Maths for Computing

Lecture 4

Thomas Nowotny
Chichester 1, Room CI 105
t.nowotny@sussex.ac.uk

“The domino effect”

INDUCTION

Example 2

- Francesco Maurolico (1575)
- First known proof by induction.

$$P(n)\ :\ \sum_{i=1}^{n}(2i-1) = 1+3+5+\ldots+2n-1 = n^2$$

Example 2 continued

- $P(1) \; : \; 1 = 1^2$ … is true.
- Assume P(n) is true, need to show P(n+1) is then also true.
- Write P(n+1) in terms of P(n):

$$P(n+1) \; : \; \sum_{i=1}^{n+1} 2i - 1 = \underbrace{\sum_{i=1}^{n} 2i - 1}_{=n^2 \text{ by Ind.}} + 2(n+1) - 1$$

$$= n^2 + 2n + 1 = (n+1)^2$$

Example 2 concluded

- So, if P(n) is true, P(n+1) is true
- And P(1) is true.

- Therefore, **by mathematical induction**,

$$\Rightarrow \forall n \in \mathbb{N} : P(n)$$

Example 3

"Geometric series"

Claim:

$$P(n)\ :\ \sum_{i=0}^{n} q^i = 1 + q + q^2 + q^3 + \ldots + q^n$$

$$= \frac{1 - q^{n+1}}{1 - q}$$

Example 3: Start

$$P(1)\ :\ \frac{1-q^2}{1-q} = \frac{(1-q)\cdot(1+q)}{1-q}$$

$$= 1 + q = \sum_{i=0}^{1} q^i$$

… so P(1) is true.

Assume now P(n) is true.

Example 3: Induction step

$$P(n+1)\ :\ \sum_{i=0}^{n+1} q^i = \underbrace{\sum_{i=0}^{n} q^i}_{=\frac{1-q^{n+1}}{1-q}} + q^{n+1}$$

by assumption

$$= \frac{1-q^{n+1}}{1-q} + q^{n+1}\frac{1-q}{1-q}$$

$$= \frac{1-q^{n+1}+q^{n+1}-q^{n+2}}{1-q}$$

$$= \frac{1-q^{n+2}}{1-q} = \frac{1-q^{(n+1)+1}}{1-q}$$

Example 3: Conclusion

By induction it follows that

$$\sum_{i=0}^{n} q^i = \frac{1 - q^{n+1}}{1 - q} \quad \forall \quad n \in \mathbb{N}$$

Proof complete.
Qed

Things about induction

- Mathematical induction can <u>only</u> be used to prove arguments for positive, whole numbers – i.e., the **natural numbers** $\mathbb{N}$.
- No need to start with P(1). Sometimes it is easier to start with P(3) or P(4) etc.
- But then the inductive proof will only be valid for P(>=3) or P(>=4) etc.

Induction and recursion

- Mathematical induction is important in computer science because it allows us to prove things about **recursive** programs.
- A recursive function is a **function that calls itself**.
- Recursion is the basis of several programming languages, e.g., PROLOG.


metro
Woman spotted yesterday reading today's paper

Recursive programming

- A technique for simplifying a problem by dividing it into subproblems of the same type.
- For example, consider this function of the factorial:

```
function n= Factorial(nm)
  if (nm <= 1)
    n= 1;
  else
    n= nm*Factorial(nm-1);
  end
end
```

Proof of correctness

Proof by induction:

1. n=1:
```
if (nm <= 1)
    n= 1;
else ...
```
$1! = 1$ Ok!

2. Now assume it is correct for n;

3. Induction: ...
```
else
   n= nm*Factorial(nm-1);
end
```
is correct by assumption $= (n-1)!$

Proof of correctness complete

Furthermore,

$$n! = n \cdot (n-1) \cdot (n-2) \cdot \ldots \cdot 2 \cdot 1 = n \cdot (n-1)!$$

…

```
  else
    n= nm*Factorial(nm-1);
  end
```

$$= (n-1)!$$

Therefore, n= nm! … the function does always return the correct value. Done.

Practical tips about Induction

- If you don’t use the assumption, you are not doing proof by induction! BB1
- Sometimes it is useful to “work from two sides” BB2
- If you forget any of the steps it is not a proof!   BB3
  (especially the start is often forgotten)

BB1 Using the assumption

Example 2 again:
We are trying to do the Induction step to show

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

Induction step:

This is “n” -> we can use the assumption here!

$$\sum_{i=1}^{n+1} 2i - 1 = \sum_{i=1}^{n} 2i - 1 + \text{something}$$

BB2 "Coming from two sides"

We need to show

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

"From the left":

$$\sum_{i=1}^{n+1} 2i - 1 = \left(\sum_{i=1}^{n} 2i - 1\right) + 2(n+1) - 1$$

using the assumption ↙ simplifying ↙

$$= n^2 + 2(n+1) - 1 = n^2 + 2n + 1$$

BB "Coming from two sides …"

"From the right":

$$(n+1)^2 = n^2 + 2n + 1$$

↑

simplifying

"From the left":

$$n^2 + 2n + 1$$

"From the right":

$$n^2 + 2n + 1$$

It's equal – success!

Wrong Wrong

BB3 Forgotten start

"Proof" that for all numbers $n = n - 1$:

1. (forgotten start)

2. Assumption: True for n, i.e. $n = n - 1$

3. Induction:

$$n + 1 = (n - 1) + 1 = n$$ q.e.d

Using assumption: $n = n - 1$

Wrong Wrong

Summary

Proof by induction always has 3 parts:

1. Start: e.g. show P(n) for n=0, or n=1
2. Assumption: P(n) is true
3. Induction step: show that P(n+1) is true using P(n)

SETS AND INTERVALS

Sets

- Sets are collections of things (typically numbers); the things in a set are called elements of the set

- Examples $\mathbb{N}$ $\mathbb{Z}$ $\mathbb{Q}$ $\mathbb{R}$ $\mathbb{C}$

- General notation:

Curly brackets for enumerating elements

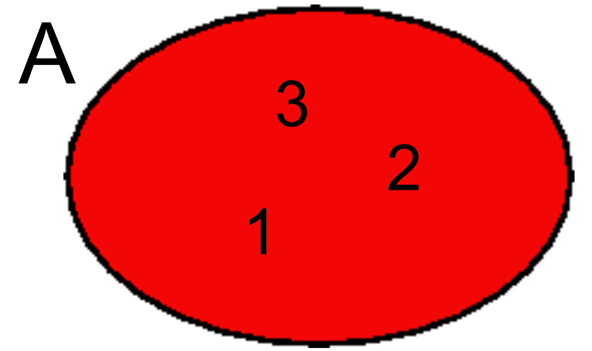
Explicit list of elements $\{1, 2, 3, 4\}$

… or description with a condition:

Examples: Set notation

$$\mathbb{N} = \{1, 2, 3, 4, \ldots\}$$

$$A = \{x \in \mathbb{N} \ : \ x < 4\} = \ \{1, 2, 3\}$$



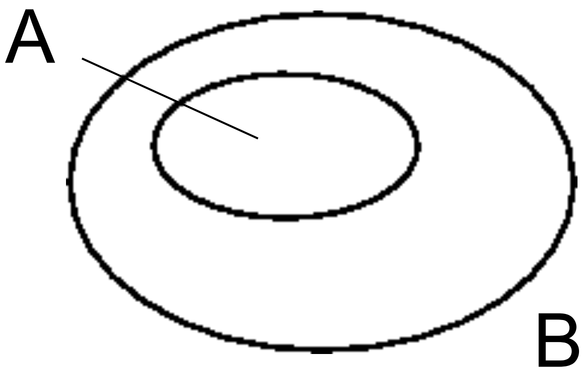
$$\mathbb{Q} = \{a/b \ : \ a \in \mathbb{Z}, \, b \in \mathbb{Z} \backslash \{0\}\}$$

“for which”

“is an element of”

“without”

Set relations



$A \subset B$ "A is a subset of B"

$A \subseteq B$ "A is a subset of or equal to B"

$B \supset A$ "B is a superset of A"

$B \supseteq A$ "B is a superset of or equal A"

Examples: Set relations

$$A = \{1, 2, 3, 4, 5, 6\},\ B = \{1, 2, 3\}$$

$$A \supset B \quad A \supseteq B$$

$$A = \mathbb{N},\ B = \mathbb{R}$$

$$A \subset B \quad A \subseteq B$$

Cardinality

The **cardinality** of a set A is the number of elements in the set:

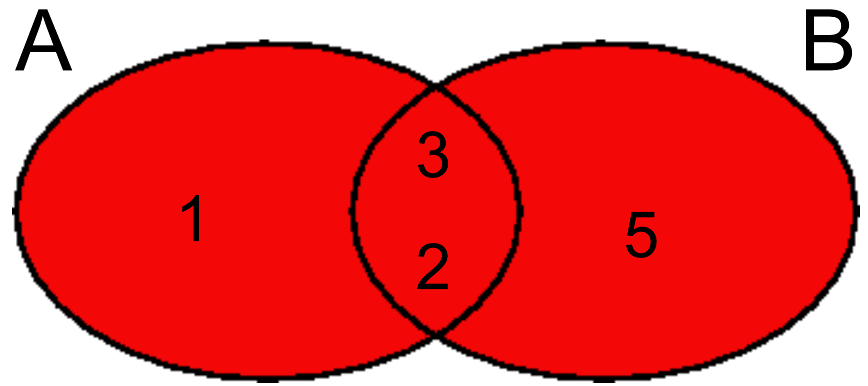
$$A = \{1, 2, 5, 19\}$$

$$\mathrm{card}(A) = |A| = 4$$

$$\mathrm{card}(\mathbb{N}) = \infty$$ (More precisely $\aleph_0$)

$$\mathrm{card}(\mathbb{R}) = \infty$$ (More precisely $\aleph_1$)

Set operations



Union:

$$A \cup B = \{x : x \in A \text{ or } x \in B\}$$

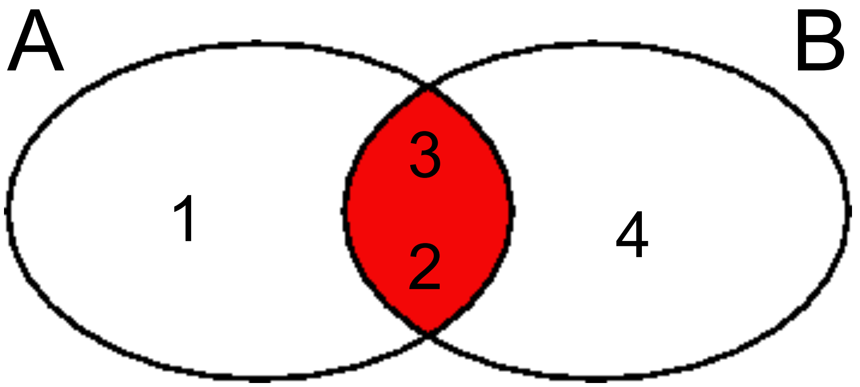
Examples:

No duplication of elements!

$$\{1, 2, 3\} \cup \{2, 3, 5\} = \{1, 2, 3, 5\}$$

$$\{1, 2, 3, \ldots\} \cup \{-1, -2, -3, \ldots\} \cup \{0\} = \mathbb{Z}$$

Set Operations



Intersection:

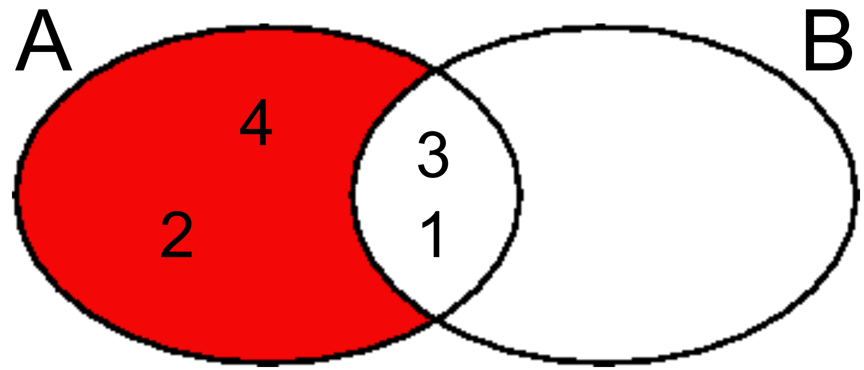
$$A \cap B = \{x : x \in A \ \text{ and } \ x \in B\}$$

Examples:

$$\{1, 2, 3\} \cap \{2, 3, 4\} = \{2, 3\}$$

$$\mathbb{N} \cap \mathbb{Z} = \mathbb{N}$$

Set Operations



Subtraction:

$$A \setminus B = \{x \in A \;:\; x \notin B\}$$

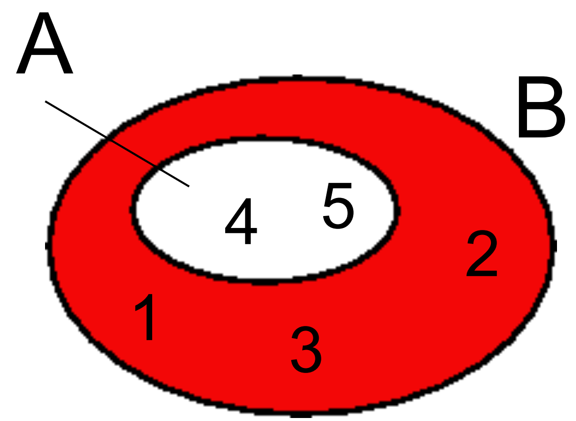
alternative notation: $A - B$

Example:

$$\{1, 2, 3, 4\} \setminus \{1, 3\} = \{2, 4\}$$

I like to read “without”

Set operations



Complement:

If $A \subset B$ then $A^C = B \setminus A$

" A^C is the complement of A in B "

Example:

$B = \{1, 2, 3, 4, 5\}$ $A = \{4, 5\}$

$A^C = \{1, 2, 3\}$

Dictionary of set theory

Symbol	Meaning	Symbol	Meaning
$\in$	Element of	$\{\ldots\}$	Set of elements
$\subset, \subseteq$	Subset	$\setminus$	Subtract, “without”
$\supset, \supseteq$	Superset	^{c}	Complement
$\cap$	Intersection	card	Cardinality
$\cup$	Union	$\emptyset$	**Empty set**

Intervals

- Special type of sets, parts of $\mathbb{R}$

In the following: $x, y \in \mathbb{R}$ and $x < y$

$$[x, y] = \{z \in \mathbb{R} : x \leq z \leq y\}$$

All numbers between x and y (**boundaries included**)

Other intervals

alternative notation

$$]x, y[= \{z \in \mathbb{R} : x < z < y\} = (x, y)$$

… as before but **boundaries not included**

$$]x, y] = (x, y]$$

$$[x, y[= [x, y)$$

… and so on.

Important

- Different brackets mean completely different things!

$[x, y]$

All numbers of $\mathbb{R}$ between x and y, including x and y. **Infinitely many numbers!**

$\{x, y\}$

Literally, just the numbers x and y. **2 numbers**