Solutions to Problem Set 3

Note: This problem set contains a number of questions that will require you to write proofs. The goal is not only to have correct proofs, but also to make sure they are clear, orderly, and well-presented.

Problem 1. Let $(a, b) \sim (c, d)$ if $a + d = b + c$. We claim that $\sim$ is an equivalence relation.

(a) Partition the set $\{0, 1, 2\} \times \{0, 1, 2\}$ into the distinct equivalence classes under $\sim$.

Solution. We can rewrite $(a, b) \sim (c, d)$ if $a + d = b + c$ as $(a, b) \sim (c, d)$ if $a - b = c - d$. This shows that with any equivalence class $\mathcal{C}$ we can associate a *difference* d such that $(a, b) \in \mathcal{C} \Leftrightarrow a - b = d$. This gives us an easy way to list the equivalence classes of $\{0, 1, 2\} \times \{0, 1, 2\}$.

- $d = -2 : \{(0, 2)\}$.
- $d = -1 : \{(0, 1), (1, 2)\}$.
- $d = 0 : \{(0, 0), (1, 1), (2, 2)\}$.
- $d = 1 : \{(1, 0), (2, 1)\}$.
- $d = 2 : \{(2, 0)\}$.

■

(b) Prove that $\sim$ is an equivalence relation on $\mathbb{Z} \times \mathbb{Z}$.

Solution. The proofs of the defining properties of an equivalence relation follow.

- *Reflexivity* $(a, b) \sim (a, b)$ since $a + b = b + a$.
- *Symmetry* $(a, b) \sim (c, d) \Rightarrow (c, d) \sim (a, b)$ since $a + d = b + c \Rightarrow c + b = d + a$.
- *Transitivity* Assume $(a, b) \sim (c, d)$, i.e. $a + d = b + c$. And, $(c, d) \sim (e, f)$, i.e. $c + f = d + e$. Adding we get $a + d + c + f = b + c + d + e$ or $a + f = b + e$, i.e. $(a, b) \sim (e, f)$. Hence $(a, b) \sim (c, d) \wedge (c, d) \sim (e, f) \Rightarrow (a, b) \sim (e, f)$.

Since $\sim$ is reflexive, symmetric and transitive it is an equivalence relation. ■

(c) How many equivalence classes under $\sim$ are there on the set $\{0, 1, \ldots, n\} \times \{0, 1, \ldots, n\}$. Explain.

Solution. Using the observation from part a), we only need to count the number of possible differenes. This is $2n + 1$ since the difference can be any value in $\{-n, \ldots, n\}$. ∎

Problem 2. Let $A = \{1, 2, \ldots, n\}$ and consider the partial order $(\mathcal{P}(A), \subseteq)$.Remember that $\mathcal{P}(A)$ is the set of all subsets of A and that $\subseteq$ is the normal subset relation.

(a) For the case when $n = 3$, draw the DAG for the relation $(\mathcal{P}(A), \subseteq)$ and label two maximal chains and two maximal antichains. Give an example of a topological sort of this relation.

Solution. See Figure 1. $\{\}, \{1\}, \{2\}, \{3\}, \{1, 2\}, \{1, 3\}, \{2, 3\}, \{1, 2, 3\}$ is a topological sort of this relation.

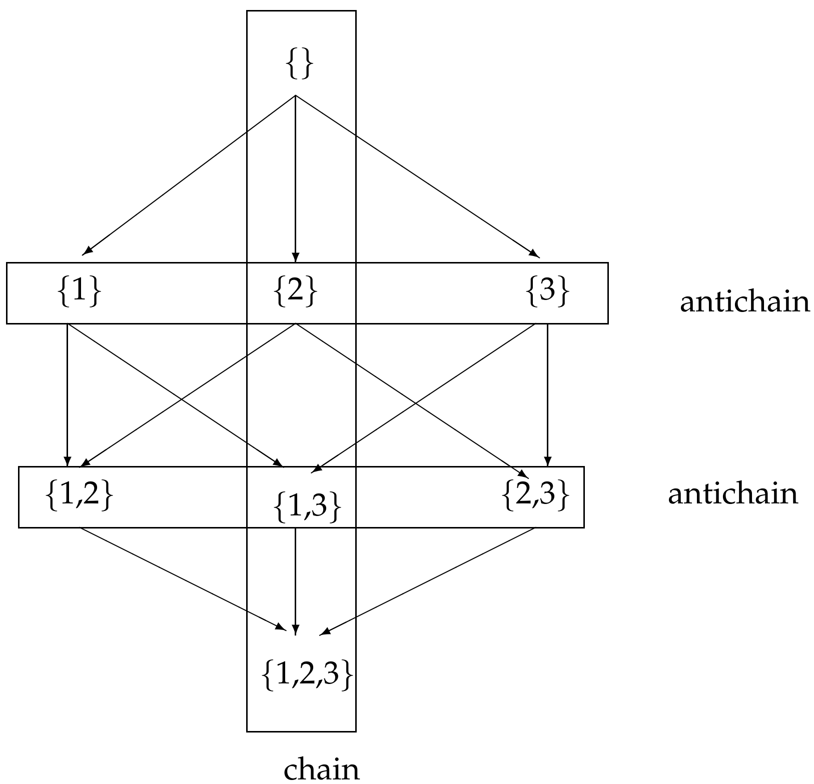

Figure 1: DAG for Problem 4c.

$(\mathcal{P}(A), \subseteq)$. ∎

(b) Prove that there exists a chain of length $n + 1$ in $(\mathcal{P}(A), \subseteq)$.

Solution. Let $A_0 = \emptyset$ and $A_i = A_{i-1} \cup \{i\}$ for $0 < i \leq n$. Then $A_i \subset A_{i+1}$ and there are $n+1$ different A_i's. ■

(c) Prove that for any integer k such that $0 < k < n$, the set $\{B | B \subseteq A \text{ and } |B| = k\}$ is an antichain in $(\mathcal{P}(A), \subseteq)$.

Solution. Let $A_k = \{B | B \subseteq A \text{ and } |B| = k\}$ and consider $B_1, B_2 \in A_k$ such that $B_1 \neq B_2$. We prove the claim by contradiction, i.e., by assuming that B_1 and B_2 are related. Thus, assume without loss of generality that $B_1 \subseteq B_2$. Since $B_1 \neq B_2$, this implies that $B_1 \subset B_2$, which implies that $|B_1| < |B_2|$, which contradicts the fact that $B_1, B_2 \in A_k$. Thus B_1 and B_2 are uncomparable, which implies that A_k is an antichain. ■

Problem 3. Let R be the lexicographic (dictionary) ordering of strings of symbols from a totally ordered alphabet as defined in Rosen p. 417.

(a) Prove that R is a total order.

Solution. If α, β are strings, let us denote by $\alpha \sqsubseteq \beta$ the fact that α is a *prefix* of β, i.e., that $\alpha\gamma = \beta$, for some γ. Let us also denote by $\alpha \restriction n$ the prefix of α of length n.

Then, the lexicographic order R is such that

$$\alpha R \beta \;\longleftrightarrow\; \alpha \sqsubseteq \beta \;\vee\; \alpha \restriction t \prec \beta \restriction t$$

where t is the length of the shortest string. That is, α comes before β iff either it is a prefix of β or its t-prefix comes *strictly* before the t-prefix of β (in the ordering of strings of length t, which we know is total).

We first show that R is a partial order. Reflexivity is obvious, and antisymmetry is deduced easily: Suppose $\alpha R \beta$ and $\beta R \alpha$. If any of the strings has its t-prefix strictly before the t-prefix of the other string, then the latter one can't be a prefix of the former; and it certainly cannot have its t-prefix strictly before the t-prefix of the former string. Hence, the only possibility is that both $\alpha \sqsubseteq \beta$ and $\beta \sqsubseteq \alpha$, which implies $\alpha = \beta$.

For transitivity, let's assume that $\alpha R \beta$ and $\beta R \gamma$, where α, β, γ are of length m, n, l, respectively, and $t = \min(m, n)$, $s = \min(n, l)$, $r = \min(m, n, l)$. Then:

- If $\beta \sqsubseteq \gamma$, then $n \leqslant l$ and hence $r = t$, and:
  - If $\alpha \sqsubseteq \beta$, then α is also a prefix of γ.
  - If $\alpha \restriction t \prec \beta \restriction t$, then $\alpha \restriction r \prec \gamma \restriction r$, too (because $r = t$ and $\gamma \restriction r = \beta \restriction r$).
- If $\beta \restriction s \prec \gamma \restriction s$, then:
  - If $\alpha \sqsubseteq \beta$, then we either have $\alpha \sqsubseteq \gamma$, or $\alpha \restriction r \prec \gamma \restriction r$.
  - If $\alpha \restriction t \prec \beta \restriction t$, then we can infer that again $\alpha \restriction r \prec \gamma \restriction r$.

Therefore, in any case, we have $\alpha R \gamma$; so R is indeed transitive, which concludes the proof R is a partial order.

To prove that R is total, consider any two α, β and note that their t-prefixes are comparable (by the fact $\preceq$ over strings of length t is total). Equality of the prefixes implies one of the strings is a prefix of the other; and any strict order of the prefixes implies a similar order for the strings. In any case, the strings are comparable. This implies that R is total. ■

(b) Prove that neither R nor R^{-1} is a well-ordering, for alphabets with more than one element. Recall that a well-ordering on a set S is a total ordering on S such that every non-empty subset of S has a smallest element.

Solution. Given any alphabet A with at least two elements, consider two distinct elements a, b of A. Without loss of generality, we may assume that $a \preceq b$. Then R is not a well ordering since the set $\{b, ab, aab, aaab, aaaab, \ldots\}$ has no least element. Moreover, R^{-1} is not a well-ordering since $\{a, aa, aaa, aaaa, \ldots\}$ has no least element. ■

Problem 4. Let R be a symmetric relation on a set A. Show that R^n is symmetric for each positive integer n. Deduce that the reflexive transitive closure, R^*, is symmetric.[1]

Hint: Use induction.

Solution. We prove the first claim by induction.

Base case ($n = 1$): Clearly, R^1 is symmetric.

Induction step: Assuming R^n is symmetric, we are to prove that R^{n+1} is. Consider any two elements a, b in A such that $aR^{n+1}b$ holds. Since $R^{n+1} = R \circ R^n$, we conclude that there must exist c such that aR^nc and cRb both hold. Since R^n is symmetric, cR^na holds; since R is symmetric, bRc holds. Since $R^{n+1} = R^n \circ R$, the above implies that $bR^{n+1}a$. Hence, R^{n+1} is symmetric, as required.

To prove the second claim, observe that $R^* ::= \bigcup_{k=0}^{\infty} R^k$. Now, suppose $(a, b) \in R^*$. Then for some natural number n, $(a, b) \in R^n$. We observe that R^n is symmetric, since if $n > 0$ this follows from the first part of the problem, and in the case $n = 0$, the identity relation is clearly symmetric. Hence, $(b, a) \in R^n$, and so, $(b, a) \in R^*$, proving the claim.

■

[1] Reminder:

$$R^* ::= \bigcup_{k=0}^{\infty} R^k,$$

where R^0 is defined to be the identity relation, id_A, on A.

Problem 5. For any function $f : A \to B$, define a binary relation, R_f, on A by the condition:

$$a_1 R_f a_2 \longleftrightarrow f(a_1) = f(a_2).$$

(a) Show that R_f is an equivalence relation.

Solution. We first prove R_f is transitive. Suppose $a_1 R_f a_2$ and $a_2 R_f a_3$. So $f(a_1) = f(a_2)$ and $f(a_2) = f(a_3)$. So $f(a_1) = f(a_3)$ (because equality is transitive, a basic fact we can assume w/o proof). That is, $a_1 R_f a_3$.

To show that R_f is reflexive, note that for any $a \in A$, $f(a) = f(a)$, so $aR_f a$. Symmetry also follows, since if, for some $a, b \in A$, $aR_f b$, then $f(a) = f(b)$, hence also $f(b) = f(a)$, and we conclude that $bR_f a$ holds. ■

(b) Show that for *every* equivalence relation E on A, there exists a set B and a function $f : A \to B$ such that $E = R_f$.

Solution. Let B be the blocks of the partition of A defined by E, that is,

$$B ::= \{[a]_E \mid a \in A\}.$$

Define $f : A \to B$ by the rule

$$f(a) ::= [a]_E.$$

So

$$\begin{aligned} a_1 R_f a_2 &\longleftrightarrow f(a_1) = f(a_2) \\ &\longleftrightarrow [a_1]_E = [a_2]_E \\ &\longleftrightarrow a_1 \, E \, a_2, \end{aligned}$$

which means that $R_f = E$ as required. ■