**Harvard University**

**Computer Science 20**

**Problem Set 3**

Due Thursday, February 22, 2021 at 11:59pm

**SELF CHECK**

- Did you clearly state the claim at the beginning of your proof?
- Did you clearly conclude your proof with a statement of what you have proved?
- Is each assertion either a given fact, a hypothesis, a definition, or a logical conclusion from prior statements?
- Are all of your variables properly introduced and quantified? Is the domain of variables clearly specified?
- Does your proof proceed logically from claim to conclusion?
- Have you removed any extraneous information or tangents that were part of your exploratory work?
- Have you considered corner cases? If you are dividing your proof into cases, have you exhausted all cases?

## PROBLEM 1

**Let $A$, $B$, and $C$ be sets. Prove that $(A - B) \cup (B - C) \subseteq (A \cup B) - (A \cap B \cap C)$.**

Claim:

Given sets $A$, $B$, and $C$, then $(A - B) \cup (B - C) \subseteq (A \cup B) - (A \cap B \cap C)$.

Proof by Cases:

: We are given sets A, B, and C and in order to prove

$(A - B) \cup (B - C) \subseteq (A \cup B) - (A \cap B \cap C)$

In general, if you want $X \subseteq Y$, then you assume $x \in X$ and then prove $x \in Y$.

We use this generalization, in our particular example with a two-prong approach:

| Case 1 | Case 2 |
|---|---|
| Let $x \in (A - B) \cup (B - C)$ | Let $x \in (A - B) \cup (B - C)$ |
| Suppose $x \in (A - B)$ | Suppose $x \in (B - C)$ |
| then $x \in A$ and $x \notin B$ | then $x \in B$ and $x \notin C$ |
| So, we can prove $x \in (A \cup B)$ | So, we can prove $x \in (A \cup B)$ |
| Since, $x \in A$, therefore $x \in (A \cup B)$ | Since, $x \in B$, therefore $x \in (A \cup B)$ |
| Furthermore, since $x \notin B$, | Furthermore, since $x \notin C$, |
| then $x \notin (A \cap B \cap C)$ | then $x \notin (A \cap B \cap C)$ |
| Thus, $x \in (A \cup B) - (A \cap B \cap C)$ | Thus, $x \in (A \cup B) - (A \cap B \cap C)$ |

In conclusion, since in both cases $x \in (A \cup B) - (A \cap B \cap C)$,

then $(A - B) \cup (B - C) \subseteq (A \cup B) - (A \cap B \cap C)$ for sets $A$, $B$, and $C$.

## PROBLEM 2

**For any integers $s$ and $t$, we'll define the set $L(s, t)$ as follows:**

$$L(s, t) = \{sx + ty \mid x, y \in Z\}$$

**Prove the following claim.**

**You may use the theorem proved in class that $a \equiv b \pmod{n}$ if and only if $n \mid (a - b)$.**

Claim:

For any integers $a$, $r$, $m$, where $m$ is positive, if $a \equiv r \pmod{m}$, then $L(a, m) \subseteq L(r, \mathrm{m})$.

Direct Proof:

We will prove that for integers $a$, $r$, $m$, where $m > 0$, if $a \equiv r \pmod{m}$, then $L(a, m) \subseteq L(a, m)$.

To prove this we pick an arbitrary element from $L(a, m)$ and prove that it is in $L(a, m)$.

Suppose some arbitrary element $c \in L(a, m)$, this means $\exists\ x,y \in \mathbb{Z}$ such that $c = ax + my$

Based on the theorem, $m \mid (r - a)$, this means $\exists\ x,y \in \mathbb{Z}$ such that $mn = r - a$

Solving for $a$, $a = r - mn$

We substitute the value of $a$ in $c = ax + my$

Thus we have:

$$c = (r - mn)x + my$$

$$= rx - mnx + my$$

$$= rx + m(-nx + y)$$

In conclusion, r multiplied by an integer plus m multiplied by an integer, which means

$x \in \mathbb{Z}$ , $-nx + y \in \mathbb{Z}$ for a set $c \in L(a, m)$.

Thus, for any integers $a$, $r$, $m$, where $m$ is positive, if $a \equiv r \pmod{m}$, then $L(a, m) \subseteq L(r, \mathrm{m})$.

# PROBLEM 3

**Let $g: Z \to Z$ be an injective function.**

**Define $f: Z^2 \to Z^2$ such that $f(x,y) = (g(x)+ g(y), g(x) - g(y))$. Show that $f$ is also injective.**

Claim:

Given $g: Z \to Z$, which is an injective function, $f: Z^2 \to Z^2$ is also an injective function.

Direct Proof:

In mathematics an injective, or one-to-one, function is a function in which each element of the range maps to one distinct element of the domain.
We can prove that for every integers $x$ and $y$, $f(x) = f(y) \to x = y$.
Let $x$ and $y$ be integers and suppose that $f(x) = f(y)$.
We need to show that $x = y$.
We know that $f(x) = f(y)$.
So, lets substitute, $x = 3x + 7$ and $y = 3y + 7$.
So $3x = 3y$ and therefore $x = y$, which proves our claim if an injective function.

Now, we need to show that f is injective.
We want to show this by $(x_1, y_1) = (x_2, y_2)$
Suppose $f(x_1, y_1) = f(x_2, y_2)$
In order for it to be injective if $f(x_1, y_1) = f(x_2, y_2)$, then $(x_1, y_1) = (x_2, y_2)$
Given $f(x,y) = (g(x)+ g(y), g(x) - g(y))$,
this means $f(x_1, y_1) = (g(x_1)+ g(y_1), g(x_1) - g(y_1))$.
Since $f(x_1, y_1) = f(x_2, y_2)$,
then $(g(x_1)+ g(y_1), g(x_1) - g(y_1)) = (g(x_2)+ g(y_2), g(x_2) - g(y_2))$.
This gives two equations:

$$g(x_1)+ g(y_1) = g(x_2)+ g(y_2)$$
$$g(x_1) - g(y_1) = g(x_2) - g(y_2)$$

Add both equations: $2g(x_1) = 2g(x_2)$
Divide by 2: $g(x_1) = g(x_2)$
Since g is injective: $x_1 = x_2$

Subtract both equations: $2g(y_1) = 2g(y_2)$
Divide by 2: $g(y_1) = g(y_2)$
Since g is injective: $y_1 = y_2$

In conclusion, since $x_1 = x_2$ and $y_1 = y_2$ then $f: Z^2 \to Z^2$ is also an injective function.