

## Quantifiers

$\forall x$  “for all  $x$ ” universal quantifier  
 $\exists x$  “there exists an  $x$  such that” existential quantifier

N.B. *Scoping*: “Every man loves a woman”

- $\forall x \exists y \text{ loves}(x, y)$

i.e. Becks loves Posh, Tony loves Cherie, Tom loves Katie ...

- $\exists y \forall x \text{ loves}(x, y)$

i.e. Becks loves Posh, Tony loves Posh, Tom loves Posh ...

## Induction

Say we wish to prove:  $\forall x \in \mathbb{N} : P(x)$

The principle of mathematical induction has the following form:

$$P(0)$$

$$P(n) \Rightarrow P(n + 1)$$

$$\therefore \forall x : P(x)$$

The hypotheses are:

H1:  $P(0)$  (the *basis step*)

H2:  $P(n) \Rightarrow P(n + 1)$  for arbitrary  $n$   
(the *inductive step*)

We first prove that the predicate is true for 0

We then show that assuming the predicate is true for an element  $n$  (the *inductive hypothesis*), then this implies it is true for element  $n + 1$

## Induction

---

Then:

- knowing  $P$  is true for the first element means it must be true for the element following the first (the second element)
- knowing it is true for the second element implies it is true for the third

and so forth.

It is like a row of dominos:

If the  $n^{\text{th}}$  domino falls over the  $(n + 1)^{\text{th}}$  must fall over, so pushing the first one down means all must fall down.

## Induction

---

For example, to prove:

$$P(n) = \sum_{i=0}^n i = \frac{n(n+1)}{2}$$

i.e.  $1 + 2 + 3 + \dots + n = \frac{n(n+1)}{2}$

We first prove H1:

$$P(0) : \sum_{i=0}^0 i = \frac{0(0+1)}{2}$$

We then state the induction hypothesis: if the statement holds for  $n = m$ , then it also holds for  $n = m + 1$ .

Assume  $P(n)$  is true when  $n = m$ ,  
i.e.  $1 + 2 + \dots + m = \frac{m(m+1)}{2}$ .

Adding  $m + 1$  (clearly the LHS's next term) to both sides gives:

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

## Induction

---

We can manipulate this RHS algebraically:

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

Thus we have:

$$1 + 2 + \dots + (m + 1) = \frac{(m+1)((m+1)+1)}{2}$$

which is exactly  $P(m + 1)$ .

We assumed that  $P(m)$  was true, and from that we derived  $P(m + 1)$ . Symbolically we showed that:  
 $P(m) \Rightarrow P(m + 1)$

By mathematical induction we have established H2, so  $P(n)$  is true for all  $n$ .

## Breadth-First Search

---

Used in situations with countably infinite sets.

Given a countable set of countably infinite sets  $A_0, A_1 \dots A_n$ , and an element  $x$ , is  $x$  a member of at least one  $A_i$ ?

Step 1: Is  $x$  the first element of  $A_0$ ?

Step  $k$ : Is  $x$  the  $k$ -th element of  $A_0$ , the  $k-1$ -th element of  $A_1$ , the  $k-2$ -th element of  $A_2 \dots$  the 1st element of  $A_{k-1}$ ?

Recall that a set is countable if:

- it is finite, or
- Its cardinality is  $\aleph_0$  (aleph 0).

## Breadth-First Search

The set of positive rational numbers  $\mathbb{Q}^+$  is countably infinite.

**Proof:**  $\mathbb{Z}^+$  is a subset of  $\mathbb{Q}^+$  so  $|\mathbb{Z}^+| = \aleph_0 \leq |\mathbb{Q}^+|$ . Now we have to show that  $|\mathbb{Q}^+| \leq \aleph_0$ .

To do this we show that the set of positive rational numbers with repetitions,  $\mathbb{Q}_R$ , is countably infinite.

Then, since  $\mathbb{Q}^+$  is a subset of  $\mathbb{Q}_R$ , it follows that  $|\mathbb{Q}^+| \leq \aleph_0$  and hence  $|\mathbb{Q}^+| = \aleph_0$

x	1	2	3	4	5	6	7
1	1/1	2/1	3/1	4/1	5/1	6/1	7/1
2	/	2/2	3/2	4/2	5/2	6/2	7/2
3	/	2/3	3/3	4/3	5/3	6/3	7/3
4	/	2/4	3/4	4/4	5/4	6/4	7/4
5	/						

The position on the path (enumeration) indicates the image of the bijective function  $f$  from  $\mathbb{N}$  to  $\mathbb{Q}_R$ :

$$f(0) = 1/1, f(1) = 1/2, f(2) = 2/1, f(3) = 3/1, \dots$$

## Countably Infinite Sets

The set of (finite length) strings  $S$  over a finite alphabet  $A$  is countably infinite. To show this we assume that

- $A$  is nonvoid
- There is an alphabetical ordering of the symbols in  $A$

**Proof:** List the strings in lexicographic order:

- all the strings of zero length,
- then all the strings of length 1 in alphabetical order,
- then all the strings of length 2 in alphabetical order, etc.

This implies a bijection from  $\mathbb{N}$  to the list of strings and hence it is a countably infinite set.

For example: Let  $A = \{a, b, c\}$

Then the lexicographic ordering of  $A$  is:

$$\{\epsilon, a, b, c, aa, ab, ac, ba, bb, bc, ca, cb, cc, aaa, aab, aac, aba, \dots\} = \{f(0), f(1), f(2), f(3), f(4), \dots\}$$

## Uncountable Sets & Diagonalisation

---

**Theorem:** The set of real numbers between 0 and 1 is uncountable.

**Proof:** We assume that it is countable and derive a contradiction.

If the set is countable we can list the elements (i.e. there is a bijection from a subset of  $\mathbb{N}$  to the set).

We show that no matter what list you produce we can construct a real number between 0 and 1 which is not in the list. Hence, there cannot exist a list and therefore the set is not countable

It's actually much bigger than countable. It is said to have the *cardinality of the continuum*,  $\mathfrak{c}$ . Represent each real number in the list using its *decimal expansion*.

$$\begin{aligned} \text{e.g., } 1/3 &= .3333333\text{.....} \\ 1/2 &= .5000000\text{.....} \\ &= .4999999\text{.....} \end{aligned}$$

If there is more than one expansion for a number, it doesn't matter as long as our construction takes this into account.

## Uncountable Sets

---

The enumeration is as follows:

$$\begin{aligned} r_1 &= .d_{11}d_{12}d_{13}d_{14}d_{15}d_{16} \dots \\ r_2 &= .d_{21}d_{22}d_{23}d_{24}d_{25}d_{26} \dots \\ r_3 &= .d_{31}d_{32}d_{33}d_{34}d_{35}d_{36} \dots \\ &\vdots \end{aligned}$$

Now construct the number  $x = .x_1x_2x_3x_4x_5x_6x_7\dots$

$$\begin{aligned} x_i &= d_{ii} + 1, & \text{if } d_{ii} < 9 \\ &= 0, & \text{otherwise} \end{aligned}$$

Then  $x$  is not equal to any number in the enumeration.

Hence, no such enumeration can exist, the interval  $(0,1)$  is uncountable.

This proof technique is called *Cantor diagonalisation*. This is an important technique for showing that sets cannot be countable.