Concordia University

Department of Computer Science & Software Engineering

COMP 232/4 **Mathematics for Computer Science** Winter 2016

Assignment 3 Due date: March 24, 2016

1. For each of the following, determine whether it is valid or invalid. If valid then give a proof. If invalid then give a counter example.

   (a) $A \subseteq C$ and $B \subseteq C \;\Leftrightarrow\; A \cup B \;\subseteq C$

   Solution: VALID:

   LHS $\equiv ((x \in A) \to (x \in C)) \wedge ((x \in B) \to (x \in C))$
   $\equiv ((x \notin A) \vee (x \in C)) \wedge ((x \notin B) \vee (x \in C))$
   $\equiv ((x \notin A) \wedge (x \notin B)) \vee (x \in C)$
   $\equiv [\neg\neg((x \notin A) \wedge (x \notin B))] \vee (x \in C)$
   $\equiv [\neg((x \in A) \vee (x \in B)) \vee (x \in C)$
   $\equiv ((x \in A) \vee (x \in B)) \to (x \in C)$
   $\equiv$ RHS

   (b) $(B \cap C) \subseteq A \quad \Rightarrow \quad (C - A) \cap (B - A) \;=\; \emptyset$

   Solution: VALID: We can prove this by contradiction: Suppose $B \cap C \subseteq A$, but $(C - A) \cap (B - A)$ is not empty. Then there exists an element $x \in (C - A) \cap (B - A)$. Thus this x satisfies $x \in C$, $x \in B$ and $x \notin A$. But this contradicts the assumption that $B \cap C \subseteq A$.

(c) $(A \cup B) - (A \cap B) \; = \; A \quad \Rightarrow \quad B = \emptyset$

Solution: VALID: We prove this by contradiction: Suppose $(A \cup B) - (A \cap B) = A$, but B is not empty. Then there exists an element $x \in B$. There are two possible cases:

i. x is also an element of the set A. Then $x \in A \cup B$ and $x \in A \cap B$. Hence $x \notin (A \cup B) - (A \cap B)$. Since $(A \cup B) - (A \cap B) = A$ it follows that $x \notin A$ which is a contradiction.

ii. x is not an element of the set A. Then $x \in A \cup B$ and $x \notin A \cap B$. Hence $x \in (A \cup B) - (A \cap B)$. Since $(A \cup B) - (A \cap B) = A$ it follows that $x \in A$ which is a contradiction.

(d) $(A \times C) \cup (B \times D) \; = \; (A \cup B) \times (C \cup D)$.

Solution: VALID:

Suppose $(x, y) \in (A \times C) \cup (B \times D)$.
Case 1: $(x, y) \in (A \times C)$. Then $x \in A$ and $y \in C \;\Rightarrow\; x \in A \cup B$ and $y \in C \cup D \;\Rightarrow\; (x, y) \in (A \cup B) \times (C \cup D)$.
Case 2: $(x, y) \in (B \times D)$: Similar to Case 1.

Suppose $(x, y) \in (A \cup B) \times (C \cup D)$. $\;\Rightarrow\;\; \Rightarrow\; x \in A \cup B$ and $y \in C \cup D)$
Case 1: $x \in A$ and $y \in C$. $\;\Rightarrow\; (x, y) \in (A \cup C) \;\Rightarrow\; (x, y) \in (A \cup C) \cup (C \times D)$
Case 2: $x \in B$ and $y \in C$. Similar.
Case 3: $x \in A$ and $y \in D$. Similar.
Case 4: $x \in B$ and $y \in D$. Similar.

2. Let $A_i = \{\ldots, -2, -1, 0, 1, 2, \ldots, i\}$ Find

   (a) $\bigcup_{i=1}^{n} A_i$

   Solution: $\{\ldots, -2, -1, 0, 1, 2, \ldots, n\} = A_n$

   (b) $\bigcap_{i=1}^{n} A_i$

   Solution: $\{\ldots, -2, -1, 0, 1\} = A_1$

3. Give one example of a function from $\mathbb{Z}^+$ to $\mathbb{Z}^+$ of each type below:

   (a) both one-to-one and onto

   Solution: $f(n) = n$.

   (b) one-to-one and not onto

   Solution: $f(n) = n + 1$.

   (c) onto and not one-to-one

   Solution: $f(n) = n,$ if n is odd, and $f(n) = n/2,$ if n is even,

   (d) neither one-to-one nor onto.

   Solution: $f(n) = 3$.

4. If A and B are sets and $f : A \to B$, then for any subset S of A we define

$$f(S) \;=\; \big\{ b \in B : b = f(a) \text{ for some } a \in S \big\} \,.$$

Similarly, for any subset T of B we define the *pre-image* of T as

$$f^{-1}(T) \;=\; \big\{ a \in A : f(a) \in T \big\} \,.$$

Note that $f^{-1}(T)$ is well defined even if f does not have an inverse !

Now let $f : \mathbb{R} \to \mathbb{R}$ be defined as $f(x) = x^2$. Let S_1 denote the closed interval $[-2, 1]$, that is all $x \in \mathbb{R}$ that satisfy $-2 \le x \le 1$, and let S_2 be the open interval $(-1, 2)$, that is all $x \in \mathbb{R}$ that satisfy $-1 < x < 2$. Also let $T_1 = S_1$ and $T_2 = S_2$.

Determine

$$f(S_1 \cup S_2)\ ,\ f(S_1) \cup f(S_2)\ ,\ f(S_1 \cap S_2)\ ,\ f(S_1) \cap f(S_2)\ ,$$

and

$$f^{-1}(T_1 \cup T_2)\ ,\ f^{-1}(T_1) \cup f^{-1}(T_2)\ ,\ f^{-1}(T_1 \cap T_2)\ ,\ \text{and } f^{-1}(T_1) \cap f^{-1}(T_2)\ .$$

Solution:

We see that

$$S_1 \cup S_2 = T_1 \cup T_2 = \big\{ x \in \mathbf{R} : -2 \le x < 2 \big\} \qquad S_1 \cap S_2 = T_1 \cap T_2 = \big\{ x \in \mathbf{R} : -1 < x \le 1 \big\}$$

$$f(S_1) = \big\{ x \in \mathbf{R} : 0 \le x \le 4 \big\} \qquad f(S_2) = \big\{ x \in \mathbf{R} : 0 \le x < 4 \big\}$$

$$f^{-1}(T_1) = \big\{ x \in \mathbf{R} : -1 \le x \le 1 \big\} \qquad f^{-1}(T_2) = \big\{ x \in \mathbf{R} : -\sqrt{2} < x < \sqrt{2} \big\}$$

so that

$$f(S_1 \cup S_2) = \big\{ x \in \mathbf{R} : 0 \le x \le 4 \big\} \qquad f(S_1) \cup f(S_2) = \big\{ x \in \mathbf{R} : 0 \le x \le 4 \big\}$$

$$f(S_1 \cap S_2) = \big\{ x \in \mathbf{R} : 0 \le x \le 1 \big\} \qquad f(S_1) \cap f(S_2) = \big\{ x \in \mathbf{R} : 0 \le x < 4 \big\}$$

$$f^{-1}(T_1 \cup T_2) = \big\{ x \in \mathbf{R} : -\sqrt{2} < x < \sqrt{2} \big\} \qquad f^{-1}(T_1) \cup f^{-1}(T_2) = \big\{ x \in \mathbf{R} : -\sqrt{2} < x < \sqrt{2} \big\}$$

$$f^{-1}(T_1 \cap T_2) = \big\{ x \in \mathbf{R} : -1 \le x \le 1 \big\} \qquad f^{-1}(T_1) \cap f^{-1}(T_2) = \big\{ x \in \mathbf{R} : -1 \le x \le 1 \big\}$$

5. Let A and B be arbitrary sets. Let S_1 and S_2 be arbitrary subsets of A, and let T_1 and T_2 be arbitrary subsets of B. For each of the following state whether it is True or False. If True then give a proof. If False then give a counterexample:

(a) $f(S_1 \cup S_2) = f(S_1) \cup f(S_2)$ (b) $f(S_1 \cap S_2) = f(S_1) \cap f(S_2)$

(c) $f^{-1}(T_1 \cup T_2) = f^{-1}(T_1) \cup f^{-1}(T_2)$ (d) $f^{-1}(T_1 \cap T_2) = f^{-1}(T_1) \cap f^{-1}(T_2)$

Solution:

(a)
$$\begin{aligned} b \in f(S_1 \cup S_2) &\iff \exists a \in A : a \in (S_1 \cup S_2) \ \wedge \ f(a) = b \\ &\iff \exists a \in A : (a \in S_1 \vee a \in S_2) \ \wedge \ f(a) = b \\ &\iff \exists a \in A : (a \in S_1 \wedge f(a) = b) \ \vee \ (a \in S_2 \wedge f(a) = b) \\ &\iff b \in f(S_1) \ \vee \ b \in f(S_2) \\ &\iff b \in f(S_1) \cup f(S_2) \ . \end{aligned}$$

(b) This identity is not always valid. A counterexample can be found in Problem 3. What is True is that $f(S_1 \cap S_2) \subseteq f(S_1) \cap f(S_2)$.

(c)
$$\begin{aligned} a \in f^{-1}(T_1 \cup T_2) &\iff \exists b \in B : b \in (T_1 \cup T_2) \ \wedge \ f(a) = b \\ &\iff \exists b \in B : (b \in T_1 \vee b \in T_2) \ \wedge \ f(a) = b \\ &\iff \exists b \in B : (b \in T_1 \wedge f(a) = b) \ \vee \ (b \in T_2 \wedge f(a) = b) \\ &\iff a \in f^{-1}(T_1) \ \vee \ a \in f^{-1}(T_2) \\ &\iff a \in f^{-1}(T_1) \cup f^{-1}(T_2) \ . \end{aligned}$$

(d)
$$\begin{aligned} a \in f^{-1}(T_1 \cap T_2) &\iff \exists b \in B : b \in (T_1 \cap T_2) \ \wedge \ f(a) = b \\ &\iff \exists b \in B : b \in T_1 \ \wedge \ b \in T_2 \ \wedge \ f(a) = b \\ &\iff \exists b \in B : b \in T_1 \wedge f(a) = b \ \wedge \ b \in T_2 \wedge f(a) = b \\ &\iff a \in f^{-1}(T_1) \ \wedge \ a \in f^{-1}(T_2) \\ &\iff a \in f^{-1}(T_1) \cap f^{-1}(T_2) \ . \end{aligned}$$

6. Let $f : \mathbb{Z} \times \mathbb{Z} \to \mathbb{Z} \times \mathbb{Z}$ be defined as $f(m, n) = (m - n, n)$.

   (a) Is f a bijection? If yes, give a proof and derive a formula for f^{-1}. If not, explain why not.

   Solution: f is one-to-one (proof by contrapositive):
   Suppose $f(m_1, n_1) = f(m_2, n_2)$ for $m_1, m_2, n_1, n_2 \in \mathbb{Z}$.
   Then $(m_1 - n_1, n_1) = (m_2 - n_2, n_2)$
   It follows that $n_1 = n_2$ and $m_1 - n_1 = m_2 - n_2$
   If we add n_1 to both sides of the latter, we get $m_1 = m_2$,
   which proofs that f is one-to-one.
   f is onto: Let $(m, n) \in \mathbb{Z} \times \mathbb{Z} \;\Rightarrow\; f(m + n, n) = (m, n)$.
   The inverse is $f^{-1}(m, n) = (m + n, n)$.

   (b) Define the *powers* of f, by $f^1 = f$ and $f^{i+1} = f \circ f^i$. Derive a formula for f^k. Is f^k a bijection? If yes, give a proof and derive a formula for $(f^k)^{-1}$. If not, explain why not.

   Solution:
   We have
   $f^1(m, n) = (m - n, n)$,
   $f^2(m, n) = (m - n - n, n)$,
   $f^3(m, n) = (m - n - n - n, n)$,
   $\ldots,$
   $f^k(m, n) = (m - kn, n)$.

   f^k is one-to-one: Suppose $(m, n) = (m', n') \;\Rightarrow\; m = m'$ and $n = n' \;\Rightarrow\; m - kn = m' - kn' \;\Rightarrow\; f^k(m, n) = f^k(m', n')$.
   f^k is onto: Let $(m, n) \in \mathbb{Z} \times \mathbb{Z} \;\Rightarrow\; f^k(m + kn, n) = (m, n)$.
   The inverse is $f^{-1}(m, n) = (m + kn, n)$.

7. Let $A = \{1, 2, 3, 4, 5\}$.

   (a) How many total functions $f : A \to A$ are there?

   Solution:
   Each of the five elements in A can be mapped (independently of how the other elements in A are mapped) to any of the five elements in A. Consequently, there are $5^5 = 3125$ possible functions $f : A \to A$.

   (b) How many of the functions in (a) are one-to-one?

   Solution:
   Suppose a function f maps 1 to any of the five elements in A. Then there are four choices left for mapping 2, three choices for 3, two choices for 4, and one choice for 5. Consequently, each of the $5! = 120$ permutations of $1, 2, 3, 4, 5$ represents a one-to-one function on A.

8. Prove or disprove the statements below.

   (a) For all positive real numbers x and y, $\lfloor x \cdot y \rfloor \leq \lfloor x \rfloor \cdot \lfloor y \rfloor$.

   Solution: The claim is false.
   Counter-example: $x = y = 1.5$. Then $\lfloor x \cdot y \rfloor = \lfloor 1.5 \cdot 1.5 \rfloor = \lfloor 2.25 \rfloor = 2$, and $\lfloor x \rfloor \cdot \lfloor y \rfloor = \lfloor 1.5 \rfloor \cdot \lfloor 1.5 \rfloor = 1 \cdot 1 = 1$.

   (b) For all positive real numbers x and y, $\lceil x \cdot y \rceil \leq \lceil x \rceil \cdot \lceil y \rceil$.

   Solution: The claim is true.
   Proof: We have $x \leq \lceil x \rceil$ and $y \leq \lceil y \rceil$, and thus $x \cdot y \leq \lceil x \rceil \cdot \lceil y \rceil$. Consequently $\lceil x \cdot y \rceil \leq \Big\lceil \lceil x \rceil \cdot \lceil y \rceil \Big\rceil = \lceil x \rceil \cdot \lceil y \rceil$.

9. (a) Suppose that Hilbert?s Grand Hotel is fully occupied, but the hotel closes all even numbered rooms for maintenance. Show that all guests can remain in the hotel.

   Solution: Move guest in room n to room $2n - 1$.

   (b) Show that a countably infinite number of guests arriving at Hilbert's fully occupied Grand Hotel can be given rooms without evicting any current guest.

   Solution: Move guest currently in room n to room $2n$. Then all odd rooms will be vacant. Since the number of odd rooms is countably infinite, you can move all new guests there.

10. (a) Let a and b be integers, and $m \geq 2$ an integer. Prove that

$$ab \equiv \Big((a \textbf{ mod } m) \times (b \textbf{ mod } m)\Big) (\textbf{mod}\, m)$$

   Solution: The claim holds if $m \Big| \Big(ab - (a \textbf{ mod } m) \times (b \textbf{ mod } m)\Big)$. Let $a = mq + r$ and $b = mq' + r'$. Then $ab = (mq + r)(mq' + r') = mqmq' + mqr' + rmq' + rr' = m(qmq' + qr' + rq') + rr'$.
   We have $(a \textbf{ mod } m)(b \textbf{ mod } m) = rr'$, so $\Big(ab - (a \textbf{ mod } m) \times (b \textbf{ mod } m)\Big) = \Big(ab - rr'\Big) = m(qmq' + qr' + rq')$, which means that $m \Big| \Big(ab - (a \textbf{ mod } m) \times (b \textbf{ mod } m)\Big)$.

   (b) Let $a, b, c,$ and d be integers and $m \geq 2$ an integer. Prove that if $a \equiv b\ (\textbf{mod}\, m)$ and $c \equiv d\ (\textbf{mod}\, m)$, then $a - c \equiv b - d\ (\textbf{mod}\, m)$

   Solution: If $a \equiv b\ (\textbf{mod}\, m)$ then textbook Theorem 4 in Chaper 4.1 tells us that $a = b + km$ for some integer k. Likewise, $c = d + k'm$ for some integer k'.
   Thus $a - c = b - d + m(k - k')$, so by the aforementioned Theorem 4 we can conclude that $a - c \equiv b - d\ (\textbf{mod}\, m)$.

11. Use a proof by cases to show that $gcd(m + n, mn) - gcd(m, n)$ is even for all integers m and n.

Solution:

Case 1: If both m and n are even then both are divisible by 2, and hence both $m + n$ and mn are divisible by 2. Thus the greatest common divisor of $m+n$ and mn must contain the factor 2, i.e., it must be even. Similarly, $gcd(m, n)$ is even. Hence $gcd(m+n, mn)-gcd(m, n)$ is even.

Case 2: If both m and n are odd then $m+n$ is even, while mn is odd. Thus $gcd(m+n, mn)$ cannot contain the factor 2, i.e., it must be odd. Similarly, $gcd(m, n)$ is odd. Hence $gcd(m + n, mn) - gcd(m, n)$ is even.

Case 3: If m is odd and n even then $m+n$ is odd, while mn is even. Thus $gcd(m+n, mn)$ cannot contain the factor 2, i.e., it must be odd. Similarly, $gcd(m, n)$ is odd. Hence $gcd(m + n, mn) - gcd(m, n)$ is even.

Case 4: The case m is even and n odd follows similarly.

12. Prove that if p is prime, and $p|a_1a_2 \cdots a_n$ where each a_i is an integer, then $p|a_i$ for some i.

Solution: Requires induction. Question postponed to Assignment 4.