Staff Solutions to Midterm Exam March 18, afternoon

Problem 1 (Predicates & Sets) (15 points).
Six assertions about sets are bulleted below. There are seven predicate formulas that express some of these assertions. Write the number of each formula next to the bulleted assertion it expresses. For example, you should write “2” next to the first assertion, since formula 2 expresses the assertion that $x = y$. Write “none” next to an assertion that no formula expresses.

Variables $x, y, z \ldots$ range over sets. More than one formula may express the same bulleted assertion.

- $x = y$.
  
  Solution. 2

- $x = \{y, z\}$.
  
  Solution. 1

- $x \subseteq y$.
  
  Solution. 3,7

- $x = y \cup z$.
  
  Solution. 4

- $|x| \leq 3$.
  
  Solution. 5

- $|x| > 3$.
  
  Solution. 6

1. $\forall w. w \in x \iff (w = y \text{ OR } w = z)$.
2. $\forall z. (z \in x \iff z \in y)$.
3. $\forall z. z \in x \implies z \in y$.
4. $\forall w. w \in x \iff (w \in y \text{ OR } w \in z)$.
5. $\exists x_1, x_2, x_3. \forall z. z \in x \implies (z = x_1 \text{ OR } z = x_2 \text{ OR } z = x_3)$.
6. $\forall x_1, x_2, x_3. \exists z. z \in x \text{ AND } z \neq x_1 \text{ AND } z \neq x_2 \text{ AND } z \neq x_3$
7. $(x - y) = \emptyset$.
Problem 2 (Remainder Arithmetic) (15 points).
What is \( \text{rem}(24^{79}, 79) \)?

*Hint:* You should not need to do any actual multiplications!

**Solution.** 24.

Note that 79 is prime.

Now Fermat’s Little Theorem says that \( n^{78} = 1 \pmod{79} \) for all \( n \in (0, 79) \). So

\[
24^{79} = 24 \cdot 24^{78} = 24 \cdot 1 = 24 \pmod{79},
\]

which is equivalent to the assertion that \( \text{rem}(24^{79}, 79) = 24 \).

\[\square\]

Problem 3 (Induction) (25 points).
Prove by induction that the gcd of a finite set of integers is an integer linear combination of the numbers in the set. You may assume that the gcd of two integers is an integer linear combination of them, which was proved in the text. You may also assume the easily verified fact that

\[
\gcd(A \cup \{a\}) = \gcd(\gcd(A), a),
\]

for any nonempty set \( A \) of integers.

Be sure to clearly state and label your Induction Hypothesis, Base case(s), and Induction step.

**Solution.** We proceed by induction on \( n \) with induction hypothesis

\[
P(n) := \text{the gcd of set of } n \text{ of integers is an integer linear combination of the integers in the set.}
\]

Alternatively,

\[
P(n) := \forall a_1, a_2, \ldots, a_n \in \mathbb{Z} \exists s_1, s_2, \ldots, s_n \in \mathbb{Z} \text{. } \gcd(a_1, a_2, \ldots, a_n) = s_1a_1 + s_2a_2 + \cdots + s_na_n.
\]

**Base case:** \( (n = 1) \). Let \( s_1 = 1 \).

**Inductive step:** Now we assume \( P(n) \) holds for some \( n \geq 1 \) and prove \( P(n + 1) \).

Let \( A := \{a_1 \cdots a_n \cdot a\} \). So \( P(n) \) implies that

\[
\gcd(A) = s_1a_1 + s_2a_2 + \cdots + s_na_n.
\]

Now

\[
\gcd(a_1, a_2, \ldots, a_{n+1}) = \gcd(\gcd(a_1, a_2, \ldots, a_n), a_{n+1}) \quad \text{(by (1))}
\]

\[
= s \gcd(a_1, a_2, \ldots, a_n) + ta_{n+1} \text{ for some } s, t \in \mathbb{Z} \quad \text{(the two element case)}
\]

\[
= s(s_1a_1 + s_2a_2 + \cdots + s_na_n) + ta_{n+1}
\]

\[
= (ss_1)a_1 + (ss_2)a_2 + \cdots + (ss_n)a_n + ta_{n+1}.
\]

This shows that \( \gcd(a_1, a_2, \ldots, a_{n+1}) \) is also a linear combination of \( a_1, a_2, \ldots, a_{n+1} \), which proves \( P(n + 1) \) holds, completing the inductive step.

By induction, the claim holds for all \( n \geq 1 \).

\[\square\]

Problem 4 (Preserved Invariant) (20 points).
The *Fast Exponentiation* state machine is defined as follows:
1. The set of states is $\mathbb{R} \times \mathbb{R} \times \mathbb{N}$,
2. The start state is $(a, 1, b)$,
3. the transitions are defined by the rule

$$(x, y, z) \rightarrow \begin{cases} (x^2, y, \text{quotient}(z, 2)) & \text{if } z \text{ is positive and even,} \\ (x^2, xy, \text{quotient}(z, 2)) & \text{if } z \text{ is positive and odd.} \end{cases}$$

(a) Verify that the predicate $P(x, y, z) := [yx^z = ab]$ is a preserved invariant.

**Solution.** We show that $P$ is preserved, namely, assuming $P(x, y, z)$, that is,

$$yx^z = ab \quad (2)$$

holds and $(x, y, z) \rightarrow (x', y', z')$ is a transition, then $P(x', y', z')$, that is,

$$y'x'^{z'} = ab$$

holds.

We consider two cases:

If $z > 0$ and is even, then we have that $x' = x^2$, $y' = y$, $z' = \text{quotient}(z, 2)$. Therefore,

$$y'x'^{z'} = yx^{2 \cdot \text{quotient}(z, 2)}
= yx^{2(z/2)}
= yx^z
= ab \quad \text{(by (2))}$$

If $z > 0$ and is odd, then we have that $x' = x^2$, $y' = xy$, $z' = \text{quotient}(z, 2)$. Therefore,

$$y'x'^{z'} = xyx^{2 \cdot \text{quotient}(z, 2)}
= xy^{1+2(z-1)/2}
= xy^{1+(z-1)}
= yx^z
= ab \quad \text{(by (2))}$$

So in both cases, $P(x', y', z')$ holds, proving that $P$ is a preserved invariant.

(b) Prove that the algorithm is partially correct: if it stops, it does so with $y = ab$.

**Solution.** $P$ holds for the start state $(a, 1, b)$ since $1 \cdot ab = ab$. So by the Invariant Principle 5.4.3, $P$ holds for all reachable states. But a stopped state must have $z = 0$, so if any stopped state $(x, y, 0)$ is reachable, then $y = yx^0 = ab$ as required.

**Problem 5 (Structural Induction) (25 points).**

**Definition.** The rational functions, RAF, of a single variable, $x$, are defined recursively as follows:

**Base cases:**
The identity function, id(x) := x, and any constant function are in RAF.

**Constructor cases:**
If f, g are in RAF, then so are f + g, f · g, and 1/f.
Prove by structural induction that RAF is closed under taking derivatives. That is, using the induction hypothesis,

\[ P(h) := [h' \in RAF], \]

where \( h' := dh/dx \), prove that \( P(h) \) holds for all functions, \( h \in RAF \).

(a) Prove the base cases of the structural induction.

**Solution.** Proof. We must show \( P(id(x)) \) and \( P(constant-function) \). But id' is the constant function 1, and the derivative of a constant function is the constant function 0, and these are in RAF by definition.
This proves that the induction hypothesis holds in the Base cases.

(b) Prove the constructor cases of the structural induction.

**Solution.** Proof. Assuming \( f, g \in RAF, P(f) \) and \( P(g) \), we must prove \( P(h) \) where

Case \( h = f + g \): In this case,

\[ h' = f' + g', \]

and since \( f' \) and \( g' \) are in RAF by hypothesis, so is their sum by the constructor rules, which proves \( P(h) \).

Case \( h = f \cdot g \):
The Product Rule of derivatives states that:

\[ h' = f' \cdot g + f \cdot g', \] (3)

and since \( f, f', g, g' \in RAF \) by hypothesis, so is the right hand side of (3) by the constructor rules, which proves \( P(h) \).

Case \( h = \frac{1}{f} \):
The Chain Rule gives:

\[ h' = \frac{-1}{f^2} \cdot f', \] (4)

and since \( f \) and \( f' \) are in RAF by hypothesis, so is the right hand side of (4) by the constructor rules, which proves \( P(h) \).

We have shown that the induction hypothesis holds in all Constructor cases. This completes the proof by structural induction.