MA 274: Exam 2 Study Guide Partial Solutions

(1) Know the precise definitions of the terms requested for your journal.

(2) Review proofs by induction.

(3) Prove that it is impossible to write a computer program that can determine if other computer programs contain an infinite loop. (i.e. the halting problem)

Solution: Suppose (to obtain a contradiction) that P is such a program and assume that P outputs "Stops" if the program inputted to it does not contain an infinite loop and "Loops" if the program does contain an infinite loop. Let Q be the program that takes the same input as P but enters into an infinite loop if P says the inputted program stops and which stops if P says the software contains an infinite loop. If we run Q on itself, then if P says Q stops, Q doesn't stop and if P says Q loops, then Q stops. Thus, P has ensnared us in a logical contradiction and it cannot exist.

(4) Prove that $A \times B = \{(a, b) : a \in A, b \in B\}$ is a set (using the axioms) if A is a set and if B is a set.

Solution: Recall that, by definition for $a \in A$ and $b \in B$,

$$(a, b) = \{\{a\}, \{a, b\}\} \in \mathcal{P}\mathcal{P}(A \cup B)$$

Thus,

$$A \times B = \{(a, b) \in \mathcal{P}\mathcal{P}(A \cup B) : a \in A \text{ and } b \in B\}$$

is a set by the Axiom of Specification.

(5) Be able to use the definition of $+$ on the natural numbers to prove basic facts about $+$. (You will, however, not be asked to prove that $+$ is commutative or associative.)

(6) Be able to prove that something is or isn't an equivalence relation.

(7) Be able to prove that something is or isn't a partial order.

(8) Understand what it means to prove that a function on equivalence classes is well-defined.

Hint: Given $f\colon X/{\sim} \to Y$ (where $\sim$ is an equivalence relation on X) you need to assume that

$$[x_1] = [x_2]$$

and prove

$$f([x_1]) = f([x_2])$$

by using the fact that $[x_1] = [x_2]$ if and only if $x_1 \sim x_2$.

(9) Be able to prove all or portions of the following facts. You should also study other homework problems

(a) The intersection of inductive sets is inductive.

Solution: Suppose that A_α is an inductive set for all α in some index set Λ. Thus, $\varnothing \in A_\alpha$ for all α and if $U \subset A_\alpha$ (for some α) then also $S(U) \subset A_\alpha$. We claim that $\bigcap_{\alpha\in\Lambda} A_\alpha$ is an inductive set. Since $\alpha \in A_\alpha$ for all α, then $\varnothing \in \bigcap_\alpha A_\alpha$. Suppose that $U \in \bigcap_\alpha A_\alpha$. Then $U \in A_\alpha$ for all α. Since each A_α is inductive, $S(U) \in A_\alpha$ for all α. Hence $S(U) \in \bigcap_\alpha A_\alpha$, as desired. Consequently the intersection of inductive sets is inductive.

(b) There exists a unique smallest inductive set.

Solution: Let X be an inductive set and let $I(X)$ be the set of all inductive subsets of X. Since X is inductive, $I(X)$ is non-empty. By the previous problem the intersection $\mathbb{N}(X) = \bigcap I(X)$ of all those inductive sets is inductive. We claim that if Y is some other inductive set, then $\mathbb{N}(X) = \mathbb{N}(Y)$, showing that there is a unique smallest inductive set.

Observe that $X \cap Y$ is inductive and that $I(X \cap Y) \subset I(X)$, since each inductive subset of $X \cap Y$ is also an inductive subset of X. Hence, $\mathbb{N}(X \cap Y) \subset \mathbb{N}(X)$. Since $\mathbb{N}(X \cap Y)$ is an inductive subset of X, $\mathbb{N}(X \cap Y) \in I(X)$. Hence it is one of the sets in the intersection forming $\mathbb{N}(X)$. Thus, $\mathbb{N}(X) \subset \mathbb{N}(X \cap Y)$. Thus, $\mathbb{N}(X) = \mathbb{N}(X \cap Y)$. Reversing the roles of X and Y in the preceding argument we see that also $\mathbb{N}(Y) = \mathbb{N}(X \cap Y)$. Hence, $\mathbb{N}(X) = \mathbb{N}(Y)$ as desired.

(c) There does not exist a set of all sets.

Solution: If there were a set U of all sets, we could form the set

$$S = \{A \in U | A \notin A\}$$

by the axiom of specification. Then either $S \in S$ or $S \notin S$. If $S \in S$, then by the criterion for membership in S, $S \notin S$, a contradiction. On the other hand, if $S \notin S$, then S satisfies the criterion and $S \in S$, another contradiction. Hence, U cannot exist.

(d) 2 + 2 = 4

(e) If $a, b, c \in \mathbb{N}_0$, then $b + a = c + a$ implies $b = c$.

Solution: We prove this by induction on a.

Base Case: $a = 0$.

By the definition of $+$, $b + a = b + 0 = b$ and $c + a = c + 0 + c$. Hence, if $b + a = c + a$, then $b = c$.

Inductive Step: Assume that for some fixed a, $b + a = c + a$. We will show that if $b + (a + 1) = c + (a + 1)$ then $b = c$.

Suppose that $b + (a + 1) = c + (a + 1)$. Since $S(a) = a + 1$, by the definition of $+$, we have $S(b + a) = S(c + a)$. By one of Peano's axioms, this implies $b + a = c + a$. By the inductive hypotheses we get $b = c$, as desired.

(f) If X is a set, then the relation

$$(A \leq B) \Leftrightarrow (A \subset B)$$

is a partial order on $\mathcal{P}(X)$.

(g) Prove that equivalence classes form a partition.

Solution: Suppose that X is a set with an equivalence relation $\sim$. We will show that $X/\sim$ is a partition of X. We begin by showing the covering property. Let $x \in X$. Since $\sim$ is reflexive, $x \sim x$. By definition, $x \in [x]$. Hence, $X/\sim$ satisfies the covering property.

We now show that $X/\sim$ satisfies the pairwise disjoint property. Let $[x], [y] \in X/\sim$. Suppose that $[x] \cap [y] \neq \varnothing$. Let $z \in [x] \cap [y]$. Then $z \in [x]$ and $z \in [y]$. Since $z \in [x]$, we have $x \sim z$. Similarly $y \sim z$. By symmetry and transitivity, $x \sim y$. I claim that this implies that $[x] = [y]$.

Let $a \in [x]$. Then $x \sim a$. Since $x \sim y$, we have $y \sim x$ (symmetry) and so $y \sim a$ (transitivity). Hence, $a \in [y]$ and so $[x] \subset [y]$. Similarly, if $b \in [y]$, then $y \sim b$. Since $x \sim y$, by transitivity, we have $x \sim b$ and so $b \in [x]$. Hence, $[y] \subset [x]$. Consequently, $[x] = [y]$.

Since we have shown that if $[x] \cap [y] \neq \varnothing$, then $[x] = [y]$ we have proven that $X/\sim$ satisfies the pairwise disjoint property and so is a partition. □

(h) Prove that if $\sim$ is an equivalence relation on X then $x \sim y$ if and only if $[x] = [y]$.

Solution: Assume, first, that $x \sim y$. Thus, $y \in [x]$. Since $\sim$ is reflexive, $y \in [y]$. Hence, $[x] \cap [y] \neq \varnothing$. By the previous problem, $[x] = [y]$.

Now assume that $[x] = [y]$. By the reflexive property, $y \in [y]$. By the equality of sets, $y \in [x]$. By definition of equivalence class, $x \sim y$.

(i) If G is a group and if H is a subgroup, then $\sim$ is an equivalence relation on G where

$$(x \sim y) \Leftrightarrow \exists h \in H \text{ such that } x = y \circ h$$

Solution: See the hand out on equivalence relation (or the course notes, for slightly different version).

(j) Using the previous equivalence relation, for all $x \in G$, prove that there exists a bijection from $[x]$ to H.

Solution: See the hand out on equivalence relation (or the course notes, for slightly different version).

(k) If G is a finite group and if H is a subgroup, then the number of elements in G is a multiple of the the number of elements in H.

Solution: See the hand out on equivalence relation.

(l) The compositions of injective (or surjective or bijective) functions is injective (or surjective or bijective).

Solution: See the student solution from Monday, April 13.

(m) A function $f\colon X \to Y$ is a bijection if and only if it has an inverse function $f^{-1}\colon Y \to X$. (That is there is a function $f^{-1}\colon Y \to X$ such that $f^{-1} \circ f(x) = x$ for all $x \in X$ and $f \circ f^{-1}(y) = y$ for all $y \in Y$.)

Solution: We haven't yet discussed this problem, it won't be on the exam.

(10) Here are some new facts for you to try to prove:

(a) Suppose that $f\colon X \to Y$ is a function. If $A \subset X$, we define $f(A) = \{y \in Y : \exists a \in A f(a) = y\}$. Suppose that A, B are subsets of X. Prove that $f(A \cup B) = f(A) \cup f(B)$. Give an example to show that $f(A \cap B)$ need not be equal to $f(A) \cap f(B)$.

Solution: We show that $f(A \cup B) \subset f(A) \cup f(B)$ and that $f(A) \cup f(B) \subset f(A \cup B)$.

Assume that $y \in f(A \cup B)$. By definition, there is an $x \in A \cup B$ such that $f(x) = y$. Since $x \in A \cup B$, either $x \in A$ or $x \in B$. Consequently, $y = f(x) \in f(A)$ or $y = f(x) \in f(B)$. Thus, $y \in f(A) \cup f(B)$.

Conversely, assume that $y \in f(A) \cup f(B)$. Then, either $y \in f(A)$ or $y \in f(B)$. In the former case, there exists $x \in A$ such that $f(x) = y$ and in the latter case, there exists $x \in B$ such that $f(x) = y$. If there is $x \in A$, then since $A \subset A \cup B$, we also have $x \in A \cup B$ and $y \in f(A \cup B)$. Similarly, if there is $x \in B$ such that $f(x) = y$, then there exists $x \in A \cup B$ so that $y = f(x)$. Hence, in this case also, $y \in f(A \cup B)$.

Consequently, by our element arguments, $f(A \cup B) = f(A) \cup f(B)$.

For the remainder of the problem, let $f\colon \mathbb{R} \to \mathbb{R}$ be the function defined by $f(x) = x^2$ for all real $x \in \mathbb{R}$. Let $A \subset \mathbb{R}$ be the interval $(-3, -1)$ and let $B \subset \mathbb{R}$ be the interval $(1, 3)$. Then $A \cap B = \varnothing$ so $f(A \cup B) = \varnothing$, but $f(A) = (1, 9)$ and $f(B) = (1, 9)$ so $f(A) \cap f(B)$ is also the interval $(1, 9)$.

(b) Let $X = \mathcal{P}(\mathbb{R})$ and define $\sim$ on X by $A \sim B$ if and only if there exists a bijection $f\colon A \to B$. Prove that $\sim$ is an equivalence relation.

Solution Sketch: The fact that $\sim$ is reflexive follows from the fact that the identity function is a bijection. Symmetry follows from the fact that the inverse of a bijection is also a bijection and transitivity follows from the fact that the composition of bijections is a bijection.

(c) Let $(X, \leq)$ and $(Y, \prec)$ be sets with partial orders. Define a partial order $\ll$ on $X \times Y$ by:

$(a, b) \ll (c, d) \Leftrightarrow (a \leq c)$ and if $a = c$ then $b \prec d$

Prove that $\ll$ is a partial order and explain how it is related to finding words in a dictionary.

(d) Prove using induction that the number of permutations of a set of n elements is $n!$. (A permutation is a bijection from a set to itself.)

Solution: Here is one possible solution. There are others (perhaps they are easier?)

Suppose that $X = \varnothing$. Then the function $\varnothing \subset \varnothing \times \varnothing = \varnothing$ is the unique function from $\varnothing$ to itself. It is a bijection and so there are $0! = 1$ bijections of X to itself. Suppose now that if X is any set with n elements then there are $n!$ bijections from X to itself. Let Y be any set with $n + 1$ elements. Choose $y \in Y$ and let $X = Y - \{y\}$. Note that there are n elements of X and so, by induction, there are $n!$ permutations of X.

Now for each permutation f of Y, we can get a permutation of X as follows: If $f(y) = y$, then the restriction of f to X is a permutation of X. If $f(y) \neq y$, then there exists $x \in X$ such that $f(y) = x$ (since Y has one more element than X). Let $g\colon Y \to Y$ switch x and y and be the identity on all other elements. Then the restriction of $g \circ f$ to X is a permutation of X. Thus, there are at most $n + 1$ possibilities for $f(y)$. Hence, the number of permutations of Y is at most $(n + 1)$ times the number of permutations of X, namely $(n + 1) \cdot n! = (n + 1)!$.

On the other hand, given a permutation q of X, we can create a permutation of Y by composing q with the function g as above. There are $n + 1$ choices for g and so we can create $(n + 1)!$ permutations of Y. So there are at least $(n + 1)!$ permutations of Y. Consequently, Y has exactly $(n + 1)!$ permutations.

(e) Suppose that $f\colon X \to X$ is a bijection on a set with n elements. Prove that there exist transpositions $f_1, \ldots, f_k$ of X such that $f = f_k \circ f_{k-1} \circ \ldots f_2 \circ f_1$. (A transposition is a bijection that simply swaps two elements and leaves all other elements unchanged.) Hint: Induct on n.

Hint: In the inductive step, let Y be the set with $n+1$ elements and choose $y \in Y$. Consider $f(y)$. If $f(y) = y$, f can be written as the composition of transpositions in the inductive hypothesis. If $f(y) \neq y$ we can apply a transposition g so that $g \circ f(y) = y$. Applying the inductive hypothesis, $g \circ f$ is the composition of transpositions. The inverse of g is g itself, and so f is also the composition of transpositions.

(f) Give an example of a permutation of $\mathbb{N}$ which is not the composition of a finite number of transpositions.

Solution: There are many possibilities. One is the permutation which switches $2n - 1$ and $2n$ for all $n \in \mathbb{N}$.