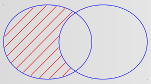
EDAA40
Discrete Structures in Computer Science



1: Sets

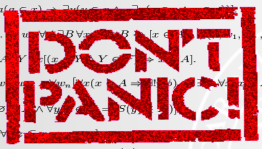
$R = \{x : x \notin x\}$

Jörn W. Janneck, Dept. of Computer Science, Lund University

axiomatic vs naïve set theory

Zermelo-Fraenkel Set Theory w/Choice (ZFC)

extensionality	$\forall x \forall y [\forall z (z \in x \Leftrightarrow z \in y) \Rightarrow x = y]$.
regularity	$\forall x [\exists a (a \in x) \Rightarrow$ [illegible]
specification	$\forall w_1, .$ [illegible] $\exists B \forall x$ [illegible] $B \Leftrightarrow [x \in$ [illegible] $, w_n, A)])$
union	$\forall \mathcal{F} \exists A$ [illegible] Y [illegible] $[(x$ [illegible] $Y \in \mathcal{F})$ [illegible] $A]$.
replacement	$\forall A \forall w$ [illegible] $\forall w_n [\forall x (x$ [illegible] $A \Rightarrow$ [illegible] $A \Rightarrow \exists y (y \in B \wedge \phi))]$.
infinity	$\exists X [\varnothing$ [illegible] $\wedge \forall y$ [illegible] $S(y)$ [illegible]
power set	$\forall x \exists y \forall$ [illegible]
choice	$\forall X \left[\emptyset \notin X \implies \exists f : X \to \bigcup X \quad \forall A \in X \, (f(A) \in A)\right]$.



s i d e b a r

This course will be about "naïve" set theory.
However, at its end, you should be able to read and understand most of the above.

sets: collections of stuff, empty set

$\{Sacramento, Albany, Austin, Salt\ Lake\ City, Springfield\}$

sets are collections of stuff

$\{red, green, blue\}$ $\{2, 3, 5, 7, 11, 13, 17\}$

$\{Marcus, 44, beige\}$ any kind of stuff

some sets are pretty large
(we'll talk more about just ***how*** large later)

$\mathbb{N}^+ = \{1, 2, 3, 4, 5, 6, 7, ...\}$

$\mathbb{N} = \{0, 1, 2, 3, 4, 5, 6, 7, ...\}$

this is the empty set

$\{\} = \emptyset$

there is but one of those

element of

Given a set A, any given thing x either is, or is not, an *element of A*.

$x \in A$ or $x \notin A$

$3 \in \{1, 2, 3, 4\}$

$11 \notin \{1, 2, 3, 4\}$

$\{3\} \notin \{1, 2, 3, 4\}$

$0.\overline{9} \in \{1, 2, 3, 4\}$?

elementhood depends on
a concept of equality

$\{2, 1\} \in \{\{1, 2\}, \{3, 4\}\}$?

extensionality

A set is defined by the elements it contains (its *extension*).

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

order, repetition do not matter,
they are just a matter of representation

$\{a, b, c\} \neq \{a, b, c, d\}$

equal sets must contain *exactly*
the same elements

$\{a, b, c\} \neq \{\{a, b, c\}\}$
$\emptyset \neq \{\emptyset\}$
$11 \neq \{11\}$

1-element sets are *singleton* sets

cardinality

The number of elements in a
set A is called its *cardinality*.

$\#(A)$ $\#A$ $|A|$

alternative syntax

$\#(\emptyset) = 0$
$\#(\{\emptyset\}) = 1$
$\#(\{a, b, c\}) = 3$
$\#(\{\{a, b, c\}\}) = 1$

For now, we will only consider the cardinality of finite sets.
We will discuss infinite sets, including their cardinality, in more detail later.
(Also, we haven't yet precisely defined these terms, "finite" and "infinite".)

inclusion

subset superset

$A \subseteq B$ this means that if $x \in A$ then $x \in B$

A and B might be the same, in fact
$A \subseteq B$ and $B \subseteq A$ iff $A = B$

"iff" is jargon for "if and only if", meaning both sides are logically equivalent

For any set A, it's always the case that
$\emptyset \subseteq A$ and $A \subseteq A$

We use $\subset$ to denote *proper (or strict) inclusion*:
$A \subset B$ iff $A \subseteq B$ and $A \neq B$

A and B are *proper (or strict) subset* and *superset*, respectively.

Sometimes, $\subset$ is used to mean $\subseteq$.
Here, we always use it to mean proper inclusion.

properties of inclusion

inclusion is *transitive**
$A \subseteq B$ and $B \subseteq C$ implies $A \subseteq C$

$\{2,3,5\} \subseteq \{2,3,4,5\} \subseteq \mathbb{N}$ therefore $\{2,3,5\} \subseteq \mathbb{N}$

inclusion is *partial:**
There are sets A and B for which neither $A \subseteq B$ or $B \subseteq A$ is true.

Example?

* We will discuss transitivity and partiality more generally later

specifying sets

enumeration of its elements $\{red, green, blue\}$

set builder notation / set comprehensions

flavor 1	flavor 2	bad flavor
$\{n \in \mathbb{N}^+ : n \text{ is prime}\}$	$\{n : n \in \mathbb{N}^+, n \text{ is prime}\}$	$\{x : x \notin x\}$
$\{n \in \mathbb{N}^+ \mid n \text{ is prime}\}$	$\{2n : n \in \mathbb{N}^+\}$	$\{x : x = x\}$

recursive definition (we will discuss this later)

enumeration w/ suspension points/ellipsis
$\{1, 2, 3, 4, 5, ...\}$
(informal stand-in for a recursive definition)

$12 \in \{2, 3, 5, 8, ...\}$?

building sets, examples

$A = \{2, 3, 5, 7, 11\}$

$B = \{x \in A : x \text{ odd}\}$
$B = \{3, 5, 7, 11\}$

$C = \{xy : x \in A, y \in B, y < x < 11\}$
$C = \{5 \cdot 3, 7 \cdot 3, 7 \cdot 5\} = \{15, 21, 35\}$

not everything that looks like a set...

sidebar

$R = \{x : x \notin x\}$ Is R an element of R? $R \in R$?

Let's assume it is, i.e. $R \in R$
This means that R satisfies the property defining R, in other words:
$R \notin R$

Okay, obviously that can't be right. Clearly that means R cannot be an element of R, i.e. $R \notin R$
But, oy veh, that means R would satisfy the property defining it, and that implies, dangnabbit: $R \in R$

This contradiction is known as *Russel's paradox*.

Well, it's great it has a name. But what does it mean for whether $R \in R$?

set building done right

So $\{x : x \notin x\}$ isn't a well-defined set. What went wrong?

The trouble is with the variable, x. It can literally stand for anything.
(And "anything" appears to include things that aren't sets.)

When using set builder notation, make sure the variables are limited to elements of a set you already know to be well-defined.

$\{n : n \in \mathbb{N}^+, n \text{ is prime}\}$ $\{2n : n \in \mathbb{N}^+\}$

$\{n \in \mathbb{N}^+ : n \text{ is prime}\}$

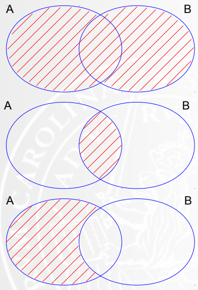
NB: This form also automatically implies a superset!

operations on sets

union $A \cup B$
all elements that are in A or B or both
$x \in A \cup B$ iff $x \in A$ or $x \in B$

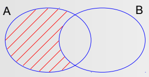
intersection $A \cap B$
all elements that are both in A and B
$x \in A \cap B$ iff $x \in A$ and $x \in B$

difference $A \setminus B$
all elements that are in A and not in B
$x \in A \setminus B$ iff $x \in A$ and $x \notin B$



difference and complement

set difference

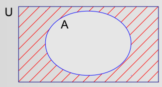


$A \setminus B$
$A - B$

There is in general no "inverse" set -A for a given set A.

However, often we work in a *local universe*, i.e. a set of everything we are potentially interested in. Let's call it U.

Examples of U?
Number theory?
Programming languages?



Then we can give the complement of a set a meaning:
$-A = U - A$

alternative syntaxes: $-_U A$ A^- A' A^c

disjointness

Two sets A and B are *disjoint* if they do not have any common elements, i.e. their intersection is empty: $A \cap B = \emptyset$

Note that every set A is disjoint from the empty set $\emptyset$.
Even the empty set!

For multiple sets A_1, ..., A_n, we say they are *pairwise disjoint* iff for any i, j, such that i ≠ j, A_i and A_j are disjoint, i.e. $A_i \cap A_j = \emptyset$

set algebra

some properties of intersection, union, and set difference:

idempotence	$A \cup A = A \cap A = A$
commutativity	$A \cup B = B \cup A$
commutativity	$A \cap B = B \cap A$
associativity	$(A \cup B) \cup C = A \cup (B \cup C)$
associativity	$(A \cap B) \cap C = A \cap (B \cap C)$
	$A \cup \emptyset = A$
	$A \cap \emptyset = \emptyset$
	$A \supseteq A \cap B \subseteq B$
	$A \subseteq A \cup B \supseteq B$
distributivity	$A \cup (B \cap C) = (A \cup B) \cap (A \cup C)$
distributivity	$A \cap (B \cup C) = (A \cap B) \cup (A \cap C)$
	$A \cap B \subseteq A \cup B$
	$A \setminus A = \emptyset$
	$A \setminus \emptyset = A$
	$-(-B) = B$

(more in the exercises of 1.4.1, 1.4.2, and 1.4.3 in SLAM)

family matters

A *family of sets* is a way of referring to a set of sets, usually *indexed* by an *index set*.*

$\underbrace{\{A_i : i \in I\}}_{\text{sets}}$ (index: i; index set: I)

$\{A_i\}_{i \in I}$ alternative syntax

Examples:

$P = \{\text{Charlie}, \text{Linus}, \text{Lucy}, \text{Patty}, \text{Sally}\}$

$\{R_p : p \in P\}$ with $R_{\text{Charlie}} = \{\text{Violet}, \text{LRHG}, \text{Peggy}\}$,

$R_{\text{Linus}} = \{\text{Sally}, \text{Mrs. Othmar}, \text{Lydia}\}$,

$R_{\text{Lucy}} = \{\text{Schroeder}\}$, $R_{\text{Patty}} = \{\text{Charlie}\}$,

$R_{\text{Sally}} = \{\text{Linus}\}$

What is $\{p \in P : q \in R_p, p \in R_q\}$

(a) What is the extension?

(b) What does it mean?

* We will come back to this notion in the lecture on functions.

large families

Often, the index set is something like the natural numbers:

$\{N_i : i \in \mathbb{N}\}$ with $N_i = \{k \in \mathbb{N} : k \geq i\}$

$\{M_i : i \in \mathbb{N}\}$ with $M_i = \{ik : k \in N_2\}$

$\{D_i : i \in \mathbb{N}^+\}$ with $D_i = \{d \in N_2 : i \in M_d\}$

What are these sets?

What is

$\{p \in N_2 : D_p = \emptyset\}$

generalized union & intersection

Let S be a set of sets. $\bigcap S = \{x : x \in s \text{ for all } s \in S\}$

$\bigcup S = \{x : x \in s \text{ for at least one } s \in S\}$

Often, S is a family of sets. Then we write...

$\bigcup\{A_i : i \in I\}$ $\quad \bigcup\{A_i\}_{i\in I}$ $\quad \bigcup_{i\in I} A_i$

$\bigcap\{A_i : i \in I\}$ $\quad \bigcap\{A_i\}_{i\in I}$ $\quad \bigcap_{i\in I} A_i$

When the index set is infinite, strange things can happen:

$\{A_i\}_{i\in\mathbb{N}^+}$ with $A_i = \left\{ q \in \mathbb{Q} : 0 \le q \le 1 - \frac{1}{i} \right\}$

$\bigcup_{i\in\mathbb{N}^+} A_i$

(a) What is the biggest number in each A?

(b) What is the biggest number in their union?

power sets

The *power set* of a set A is the set of all its subsets. $\mathcal{P}(A) = \{s : s \subseteq A\} = 2^A$

alternative syntax

$\mathcal{P}(\emptyset) = \{\emptyset\}$

$\mathcal{P}(\{a\}) = \{\emptyset, \{a\}\}$

$\mathcal{P}(\{a,b\}) = \{\emptyset, \{a\}, \{b\}, \{a,b\}\}$

$\mathcal{P}(\{a,b,c\}) = \{\emptyset, \{a\}, \{b\}, \{c\}, \{a,b\}, \{a,c\}, \{b,c\}, \{a,b,c\}\}$

Some properties:

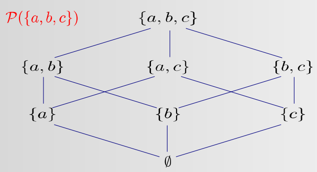
$\emptyset \in \mathcal{P}(A)$

$A \in \mathcal{P}(A)$

$\#(\mathcal{P}(A)) = 2^{\#(A)}$ Why is that?

structure of power sets

Power sets have a peculiar structure with respect to inclusion:



This is a *Hasse diagram* of the inclusion relation on a power set. We will come back to this when we talk about relations.

A connection means that the upper set properly includes the lower one.

Implied connections are omitted.