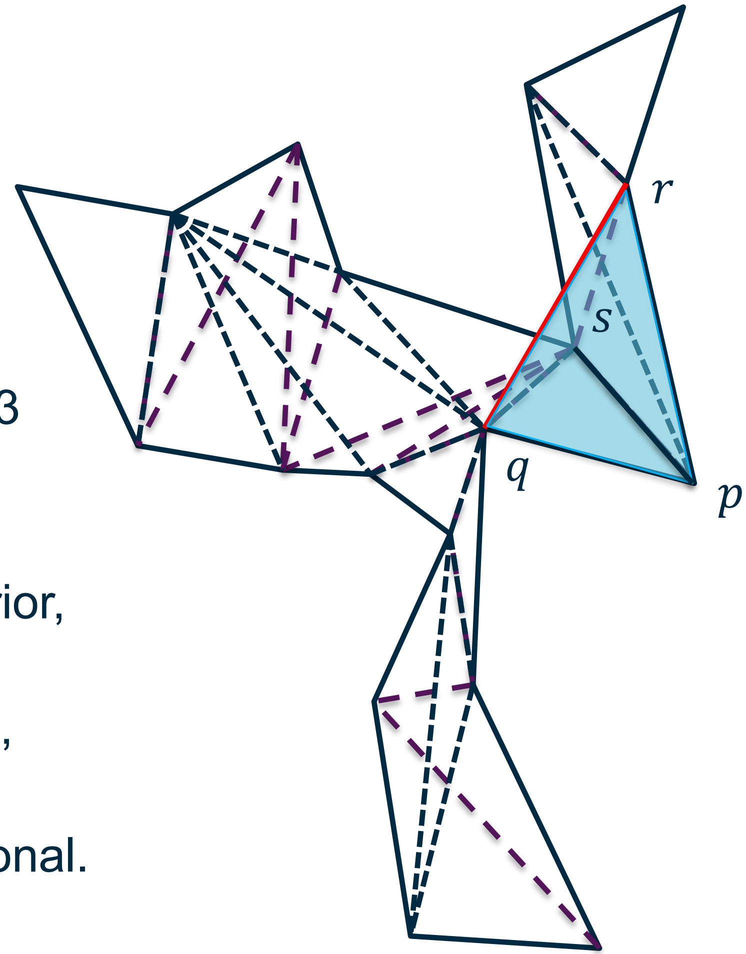
Lemma: Every simple polygon with more than 3 sides has an interior diagonal.

Proof: Pick a convex vertex p, e.g. rightmost.

Let the neighbours of p be q and r. If qr is interior, we are done.

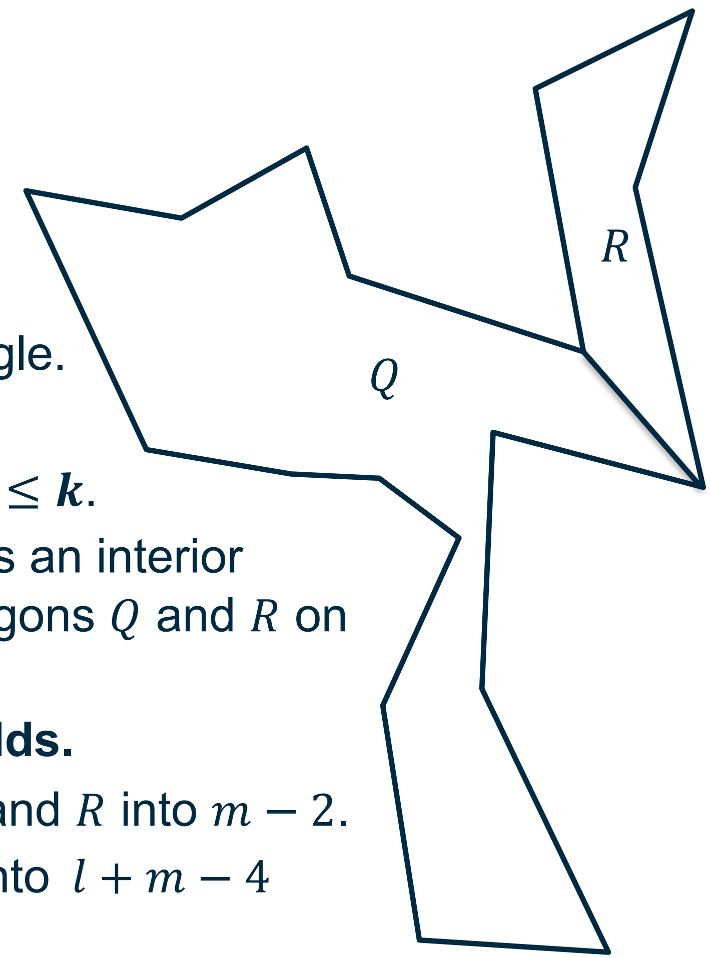
Otherwise there is a vertex s in the triangle pqr,

If more than one pick closest to p in direction perpendicular to qr. Then sp is an interior diagonal.



Durham University

Variations on induction: Strong Induction



Theorem: Every simple polygon with $n \geq 3$ sides can be triangulated into $n - 2$ triangles.

Proof: Base case: If $n = 3$, it is already 1 triangle.

Ind. Step:

Assume the statement holds for all $\boldsymbol{n, 3 \leq n \leq k}$.

Let $n = k + 1 > 3$. Then, by the lemma, there is an interior diagonal which splits the polygon into two polygons Q and R on l and m sides, where $l + m = k + 3$.

$\boldsymbol{3 \leq l, m \leq k}$ so the inductive hypothesis holds.

Then Q can is triangulated into $l - 2$ triangles and R into $m - 2$.

Therefore the original polygon is triangulated into $l + m - 4$

$= k - 1 = n - 2$ triangles.