Algorithmic Foundations 2 - Tutorial Sheet 1

Propositional Logic and Logical Equivalences

---

1. Which of the following are propositions and what are the truth values of those that are propositions?
   (a) Do not pass go

   > **Solution:** Not a proposition - this is a command

   (b) What time is it?

   > **Solution:** Not a proposition - this is a question

   (c) Glasgow is the largest city in Scotland

   > **Solution:** A proposition which is `true`

   (d) $4+x = 5$

   > **Solution:** Not a proposition - the truth value depends on the value of x (for example, if $x = 1$, then the statement is `true` and is `false` for any other value of x)

   (e) $4+1 = 6$

   > **Solution:** A proposition which is `false`

2. Let p, q and r be the propositions:
   - p: you have the flu;
   - q: you miss the final exam;
   - r: you pass the course.

3. Express each of the following propositions as an English sentence
   (a) $p \rightarrow q$

   > **Solution:** If you have the flu, then you miss the final exam.

   (b) $\neg q \leftrightarrow r$

   > **Solution:** You do not miss the final exam if and only if you pass the course.

   (c) $q \rightarrow \neg r$

   > **Solution:** If you miss the final exam, then you do not pass the course.

   (d) $p \vee q \vee r$

Solution: Either you have the flu, or you miss the final exam, or you pass the course.

(e) $(p \to \neg r) \vee (q \to \neg r)$

Solution: Either it holds that if you have the flu, then you do not pass the course, or it holds that if you miss the final exam, then you do not pass the course (or both).

(f) $(p \wedge q) \vee (\neg q \wedge r)$

Solution: Either you have the flu and miss the final exam, or you do not miss the final exam and pass the course.

4. Let p, q and r be the propositions:

   - p: you get an A in the final exam;
   - q: you do every tutorial exercise;
   - r: you get an A for this module.

   Write the following propositions using p, q, r and logical connectives.

   (a) You get an A for this module, but you do not do every tutorial exercise.

   Solution: $r \wedge \neg q$

   (b) You get an A in the final exam, you do every tutorial exercise and you get an A for this module.

   Solution: $p \wedge q \wedge r$

   (c) To get an A for this module, it is necessary for you to get an A in the final exam.

   Solution: $r \to p$

   (d) You get an A in the final exam, but you do not do every tutorial exercise; nevertheless, you get an A for this module.

   Solution: $p \wedge \neg q \wedge r$

   (e) Getting an A in the final exam and doing every tutorial exercise is sufficient for getting an A for this module.

   Solution: $(p \wedge q) \to r$

   (f) You get an A for this module if and only if you either do every tutorial exercise or you get an A in the final exam.

   Solution: $r \leftrightarrow (q \vee p)$

5. Construct a truth table for each of the following compound propositions.

(a) $\neg p \oplus \neg q$

Solution:

p	q	$\neg p$	$\neg q$	$\neg p \oplus \neg q$
0	0	1	1	0
0	1	1	0	1
1	0	0	1	1
1	1	0	0	0

(b) $(p \vee q) \wedge \neg r$

Solution:

p	q	r	$p \vee q$	$\neg r$	$(p \vee q) \wedge \neg r$
0	0	0	0	1	0
0	0	1	0	0	0
0	1	0	1	1	1
0	1	1	1	0	0
1	0	0	1	1	1
1	0	1	1	0	0
1	1	0	1	1	1
1	1	1	1	0	0

(c) $(p \to q) \to r$

Solution:

p	q	$p \to q$	r	$(p \to q) \to \neg r$
0	0	1	0	0
0	0	1	1	1
0	1	1	0	0
0	1	1	1	1
1	0	0	0	1
1	0	0	1	1
1	1	1	0	0
1	1	1	1	1

(d) $(p \wedge \neg q) \leftrightarrow (p \wedge r)$

Solution:

p	q	$\neg q$	$p \wedge \neg q$	r	$p \wedge r$	$(p \wedge \neg q) \leftrightarrow (p \wedge r)$
0	0	1	0	0	0	1
0	0	1	0	1	0	1
0	1	0	0	0	0	1
0	1	0	0	1	0	1
1	0	1	1	0	0	0
1	0	1	1	1	1	1
1	1	0	0	0	0	1
1	1	0	0	1	1	0

6. Show that each of the following implications is a tautology by using truth tables.

(a) $(p \wedge q) \to q$

Solution:

p	q	$p \wedge q$	$(p \wedge q) \rightarrow q$
0	0	0	1
0	1	0	1
1	0	0	1
1	1	1	1

(b) $(\neg p \wedge (p \vee q)) \rightarrow q$

Solution:

p	q	$\neg p$	$p \vee q$	$\neg p \wedge (p \vee q)$	$(\neg p \wedge (p \vee q)) \rightarrow q$
0	0	1	0	0	1
0	1	1	1	1	1
1	0	0	1	0	1
1	1	0	1	0	1

(c) $(p \wedge (p \rightarrow q)) \rightarrow q$

Solution:

p	q	$p \rightarrow q$	$p \wedge (p \rightarrow q)$	$(p \wedge (p \rightarrow q)) \rightarrow q$
0	0	1	0	1
0	1	1	0	1
1	0	0	0	1
1	1	1	1	1

7. Show that each implication in Exercise 6 is a tautology without using truth tables.

(a) $(p \wedge q) \rightarrow q$

Solution:

$$
\begin{aligned}
(p \wedge q) \rightarrow q &\equiv \neg(p \wedge q) \vee q && \text{implication law} \\
&\equiv (\neg p \vee \neg q) \vee q && \text{de Morgan law} \\
&\equiv \neg p \vee (\neg q \vee q) && \text{associative law} \\
&\equiv \neg p \vee (q \vee \neg q) && \text{commutative law} \\
&\equiv \neg p \vee \texttt{true} && \text{tautology law} \\
&\equiv \texttt{true} && \text{domination law}
\end{aligned}
$$

Alternative solution: If the hypothesis $p \wedge q$ is `false`, then the overall proposition is `true`. Therefore it remains to consider the case when the hypothesis is `true`. In this case, both p and q must be `true`, and hence the conclusion of the proposition is also `true`, again making the overall proposition `true`.

(b) $(\neg p \wedge (p \vee q)) \rightarrow q$

Solution:

$$
\begin{aligned}
(\neg p \wedge (p \vee q)) \rightarrow q &\equiv \neg(\neg p \wedge (p \vee q)) \vee q && \text{implication law}\\
&\equiv (\neg\neg p \vee \neg(p \vee q)) \vee q && \text{de Morgan law}\\
&\equiv (p \vee \neg(p \vee q)) \vee q && \text{double negation law}\\
&\equiv (p \vee (\neg p \wedge \neg q)) \vee q && \text{de Morgan law}\\
&\equiv ((p \vee \neg p) \wedge (p \vee \neg q)) \vee q && \text{distributive law}\\
&\equiv (\texttt{true} \wedge (p \vee \neg q)) \vee q && \text{tautology law}\\
&\equiv (p \vee \neg q) \vee q && \text{identity law}\\
&\equiv p \vee (\neg q \vee q) && \text{associative law}\\
&\equiv p \vee (q \vee \neg q) && \text{commutative law}\\
&\equiv p \vee \texttt{true} && \text{tautology law}\\
&\equiv \texttt{true} && \text{domination law}
\end{aligned}
$$

Alternative solution: If the hypothesis $\neg p \wedge (p \vee q)$ is `false`, then the overall proposition is `true`. Therefore, it remains to consider the case when the hypothesis is `true`. In this case, $\neg p$ must be `true`, so p is `false`. Since p is `false` and $(p \vee q)$ must be `true` for the hypothesis to hold, we have that q must be `true`. Hence the conclusion of the proposition is `true`, making the overall proposition `true`.

(c) $(p \wedge (p \rightarrow q)) \rightarrow q$

Solution:

$$
\begin{aligned}
(p \wedge (p \rightarrow q)) \rightarrow q &\equiv (p \wedge (\neg p \vee q)) \rightarrow q && \text{implication law}\\
&\equiv ((p \wedge \neg p) \vee (p \wedge q)) \rightarrow q && \text{distributive law}\\
&\equiv (\texttt{false} \vee (p \wedge q)) \rightarrow q && \text{contradiction law}\\
&\equiv (p \wedge q) \rightarrow q && \text{identity law}\\
&\equiv \neg(p \wedge q) \vee q && \text{implication law}\\
&\equiv (\neg p \vee \neg q) \vee q && \text{de Morgan law}\\
&\equiv \neg p \vee (\neg q \vee q) && \text{associative law}\\
&\equiv \neg p \vee (q \vee \neg q) && \text{commutative law}\\
&\equiv \neg p \vee \texttt{true} && \text{tautology law}\\
&\equiv \texttt{true} && \text{domination law}
\end{aligned}
$$

Alternative solution: If the hypothesis $p \wedge (p \rightarrow q)$ is `false`, then the overall proposition is `true`. Therefore it remains to consider the case when the hypothesis is `true`. In this case, we have both p and $p \rightarrow q$ are `true` which forces q to also be `true`. Hence the conclusion of the proposition is `true`, making the overall proposition `true`.

8. State the converse and contrapositive of each of the following implications:

   (a) If it snows tonight, then I will stay at home.

   Solution: *Converse* $(q \rightarrow p)$: If I stay at home, then it will snow tonight.
   Contrapositive $(\neg q \rightarrow \neg p)$: If I do not stay at home, then it will not snow tonight.

   (b) I go to the beach whenever it is a sunny summer day.

Solution: *Converse* ($q \to p$): If I go to the beach, then it is a sunny summer day.
Contrapositive ($\neg q \to \neg p$): If I do not go to the beach, then it is not a sunny summer day.

(c) When I stay up late, it is necessary that I sleep until noon.

Solution: *Converse* ($q \to p$): If I sleep until noon, then I stay up late.
Contrapositive ($\neg q \to \neg p$): If I do not sleep until noon, then I do not stay up late.

Difficult/challenging questions.

9. Suppose that a truth table in n Boolean variables is specified. Show that a compound proposition with this truth table can be formed by taking the disjunction of conjunctions of the variables or their negations. (Hint: there should be one conjunction included for each combination of values for which the proposition is true.) Note that the resulting compound proposition is said to be in disjunctive normal form.

Solution: Each line of the truth table corresponds to exactly one combination of truth values for the n Boolean variables involved. We can write down a conjunction that is `true` precisely in this case, namely the conjunction of all the Boolean variables that are `true` together with the negation of all the Boolean variables that are `false`. If we do this for each line of the truth table for which the value of the compound proposition is `true` and take the disjunction of the resulting propositions, then we have the desired proposition in its disjunctive normal form. For example, consider the following truth table involving three Boolean variables, p, q and r:

p	q	r	truth value	corresponding conjunction
0	0	0	0	-
0	0	1	1	$\neg p \wedge \neg q \wedge r$
0	1	0	0	-
0	1	1	0	-
1	0	0	1	$p \wedge \neg q \wedge \neg r$
1	0	1	0	-
1	1	0	0	-
1	1	1	1	$p \wedge q \wedge r$

The desired proposition in *Disjunctive Normal Form* is therefore:

$$(\neg p \wedge \neg q \wedge r) \vee (p \wedge \neg q \wedge \neg r) \vee (p \wedge q \wedge r).$$

Recall from the lecture that, due to the associativity laws, there is no ambiguity in writing a sequence of conjunctions (or disjunctions) as $p_1 \wedge p_2 \wedge \cdots \wedge p_n$ without parentheses.

10. The proposition $p\,NOR\,q$ is true when both p and q are false and is denoted by the formula $p \downarrow q$. Write the truth table for the logical operator $\downarrow$ and then find a logical proposition equivalent to $p \to q$ using only the operator $\downarrow$.

If you want a further exercise express all logical connectives using just $\downarrow$ without using the logical equivalences you have been given.

Hint. First consider constructing the formula $\neg(p \to q)$, second consider how to define negation using only $\downarrow$ and finally combine these results.

Solution:

p	q	$p \downarrow q$
0	0	1
0	1	0
1	0	0
1	1	0

and a formula equivalent to $p \to q$ is $((p \downarrow p) \downarrow q) \downarrow ((p \downarrow p) \downarrow q)$.

The remaining operators can be expressed as follows:

$$\begin{aligned}
\neg p &\equiv p \downarrow p \\
p \wedge q &\equiv (p \downarrow p) \downarrow (q \downarrow q) \\
p \vee q &\equiv (p \downarrow q) \downarrow (p \downarrow q) \\
p \oplus q &\equiv (p \downarrow q) \downarrow ((p \downarrow p) \downarrow (q \downarrow q)) \\
p \leftrightarrow q &\equiv (p \downarrow p) \downarrow q) \downarrow ((q \downarrow q) \downarrow p)
\end{aligned}$$

Algorithmic Foundations 2 - Tutorial Sheet 2

Predicate Logic and Sets

Predicates and Quantifiers

1. Suppose $P(x, y)$ is the statement $x + 2{\cdot}y = x{\cdot}y$, where the universe of discourse for both x and y is the set of integers $\mathbb{Z}$. What are the truth values of
   (a) $P(1, -1)$

   Solution: `true` - since $1 + 2{\cdot}(-1) = -1 = 1{\cdot}(-1)$.

   (b) $P(0, 0)$

   Solution: `true` - since $0 + 2{\cdot}0 = 0 = 0{\cdot}0$.

   (c) $P(2, 1)$

   Solution: `false` - since $2 + 2{\cdot}(1) = 4 \neq 2 = 1{\cdot}2$.

2. Suppose that $Q(x)$ is the statement $x{+}1 = 2{\cdot}x$. What are the truth values of
   (a) $Q(2)$

   Solution: `false` - since $2{+}1 = 3 \neq 4 = 2{\cdot}2$.

   (b) $\forall x \in \mathbb{R}.\, Q(x)$

   Solution: `false` - since, for example if $x{=}2$, then $2{+}1 = 3 \neq 4 = 2{\cdot}2$.

   (c) $\exists x \in \mathbb{R}.\, Q(x)$

   Solution: `true` - since, for example taking $x{=}1$ we have $1{+}1 = 2 = 2{\cdot}1$.

3. Let $P(m, n)$ be the statement $n \geq m$. What is the truth value of
   (a) $\forall n \in \mathbb{N}.\, P(0, n)$

   Solution: `true` - all natural numbers are greater than or equal to 0.

   (b) $\exists n \in \mathbb{N}.\, \forall m \in \mathbb{N}.\, P(m, n)$

   Solution: `false` - there is no largest natural number. For example, for any natural number n, letting $m = n{+}1$ we have $m \in \mathbb{N}$ and $P(m, n)$ does not hold.

   (c) $\forall m \in \mathbb{N}.\, \exists n \in \mathbb{N}.\, P(m, n)$

   Solution: `true` - for any $m \in \mathbb{N}$ letting $n = m{+}1$ we have $n \in \mathbb{N}$ and $P(m, n)$ holds.

4. Suppose $\mathcal{S}$ is the set of all students, $\mathcal{C}$ is the set of all courses, and we are given the following list of predicates:

   - $H(y)$: x is an honours course;
   - $C(x)$: x is a CS course;
   - $S(x)$: x is a second-year;
   - $P(x)$: x is a part-time student;
   - $F(x)$: x is a full-time student;
   - $T(x, y)$: x is taking course y.

5. Write each of the following statements using these predicates and quantifiers where necessary.

   (a) "Sarah is taking AF2"

   Solution: $T(Sarah, AF2)$

   (b) "all students are second-years"

   Solution: $\forall x \in \mathcal{S}.\, S(x)$

   (c) "every second-year is a full-time student"

   Solution: $\forall x \in \mathcal{S}.\, (S(x) \rightarrow F(x))$

   (d) "no CS course is an honours course"

   Solution: $\forall y \in \mathcal{C}.\, (C(y) \rightarrow \neg H(y))$.

   Alternative (and equivalent) solutions include $\forall y \in \mathcal{C}.\, \neg(C(y) \wedge H(y))$ and $\neg\exists y \in \mathcal{C}.\, (C(y) \wedge H(y))$.

   (e) "every student is taking at least one course"

   Solution: $\forall x \in \mathcal{S}.\, \exists y \in \mathcal{C}.\, T(x, y)$

   (f) "there is a part-time student who is not taking any CS course"

   Solution: $\exists x \in \mathcal{S}.\, \forall y \in \mathcal{C}.\, (P(x) \wedge (C(y) \rightarrow \neg T(x, y)))$ or alternatively
   $\exists x \in \mathcal{S}.\, (P(x) \wedge \forall y \in \mathcal{C}.\, (C(y) \rightarrow \neg T(x, y)))$

   (g) "every part-time second-year is taking some honours course"

   Solution: $\forall x \in \mathcal{S}.\, \exists y \in \mathcal{C}.\, ((P(x) \wedge S(x)) \rightarrow (H(y) \wedge T(x, y)))$ or alternatively
   $\forall x \in \mathcal{S}.\, ((P(x) \wedge S(x)) \rightarrow \exists y \in \mathcal{C}.\, (H(y) \wedge T(x, y)))$

6. Using the predicates from the previous question, write each of the following in good English without using variables in your answers.

   (a) $S(Helen)$

Solution: "Helen is a second-year student"

(b) $\neg\exists y \in \mathcal{C}.\, T(Joe, y)$

Solution: "Joe is not taking any course"

(c) $\exists x \in \mathcal{S}.\, (P(x) \wedge \neg S(x))$

Solution: "some part-time students are not second-years"

(d) $\exists x \in \mathcal{S}.\, \forall y \in \mathcal{C}.\, T(x, y)$

Solution: "some student is taking every course"

(e) $\forall x \in \mathcal{S}.\, \exists y \in \mathcal{C}.\, ((F(x) \wedge S(x)) \rightarrow (C(y) \wedge T(x, y)))$

Solution: "every full-time second year is taking a CS course"

7. Explain why the negation of "Some students in my class use e-mail" is not "Some students in my class do not use e-mail".

Solution: Short answer: both statements can be true at the same time. Longer answer: the negation is "all students in my class do not use e-mail" which is not the same as saying "some students in my class do not use e-mail".

8. Let $\mathcal{S}$ be the set of all sets and consider the following predicates:

   - $F(x)$: x is a finite set;
   - $I(x)$: x is an infinite set;
   - $S(x, y)$: x is contained in y;
   - $E(x)$: x is the emptyset.

   Translate the following into logical expressions:

   (a) "not all sets are finite"

   Solution: $\exists x \in \mathcal{S}.\, \neg F(x)$ or $\exists x \in \mathcal{S}.\, I(x)$

   (b) "every subset of a finite set is finite"

   Solution: $\forall x \in \mathcal{S}.\, \forall y \in \mathcal{S}.\, ((F(y) \wedge S(x, y)) \rightarrow F(x))$

   (c) "no infinite set can be contained in a finite set"

   Solution: $\neg\exists x \in \mathcal{S}.\, \exists y \in \mathcal{S}.\, (I(x) \wedge F(y) \wedge S(x, y))$
   An alternatively would be $\forall x \in \mathcal{S}.\, (I(x) \rightarrow \neg(\exists y \in \mathcal{S}.\, (F(y) \wedge S(x, y))))$

Below is a proof showing these two formulae are logically equivalent:

$$
\begin{aligned}
&\forall x \in \mathcal{S}.\,(I(x) \to \neg(\exists y \in \mathcal{S}.\,(F(y) \wedge S(x,y)))) \\
&\equiv\ \forall x \in \mathcal{S}.\,(\neg I(x) \vee \neg(\exists y \in \mathcal{S}.\,(F(y) \wedge S(x,y)))) && \text{implication law} \\
&\equiv\ \forall x \in \mathcal{S}.\,\neg(I(x) \wedge (\exists y \in \mathcal{S}.\,(F(y) \wedge S(x,y)))) && \text{De Morgan law} \\
&\equiv\ \neg\exists x \in \mathcal{S}.\,\neg\neg(I(x) \wedge (\exists y \in \mathcal{S}.\,(F(y) \wedge S(x,y)))) && \text{negation law} \\
&\equiv\ \neg\exists x \in \mathcal{S}.\,(I(x) \wedge (\exists y \in \mathcal{S}.\,(F(y) \wedge S(x,y)))) && \text{double negation law} \\
&\equiv\ \neg\exists x \in \mathcal{S}.\,\exists y \in \mathcal{S}.\,(I(x) \wedge F(y) \wedge S(x,y)) && \text{since } y \text{ does not appear in } I(x)
\end{aligned}
$$

(d) "the empty set is a subset of every finite set"

Solution: $\forall x \in \mathcal{S}.\,\forall y \in \mathcal{S}.\,((E(x) \wedge F(y)) \to S(x,y))$

Difficult/challenging questions (Predicate Logic).

9. A statement is in *prenex normal form* when it is of the form:

$$\nabla_1 x_1.\,\nabla_2 x_2 \ldots \nabla_n x_n.\,P(x_1, x_2, \ldots, x_n)$$

where $\nabla_i \in \{\forall, \exists\}$ for $1 \leq i \leq n$ and $P(x_1, x_2, \ldots, x_n)$ is a predicate involving no quantifiers. For example we have that $\exists x.\,\forall y.\,(P(x,y) \vee Q(y))$ is in prenex normal form, while $\forall x.\,P(x) \wedge \exists y.\,Q(y)$ is not. Using the rules for logical equivalence write the following formulae in prenex normal form.

(a) $\exists x.\,P(x) \vee \exists x.\,Q(x) \vee R$ where R is a propositional formula, containing no variables or quantifiers;

Solution: Changing the variable x to y in the subforumula $\exists x.\,Q(x)$ we have:

$$
\begin{aligned}
\exists x.\,P(x) \vee \exists x.\,Q(x) \vee R &\equiv\ \exists x.\,P(x) \vee \exists y.\,Q(y) \vee R \\
&\equiv \exists x.\,\exists y.\,(P(x) \vee Q(y) \vee R)
\end{aligned}
$$

since y does not appear free in $\exists x.\,P(x)$, x does not appear free in $\exists y.\,Q(y)$ and neither x nor y appear free in R.

(b) $\neg(\forall x.\,P(x) \vee \forall x.\,Q(x))$

Solution: Changing the variable x to y in the subforumula $\forall x.\,Q(x)$ we have:

$$
\begin{aligned}
\neg(\forall x.\,P(x) \vee \forall x.\,Q(x)) &\equiv\ \neg(\forall x.\,P(x) \vee \forall y.\,Q(y)) \\
&\equiv\ \neg\forall x.\,P(x) \wedge \neg\forall y.\,Q(y) && \text{De Morgan law} \\
&\equiv\ \neg\forall x.\,\neg\neg P(x) \wedge \neg\forall y.\,\neg\neg Q(y) && \text{double negation law (twice)} \\
&\equiv\ \exists x.\,\neg P(x) \wedge \exists y.\,\neg Q(y) && \text{quantifier law} \\
&\equiv\ \exists x.\,\exists y.\,(\neg P(x) \wedge \neg Q(y))
\end{aligned}
$$

since y does not appear free in $\forall x.\,\neg P(x)$ and x does not appear free in $\exists y.\,\neg Q(y)$.

(c) $\exists x.\, P(x) \to \exists x.\, Q(x)$

Solution: Changing the variable x to y in the second sub-forumula we have:

$$\begin{aligned}
&\exists x.\, P(x) \to \exists x.\, Q(x) \;\equiv\; \exists x.\, P(x) \to \exists y.\, Q(y) \\
&\equiv\; \neg\exists x.\, P(x) \vee \exists y.\, Q(y) && \text{implication law} \\
&\equiv\; \neg\exists x.\, \neg\neg P(x) \vee \exists y.\, Q(y) && \text{double negation law} \\
&\equiv\; \forall x.\, \neg P(x) \vee \exists y.\, Q(y) && \text{quantifier law} \\
&\equiv\; \forall x.\, \exists y.\, (\neg P(x) \vee Q(y))
\end{aligned}$$

since y does not appear free in $\forall x.\, \neg P(x)$ and x does not appear free in $\exists y.\, Q(y)$.

Sets and Set Operations

10. List the members of the following sets (recall that $\mathbb{Z}$ is the set of integers and $\mathbb{N}$ is the set of natural numbers).

(a) $\{x \mid x \in \mathbb{Z} \wedge x^2{=}5\}$

Solution: $\varnothing$

(b) $\{5{\cdot}x \mid x \in \mathbb{Z} \wedge (-2{\leq}x{\leq}2)\}$

Solution: $\{-10, -5, 0, 5, 10\}$

(c) $\{x \mid x \in \mathbb{N} \wedge x^2 \in \{1, 4, 9\}\}$

Solution: $\{1, 2, 3\}$

(d) $\{x \mid x \in \mathbb{Z} \wedge x^2 \in \{1, 4, 9\}\}$

Solution: $\{-3, -2, -1, 1, 2, 3\}$

11. Use set builder notation to give a description of each of the following sets.

(a) $\{0, 3, 6, 9, 12\}$

Solution: $\{3{\cdot}x \mid x \in \mathbb{N} \wedge 0{\leq}x{\leq}4\}$

(b) $\{-3, -2, -1, 0, 1, 2, 3\}$

Solution: $\{x \mid x \in \mathbb{Z} \wedge -3{\leq}x{\leq}3\}$

(c) $\{1, 4, 9, 16, 25, 36, 49\}$

Solution: $\{x^2 \mid x \in \mathbb{N} \wedge 1 \leq x \leq 7\}$

12. Suppose $A = \{a, b, c\}$ and $B = \{b, \{c\}\}$. Mark each of the following `true` or `false`.

(a) $\{a, c\} \in A$

Solution: `false` ($\{a, c\}$ is actually a strict subset of A, i.e. $\{a, b\} \subset A$)

(b) $\{c\} \subseteq B$

Solution: `false` (actually we have $\{c\} \in B$)

(c) $B \subseteq A$

Solution: `false` (for example, $\{c\} \in B$ and $\{c\} \notin A$)

(d) $\{b, c\} \in \mathcal{P}(A)$

Solution: `true` (b and c are elements of A, and hence $\{b, c\}$ is a subset of A)

(e) $\{\{a\}\} \subseteq \mathcal{P}(A)$

Solution: `true` ($\{a\}$ is an element of $\mathcal{P}(A)$ so the set containing $\{a\}$ is a subset of $\mathcal{P}(A)$)

(f) $\{b, \{c\}\} \in \mathcal{P}(B)$

Solution: `true` (since a set is element of its powerset)

(g) $\{\{\{c\}\}\} \subseteq \mathcal{P}(B)$

Solution: `true` ($\{c\} \in B$ implies $\{\{c\}\} \in \mathcal{P}(B)$ which implies $\{\{\{c\}\}\} \subseteq \mathcal{P}(B)$)

(h) $|\mathcal{P}(A \times B)| = 32$

Solution: `false` ($|A \times B| = 3 \cdot 2 = 6$ so the power set is of size $2^6 = 64$)

(i) $\{a, b\} \in A \times A$

Solution: `false` (the set $A \times A$ contains ordered pair, but $\{a, b\}$ is the set containing the elements a and b)

(j) $\varnothing \subseteq A \times A$

Solution: `true` (the emptyset is a subset of any set - to prove a set A is a subset of B we need to show any element of A is in B, when A is the empty set this holds vacuously as there are no elements in A)

(k) $(c, c) \in A \times A$

Solution: `true` - since $c \in A$

13. Prove that $A \cap (B \cup C) = (A \cap B) \cup (A \cap C)$ by giving

(a) a containment proof;

Solution: First we show $A \cap (B \cup C) \subseteq (A \cap B) \cup (A \cap C)$. Considering any $x \in A \cap (B \cup C)$, by definition of intersection we have:

$x \in A \cap (B \cup C) \Rightarrow x \in A$ and $x \in B \cup C$
$\Rightarrow x \in A$ and either $x \in B$ or $x \in C$ by definition of union
$\Rightarrow$ either $x \in A$ and $x \in B$, or $x \in A$ and $x \in C$ rearranging
$\Rightarrow$ either $x \in A \cap B$ or $x \in A \cap C$ by definition of intersection
$\Rightarrow x \in (A \cap B) \cup (A \cap C)$ by definition of union

and hence, since $x \in A \cap (B \cup C)$ was arbitrary, we have $A \cap (B \cup C) \subseteq (A \cap B) \cup (A \cap C)$ as required.

To complete the proof we show $(A \cap B) \cup (A \cap C) \subseteq A \cap (B \cup C)$. Considering any $x \in (A \cap B) \cup (A \cap C)$, by definition of union we have:

$x \in (A \cap B) \cup (A \cap C) \Rightarrow$ either $x \in A \cap B$ or $x \in A \cap C$
$\Rightarrow$ either $x \in A$ and $x \in B$, or $x \in A$ and $x \in C$ by definition of intersection
$\Rightarrow x \in A$ and either $x \in B$ or $x \in C$ rearranging
$\Rightarrow x \in A$ and $x \in B \cup C$ by definition of union
$\Rightarrow x \in A \cap (B \cup C)$ by definition of intersection

and hence, since $x \in (A \cap B) \cup (A \cap C)$ was arbitrary, we have $(A \cap B) \cup (A \cap C) \subseteq A \cap (B \cup C)$ completing the proof.

(b) an element table proof;

Solution:

A	B	C	$A \cap B$	$A \cap C$	$B \cup C$	$A \cap (B \cup C)$	$(A \cap B) \cup (A \cap C)$
0	0	0	0	0	0	**0**	**0**
0	0	1	0	0	1	**0**	**0**
0	1	0	0	0	1	**0**	**0**
0	1	1	0	0	1	**0**	**0**
1	0	0	0	0	0	**0**	**0**
1	0	1	0	1	1	**1**	**1**
1	1	0	1	0	1	**1**	**1**
1	1	1	1	1	1	**1**	**1**

Each set has the same values in the element table: the value is 1 if and only if A has the value 1 and either B or C has the value 1.

(c) a proof using logical equivalence.

Solution:

$$\begin{aligned}
A \cap (B \cup C) &= \{x \mid x \in A \cap (B \cup C)\} && \text{by definition} \\
&= \{x \mid (x \in A) \wedge (x \in (B \cup C))\} && \text{by definition of } \cap \\
&= \{x \mid (x \in A) \wedge ((x \in B) \vee (x \in C))\} && \text{by definition of } \cup \\
&= \{x \mid ((x \in A) \wedge (x \in B)) \vee ((x \in A) \wedge (x \in C))\} && \text{distributive law} \\
&= \{x \mid (x \in A \cap B) \vee (x \in A \cap C)\} && \text{by definition of } \cap \\
&= \{x \mid x \in (A \cap B) \cup (A \cap C)\} && \text{by definition of } \cup \\
&= (A \cap B) \cup (A \cap C).
\end{aligned}$$

14. Prove or disprove: $A-(B \cap C) = (A-B) \cup (A-C)$.

Solution: Proof. By definition of set difference:

$$\begin{aligned}
A-(B \cap C) &= A \cap (\overline{B \cap C}) \\
&= A \cap (\overline{B} \cup \overline{C}) && \text{de Morgan} \\
&= (A \cap \overline{B}) \cup (A \cap \overline{C}) && \text{distributivity} \\
&= (A-B) \cup (A-C) && \text{definition of set difference}
\end{aligned}$$

15. Prove or disprove: $A-(B \cap C) = (A-B) \cap (A-C)$.

Solution: `false` - for example, if $A = \{1, 2\}$, $B = \{1\}$, $C = \{2\}$, then $A-(B \cap C) = A$ while $(A-B) \cap (A-C) = \varnothing$

16. Prove or disprove: $A \oplus (B \oplus C) = (A \oplus B) \oplus C$.

Solution: `true` - this is easiest with a membership table showing each set has the same values: the value is 1 if and only if exactly one of A, B and C has the value 1, or all three have value 1.

Proving with the other methods is possible, but is more involved.

17. Let $A_i = \{1, 2, \ldots, i\}$ for $i \in \mathbb{Z}^+$, find $\cup_{i=1}^{n} A_i$ and $\cap_{i=1}^{n} A_i$ for $n \in \mathbb{Z}^+$.

Solution: We have $\cup_{i=1}^{n} A_i = A_n$ and $\cap_{i=1}^{n} A_i = \{1\}$

18. Mark each of the following `true` or `false`:
    (a) $A-(B-C) = (A-B)-C$

Solution: `false` - for example, consider $A = B = \{a, b\}$ and $C = \{b\}$, then $A-(B-C) = \{a, b\} - \{a\} = \{b\}$ while $(A-B)-C = \varnothing-\{b\} = \varnothing$

(b) $(A-C)-(B-C) = A-B$

Solution: `false` - for example, take $A = \{a\}$, $B = \{b\}$ and $C = \{a, b\}$, then $(A-C)-(B-C) = \varnothing - \varnothing = \varnothing$ while $A-B = \{a\}$

(c) $A \cup (B \cap C) = (A \cup B) \cap (A \cup C)$

Solution: `true` - below is a containment proof:
First we show $A \cup (B \cap C) \subseteq (A \cup B) \cap (A \cup C)$. Therefore, considering any $x \in A \cup (B \cap C)$, by definition of union:

$$
\begin{aligned}
& x \in A \cup (B \cap C) \Rightarrow x \in A \text{ or } x \in B \cap C \\
& \Rightarrow x \in A \text{ or both } x \in B \text{ and } x \in C && \text{by definition of intersection} \\
& \Rightarrow x \in A \text{ or } x \in B, \text{ and } x \in A \text{ or } x \in C && \text{rearranging} \\
& \Rightarrow x \in A \cup B, \text{ and } x \in A \cup C && \text{by definition of union} \\
& \Rightarrow x \in (A \cup B) \cap (A \cup C) && \text{by definition of intersection}
\end{aligned}
$$

and, since $x \in A \cup (B \cap C)$ was arbitrary, we have $A \cup (B \cap C) \subseteq (A \cup B) \cap (A \cup C)$ are required.
To complete the proof we show $(A \cup B) \cap (A \cup C) \subseteq A \cup (B \cap C)$. Considering any $x \in (A \cup B) \cap (A \cup C)$, definition of intersection we have:

$$
\begin{aligned}
& x \in (A \cup B) \cap (A \cup C) \Rightarrow x \in A \cup B, \text{ and } x \in A \cup C \\
& \Rightarrow x \in A \text{ or } x \in B, \text{ and } x \in A \text{ or } x \in C && \text{by definition of union} \\
& \Rightarrow x \in A \text{ or both } x \in B \text{ and } x \in C && \text{rearranging} \\
& \Rightarrow x \in A \text{ or } x \in B \cap C && \text{by definition of intersection} \\
& \Rightarrow x \in A \cup (B \cap C) && \text{by definition of union.}
\end{aligned}
$$

Hence, since $x \in (A \cup B) \cap (A \cup C)$ was arbitrary, we have $(A \cup B) \cap (A \cup C) \subseteq A \cup (B \cap C)$ completing the proof.

(d) $A \cap (B \cup C) = (A \cup B) \cap (A \cup C)$

Solution: `false` - for example, if $A = \{a\}$ and $B = C = \{b\}$, then $A \cap (B \cup C) = \{a\} \cap \{b\} = \varnothing$ while $(A \cup B) \cap (A \cup C) = \{a, b\} \cap \{a, b\} = \{a, b\}$

(e) If $A \cup C = B \cup C$, then $A = B$

Solution: `false` - for example, consider $A = \{a\}$, $B = \{b\}$ and $C = \{a, b\}$

(f) If $A \cap C = B \cap C$, then $A = B$

Solution: `false` - for example, consider $A = \{a, c\}$, $B = \{b, c\}$ and $C = \{c\}$

(g) If $A \cap B = A \cup B$, then $A = B$

Solution: `true`. Below we give a containment proof showing $A = B$ using the

hypothesis $A \cap B = A \cup B$. First we show $A \subseteq B$, by definition of union we have:

$$\begin{aligned} x \in A \Rightarrow\ & x \in A \cup B \\ \Rightarrow\ & x \in A \cap B && \text{by the hypothesis} \\ \Rightarrow\ & x \in B && \text{by the definition of intersection} \end{aligned}$$

and hence $A \subseteq B$.

To complete the proof we show $B \subseteq A$. Considering any $x \in B$, by definition of union we have:

$$\begin{aligned} x \in B \Rightarrow\ & x \in A \cup B \\ \Rightarrow\ & x \in A \cap B && \text{by the hypothesis} \\ \Rightarrow\ & x \in A && \text{by the definition of intersection} \end{aligned}$$

and hence $B \subseteq A$ completing the proof.

(h) If $A \oplus B = A$, then $A = B$

Solution: `false` - for example, if $A = \{a\}$ and $B = \varnothing$, then $A \oplus B = (A - B) \cup (B - A) = \{a\} \cup \varnothing = \{a\}$

(i) there is a set A such that $|P(A)| = 12$

Solution: `false` - from the lectures we have that the size of the power set equals 2^n where n is the size of the set

(j) $A \oplus A = A$

Solution: `false` - for example, if $A = \{a\}$, then $A \oplus A = (A - A) \cup (A - A) = \varnothing \cup \varnothing = \varnothing$.

We actually have that $A \oplus A = \varnothing$ for all sets A. Below is a proof of this fact using using set comprehension and logical equivalences.

$$\begin{aligned} A \oplus A = & \{x \mid x \in A \oplus A\} && \text{by definition} \\ = & \{x \mid x \in (A - A) \cup (A - A)\} && \text{by definition of symmetric difference} \\ = & \{x \mid (x \in A - A) \vee (x \in A - A)\} && \text{by definition of } \cup \\ = & \{x \mid x \in A - A\} && \text{idempotent law} \\ = & \{x \mid (x \in A) \wedge (x \notin A)\} && \text{by definition of set difference} \\ = & \{x \mid (x \in A) \wedge \neg(x \in A)\} && \text{by definition of negation} \\ = & \{x \mid \texttt{false}\} && \text{contradiction law} \\ = & \varnothing \end{aligned}$$

Difficult/challenging questions (Sets and Set Operations).

19. Prove or disprove: $A \oplus (B \oplus C) = (A \oplus B) \oplus C$.

> **Solution:** `true` - this is easiest with a membership table showing each set has the same values: the value is 1 if and only if exactly one of A, B and C has the value 1, or all three have value 1.
>
> Proving with the other methods is possible, but is more involved.

20. Suppose that A, B and C are sets such that $A \oplus C = B \oplus C$, does it follow that $A = B$.

> **Solution:** The answer is yes. We will prove using a containment proof.
>
> First we show $A \subseteq B$. Considering any $x \in A$ we split the proof into the following two cases.
>
> - If $x \in C$, then by definition of set difference $x \notin A \oplus C$, and hence since $A \oplus C = B \oplus C$ it follows that $x \notin B \oplus C$. Now since $x \in C$ and $x \notin B \oplus C$, by definition of set difference it must be the case that $x \in B$.
> - If $x \notin C$, then by definition of set difference $x \in A \oplus C$, and hence since $A \oplus C = B \oplus C$ it follows that $x \in B \oplus C$. Now since $x \notin C$ and $x \in B \oplus C$, by definition of set difference it must be the case that $x \in B$.
>
> Since these are all the cases to consider ot follows that $x \in B$ and $A \subseteq B$.
>
> The proof that $B \subseteq A$ follows similarly, and therefore we have that $A = B$.

Algorithmic Foundations 2 - Tutorial Sheet 3

Functions, Sequences, Summation, Integers and Division

Functions

1. Determine which of the following are functions (with the given domain and codomain).
   (a) $f_1 : \mathbb{N} \to \mathbb{N}$ where $f_1(n) = \sqrt{n}$

   Solution: `false` - the codomain does not match the function, e.g. $f_1(2) = \sqrt{2} \notin \mathbb{N}$

   (b) $f_2 : \mathbb{R} \to \mathbb{R}$ where $f_2(x) = \sqrt{x}$

   Solution: `false` - the domain does not match the function, e.g. $f_2(-2) = \sqrt{-2} \notin \mathbb{R}$

   (c) $f_3 : \mathbb{N} \to \mathbb{N}$ where $f_3(n)$ equals any integer greater than n

   Solution: `false` - there is no unique value for any given element of the domain

   (d) $f_4 : \mathbb{Z} \to \mathbb{R}$ where $f_4(x) = 1/(x-5)$

   Solution: `false` - the codomain does not match the function, e.g. $f_4(5) = 1/0 \notin \mathbb{R}$

   (e) $f_5 : \mathbb{R} \to \mathbb{R}$ where $f_5(x) = 1/(x^2-5)$

   Solution: `false` - the codomain does not match the function, e.g. $f_5(\sqrt{5}) = 1/0 \notin \mathbb{R}$

   (f) $f_6 : \mathbb{Z} \to \mathbb{Z}$ where $f_6(x) = 1/(x^2-5)$

   Solution: `false` - the codomain does not match the function, e.g. $f_6(1) = -1/4 \notin \mathbb{Z}$

   (g) $f_7 : \mathbb{R} \to \mathbb{R}$ where $f_7(x) = \begin{cases} x+2 & \text{if } x \geq 0 \\ x-1 & \text{if } x \leq 4 \end{cases}$

   Solution: `false` - there is no unique value when $0 \leq x \leq 4$

   (h) $f_8 : \mathbb{R} \to \mathbb{R}$ where $f_8(x) = \begin{cases} x^2 & \text{if } x \leq 2 \\ x-1 & \text{if } x \geq 4 \end{cases}$

   Solution: `false` - the domain does not match the function as there is no value when $2 < x < 4$

2. (a) Give an example function $g_1 : \mathbb{Z} \to \mathbb{Z}$ that is injective and not surjective.

   Solution: $g_1(x) = 2 \cdot x$ – not surjective since there is no x such that $g(x) = 1$

   (b) Give an example function $g_2 : \mathbb{Z} \to \mathbb{Z}$ that is surjective but not injective.

Solution: $g_2(x) = \lfloor x/2 \rfloor$ – not injective since for example $g_2(2) = g_2(3) = 1$.

(c) Give an example function $g_3 : \mathbb{Z} \to \mathbb{N}$ that is bijective.

Solution:

$$g_3(x) = \begin{cases} -2{\cdot}x & \text{if } x{\leq}0 \\ 2{\cdot}x - 1 & \text{otherwise} \end{cases}$$

This is similar to the mapping from natural numbers to even numbers from the lecture. Essentially we map negative integers to the even natural numbers and positive integers to the odd natural numbers (and 0 to 0).

(d) Give an example function $g_4 : \mathbb{N} \to \mathbb{Z}$ that is bijective.

Solution:

$$g_4(x) = \begin{cases} -x/2 & \text{if } x \text{ is even} \\ (x{+}1)/2 & \text{otherwise} \end{cases}$$

This is the reverse of the previous solution (and is in fact the inverse of g_3 which exists as g_3 is a bijection)

(e) Give an example function $g_5 : \mathbb{Z} \to \mathbb{N}$ that is injective but not surjective.

Solution:

$$g_5(x) = \begin{cases} -2{\cdot}x & \text{if } x{\leq}0 \\ 2{\cdot}x{+}1 & \text{otherwise} \end{cases}$$

Not surjective since, there does not exist x such that $g_5(x) = 1$.
This is similar to the answer to (c), mapping the negative integers to the even natural numbers and positive integers to odd natural numbers. However, to prevent the function from being surjective, we omit 1 from the range (notice '+1' in the second case whereas in (c) we had '-1').

(f) Give an example function $g_6 : \mathbb{N} \to \mathbb{Z}$ that is surjective and not injective.

Solution:

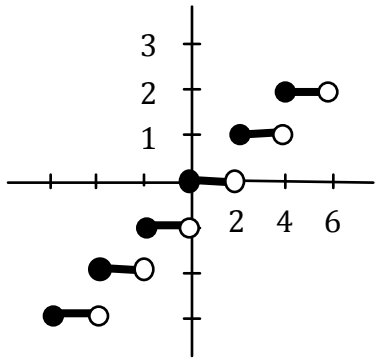
$$g_6(x) = \begin{cases} -x/2 & \text{if } x \text{ is even} \\ (x{-}1)/2 & \text{otherwise} \end{cases}$$

Not injective since, for example, $g_6(1){=}g_6(0)$.
This uses the answer to (d), in this case including 0 in the range when restricting to both the even and odd numbers (notice the use of '-1' in the second case while '+1' was used in (d)).

3. Suppose $f : \mathbb{R} \to \mathbb{R}$ where $f(x) = \lfloor x/2 \rfloor$.

(a) Draw the graph of f.

Solution:



(b) Is f injective?

Solution: No $f(x) = f(y)$ for $x, y \in [n, 2{\cdot}n - 1)$ for any $n \in \mathbb{Z}$

(c) Is f surjective?

Solution: No, for example there does not exist x such that $f(x) = 1/2$.

(d) If $S = \{x \,|\, x \in \mathbb{R} \wedge 1{\leq}x{\leq}6\}$ what is $f(S)$?

Solution: $f(S) = \{0, 1, 2, 3\}$

(e) If $T = \{3, 4, 5\}$, what is $f^{-1}(T)$?

Solution: f^{-1} does not exist as the function is not bijective (it is neither injective nor surjective)

4. Suppose $f : A \to B$ and $g : B \to C$ where $A = \{1, 2, 3, 4\}$, $B = \{a, b, c\}$, $C = \{2, 7, 10\}$ and f and g are defined by:

$$\begin{aligned} f &= \{(1, b), (2, a), (3, a), (4, b)\} \\ g &= \{(a, 10), (b, 7), (c, 2)\}\,. \end{aligned}$$

(a) Find $g \circ f$.

Solution: $\{(1, 7), (2, 10), (3, 10), (4, 7)\}$

(b) Find g^{-1}.

Solution: g is bijective so inverse exists and is given by $\{(2, c), (7, b), (10, a)\}$

5. For the following functions, find the inverse or explain why the function has no inverse.

(a) $h_1 : \mathbb{Z} \to \mathbb{Z}$ where $h_1(x) = x \bmod 10$

Solution: Function is neither injective nor surjective, for example $h_1(10) = h_1(20)$ and there does not exist x such that $h_1(x) = 11$, and hence inverse does not exist.

(b) $h_2 : A \to B$ where $A = \{a, b, c\}$, $B = \{1, 2, 3\}$ and $h_2 = \{(a, 2), (b, 1), (c, 3)\}$

> **Solution:** Function is injective and bijective so inverse exists and is given by $h_2^{-1} = \{(1, b), (2, a), (3, c)\}$

(c) $h_3 : \mathbb{R} \to \mathbb{R}$ where $h_3(x) = 3{\cdot}x{-}5$

> **Solution:** Function is injective and bijective so inverse exists and is given by $h_3^{-1}(x) = (5 + x)/3$

(d) $h_4 : \mathbb{R} \to \mathbb{R}$ where $h_4(x) = \lfloor 2{\cdot}x \rfloor$

> **Solution:** Function is neither injective or surjective, for example, $h_4(1) = h_4(1.1)$ and there does not exist an x such that $h_4(x) = 0.1$, therefore inverse does not exist.

(e) $h_5 : \mathbb{Z} \to \mathbb{Z}$ where $h_5(x) = \begin{cases} x + 2 & \text{if } x \geq 5 \\ x{-}1 & \text{if } x \leq 4. \end{cases}$

> **Solution:** Function is injective but not surjective, for example, there does not exist an x such that $h_5(x) = 4$, and hence inverse does not exist.

Difficult/challenging questions (Functions and Sequences).

6. If f and $f \circ g$ are injective, does it follow that g is injective?

> **Solution:** In this case the answer is yes. Let $g : A \to B$ and $f : B \to C$ and suppose for a contradiction g is not injective. Therefore there exists $a_1 \neq a_2 \in A$ such that $g(a_1) = g(a_2)$. Since $g(a_1) = g(a_2)$ we have $f(g(a_1)) = f(g(a_2))$. It therefore follows by defintion of function composition that $(f \circ g)(a_1) = (f \circ g)(a_2)$, which contradicts the fact that $f \circ g$ is injective. (Other proof methods are also possible.)

7. If g and $f \circ g$ are injective, does it follow that f is injective?

> **Solution:** The answer is no and the reason is that g may map only onto the part of f's domain for which f is injective over this subdomain.
>
> As an example consider $f : \mathbb{Z} \to \mathbb{Z}$ where $f(x) = x^2$ and where $g(x) : \mathbb{Z}^+ \to \mathbb{Z}$ where $g(x) = x$. Clearly we have both g and $f \circ g$ are injective, while f is not. (Many other counter examples are possible.)

8. If f and $f \circ g$ are surjective, does it follow that g is surjective?

Solution: In this case the answer is no as we may only need a subset of g's range (f's domain) to map onto the entire range of f.

For example consider $f : \mathbb{Z} \to \mathbb{Z}$ where $f(x) = |x|$ and $g : \mathbb{Z} \to \mathbb{N}$ where $g(x) = |x|$. Clearly we have both f and $f \circ g$ are surjective, while g is not. (Many other counter examples are possible.)

9. If g and $f \circ g$ are surjective, does it follow that f is surjective?

Solution: Suppose $g : A \to B$ and $f : B \to C$. Now since for any $c \in C$, there exists $a \in A$ such that $(f \circ g)(a) = c$ since $f \circ g$ is surjective. Hence by definition of $f \circ g$ we have that $f(g(a)) = c$, i.e. there exists $b = f(a)$ such that $f(b) = c$. Since c was arbitrary we have f is surjective. (Other proof methods are also possible.)

Sequences, Summation, Integers and Division

10. What are the terms a_0, a_1, a_2 and a_3 of the sequence $\langle a_n \rangle_{n \in \mathbb{N}}$, when a_n equals:
    (a) $(-2)^n$?

    Solution: 1, -2, 4, -8

    (b) 3?

    Solution: 3, 3, 3, 3

    (c) $7 + 4^n$?

    Solution: 8, 11, 23, 71

    (d) $2^n + (-2)^n$?

    Solution: 2, 0, 8, 0

11. For each of the following lists of integers, provide a simple formula that generates the terms of an integer sequence that begins with the given list.
    (a) 7, 11, 15, 19, 23, 27, 31, 35, 39, 43, ...

    Solution: $a_0 = 7$ and $a_n = a_{n-1} + 4$ for $n \geq 1$.

    This is an arithmetic progression in which the nth term is given by $a_n = 7 + 4 \cdot n$ for $n \geq 0$.

    (b) 2, 6, 18, 54, 162, 486, 1458, 4374, 13122, 39366, ...

Solution: $a_0 = 2$ and $a_n = 3{\cdot}a_{n-1}$ for $n \geq 1$.

This is a geometric progression in which the nth term is given by $a_n = 2{\cdot}3^n$ for $n \geq 0$.

(c) 5, 12, 19, 26, 33, 40, 47, 54, 61, 68, ...

Solution: $a_0 = 5$ and $a_n = a_{n-1} + 7$ for $n \geq 1$.

This is an arithmetic progression in which the nth term is given by $a_n = 5 + 7{\cdot}n$ for $n \geq 0$.

(d) 6, 24, 96, 384, 1536, 6144, 24576, 98304, 393216, 1572864, ...

Solution: $a_0 = 6$ and $a_n = 4{\cdot}a_{n-1}$ for $n \geq 1$.

This is a geometric progression in which the nth term is given by $a_n = 6{\cdot}4^n$ for $n \geq 0$.

12. Find the value of each of the following sums. In your calculations, using the theorems:

- $\sum_{i=1}^{n} i = n{\cdot}(n{+}1)/2$
- if $r{=}1$, then $\sum_{i=0}^{n} a{\cdot}r^i = (n{+}1){\cdot}a$
- if $r{\neq}1$, then $\sum_{i=0}^{n} a{\cdot}r^i = (a{\cdot}r^{n+1} - a)/(r-1)$.

(a) $\sum_{j=0}^{8}(1 + (-1)^j)$

Solution:

$$\begin{aligned}\sum_{j=0}^{8}(1+(-1)^j) &= \sum_{j=0}^{8}1 + \sum_{j=0}^{8}(-1)^j \\ &= 9 + (1{\cdot}(-1)^9 - 1)/(-1-1) \\ &= 9 + (-2)/(-2) \\ &= 9 + 1 \\ &= 10\end{aligned}$$

(b) $\sum_{j=1}^{4}(2^j + 3{\cdot}j)$

Solution:

$$\begin{aligned}\sum_{j=1}^{4}(2^j + 3{\cdot}j) &= \sum_{j=1}^{4}2^j + 3{\cdot}\left(\sum_{j=1}^{4}j\right) \\ &= \sum_{j=0}^{3}2{\cdot}2^j + 3{\cdot}\left(\sum_{j=1}^{4}j\right) \\ &= (2{\cdot}2^4 - 1)/(2-1) + 3{\cdot}(4{\cdot}5/2) \\ &= (32-2)/1 + 3{\cdot}10 \\ &= 30 + 30 \\ &= 60\end{aligned}$$

(c) $\sum_{j=0}^{5} 5{\cdot}2^j$

Solution:

$$\sum_{j=0}^{5} 5{\cdot}2^j = (5{\cdot}2^6 - 5)/(2-1) = 315$$

(d) $\sum_{i=0}^{2} \sum_{j=0}^{3} (2{\cdot}i + 3{\cdot}j)$

Solution:

$$\begin{aligned}
\textstyle\sum_{i=0}^{2}\sum_{j=0}^{3}(2{\cdot}i + 3{\cdot}j) &= \left(\textstyle\sum_{i=0}^{2}\sum_{j=0}^{3} 2{\cdot}i\right) + \left(\textstyle\sum_{i=0}^{2}\sum_{j=0}^{3} 3{\cdot}j\right) \\
&= 2{\cdot}\left(\textstyle\sum_{i=0}^{2} i{\cdot}\left(\sum_{j=0}^{3} 1\right)\right) + 3{\cdot}\left(\textstyle\sum_{i=0}^{2}\left(\sum_{j=0}^{3} j\right)\right) \\
&= 2{\cdot}\left(\textstyle\sum_{i=0}^{2} i{\cdot}4\right) + 3{\cdot}\left(\textstyle\sum_{i=0}^{2}(4{\cdot}3)/2\right) \\
&= 8{\cdot}\left(\textstyle\sum_{i=0}^{2} i\right) + 18{\cdot}\left(\textstyle\sum_{i=0}^{2} 1\right) \\
&= 8{\cdot}(3{\cdot}2)/2 + 18{\cdot}3 \\
&= 78
\end{aligned}$$

(e) $\sum_{i=0}^{3} \sum_{j=0}^{2} (3{\cdot}i + 2{\cdot}j)$

Solution: 78 - this is the same as (d) after swapping i and j, the order of the summations and the commutativity of addition, i.e. $a{+}b = b{+}a$.

(f) $\sum_{j=0}^{19} 7{\cdot}8^j$

Solution:

$$\textstyle\sum_{j=0}^{19} 7{\cdot}8^j \;=\; (7{\cdot}8^{20} - 7)/7 \;=\; 8^{20} - 1$$

13. Prove or disprove each of the following statements.

(a) If $a|b$ and $c|d$, then $(a{+}c)|(b{+}d)$.

Solution: `false` - for example, consider $a = b = c = 1$ and $d = 2$, then 1 divides both 1 and 2, but 2 does not divide 3.

(b) If $a|b$ and $b|c$, then $a|c$.

Solution: `true` - If $b = a{\cdot}k$ and $c = b{\cdot}l$, then $c = a{\cdot}(k{\cdot}l)$, so $a|c$

(c) If $a|c$ and $b|c$, then $(a{+}b)|c$.

Solution: `false` - for example, consider $a = b = c = 1$, then 1 divides 1, but 2 does not divide 1

(d) If $a|b$ and $c|d$, then $(a{\cdot}c)|(b{+}d)$.

Solution: `false` - for example, consider $a = b = 2$ and $c = d = 1$, then 2 divides 2 and 1 divides 1, but 2 does not divide 3

(e) If $a|b$ and $b|a$, then a=b.

Solution: `false` - for example, consider $a = 1$ and $b = -1$, then 1 divides -1 and -1 divides 1, but 1 and -1 are not equal

(f) If $a|(b + c)$, then $a|b$ and $a|c$.

Solution: `false` - for example, consider $a = 2, b = c = 3$, then 2 divides 6, but 2 does not divide 3

(g) If $a|b{\cdot}c$, then $a|b$ or $a|c$.

Solution: `false` - for example, consider $a = 4$, $b = 2$, $c = 6$, then 4 divides 12, but 4 divides neither 2 nor 6

(h) If $a|c$ and $b|c$, then $(a{\cdot}b)|c^2$.

Solution: `true` - if $c = a{\cdot}k$ and $c = b{\cdot}l$, then $c^2 = (a{\cdot}b){\cdot}(k{\cdot}l)$, so $(a{\cdot}b)|c^2$

14. Find the unique prime factorisation of 2940.

Solution: Following the approach in the lecture:

- $N = 2940$, $p = 2$ and $rootN = 54$
- `print`(2)
- $N = 1470$, $p = 2$ and $rootN = 38$
- `print`(2)
- $N = 735$, $p = 2$ and $rootN = 27$
- $p =$ `nextPrime`(2)
- `print`(3)
- $N = 245$, $p = 3$ and $rootN = 15$
- $p =$ `nextPrime`(3)
- `print`(5)
- $N = 49$, $p = 5$ and $rootN = 7$
- $p =$ `nextPrime`(5)
- `print`(7)
- $N = 7$, $p = 5$ and $rootN = 2$
- `print`(7)

This yields the prime factorisation $2940 = 2^2{\cdot}3{\cdot}5{\cdot}7^2$

Difficult/challenging questions (Sequences, Summation, Integers and Division).

15. Provide a simple formula that generates the terms of the integer sequence 3, 6, 11, 18, 27, 38, 51, 66, 83, 102, ...

> **Solution:** $a_1 = 3$ and $a_n = a_{n-1} + (2{\cdot}n{-}1)$ for $n \geq 2$ (i.e. the next value is the previous value plus the next odd number starting from 3, so 3+3, 6+5, 11+7, ...)
>
> For information, the nth term is given by $a_n = n^2 + 2$ for $n \geq 1$.

16. Let $\langle a_j \rangle_{j \in \mathbb{N}}$ be an arithmetic progression, given by $a_0 = c$ and $a_j = a_{j-1} + d$ for $j{\geq}1$ (where c and d are constants).

    (a) Write an expression for a_j in terms of c, d and j ($j \geq 0$)

    > **Solution:** $a_j = c + j{\cdot}d$ for $j \geq 0$

    (b) Write an expression for the sum in terms of c, d and n

    > **Solution:** From the solution to the previous part of the question we have:
    >
    > $$\begin{aligned}
    > &\textstyle\sum_{j=0}^{n} a_j \;=\; \sum_{j=0}^{n}(c + j{\cdot}d) \\
    > &= \left(\textstyle\sum_{j=0}^{n} c\right) + \left(\sum_{j=0}^{n} j{\cdot}d\right) && \text{rearranging} \\
    > &= (n{+}1){\cdot}c + \left(\textstyle\sum_{j=0}^{n} j{\cdot}d\right) && \text{since adding } c \text{ together } n{+}1 \text{ times equals } (n{+}1){\cdot}c \\
    > &= (n{+}1){\cdot}c + \left(\textstyle\sum_{j=0}^{n} j\right){\cdot}d && \text{using the fact } x{\cdot}z + y{\cdot}z = (x+y){\cdot}z \\
    > &= (n{+}1){\cdot}c + \left(0 + \textstyle\sum_{j=1}^{n} j\right){\cdot}d && \text{rearranging} \\
    > &= (n{+}1){\cdot}c + \left(\frac{n{\cdot}(n{+}1)}{2}\right){\cdot}d && \text{using the theorem from the lectures} \\
    > &= (n{+}1) \cdot \left(c + \frac{n{\cdot}d}{2}\right) && \text{rearranging.}
    > \end{aligned}$$

17. Determine whether each of the following sets are countable. For those that are countably infinite, construct a bjectition between the set of natural numbers and that set.

    (a) the integers 1, 2, 4, 8, 16, 32, ...;

    > **Solution:** The set is countably infinite and one possible bijection is given by $f(i) = 2^i$ for all $i \in \mathbb{N}$.

    (b) integers divisible by 3;

Solution: The set is countably infinite and one possible bijection is given by:

$$f(i) = \begin{cases} 3{\cdot}(i/2) & \text{if } i \text{ is even} \\ -3{\cdot}((i+1)/2) & \text{if } i \text{ is odd} \end{cases}$$

for all $i \in \mathbb{N}$.

(c) real numbers whose decimal expansions comprise 3's and 7's;

Solution: This set is uncountable - the proof follows the argument used to show the real numbers between 0 and 1 are uncountable (this approach is called Cantor's diagonal argument). In particular, we assume this set is countable which means that we can list the set:

$$\begin{aligned} r_0 &= 0.x_0^0 x_1^0 x_2^0 \dots x_i^0 \dots \\ r_1 &= 0.x_0^1 x_1^1 x_2^1 \dots x_i^1 \dots \\ &\vdots \qquad\qquad \vdots \\ r_n &= 0.x_0^n x_1^n x_2^n \dots x_i^n \dots \\ &\vdots \qquad\qquad \vdots \end{aligned}$$

where $x_i^n \in \{0, 3, 7\}$ for all $n, j \in \mathbb{N}$. Note x_j^n can equal 0 corresponding to the case when the decimal expansion is finite and we then add zero, e.g. 0.73 is expressed as $0.73000\dots$.

Now, using the list we can create a number $r = 0.x_0 x_1 x_2 \dots x_i \dots$ in the set but not in the list by choosing for each i the value x_i such that:

$$x_i = \begin{cases} 7 & \text{if } x_i^i \in \{3, 0\} \\ 3 & \text{otherwise (i.e. if } x_i^i = 7). \end{cases}$$

By construction, r in the set but not equal to r_i for any i, which contradicts the fact that the list contained all the elements of the set. Therefore, we cannot construct such a list and the set must be uncountable.

(d) A subset A of a countable set B.

Solution: As B is countable, we can list the elements of B as $b_0, b_1, b_2, b_3, \dots$. Now since A is a subset of B, there are integers $0 \leq i_0 < i_1 < i_2 < i_3 < \dots$ such that $b_{i_j} \in A$, and if $b_k \in A$ for some k, then $k = i_j$ for some $j \geq 0$.

If A is not finite (i.e. the sequence $i_1, i_2, \dots$ is infinite), then it is countably infinite and one possible bijection is given by $f(j) = b_{i_j}$ for $j \in \mathbb{N}$.

Algorithmic Foundations 2 - Tutorial Sheet 4

Integers and Matrices

---

1. Applying the division algorithm with $a = -35$ and $d = 6$ yields what value of r?

> **Solution:** The answer 1 since $-35 = 6 \cdot (-6) + 1$. Recall that we must find q and r such that $0 \leq r < 6$.

2. Find:
   (a) $\gcd(20!, 12!)$;

> **Solution:** We have that 12! divides itself and 20! (since $20! = 12! \cdot 13 \cdot 14 \cdot 15 \cdots 19 \cdot 20$), and hence $\gcd(20!, 12!) = 12!$.

   (b) $\gcd(289, 2346)$;

> **Solution:** Using the Euclidean algorithm:
>
> $$\begin{aligned} 2346 &= 289 \cdot 8 + 34 \\ 289 &= 34 \cdot 8 + 17 \\ 34 &= 17 \cdot 2 + 0 \end{aligned}$$
>
> and therefore $\gcd(2346, 289) = 17$

   (c) $\text{lcm}(20!, 12!)$;

> **Solution:** For similar reasoning to part (a) we have $\text{lcm}(20!, 12!) = 20!$

   (d) $\text{lcm}(289, 2346)$.

> **Solution:** Computing the prime factorisations, first 289 is not divisible by 2, 3, 5, ..., 13, nor 15 and $289/17 = 17$, it follows that $289 = 17^2$. Considering the prime factorisation of 2346 we have:
>
> - $2346/2 = 1173$ and 1173 is not divisible by 2;
> - $1173/3 = 391$ and 391 is not divisible by 3, 5, 7, 9, 11, nor 13;
> - $391/17 = 23$ and $\sqrt{23} < 17$
>
> and hence $2346 = 2^1 \cdot 3^1 \cdot 17^1 \cdot 23^1$.
> Combining these results with the approach for computing lcms explained in the lectures, it follows that $\text{lcm}(289, 2346) = 2^1 \cdot 3^1 \cdot 17^2 \cdot 23^1 = 39882$.

3. List all positive integers less than 21 that are relatively prime to 33.

Solution: The number p is relatively prime to 33 if $\gcd(p, 33) = 1$, hence the relatively prime positive integers less than 21 are: 1, 2, 4, 5, 7, 8, 10, 13, 14, 16, 17, 19, 20

4. Find:
   (a) 18 mod 7

   Solution: Using the division algorithm we have $18 = 7{\cdot}2{+}4$, and hence $18 \bmod 7 = 4$

   (b) -88 mod 13

   Solution: Using the division algorithm we have $-88 = 13{\cdot}(-7) + 3$, and hence $18 \bmod 7 = 3$

   (c) 289 mod 17

   Solution: Using the division algorithm we have $289 = 17{\cdot}17 + 0$, and hence $289 \bmod 17 = 0$

5. Determine whether each of the following 'theorems' is `true` or `false`. Assume that a, b, c, d and m are integers with $m{>}1$.
   (a) If $a \equiv b \pmod{m}$, and $a \equiv c \pmod{m}$, then $a \equiv b + c \pmod{m}$

   Solution: `false` - for example considering $a = b = 1$, $c = 3$ and $m = 2$, then:

   - $1 \equiv 1 \pmod{2}$ since 2 divides $1{-}1 = 0$ 2;
   - $1 \equiv 3 \pmod{2}$ since 2 divides $1{-}3 = -2$ 2;
   - $1 \not\equiv 4 \pmod{2}$ since 2 does not divide $1{-}4 = -3$.

   (b) If $a \equiv b \pmod{m}$, and $c \equiv d \pmod{m}$, then $a{\cdot}c \equiv b{+}d \pmod{m}$

   Solution: `false` - for example, considering $a = 0$, $b = 2$, $c = 1$, $d = 1$ and $m = 2$, then

   - $0 \equiv 2 \pmod{2}$ since 2 divides $0{-}2 = -2$;
   - $1 \equiv 1 \pmod{2}$ since 2 divides $1{-}1 = 0$;
   - $0 \not\equiv 3 \pmod{2}$ since 2 does not divide $0{-}3 = -3$.

   (c) If $a \equiv b \pmod{m}$, then $2{\cdot}a \equiv 2{\cdot}b \pmod{m}$

   Solution: `true` - if m divides $a - b$, then clearly m divides $2{\cdot}(a - b) = 2{\cdot}a - 2{\cdot}b$

   (d) If $a \equiv b \pmod{m}$, then $2{\cdot}a \equiv 2{\cdot}b \pmod{2{\cdot}m}$

   Solution: `true` - if m divides $a - b$, then clearly $2{\cdot}m$ divides $2{\cdot}(a - b) = 2{\cdot}a - 2{\cdot}b$

   (e) If $a \equiv b \pmod{m}$, then $a \equiv b \pmod{2{\cdot}m}$

Solution: `false` - for example, considering $a = 1$, $b = 3$ and $m = 2$, then

- $1 \equiv 3 \pmod 2$ since 2 divides $1-3 = -2$;
- $1 \not\equiv 3 \pmod 4$ since 4 does not divide $1-3 = -2$.

(f) If $a \equiv b \pmod{2 \cdot m}$, then $a \equiv b \pmod m$

Solution: `true` - if $2 \cdot m$ divides $a - b$, then, since m divides $2 \cdot m$, it follows that m divides $a - b$

(g) If $a \equiv b \pmod{m^2}$, then $a \equiv b \pmod m$

Solution: `true` - if m^2 divides $a - b$, then, since m divides m^2, it follows that m divides $a - b$

6. Use the Euclidean algorithm to find:

(a) $\gcd(44, 52)$;

Solution:

$$\begin{aligned} 52 &= 44 \cdot 1 + 8 \\ 44 &= 8 \cdot 5 + 4 \\ 8 &= 4 \cdot 2 + 0 \end{aligned}$$

Therefore $\gcd(44, 52) = 4$

(b) $\gcd(201, 302)$;

Solution:

$$\begin{aligned} 302 &= 201 \cdot 1 + 101 \\ 201 &= 101 \cdot 1 + 100 \\ 101 &= 100 \cdot 1 + 1 \\ 100 &= 1 \cdot 100 + 0 \end{aligned}$$

Therefore $\gcd(201, 302) = 1$

(c) $\gcd(184, 233)$.

Solution:

$$\begin{aligned} 233 &= 184 \cdot 1 + 49 \\ 184 &= 49 \cdot 3 + 37 \\ 49 &= 37 \cdot 1 + 12 \\ 37 &= 12 \cdot 3 + 1 \\ 12 &= 1 \cdot 12 + 0 \end{aligned}$$

Therefore $\gcd(184, 233) = 1$

7. Compute $A+B$ when the matrices A and B are given by:

$$A = \begin{pmatrix} 4 & -1 & 0 & 3 \\ 3 & 0 & 8 & 6 \\ 12 & 3 & -6 & 2 \end{pmatrix} \quad \text{and} \quad B = \begin{pmatrix} 0 & -5 & 4 & 1 \\ 2 & 0 & 12 & 3 \\ 9 & 6 & 7 & -5 \end{pmatrix}$$

Solution:

$$A+B = \begin{pmatrix} 4+0 & -1+(-5) & 0+4 & 3+1 \\ 3+2 & 0+0 & 8+12 & 6+3 \\ 12+9 & 3+6 & -6+7 & 2+-5 \end{pmatrix} = \begin{pmatrix} 4 & -6 & 4 & 4 \\ 5 & 0 & 20 & 9 \\ 21 & 9 & 1 & -3 \end{pmatrix}$$

8. Compute $A\times B$ when the matrices A and B are given by:

$$A = \begin{pmatrix} 4 & -1 & 0 & 3 \\ 3 & 0 & 8 & 6 \\ 12 & 3 & -6 & 0 \end{pmatrix} \quad \text{and} \quad B = \begin{pmatrix} 8 & 4 & 13 & 6 & 0 \\ 0 & -5 & 4 & 7 & 3 \\ 2 & 0 & 12 & -4 & 1 \\ 9 & 6 & -7 & 0 & 5 \end{pmatrix}$$

Solution:

$$A\times B = \begin{pmatrix} 32+0+0+27 & 16+5+0+18 & 52-4+0-21 & 24-7+0+0 & 0-3+0+15 \\ 24+0+16+54 & 12-0+0+36 & 39+0+96-42 & 18+0-32+0 & 0+0+8+30 \\ 96+0-12+0 & 48-15+0+0 & 156+12-72+0 & 72+21+24+0 & 0+9-6+0 \end{pmatrix}$$

$$= \begin{pmatrix} 59 & 39 & 27 & 17 & 12 \\ 94 & 48 & 93 & -14 & 38 \\ 84 & 33 & 96 & 117 & 3 \end{pmatrix}$$

9. (a) Suppose A and B are $m\times k$ matrices and C is a $k\times n$ matrix, show that:

$$(A+B)\times C \;=\; A\times C + B\times C\,.$$

Solution: If $A=[a_{i,j}]$, $B=[b_{i,j}]$ and $C=[c_{i,j}]$, then by definition of matrix sum $A+B=[a_{i,j}+b_{i,j}]$ and by definition of matrix product:

$$\begin{aligned}
(A+B)\times C &= \left[\textstyle\sum_{r=1}^{k}(a_{i,r}+b_{i,r})\cdot c_{r,j}\right] \\
&= \left[\textstyle\sum_{r=1}^{k}(a_{i,r}\cdot c_{r,j}+b_{i,r}\cdot c_{r,j})\right] && \text{rearranging} \\
&= \left[\textstyle\sum_{r=1}^{k}a_{i,r}\cdot c_{r,j}+\sum_{r=1}^{k}b_{i,r}\cdot c_{r,j}\right] && \text{rearranging} \\
&= \left[\textstyle\sum_{r=1}^{k}a_{i,r}\cdot c_{r,j}\right]+\left[\textstyle\sum_{r=1}^{k}b_{i,r}\cdot c_{r,j}\right] && \text{by definition of matrix sum} \\
&= A\times C + B\times C && \text{by definition of matrix product}
\end{aligned}$$

(b) Suppose C is an $m\times k$ matrix and A and B are $k\times n$ matrices, show that:

$$C\times(A+B) \;=\; C\times A + C\times B\,.$$

Solution: If $A=[a_{i,j}]$, $B=[b_{i,j}]$ and $C=[c_{i,j}]$, then by definition of matrix sum $A+B=[a_{i,j}+b_{i,j}]$ and by definition of matrix product:

$$\begin{aligned}
C\times(A+B) &= \left[\textstyle\sum_{r=1}^{k} c_{i,r}\cdot(a_{r,j}+b_{r,j})\right] \\
&= \left[\textstyle\sum_{r=1}^{k} (c_{i,r}\cdot a_{r,j} + c_{i,r}\cdot b_{r,j})\right] && \text{rearranging} \\
&= \left[\textstyle\sum_{r=1}^{k} c_{i,r}\cdot a_{r,j} + \sum_{r=1}^{k} c_{i,r}\cdot b_{r,j}\right] && \text{rearranging} \\
&= \left[\textstyle\sum_{r=1}^{k} c_{i,r}\cdot a_{r,j}\right] + \left[\textstyle\sum_{r=1}^{k} c_{i,r}\cdot b_{r,j}\right] && \text{by definition of matrix sum} \\
&= C\times A + C\times B && \text{by definition of matrix product}
\end{aligned}$$

10. Let A and B be two $n\times n$ matrices, show that:

(a) $(A+B)^t = A^t + B^t$;

Solution: If $A=[a_{i,j}]$ and $B=[b_{i,j}]$, then by definition of matrix sum $A+B=[c_{i,j}]=[a_{i,j}+b_{i,j}]$ and hence, by definition of transpose:

$$\begin{aligned}
(A+B)^t &= [c_{j,i}] \\
&= [a_{j,i}+b_{j,i}] && \text{from above} \\
&= [a_{j,i}] + [b_{j,i}] && \text{by definition of matrix sum} \\
&= A^t + B^t && \text{by definition of matrix transpose}
\end{aligned}$$

(b) $(A\times B)^t = B^t\times A^t$.

Solution: If $A=[a_{i,j}]$ and $B=[b_{i,j}]$, then by definition of matrix product $A\times B=[c_{i,j}]=[\sum_{r=1}^{m} a_{i,r}\cdot b_{r,j}]$ and hence, by definition of matrix transpose:

$$\begin{aligned}
(A\times B)^t &= [c_{j,i}] \\
&= [\textstyle\sum_{r=1}^{m} a_{j,r}\cdot b_{r,i}] && \text{from above} \\
&= [\textstyle\sum_{r=1}^{m} b_{r,i}\cdot a_{j,r}] && \text{rearranging} \\
&= B^t\times A^t && \text{by definition of matrix product and transpose}
\end{aligned}$$

Difficult/challenging questions.

11. Show we can easily factor a number n when we know that it is the product of two primes p and q and we know the value of $(p-1)\cdot(q-1)$.

Solution: Factoring in this case reduces to finding the values of p and q when we know the value of their product, i.e. n and the value of $(p-1)\cdot(q-1)$. Now letting $(p-1)\cdot(q-1) = m$ we have:

$$m = (p-1)\cdot(q-1) = p\cdot q - p - q + 1$$

rearranging and using the fact that $n = p\cdot q$ ir follows that:

$$p + q = n + 1 - m$$

Now, again using the fact that $n = p\cdot q$, we have:

$$\begin{aligned} p + n/p = n + 1 - m \Rightarrow\ & p^2 + n = (n+1-m)\cdot p && \text{rearranging} \\ \Rightarrow\ & p^2 - (n+1-m)\cdot p + n = 0 && \text{rearranging again.} \end{aligned}$$

Similarly, we can show:

$$q^2 - (n+1-m)\cdot q + n = 0$$

and hence p and q are the two solutions of the quadratic equation:

$$x^2 - (n+1-m)\cdot x + n = 0$$

and since we know the values of n and m we can easily solve this using the formula:

$$x = \frac{-b \pm \sqrt{b^2 - 4a\cdot c}}{2}$$

with $a = 1$, $b = -(n+1-m)$ and $c = n$.

12. Let A be a 2×2 matrix where:

$$A = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$$

Under the assumption that $a\cdot d - b\cdot c \neq 0$ find the inverse of A.

Solution: Suppose the inverse of A is given by:

$$A^{-1} = \begin{pmatrix} e & f \\ g & h \end{pmatrix}$$

then by definition of matrix multiplication we have:

$$A\times A^{-1} = \begin{pmatrix} a\cdot e + b\cdot g & a\cdot f + b\cdot h \\ c\cdot e + d\cdot g & c\cdot f + d\cdot h \end{pmatrix}$$

Now to be the inverse we require that the product equals the identity matrix and therefore:

$$\begin{aligned} a\cdot e + b\cdot g &= 1 \\ a\cdot f + b\cdot h &= 0 \\ c\cdot e + d\cdot g &= 0 \\ c\cdot f + d\cdot h &= 1 \end{aligned}$$

Solving these equations for e, f, g and h, under the assumption $a\cdot d - b\cdot c \neq 0$, we find that:

$$A^{-1} = \begin{pmatrix} \frac{d}{a\cdot d - b\cdot c} & \frac{-b}{a\cdot d - b\cdot c} \\ \frac{-c}{a\cdot d - b\cdot c} & \frac{a}{a\cdot d - b\cdot c} \end{pmatrix}$$

Algorithmic Foundations 2 - Tutorial Sheet 5

Methods of Proof

---

1. Write out the following arguments using quantifiers, connectives, and symbols to stand for propositions as necessary, explaining which rules of inference are used for each step.

   (a) "Linda, a student in this class, owns a Porsche. Everyone who owns a Porsche has been caught speeding. Therefore, someone in this class has been caught speeding".

   Solution: Let x be in the universe of all students and define the following predicates:

   - $C(x)$: x is in this class;
   - $P(x)$: x owns a Porsche;
   - $S(x)$: x has been caught speeding.

   We are therefore given the premises $C(Linda)$, $P(Linda)$ and $\forall x.\,(P(x) \rightarrow S(x))$. We want to conclude that $\exists x\,.(C(x) \wedge S(x))$.

1. $\forall x.\,(P(x) \rightarrow S(x))$	premise
2. $P(Linda) \rightarrow S(Linda)$	universal instantiation using 1
3. $P(Linda)$	premise
4. $S(Linda)$	modus ponens using 2,3
5. $C(Linda)$	premise
6. $C(Linda) \wedge S(Linda)$	conjunction using 4,5
7. $\exists x.(C(x) \wedge S(x))$	existential generalisation using 6

   (b) "Each of five flatmates, Tracy, Alan, Susan, John and Catherine, has taken AF2. Every student who has taken AF2 can take Algorithmics 3. Therefore, all five flatmates can take Algorithmics 3 next year".

   Solution: Let x be in the universe of all students and define the following predicates:

   - $F(x)$: x is one of the five flatmates listed;
   - $AF2(x)$: x has taken AF2;
   - $Alg3(x)$: x can take Algorithmics 3.

   We are therefore given the premises $\forall x.\,(F(x) \rightarrow AF2(x))$ and $\forall x.\,(AF2(x) \rightarrow Alg3(x))$ and we want to conclude that $\forall x.\ (F(x) \rightarrow Alg3(x))$. In the below, let y be an arbitrary student.

1. $\forall x.\,(F(x) \rightarrow AF2(x))$	premise
2. $F(y) \rightarrow AF2(y)$	universal instantiation using 1
3. $\forall x.\,(AF2(x) \rightarrow Alg3(x))$	premise
4. $AF2(y) \rightarrow Alg3(y)$	universal instantiation using 3
5. $F(y) \rightarrow Alg3(y)$	hypothetical syllogism using 2,4
6. $\forall x.\,(F(x) \rightarrow Alg3(x))$	universal generalisation using 5

2. The following argument is an incorrect proof of the conjecture "if n^2 is not divisible by 3, then n is not divisible by 3".

   > "If n^2 is not divisible by 3, then n^2 does not equal $3{\cdot}k$ for some integer k. Hence n does not equal $3{\cdot}l$ for some integer l. Therefore, n is not divisible by 3".

   The reason it is incorrect is that circular reasoning has been used. Where has the error in reasoning been made?

   Ignoring the incorrect proof, does the original conjecture hold (i.e. if n^2 is not divisible by 3, then n is not divisible by 3)? If it is `true`, then give a proof; if not, give a counterexample.

   Solution: The statement beginning with the word "Hence" does not follow from what has preceded it. The writer has implied that it does, but nothing in the statement "n^2 does not equal $3{\cdot}k$ for some integer k" immediately allows us to conclude that "n does not equal $3{\cdot}l$ for some integer l". The writer must prove this.

   Even though this particular proof is incorrect, the conjecture is `true`. This can be demonstrated using for example an indirect proof. In other words, we prove that if n is divisible by 3, then n^2 is divisible by 3.

   Suppose that n is divisible by 3, then $n = 3{\cdot}l$ for some integer l. Hence $n^2 = 9{\cdot}l^2 = 3{\cdot}(3{\cdot}l^2)$, and therefore n^2 is divisible by 3 as required.

3. (a) Prove the proposition $P(0)$, where $P(n)$ is the proposition "if n is a positive integer greater than 1, then $n^2 > n$". What kind of proof did you use?

   Solution: The proposition is vacuously `true` since 0 is not a positive integer greater than 1. So a vacuous proof was used.

   (b) Prove the proposition $P(1)$, where $P(n)$ is the proposition "if n is a positive integer, then $n^2 \geq n$". What kind of proof did you use?

   Solution: We need to prove the proposition "if 1 is a positive integer, then $1^2 \geq 1$". The conclusion is the `true` statement $1 \geq 1$. Therefore the implication is `true`. This is an example of a trivial proof, since we did not use the hypothesis in order to show that the conclusion is `true`.

4. Prove that the square of an even integer is an even integer by using:

   (a) a direct proof

   Solution: If n is an even integer, then $n = 2{\cdot}k$ for some integer k. Hence, $n^2 = 4{\cdot}k^2 = 2{\cdot}(2{\cdot}k^2)$, and therefore n^2 is an even integer as required.

   (b) an indirect proof

   Solution: In an indirect proof we need to show that if n^2 is not even, then n is not even, i.e. if n^2 is odd, then n is odd. Therefore we assume n^2 is odd, by definition there exists $k \in \mathbb{N}$ such that

   $$\begin{aligned} n^2 = 2{\cdot}k + 1 &\Rightarrow n^2 - 1 = 2{\cdot}k && \text{rearranging} \\ &\Rightarrow (n{-}1)(n{+}1) = 2{\cdot}k && \text{rearranging.} \end{aligned}$$

Therefore, by definition, we have that $(n-1)(n+1)$ is even, which implies that either $(n-1)$ or $(n+1)$ is even, in either case this implies that n is odd as required.

(c) a proof by contradiction.

Solution: Suppose that n is even and for a contradiction that n^2 is not even (i.e. n^2 is odd). Using the same arguments as in the indirect proof above, from the fact that n^2 is odd, we can show that n is odd yielding a contradiction, and hence n^2 is even.

5. Prove that the product of two rational numbers is rational.

   Note: a rational number is a number which can be expressed as a fraction of the form p/q, where p and q are integers and $q \neq 0$.

Solution: If a and b are rational numbers, then we can write $a = p/q$ and $b = r/s$ for integers p, q, r and s such that $q \neq 0$ and $s \neq 0$. Therefore $a \cdot b = (p \cdot r)/(q \cdot s)$ which is a rational number, since $p \cdot r$ and $r \cdot s$ are integers and $q \cdot s \neq 0$.

Note this is a direct proof.

6. Prove or disprove that the product of two irrational numbers is irrational

   Note: an irrational number is a number that cannot be expressed as a fraction p/q, where p and q are integers and $q \neq 0$.

Solution: The statement is `false`. If $a = b = \sqrt{2}$ ($\sqrt{2}$ was shown to be irrational in the lectures), then $a \cdot b = 2$ which is a rational number.

Note this is a proof by counterexample.

7. Prove that the following statements are equivalent, where n is an integer:

   1. n is even;
   2. $n + 1$ is odd;
   3. $3 \cdot n + 1$ is odd.

Solution:

1 → 2: If n is even, then $n = 2 \cdot k$ for some integer k. Therefore $n+1 = 2 \cdot k+1$, and hence $n+1$ is odd.

2 → 3: If $n+1$ is odd, then $n+1 = 2 \cdot k+1$ for some integer k. Therefore $n = 2 \cdot k$ and $3 \cdot n+1 = 3 \cdot (2 \cdot k)+1 = 2 \cdot (3 \cdot k)+1$, and hence $3 \cdot n+1$ is odd.

3 → 1: If $3 \cdot n+1$ is odd and for a contradiction that n is odd. Then $n = 2 \cdot k+1$ for some integer k, so that $3 \cdot n+1 = 3 \cdot (2 \cdot k+1)+1 = 2 \cdot (3 \cdot k+2)$, and hence $3 \cdot n+1$ is even yielding a contradiction. Hence n is even.

As explained in the lectures, using the hypothetical syllogism rule of inference the equivalences between the statements follows. In particular, we have:

- from $\mathbf{2} \rightarrow \mathbf{3}$ and $\mathbf{3} \rightarrow \mathbf{1}$, it follow (using hypothetical syllogism) that $\mathbf{2} \rightarrow \mathbf{1}$.
- from $\mathbf{1} \rightarrow \mathbf{2}$ and $\mathbf{2} \rightarrow \mathbf{3}$, it follows (using hypothetical syllogism) that $\mathbf{1} \rightarrow \mathbf{3}$.
- from $\mathbf{3} \rightarrow \mathbf{1}$ and $\mathbf{1} \rightarrow \mathbf{2}$, it follows (using hypothetical syllogism) that $\mathbf{3} \rightarrow \mathbf{2}$.

8. Use a proof by cases to show that if x and y are real numbers, then $\min(x, y)+\max(x, y) = x+y$.

Solution: We have the following cases to consider.

- If $x<y$, then $\min(x, y) = x$ and $\max(x, y) = y$. Hence $\min(x, y)+\max(x, y) = x+y$.
- If $x=y$, then $\min(x, y) = \max(x, y) = x = y$. Hence $\min(x, y)+\max(x, y) = x+y$.
- If $x>y$, then $\min(x, y) = y$ and $\max(x, y) = x$. Hence $\min(x, y)+\max(x, y) = x+y$.

Since these are the only cases to consider the property holds.

9. Give a constructive proof of the proposition "for every positive integer n, there is an integer divisible by more than n primes".

Solution: Let n be a given positive integer, and assume that p_1, p_2, $\ldots$,p_n, p_{n+1} denotes the first $n+1$ primes (from the lectures we have shown there are an infinite number of primes). Then the integer $p_1 \cdot p_2 \cdots p_n \cdot p_{n+1}$ is divisible by more than n primes.

Difficult/challenging questions.

10. Prove that the cube root of 3 is irrational.

    Hint: As a preliminary result, show if a^3 is divisible by 3, then a is divisible by 3. This can be proved using the fundamental theorem of arithmetic and the fact the 3 is prime.

Solution: As suggested in the hint we first show: if a^3 is divisible by 3, then a is divisible by 3. Using the fundamental theorem of arithmetic (FTA) we can express a as a unique product of primes, i.e. we have $a = p_1^{n_1} \cdot p_2^{n_2} \cdots p_k^{n_k}$ such that p_i is prime and $n_i>0$ for $1 \leq i \leq k$, and hence $a^3 = p_1^{3 \cdot n_1} \cdot p_2^{3 \cdot n_2} \cdots p_k^{3 \cdot n_k}$. Using the FTA again, we have that this is the unique representation of a^3 in terms of primes and, since 3 dividies a^3 and 3 is prime, it follows that $p_i = 3$ for some $1 \leq i \leq k$, giving 3 divides a as required.

Now for the main part of the proof. Suppose for a contradiction that the cube root of 3 is rational. By definition $\sqrt[3]{3} = a/b$ for some integers a and b such that $\gcd(a, b)=1$, and

hence $a^3 = 3{\cdot}b^3$. Therefore a^3 is divisible by 3 which, using the property above, implies that a is divisible by 3, and therefore $a = 3{\cdot}k$ for some integer k. Thus $3{\cdot}b^3 = (3{\cdot}k)^3 = 3^3{\cdot}k^3$ which rearranging yields $b^3 = 3{\cdot}(3{\cdot}k^3)$ which, again using the property above, gives us that b is divisible by 3. This contradicts our assumption that $\gcd(a, b) = 1$, since both a and b are divisible by 3. Hence our hypothesis that the cube root of 3 is rational is `false`, and the cube root of 3 must be irrational as required.

11. Let $S = x_1{\cdot}y_1 + x_2{\cdot}y_2 + \cdots + x_n{\cdot}y_n$ where $x_1, x_2, \ldots, x_n$'s and the $y_1, y_2, \ldots, y_n$ are both sequences of real numbers. Show that:

    - S takes the maximum value when both sequences are sorted (e.g. in non-decreasing order).
    - S takes minimum value when one sequence is in non-decreasing while the other is in non-increasing order.

    Hint: Any other arrangement of the sequences can be obtained by permuting one sequence and any permutation can be written as a sequence of transpositions which act on distinct elements, i.e. each element is transposed at most once (a transposition is a permutation which only changes two elements and everything else remains the same).

Solution: The idea here is to consider the transposition steps required to get to any other arrangement of the summation and show that after each step the summation does not decrease (for the first part) or increase (for the second part). Note that this is only possible under the assumption that each element is transposed at most once, as otherwise we cannot use the fact the sequences are initially ordered.

For example consider the first case and suppose in one of the transposition steps we swap x_i with x_j and move from summation S' to summation S''. Now with out loss of generality we can suppose $i < j$ and since this is the only time x_i and x_j are transposed, since the sequence $x_1, x_2, \ldots, x_n$ is sorted we have $x_i \leq x_j$. Now since all that differs in the summations S' and S'' is that x_i and x_j are swapped we have:

$$\begin{aligned} S' - S'' &= (x_i{\cdot}y_i + x_j{\cdot}y_j) - (x_j{\cdot}y_i + x_i{\cdot}y_j) \\ &= (x_i{\cdot}y_i - x_j{\cdot}y_i) + (x_j{\cdot}y_j - x_i{\cdot}y_j) && \text{rearranging} \\ &= y_i{\cdot}(x_i - x_j) + y_j{\cdot}(x_j - x_i) && \text{rearranging} \\ &= -y_i{\cdot}(x_j - x_i) + y_j{\cdot}(x_j - x_i) && \text{rearranging} \\ &= y_j{\cdot}(x_j - x_i) - y_i{\cdot}(x_j - x_i) && \text{rearranging} \end{aligned}$$

Now, from above we have since the sequence $y_1, y_2, \ldots, y_n$ is in non-decreasing order and $i < j$ we have $y_i \leq y_j$ and combining this with the fact $x_i \leq x_j$ it follows that $S' - S'' \geq 0$. Since this was for an arbitrary transposition step it follows that the resulting summation will be no larger, and hence S is maximal when both sequences are sorted (e.g. in non-decreasing order) as the other sequence was also arbitrary.

The second part follows similarly, if we assume the first sequence is ordered non-decreasing and the second non-increasing, then we derive that:

$$S' - S'' = y_j{\cdot}(x_j - x_i) - y_i{\cdot}(x_j - x_i)$$

and then use the fact that $x_i \leq x_j$ and $y_i \geq y_j$ to show $S' - S'' \leq 0$.

Algorithmic Foundations 2 - Tutorial Sheet 6

Induction and Recursive Definitions

---

1. Use the principle of mathematical induction to show $\sum_{i=1}^{n} i{\cdot}(i!) = (n{+}1)! - 1$ for all $n \in \mathbb{N}$.

Solution: Let $P(n)$ be the proposition $\sum_{i=1}^{n} i{\cdot}(i!) = (n{+}1)! - 1$.

Base case: $P(1)$ holds since $1{\cdot}(1!) = 1 = 2{-}1 = (1{+}1)! - 1$.

Inductive step: We now assume $P(n)$ is true for some $n \in \mathbb{N}$. Considering $n{+}1$ we have:

$$\begin{aligned}
\textstyle\sum_{i=1}^{n+1} i{\cdot}(i!) &= \textstyle\sum_{i=1}^{n} i{\cdot}(i!) + (n{+}1){\cdot}(n{+}1)! \\
&= \Big((n+1)! - 1\Big) + (n+1){\cdot}(n+1)! && \text{by the inductive hypothesis} \\
&= \Big(1 + (n{+}1)\Big){\cdot}(n+1)! - 1 && \text{rearranging} \\
&= (n+2){\cdot}(n+1)! - 1 && \text{simplifying} \\
&= (n+2)! - 1 && \text{by definition of factorial}
\end{aligned}$$

and hence $P(n{+}1)$ holds.
Therefore by the principle of induction we have proved that $P(n)$ holds for all $n \in \mathbb{N}$.

2. Use the principle of mathematical induction to show $3^n < n!$ for all $n{>}6$.

Solution: Let $P(n)$ be the proposition $3^n < n!$.

Base case: $P(7)$ is true, since $3^7 = 2187 < 5040 = 7!$

Inductive step: Assume that $P(n)$ is true for some $n{>}6$. Now considering $n{+}1$ we have:

$$\begin{aligned}
3^{n+1} &= 3{\cdot}3^n && \text{rearranging} \\
&< 3{\cdot}n! && \text{by the inductive hypothesis} \\
&< (n+1){\cdot}n! && \text{since } n{>}6 \\
&= (n+1)! && \text{by definition of factorial}
\end{aligned}$$

and hence $P(n{+}1)$ holds.
Therefore by the principle of induction we have proved that $P(n)$ holds for all $n{>}6$.

3. Use the principle of mathematical induction to show $n^3 > n^2 + 3$ for all $n \geq 2$.

Solution: Let $P(n)$ be the proposition $n^3 > n^2 + 3$.

Base case: $P(2)$ is true, since $2^3 = 8 > 7 = 2^2 + 3$.

Inductive step: Assume that $P(n)$ is true for some $n \geq 2$ and consider $n{+}1$. Now, expanding we have:

$$\begin{aligned}
(n+1)^3 &= n^3 + 3{\cdot}n^2 + 3{\cdot}n + 1 \\
&> (n^2+3) + 3n^2 + 3n + 1 && \text{by the inductive hypothesis} \\
&= 4n^2 + 3n + 1 + 3 && \text{rearranging} \\
&\geq n^2 + 2n + 1 + 3 && \text{since } n{\geq}0 \\
&= (n{+}1)^2 + 3 && \text{since } (n{+}1)^2 = n^2 + 2{\cdot}n + 1
\end{aligned}$$

and hence $P(n{+}1)$ holds.

Therefore by the principle of induction we have proved that $P(n)$ holds for all $n \geq 2$.

4. Suppose that

   - $a_1 = 2$;
   - $a_2 = 9$;
   - $a_n = 2{\cdot}a_{n-1} + 3{\cdot}a_{n-2}$ for $n \geq 3$.

   Use (the second principle of) mathematical induction to show $a_n \leq 3^n$ for all $n \in \mathbb{Z}^+$.

Solution: Let $P(n)$ be the proposition that $a_n \leq 3^n$.

Base cases: $P(1)$ and $P(2)$ are true, since $a_1 = 2 \leq 3 = 3^1$ and $a_2 = 9 = 3^2$.

Inductive step: Let $n{\geq}2$ and assume that $P(k)$ is true for all $1{\leq}k{\leq}n$. Now by definition we have

$$\begin{aligned}
a_{n+1} &= 2{\cdot}a_n + 3{\cdot}a_{n-1} \\
&\leq 2{\cdot}3^n + 3{\cdot}3^{n-1} && \text{by the inductive hypothesis (using both } P(n) \text{ and } P(n{-}1)) \\
&= 2{\cdot}3^n + 3^n && \text{rearranging} \\
&= 3{\cdot}3^n && \text{rearranging} \\
&= 3^{n+1} && \text{and hence } P(n{+}1) \text{ holds.}
\end{aligned}$$

Therefore by the principle of induction we have proved that $P(n)$ holds for all $n \in \mathbb{Z}^+$.

5. Use the principle of mathematical induction to show a function f defined by specifying $f(0)$ and a rule for obtaining $f(n{+}1)$ from $f(n)$ (for each $n \geq 0$) is well-defined.

Solution: Let $P(n)$ be the proposition that $f(n)$ is well-defined.

Base case: $P(0)$ is true, since $f(0)$ is well-defined.

Inductive step: Assume that $P(n)$ is true for some $n \in \mathbb{Z}^+$. Now $f(n{+}1)$ is defined in terms of $f(n)$ and by the inductive hypothesis, $f(n)$ is well-defined. Therefore $f(n{+}1)$ is well-defined and $P(n{+}1)$ holds.

Therefore by the principle of induction we have proved that $P(n)$ holds for all $n \in \mathbb{Z}^+$.

6. Find $f(i)$ for $i = 1, 2, 3, 4$ given $f(n)$ is defined recursively by $f(0) = 3$ and for each $n \geq 0$:
   (a) $f(n{+}1) = -2{\cdot}f(n)$;

   Solution: -6, 12, -24, 48

   (b) $f(n{+}1) = 3{\cdot}f(n) + 7$;

   Solution: 16, 55, 172, 523

   (c) $f(n{+}1) = f(n)^2 - 2{\cdot}f(n) - 2$;

   Solution: 1, -3, 13, 141

   (d) $f(n{+}1) = 3{\cdot}f(n)/3$.

   Solution: 3, 3, 3, 3

7. Give a recursive definition for each of the following non-recursive definitions:
   (a) $g_1(n) = 4{\cdot}7^n$ for all $n \geq 0$;

   Solution: $g_1(0) = 4$ and $g_1(n{+}1) = 7{\cdot}g_2(n)$ for $n \geq 0$

   This can derived as follows: by definition we have $g_1(0) = 4{\cdot}7^0 = 4{\cdot}1 = 4$, while expanding $g_1(n{+}1)$ yields:

   $$\begin{aligned} g_1(n{+}1) &= 4{\cdot}7^{n+1} && \text{by definition} \\ &= 7{\cdot}(4{\cdot}7^n) && \text{rearranging} \\ &= 7{\cdot}g_1(n) && \text{by definition of } g_1 \end{aligned}$$

   (b) $g_2(n) = 3{\cdot}n + 5$ for all $n \geq 0$;

   Solution: $g_2(0) = 5$ and $g_2(n{+}1) = g_2(n) + 3$ for $n \geq 0$ This can derived as follows: by definition we have $g_2(0) = 3{\cdot}0 + 5 = 0 + 5 = 5$, while expanding $g_2(n{+}1)$ yields:

   $$\begin{aligned} g_2(n{+}1) &= 3{\cdot}(n{+}1) + 5 && \text{by definition} \\ &= 3{\cdot}n + 3 + 5 && \text{rearranging} \\ &= (3{\cdot}n + 5) + 3 && \text{rearranging} \\ &= g_2(n) + 3 && \text{by definition of } g_2 \end{aligned}$$

   (c) $g_3(n) = n!$ for all $n \geq 1$;

   Solution: $g_3(1) = 1$ and $g_3(n{+}1) = (n+1){\cdot}g_3(n)$ for $n \geq 1$ This can derived as follows: by definition we have $g_3(1) = 1! = 1$, while expanding $g_2(n{+}1)$ yields:

   $$\begin{aligned} g_2(n{+}1) &= (n{+}1)! && \text{by definition} \\ &= (n{+}1){\cdot}n! && \text{rearranging since } n \geq 1 \\ &= (n{+}1){\cdot}g_3(n) && \text{by definition of } g_3 \end{aligned}$$

(d) $g_4(n) = n^2$ for all $n \geq 0$.

Solution: $g_4(0) = 0$ and $g_4(n{+}1) = g_4(n) + 2{\cdot}n + 1$ for $n \geq 0$

This can derived as follows: by definition we have $g_4(0) = n^2 = 0$, while expanding $g_4(n{+}1)$ yields:

$$\begin{aligned} g_4(n{+}1) &= (n{+}1)^2 && \text{by definition} \\ &= n^2 + 2{\cdot}n + 1 && \text{rearranging} \\ &= g_4(n) + 2{\cdot}n + 1 && \text{by definition of } g_4 \end{aligned}$$

8. Give recursive definitions of the functions max and min, so that $\max(a_1, a_2, \ldots, a_n)$ and $\min(a_1, a_2, \ldots, a_n)$ are the maximum and minimum of the n real numbers $a_1, a_2, \ldots, a_n$ respectively.

Solution: The recursive definitions of the max and min functions are denoted here by $\max_r$ and $\min_r$ respectively.

$$\begin{aligned} \max_r(a_1) &= a_1 \\ \max_r(a_1, a_2, \ldots, a_n, a_{n+1}) &= \max(\max_r(a_1, a_2, \ldots, a_n), a_{n+1}) \\ \min_r(a_1) &= a_1 \\ \min_r(a_1, a_2, \ldots, a_n, a_{n+1}) &= \min(\min_r(a_1, a_2, \ldots, a_n), a_{n+1}) \end{aligned}$$

where

$$\max(x, y) = \begin{cases} y & \text{if } x \leq y \\ x & \text{if } x > y \end{cases} \quad \text{and} \quad \min(x, y) = \begin{cases} x & \text{if } x \leq y \\ y & \text{if } x > y \end{cases}$$

9. Give a recursive definition of the following sets:

(a) the odd positive integers;

Solution: $1 \in S$ and if $x \in S$, then $x{+}2 \in S$

(b) the positive integer powers of 3;

Solution: $3 \in S$ and if $x \in S$, then $3{\cdot}x \in S$

(c) the polynomials with integer coefficients.

Solution: $q \in S$ for any $q \in \mathbb{Z}$ and if $p(x) \in S$, then $x{\cdot}p(x) + q \in S$ for any $q \in \mathbb{Z}$.

10. Give recursive definitions with initial condition(s) for each of the following sets:

(a) $\{0.1, 0.01, 0.001, \ldots\}$

Solution: $0.1 \in S$ and if $x \in S$, then $x/10 \in S$

(b) the set of positive integers congruent to 4 (mod 7)

Solution: $4 \in S$ and if $x \in S$, then $x{+}7 \in S$

(c) the set of integers not divisible by 3

Solution: $1 \in S$, $2 \in S$ and if $x \in S$, then $x{+}3 \in S$ and $x{-}3 \in S$

11. Assume that we have a list l, and are given the functions:

- `head`(l) which returns the first element of a non-empty list;
- `tail`(l) which returns the tail of a non-empty list;
- `isEmpty`(l) returns `true` if the list is empty and `false` otherwise.

For example if l equals $\langle 5, 3, 4, 2, 7, 8, 3, 4\rangle$, then `head`$(l)$ would deliver 5, `tail`(l) would deliver $\langle 3, 4, 2, 7, 8, 3, 4\rangle$, and `isEmpty`$(l)$ would deliver `false`.

Using the above functions, in a pseudo code of your choice:

(a) write a recursive function `length`(l) that returns the length of the list l as an integer.

For example, `length`$(\langle 1, 5, 2, 9, 8, 3, 2\rangle)$ would return 7.

Solution:

$$\texttt{length}(l) = \textbf{if } \texttt{isEmpty}(l) \textbf{ then } 0 \textbf{ else } 1 + \texttt{length}(\texttt{tail}(l))$$

(b) write a recursive function `sum`(l), that returns the summation of the elements in a list.

For example, `sum`$(\langle 1, 5, 2, 3\rangle)$ returns $1 + 5 + 2 + 3 = 11$.

Solution:

$$\texttt{sum}(l) = \textbf{if } \texttt{isEmpty}(l) \textbf{ then } 0 \textbf{ else } \texttt{head}(l) + \texttt{sum}(\texttt{tail}(l))$$

(c) write a recursive function `present`(e, l), that delivers `true` if e appears in the list l and `false` otherwise.

For example, `present`$(6, \langle 1, 5, 2, 3\rangle)$ returns `false` and `present`$(4, \langle 1, 2, 3, 1, 2, 4, 2\rangle)$ returns `true`.

Solution:

$$\begin{aligned}\texttt{present}(e, l) = \ & \textbf{if } \texttt{isEmpty}(l) \textbf{ then } \texttt{false} \textbf{ else} \\ & \mathit{Equals}(e, \texttt{head}(l)) \vee \texttt{present}(e, \texttt{tail}(l))\end{aligned}$$

where $\mathit{Equals}(x, y)$ is the predicate that returns `true` if and only if $x{=}y$.

(d) write a recursive function `remove`(e, l) that removes all occurrences of e from the list l.

For example, `remove`$(5, \langle 1, 5, 2, 3, 5\rangle)$ returns $\langle 1, 2, 3\rangle$.

Solution:

$$\begin{aligned}\texttt{remove}(e, l) = &\textbf{if } \texttt{isEmpty}(l) \textbf{ then } l\\ &\textbf{else if } \mathit{Equals}(e, \texttt{head}(l)) \textbf{ then } \texttt{remove}(e, \texttt{tail}(l))\\ &\textbf{else } \langle \texttt{head}(l), \texttt{remove}(e, \texttt{tail}(l))\rangle\end{aligned}$$

Difficult/challenging questions.

12. Show that the set S defined by:

    - $5 \in S$;
    - if $s \in S$ and $t \in S$, then $s + t \in S$

    is the set of positive integers divisible by 5.

Solution: Let T be the set of positive integers divisible by 5. In order to show that $S = T$, we prove that $S \subseteq T$ and $T \subseteq S$.

- In order to prove that $S \subseteq T$, we use the following method of mathematical induction over the recursively defined set S:

  Let $P(s)$ be the proposition that $s \in T$, for each $s \in S$. The proof by induction consists of establishing the following:

  Base case: $P(5)$ holds;
  Inductive step: if $P(s)$ and $P(t)$ hold for $s \in S$ and $t \in S$, then $P(s{+}t)$ holds.

  Notice that this is a different form of induction from the one we have used previously; however, in view of the recursive definition of S, establishing each of these steps corresponds exactly to showing that $S \subseteq T$.

  Clearly the base case holds, since $5 = 5{\cdot}1$. For the inductive step, assume that $P(s)$ is true and $P(t)$ is true, for some $s \in S$ and $t \in S$. Then each of s and t is divisible by 5, so that $s{+}t$ is divisible by 5, and hence $P(s{+}t)$ is true.

  Thus by unduction $P(s)$ holds for all $s \in T$, and hence $S \subseteq T$.

- In order to prove that $T \subseteq S$, we again use induction again, but this time over $\mathbb{N}$ rather than over the recursive set S. Let $Q(n)$ be the proposition that $5{\cdot}n \in S$, for each $n \in \mathbb{Z}^+$.

  Base case: $Q(1)$ is true since $5 \in S$.

  Inductive step: Assume that $Q(n)$ is true for some $n \in \mathbb{Z}^+$. Now combining the facts:

  - using the inductive hypothesis we have $5{\cdot}n \in S$;
  - using the initial conditions of S we have $5 \in S$.
  - $5{\cdot}(n{+}1) = 5{\cdot}n + 5$;

– by the definition of S, if $s, t \in S$, then $s + t \in S$;

we have $5{\cdot}n + 5 \in S$, and hence $Q(n{+}1)$ is true.

Therefore by mathematical induction $Q(n)$ holds for all $n \in \mathbb{Z}^+$. Now suppose $t \in T$, by definition $t = 5{\cdot}k$ for some positive integer k and since $Q(k)$ holds, it follows that $t \in S$, and hence $T \subseteq S$ completing the proof.

13. Prove that

$$\sum_{j=0}^{n} \left(-\frac{1}{2}\right)^j = \frac{2^{n+1} + (-1)^n}{3{\cdot}2^n}$$

for all $n \in \mathbb{N}$.

Solution: Let $P(n)$ be the proposition that $\sum_{j=0}^{n}(-\frac{1}{2})^j = \frac{2^{n+1}+(-1)^n}{3\cdot 2^n}$, for each $n \in \mathbb{N}$.

Base case: For $P(0)$ we have:

$$\sum_{j=0}^{0} \left(-\frac{1}{2}\right)^j = \left(-\frac{1}{2}\right)^0 = 1 = \frac{3}{3} = \frac{2+1}{3{\cdot}1} = \frac{2^{0+1} + (-1)^n}{3{\cdot}2^0}$$

Inductive step: Assume that $P(n)$ holds for some $n \in \mathbb{N}$. To prove that $P(n{+}1)$ holds we will split into two cases: when n is even and when n odd.

- If n is even, then considering $n{+}1$ we have that:

$$\begin{aligned}
\sum_{j=0}^{n+1} \left(-\frac{1}{2}\right)^j &= \sum_{j=0}^{n} \left(-\frac{1}{2}\right)^j + \left(-\frac{1}{2}\right)^{n+1} && \text{rearranging} \\
&= \frac{2^{n+1} + (-1)^n}{3{\cdot}2^n} + \left(-\frac{1}{2}\right)^{n+1} && \text{by induction} \\
&= \frac{2^{n+1} + 1}{3{\cdot}2^n} - \frac{1}{2^{n+1}} && \text{since } n \text{ is even (and } n{+}1 \text{ is odd)} \\
&= \frac{2^{n+2} + 2 - 3}{3{\cdot}2^{n+1}} && \text{rearranging} \\
&= \frac{2^{(n+1)+1} - 1}{3{\cdot}2^{n+1}} && \text{rearranging} \\
&= \frac{2^{(n+1)+1} + (-1)^{n+1}}{3{\cdot}2^{n+1}} && \text{since } n \text{ is even (and } n{+}1 \text{ is odd)}
\end{aligned}$$

and hence $P(n{+}1)$ holds in this case.

- If n is odd, then considering $n{+}1$ we have:

$$\begin{aligned}
\sum_{j=0}^{n+2}\left(-\frac{1}{2}\right)^j &= \sum_{j=0}^{n}\left(-\frac{1}{2}\right)^j + \left(-\frac{1}{2}\right)^{n+1} && \text{rearranging}\\
&= \frac{2^{n+1}+(-1)^n}{3{\cdot}2^n} + \left(-\frac{1}{2}\right)^{n+1} && \text{by induction}\\
&= \frac{2^{n+1}-1}{3{\cdot}2^n} + \frac{1}{2^{n+1}} && \text{since } n \text{ is odd (and } n{+}1 \text{ is even)}\\
&= \frac{2^{n+2}-2+3}{3{\cdot}2^{n+1}} && \text{rearranging}\\
&= \frac{2^{n+2}+1}{3{\cdot}2^{n+1}} && \text{rearranging}\\
&= \frac{2^{((n+1)+1)+1}+1}{3{\cdot}2^{n+1}} && \text{rearranging}\\
&= \frac{2^{((n+1)+1)+1}+(-1)^{n+2}}{3{\cdot}2^{n+1}} && \text{since } n \text{ is odd (and } n{+}1 \text{ is even)}
\end{aligned}$$

  and hence $P(n{+}1)$ holds in this case.

Since these are the only cases to consider we have proved $P(n{+}1)$ holds.

Therefore by the principle of induction we have proved that $P(n)$ holds for all $n \in \mathbb{N}$.

Algorithmic Foundations 2 - Tutorial Sheet 7

Counting

---

1. Suppose that a password is of length between 6 and 8 characters, consists of letters and digits, and is case-sensitive.

   (a) How many distinct passwords are there?

   Solution: There are (26+26+10=)62 possible characters in each position of the password, therefore using both the product and sum rules we have a total of:

   $$\begin{aligned} 62^6 + 62^7 + 62^8 &= 56,800,235,584 + 3,521,614,606,208 + 218,340,105,584,896 \\ &= 7221,918,520,426,688 \end{aligned}$$

   (b) How many contain at least one letter and at least one digit?

   Solution: We need to exclude all passwords containing only letters and those containing only digits, this gives a total of

   $$\begin{aligned} &62^6 + 62^7 + 62^8 - (52^6 + 52^7 + 52^8) - (10^6 + 10^7 + 10^8) \\ &= 221,918,520,426,688 - 54,507,570,843,648 - 111,000,000 \\ &= 167,410,838,583,040 \end{aligned}$$

   (c) How long would it take a hacker to test all passwords at 2.8×10^9 tests per second?

   Solution: The seconds required equals $7221,918,520,426,688/(2.8 \times 10^9)$ which is approximately $79,256$ which yields $1,320$ minutes or alternatively 22 hours.

2. How many one-one functions are there from a set with 5 elements to a set with the following number of elements:

   (a) 4

   Solution: 0 since size of domain is larger than size of codomain.

   (b) 5

   Solution: 120 (5 choices for first value in domain; 4 choices for second value in domain,. . . ,1 choice for fifth value in domain, so $5! = 120$ different functions by the product rule).

   (c) 6

   Solution: 720 (6 choices for first value in domain; 5 choices for second value in domain,. . . ,2 choices for fifth value in domain, so $6{\cdot}5{\cdot}4{\cdot}3{\cdot}2 = 720$ different functions by the product rule).

(d) 7

> **Solution:** 2,520 (7 choices for first value in domain; 6 choices for second value in domain,...,3 choices for fifth value in domain, so $7{\cdot}6{\cdot}5{\cdot}4{\cdot}3 = 2520$ different functions by the product rule).

3. How many bit strings of length seven either begin with two 0's or end with three 1's?

> **Solution:** There are $2^5 = 32$ bit strings which begin with two 0's (two choices for each of the five remaining positions). There are $2^4 = 16$ bit strings which end with three 1's (two choices for each of the four remaining positions). There are $2^2 = 4$ bit strings which begin with two 0's and end with three 1's (two choices for each of the two remaining positions). Hence by the Principle of Inclusion-Exclusion, the number of bit strings of length seven which either begin with two 0's or end with three 1's is $32 + 16 - 4 = 44$.

4. How many bit strings of length eight either start with two 1's, or end with two 1's, or have four 1's in the middle four places?

> **Solution:** Let A be the set of bit strings starting with two 1's, B the set ending with two 1's, and C the set with four 1's in the middle four places. Now we have:
>
> $$\begin{aligned} |A| = |B| &= 2^6 = 64 \\ |C| &= 2^4 = 16 \\ |A \cap B| &= 2^4 = 16 \\ |A \cap C| = |B \cap C| &= 2^2 = 4 \\ |A \cap B \cap C| &= 2^0 = 1 \end{aligned}$$
>
> So, applying the Inclusion-Exclusion Principle, we have:
>
> $$\begin{aligned} |A \cup B \cup C| &= |A| + |B \cup C| - |A \cap (B \cup C)| \\ &= |A| + |B| + |C| - |B \cap C| - |A \cap (B \cup C)| && \text{Inclusion-Exclusion Principle} \\ &= |A| + |B| + |C| - |B \cap C| - |(A \cap B) \cup (A \cap C)| && \text{distributivity} \\ &= |A| + |B| + |C| - |B \cap C| - (|A \cap B| + |A \cap C| - |A \cap B \cap C|) && \text{set counting rule} \\ &= 64 + 64 + 16 - 4 - (16 + 4 - 1) && \text{from above} \\ &= 121 \end{aligned}$$

5. How many bit strings of length ten have:

(a) exactly three 0's?

> **Solution:** There are $C(10, 3) = 120$ bit strings, since there are $C(10, 3)$ ways to choose the positions for the three 0's, and that is the only choice to be made (all other positions take value 1).

(b) the same number of 0's as 1's?

Solution: There are $C(10,5) = 252$ bit strings, since there are $C(10,5)$ ways to choose the positions for the five 0's, and that is the only choice to be made (all other positions take value 1).

(c) at least seven 1's?

Solution: In this case we need to count the number of bit strings with exactly seven, eight, nine and ten 1's. By the same reasoning as above, the number of such strings is $C(10,7) + C(10,8) + C(10,9) + C(10,10) = 120 + 45 + 10 + 1 = 176$.

(d) at least three 1's?

Solution: It is easier to count the number of bit strings containing fewer than three 1's and then subtract this number from the total number of bit strings. To contain fewer than three 1's, there must be either precisely 0, 1 or 2, yielding the total $C(10,0) + C(10,1) + C(10,2) = 1 + 10 + 45 = 56$. Therefore, since the total number of bit strings is $2^{10} = 1,024$, we have $1,024 - 56 = 968$ bit strings have at least three 1's.

6. How many bit strings contain exactly five 0's and fourteen 1's if every 0 must be immediately followed by two 1's?

Solution: We need two 1's to be to the right of each 0 so we need five copies of 011, this gives ten 1's in the string so we need another four 1's. To calculate the number of strings we need to find the number of ways of rearranging the four 1's and five copies of 011. More precisely, we have 9 objects of which the four 1's and and the five 011's are instinguishable, therefore we have:

$$\frac{9!}{4!5!} = \frac{9{\cdot}8{\cdot}7{\cdot}6}{4{\cdot}3{\cdot}2{\cdot}1} = 9{\cdot}7{\cdot}2 = 126\,.$$

7. A lottery ticket consists of six distinct numbers in the range 1-49.

(a) What are the chances of having exactly four of the winning numbers?

Solution: There are $C(6,4) = 15$ ways of choosing four of the winning numbers, and $C(43,2) = 903$ ways of choosing two losing numbers, giving $15{\cdot}903 = 13,545$ ways of having exactly four winning numbers. The odds are $13,545$ in $C(49,6) = 13,983,816$, that is around 1 in $1,032$.

(b) Exactly three of the winning numbers?

Solution: There are $C(6,3) = 20$ ways of choosing three of the winning numbers, and $C(43,3) = 12,341$ ways of choosing three losing numbers. So, there are $20{\times}12341 = 2,468,20$ ways of choosing exactly three winning numbers and three losing numbers (about 1 in 57).

(c) Is it more likely to have at least one of the winning numbers, or none of them?

Solution: There are $C(43,6) = 6,096,454$ ways of choosing no winning numbers. This is less than half $C(49,6) = 13,983,816$, so it is more likely to have at least one winning number than none.

8. In a substitution cipher, a one-to-one mapping is given from the alphabet to itself, and each letter is replaced by its image under this mapping. For example, a simple "rotate 13" cipher maps each letter to the letter in it's position plus 13 (modulo 26); i.e., $a \mapsto n$, $b \mapsto m$, ..., $m \mapsto z$,$n \mapsto a$, ..., $z \mapsto m$. This particular cipher encodes the message "hello" as "uryyb".

   (a) How many substitution ciphers are there?

   Solution: This is the number of permutations of the alphabet:

   $$26! = 403,291,461,126,605,635,584,000,000$$

   (b) If 10^{10} checks per second are performed, how long would it take to test all substitution ciphers?

   Solution: Checking them all would take around 1.3 billion years.

9. A bowl contains 10 red balls and 10 blue balls. A student selects balls at random without looking at them.

   (a) How many balls must be selected to be sure of having at least three balls of the same colour?

   Solution: Let there be two containers (pigeonholes) representing the colours red and blue. We want to calculate the fewest number of objects (balls) needed to ensure that at least one of the containers contains 3 objects. By the Generalised Pigeonhole Principle, we need the smallest n such that $\texttt{ceil}(n/2) = 3$, and hence 5 balls are required.

   (b) How many balls must be selected to be sure of having at least three blue balls?

   Solution: One needs to select 13 balls in order to ensure that there are at least three blue ones. Essentially, since there are a total of 10 red balls, if 12 or fewer balls are selected, then 10 can be red meaning two or less may be blue.
   Notice that the number of each colour was relevant here but not in part (a).

10. A palindrome is a string that reads the same forwards as backwards; for example,"hannah" and "minim". How many bit strings of length n are palindromes?

    Solution: If n is even, each of the first $n/2$ bits can be chosen in two ways, and the remaining bits are then all fixed. This gives $2^{n/2}$ possibilities.

    If n is odd, then each of the first $(n-1)/2+1 = (n+1)/2$ bits can be chosen in two ways, and the remaining bits are then all fixed. This gives $2^{(n+1)/2}$ possibilities.

11. The staff of a Computing Science department comprises fifteen women and ten men. How many ways are there to select a committee of six members of staff so that:

(a) At least one woman must be on the committee?

> **Solution:** There are $C(25,6) = 177,100$ ways of choosing the committee if there are no restrictions on membership and there are $C(10,6) = 210$ ways of choosing the committee if no women serve on the committee. Therefore there are $177,100 - 210 = 176,890$ ways of choosing the committee if at least one woman must serve on the committee.

(b) At least one woman and at least one man must be on the committee?

> **Solution:** Using part (a), there are $177,100$ ways of choosing the committee if there are no restrictions on membership and 210 ways of choosing the committee if no women serve on the committee. Furthermore, there are $C(15,6) = 5,005$ ways of choosing the committee if no men serve on the committee. Since the cases where no women and no men do not overlap, there are $177,100 - (210 + 5,005) = 17,1885$ ways of choosing the committee if at least one man and at least one woman must serve on the committee.

(c) The numbers of men and women are equal?

> **Solution:** There are $C(10,3) = 120$ ways to choose the 3 men, and there are $C(15,3) = 455$ ways to choose the 3 women. Hence by the product rule, the number of ways of choosing the committee is $120 \cdot 455 = 54,600$ if the numbers of men and women are to be equal.

(d) There are more women than men?

> **Solution:** There are the following three cases for have more women than men: (i) 6 women and 0 men; (ii) 5 women and 1 man and (iii) 4 women and 2 men. Using the product rule, the number of ways of forming a committee according to cases (i),(ii) and (iii) are $C(15,6) \cdot C(10,0) = 5,005$, $C(15,5) \cdot C(10,1) = 30,030$ and $C(15,4) \cdot C(10,2) = 61,425$ respectively. Since the cases are disjoint, using the sum rule, the total number of ways of choosing the committee such that the number of women is more than the number of men is $5,005+30,030+61,425 = 96460$.

12. A department teaches three courses, each with two lectures per week. There are six timetable slots set aside in the week for these lectures.

(a) How many different ways can the lectures be distributed among the slots?

> **Solution:** Call the lecture courses A, B and C. Filling the slots involves forming a permutation of the string $AABBCC$, of which there are $6!/(2! \cdot 2! \cdot 2!) = 720/8 = 90$ ways.

(b) At least one of the courses has consecutive slots?

> **Solution:** If the slots for A are consecutive, then we can treat AA as a single symbol (say X) and therefore the number of ways the lectures can be distributed with A consecutive is the number of permutations of $XBBCC$ and there are $5!/(2! \cdot 2!) = 120/4 = 30$ of these. Similarly, there are 30 ways of having B or C consecutive.
>
> However, we need to also consider the cases when two or more courses are consecutive. If two courses are consecutive, then there are $4!/2! = 12$ ways (e.g. permutations

of $XYCC$). If all courses are consecutive, there are $3! = 6$ ways (permutations of XYZ).
Letting S_A, S_B and S_B be the ways of having the lectures A, B and C consecutive respectively, by the Inclusion-Exclusion Principle:

$$\begin{aligned}|S_A \cup S_B \cup S_C| &= |S_A| + |S_B| + |S_C| - |S_A \cap S_B| - |S_A \cap S_B| - |S_B \cap S_C| + |S_A \cap S_B \cap S_C| \\ &= 30 + 30 + 30 - 12 - 12 - 12 + 6 \\ &= 60\end{aligned}$$

Therefore there are 60 allocations in which at least one of the courses occupies consecutive slots.

(c) What is the answer if no course is to have both lectures in consecutive slots?

Solution: Using the answers to parts (a) and (b), the number of solutions in which none of the lectures are in consecutive slots is $90 - 60 = 30$.

13. Consider the letters of the word '*success*'.

(a) How many permutations are there in which the two 'c' characters are not consecutive?

Solution: There are seven letters, which suggests $7! = 5,040$ permutations. However, these 5,040 permutations include identical rearrangments of letters 's' and 'c'. There are $3! = 6$ ways of rearranging the three 's' characters, and $2! = 2$ ways of rearranging 'c' characters. So, altogether there are $5040/(6!{\cdot}2!) = 420$ distinct permutations.
We can find the number of permutations in which the two 'c' characters are consecutive by considering the two 'c' characters together as a single character. That gives $6!/3! = 120$ distinct permutations in which two 'c' characters are consecutive, and therefore $420 - 120 = 300$ permutations in which the two 'c' characters are not consecutive.

(b) How many of the permutations in which the two 'c' characters are not consecutive and also do not have not all three of the 's' characters consecutive?

Solution: Let A be the set of permutations in which the two 'c' characters are consecutive, and B the set in which the three 's' characters are consecutive. Imagine the 'c' or 's' characters are "glued together" (so that choosing the first 'c' is actually choosing 'cc', and choosing the first 's' is actually choosing 'sss'). We thus have $|A| = 6!/3! = 120$ distinct permutations involving 'cc', $|B| = 5!/2! = 60$ distinct permutations involving 'sss', and $|A \cap B| = 4! = 24$.
By the Inclusion-Exclusion Principle, $|A \cup B| = |A| + |B| - |A \cap B| = 120 + 60 - 24 = 156$. However, we want the complement of this set, and hence the answer is $420 - 156 = 264$ (using the fact that from (a) there are 420 permutations of '*success*').

14. (a) How many sets are there containing five letters of the alphabet?

Solution: The number of sets is $C(26, 5) = 65,780$.

(b) How many bags (sets in which duplicates are permitted) are there containing five letters of the alphabet?

Solution: Calculating the number of bags requires counting combinations with repetition. You can think of combinations with repetition as a loop which at each iteration either selects a letter or moves on to consider the next letter. Zero or more selections can occur between each move. If we write 's' for "select" and '.' for "move", each execution of the loop is a sequence of the form "$s.s.ss..s$....." (there are 25 '.' because the loop starts on the letter 'a', and only has to advance 25 times to get to 'z'). This is the same as saying there are 5+25 items of which you get to choose five; i.e. $C(30, 5) = 142,506$.

Difficult/challenging questions.

15. There are 51 houses on a particular block of a street. Each house in this block has an address between 100 and 199. Show that at least two houses in this block have addresses that are consecutive integers.

Solution: Let $a_1, a_2, \ldots, a_{51}$ denote the house numbers in increasing order, so that $100 \leq a_i < a_j \leq 199$ for $1 \leq i < j \leq 51$. Now let $b_1, b_2, \ldots, b_{51}$ be an increasing sequence of integers such that $b_i = a_i + 1$ for $1 \leq i \leq 51$. Then the sequence

$$a_1, a_2, \ldots, a_{51}, b_1, b_2, \ldots, b_{51}$$

contains 102 values in the range $[100, 200]$. However, the range $[100, 200]$ contains only 101 integers. Hence by the pigeonhole principle, at least two of the values in the sequence are equal. Since by construction $a_i \neq a_j$ for $1 \leq i < j \leq 51$ and $b_i \neq b_j$ for $1 \leq i < j \leq 51$, it follows that $a_i = b_j$ for some i and j, and hence by definition of b_j we have $a_i = a_j + 1$. Thus there are two houses with consecutive numbers.

16. Prove that, at a party where there are at least two people, there are two people who each know the same number of other people there. (Assume that if person x knows person y, then y knows x.)

Solution: Let $K(x)$ denote the number of other people that person x knows. Therefore $0 \leq K(x) \leq n-1$. Now it is impossible for both 0 and $n-1$ to be in the domain of K. For, if somebody knows everybody, then it cannot be the case that somebody knows nobody (recall that if x knows y then y knows x). Hence the range of K has at most $n - 1$ elements. Since the domain of K has n elements, then the pigeonhole principle tells us that at least two elements in the domain map to the same integer in the codomain. That is, there are two people at the party who each know the same number of other people there.

17. Suppose there are 12 students in a tutorial group. In how many different ways can the 12 students be split into six pairs?

Solution: There are $12! = 479,001,600$ permutations of 12 students. Once permuted, the pairs can be read off, student1 with student2, student3 with student4, etc. For a given permutation, we need to know the number of ways it can be rearranged so the pairing outcome is the same. First, each pair can be reversed, giving $2^6 = 64$ possibilities. Next, each of the six pairings can be permuted in $6! = 720$ different ways. Each of these two rearrangements is independent, giving $64 \cdot 6!$.

The overall answer is therefore $12!/(64 \cdot 6!) = 10,395$.

Algorithmic Foundations 2 - Tutorial Sheet 8

Probability (and more Counting)

---

1. In roulette there is a wheel with 38 numbers of these 18 are red and 18 are black. The other two numbers are 0 and 00 which are neither red nor black. The probability that when the wheel is spun it lands an a particular number is 1/38.

   (a) What is the probability the wheel lands on a red number?

   > **Solution:** Since 18 numbers are red out of a total of 38, the probability is $18/38 = 9/19$.

   (b) What is the probability the wheel lands on a black number twice in a row?

   > **Solution:** Using the product rule there are $38{\cdot}38 = 1,444$ equally likely outcomes for two spins. Of these, again using the product rule $18{\cdot}18 = 182$ are a pair of black numbers. Therefore the probability is $182/1,444 = 91/722$.

   (c) What is the probability the wheel lands on 0 or 00?

   > **Solution:** There are 2 outcomes out of the 38 equally possible, therefore the probability is $2/38 = 1/19$.

   (d) What is the probability in five spins the wheel neither lands on 0 nor 00?

   > **Solution:** Using the product rule there are $38{\cdot}38{\cdot}38{\cdot}38{\cdot}38 = 79,235,168$ outcomes for five spins. Since 36 outcomes on each spin are neither 0 no 00, there are $36{\cdot}36{\cdot}36{\cdot}36{\cdot}36 = 60,466,176$ outcomes that meet the requirement considered. Therefore the probability is $60,466,176/79,235,168 = 1,889,568/2,476,099$.

   (e) What is the probability the wheel lands on one of the first six integers on one spin, but does not land on any of them on the next spin?

   > **Solution:** In this case the total number of outcomes is $38{\cdot}38 = 1,444$ using the product rule. Using the product rule again there are $6{\cdot}(38-6) = 192$ outcomes that meet the specification. Therefore the probability is $192/1,444 = 48/361$.

2. For each of the following pairs of events determine there probabilities and if they are independent or not when a coin is tossed three times.

   (a) E_1: the first coin comes up `tails`.
   E_2: the second coin comes up `heads`.

   > **Solution:** The total number of outcomes are, using the product rule, $2{\cdot}2{\cdot}2 = 2^3$ and each is equally likely (we will also use this result in the other parts to the question). Using the product rule again we have:
   >
   > - there are $1{\cdot}2{\cdot}2 = 2^2$ outcomes in E_1;
   > - there are $2{\cdot}1{\cdot}2 = 2^2$ outcomes in E_2;

- there are $1{\cdot}1{\cdot}2 = 2$ outcomes in $E_1 \cap E_2$.

These events are independent since $\mathbf{P}[E_1] = \mathbf{P}[E_2] = 2^2/2^3 = 1/2$ and $\mathbf{P}[E_1 \cap E_2] = 2/2^3 = 1/2^2 = (1/2){\cdot}‘(1/2)$.

(b) E_3: the first coin comes up `tails`.
E_4: precisely two `heads` in a row.

Solution: Using the product and sum rules:

- there are $1{\cdot}2{\cdot}2 = 2^2$ outcomes in E_3;
- there are $1{\cdot}1{\cdot}1 + 1{\cdot}1{\cdot}1 = 2$ outcomes in E_4;
- there are $1{\cdot}1{\cdot}1 = 1$ outcomes in $E_3 \cap E_4$.

These events are independent since $\mathbf{P}[E_3] = 2^2/2^3 = 1/2$, $\mathbf{P}[E_4] = 2/2^3 = 1/4$ and $\mathbf{P}[E_3 \cap E_4] = (1/2)^3 = 1/8 = (1/2){\cdot}(1/4)$.

(c) E_5: the second coin comes up `tails`.
E_6: precisely two `heads` in a row.

Solution: Using the product rule:

- there are $2{\cdot}1{\cdot}2 = 2^2$ outcomes in E_5;
- there are $21{\cdot}1{\cdot}1 + 1{\cdot}1{\cdot}1 = 2$ outcomes in E_6;
- there are 0 outcomes in $E_5 \cap E_6$.

These events are dependent since $\mathbf{P}[E_5] = 2^2/2^3 = 1/2$ and $\mathbf{P}[E_6] = 2/2^3 = 1/4$ $\mathbf{P}[E_3 \cap E_4] = (1/2)^3 = 0 \neq (1/2){\cdot}(1/4)$.

3. What probabilities should be assigned to the outcomes of a biased coin if the probability of heads equals four times the probability of tails.

Solution: The requirement is $\mathbf{P}[\texttt{heads}] = 4{\cdot}\mathbf{P}[\texttt{tails}]$. From the first and third axiom of probability it follows that $\mathbf{P}[\texttt{heads}] + \mathbf{P}[\texttt{tail}] = 1$. Solving these simultaneous equations we have $\mathbf{P}[\texttt{heads}] = 1/5$ and $\mathbf{P}[\texttt{tails}] = 4/5$.

4. What is the conditional probability that a randomly generated bit string of length four contain at least two consecutive `0`'s, given that the first bit is a `1`?

Solution: Let A be the event that the string contain at least two consecutive `0`'s and B the event that the first bit is a `1`. There are 2^4 outcomes in total, the number satisfying B is 2^3 and therefore $\mathbf{P}[B] = 1/2$, and the number satisfying $A \cap B$ is 3 (the bit strings `1000`, `1100`, `1001`) and therefore $\mathbf{P}[A \cap B] = 3/16$. By the definition of conditional probability:

$$\mathbf{P}[A \mid B] = \frac{\mathbf{P}[A \cap B]}{\mathbf{P}[B]} = \frac{3/16}{1/2} = 3/8\,.$$

5. A *Bernoulli trial* is an experiment which can have only two possible outcomes (denoted *success* and *failure*).

   Find each of the probabilities when n independent Bernoulli trials are carried out, each with a probability of success equal to p.

   (a) The probability of no successes.

   > **Solution:** Using the fact that the experiments are independent, the probability equals $(1-p)^n$.

   (b) The probability of at least one success.

   > **Solution:** Using the result from part (a), the probability of at least one success equals $1-(1-p)^n$.

   (c) The probability of at most one success.

   > **Solution:** At most one success means one of the n is a success and all others are failures or all are failures. In the first case, since there are n trials, there are n different positions the success can be in, and therefore, using fact the experiments are independent, the probability equals $n\cdot(p\cdot(1-p)^{n-1})$. In the second case this is just probability $(1-p)^n$. Since these two events are mutually exclusive we an add the probabilities to give the result:
   >
   > $$(1-p)^n + n\cdot(p\cdot(1-p)^{n-1})$$

   (d) The probability of precisely two successes.

   > **Solution:** The number of outcomes with precisely two successes is all the permutations of two `s`'s, and $n-2$ `f`'s where the `s`'s and the `f`'s are indistinguishable. Furthermore, since the experiments are independent, each of these outcomes has probability $p^2\cdot(1-p)^{n-2}$. Finally, since the outcomes are mutually exclusive, using axiom 3 the probability equals:
   >
   > $$n!/((n-2)!\cdot 2!)\cdot p^2\cdot(1-p)^{n-2} = (n\cdot(n-1))/2\cdot p^2\cdot(1-p)^{n-2}\,.$$

   (e) The probability of at least two successes.

   > **Solution:** Here it is easier to compute the complement and then subtract this probability from 1. The complement is at most one success, i.e. part (c), and therefore the probability of at least two successes equals:
   >
   > $$1-\left((1-p)^n + n\cdot(p\cdot(1-p)^{n-1})\right).$$

6. Suppose there are two boxes of balls, the first box contains two white balls and three blue balls, while the second contains four white and one blue ball.

   Suppose you choose a box at random and then select a ball from that box at random, what is the probability that a ball from the first box was chosen, given you selected a blue ball.

Solution: Let A_i be the event choose the ith box and B a blue ball is chosen. We want to find $\mathbf{P}[A_1 \mid B]$. Clearly $\mathbf{P}[A_i] = 1/2$ for $1 \leq i \leq 2$, $\mathbf{P}[B \mid A_1] = 3/5$ and $\mathbf{P}[B \mid A_2] = 1/5$. Now since $\mathbf{P}[A_1] + \mathbf{P}[A_2] = 1$, using Bayes' law we have:

$$\mathbf{P}[A_1 \mid B] = \frac{\mathbf{P}[B \mid A_1]\mathbf{P}[A_1]}{\mathbf{P}[B \mid A_1]\mathbf{P}[A_1] + \mathbf{P}[B \mid A_2]\mathbf{P}[A_2]} = \frac{3/10}{3/10 + 1/10} = \frac{3/10}{4/10} = \frac{3}{4}\,.$$

7. Given three cards where:

   - the first is red on each side;
   - the second is green on each side;
   - and the third is red on one side and green on the other.

   If we draw one card at random and look at one side only, what is the probability that given the side we are looking at is green that the other side is also green?

Solution: This is a conditional probability, let G_1 be the side we are looking at is green and G_2 the other side is green. There are 6 sides and 3 are green, therefore the probability the other side of a card we are looking at is green equals $1/2$. Alternatively, if you think you look at a side with equal chance, then you can use the law of total probability:

$$\begin{aligned}
&\mathbf{P}[G_2 \mid \mathit{card}_1] + \mathbf{P}[G_2 \mid \mathit{card}_2] + \mathbf{P}[G_2 \mid \mathit{card}_3] \\
&= \mathbf{P}[G_2 \cup \mathit{card}_1]\mathbf{P}[\mathit{card}_1] + \mathbf{P}[G_2 \cup \mathit{card}_2]\mathbf{P}[\mathit{card}_1] + \mathbf{P}[G_2 \cup \mathit{card}_3]\mathbf{P}[\mathit{card}_1] \\
&= 0{\cdot}(1/3) + 1{\cdot}(1/3) + (1/2){\cdot}(1/3) = 1/3 + 1/6 = 1/2\,.
\end{aligned}$$

The probability we choose a card which is green on both side ($G_1 \cap G_2$) equals $1/3$, i.e. the probability you choose the second card. Therefore by definition of conditional probability we have:

$$\mathbf{P}[G_1 \mid G_2] = \frac{\mathbf{P}[G_1 \cap G_2]}{\mathbf{P}[G_2]} = \frac{1/3}{1/2} = \frac{2}{3}\,.$$

8. Suppose a test for opioids use has a 2% false positive rate and a 5% false negative rate. (More precisely, 2% of people who have not taken opioids test positive and 5% of people who have taken opioids test negative.) Assume that 1% of people have taken opioids.

   (a) Find the probability that someone who tests negative for opioids has not taken opioids.

Solution: Let O and $\neg O$ be the events have and have not taken opioids, while P and N the events testing positive and negative. Clearly we have $\mathbf{P}[O] + \mathbf{P}[\neg O] = 0.01 + 0.99 = 1$. Therefore using Bayes' theorem we have:

$$\begin{aligned}
\mathbf{P}[\neg O \mid N] &= \frac{\mathbf{P}[N \mid \neg O]\mathbf{P}[\neg O]}{\mathbf{P}[N \mid \neg O]\mathbf{P}[\neg O] + \mathbf{P}[N \mid O]\mathbf{P}[O]} \\
&= \frac{0.98{\cdot}0.99}{0.98{\cdot}0.99 + 0.05{\cdot}0.01} = \frac{0.9702}{0.9707} = 0.9995\,.
\end{aligned}$$

   (b) Find the probability that someone who tests positive for opioids has actually taken opioids.

Solution: Using the notation from the first part and applying Bayes' law:

$$\begin{aligned}\mathbf{P}[O \mid P] &= \frac{\mathbf{P}[P \mid O]\mathbf{P}[O]}{\mathbf{P}[P \mid O]\mathbf{P}[O] + \mathbf{P}[P \mid \neg O]\mathbf{P}[\neg O]} \\ &= \frac{0.95{\cdot}0.01}{0.95{\cdot}0.01 + 0.02{\cdot}0.99} = \frac{0.0095}{0.0293} = 0.3242\,.\end{aligned}$$

9. A box contains 3 yellow balls and 5 red balls. A ball is chosen at random from the box, then replaced in the box along with two other balls of the same colour.
   (a) If a second ball is now chosen at random from the box, what is the probability that it will be red?

Solution: The second ball is dependent on the choice of the first so let R_i and Y_i be the event the ith ball is red and yellow respectively. We have:

$$\begin{aligned}\mathbf{P}[R_2] &= \mathbf{P}[R_2 \cap R_1] + \mathbf{P}[R_2 \cap Y_1] \\ &= (5/8){\cdot}(7/10) + (3/8){\cdot}(5/10) = 50/80 = 5/8\,.\end{aligned}$$

   (b) Given that the second ball is red, what is the probability that the first ball was yellow?

Solution: Using Bayes' law we have:

$$\mathbf{P}[Y_1 \mid R_2] = \frac{\mathbf{P}[R_2 \mid Y_1]\mathbf{P}[Y_1]}{\mathbf{P}[R_2]} = \frac{\mathbf{P}[R_2 \cap Y_1]}{\mathbf{P}[R_2]} = \frac{(3/8){\cdot}(5/10)}{5/8} = 3/10\,.$$

10. An *octahedral die* has eight faces that are number 1 to 8. What are the expected value and the variance when a fair octahedral die is rolled.

Solution: The expected value is given by

$$\mathbf{E}[X] = \sum_{i=1}^{8}(i{\cdot}(1/8)) = (1/8)\cdot\left(\sum_{i=1}^{8} i\right) = (1/8)\cdot(8{\cdot}9/2) = 9/2$$

On the other hand the variance is given by:

$$\begin{aligned}\mathbf{V}[X] &= \sum_{i=1}^{8}((i-9/2)^2{\cdot}(1/8)) \\ &= (1/8)\cdot\left(\sum_{i=1}^{8}(i-9/2)^2\right) \\ &= (1/8)\cdot\left(\sum_{i=1}^{8}(i^2 - 9{\cdot}i + 81/4\right) \\ &= (1/8)\cdot\left(\sum_{i=1}^{8} i^2\right) - 9{\cdot}\left(\sum_{i=1}^{8} i\right) + 81/4{\cdot}\left(\sum_{i=1}^{8} 1\right) \\ &= (1/8){\cdot}((8{\cdot}9{\cdot}17)/6 - 9{\cdot}((8{\cdot}9)/2) + 8{\cdot}(81/4)) \\ &= 5.25\end{aligned}$$

where final steps follow from the following results you can/have proved by induction. For any $n \in \mathbb{Z}$:

$$\sum_{i=1}^{n} i^2 = \frac{n{\cdot}(n{+}1){\cdot}(2{\cdot}n{+}1)}{6}\,, \qquad \sum_{i=1}^{n} i = \frac{n{\cdot}(n{+}1)}{2} \qquad \text{and} \qquad \sum_{i=1}^{n} 1 = n\,.$$

Difficult/challenging questions.

11. Both undergraduates and postgraduates can use the university cafeteria. Each diner can choose between buying a meal or bringing a packed lunch. (Everyone has exactly one meal each, no more and no less). The cafeteria offers a daily choice between a hot meal or a cold meal. A survey of undergraduate diners finds that 40% of them bring their own food. Overall, only 25% of the diners bring their own food. Postgraduates make up one fifth of the diners in the cafeteria.

    (a) What is the probability that a diner is an undergraduate and buys a meal?

    Solution: From the assumptions it follows that the probability an undergraduate buy lunch is 0.6 and the probability a student is an undergraduate is 0.8. Therefore we have:

    $$\begin{aligned} \mathbf{P}[\mathit{buys} \cap \mathit{undergrad}] &= \mathbf{P}[\mathit{buys} \mid \mathit{undergrad}] \cdot \mathbf{P}[\mathit{undergrad}] \\ &= 0.6{\cdot}0.8 = 0.48\,. \end{aligned}$$

    (b) What is the probability that someone that buys a meal is a postgraduate?

    Solution: First using the definition of conditional probabilities:

    $$\mathbf{P}[\mathit{postgrad} \mid \mathit{buys}] = \frac{\mathbf{P}[\mathit{postgrad} \cup \mathit{buys}]}{\mathbf{P}[\mathit{buys}]}\,.$$

    However we do not currently have a value for $\mathbf{P}[\mathit{postgrad} \cap \mathit{buys}]$. Using the law of total probability:

    $$\mathbf{P}[\mathit{buys}] = \mathbf{P}[\mathit{postgrad} \cap \mathit{buys}] + \mathbf{P}[\mathit{undergrad} \cap \mathit{buys}]$$

    So rearranging we have

    $$\begin{aligned} \mathbf{P}[\mathit{postgrad} \cap \mathit{buys}] &= \mathbf{P}[\mathit{buys}] - \mathbf{P}[\mathit{undergrad} \cap \mathit{buys}] \\ &= 0.75 - 0.48 \qquad \text{(using the answer to part (a) and the assumptions)} \\ &= 0.27 \end{aligned}$$

    and hence using the expression above for the conditional probability:

    $$\mathbf{P}[\mathit{postgrad} \mid \mathit{buys}] = \frac{0.27}{0.75} = 0.36$$

12. The *Birthday Problem* asks what is the minimum number of people who need to be in a room so the probability at least two people have the same birthday is greater than 1/2.

    Find this number under the assumption that the birthdays of the people in the room are independent, each birthday is equally likely and the number of days in a year is 366.

    Solution: Here it is easier to calculate the complement probability, i.e. that all people have different birthdays and then find the actual probability by subtracting this probability from 1. We can consider one person at a time, the first can have any birthday, then the second must have a different birthday (i.e. from the remaining 365 days), then the third again must have a different birthday (i.e. from the remaining 364) and so on (so the nth must have a birthday from the remaining $366-(n-1)$ days). Using the fact that the birthdays of people are independent yields the probability p_n for at least two out of n people having the same birthday:

    $$p_n = 1 - \frac{366}{366}\cdot\frac{365}{366}\cdots\frac{366-(n-2)}{366}\cdot\frac{366-(n-1)}{366}\,.$$

    After some trial and error we find $p_{22} < 0.5$ and $p_{23} > 0.5$.

13. A space probe near Neptune communicates with Earth using bit strings. Suppose that in its transmissions it sends `1`'s one-third of the time and `0`'s the remaining two thirds. When a `0` is sent, the probability that a `0` is received is 0.9 (and a `1` is received with probability 0.1). On the other hand, when a `1` is sent, the probability that a `1` is received is 0.8 (and a `0` is received with probability 0.2).

    (a) What is the probability that a `0` is received.

    Solution: Let T_i and R_i be the events of transmitting and receiving a `i` respectively. Using the law of total probability:

    $$\mathbf{P}[R_0] = \mathbf{P}[R_0 \mid T_0]\mathbf{P}[T_0] + \mathbf{P}[R_0 \mid T_1]\mathbf{P}[T_1] = 9/10{\cdot}2/3 + 2/10{\cdot}1/3 = 20/30 = 2/3\,.$$

    (b) What is the probability that a `0` was transmitted given that a `0` was received.

    Solution: Using the notation from the first part and Bayes' law:

    $$\begin{aligned}\mathbf{P}[T_0 \mid R_0] &= \frac{\mathbf{P}[R_0 \mid T_0]\mathbf{P}[T_0]}{\mathbf{P}[R_0 \mid T_0]\mathbf{P}[T_0] + \mathbf{P}[R_0 \mid T_1]\mathbf{P}[T_1]} \\ &= \frac{(9/10){\cdot}(2/3)}{(9/10){\cdot}(2/3) + (2/10){\cdot}(1/3)} = \frac{3/5}{18/30 + 2/30} = \frac{3/5}{20/30} = \frac{9}{10}\,.\end{aligned}$$

Algorithmic Foundations 2 - Tutorial Sheet 9

Graphs and Relations

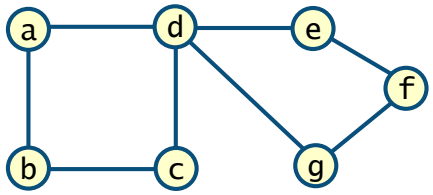
---

1. Consider the following graph:

$$G = (\{a, b, c, d, e, f, g\}, \{\{a, b\}, \{b, c\}, \{c, d\}, \{a, d\}, \{d, g\}, \{d, e\}, \{f, g\}, \{e, f\}\})$$

(a) Draw the graph

Solution:



(b) Is the graph G connected?

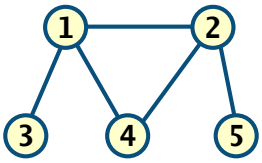
Solution: The graph is connected, i.e. every pair of vertices is joined by a path.

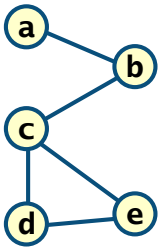
2. How many simple undirected graphs are there with 20 vertices and 60 edges?

Solution: The number of possible edges between 20 vertices is $C(20, 2)$, i.e. the number of 2-combinations from a set of size 20. This yields $20 \cdot 19/2 = 190$ different edges. For a graph to have 60 edges we need to choose 60 out of 190 possible edges i.e. an 60-combination from a set of size 190. The number of graphs therefore equals:

$$C(190, 60) = \frac{190!}{60! \cdot 130!}$$

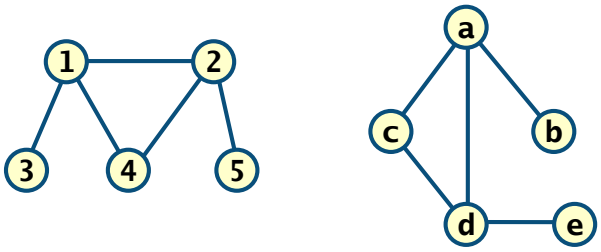
3. Decide whether or not the two graphs below are isomorphic. Explain your answer.





Solution: The graphs are not isomorphic, for example the graph on the left has two vertices with degree 3 (vertices 1 and 2), while the graph on the right has only one vertex with degree 3 (vertex c).

4. Decide whether or not the two graphs below are isomorphic. Explain your answer.



Solution: The graphs are isomorphic as demonstrated by the following bijection:

$$\begin{array}{ccc} 1 & \mapsto & d \\ 2 & \mapsto & a \\ 3 & \mapsto & e \\ 4 & \mapsto & c \\ 5 & \mapsto & b \end{array}$$

5. What is an Euler circuit?

Solution: A Euler circuitis a circuit that contains every edge, where a circuit is a path of length at least 2 that begins and ends with the same vertex.

6. What is a Hamiltonian circuit?

Solution: A Hamiltonian circuit is a circuit that visits each vertex exactly once, where a circuit is a path of length at least 2 that begins and ends with the same vertex.

7. Determine whether each of the following binary relations is
   - reflexive;
   - symmetric;
   - anti-symmetric;
   - transitive.

   (a) The relation R_1 over $\mathbb{N}\times\mathbb{N}$ where $(a, b) \in R_1$ if and only if $a|b$.

   Solution:
   - R_1 is reflexive since $a|a$ for any $a \in \mathbb{N}$;
   - R_1 is not symmetric since, for example $1|2$ while 2 does not divide 1;
   - R_1 is anti-symmetric since, for any $a, b \in \mathbb{N}$, if $a|b$ and $b|a$, then $a{=}b$;

- R_1 is transitive since if $a|b$ and $b|c$ for any $a, b, c \in \mathbb{N}$, then $a|c$ (this was proved in the lectures).

Proof for anti-symmetric case: if $a|b$ and $b|a$ for any $a, b \in \mathbb{N}$, then $a = c_1 \cdot b$ and $b = c_2 \cdot a$ for some $c_1, c_2 \in \mathbb{N}$, and hence $a = c_1 \cdot c_2 \cdot a$ and $b = c_1 \cdot c_2 \cdot b$. Therefore, since $a, b, c_1, c_2 \in \mathbb{N}$, we have either $a = b = 0$ or $c_1 = c_2 = 1$, in either case it follows that $a = b$ as required.

(b) The relation R_2 over $S \times S$ where $S = \{w, x, y, z\}$ and

$$R_2 = \{(w, w), (w, x), (x, w), (x, x), (x, z), (y, y), (z, y), (z, z)\}.$$

Solution:

- R_2 is reflexive since $(a, a) \in R$ for all $a \in S$;
- R_2 is not symmetric, e.g. $(x, z) \in R$ while $(z, x) \notin R$;
- R_2 is not anti-symmetric, e.g. $(w, x) \in R$ and $(x, w) \in R$;
- R_2 is not transitive, e.g. $(w, x) \in R$ and $(x, z) \in R$ while $(w, z) \notin R$

(c) The relation R_3 over $\mathbb{Z} \times \mathbb{Z}$ where $(a, b) \in R_3$ if and only if $a \neq b$.

Solution:

- R_3 is not reflexive since $a = a$ for all $a \in \mathbb{R}$
- R_3 is symmetric since if $a \neq b$ for any $a, b \in \mathbb{Z}$, then $b \neq a$
- R_3 is not anti-symmetric, e.g. $1 \neq 2$ and $2 \neq 1$;
- R_3 is not transitive, e.g. $1 \neq 2$, $2 \neq 1$ and not $1 \neq 1$.

(d) The relation R_4 over $P(X) \times P(X)$ where $X = \{1, 2, 3, 4\}$ and $(S, T) \in R_4$ if and only if $S \subseteq T$.

Solution:

- R_4 is reflexive since $S \subseteq S$ for any $S \subseteq X$;
- R_4 is not symmetric e.g. $\{1\} \subseteq \{1, 2\}$ and not $\{1, 2\} \subseteq \{1\}$;
- R_4 is anti-symmetric since if $S \subseteq T$ and and $T \subseteq S$ for any $S, T \subseteq X$, then $S = T$;
- R_4 is transitive since if $S \subseteq T$ and $T \subseteq U$ for any $S, T, U \subseteq X$, then $S \subseteq U$.

(e) The relation R_5 over *People*$\times$*People* where *People* is the set of all people and $(a, b) \in R_5$ if and only if a is younger than b.

Solution:

- R_5 is not reflexive as a person is not younger than them self;

- R_5 is not symmetric as if a is younger than b, then b is not younger than a;
- R_5 is anti-symmetric if a is younger than b and b is younger than a, then $a = b$ (note that this is implication is vacuously true);
- R_5 is transitive since if a is younger than b and b is younger than c, then a is younger than c.

8. Give an example of a relation on a set that is

   (a) symmetric and anti-symmetric

   Solution: For any set A, define a relation R over $A \times A$ by $(a, b) \in R$ if and only if $a = b$, for any $a, b \in A$. Then R is symmetric and anti-symmetric.

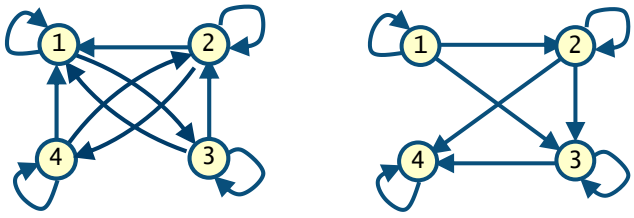
   (b) neither symmetric nor anti-symmetric

   Solution: Define a relation R over $\mathbb{Z} \times \mathbb{Z}$ by $(a, b) \in R$ if and only if $a|b$. Then R is not symmetric, e.g. choose $a = 1$ and $b = 2$. Also R is not anti-symmetric e.g. choose $a = 2$ and $b = -2$.

9. Draw the directed graph for the following relations

$$R_1 = \{(1,1),(1,3),(2,1),(2,2),(2,4),(3,1),(3,2),(3,3),(4,1),(4,2),(4,4)\}$$
$$R_2 = \{(1,1),(1,2),(1,3),(2,2),(2,3),(2,4),(3,3),(3,4),(4,4)\}$$

Solution:



10. Suppose that the relation R over $A \times A$ is reflexive. Show that R^* is reflexive.
    R^* is the transitive closure of R and is given by $R^* = \cup_{i=1}^{\infty} R^n = R \cup R^2 \cup R^3 \cup R^3 \cup \ldots$.

Solution: By construction $R \subseteq R^*$, and hence for any $a \in A$, if $(a, a) \in R$, then $(a, a) \in R^*$. The result then follows from the fact that R is reflexive.

11. If a relation R over $A \times A$ is irreflexive, then is the relation R^2 necessarily irreflexive?

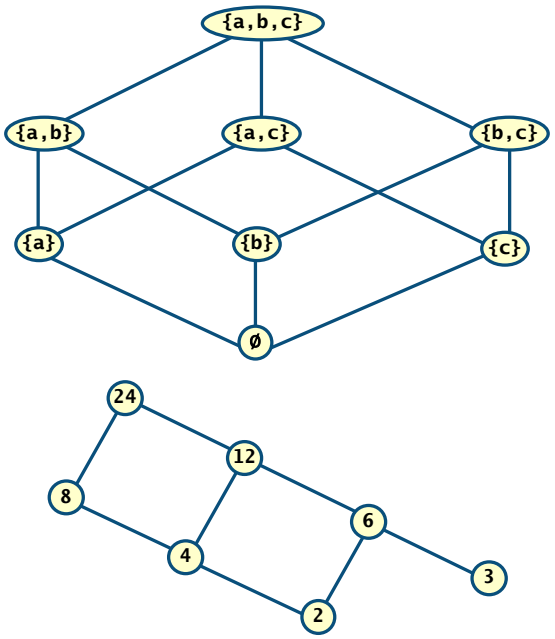
Solution: The answer is no, for example if $A = \{a, b\}$ and $R = \{(a, b), (b, a)\}$, then R is irreflexive while R^2 equals $\{(a, a), (b, b)\}$ and is therefore reflexive.

12. Consider the partially ordered sets:

- $(P(S), \subseteq)$ where $S = \{a, b, c\}$;
- $(\{2, 3, 4, 6, 8, 12, 24\}, |)$, i.e. where the relation is the divides relation.

(a) Draw a Hass diagram for each of the partially ordered sets.

Solution:



(b) State both the maximal and minimal elements of each partially ordered set and the greatest and/or least elements when they exist.

Solution: In the first case there is a single maximal element (the set $\{a, b, c\}$) and a single minimal element (the emptyset), these are also the greatest and least elements, respectively, of this partially ordered set.

For the second partially ordered set, 2 and 3 are both minimal, while 24 is maximal. This partially ordered set has no least element, while 24 is the greatest element.

Difficult/challenging questions.

13. What is the minimum number of edges required to produce a connected undirected graph?

Solution: The minimum number of edges equals $n-1$ where n is the number of vertices.

We first show that given n vertices $V = \{v_1, \ldots, v_n\}$ we can construct a connected graph with $n-1$ edges. Considering the graph $G = (V, E)$ where

$$E = \{\{v_i, v_{i+1}\} \mid 1 \leq i \leq n-1\}$$

we have that G has $n-1$ edges. Now for any distinct vertices v_i and v_j, without loss of generality we can assume $i < j$ and we can construct the path between v_i and v_j as follows:

$$\{v_i, v_{i+1}\}, \{v_{i+1}, v_{i+2}\}, \ldots, \{v_{j-1}, v_j\}$$

Therefore, since v_i and v_j were arbitrary, the graph is connected.

Next we show that we cannot construct a connected graph with n vertices and $n-2$ edges. We start with the edgeless graph G, and add edges till the graph is connected.

- First, pick any two vertices of G, label them v_1 and v_2 for convenience, and use one edge to connect them, labelling that edge e_1.
- Second, pick any other vertex, label it v_3, and use one edge to connect it to either v_1 or v_2, labelling that edge e_2.
- Third, pick any other vertex, label it v_4, and use one edge to connect it to v_1, v_2 or v_3, labelling that edge e_3.
- Continue in this way, until we pick a vertex, label it v_{n-1}, and use one edge to connect it to either v_1, v_2, …, v_{n-2} labelling that edge e_{n-2}.

This is the last of our edges, and we still have not connected the last vertex.

14. Prove that an undirected graph with more than $(n-1)\cdot(n-2)/2$ edges is connected.

Solution: Here we consider the dual problem and find the maximum number of edges allowed for a graph to be disconnected and show this equals $(n-1)\cdot(n-2)/2$.

Therefore, consider the highest number of edges a graph can have without being connected. It must have two connected components, and, to maximize the number of edges, they must be size $n-1$ and 1. To maximize the edges, the large component must be a complete graph (there can be no edges in the other graph as it only has one vertex), which will have $C(n-1, 2) = (n-1)(n-2)/2$ edges.

15. Prove that a relation R over $A \times A$ is transitive if and only if R^n is a subset of R for all $n \in \mathbb{Z}^+$.

Solution: This is an if and only if so we need to prove both directions.

First we show if $R^n \subseteq R$ for all $n \in \mathbb{Z}^+$, then R is transitive. Consider any $(a, b) \in R$ and $(b, c) \in R$, since (a, b) and (b, c) are arbitrary elements of R it is sufficient to show $(a, c) \in R$. Now by definition of R^2 we have $(a, c) \in R^2$ and by the hypothesis we have $R^2 \subseteq R$, and hence $(a, c) \in R$ as required.

Second we show if R is transitive, then $R^n \subseteq R$ for all $n \in \mathbb{Z}^+$. We need to show this holds for all positive integers n so prove by induction on n.

Base case: if $n = 1$, then trivially $R^1 = R \subseteq R$ as required.

Inductive step: we assume $R^n \subseteq R$ and consider any $(a, c) \in R^{n+1}$. Since (a, c) is arbitrary, it is sufficient to prove $(a, c) \in R$. Now, by definition we have $R^{n+1} = R^n \circ R$,

and therefore there exists $b \in A$ such that $(a, b) \in R^n$ and $(b, c) \in R$. By the induction hypothesis we have $(a, b) \in R$, i.e. since $R^n \subseteq R$ and $(a, b) \in R^n$, and hence by transitivity of R we have $(a, c) \in R$ as required.

Therefore by the principle of induction we have proved that if R is transitive, then $R^n \subseteq R$ for all $n \in \mathbb{Z}^+$.

16. Let R be a relation that is reflexive and transitive. Show that $R^n = R$ for all $n \geq 1$.

Solution: From results presented in the lectures, since R is transitive we have $R^n \subseteq R$ for all $n \geq 1$. Thus it remains to prove that $R \subseteq R^n$ for all $n \geq 1$. The proof is by mathematical induction on $n \in \mathbb{N}$. Clearly the base case holds with $n = 1$. Now assume that $R \subseteq R^n$ for some $n \in \mathbb{N}$, and consider any $(a, b) \in R$. Since R is reflexive, $(b, b) \in R$. Hence by induction hypothesis, $(b, b) \in R^n$. Thus by definition of the composition operator on relations, $(a, b) \in R^{n+1}$, since $(a, b) \in R$ was arbitrary we have $R \subseteq R^{n+1}$ as required.

17. Let R be a symmetric relation. Show that R^n is symmetric for all $n \in \mathbb{Z}^+$.

Solution: The proof is by induction on $n \in \mathbb{Z}^+$. The proof relies on first showing that for any relation S and $n \in \mathbb{Z}^+$ we have $S^{n+1} = S \circ S^{n+1}$ which follows from the fact that $\circ$ is associative.

Base case. The base holds as $R^1 = R$ and since R is symmetric.

Inductive step. Suppose R^n is symmetric and consider any $(a, c) \in R^{n+1}$, by definition of R^{n+1} there exists b such that $(a, b) \in R^n$ and $(b, c) \in R$. By by the hypothesis R is symmetric and by the inductive hypothesis we have R^n is symmetric. Therefore we have $(c, b) \in R$ and $(b, a) \in R^n$, and hence since $R^{n+1} = R \circ R^{n+1}$ we have $(c, a) \in R^{n+1}$. Since $(a, c) \in R^{n+1}$ was arbitrary it follows that R^{n+1} is symmetric.

Therefore by the principle of induction we have proved that R^n is symmetric for all $n \in \mathbb{Z}^+$.