Problem Set 6 Solutions

Due: Monday, October 19

Problem 1. [20 points] [15] For each of the following, either prove that it is an equivalence relation and state its equivalence classes, or give an example of why it is not an equivalence relation.

(a) [5 pts] $R_n := \{(x, y) \in \mathbb{Z} \times \mathbb{Z} \text{ s.t. } x \equiv y \pmod{n}\}$

Solution. It is an equivalence relation. To prove this, we will show that R_n is symmetric, transitive, and reflexive.

- **Reflexive**: $x \equiv x \pmod{n}$. This is because $x = x + 0 \cdot n$.
- **Symmetric**: We want to show that $R_n(x, y) \Rightarrow R_n(y, x)$. If $R_n(x, y)$, then there is some $c \in \mathbb{Z}$ such that $x = y + c \cdot n$. But then, subtracting $c \cdot n$ from both sides, we have that $y = x + (-c) \cdot n$, so $y \equiv x \pmod{n}$. So $R_n(y, x)$, and the symmetric property holds.
- **Transitivity**. Suppose $R_n(x, y)$ and $R_n(y, z)$. From the first statement, we know that there is some $c \in \mathbb{Z}$ such that $x = y + c \cdot n$. From the second, we know that there is some $d \in \mathbb{Z}$ such that $y = z + d \cdot n$. Substituting in this value of y, we see that $x = (z + d \cdot n) + c \cdot n = z + (d + c) \cdot n$. The sum $c + d$ is an integer, so $R_n(x, z)$ holds.

The equivalence classes are then the sets of numbers congruent to the numbers $\{0, 1, \ldots, n-1\}$ modulo n. ■

(b) [5 pts] $R := \{(x, y) \in P \times P \text{ s.t. } x \text{ is taller than } y\}$ where P is the set of all people in the world today.

Solution. This is not an equivalence relation, because the concept of symmetry is broken. If y is taller than x, then x is not taller than y. ■

(c) [5 pts] $R := \{(x, y) \in \mathbb{Z} \times \mathbb{Z} \text{ s.t. } gcd(x, y) = 1\}$

Solution. This is not an equivalence relation, because transitivity is broken. Consider the case when $x = 3$, $y = 7$, and $z = 15$. Then, $gcd(x, y) = 1$ and $gcd(y, z) = 1$, but $gcd(x, z) = 3 \neq 1$. ■

(d) [5 pts] $R_G :=$ the set of $(x, y) \in V \times V$ such that V is the set of vertices of a graph G, and there is a path $x, v_1, \ldots, v_k, y$ from x to y along the edges of G.

Solution. This is an equivalence relation. We will show this by proving that it obeys reflexivity, symmetry, and transitivity.

- **Reflexivity**: Any vertex is connected to itself.
- **Symmetry**: If $R_G(x, y)$, then there is a path $x, v_1, \ldots, v_k, y$ from x to y. The reverse of this path is $y, v_k, \ldots, v_1, x$, and is a path from y to x. So $R_G(y, x)$.
- **Transitivity**: Suppose $R_G(x, y)$ and $R_G(y, z)$. Then, there is a path from x to y: $x, v_1, \ldots, v_k, y$. Furthermore, there is a path from y to z: $y, w_1, \ldots, w_l, z$. But then, the concatenation of those two is a path $x, v_1, \ldots, v_k, y, w_1, \ldots, w_l, z$ from x to z. So $R_G(x, z)$.

Thus we have shown that R_G is an equivalence relation on a graph G, and the equivalence classes are the connected components of G. ■

Problem 2. [20 points] Every function has some subset of these properties:

injective surjective bijective

Determine the properties of the functions below, and briefly explain your reasoning.

(a) [5 pts] The function $f : \mathbb{R} \to \mathbb{R}$ defined by $f(x) = x \sin(x)$.

Solution. This function is surjective, because for every $y \in \mathbb{R}$ there is a $x \in \mathbb{R}$ such that $x \sin(x) = y$. You can see that, because the function is continuous and for every positive N there is an x such that $f(x) > N$ and an x' such that $f(x') < -N$. The function is not injective, because there are values of y which equal $f(x_1) = f(x_2)$ for some different values of x_1, x_2. For example, $f(0) = f(\pi)$. Consequently, the function is not bijective either. ■

(b) [5 pts] The function $f : \mathbb{R} \to \mathbb{R}$ defined by $f(x) = 99x^{99}$.

Solution. This function is surjective, because for every $y \in \mathbb{R}$ there is a $x \in \mathbb{R}$ such that $99x^{99} = y$. You can see that, for the same reasons as the function in part a. The function is also injective, because for every values of $y \in R$, there is exactly one $x \in R$ such that $y = f(x)$. This holds, since the function is strictly increasing. Consequently, the function is also bijective. ■

(c) [5 pts] The function $f : \mathbb{R} \to \mathbb{R}$ defined by $\tan^{-1}(x)$.

Solution. This function is not surjective, because for all $x \in R$, $-\frac{\pi}{2} \leq tan^{-1}(x) \leq \frac{\pi}{2}$. Consequently, there are some numbers $y \in R$, for example $y = 3$, such that no $x \in R$ for which $y = tan^{-1}(x)$ exists. The function is also injective, because for every values of $y \in R$, there is exactly one $x \in R$ such that $y = f(x)$. This holds, since the function is strictly increasing. Finally, the funcion is not bijective, because it is not surjective. ■

(d) [5 pts] The function $f : \mathbb{N} \to \mathbb{N}$ defined by $f(x) =$ the number of numbers that divide x. For example, $f(6) = 4$ because $1, 2, 3, 6$ all divide 6. *Note: We define here the set* $\mathbb{N}$ *to be the set of all positive integers* $(1, 2, \ldots)$.

Solution. We claim that f is surjective but not injective. To see that it is not injective, note that $f(6) = 4 = f(10)$.

However, we must now show that it is surjective. Given number n, we know from the fundamental theorem of arithmetic that it has a unique prime factorization $p_1^{k_1} p_2^{k_2} \ldots p_m^{k_m}$. Note that the numbers that divide n are simply numbers of the form $p_1^{r_1} p_2^{r_2} \ldots p_m^{r_m}$, where $r_i \leq k_i$ for all indices i. Because the p_i in this product are unique primes, every combination of choices of exponents $\{r_i\}$ will yield a different number that divides n. So the total number of numbers that divides n is $\prod_{i=1}^{m} k_i$. One easy way to see that $f(n)$ is surjective, then, is to consider $n = 2^k$. Then, for any integer k, $f(2^{k-1}) = k$. So f is surjective on the positive integers. ■

Problem 3. [20 points] In this problem we study partial orders (posets). Recall that a partial order $\preceq$ on a set X is reflexive ($x \preceq x$), anti-symmetric ($x \preceq y \wedge y \preceq x \to x = y$), and transitive ($x \preceq y \wedge y \preceq z \to x \preceq z$). Note that it may be the case that neither $x \preceq y$ nor $y \preceq x$. A chain is a list of *distinct* elements $x_1, \ldots, x_i$ in X for which $x_1 \preceq x_2 \preceq \cdots \preceq x_i$. An antichain is a subset S of X such that for all distinct $x, y \in S$, neither $x \preceq y$ nor $y \preceq x$.

The aim of this problem is to show that any sequence of $(n-1)(m-1)+1$ integers either contains a non-decreasing subsequence of length n or a decreasing subsequence of length m. Note that the given sequence may be out of order, so, for instance, it may have the form $1, 5, 3, 2, 4$ if $n = m = 3$. In this case the longest non-decreasing and longest decreasing subsequences have length 3 (for instance, consider $1, 2, 4$ and $5, 3, 2$).

(a) [7 pts] Label the given sequence of $(n-1)(m-1)+1$ integers $a_1, a_2, \ldots, a_{(n-1)(m-1)+1}$. Show the following relation $\preceq$ on $\{1, 2, 3, \ldots, (n-1)(m-1)+1\}$ is a poset: $i \preceq j$ if and only if $i \leq j$ and $a_i \leq a_j$ (as integers).

Solution. We show reflexivity, anti-symmetry, and transitivity. Clearly $i \preceq i$ since $i \leq i$ and $a_i \leq a_i$, so $\preceq$ is reflexive. Next, suppose $i \preceq j$ and $j \preceq i$. Then $i \leq j \leq i$, so $i = j$, and $\preceq$ is anti-symmetric. Finally, suppose $i \preceq j$ and $j \preceq k$. Then $i \leq j$ and $j \leq k$, so $i \leq k$. Moreover, $a_i \leq a_j$ and $a_j \leq a_k$, so $a_i \leq a_k$. Thus, $\preceq$ is transitive. ■

For the next part, we will need to use Dilworth's theorem, as covered in lecture. Recall that Dilworth's theorem states that if $(X, \preceq)$ is any poset whose longest chain has length n, then X can be partitioned into n disjoint antichains.

(b) [7 pts] Show that in any sequence of $(n-1)(m-1)+1$ integers, either there is a non-decreasing subsequence of length n or a decreasing subsequence of length m.

Solution. Consider the $\preceq$ relation on $\{1, 2, \ldots, (n-1)(m-1)+1\}$ defined above. The length of the longest non-decreasing subsequence of the given integers is just the length of the longest chain in this poset. If the longest chain has length at least n, we are done, so suppose the length of the longest chain is at most $c \leq n-1$.

Then, by the first part we know that $\{1, 2, \ldots, (n-1)(m-1)+1\}$ can be decomposed into c disjoint antichains. Consider the indices $i_1 \leq i_2 \leq \cdots \leq i_s$ in any antichain A. Then it must be the case that $a_{i_1} > a_{i_2} > \cdots > a_{i_s}$, as otherwise we would have $a_{i_j} \leq a_{i_{j'}}$ for some $j < j'$, and thus $j \preceq j'$, and A could not be an antichain. It follows that there is a decreasing subsequence of length at least $|A|$.

Since it is possible to partition $\{1, 2, \ldots, (n-1)(m-1)+1\}$ into $c \leq n-1$ disjoint antichains, one such antichain must have size at least

$$\frac{(n-1)(m-1)+1}{c} \geq \frac{(n-1)(m-1)+1}{n-1} \geq m - 1 + \frac{1}{n-1} \geq m,$$

which completes the proof. ■

(c) [6 pts] Construct a sequence of $(n-1)(m-1)$ integers, for arbitrary n and m, that has no non-decreasing subsequence of length n and no decreasing subsequence of length m. Thus in general, the result you obtained in the previous part is best-possible.

Solution. Consider the set of integers $\{1, 2, \ldots, (n-1)(m-1)\}$. For each $1 \leq i \leq n-1$, define the decreasing subsequence of length $m-1$:

$$B_i = i(m-1), \ldots, (i-1)(m-1)+1.$$

Then the B_i partition $\{1, 2, \ldots, (n-1)(m-1)\}$. Consider the sequence

$$S = B_1 \circ B_2 \circ \cdots \circ B_{n-1}.$$

Any non-decreasing subsequence of S can contain at most one integer from any single B_i, since the B_i are decreasing subsequences. Thus, the length of the longest non-decreasing subsequence is at most $n-1$.

Any decreasing subsequence must be entirely contained in a single B_i, since for $j > i$, any integer in B_j is larger than any integer in B_i. Thus, the length of the longest decreasing subsequence is at most $m-1$. ■

Problem 4. [20 points] Louis Reasoner figures that, wonderful as the Beneš network may be, the butterfly network has a few advantages, namely: fewer switches, smaller diameter, and an easy way to route packets through it. So Louis designs an N-input/output network he modestly calls a *Reasoner-net* with the aim of combining the best features of both the butterfly and Beneš nets:

> The ith input switch in a Reasoner-net connects to two switches, a_i and b_i, and likewise, the jth output switch has two switches, y_j and z_j, connected to it. Then the Reasoner-net has an N-input Beneš network connected using the a_i switches as input switches and the y_j switches as its output switches. The Reasoner-net also has an N-input butterfly net connected using the b_i switches as inputs and¡ the z_j switches as outputs.

In the Reasoner-net the minimum latency routing does not have minimum congestion. The *latency for min-congestion* (LMC) of a net is the best bound on latency achievable using routings that minimize congestion. Likewise, the *congestion for min-latency* (CML) is the best bound on congestion achievable using routings that minimize latency.

Fill in the following chart for the Reasoner-net and briefly explain your answers.

diameter	**switch size(s)**	**# switches**	**congestion**	**LMC**	**CML**

Solution.

diameter	**switch size(s)**	**# switches**	**congestion**	**LMC**	**CML**
$\log N + 4$	2×2	$3N(\log N + 1)$	1	$2\log N + 3$	$\sqrt{N}$

The diameter of a Reasoner-net is the smaller diameter of the two components plus 2 (to connect to switch to input/output). The diameter of the butterfly component is $\log N + 2$, while the diameter of the Beneš component is $2\log N + 1$, so overall diameter is 2 + diameter of butterfly = $\log N + 4$.

The number of switches is the number of input and output switches in the Reasoner-net, $4N$, plus the number of switches in its butterfly component, $N(\log N + 1)$, and its Beneš component, $2N \log N$.

The congestion is the congestion of the better of the two component nets, which is the congestion of the Beneš component.

The LMC for the butterfly net equals its diameter, and likewise for the LMC of the Beneš net. So the LMC of the Reasoner-net is 2 plus the LMC of the routing through the component with minimum congestion, namely, 2 plus the diameter of the Beneš net.

The CML equals the congestion of the routing through the component with minimum latency, namely, the congestion of the butterfly net. ■

Problem 5. [20 points] Let B_n denote the butterfly network with $N = 2^n$ inputs and N outputs, as defined in Notes 6.3.8. We will show that the congestion of B_n is exactly $\sqrt{N}$ when n is even.

Hints:

- For the butterfly network, there is a unique path from each input to each output, so the congestion is the maximum number of messages passing through a vertex for any matching of inputs to outputs.
- If v is a vertex at level i of the butterfly network, there is a path from exactly 2^i input vertices to v and a path from v to exactly 2^{n-i} output vertices.
- At which level of the butterfly network must the congestion be worst? What is the congestion at the node whose binary representation is all 0s at that level of the network?

(a) [10 pts] Show that the congestion of B_n is at most $\sqrt{N}$ when n is even.

Solution. First we will show that the congestion is at most $\sqrt{N}$.

Let v be an arbitrary vertex at some level i. Let S_v be the set of inputs that can reach vertex v. Let T_v be the set of outputs that are reachable from vertex v.

By the hint, we have $|S_v| = 2^i$ and $|T_v| = 2^{n-i}$. The number of inputs in S_v that are matched with outputs in T_v is at most $\min\{2^i, 2^{n-i}\}$. To obtain an upper-bound on the congestion of the network, we need to find the maximum value of $\min\{2^i, 2^{n-i}\}$, where the maximum is taken over all i. The maximum value is achieved when 2^i and 2^{n-i} are as equal as possible. Since n is even, these two quantities are equal when $i = n/2$, hence the maximum congestion is

$$2^{n/2} = N^{1/2} = \sqrt{N}.$$

■

(b) [10 pts] Show that the congestion achieves $\sqrt{N}$ somewhere in the network and conclude that the congestion of B_n is exactly $\sqrt{N}$ when n is even.

Solution. We concluded that the congestion of $\sqrt{N}$ can be achieved only at a node at level $\frac{n}{2}$. Consider the node at that level whose binary representation is all 0s. Any packet from the input in the form $z\underbrace{0\ldots000}_{n/2\ bits}$ with destination $\underbrace{000\ldots0}_{n/2\ bits}z'$, where z and z' are any $\frac{n}{2}$-bit numbers, must pass through this node. In the worse case, all packets from input in the form $z\underbrace{0\ldots000}_{n/2\ bits}$ will have destination in the form $\underbrace{000\ldots0}_{n/2\ bits}z'$. But there are $2^{n/2} = \sqrt{N}$ of such possible packets, giving the node load $\sqrt{N}$. Therefore, we can conclude that the congestion of B_n is exactly $\sqrt{N}$ when n is even. ■