Lecture 15

Proof Techniques seen so far :

- Proof of Existence by explicit construction

  $P(a) \Rightarrow \exists x \; P(x)$

- Proof via contradiction

  $(P \Rightarrow F) \Rightarrow \neg P$

- Proof via contrapositive

  $(P \Rightarrow Q) \Leftrightarrow (\neg Q \Rightarrow \neg P)$

- Proof using induction

  $\Big(P(1) \wedge (\forall i, \; P(i) \Rightarrow P(i+1)) \Big) \Rightarrow (\forall x \in \mathbb{N}, \; P(x))$

Plan for next few lectures :

Proof of existence, but without explicit construction.

- Pigeonhole Principle
- Probabilistic Method

PIGEONHOLE PRINCIPLE (PHP):

$n+1$ objects are assigned to n boxes.
There exists at least one box with two objects assigned to it.

$\forall n$, $\forall$ sets A of size $n+1$, $\forall f : A \to [n]$,
$\exists\, a_0, a_1 \in A$ s.t. $a_0 \neq a_1$ and $f(a_0) = f(a_1)$

PHP can be derived using PMI.

Simple applications of PHP :

1. Let $S \subseteq [99]$, $|S| = 51$. $S = \{a_1, \dots, a_{51}\}$
$\exists$ $a_i, a_j \in S$, $i \neq j$ s.t.
100 divides $a_i + a_j$.

Pf: Consider $P_i = \{i, 100-i\}$, $1 \le i \le 49$
$P_{50} = \{50\}$

$$[99] = \left(\bigcup_{i=1}^{50} P_i\right), \quad P_i \cap P_j = \phi \text{ if } i \neq j.$$

Consider any $S \subseteq [99]$, $|S| = 51$.
Each element of S belongs to exactly one P_i.

For every $z \in S$, let label (z) denote the index i s.t. $z \in P_i$.

Using PHP :
Since $|S| > 50$, there exist two elements $z, z' \in S$,
$z \neq z'$ such that label (z) = label (z').

$\Rightarrow \exists$ $z, z' \in S$, $i \in [49]$ s.t. $z \neq z'$, $P_i = \{z, z'\}$
$\Rightarrow \exists$ $z, z' \in S$ s.t. $z + z' = 100$. Follows from def. of P_i.

■

2. Any 21-element subset of $[99]$ has 4 elements a, b, c, d s.t. $a+b = c+d$.

<u>Proof</u>: Take any $S \subseteq [99]$, $|S| = 21$.

Number of possible unordered pairs in S

$$= \frac{21 \times 20}{2} = 210.$$

Suppose no two unordered pairs have the same sum. The sum of each pair is at most $99 + 98 = 197$, and at least 3.

Hence, using PHP, $\exists\ T_i, T_j \subseteq S$, $T_i \neq T_j$, $|T_i| = |T_j| = 2$ and $\sum_{x \in T_i} x = \sum_{y \in T_j} y$.

Note that $T_i \cap T_j = \phi$.

Hence, $\exists\ a, b, c, d \in S$ s.t. $a+b = c+d$.

$\blacksquare$

Flawed approach: we discussed the following flawed approach in class. Take any 4 sized subset $\{a, b, c, d\}$, and consider $a+b-c-d$. This can take value at least -197, and at most 197. ${}^{21}C_4 > 2 \cdot 197 + 1$.
However, we cant conclude that $\exists\ a, b, c, d$ s.t. $a+b-c-d = 0$.

3. $S \subseteq [99]$, $|S| = 51$. Prove that $\exists\ a_i, a_j \in S$ s.t. a_i divides a_j.

Attempt 1: Consider $P_t = \{t, 2t\}$: $1 \leq t \leq 49$.

Can we conclude that $\forall\ S \subseteq [99]$ $|S| = 51$, $\exists\ t$ s.t. $P_t \subseteq S$?

Doesn't work since $\bigcup_{t=1}^{49} P_t \neq [99]$

Note that the P_js are not disjoint. However, this is not the main issue in the above approach.

Attempt 2: Let $2 = p_1 < p_2 < \cdots < p_t$ be all prime numbers less than 100.

Every number $n \in [99]$ can be expressed as $n = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_t^{\alpha_t}$, $\alpha_i \in \mathbb{N} \cup \{0\}$.

Let $\alpha(n) = (\alpha_1, \alpha_2, \ldots, \alpha_t)$.

n_1 divides $n_2 \Rightarrow \alpha(n_1) \leq \alpha(n_2)$

by appropriately defining $\leq$ op.

How to proceed from here ?

Attempt 3: Mix of attempt 1 & attempt 2.

$$P_1 = \{1, 2, 4, 8, 16, \dots\}$$
$$P_3 = \{3, 6, 12, 24, 48, \dots\}$$
$$P_5 = \{5, 10, 20, 40, 80\}$$

For any odd number $t \in [99]$, define
$$P_t = \{t, 2t, 4t, 8t, \dots\}$$

Obs 1: For any odd $t \in [99]$, any $a_i, a_j \in P_t$,
$a_i < a_j \Rightarrow a_i$ divides a_j.

Obs 2: $\bigcup_{t=1}^{50} P_{2t-1} = [99]$

For each $z \in S$, let label(z) denote the index i s.t. $z \in P_{2i-1}$. label$(z) \in [50]$.

Using Pigeonhole Principle, if we pick 51 elements from $[99]$, at least two of them have the same label, and therefore, $\exists\, t \in [50]$ s.t. both belong to same partition P_{2t-1}.

Using Observation 1, we conclude that $\exists\, a_i, a_j \in S$, $i \neq j$ s.t. a_i divides a_j. $\blacksquare$

4. [Erdős - Szekeres Theorem]

Consider any sequence of n^2+1 distinct numbers. There exists an $n+1$ length increasing subsequence, or an $n+1$ length decreasing subsequence.

This theorem is tight, there exists a sequence of length n^2 that has no inc./dec. subseq. of length $n+1$.

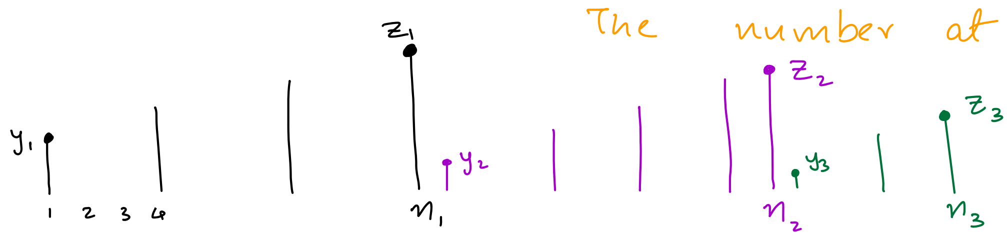
eg. $n = 3$

$(7, 8, 9, 4, 5, 6, 1, 2, 3)$.

Recall the infinite version of this theorem: any infinite length sequence of distinct numbers either has an infinite inc. subseq. or an infinite dec. subseq.

The infinite version is easier to prove. Suppose, there doesn't exist an infinite inc. subseq. Start with the first number y_1, and look at the longest inc. subseq. that starts with y_1. Suppose this seq. ends at pos.^{n} n_1.

The number at pos.^{n} n_1 : z_1.



Look at the next number, say y_2. Again look at the longest subseq. starting at y_2. Suppose this ends at n_2, and the value at n_2 : z_2

Note that $z_1 > z_2$.

Now, look at the number at position n_2+1, say y_3. Similarly, define n_3 and z_3.

And note that $z_1 > z_2 > z_3$.

Continuing in this manner, we get an infinite dec. seq. $z_1 > z_2 > z_3 > \cdots$

Will this idea work for finite seq ? Unfortunately, it does not. Let $(a_1, a_2, \ldots, a_{n^2+1})$ be the sequence. The longest inc. subseq. starting at a_1 can end at position n^2, leaving us no room for the next inc. subseq.

Proof : Take any seq. $(a_1\ a_2 \cdots a_{n^2}\ a_{n^2+1})$ Suppose $\nexists$ $n+1$ length inc. subseq.

Let S^i denote the longest inc. subseq. starting at a_i.

$1 \leq |s^i| \leq n$. There are n^2+1 such subseq.

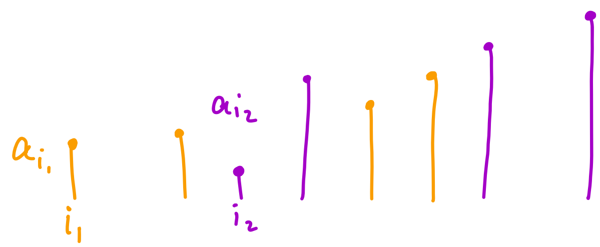
For each $i \in [n^2+1]$, let $label(i) = |s^i|$.

$1 \leq label(i) \leq n$.

Therefore, by PHP, there exist at least $n+1$ such s^i of the same length. More formally,

$$\exists\, t \in [n] \text{ s.t. } \underbrace{\left|\{ i : |s^i| = t \}\right|}_{I = \{i_1, \ldots, i_k\}} \geq n+1$$

$i_1 < i_2 < \ldots < i_k$



Observation: If $i, j \in I$, $i < j$, then $a_i > a_j$.

<u>Proof</u>: Suppose $a_i < a_j$. Then we have a longer inc. subseq. starting at a_i.

$$a_i \quad \underbrace{a_j \;\cdots}_{s^j}$$

Observation: $a_{i_1} > a_{i_2} > \ldots > a_{i_k}$.

Since $k \geq n+1$, we have a dec. subseq. of length $n+1$ $\blacksquare$