Staff Solutions to Midterm Exam March 18

Problem 1 (Predicates & Relations) (15 points). (a) Five assertions about a binary relation \( R : A \to B \) are bulleted below. There are six predicate formulas that express some of these assertions. Write the number of each formula next to the bulleted assertion it expresses, if there is one. For example, you should write “2” next to the last bulleted assertion, since formula 2 expresses that \( R \) is the identity relation. Write “none” next to an assertion that no formula expresses.

Variables \( a, a_1, \ldots \) range over the domain \( A \) and \( b, b_1, \ldots \) range over the codomain \( B \). More than one formula may express the same bulleted assertion, and some formulas may not express any bulleted assertion.

- \( R \) is a surjection
  
  Solution. none

- \( R \) is an injection
  
  Solution. 5

- \( R \) is a function
  
  Solution. 4,6

- \( R \) is total
  
  Solution. 1

- \( R \) is the identity relation.
  
  Solution. 2

1. \( \forall a. \exists b. a \mathbin{R} b \).
2. \( \forall a, b. a \mathbin{R} b \iff a = b. \)
3. \( \forall a, b. a \mathbin{R} b \text{ OR } a \neq b. \)
4. \( \forall b_1, b_2, a. (a \mathbin{R} b_1 \text{ AND } a \mathbin{R} b_2) \implies b_1 = b_2. \)
5. \( \forall a_1, a_2, b. (a_1 \mathbin{R} b \text{ AND } a_2 \mathbin{R} b) \implies a_1 = a_2. \)
6. \( \forall a_1, a_2, b_1, b_2. (a_1 \mathbin{R} b_1 \text{ AND } a_2 \mathbin{R} b_2 \text{ AND } b_1 \neq b_2) \implies a_1 \neq a_2. \)

(b) Give an example of a relation \( R \) that satisfies three of the properties surjection, injection, total, and function (you indicate which) but is not a bijection.

Solution. Let

\[
A ::= \{1, 2\}, B ::= \{1\}, \text{graph}(R) ::= \{(1, 1)\}.
\]

Then \( R \) is not a bijection because it is not total, and indeed \( |A| \neq |B| \). But \( R \) is an injective, surjective function.

There are lots more possible answers.
Problem 2 (Remainder Arithmetic) (20 points). (a) Calculate the remainder of $35^{86}$ divided by 29.

Solution. Since 29 is prime and 35 is not a multiple of 29, Fermat’s Little Theorem implies that

$$35^{28} \equiv 1 \pmod{29}.$$ 

But $35 = 6 \pmod{29}$ and $86 = 3 \cdot 28 + 2$, so

$$35^{86} = 35^{3 \cdot 28 + 2} = (35^{28})^3 \cdot 35^2 \equiv 1^3 \cdot 6^2 \equiv 7 \pmod{29}.$$ 

Therefore, rem$(35^{86}, 29) = 7$.

(b) Part (a) implies that the remainder of $35^{86}$ divided by 29 is not equal to 1. So there must be a mistake in the following proof, where all the congruences are taken with modulus 29:

\[
\begin{align*}
1 & \neq 35^{86} \quad \text{(by part (a))} \quad (1) \\
& \equiv 6^{86} \quad \text{(since } 35 \equiv 6 \pmod{29}) \quad (2) \\
& \equiv 6^{28} \quad \text{(since } 86 \equiv 28 \pmod{29}) \quad (3) \\
& \equiv 1 \quad \text{(by Fermat’s Little Theorem)} \quad (4)
\end{align*}
\]

Identify the exact line containing the mistake and explain the logical error.

Solution. The mistake occurs at line (3).

Exponents can be replaced by their remainders on division by $\phi(29) = 28$, not on division by 29. So the “explanation” that $86 \equiv 28 \pmod{29}$ on the third line is true, but does not justify that mistaken step.

Problem 3 (Well Ordering) (25 points).

Use the Well Ordering Principle to prove 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 define and clearly label the set of counterexamples you are assuming is nonempty.

Solution. Let

$$C := \{n \geq 1 \mid \exists A \subset \mathbb{Z}, |A| = n \text{ AND } \not\exists \text{gcd}(A) \text{ is a linear combination of } a \in A, \}$$

and assume for the sake of contradiction that $C$ is not empty.

By the WOP, there is a least integer $m \in C$. So there must be integers $a_1, a_2, \ldots, a_m$ such that $\gcd(a_1, a_2, \ldots, a_m)$ is not a linear combination of $a_1, a_2, \ldots, a_m$.

Since $\gcd(\{a_1\}) = 1 \cdot a_1$, we know that $m - 1 \geq 1$. Since $m$ is the smallest element of $C$, it follows that

$$\gcd(a_1, \ldots, a_{m-1}) = s_1a_1 + s_2a_2 + \cdots + s_{m-1}a_{m-1}.$$
Now
\[ \gcd(a_1, a_2, \ldots, a_m) = \gcd(\gcd(a_1, a_2, \ldots, a_{m-1}), a_m) \]  
(by (5))
\[ = s \gcd(a_1, a_2, \ldots, a_{m-1}) + ta_m \text{ for some } s, t \in \mathbb{Z} \]  
(the two element case)
\[ = s(s_1a_1 + s_2a_2 + \cdots + s_na_{m-1}) + ta_m \]
\[ = (ss_1)a_1 + (ss_2)a_2 + \cdots + (ss_{m-1})a_{m-1} + ta_m. \]

This shows that \( \gcd(a_1, a_2, \ldots, a_m) \) is also a linear combination of \( a_1, a_2, \ldots, a_m \), contradicting the choice of \( m \).

The contradiction implies that \( C \) must be empty, proving that the claim holds for all \( n \geq 1 \). \( \blacksquare \)

**Problem 4 (Preserved Invariant) (20 points).**
The following Binary GCD state machine computes the GCD of integers \( a > b > 0 \):

- **states** := \( \mathbb{N}^3 \)
- **start state** := \( (a, b, 1) \)
- **transitions** := if \( \min(x, y) > 0 \), then \( (x, y, e) \rightarrow \) the first possible state according to the rules:
  
  \[
  \begin{align*}
  (1, 0, ex) & \quad \text{(if } x = y) \\
  (1, 0, e) & \quad \text{(if } y = 1), \\
  (x/2, y/2, 2e) & \quad \text{(if } 2 \mid x \text{ and } 2 \mid y), \\
  (x/2, y, e) & \quad \text{(if } 2 \mid x) \\
  (x, y/2, e) & \quad \text{(if } 2 \mid y) \\
  (y, x, e) & \quad \text{(if } y > x) \\
  (x - y, y, e) & \quad \text{(otherwise)}. 
  \end{align*}
  \]

The predicate
\[ \gcd(a, b) = e \gcd(x, y) \]
is claimed to be a preserved invariant of this state machine.

(a) Verify that this predicate is a preserved invariant for the 3rd: \( (x/2, y/2, 2e) \), 4th: \( (x/2, y, e) \) and last: \( (x - y, y, e) \) of the above transition rules. You may assume without proof elementary properties of GCD, but be sure to state your assumptions explicitly.

**Solution.** To verify preserved invariance, we assume the invariant holds for state \( (x, y, e) \) and show that if \( (x, y, e) \rightarrow (x', y', e') \), then \( \gcd(a, b) = e' \gcd(x', y') \).

The proof is by cases according to which kind of transition occurs.

**Case:** \( 2 \mid x \) and \( 2 \mid y \). In this case, \( (x', y', e') = (x/2, y/2, 2e) \).

We use the easily verified fact
\[ \gcd(au, av) = a \gcd(u, v). \]  
(6)

Now
\[ \gcd(a, b) = e \gcd(x, y) \]  
(by the invariant for \( (x, y, e) \))
\[ = e2 \gcd(x/2, y/2) \]  
(by (6))
\[ = e' \gcd(x', y'). \]
which shows that the invariant holds for \((x', y', e')\).

**Case:** (2 \mid x and 2 does not divide \(y\)). In this case, \((x', y', e') = (x/2, y, e)\).

We use the easily verified fact
\[
\gcd(a, u, v) = \gcd(u, v)
\]  (7)
for \(a\) relatively prime to \(v\).

Now
\[
gcd(a, b) = e \gcd(x, y) = e \gcd(x/2, y) = e' \gcd(x', y')
\]
which shows that the invariant holds for \((x', y', e')\).

**Case:** (otherwise clause). In this case \((x', y', e') = (x - y, y, e)\).

We use the easily verified fact that
\[
gcd(u - v, v) = \gcd(u, v)
\]  (8)
Now,
\[
gcd(a, b) = e \gcd(x, y) = e \gcd(x - y, y) = e' \gcd(x', y')
\]
proving that the invariant holds for \((x', y', e')\).

Verification of the remaining cases follows similarly.

(b) Use the Invariant Principle to conclude that if this machine reaches a stopped state \((1, 0, e')\), then \(e' = \gcd(a, b)\).

**Solution.** We first observe that the preserved invariant holds trivially in the start state \((a, b, 1)\) because \(\gcd(a, b) = 1 \cdot \gcd(a, b)\). The Invariant Principle allows us to conclude that the preserved invariant holds in every reachable state.

If a stopped state \((1, 0, e')\) is reachable, then the invariant implies
\[
gcd(a, b) = e' \gcd(1, 0) = e',
\]
as required.

---

**Problem 5 (Structural Induction mod \(n\)) (20 points).**

**Definition.** The set, \(P\), of integer polynomials can be defined recursively:

**Base cases:**
- the identity function, \(i(x) ::= x\) is in \(P\).
- for any integer, \(k\), the constant function, \(c_k(x) ::= k\) is in \(P\).
Constructor cases. If \( r, s \in P \), then \( r + s \) and \( r \cdot s \in P \).

(a) Using the recursive definition of integer polynomial given below, prove by structural induction that for all \( q \in P \),

\[
  j \equiv k \pmod{n} \quad \text{IMPLIES} \quad q(j) \equiv q(k) \pmod{n},
\]

for all integers \( j, k, n \) where \( n > 1 \).

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

**Solution.** The proof is by structural induction on the definition of \( P \). The hypothesis \( H(q) \) is:

\[
  H(q) := j \equiv k \pmod{n} \quad \text{IMPLIES} \quad q(j) \equiv q(k) \pmod{n},
\]

for all \( j, k, n \in \mathbb{Z} \), where \( n > 1 \).

- **Base cases:** \( H(i) \) holds because \( j = i(j) \) and \( k = i(k) \). \( H(c_k) \) holds because \( c_k(i) = c_k(j) \).

- **Constructor cases.** Suppose \( H(r) \) and \( H(t) \) hold, and let \( t := r + s \). To show \( H(t) \), suppose \( j \equiv k \pmod{n} \). Since \( H(r) \) holds, we have that \( r(j) \equiv r(k) \pmod{n} \). Likewise, \( s(j) \equiv s(k) \pmod{n} \). So

\[
  r(j) + s(s) \equiv r(j) + s(k) \pmod{n},
\]

by additivity of congruences Lemma 8.6.4(8.7), that is, \( t(j) \equiv t(k) \pmod{n} \).

The proof for \( t := r \cdot s \) is the same with “\( + \)” replacing “\( \cdot \).”

(b) We’ll say that \( q \) produces multiples if, for every integer greater than one in the range of \( q \), there are infinitely many different multiples of that integer in the range. For example, if \( q(4) = 7 \) and \( q \) produces multiples, then there are infinitely many different multiples of 7 in the range of \( q \).

Prove that if \( q \) has positive degree and positive leading coefficient, then \( q \) produces multiples. You may assume that every such polynomial is strictly increasing for large arguments.

**Hint:** Observe that all the elements in the sequence

\[
  q(k), q(k + v), q(k + 2v), q(k + 3v), \ldots,
\]

are congruent modulo \( v \). Let \( v = q(k) \).

**Solution.** If \( 1 < v \in \text{range}(q) \), then \( v = q(k) \) for some integer \( k \), and we have immediately that

\[
  q(k) \equiv 0 \pmod{v}.
\]

Since \( k \equiv k + nv \pmod{v} \), part (a) implies that each of the elements in the sequence

\[
  q(k), q(k + v), q(k + 2v), q(k + 3v), \ldots
\]

is \( q(k) \equiv 0 \pmod{v} \). So all the elements in the sequence are multiples of \( v \).

Since \( q(k) \) is strictly increasing\(^1\) for \( k \geq b \) for some bound, \( b > 0 \), all the elements in the sequence are different after a certain point (no later than after \( (b/2) \) elements). So there are arbitrarily large multiples of \( v \) in the range of \( q \). Since \( v > 1 \) was an arbitrary element, we conclude there are infinitely many multiples of every element \( v > 1 \) in the range of \( q \). That is, \( q \) produces multiples.

\(^1\)We’ll prove this and similar “growth rate” facts about polynomials and other functions in Chapter 13.
Part (b) implies that an integer polynomial with positive leading coefficient and degree has infinitely many nonprimes in its range. This fact no longer holds true for multivariate polynomials. An amazing consequence of Matijasevich’s solution to Hilbert’s Tenth problem, is that multivariate polynomials can be understood as general purpose programs for generating sets of integers. If a set of nonnegative integers can be generated by any program, then it equals the set of nonnegative integers in the range of a multivariate integer polynomial! In particular, there is an integer polynomial $p(x_1, \ldots, x_7)$ whose nonnegative values as $x_1, \ldots, x_7$ range over $\mathbb{Z}$ are precisely the set of all prime numbers!