CSE 20, Fall 2020 - Homework 8

Due: Monday 12/7 at 11 am PDT

Instructions

Upload a single file to Gradescope for each group. All group members' names and PIDs should be on each page of the submission. You should select appropriate pages for each question when submitting to Gradescope. Your assignments in this class will be evaluated not only on the correctness of your answers, but on your ability to present your ideas clearly and logically. You should always explain how you arrived at your conclusions, using mathematically sound reasoning. Whether you use formal proof techniques or write a more informal argument for why something is true, your answers should always be well-supported. Your goal should be to convince the reader that your results and methods are sound.

Reading Definitions 1-5 Section 9.1 (pp. 574-578) -Binary Relation, Relation on a Set, Reflexivity, Symmetry, Transitivity; Definitions 1, 3 Section 9.5 (p. 609), Definition of partition, Section 9.6 (p. 612)

Key Concepts Equivalence Relations; Modular arithmetic

Problem 1 (20 points)

For each of the following relations R on the set of natural numbers $\mathbb{N}$, determine if it is symmetric or not. **Prove your answer**.

1.
2. $R = \{(a, b) \mid a \neq b\}$

Solution:

1. R is not symmetric. (1,3) belongs to R but (3,1) does not.
2. R is symmetric. If (a,b) belongs to R, i.e a not equal to b, then this implies that b not equal a, so (b,a) also belongs to R by its definition.

Problem 2 (20 points)

Is intersection of two equivalence relations itself an equivalence relation? **Prove your answer.**

Solution:
Let E1 and E2 be two equivalence relations on a set A. Then, we want to show that $E3 = E1 \cap E2$ is also an equivalence relation on set A. To see why this is true, we will prove the three properties are true for E3.

1. Reflexive: To prove (x,x) belongs to E3 for all x in A. Note that (x,x) belongs to both E1 and E2 (since they are both equivalence relations). Therefore, (x,x) belongs to $E1 \cap E2$ = E3.
2. Symmetric: We want to show that if (a,b) belongs to E3, then (b,a) belongs to E3. Note that (a,b) belongs to E3 implies (a,b) belongs to E1 and E2. Since, both E1 and E2 are symmetric, (b,a) belongs to both E1 and E2. Therefore, $(b, a) \in E1 \cap E2$ = E3.
3. Transitive: We want to show that if (a,b) and (b,c) belongs to E3, then (a,c) belongs to E3. Note that (a,b) and (b,c) belongs to E3 implies (a,b) and (b,c) belongs to E1 and E2. Since, both E1 and E2 are transitive, (a,c) belongs to both E1 and E2. Therefore, $(a, c) \in E1 \cap E2$ = E3.

Problem 3 (20 points)

For each of the following relations R on the set of real numbers $\mathbb{R}$, determine if it is transitive or not. **Prove your answer**.

1. $R = \{(a, b) \mid |a - b| \leq 1\}$
2. $R = \{(a, b) \mid a \leq b\}$

Solution:

1. R is **not transitive**. (0.75, 1) and (1,1.75) belong to R but (0.75, 1.75) does not.

2. R is **transitive**. If (a,b) and (b,c) belong to R, then $a \leq b$ and $b \leq c$. This implies $a \leq c$ i.e (a,c) belongs to R.

Problem 4 (20 points)

Let $f: C \rightarrow D$ be a function and let R_f be the binary relation on C defined by:

$$R_f = \{(x, y) \mid f(x) = f(y)\}$$

a. Prove that R_f is an equivalence relation

- Reflexive: For any x, $f(x) = f(x)$ so xR_fx
- Symmetric: Let x, y be such that xR_fy. Then by the definition of R_f, $f(x) = f(y)$. Then $f(y) = f(x)$, and thus, yR_fx.
- Transitive: Let x, y, z be such that xR_fy and yR_fz. Then $f(x) = f(y)$ and $f(y) = f(z)$, which imply $f(x) = f(z)$. Hence xR_fz.

b. For each of the two scenarios listed below, answer all of the following questions OR state that there is not enough information to tell:
   - Is D finite?
   - Is f one-to-one?
   - Is f onto?

   Please briefly justify your answer for each question.

   Two scenarios:

   1. **C is finite, and R_f partitions C into |C| equivalence classes**

- f is **one-to-one**. The only way to partition a finite set C into |C| classes is to have one element per class. Then by the definition of equivalence classes, it must be that for any distinct elements x, y, $\neg(xR_fy)$. Then by the definition of R_f, f(x) !=f(y)

- **There is not enough information to answer the other questions**. If, for example, $C \subseteq D$ and f(x) =x, then if C=D, fis onto and D is finite, but if $D = Z \cup C$ (or any other infinite superset of A), then f is not onto and D is infinite.

   2. **C is finite, and R_f partitions C into |D| equivalence classes**

- From the definition of equivalence class, we can say that D is finite and |D| <= |C| because if |D| > |C|, even if we try to put only one element in one class, there will still be some equivalence classes that do not contain any element. This is a contradiction (equivalence classes are non-empty sets). Therefore, **D is finite.**

- **f is onto**. Consider a subset of C consisting of one element from each of the |D| equivalence classes. As above, no two of these elements map to the same element of D (or else they would be in the same class). Thus they map to |D| distinct elements of D.

Since **D is finite**, mapping to |D| distinct elements of D means mapping to all the elements of D (this isn't true for infinite sets), so f is onto.

- **There is not enough information to decide if f is one-to-one**. If, for example, D = {42} and f(x) = 42, then if |C|= 1, f is one-to-one, but if C is any larger then f is not one-to-one.

Problem 5 (20 points)

Prove by induction on integer $n \geq 0$ that for any integers $a, b, c \geq 1$ we have:
$(a^b \mod c)^n \mod c = a^{bn} \mod c$

Note: This result above guarantees that under the Diffie-Hellman key exchange protocol that we learned in class, the key $A^{k_2} \bmod p$ (with $A = a^{k_1} \bmod p$) computed by Alice and the key $B^{k_1} \bmod p$ (with $B = a^{k_2} \bmod p$) computed by Bob are the same.

SOLUTION

Basic step: When n = 0, we have:

$$(a^b \mod c)^0 \mod c = a^{b\hat{0}} \mod c$$

$$1 \mod c = 1 \mod c$$

This equality holds for any $a, b, c \geq 1$

Inductive step: Fix the values for a,b,c and let k be an arbitrary integer. As induction hypothesis, suppose that:

$$(a^b \mod c)^k \mod c = a^{bk} \mod c$$

We want to show:

$$(a^b \mod c)^{k+1} \mod c = a^{b(k+1)} \mod c$$

Using the property that $xy \mod z = (x \mod z)(y \mod z) \mod z$ and the induction hypothesis, we'll have:

$$\begin{aligned}(a^b \mod c)^{k+1} \mod c &= ((a^b \mod c)^k \cdot (a^b \mod c)) \mod c \\ &= ((a^{bk} \mod c) \cdot (a^b \mod c)) \mod c \\ &= (a^{bk} \cdot a^b) \mod c \\ &= a^{b(k+1)} \mod c\end{aligned}$$

Thus, by induction principle, $(a^b \mod c)^n \mod c = a^{bn} \mod c$ for all $n \geq 0$ and $a, b, c \geq 1$

Problem 6 - Bonus (10 points)

Let S be a set of size |S| = 5.

a. How many binary relations on S are there?
   i. 2^{25} **binary relations**

   There are $5^2 = 25$ pairs of numbers, and there's two possibilities of whether or not each pair is included in the binary relation, so there's 2^{25} binary relation on S.

b. How many reflexive binary relations on S are there?
   i. 2^{20} **reflexive binary relations**

   Suppose $S = \{a_1, a_2, a_3, a_4, a_5\}$

   In this case, any reflexive binary relation on S must contain all the pairs of the form $(a_1, a_1), \ldots, (a_5, a_5)$

   We can write a relation **R** on **S** as $R = \{(a_1, a_1), \ldots, (a_5, a_5)\} \cup B$

where B is any subset of $M := (S \times S) - \{(a_1, a_1), \ldots, (a_5, a_5)\}$.
So the number of reflexive relations on S is equal to the number of subsets of M.
Here, $|M| = |P((S \times S) - \{(a_1, a_1), \ldots, (a_5, a_5\})| = 2^{5^2-5} = 2^{20}$

c. How many <u>symmetric</u> binary relations on S are there?
   i. 2^{15} **symmetric binary relations**
   In this case, a symmetric relation can be seen as a subset of $\Delta := \{(a_i, a_j) \mid 1 \leq i \leq j \leq 5\}$. Since $|\Delta| = 5 \cdot (5 + 1)/2 = 15$, we know that the number of symmetric binary relations is the same as the cardinality of $P(\Delta)$
   where $|P(\Delta)| = 2^{5 \cdot (5+1)/2} = 2^{15}$