MAT200: Logic Language and Proof

Lecture 14 - March 24 2021

Last Time:

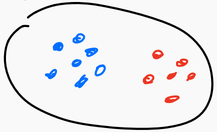
- Counting

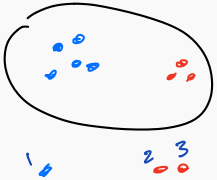
Today: Using the pigeonhole principle

Theorem **(PHP)**:
Let X and Y be finite sets. If $|X| > |Y|$ then there are no injective functions $f : X \to Y$.

Suppose you 13 blue socks and 13 red socks in a drawer.
If you pick out 3 socks, you are guaranteed to have a matching pair.

Proof idea:





$f(1) = \text{blue}$

$f(2) = \text{red}$

$f(3) = \text{red}.$

Proof using PHP:

Let A, B be finite sets.
Let $f: A \to B$.
If $|A| > |B|$, then f is not injective.

1. Let $A = \{1, 2, 3\}$.
2. Let $B = \{\text{blue}, \text{red}\}$.
3. Let $f: A \to B$, $f(a) =$ the color of the a'th sock.
4. By PHP, f is not injective
   $\Rightarrow \exists a_1, a_2$ such that $a_1 \neq a_2$, $f(a_1) = f(a_2)$

   the color of the a_1'th sock. = the color of the a_2'th sock.

In other words, a_1'th sock match the a_2'th sock.

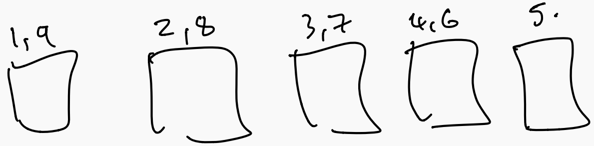
QED.

$P \Rightarrow f$ is not injective. f ~~is injective~~

Example 2

Theorem If 6 distinct numbers are chosen from {1,2,3,4,5,6,7,8,9}, then 2 of them sum to 10.

Proof idea:



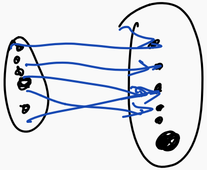
Quiz: How many elements in B?

a) 5 ←

b) 9

c) 10.

E.g. $f(3) = \{3,4\}$.



$\boxed{\text{PHP: Let } A, B \text{ be finite sets. Let } f: A \to B. \text{ If } |A| > |B|, \text{ then } f \text{ is not injective.}}$

1. Let A = The set of 6 numbers chosen

2. Let $B = \{\{1,9\}, \{2,8\}, \{3,7\}, \{4,6\}, \{5\}, \{-3,13\}\}$

a 3. Let $f: A \to B$, $f(a)$ = The set in B that contains a

b) 4. $|A| > |B|$, so By PHP, f is not injective

$\Rightarrow \exists a_1, a_2$ such that

$a_1 \neq a_2$, $f(a_1) = f(a_2)$

c) So there exists $a_1 \neq a_2$ s.t.

The set in B that contains a_1 = The set in B that contains a_2

d $\Rightarrow a_1 + a_2 = 10$.

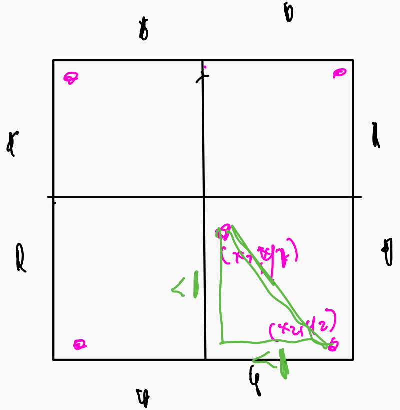
QED.

You want to prove a statement, and you’ve decided that PHP would be suitable.
Here is what you need to have a complete proof:

1. Pick an appropriate set A.
2. Pick an appropriate set B, such that |A|>|B|.
3. Pick a function f:A->B.
4. Use pigeonhole principle to deduce f is not injective.
5. Explain why f not being injective proves the statement.

Theorem: If 5 points are chosen in a square of side length 2,
Then 2 of them are ~~within~~ $\leq$ $\sqrt{2}$ of each other.

Proof idea:



unit square.

Proof using PHP:

1. Let A = The 5 points chosen.
2. Let B = The 4 quadrants of the square.

a) 3. Let $f: A \to B$, $f(a)$ = the quadrant containing a.

b) 4. By PHP, f is not injective
$\Rightarrow \exists a_1, a_2$ such that $a_1 \neq a_2$, $f(a_1) = f(a_2)$

the quadrant containing a_1
=
the quadrant containing a_2.

$B = \{((0.1, 0.1), (0,0)),$
$((0.2, 0.2), (0.1, 0.1)),$
$((0.3, 0.35), (0.1, 0.1)),$
$\vdots$

c) 5. So 2 points (x_1, y_1) (x_2, y_2) in same unit square

d) $\Rightarrow$ dist $= \sqrt{(x_1 - x_2)^2 + (y_1 - y_2)^2} \leq \sqrt{1+1} = \sqrt{2}$

Theorem: If ~~X~~ is a set of $n+1$ integers, there exists two whose difference is divisible by n.

Proof idea:

Question:
Suppose $n = 10$.
Which of these are in $f(34)$.

a) 7
b) 24 ✓
c) 104 ✓
d) 37

Answer:

$f(34) =$ the set in B containing 34.

$= \{nk+4 : k \in \mathbb{Z}\}$.

$= \{14, 24, 34, 44, 54, \ldots\}$

Proof using PHP:

1. Let $A = X$, the $n+1$ integers.
2. Let $B = \{ \{nk : k \in \mathbb{Z}\}, \{nk+1 : k \in \mathbb{Z}\}, \{nk+2 : k \in \mathbb{Z}\}, \{nk+3 : k \in \mathbb{Z}\}, \ldots, \{nk+n-1 : k \in \mathbb{Z}\} \}$.

   $\{10, 20, 30, 40, \ldots\}$ $\quad$ $\{11, 21, 31, 41, \ldots\}$
3. Let $f : \underset{n+1 \text{ elems}}{A} \to \underset{n \text{ elems.}}{B}$, $f(a) =$ the set in B containing a.
4. By PHP, f is not injective

   $\Rightarrow \exists a_1, a_2$ such that $a_1 \neq a_2$, $f(a_1) = f(a_2)$

   $\Rightarrow a_1 \in \{nk+j : k \in \mathbb{Z}\} \Rightarrow a_1 = nk_1 + j$

   $a_2 \in \{nk+j : k \in \mathbb{Z}\}. \Rightarrow a_2 = nk_2 + j$

   $\Rightarrow a_1 - a_2 = nk_1 + j - (nk_2 + j) = n(k_1 - k_2)$.
5. So $a_1 - a_2$ is divisible by n.

Theorem: If ~~A~~ X is a set of 31 distinct integers in {1,2,…,60}, then there are two elements in ~~A~~ X, one of which divides the other.

Proof using PHP:

The proof relies on:

Fact: Every integer n may be written in uniquely in the form $n = 2^j m$ where m is odd.

E.g. $57 = 2^0 \cdot 57$

$36 = 2^2 \cdot 9$

So $f(57) = 57$, $f(36) = 9$

Proof: Just keep dividing by 2.

(Formally, induction).

1. Let $A = X$
2. Let $B = \{1, 3, 5, \ldots, 59\}$.

...

3. Let $f: A \to B$, $f(a) =$ the unique odd m such that $a = 2^j \cdot m$.

31 elems 30 elems. (This is well defined by fact).

4. By PHP, f is not injective

$\Rightarrow \exists a_1, a_2$ such that $a_1 \neq a_2$, $f(a_1) = f(a_2) = m$

$\Rightarrow a_1 = 2^{j_1} m$, $a_2 = 2^{j_2} m$.

$\Rightarrow a_1$ divis by a_2 or vice versa. ∎

- Last lecture, I claimed that **the ability to count** is import ant. because it allows us to **determine whether or not there are injective functions.**
    - Pigeonhole principle: If |X|>|Y|, there are no injections $f : X \to Y$
- Today, we saw how many problems can be reduced to checking **whether or not there is an injective function between certain sets.**
    - Applications of pigeonhole principle
    - Template for proving things using the PHP.

Next time we will prove some shortcuts that are useful for counting.