

Sets

A **set** is a collection or group of objects or *elements* or *members*. (Cantor 1895)

- A set is said to *contain* its elements.
- There must be an underlying universal set U , either specifically stated or understood.

Notation:

- list the elements between braces:

$$S = \{a, b, c, d\} = \{b, c, a, d, d\}$$

- specification by predicates:

$$S = \{x | P(x)\},$$

S contains all the elements from U which make the predicate P true.

- brace notation with ellipses:

$$S = \{\dots, -3, -2, -1\},$$

the negative integers.

Common Universal Sets

- \mathbb{R} = reals
- \mathbb{N} = natural numbers = $\{0, 1, 2, 3, \dots\}$, the *counting* numbers
- \mathbb{Z} = integers = $\{\dots, -3, -2, -1, 0, 1, 2, 3, 4, \dots\}$
- \mathbb{Q} = rationals = m/n , where $m, n \in \mathbb{Z}, n \neq 0$

Notation:

x is a member of S or x is an element of S :

$$x \in S$$

x is not an element of S :

$$x \notin S$$

Subsets

Definition: The set A is a *subset* of the set B , denoted $A \subseteq B$, iff

$$\forall x : x \in A \Rightarrow x \in B$$

Definition: The *void* set, the *null* set, the *empty* set, denoted \emptyset , is the set with no members.

Note:

- the assertion $x \in \emptyset$ is always false.
- \emptyset is a subset of every set.
- A set B is always a subset of itself.

Definition: If $A \subseteq B$ but $A \neq B$ then we say A is a *proper* subset of B , denoted $A \subset B$ (in some texts).

Definition: The set of all subsets of a set A , denoted $\wp(A)$, is called the *power set* of A .

Example: If $A = \{a, b\}$ then:

$$\wp(A) = \{\emptyset, \{a\}, \{b\}, \{a, b\}\}$$

Cardinality

Definition: The number of (distinct) elements in A , denoted $|A|$, is called the *cardinality* of A .

If the cardinality is a natural number (in \mathbb{N}), then the set is called *finite*, otherwise it is *infinite*.

Example:

$$A = \{a, b\}$$

$$|\{a, b\}| = 2$$

$$|\wp(\{a, b\})| = 4$$

A is finite and so is $\wp(A)$.

Useful Fact: $|A| = n$ implies $|\wp(A)| = 2^n$

\mathbb{N} is infinite since $|\mathbb{N}|$ is not a natural number. It is called a *transfinite cardinal number*.

Set Membership and Paradoxes

Note: Sets can be both members and subsets of other sets.

Example:

$$A = \{\emptyset, \{\emptyset\}\}.$$

A has two elements and hence four subsets:

$$\emptyset, \{\emptyset\}, \{\{\emptyset\}\}, \{\emptyset, \{\emptyset\}\}$$

Note that \emptyset is both a member of A and a subset of A !

Russell's paradox: Let S be the set of all sets which are not members of themselves. Is S a member of itself?

Another paradox: Henry is a barber who shaves all people who do not shave themselves. Does Henry shave himself?

Cartesian Product

Definition: The Cartesian product of A with B , denoted $A \times B$, is the set of *ordered pairs* $\{\langle a, b \rangle \mid a \in A \wedge b \in B\}$

Note: The Cartesian product of anything with \emptyset is \emptyset . (why?)

Example:

$$A = \{a, b\}$$

$$B = \{1, 2, 3\}$$

$$A \times B = \{\langle a, 1 \rangle, \langle a, 2 \rangle, \langle a, 3 \rangle, \langle b, 1 \rangle, \langle b, 2 \rangle, \langle b, 3 \rangle\}$$

What is $B \times A$?

$$A \times B \times A?$$

If $|A| = m$ and $|B| = n$, what is $|A \times B|$?

Functions

A *function (mapping, map)* f from set A to set B is denoted by $f : A \rightarrow B$

f associates with each x in A one and only one y in B .

A is called the *domain* and B is called the *codomain*.

If $f(x) = y$:

y is called the *image* of x under f

x is called a *preimage* of y

Note that there may be more than one preimage of y but there is only one image of x .

The *range* of f , denoted by $f(A)$, is the set of all images of points in A under f .

Injections, Surjections and Bijections

Let f be a function from A to B .

Definition: f is *one-to-one* (denoted 1-1) or *injective* if $a \neq b$ implies $f(a) \neq f(b)$

Definition: f is *onto* or *surjective* if $f(A) = B$

Definition: f is *bijection* if it is surjective and injective (one-to-one and onto).

Definition: Let f be a bijection from A to B . Then the *inverse* of f , denoted f^{-1} , is the function from B to A defined as $f^{-1}(y) = x$ iff $f(x) = y$

Definition: Let $f : B \rightarrow C, g : A \rightarrow B$. The *composition* of f with g , denoted $f \circ g$, is the function from A to C defined by $f \circ g(x) = f(g(x))$

Countability

Definition: If a set has the same cardinality as a subset of the natural numbers \mathbb{N} , then the set is called *countable*.

If $|A| = |\mathbb{N}|$, the set A is *countably infinite* or *denumerable*. The (transfinite) cardinal number of the set \mathbb{N} is *aleph null* $= \aleph_0$.

If a set is not countable we say it is *uncountable*. The following sets are uncountable (we show later):

- The real numbers in $[0, 1]$
- $\wp(\mathbb{N})$, the power set of \mathbb{N}
- The set of functions from \mathbb{N} to \mathbb{N}

Note: With infinite sets proper subsets can have the same cardinality. This cannot happen with finite sets.

Countability carries with it the implication that there is a *listing* or *enumeration* of the elements of the set.

Examples

Theorem: $|A| \leq |B|$ if there is an injection from A to B .

Example: if A is a subset of B then $|A| \leq |B|$

Proof: the function $f(x) = x$ is an injection from A to B

Theorem: $|A| = |B|$ iff is a bijection from A to B

Example: $|\mathbb{E}| = |\mathbb{N}|$, where \mathbb{E} is the set of even integers (even though \mathbb{E} is a proper subset of $|\mathbb{N}|$)

Proof: Let $f(x) = 2x$. Then f is a bijection from \mathbb{N} to \mathbb{E} :

0	1	2	3	4	5	6	. . .
↑	↑	↑	↑	↑	↑	↑	
↓	↓	↓	↓	↓	↓	↓	
0	2	4	6	8	10	12	. . .

Countably Infinite Sets

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

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

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*.

$$\begin{aligned} \text{e.g., } 1/3 &= .3333333\text{.....} \\ 1/2 &= .500000\text{.....} \\ &= .499999\text{.....} \end{aligned}$$

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. We will see more examples of this later.

Uncountable Sets

Theorem: The power set of \mathbb{N} , $\wp(\mathbb{N})$, 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). The enumeration is as follows:

$$S_1 = \{n_{11}, n_{12}, n_{13}, n_{14}, n_{15}, n_{16} \dots\}$$

$$S_2 = \{n_{21}, n_{22}, n_{23}, n_{24}, n_{25}, n_{26} \dots\}$$

$$S_3 = \{n_{31}, n_{32}, n_{33}, n_{34}, n_{35}, n_{36} \dots\}$$

⋮

where each S_i is a subset of \mathbb{N}

Now construct the set $T = \{n \in \mathbb{N} \mid n \notin S_n\}$

$T \subseteq \mathbb{N}$, so $T = S_i$ for some number i

If $i \in T$, then $i \in S_i$, so we must have $i \notin T$

If $i \notin T$, then $i \notin S_i$, so we must have $i \in T$

A contradiction!!

Hence, we have a subset of \mathbb{N} which is not in the enumeration, so $\wp(\mathbb{N})$ is uncountable.

Uncountable Sets

Theorem: The set of all functions from \mathbb{N} to \mathbb{N} is uncountable.

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

If this set is countable, then we must have an enumeration $f_0, f_1, f_2, f_3, \dots$

Now, construct the function:

$$g(x) = f_x(x) + 1$$

This is a function from \mathbb{N} to \mathbb{N} , but it is not in our enumeration as it differs from each f_i for at least one argument.

Hence the set of all functions from \mathbb{N} to \mathbb{N} is not countable.

Other Infinite Cardinals

Theorem: For any set S , $|S|, |S| < |\wp(S)|$

Proof: $|S| \leq |\wp(S)|$ (since $S \subseteq \wp(S)$)

We therefore need to prove that $|S| \neq |\wp(S)|$

We assume that $|S| = |\wp(S)|$ and derive a contradiction.

If $|S| = |\wp(S)|$, then there is a bijection b which maps elements of S into $\wp(S)$

We construct the set $T = \{s \in S \mid s \notin b(s)\}$

Since this is in the power set of S , the bijection b must map some element of S (let's call it t) to it, i.e. $b(t) = T$

If $t \in T$, then $t \in b(t)$, so we must have $t \notin T$

If $t \notin T$, then $t \notin b(t)$, so we must have $t \in T$

Applying this iteratively to \mathbb{N} , we get a sequence of infinite cardinals that are all different:

$$|\mathbb{N}| < |\wp(\mathbb{N})| < |\wp(\wp(\mathbb{N}))| < |\wp(\wp(\wp(\mathbb{N})))| < \dots$$

or:

$$\aleph_0 < \aleph_1 < \aleph_2 < \aleph_3 < \dots$$

The (generalised) *continuum hypothesis* states that there is no infinite cardinal between \aleph_i and \aleph_{i+1}

Countability of Programs

The set of all Java programs is countable.

Proof: Let S be the set of legitimate characters which can appear in a Java program.

- A Java compiler will determine if an input program is a syntactically correct Java program (the program doesn't have to do anything useful).
- Use the lexicographic ordering of S and feed the strings into the compiler.
- If the compiler says YES, this is a syntactically correct Java program, we add the program to the list.
- Else we move on to the next string.

In this way we construct a list or an implied bijection from \mathbb{N} to the set of Java programs.

Hence, the set of Java programs is countable.

Uncomputable Problems

Any program can be regarded as a function which takes some input, does some manipulation, and produces some output.

Since all data will be represented as a binary number eventually, a program can be regarded as a function from \mathbb{N} to \mathbb{N} .

We have already shown that there are uncountably many functions from \mathbb{N} to \mathbb{N} . Hence there must exist functions of this type for which no program exists.

Similarly, we can show that there exists a number x between 0 and 1 which is not computable.

There does not exist a Java program (or a program in any other language) which will compute it!

Why? Because there are more numbers between 0 and 1 than there are Java programs to compute them (in fact there are \mathfrak{c} such numbers!)

Languages

Definition: An *alphabet* is a finite, nonempty set of symbols. We use Σ to denote this alphabet.

A *string* is a finite sequence of symbols from Σ .

The length of a string s , denoted $|s|$, is the number of symbols in it.

The empty string, ϵ , is the string of length zero.

Σ^* denotes the set of all sequences of strings that are composed of zero or more symbols of Σ .

Σ^+ denotes the set of all sequences of strings composed of one or more symbols of Σ , i.e. $\Sigma^* - \{\epsilon\}$.

A *language* is a subset of Σ^* .

Operations on languages

Operation	Definition
union of L and M	$L \cup M = \{s \mid s \in L \text{ or } s \in M\}$
concatenation of L and M	$LM = \{st \mid s \in L \text{ and } t \in M\}$
Kleene closure of L	$L^* = \bigcup_{i=0}^{\infty} L^i$
positive closure of L	$L^+ = \bigcup_{i=1}^{\infty} L^i$

Exponential notation can be used to indicate the number of items (symbols, strings or languages) being concatenated.

If $a \in \Sigma, x \in \Sigma^*, L \subseteq \Sigma^*$:

$$\begin{aligned} a^k &= aa \dots a \quad (a^0 = \epsilon) \\ x^k &= xx \dots x \quad (x^0 = \epsilon) \\ \Sigma^k &= \Sigma \Sigma \dots \Sigma \quad (\Sigma^0 = \{\epsilon\}) \\ L^k &= LL \dots L \quad (L^0 = \{\epsilon\}) \end{aligned}$$

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^{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:

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

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 .

Recursive Definitions

Recursive or *inductive* definitions of sets and functions on recursively defined sets are similar.

1. *Basis* step:
 - For sets: state the basic building blocks (BBB's) of the set
 - For functions: state the values of the function on the BBBs
2. *Inductive* or *recursive* step:
 - For sets: show how to build new things from old with some construction rules
 - For functions: show how to compute the value of a function on the new things that can be built knowing the value on the old things.

Recursive Definitions

Example: a recursive definition of \mathbb{N} :

1. *Basis*:

0 is in \mathbb{N} (0 is the BBB)

2. *Induction*:

if n is in \mathbb{N} then so is $n + 1$ (how to build new objects from old: “add one to an old object to get a new one”)

Now given the above recursive definition of \mathbb{N} we can give recursive definitions of functions on \mathbb{N} :

1. $f(0) = 1$ (the *initial condition* or the value of the function on the BBBs).
2. $f(n+1) = (n+1) f(n)$ (the *recurrence equation*, how to define f on the new objects based on its value on old objects)

Recursive Definitions

Some examples of recursive definitions:

The factorial function $f(n) = n!$:

Basis: $f(0) = 1$

Induction: $f(n+1) = (n+1) * f(n)$

The Fibonacci sequence:

Basis: $f(0) = f(1) = 1$

Induction: $f(n+1) = f(n) + f(n-1)$

The power function:

Basis: $a^0 = 1$

Induction: $a^{n+1} = a * a^n$

Recursive Definitions

Some more examples of recursive definitions:

The set of strings over a finite alphabet Σ :

Basis: $\epsilon \in \Sigma^*$

Induction: If $w \in \Sigma^*$ and $a \in \Sigma$, then $wa \in \Sigma^*$

The set of strings P which contain matched parentheses:

Basis: $() \in P$

Induction: If $w \in P$, then $(w), w() \in P$

The set of strings A which contain an odd number of a 's

Basis: $a \in A$

Induction: If $w \in A$, then $aaaw \in A$

Structural Induction

Proof of assertions about recursively defined objects (sets, functions, etc.) usually involve a proof by *structural induction*. This has the following form:

- Prove the assertion is true for the BBBs in the basis step.
- Prove that if the assertion is true for the old objects it must be true for the new objects you can build from the old objects.
- Conclude the assertion must be true for all objects.

Example:

Theorem: $a^m a^n = a^{m+n}$

Proof:

1. *Basis step:* Show it holds for $n = 0$ ($a^m a^0 = a^{m+0}$)

Left hand side = $a^m a^0 = a^m(\mathbf{1}) = a^m$

The right side = $a^{m+0} = a^m$

Hence, the two sides are equal.

Structural Induction

2. *Induction step:*

The Induction hypothesis: assume the assertion is true for n ($a^m a^n = a^{m+n}$)

Now show it is true for $n + 1$ ($a^m a^{n+1} = a^{m+(n+1)}$)

Left hand side = $a^m a^{n+1} = a^m (a^n a) = (a^m a^n) a = a^{m+n} a$

(by the inductive step in the definition of a^n and the induction hypothesis)

Right hand side = $a^{m+(n+1)} = a^{(m+n)+1} = a^{m+n} a$
(by the inductive step in the definition of a^n)

Hence, we have shown for arbitrary m that $a^m a^n = a^{m+n}$ by structural induction.

Structural Induction

Theorem: All strings in the language of matched parentheses (the set P defined earlier) contain the same number of '('s as ')'s

Proof:

1. *Basis step:* Show that it holds for $()$

This is trivial since there is one '(' and one ')'

2. *Induction step:*

The induction hypothesis: assume the assertion is true for w (w contains the same number of '('s as ')'s)

Now show that it is true for $()w$, (w) and $w()$

This is obviously true, since each possibility adds one '(' and one ')', and w contains the same number of '('s and ')'s (by the induction hypothesis).

Structural Induction

Theorem: All strings in the set of strings A defined earlier contain an odd number of 'a's

Proof:

1. *Basis step:* Show that it holds for a

This is trivial since the string contains one 'a'

2. *Induction step:*

The induction hypothesis: assume the assertion is true for w (w contains an odd number of 'a's')

Now show that it is true for $aaaw$

This is obviously true, since we are adding two 'a's, and w contains an odd number of 'a's by the induction hypothesis (adding two to an odd number is still an odd number).