Full name	Andrew ID

21-127 Final (practice)

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 18–21), 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 22 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 tautology **[5]**

Suggested solution:

A proposition is a tautology when it is always true regardless of the truth values of its propositional variables.

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

$$\varphi : \forall X, \forall Y, [(\exists n \in \mathbb{N}, |X| = n \wedge \exists f : X \to Y, f \text{ is injective}) \Rightarrow \exists m \in \mathbb{N}, |Y| = m]$$

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

Suggested solution:

For any sets X, Y, if X has a finite size (size n for some natural number n) and there is an injection from X to Y, then Y also has a finite size (size m for some natural number m).

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

Suggested solution:

$$\neg\varphi : \exists X, \exists Y, [(\exists n \in \mathbb{N}, |X| = n \wedge \exists f : X \to Y, f \text{ is injective}) \wedge (\forall m \in \mathbb{N}, |Y| \neq m]$$

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

Suggested solution:

$\neg\varphi$ is true: Let $X = \{1\}$, $Y = \mathbb{N}$ and $f : \{1\} \to \mathbb{N}$ be defined by $f(1) = 1$. Then X is finite but Y is infinite.

More space for (Q1)

2. (a) Write the set $\{X \in \mathscr{P}(\{1,2,3\}) : 3 \in X\}$ in list notation **[5]**

Suggested solution:

$$\{\{3\},\{1,3\},\{2,3\},\{1,2,3\}\}$$

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

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

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

Suggested solution:

True: Let $(x,y) \in (A \cap B) \times A$. Then $x \in A \cap B$ and $y \in A$. Since $x \in A \cap B$, $x \in A$ and $x \in B$. Since $x \in A$ and $y \in A$, $(x,y) \in A \times A$. Since $x \in B$ and $y \in A$, $(x,y) \in B \times A$. Therefore $(x,y) \in (A \times A) \cap (B \times A)$.

Conversely, let $(x,y) \in (A \times A) \cap (B \times A)$. Then $(x,y) \in A \times A$ and $(x,y) \in B \times A$. The former implies $x \in A$ and $y \in A$. The latter implies $x \in B$ (and $y \in A$). Since $x \in A$ and $x \in B$, we have $x \in A \cap B$. Combining with $y \in A$, we have $(x,y) \in (A \cap B) \times A$.

More space for (Q2)

3. (a) Define composition of functions **[5]**

Suggested solution:

Let $f : X \to Y$, $g : Y \to Z$. The composition $g \circ f$ is a function $X \to Z$ such that for all $x \in X$, we have $(g \circ f)(x) = g(f(x))$.

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

$$f[(g \circ f)^{-1}[B]] = g^{-1}[B]$$

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

Suggested solution:

Let $f : \mathbb{R} \to \mathbb{R}$ be defined by $f(x) = x^2$; $g : \mathbb{R} \to \mathbb{R}$ be defined by $g(x) = x$, $B = \mathbb{R}$, $C = \{x \in \mathbb{R} \mid x \geq 0\} \subset B$.

LHS$= f[f^{-1}[B]] = f[\mathbb{R}] = C$.

RHS$= g^{-1}[B] = B \neq C$.

(ii) 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 solution:

We prove $f[(g \circ f)^{-1}[B]] \subseteq g^{-1}[B]$. Let $y \in f[(g \circ f)^{-1}[B]]$. There is $x \in (g \circ f)^{-1}[B]$ such that $f(x) = y$. Since $x \in (g \circ f)^{-1}[B]$, $g \circ f(x) \in B$. Then $g(y) \in B$, showing that $y \in g^{-1}[B]$.

More space for (Q3)

4. (a) Prove that for all $n \in \mathbb{N}$, $4|5^n - 1$ **[10]**

Suggested solution:

Base case: $5^0 - 1 = 1 - 1 = 0$ is divisible by 4.

Assume $4|5^n - 1$ for some $n \in \mathbb{N}$. Then there exists $k \in \mathbb{N}$ such that $5^n - 1 = 4k$.

Inductive step: $5^{n+1} - 1 = 5 \cdot 5^n - 1 = 5 \cdot (4k+1) - 1 = 4(5k+1)$ which is divisible by 4.

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

$$\sum_{k=0}^{n} 4^k = \frac{4^{n+1} - 1}{3}$$

Suggested solution:

Base case: $\sum_{k=0}^{0} 4^k = 4^0 = 1$ and $\frac{4^1 - 1}{3} = 1$.

Assume for some $n \in \mathbb{N}$, $\sum_{k=0}^{n} 4^k = \frac{4^{n+1}-1}{3}$.

Inductive step:

$$\begin{aligned}
\sum_{k=0}^{n+1} 4^k &= \sum_{k=0}^{n} 4^k + 4^{n+1} \\
&= \frac{4^{n+1} - 1}{3} + 4^{n+1} \\
&= \frac{4^{n+1} - 1 + 3 \cdot 4^{n+1}}{3} \\
&= \frac{4^{n+2} - 1}{3}
\end{aligned}$$

More space for (Q4)

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

Suggested solution:

Let $m,n,q \in \mathbb{N}$, X,Y be sets such that $|X| = m$, $|Y| = n$, $f : X \to Y$. If $m > q \cdot n$, then there exists $y \in Y$ such that $|f^{-1}[\{y\}]| > q$.

(b) Let S be the set of all functions from $[9]$ to $[4]$ that send 2 and 3 to the same output and 1 and 8 to the same output. That is **[10]**

$$S = \{f : [9] \to [4] : f(2) = f(3) \wedge f(1) = f(8)\}$$

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

Suggested solution:

To decide a function $f \in S$, it suffices to define the values $f(x)$ for $x = 1,\dots,9$. $f(3)$ and $f(8)$ will be the same as $f(2)$ and $f(1)$ respectively, so we only need to consider the 7 inputs $x = 1,2,4,5,6,7,9$. There are 4 possible outputs for each input. Therefore $|S| = 4^7$.

More space for (Q5)

6. (a) Use the Euclidean Algorithm to decide whether 74 has a multiplicative inverse mod 383. If it does, use the Extended Euclidean Algorithm to find such an inverse **[10]**

Suggested solution:

$$\begin{aligned}
383 &= 5 \cdot 74 + 13 \\
74 &= 5 \cdot 13 + 9 \\
13 &= 9 + 4 \\
9 &= 2 \cdot 4 + 1
\end{aligned}$$

Since $\gcd(74, 383) = 1$, 74 has a multiplicative inverse modulo 383.

$$\begin{aligned}
1 &= 9 - 2 \cdot 4 \\
&= 9 - 2 \cdot (13 - 9) \\
&= 3 \cdot (74 - 5 \cdot 13) - 2 \cdot 13 \\
&= 3 \cdot 74 - 17 \cdot (383 - 5 \cdot 74) \\
&= 88 \cdot 74 - 17 \cdot 383
\end{aligned}$$

Thus $88 \cdot 74 - 17 \cdot 383 = 1$ and 88 is a multiplicative inverse of 74.

(b) Let p be a prime. Use Euclid's Lemma to prove that $\sqrt{p}$ is irrational **[10]**

Suggested solution:

Suppose $\sqrt{p}$ is rational. There exists $a \in \mathbb{Z}$, $b \in \mathbb{Z} \setminus \{0\}$ such that $\sqrt{p} = a/b$. By cancelling common factors, we may assume $\gcd(a, b) = 1$.

$$\begin{aligned}
\sqrt{p} &= a/b \\
p &= a^2/b^2 \\
pb^2 &= a^2 \\
p &\mid a^2 \\
p &\mid a \text{ by Euclid's Lemma} \\
a &= kp \text{ for some integer } k \\
pb^2 &= a^2 = k^2 p^2 \\
b^2 &= k^2 p \\
p &\mid b^2 \\
p &\mid b \text{ by Euclid's Lemma}
\end{aligned}$$

contradicting $\gcd(a, b) < p$.

More space for (Q6)

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

Suggested solution:

Let $\{U_i \mid i \leq n\}$ be a partition of a set X where each U_i is finite and $n \in \mathbb{N}$. Then X is finite and $|X| = \sum_{i=1}^{n} |U_i|$.

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

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

Suggested solution:

LHS picks the number of 3-element subsets A from $[n]$.

RHS: Let k be the value of the smallest element of A. Then k is between 1 and $n-2$. After k is decided, the middle and largest elements are from $k+1,\ldots,n$. There are $\binom{n-k}{2}$ choices, which is the same as $\frac{(n-k)(n-k-1)}{2}$ (there are $(n-k)(n-k-1)$ to pick two elements in order, and we half the number to count unordered sets). Since the cases for k is mutually exclusive and exhaustive, there are $\sum_{k=1}^{n-2} \frac{(n-k)(n-k-1)}{2}$ choices in total.

More space for (Q7)

8. (a) Let S be all the functions from $[3]$ to $[3]$. Define the relation $\preccurlyeq$ on S as follows: **[10]**

$$\forall f,g \in S, (f \preccurlyeq g \Leftrightarrow \forall x \in [3], f(x) \leq g(x)$$

Prove that $(S, \preccurlyeq)$ is a poset

Suggested solution:

Reflexivity: Let $f \in S$ and $x \in [3]$. Then $f(x) \leq f(x)$ trivially. So $f \preccurlyeq f$.

Anti-symmetry: Let $f,g \in S$ and assume $f \preccurlyeq g$ and $g \preccurlyeq f$. Then for each $x \in [3]$, $f(x) \leq g(x)$ and $g(x) \leq f(x)$. Therefore $f(x) = g(x)$. Since x is arbitrary, $f = g$.

Transitivity: Let $f,g,h \in S$ and assume $f \preccurlyeq g$ and $g \preccurlyeq h$. Then for each $x \in [3]$, $f(x) \leq g(x)$ and $g(x) \leq h(x)$. Therefore $f(x) \leq h(x)$. Since x is arbitrary, $f \preccurlyeq h$.

(b) Find an example of a subset T of S that has a infimum but does not have a least element. **[5]**
Justify your answer

Suggested solution:

Let $T = \{f,g\}$ where $f(1) = 1$, $f(2) = 1$, $f(3) = 2$, $g(1) = 1$, $g(2) = 2$, $g(3) = 1$. T does not have a least element because $f(3) > g(3)$ so $f \not\preccurlyeq g$; $g(2) > f(2)$ so $g \not\preccurlyeq f$.

The only lower bound (hence infimum) of T is the constant function $1 \notin T$.

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** $(\mathbb{R}\times\mathbb{Z})\cap(\mathbb{Z}\times\mathbb{R}) = \mathbb{Z}\times\mathbb{Z}$ **[3]**

Suggested solution: T

(b) **T** **F** Let $f : X \to Y$ be an injective function. Then for all $y \in Y$, $|f^{-1}[\{y\}]| = 1$ **[3]**

Suggested solution: F ($|f^{-1}[\{y\}]| = 0$ when y is not in the range of f; f is not surjective).

(c) **T** **F** Let a, b, n be positive integers. Then **[3]**

$$ab \equiv 0 \mod n \Rightarrow (a \not\equiv 0 \mod n) \vee (b \not\equiv 0 \mod n)$$

.

Suggested solution: F ($a = b = n = 3$)

(d) **T** **F** The pigeonhole principle implies that if we place $n+1$ pigeons into n holes, then each hole will have at least one pigeon. **[3]**

Suggested solution: F (it guarantees that *there exists* a hole with two pigeons; the function might not be surjective)

(e) **T** **F** Let $A \subseteq X$ where both A and X are infinite sets. Then, $|X \setminus A| < |X|$. **[3]**

Suggested solution: F ($X = \mathbb{Z}, A = \mathbb{N}$)

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 18).

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).

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 21).

Do not write on this page