Indian Institute of Information Technology
Design and Manufacturing, Kancheepuram
Chennai – 600 127, India
An Autonomous Institute under MHRD, Govt of India
An Institute of National Importance
www.iiitdm.ac.in
COM 205T Discrete structures for computing-Lecture Notes

Instructor
N.Sadagopan
Scribe:
S.Dhanalakshmi
Renjith.P

Invitation to Proof techniques

Motivation- Some interesting questions

1. Prove that, if n is odd, then n^2 is odd, where n is an integer.
2. Prove that, if n is an integer and $3n + 2$ is odd then, n is odd.
3. Do C-programs exist for all computational problems ? Does there exist a computational problem for which no C-program exists ?
4. Let A be the set of all computational problems and B be the set of all C-programs. Which set has a larger cardinality ?
5. (Ramsey) In a group of six people there exist at least three mutual friends or three mutual enemies. Prove or Disprove.
6. In a group of six people there exist at least two with equal number of friends. Prove or Disprove.
7. Prove that the number of diagonals in an n-sided polygon is $\frac{n(n-3)}{2}$, $n \geq 3$.
8. (Cantor) Between $\mathcal{N}$ and $\mathcal{I}$, which set is of larger cardinality ?
9. How do we show that for all inputs, insertion sort indeed works ?
10. Prove that for any unsorted array of size n, the minimum number of comparisons required to find MIN and MAX is $3\lceil \frac{n}{2} \rceil - 2$.

To prove the above questions, one is expected to give a logical argument consisting of a sequence of known facts, observations and inferences. Given a logical argument, we need a formal framework to assess whether the argument is true or false. Towards this end, in this section we shall explore proof techniques in detail.

Proof Techniques: A proof is a valid argument that establishes the truth value of a logical argument. There are different proof techniques:

1. Direct Proof
2. Proof by contraposition
3. Proof by contradiction
4. Mathematical Induction (Discovered by De Morgan)
5. Pigeon hole principle
6. Proofs based on counting arguments
7. Lower bound theory
8. Proof by minimal counter example

Now, let us prove some logical arguments to understand and appreciate the power of proof techniques.

1. **Claim:** If n is odd then, n^2 is odd, where n is an integer.

   Direct Proof: $\forall n \ \exists k \geq 0$ such that $n = 2k + 1$
   $\Rightarrow n^2 = (2k+1)^2 = 4k^2+4k+1=2(2k^2+2k)+1$, clearly this is an odd number. Hence the claim.

Suppose we attempt a proof by contraposition, then the flow of the proof looks like;
P$\rightarrow$Q $\leftrightarrow$ $\neg$Q$\rightarrow$ $\neg$P
Suppose n^2 is even.
n^2=$2k$, for some $k \geq 0$.
It is not clear how to proceed further to complete the proof. So this may not be the right proof technique for this problem. Therefore, identifying the right proof technique is an art and comes by practice.

How proof by contraposition works:

For proving $p \rightarrow q$, we prove $\neg q \rightarrow \neg p$, i.e., the negation of q implies the negation of p.

2. **Claim:** If n is an integer and $3n + 2$ is odd, then n is odd.

   Proof by contraposition: Assume $\neg q$. I.e., n is even. Since n is even, $n = 2k$ for some integer $k \geq 0$, then $3n + 2 = 3 \cdot 2k + 2 = 2 \cdot (3k + 1)$.
   This implies that $3n + 2$ is even, which is $\neg p$ □

How proof by contradiction works:

For proving $p \rightarrow q$, and the base assumption of p being true (premise), suppose, on the contrary, we assume $\neg q$ to be true. Through logical arguments, we arrive at $\neg p$, which contradicts the premise. This implies that the assumption is wrong and hence, q follows from p.

3. **Claim:** Prove that $\sqrt{2}$ is irrational.

   Proof by contradiction: On the contrary, assume that $\sqrt{2}$ is rational. i.e., $\sqrt{2} = \frac{a}{b}$, where $a, b \in I, b \neq 0$ such that $gcd(a, b)$=1, a and b are co-primes.
   $a^2 = 2b^2 \Rightarrow a^2$ is even $\Rightarrow a$ is even.
   $a = 2c$ for some $c \geq 0$. $a^2 = 4c^2$; $4c^2 = 2b^2 \Rightarrow b^2 = 2c^2 \Rightarrow b^2$ is even $\Rightarrow b$ is even.
   Therefore, $gcd(a, b) \geq 2$. This is a contradiction to the fact that $gcd(a, b) = 1$, and our assumption is wrong. Therefore, $\sqrt{2}$ is irrational. □

Remark: In proof by contraposition, to show $p \rightarrow q$, we assume $\neg q$ is true and through logical arguments, we arrive at $\neg p$. Due to equivalence property, it follows that $p \rightarrow q$. The idea in proof by contradiction is slightly tricky. Given p, which is a premise and hence assumed to be true, to show that q follows logically from p, we assume q does not imply from p. By assuming $\neg q$, we proceed with a sequence of logical arguments and finally arrive at $\neg p$. I.e., p and $\neg q$ implies $\neg p$ which contradicts the premise. We obtain such a contradiction due to our assumption that $\neg q$ is true. Hence, our assumption that $\neg q$ is true, is false, and q is implied from p.

How induction works:

There are two induction techniques: weak mathematical induction and strong mathematical induction. We shall discuss weak mathematical induction in detail and throw some lights on strong mathematical induction.

Weak Mathematical Induction: Let $P(n)$ be a proposition. A proof by mathematical induction has two parts, a `basis step`, where we show that $P(1)$ is true, and an `inductive step`, where we show that for all positive integers $k, k \geq 1$, if $P(k)$ is true, then $P(k+1)$ is true. Induction hypothesis acts as a bridge between the base case and the induction step. By assuming $P(1)$ (which is a true assumption as the base case is already proved), we show that it is true for $P(2)$ using the induction step. Since $P(2)$ is proved, by assuming $P(2)$, we show using the induction step that the claim is true for $P(3)$ and so on. Now, it is clear why it is appropriate to assume *if* $P(k)$ *is true* as part of the induction hypothesis.

Note: Note that the basis step need not be at $k = 1$ always. It can be, say, at $k = 10$, provided that the values taken by n form a well ordering (`See lecture notes on Relations and Functions`) and $k = 10$ forms the starting point of the ordering.

Strong Mathematical Induction: In strong induction, as part of the hypothesis step, we assume all values less than $(k+1)$ is true, and with this assumption, we show the claim is true for $P(k+1)$ as part of the inductive step. In the induction step, we show that for all positive integers $k, k \geq 1$, if $P(l)$ is true, for all $1 \leq l \leq k$, then $P(k+1)$ is true.

4. **Claim:** Prove that the number of diagonals in an n-sided polygon is $\frac{n(n-3)}{2}$, $n \geq 3$.

Mathematical Induction on n:
Basis step: In a triangle, there are no diagonals. i.e., when $n = 3$, the number of diagonals$= \frac{3(3-3)}{2} = 0$.
Induction Hypothesis: Assume that for all k-sided polygon, $k \geq 3$, the number of diagonals $= \frac{k(k-3)}{2}$
Induction Step/ Anchor step: Consider a $(k+1)$-sided polygon, whose vertices be $v_1, v_2, \ldots, v_k, v_{k+1}$. Note that by the induction hypothesis, there are $\frac{k(k-3)}{2}$ diagonals among $v_1, v_2, \ldots, v_k$. Note that there are $(k-2)$ diagonals incident on v_{k+1} and $\{v_1, v_k\}$ is also a diagonal.
Therefore, the total number of diagonals in a $(k+1)$-sided polygon $= \frac{k(k-3)}{2} + k - 2 + 1$

$= \frac{k(k-3)+2k-4+2}{2} \quad = \frac{k^2-3k+2k-2}{2}$

$= \frac{k^2-k-2}{2} \quad = \frac{(k+1)(k-2)}{2}$ □

5. **Claim:** In a closed polygon of size n, the number of triangles is $\frac{n(n-1)(n-2)}{6}$, $n \geq 3$.

Let us prove this by induction on the size of the polygon, n.
Base Case: For $n = 3$, the number of triangles $= 1$, which is $\frac{3 \cdot 2 \cdot 1}{6}$.
Hypothesis: Let us assume that the claim is true for $n = k$, where $k \geq 3$.
Induction Step: Let the size of the polygon be $n = k+1, k \geq 3$.
The number of triangles in a closed polygon of size $k+1$ = Number of triangles in a closed polygon of size k + Number of triangles formed after adding $(k+1)^{th}$ vertex(node)
$= \frac{k(k-1)(k-2)}{6} + \binom{k}{2} = \frac{k(k-1)(k-2)}{6} + \frac{k(k-1)}{2} = \frac{k(k-1)(k-2)}{6} + \frac{3k(k-1)}{6} = \frac{(k+1)k(k-1)}{6}$.
Note that $(k+1)^{th}$ vertex, can pick any two vertices from k-vertex polygon and each such selection gives one new triangle. Thus, there are $\binom{k}{2}$ new triangles due to $(k+1)^{th}$ vertex.

The induction is complete and the claim is true for the polygon of size $k+1$.
Therefore, the claim is true for every $n \geq 3$. □

6. **Claim:** Let n and x be any two natural numbers. Prove that $x^n - 1$ is divisible by $x-1$.

   Solution:
   Let us prove this by induction on n. The proof does not focus on x and works for any x. In general, if an expression contains more than one parameter, induction is applied on one parameter and the other parameters are not taken into account.
   Base Case: For $n = 1$, $x^1 - 1$ is divisible by $x-1$, $x \geq 2$.
   Hypothesis: Assume $\forall n$, $x^n - 1$ is divisible by $x-1$, $n \geq 1$.
   Induction Step: Our claim is to prove that, $x^{n+1} - 1$ is divisible by $x-1$, $n \geq 1$.

$$x^{n+1} - 1 = x^{n+1} - 1 - x + x = x^{n+1} - x + (x-1) = x(x^n - 1) + (x-1),$$

   where $x^n - 1$ is divisible by $x-1$ by the hypothesis and $x-1$ is divisible by $x-1$. Thus, $x(x^n-1) + (x-1)$ is divisible by $x-1$. Thus, the claim is true for $n+1$. Therefore, the claim is true for all natural numbers n and x. □

7. **Claim:** Show that $\frac{1}{2} + \frac{1}{4} + \ldots + \frac{1}{2^n} < 1$, $\forall n \geq 1$.

   Solution:
   Let us prove this by induction on n.
   Base Case: For $n = 1$, $\frac{1}{2} < 1$.
   Hypothesis: Assume, $\frac{1}{2} + \frac{1}{4} + \ldots + \frac{1}{2^n} < 1$, $\forall n \geq 1$.
   Induction Step: For $n+1$, $n \geq 1$,

$$\frac{1}{2} + \frac{1}{4} + \ldots + \frac{1}{2^n} + \frac{1}{2^{n+1}}$$

$$= \frac{1}{2}\left(1 + \frac{1}{2} + \frac{1}{4} + \ldots + \frac{1}{2^n}\right)$$

$$= \frac{1}{2} + \left(\frac{1}{2}\left(\frac{1}{2} + \frac{1}{4} + \ldots + \frac{1}{2^n}\right)\right)$$

$$< \frac{1}{2} + \frac{1}{2}(1) \text{ By the induction hypothesis}$$

   < 1. The induction is complete and the claim is true for all $n \geq 1$. □

8. **Claim:** Show that $n! < n^n$, $\forall n \geq 2$.

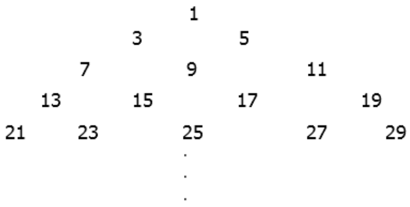
   Solution:
   Let us prove this by induction on n.
   Base Case: For $n = 2$, $2! < 2^2 = 4$. $P(2)$ is true.
   Hypothesis: Assume that, $\forall n,\ n! < n^n$, $\forall n \geq 2$. (i.e., $P(n)$ is true).
   Induction Step: Our aim is to prove that $P(n+1)$ is true from the induction hypothesis. i.e., to prove $(n+1)! < (n+1)^{(n+1)}$, $n \geq 2$

   Consider, $(n+1)! = (n+1)(n!) < (n+1)n^n$ (by the hypothesis)

$$< (n+1)(n+1)^n = (n+1)^{(n+1)}.$$

Hence, $\forall n \geq 2$, $P(n+1)$ is true if $P(n)$ is true. Thus, we conclude $P(n)$ is true for every $n \geq 2$. □

Practice Question: Find an expression for the sum of the i^{th} row, $i \geq 1$:



9. **Claim:** Suppose we remove a 1×1 square from a standard $2^n \times 2^n$ chessboard. Show that the remaining $n^2 - 1$ squares can be tiled using L-shaped triominoes, $n \geq 1$. L-shaped triomino consists of three 1×1 squares arranged as though any single 1×1 square has been removed from a 2×2 chess board. Further, it has four orientations.

Solution:
Let us prove this by induction on $n \geq 1$.
Base Case: For $n = 1$, In a 2×2 chessboard, if we remove one square R (see Figure 1), the remaining will be arranged in a L-shaped triomino, therefore $P(1)$ is true.
Hypothesis: Assume that, the statement is true for all $n = k$, $k \geq 1$. I.e., a $2^k \times 2^k$ chessboard without a single square can be arranged using L-shaped triominoes.

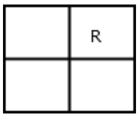


Fig. 1. Base Case

Induction Step: For $n = k+1$, $k \geq 1$.
In $2^{k+1} \times 2^{k+1}$ chessboard, divide the chessboard into C_1, C_2, C_3 and C_4 as shown in Figure 2. Remove the square R_1 from the chessboard. The squares R_2, R_3 and R_4 form a L-shape triomino. By our hypothesis, $C_1 \backslash R_1$, $C_2 \backslash R_2$, $C_3 \backslash R_3$ and $C_4 \backslash R_4$ can be tiled using $L-$shaped triominoes, where $C_i \backslash R_i$ indicates the partition of chessboard C_i upon the removal of square R_i, $i \in \{1, 2, 3, 4\}$. It is clear that the placement of L-shaped triominoes given by the hypothesis and the new triomino placed at R_2, R_3 and R_4 is a placement of L-shaped triominoes for $2^{k+1} \times 2^{k+1}$ chessboard. This completes the induction.

□

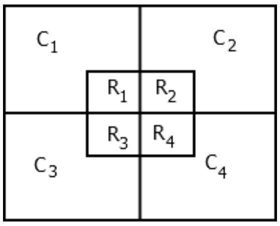


Fig. 2. Induction Step

10. **Claim:** The number of r-sized subsets of an $n-$element set is $\frac{n!}{(n-r)!r!}$, $n \geq 0, n \geq r \geq 0$.

    Solution:
    Let us prove this by induction on n. As mentioned before, we focus on n and do not care about r. Further, the proof works for any r.
    Base Case: If $n = 2$ then,
    Case 1: $r = 0$, the number of 0-size subsets is 1 which is the empty set.
    Case 2: $r = 1$, the number of 1-size subsets is 2.
    Case 3: $r = 2$, the number of 2-size subsets is 1.
    Thus, $P(2)$ is true.
    Note that the base case can be of $n = 0$ (null set) as it only has one subset of size $r = 0$ which is itself.
    Hypothesis: Assume that, the claim is true for n, $n \geq 2$.
    Induction Step: For $n + 1$, $n \geq 2$.
    The number of r-sized subsets on an $(n + 1)$-sized set $= C(n + 1, r)$
    We know that $C(n + 1, r)$ is

    $$= n_{c_{r-1}} + n_{c_r}$$

    By the induction hypothesis;

    $$= \frac{n!}{(n-(r-1))!(r-1)!} + \frac{n!}{(n-r)!r!}$$
    $$= \frac{n!}{(n-(r-1))(n-r)!(r-1)!} + \frac{n!}{(n-r)!r(r-1)!}$$
    $$= \frac{n!}{(n-r)!(r-1)!} \left(\frac{1}{(n-(r-1))} + \frac{1}{r} \right)$$
    $$= \frac{n!}{(n-r)!(r-1)!} \left(\frac{n+1}{r(n-r+1)} \right)$$
    $$= \frac{(n+1)n!}{((n+1)-r)!r(r-1)!}$$
    $$= \frac{(n+1)!}{((n+1)-r)!r!}$$

    Hence, $\forall n \geq 2$, $P(n + 1)$ is true if $P(n)$ is true.
    Thus, we conclude, the claim is true for all $n \geq 0$. □

11. **Problem:** Suppose we have stamps of two denominations: 3 cents and 5 cents. Is it possible to compose any postage of 8 cents or more using exactly these denominations ?

    Solution:
    Let us prove this by induction on $k \geq 8$.
    Basis step: For $k = 8$, one 3-cent and one 5-cent stamp are required to make up 8-cents.
    Inductive step: We want to show that if it is possible to make up exactly a postage of k cents using 3-cent and 5-cent stamps, then it is also possible to make up exactly a postage of $k + 1$ cents using 3-cent and 5-cent stamps. We examine two cases: suppose we make up a postage of k cents using at least one 5-cent stamp. Replacing a 5-cent stamp by two 3-cent stamps will yield a way to make up a postage of $k + 1$ cents. On the other hand, suppose we make up a postage of k cents using 3-cent stamps only. Since $k \geq 8$, there must be at least three 3-cent stamps. Replacing three 3-cent stamps by two 5-cent stamps will yield a way to make up a postage of $k + 1$ cents. Since it is obvious how we can make up a postage of 8 cents, we conclude that we can make up a postage of 9 cents, which, in turn, leads us to conclude that we can make up a postage of 10 cents, which, in turn, leads us to conclude that we can make up a postage of 11 cents, and so on. Thus, we conclude that any postage of 8 cents or more can be composed using 3 and 5 cents. □

Pigeonhole Principle

Consider the following puzzle: a box contains red, black and white balls. The objective is to pick balls satisfying some constraints (of course, without seeing the balls). How many balls must be taken to ensure that there is a pair of same color? The key to solve this puzzle is pigeonhole principle (henceforth PHP). We shall now discuss a variety of examples and learn PHP by example.

Principle: If n pigeons are nesting in m pigeonholes, where $n > m$, then at least one pigeonhole has more than one pigeon.
In general, if $n(r-1)+1$ objects are distributed into n boxes, then there exists a box containing at least r objects.

1. Among any group of 367 people, there must be at least two with the same birth date. Assume that there are 366 days in a year. Prove using PHP.

   The first step in solving PHP based puzzles is to identify pigeons and pigeon holes. Consider each day in a year as a pigeonhole, i.e., each pigeon hole is labeled as 1-Jan, 2-Jan, 3-Jan, etc., and people as pigeons. A pigeon (person) is placed in the hole labeled 1-Jan if his birth date is 1-Jan. Since there are 366 pigeons and 367 people, by pigeonhole principle, there exist more than one person having the same birth date.

2. Among any group of 13 people there must be at least two with the same birth month.

   Consider months in a year as pigeonholes and people as pigeons. Thus, by pigeonhole principle, there exists more than one people having the same birth month.

3. Assuming discrete mathematics follows 4 grade grading pattern - A, B, C, D, what is the minimum number of students required in DM class to be sure that at least six receive the same grade.

   Consider grades as boxes, $n = 4$ and students as objects. For $r = 6$, by generalized pigeonhole principle, there should exist at least $n(r-1)+1$ students $= 4(6-1)+1 = 21$ students.

4. From integers 1 to 200, 101 distinct integers are chosen arbitrarily. Show that among the chosen numbers, there exist two integers such that one divides another perfectly.

   We create 100 boxes (pigeonholes) as follows. Boxes are labeled with odd numbers as $1, 3, 5, \ldots, 197, 199$. Note that each integer can be represented as $x \cdot 2^i$, $i \geq 0$, where x is an odd integer. A chosen integer $y = x \cdot 2^i$ is placed in the box with label x. As an example, $52 = 13 \cdot 2^2$ is placed in box labeled 13, and $7 = 7 \cdot 2^0$ is placed in box labeled 7. Since there exist 101 distinct integers (*pigeons*), by pigeonhole principle, there exists a box y with at least two integers say x_j, x_k, such that $x_j = y \cdot 2^{p_j}$, $x_k = y \cdot 2^{p_k}$. Observe that $p_j \neq p_k$ as the chosen integers are distinct. It follows that x_k divides x_j if $p_j > p_k$ and x_j divides x_k if $p_k > p_j$. Therefore, there exist at least two integers such that one divides another.

5. A chess player wants to prepare for a championship match by playing some practice games in 77 days. She wants to play at least one game a day but not more than 132 games altogether. Show that no matter how she schedules the games, there is a period of consecutive days during which she plays exactly 21 games.

   Let a_i, $1 \leq i \leq 77$ be the number of games played till i^{th} day, including the games played on the i^{th} day. Then,
   $a_1 < a_2 < \ldots < a_{77} \leq 132.$ (1)
   $a_1 + 21 < a_2 + 21 < \ldots < a_{77} + 21 \leq 132 + 21 = 153.$ (2)
   Note that there does not exist a_i, a_j such that $i \neq j$, $1 \leq i, j \leq 77$ and $a_i = a_j$. Similarly, in equation (2), $a_1 + 21$ to $a_{77} + 21$ are distinct. It follows that there exist $2 \times 77 = 154$ summands (*pigeons*), and 153 distinct integer values (*pigeonholes*). Therefore, there exist two summands having the same value. i.e., $a_i = a_j + 21$ and this implies that $a_i - a_j = 21$. Thus, there exist a period of $i-j$ consecutive days during which exactly 21 games are played, i.e., days $j+1, j+2, \ldots, i$.

6. Show that in any 52 distinct integers, there exist two of them whose sum or else difference is divisible by 100.
   Let the integers (*pigeons*) be placed in 51 groups (*pigeonholes*) labeled 0 through 50 as follows.
   An integer i is in group j, $0 \leq j \leq 50$ if:
   1. i mod $100 \leq 50$ and i mod $100 = j$
   2. i mod $100 > 50$ and $100 - (i \bmod 100) = j$,
   As an example, 103, 297 are placed in group-3 and $405, 1305$ are placed in group-5. Implicitly, each pigeon hole corresponds to a pair of integers; group-0 denotes $\{0\}$, group-1 denotes $\{1, 99\}$, group-2 denotes $\{2, 98\}$, and group-i denotes $\{i, 100-i\}$. If the remainder is 2 or 98, then the integer i is placed in group-2. Now we can see that there are 51 groups, group-0 to group-50, and by pigeonhole principle, among the 52 distinct integers (*pigeons*), there exist at least two integers say a, b in a group, say group-k.
   $k = (a \bmod 100)$ or $[100 - (a \bmod 100)]$
   and $k = (b \bmod 100)$ or $[100 - (b \bmod 100)]$, where $a \neq b$.
   Note that each group implicitly denotes a pair and in particular group-k denotes a pair $\{l, l'\}$ and further $l + l' = 100$, a mod 100 and b mod 100 are either same (either both are l or both are l') or a mod 100 is l and b mod 100 is l'. This shows that either $a+b$ or $a-b$ is divisible by 100.
   As an example, 103 and 297 leave remainder 3 on performing 'mod 100', and their sum, $103 + 297 = 400$ is divisible by 100. For 405 and 1305, the remainder is 5, and their difference, $1305 - 405 = 900$ is divisible by 100.

7. Prove that in a group of n people, there exist at least two with equal number of friends.

   Observe that the number of friends a person can have is in the range 0 to $n-1$. Interestingly, we can observe some interesting facts as follows. Note that if a person has $n-1$ friends, then there does not exist a person having 0 friends. Similarly, If there exist a person having 0 friends, then there does not exist a person having $n-1$ friends. It follows that the number of friends ranges from 0 to $n-2$ or 1 to $n-1$. Therefore we see two cases, and in both, there exist $n-1$ distinct numbers (*pigeonholes*) which represents the cardinality of the number of friends of a person (*pigeons*). Therefore by pigeonhole principle, there exist at least two people with the same cardinality representing the number of friends they have.

8. Prove that in a sequence of n^2+1 distinct integers, there is either an increasing subsequence of length $n+1$ or a decreasing subsequence of length $n+1$. The subsequence need not be contiguous.

   Let $a_1, a_2, \ldots, a_{n^2+1}$ be the distinct integers. For each integer a_i, $1 \le i \le (n^2+1)$ we associate a pair (x_i, y_i) such that
   $x_i =$ the length of the longest increasing subsequence from a_i to a_{n^2+1}.
   $y_i =$ the length of the longest decreasing subsequence from a_i to a_{n^2+1}.
   On the contrary suppose that the length of the longest increasing and longest decreasing subsequences are both at most n. i.e., $x_i \in \{1, 2, \ldots, n\}$ and $y_i \in \{1, 2, \ldots, n\}$, $1 \le i \le (n^2+1)$. This implies that the maximum number of distinct pairs possible are n^2. Therefore, among the n^2+1 integers, there exist integers a_i, a_j such that the associated pairs are the same. i.e., there exists a pair $(x_i = x_j, y_i = y_j)$ corresponding to a_i and a_j. Since all the elements are distinct, we see the following cases.
   Case 1: If $a_i < a_j$, then it contradicts the fact that the length of the longest increasing subsequence, from a_i is greater than that of a_j. i.e., $x_i > x_j$
   Case 2: If $a_i > a_j$, then it contradicts the fact that the length of the longest decreasing subsequence, from a_j is greater than that of a_i. i.e., $y_j > y_i$
   Therefore, our assumption is wrong and it follows that there exists either an increasing subsequence of length $n+1$ or a decreasing subsequence of length $n+1$.

9. Show that one of any n consecutive integers is divisible by n.

   On the contrary, we assume that there does not exist a number divisible by n in a set of n consecutive integers. By pigeon hole principle, we can place integers in congruence classes, i mod n, $1 \le i \le n-1$ corresponding to pigeonholes. Observe that n integers (*pigeons*) when placed into holes, by pigeonhole principle, there is a pigeon hole with more than one integer. This is a contradiction to the fact that the n integers which are consecutive are distinct and therefore, no two among them belong to same congruent (*congruent modulo n*) class. Therefore, our assumption is wrong and one of any n-consecutive integers is divisible by n.
   Aliter: Possible remainders when divided by n are $\{0, \ldots, n-1\}$. If there does not exist a number divisible by n in a set of n consecutive integers, then two integers a_i, a_j are in the same pigeon hole, say x. i.e. $a_i = n \cdot r + x$ and $a_j = n \cdot s + x$ Since a_i and a_j are distinct, $r \neq s$. Further, $a_i - a_j = n(r-s)$ and $r - s \ge 1$. Therefore, a_i and a_j are apart by more than n integers. A contradiction.

10. Show that the decimal expansion of a rational number, must after some point become periodic.

    Consider a decimal expansion of a rational number $\frac{p}{q}$. Without loss of generality, assume that there are more than 9 digits after the decimal point. Note that each integer after the decimal point belongs to the set $\{1, 2, \ldots, 9\}$. Note that if we see a '0' after a decimal point, it becomes periodic (or expansion terminates). Thus, we designate nine boxes as pigeonholes with labels $1-9$. Each decimal number in the expansion is placed in the box correspond-

ing to the label. Since there are more than 9 digits after the decimal point, by pigeonhole principle, there exist at least one box with more than one integer, which implies that there exist an integer occurring second time in the expansion. Clearly, from the second occurrence onwards, the expansion is periodic.
It is important to note that PHP technique exploits the representation $\frac{p}{q}$ and constructs pigeons and pigeon hole based on it. It is because of this, we are able to argue that a rational number becomes periodic after some time in the expansion. Since irrational numbers do not have such a representation, we are unable to comment on its decimal representation. Moreover, we know that irrational numbers never become periodic.

11. A distinct set of 51 natural numbers are chosen from the first 100 natural numbers. Prove that two of them add to 101.

Let there be 50 boxes labeled as pairs, $(1, 100), (2, 99), (3, 98), \ldots, (50, 51)$. There exists 51 distinct integers (*pigeons*) and 50 boxes (*pigeonholes*). By pigeonhole principle, there exist at least one box having two integers a, b such that $a + b = 101$.

12. Prove that any 5 points within a square of side length 2 units has two points whose distance apart is at most $\sqrt{2}$ units.

Divide the square into 4 sub squares of size 1×1. Note that only 4 such squares (*pigeonholes*) are possible and there exist 5 points (*pigeons*). By pigeonhole principle, there exists a square with more than one point. Maximum distance between any two points in a square of side a is $a\sqrt{2}$. It follows that there exist two points whose distance apart is at most $\sqrt{2}$.

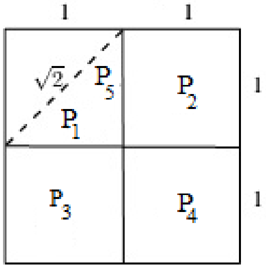


Fig. 3. *An illustration for 5-point square problem*

13. Given m integers $a_1, a_2, \ldots, a_m$. There exist k, l, $1 \le k \le l \le m$ such that $a_{k+1} + a_{k+2} + \ldots + a_l$ is divisible by m.

Let $S_i = \sum_{j=1}^{i} a_j$ and $R_i = S_i \; mod \; m$, $1 \le i \le m$ i.e., remainder $R_i = (a_1 + a_2 + \ldots + a_i) \; mod \; m$. If there exists $R_i = 0$ for some i, then $a_1 + a_2 + \ldots + a_i$ is divisible by m. Otherwise for all i, $R_i \in \{1, 2, \ldots, (m-1)\}$. We consider *pigeonholes* as $m - 1$ remainder values ranging from 1 to $(m - 1)$ and *pigeons* as m remainders R_1 to R_m. By pigeonhole principle, there exist at least two remainders A, B such that $A = a_1 + a_2 + \ldots + a_k = m \cdot c + r$, and $B = a_1 + a_2 + \ldots + a_l = m \cdot d + r$. Without loss of generality, let $l > k$ and thus $d > c$. It follows that $B - A = a_{k+1}, a_{k+2}, \ldots, a_l = m(d - c)$. Therefore, there exist k, l, $1 \leq k \leq l \leq m$ such that $a_{k+1} + a_{k+2} + \ldots + a_l$ is divisible by m.

14. It is proposed to build a computer science lab with 15 workstations and 10 servers. For each server only one direct connection (internet cable) can be active at any time. What is the minimum number of cables required so that we can guarantee that at any time, any set of 10 or fewer workstations can simultaneously access different servers via direct connections?

    We can achieve this using $15 \times 10 = 150$ connections. We will now look for an efficient structure to minimize the number of connections. Let $w_1, w_2, \ldots, w_{15}$ be the workstations and $s_1, s_2, \ldots, s_{10}$ be the servers. One of the optimum ways is as follows. Connect 10 workstations, say $w_1, w_2, \ldots, w_{10}$ directly to $s_1, s_2, \ldots, s_{10}$ such that there exists one connection each from w_i to s_i, $1 \leq i \leq 10$. Connect the remaining 5 workstations to all servers. i.e., connect w_j, $11 \leq j \leq 15$ to s_i, $1 \leq i \leq 10$. Therefore there are altogether $10 + 50 = 60$ connections.

Principle of Inclusion and Exclusion

Like mathematical induction and pigeon hole principle, principle of inclusion and exclusion (PIE) is a popular proof technique applied to many classical counting problems. The idea is to include sets satisfying some properties, while doing so due to overlap between sets, some elements may be counted more than once which would be excluded subsequently. This ensures that each element is counted exactly once.

Problem 1: Given a set $\{1, 2, \ldots, 100\}$ of integers. How many are divisible by 3 or 5 ?
Solution:
Let A_3 denotes the number of integers divisible by 3 in the set $\{1, 2, \ldots, 100\}$, A_5 denotes the number of integers divisible by 5 in the set $\{1, 2, \ldots, 100\}$ and A_{15} denotes the number of integers divisible by 15 in the set $\{1, 2, \ldots, 100\}$.

$A_3 = \lfloor \frac{100}{3} \rfloor = 33$

$A_5 = \lfloor \frac{100}{5} \rfloor = 20$

$A_{15} = \lfloor \frac{100}{15} \rfloor = 6$

$$\begin{aligned} A_3 \cup A_5 &= A_3 + A_5 - A_3 \cap A_5 \\ &= A_3 + A_5 - A_{15} \\ &= \text{33+20-6} = 47 \end{aligned}$$

Problem 2: Given a set $\{1, 2, \ldots, 100\}$ of integers. How many are divisible by 2 or 3 or 5 ?
Solution:
Let A_i denotes the number of integers divisible by i in the set $\{1, 2, \ldots, 100\}$, where $i = \{2, 3, 5, 6, 10, 15, 30\}$.

$A_2 = \lfloor \frac{100}{2} \rfloor = 50$

$A_3 = \lfloor \frac{100}{3} \rfloor = 33$

$A_5 = \lfloor\frac{100}{5}\rfloor = 20$

$A_6 = \lfloor\frac{100}{6}\rfloor = 16$

$A_{10} = \lfloor\frac{100}{10}\rfloor = 10$

$A_{15} = \lfloor\frac{100}{15}\rfloor = 6$

$A_{30} = \lfloor\frac{100}{30}\rfloor = 3$

$$\begin{aligned} A_2 \cup A_3 \cup A_5 &= A_2 + A_3 + A_5 - A_3 \cap A_2 - A_3 \cap A_5 - A_2 \cap A_5 + A_2 \cap A_3 \cap A_5 \\ &= A_2 + A_3 + A_5 - A_6 - A_{15} - A_{10} + A_{30} \\ &= \text{50+33+20-16-6-10+3} = 74 \end{aligned}$$

Problem 3: Given a set $\{1, 2, \ldots, 1000\}$ of integers. How many are divisible by 3 or 5 ?
Solution:
Let A_3 denotes the number of integers divisible by 3 in the set $\{1, 2, \ldots, 1000\}$, A_5 denotes the number of integers divisible by 5 in the set $\{1, 2, \ldots, 1000\}$ and A_{15} denotes the number of integers divisible by 15 in the set $\{1, 2, \ldots, 1000\}$.

$A_3 = \lfloor\frac{1000}{3}\rfloor = 333$

$A_5 = \lfloor\frac{1000}{5}\rfloor = 200$

$A_{15} = \lfloor\frac{1000}{15}\rfloor = 66$

$$\begin{aligned} A_3 \cup A_5 &= A_3 + A_5 - A_3 \cap A_5 \\ &= A_3 + A_5 - A_{15} \\ &= \text{333+200-66} = 467 \end{aligned}$$

Problem 4: Given a set $\{1, 2, \ldots, 1000\}$ of integers. How many are divisible by 3 or 5 or 7 ?
Solution:
Let A_i denotes the number of integers divisible by i in the set $\{1, 2, \ldots, 1000\}$, where $i = \{3, 5, 7, 21, 15, 35, 105\}$.
$A_3 = \lfloor\frac{1000}{3}\rfloor = 333$

$A_5 = \lfloor\frac{1000}{5}\rfloor = 200$

$A_7 = \lfloor\frac{1000}{7}\rfloor = 142$

$A_{15} = \lfloor\frac{1000}{15}\rfloor = 66$

$A_{35} = \lfloor\frac{1000}{35}\rfloor = 28$

$A_{21} = \lfloor\frac{1000}{21}\rfloor = 47$

$A_{105} = \lfloor\frac{1000}{105}\rfloor = 9$

$$\begin{aligned} A_3 \cup A_5 \cup A_7 &= A_3 + A_5 + A_7 - A_3 \cap A_5 - A_5 \cap A_7 - A_3 \cap A_7 + A_3 \cap A_5 \cap A_7 \\ &= A_3 + A_5 + A_7 - A_{15} - A_{35} - A_{21} + A_{105} \\ &= \text{333+200+142-66-28-47+9} = 543 \end{aligned}$$

Theorem: Given $A_1, A_2, \ldots, A_n$ satisfying some property. $A_1 \cup A_2 \cup \ldots \cup A_n =$

$$\sum_{1 \leq i \leq n} A_i - \sum_{1 \leq i < j \leq n} A_i \cap A_j + \sum_{1 \leq i < j < k \leq n} A_i \cap A_j \cap A_k - \ldots + (-1)^{n+1} \sum_{1 \leq i < j < k < \ldots \leq n} A_1 \cap A_2 \cap \ldots \cap A_n$$

.

Proof:

We now show that each element satisfying a property is counted exactly once in the above expression.

Suppose an element x occurs r times, say in $A_1, A_2, \ldots, A_r$.

The element x is counted r_{c_1} times in $\sum A_i$, r_{c_2} times in $\sum(A_i \cap A_j)$, ..., r_{c_r} times in $\sum(A_i \cap A_j \ldots A_k)$

Therefore, the total count of element x

$= r_{c_1} - r_{c_2} + r_{c_3} - r_{c_4} + \ldots (-1)^{r+1} r_{c_r}$

We next show that the above expression evaluates to one, meaning x occurs exactly once the in counting.

It is known that $r_{c_0} - r_{c_1} + r_{c_2} - \ldots (-1)^r r_{c_r} = (1 + (-1))^r = 0$

Further, $r_{c_1} - r_{c_2} + \ldots + (-1)^{r+1} r_{c_r} = r_{c_0} = 1$

Hence, $r_{c_1} - r_{c_2} + r_{c_3} - r_{c_4} + \ldots (-1)^{r+1} r_{c_r} = 1$

Therefore, x is counted exactly once, the counting expression is indeed true.

Derangements

(De-Arrangement) A permutation of the set $\{1, \ldots, n\}$ such that the element $'i'$ does not occur in its natural position (element i does not occur at i^{th} position).

- For example, derangements of the set $\{1, 2, 3\}$ are $(2, 3, 1)$ and $(3, 1, 2)$.

Number of derangements

Number of derangements of a set with n elements$(D_n) =$

Number of permutations with n elements - Number of permutations in which i occurs in its natural position

Number of permutations with n elements $= n!$

Let A_i denotes the number of permutations in which element i occurs in its natural position i.

$\mid A_i \mid = n_{c_1}(n-1)!$

Let $A_i \cap A_j$ denotes the number of permutations in which elements i, j occurs in their respective natural positions. $\mid A_i \cap A_j \mid = n_{c_2}(n-2)!$

Therefore, the number of derangements =

$$D_n = n! - \left[n_{c_1}(n-1)! - n_{c_2}(n-2)! + n_{c_3}(n-3)! - \ldots + (-1)^{n+1} n_{c_n}(n-n)!\right]$$

$$D_n = n! - \left[\tfrac{n!}{1!} - \tfrac{n!}{2!} + \tfrac{n!}{3!} - \ldots + (-1)^{n+1}\tfrac{n!}{n!}\right]$$

$$D_n = \textstyle\sum_{i=2}^{n} (-1)^i \ \tfrac{n!}{i!} \text{ or } D_n = \textstyle\sum_{i=0}^{n} (-1)^i \ \tfrac{n!}{i!}$$

Number of onto functions

We shall next count the number of onto functions using PIE. *Suggestion:* This section may be revisited after reading functions for better understanding.
Let $\mid A \mid = n$ and $\mid B \mid = m$.
Number of onto functions = Number of functions - Number of functions that are not onto.

The number of functions from A to $B = m^n$
Let $B = \{a_1, a_2, \ldots\}$. The number of functions between A and B in which there is no pre-image for $a_1 = (m-1)^n$. Similarly, for $a_2, a_3, \ldots$
Therefore, the total number of functions in which there is no pre-image for $a_i = m_{c_1}(m-1)^n$.
Similarly, the total number of functions in which there is no pre-image for $(a_1, a_2) = (m-2)^n$.
Therefore, for any two $(a_i, a_j) = m_{c_2}(m-2)^n$.

Thus, the number of onto functions =

$$m^n - \left[m_{c_1}(m-1)^n - m_{c_2}(m-2)^n + m_{c_3}(m-3)^n - \ldots + (-1)^m m_{c_{m-1}}(1)^n\right]$$

Distribution of m jobs and n servers

Distribute m-jobs among n-servers such that each server gets at least one job. This problem is equivalent to, distributing m-balls among n-boxes such that each box gets at least one ball, which is same as finding the number of integral solutions to the equation $x_1 + x_2 + \ldots + x_n = m$ with the constraint, for each i, $x_i \geq 1$. Further, this is precisely the number of onto functions between sets of size m and n

Acknowledgements: Lecture contents presented in this module and subsequent modules are based on the text books mentioned at the reference and most importantly, lectures by discrete mathematics exponents affiliated to IIT Madras; Prof P.Sreenivasa Kumar, Prof Kamala Krithivasan, Prof N.S.Narayanaswamy, Prof S.A.Choudum, Prof Arindama Singh, and Prof R.Rama. Author sincerely acknowledges all of them. Special thanks to Teaching Assistants Mr.Renjith.P and Ms.Dhanalakshmi.S for their sincere and dedicated effort and making this scribe possible. This lecture scribe is based on the course 'Discrete Structures for Computing' offered to B.Tech COE 2014 batch during Aug-Nov 2015. The author greatly benefited by the class room interactions and wishes to appreciate the following students: Mr.Vignesh Sairaj, Ms.Kritika Prakash, and Ms.Lalitha. Finally, author expresses sincere gratitude to Ms.Kritika Prakash for thorough proof reading and valuable suggestions for improving the presentation of this article. Her valuable comments have resulted in a better article.

References:

1. K.H.Rosen, Discrete Mathematics and its Applications, McGraw Hill, 6th Edition, 2007
2. D.F.Stanat and D.F.McAllister, Discrete Mathematics in Computer Science, Prentice Hall, 1977.
3. C.L.Liu, Elements of Discrete Mathematics, Tata McGraw Hill, 1995

[1] Paul Erdos .

"Aliens invade the earth and threaten to obliterate it in a year's time unless human beings can find [R(5,5)]. We could marshal the world's best minds and fastest computers, and within a year we could probably calculate the value If the aliens demanded [R(6,6)], however, we would have no choice but to launch a preemptive attack"

[1] Scientific American: pp. 112-117, 1990.