Relations

Definition 91 *A (binary) relation* R *from a set* A *to a set* B *, denoted*

$$R : A \mathrel{-\!\!\!+\!\!\!\to} B \quad \text{or} \quad R \in \mathrm{Rel}(A, B) \quad ,$$

is a subset of the product set $A \times B$*; that is,*

$$R \subseteq A \times B$$

or, equivalently,

$$R \in \mathcal{P}(A \times B) \quad .$$

Notation 92 *One typically writes* $a \, R \, b$ *for* $(a, b) \in R$*.*

NB Binary relations come with a *source* and a *target*.

One may also consider more general n*-ary relations*, for any natural number n. These are defined as subsets of n-ary products; that is, elements of

$$\mathcal{P}(A_1 \times \cdots \times A_n)$$

for sets $A_1, \cdots, A_n$.

Informal examples:

- Computation.
- Typing.
- Program equivalence.
- Networks.
- Databases.

Examples:

- Empty relation.
  $\emptyset : A \mathrel{-\!\!\!+\!\!\!\to} B$ $\qquad (a \, \emptyset \, b \iff \mathbf{false})$
- Full relation.
  $(A \times B) : A \mathrel{-\!\!\!+\!\!\!\to} B$ $\qquad (a \, (A \times B) \, b \iff \mathbf{true})$
- Identity (or equality) relation.
  $I_A = \{ (a, a) \mid a \in A \} : A \mathrel{-\!\!\!+\!\!\!\to} A$ $\qquad (a \, I_A \, a' \iff a = a')$
- Integer square root.
  $R_2 = \{ (m, n) \mid m = n^2 \} : \mathbb{N} \mathrel{-\!\!\!+\!\!\!\to} \mathbb{Z}$ $\qquad (m \, R_2 \, n \iff m = n^2)$

Internal diagrams

Example:

$$R = \{ (0,0), (0,-1), (0,1), (1,2), (1,1), (2,1) \} : \mathbb{N} \rightarrow\!\!\!\!\!+\ \mathbb{Z}$$

$$S = \{ (1,0), (1,2), (2,1), (2,3) \} : \mathbb{Z} \rightarrow\!\!\!\!\!+\ \mathbb{Z}$$

Relational composition

Definition 93 *The composition of two relations $R : A \rightarrow\!\!\!\!\!+\ B$ and $S : B \rightarrow\!\!\!\!\!+\ C$ is the relation*

$$S \circ R : A \rightarrow\!\!\!\!\!+\ C$$

defined by setting

$$a \, (S \circ R) \, c \iff \exists b \in B. \; a \, R \, b \;\&\; b \, S \, c$$

for all $a \in A$ and $c \in C$.

Theorem 94 *Relational composition is associative and has the identity relation as neutral element. That is,*

- *Associativity.*

  For all $R : A \rightarrow\!\!\!\!\!+\ B$, $S : B \rightarrow\!\!\!\!\!+\ C$, and $T : C \rightarrow\!\!\!\!\!+\ D$,

  $$(T \circ S) \circ R \;=\; T \circ (S \circ R)$$

- *Neutral element.*

  For all $R : A \rightarrow\!\!\!\!\!+\ B$,

  $$R \circ I_A \;=\; R \;=\; I_B \circ R \quad .$$

Relations and matrices

Definition 95

1. *For positive integers m and n, an $(m \times n)$-matrix M over a semiring $(S, 0, \oplus, 1, \odot)$ is given by entries $M_{i,j} \in S$ for all $0 \le i < m$ and $0 \le j < n$.*

   Btw *Rows and columns are enumerated from 0, and not 1. This is non-standard, but convenient for what follows.*

2. *The* identity $(n \times n)$*-matrix* I_n *has entries*

$$(I_n)_{i,j} = \begin{cases} 1 & \text{, if } i = j \\ 0 & \text{, if } i \neq j \end{cases}$$

3. *The* multiplication *of an* $(\ell \times m)$*-matrix* L *with an* $(m \times n)$*-matrix* M *is the* $(\ell \times n)$*-matrix* $M \cdot L$ *with entries*

$$\begin{aligned} (M \cdot L)_{i,j} &= (M_{0,j} \odot L_{i,0}) \oplus \cdots \oplus (M_{m-1,j} \odot L_{i,m-1}) \\ &= \bigoplus_{k=0}^{m-1} M_{k,j} \odot L_{i,k} \end{aligned}$$

Theorem 96 *Matrix multiplication is associative and has the identity matrix as neutral element.*

Definition 97

1. *The* null $(m \times n)$*-matrix* $Z_{m,n}$ *has entries*

$$(Z_{m,n})_{i,j} = 0 \ .$$

2. *The* addition *of two* $(m \times n)$*-matrices* M *and* L *is the* $(m \times n)$*-matrix* $M + L$ *with entries*

$$(M + L)_{i,j} = M_{i,j} \oplus L_{i,j} \ .$$

Theorem 98

1. *Matrix addition is associative, commutative, and has the null matrix as neutral element.*

2. *For every* $(\ell \times m)$*-matrices* L, L' *and* $(m \times n)$*-matrices* M, M', *the distributive laws*

$$M \cdot Z_{\ell,m} = Z_{\ell,n} \quad , \quad Z_{m,n} \cdot L = Z_{\ell,n}$$

and

$$\begin{aligned} M \cdot (L + L') &= (M \cdot L) + (M \cdot L') \\ (M + M') \cdot L &= (M \cdot L) + (M' \cdot L) \end{aligned}$$

hold.

Definition 99 *For every natural number* n, *let*

$$[n] = \{0, \ldots, n-1\} \ .$$

NB Cunningly enough, $[0] = \emptyset$; so that $\# [n] = n$.

A relation $R : [m] \longrightarrow\!\!\!\!\!\!\!+ \;\; [n]$ can be seen as the $(m \times n)$-matrix $\mathrm{mat}(R)$ over the commutative semiring of Booleans

$$\big(\{\mathbf{false}, \mathbf{true}\}, \ \mathbf{false}\,, \ \vee\ , \ \mathbf{true}\,, \ \&\ \big)$$

given by

$$\mathrm{mat}(R)_{i,j} \ = \ \big[\ (i,j) \in R\ \big] \quad .$$

Conversely, every $(m \times n)$-matrix M can be seen as the relation $\mathrm{rel}(M) : [m] \longrightarrow\!\!\!\!\!\!\!+ \;\; [n]$ given by

$$(i,j) \in \mathrm{rel}(M) \iff M_{i,j} \quad .$$

In fact,

$$\mathrm{rel}\big(\mathrm{mat}(R)\big) = R \quad \text{and} \quad \mathrm{mat}\big(\mathrm{rel}(M)\big) = M \quad .$$

Hence, relations from $[m]$ to $[n]$ and $(m \times n)$-matrices over Booleans provide two alternative views of the same structure.

More interestingly, this carries over to identities :

$$\mathrm{mat}(I_{[n]}) = I_n \quad \text{and} \quad \mathrm{rel}(I_n) = I_{[n]} \quad ,$$

and to composition/multiplication :

$$\mathrm{mat}(S \circ R) = \mathrm{mat}(S) \cdot \mathrm{mat}(R) \quad \text{and} \quad \mathrm{rel}(M \cdot L) = \mathrm{rel}(M) \circ \mathrm{rel}(L) \quad .$$

Indeed,

$$\begin{aligned}
&(i,j) \in \mathrm{rel}\big(\mathrm{mat}(S) \cdot \mathrm{mat}(R)\,\big) \\
&\qquad \iff \quad \big(\,\mathrm{mat}(S) \cdot \mathrm{mat}(R)\,\big)_{i,j} \\
&\qquad \iff \quad \textstyle\bigvee_{k=0}^{m-1} \ \mathrm{mat}(S)_{k,j} \ \& \ \mathrm{mat}(R)_{i,k} \\
&\qquad \iff \quad \exists\, k \in [m].\ \ (k,j) \in S \ \& \ (i,k) \in R \\
&\qquad \iff \quad (i,j) \in \big(S \circ R\big)
\end{aligned}$$

Thus, the composition of relations between finite sets can be implemented by means of matrix multiplication:

$$S \circ R = \mathrm{rel}\big(\,\mathrm{mat}(S) \cdot \mathrm{mat}(R)\,\big) \quad .$$

Directed graphs

Definition 100 *A directed graph (A, R) consists of a set A and a relation R on A (i.e. a relation from A to A).*

Notation 101 *We write $\mathrm{Rel}(A)$ for the set of relations on a set A; that is, $\mathrm{Rel}(A) = \mathcal{P}(A \times A)$.*

Corollary 102 *For every set A, the structure*

$$(\ \mathrm{Rel}(A)\ ,\ I_A\ ,\circ\ )$$

is a monoid.

Definition 103 *For $R \in \mathrm{Rel}(A)$ and $n \in \mathbb{N}$, we let*

$$R^{\circ n} = \underbrace{R \circ \cdots \circ R}_{n \text{ times}} \in \mathrm{Rel}(A)$$

be defined as I_A for $n = 0$, and as $R \circ R^{\circ m}$ for $n = m + 1$.

Paths

Definition 104 *Let (A, R) be a directed graph. For $s, t \in A$, a path of length $n \in \mathbb{N}$ in R, with source s and target t, is a tuple $(a_0, \ldots, a_n) \in A^{n+1}$ such that $a_0 = s$, $a_n = t$, and $a_i \ R \ a_{i+1}$ for all $0 \leq i < n$.*

NB Cunningly enough, the unary tuple (a_0) is a path of length 0 with source s and target t iff $s = a_0 = t$.

Proposition 105 *Let (A, R) be a directed graph. For all $n \in \mathbb{N}$ and $s, t \in A$, $s \ R^{\circ n} \ t$ iff there exists a path of length n in R with source s and target t.*

PROOF:

Definition 106 *For $R \in \mathrm{Rel}(A)$, let*

$$R^{\circ *} = \bigcup \left\{ R^{\circ n} \in \mathrm{Rel}(A) \mid n \in \mathbb{N} \right\} = \bigcup_{n \in \mathbb{N}} R^{\circ n} \quad .$$

Corollary 107 *Let (A, R) be a directed graph. For all $s, t \in A$, $s \ R^{\circ *} \ t$ iff there exists a path with sourse s and target t in R.*

The $(n \times n)$-matrix $M = \mathrm{mat}(R)$ of a finite directed graph $([n], R)$ for n a positive integer is called its *adjacency matrix*.

The adjacency matrix $M^* = \mathrm{mat}(R^{\circ *})$ can be computed by matrix multiplication and addition as M_n where

$$\begin{cases} M_0 = I_n \\ M_{k+1} = I_n + (M \cdot M_k) \end{cases}$$

This gives an algorithm for establishing or refuting the existence of paths in finite directed graphs.

NB The same algorithm but over other semirings (rather than over the Boolean semiring) can be used to compute other information on paths[a]; like the weight of shortest paths[b], or the set of paths.

[a](for which you may see http://www.cl.cam.ac.uk/teaching/1314/L11/)

[b](for which you may see Chapter 25.1 of *Introduction to Algorithms (Second Edition)* by T. H. Cormen, C. E. Leiserson, R. L. Rivest, and C. Stein)

Go to Workout 27
on page 498

Preorders

Definition 108 *A* preorder $(P, \sqsubseteq)$ *consists of a set* P *and a relation* $\sqsubseteq$ *on* P *(i.e.* $\sqsubseteq \in \mathcal{P}(P \times P)$*) satisfying the following two axioms.*

- *Reflexivity.*

$$\forall x \in P.\ x \sqsubseteq x$$

- *Transitivity.*

$$\forall x, y, z \in P.\ (x \sqsubseteq y \ \&\ y \sqsubseteq z) \implies x \sqsubseteq z$$

Definition 109 *A* partial order*, or* poset[a]*, is a preorder* $(P, \sqsubseteq)$ *that further satisfies*

- *Antisymmetry.*

$$\forall x, y \in P.\ (x \sqsubseteq y \ \&\ y \sqsubseteq x) \implies x = y$$

[a](standing for *partially ordered set*)

Examples:

- $(\mathbb{R}, \leq)$ and $(\mathbb{R}, \geq)$.
- $(\mathcal{P}(A), \subseteq)$ and $(\mathcal{P}(A), \supseteq)$.
- $(\mathbb{Z}, \mid)$.

Theorem 110 *For* $R \subseteq A \times A$, *let*

$$\mathcal{F}_R = \{ Q \subseteq A \times A \mid R \subseteq Q \;\&\; Q \textit{ is a preorder} \} \quad .$$

Then, (i) $R^{\circ *} \in \mathcal{F}_R$ *and* (ii) $R^{\circ *} \subseteq \bigcap \mathcal{F}_R$. *Hence,* $R^{\circ *} = \bigcap \mathcal{F}_R$.

NB This result is typically interpreted in various forms as stating that:

- $R^{\circ *}$ is the reflexive-transitive closure of R.
- $R^{\circ *}$ is the least preorder containing R.
- $R^{\circ *}$ is the preorder freely generated by R.

PROOF:

Go to Workout 28
on page 500

Partial functions

Definition 111 *A relation $R : A \rightarrowtriangle B$ is said to be functional, and called a partial function, whenever it is such that*

$$\forall a \in A. \forall b_1, b_2 \in B.\ a\,R\,b_1\ \&\ a\,R\,b_2 \implies b_1 = b_2 \quad .$$

NB $R : A \rightarrowtriangle B$ is *not* functional if there are a in A and $b_1 \neq b_2$ in B such that both (a, b_1) and (a, b_2) are in R.

Example: The relation

$$\{ (x, y) \mid y = x^2 \} : \mathbb{Z} \rightarrowtriangle \mathbb{N}$$

is functional, while the relation

$$\{ (m, n) \mid m = n^2 \} : \mathbb{N} \rightarrowtriangle \mathbb{Z}$$

is not because, for instance, both $(1, 1)$ and $(1, -1)$ are in it.

Notation 112 *We write $f : A \rightharpoonup B$ to indicate that f is a partial function from A to B, and let*

$$\mathrm{PFun}(A, B) = (A \rightrightarrows B) \subseteq \mathrm{Rel}(A, B)$$

denote the set of partial functions from A to B.

Every partial function $f : A \rightharpoonup B$ satisfies that

> for each element a of A there is at most one element b of B such that b is a value of f at a.

The expression

$$f(a)$$

is taken to denote “the value” of f at a whenever this exists and considered *undefined* otherwise.

To see this in action, let $f : A \rightharpoonup B$ and $g : B \rightharpoonup C$ and consider the expression

$$g\big(f(a)\big) \quad .$$

This is defined iff $f(a)$ is defined (and hence an element of B) and also $g\big(f(a)\big)$ is defined (and hence an element of C), in which case it denotes the value of $(g \circ f)$ at a.

One typically writes $f(a)\downarrow$ (respectively $f(a)\uparrow$) to indicate that the partial function f is defined (respectively undefined) at a.

Thus, in symbols,

$$\big[\ f(a)\downarrow\ \&\ g\big(f(a)\big)\downarrow\ \big] \implies \big[\ \big(g \circ f\big)(a)\downarrow\ \ \&\ \big(g \circ f\big)(a) = g\big(f(a)\big)\ \big] \ .$$

Theorem 113 *The identity relation is a partial function, and the composition of partial functions yields a partial function.*

In practice, a partial function $f : A \rightharpoonup B$ is typically defined by specifying:

- a *domain of definition* $D_f \subseteq A$, and
- a *mapping*

  $$f : a \mapsto b_a$$

  given by a *rule* that to each element a in the domain of definition D_f assigns a unique element b_a in the target B (so that $f(a) = b_a$).

Warning: When proceeding as above, it is important to note that you need make sure that:

1. D_f is a subset of A,
2. for every a in D_f, the b_a as described by your mapping is unique and is in B (so that it is a well-defined value for f at a).

Example: The following defines a partial function $\mathbb{Z} \times \mathbb{Z} \rightharpoonup \mathbb{Z} \times \mathbb{Z}$:

- for $n \geq 0$ and $m > 0$,
  $(n, m) \mapsto \big(\operatorname{quo}(n, m)\,,\, \operatorname{rem}(n, m)\big)$
- for $n \geq 0$ and $m < 0$,
  $(n, m) \mapsto \big(-\operatorname{quo}(n, -m)\,,\, \operatorname{rem}(n, -m)\big)$
- for $n \leq 0$ and $m > 0$,
  $(n, m) \mapsto \big(-\operatorname{quo}(-n, m) - 1\,,\, \operatorname{rem}(m - \operatorname{rem}(-n, m), m)\big)$
- for $n \leq 0$ and $m < 0$,
  $(n, m) \mapsto \big(\operatorname{quo}(-n, -m) + 1\,,\, \operatorname{rem}(-m - \operatorname{rem}(-n, -m), -m)\big)$

Its domain of definition is $\big\{\, (n, m) \in \mathbb{Z} \times \mathbb{Z} \mid m \neq 0 \,\big\}$.

Btw There are alternative notations for mappings

$$f : a \mapsto b_a$$

that, although with different syntax, you have already encountered; namely, the notations

$$f(a) = b_a \qquad \text{and} \qquad f = \lambda a.\, b_a$$

from which the ML declaration styles

$$\texttt{fun } f(a) = b_a \qquad \text{and} \qquad \texttt{val } f = \texttt{fn } a \texttt{ => } b_a$$

come from.

Proposition 114 *For all finite sets* A *and* B*,*

$$\#(A \rightharpoonup B) = (\#B + 1)^{\#A} .$$

PROOF IDEA [a] :

[a]See Theorem 129.4 on page 398.

Go to Workout 29
on page 502

Functions (or maps)

Definition 115 *A partial function is said to be total, and referred to as a (total) function or map, whenever its domain of definition coincides with its source.*

The notation $f : A \to B$ is used to indicate that f is a function from A to B, and we write

$$\mathrm{Fun}(A, B) = (A \Rightarrow B)$$

for the set of functions from A to B.

Thus,

$$(A \Rightarrow B) \subseteq (A \rightharpoonup B) \subseteq \mathrm{Rel}(A, B)$$

and we have the following result:

Theorem 116 *For all* $f \in \mathrm{Rel}(A, B)$,

$$f \in (A \Rightarrow B) \iff \forall\, a \in A.\, \exists!\, b \in B.\ a\, f\, b \quad .$$

PROOF:

Proposition 117 *For all finite sets* A *and* B,

$$\#\,(A \Rightarrow B) \;=\; \#B^{\#A} \quad .$$

PROOF IDEA[a]:

[a]See Theorem 129.5 on page 398.

Our discussion on how to define partial functions also applies to functions; but, because of their total nature, simplifies as follows.

In practice, a function $f : A \to B$ is defined by specifying a mapping

$$f : a \mapsto b_a$$

given by a *rule* that to each $a \in A$ assigns a unique element $b_a \in B$ (which is the value of f at a denoted $f(a)$).

Warning: When proceeding as above, it is important to note that your mapping should be defined for every a in A and that the described b_a should be a uniquely determined element of B.

Theorem 118 *The identity partial function is a function, and the composition of functions yields a function.*

NB For all sets A, the identity function $\mathrm{id}_A : A \to A$ is given by the rule

$$\mathrm{id}_A(a) = a$$

and, for all functions $f : A \to B$ and $g : B \to C$, the composition function $g \circ f : A \to C$ is given by the rule

$$(g \circ f)(a) = g\big(f(a)\big) \quad .$$

Go to Workout 30
on page 504

Bijections, I

Definition 119 *A function* $f : A \longrightarrow B$ *is said to be* bijective*, or a* bijection*, whenever there exists a (necessarily unique) function* $g : B \longrightarrow A$ *(referred to as the* inverse *of* f*) such that*

1. g *is a* left inverse *for (or a* retraction *of)* f*:*

$$g \circ f = \mathrm{id}_A \quad ,$$

2. g *is a* right inverse *for (or a* section *of)* f*:*

$$f \circ g = \mathrm{id}_B \quad .$$

Notation 120 *The inverse of a function* f *is necessarily unique and typically denoted* f^{-1}*.*

Example: The mapping mat associating an $(m \times n)$-matrix to a relation from $[m]$ to $[n]$ is a bijection, with inverse the mapping rel; see page 347 for definitions.

The set of bijections from A to B is denoted

$$\mathrm{Bij}(A, B)$$

and we thus have

$$\mathrm{Bij}(A, B) \subseteq \mathrm{Fun}(A, B) \subseteq \mathrm{PFun}(A, B) \subseteq \mathrm{Rel}(A, B) \quad .$$

Proposition 121 *For all finite sets* A *and* B*,*

$$\#\,\mathrm{Bij}(A, B) = \begin{cases} 0 & \text{, if } \#A \neq \#B \\ n! & \text{, if } \#A = \#B = n \end{cases}$$

PROOF IDEA[a]:

[a]See Theorem 129.6 on page 398.

Theorem 122 *The identity function is a bijection, and the composition of bijections yields a bijection.*

Definition 123 *Two sets* A *and* B *are said to be* isomorphic *(and to have the* same cardinatity*) whenever there is a bijection between them; in which case we write*

$$A \cong B \quad \textit{or} \quad \#A = \#B \quad .$$

Example:

1. $\{0, 1\} \cong \{\mathbf{false}, \mathbf{true}\}$.
2. $\mathbb{N} \cong \mathbb{N}^+$, $\mathbb{N} \cong \mathbb{Z}$, $\mathbb{N} \cong \mathbb{N} \times \mathbb{N}$, $\mathbb{N} \cong \mathbb{Q}$.

Go to Workout 31
on page 505

Equivalence relations and set partitions

► Equivalence relations.

Definition 124 *A relation* E *on a set* A *is said to be an* equivalence relation *whenever it is:*

1. *reflexive*

   $$\forall x \in A.\, x \mathrel{E} x$$

2. *symmetric*

   $$\forall x, y \in A.\, x \mathrel{E} y \implies y \mathrel{E} x$$

3. *transitive*

   $$\forall x, y, z \in A.\, (x \mathrel{E} y \;\&\; y \mathrel{E} z) \implies x \mathrel{E} z$$

The set of all equivalence relations on A *is denoted* $\mathrm{EqRel}(A)$.

- Set partitions.

Definition 125 *A* partition P *of a set* A *is a set of non-empty subsets of* A *(that is,* $P \subseteq \mathcal{P}(A)$ *and* $\emptyset \notin P$*), whose elements are typically referred to as* blocks*, such that*

1. *the union of all blocks yields* A*:*

$$\bigcup P = A \quad ,$$

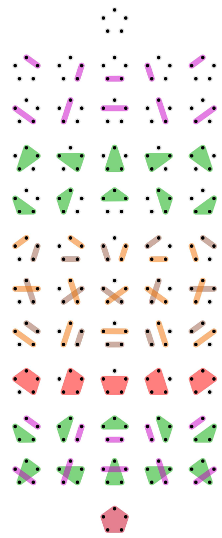
and

2. *all blocks are pairwise disjoint:*

$$\text{for all } b_1, b_2 \in P,\ b_1 \neq b_2 \implies b_1 \cap b_2 = \emptyset \quad .$$

The set of all partitions of A *is denoted* $\mathrm{Part}(A)$*.*

The partitions of a 5-element set[a]



[a]From http://en.wikipedia.org/wiki/Partition_of_a_set.

Theorem 126 *For every set* A*,*

$$\mathrm{EqRel}(A) \cong \mathrm{Part}(A) \quad .$$

PROOF OUTLINE:

1. Prove that the mapping

$$E \mapsto A/_E = \{\, b \subseteq A \mid \exists a \in A.\, b = [a]_E \,\}$$

where $[a]_E = \{ x \in A \mid x \, E \, a \}$

yields a function $\mathrm{EqRel}(A) \to \mathrm{Part}(A)$.

2. Prove that the mapping

$$P \mapsto \equiv_P$$

where $x \equiv_R y \iff \exists b \in P.\ x \in b \ \&\ y \in b$

yields a function $\mathrm{Part}(A) \to \mathrm{EqRel}(A)$.

3. Prove that the above two functions are inverses of each other.

Proposition 127 *For all finite sets* A*,*

$$\#\mathrm{EqRel}(A) = \#\mathrm{Part}(A) = B_{\#A}$$

where, for $n \in \mathbb{N}$*, the so-called* Bell numbers *are defined by*

$$B_n = \begin{cases} 1 & \text{, for } n = 0 \\ \sum_{i=0}^{m} \binom{m}{i} B_i & \text{, for } n = m+1 \end{cases}$$

PROOF IDEA [a] :

[a]See Theorem 129.7-8 on page 398.

Go to Workout 32
on page 506

Calculus of bijections, I

- $A \cong A$, $A \cong B \implies B \cong A$, $(A \cong B \;\&\; B \cong C) \implies A \cong C$
- If $A \cong X$ and $B \cong Y$ then
$$\mathcal{P}(A) \cong \mathcal{P}(X) \quad , \quad A \times B \cong X \times Y \quad , \quad A \uplus B \cong X \uplus Y \quad ,$$
$$\mathrm{Rel}(A, B) \cong \mathrm{Rel}(X, Y) \quad , \quad (A \rightharpoonup B) \cong (X \rightharpoonup Y) \quad ,$$
$$(A \Rightarrow B) \cong (X \Rightarrow Y) \quad , \quad \mathrm{Bij}(A, B) \cong \mathrm{Bij}(X, Y)$$
- $[1] \times A$, $(A \times B) \times C \cong A \times (B \times C)$, $A \times B \cong B \times A$
- $[0] \uplus A \cong A$, $(A \uplus B) \uplus C \cong A \uplus (B \uplus C)$, $A \uplus B \cong B \uplus A$
- $[0] \times A \cong [0]$, $(A \uplus B) \times C \cong (A \times C) \uplus (B \times C)$

- $\big(A \Rightarrow [1]\big) \cong [1]$, $\big(A \Rightarrow (B \times C)\big) \cong (A \Rightarrow B) \times (A \Rightarrow C)$
- $\big([0] \Rightarrow A\big) \cong [1]$, $\big((A \uplus B) \Rightarrow C\big) \cong (A \Rightarrow C) \times (B \Rightarrow C)$
- $([1] \Rightarrow A) \cong A$, $\big((A \times B) \Rightarrow C\big) \cong \big(A \Rightarrow (B \Rightarrow C)\big)$
- $(A \rightharpoonup B) \cong \big(A \Rightarrow (B \uplus [1])\big)$
- $\mathcal{P}(A) \cong \big(A \Rightarrow [2]\big)$

Characteristic (or indicator) functions

$$\boldsymbol{\mathcal{P}(A) \cong \big(A \Rightarrow [2]\big)}$$

Example: The key combinatorial argument in proving Pascal's rule resides in the bijection

$$\mathcal{P}\big(X \uplus [1]\big) \cong \mathcal{P}(X) \uplus \mathcal{P}(X)$$

deducible as

$$\begin{aligned}
\mathcal{P}\big(X \uplus [1]\big) &\cong \big((X \uplus [1]) \Rightarrow [2]\big) \\
&\cong \big(X \Rightarrow [2]\big) \times \big([1] \Rightarrow [2]\big) \\
&\cong \mathcal{P}(X) \times [2] \\
&\cong \mathcal{P}(X) \times \big([1] \uplus [1]\big) \\
&\cong \big(\mathcal{P}(X) \times [1]\big) \uplus \big(\mathcal{P}(X) \times [1]\big) \\
&\cong \mathcal{P}(X) \uplus \mathcal{P}(X)
\end{aligned}$$

Go to Workout 33
on page 510

Finite cardinality

Definition 128 *A set A is said to be* finite *whenever $A \cong [n]$ for some $n \in \mathbb{N}$, in which case we write $\#A = n$.*

Theorem 129 *For all $m, n \in \mathbb{N}$,*

1. $\mathcal{P}\big([n]\big) \cong [2^n]$
2. $[m] \times [n] \cong [m \cdot n]$
3. $[m] \uplus [n] \cong [m + n]$
4. $\big([m] \rightharpoonup [n]\big) \cong \big[(n+1)^m\big]$
5. $\big([m] \Rightarrow [n]\big) \cong [n^m]$
6. $\mathrm{Bij}\big([n], [n]\big) \cong [n!]$
7. $\mathrm{Part}\big([0]\big) \cong [1]$
8. $\mathrm{Part}\big([n+1]\big) \cong \biguplus_{S \subseteq [n]} \mathrm{Part}(S^c)$

Go to Workout 34 on page 513

Infinity axiom

There is an infinite set, containing $\emptyset$ and closed under successor.

Bijections, II

Proposition 130 *For a function $f : A \to B$, the following are equivalent.*

1. *f is bijective.*
2. *$\forall\, b \in B.\, \exists!\, a \in A.\, f(a) = b$.*
3. $$\begin{array}{l} \big(\forall\, b \in B.\, \exists\, a \in A.\, f(a) = b\big) \\ \& \\ \big(\forall\, a_1, a_2 \in A.\, f(a_1) = f(a_2) \implies a_1 = a_2\big) \end{array}$$

Surjections

Definition 131 *A function $f : A \to B$ is said to be surjective, or a surjection, and indicated $f : A \twoheadrightarrow B$ whenever*

$$\forall\, b \in B.\, \exists\, a \in A.\, f(a) = b \quad .$$

Examples:

1. Every bijection is a surjection.
2. The unique function $A \to [1]$ is surjective iff $A \neq \emptyset$.
3. The quotient function $A \to A_{/E} : a \mapsto [a]_E = \{\, x \in A \mid x \mathrel{E} a \,\}$ associated to an equivalence relation E on a set A is surjective.

4. The projection function $A \times B \to A : (a, b) \mapsto a$ is surjective iff $B \neq \emptyset$ or $A = \emptyset$.
5. For natural numbers m and n with $m < n$, there is no surjection from $[m]$ to $[n]$.

Theorem 132 *The identity function is a surjection, and the composition of surjections yields a surjection.*

The set of surjections from A to B is denoted

$$\mathrm{Sur}(A, B)$$

and we thus have

$$\mathrm{Bij}(A, B) \subseteq \mathrm{Sur}(A, B) \subseteq \mathrm{Fun}(A, B) \subseteq \mathrm{PFun}(A, B) \subseteq \mathrm{Rel}(A, B) \ .$$

Proposition 133

1. *For all finite sets A and natural numbers n, the cardinality of the set $\mathrm{Part}_n(A)$ of partitions of A in n blocks has cardinality $S(\#A, n)$, where the* Stirling numbers of the second kind *$S(m, n)$ are defined by*
   - $S(0, 0) = 1$;
   - $S(k, 0) = S(0, k) = 0$, *for* $k \geq 1$;
   - $S(m+1, n+1) = S(m, n) + (n+1) \cdot S(m, n+1)$, *for* $m, n \geq 0$.
2. *For all finite sets A and B,*

$$\#\mathrm{Sur}(A, B) = S(\#A, \#B) \cdot (\#B)! \ .$$

PROOF IDEA:

Go to Workout 35
on page 514

Enumerability

Definition 134

1. *A set A is said to be enumerable whenever there exists a surjection $\mathbb{N} \twoheadrightarrow A$, referred to as an enumeration.*
2. *A countable set is one that is either empty or enumerable.*

Btw For an enumeration $e : \mathbb{N} \twoheadrightarrow A$, if

$$e(n) = a \qquad (n \in \mathbb{N}, a \in A)$$

we think of the natural number n as a *code* for the element a of A. Codes need not be unique, but since

$$\{\, e(n) \in A \mid n \in \mathbb{N} \,\} = A$$

every element of A is guaranteed to have a code. These will be unique whenever the enumeration is a bijection.

Examples:

1. A bijective enumeration of $\mathbb{Z}$.

$\cdots$	-3	-2	-1	0	1	2	3	$\cdots$
$\cdots$	5	3	1	0	2	4	6	$\cdots$

2. A bijective enumeration of $\mathbb{N} \times \mathbb{N}$.

	0	1	2	3	4	5	$\cdots$
0	0	2	3	9	10	$\cdots$	
1	1	4	8	11			
2	5	7	12				
3	6	13					
4	14						
$\vdots$	$\vdots$						

Proposition 135 *Every non-empty subset of an enumerable set is enumerable.*

YOUR PROOF:

MY PROOF: Let $\emptyset \neq S \subseteq A$ and let $e : \mathbb{N} \twoheadrightarrow A$ be surjective.

Note that $\{ n \in \mathbb{N} \mid e(n) \in S \} \neq \emptyset$ and let

$$\mu(0) = \min\{ n \in \mathbb{N} \mid e(n) \in S \} \quad .$$

Furthermore, define by induction

$$\mu(k+1) = \min\{ n \in \mathbb{N} \mid n > \mu(k) \ \& \ e(n) \in S \} \qquad (k \in \mathbb{N})$$

where, by convention, $\min \emptyset = \mu(0)$.[a]

Finally, one checks[b] that the mapping

$$k \mapsto e\big(\mu(k)\big) \qquad (k \in \mathbb{N})$$

defines a function $\mathbb{N} \twoheadrightarrow S$ that is surjective.

[a] Btw, the operation of *minimisation* is at the heart of recursion theory.
[b] Please do it!

Countability

Proposition 136

1. *$\mathbb{N}$, $\mathbb{Z}$, $\mathbb{Q}$ are countable sets.*
2. *The product and disjoint union of countable sets is countable.*
3. *Every finite set is countable.*
4. *Every subset of a countable set is countable.*

Btw Corollary 145 (on page 431) provides more examples.

Go to Workout 36
on page 515

Axiom of choice

$\boxed{\text{Every surjection has a section.}}$

Injections

Definition 137 *A function* $f : A \to B$ *is said to be* injective*, or an* injection*, and indicated* $f : A \rightarrowtail B$ *whenever*

$$\forall a_1, a_2 \in A. \left(f(a_1) = f(a_2)\right) \implies a_1 = a_2 \quad .$$

Examples:

- Every section is an injection; so that, in particular, bijections are injections.
- All functions including a set into another one are injections.
- For all natural numbers k, the function $\mathbb{N} \to \mathbb{N} : n \mapsto n + k$ is an injection.
- For all natural numbers k, the function $\mathbb{N} \to \mathbb{N} : n \mapsto n \cdot k$ is an injection iff $k \geq 1$.
- For all natural numbers k, the function $\mathbb{N} \to \mathbb{N} : n \mapsto k^n$ is an injection iff $k \geq 2$.

Theorem 138 *The identity function is an injection, and the composition of injections yields an injection.*

The set of injections from A to B is denoted

$$\mathrm{Inj}(A, B)$$

and we thus have

$$\begin{tikzcd}[row sep=small, column sep=small]
 & \mathrm{Sur}(A,B) \arrow[dr, phantom, "\subseteq" sloped] & \\
\mathrm{Bij}(A,B) \arrow[ur, phantom, "\subseteq" sloped] \arrow[dr, phantom, "\subseteq" sloped] & & \mathrm{Fun}(A,B) \subseteq \mathrm{PFun}(A,B) \subseteq \mathrm{Rel}(A,B) \\
 & \mathrm{Inj}(A,B) \arrow[ur, phantom, "\subseteq" sloped] &
\end{tikzcd}$$

with

$$\mathrm{Bij}(A, B) = \mathrm{Sur}(A, B) \cap \mathrm{Inj}(A, B) \quad .$$

Proposition 139 *For all finite sets* A *and* B,

$$\#\mathrm{Inj}(A,B) = \begin{cases} \binom{\#B}{\#A} \cdot (\#A)! & \text{, if } \#A \leq \#B \\ 0 & \text{, otherwise} \end{cases}$$

PROOF IDEA:

Go to Workout 37
on page 516

Cantor-Schroeder-Berstein theorem

Definition 140 *A set* A *is of* less than or equal cardinality *to a set* B *whenever there is an injection* $A \rightarrowtail B$, *in which case we write*

$$A \lesssim B \quad \text{or} \quad \#A \leq \#B \quad .$$

NB It follows from the axiom of choice that the existence of a surjection $B \twoheadrightarrow A$ implies $\#A \leq \#B$.

Theorem 141 (Cantor-Schroeder-Bernstein theorem) *For all sets* A *and* B,

$$\big(A \lesssim B \ \& \ B \lesssim A\big) \implies A \cong B \quad .$$

Images

Definition 142 *Let* $R : A \rightarrow\!\!\!\!\!+\,\, B$ *be a relation.*

- *The* direct image *of* $X \subseteq A$ *under* R *is the set* $\overrightarrow{R}(X) \subseteq B$, *defined as*

$$\overrightarrow{R}(X) \;=\; \{\, b \in B \mid \exists\, x \in X.\, x\, R\, b \,\} \;.$$

NB *This construction yields a function* $\overrightarrow{R} : \mathcal{P}(A) \to \mathcal{P}(B)$.

- *The* inverse image *of* $Y \subseteq B$ *under* R *is the set* $\overleftarrow{R}(Y) \subseteq A$, *defined as*

$$\overleftarrow{R}(Y) \;=\; \{\, a \in A \mid \forall\, b \in B.\, a\, R\, b \implies b \in Y \,\}$$

NB *This construction yields a function* $\overleftarrow{R} : \mathcal{P}(B) \to \mathcal{P}(A)$.

Go to Workout 38
on page 518

Replacement axiom

The direct image of every definable functional property on a set is a set.

Set-indexed constructions

For every mapping associating a set A_i to each element of a set I, we have the set

$$\bigcup_{i\in I} A_i = \bigcup \{A_i \mid i \in I\} = \{a \mid \exists i \in I.\, a \in A_i\} \quad .$$

Examples:

1. Indexed disjoint unions:

$$\biguplus_{i\in I} A_i = \bigcup_{i\in I} \{i\} \times A_i$$

2. Finite sequences on a set A:

$$A^* = \biguplus_{n\in\mathbb{N}} A^n$$

3. Finite partial functions from a set A to a set B:

$$(A \rightharpoonup_{\text{fin}} B) = \biguplus_{S\in\mathcal{P}_{\text{fin}}(A)} (S \Rightarrow B)$$

   where

$$\mathcal{P}_{\text{fin}}(A) = \{ S \subseteq A \mid S \text{ is finite} \}$$

4. Non-empty indexed intersections: for $I \neq \emptyset$,

$$\bigcap_{i\in I} A_i = \{ x \in \bigcup_{i\in I} A_i \mid \forall i \in I.\, x \in A_i \}$$

5. Indexed products:

$$\prod_{i\in I} A_i = \left\{ \alpha \in (I \Rightarrow \bigcup_{i\in I} A_i) \;\middle|\; \forall i \in I.\, \alpha(i) \in A_i \right\}$$

Proposition 143 *An enumerable indexed disjoint union of enumerable sets is enumerable.*

YOUR PROOF:

MY PROOF: Let $\{ A_i \}_{i\in I}$ be a family of sets indexed by a set I. Furthermore, let $e : \mathbb{N} \twoheadrightarrow I$ be a surjection and, for all $i \in I$, let $e_i : \mathbb{N} \twoheadrightarrow A_i$ be surjections.

The function $\varepsilon : \mathbb{N} \times \mathbb{N} \to \biguplus_{i\in I} A_i$ defined, for all $(m, n) \in \mathbb{N} \times \mathbb{N}$, by

$$\varepsilon(m, n) = \big(i, e_i(n)\big) \quad , \quad \text{where } i = e(m)$$

is a surjection, which pre-composed with any surjection $\mathbb{N} \twoheadrightarrow \mathbb{N} \times \mathbb{N}$ yields a surjection $\mathbb{N} \twoheadrightarrow \biguplus_{i\in I} A_i$ as required.

Corollary 144 *A countable indexed disjoint union of countable sets is countable.*

Corollary 145 *If X and A are countable sets then so are A^*, $\mathcal{P}_{\mathrm{fin}}(A)$, and $(X \Rightarrow_{\mathrm{fin}} A)$.*

Calculus of bijections, II

- $\biguplus_{i\in[n]} A_i \cong \big((\cdots(A_0 \uplus A_1)\cdots) \uplus A_{n-1}\big)$
- $\prod_{i\in[n]} A_i \cong \big((\cdots(A_0 \times A_1)\cdots) \times A_{n-1}\big)$
- $\big(\biguplus_{i\in I} A_i\big) \times B \cong \biguplus_{i\in I}(A_i \times B)$
- $\big(A \Rightarrow \prod_{i\in I} B_i\big) \cong \prod_{i\in I}(A \Rightarrow B_i)$
- $\big(\big(\biguplus_{i\in I} A_i\big) \Rightarrow B\big) \cong \prod_{i\in I}(A_i \Rightarrow B)$
- $A \cong \biguplus_{a\in A}[1]$
- $(A \Rightarrow B) \cong \prod_{a\in A} B$

Combinatorial examples:

1. The combinatorial content of the binomial theorem comes from a bijection

$$\big(U \Rightarrow (X \uplus Y)\big) \;\cong\; \biguplus_{S\in\mathcal{P}(U)} (S \Rightarrow X) \times (S^c \Rightarrow Y)$$

available for any triple of sets U, X, Y.

2. The combinatorial content underlying the Bell numbers comes from a bijection

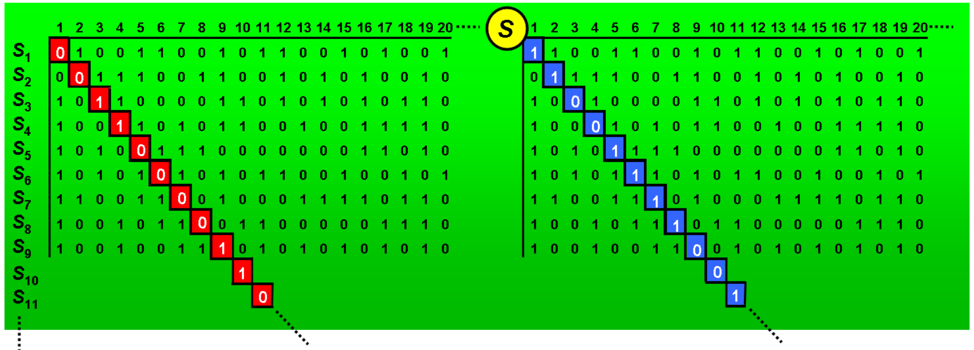
$$\mathrm{Part}\big(A \uplus [1]\big) \;\cong\; \biguplus_{S\subseteq A} \mathrm{Part}(S^c) \quad .$$

available for all sets A.

Go to Workout 39
on page 522

THEOREM OF THE DAY

Cantor's Uncountability Theorem *There are uncountably many infinite 0-1 sequences.*



Proof: Suppose you *could* count the sequences. Label them in order: $S_1, S_2, S_3, \ldots$, and denote by $S_i(j)$ the j-th entry of sequence S_i. Now define a new sequence, S, whose i-th entry is $S_i(i)+1 \pmod 2$. So S is $S_1(1)+1, S_2(2)+1, S_3(3)+1, S_4(4)+1, \ldots$, with all entries remaindered modulo 2. S is certainly an infinite sequence of 0s and 1s. So it must appear in our list: it is, say, S_k, so its k-th entry is $S_k(k)$. But this is, by definition, $S_k(k)+1 \pmod 2 \neq S_k(k)$. So we have contradicted the possibility of forming our enumeration. QED.

The theorem establishes that the real numbers are *uncountable* — that is, they cannot be enumerated in a list indexed by the positive integers $(1, 2, 3, \ldots)$. To see this informally, consider the infinite sequences of 0s and 1s to be the binary expansions of fractions (e.g. $0.010011\ldots = 0/2 + 1/4 + 0/8 + 0/16 + 1/32 + 1/64 + \ldots$). More generally, it says that the set of subsets of a countably infinite set is uncountable, and to see *that*, imagine every 0-1 sequence being a different recipe for building a subset: the i-th entry tells you whether to include the i-th element (1) or exclude it (0).

Georg Cantor (1845–1918) discovered this theorem in 1874 but it apparently took another twenty years of thought about what were then new and controversial concepts: 'sets', 'cardinalities', 'orders of infinity', to invent the important proof given here, using the so-called *diagonalisation method*.

Web link: www.math.hawaii.edu/~dale/godel/godel.html. There is an interesting discussion on mathoverflow.net about the history of diagonalisation: type 'earliest diagonal' into their search box.

Further reading: *Mathematics: the Loss of Certainty* by Morris Kline, Oxford University Press, New York, 1980.

Created by Robin Whitty for www.theoremoftheday.org

Unbounded cardinality

Theorem 146 (Cantor's diagonalisation argument) *For every set A, no surjection from A to $\mathcal{P}(A)$ exists.*

YOUR PROOF:

Btw The *diagonalisation technique* is very important in both logic and computation.

MY PROOF: Assume, by way of contradiction, a surjection $e : A \twoheadrightarrow \mathcal{P}(A)$, and let $a \in A$ be such that

$$e(a) = \{ x \in A \mid x \notin e(x) \} \quad .$$

Then,

$$\forall x \in A. \, x \in e(a) \iff x \notin e(x)$$

and hence

$$a \in e(a) \iff a \notin e(a) \quad ;$$

that is, a contradiction. Therefore, there is no surjection from A to $\mathcal{P}(A)$.

Definition 147 *A fixed-point of a function $f : X \to X$ is an element $x \in X$ such that $f(x) = x$.*

Btw Solutions to many problems in computer science are computations of fixed-points.

Theorem 148 (Lawvere's fixed-point argument) *For sets A and X, if there exists a surjection $A \twoheadrightarrow (A \Rightarrow X)$ then every function $X \to X$ has a fixed-point; and hence X is a singleton.*

YOUR PROOF:

MY PROOF: Assume a surjection $e : A \twoheadrightarrow (A \Rightarrow X)$. Then, for an arbitrary function $f : X \to X$ let $a \in A$ be such that

$$e(a) = \lambda\, x \in A.\, f\big(e(x)(x)\big) \;\in (A \Rightarrow X) \quad .$$

Then,

$$e(a)(a) = f\big(e(a)(a)\big) \quad ,$$

and we are done.

Version of February 12, 2014

Corollary 149 *The sets*

$$\mathcal{P}(\mathbb{N}) \;\cong\; \big(\mathbb{N} \Rightarrow [2]\big) \;\cong\; [0,1] \;\cong\; \mathbb{R}$$

are not enumerable.

Corollary 150 *There are* non-computable *infinite sequences of bits; that is, there are infinite sequences of bits* σ *with the property that for all programs* p *that forever print bits there is a natural number index* i_p *for which the* i_p *bit of* σ *disagrees with the* i_p *bit output by* p*.*

Version of February 12, 2014

Corollary 151 *For a set* D*, there exists a surjection* $D \twoheadrightarrow (D \Rightarrow D)$ *iff* D *is a singleton.*

Note however that in ML we have the

```
datatype
  D = afun of D -> D
```

coming with functions

```
afun                          : (D->D) -> D

fn x => case x of afun f => f  : D -> (D->D)
```

that is highly non-trivial!

Version of February 12, 2014

And indeed is inhabited by an enumerable infinitude of elements; for instance,

```
afun( fn x => x )                              : D

afun( fn x => case x of afun f => f x )        : D

afun( fn x => case x of afun f => f f x )      : D

afun( fn x => case x of
        afun f => case f x of
          afun g => g x )                      : D
```

Go to Workout 40
on page 523

Foundation axiom

The membership relation is well-founded.

Thereby, providing a

Principle of $\in$*-Induction* .

Workout 27
from page 357

1. Let $A = \{1,2,3,4\}$ and $B = \{a,b,c,d\}$, and $C = \{x,y,z\}$. Let $R = \{(1,a),(2,d),(3,a),(3,b),(3,d)\} : A \twoheadrightarrow B$ and $S = \{(b,x),(b,x),(c,y),(d,z)\} : B \twoheadrightarrow C$. What is their composition $S \circ R : A \twoheadrightarrow C$?

2. Prove Theorem 94 on page 341.

3. For a relation $R : A \twoheadrightarrow B$, let its *opposite*, or *dual*, $R^{op} : B \twoheadrightarrow A$ be defined by

$$b\, R^{op}\, a \iff a\, R\, b \quad .$$

For $R, S : A \twoheadrightarrow B$, prove that

(a) $R \subseteq S \implies R^{op} \subseteq S^{op}$.

(b) $(R \cap S)^{op} = R^{op} \cap S^{op}$.

(c) $(R \cup S)^{op} = R^{op} \cup S^{op}$.

4. Show that in a directed graph on a finite set with cardinality n there is a path between two nodes iff there is a path of length $n-1$.

Workout 28
from page 362

1. For a relation R on a set A, prove that R is antisymmetric iff $R \cap R^{op} \subseteq I_A$.

2. Let $\mathcal{F} \subseteq \mathcal{P}(A \times B)$ be a collection of relations from A to B. Prove that,

(a) for all $R : X \twoheadrightarrow A$,

$$\left(\bigcup \mathcal{F}\right) \circ R = \bigcup \{\, S \circ R \mid S \in \mathcal{F} \,\} : X \twoheadrightarrow B \quad ,$$

and that,

(b) for all $R : B \twoheadrightarrow Y$,

$$R \circ \left(\bigcup \mathcal{F}\right) = \bigcup \{\, R \circ S \mid S \in \mathcal{F} \,\} : A \twoheadrightarrow Y \quad .$$

What happens in the case of big intersections?

3. For a relation R on a set A, let

$$\mathcal{T}_R = \{\, Q \subseteq A \times A \mid R \subseteq Q \ \& \ Q \text{ is transitive} \,\} \quad .$$

For $R^{\circ+} = R \circ R^{\circ*}$, prove that (i) $R^{\circ+} \in \mathcal{T}_R$ and (ii) $R^{\circ+} \subseteq \bigcap \mathcal{T}_R$. Hence, $R^{\circ+} = \bigcap \mathcal{T}_R$.

Workout 29
from page 373

1. Let $A_2 = \{1, 2\}$ and $A_3 = \{a, b, c\}$. List the elements of the four sets $(A_i \Rightarrow A_j)$ for $i, j \in \{2, 3\}$.
2. Prove Theorem 113 on page 367.
3. Show that $\big(\mathrm{PFun}(A, B), \subseteq\big)$ is a partial order.
4. Show that the intersection of a collection of partial functions in $\mathrm{PFun}(A, B)$ is a partial function in $\mathrm{PFun}(A, B)$.

5. Show that the union of two partial functions in $\mathrm{PFun}(A, B)$ is a relation that need not be a partial function. But that for $f, g \in \mathrm{PFun}(A, B)$ such that $f \subseteq h \supseteq g$ for some $h \in \mathrm{PFun}(A, B)$, the union $f \cup g$ is a partial function in $\mathrm{PFun}(A, B)$.

Workout 30
from page 379

1. Let $A_2 = \{1, 2\}$ and $A_3 = \{a, b, c\}$. List the elements of the four sets $(A_i \Rightarrow A_j)$ for $i, j \in \{2, 3\}$.
2. Prove Theorem 118 on page 378.

Workout 31
from page 385

1. Prove Theorem 122 on page 383.
2. For $f : A \longrightarrow B$, prove that if there are $g, h : B \longrightarrow A$ such that $g \circ f = \mathrm{id}_A$ and $f \circ h = \mathrm{id}_B$ then $g = h$.

   Conclude as a corollary that, whenever it exists, the inverse of a function is unique.

Workout 32
from page 391

1. For a relation R on a set A, prove that
   - R is reflexive iff $I_A \subseteq R$,
   - R is symmetric iff $R \subseteq R^{op}$,
   - R is transitive iff $R \circ R \subseteq R$.
2. Prove that the isomorphism relation $\cong$ between sets is an equivalence relation.
3. Prove that the identity relation I_A on a set A is an equivalence relation and that $A_{/I_A} \cong A$.

4. For an equivalence relation E on a set A, show that $[a_1]_E = [a_2]_E$ iff $a_1 \mathrel{E} a_2$, where $[a]_E = \{ x \in A \mid x \mathrel{E} a \}$ as on page 389.
5. Let E be an equivalence relation on a set A. We want to show here that to define a function out of the quotient set $A_{/E}$ is, essentially, to define a function out of A that identifies equivalent elements.

   To formalise this, you are required to show that for any function $f : A \to B$ such that $f(x) = f(y)$ for all $(x, y) \in E$ there exists a unique function $f_{/E} : A_{/E} \to B$ such that $f_{/E} \circ q = f$, where $q : A \twoheadrightarrow A_{/E}$ denotes the quotient function.

   Btw This proof needs some care, so please revise your argument. Sample applications of its use follow.

6. For a positive integer m, let $\equiv_m$ be the equivalence relation on $\mathbb{Z}$ given by
   $$x \equiv_m y \iff x \equiv y \pmod{m} \quad .$$
   Define a mapping $\mathbb{Z}_{/\equiv_m} \to \mathbb{Z}_m$ and prove it bijective.
7. Show that the relation $\equiv$ on $\mathbb{Z} \times \mathbb{N}^+$ given by
   $$(a, b) \equiv (x, y) \iff a \cdot x = y \cdot b$$
   is an equivalence relation. Define a mapping $(\mathbb{Z} \times \mathbb{N}^+)_{/\equiv} \to \mathbb{Q}$ and prove it bijective.
8. Let B be a subset of a set A. Define the relation E on $\mathcal{P}(A)$ by
   $$(X, Y) \in E \iff X \cap B = Y \cap B \quad .$$
   Show that E is an equivalence relation. Define a mapping $\mathcal{P}(A)_{/E} \to \mathcal{P}(B)$ and prove it bijective.

9. We will see here that there is a canonical way in which every preorder can be turned into a partial order.

   (a) Let $(P, \sqsubseteq)$ be a preorder. Define $\simeq \subseteq P \times P$ by setting
   $$x \simeq y \iff (x \sqsubseteq y \ \& \ y \sqsubseteq x)$$
   for all $x, y \in P$.

   Prove that $\simeq$ is an equivalence relation on P.

   (b) Consider now $P_{/\simeq}$ and define $\underset{\sim}{\sqsubset} \subseteq P_{/\simeq} \times P_{/\simeq}$ by setting
   $$X \underset{\sim}{\sqsubset} Y \iff \forall x \in X. \exists y \in Y. x \sqsubseteq y$$
   for all $X, Y \in P_{/\simeq}$.

   Prove that $\left(P_{/\simeq}, \underset{\sim}{\sqsubset}\right)$ is a partial order.

Workout 33
from page 396

1. Make sure that you understand the calculus of bijections on pages 392 and 393.
2. Write ML functions describing the calculus of bijections, where the set-theoretic product $\times$ is interpreted as the product type `*`, the set-theoretic disjoint union $\uplus$ is interpreted as the sum datatype `sum` (see page 496), and the set-theoretic function $\Rightarrow$ is interpreted as the arrow type `->`.

   Btw The theory underlying this question is known as the *Curry-Howard correspondence*.

For instance,

- for the bijection

  $$\big((A \times B) \Rightarrow C\big) \cong \big(A \Rightarrow (B \Rightarrow C)\big)$$

  you need provide ML functions of types

  ```
  (('a*'b)->'c) -> (a->(b->c))
  ```

  and

  ```
  ((a->(b->c)) -> (('a*'b)->'c)
  ```

  such that when understood as functions on sets yield a bijection, and

- for the implication

  $$(X \cong A \ \& \ B \cong Y) \implies (A \Rightarrow B) \cong (X \Rightarrow Y)$$

  you need provide an ML function of type

  ```
  ('x->'a)*('b->'y) -> ('a->'b)->('x->'y)
  ```

  such that when understood as a function between sets it constructs the required compound bijection from the two given component ones.

Workout 34
from page 399

1. Prove Theorem 129.

Workout 35
from page 407

1. Give three examples of functions that are surjective and three examples of functions that are not.
2. Prove Theorem 132 on page 404.
3. From surjections $A \twoheadrightarrow B$ and $X \twoheadrightarrow Y$ define, and prove surjective, functions $A \times B \twoheadrightarrow X \times Y$ and $A \uplus B \twoheadrightarrow X \uplus Y$.
4. For an infinite set S, prove that if there is a surjection $\mathbb{N} \to S$ then there is a bijection $\mathbb{N} \to S$.

Workout 36
from page 414

1. Prove Proposition 136.

Workout 37
from page 420

1. Give three examples of functions that are injective and three of functions that are not.
2. Prove Theorem 138 on page 418.
3. For a set X, prove that there is no injection $\mathcal{P}(X) \to X$.

   [Hint: By way of contradiction, assume an injection $f : \mathcal{P}(X) \to X$, consider

   $$W = \{\, x \in X \mid \exists Z \in \mathcal{P}(X).\, x = f(Z) \ \&\ x \notin Z \,\} \in \mathcal{P}(X) \quad ,$$

   and ask whether or not $f(W) \in X$ is in W.]

4. For an infinite set S, prove that the following are equivalent:
   (a) There is a bijection $\mathbb{N} \to S$.
   (b) There is an injection $S \to \mathbb{N}$.
   (c) There is a surjection $\mathbb{N} \to S$

Workout 38
from page 425

1. What is the direct image of $\mathbb{Z}$ under the negative-doubling function $\mathbb{Z} \to \mathbb{Z} : n \mapsto -2 \cdot n$? And the direct image of $\mathbb{N}$?

2. For a relation $R : A \twoheadrightarrow B$ and $X \subseteq A$, show that
$$\overrightarrow{R}(X) \;=\; \bigcup_{x \in X} \overrightarrow{R}\big[\{x\}\big] \quad .$$

3. For a relation $R : A \twoheadrightarrow B$ and $Y \subseteq B$, show that
$$\overleftarrow{R}(Y) \;=\; \big\{\, a \in A \mid \overrightarrow{R}\big(\{a\}\big) \subseteq Y \,\big\} \quad .$$
Conclude as a corollary that, for a function $f : A \to B$,
$$\overleftarrow{f}(Y) \;=\; \big\{\, a \in A \mid f(a) \in Y \,\big\} \quad .$$

4. Show that, by inverse image,

every map $A \to B$ induces a
Boolean algebra map $\mathcal{P}(B) \to \mathcal{P}(A)$.

That is, for every function $f : A \to B$,

- $\overleftarrow{f}(\emptyset) = \emptyset$
- $\overleftarrow{f}(X \cup Y) = f^{-1}[X] \cup f^{-1}[Y]$
- $\overleftarrow{f}(B) = A$
- $\overleftarrow{f}(X \cap Y) = \overleftarrow{f}(X) \cap \overleftarrow{f}(Y)$
- $\overleftarrow{f}(X^c) = \big(\overleftarrow{f}(X)\big)^c$

for all $X, Y \subseteq B$.

(If you like this kind of stuff, investigate what happens with partial functions and relations; and also look at direct images.)

5. Show that

the inverse and direct images of a relation form a
Galois connection[a]

That is, for all $R : A \twoheadrightarrow B$, the direct image and inverse image functions

$$\begin{tikzcd} \mathcal{P}(A) \arrow[r, shift left, "\overrightarrow{R}"] & \mathcal{P}(B) \arrow[l, shift left, "\overleftarrow{R}"] \end{tikzcd}$$

are such that

- for all $X \subseteq X'$ in $\mathcal{P}(A)$, $\overrightarrow{R}(X) \subseteq \overrightarrow{R}(X')$;
- for all $Y \subseteq Y'$ in $\mathcal{P}(B)$, $\overleftarrow{R}(Y) \subseteq \overleftarrow{R}(Y')$;
- for all $X \in \mathcal{P}(A)$ and $Y \in \mathcal{P}(B)$, $\overrightarrow{R}(X) \subseteq Y \iff X \subseteq \overleftarrow{R}(Y)$.

[a] This is a fundamental mathematical concept, with many applications in computer science (e.g. in the context of abstract interpretations for static analysis).

6. Prove that for a surjective function $f : A \twoheadrightarrow B$, the direct image function $\overrightarrow{f} : \mathcal{P}(A) \to \mathcal{P}(B)$ is surjective.

7. For sets A and X, show that the mapping
$$f \;\mapsto\; \big\{\, b \subseteq A \mid \exists x \in X.\, b = \overleftarrow{f}\big[\{x\}\big] \,\big\}$$
yields a function $\mathrm{Sur}(A, X) \to \mathrm{Part}(A)$. Is it surjective? And injective?

Workout 39
from page 434

1. Prove Corollary 145 on page 431.
2. Make sure that you understand the calculus of bijections on page 432.

Workout 40
from page 443

1. Which of the following sets are finite, which are infinite but countable, and which are uncountable?
   (a) $\{ f \in (\mathbb{N} \Rightarrow [2]) \mid \forall n \in \mathbb{N}.\, f(n) \leq f(n+1) \}$
   (b) $\{ f \in (\mathbb{N} \Rightarrow [2]) \mid \forall n \in \mathbb{N}.\, f(2 \cdot n) \neq f(2 \cdot n + 1) \}$
   (c) $\{ f \in (\mathbb{N} \Rightarrow [2]) \mid \forall n \in \mathbb{N}.\, f(n) \neq f(n+1) \}$
   (d) $\{ f \in (\mathbb{N} \Rightarrow [2]) \mid \forall n \in \mathbb{N}.\, f(n) \leq f(n+1) \}$
   (e) $\{ f \in (\mathbb{N} \Rightarrow [2]) \mid \forall n \in \mathbb{N}.\, f(n) \geq f(n+1) \}$