Discrete Mathematics for Part I CST 2014/15
Sets
Lent Supervision Exercises

Marcelo Fiore

January 15, 2015

1 Basic exercises

1.1 On sets

1. Prove the following statements:

   (a) Reflexivity: $\forall \textsf{ sets } A.\, A \subseteq A$.

   (b) Transitivity: $\forall \textsf{ sets } A, B, C.\, (A \subseteq B \wedge B \subseteq C) \implies A \subseteq C$.

   (c) Antisymmetry: $\forall \textsf{ sets } A, B.\, (A \subseteq B \wedge B \subseteq A) \iff A = B$.

2. Prove the following statements:

   (a) $\forall \textsf{ set } S.\, \emptyset \subseteq S$.

   (b) $\forall \textsf{ set } S.\, (\forall x.\, x \notin S) \iff S = \emptyset$.

3. Find the union and intersection of:

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

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

4. Establish the laws of the powerset Boolean algebra.

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

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

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

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

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

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

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

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

   (b) $A \subseteq B$.

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

(d) $B^{\mathrm{c}} \subseteq A^{\mathrm{c}}$.

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

   (a) $A^{\mathrm{c}} = B \iff (A \cup B = U \ \wedge\ A \cap B = \emptyset)$,

   (b) $(A^{\mathrm{c}})^{\mathrm{c}} = A$, and

   (c) the De Morgan's laws:
   $$(A \cup B)^{\mathrm{c}} = A^{\mathrm{c}} \cap B^{\mathrm{c}} \text{ and } (A \cap B)^{\mathrm{c}} = A^{\mathrm{c}} \cup B^{\mathrm{c}} \ .$$

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

9. For sets A, B, C, D, either prove or disprove the following statements.

   (a) $(A \subseteq B \ \wedge\ C \subseteq D) \implies A \times C \subseteq B \times D$.

   (b) $(A \cup C) \times (B \cup D) \subseteq (A \times B) \cup (C \times D)$.

   (c) $(A \times B) \cup (C \times D) \subseteq (A \cup C) \times (B \cup D)$.

   (d) $A \times (B \cup D) \subseteq (A \times B) \cup (A \times D)$.

   (e) $(A \times B) \cup (A \times D) \subseteq A \times (B \cup D)$.

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

10. Let $I = \{2, 3, 4, 5\}$, and for each $i \in I$ let $A_i = \{i, i+1, i-1, 2 \cdot i\}$.

    (a) List the elements of all the sets A_i for $i \in I$.

    (b) Let $\{\, A_i \mid i \in I \,\}$ stand for $\{A_2, A_3, A_4, A_5\}$. Find $\bigcup\{A_i \mid i \in I\}$ and $\bigcap\{A_i \mid i \in I\}$.

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

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

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

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

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

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

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

1.2 On relations

1. Let $A = \{1, 2, 3, 4\}$, $B = \{a, b, c, d\}$, and $C = \{x, y, z\}$.

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

2. Prove that relational composition is associative and has the identity relation as neutral element.

3. For a relation $R : A \mathrel{-\!\!\!\!+\!\!\!\!\rightarrow} B$, let its *opposite*, or *dual*, $R^{\mathrm{op}} : B \mathrel{-\!\!\!\!+\!\!\!\!\rightarrow} A$ be defined by

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

For $R, S : A \rightarrow\!\!\!\!\!\!+\, B$, prove that

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

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

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

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

1.3 On partial functions

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

2. Prove that a relation $R : A \rightarrow\!\!\!\!\!\!+\, B$ is a partial function iff $R \circ R^{\mathrm{op}} \subseteq \mathrm{id}_B$.

3. Prove that the identity relation is a partial function, and that the composition of partial functions yields a partial function.

1.4 On functions

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

2. A relation $R : A \rightarrow\!\!\!\!\!\!+\, B$ is said to be total whenever $\forall\, a \in A.\, \exists\, b \in B.\, a\,R\,b$. Prove that this is equivalent to $\mathrm{id}_A \subseteq R^{\mathrm{op}} \circ R$.

   Conclude that a relation $R : A \rightarrow\!\!\!\!\!\!+\, B$ is a function iff $R \circ R^{\mathrm{op}} \subseteq \mathrm{id}_B$ and $\mathrm{id}_A \subseteq R^{\mathrm{op}} \circ R$.

3. Prove that the identity partial function is a function, and that the composition of functions yields a function.

4. Find endofunctions $f, g : A \to A$ such that $f \circ g \neq g \circ f$. Prove your claim.

1.5 On bijections

1. (a) Give examples of functions that have (i) none, (ii) exactly one, and (iii) more than one retraction.

   (b) Give examples of functions that have (i) none, (ii) exactly one, and (iii) more than one section.

2. Let n be an integer.

   (a) How many sections are there for the absolute-value map $[-n..n] \to [0..n] : x \mapsto |\,x\,|$?

   (b) How many retractions are there for the exponential map $[0..n] \to [0..2^n] : x \mapsto 2^x$?

3. Give an example of two sets A and B and a function $f : A \to B$ satisfying both:

   (i) there is a retraction for f, and

   (ii) there is no section for f.

Explain how you know that f has these two properties.

4. Prove that the identity function is a bijection, and that the composition of bijections yields a bijection.

5. For $f : A \to B$, prove that if there are $g, h : B \to A$ such that $g \circ f = \mathrm{id}_A$ and $f \circ h = \mathrm{id}_B$ then $g = h$.

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

6. We say that two functions $s : A \to B$ and $r : B \to A$ are a *section-retraction* pair whenever $r \circ s = \mathrm{id}_A$; and that a function $e : B \to B$ is an *idempotent* whenever $e \circ e = e$.

   (a) Show that if $s : A \to B$ and $r : B \to A$ are a section-retraction pair then the composite $s \circ r : B \to B$ is an idempotent.

   (b) Prove that for every idempotent $e : B \to B$ there exists a set A and a section-retraction pair $s : A \to B$ and $r : B \to A$ such that $s \circ r = e$.

   (c) Let $p : C \to D$ and $q : D \to C$ be functions such that $p \circ q \circ p = p$. Can you conclude that

   - $p \circ q$ is idempotent? If so, how?
   - $q \circ p$ is idempotent? If so, how?

7. Prove the isomorphisms of the *Calculus of Bijections, I.*

8. Prove that, for all $m, n \in \mathbb{N}$,

   (a) $\mathcal{P}\big([n]\big) \cong [2^n]$

   (b) $[m] \times [n] \cong [m \cdot n]$

   (c) $[m] \uplus [n] \cong [m + n]$

   (d) $\big([m] \rightharpoonup [n]\big) \cong [(n+1)^m]$

   (e) $\big([m] \Rightarrow [n]\big) \cong [n^m]$

   (f) $\mathrm{Bij}\big([n], [n]\big) \cong [n!]$

1.6 On equivalence relations

1. For a relation R on a set A, prove that

   - R is reflexive iff $\mathrm{id}_A \subseteq R$,
   - R is symmetric iff $R \subseteq R^{\mathrm{op}}$,
   - R is transitive iff $R \circ R \subseteq R$.

2. Prove that the isomorphism relation $\cong$ between sets is an equivalence relation.

3. Prove that the identity relation id_A on a set A is an equivalence relation and that $A/_{\mathrm{id}_A} \cong A$.

4. Show that, for a positive integer m, the relation $\equiv_m$ on $\mathbb{Z}$ given by

$$x \equiv_m y \iff x \equiv y \pmod{m} \quad .$$

is an equivalence relation.

5. Show that the relation $\equiv$ on $\mathbb{Z} \times \mathbb{N}^+$ given by

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

is an equivalence relation.

6. Let B be a subset of a set A. Define the relation E on $\mathcal{P}(A)$ by

$$\big(X, Y\big) \in E \iff X \cap B = Y \cap B \quad .$$

Show that E is an equivalence relation.

1.7 On surjections

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

2. Prove that the identity function is a surjection, and that the composition of surjections yields a surjection.

3. From surjections $A \twoheadrightarrow B$ and $X \twoheadrightarrow Y$ define, and prove surjective, functions $A \times X \twoheadrightarrow B \times Y$ and $A \uplus X \twoheadrightarrow B \uplus Y$.

1.8 On injections

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

2. Prove that the identity function is an injection, and that the composition of injections yields an injection.

1.9 On images

1. What is the direct image of $\mathbb{N}$ under the integer square-root relation $R_2 = \{\, (m, n) \mid m = n^2 \,\} : \mathbb{N} \mathrel{\rightarrow\!\!\!\!\!+} \mathbb{Z}$? And the inverse image of $\mathbb{N}$?

2. For a relation $R : A \mathrel{\rightarrow\!\!\!\!\!+} B$, show that

   (a) $\overrightarrow{R}(X) \;=\; \bigcup_{x \in X} \overrightarrow{R}\big(\{x\}\big)$ for all $X \subseteq A$, and

   (b) $\overleftarrow{R}(Y) \;=\; \big\{\, a \in A \mid \overrightarrow{R}\big(\{a\}\big) \subseteq Y \big\}$ for all $Y \subseteq B$.

3. For $X \subseteq A$, prove that the direct image $\overrightarrow{f}(X) \subseteq B$ under an injective function $f : A \rightarrowtail B$ is in bijection with X; that is, $X \cong \overrightarrow{f}(X)$.

1.10 On indexed sets

1. Prove the isomorphisms of the *Calculus of Bijections, II.*

2 Advanced exercises

2.1 On induction

1. Prove that for all natural numbers $n \geq 3$, if n distinct points on a circle are joined in consecutive order by straight lines, then the interior angles of the resulting polygon add up to $180 \cdot (n-2)$ degrees.

2. Prove that, for any positive integer n, a $2^n \times 2^n$ square grid with any one square removed can be tiled with L-shaped pieces consisting of 3 squares.

3. The set of *(univariate) polynomials* (over the rationals) on a variable x is defined as that of arithmetic expressions equal to those of the form $\sum_{i=0}^{n} a_i \cdot x^i$, for some $n \in \mathbb{N}$ and some $a_1, \ldots, a_n \in \mathbb{Q}$.

   (a) Show that if $p(x)$ and $q(x)$ are polynomials then so are $p(x) + q(x)$ and $p(x) \cdot q(x)$.

   (b) Deduce as a corollary that, for all $a, b \in \mathbb{Q}$, the linear combination $a \cdot p(x) + b \cdot q(x)$ of two polynomials $p(x)$ and $q(x)$ is a polynomial.

   (c) Show that there exists a polynomial $p_2(x)$ such that, for every $n \in \mathbb{N}$, $p_2(n) = \sum_{i=0}^{n} i^2 = 0^2 + 1^2 + \cdots + n^2$.[1]
   Hint: Note that for every $n \in \mathbb{N}$,
   $$(n+1)^3 \quad = \quad \textstyle\sum_{i=0}^{n}(i+1)^3 - \sum_{i=0}^{n} i^3 \quad . \tag{†}$$

   (d) Show that, for every $k \in \mathbb{N}$, there exists a polynomial $p_k(x)$ such that, for all $n \in \mathbb{N}$, $p_k(n) = \sum_{i=0}^{n} i^k = 0^k + 1^k + \cdots + n^k$.
   Hint: Generalise
   $$(n+1)^2 \quad = \quad \textstyle\sum_{i=0}^{n}(i+1)^2 - \sum_{i=0}^{n} i^2$$
   and (†) above.

2.2 On sets

1. For $\mathcal{F} \subseteq \mathcal{P}(A)$, let $\mathcal{U} = \{\, X \subseteq A \mid \forall S \in \mathcal{F}.\ S \subseteq X \,\} \subseteq \mathcal{P}(A)$. Prove that $\bigcup \mathcal{F} = \bigcap \mathcal{U}$. Analogously, define $\mathcal{L} \subseteq \mathcal{P}(A)$ such that $\bigcap \mathcal{F} = \bigcup \mathcal{L}$. Also prove this statement.

2. Prove that, for all collections of sets $\mathcal{F}$, it holds that
   $$\forall \textsf{ set } U.\ \bigcup \mathcal{F} \subseteq U \iff \big(\forall X \in \mathcal{F}.\, X \subseteq U\big) \quad .$$

3. Prove that for all collections of sets $\mathcal{F}_1$ and $\mathcal{F}_2$,
   $$\big(\bigcup \mathcal{F}_1\big) \cup \big(\bigcup \mathcal{F}_2\big) = \bigcup(\mathcal{F}_1 \cup \mathcal{F}_2) \quad .$$
   State and prove the analogous property for intersections of non-empty collections of sets.

[1] Chapter 2.5 of *Concrete Mathematics: A Foundation for Computer Science* by R.L. Graham, D.E. Knuth, and O. Patashnik looks at this in great detail.

2.3 On relations

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

   (a) for all $R : X \rightarrow\!\!\!\!\!\!\!\;+\!\!\!\!\rightarrow A$,
   $$\big(\bigcup \mathcal{F}\big) \circ R \;=\; \bigcup \big\{\, S \circ R \mid S \in \mathcal{F} \,\big\} \;: X \rightarrow\!\!\!\!\!\!\!\;+\!\!\!\!\rightarrow B \quad ,$$
   and that,

   (b) for all $R : B \rightarrow\!\!\!\!\!\!\!\;+\!\!\!\!\rightarrow Y$,
   $$R \circ \big(\bigcup \mathcal{F}\big) \;=\; \bigcup \big\{\, R \circ S \mid S \in \mathcal{F} \,\big\} \;: A \rightarrow\!\!\!\!\!\!\!\;+\!\!\!\!\rightarrow Y \quad .$$

   What happens in the case of big intersections?

2. For a relation R on a set A, let
   $$\mathcal{T}_R \;=\; \big\{\, Q \subseteq A \times A \;\mid\; R \subseteq Q \,\wedge\, Q \text{ is transitive} \,\big\} \quad .$$
   For $R^{\circ+} = R \circ R^{\circ*}$, prove that (i) $R^{\circ+} \in \mathcal{T}_R$ and (ii) $R^{\circ+} \subseteq \bigcap \mathcal{T}_R$. Hence, $R^{\circ+} = \bigcap \mathcal{T}_R$.

2.4 On partial functions

1. Show that $\big(\mathrm{PFun}(A, B), \subseteq\big)$ is a partial order.

2. Show that the intersection of a non-empty collection of partial functions in $\mathrm{PFun}(A, B)$ is a partial function in $\mathrm{PFun}(A, B)$.

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

2.5 On functions

1. Let $\chi : \mathcal{P}(U) \to (U \Rightarrow [2])$ be the function mapping subsets S of U to their characteristic (or indicator) functions $\chi_S : U \to [2]$.

   (a) Prove that, for all $x \in U$,
   - $\chi_{A \cup B}(x) \;=\; \big(\chi_A(x) \text{ OR } \chi_B(x)\big) \;=\; \max\big(\chi_A(x), \chi_B(x)\big)$,
   - $\chi_{A \cap B}(x) \;=\; \big(\chi_A(x) \text{ AND } \chi_B(x)\big) \;=\; \min\big(\chi_A(x), \chi_B(x)\big)$,
   - $\chi_{A^c}(x) \;=\; \text{NOT}\big(\chi_A(x)\big) \;=\; \big(1 - \chi_A(x)\big)$.

   (b) For what construction $A?B$ on sets A and B it holds that
   $$\chi_{A?B}(x) \;=\; \big(\chi_A(x) \text{ XOR } \chi_B(x)\big) \;=\; \big(\chi_A(x) +_2 \chi_B(x)\big)$$
   for all $x \in U$? Prove your claim.

2.6 On equivalence relations

1. Let E_1 and E_2 be two equivalence relations on a set A. Either prove or disprove the following statements.

   (a) $E_1 \cup E_2$ is an equivalence relation on A.

   (b) $E_1 \cap E_2$ is an equivalence relation on A.

2. For an equivalence relation E on a set A, show that $[a_1]_E = [a_2]_E$ iff $a_1 \mathrel{E} a_2$, where $[a]_E = \{\, x \in A \mid x \mathrel{E} a \,\}$.

3. For a function $f : A \to B$ define a relation $\equiv_f$ on A by the rule

$$a \equiv_f a' \iff f(a) = f(a')$$

   for all $a, a' \in A$.

   (a) Show that for every function $f : A \to B$, the relation $\equiv_f$ is an equivalence on A.

   (b) Prove that every equivalence relation E on a set A is equal to $\equiv_q$ for q the quotient function $A \twoheadrightarrow A_{/E} : a \mapsto [a]_E$.

   (c) Prove that for every surjection $f : A \twoheadrightarrow B$,

$$B \;\cong\; \left(A_{/\equiv_f}\right) \quad .$$

2.7 On countability

1. For an infinite set S, prove that if there is a surjection $\mathbb{N} \to S$ then there is a bijection $\mathbb{N} \to S$.

2. Prove that:

   (a) $\mathbb{N}$, $\mathbb{Z}$, $\mathbb{Q}$ are countable sets.

   (b) The product and disjoint union of countable sets is countable.

   (c) Every finite set is countable.

   (d) Every subset of a countable set is countable.

3. For an infinite set S, prove that the following are equivalent:

   (a) There is a bijection $\mathbb{N} \to S$.

   (b) There is an injection $S \to \mathbb{N}$.

   (c) There is a surjection $\mathbb{N} \to S$

4. For a set X, prove that there is no injection $\mathcal{P}(X) \to X$.

2.8 On images

1. For a relation $R : A \rightarrowtriangle\!\!\!\!\rightarrow B$, prove that

   (a) $\overrightarrow{R}\big(\bigcup \mathcal{F}\big) = \bigcup\big\{\, \overrightarrow{R}(X) \mid X \in \mathcal{F} \,\big\} \in \mathcal{P}(B)$ for all $\mathcal{F} \in \mathcal{P}(\mathcal{P}(A))$, and

   (b) $\overleftarrow{R}\big(\bigcap \mathcal{G}\big) = \bigcap\big\{\, \overleftarrow{R}(Y) \mid Y \in \mathcal{G} \big\} \in \mathcal{P}(A)$ for all $\mathcal{G} \in \mathcal{P}(\mathcal{P}(B))$.

2. Show that, by inverse image,

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

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

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

   for all $X, Y \subseteq B$.

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

2.9 On indexed sets

1. Prove that if X and A are countable sets then so are A^*, $\mathcal{P}_{\mathrm{fin}}(A)$, and $(X \rightharpoonup_{\mathrm{fin}} A)$.