Cardinality

Cardinals

Def. Two sets A and B have the same cardinality (are equinumerous) if there is a bijection $f: A \to B$. Notation $A \sim B$, or $|A| = |B|$.

$|A| = [A]_{\sim}$

cardinal numbers are ~ equivalence classes

Prop. The relation ~ is an equivalence relation on sets.

Def. A set A has at most as large cardinality as a set B if there is an injection $f: A \to B$. Notation $|A| \leq |B|$.

Def. A set A has at least as large cardinality as a set B if there is a surjection $f: A \to B$. Notation $|A| \geq |B|$.

Def. A set A has smaller cardinality than a set B if there is an injection $f: A \to B$ and there is no surjection $f: A \to B$. Notation $|A| < |B|$.

Theorem (Cantor)

If $|A| \leq |B|$ and $|B| \leq |A|$, then $|A| = |B|$.

Operations on cardinals

$|A| = [A]_{\sim}$

cardinal numbers are ~ equivalence classes

Def. Let A and B be two disjoint sets. Then
$|A| + |B| = |A \cup B|$.

Def. Let A and B be two sets. Then
$|A| \cdot |B| = |A \times B|$.

Def. Let A and B be two sets. Then
$|A|^{|B|} = |A^B|$ where A^B is the set of all functions from B to A, i.e. $A^B = \{f \mid f: B \to A\}$.

Prop. Let A be a set. Then $|\mathcal{P}(A)| = 2^{|A|}$.

Note: $2 = |\{0,1\}|$

Finite sets, finite cardinals

We write $\mathbb{N}_k$ for the set $\{0,1,..., k-1\}$. Then $\mathbb{N}_0 = \varnothing$.

We will also write k for $|\mathbb{N}_k|$.

$|A| = [A]_\sim$

cardinal numbers are ~ equivalence classes

Def. A set A is finite if and only if $|A| = k$, for some $k \in \mathbb{N}$.

Hence A set A is finite if and only if there is a natural number $k \in \mathbb{N}$ and a bijection $f: A \to \mathbb{N}_k$.

if and only if A has k elements, for some $k \in \mathbb{N}$

E.g. If $|A| = k$ and $|B| = m$ for some $k,m \in \mathbb{N}$

then $|A \times B| = k \cdot m$

The operations on cardinals when restricted to finite cardinals coincide with the operations on natural numbers!
This justifies the notation.

Infinite, countable and uncountable sets

Time for a video!

Hilbert's
infinite hotel :-)

Infinite, countable and uncountable sets

We write $\aleph_0$ for the cardinality of natural numbers.
Hence $\aleph_0 = |\mathbb{N}|$.

$|A| = [A]_{\sim}$

cardinal numbers are $\sim$ equivalence classes

Def. A set A is countable iff $|A| = \aleph_0$.

Prop. $\mathbb{N}$ is countable.
$\mathbb{Z}$ is countable.
$\mathbb{Q}$ is countable.

Def. A set is infinite iff $|A| \geq \aleph_0$.

Hence, every countable set is infinite

Def. A set is uncountable iff $|A| > \aleph_0$.

Prop. $\mathbb{R}$ is uncountable.

We write c for $|\mathbb{R}|$

Cardinals are unbounded

$|A| = [A]_\sim$

cardinal numbers are ~ equivalence classes

Theorem (Cantor)

For every set A we have $|A| < |\mathcal{P}(A)|$.

Hence, for every cardinal there is a larger one.

Finite Automata

Alphabets and Languages

Def

$\Sigma^0 = \{\varepsilon\}$ contains only the empty word

Σ - alphabet (finite set)

$\Sigma^n = \{a_1 a_2..a_n \mid a_i \in \Sigma\}$ is the set of words of length n

$\Sigma^* = \{w \mid \exists n \in \mathbb{N}.\ \exists\ a_1, a_2, .., a_n \in \Sigma.\ w = a_1 a_2..a_n\}$ is the set of all words over Σ

A language L over Σ is a subset $L \subseteq \Sigma^*$

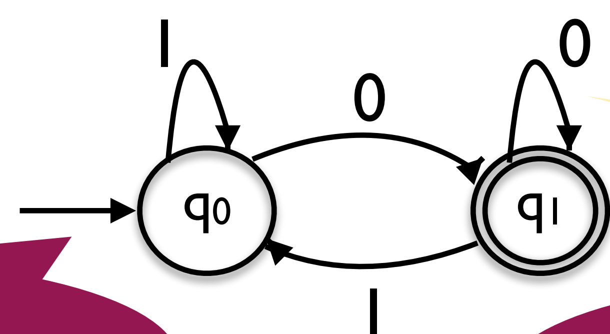
Deterministic Automata (DFA)

alphabet

Informal example

$\Sigma = \{0, 1\}$

M_1:



q_0, q_1 are states

q_0 is initial

q_1 is final

transitions, labelled by alphabet symbols

Accepts the language $L(M_1) = \{w \in \Sigma^* \mid w \text{ ends with a } 0\} = \Sigma^* 0$

regular language

regular expression

DFA

Definition

A deterministic automaton M is a tuple $M = (Q, \Sigma, \delta, q_0, F)$ where

Q is a finite set of states
Σ is a finite alphabet
$\delta: Q \times \Sigma \longrightarrow Q$ is the transition function
q_0 is the initial state, $q_0 \in Q$
F is a set of final states, $F \subseteq Q$

In the example M

$M_1 = (Q, \Sigma, \delta, q_0, F)$ for

$Q = \{q_0, q_1\}$ $F = \{q_1\}$

$\Sigma = \{0, 1\}$

$\delta(q_0, 0) = q_1$, $\delta(q_0, 1) = q_0$
$\delta(q_1, 0) = q_1$, $\delta(q_1, 1) = q_0$

DFA

The extended transition function

Given $M = (Q, \Sigma, \delta, q_0, F)$ we can extend $\delta: Q \times \Sigma \longrightarrow Q$ to

$\delta^*: Q \times \Sigma^* \longrightarrow Q$

In M_1, $\delta^*(q_0, 110010) = q_1$

inductively, by:

$\delta^*(q, \varepsilon) = q$ and $\delta^*(q, wa) = \delta(\delta^*(q, w), a)$

Definition

$L(M_1) = \{w0 \mid w \in \{0,1\}^*\}$

The language recognised / accepted by a deterministic finite automaton $M = (Q, \Sigma, \delta, q_0, F)$ is

$$L(M) = \{w \in \Sigma^* \mid \delta^*(q_0, w) \in F\}$$

Regular languages and operations

$L(M_1) = \{w0 | w \in \{0,1\}^*\}$
is regular

Definition

Let Σ be an alphabet. A language L over Σ ($L \subseteq \Sigma^*$) is regular iff it is recognised by a DFA.

Regular operations

Let L, L_1, L_2 be languages over Σ. Then $L_1 \cup L_2$, $L_1 \cdot L_2$, and L^* are languages, where

$$L_1 \cdot L_2 = \{w_1 \cdot w_2 \mid w_1 \in L_1, w_2 \in L_2\}$$

$$L^* = \{w \mid \exists n \in \mathbb{N}.\ \exists\, w_1, w_2, .., w_n \in L.\ w = w_1 w_2 .. w_n\}$$

$\varepsilon \in L^*$ always

Closure under regular operations

also under intersection

Theorem C1

The class of regular languages is closed under union

We can already prove these!

Theorem C2

The class of regular languages is closed under complement

Theorem C3

The class of regular languages is closed under concatenation

But not yet these two…

Theorem C4

The class of regular languages is closed under Kleene star