# Problem Set 5

Parvesh Adi Lachman

October 2023

## 1 Problem 1

a) **Claim:** $\forall w, x, y, z \in \mathbb{Z} : 3 \mid (w-y)(w-z)(x-w)(x-y)(x-z)(y-z)$

**Proof:**

- Let the pigeons $(A)$ be the set $\{x, y, z, w\}$ where $x, y, z, w \in \mathbb{Z}$;
- Let the pigeonholes $(B)$ be the set $\{0, 1, 2\}$;
- Let $f : A \to B$ be defined $f(a) := remainderDivBy3(a)$. Note that $f$ is a well defined function:
  1. for any pigeon $a \in \{x, y, z, w\}$, $f(a) = remainderDivBy3(a)$ is computable because $a \div 3$ is defined,
  2. for any pigeon $a \in \{x, y, z, w\}$, if $remainderDivBy3(a) = b$ and $remainderDivBy3(a) = c$ then $b = c$, ,
  3. for any pigeon $a \in \{x, y, z, w\}$, $remainderDivBy3(a)$ is within the codomain $\{0, 1, 2\}$ by def of divisible by 3

| | **Mathematical Reasoning** | **Reason this Statement is True (From the Approved List)** |
|---|---|---|
| $\Rightarrow$ | $\lvert A\rvert = 4$ | Because $A = \{x, y, z, w\}$ |
| $\Rightarrow$ | $\lvert B\rvert = 3$ | Because $B = \{0, 1, 2\}$ |
| $\Rightarrow$ | $\lvert A\rvert > \lvert B\rvert$ | Since $4 > 3$ |
| $\Rightarrow$ | $\exists a_1, a_2 \in A : [(a_1 \neq a_2) \wedge (f(a_1) = f(a_2))]$ (i.e. pigeons $a_1 \neq a_2$ with same pigeonhole) | By def of pigeonhole principle |
| $\Rightarrow$ | $a_1, a_2 \in x, y, z, w \wedge (a_1 \neq a_2) \wedge (remainderDivBy3(a_1) = remainderDivBy3(a_2))$ | By def of $A$ and $f$ |
| $\Rightarrow$ | $3 \mid (a_1 - a_2)$ and $3 \mid (a_2 - a_1)$ | Since difference of two ints of the same function is also divisible by 3, and by def of equivalence class |
| $\Rightarrow$ | at least one of $(w-y), (w-z), (x-w), (x-y), (x-z), (y-z)$ is divisible by 3 | Since this is all pairs and $a_1 \neq a_2$ |
| $\Rightarrow$ | $(w-y)(w-z)(x-w)(x-y)(x-z)(y-z)$ is divisible by 3 | Since prod of div by 3 ints is still div by 3 |
| $\Rightarrow$ | $3 \mid (w-y)(w-z)(x-w)(x-y)(x-z)(y-z)$ | By def of divisible by 3 |

b) The claim would hold true. Let us remove $(w - z)$.

**Proof:**

| | **Mathematical Reasoning** | **Reason this Statement is True (From the Approved List)** |
|---|---|---|
| $\Rightarrow$ | $\lvert A\rvert = 4$ | Because $A = \{x, y, z, w\}$ |
| $\Rightarrow$ | $\lvert B\rvert = 3$ | Because $B = \{0, 1, 2\}$ |
| $\Rightarrow$ | $\lvert A\rvert > \lvert B\rvert$ | Since $4 > 3$ |
| $\Rightarrow$ | $\exists a_1, a_2 \in A : [(a_1 \neq a_2) \wedge (f(a_1) = f(a_2))]$ (i.e. pigeons $a_1 \neq a_2$ with same pigeonhole) | By def of pigeonhole principle |
| $\Rightarrow$ | $a_1, a_2 \in x, y, z, w \wedge (a_1 \neq a_2) \wedge (remainderDivBy3(a_1) = remainderDivBy3(a_2))$ | By def of $A$ and $f$ |
| $\Rightarrow$ | $3 \mid (a_1 - a_2)$ and $3 \mid (a_2 - a_1)$ | Since difference of two ints of the same function is also divisible by 3, and by def of equivalence class |
| $\Rightarrow$ | at least one of $(w-y), (x-w), (x-y), (x-z), (y-z)$ is divisible by 3 | Since this is all pairs and $a_1 \neq a_2$ |
| $\Rightarrow$ | $(w-y)(x-w)(x-y)(x-z)(y-z)$ is divisible by 3 | Since prod of div by 3 ints is still div by 3 |
| $\Rightarrow$ | $3 \mid (w-y)(x-w)(x-y)(x-z)(y-z)$ | By def of divisible by 3 |

## 2 Problem 2

a) Let $n$ be any positive integer, let $A_n = \{1, 2, ...., n\}$ and let $f_n : \mathcal{P}(A_n) \to \{0, 1\}^n$ be defined by $f_n(A) = b_1 b_2 ... b_n$ where

$$b_i = \begin{cases} 1 & \text{if } i \in A \\ 0 & \text{if otherwise} \end{cases} \tag{1}$$

| | | | |
|---|---|---|---|
| $n = 1$ | $A_1 = \{1\}$ | | |
| $f_1(\emptyset) = 0$ | $f_1(\{1\}) = 1$ | | |
| $n = 2$ | $A_2 = \{1, 2\}$ | | |
| $f_2(\emptyset) = 00$ | $f_2(\{1\}) = 10$ | $f_2(\{2\}) = 01$ | $f_2(\{1, 2\}) = 11$ |
| $n = 3$ | $A_3 = \{1, 2, 3\}$ | | |
| $f_3(\emptyset) = 000$<br>$f_3(\{3\}) = 001$ | $f_3(\{1\}) = 100$<br>$f_3(\{1, 3\}) = 101$ | $f_3(\{2\}) = 010$<br>$f_3(\{2, 3\}) = 011$ | $f_3(\{1, 2\}) = 110$<br>$f_3(\{1, 2, 3\}) = 111$ |

b) **Prove:** $f_n : \mathcal{P}(A_n) \to \{0, 1\}^n$ is onto, for any positive integer $n$.

Formal definition: $\forall b \in B\ \exists a \in A : f(a) = b$.

To prove $f$, WTS $\forall b \in B\ \exists a \in A : f(a) = b \equiv$ if $b \in B$ then $\exists a \in A : f(a) = b$.

**Proof:**

| | **Mathematical Reasoning** | **Reason this Statement is True (From the Approved List)** |
|---|---|---|
| Suppose | $B \in \{0, 1\}^n$ | By assumption |
| $\Rightarrow$ | $b_1 b_2 ... b_i \in \{0, 1\}$ | By def of n |
| $\Rightarrow$ | $b = b_1 b_2 ... b_n$ | By def of $b_i$ |
| $\Rightarrow$ | $A = \{i \in A_n \mid b_i = 1\}$ | Def of $b_i$ and $A$ |
| $\Rightarrow$ | $f_n(A) = b' = b'_1 b'_2 .. b'_n$ | By def of $f$ and $b'_n$ |
| $\Rightarrow$ | $f_n(A) = b_1 b_2 ... b_n$ | Since $b'_i = 1$ iff $i \in A$ iff $b_i = 1$ |

c) The ChatGPT proof is a direct proof since it assumed that $A$ and $B$ are distinct sets meaning $A \neq B$ and shows that $f(A) \neq f(B)$. Which is a direct proof.

d) A proof by contrapositive: Suppose $a_1 a_2 \in A$ and $f(a_1) = f(a_2)$, WTS $a_1 = a_2$

**Proof:**

| | **Mathematical Reasoning** | **Reason this Statement is True (From the Approved List)** |
|---|---|---|
| **Suppose** | if $f_n(A) = f_n(B)$ | By assumption |
| **WTS** | $A = B$ | |
| $\Rightarrow$ | $b_1 b_2 ... b_n = b'_1 b'_2 ... b'_n$ | By def of $f_n$ |
| $\Rightarrow$ | WLOG $A = \{i \in A_n \mid b_i = 1\}$ | By def of $b_i$ and $A$ |
| $\Rightarrow$ | $b_1 b_2 ... b_n = b'_1 b'_2 ... b'_n$ | Since $b'_i = 1$ iff $i \in A$ iff $b_i = 1$ defined by $f_n$, since $f_n(A) = f_n(B)$ |
| $\Rightarrow$ | $b_1 b_2 ... b_n = b_1 b_2 ... b_n$ | Since $b'_i = b_i$ iff $i \in A$ |
| $\Rightarrow$ | $A = B$ | By substitution |

## 3 Problem 3

**Claim:** Let $n, k$ be positive integers such that $k < 2^n$ and let $S$ be a set of $n$ integers, e.g. $S \subseteq \mathbb{Z}$ and $|S| = n$. Then there are distinct $U, V \subseteq S$ such that

$$\left[\sum_{x\in U} x\right] \bmod k = \left[\sum_{x\in V} x\right] \bmod k \tag{2}$$

**Pigeons:** Let the pigeons $(A)$ be possible subsets of $S$

**Pigeonholes:** Let the pigeonholes $(B)$ be $\left[\sum_{x\in U} x\right] \bmod k$

**Function:** Thus $f(U) := \left[\sum_{x\in U} x\right] \bmod k$ such that there exist distinct subsets $U$ and $V$ in $S$ such that $f(U) = f(V)$

| | **Mathematical Reasoning** | **Reason this Statement is True (From the Approved List)** |
|---|---|---|
| $\Rightarrow$ | $\lvert A\rvert = 2^n$ | By def of $A$ and claim |
| $\Rightarrow$ | $\lvert B\rvert = k$ | By def of $B$ since it represents the number of possible remainders of the summation mod $k$ |
| $\Rightarrow$ | $\lvert A\rvert > \lvert B\rvert$ | Since $k < 2^n$ |
| $\Rightarrow$ | $\exists a_1, a_2 \in A$: $[(a_1 \neq a_2) \wedge (f(a_1) = f(a_2))]$ | By def of the Pigeonhole Principle |
| $\Rightarrow$ | $\exists U, V \subseteq S : [(U \neq V) \wedge (\sum_{x\in U} x \bmod k = \sum_{x\in V} x \bmod k)]$ | By def of $f$, $a_1$ being $U$, and $a_2$ being $V$ as subsets of $S$ |