Workouts

for Part IA CST 2013/14

Discrete Mathematics For Computer Science

<cl.cam.ac.uk/teaching/1314/DiscMath>

Prof Marcelo Fiore

Marcelo.Fiore@cl.cam.ac.uk

Workout 1
from page 45

NB The main aim here is for you to practice the analysis and understanding of mathematical statements (e.g. by isolating the different components of composite statements), and exercise the art of presenting a logical argument in the form of a clear proof (e.g. by following proof strategies and patterns).

Prove or disprove the following statements.

1. The product of two even natural numbers is even.
2. The product of an even and an odd natural number is odd.
3. If $x > 3$ and $y < 2$ then $x^2 - 2 \cdot y > 5$.

Workout 2
from page 52

NB The main aim here is for you to practice the analysis and understanding of mathematical statements (e.g. by isolating the different components of composite statements), and exercise the art of presenting a logical argument in the form of a clear proof (e.g. by following proof strategies and patterns).

Prove or disprove the following statements.

1. Suppose n is a natural number larger than 2, and n is not a prime number. Then $2 \cdot n + 13$ is not a prime number.

2. If $x^2 + y = 13$ and $y \neq 4$ then $x \neq 3$.

Workout 3
from page 63

1. Characterise those integers d and n such that:

   (a) $0 \mid n$,

   (b) $d \mid 0$.

2. Write an ML function

   ```
   divides:  int * int -> bool
   ```

   such that, for all integers m and n, $\texttt{divides}(m,n) = \texttt{true}$ iff $m \mid n$ holds.

You may use `div`, but note that the function

```
fn (m,n) => ( n div m ) = 0
```

will not do.

3. Let n be a natural number. Show that $n \mid n$.

Workout 4
from page 66

1. Let i, j be integers and let m be a positive integer. Show that:

   (a) $i \equiv i \pmod{m}$

   (b) $i \equiv j \pmod{m} \implies j \equiv i \pmod{m}$

   (c) $i \equiv j \pmod{m} \implies i^2 \equiv j^2 \pmod{m}$

2. Find integers i, j, natural numbers k, l, and a positive integer m for which both $i \equiv j \pmod{m}$ and $k \equiv l \pmod{m}$ hold while $i^k \equiv j^l \pmod{m}$ does not.

3. Find an integer i, natural numbers k, l, and a positive integer m for which $k \equiv l \pmod{m}$ holds while $i^k \equiv i^l \pmod{m}$ does not.

4. Formalise and prove the following statement: A natural number is a multiple of 3 iff so is the number obtained by summing its digits. What about multiples of 9? And multiples of 11?

Workout 5
from page 68

NB The main aim here is for you to practice the analysis and understanding of mathematical statements (e.g. by isolating the different components of composite statements), and exercise the art of presenting a logical argument in the form of a clear proof (e.g. by following proof strategies and patterns).

1. Prove or disprove that, for an integer n, n^2 is even if and only if n is even.

2. Show that for all integers d and n the following statements are equivalent:
   (a) $d \mid n$.
   (b) $-d \mid n$.
   (c) $d \mid -n$.
   (d) $-d \mid -n$.

3. Let k, m, n be integers with k positive. Show that:

$$(k \cdot m) \mid (k \cdot n) \iff m \mid n \quad .$$

Workout 6
from page 77

NB The main aim here is for you to practice the analysis and understanding of mathematical statements (e.g. by isolating the different components of composite statements), and exercise the art of presenting a logical argument in the form of a clear proof (e.g. by following proof strategies and patterns).

1. Prove or disprove the following statements.

   (a) For real numbers a and b, if $0 < a < b$ then $a^2 < b^2$.

   (b) For real numbers a, b, and c with $a > b$, if $a \cdot c \leq b \cdot c$ then $c \geq 0$.

2. Prove or disprove that for all natural numbers n, $2 \mid 2^n$.

3. Let $P(m)$ be a statement for m ranging over the natural numbers, and consider the derived statement

$$P^{\#}(m) \;=\; \forall\,\text{integer}\ k.\ 0 \leq k \leq m \implies P(k)$$

again for m ranging over the natural numbers.

Prove the following equivalences:

- $P^{\#}(0) \iff P(0)$
- $\big(P^{\#}(n) \implies P^{\#}(n+1)\big) \iff \big(P^{\#}(n) \implies P(n+1)\big)$
- $$\begin{array}{l} \quad\forall\,\text{natural number}\ m.\ P^{\#}(m) \\ \iff \\ \quad\forall\,\text{natural number}\ m.\ P(m) \end{array}$$

Workout 7
from page 85

1. Taking inspiration from the proof of Theorem 20 (on page 83), or otherwise, prove that for all integers n,

$$30 \mid n \iff (2 \mid n \ \& \ 3 \mid n \ \& \ 5 \mid n) \quad .$$

   Can you spot a pattern here? Can you formalise it, test it, and prove it?

2. Find a counterexample to the statement: For all positive integers k, m, n, if $m \mid k \ \& \ n \mid k$ then $(m \cdot n) \mid k$.

3. Show that for all integers l, m, n,

$$l \mid m \ \& \ m \mid n \implies l \mid n \ .$$

4. Prove that for all integers d, k, l, m, n,

   (a) $d \mid m \ \& \ d \mid n \implies d \mid (m + n)$,

   (b) $d \mid m \implies d \mid k \cdot m$,

   (c) $d \mid m \ \& \ d \mid n \implies d \mid (k \cdot m + l \cdot n)$.

5. Prove that for all integers i, j, k, l, m, n with m positive and n nonnegative,

   (a) $i \equiv j \pmod{m} \ \& \ j \equiv k \pmod{m} \implies i \equiv k \pmod{m}$

   (b) $i \equiv j \pmod{m} \ \& \ k \equiv l \pmod{m} \implies i + k \equiv j + l \pmod{m}$

   (c) $i \equiv j \pmod{m} \ \& \ k \equiv l \pmod{m} \implies i \cdot k \equiv j \cdot l \pmod{m}$

   (d) $i \equiv j \pmod{m} \implies i^n \equiv j^n \pmod{m}$

Workout 8
from page 99

NB The main aim here is for you to practice the analysis and understanding of mathematical statements (e.g. by isolating the different components of composite statements), and exercise the art of presenting a logical argument in the form of a clear proof (e.g. by following proof strategies and patterns).

Prove or disprove the following statements.

1. For every real number x, if $x > 0$ then there is a real number y such that $y(y + 1) = x$.

2. For all real numbers x and y there is a real number z such that $x + z = y - z$.

3. For all integers x and y there is an integer z such that $x + z = y - z$.

4. For every real number x, if $x \neq 2$ then there is a unique real number y such that $2y/(y + 1) = x$.

5. The addition of two rational numbers is a rational number.

6. Prove that for all natural numbers p, p_1, p_2,

   (a) $\min(p, p_1 + p_2) = \min\big(p, \min(p, p_1) + \min(p, p_2)\big)$, and

   (b) $\min(p, p_1 + p_2) = \min(p, p_1) + \min\big(p - \min(p, p_1), p_2\big)$.

Workout 9
from page 106

NB The main aim here is for you to practice the analysis and understanding of mathematical statements (e.g. by isolating the different components of composite statements), and exercise the art of presenting a logical argument in the form of a clear proof (e.g. by following proof strategies and patterns).

1. Prove or disprove that for integers m and n, if $m \cdot n$ is even, then either m is even or n is even.

2. If every pair of people in a group has met, then we will call the group a *club*. If every pair of people in a group has not met, then we will call it a group of *strangers*.

   Prove that every collection of 6 people includes a club of 3 people or a group of 3 strangers.

3. Show that for all integers m and n,

   $$m \mid n \ \& \ n \mid m \implies m = n \vee m = -n \ .$$

4. Prove or disprove that for all positive integers k, m, n,

   if $k \mid (m \cdot n)$ then $k \mid m$ or $k \mid n$.

5. Prove that for all integers n, there exist natural numbers i and j such that $n = i^2 - j^2$ iff either $n \equiv 0 \pmod 4$, or $n \equiv 1 \pmod 4$, or $n \equiv 3 \pmod 4$. [Hint: Recall Proposition 22 (on page 91).]

Workout 10
from page 127

1. Search for “Fermat’s Little Theorem” in YouTube and watch a video or two about it.

2. Let i and n be positive integers and let p be a prime. Show that if $n \equiv 1 \pmod{p-1}$ then $i^n \equiv i \pmod{p}$ for all i not multiple of p.

Workout 11
from page 130

Justify the boolean equivalences:

$$\begin{aligned}
\neg(P \Longrightarrow Q) &\quad\Longleftrightarrow\quad P \mathbin{\&} \neg Q \\
\neg(P \Longleftrightarrow Q) &\quad\Longleftrightarrow\quad P \Longleftrightarrow \neg Q \\
\neg(P \mathbin{\&} Q) &\quad\Longleftrightarrow\quad (\neg P) \vee (\neg Q) \\
\neg(P \vee Q) &\quad\Longleftrightarrow\quad (\neg P) \mathbin{\&} (\neg Q) \\
\neg(\neg P) &\quad\Longleftrightarrow\quad P \\
\neg P &\quad\Longleftrightarrow\quad (P \Rightarrow \mathbf{false}) \\
(P \Longrightarrow Q) &\quad\Longleftrightarrow\quad (\neg Q \Longrightarrow \neg P) \\
(\mathbf{false} \Longrightarrow P) &\quad\Longleftrightarrow\quad \mathbf{true}
\end{aligned}$$

$$\left(P_1 \implies (P_2 \implies Q)\right) \iff \left((P_1 \,\&\, P_2) \implies Q\right)$$

$$(P \iff Q) \iff \left((P \implies Q) \,\&\, (Q \implies P)\right)$$

by means of truth tables, where the truth tables for the boolean statements are:

P	Q	$P \implies Q$	$P \iff Q$	$P \,\&\, Q$	$P \vee Q$	$\neg P$
true	**true**	**true**	**true**	**true**	**true**	**false**
false	**true**	**true**	**false**	**false**	**true**	**true**
true	**false**	**false**	**false**	**false**	**true**	
false	**false**	**true**	**true**	**false**	**false**	

Workout 12
from page 143

Give three justifications for the following scratch work:

Before using the strategy

Assumptions	Goal
	$P \Longrightarrow Q$
$\vdots$	

After using the strategy

Assumptions	Goal
	contradiction
$\vdots$	
$P \quad , \quad \neg Q$	

Workout 13
from page 171

1. Show that for every integer n, the remainder when n^2 is divided by 4 is either 0 or 1.

2. Write the division algorithm in imperative code.

3. Prove that for all natural numbers k, l, and positive integer m,

   (a) $\mathrm{rem}(k+l,m) = \mathrm{rem}\big(k + \mathrm{rem}(l,m), m\big)$, and

   (b) $\mathrm{rem}(k \cdot l,m) = \mathrm{rem}\big(k \cdot \mathrm{rem}(l,m), m\big)$.

4. Prove the following Linearity Property of the Division Algorithm: for all positive integers k, m, n,

$$\mathtt{divalg}(k \cdot m, k \cdot n) = \big(\mathrm{quo}(m,n), k \cdot \mathrm{rem}(m,n)\big) \quad .$$

5. Prove the General Division Theorem for integers:

   For every integer m and non-zero integer n, there exists a unique pair of integers q and r such that $0 \leq r < |n|$, and $m = q \cdot n + r$.

6. Prove that for all positive integers m and n,

   (a) $n < m \implies \mathrm{quo}(n, m) = 0 \ \& \ \mathrm{rem}(n, m) = n$, and

   (b) $n \leq m \implies \mathrm{rem}(m, n) < m/2$.

Workout 14
from page 178

1. Calculate that $2^{153} \equiv 53 \pmod{153}$.

   Btw, at first sight this seems to contradict Fermat's Little Theorem, why isn't this the case though?

2. Let m be a positive integer.

   (a) Prove the associativity of the addition and multiplication operations in $\mathbb{Z}_m$; that is, that for all i, j, k in $\mathbb{Z}_m$,

   $(i +_m j) +_m k = i +_m (j +_m k)$, and

   $(i \cdot_m j) \cdot_m k = i \cdot_m (j \cdot_m k)$.

   [Hint: Use Workout 13.3 on page 472.]

(b) Prove that the additive inverse of k in $\mathbb{Z}_m$ is $[-k]_m$.

3. Calculate the addition and multiplication tables, and the additive and multiplicative inverses tables for $\mathbb{Z}_3$, $\mathbb{Z}_6$, and $\mathbb{Z}_7$. Can you spot any patterns?

Workout 15
from page 215

1. Write Euclid's Algorithm in imperative code.
2. Calculate the set $\mathrm{CD}(666, 330)$ of common divisors of 666 and 330.
3. Show that for all integers k, the conjuction of the two statements

   - $k \mid m \ \& \ k \mid n$, and
   - for all positive integers d, $d \mid m \ \& \ d \mid n \implies d \mid k$

   is equivalent to the single statement

   for all positive integers d, $d \mid m \ \& \ d \mid n \iff d \mid k$.

4. Prove that for all positive integers m and n,

$$\gcd(m, n) = m \iff m \mid n \ .$$

5. Prove that, for all positive integers m and n, and integers k and l,

$$\gcd(m, n) \mid (k \cdot m + l \cdot n) \ .$$

6. Prove that, for all positive integers m and n, there exist integers k and l such that $k \cdot m + l \cdot n = 1$ iff $\gcd(m, n) = 1$.

7. For all positive integers m and n, define

$$m' = \frac{m}{\gcd(m,n)} \quad \text{and } n' = \frac{n}{\gcd(m,n)} \quad .$$

Prove that

(a) m' and n' are positive integers, and that

(b) $\gcd(m', n') = 1$.

Conclude that the representation in lowest terms of the fraction m/n is m'/n'.

8. Use the Key Lemma 56 (on page 189) to show the correctness of the following algorithm

```
fun gcd0( m , n )
  = if m = n then m
    else
      let
        val p = min(m,n) ; val q = max(m,n)
      in
        gcd0( p , q - p )
      end
```

for computing the gcd of two positive integers. Give an analysis of the time complexity.

Workout 16
from page 221

1. Revisit Theorem 20 (on page 83) and Workout 7.1 (on page 462) using Euclid's Theorem (Corollary 64 on page 64) to give new proofs for them. Can you now state and prove a general result from which these follow?

Workout 17
from page 235

1. Write the Extended Euclid's Algorithm in imperative code.

2. Prove Theorem 68 (on page 226).

3. Let m and n be positive integers with $\gcd(m, n) = 1$. Prove that for every natural number k,

$$m \mid k \;\&\; n \mid k \implies (m \cdot n) \mid k \quad .$$

4. Prove that for all positive integers l, m, and n, if $\gcd(l, m \cdot n) = 1$ then $\gcd(l, m) = 1$ and $\gcd(l, n) = 1$.

5. Prove that for all integers n and primes p, if $n^2 \equiv 1 \pmod{p}$ then either $n \equiv 1 \pmod{p}$ or $n \equiv -1 \pmod{p}$.

6. (a) Show that the $\gcd$ of two linear combinations of positive integers m and n is itself a linear combination of m and n.

   (b) Argue that the output $((s, t), r)$ of calling `egcditer` with input

$$\Big(\big((s_1, t_1) \, , \, s_1 \cdot m + t_1 \cdot n \big) \, , \, \big((s_2, t_2) \, , \, s_2 \cdot m + t_2 \cdot n \big) \Big)$$

   is such that

$$\gcd\big(s_1 \cdot m + t_1 \cdot n \, , \, s_2 \cdot m + t_2 \cdot n \big) = r = s \cdot m + t \cdot n \quad .$$

Workout 18
from page 240

1. Search for “Diffie-Hellman Key Exchange” in YouTube and watch a video or two about it.

Workout 19
from page 259

1. State the Principle of Induction for the ML

```
datatype
  N = zero | succ of N
```

2. Establish the following:

   (a) For all positive integers m and n,

   $$(2^n - 1) \cdot \sum_{i=0}^{m-1} 2^{i \cdot n} = 2^{m \cdot n} - 1 \quad .$$

   (b) Suppose k is a positive integer that is not prime. Then $2^k - 1$ is not prime.

3. Recall that the Fibonacci numbers F_n for n ranging over the natural numbers are defined by $F_0 = F_1 = 1$ and $F_n = F_{n-1} + F_{n-2}$ for $n \geq 2$.

   (a) Prove that $\mathtt{gcd}(F_{n+1}, F_n)$ terminates in $n + 1$ steps for all natural numbers n.

   (b) Prove that for all natural numbers n,

$$F_n \cdot F_{n+2} = {F_{n+1}}^2 + (-1)^n \ .$$

Workout 20
from page 283

1. Equation $(\star)$ on page 282 gives a *Transfer Principle* of additive properties of $\min$ as multiplicative properties of $\gcd$. To see this, prove that for all positive integers m, m_1, m_2,

   (a) $\gcd(m, m_1 \cdot m_2) = \gcd\big(m\,,\ \gcd(m, m_1) \cdot \gcd(m, m_2)\big)$, and

   (b) $\gcd(m, m_1 \cdot m_2) = \gcd(m, m_1) \cdot \gcd\left(\frac{m}{\gcd(m,m_1)}, m_2\right)$.

   [Hint: Use Workout 8.6 on page 465.]

2. Give two proofs of the following proposition

   > For all positive integers m, n, p, q such that $\gcd(m, n) = \gcd(p, q) = 1$, if $m \cdot q = p \cdot n$ then $m = p$ and $n = q$.

   respectively using Theorem 63 and Equation $(\star)$ on page 282.

Workout 21
from page 296

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 301

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 313

1. Referring to the definitions on pages 186 and 187, show that $\mathrm{CD}(m, n) = \mathrm{D}(m) \cap \mathrm{D}(n)$.

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 $\mathcal{P}\big(\mathcal{P}(\mathcal{P}(\emptyset))\big)$, 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:

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

If you like this kind of stuff, push on.

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

(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) $A^c = \mathcal{U} \triangle A$.

(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 $\mathcal{U}$, the structure $\big(\mathcal{P}(\mathcal{U}), \emptyset, \triangle, \mathcal{U}, \cap\big)$ is a commutative ring.

    (a) Prove that $(\mathcal{P}(\mathcal{U}), \emptyset, \triangle)$ is a commutative group; that is, a commutative monoid (refer to page 154) in which every element has an inverse (refer to page 159).

    (b) Prove that $\mathcal{P}(\mathcal{U})$ with additive structure $(\emptyset, \triangle)$ and multiplicative structure $(\mathcal{U}, \cap)$ is a commutative semiring.

Workout 24
from page 322

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 $A \times \mathrm{B}$.

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 334

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 $\left\{\, A_i \mid i \in I \,\right\}$ stand for $\left\{A_2, A_3, A_4, A_5\right\}$.
   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.

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

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

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.

Workout 26
from page 339

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

Workout 27
from page 363

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

2. Prove Theorem 96 (on page 347).

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

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

For $R, S : A \relbar\joinrel\mapsto B$, prove that

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

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

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

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 368

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

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

   (a) for all $R : X \longrightarrow\!\!\!\!\!\!\!+\;\; A$,

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

   and that,

   (b) for all $R : B \longrightarrow\!\!\!\!\!\!\!+\;\; Y$,

   $$R \circ \left(\bigcup \mathcal{F}\right) = \bigcup \{ R \circ S \mid S \in \mathcal{F} \} : A \longrightarrow\!\!\!\!\!\!\!+\;\; Y \quad .$$

   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 379

1. Let $A_2 = \{1,2\}$ and $A_3 = \{a,b,c\}$. List the elements of the four sets $(A_i \rightrightarrows A_j)$ for $i,j \in \{2,3\}$.

2. Prove Theorem 115 (on page 373).

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 385

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 120 (on page 384).

Workout 31
from page 391

1. Prove Theorem 124 (on page 389).

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 397

1. For a relation R on a set A, prove that
   - R is reflexive iff $I_A \subseteq R$,
   - R is symmetric iff $R \subseteq R^{\mathrm{op}}$,
   - 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 395.

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
$$(a, b) \equiv (x, y) \iff a \cdot y = x \cdot b$$
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 402

1. Make sure that you understand the calculus of bijections on pages 398 and 399.

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 502), 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 405

1. Prove Theorem 131 (on page 404).

Workout 35
from page 413

1. Give three examples of functions that are surjective and three examples of functions that are not.

2. Prove Theorem 134 (on page 410).

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 420

1. Prove Proposition 138 (on page 419).

Workout 37
from page 426

1. Give three examples of functions that are injective and three of functions that are not.

2. Prove Theorem 140 (on page 424).

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 $\mathbb{N} \longrightarrow S$.
   (b) There is an injection $S \longrightarrow \mathbb{N}$.
   (c) There is a surjection $\mathbb{N} \longrightarrow S$

Workout 38
from page 431

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

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

3. For a relation $R : A \longrightarrow\!\!\!\!\!\!+\;\; B$ 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 $f : A \longrightarrow B$,
$$\overleftarrow{f}(Y) \;=\; \big\{\, a \in A \mid f(a) \in Y \,\big\} \quad .$$

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 $f : A \to B$,

- $\overleftarrow{f}(\emptyset) = \emptyset$
- $\overleftarrow{f}(X \cup Y) = \overleftarrow{f}(X) \cup \overleftarrow{f}(Y)$
- $\overleftarrow{f}(B) = A$
- $\overleftarrow{f}(X \cap Y) = \overleftarrow{f}(X) \cap \overleftarrow{f}(Y)$
- $\overleftarrow{f}(X^c) = \left(\overleftarrow{f}(X)\right)^c$

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

$$f \mapsto \{\, b \subseteq A \mid \exists x \in X.\, b = \overleftarrow{f}\left(\{x\}\right) \,\}$$

yields a function $\mathrm{Sur}(A, X) \to \mathrm{Part}(A)$. Is it surjective? And injective?

Workout 39
from page 440

1. Prove Corollary 147 on page 437.
2. Make sure that you understand the calculus of bijections on page 438.

Workout 40
from page 449

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) $\{\, f \in (\mathbb{N} \Rightarrow [2]) \mid \forall n \in \mathbb{N}.\, f(n) \geq f(n+1) \,\}$