Sets

Objective

To introduce the basics of the theory of sets and some of its applications.

Complementary reading:

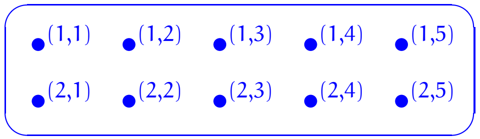
- Chapters 1, 30, and 31 of *How to Think Like a Mathematician* by K. Houston.
- Chapters 4.1 and 7 of *Mathematics for Computer Science* by E. Lehman, F. T. Leighton, and A. R. Meyer.
- Chapters 1.3, 1.4, 4, 5, and 7 of *How to Prove it* by D. J. Velleman.

Sets

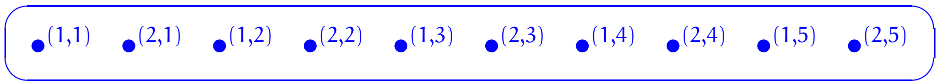
adapted from Section 1.1 of *Sets for Mathematics*
by F.W. Lawvere and R. Rosebrugh

An *abstract set* is supposed to have elements, each of which has no structure, and is itself supposed to have no internal structure, except that the elements can be distinguished as equal or unequal, and to have no external structure except for the number of elements. There are sets of all possible sizes, including finite and infinite sizes.

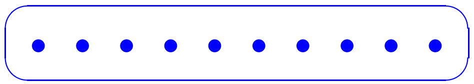
It has been said that a set is like a mental "bag of dots", except of course that the bag has no shape; thus,



may be a convenient way of picturing a certain set for some considerations, but what is apparently the same set may be pictured as



or even simply as



for other considerations.

Set Theory

Set Theory[a] is the branch of mathematical logic that studies axiom systems for the notion of abstract set as based on a membership predicate (recall page 178). As we will see (on page 296), care must be taken in such endeavour.

Set Theory aims at providing foundations for mathematics. There are however other approaches, as *Category Theory* and *Type Theory*, that also play an important role in Computer Science.

[a](for which you may start by consulting the book *Naive Set Theory* by P. Halmos)

A widely used set theory is ZFC: Zermelo-Fraenkel Set Theory with Choice. It embodies postulates of: extensionality (page 291); separation [aka restricted comprehension, subset, or specification] (page 294); powerset (page 300); pairing (page 313); union (page 326); replacement; infinity; foundation [aka regularity]; and choice.

We are not going to be formally studying Set Theory here; rather, we will be *naively* looking at ubiquitous structures that are available within it.

Extensionality axiom

$\boxed{\text{Two sets are equal if they have the same elements.}}$

Thus,

$$\forall \text{ sets } A, B.\ A = B \iff (\ \forall x.\, x \in A \iff x \in B\ )$$

Example:

$$\{0\} \neq \{0,1\} = \{1,0\} \neq \{2\} = \{2,2\}$$

Subsets and supersets

Definition 80 *For sets A and B, A is said to be a subset of B, written $A \subseteq B$, and B is said to be a superset of A, written $B \supseteq A$, whenever the statement*

$$\forall x.\, x \in A \implies x \in B$$

holds.

Example:

$$\{0\} \subseteq \{0,1\} \supseteq \{1\}$$

Notation 81 *The proper subset notation $A \subset B$ stands for $(A \subseteq B\ \&\ A \neq B)$. Analogously, the proper superset notation $B \supset A$ stands for $(B \supseteq A\ \&\ B \neq A)$.*

Go to Workout 21 on page 437

Separation principle

For any set A and any definable property P, there is a set containing precisely those elements of A for which the property P holds.

Set comprehension

The set whose existence is postulated by the separation principle for a set A and a property P typically denoted

$$\{x \in A \mid P(x)\} \quad .$$

(Recall the discussion on set comprehension on page 181.)

Thus, the statement $(\dagger)$ on page 181 follows.

Russell's paradox

The separation principle does not allow us to consider the class of those R such that $R \notin R$ as a set (and, btw, the same goes for the class of all sets). This is not a bug, but a feature!

Empty set

The set whose existence is postulated by the separation principle for a set A and the absurd property **false** typically denoted

$$\emptyset \quad \text{or} \quad \{\} \quad .$$

Its defining statement is

$$\forall x.\, x \notin \emptyset$$

or, equivalently, by

$$\neg(\exists x.\, x \in \emptyset) \quad .$$

Go to Workout 22
on page 438

Cardinality

The *cardinality* of a set specifies its size. If this is a natural number, then the set is said to be *finite*.

Typical notations for the cardinality of a set S are $\#S$ or $|S|$.

Example:

$$\#\emptyset = 0$$

Powerset axiom

For any set, there is a set consisting of all its subsets.

The set of all subsets of a set U whose existence is postulated by the powerset axiom is typically denoted

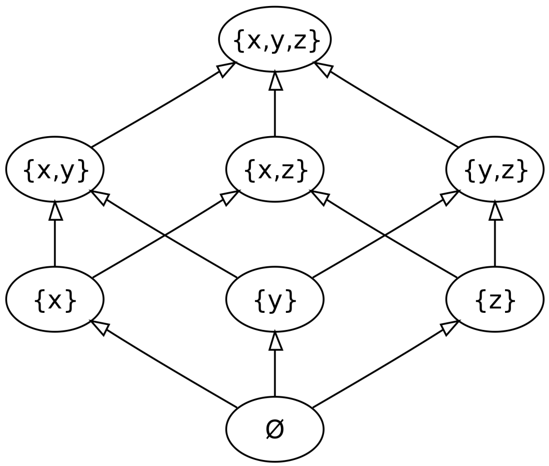
$$\mathcal{P}(U) \quad .$$

Thus,

$$\forall X.\ X \in \mathcal{P}(U) \iff X \subseteq U \quad .$$

Hasse diagrams[a]

Example: $\mathcal{P}(\{x, y, z\})$



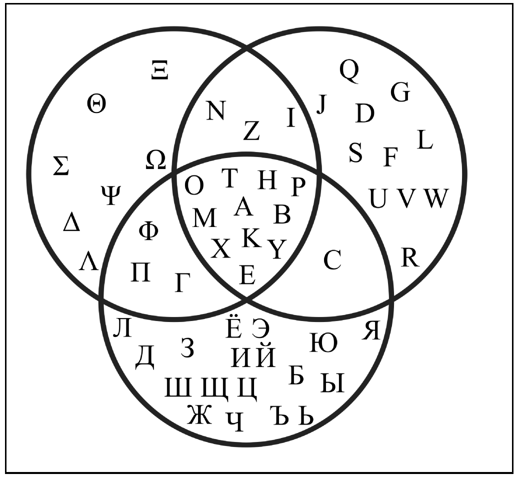
[a]From http://en.wikipedia.org/wiki/Powerset; see also http://en.wikipedia.org/wiki/Hasse_diagram.

Proposition 82 *For all finite sets* $\mathcal{U}$,

$$\#\,\mathcal{P}(\mathcal{U}) = 2^{\#\mathcal{U}} \quad .$$

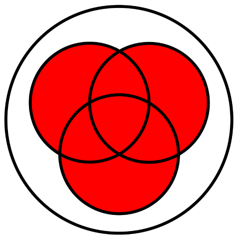
PROOF IDEA:

Venn diagrams[a]

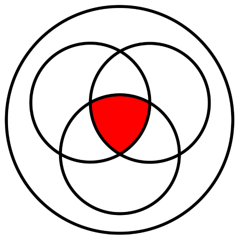


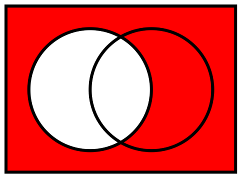
[a]From http://en.wikipedia.org/wiki/Union_(set_theory) and http://en.wikipedia.org/wiki/Intersection_(set_theory); see also http://en.wikipedia.org/wiki/Venn_diagram.

Union



Intersection





Complement

The powerset Boolean algebra

$$(\ \mathcal{P}(\mathcal{U})\ ,\ \ \emptyset\ ,\ \ \mathcal{U}\ ,\ \ \cup\ ,\ \ \cap\ ,\ \ (\cdot)^c\ )$$

$$\begin{aligned} A \cup B &= \{\, x \in \mathcal{U} \mid x \in A \ \vee\ x \in B \,\} \\ A \cap B &= \{\, x \in \mathcal{U} \mid x \in A \ \&\ x \in B \,\} \\ A^c &= \{\, x \in \mathcal{U} \mid \neg(x \in A) \,\} \end{aligned}$$

- The union operation $\cup$ and the intersection operation $\cap$ are associative, commutative, and idempotent.

- The *empty set* $\emptyset$ is a neutral element for $\cup$ and the *universal set* $\mathcal{U}$ is a neutral element for $\cap$.

- The empty set $\emptyset$ is an annihilator for $\cap$ and the universal set $\mathcal{U}$ is an annihilator for $\cup$.

- With respect to each other, the union operation $\cup$ and the intersection operation $\cap$ are absorptive and distributive.

- The complement operation $(\cdot)^c$ satisfies complementation laws.

Sets and logic

$\mathcal{P}(U)$	$\{\,\mathbf{false}\,,\,\mathbf{true}\,\}$
$\emptyset$	$\mathbf{false}$
U	$\mathbf{true}$
$\cup$	$\vee$
$\cap$	$\&$
$(\cdot)^c$	$\neg(\cdot)$

Go to Workout 23
on page 439

Pairing axiom

For every a and b, there is a set with a and b as its only elements.

The set whose existence is postulated by the pairing axiom for a and b is typically denoted by

$$\{\,a\,,\,b\,\}\quad .$$

Thus, the statement

$$\forall x.\, x \in \{a, b\} \iff (x = a \vee x = b)$$

holds, and we have that:

$$\#\{a, b\} = 1 \iff a = b \quad \text{and} \quad \#\{a, b\} = 2 \iff a \neq b \quad .$$

Singletons

For every a, the pairing axiom provides the set $\{a, a\}$ which is abbreviated as

$$\{a\} \quad ,$$

and referred to as a *singleton*.

NB

$$\#\{a\} = 1$$

Examples:

$$\emptyset \subset \{\emptyset\} \subset \{\emptyset, \{\emptyset\}\} \supset \{\{\emptyset\}\} \supset \emptyset$$

- $\#\{\emptyset\} = 1$
- $\#\{\{\emptyset\}\} = 1$
- $\#\{\emptyset, \{\emptyset\}\} = 2$

NB

$$\{\emptyset\} \in \{\{\emptyset\}\} \quad , \quad \{\emptyset\} \not\subseteq \{\{\emptyset\}\} \quad , \quad \{\{\emptyset\}\} \not\subseteq \{\emptyset\}$$

Ordered pairing

For every pair a and b, three applications of the pairing axiom provide the set $\big\{\{a\}, \{a, b\}\big\}$ which is typically abbreviated as

$$\langle a, b\rangle \quad ,$$

and referred to as an *ordered pair*.

Proposition 83 (Fundamental property of ordered pairing) *For all* a, b, x, y*,*

$$\langle a, b\rangle = \langle x, y\rangle \iff \big(a = x \;\&\; b = y\big) \quad .$$

PROOF:

Products

The *product* $A \times B$ of two sets A and B is the set

$$A \times B = \{\, x \mid \exists\, a \in A, b \in B.\, x = (a, b) \,\}$$

where

$$\begin{aligned} &\forall a_1, a_2 \in A, b_1, b_2 \in B.\\ &\quad (a_1, b_1) = (a_2, b_2) \iff (a_1 = a_2 \;\&\; b_1 = b_2) \quad . \end{aligned}$$

Thus,

$$\forall x \in A \times B.\, \exists!\, a \in A, b \in B.\, x = (a, b) \quad .$$

More generally, for a fixed natural number n and sets $A_1, \ldots, A_n$, we have

$$\begin{aligned} \textstyle\prod_{i=1}^{n} A_i &= A_1 \times \cdots \times A_n \\ &= \{\, x \mid \exists\, a_1 \in A_1, \ldots, a_n \in A_n.\, x = (a_1, \ldots, a_n) \,\} \end{aligned}$$

where

$$\begin{aligned} &\forall\, a_1, a_1' \in A_1, \ldots, a_n, a_n' \in A_n.\\ &\quad (a_1, \ldots, a_n) = (a_1', \ldots, a_n') \iff (a_1 = a_1' \;\&\; \cdots \;\&\; a_n = a_n') \quad . \end{aligned}$$

NB Cunningly enough, the definition is such that $\prod_{i=1}^{0} A_i = \{\, ()\, \}$.

Notation 84 *For a natural number* n *and a set* A*, one typically writes* A^n *for* $\prod_{i=1}^{n} A$.

Proposition 85 *For all finite sets* A *and* B*,*

$$\#(A \times B) = \#A \cdot \#B \quad .$$

PROOF IDEA:

Go to Workout 24
on page 446

Big unions and intersections

Definition 86 *Let* U *be a set. For a collection of sets* $\mathcal{F} \subseteq \mathcal{P}(U)$,

- *let the* big union *(relative to* U*) be defined as*

$$\bigcup \mathcal{F} = \{ x \in U \mid \exists A \in \mathcal{F}.\, x \in A \} \ ,$$

and

- *let the* big intersection *(relative to* U*) be defined as*

$$\bigcap \mathcal{F} = \{ x \in U \mid \forall A \in \mathcal{F}.\, x \in A \} \ .$$

Examples: For $A, A_1, A_2 \in \mathcal{P}(U)$,

$$\bigcup \emptyset = \emptyset \qquad \bigcap \emptyset = U$$

$$\bigcup \{A\} = A \qquad \bigcap \{A\} = A$$

$$\bigcup \{A_1, A_2\} = A_1 \cup A_2 \qquad \bigcap \{A_1, A_2\} = A_1 \cap A_2$$

$$\bigcup \{A, A_1, A_2\} = A \cup A_1 \cup A_2 \qquad \bigcap \{A, A_1, A_2\} = A \cap A_1 \cap A_2$$

Theorem 87 *Let*

$$\mathcal{F} = \left\{ S \subseteq \mathbb{R} \,\middle|\, (0 \in S) \ \& \ \big(\forall x \in \mathbb{R}.\, x \in S \implies (n+1) \in S\big) \right\} \ .$$

Then, (i) $\mathbb{N} \in \mathcal{F}$ *and* (ii) $\mathbb{N} \subseteq \bigcap \mathcal{F}$*. Hence,* $\bigcap \mathcal{F} = \mathbb{N}$*.*

NB This result is typically interpreted as stating that:

> $\mathbb{N}$ is the least set of numbers containing 0 and closed under taking successors.

PROOF:

Union axiom

$\boxed{\text{Every collection of sets has a union.}}$

The set whose existence is postulated by the union axiom for a collection $\mathcal{F}$ is typically denoted

$$\bigcup \mathcal{F}$$

and, in the case $\mathcal{F} = \{A, B\}$, abbreviated to

$$A \cup B \quad .$$

Thus,

$$x \in \bigcup \mathcal{F} \iff \exists X \in \mathcal{F}.\, x \in X \quad ,$$

and hence

$$x \in (A \cup B) \iff (x \in A) \vee (x \in B) \quad .$$

Using the separation and union axioms, for every collection $\mathcal{F}$, consider the set

$$\left\{ x \in \bigcup \mathcal{F} \mid \forall X \in \mathcal{F}.\, x \in X \right\} \quad .$$

For *non-empty* $\mathcal{F}$ this set is denoted

$$\bigcap \mathcal{F}$$

because, in this case,

$$\forall x.\ x \in \bigcap \mathcal{F} \iff \big(\forall X \in \mathcal{F}.\, x \in X\big) \quad .$$

In particular, for $\mathcal{F} = \{A, B\}$, this is abbreviated to

$$A \cap B$$

with defining property

$$\forall x.\ x \in (A \cap B) \iff (x \in A)\ \&\ (x \in B) \quad .$$

Go to Workout 25
on page 448

Tagging

The construction

$$\{\ell\} \times A = \left\{ (\ell, a) \mid a \in A \right\}$$

provides copies of A, as tagged by labels ℓ.

Indeed, note that

$$\forall y \in \big(\{\ell\} \times A\big).\, \exists!\, x \in A.\ y = (\ell, x) \quad ,$$

and that $\{\ell_1\} \times A_1 = \{\ell_2\} \times A_2 \iff (\ell_1 = \ell_2)\ \&\ (A_1 = A_2)$ so that

$$\{\ell_1\} \times A = \{\ell_2\} \times A \iff \ell_1 = \ell_2 \quad .$$

Disjoint unions

Definition 88 *The* disjoint union $A \uplus B$ *of two sets* A *and* B *is the set*

$$A \uplus B \;=\; \big(\{1\} \times A\big) \cup \big(\{2\} \times B\big) \quad .$$

Thus,

$$\forall x.\, x \in (A \uplus B) \iff \big(\exists a \in A.\, x = (1,a)\big) \vee \big(\exists b \in B.\, x = (2,b)\big) \,.$$

More generally, for a fixed natural number n and sets $A_1, \ldots, A_n$, we have

$$\begin{aligned} \biguplus_{i=1}^{n} A_i &= A_1 \uplus \cdots \uplus A_n \\ &= \big(\{1\} \times A_1\big) \cup \cdots \cup \big(\{n\} \times A_n\big) \end{aligned}$$

NB Cunningly enough, the definition is such that $\biguplus_{i=1}^{0} A_i = \emptyset$.

Notation 89 *For a natural number* n *and a set* A*, one typically writes* $n \cdot A$ *for* $\biguplus_{i=1}^{n} A$.

Proposition 90 *For all finite sets* A *and* B*,*

$$\#(A \uplus B) \;=\; \#A + \#B \quad .$$

PROOF IDEA:

Go to Workout 26
on page 451

Workout 21
from page 293

1. Write an ML function

```
subset: ''a list * ''a list -> bool
```

such that for every list `xs` representing a finite set X and every list `ys` representing a finite set Y, `subset(xs,ys)=true` iff $X \subseteq Y$.

2. Prove the following statements:

(a) $\forall$ sets $A.\, A \subseteq A$.

(b) $\forall$ sets $A, B, C.\, (A \subseteq B \;\&\; B \subseteq C) \implies A \subseteq C$.

(c) $\forall$ sets $A.\, (A \subseteq B \;\&\; B \subseteq A) \iff A = B$.

Workout 22
from page 298

Prove the following statements:

1. $\forall$ set $S.\, \emptyset \subseteq S$.

2. $\forall$ set $S.\, (\forall x.\, x \notin S) \iff S = \emptyset$.

Workout 23
from page 312

1. Referring to the definitions on pages 183 and 184, show that $\mathrm{CD}(m, n) = \mathrm{D}(m) \cap \mathrm{D}(n)$ for all natural numbers m and n.

2. Find the union and intersection of:

(a) $\{1, 2, 3, 4, 5\}$ and $\{-1, 1, 3, 5, 7\}$;

(b) $\{x \in \mathbb{R} \mid x > 7\}$ and $\{x \in \mathbb{N} \mid x > 5\}$.

3. Write ML functions

```
union: 'a list * 'a list -> 'a list
intersection: ''a list * ''a list -> 'a list
```

such that for every list `xs` representing a finite set X and every list `ys` representing a finite set Y, the lists `union(xs,ys)` and `intersection(xs,ys)` respectively represent the finite sets $X \cup Y$ and $X \cap Y$.

Use these functions to check your answer to the first part of the previous item.

4. Give an explicit description of $\mathcal{P}(\mathcal{P}(\mathcal{P}(\emptyset)))$, and draw its Hasse diagram.

5. Write an ML function

```
powerset: 'a list -> 'a list list
```

such that for every list `as` representing a finite set A, the list of lists `powerset(as)` represents the finite set $\mathcal{P}(A)$.

6. Establish the laws of the powerset Boolean algebra.

7. Either prove or disprove that, for all sets A and B,

   (a) $A \subseteq B \implies \mathcal{P}(A) \subseteq \mathcal{P}(B)$,

   (b) $\mathcal{P}(A \cup B) \subseteq \mathcal{P}(A) \cup \mathcal{P}(B)$,

   (c) $\mathcal{P}(A) \cup \mathcal{P}(B) \subseteq \mathcal{P}(A \cup B)$.

   (d) $\mathcal{P}(A \cap B) \subseteq \mathcal{P}(A) \cap \mathcal{P}(B)$,

   (e) $\mathcal{P}(A) \cap \mathcal{P}(B) \subseteq \mathcal{P}(A \cap B)$.

8. Let U be a set. For all $A, B \in \mathcal{P}(U)$ prove that the following statements are equivalent.

   (a) $A \cup B = B$.

   (b) $A \subseteq B$.

   (c) $A \cap B = A$.

   (d) $B^c \subseteq A^c$.

9. Let U be a set. For all $A, B \in \mathcal{P}(U)$ prove that

   (a) $A^c = B \iff (A \cup B = U \ \& \ A \cap B = \emptyset)$,

   (b) $(A^c)^c = A$, and

   (c) the De Morgan's laws:

$$(A \cup B)^c = A^c \cap B^c \text{ and } (A \cap B)^c = A^c \cup B^c \ .$$

10. Draw Venn diagrams for the following constructions on sets.

   (a) Difference:

$$A \setminus B = \{x \in A \mid x \notin B\}$$

   (b) Symmetric difference:

$$A \triangle B = (A \setminus B) \cup (B \setminus A)$$

$\boxed{\text{If you like this kind of stuff, push on.}}$

11. Let U be a set. Prove that, for all $A, B \in \mathcal{P}(U)$,

   (a) $A \subseteq B \implies \big(A \setminus B = \emptyset \ \& \ A \triangle B = B \setminus A\big)$.

   (b) $A \cap B = \emptyset \implies A \triangle B = A \cup B$,

   (c) $(A \triangle B) \cap (A \cap B) = \emptyset \ \& \ (A \triangle B) \cup (A \cap B) = A \cup B$,

   and establish as corollaries that

   (d) $A^c = U \triangle A$.

   (e) $A \cup B = (A \triangle B) \triangle (A \cap B)$,

   thereby expressing complements and unions in terms of symmetric difference and intersections.

12. The purpose of this exercise is to show that, for a set U, the structure $(\mathcal{P}(U), \emptyset, \triangle, U, \cap)$ is a commutative ring.
    (a) Prove that $(\mathcal{P}(U), \emptyset, \triangle)$ is a commutative group; that is, a commutative monoid (refer to page 151) in which every element has an inverse (refer to page 156).
    (b) Prove that $\mathcal{P}(U)$ with additive structure $(\emptyset, \triangle)$ and multiplicative structure $(U, \cap)$ is a commutative semiring.

Workout 24
from page 321

1. Find the product of $\{1, 2, 3, 4, 5\}$ and $\{-1, 1, 3, 5, 7\}$.
2. Write an ML function

```
product:  'a list * 'b list -> ( 'a * 'b ) list
```

   such that for every list `as` representing a finite set A and every list `bs` representing a finite set B, the list of pairs `product(as,bs)` represents the product set $A \times B$.

   Use this function to check your answer to the previous item.

3. For sets A, B, C, D, either prove or disprove the following statements.
    (a) $(A \subseteq B \ \& \ C \subseteq D) \implies A \times C \subseteq B \times D$.
    (b) $(A \cup C) \times (B \cup D) \subseteq (A \times B) \cup (C \times D)$.
    (c) $(A \times B) \cup (C \times D) \subseteq (A \cup C) \times (B \cup D)$.
    (d) $A \times (B \cup D) \subseteq (A \times B) \cup (A \times D)$.
    (e) $(A \times B) \cup (A \times D) \subseteq A \times (B \cup D)$.

   What happens with the above when $A \cap C = \emptyset$ and/or $B \cap D = \emptyset$?

Workout 25
from page 328

1. Let $I = \{2, 3, 4, 5\}$, and for each $i \in I$ let $A_i = \{i, i+1, i-1, 2 \cdot i\}$.
    (a) List the elements of all the sets A_i for $i \in I$.
    (b) Let $\{A_i \mid i \in I\}$ stand for $\{A_2, A_3, A_4, A_5\}$. Find $\bigcup\{A_i \mid i \in I\}$ and $\bigcap\{A_i \mid i \in I\}$.

2. Write ML functions

```
bigunion:  'a list list -> 'a list
bigintersection:  'a list list -> 'a list
```

such that for every list of lists `as` representing a finite set of finite sets A, the lists `bigunion(as)` and `bigintersection(as)` respectively represent the finite sets $\bigcup X$ and $\bigcap X$.

Use these functions to check your answer to the previous item.

3. For $\mathcal{F} \subseteq \mathcal{P}(A)$, let $\mathcal{U} = \{ X \subseteq A \mid \forall S \in \mathcal{F}.\ S \subseteq X \} \subseteq \mathcal{P}(A)$. Prove that $\bigcup \mathcal{F} = \bigcap \mathcal{U}$.

Analogously, define $\mathcal{L} \subseteq \mathcal{P}(A)$ such that $\bigcap \mathcal{F} = \bigcup \mathcal{L}$. Also prove this statement.

Version of February 4, 2014

NB For intuition when tackling the following exercises it might help considering the case of finite collections first.

4. Prove that, for all collections $\mathcal{F}$, it holds that

$$\forall \text{ set } U.\ \bigcup \mathcal{F} \subseteq U \iff (\forall X \in \mathcal{F}.\ X \subseteq U) \quad .$$

State and prove the analogous property for intersections of big intersections of non-empty collections.

5. Prove that for all collections $\mathcal{F}_1$ and $\mathcal{F}_2$,

$$\left(\bigcup \mathcal{F}_1\right) \cup \left(\bigcup \mathcal{F}_2\right) = \bigcup (\mathcal{F}_1 \cup \mathcal{F}_2) \quad .$$

State and prove the analogous property for intersections of non-empty collections.

Version of February 4, 2014

Workout 26
from page 333

1. Find the disjoint union of $\{1, 2, 3, 4, 5\}$ and $\{-1, 1, 3, 5, 7\}$.

2. Let

```
datatype ('a,'b) sum = one of 'a | two of 'b  .
```

Write an ML function

```
dunion:  'a list * 'b list -> ('a ,'b) sum list
```

such that for every list `as` representing a finite set A and every list `bs` representing a finite set B, the list of tagged elements `dunion(as,bs)` represents the disjoint union $A \uplus B$.

Use this function to check your answer to the previous item.

3. Prove or disprove the following statements for all sets A, B, C, D:

(a) $(A \subseteq B \ \&\ C \subseteq D) \implies A \uplus C \subseteq B \uplus D$,

(b) $(A \cup B) \uplus C \subseteq (A \uplus C) \cup (B \uplus C)$,

(c) $(A \uplus C) \cup (B \uplus C) \subseteq (A \cup B) \uplus C$,

(d) $(A \cap B) \uplus C \subseteq (A \uplus C) \cap (B \uplus C)$,

(e) $(A \uplus C) \cap (B \uplus C) \subseteq (A \cap B) \uplus C$.