Full name	Andrew ID

21-127 Final

Friday, 5 May 2023

Please read the following instructions carefully before the test begins.

Before the test

- Do not open the test until instructed to do so.
- Write your full name and Andrew ID in the boxes at the top of this page.
- Place your Carnegie Mellon University ID card face-up in front of you.
- Turn off your electronic devices (e.g. phone, tablet, laptop, calculator), and store any devices, notes or books out of sight (e.g. in a closed bag).

During the test

- Write clearly and legibly with a pen or pencil that is dark enough to be readable when scanned.
- You must justify all answers and claims with mathematical proof, unless otherwise specified.
- If you continue a solution on one of the extra pages (pages 19–20), you should clearly indicate in your solution the page number where it is continued.
- You may not use notes, books, other reference materials, calculators or electronic devices on this test.
- You may not communicate with others or attempt to look at other students' work during the test.
- If you require assistance, please raise your hand and wait for a proctor to come to you.
- If you need to leave the classroom (e.g. to use the bathroom), please raise your hand, show your CMU ID card to a proctor, and leave your belongings in the classroom.
- If you finish the test with 5 minutes or more remaining, you may turn in your test and leave the classroom discreetly; otherwise, please remain seated until the test ends.

After the test

- Stop working immediately when you are instructed to do so.
- Turn in all 21 pages of this test; if you tore out any pages, put them back in their correct positions.

Do not write on this page

1. (a) Define what it means for a proposition to be a contradiction **[5]**

(b) Consider the following logical formula **[15]**

$$\varphi : \forall n \in \mathbb{Z}^+, \forall m \in \mathbb{Z}^+, [\exists x, y \in \mathbb{Z}, nx + my = 1 \Rightarrow \exists a \in \mathbb{Z}, na \equiv 1 \mod m]$$

(i) Express the above statement in natural English. **[5]**

(i) Write the negation of the above logical formula in a maximally negated form **[5]**

(i) Determine whether φ or $\neg\varphi$ is true. Justify your answer **[5]**

Suggested solutions:

(a) A proposition is a contradiction when it is always false regardless of the truth values of its propositional variables.

(b) (i) For any positive integers n, m, if there are integers x, y such that $nx + my = 1$, then n has a multiplicative inverse modulo m (there is an integer a such that na is congruent to 1 modulo m).

(ii) $\exists n \in \mathbb{Z}^+, \exists m \in \mathbb{Z}^+, [\forall x, y \in \mathbb{Z}, nx + my = 1 \wedge \forall a \in \mathbb{Z}, na \not\equiv 1 \pmod{m}]$

(iii) φ is true: Let $n, m \in \mathbb{Z}^+$. Assume there are $x, y \in \mathbb{Z}$ such that $nx + my = 1$. Then $nx = 1 - my$ and $nx \equiv 1 \pmod{m}$. Therefore $\exists a \in \mathbb{Z}, na \equiv 1 \pmod{m}$ (when $a = x$).

More space for (Q1)

2. (a) Write the set $\mathscr{P}(\{1,2\} \times \{0\})$ in list notation **[5]**

(b) Let A and B be sets. Decide whether the following statement is true: **[10]**

$$(A \times B) \setminus (B \times B) = (A \setminus B) \times B$$

If it is true, prove it. Otherwise, provide a counterexample.

Suggested solutions:

(a) $\{1,2\} \times \{0\} = \{(1,0),(2,0)\}$ so

$$\mathscr{P}(\{1,2\} \times \{0\}) = \{\emptyset, \{(1,0)\}, \{(2,0)\}, \{(1,0),(2,0)\}\}$$

(b) True: Let $(x,y) \in (A \times B) \setminus (B \times B)$. $(x,y) \in A \times B$ and $(x,y) \notin B \times B$. The former implies $x \in A$ and $y \in B$. Since $(x,y) \notin B \times B$ and $y \in B$, we have $x \notin B$. Combining with $x \in A$, we have $x \in A \setminus B$. Therefore $(x,y) \in (A \setminus B) \times B$.

Conversely, let $(x,y) \in (A \setminus B) \times B$. $x \in A \setminus B$ and $y \in B$. The former implies $x \in A$ and $x \notin B$. Since $x \in A$ and $y \in B$, $(x,y) \in A \times B$. Since $x \notin B$ (regardless of where y is in), $(x,y) \notin B \times B$. Therefore, $(x,y) \in (A \times B) \setminus (B \times B)$.

More space for (Q2)

3. (a) Define the two-sided inverse of a function **[5]**

(b) Let $f : X \to Y$ and $g : Y \to Z$ be functions. Let A be a subset of X. Consider the statement **[15]**

$$g^{-1}[g \circ f[A]] = f[A]$$

(i) Find a counterexample to prove that the above statement is false **[5]**

(i) One of the set inclusions ($\subseteq$ or $\supseteq$) for the above statement is always true. Determine which inclusion is true and prove it. **[10]**

Suggested solutions:

(a) Let $f : X \to Y$. The two-sided inverse g of f satisfies $g \circ f = \mathrm{id}_X$ and $f \circ g = \mathrm{id}_Y$.

(b) (i) Let $f : \mathbb{R} \to \mathbb{R}$ be defined by $f(x) = x$ for $x \in \mathbb{R}$, $A = \{1\}$, $g : \mathbb{R} \to \mathbb{R}$ be defined by $g(x) = x^2$ for $x \in \mathbb{R}$. Then $g^{-1}[g \circ f[A]] = g^{-1}[\{1\}] = \{-1, 1\}$ while $f[A] = \{1\} \neq \{-1, 1\}$.

(ii) We prove $f[A] \subseteq g^{-1}[g \circ f[A]]$. Let $y \in f[A]$. There exists $x \in A$ such that $y = f(x)$. Consider $g(y) = g(f(x)) = g \circ f(x) \in g \circ f[A]$. By the definition of pre-image, $y \in g^{-1}[g \circ f[A]]$ as desired.

More space for (Q3)

4. (a) Prove that for all $n \in \mathbb{N}$, $2|(3^n - 1)$ **[10]**

(b) Prove that for all $n \in \mathbb{N}$, **[10]**

$$\sum_{k=0}^{n} k \cdot k! = (n+1)! - 1$$

Suggested solutions:

(a) Base case $n = 0$: $3^0 - 1 = 1 - 1 = 0$ is divisible by 2. Assume $2 \mid 3^n - 1$ for some $n \in \mathbb{N}$. There is $k \in \mathbb{N}$ such that $2k = 3^n - 1$. Inductive step: $3^{n+1} - 1 = 3 \cdot 3^n - 1 = 2 \cdot 3^n + (3^n - 1) = 2 \cdot (3^n + k)$ which is also divisible by 2.

(b) Base case $n = 0$: LHS$= \sum_{k=0}^{0} k \cdot k! = 0 \cdot 0! = 0 \cdot 1 = 0$. RHS$= (0+1)! - 1 = 1 - 1 = 0 =$LHS. Assume $\sum_{k=0}^{n} k \cdot k! = (n+1)! - 1$ for some $n \in \mathbb{N}$.

$$\begin{aligned}
\sum_{k=0}^{n+1} k \cdot k! &= \sum_{k=0}^{n} k \cdot k! + (n+1) \cdot (n+1)! \\
&= (n+1)! - 1 + (n+1) \cdot (n+1)! \\
&= (n+1)!(1 + (n+1)) - 1 \\
&= (n+1)!(n+2) - 1 \\
&= (n+2)! - 1
\end{aligned}$$

More space for (Q4)

5. (a) State the addition principle **[5]**

(b) Let $n \geq 3$. Use the addition and the multiplication principles to prove that **[10]**

$$\binom{n}{4} = \sum_{k=3}^{n-1} (n-k) \binom{k-1}{2}$$

Suggested solutions:

(a) Let $\{X_i : i \in I\}$ be a finite family of finite sets that partition X. Then X is finite and $|X| = \sum_{i \in I} |X_i|$.

(b) LHS: Pick a 4-element subset A from $[n]$.

RHS: Let k be the second-largest element of A. k is between 3 and $n-1$. Fix k. We need to form A. It suffices to pick the smallest, the second-smallest and the largest elements. The smallest and the second-smallest elements are picked from $1, \ldots, k-1$. There are $\binom{k-1}{2}$ choices. The largest element is picked from $k+1, \cdots, n$. There are $\binom{n-k}{1} = n-k$ choices. By the multiplication principle, there are $(n-k)\binom{k-1}{2}$ to form A. By the addition principle as k varies, there are $\sum_{k=3}^{n-1}(n-k)\binom{k-1}{2}$ choices.

More space for (Q5)

6. (a) Define the binomial coefficient as the cardinality of a set **[5]**

(b) Let S be the set of all functions from $[9]$ to $[4]$ that send exactly 3 inputs to 1. That is **[10]**

$$S = \{f : [9] \to [4] : |f^{-1}[\{1\}]| = 3\}$$

Find $|S|$ and use a combinatorial argument to justify your answer

Suggested solutions:

(a) Let $k \leq n$ be natural numbers. $\binom{n}{k}$ is the number of k-element subsets of $[n]$.

(b) $|S| = \binom{9}{3} \cdot 3^6$.

There are $\binom{9}{3}$ choices to pick 3 elements from the domain that map to 1. The rest of the 6 elements will go to $\{2,3,4\}$. There are three choices for each of them. By the multiplication principle, there are 3^6 choices for those 6 elements. In total there are $\binom{9}{3} \cdot 3^6$ choices.

More space for (Q6)

7. (a) Use the Euclidean Algorithm to decide whether 35 has a multiplicative inverse mod 254. If it does, use the Extended Euclidean Algorithm to find such an inverse **[10]**

(b) Let p and q be distinct primes. Prove that **[10]**

$$\forall a \in \mathbb{Z}, [pq \mid a^2 \Rightarrow p \mid a \wedge q \mid a]$$

(Make sure to clearly state any theorems used in your proof)

Suggested solutions:

(a)

$$\begin{aligned} 254 &= 7 \cdot 35 + 9 \\ 35 &= 3 \cdot 9 + 8 \\ 9 &= 8 + 1 \\ 1 &= 9 - 8 \\ &= 9 - (35 - 3 \cdot 9) \\ &= 4 \cdot 9 - 35 \\ &= 4 \cdot (254 - 7 \cdot 35) - 35 \\ &= 4 \cdot 254 - 29 \cdot 35 \end{aligned}$$

The multiplicative inverse of 35 modulo 254 is -29.

(b) Let $a \in \mathbb{Z}$. Assume $pq \mid a^2$. Then both $p \mid a^2$ and $q \mid a^2$. Since $p \mid a^2$, by Euclid's Lemma, $p \mid a$ (or $p \mid a$). Similarly, since $q \mid a^2$, by Euclid's Lemma, $q \mid a$. Therefore $p \mid a \wedge q \mid a$.

More space for (Q7)

8. Let A be a nonempty set and suppose that R and S are two equivalence relations on A. Define another relation $\approx$ on A as follows **[15]**

$$\forall a, b \in A, [a \approx b \Leftrightarrow aRb \vee aSb]$$

That is, $a \approx b$ if and only if a and b are related under R or a and b are related under S. Prove or provide a counterexample for each of the following:

(a) $\approx$ is reflexive **[5]**

(b) $\approx$ is symmetric **[5]**

(c) $\approx$ is transtive **[5]**

Suggested solutions:

(a) True: Let $a \in A$. Since R is an equivalence relation on A, R is reflexive and we have aRa. Thus $aRa \vee aSa$. It means $a \approx a$. Since a is arbitrary, $\approx$ is reflexive.

(b) True: Let $a, b \in A$. Assume $a \approx b$. Then $aRb \vee aSb$. Without loss of generality assume aRb. By the symmetry of R, we have bRa. Hence $bRa \vee bSa$. It means $b \approx a$. Therefore $\approx$ is symmetric.

(c) False: Let $A = \mathbb{N}$, R be $\equiv \pmod 2$ and S be $\equiv \pmod 3$. Then $1R3$ and $3S6$. This implies $1R3 \vee 1S3$ and $3R6 \vee 3S6$. However, $1R6 \vee 1S6$ is not true because $6 - 1 = 5$ is not divisible by 2 or 3.

Comments:

Students should state what properties of R and S they use. For (b), they should explain how the symmetry properties distribute across the disjunction (by cases or without loss of generality). For (c), it is not sufficient to state where a specific proof does not go through – there might be other ways to prove the statement. A counterexample should include a definition of A, R, S. The relations $\leq$ and $\geq$ are partial orders but not equivalence relations.

More space for (Q8)

9. Decide if each of the following is true or false by circling **T** or **F**. No justification needed.

(a) **T** **F** $(\mathbb{R} \times \mathbb{Z}) \cup (\mathbb{Z} \times \mathbb{R}) = \mathbb{R} \times \mathbb{R}$ **[3]**

(b) **T** **F** Let $f : X \to Y$ be a surjective function. Then for all $y \in Y$, $f^{-1}[\{y\}] \neq \varnothing$ **[3]**

(c) **T** **F** In a poset $(S, \preccurlyeq)$, there could be a subset $T \subseteq S$ that has a greatest element but does not have a supremum **[3]**

(d) **T** **F** Let n be a positive integer. The Pigeonhole Principle tells us that if we place $3n$ pigeons into n holes then one hole will have at least 3 pigeons. **[3]**

(e) **T** **F** Let $a, b, d \in \mathbb{Z}$. If there exist integers r and s such that $ra + sb = d$, then $d = \gcd(a, b)$. **[3]**

Suggested solutions:

(a) F ($(0.5, 0.5)$ is on RHS but not LHS)

(b) T

(c) F (A greatest element is automatically the supremum.)

(d) T

(e) F ($\gcd(a, b) \mid d$ instead of $\gcd(a, b) = d$.)

If you use this page to continue a solution to a question, please clearly indicate on the first page of your solution where it is continued (this is page 19).

If you use this page to continue a solution to a question, please clearly indicate on the first page of your solution where it is continued (this is page 20).

Initials

Do not write on this page