CS207 Counting

By: Harsh Shah

October 2021

Contents

1 Permutations and Combinations

1.1 String

A string is an ordered collection of elements from an alphabet(a finite set).
Mathematically, it is a mapping of each position in the string to an element in alphabet,

$$String(\sigma) : \{1, 2, \dots k\} \to B$$

Number of strings of length k from an alphabet of size n: n^k

If n=2, then the string is called a **binary string**.
Binary strings can be used to represent subsets of $[k] = \{1, 2 \dots k\}$.
Let the alphabet be {0,1}. Then the subset of $[k]$ corresponding to a binary sting is:

$$S_\sigma = \{x | \sigma_x = 1\}$$

1.2 Permutations

Permutations refer to the arrangements of elements of alphabet without repetitions of the elements.
The number of permutations of length k from a alphabet of size n is denoted as P(n,k).

$$P(n,k) = \begin{cases} 0 & if \quad k > n \\ \frac{n!}{(n-k)!} & if \quad k \leq n \end{cases}$$

The above expression can be proved by induction on n and using the relation

$$P(n,k) = n \cdot P(n-1, k-1)$$

in the induction step.

1.3 Combinations

Combinations can considered as subsets of a given set. The number of subsets of size k from a set of size n is given by:

$$C(n,k) = \frac{P(n,k)}{k!}$$

Important property: **C(n,k)=C(n-1,k-1)+C(n-1,k)**
The above property can be used find the coefficients of x^k in expansion of $(1+x)^k$, inductively.
The property also gives a **recursive definition** of C(n,k) with base cases $C(n,0) = C(n,n) = 1$

2 Balls and Bins

Let the number of balls be k and number of bins be n.
We need to allot each ball to exactly one bin.
Consider the following different cases(N is the number of ways):

2.1 Labelled balls and labelled bins

2.1.1 No restriction

N = number of functions from set of size k to set of size n = n^k

2.1.2 Atmost one ball in every bin

N=number of injective functions = $P(n,k)$

2.1.3 No bin empty

N=number of onto functions=N(k,n)

$$N(k,n) = \begin{cases} \sum_{i=0}^{i=n} (-1)^i \cdot C(n,i) \cdot (n-i)^k & if \quad n \leq k \\ 0 & if \quad n > k \end{cases}$$

The above equation can be proved by inclusion-exclusion principle.

2.2 Unlabelled balls labelled bins

2.2.1 No restriction

This case can be represented by a multi-set, which is a set in which multiple entries of an element can occur, but is unordered. Each multi-set of length k having elements from the bin set represents one way of distribution.
In this case, N can be found by partitioning the the set of identical balls. The problem can be reformulated as ways of arranging k identical balls and n-1 identical sticks in a row, which is

$$N = \frac{(k+n-1)!}{(n-1)!(k)!} = C(k+n-1, n-1)$$

2.2.2 Atmost one ball in every bin

N=ways of selecting k bins out of n bins (remaining will be empty)=C(n,k)

2.2.3 No bin empty

This case is similar to no restriction case after giving one ball to each bin. Hence,

$$N = C(k-1, n-1)$$

2.3 Labelled balls and unlabelled bins

2.3.1 No restriction

This case can be reformulated as number of ways of partitioning a set of length k. The number of ways of partitioning a set of length k into n non-empty subsets is given by **Stirling's number of second kind** and is denoted by S(k,n).
Hence N is given by,

$$N = B_k(\text{Bell number}) = \sum_{i=1}^{i=k} S(k,i) \quad [= \sum_{i=1}^{i=n} S(k,i))]$$

where,

$$S(k,n) = \frac{N(k,n)}{n!}$$

2.3.2 Atmost one ball in every bin

$$N = \begin{cases} 1 & if \quad n \geq k \\ 0 & if \quad n < k \end{cases}$$

2.3.3 No bin empty

$$N = S(k,n)$$

2.4 Unlabelled balls and unlabelled bins

2.4.1 No restriction

The problem cn be reformulated as number of integer solutions $(x_1, x_2, \ldots x_n)$ such that,

$$x_1 + x_2 \ldots x_n = k$$

and

$$0 \leq x_1 \leq x_2 \cdots \leq x_n$$

If the bins are non-empty ,i.e., 1 instead of 0 in the above relation(the no bin empty case) then the number of such ways has a name, partition number(denoted by $P_n(k)$).
Therefore in this case, just add n 1's on both sides of the equation. This given,

$$N = P_n(n+k)$$

2.4.2 Atmost one ball in every bin

$$N = \begin{cases} 1 & if \quad n \geq k \\ 0 & if \quad n < k \end{cases}$$

2.4.3 No bin empty

$$N = P_n(k)$$

How to calculate $P_n(k)$?
$P_n(k)$ can be calculated recursively as follows:
Base case: $P_n(k) = 0$ if $n > k$; and $P_0(0) = 1$; and $P_0(k) = 0$ if $k > 0$
Recursive relation: $P_n(k) = P_n(k-n) + P_{n-1}(k-1)$
Above relation can be proved by considering exhaustive cases $x_1 > 1$ or $x_1 = 1$.

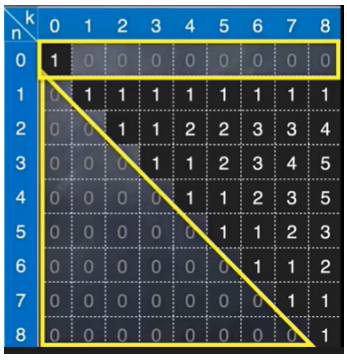

Figure 1: Partition number; Source : CS207 Lectures 2021

CS207 Functions

By: Harsh Shah

October 2021

Contents

1 Basics

- A function maps each element in domain to co-domain
- All elements of co-domain may not be used. The elements in co-domain which are used form image set. Mathematically,

$$Im(f) = \{x \in \text{co-domain}(f) | \exists y \in \text{domain}(f)\ f(y) = x\}$$

- Functions can be considered as a heterogeneous relation between domain and co-domain.

$$R_f = \{(x, f(x)) | x \in domain(f)\}$$

- Composition of two functions $(f \circ g)$ is a function mapping domain of f to co-domain of g

$$f \circ g(x) \equiv f(g(x))$$

  Defined only if $Im(f) \subseteq domain(g)$

2 Types of functions

- Onto(surjection): Im(f)=co-domain(f) i.e., $\forall x \in$ co-domain$(f) \exists y \in$ domain(f) s.t. $f(y) = x$
- One-to-one(injection): f(x)=f(y) $\implies$ x=y
- Bijection: Surjection+Injection

Invertible function: A function is said to be invertible if $\exists g$ such that $g \circ f =$ Identity
Claim: **Injective functions are invertible.**
Proof:$\forall y \in Im(f)$ let g(y)=x, where f(x)=y
$\forall y \in$ co-domain$(f) - Im(f)$ let g(y)=x (arbitrary) where $x \in$ domain(f)
Note that g may not be invertible in such a mapping.

Claim: **Invertible functions are one-to-one**
Proof: Suppose invertible functions are not one-to-one.
Apply mapping g to $f(x_1) = f(x_2)$, then $x_1 = x_2$. Contradiction.

Inverse of a bijective function is also invertible.

3 Important Properties

Suppose $f : A \to B$ Some properties(if A and B are finite sets):-

- $|A| \leq |Im(f)|$, equality iff f is injective
- $|B| \leq |Im(f)|$, equality iff f is surjective
- If f is onto, then $|A| \geq |B|$
- If f is injective, then $|A| \leq |B|$
- If f is bijective, then $|A| = |B|$

Properties of composition of functions f and g (assume **co-domain(f)=domain(g)**):

- If f and g are onto, then $g \circ f$ is also onto. Converse does not hold. However, if $g \circ f$ is onto, then g is onto.
- If f and g are injective, then $g \circ f$ is injective. Agsin converse does not hold. However, if $g \circ f$ is injective, then f is injective.

Above results may change if the assumption **co-domain(f)=domain(g)** is modified.

CS207 Graphs

By: Harsh Shah

October 2021

Contents

1 Definition

A simple graph $G := (V, E)$ represents a set of vertices V and edges E, where,

$$E \subseteq \{\{a, b\} | a, b \in V; a \neq b\}$$

A simple graph can be considered a symmetric(since undirected edges) and irreflexive(no self-loops).
A non-simple graph can have multiple edges between vertices, and can even have weights associated with edges.

2 Examples

2.1 Complete graph(K_n)

A graph with n vertices in which there is an edge between every possible pair of vertices. Mathematically,

$$E = \{\{a, b\} | a, b \in V; a \neq b\}$$

2.2 Cycle graph(C_n)

A graph with n vertices $V = \{v_1, \dots v_n\}$, in which the edge set is given as

$$E = \{\{v_i, v_{i+1}\} | i = [n-1]\} \cup \{\{v_n, v_1\}\}$$

2.3 Bipartite graph

A graph is called bipartite graph if V can be partitioned into V_1 and V_2 such that $V_1 \cap V_2 = \Phi$ and there does not exist any edge between vertices of same set. Mathematically,

$$E \subseteq \{\{a, b\} | a \in V_1; b \in V_2\}$$

2.4 Complete Bipartite graph

A graph is called bipartite graph if V can be partitioned into V_1 and V_2(both non-empty) such that $V_1 \cap V_2 = \Phi$ and edge set is given by

$$E = \{\{a, b\} | a \in V_1; b \in V_2\}$$

2.5 Isomorphic graphs

Two graphs $G_1 = (V_1, E_1)$ and $G_2 = (V_2, E_2)$ are said to be isomorphic if there exists a bijection $f : V_1 \to V_2$ such that

$$\{u, v\} \in E_1 \iff \{f(u), f(v)\} \in E_2$$

Finding whether given two graphs are isomorphic or not is a computationally hard problem.

2.6 Subgraphs

A subgraph of a given graph $G = (V, E)$ is a graph $G' = (V', E')$ such that

$$V' \subseteq V; E' \subseteq E$$

An induced subgraph is the one in which all the possible edges between vertices i V' are present in G' (and are also present in E).

3 Walks and Path

3.1 Walk

A walk of length k from vertex a to vertex b is a ordered set of $k+1$ vertices $(v_0, \dots v_k)$ such that

- $v_0 = a$ and $v_k = b$
- $\{v_i, v_{i+1}\} \in E \forall i = 0, \dots k-1$

3.2 Path

A walk with **no repeating** vertices.

3.3 Cycle

A walk of length $k \geq 3$ with **only repeating** vertices being the first and the last element of the walk.
A graph G is acyclic if there does not exist a subgraph of G such that it is isomorphic to C_n

3.4 Connectivity

Vertex u is said to be connected to vertex v if there exists a walk from u to v.
Connected(u, v) is an equivalence relation, and the equivalence classes of this relation form connected components of the graph G.

3.5 Degree of a vertex($deg(v)$)

Number of edges incident on v. Mathematically,

$$deg(v) = |\{u | \{u, v\} \in E\}|$$

Important result: $\sum_{v \in V} deg(v) = 2|E|$
Degree sequence: Sorted list of degrees(invariant under isomorphism)
To check if a degree sequence is possible, distribute the highest degree among other degree(and hence subtracting from other degrees at top till the highest degree is exhausted), and then recursively solve the smaller problems.

3.6 Eulerian trail

A walk visiting every edge **exactly** once.
Property: Eulerian trail exists $\implies$ At most two odd degree vertices
Proof: There must be an edge to leave a particular vertex for every edge used for walking into the vertex, except for the extreme vertices.

Eulerian circuit: A **closed** walk visiting every edge **exactly** once.
Property: Eulerian trail exists $\implies$ No odd degree vertices Proof: There must be an edge to leave a particular vertex for every edge used for walking into the vertex.

Property: If a connected graph has no odd degree nodes then there exists an Eulerian circuit.
Proof: Given a graph G is connected and has no odd degree vertices, the graph must be cyclic(start from a walk from a vertex and keep visiting vertices until a repeating vertex is found). Them remove the edges of the cycle found to form multiple connected components, where each of the connected components would have no odd degree vertices. Then inductively carry out the above

process to find smaller Eulerian circuits and finally stitch them to get Eulerian circuit of original graph.

3.7 Hamiltonian cycle

A **cycle** that has all the vertices of a graph.
No efficient algorithm to compute Hamiltonian cycle exists.

3.8 Distance

Length of the shortest walk between two vertices.
A shortest walk between two vertices is always a path. (proof by contradiction)
Diameter is the largest distance over all the pairs of vertices of the graph.

4 Graph coloring

A coloring is a mapping from the vertices to a set of colors.(usually term coloring is used for proper coloring)
A perfect coloring(of k colors) is the one in which no two vertices sharing an edge has the same color. Mathematically,

$$u, v \in E \implies c(u) \neq c(v)$$

Chromatic number($\chi(G)$): Least k such that a proper coloring of k colors exist. Eg, $\chi(K_n) = n$

$$\text{G has k-coloring} \iff \chi(G) \leq k$$

Results:

- If H is a subgraph of G, then $\chi(G) \geq \chi(H)$
- Isomorphism preserves χ

Efficient algorithms for coloring a graph is known but finding chromatic number of a graph is believed to be NP-hard problem.
Claim: $\forall n \geq 1$, C_{2n+1} is not bipartite
Proof: By contradiction,
If bipartite, start coloring the vertices with two colors clockwise, leading to contradiction.

Claim: A graph is bipartite (with $|V| > 1$) $\iff$ it has no odd length cycles.
Proof: Forward implication is easy to prove. For reverse implication, that is, no odd length cycle implies bipartite,
Let's prove the contrapositive, if not bipartite then odd length cycle exists.
Now, not bipartite $\implies$ there exists a connected component C which is not bipartite
Consider a vertex v in C and partition C such that vertices with even distance are in one component and with odd distances are in another component. There must be an edge joining vertices within these component since the graph is not bipartite. But this would result in odd length cycle.

Claim: $\chi(G) = n \iff G$ **is isomorphic to** K_n Proof: Reverse implication is simple to prove. For forward implication we have to prove,
If $\chi(G) = n$, then G is isomorphic to K_n
Suppose there exists a pair $\{u, v\}$ which does not have an edge. Then give same color to the two vertices and different $n-2$ colors for remaining vertices. This is a proper coloring with $n-1$ colors, hence contradiction.

4.1 Clique number($\omega(G)$)

It is the largest natural number c such that G has a subgraph isomorphic to K_c

4.2 Independence number($\alpha(G)$)

Largest m such that G has a set of m vertices with no edges between them.
Given a proper coloring, the vertices with same color form a independent set.
Important Results:

- $n = \sum_c$number of vertices with color $c \leq \alpha(G)\chi(G)$
- $\chi(G) \leq maxdeg(G) + 1$
  Proof: Induction on number of vertices. Take any arbitrary graph and remove a vertices and corresponding edges. Color the graph using $\chi(G') \leq maxdeg(G') + 1 \leq maxdeg(G) + 1$. For the removed vertex, there would exists atleast one color different from the $deg(v) \leq maxdeg(G)$ vertices connected to it.
  Fact: Equality holds only for K_n and C_{2n+1}

5 Other families of graph

5.1 Path graph(P_n)

$V = [n]$ and $E = \{\{i, i+1\}|i \in [n-1]\}$
Bipartite graph

5.2 Wheel graph(W_n)

Cycle graph(C_n) with additional vertex and an edge between the vertex and every vertex of C_n

5.3 Ladder graph(L_n)

$V = \{0, 1\} \times [n]$
$E = \{\{(0, i), (1, i)\}|i \in [n]\} \cup \{\{(b, i), (b, i+1)\}|b \in \{0, 1\}; i \in [n-1]\}$
Bipartite graph

5.4 Cyclic Ladder(CL_n)

Two additional edges to L_n :{(0,1),(0,n)} and {(1,1),(1,n)}

5.5 Hypercube graph(Q_n)

$V =$ all possible n-bit strings (2^n vertices)
$E = \{\{u, v\}|$u and v differ in only one bit$\}$
Diameter of the graph $= n$
Bipartite graph

5.6 $\overline{KG}_{n,k}$

Consider a graph Q_n and let the vertices(which are represented as n-bit strings) be represented as sets storing the positions at which 1 occurs. Let the vertices with same size,k , of such sets be V and let there be an edge between them if there is non-empty intersection of their corresponding sets.

The resulting graph is $\overline{KG}_{n,k}$.
A clique(completely connected component) in the above graph can have a maximum of ${}^{n-1}C_{k-1}$ vertices (having only one element common between each pair), if $k \leq n/2$(Erdos-ko-Rado Theorem).

5.7 Kneser Graph

Complement graph of $\overline{KG}_{n,k}$.(Complement of a graph: Interchange edges and non-edges)

6 Graph operations

Intersection/union of two graphs is component wise(for vertices and edges) intersection/union.

6.1 Powering

Given $G = (V, E)$. Then $G^2 = (V, E')$ is defined as

$$E' = \{\{u, v\} | \exists w \quad s.t.\ \{u, w\} \in E; \{v, w\} \in E\}$$

Moe generally, G^k has edge $\{x, y\} \iff$ There exists a path of length k in G between x and y.

6.2 Cross product

Let $G_1 = (V_1, E_1)$ and $G_2 = (V_2, E_2)$. $G_1 \times G_2 = (V, E)$ where,

$$E = \{\{(u_1, u_2), (v_1, v_2)\} | \{u_1, v_1\} \in E_1 \wedge \{u_2, v_2\} \in E_2\}$$

6.3 Box product

Let $G_1 = (V_1, E_1)$ and $G_2 = (V_2, E_2)$. $G_1 \square G_2 = (V, E)$ where,

$$E = \{\{(u_1, u_2), (v_1, v_2)\} | (\{u_1, v_1\} \in E_1 \wedge u_2 = v_2) \vee (\{u_2, v_2\} \in E_2 \wedge u_1 = v_1)\}$$

Eg, $Q_m \square Q_n = Q_{m+n}$

6.4 Hamming graph($H_{n,q}$)

Generalization of hypercubes.
$H_{n,q} = K_q \square \ldots \square K_q$ (n times K_q)
For $q = 2$, Hamming graphs are same as hypercube graphs.

7 Matching

A matching, M, is a subset of E having no common vertices between any two pairs of edges. Mathematically,

$$M \subseteq \ s.t. \quad \forall e_1, e_2 \in M, e_1 \neq e_2 \implies e_1 \cap e_2 = \Phi$$

Perfect matching: Matching with all vertices covered.
Efficient algorithms exist for finding maximum matching.

7.1 Matching in bipartite graphs

Given a bipartite graph, $G = (X, Y, E)$, a complete matching M from X to Y is a matching having $|M| = |X|$.
If$|X| = |Y|$, a complete matching from X to Y is also a complete matching from Y to X, and the matching is also a perfect matching.

7.2 Neighbourhood

Neighbourhood of a set of vertices is given by,

$$\Gamma(S) = \bigcup_{v \in S} \{u | \{u, v\} \in E\}$$

For a bipartite graph $G = (X, Y, E)$, let $S \subseteq X$

- S is shrinking if $|\Gamma(S)| < |S|$
- Let $B \subseteq Y$. Then S is shrinking in B if $|\Gamma(S) \cap B| < |S|$

7.3 Hall's Theorem

A bipartite graph $G = (X, Y, E)$ has a complete matching from X to Y **iff** no subset of X is shrinking.

Proof: Forward implication is simple to proof. For reverse implication, we need to prove
No shrinking $S \subseteq X \implies$ a complete matching from X to Y exists
Proof by induction. True for $|X| = 1$. Assume the claim for $|X| = k$
Induction step: Consider any arbitrary bipartite graph, with non-shrinking X, and $|X| = k + 1$. Consider any vertex,u , in X and find the its neighbour v in Y. If $\exists$ a complete matching from $X - \{u\}$ to $Y\{y\}$ then we have found a complete matching from X to Y(by including the removed vertices). However if not, then consider the shrinking subset,S of $X - \{u\}$ and complete matching into $\Gamma(S)$ can be found by induction hypothesis. Further it can be proved that there cannot be a shrinking subset of $X - S$ in $Y - \Gamma(S)$. This way a matching for the original graph is found.

Application: The edge set of a $d-$ regular bipartite graph can be partitioned into d complete matchings. (Proof by induction on d and using Hall's theorem after proving the non-shrinking property to remove a perfect matching from $d = k + 1$ regular graph).

8 Vertex cover

A vertex cover is a set of vertices, $C \subseteq V$ such that any edge has atleast one vertex in C, that is,

$$\forall e \in E \quad e \cup C \neq \Phi$$

Finding the smallest vertex cover for a arbitrary graph is a NP-hard problem.
Important result: For any graph G, $|C| \geq |M|$, $\forall$ vertex cover C and $\forall$ matchings M. (Proof: Any vertex in a vertex cover can correspond to atmost one edge in a matching, and all the edges of the matching must be used up).

8.1 Konig's Theorem

For a bipartite graph, the size of smallest vertex cover is equal to the size of the largest matching.
Proof: We need to prove that for the smallest vertex cover C there exists a matching M, such that $|M| \geq |C|$

Proof: Consider the sets $A = X \cup C$ and $B = Y \cup C($ where C is the smallest vertex set). Find a complete matching from A to $Y - B$ and from B to $X - A$. Hall's theorem can be used and it can be shown that there cannot be a shrinking subset of A, say S, in $Y - B$, because,

$$|C \cup \Gamma(S) - S| = |C| + |\Gamma(S) - B| - |S|(< |C| \text{ if shrinking})$$

(not possible since C is smallest)

8.2 Maximal matching

A maximal matching is a matching, having the property that adding any edge would violate the matching property.
If M is a maximal matching, $\exists$ a vertex cover of size $2|M|$.
This can be used to bound the size of smallest vertex cover C.

$$|M| \leq |C| \leq 2|M|$$

8.3 Independent set

I is an independent set(that is, set of vertices having no edges between them) of a graph $G \iff \overline{I}$ is vertex cover.

Therefore, **size of smallest vertex cover + size of largest independent set =** n

9 Trees

A connected acyclic graph is called a tree.
An acyclic graph is called a forest, and each connected component is a tree.
A leaf in a tree is a vertex with degree one.

Claim: Every tree with $|V| \geq 2$, has atleast 2 leaves.
Proof: Consider a maximal path. If the extreme vertices of the path are not leaves then the path would not be maximal(since they cannot be connected to any internal vertex of the path since trees are acyclic).

Claim: Deleting a leaf vertex of a tree and the edge incident on that vertex results in a tree.
Proof: Deleting a vertex cannot induce a cycle. And the vertices in the new tree are connected.

Claim: In a tree, for all pairs of vertices u, v, there is exactly one u-v path.
Proof: By contradiction,
If there exists two distinct paths, then there exists a cycle. But a tree is acyclic.

Claim: Number of edges in a tree $= |V| - 1$
Proof: Can be proved by induction on number of vertices and deleting a leaf in the induction step.

Claim: If a graph is connected and $|E| = |V| - 1$, then the graph is a tree.
Proof: By contradiction,
If a graph is connected and $|E| = |V| - 1$, has a cycle, delete any vertex of the cycle(the graph is still connected), and keep on doing so until no cycles are left. The remaining graph is a tree with $|E| < |V| - 1$(Contradiction)

Claim: In a forest the number of connected components $c = |V| - |E|$
Proof: Sum up edges in each connected component...

Claim: Deleting a degree d vertex from a tree results in d connected components.
Proof: From the above result.

10 Dilworth's Theorem

In a poset, size of any anti-chain $\leq$ size of any chain decomposition(partition of the poset into chains).
Dilworth's theorem states that equality is achieved.

Recall that, in a poset, size of any chain $\leq$ size of any anti-chain decomposition and **Mirsky's theorem** guarantees equality.

Proof sketch: We can prove that there exists an anti-chain atleast as large as a chin decomposition.
Consider a bipartite graph $G = (\{S\} \times \{0\}, \{S\} \times \{0\}, E)$, where

$$E = \{\{(u, 0), (v, 1)\} | u \leq v\}$$

Consider a vertex cover C and a matching M in G.
To get a large antichain, construct B such that it is the first element of all vertices in G(irrespective of the 0 or 1).
Then $A = S - B$ is an antichain, with property $|A| \geq |S| - |C|$
(since $|B| \leq |C|$)
Now using M construct $F = (S, \{\{u, v\} | \{(u, 0), (v, 1)\} \in M\})$.
It can be easily proved that F is a forest and each connected component of F is a **path**.
Number of connected components = Size of a chain decomposition = $|S|$-$|edges(F)|$
Now, using Konig's theorem $\exists$ C and M such that $|C| = |M|$. Hence proved.

10.1 Comparison graph

Given a poset $(S, \leq)$, its comparison graph $G = (S, E)$ is given as,

$$E = \{\{u, v\} | u \leq v; u \neq v\}$$

Important results:

- **Any induced subgraph of G is also a comparison graph.** (because a subset of poset is also a poset)
- **A chain corresponds to a clique(completely connected component) in G and an anti-chain corresponds to independent set in G(equivalently a clique $\overline{G}$).**
- **An anti-chain decomposition corresponds to a coloring in G and a chain decomposition corresponds to coloring of $\overline{G}$.**

10.2 Mirsky's Theorem and Dilworth's Theorem restated

Mirsky's Theorem: For a comparison graph, $\chi(G) = \omega(G)$
Dilworth's Theorem: For a comparison graph, $\chi(\overline{G}) = \omega(\overline{G})$

10.3 Perfect graph

A graph G is perfect if every induced sub graph, G' of G has property: $\chi(G') = \omega(G')$
Comparison graphs are perfect(using Mirsky's theorem).

CS207 Sets and relations

By: Harsh Shah

September 2021

Contents

1 Basics

- Set : Unordered collection of elements
- Set membership(belongs to) : $73 \in \mathbb{Z}$
- Set inclusion (subset) : $\mathbb{Z} \subseteq \mathbb{R}$
- Set operations : union, intersection,...

1.1 Sets as predicate

Sets can be considered as predicates which maps all the elements present in it to true and all the remaining elements in the domain to false.
Eg, wingset=$\{x|wing(x)\}$

1.2 Binary/unary operators for set operations

Let S and T be sets and inS(.) and inT(.) be their corresponding predicates. Then

- $in\bar{S}(x) \equiv\sim inS(x)$
- $inS \cup T(x) \equiv inS(x) \vee inT(x)$
- $inS \cap T(x) \equiv inS(x) \wedge inT(x)$
- $inS - T(x) \equiv inS(x) \nrightarrow inT(x)$
- $inS\Delta T(x) \equiv inS(x) \oplus inT(x)$

1.3 Set inclusion

- $S \subseteq T \equiv inS(x) \rightarrow inT(x)$
- If $S \subseteq T$ and $T \subseteq R$, then $S \subseteq R$
- $S \subseteq T \equiv \bar{T}(x) \subseteq \bar{S}(x)$

General template to prove S=T: Prove that $S \subseteq T$ and $T \subseteq S$
Inclusion-Exclusion principle: $|S \cup T| = |S| + |T| - |S \cap T|$
where $|X|$ is the number of elements in set X.

1.4 Cartesian Product

Let S and T be sets.
$S \times T = \{(s,t)|s \in S; t \in T\}$
$|S \times T| = |S| \cdot |T|$ Properties:

- $(A \cup B) \times C = (A \times C) \cup (B \times C)$
- $\overline{S \times T} = (\bar{S} \times T) \cup (S \times \bar{T}) \cup (\bar{S} \times \bar{T})$

2 Relation

A relation can be defined as a predicate over $S \times S$.
(Note: We are considering binary homogeneous relations)

Ways of representation of relations:

1. **Set:** $\{(r,s)|r \sqsubset s\}$
2. **Boolean Matrix:** $M_{r,s} = True/1$ iff $r \sqsubset s$
3. **Directed graphs:** Edge directed from node r to node s iff $r \sqsubset s$

Note: $r \sqsubset s$ is same as r is related to s.

Since relation is a set, all the set operations can be extended to relation. Other operations can also be defined, like:

- Transpose: $R^T = (x,y)|(y,x) \in R$
- Composition: $R \circ R' = (x,y)|\exists w[(x,w) \in R \wedge (w,y) \in R']$

Composition can be considered as matrix multiplication. $(M \circ M')_{x,y} = \vee_w (M_{x,w} \wedge M'_{w,y})$

2.1 Types of relations

2.1.1 Reflexive and Irreflexive relation

A relation R, defined on set S, is said to be reflexive iff $\forall x \in S\ (x,x) \in R$.
In terms of boolean matrix, all diagonal entries should be true.
In terms of directed graphs, each node should have a self-loop.

A relation R, defined on set S, is said to be **ir**reflexive iff $\forall x \in S\ (x,x) \notin R$.
In terms of boolean matrix, all diagonal entries should be false.
In terms of directed graphs, no node should have a self-loop.

2.1.2 Symmetric and anti-symmetric relations

A relation R, defined on set S, is said to be symmetric iff $(x,y) \in R \implies (y,x) \in R$.
In terms of boolean matrix, the matrix is symmetric.
In terms of directed graphs, all edges are bidirectional.

A relation R, defined on set S, is said to be anti-symmetric iff $(x,y) \in R \wedge x \neq y \implies (y,x) \notin R$.
In terms of directed graphs, none of the edges are bidirectional.

2.1.3 Transitive relation

A relation R, defined on set S, is said to be transitive relation, iff $(x, y) \in R \wedge (y, z) \in R \implies (x, z) \in R$.
Equivalently, R is transitive iff $R \circ R \subseteq R \iff R^k \subseteq R \forall k > 1$. R^k is k times composition of R.
In terms of directed graphs, if there is a path from a to z, there is an edge (a,z).

A relation R, defined on set S, is said to be intransitive relation, iff $(x, y) \in R \wedge (y, z) \in R \implies (x, z) \notin R$.
A complete relation is reflexive, symmetric and transitive.
Various closures on R:

1. Reflexive closure on R: R' is minimal relation such that $R \subseteq R' \wedge R'$ is reflexive
2. Symmetric closure on R: R' is minimal relation such that $R \subseteq R' \wedge R'$ is symmetric
3. Transitive closure on R: R' is minimal relation such that $R \subseteq R' \wedge R'$ is transitive

Note: Minimal relation means, removing any edge violates subset condition or relation condition.
Each of these closures are unique for a given relation R.

2.1.4 Equivalence relation

A relation is called equivalence iff it is reflexive, symmetric and transitive.
Equivalence class(Eq(.)): $Eq(x) = \{y | x \sim y\}$
Every element is in its own equivalence class.(which means every element is present in atleast one equivalence class)
Claim: If $Eq(x) \cap Eq(y) \neq \phi$, then $Eq(x) = Eq(y)$
Proof:Let $z \in Eq(x) \cap Eq(y)$. Let $w \in Eq(x)$. Now, $x \sim z$ hence $z \sim x$. Also, $x \sim w$ and $w \sim x$.
Hence, $z \sim w$. And $y \sim w$.
Therefore, $w \in Eq(y) \implies Eq(x) \subseteq Eq(y)$.
Similarly, $Eq(y) \subseteq Eq(x)$.

Equivalence classes partition the domain.(The relation set).
This means that their union is the relation set, and intersection of any distinct pair of equivalence classes is unique.

3 Partially ordered sets

A relation that is reflexive, transitive and anti-symmetric is a partially ordered relations. Eg: $\leq$
A relation that is **ir**reflexive, transitive and anti-symmetric is a strictly partially ordered relations.
A relation that i transitive and anti-symmetric has no closed loops(acyclic).

A poset is a partial order relation defined over a non-empty set. It can be denoted as $(S, \leq)$.

3.1 Extremal and Extremum

3.1.1 Minimal and Maximal elements

$x \in S$ is minimal if $\nexists y$ such that $y \neq x$ and $y \leq x$.(all arrows except self-loops directed out)
Similarly, $x \in S$ is maximal if $\nexists y$ such that $y \neq x$ and $x \leq y$.(all arrows except self-loops directed in)
Minimal and maximal elements may not exists(eg, $S = \mathbb{Z}$) and if they exist, they may not be unique(eg, for $(\mathbb{Z}^+ - 1, |(divisibility))$ all prime numbers are minimal).

Claim: Every finite poset has atleast one minimal and one maximal element.
Proof: Induction on $|S|$
True for $|S| = 1$. Le it be true for $|S| = k$.
Then for $|S| = k + 1$, let S be parted into a k-element set and 1-element set(having element z).
Let x be a minimal in the prior set.
If $x \leq z$ or x and z are not related, then minimal of set S is x.
If $z \leq x$, the z is minimal of S using transitivity.
Similarly, for maximal.
(QED)

3.1.2 Greatest and least element

$x \in S$ is the greatest element if $\forall y \in S \ y \leq x$.
$x \in S$ is the least element if $\forall y \in S \ x \leq y$.
There may not exist least or greatest elements even for finite poset. However if they exist they are unique.

3.2 Reductions

- Reflexive reduction: $<$ is called reflexive reduction of $\leq$ if $\leq$ is reflexive closure of $<$ and $<$ is irreflexive. In other words, remove all self-loops.
- Transitive reduction:$\sqsubseteq$ is called transitive reduction of $\leq$, if $\leq$ is transitive closure of $\sqsubseteq$, and $\forall a, b \ (a \sqsubseteq b \implies \nexists m \text{ s.t.} m \notin \{a, b\} \ a \leq m \leq b)$

For finite posets, transitive reductions are well-defined, but may or may not exist for infinite posets.eg:(R,$\leq$)
Divisibility poset(on Z^+) has a well-defined transitive reduction even though it is infinite.

3.3 Hasse diagram

For a poset (S,$\leq$), the transitive reduction of its reflexive reduction(if they exists) has all information of the original poset(that is the poset can be reconstructed from the new relation).

3.4 Lower and upper bound

Let $T \subseteq S$. Define minimal, maximal, least and, greatest element on T.
Lower bound of T: $x \in S$ such that $x \leq y \ \forall y \in T$
Upper bound of T: $x \in S$ such that $y \leq x \ \forall y \in T$

Least upper bound for T: Least in $\{x | x$ is u.b. of T$\}$
Greatest lower bound for T: Greatest in $\{x | x$ is l.b. of T$\}$

3.5 Total/Linear order

If in a poset, every pair of elements are comparable(that is there is an edge between all pairs), then the poset is totally ordered.
Such a poset can be represented in linear fashion with all possible right pointing arrows.
Finite total order posets have unique maximal and unique minimal element.

Order Extension:
A poset (s,$\sqsubseteq$) is an extension of poset (S,$\leq$), iff
$a \leq b \implies a \sqsubseteq b$
Any finite poset can be extended to total ordering.
For infinite posets, "order extension principle" is taken as an axiom.

4 Chains and anti-chains

For a poset defined by (S,$\leq$)

Chain: $C \in S$ is said to be a chain if $\forall a, b \in C$, either $a \leq b$ or $b \leq a$. That is, $(C, \leq)$ is a total order.

Anti-chain: $A \in S$ is said to be a chain if $\forall a, b \in A$, neither $a \leq b$ nor $b \leq a$ unless $a = b$.
Subset of chain is a chain. Similar result for anti-chain.

Any chain and anti-chain can have atmost one element common($|A \cap C| = 1$). Also, a singleton set is both chain and anti-chain.

4.1 Height in a poset

Definition: For any element $a \in S$, height(a)=size of maximum chain with a as maximum. Note that height(.)geq1.
Eg: For poset $(Z^+, |)$, if $m = p_1^{d1} \dots p_i^{di}$, then height(m)=$1 + \sum_{j=1}^{j=i} d_j$.
We can also define height of poset (S,$\leq$) as max{height(a)$|a \in S$}=max{$|C|; C$ is chain}.

4.2 Anti-chains from height

Let $A_h = \{a | height(a) = h\}$
Claim: A_h form anti-chains.
Proof: If any two elements are related then the height of one of them would be greater than h.
Claim: $max\{h | A_h \neq \phi\}$ = height of poset
Proof: Can be easily proved by definition of height of poset.
Note: In a finite poset since every element has a finite height, every element occurs in atleast A_h.

4.3 Mirsky's Theorem

Least number of chains required to partition a set S is the size of largest chain.
Proof: The anti-chains A_h make one such partition.
Now, consider the largest chain C. Any anti-chain cannot have more than one elements in common with C. Hence, atleast $|C|$ anti-chains are required to have elements of the C.

Problem Set 1

Released: August 21, 2021

1. **Contrapositive.** Show that $p \to q \equiv \neg q \to \neg p$.

   This illustrates the equivalence of the statements "If today is a Sunday then today is a holiday" and "If today is not a holiday, then today is not a Sunday." (Note that these statements are **not equivalent** to "If today is not a Sunday, then today is not a holiday," or, $\neg p \to \neg q$.)

   Solution: We have $\neg q \to \neg p \equiv \neg(\neg q) \vee \neg p \equiv q \vee \neg p \equiv p \to q$.

2. **Distributive Property.** To show the equivalences below, you can derive the truth table of the formulas on the LHS and RHS, and compare them. Alternately, for a quicker argument, you can consider two cases, $p \equiv T$ and $p \equiv F$.

   (a) Show that $p \wedge (q \vee r) \equiv (p \wedge q) \vee (p \wedge r)$.

   (b) Show that $p \vee (q \wedge r) \equiv (p \vee q) \wedge (p \vee r)$.

   (c) What is the condition on a binary operator $\star$ so that $\wedge$ distributes over $\star$ (i.e., $p \wedge (q \star r) \equiv (p \wedge q) \star (p \wedge r)$)? What is the condition for $\vee$ to distribute over $\star$?

   Solution: Restricted to $p \equiv T$, irrespective of what $\star$ is, we have $p \wedge (q \star r) \equiv q \star r \equiv (p \wedge q) \star (p \wedge r)$. However, for $p \equiv F$, we have $p \wedge (q \star r) \equiv F$, but $(p \wedge q) \star (p \wedge r) \equiv F \star F$. So, $\wedge$ distributes over $\star$ iff $F \star F \equiv F$.
   Similarly, $\vee$ distributes over $\star$ iff $T \star T \equiv T$.

   (d) Does $\wedge$ distribute over $\oplus$? Does $\vee$ distribute over $\oplus$?

   Solution: By the conditions above, $\wedge$ distributes over $\oplus$, but $\vee$ does not.

3. **Simplifying formulas.**

   Every formula in two variables is equivalent to a binary operator. Identify the operator in the following cases, and write down an equivalent expression.

   (Thus your answer should be one of the 16 possibilities: T, F, p, q, $\neg p$, $\neg q$, $p \oplus q$, $p \leftrightarrow q$, $p \wedge q$, $p \vee q$, $p \uparrow q$, $p \downarrow q$, $p \to q$, $q \to p$, $p \not\to q$ and $q \not\to p$.)

   You could prepare a truth table for each formula to help with the task. You could also employ the distributive property, De Morgan's law and other equivalences from the lecture.

   (a) $p \wedge \neg q$
   Solution: $p \wedge \neg q$ evaluates to T exactly when $p \equiv T$ and $q \equiv F$. This corresponds to the truth table of $p \not\to q$. (Alternately, note that $p \not\to q \equiv \neg(p \to q) \equiv \neg(\neg p \vee q) \equiv p \wedge \neg q$.)

   (b) $(p \to q) \wedge \neg q$
   Solution: $\neg(p \vee q) \equiv p \downarrow q$.

   (c) $p \vee \neg(q \to p)$
   Solution: $p \vee q$.

   (d) $(p \wedge q) \to q$
   Solution: T.

   (e) $(p \wedge q) \leftrightarrow q$
   Solution: $q \to p$.

   (f) $(p \leftrightarrow q) \leftrightarrow ((p \wedge q) \vee (\neg p \wedge \neg q))$
   Solution: T.

4. **Functional Completeness.** A set of operators is *functionally complete* if all n-ary logical operations, for any $n > 0$, can be expressed as formulas that use only operators from this set. In other words, all possible truth tables *over any number of inputs* can be produced by formulas that use only these operators.

   Show that the set $\{\neg, \wedge, \vee\}$ is functionally complete.

   [*Hint: First consider an n-ary operation which has a single row in its truth table evaluating to T. Can you design an equivalent formula with just $\neg$s and $\wedge$s? Next, if an operation's truth table has k rows that evaluate to T, can you design a formula with k terms of the above kind, combined using $\vee$s?*]

Solution: Consider an arbitrary n-ary logical operation f, for an arbitrary integer $n > 0$. We shall construct a formula for $f(X_1, \ldots, X_n)$.

Let N denote the number of rows in the truth table of f which evaluate to T. Let the i^{th} such row be indexed by a vector $(\alpha_{i,1}, \ldots, \alpha_{i,n}) \in \{T, F\}^n$, such that $f(\alpha_{i,1}, \ldots, \alpha_{i,n}) = T$. Then, for any vector $(x_1, \ldots, x_n) \in \{T, F\}^n$, we have that $f(x_1, \ldots, x_n) = T$ iff $(x_1, \ldots, x_n) \in \{(\alpha_{1,1}, \ldots, \alpha_{1,n}), \ldots, (\alpha_{N,1}, \ldots, \alpha_{N,n})\}$. Now, we construct a formula for f. For each $i \in \{1, \ldots, N\}$, define:

$$G_i(X_1, \ldots, X_n) \equiv (X_1 \leftrightarrow \alpha_{i,1}) \wedge \cdots \wedge (X_n \leftrightarrow \alpha_{i,N})).$$

Note that $G_i(x_1, \ldots, x_n) = T$ if and only if $(x_1, \ldots, x_n) = (\alpha_{i,1}, \ldots, \alpha_{i,n})$. Now let

$$F(X_1, \ldots, X_n) \equiv G_1(X_1, \ldots, X_n) \vee \cdots \vee G_N(X_1, \ldots, X_n).$$

We note that $F(x_1, \ldots, x_n) = T$ iff $(x_1, \ldots, x_n) \in \{(\alpha_{1,1}, \ldots, \alpha_{1,n}), \ldots, (\alpha_{N,1}, \ldots, \alpha_{N,n})\}$. Also, as noted above $f(x_1, \ldots, x_n) = T$ iff $(x_1, \ldots, x_n)$ belongs to the same set. Thus $f(X_1, \ldots, X_n) \equiv F(X_1, \ldots, X_n)$

As defined above, F appears to use the operators $\wedge, \vee$ and $\leftrightarrow$. However, the last one is used only in the form $X_j \leftrightarrow \alpha_{i,j}$ where $\alpha_{i,j}$ is specified. If $\alpha_{i,j} \equiv T$, we write $X_j \leftrightarrow \alpha_{i,j}$ as X_j and if $\alpha_{i,j} \equiv F$, we write $X_j \leftrightarrow \alpha_{i,j}$ as $\neg X_j$. Now, F uses only the operators $\wedge$, $\vee$ and $\neg$. Since f could be any n-ary operator for any $n > 0$, we conclude that the set $\{\wedge, \vee, \neg\}$ is functionally complete.

5. **A Tautology.** Prove that $\exists x \forall y\ P(x) \rightarrow P(y)$ is true no matter what the predicate P is (assuming that the domain is non-empty).

   [Hint: consider two cases, depending on whether $\forall y\ P(y)$ is true or false.]

   Solution: There are two possible cases
   Case 1: $\forall y P(y)$ is true.

   - Since the domain is non-empty, there exists at least one element in the domain, let's say w.
   - Note that $P(w) \rightarrow P(y)$ for every y since $P(y)$ is true for all y.
   - Hence, $(\forall y P(w) \rightarrow P(y))$ is true.
   - From this we can conclude that $\exists x \forall y P(x) \rightarrow P(y)$ is true.

   Case 2:

   - $\forall y P(y)$ is false which means $\exists y \neg P(y)$ is true. So, let a be an element such that $\neg P(a)$ is true. Then $P(a)$ is false.
   - Since $P(a)$ is false, $P(a) \rightarrow P(y)$ is true for any y. That is, $\forall y,\ P(a) \rightarrow P(y)$ is true.
   - Since, $\forall y,\ P(a) \rightarrow P(y)$ is true, $\exists x \forall y,\ P(x) \rightarrow P(y)$ is true (by considering x to be a).

6. **Pointless Games.** Suppose a game has the following structure: Alice specifies an integer a, then Bob specifies an integer b, and finally Alice specifies an integer c. Alice wins the game if $g(a, b, c) = 0$, where g is a function associated with the game; if $g(a, b, c) \neq 0$ Bob wins.

   Alice is said to have a *winning strategy* if there is some way for her to play the game (i.e., pick a and c) to ensure that she will win no matter how Bob plays (i.e., picks b). Note that Alice can pick c *after seeing* Bob's number b.

   (a) Suppose $g(a, b, c) = a + b + c$. Specify a winning strategy for Alice.
   Solution: Alice chooses $a = 0$ and $b = -c$.

   (b) Suppose $g(a, b, c) = \max\{a + b, b + c\}$. Specify a winning strategy for Bob.
   Solution: Bob chooses $b = 1 - a$.

   (c) Express the proposition that Alice has a winning strategy in the language of first-order predicate calculus.
   Solution: $\exists a \in \mathbb{Z}\ \forall b \in \mathbb{Z}\ \exists c \in \mathbb{Z}\ g(a + b + c) = 0$.

   (d) Express the proposition that Bob has a winning strategy.
   Solution: $\forall a \in \mathbb{Z}\ \exists b \in \mathbb{Z}\ \forall c \in \mathbb{Z}\ g(a + b + c) \neq 0$.

   (e) Argue that, irrespective of what function g is used, this is a "pointless game": either Alice or Bob has a winning strategy.
   Solution: The condition that Bob has a winning strategy is the negation of the condition that Alice has a winning strategy. So, if Alice does not have a winning strategy, the Bob has one.

Problem Set 2

Released: August 21, 2021

1. Prove that $((p \to r) \wedge (r \to q)) \to (p \to q)$, by three methods:

   (a) First, prove it by expanding this expression using distributive properties and conclude that it is equivalent to True.

   (b) Secondly, prove it by analysing two cases based on the truth value of r.

   (c) Finally, prove it by analysing 8 cases based on the truth values of p, q, r.

   Solution: (a) Firstly, note that

$$\alpha \to (\beta \to \gamma) \equiv \neg\alpha \vee \neg\beta \vee \gamma \equiv (\alpha \wedge \beta) \to \gamma$$

   Hence,

$$\begin{aligned}
((p \to r) \wedge (r \to q)) \to (p \to q) &\equiv ((p \to r) \wedge (r \to q) \wedge p) \to q \\
&\equiv ((p \wedge r) \wedge (r \to q)) \to q && \text{since } (p \to r) \wedge p \equiv p \wedge r \\
&\equiv (p \wedge r \wedge q) \to q && \text{since } r \wedge (r \to q) \equiv r \wedge q \\
&\equiv T && \text{since } (\alpha \wedge q) \to q \equiv \neg\alpha \vee \neg q \vee q \equiv T
\end{aligned}$$

   Hence proved.

   (b) We now prove that the formula evaluates to tautology based on case study of truth value of r. We use the following, for any proposition p, we have,

$$\begin{aligned}
p \to T &\equiv T \\
T \to p &\equiv p \\
p \to F &\equiv \neg p \\
F \to p &\equiv T
\end{aligned}$$

   Each of the above equality follows from properties of implication.

   Case 1: $r = T$.

   In this case, the formula evaluates as,

$$\begin{aligned}
((p \to r) \wedge (r \to q)) \to (p \to q) &\equiv ((p \to T) \wedge (T \to q)) \to (p \to q) \\
&\equiv (T \wedge q) \to (p \to q) \\
&\equiv q \to (p \to q) \\
&\equiv \neg q \vee (p \to q) \\
&\equiv \neg q \vee (\neg p \vee q) \\
&\equiv (\neg q \vee q) \vee p \\
&\equiv T
\end{aligned}$$

   Therefore, the formula evaluates to tautology in this case.

   Case 2: $r = F$.

   In this case, the formula evaluates as,

$$\begin{aligned}
((p \to r) \wedge (r \to q)) \to (p \to q) &\equiv ((p \to F) \wedge (F \to q)) \to (p \to q) \\
&\equiv (\neg p \wedge T) \to (p \to q) \\
&\equiv \neg p \to (p \to q) \\
&\equiv \neg(\neg p) \vee (p \to q) \\
&\equiv p \vee (\neg p \vee q) \\
&\equiv (p \vee \neg p) \vee q \\
&\equiv T
\end{aligned}$$

Therefore, the formula also evaluates to tautology in this case. Since the above two cases cover all possibilities for truth values assignments of the propositions p, q, r, we have that the formula evaluates to tautology. Hence, proved.

(c) The formula needs to be evaluated for each of the 8 possible assignments to the propositions p, q, r. We see that it turns out to be true in each case.

p	q	r	$\alpha := p \to r$	$\beta := r \to q$	$\gamma := p \to q$	$\delta := \alpha \wedge \beta$	$\delta \to \gamma$
T	T	T	T	T	T	T	T
T	T	F	F	T	T	T	T
T	F	T	T	F	F	F	T
T	F	F	F	T	F	F	T
F	T	T	T	T	T	T	T
F	T	F	T	T	T	T	T
F	F	T	T	F	T	F	T
F	F	F	T	T	T	T	T

2. **Contrapositive.** Prove each of the following by stating and proving its contrapositive.

   (a) If x and y are real numbers such that the product xy is an irrational number, then either x or y must be an irrational number.

   Solution: Given that the domain we are working in is the set of real number, let p be the statement "xy is an irrational number" and let q be the statement "either x or y is an irrational number". We want to show that $p \to q$. The contrapositive of this statement is $\neg q \to \neg p$, that is, "If neither x nor y is an irrational number, then xy is not an irrational number". This can be further simplified to "If x and y are rational numbers, then xy is a rational number".
   Proving this is an easy job; suppose x and y are rationals, say $x = \frac{p}{q}$ and $y = \frac{r}{s}$ where p, q, r, s are integers, and q, s are non-zero. Then $xy = \frac{pr}{qs} = \frac{m}{n}$, where $m = pr$ and $n = qs$ are integers and n is non-zero. Therefore xy is rational too.

   (b) If x and y are two integers whose product is odd, then both must be odd.

   Solution: The domain we are working in is the set of integers. Let p be the statement "xy is odd" and let q be the statement "x and y are both odd". To show $p \to q$, we state and prove its contrapositive as we did before. The contrapositive is $\neg q \to \neg p$, that is, "If either x or y is not odd, then xy is not odd". Since an integer that is not odd is necessarily even, this can be written equivalently as "If either x or y is even, then xy is even".
   Now we prove this reformulation. Suppose one of x or y is even, say x is even (without loss of generality). Then $x = 2k$ for some integer k. Then, $xy = 2ky = 2m$, where $m = ky$ is an integer. This means xy is even, as required.

   (c) If n is a positive integer such that n leaves a remainder of 2 when divided by 3, then n is not a perfect square.

   Solution: The domain we are working in is the set of natural numbers. Let p be the statement "n leaves a remainder of 2 when divided by 3", and let q be the statement "n is not a perfect square". Again, we need to show $p \to q$, and the contrapositive $\neg q \to \neg p$ can be written as "If n is a perfect square, then n does **not** leave a remainder of 2 when divided by 3".
   Let us try to prove this statement. Suppose $n = m^2$ for some positive integer m. We take cases on the remainder when m is divided by 3. Suppose m leaves a remainder of 0 when divided by 3, that is, suppose $m = 3k$ for some integer k. Then, $n = (3k)^2 = 3(3k^2)$, so n divided by 3 leaves a remainder 0. Instead, suppose m leaves a remainder of 1 when divided by 3, that is, $m = 3k + 1$ for some integer k. Then, $n = (3k + 1)^2 = 3(3k^2 + 2k) + 1$, so n leaves remainder 1 when divided by 3. Finally, suppose m leaves a remainder of 2 when divided by 3, that is, $m = 3k + 2$ for some integer k. Then, $n = (3k + 2)^2 = 3(3k^2 + 4k + 1) + 1$, so n leaves remainder 1 when divided by 3.
   In either of the three cases, n does not leave remainder 2 when divided by 3, so we are done.

   (d) If n is a positive integer such that n leaves a remainder of 2 or 3 on division by 4, then n is not a perfect square.

   Solution: The domain we are working in is the set of positive integers. Let p be the statement "n leaves a remainder of 2 or 3 when divided by 4", and let q be the statement "n is not a perfect square". Again, we need to show $p \to q$, and the contrapositive $\neg q \to \neg p$ can be written as "If n is a perfect square, then n does not leave remainder 2 or 3 on division by 4".
   This can be proved in a similar fashion as the previous problem; let $n = m^2$ for some positive integer m, and take cases modulo 4 for m. However, we can reduce case-work by taking cases modulo 2 instead.
   Suppose m leaves remainder 0 when divided by 2. Then $m = 2k$ for some integer k. This means $n = 4k^2$, so n leaves remainder 0 when divided by 4. Instead, suppose m leaves remainder 1 when divided by 2, that is, $m = 2k + 1$ for some integer k. This means $n = (2k + 1)^2 = 4(k^2 + k) + 1$, so n leaves remainder 1 when divided by 4.
   In either case, n does not leave remainder 2 or 3 upon division by 4, so we are done.

3. **Proof by Contradiction.**

(a) There are no positive integer solutions to the equation $x^2 - y^2 = 10$. (Such a problem, when an integral solution is sought for a polynomial equation, the equations is called a *Diophantine equation*.)

Solution: Suppose, for the sake of contradiction, that there is an integer solution (x, y) such that $x^2 - y^2 = 10$. Then, we have $(x+y)(x-y) = 10$. Note that $x-y$ and $x+y$ are both even or both odd (because, $x-y = (x+y)-2y$). If both are odd, their product is odd; if both are even then their product is a multiple of 4. Hence, in both cases, their product cannot be 10, which is a contradiction.

(b) There is no rational solution to the equation $x^5 + x^4 + x^3 + x^2 + 1 = 0$.

[Hint: A rational number can be written as $\frac{p}{q}$ where p, q are integers which have no common factors.]

Solution: Suppose, for the sake of contradiction, that there is a rational solution, $x = \frac{p}{q}$, for integers p, q, which have no common factors. Then,

$$p^5 + p^4q + p^3q^2 + p^2q^3 + q^5 = 0.$$

At least one of p, q is odd (since they have no common factors). We consider 3 cases: both p, q are odd, only p is odd, and only q is odd. In the first case, all 5 terms on the LHS are odd, and hence their sum should be odd, and hence cannot be 0. In the second and third cases, exactly one term on the LHS (p^5 or q^5) is odd, and hence the sum is again odd, and cannot be 0.

(c) We say that a point $P = (x, y)$ in the Cartesian plane is rational if both x and y are rational. More precisely, P is rational if $P = (x, y) \in \mathbb{Q}^2$. An equation $F(x, y) = 0$ is said to have a rational point if there exists $x_0, y_0 \in \mathbb{Q}$ such that $F(x_0, y_0) = 0$. For example, the equation $x^2 + y^2 - 1 = 0$ has rational points $(0, \pm 1)$ and $(\pm 1, 0)$. Show that the equation $x^2 + y^2 - 3 = 0$ has no rational points.

[Hint: Prove by contradiction. It would be useful to consider whether the largest power of 3 that divides an integer is even or odd. Also, it will be useful to know what values can appear as the remainder of a perfect square when divided by 3.]

Solution: Suppose, for the sake of contradiction, that there is a rational solution $(x, y) = (\frac{p_1}{q_1}, \frac{p_2}{q_2})$ such that $x^2 + y^2 = 3$. Then, $p_1^2q_2^2 + p_2^2q_1^2 = 3(q_1^2q_2^2)$. The largest power of 3 that divides the RHS is odd. Suppose the largest power of 3 that divides p_1q_2 and p_2q_1 be a and b respectively. We analyze three cases based on a, b and derive a contradiction in each case.

Case 1, $a = b$: In this case the LHS is of the form $3^{2a}(c^2 + d^2)$, where c, d are not multiples of 3. Then c^2, d^2 leave a remainder of 1 when divided by 3 (because $(3n \pm 1)^2 = 3(3n^2 \pm 2n) + 1$), and hence $c^2 + d^2$ is not a multiple

Case 2, $a > b$: In this case the LHS is of the form $3^{2b}(c^2 + d^2)$ where c a multiple of 3 but d is not. Then $c^2 + d^2$ leaves a remainder of 1 when divided by 3. Hence, the largest power of 3 that divides the LHS is $2b$, which is even.

Case 3, $b > a$: This is analogous to the above case, and the largest power of 3 that divides the LHS is $2a$, which is even.

(d) Use (c) to show that $\sqrt{3}$ is irrational.

4. **Weak Induction**. Prove by induction that the following hold for every positive integer n:

(a) $1^2 - 2^2 + 3^2 - \cdots + (-1)^{n-1}n^2 = (-1)^{n-1}\dfrac{n(n+1)}{2}$.

Solution: Base Case :

$$1^2 = (-1)^0\frac{1(2)}{2}$$
$$1 = 1$$

Induction Step : Assume that $1^2 - 2^2 + 3^2 - \ldots + (-1)^{n-1}n^2 = (-1)^{n-1}\dfrac{n(n+1)}{2}$ for some $n > 1$.

$$\begin{aligned}
1^2 - 2^2 + 3^2 - \ldots + (-1)^n(n+1)^2 &= \left((-1)^{n-1}\frac{n(n+1)}{2}\right) + \left((-1)^n(n+1)^2\right) \\
&= (-1)^{n-1}(n+1)\left[\frac{n}{2} - (n+1)\right] \\
&= (-1)^{n-1}(n+1)\left[\frac{n-2n-2}{2}\right] \qquad (1) \\
&= (-1)^{n-1}(n+1)\left[\frac{(-1)(n+2)}{2}\right] \\
&= (-1)^n\frac{(n+1)(n+2)}{2}
\end{aligned}$$

(b) if $h > -1$, then $1 + nh \leq (1+h)^n$.

Solution:

Base case : $1 + 0 \leq (1+h)^0$

Induction Step : Assume that

$$1 + nh \leq (1+h)^n$$

for some $n > 1$. Then,

$$1 + (n+1)h = 1 + nh + h \leq (1+h)^n + h$$

To complete the proof, it suffices to show that

$$h \leq h(1+h)^n$$

. Consider 2 cases :

i. $-1 < h < 0$: It follows that

$$0 < 1 + h < 1$$

Hence

$$0 < (1+h)^n < 1$$

for $n \geq 1$. Thus, $h(1+h)^n$ will be a negative number with a smaller magnitude than h.

ii. $h \geq 0$: This means that $1 + h \geq 1$ and hence

$$h \leq h(1+h)^n$$

for $n \geq 1$.

(c) 12 divides $n^4 - n^2$.

Solution: Let $D(n) = n^4 - n^2$ and $P(n)$ denote the predicate which evaluates to true when 12 divides $D(n)$.

Base Case : $D(1) = 0$ implies $P(1)$ holds trivially.

Induction Step : Assume that $P(k)$ holds for some integer $k \geq 1$. We shall prove that $P(k+1)$ also holds. For $P(k)$ to hold, it must be the case that $D(k)$ is divisible by both 3 and 4. Note that $D(k) = k^2(k^2-1)$, a product of two consecutive integers. Two consecutive integers are always co-prime i.e. they have no common factors. Hence, there are 4 possibilities :

i. k^2 is divisible by both 3 and 4. It follows that k is divisible by both 3 and 2. Hence, both k and $k+2$ are even. Note that $D(k+1) = k(k+1)^2(k+2)$. Therefore, $D(k+1)$ is divisible by 3 (via k) and also divisible by 4 (via k and $k+2$).

ii. $k^2 - 1$ is divisible by both 3 and 4. Since $k^2 - 1 = (k-1)(k+1)$, it follows that both $k-1$ and $k+1$ are even. Also, either $k-1$ (and hence $k+2$) or $k+1$ are divisible by 3. Combining the above results, it can be claimed that $P(k+1)$ holds.

iii. k^2 is divisible by 3 and $k^2 - 1$ is divisible by 4. It follows that both $k-1$ and $k+1$ are even. Note that $D(k+1)$ is divisible by 4 because $k+1$ is even. For k^2 to be divisible by 3, k must also be divisible by 3 (as 3 is a prime number). Hence, $P(k+1)$ holds.

iv. k^2 is divisible by 4 and $k^2 - 1$ is divisible by 3. Either $k-1$ or $k+1$ should be divisible by 3. It follows that either $k+2$ or $k+1$ is divisible by 3. When k^2 is divisible by 4, both k and $k+2$ are even. Hence, $P(k+1)$ holds.

Here is a proof which does not use induction. A quantity is divisible by 12 if it has a factor of 4 and a factor of 3. Note that $n^4 - n^2 = n^2(n^2-1) = n^2(n-1)(n+1)$. If n is even, then n^2 has a factor of 4. If n is odd, then both $n-1$ and $n+1$ are even, and hence $(n-1)(n+1)$ has a factor of 4. In either case $4|(n^4 - n^2)$. Also, among $n-1, n, n+1$, one of them is a multiple of 3. Hence $3|n(n-1)(n+1)$, and hence $3|(n^4 - n^2)$. Hence $12|(n^4 - n^2)$.

5. **Strong induction.** An $a \times b$ chocolate bar is a rectangular piece of chocolate consisting of ab square pieces of chocolate. Your job is to break this chocolate into the ab individual square pieces. At any point during this task, you will have one or more pieces of the chocolate bar; you can pick any piece and break it into two, along a vertical or horizontal line separating the square pieces. For instance, if you start with a 2×2 bar, you can first break it vertically to get two 2×1 bars; then each of them you can break once horizontally, to end up with all 4 individual squares. In this process you made 3 breaks in all (one vertical, two horizontal).

   Show that to completely break an $a \times b$ bar into individual squares, you need exactly $ab - 1$ breaks, no matter which breaks you make.

[Hint: Induct on the number of squares. A single break splits a piece of chocolate into two smaller pieces with the same total number of squares.]

Solution:

Base Case: Consider $n = 1$. If we have 1 chocolate square, number of breaks = 0

Induction Step: For some $k \geq 1$, assume that claim is true for all chocolate bars with $n \leq k$ squares: that is, no matter what sequence of breaks are made, any such chocolate bar needs exactly $k - 1$ breaks. We need to show that claim is true for all chocolate bars with $n = k + 1$ squares.

Consider an arbitrary chocolate bar with $k + 1$ squares. Consider any sequence of breaks that break it into individual squares. The first break breaks the bar into two pieces of n_1 and n_2 squares for some integers $n_1, n_2 > 0$ such that $n_1 + n_2 = k + 1$. Thus $n_1 \leq k$ and $n_2 \leq k$.

Now, the sequence of breaks we are considering must break these two pieces into individual squares. Further, any break affects (pieces obtained from) only one of these two pieces. Thus the subsequent breaks can be partitioned into two sequences, one which breaks the n_1-square piece completely, and one which breaks the n_2-square piece completely. By the induction hypothesis, the first sequence has exactly $n_1 - 1$ breaks and the second sequence has exactly $n_2 - 1$ breaks.

So the total number of breaks in the original sequence (including the first break) is $1+(n_1-1)+(n_2-1) = n_1+n_2-1 = k$.

Thus we have shown that for any chocolate bar with $k + 1$ squares, any sequence of breaks that break it into individual bars must have exactly k breaks. This completes the induction step.

6. **Well Ordering Principle.** Prove the Well-Ordering Principle – that every non-empty subset of $\mathbb{Z}^+$ has a minimum element – using mathematical induction.

   [Hint: Use *strong induction* to prove the contrapositive of the above statement, i.e. if a subset of $\mathbb{Z}^+$ does not have a least element, then it must be empty.]

   Solution:

   We need to show that if a subset S of $\mathbb{Z}^+$ does not have a minimum element, then it must be empty. In other words, we need to prove that $P(k)$ holds for all $k \in \mathbb{Z}^+$, where the predicate P is defined by $P(k) \leftrightarrow k \notin S$.

   Base Case: $P(1)$ holds because if $1 \in S$ then 1 will be the minimum element of the set S, as $n \geq 1$ for all $n \in \mathbb{Z}^+$. Since $S \subseteq \mathbb{Z}^+$, this implies that $n \geq 1$ for all $n \in S$.

   Induction Step: Assume that $P(m)$ holds for all $1 \leq m \leq k$ for some integer $k \geq 1$. We shall now prove that $P(k + 1)$ also holds.

   For the sake of contradiction, assume that $P(k+1)$ does not hold, implying that $k+1 \in S$. By the inductive hypothesis, all positive integers $1 \leq m \leq k$ satisfy that $m \notin S$. Since the set S only consists of positive integers, it follows that $n \geq k + 1$ for all $n \in S$. Combining this result with the induction hypothesis, we obtain that $k + 1$ is the least element of the set S, thus leading to contradiction.

7. Suppose that 9 bits – five ones and four zeros – are arranged around a circle in some order. Between any two equal bits you insert a 0 and between any two unequal bits you insert a 1 to produce nine new bits. Then you erase the nine original bits. Show that when you iterate this procedure, you can never get nine zeros. [Hint: Prove using the well ordering principle, or by mathematical induction.]

   Solution: We prove this using mathematical induction. Let Z_i denote the number of zeroes and O_i denote the number of ones respectively around the circle in the i^{th} configuration. We claim that $Z_i \geq 1$ and $O_i \geq 1 \ \ \forall i \geq 1$.

   (a) Base case : $Z_0 = 4$ and $O_0 = 5$.

   (b) Let's assume that $Z_i \geq 1$ and $O_i \geq 1$ for some $i > 1$. We need to prove that $Z_{i+1} \geq 1$ and $O_{i+1} \geq 1$.

      i. Let's assume that $O_{i+1} = 0$. This means that all the bits present in the $(i + 1)^{th}$ configuration are zeroes. The only way in which this is possible is if all the bits in the i^{th} iteration are equal. That leads to a contradiction since the i^{th} iteration has at least one zero and a one. So, $O_{i+1} \geq 1$.

      ii. Let's assume that $Z_{i+1} = 0$. This means all bits are ones in the $(i + 1)^{th}$ configuration. This is possible only when every possible pair of 2 consecutive bits in the i^{th} iteration are opposite (a zero and a one). Let's suppose we start traversing the circle in the clockwise direction with the bit one (this is possible because $O_i \geq 1$). Then it's neighbour must be a zero. The neighbour of this bit zero must be a one. Thus, all bits traversed in the odd turn are ones and those traversed in the even turns are zeroes. A total of 9 bits means that the 9^{th} bit must be a one which will also be the neighbour of the first one we traversed. This leads to a contradiction as we've found a pair of 2 consecutive equal bits. So, $Z_{i+1} \geq 1$.

8. Let $a_1, a_2, \ldots$. be a sequence of real numbers satisfying $a_{i+j} \leq a_i + a_j$ for all positive integers i and j. Use strong induction to prove :

$$a_n \leq a_1 + \frac{a_2}{2} + \frac{a_3}{3} + \ldots + \frac{a_n}{n}.$$

[Hint: You can write $a_n \leq a_i + a_{n-i}$ for $i = 1, \ldots, n-1$. You will want to use all $n-1$ of these inequalities. Use the strong inductive hypothesis to reason about a_i or a_{n-i}. It may help to work out examples for small values of n.]

Solution: For $n = 1$, the claim is $a_1 \leq a_1$, which is true. Now, for any arbitrary $k \geq 1$, suppose for all $1 \leq n \leq k$, it holds that $a_n \leq \sum_{j=1}^{n} \frac{a_j}{j}$. We shall prove that $a_{k+1} \leq \sum_{j=1}^{k+1} \frac{a_j}{j}$, or equivalently, $ka_{k+1} \leq \sum_{j=1}^{k} \frac{a_j}{j}$.

We know that $a_{k+1} \leq a_i + a_{k+1-i}$ for $i = 1, \ldots, k$. Summing up these inequalities we have, $ka_{k+1} \leq \sum_{i=1}^{k}(a_i + a_{k+1-i}) = 2\sum_{i=1}^{k} a_i$. Applying the strong induction hypothesis to each a_i we have

$$\begin{aligned}\sum_{1=1}^{k} a_i &\leq \sum_{i=1}^{k}\sum_{j=1}^{i} \frac{a_j}{j} = \sum_{j=1}^{k}\sum_{i=j}^{k} \frac{a_j}{j} \\ &= \sum_{j=1}^{k}(k+1-j)\frac{a_j}{j}.\end{aligned}$$

Adding to this $\sum_{1=1}^{k} a_i = \sum_{j=1}^{k} j\frac{a_j}{j}$, we get $2\sum_{i=1}^{k} a_i \leq \sum_{j=1}^{k}(k+1)\frac{a_j}{j}$. Hence, $ka_{k+1} \leq (k+1)\sum_{j=1}^{k} \frac{a_j}{j}$ as required.

9. There are n identical cars on a circular track, at arbitrary distances from each other. All of them together have just enough petrol required for one car to complete a lap. Show, using induction, that there is a car which can complete a lap by collecting petrol from the other cars on its way around.

[Hint: It will be helpful to prove a stronger statement, that there is a car which can complete a lap in the clockwise direction. Your proof in the induction step may have following steps:

- Consider an arbitrary configuration of $k+1$ cars (satisfying the given condition).
- First argue that there is a car who can reach its clockwise neighbouring car with the petrol it has. (Use proof by contradiction.)
- Use these two cars to change the given instance of the problem into an instance with k cars.
- Use the induction hypothesis to get some solution of the smaller instance; translate it into a solution for the original instance of the problem.]

Solution: We shall inductively prove that there is always a solution in which a car moves clockwise. As the base case, note that if $n = 1$ – i.e., there is a single car – we are guaranteed that it has enough petrol to cover a full lap.

Now, fix any $k \geq 1$, and suppose the claim holds for every k car configuration with the total petrol being sufficient to make a full lap. We shall use this assumption to show that the same holds for any $k+1$ car configuration.

Suppose we are given an arbitrary configuration with $k+1$ cars. Firstly, following the hint, if all cars had strictly less petrol than needed to cover the distance to their clockwise neighbour, then the total petrol across all cars is strictly less than what is needed for a full lap. Hence, at least one car, say A has sufficient petrol to reach its clockwise neighbour B. Now we derive a k car configuration as follows. We remove the car B, and give all the petrol it had to A. Since the total amount of petrol has not changed, we can invoke the induction hypothesis to get a solution for this configuration in which a car moves clockwise. We shall use the same solution for our $k+1$ car configuration.

Note that in this solution the car will have to reach A before reaching the position of B (because it cannot start at B, or strictly between A and B). Till it reaches A, the car has the same amount of petrol in the $k+1$ car configuration as in the k car configuration. When it reaches A, in the $k+1$ car configuration it collects less petrol than in the $k+1$ car configuration. However, since A stores enough petrol to reach B, the car will not run out of petrol before it reaches B. On reaching B its petrol level rises to the same level as in the k car configuration. Thus we obtain a solution with a car moving in the clockwise direction for the given $k+1$ car configuration, as desired.

Problem Set 3a

Released: August 27, 2021

1. How many zeros does the integer 100! end with (when written in decimal)?

   Solution: First, note that for any natural number n and any prime p, the highest power of p that divides $n!$ is

   $$\sum_{k=1}^{\infty} \left\lfloor \frac{n}{p^k} \right\rfloor$$

   (this is sometimes called Legendre's formula or de Polignac's formula). Note that even though this summation extends to infinity, all but finitely many terms of the summation will be non-zero.

   Now, the number of zeros at the end of 100! is equal to the highest power of 10 that divides it. But the highest power of 10 is equal to the smaller of the highest powers of 2 and 5 in 100!. Let us compute both of them:

   $$\begin{aligned} v_2(100!) &= \sum_{k=1}^{\infty} \left\lfloor \frac{100}{2^k} \right\rfloor \\ &= \left\lfloor \frac{100}{2} \right\rfloor + \left\lfloor \frac{100}{2^2} \right\rfloor + \cdots + \left\lfloor \frac{100}{2^6} \right\rfloor \\ &= 50 + 25 + 12 + 6 + 3 + 1 \\ &= 97 \\ v_5(100!) &= \sum_{k=1}^{\infty} \left\lfloor \frac{100}{5^k} \right\rfloor \\ &= \left\lfloor \frac{100}{5} \right\rfloor + \left\lfloor \frac{100}{5^2} \right\rfloor \\ &= 20 + 4 \\ &= 24 \end{aligned}$$

   Therefore the highest power of 10 in 100! is 24. So 100! ends with 24 zeros.

2. Prove or disprove that $n^2 - 79n + 1601$ is prime whenever n is a positive integer.

   Solution: The statement is FALSE. Take $n = 1601$. Then

   $$\begin{aligned} n^2 - 79n + 1601 &= 1601^2 - 79 \cdot 1601 + 1601 \\ &= 1601 \cdot (1601 - 79 + 1) = 1601 \cdot 1523 \end{aligned}$$

   In fact, it is true that for any non-constant polynomial $p(x)$ with integer coefficients, it is not possible for $p(n)$ to be prime for all natural numbers n (although it is possible for $p(n)$ to be prime for infinitely many natural numbers n; for example, take $p(n) = 4n + 3$).

3. Prove or disprove that for every two positive integers a, b, if an integer linear combination of a and b^2 equals 1, then so does an integer linear combination of a^2 and b.

   Solution: Since there is an integer linear combination of a and b^2 that equates to 1, so $\gcd(a, b^2) = 1$. In particular, a and b^2 have no common prime factor. But b^2 and b have the same set of prime factors, and a^2 and a also have the same set of prime factors. So this means a^2 and b also do not share any common prime factors. Therefore $\gcd(a^2, b) = 1$ as well, which implies there exists an integer linear combination of a^2 and b that equals 1.

   Alternately, one can compute such an integer linear combination explicitly. Suppose there exist integers x and y such that $ax + b^2y = 1$. Then squaring both sides, we get $(ax + b^2y)^2 = 1$. Expanding and grouping the terms appropriately, we get

   $$a^2x^2 + b(2abxy + b^3y^2) = 1.$$

   If $x^2 = x_0$ and $2abxy + b^3y^2 = y_0$, then x_0, y_0 are integers, and the above equation reads

   $$a^2x_0 + by_0 = 1,$$

   so there is an integer linear combination of a^2 and b which equates to 1.

4. Show that if $2^m + 1$ is an odd prime, then $m = 2^n$ for some non negative integer n.

Hint: If m is not a power of 2, then it has an odd factor $k > 1$. Can you factorize $2^{tk} + 1$? You can use the fact that for any integers a, b and positive integer k, it holds that $(a - b)|(a^k - b^k)$. You could prove this fact using strong induction by noting that $a^{k+1} - b^{k+1} = (a^k - b^k)(a + b) - (a^{k-1} - b^{k-1})ab$.

Solution: Consider the contrapositive of the given statement; we want to show that if m is not a non-negative power of 2, then $2^m + 1$ is not an odd prime.
If m is not a non-negative power of 2, it has an odd factor $k > 1$. Let $m = tk$ for some natural number t. Then $2^m + 1 = 2^{tk} + 1$. But, by the fact in the hint, using $a = 2^t$ and $b = -1$, we have that, for an odd k, $2^t + 1$ is a factor of $2^{tk} - (-1)^k = 2^{tk} + 1$. (This factorization is more explicitly given by $x^k + 1 = (x + 1)(x^{k-1} - x^{k-2} + \cdots - x + 1)$, with $x = 2^t$, and k odd, where the second factor has an alternating summation.) Also, $k > 1$ and $t \geq 1$, so $1 < 2^t + 1 < 2^m + 1$, so the factor is non-trivial. This means $2^m + 1$ is not a prime, which is what we wanted to show.

5. Recall the *Skippy Clock* from the lecture: It has numbers $0, 1, .., m - 1$ on its dial, and the needle, starting at 0, moves a steps at a time (i.e., hits numbers $0, a, 2a, \dots$). Show that needle will hit exactly all the multiples of $\gcd(a, m)$ that are on the dial.

Hint: You can use the fact that the "one-dimensional lattice" $L(a, m) \triangleq \{au + mv | u, v \in \mathbb{Z}\}$ consists of exactly all the multiples of $\gcd(a, m)$. However, note that in defining $L(a, m)$, u and v can be negative, whereas the clock's needle moves only clockwise.

Solution: Following the hint, it is enough to show that the set of numbers that the needle will hit are exactly all the numbers in $L(a, m) = \{au + mv | u, v \in \mathbb{Z}\}$ that are in the range $[0, m)$.

Now, the numbers hit by the needle are exactly the numbers in the range $[0, m)$ that are of the form $ax - qm$ for some non-negative integers x and q (x being the number of steps taken and q being the number of full laps of the clock completed by then). Thus every number hit is in $L(a, m)$.

Conversely, consider some number d on the dial that is in $L(a, m)$. That is, $d \in [0, m)$ and $d = au + mv$ for some $u, v \in \mathbb{Z}$. We consider two cases:

Case $u \geq 0$: In this case, after moving u times, the needle will be on a number t on the dial, of the form $au - qm$. Then $t \equiv d \pmod{m}$. But since each number on the dial (i.e., each of 0 to $m - 1$) has a different remainder w.r.t. m, it must be the case that $d = t$.

Case $u < 0$: Consider $u' = u - mu = u(1 - m)$. Note that $u' \geq 0$. Hence, after moving u' steps, the needle will be on a number $t = au' - qm = au - amu - qm = d - m(au + q + v)$, for some integer q. Since $t \equiv d \pmod{m}$, and t and d are both numbers on the dial, it must be the case that they are equal.

Thus in either case, the needle hits the number d. Since d was an arbitrary number on the dial that is in $L(a, m)$, we conclude that the needle hits all such numbers.

Thus, the needle hits exactly those numbers on the dial that are in $L(a, m)$.

6. Here is a game you can analyze with what you have learnt in class and always beat me. We start with two positive integers, a, b, written on a blackboard such that $a > b$ and $\gcd(a, b) = 1$. Now we take turns. I'll let you decide who goes first after seeing a, b. At each turn, the player must write a *new* positive integer on the board that is the difference of two numbers that are already there. If a player cannot play, then they lose.

For example, suppose $a = 5$, $b = 3$ and you choose to make the first move. Then your first move must be to play $5 - 3 = 2$. Then I can play $1 = 3 - 2$ (I cannot play $5 - 2 = 3$ as it is already on the board). You can play $5 - 1 = 4$. At this point I cannot make a move, and I lose.

(a) Show that the game must terminate, and when it terminates, every integer in the range $[1, a]$ is on the board.

Solution: Note that no number larger than a can ever be written on the board. (Otherwise, consider the first turn in which a number $x > a$ is written; then $x = y - z$ for two positive numbers already on the board, and hence $y \leq a$, yielding a contradiction as $x \leq y \leq a$.) Thus every turn before the game terminates writes a new integer in the range $[1, a]$; hence the game terminates after at most $a - 2$ turns (two numbers being already on the board).

To prove that all numbers in the range $[1, a]$ must appear on the board before the game terminates, we shall first prove that the number 1 should appear on the board.

Consider the Extended Euclidean algorithm to derive $\gcd(a, b) = 1$. It gives a decreasing sequence of positive numbers of the form $x_0 = a, x_1 = b, x_2 = \text{rem}(x_0, x_1), \dots, x_{i+1} = \text{rem}(x_{i-1}, x_i), \dots, x_n = 1$. Note that

$\text{rem}(x_{i-1}, x_i) = x_{i-1} - qx_i$ for some positive integer q; we shall insert integers $x_{i-1} - x_i, \ldots, x_{i-1} - (q-1)x_i$ between x_i and x_{i+1}. In the resulting decreasing sequence, $z_0 = a, z_1 = b, z_2 = a - b, \ldots, z_{n'} = 1$, every element z_j for $j > 1$ can be obtained as the difference of two previous elements.

Now, if the game terminates before 1 appears on the board, consider the first element z_j in the sequence that does not appear on the board. (There must be such an element since 1 is in the sequence.) Note that $j > 1$ since a, b have to be on the board. So, z_j can be expressed as the difference of two elements before it in the sequence. But since they are all on the board, the game cannot terminate at that point.

Thus when the game terminates, 1 must be on the board.

Now, suppose the game terminates before all integers in the range $[1, a]$ are on the board. Let w be the largest missing number. Note that $w \neq a$ (because a is on the board). Hence $w + 1$ is in the range $[1, a]$ and must be on the board. We also showed above that 1 must be on the board. But this contradicts the assumption that the game has terminated, since w can be written as $(w + 1) - 1$ as the next move. Hence, the game cannot terminate before all numbers in the range $[1, a]$ appear on the board.

(b) Describe a strategy that lets you win this game every time.

Solution: The game will terminate after exactly $a - 2$ moves. So, if a is odd, you shall choose to start the game, and if a is even, you let me start. In either case, you will make the last move, and I will lose the game.

7. A number is said to be *perfect* if it is equal to the sum of its positive divisors, other than itself. The smallest perfect number is 6 (with $6 = 1 + 2 + 3$, where 1, 2, 3 are its divisors, excluding itself). Around 300 B.C., Euclid proved that *if* $2^n - 1$ is a prime number[1] then $(2^n - 1)2^{n-1}$ is a perfect number. Can you prove this result of Euclid?

Solution: If p is a prime number, then by the fundamental theorem of arithmetic, the unique prime factorization of $m = p2^{n-1}$ consists of p and $n - 1$ powers of 2. Then, the positive divisors of m are exactly all the numbers of the form $p^a 2^b$, where a, b are integers, $0 \leq a \leq 1$ and $0 \leq b \leq n - 1$. Hence the sum of all the positive divisors of $m = p2^{n-1}$ (including itself)

$$\sum_{a=0}^{1} \sum_{b=0}^{n-1} p^a 2^b = \sum_{a=0}^{1} p^a (\sum_{b=0}^{n-1} 2^b) = \sum_{a=0}^{1} p^a (2^n - 1) = (2^n - 1)(1 + p)$$

For $p = 2^n - 1$, we have this evaluate to $(2^n - 1)2^n = 2(2^n - 1)2^{n-1} = 2m$. Hence the sum of all positive divisors of m excluding itself equals m, as required to prove.

8. Find all $m \in \mathbb{Z}^+$ such that, for all integers a, b, $a^2 \equiv b^2 \pmod{m}$ iff $a \equiv b \pmod{m}$.

Solution: By definition, $a \equiv b \pmod{m}$ implies that m divides $a - b$. Since $a^2 - b^2 = (a - b)(a + b)$, it follows that m also divides $a^2 - b^2$. Hence, implication in the backward direction follows.

For the forward direction to hold, it must be the case that for all integers a, b whenever m divides $a^2 - b^2$ it must also divide $a - b$. Let us consider the following cases for m :

(a) $m = 1$: The implication holds trivially as 1 divides every integer.

(b) $m = 2$: Assume that 2 divides $a^2 - b^2$. Note that the integers given by $a - b$ and $a + b$, for integer choices of a and b, have the same parity i.e., either both these integers are odd or both are even. To satisfy the hypothesis, it must be the case that $a - b$ is also even as product of two odd numbers cannot be even.

(c) $m > 2$: Consider $a = m - 1$ and $b = 1$. Check that m divides $a^2 - b^2$ but does not divide $a - b$.

We have shown that only for $m \in \{1, 2\}$ it holds that $a^2 \equiv b^2 \pmod{m}$ iff $a \equiv b \pmod{m}$ for all integers a, b.

9. Suppose $m \in \mathbb{Z}^+$. Show that every $a \in \mathbb{Z}_m$ has at most one multiplicative inverse in $\mathbb{Z}_m$.

Solution: Suppose $a, b, c \in \mathbb{Z}_m$ such that $ab \equiv 1 \pmod{m}$ and $ac \equiv 1 \pmod{m}$. Then we have $b \equiv (ab)b \equiv (ac)b \equiv (ab)c \equiv c \pmod{m}$. Hence all multiplicative inverses of a (if any) are equal to each other.

[1] Such a prime number is called a Mersenne prime. To date, only 51 such numbers are known, the largest of which was discovered in December 2018. The last 17 such discoveries were made by *The Great Internet Mersenne Prime Search* (GIMPS), a project that started in 1996.

10. Suppose $m \in \mathbb{Z}^+$ and $a, b \in \mathbb{Z}$. Show that there is an integer x such that $ax \equiv b \pmod{m}$ iff $\gcd(a, m)|b$. Describe an algorithm to find a solution when it exists. (You can use the algorithms covered in the lectures.)

Solution: In one direction, if $ax \equiv b \pmod{m}$, then $ax - b = mq$ for some integer q, and hence $b = ax - mq \in L(a, m)$. Since we have seen that every element in $L(a, m)$ is a multiple of $\gcd(a, m)$, so is b.

Conversely, suppose $\gcd(a, m)|b$. Let $d = \gcd(a, m)$. Consider $a' = a/d$, $m' = m/d$. Note that $\gcd(a', m') = 1$. Hence, modulo m', a' has a multiplicative inverse. Let $za' \equiv 1 \pmod{m'}$, where z can be computed using the Extended Euclidean Algorithm. Then $za' = 1 + qm'$ for some integer q, and hence $(b'z)a' = b' + b'qm'$, where $b' = b/d$ is an integer. Now, multiplying throughout by d, we have $(b'z)a = b + (b'q)m$. Thus $x = b'z$ is a solution for $ax \equiv b \pmod{m}$.

Problem Set 3b

Released: August 29, 2021

1. **Extended Euclidean Algorithm.** Consider the following recursive description of Euclid's GCD algorithm.

   [1] Euclid$a \in \mathbb{Z}^+, b \in \mathbb{Z}^+$ $a > b$ EUCLID(b, a) In the following, we assume $a \leq b$ $a|b$ a $(q, r) \leftarrow$ DIVIDE(b, a) DIVIDE(c, d) returns (q, r) such that $c = dq + r$, where $0 \leq r < |d|$ EUCLID(r, a)

   (a) Modify the above function to return a pair of integers (u, v) such that $au + bv = \gcd(a, b)$.

   Solution: The modified lines are shown in colour. [1] Euclid$a \in \mathbb{Z}^+, b \in \mathbb{Z}^+$ $a > b$ EUCLID(b, a) In the following, we assume $a \leq b$ $a|b$ $(1, 0)$ $\gcd(a, b) = a = a{\cdot}1 + b{\cdot}0$. $(q, r) \leftarrow$ DIVIDE(b, a) DIVIDE(c, d) returns (q, r) such that $c = dq + r$, where $0 \leq r < |d|$ $(u, v) \leftarrow$ EUCLID(r, a) $(v - qu, u)$ $\gcd(a, b) = \gcd(r, a) = ru + av = (b - aq)u + av = a(v - qu) + bu$

   (b) Compute the output of our modified function on the input pair $(1918, 2019)$.

   Hint: You can use a table with three columns for the input (a, b), the intermediate value (q, r) and the output (u, v), for each call to the function. You would fill the first two columns from top to bottom, and the last column in the reverse direction.

   Solution:

(a, b)	(q, r)	(u, v)
$(1918, 2019)$	$(1, 101)$	
$(101, 1918)$	$(18, 100)$	
$(100, 101)$	$(1, 1)$	
$(1, 100)$	base case	$(1, 0)$

   $\rightarrow$

(a, b)	(q, r)	(u, v)
$(1918, 2019)$	$(1, 101)$	$(-20, 19)$
$(101, 1918)$	$(18, 100)$	$(19, -1)$
$(100, 101)$	$(1, 1)$	$(-1, 1)$
$(1, 100)$	base case	$(1, 0)$

   The output is $(-20, 19)$.

2. Prove that $\phi(3n) = 2\phi(n)$ if and only if 3 does not divide n. (For this claim to hold for all $n \in \mathbb{Z}^+$, use the convention that $\phi(1) = 1$.)

   Solution: First, we show that if 3 does not divide n then $\phi(3n) = 2\phi(n)$. Since 3 and n are coprime, we can write

   $$\phi(3n) = \phi(3)\phi(n) = (3 - 1)\phi(n) = 2\phi(n)$$

   (This holds for all $n \in \mathbb{Z}^+$, where, by convention, $\phi(1) = 1$.)

   Now we prove the other side, i.e., if $\phi(3n) = 2\phi(n)$ then 3 does not divide n. Let's assume for the sake of contradiction that 3 divides n i.e. $n = 3^k l$ where $k, l \geq 1$ and 3 does not divide l. It follows that

   $$\phi(3n) = \phi(3^{k+1}l) = \phi(3^{k+1})\phi(l) = 2.3^k\phi(l)$$

   On the other hand,

   $$2\phi(n) = 2\phi(3^k l) = 2\phi(3^k)\phi(l) = 2^2 3^{k-1}\phi(l) \neq 2 \cdot 3^k\phi(l) = \phi(3n)$$

   We have reached a contradiction.

3. Find all $n \in \mathbb{Z}^+$ such that $\phi(n)$ is not divisible by 4.

   Solution: According to the fundamental theorem of arithematic, any integer $n \geq 2$ can be written as $n = p_1^{k_1} p_2^{k_2} \dots p_l^{k_l}$ where $p_1, p_2, \dots p_l$ are distinct primes, $k_1, k_2, \dots k_l \geq 1$ and $l \geq 1$. It follows that

   $$\begin{aligned}\phi(n) &= n\left(1 - \frac{1}{p_1}\right)\left(1 - \frac{1}{p_2}\right)\dots\left(1 - \frac{1}{p_l}\right) \\ &= \frac{n(p_1 - 1)(p_2 - 1)\dots(p_l - 1)}{p_1 p_2 \dots p_l} \\ &= p_1^{k_1 - 1} p_2^{k_2 - 1} \dots p_l^{k_l - 1}(p_1 - 1)(p_2 - 1)...(p_l - 1)\end{aligned}$$

   Let's assume that n has at least 2 odd prime factors, say p_i and p_j. Then $\phi(n)$ will have at least 2 even terms in the expansion above, $p_i - 1$ and $p_j - 1$ and hence will be divisible by 4. Thus, there can be at most 1 odd prime factor of n, let's say p.

   Also, $p \equiv 3 \pmod 4$. This is because if $p \equiv 1 \pmod 4$, then $p - 1$ will be divisible by 4. Also, there is no other possibility modulo 4 for p as it is odd.

Thus, $n = 2^{k_1}p^{k_2}$ where $p \equiv 3 \pmod 4$. Then,

$$\phi(n) = 2^{k_1-1}p^{k_2-1}(p-1)$$

if $k_1, k_2 \geq 1$ and

$$\phi(n) = 2^{k_1-1}$$

if $k_1 \geq 1$ and $k_2 = 0$. In the first case, $k_1 - 1 \leq 0$ because 2 divides $p-1$. In the second case, $k_1 - 1 \leq 1$.

Hence, the possibilities for such n are 1, 2, 4, p^k or $2p^k$ where $p \equiv 3 \pmod 4$ and $k \geq 1$.

4. Find all $n \in \mathbb{Z}^+$ such that $\phi(n)|n$.

Solution: Any integer $n \geq 2$ has a unique representation as a product of prime numbers i.e. $n = p_1^{k_1}p_2^{k_2}\dots p_\ell^{k_\ell}$ where $p_1, p_2, \dots p_\ell$ are distinct primes, $k_1, k_2, \dots k_\ell \geq 1$ and $\ell \geq 1$. It follows that

$$\phi(n) = n\left(1-\frac{1}{p_1}\right)\left(1-\frac{1}{p_2}\right)\dots\left(1-\frac{1}{p_\ell}\right) = \frac{n(p_1-1)(p_2-1)\dots(p_\ell-1)}{p_1p_2\dots p_\ell}$$

In other words, we can write $n = \frac{N}{D}\phi(n)$, where

$$N = p_1p_2\dots p_\ell$$

and

$$D = (p_1-1)(p_2-1)\dots(p_\ell-1)$$

It follows that $\phi(n)|n$ iff $D|N$.

Suppose that n is divisible by at least 2 distinct odd primes, say p_i and p_j. Then, $D \equiv 0 \pmod 4$ (for an odd prime p, $p-1$ is even), but $N \equiv 2 \pmod 4$ or N is odd, contradicting the requirement that $D|N$. Therefore, it can be assumed that n is divisible by at most one odd prime, say p. So, $n = 2^{k_1}p^{k_2}$ for an odd prime p and $k_1, k_2 \geq 0$. We consider the following cases:

Case $k_2 = 0$: In this case $n = 2^{k_1}$. If $k_1 > 0$, $\phi(n) = n/2$ and if $k_1 = 0$, then $n = 1$ and $\phi(n) = 1$. In both cases $\phi(n)|n$.

Case $k_2 > 0$: Now, if $k_1 = 0$, we have $n = p^{k_2}$ then $N = p$ and $D = p-1$. For N to be divisible by D, it must be the case that $p = 2$ but this contradicts the fact that p is an odd prime.
If $k_1 > 0$ then $N = 2p$ and $D = p-1$. For N to be divisible by D, the only possibility is if $p = 3$ as p and $p-1$ are always co-prime.

Thus $\phi(n)|n$ iff n is of the form 2^k for $k \geq 0$ or $2^{k_1}3^{k_2}$ where $k_1, k_2 > 0$.

5. Define the *order* of $a \in \mathbb{Z}_m^*$ to be

$$\text{ord}(a, m) = \min\{d > 0 | a^d \equiv 1 \pmod m\}.$$

Prove that for every $a \in \mathbb{Z}_m^*$, $\text{ord}(a, m)|\phi(m)$.

Hint: Use Euler's Totient theorem. If $\text{ord}(a, m)$ *does not divide* $\phi(m)$*, what can you say about its remainder?*

Solution: For $a \in \mathbb{Z}_m^*$, let $S = \{d > 0 | a^d \equiv 1 \pmod m\}$ and g be $\text{ord}(a, m)$, that is, the minimum element in S.

We prove that g divides $\phi(m)$ by contradiction.

Suppose, for the sake of contradiction, g doesn't divide $\phi(m)$. That is,

$$\phi(m) = gq_1 + r_1$$

where q_1 is the quotient and $0 < r_1 < g$.

Consider,

$$\begin{aligned} a^{\phi(m)} &\equiv a^{gq_1+r_1} \pmod m \\ &\equiv (a^g)^{q_1} \cdot a^{r_1} \pmod m \\ &\equiv (1)^{q_1} \cdot a^{r_1} \pmod m && \text{since } g \in S \\ &\equiv a^{r_1} \pmod m \end{aligned}$$

But by Euler's Totient theorem, we have, $a^{\phi(m)} \bmod \text{m} = 1$.

This implies, $a^{r_1} \bmod \text{m} = 1$ and $r_1 > 0$. Therefore, r_1 must be in S. But as $r_1 < g$, this contradicts the minimality of g. Therefore, our assumption is false and hence order(a, m) divides $\phi(m)$.

6. Define the *maximum order* in $\mathbb{Z}_m^*$ to be

$$\text{maxord}(m) = \max_{a \in \mathbb{Z}_m^*} \text{ord}(a, m).$$

In the lectures, it was mentioned that for many m, $\text{maxord}(m) = \phi(m)$. In particular, this is the case when m is of the form p^k for odd primes p. In this problem you explore some cases when it is not so.

(a) What is maxord(8)? Compute this by enumerating $\text{ord}(a, 8)$ for all $a \in \mathbb{Z}_8^*$.
Solution: We have $\mathbb{Z}_8^* = \{1, 3, 5, 7\}$. The corresponding order of these elements modulo 8 are $\{1, 2, 2, 2\}$. Hence $\text{maxord}(8) = 2$.

(b) Suppose p, q are distinct primes. Let $r = \text{maxord}(p)$ and $s = \text{maxord}(q)$. Prove that $\text{maxord}(pq) = \text{lcm}(r, s)$.

Hint: Use CRT. To prove that $\text{maxord}(pq) = d$ *you can show that* $\forall a \in \mathbb{Z}_{pq}^*$, $a^d = 1$ and $\exists a \in \mathbb{Z}_{pq}^*$ *s.t.* $\text{ord}(a) = d$.
Solution: Firstly, recall the fact that when p is a prime, $\mathbb{Z}_p^*$ has a generator, say g. Then $\text{ord}(g, p) = p - 1$. On the other hand, for all $a \in \mathbb{Z}_p^*$, by Fermat's little theorem, $a^{p-1} \equiv 1 \pmod{p}$, and hence $\text{ord}(a, p) \leq p - 1$. Thus $\text{maxord}(p) = p - 1$. Similarly, $\text{maxord}(q) = q - 1$.
Let $d = \text{lcm}(r, s)$, where $r = p - 1$, $s = q - 1$. We shall show that $\text{maxord}(pq) = d$.
To show that $\text{maxord}(pq) \leq d$, consider an arbitrary $a \in \mathbb{Z}_{pq}^*$. Since $r|d$ and $s|d$, by Fermat's little theorem we have $a^d \equiv 1 \pmod{p}$ and $a^d \equiv 1 \pmod{q}$. Thus the CRT representation of $a^d \in \mathbb{Z}_{pq}^*$ is $(1, 1) \in \mathbb{Z}_p^* \times \mathbb{Z}_q^*$. Since $(1, 1)$ is the CRT representation of 1, $a^d \equiv 1 \pmod{pq}$. Thus $\text{ord}(a, pq) \leq d$. Since this holds for all $a \in \mathbb{Z}_{pq}^*$, $\text{maxord}(pq) \leq d$.
To show that $\text{maxord}(pq) \geq d$, we shall find one element z such that $\text{ord}(z, pq) \geq d$. Let g and h be generators of $\mathbb{Z}_p^*$ and $\mathbb{Z}_q^*$, respectively. We define z to be the element with CRT representation (g, h). Now, suppose $\text{ord}(z, pq) = t$. Then, $t > 0$ and $z^t \equiv 1 \pmod{pq}$. Then, by CRT $g^t \equiv 1 \pmod{p}$ and $h^t \equiv 1 \pmod{q}$. Since g, h are generators, this requires $r|t$ and $s|t$. But $d = \text{lcm}(r, s)$ is the smallest positive common multiple of r, s. Hence $t \geq d$. Thus, $\text{ord}(z, pq) \geq d$ as required.

(c) Use part (b) to argue that when p, q are two distinct odd primes, $\text{maxord}(p, q) \neq \phi(pq)$.
Solution: From (b) we have, $\text{maxord}(p, q) = \text{lcm}(\text{maxord}(p), \text{maxord}(q)) = \text{lcm}(p - 1, q - 1)$. On the other hand, $\phi(pq) = (p - 1)(q - 1)$. Since p, q are odd, 2 is a common factor of $p - 1$ and $q - 1$ and hence $\text{lcm}(p - 1, q - 1) = pq/\gcd(p - 1, q - 1) \leq (p - 1)(q - 1)/2$. Hence $\text{maxord}(pq) \neq \phi(pq)$.

7. If possible, solve the following system of congruences using the Chinese Remainder theorem :

$$2x \equiv 11 \pmod{23}$$
$$9x \equiv 12 \pmod{31}$$

Hint: First write this system in a form to which CRT applies.

Solution:

We first rewrite the equations in a form where CRT can be applied.

We note that inverse of 2 modulo 23 is 12 and inverse of 9 modulo 31 is 7.

Therfore, multiplying the first equation by 12 and the second by 7, we get,

$$x \equiv 11 \cdot 12 \pmod{23}$$
$$x \equiv 12 \cdot 7 \pmod{31}$$

Which are equivalent by modulo arithmetic to,

$$x \equiv 17 \pmod{23}$$
$$x \equiv 22 \pmod{31}$$

Now, as $\gcd(23, 31) = 1$, we have a unique solution modulo $(23 \cdot 31)$ to the above system. We shall find integers u, v such that $23u + 31v = 1$, and then we can set $x = 31 \cdot v \cdot 17 + 23 \cdot u \cdot 22$. For this, we execute the Extended Euclidean Algorithm, and go through the following sequence of pairs:

$$(23, 31) \to (23, 8 = 31 - 23) \to (7 = 23 - 2 \cdot 8, 8) \to (7, 1 = 8 - 7).$$

Working backwards, we have $1 = 8 - 7 = 8 - (23 - 2 \cdot 8) = 3 \cdot 8 - 23 = 3(31 - 23) - 23 = 3 \cdot 31 - 4 \cdot 23$. That is, $u = -4$ and $v = 3$. Hence, we set

$$x = 31 \cdot 3 \cdot 17 + 23 \cdot (-4) \cdot 22 = -443$$

, or $x \equiv 270 \pmod{713}$.

8. Solve the following system of congruences :

$$2x + 5y \equiv 4 \pmod{11}$$
$$x + 3y \equiv 7 \pmod{11}$$

Hint: How would you solve such a system over the real or rational numbers, instead of modulo 11? You can proceed similarly, 11 being a prime.

Solution:

Subtracting the first equation from 2 times the second equation, we have

$$y \equiv 2 \cdot 7 - 4 \pmod{11}.$$

That is $y \equiv 10 \pmod{11}$. Substituting this into the second equation, we have $x \equiv 7 - 30 \pmod{11}$. That is, $x \equiv 10 \pmod{11}$.

9. Find the last 2 digits of 2^{2018}.

Hint: Note that 2 is not coprime with 100.

Solution: We need to find $2^{2018} \pmod{100}$. But since 2 is not coprime to 100, we cannot apply Euler's Theorem directly. Instead, we find 2^{2018} modulo 25 and modulo 4 separately, and then use CRT to combine them.

By Euler's Theorem,

$$2^{20} \equiv 1 \pmod{25}$$

because $\phi(25) = 20$. Since $2018 \equiv -2 \pmod{20}$, we have

$$\begin{aligned} 2^{2018} &\equiv 2^{20q-2} \pmod{25} && \text{for some } q \\ &\equiv 13^2 \pmod{25} && \text{since } 2^{-1} \equiv 13 \pmod{25} \\ &\equiv 19 \pmod{25} && \text{since } 13^2 = 169 = 150 + 19. \end{aligned}$$

Also, $2^{2018} \equiv 0 \pmod{4}$. While one can solve for x s.t., $x \equiv 19 \pmod{25}$ and $x \equiv 0 \pmod{4}$, in this case it is easier to enumerate the four values of $x \pmod{100}$ which satisfies the first congruence: $19, 44, 69, 94$ and note that 44 is the one which satisfies the second congruence. Thus the last two digits of 2^{2018} are 44.

10. **Square-Roots of 1.** In the lecture, we discussed the square-roots of 1 modulo a prime number.

(a) Find all solutions of $x^2 \equiv 1 \pmod{p^k}$ where p is prime and $k \geq 1$.

Hint: Separately analyze the cases when p is odd and $p = 2$.

Solution: Firstly, $x^2 \equiv 1 \pmod{m}$ iff $(x+1)(x-1) \equiv 0 \pmod{m}$. That is $m|(x+1)(x-1)$. When $m = p^k$ where p is a prime, this means that $p^i|(x+1)$ and $p^j|(x-1)$ for some i, j such that $i + j \geq k$.

Following the hint, we treat the cases when p is even and odd separately.

Case 1: p is odd. We cannot have $p|(x+1)$ and $p|(x-1)$, because otherwise $p|2$. Hence, either $p^k|(x+1)$ or $p^k|(x-1)$. Correspondingly, we require $x \equiv \pm 1 \pmod{p^k}$. In either case, $x^2 \equiv 1 \pmod{p^k}$. So these are exactly the two possible solutions.

Case 2: $p = 2$. Suppose $2^i|(x+1)$ and $2^j|(x-1)$. Note that if $i \geq 2$ and $j \geq 2$, then $4|(x+1)$ and $4|(x-1)$, which implies that $4|2$, a contradiction. So we have the following 4 cases where at least one of i, j is < 2:

- $i = 0$. In this case $j \geq k$, and so $2^k|(x-1)$. That is $x \equiv 1 \pmod{2^k}$.
- $i = 1$. In this case $j \geq k-1$, and so $2^{k-1}|(x-1)$. That is $x - 1 = q2^{k-1}$. If q is even, have $x \equiv 1 \pmod{2^k}$ as in the previous case. Otherwise, $x \equiv 2^{k-1} + 1 \pmod{2^k}$.
- $i \geq k-1, j = 1$. In this case, working as above, we get $x \equiv -1 \pmod{2^k}$ or $x \equiv 2^{k-1} - 1 \pmod{2^k}$.
- $i \geq k, j = 0$. In this case, working as above, we get $x \equiv -1 \pmod{2^k}$.

Thus, for $m = 2^k$, the set of possible solutions for the congruence $x^2 \equiv 1 \pmod{m}$ are $\{\pm 1, \frac{m}{2} \pm 1\}$. We note that all these values indeed satisfy the congruence.

(b) Find all solutions of $x^2 \equiv 1 \pmod{144}$.

Solution: By CRT, $x^2 \equiv 1 \pmod{144}$ if and only if x satisfies the system of congruences $x^2 \equiv 1 \pmod{16}$ and $x^2 \equiv 1 \pmod{9}$. From (a), solutions to the $x^2 \equiv 1 \pmod{16}$ are $1, -1, 7, 9 \pmod{16}$ and solutions to the $x^2 \equiv 1 \pmod{9}$ are $1, -1 \pmod{9}$. That is, the set of solutions of $x^2 \equiv 1 \pmod{144}$ are exactly those which satisfy

$$x \equiv 1, -1, 7 \text{ or } 9 \pmod{16}$$
$$x \equiv 1, -1 \pmod{9}.$$

Each of the 8 pairs in $\{\pm 1, 8 \pm 1\} \times \{\pm 1\}$ corresponds to the CRT representation of a unique x modulo 144. Using the fact that $16 \cdot 4 + 9 \cdot (-7) = 1$, we obtain these 8 solutions as 1, 127, 55, 73, 17, 143, 71, 89.

Problem Set 4

Released: October 11, 2021

1. Given a set S, its powerset is defined as the set of all subsets of S. That is, $\mathcal{P}(S) = \{T \mid T \subseteq S\}$. Describe $\mathcal{P}(\{1,2\}))$ explicitly.

   Solution: The different subsets of $S = \{1,2\}$ are $\emptyset, \{1\}, \{2\}$ and $\{1,2\}$. Thus, $\mathcal{P}(S) = \{\emptyset, \{1\}, \{2\}, \{1,2\}\}$.

2. **Subsets as bit strings.** Given a set S with $|S| = n$, we may use bit-strings to conveniently represent the subsets of S. For this, we fix an arbitrary ordering of the n elements in S. Then, $T \subseteq S$ is represented by the n-bit string x_T such that the i^{th} bit of x_T is 1 iff the i^{th} element of S (in the order we have fixed) is in T. In answering the following, you can use boolean operators to n-bit strings, where the operation is applied bit-wise (e.g., $001 \oplus 010 = 011$, $\neg 001 = 110$).

   (a) Express $x_{A\cap B}, x_{A\cup B}$ and x_{A-B} in terms of x_A and x_B.

   Solution: $x_{A\cap B} = x_A \wedge x_B$ because the i^{th} element of $S \in A \cap B$ iff it belongs to both A and B. Similarly, $x_{A\cup B} = x_A \vee x_B$ i.e. the bit-wise OR of the 2 bit strings. Also, the i^{th} element $\in x_{A-B}$ iff it belongs to A but not in B. Thus, $x_{A-B} = x_A \wedge (\neg x_B)$.

   (b) Describe the set T in terms of A, B, C, if $x_T = x_A \oplus x_B \oplus x_C$.

   Solution: For any 3 bits p, q and r, $p \oplus q \oplus r =$ True iff odd number of variables are True i.e. either only p, q or r are True or all 3 of them are True. This translates to T as all the elements which are present in any one of A, B or C along with the elements which are present in all the 3 sets.

3. **A Set representing Prime Factorization.** For every positive integer n, define a set $PF_n \subseteq \mathbb{Z}^+ \times \mathbb{Z}^+$ to denote the prime factors of n, as follows.

$$PF_n = \{(p,i) : p \text{ is prime}, i \in \mathbb{Z}^+ \text{ and } (p^i \mid n)\}.$$

   (a) What is PF_1?

   Solution: $PF_1 = \emptyset$ because the only integer that divides 1 is 1 itself and 1 is not a prime.

   (b) Explicitly write down PF_{12} and PF_{30}.

   Solution: $PF_{12} = \{(2,1),(2,2),(3,1)\}$ as $12 = 2^2 3^1$. Similarly, $PF_{30} = \{(2,1),(3,1),(5,1)\}$ as $30 = 2^1 3^1 5^1$.

   (c) Write down $PF_{\text{gcd}(12,30)}$.

   Solution: One can calculate $\text{gcd}(12,30) = 6$. Hence, $PF_{\text{gcd}(12,30)} = PF_6 = \{(2,1),(3,1)\}$ because $6 = 2^1 3^1$.

   (d) Write down $PF_{\text{lcm}(12,30)}$.

   Solution: One can calculate $\text{lcm}(12,30) = 60$. Hence, $PF_{\text{lcm}(12,30)} = PF_{60} = \{(2,1),(2,2),(3,1),(5,1)\}$ because $60 = 2^2 3^1 5^1$.

   (e) Suppose $a|b$ for positive integers a, b. What is the relation between PF_a and PF_b?
   Solution: $PF_a \subseteq PF_b$. To see this, consider $(p,i) \in PF_a$. By definition of PF_a, $p^i \mid a$. But since $a|b$, we have $p^i \mid b$. Thus $(p,i) \in PF_b$.

   (f) For any two positive integers m and n, give formulas for $PF_{\text{gcd}(m,n)}$ and $PF_{\text{lcm}(m,n)}$ in terms of PF_m and PF_n.
   Solution:
   CLAIM: $PF_{\text{gcd}(m,n)} = PF_m \cap PF_n$.
   PROOF: Firstly, we note that $a|b$ iff $PF_a \subseteq PF_b$. One direction was shown above. In the other direction note that $a = \prod_{(p,i)\in PF_a} p$. Hence if $PF_a \subseteq PF_b$, then $b = (\prod_{(p,i)\in PF_a} p)(\prod_{(p,i)\in PF_b - PF_a} p)$, and so $a|b$.
   Hence, g is a common divisor of m, n iff $PF_g \subseteq PF_m \cap PF_n$. Let $g^* = \prod_{(p,i)\in PF_m \cap PF_n} p$. That is, for each prime p, the highest power of p that is a divisor for g^* is the smaller of those for m and n. Then it can be seen that $PF_{g^*} = PF_m \cap PF_n$. Hence g^* is a common divisor of m, n. Further, any common divisor g is such that $g|g^*$ and hence $g \leq g^*$. Thus $g^* = \text{gcd}(m,n)$.
   CLAIM: $PF_{\text{lcm}(m,n)} = PF_m \cup PF_n$.
   PROOF: Using the fact (argued above) that $a|b$ iff $PF_a \subseteq PF_b$, we have that h is a common multiple of m, n iff $PF_m \cup PF_n \subseteq PF_h$. Now let $h^* = \prod_{(p,i)\in PF_m \cup PF_n}$ so that $PF_{h^*} = PF_m \cup PF_n$. Hence h^* is a common multiple of m, n and further, for any common multiple h, we have $h^*|h$ and hence $h^* \leq h$. Thus $h^* = \text{lcm}(m,n)$.

(g) Conclude from the above that, if x is a common divisor and y is a common multiple of two positive integers m, n, then $x|\gcd(m,n)$ and $\text{lcm}(m,n)|y$.

4. Give an example for each of the following, if such an example exists. Else prove why it cannot exist.

(a) A relation that is irreflexive, antisymmetric and not transitive.

Solution: A simple finite example is a relation defined over a set $\{1,2,3\}$ by the set of pairs $\{(1,2),(2,3)\}$.
As an example over an infinite set, we define relation $a \sqsubset b$ to hold iff $b = a^2$ where $a, b \in \mathbb{Z}^+ \backslash \{1\}$. This relation is irreflexive as for any $a \geq 2$, $a^2 \neq a$. It is antisymmetric because if $b = a^2$ then $a \neq b^2$ as the only integer values for b that solve this equation are $b = \{0,1\}$. It is not transitive because $b = a^2$ and $c = b^2$ implies $c = a^4$ and not $c = a^2$.

(b) A relation that is neither symmetric nor antisymmetric.

Solution: Suppose we define $a \sqsubseteq b$ as $\text{slope}(a) \geq \text{slope}(b)$ where the set S is the set of all lines in 2-D. For 2 different lines l_1, l_2 such that $\text{slope}(l_1) = \text{slope}(l_2)$, both $l_1 \sqsubseteq l_2$ and $l_2 \sqsubseteq l_1$ but for 2 lines with different slopes, only one of these possibilities can happen.

(c) An antisymmetric relation which has a symmetric relation as its subset.

Solution: Given any antisymmetric relation R_A, consider all $(a,a) \in R_A$. All such elements taken together will give a symmetric relation (trivially) which will be a subset of R_A.

(d) Relations R_1 and R_2 on set S such that both are symmetric but $R_1 \cap R_2$ is not symmetric.

Solution: We can prove that given 2 symmetric relations R_1 and R_2, $R_1 \cap R_2$ is also symmetric. For the sake of contradiction, assume that $R_1 \cap R_2$ is not symmetric. Thus, $\exists (a,b) \in R_1 \cap R_2$ such that $(b,a) \notin R_1 \cap R_2$. We can say that $(a,b) \in R_1$ and $(a,b) \in R_2$ (definition of intersection). Hence, $(b,a) \in R_1$ and $(b,a) \in R_2$ (both R_1 and R_2 are symmetric). Thus, $(b,a) \in R_1 \cap R_2$. Hence, we get a contradiction.

5. Given a relation R over a ground set S, and a subset $T \subseteq S$, define the relation $R|_T$ *induced* by R on T as follows:

$$R|_T = R \cap (T \times T).$$

That is, for every pair $(a,b) \in T \times T$, $(a,b) \in R|_T$ iff $(a,b) \in R$. Which of the following statements are true for any relation R over S and any $T \subseteq S$? Justify your answer with a proof or a counterexample.

(a) If R is symmetric, so is $R|_T$.

Solution: True. Suppose R is symmetric and let $(x,y) \in R|_T$. Then $(x,y) \in T \times T$ and $(x,y) \in R$. Since R is symmetric, $(y,x) \in R$. Also, $(y,x) \in T \times T$. Therefore, $(y,x) \in R|_T$. Hence, $R|_T$ is symmetric.

(b) If R is irreflexive, so is $R|_T$.

Solution: True. We prove this by contradiction. Suppose R is irreflexive and let $(x,x) \in R|_T$. Then, by definition, $(x,x) \in R$, which means R is not irreflexive, which is a contradiction. Therefore, R is irreflexive.

(c) If R is not reflexive, nor is $R|_T$.

Solution:
False. Consider S = $\{1,2\}$, R = $\{(1,1),(1,2)\}$, T = $\{1\}$. Then, $R|_T = \{(1,1)\}$. Clearly, R is not reflexive over S, but $R|_T$ is over T. Therefore, the proposition is false.

(d) If R is a partial order, so is $R|_T$.

Solution: True. In addition to (a), we prove the following.
(i) If R is reflexive, so is $R|_T$.
(ii) If R is transitive, so is $R|_T$.
Suppose, R is reflexive. Then $\forall x \in T \subseteq S$, $(x,x) \in R$. But as $(x,x) \in T \times T$, $(x,x) \in R|_T$. Hence, (i) is true.
Suppose R is transitive and $(x,y),(y,z) \in R|_T$. Then, $(x,y),(y,z) \in R$ and $x,y,z \in T$. Since, R is transitive, $(x,z) \in R$ and $(x,z) \in T \times T$. Therefore, $(x,z) \in R|_T$. Hence, (ii) is true.
Now, if R is a partial order, then R is reflexive, symmetric and transitive. From above, this implies that $R|_T$ is reflexive, symmetric and transitive. Therefore $R|_T$ is also a partial order.

6. Given a relation R, define R^2 as follows:

$$R^2 = \{(a,b) | \exists c\ (a,c) \in R \text{ and } (c,b) \in R\}.$$

Show the following.

(a) If R is symmetric, so is R^2.

Solution: Suppose R is symmetric. Let $(x,y) \in R^2$. This implies $\exists z$ s.t $(x,z) \in R, (z,y) \in R$. Since, R is symmetric, this means $(y,z) \in R, (z,y) \in R$. Therefore, $(y,x) \in R^2$. Hence, R^2 is symmetric.

(b) R^2 being symmetric does not imply that R is symmetric.

Solution: We prove this by giving a counter example. Let R = $\{(1,4),(1,2),(2,3),(2,1),(3,2)\}$ be a relation over S = $\{1,2,3,4\}$. Then, $R^2 = \{(1,3),(3,1)\}$. It can be seen that R^2 is symmetric but not R. Hence, the statement is true.

(c) If R is reflexive and transitive, $R = R^2$.

Solution: Suppose R is reflexive and transitive. We shall prove that $R \subseteq R^2$ and $R^2 \subseteq R$.
Let $(x,y) \in R$. Since, R is reflexive, $(y,y) \in R$. Therefore, by definition of R^2, $(x,y) \in R^2$. Thus, for all $(x,y) \in R$, $(x,y) \in R^2$.
Let $(x,y) \in R^2$, then by definition, $\exists z, (x,z) \in R, (z,y) \in R$. Since, R is transitive, and $(x,z),(z,y) \in R$, $(x,y) \in R$. Thus, for all $(x,y) \in R^2$, $(x,y) \in R$.
From the above two, we conclude that, $R = R^2$.

7. Let S be the set of all colourings of the 2×2 checkerboard where each of the four squares is coloured either red or blue. Note that S has 16 elements. Let R be a relation on S, so that $(C_1, C_2) \in R$ if and only if C_2 can be obtained from C_1 by rotating the checkerboard.

(a) Show that R is an equivalence relation.

Solution: Let's define a turn as rotating the board by 90^o clockwise and a negative turn as rotating in anticlockwise.
As every board can be obtained by rotating 0 turns, R is reflexive relation.
Let for board positions C_1, C_2, $(C_1, C_2) \in R$ and let C_2 can be obtained by rotating C_1 x turns. Then rotating C_2 by $-x$ turns give C_1. Therefore, $(C_2, C_1) \in R$. Hence, R is symmetric.
Let (C_1, C_2) and $(C_2, C_3) \in R$ and C_2 is obtained by turning C_1 by x turns and C_3 is obtained by turning C_2 by y turns. Then, C_3 is obtained by turning C_1 $(x+y)$ turns. Hence, (C_1, C_3) is in R.
Hence, R is transitive.
From above, we conclude that R is an equivalence relation.

(b) What are the equivalence classes of R? For each equivalence class, describe one member in the class and the size of the class.

Solution: In each of the equivalence classes of R each board position can be obtained from other by rotation. We denote an equivalence class, as 4-tuple, the colours of the tiles in clockwise direction. R stands for colour red and B stands for Blue. There 6 equivalence classes in R. They are,
1. All the tiles are coloured red. (R, R, R, R). It has 1 element.
2. All the tiles are coloured blue. (B, B, B, B). It has 1 element.
3. 3 tiles are coloured blue. (B, B, B, R). It has 4 element.
4. 3 tiles are coloured red. (R, R, R, B). It has 4 element.
5. 2 tiles are coloured red. (B, B, R, R). It has 4 elements.
6. 2 tiles are coloured red. (R, B, R, B). It has 2 elements.

8. Let $(S, \preceq)$ be a (non-empty) poset. We write $a \prec b$ if we have $a \preceq b$ and $a \neq b$. An element $a \in S$ is called *maximal* if $\nexists b \in S$ s.t. $a \prec b$. Similarly, an element $a \in S$ is called *minimal* if $\nexists b \in S$ s.t. $b \prec a$.

(a) Consider a restriction of the divisibility poset to a small set, $(\{2,4,5,10,12,20,25\}, |)$. What are its maximal and minimal elements?

Solution: The minimal elements are 2 and 5. The maximal elements are 12,20, and 25.

(b) Consider poset $(\mathcal{P}(S), \subseteq)$ for some set S. What are its maximal and minimal elements?

Solution: Clearly, the empty set ϕ is a minimal element of this poset. Also, for any other subset X of S, $\phi \subseteq X$ and $X \neq \phi$, so X cannot be a minimal element. Therefore, ϕ is the only minimal element of the poset.
Similarly, it is easy to see that S is a maximal element of this poset. For any other subset X of S, $X \subseteq S$ and $X \neq S$, so X cannot be a maximal element. Therefore S is the only maximal element of the poset.

(c) Show that every maximal chain in a finite poset $(S, \preceq)$ contains a minimal element of S. (A maximal chain is a chain that is not a subset of a larger chain.)

Solution: Let C be a maximal chain in S. Consider the element a in C such that $a \preceq b$ for all b in C. We claim a is a minimal element in S.
Suppose not. Then there exists an element s in S such that $s \preceq a$ and $s \neq a$. Consider the subset $C' = C \cup \{s\}$. We claim C' is a chain in S. Indeed, for any two elements b, c in C', if neither b nor c equals s, then b, c are elements in C, so they are comparable. Furthermore, s is comparable with any element in C. This is because for any element b in C, $s \preceq a$ and $a \preceq b$, so $s \preceq b$ by transitivity.
However, C' is now a chain strictly containing C, which is a maximal chain. This is a contradiction to the maximality of C. Therefore a is a minimal element in S.

9. In the context of relations, the term *lattice* is used to refer to a poset in which every finite set of elements has both a least upper bound and a greatest lower bound. Prove that the following posets are lattices. In each case, define the least upper bound and greatest lower bound of any finite set of elements.

(a) $(\mathcal{P}(X), \subseteq)$, the set of subsets of X with the inclusion relation.

Solution: Consider a finite set $T \subseteq \mathcal{P}(X)$. Let $T = \{X_1, X_2, \cdots, X_k\}$ where each $X_i \in \mathcal{P}(X)$ (i.e., $X_i \subseteq X$). Let $W = X_1 \cup \cdots \cup X_k$ and $Z = X_1 \cap \cdots \cap X_k$. We claim that W is the lowest upper bound and Z the greatest lower bound of T. Firstly, Z is a lower bound of T, because $Z \subseteq X_i$ for all $1 \leq i \leq k$. Furthermore, suppose Y is some lower bound of T. Then $Y \subseteq X_i$ for all $1 \leq i \leq k$, and hence $Y \subseteq Z$. Thus, Z is a lower bound of T and for every lower bound Y, it holds that $Y \subseteq Z$. Thus Z is the greatest lower bound of T. Similarly, W can be shown to be the least upper bound of T.

(b) The divisibility poset, $(\mathbb{Z}^+, |)$.

Hint: You may use the fact from Problem 3(g) generalized to any finite number of integers.

Solution: Let $T = \{m_1, \cdots, m_k\}$, where each $m_i \in \mathbb{Z}^+$. We claim $g = \gcd(m_1, \cdots, m_k)$ is the greatest lower bound of T. Indeed, it is easy to see that g is a lower bound, because $g \mid m_i$ for all $1 \leq i \leq k$. Furthermore, if s is any other lower bound, then $s \mid m_i$ for all $1 \leq i \leq k$. That is s is a common divisor of these k numbers. Suppose the prime factorization of s is $\prod_{i=1}^{t} p_i^{d_i}$. Then we know (using the hint) that $s \mid g$. That is g is a lower bound for T and for every lower bound s it holds that $s \mid g$. Therefore g is the greatest lower bound of T in this poset. Similarly, it can be shown that $l = \text{lcm}(m_1, m_2, \cdots, m_k)$ is the least upper bound of T.
An alternate argument is to identify the divisibility poset as an inclusion poset over the power set of $P \times \mathbb{Z}^+$ where P is the set of primes (using Problem 3), and then appeal to the previous part.

10. Recall that the Mirsky's theorem stated in class states that in a poset P, the size of the largest chain in a poset P is of size k, is exactly equal to the smallest number of anti-chains that can partition P.

(a) Write out a formal proof for this, filling in all the details.

Solution: We prove the theorem by induction on k. For convenience of notation, let $P = (S, \preceq)$.
Base Case: If $k = 1$, then no two distinct elements in S can be related to each other (otherwise those two elements form a chain of size $2 > k$). This means the entire poset P is an anti-chain, so we need only one part to partition P into anti-chains.
Induction Hypothesis: Now, suppose the result is true for $k = m$. We now need to show that if the size of the largest chain in P is $m + 1$, then the smallest number of anti-chains needed to partition P is equal to $m + 1$. Let this smallest number of anti-chains required be denoted by a. Also, let C be a chain of size $m + 1$ in P; let the $m + 1$ distinct elements of C be $c_1 \preceq c_2 \preceq \cdots \preceq c_{m+1}$.
Induction Step: The first observation is that $a \geq m + 1$. Indeed, in any anti-chain A of P, no two elements of C can both be in A (as they are comparable). This means we need at least as many anti-chains to partition P as the number of elements in C, which is $m + 1$.

Now, consider all minimal elements M of P. Note that minimal elements form an anti-chain. Remove M from the set S, and consider the poset P' on the remaining elements. We claim that the maximum size of a chain in P', denoted by m', is equal to m.

Recall from problem 8 that c_1 is a minimal element in S. Also, no other element in C can be a minimal element. Therefore, $C \backslash \{c_1\}$ is a chain of size m, which proves $m' \geq m$.
Now we show $m' \leq m$. Suppose not. Then P' has a chain of size $m+1$, say D. This chain D is also a chain in the original poset P before deletion of the elements in M. But from problem 8, D has a minimal element d. This means $d \in M$, which is a contradiction, as we had deleted all minimal elements. Therefore $m' \leq m$, and combined with $m' \geq m$, we get $m' = m$.

By induction hypothesis, P' can be partitioned into m anti-chains. Combined with M, we obtain a partition of P into $m+1$ anti-chains, proving $a \leq m+1$. Therefore, $a = m+1$, as required.

(b) Prove that any poset with n elements must have either (i) a chain *and* an anti-chain both of length equal to $\sqrt{n}$, or (ii) a chain *or* an anti-chain of length greater than $\sqrt{n}$.

Solution: Suppose k is the size of the largest chain in a poset P with n elements. By Mirsky's Theorem, P can be partitioned into k anti-chains. By Pigeonhole Principle, one of these anti-chains, A, has size at least $\frac{n}{k}$.
If $k > \sqrt{n}$, then we have found a chain of length greater than $\sqrt{n}$. Else if $k < \sqrt{n}$, then the anti-chain A has size strictly greater than $\frac{n}{\sqrt{n}} = \sqrt{n}$. Otherwise $k = \sqrt{n}$, so $\sqrt{n}$ is an integer. Now, A has size at least $\sqrt{n}$ too; take a subset of A of size $\sqrt{n}$; this subset is an anti-chain of size $\sqrt{n}$. Therefore we found a chain of size $\sqrt{n}$ and an anti-chain of size $\sqrt{n}$.

(c) Consider the numbers from 1 to n arranged in an arbitrary order on a line. Prove that there must exist a $\sqrt{n}$-length subsequence of these numbers that is completely increasing or completely decreasing as you move from right to left. For example, the sequence 7, 8, 9, 4, 5, 6, 1, 2, 3 has an increasing subsequence of length 3, for example: 1, 2, 3, and a decreasing subsequence of length 3, for example: 9, 6, 3. *Hint: Define an appropriate poset that considers the value of each number as well as its position on the line.*

Solution: Each entry on the line can be represented by a pair of natural numbers (v, p), where v is the value of the number, and p is the position of the number on the line. Here, $1 \leq v, p \leq n$. Note that there are n such pairs of naturals; let the set containing these elements be S.
Define a relation $\preceq$ on the elements of S as follows: $(v_1, p_1) \preceq (v_2, p_2)$ if $v_1 \leq v_2$ and $p_1 \leq p_2$. It is a straightforward check that $\preceq$ is in fact, a partial order on S. Let $P = (S, \preceq)$.
Using the previous problem, there exists either a chain of length at least $\sqrt{n}$ or an anti-chain of length at least $\sqrt{n}$, in P. Suppose the former is true, that is, C is a chain of length $k \geq \sqrt{n}$ in P. Then the elements of C can be written as $(v_1, p_1) \preceq (v_2, p_2) \preceq \cdots (v_k, p_k)$. This means the values $v_1, v_2, \cdots, v_k$ form an increasing sequence from left to right (that is, a decreasing sequence from right to left).
Otherwise, suppose the later is true, that is, A is an antichain of length $k \geq \sqrt{n}$ in P. Let the elements of A be $(v_1, p_1), (v_2, p_2), \cdots, (v_k, p_k)$, where $v_1 < v_2 < \cdots < v_k$ (note that $v_i \neq v_j$, because the line has all n distinct naturals arranged on it). For any $i < j$, since $v_i < v_j$ and (v_i, p_i) and (v_j, p_j) are incomparable, we must have $p_i > p_j$. This means $p_1 > p_2 > \cdots > p_k$. This implies that the values $v_1, v_2, \cdots, v_k$ form an increasing sequence from right to left.

Problem Set 5

Released: October 11, 2021

1. **Equivalence Closure**

   (a) Show that the transitive closure of the symmetric closure of the reflexive closure of a relation R is the smallest equivalence relation that contains R.

   Solution: Let R_r be the reflexive closure of R, R_{rs} be the symmetric closure of R_r and R_{rst} be the transitive closure of R_{rs}. First we need to show that R_{rst} is an equivalence relation.

   i. Reflexive - Since $R_r \subseteq R_{rst}$, hence R_{rst} is reflexive.

   ii. Symmetric - We need to show that the transitive closure of a symmetric set is symmetric. For $(a,b) \in R_{rst}$, either $(a,b) \in R_{rs}$ or $\exists c$ s.t. $(a,c) \in R_{rs}$ and $(c,b) \in R_{rs}$. If $(a,b) \in R_{rs}$, then $(b,a) \in R_{rs}$ and hence $(b,a) \in R_{rst}$. If $(a,c) \in R_{rs}$ and $(c,b) \in R_{rs}$ then $(c,a) \in R_{rs}$ and $(b,c) \in R_{rs}$ which implies $(b,a) \in R_{rst}$. Hence, R_{rst} is symmetric.

   iii. Transitive - By definition, the transitive closure of a relation is transitive.

   Now we need to show that R_{rst} is the smallest equivalence relation which contains R. Let us consider an equivalence relation R_e which contains R. Then R_e must contain R_r because R_e is reflexive and contains R and by definition of reflexive closure, R_r is the smallest such relation. Thus, $R_r \subseteq R_e$. Also, R_e is symmetric and contains R_r. By definition of symmetric closure, R_{rs} is the smallest such relation. Hence, $R_{rs} \subseteq R_e$. Similarly, we can use the definition of transitive closure to claim $R_{rst} \subseteq R_e$.

   (b) Give an example such that the symmetric closure of the transitive closure of the reflexive closure of a relation R is not an equivalence relation.

   Solution: Consider a relation R on $\{1,2,3\}$ such that $R = \{(1,2),(3,2)\}$. The reflexive closure of R is $R_1 = \{(1,2),(3,2),(1,1),(2,2),(3,3)\}$. The transitive closure of R_1 is R_1 itself. The symmetric closure of R_1 is $R_2 = \{(1,2),(2,1),(3,2),(2,3),(1,1),(2,2),(3,3)\}$. Clearly, R_2 is not transitive as $(1,2) \in R_2$ and $(2,3) \in R_2$ but $(1,3) \notin R_2$. Hence, R_2 is not an equivalence relation.

2. Let $f : \mathbb{R}^2 \to \mathbb{R}^2$ be defined as $f((x,y)) = (y, y-x)$. Then define f^{-1}, or show that there is no unique inverse for f.

   Solution: We can define $f^{-1} : \mathbb{R}^2 \to \mathbb{R}^2$ as $f^{-1}(x,y) = (x-y, x)$. To show that this is the inverse function of f, we need to consider the compositions

   $$f^{-1} \circ f(x,y) = f^{-1}(f(x,y)) = f^{-1}(y, y-x) = (y-(y-x), y) = (x,y)$$

   By definition, f^{-1} is a valid inverse function for f. Also, since the image of f is the entire co-domain $\mathbb{R}^2$ (not very hard to verify), the inverse is unique.

3. Define a relation $\sim$ on the set of all functions from $\mathbb{R}$ to $\mathbb{R}$ by the rule $f \sim g$ if and only if there is a $z \in \mathbb{R}$ such that $f(x) = g(x)$ for every $x \geq z$. Prove that $\sim$ is an equivalence relation.

   Solution:

   (a) Reflexive - Pick any $z \in \mathbb{R}$. Trivially, $f(x) = f(x)$ for every $x \geq z$ which implies $f \sim f$.

   (b) Symmetric - Suppose $f \sim g$ where f and g are functions from $\mathbb{R}$ to $\mathbb{R}$. This means that $\exists z \in \mathbb{R}$ such that $f(x) = g(x)$ for every $x \geq z$. We can also write this as $g(x) = f(x)$ for every $x \geq z$. Hence, $g \sim f$.

   (c) Transitive - Consider $f \sim g$ and $g \sim h$ for f, g and h being functions from $\mathbb{R}$ to $\mathbb{R}$. Thus, $\exists z_1, z_2 \in \mathbb{R}$ s.t. $f(x) = g(x)\ \forall\ x \geq z_1$ and $g(x) = h(x)\ \forall\ x \geq z_2$. Consider $z = max\{z_1, z_2\}$. Then, $f(x) = h(x)\ \forall\ x \geq z$. Hence, $f \sim h$.

4. If functions $f : A \to B$ and $g : B \to C$ are such that $g \circ f$ is onto, then prove that g is onto. Use precise mathematical notation to prove this, starting from the definitions of onto and composition.

   Solution: Given that the function, $g \circ f : A \to C$ is an onto function. This means, $\forall y \in C, \exists x \in A\ (g \circ f)(x) = y$. By definition of composition we have, $(g \circ f)(x) = g(f(x))$. Therefore, we conclude that, $\forall y \in C, \exists x \in A\ g(f(x)) = y$. Since, $\forall x \in A, f(x) \in B$, we have $\forall y \in C, \exists z \in B\ g(z) = y$. Hence, g is an onto function.

5. Suppose $f : A \to B$ and $g : B \to C$ are such that $g \circ f$ is one-to-one. Is f necessarily one-to-one? Is g necessarily one-to-one? Justify.

Solution: Yes, f is necessarily a one-one function. We prove this as follows. Suppose, for $x_1, x_2 \in A$, $f(x_1) = f(x_2)$. Then,

$$\begin{aligned} &\implies g(f(x_1)) = g(f(x_2)) && \text{(applying g on both sides.)} \\ &\implies (g \circ f)(x_1) = (g \circ f)(x_2) && \text{(By definition of composition)} \\ &\implies x_1 = x_2 && \text{(As } g \circ f \text{ is one-one)} \end{aligned}$$

Therefore, $\forall x_1, x_2 \in A, f(x_1) = f(x_2) \implies x_1 = x_2$. Hence, f is one-one.

No, g need not be one-one. We prove this by giving a counter example. let $f : \mathbb{N}^+ \to \mathbb{N}^+$ be $f(x) = x+1$ and $g : \mathbb{N}^+ \to \mathbb{N}^+$ be $g(1) = 2$ and $g(x) = x$, if $x \geq 2$. Now, g is not one-one as $g(1) = g(2)$ but $(g \circ f)(x) = x + 1$ is one-one. Hence, g need not be one-one.

6. Suppose $f : A \to A$ is a function and $f \circ f$ is a bijection. Is f necessarily a bijection?

Solution: Yes, f is necessarily a bijection. Given that, $f \circ f : A \to A$ is a bijection, which means, $f \circ f$ is both one-one and onto. By Q4, we have that f is one-one and by Q5, we have that f is onto. Therefore, f is necessarily a bijection.

7. Given a function $f : A \to B$, define another function $f' : \mathcal{P}(A) \to \mathcal{P}(B)$ (where $\mathcal{P}(A)$ stands for the power-set of A), as follows: for any $S \subseteq A$, $f'(S) = \{f(x) | x \in S\}$. Show that $f'(S \cap T) \subseteq f'(S) \cap f'(T)$. Give an example of f and S, T such that $f'(S \cap T) \neq f'(S) \cap f'(T)$.

Solution: Suppose $b \in f'(S \cap T)$. By definition of f', $b = f(a)$ for some $a \in S \cap T$. Since $a \in S \cap T$, $a \in S$ and $a \in T$. Again, by definition of f', this means $b = f(a)$ is an element of $f'(S)$ and of $f'(T)$. Therefore $b \in f'(S) \cap f'(T)$. Therefore $f'(S \cap T) \subseteq f'(S) \cap f'(T)$.

Consider the function $f : \mathbb{Z} \to \mathbb{Z}$ defined as $f(n) = n^2$ for all integers n. Take $S = \{0, 1\}$ and $T = \{0, -1\}$. Then,

$$f'(S \cap T) = f'(\{0\}) = \{f(0)\} = \{0\}$$

On the other hand

$$f'(S) \cap f'(T) = f'(\{0, 1\}) \cap f'(\{0, -1\}) = \{0, 1\} \cap \{0, 1\} = \{0, 1\}$$

Clearly, $f'(S \cap T) \neq f'(S) \cap f'(T)$.

8. Given a function $f : A \to B$, we define another function $\text{inv}_f : \mathcal{P}(B) \to \mathcal{P}(A)$ as follows: for any $S \subseteq B$, $\text{inv}_f(S) = \{x | f(x) \in S\}$. Now, given functions $f : A \to B$ and $g : B \to C$, express $\text{inv}_{g \circ f}$ in terms of inv_f and inv_g. Justify.

Solution: Since $g \circ f$ is a function from A to C, $\text{inv}_{g \circ f}$ is a function from $\mathcal{P}(C)$ to $\mathcal{P}(A)$. For any subset S of C, we have

$$\text{inv}_{g \circ f}(S) = \{x | g(f(x)) \in S\}$$

We claim

$$\text{inv}_{g \circ f} = \text{inv}_f \circ \text{inv}_g$$

Let S be a subset of C. Suppose $x \in \text{inv}_{g \circ f}(S)$. Then $g(f(x)) \in S$. This means, by definition, that $f(x) \in \text{inv}_g(S)$. This in turn means $x \in \text{inv}_f(\text{inv}_g(S))$.
On the other hand, suppose $x \in \text{inv}_f(\text{inv}_g(S))$. This means $f(x) \in \text{inv}_g(S)$. This in turn means $g(f(x)) \in S$, so $x \in \text{inv}_{g \circ f}(S)$. Therefore $\text{inv}_{g \circ f}(S) = \text{inv}_f \circ \text{inv}_g(S)$. Since S was arbitrary, we have proved the claim.

9. Construct a bijection $f : \mathbb{Z} \to \mathbb{Z}^+$.

Solution: Let us first construct the bijection informally; we want to arrange the integers on a sequence. A natural candidate would be

$$0, 1, -1, 2, -2, 3, -3, \cdots$$

Formally, the bijection $f : \mathbb{Z} \to \mathbb{Z}^+$ is given by

$$f(x) = \begin{cases} 2x & x > 0 \\ -2x + 1 & x \leq 0 \end{cases}$$

It is not hard to show this is indeed a bijection.

10. Construct a bijection $f : \mathbb{Z}^2 \to \mathbb{Z}$.

Solution: We want to provide a bijection from $\mathbb{Z}^2$ to $\mathbb{Z}$. It suffices to construct a bijection from $\mathbb{Z}^{+^2}$ to $\mathbb{Z}^+$.
Infroamlly, we have lattice points in the first quadrant, and we want to arrange them in a sequence, such that every element in $\mathbb{Z}^{+^2}$ occurs exactly once. Consider the bijection

$$g(m,n) = \frac{(m+n-1)(m+n-2)}{2} + m$$

This is one possible bijection. To get a motivation as to how this bijection comes, observe that $f(1,1) = 1, f(1,2) = 2, f(2,1) = 3, f(1,3) = 4, f(2,2) = 5$, etc. This forms a "diagonal" pattern over the lattice points.
There are many other bijections possible. The following is also a bijection:

$$f(m,n) = 2^{m-1} \cdot (2n-1)$$

which relies on uniqueness of prime factorisation. Proving this is a bijection is easy. Suppose $f(m_1,n_1) = f(m_2,n_2)$. Then

$$2^{m_1-1} \cdot (2n_1 - 1) = 2^{m_2-1} \cdot (2n_2 - 1)$$

Comparing the powers of two both sides, we get $m_1 - 1 = m_2 - 1$, so $m_1 = m_2$. Cancelling, we get $2n_1 - 1 = 2n_2 - 1$, so $n_1 = n_2$. Therefore the function is injective.
Furthermore, for any natural number q, we can write it as $2^l \cdot k$, where $l \geq 0$, and k is odd. Then $l+1$ and $\frac{k+1}{2}$ are both naturals, and

$$f\left(l+1, \frac{k+1}{2}\right) = 2^{(l+1)-1} \cdot \left(2 \cdot \frac{k+1}{2} - 1\right) = q$$

Therefore f is surjective as well.

Problem Set 6

Released: October 11, 2021

1. How many relations are there on a set with n elements that are:

   (a) reflexive?

   (b) irreflexive?

   (c) symmetric?

   (d) antisymmetric?

   (e) asymmetric?

   (f) equivalence?

   Hint: Where appropriate, you may use $S(k, n)$, the Stirling number of the second kind.

   Solution: Let A be the domain for the relation R with n elements. Then are a total of n^2 elements in $A \times A$.

   (a) For a relation to be reflexive, it must contain pairs of the form (x, x) for all $x \in A$. There are n such pairs. For the remaining $n^2 - n$ pairs, both possibilities (of being present in R or not) do not affect the reflexive property. It follows that the total number of reflexive relations is 2^{n^2-n}.

   (b) For a relation to be irreflexive, it must not contain pairs of the form (x, x) for any $x \in A$. Any possibility is equally valid for the remaining pairs. Hence, the total number of irreflexive relations is 2^{n^2-n}.

   (c) In a symmetric relation, for $x \neq y$, either both (x, y) and (y, x) are in the relation or none of them is. Thus, there are two possibilities for $\frac{n^2-n}{2}$ tuples of unequal pairs i.e. tuples of the form $\{(x, y), (y, x)\}$ for $x \neq y$. The n pairs of the form (x, x) do not affect symmetricity. Therefore, the number of symmetric relations is $2^n 2^{\frac{n^2-n}{2}}$.

   (d) In an antisymmetric relation, for $x \neq y$, atmost one of (x, y) and (y, x) is present in the relation. Thus, there are three possibilities for $\frac{n^2-n}{2}$ tuples of unequal pairs i.e. exactly one of them is present (two possibilities) or none of them is. The n equal pairs do not affect the desired property. Therefore, the number of antisymmetric relations is $2^n 3^{\frac{n^2-n}{2}}$.

   (e) A asymmetric relation is like an antisymmetric relation along with the additional requirement that no pair of the form (x, x) can be present in the relation. Therefore, the total number of such relations is $3^{\frac{n^2-n}{2}}$.

   (f) An equivalence relation can be characterized by the equivalence partition of the domain. The number of partitions with exactly k parts is given by $S(n, k)$. Since the number of parts can range from 1 to n, the number of equivalence relations is $\sum_{k=1}^{n} S(n, k)$.

2. This problem considers proving that $\sum_{k=1}^{n} k\binom{n}{k} = n2^{n-1}$.

   (a) Give a combinatorial proof, by counting the number of ways to select a (non-empty) committee, with one member being the leader of the committee.

   (b) Prove this using the formula for $\binom{n}{k}$. First show that $k\binom{n}{k} = n\binom{n-1}{k-1}$.

   (c) Here is a trick we have not covered in the class, that uses your knowledge of calculus. Consider the polynomial $P(x) = (1 + x)^n$. Let $P'(x)$ be the polynomial obtained as the derivative of $P(x)$. Write two expressions for $P'(x)$, and use them to evaluate $P'(1)$.

   Solution:

   (a) Given n persons, we need to select a non-empty committee and a leader for the committee. One way to do that would be to first select a leader by choosing a person from the n people. All the remaining $n - 1$ persons may or may not be part of the committee without affecting its non-emptiness (since the leader is already a member). This gives us $n2^{n-1}$ ways. Another possibility would be to first form the committee and then the leader. Let the size of the committee be k. Such a committee can be selected in $\binom{n}{k}$ ways. The leader of this committee could be selected in k ways. Since k can range from 1 to n, this gives us $\sum_{k=1}^{n} k\binom{n}{k}$ ways.

(b) First, we can prove that

$$\begin{aligned} k\binom{n}{k} &= k\frac{n!}{k!(n-k)!} \\ &= \frac{n!}{(k-1)!(n-k)!} \\ &= n\frac{(n-1)!}{(k-1)!(n-k)!} \\ &= n\binom{n-1}{k-1} \end{aligned}$$

Therefore,

$$\begin{aligned} \sum_{k=1}^{n} k\binom{n}{k} &= \sum_{k=1}^{n} n\binom{n-1}{k-1} \\ &= n\sum_{k=1}^{n}\binom{n-1}{k-1} \\ &= n2^{n-1} \end{aligned}$$

(c) Using binomial theorem, we can write

$$(1+x)^n = \sum_{k=0}^{n}\binom{n}{k}x^k$$

Taking the derivative on both sides,

$$n(1+x)^{n-1} = \sum_{i=1}^{n}\binom{n}{k}kx^{k-1}$$

Evaluating this equation at $x = 1$,

$$n2^{n-1} = \sum_{k=1}^{n} k\binom{n}{k}$$

3. How many ways are there to travel in $xyzw$ space from the origin (0,0,0,0) to the point (4,3,5,4) by taking steps one unit in the positive x, positive y, positive z, or positive w direction? **Solution:** Each step will look like (0, 0, 0, 1), (0, 0, 1, 0), (0, 1, 0, 0) or (1, 0, 0, 0). Hence, a total of 16 steps will be taken to reach (4, 3, 5, 4) across each path from the origin. Each step can be labelled as $1_x, 1_y, 1_z$ or 1_z depending along which direction the step is taken. A path can be labelled as a permutation of these symbols with 4 1_x, 3 1_y, 5 1_z and 4 1_z symbols occurring in each permutation. Hence, the total number of such permutations are $\frac{16!}{4!3!5!4!}$.

4. A sequence of integers is said to be *smooth* if any two consecutive integers in the sequence differ by exactly 1. For instance, $5, 4, 5, 6, 5, 4$ is a smooth sequence of length 6.

   How many smooth sequences of length 16 are there that start with 5 and end with 10? **Solution:** The differences form a ± 1 sequence of length 15. The number of $+1$s should be 5 more than the number of -1s. Solving $x+y = 15$, $x-y = 5$, we have $x = 10$ $+1$s and $y = 5$ -1s. So $\binom{15}{5}$ ways.

5. A sequence of positive integers $a_1, a_2, \ldots, a_m$ is said to be *decreasing* if for all i, we have $a_i \geq a_{i+1}$. A decreasing sequence is said to *strictly decreasing* if any integer appears at most once in the sequence. A decreasing sequence is said to be *almost strictly decreasing* if any integer appears at most twice in the sequence.

   (a) How many strictly decreasing sequences of positive integers are there with $a_1 = n$ (of all possible lengths)?
   Solution: Any subset of $\{1, \ldots, n-1\}$ when sorted gives exactly one such sequence. So, 2^{n-1} sequences.

   (b) There are infinitely many decreasing sequences of positive integers that start with $a_1 = n$. How about almost strictly decreasing sequences?
   Solution: An almost strictly decreasing sequence is obtained by including each element in $\{1, \ldots, n-1\}$ 0, 1 or 2 times, along with n, which can be included 1 or 2 times. So $2 \cdot 3^{n-1}$ times.

   (c) How many strictly decreasing sequences of positive integers of length m exist with $a_1 = n$?
   Solution: $\binom{n-1}{m-1}$.

(d) How many decreasing sequences of positive integers of length m exist with $a_1 = n$?

Solution: Choose $m-1$ elements with repetition from $\{1, \ldots, n\}$ (and sort them). Using "$m-1$ stars and $n-1$ bars," $\binom{n+m-2}{m-1}$ ways.

6. Consider the standard deck of 52 playing cards. A balanced hand is a subset of 13 cards containing four cards of one suit and three cards of each of the remaining three suits.

(a) Find the number of balanced hands.

Solution: The suit S_1 with 4 cards in the hand can be picked in 4 possible ways. The rest of the suits will have 3 cards each. Given S_1, 4 cards from S_1 can be selected in $\binom{13}{4}$ ways. For the remaining three suits, the cards can be selected in $\binom{13}{3}$ ways from each suit and hence the total number of balanced decks is given by $4\binom{13}{4}\binom{13}{3}^3$.

(b) Find the number of ways of dealing the cards to four (distinguishable) players so that each player gets a balanced hand.

Solution: Each player gets 4 cards from a unique suit. A unique suit could be assigned to a player in 4! ways. Once this assignment is done, the number of ways for P_1 to be dealt a balanced hand are given by $\binom{13}{4}\binom{13}{3}^3$. For P_2, the number of possibilities have reduced to $\binom{10}{4}\binom{9}{3}\binom{10}{3}^2$. For P_3, the number of ways are then given by $\binom{7}{4}\binom{7}{3}\binom{6}{3}^2$. Once these three players have been dealt balanced hands, the remaining cards will form a balanced hand which gives only 1 way for P_4. All this time, we have assumed an ordering among the players, which can be achieved in 4! ways. Hence, the total number of ways is given by $(4!)^2\binom{13}{4}\binom{13}{3}^3\binom{10}{4}\binom{10}{3}^2\binom{9}{3}\binom{7}{4}\binom{7}{3}\binom{6}{3}^2$.

7. Suppose k universities are to be ranked by the Ministry of Education according to some arbitrary criteria. The ranking allows mutiple universities to be tied.

For instance, universities $\{A, B, C, D\}$ may be ranked as $B > A = C > D$, to mean that B is top-ranked, A, C are tied below that, and D is ranked at the bottom; note that $B > C = A > D$ refers to the same ranking.

What is the total number of such possible rankings? You may express your answer in the form of a summation, involving quantities used in the *balls-and-bins* problems.

Solution: A ranking could be viewed as assigning a rank to each university, making sure that the set of ranks used is exactly $[n]$ for some n. For each $n \in [k]$, the number of rankings that use exactly n ranks is $N(k, n)$, the number of onto functions from $[k]$ to $[n]$. So the total number of rankings is $\sum_{n=1}^{k} N(k, n)$.

Alternately, a ranking involves first grouping together universities that are to be tied with each other, and then ordering these groups. There are $S(k, n)$ ways of partitioning the universities into exactly n groups, and then $n!$ ways of ordering the groups. So the total number of rankings is $\sum_{n=1}^{k} n!S(k, n)$.

8. A variant of the balls-and-bins problem, when the balls are distinguishable, is that within each bin, the balls are ordered. Let $L(k, n)$ denote the number of ways k labelled items can be distributed among n lists (i.e., bins with order), where the lists themselves are unlabelled, such that no list is empty. E.g., $L(3, 2) = 6$ since $\{a, b, c\}$ can be split into 2 lists as $\{(a), (b, c)\}$, $\{(a), (c, b)\}$, $\{(b), (a, c)\}$, $\{(b), (c, a)\}$, $\{(c), (a, b)\}$, or $\{(c), (b, a)\}$.

Give a closed form expression for $L(k, n)$.

Hint: First consider the case where the lists are labelled. You may use a variant of stars and bars, with labelled stars. To ensure that no list is empty, you may use stars themselves as bars.

Solution: When the lists are distinguishable, each distribution corresponds to an ordering of all the k elements obtained by concatenating the n lists, with the first item in each list marked. Thus we need to count the ways in which the k elements can be ordered, and n of them marked; but the first element is required to be marked, and we may only choose $n-1$ of the remaining $k-1$ to be marked. This can be done in $k!\binom{k-1}{n-1}$ ways. Compared to when the lists are indistinguishable, this counts each partition into n lists in $n!$. Hence $L(k, n) = \frac{k!}{n!}\binom{k-1}{n-1}$.

Problem Set 7a

Released: November 1, 2021

1. **Degree Sequence.** In each of the following problems, either show that the given sequence cannot be the degree sequence of a graph, or give an example of a graph with that degree sequence.

   (a) $(1, 1, 1, 1, 0)$

   Solution: Consider $V = \{1, 2, 3, 4, 5\}$ and $E = \{(1, 2), (3, 4)\}$. All the 4 vertices {1, 2, 3, 4} have degree 1 while vertex {5} has degree 0.

   (b) $(2, 2, 2, 2, 2)$

   Solution: The cycle C_5 has 5 vertices and each of these vertices have degree 2.

   (c) $(3, 3, 2, 2, 1)$

   Solution: This is not possible because $\sum_{v \in V} deg(v) = 3+3+2+2+1 = 11$ which is odd but $\sum_{v \in V} deg(v) = 2|E|$ which implies that the sum must be even.

   (d) $(4, 4, 3, 2, 1)$

   Solution: This is not possible because there are 2 vertices which are connected to every other vertex implying that the degree of each vertex must be at least 2.

   (e) $(4, 3, 3, 3, 3)$

   Solution: The wheel W_4 has this degree sequence.

2. Define a pseudograph to be an undirected graph with one or more self-loops allowed in each node. The degree of a node in a pseudograph is defined by counting each self-loop as two edges incident on the node.

   Show that every (sorted) sequence of non-negative integers with an even sum of its terms is the degree sequence of a pseudograph.

   Hint: Construct such a graph by first adding as many self-loops as possible at each vertex. What does the residual degree sequence (i.e., degrees that remain to be satisfied) look like?

   Solution: Suppose there are k odd numbers and $n-k$ even numbers in the degree sequence. Since the sum of the terms is given to be even, so k is even.

   Now, for each even degree $2d$ in the degree sequence, where $d \geq 0$, put d self-loops on a vertex, and join it to no other vertex. For each odd degree $2d+1$ in the degree sequence, where $d \geq 0$, put d self-loops on a vertex. This leaves us with k vertices (corresponding to the odd degrees) that still have one more edge to be incident on them. Since k is even, we can simply make $\frac{k}{2}$ disjoint edges within themselves (a matching, to be precise), and we are done.

3. **Regular Graphs.**

   (a) For any integer $n \geq 3$ and any even integer d with $2 \leq d \leq n-1$, show that there exists a d-regular graph with n nodes, by giving an explicit graph (V, E), where $V = \mathbb{Z}_n$ and E is formally defined using modular arithmetic. (You may find it convenient to use S_a to denote $\{1, \ldots, a\} \subseteq \mathbb{Z}_n$.)

   Hint: What would you do for $d = 2$? Then consider adding additional edges for larger values of d.

   Solution: Consider the cycle C_n such that the neighbours of $i \in \mathbb{Z}_n$ are $i-1 \pmod n$ and $i+1 \pmod n$. This is a 2-regular graph on n vertices.

   One can similarly get a d-regular graph where d is even. For each node $i \in Z_n$, its neighbours are $i - \frac{d}{2} \pmod n, i - \frac{d}{2} + 1 \pmod n, ..., i-1, i+1, ..., i + \frac{d}{2} - 1 \pmod n, i + \frac{d}{2} \pmod n$.
   Formally, let $E = \{\{i, j\} \mid i-j \in S_{d/2} \text{ or } j-i \in S_{d/2}\}$. Then $\Gamma[i] = (i+S_{d/2}) \cup (i-S_{d/2})$, where $i \pm S = \{i \pm x | x \in S\}$. Note that these two sets are each of size $d/2$ and they are disjoint: Otherwise $i + x = i - y$ where $x, y \in S_{d/2}$, implying $x + y \equiv 0 \pmod n$, which is not possible as $x + y \in \{2, \cdots, n-1\}$.

(b) For any even integer $n \geq 2$ and any integer d with $1 \leq d \leq n-1$ show that there exists a d-regular graph with n nodes.

Hint: Use the previous part for even d. For odd d, use the previous part to first construct a $(d-1)$-regular graph, and find a way to add new edges so that all nodes have their degree incremented by 1.

Solution: For any even integer n, consider a 1-regular graph on n nodes in $\mathbb{Z}_n$ such that $E = \{(0,1),(2,3),...,(n-2,n-1)\}$. This is a complete bi-partite graph on n nodes. Since this is the only possibility for $n = 2$, we can reduce our proof for the cases of even $n \geq 3$ with $2 \leq d \leq n-1$. For even d, this problem reduces to part (a). Consider odd d such that $3 \leq d \leq n-1$ with even n. Our aim is to construct a $d-$regular graph on n vertices.

Consider the $(d-1)-$regular graph on n vertices from the construction in (a). Therefore, each $i \in \mathbb{Z}_n$ has neighbours $i - \frac{d-1}{2} \pmod n, ..., i-1, i+1, ..., i+\frac{d-1}{2} \pmod n$. Add a neighbour $i+\frac{n}{2} \pmod n$ to the vertex i i.e. the diagonally opposite node to i. This is possible because $d \leq n-1$ implying $\frac{d-1}{2} \leq \frac{n}{2} - 1$ which shows that $i + \frac{n}{2} \pmod n$ is not already a neighbour of i. The degrees of i and $i + \frac{n}{2} \pmod n$ have been increased from $d-1$ to d. Proceed similarly for each i with $0 \leq i < \frac{n}{2}$. Since n is even, a diagonally opposite element exists for each node. Hence, we have a $d-$regular graph on n vertices.

4. A graph with vertices $(v_1, \ldots, v_n)$ is said to be a *graph realization* of a sequence $d_1 \geq \ldots \geq d_n$ of non-negative integers, if for each i, $\deg(v_i) = d_i$ in the graph. There are efficient algorithms to check if a given sequence has a graph realization. In this problem you shall see one such algorithm.

a) Show that if $d_1 \geq \ldots \geq d_n$ has a graph realization, then it has a graph realization such that v_1 is adjacent to the d_1 nodes $v_2, \ldots, v_{d_1+1}$.

Hint: Among all the realizations, consider one which maximizes the sum of degrees of the nodes adjacent to v_1. If its vertices cannot be relabelled to be of the required form, then there are nodes v_i, v_j with $d_i > d_j$ and v_1 adjacent to v_j but not adjacent to v_i. **Solution:** Suppose the degree sequence $d_1 \geq d_2 \geq \cdots \geq d_n$ has a graph realisation. Among all graphs that realise this degree sequence, chose one which maximises the sum of degrees of those nodes which are adjacent to v_1. Call this graph G. We now assume the contrary, that is, suppose there exists no graph realising the given degree sequence such that v_1 is adjacent to $v_2, v_3, \cdots, v_{d_1+1}$. In particular, this is true for G as well. Consider the smallest index i for which v_1 is not adjacent to v_i. There must be some $j > i$ for which v_1 is adjacent to i (otherwise v_1 is adjacent to, and only to, $v_2, v_3, \cdots, v_{i-1}$, in which case $i = d_1+2$ and we are done).

If $d_i = d_j$, then we can swap the labels i and j, so that v_1 becomes adjacent to v_i (which was formerly v_j); this swap preserves the sum of degrees of the nodes adjacent to v_1. If we can keep doing such swaps and make v_1 adjacent to $v_2, v_3, \cdots, v_{d_1+1}$, then we arrive at a contradiction to our assumption. So the problem occurs when a swap is not possible, that is, there exist indices $i < j$ (these i and j may not be the i and j mentioned before) such that v_1 is adjacent to v_j but not to v_i, and $d_i > d_j$.

Since $d_i > d_j$, there exists some vertex v_k such that v_i is adjacent to v_k but v_j is not adjacent to v_k. Now, consider a new graph G' formed from G as follows: Remove the edges v_1v_j and v_iv_k, and add the edges v_1v_i and v_jv_k. This preserves the degree of each vertex as is. Furthermore, we now have v_i adjacent to v_1 and v_j not adjacent to v_1. The sum of the degrees of the nodes adjacent to v_1 changes by $d_i - d_j > 0$, which contradicts our choice of G.

Therefore, our assumption is wrong. This means if $d_1 \geq d_2 \geq \cdots \geq d_n$ has a graph realisation, then it has one such that v_1 is adjacent to the d_1 nodes $v_2, \cdots, v_{d_1+1}$.

b) Show that the sequence $d_1 \geq \ldots \geq d_n$ has a graph realization if and only if the sequence obtained by sorting $(d_2 - 1), ..., (d_{d_1+1} - 1), d_{d_1+2}, ..., d_n$ has a graph realization.

Note: This reduces the problem of checking realizability of n-long sequences to a problem of $(n-1)$-long sequences. This leads to a recursive algorithm. **Solution:** Suppose $d_1 \geq d_2 \geq \cdots \geq d_n$ has a graph realisation. From the previous problem, it has a graph realisation G such that if $V(G) = \{v_1, \cdots, v_n\}$ and $d_i = \deg(v_i)$ for every i, then v_1 is adjacent to $v_2, \cdots, v_{d_1+1}$.

Delete the vertex v_1 along with the edges incident on it. This leaves us with a graph G' with unsorted degree sequence $d_2 - 1, \cdots, d_{d_1+1} - 1, d_{d_1+2}, \cdots, d_n$. Therefore this degree list has a graph realisation too.

Conversely, suppose the unsorted degree sequence $d_2 - 1, \cdots, d_{d_1+1} - 1, d_{d_1+2}, \cdots, d_n$ has a graph realisation G'. Construct a graph G from G' by introducing a new vertex v, and joining v to the vertices with degrees

$d_2 - 1, \cdots, d_{d_1+1} - 1$. This graph has degrees $d_1, d_2, \cdots, d_{d_1+1}, d_{d_1+2}, \cdots, d_n$. Therefore $d_1 \geq d_2 \geq \cdots \geq d_n$ has a graph realisation.

This polynomial time algorithm is called the **Havel-Hakimi** algorithm.

5. **Complement of a Graph.** We define the *complement of a graph* as a graph which has the same vertex set, but with exactly those edges that are absent from the original graph. Formally, if $G = (V, E)$, its complement $\overline{G} = (V, \overline{E})$, such that $\overline{E} = K_V - E$ where $K_V = \{\{a, b\} | a \in V, b \in V, a \neq b\}$.

   Show that if a graph with n vertices is isomorphic to its complement, then $n \equiv 0 \pmod 4$ or $n \equiv 1 \pmod 4$.

   Solution: Suppose the graph $G = (V, E)$ with n vertices has e_1 edges and it's complement graph $\bar{G}$ has e_2 edges. Then,

   $$e_1 + e_2 = \binom{n}{2} = \frac{n(n-1)}{2}$$

   because $(v_1, v_2) \notin E$ iff $(v_1, v_2) \in \bar{E}$ implying all possible combinations of 2 vertices from n vertices is counted exactly once, either in e_1 (edges of G) or in e_2 (edges of $\bar{G}$). Also, 2 isomorphic graphs have the same number of edges implying

   $$e_1 = e_2 = \frac{n(n-1)}{4}$$

   Since the number of edges can only be an integer,

   $$n(n-1) \equiv 0 \pmod 4$$

   For any $n \geq 1$, n and $n-1$ are co-prime to each other because $\gcd(n, n-1) = 1$ using Euclid's algorithm. Hence, either $n \equiv 0 \pmod 4$ or $n - 1 \equiv 0 \pmod 4$.

6. Match each graph on the left with a description of its complement:

   (a) K_4

   (b) C_4

   (c) $K_{1,3}$

   (d) P_4

   (a) A graph with no edges.

   (b) A graph with a single edge.

   (c) A path with two edges.

   (d) A matching with two edges.

   (e) A graph isomorphic to its complement.

   (f) A complete graph.

   (g) A cyclic graph.

   Solution:

   - The complement of K_4 is clearly the empty graph on 4 vertices. So (a) matches with (a).
   - The complement of C_4 is a graph with "opposite" vertices of C_4 now joined together. The graph has four vertices and two disjoint edges, that is, a matching with two edges. (b) matches with (d).
   - The complement of $K_{1,3}$ is an isolated vertex and a cycle on three vertices. (c) matches option (g), that is, the graph is cyclic (a graph is said to be cyclic if it has a cycle).
   - The complement of P_4 is P_4 again! Therefore (d) matches only (e).

7. **What is Wrong With this Proof?**

   Claim: If every vertex in a graph has degree at least 1, then the graph is connected.

   Proof. We use induction. Let $P(n)$ be the proposition that if every vertex in an n-vertex graph has degree at least 1, then the graph is connected.

   Base case: There is only one graph with a single vertex and it has degree 0. Therefore, $P(1)$ is vacuously true.

   Inductive step: We must show that $P(n)$ implies $P(n+1)$ for all $n \geq 1$.

   Consider an n-vertex graph G in which every vertex has degree at least 1. By the induction hypothesis, G is connected; that is, there is a path between every pair of vertices. Now we add one more vertex x to G to obtain an $(n+1)$-vertex graph H. Since x must have degree at least one, there is an edge from x to some other vertex; call it y. Since y is connected to every other node in the graph, x will be connected to every other node in the graph. QED

- ☐ A. The proof needs to consider base case $n = 2$.
- ☐ B. The proof needs to use strong induction.
- ☐ C. The proof should instead induct on the degree of each node.
- ☐ D. The proof only considers $(n+1)$ node graphs with minimum degree 1 from which deleting a vertex gives a graph with minimum degree 1.
- ☐ E. The proof only considers n node graphs with minimum degree 1 to which adding a vertex with non-zero degree gives a graph with minimum degree 1.
- ☐ F. This is a trick question. There is nothing wrong with the proof!

Solution: Let us analyse each step carefully. $P(1)$ is true, so the base case of $n = 1$ is not wrong as such. Also, even if we consider the base case $n = 2$, the only graph with some vertex of degree at least 1 is the graph where the vertices are connected to each other, in which case the claim is true too. So the base case is probably not the problem.

The next two options also do not seem right; the fallacy in the proof has nothing to do with what should have been done in the proof itself.

Finally, option (F) is certainly wrong; there are graphs with smallest degree at least one, such that the graph is disconnected.

Here is the problem in the proof. When we want to show something to be true for $n + 1$, we must take an **arbitrary** graph G on $n+1$ vertices, because we want to show that the statement holds for all graphs on $n+1$ vertices. The proof given, however, starts with a graph on n vertices with minimum degree 1, and then adds a vertex to G to get a graph H on $n + 1$ vertices.

More rigorously, the only type of $n + 1$ node graphs considered are those that can be formed by adding a vertex to an n node graph with least degree 1. Consider the graph on 4 vertices which is isomorphic to the complement of C_4. This graph H is a matching on two edges, and has minimum degree 1. However, there exists no graph G on n vertices with minimum degree 1 to which a vertex can be added to form H.

So the true issue is option (D). The issue is not in considering n node graphs of other type. Even if you consider all graphs on n vertices, it does not quite solve the issue. Instead, the issue is not starting with an arbitrary $n + 1$ node graph.

8. **Prove using Induction.** Prove that for any positive integer n, for any triangle-free graph $G = (V, E)$ with $|V| = 2n$, it must be the case that $|E| \leq n^2$.

   Solution: Use weak induction on n to prove this. For $n = 1$, $V = \{1, 2\}$ and hence there can be at most one edge in G. Thus, $|E| \leq 1 = n^2$. Assume that for a positive integer $n = k > 1$, for any triangle-free graph $G = (V, E)$ with $|V| = 2k$, $|E| \leq k^2$. We need to prove that the same holds for $n = k + 1$.

   Given a triangle-free graph $G = (V, E)$ such that $|V| = 2k + 2$. Consider a pair of adjacent vertices $i, j \in V$ (if there are no such i, j, then the problem is trivially true). Consider the subgraph $G^{'}$ obtained by removing i, j and all edges incident on these 2 vertices from G. $G^{'}$ is also triangle-free because $G^{'}$ is itself an induced subgraph of G implying that if $G^{'}$ had a induced subgraph isomorphic to a triangle then G should also have this induced subgraph. Note that $|V^{'}| = 2k$.

   Using the inductive hypothesis, $|E^{'}| \leq k^2$. Now, since i and j are adjacent, and the graph G is triangle-free, therefore no vertex l in G' can be adjacent to both i and j because if that is the case then i, j and l will give rise to an induced subgraph isomorphic to a triangle. Therefore, the maximum number of edges added to $G^{'}$ in order to add i, j are $2k + 1$ (there is 1 edge between i and j and more than $2k$ vertices in $G^{'}$ linked to either of i or j by an edge would imply that there is a vertex linked to both via pigeonhole principle). Therefore, $|E| \leq k^2 + (2k + 1) = (k + 1)^2$.

9. **Walks and Paths.** In this problem, you shall prove that for any graph G and any two nodes a and b in G, if there is a walk from a to b, then there is a path from a to b.

(a) Prove this using strong induction. Induct on the length of the walk. **Solution:** We strong induct on the length l of the walk. If $l = 1$, then the walk is simply an edge from a to b, so we are done.
Suppose the statement is true for all naturals less than or equal to l, where $l \geq 1$. Consider, now, a walk of length $l+1$. If this walk has no repeated vertices, then it is also a path, so we are done. Otherwise, the walk $v_0v_1 \cdots v_lv_{l+1}$, where $a = v_0$ and $b = v_{l+1}$, has some vertex occurring at least once. Suppose $i < j$ and $v_i = v_j$. Then, the following is also a walk: $v_0v_1 \cdots v_iv_{j+1} \cdots v_{l+1}$. This walk from a to b has length $l + 1 - (j - i) < l + 1$. By strong induction hypothesis, there is a path from a to b, and we are done.

(b) Prove this using the well-ordering principle, and by proving a stronger statement: A shortest walk from a to b is a path from a to b. **Solution:** Let W defined as $a = v_0, v_1, \cdots, v_k = b$ be a shortest walk from a to b of length k. Suppose W is not a path. Then there exist indices $0 \leq i < j \leq k$ such that $v_i = v_j$. Then, the truncated sequence $v_0, v_1, \cdots, v_i, v_{j+1}, \cdots v_k$ is also a walk W' of length $k - (j - i) < k$, contradicting the choice of W. Therefore, W is a path.

Now, suppose there is a walk from a to b. By well-ordering on naturals, there is a walk of minimum possible length. This walk is a path from a to b, as required.

10. **Connectivity and Cycles.** Show that if a graph has a cycle, then deleting any edge in that cycle results in a graph which has the same connectivity relation (i.e., if there is a walk from u to v before deleting the edge, then after deleting the edge too there is such a walk).

Solution: Let $C = u_1u_2 \cdots u_k$ be a cycle of length $k \geq 3$ in a graph G. Without any loss of generality, suppose the edge removed from the cycle is u_1u_k; call this new graph G'. We want to show that any $v, w \in V(G) = V(G')$ are connected in G if and only if they are connected in G'.

Suppose v and w are connected in G', and let P be a path from v to w in G'. This path P is clearly a path in G as well, so v and w are connected in G as well.

Now suppose v and w are connected in G; let P be a path from v to w. If this path does not use the edge u_1u_n, then P is present in G' too. This would mean v and w are connected in G as well. Otherwise, suppose P does use u_1u_n as an edge. Replace the edge u_1u_n in P by $u_1u_2 \cdots u_n$. This new trail is a walk W from v to w not using the edge u_1u_n. This means W is a walk in G' as well, so v and w are connected in G'.

11. Show that any two *maximum* length paths in a connected graph should have a common vertex.

Hint: Consider a shortest path that connects the two paths.

Solution: Consider 2 maximum length paths P_1 and P_2 of length k in G. WLOG we can label these paths as $u_1u_2...u_{k+1}$ and $v_1v_2...v_{k+1}$. Also, for the sake of contradiction assume that these paths have no common vertex. Since the graph is connected, there must be a shortest path $P = u_i...v_j$ that connects the 2 paths P_1 and P_2 in G (since the graph is connected). It can be seen that P has no vertex in common with P_1 apart from u_i because in that case we can get a shorter path connecting P_1 and P_2. Similarly, P has no vertex in common with P_2 apart from v_j. Also, WLOG we can assume that $i \leq j$. Now consider the path $P^{'} = v_1...v_j...u_i...u_{k+1}$ taken from P_2, P and P_1 respectively. Since $i \leq j$, $k - i \geq k - j$ which implies that length of $P^{'}$ is at least $k + 1$ which is contradiction.

12. **Triangle-Free and Claw-Free Graphs.** Recall that an *induced subgraph* of G is obtained by removing zero or more vertices of G as well as all the edges incident on the removed vertices. (No further edges can be removed.) Formally, $G' = (V', E')$ is an induced subgraph of $G = (V, E)$ if $V' \subseteq V$ and $E' = \{\{a, b\} \mid a \in V', b \in V', \{a, b\} \in E\}$.

A graph G is said to be *H-free* if no induced subgraph of G is isomorphic to H. For example, $G = (V, E)$ is K_3-free (or triangle free) if and only if there are no three distinct vertices a, b, c in V such that $\{\{a, b\}, \{b, c\}, \{c, a\}\} \subseteq E$.

Prove that the complement of a K_3-free graph is a $K_{1,3}$-free graph.[1]

Hint: Prove the contrapositive.

Solution: The contrapositive of the above statement is that if a graph G has $K_{1,3}$ as an induced subgraph then it's complement graph $\bar{G}$ will have K_3 as an induced subgraph. To prove this, assume that the input graph G has $K_{1,3}$ as

[1]The graph $K_{1,3}$ is often called the "claw" graph. So this problem can be restated as asking you to prove that the complement of a triangle-free graph is a claw-free graph.

an induced subgraph. Consider this subgraph i.e. $V^{'} = \{v_1, v_2, v_3, v_4\}$ with $E^{'} = \{(v_1, v_2), (v_1, v_3), (v_1, v_4)\}$ without loss of generality. This implies that $(v_2, v_3), (v_2, v_4), (v_3, v_4) \notin E^{'}$ and hence not contained in E because this is an induced subgraph implying that all edges present in G between the vertices of the subgraph are also present in the subgraph. Therefore, $(v_2, v_3), (v_2, v_4), (v_3, v_4) \in \bar{E}$ and hence the induced subgraph of $\bar{G}$ with $\bar{V}^{'} = \{v_2, v_3, v_4\}$ is isomorphic to K_3.

13. If a graph G has chromatic number $k > 1$, prove that its vertex set can be partitioned into two nonempty sets V_1 and V_2, such that

$$\chi(G(V_1)) + \chi(G(V_2)) = k$$

where $G(V_1)$ denotes the induced subgraph of G with vertex set V_1.

Solution: Let $C : V \to [k]$ be a proper colouring of G. Note that C is onto, otherwise G would have a smaller chromatic number than k.
Let V_1 be the set of vertices v for which $C(v) = 1$. Let V_2 be all other vertices. Note that V_1 and V_2 are non-empty, because C is onto and $k > 1$.

Now, the chromatic number of $G(V_1)$ is at most (and hence exactly) 1, because the colouring C for G also acts as a proper colouring for $G(V_1)$, and the only colour used for the vertices of V_1 is the colour 1. Similarly, the chromatic number of $G(V_2)$ is at most $k - 1$. Suppose now that V_2 has chromatic number k', say. Let $C' : V_2 \to [k']$ be an onto proper colouring of $G(V_2)$. Consider the following colouring $C : V \to [k' + 1]$ for G; $C(v) = C'(v)$ for all $v \in V_2$, and $C(v) = k' + 1$ for all $v \in V_1$. It is easy to show that C is a proper colouring for G. Also note that every colour in $[k' + 1]$ is used for V. Therefore, we have $k' + 1 \geq k$, so $k' \geq k - 1$. This, along with the previous observation, proves that $k' = k - 1$, so

$$\chi(G(V_1)) + \chi(G(V_2)) = k$$

as required.

14. The union of 2 graphs on the same vertex set $G_1 = (V, E_1)$ and $G_2 = (V, E_2)$ is defined as $(V, E_1 \cup E_2)$. Prove that the chromatic number of the union of G_1 and G_2 is at most $\chi(G_1)\chi(G_2)$.

Solution: Let $C_1 : V \to \{1, 2, ..., \chi(G_1)\}$ be a proper coloring of G_1 and $C_2 : V \to \{1, 2, ..., \chi(G_2)\}$ be a proper coloring of G_2. Consider the coloring $C : V \to \{1, 2, ..., \chi(G_1)\} \times \{1, 2, ..., \chi(G_2)\}$ given by $C(v) = (C_1(v), C_2(v))$. Consider a pair of vertices $i, j \in V$ such that $C(i) = C(j)$ which can also be written as $(C_1(i), C_2(i)) = (C_1(j), C_2(j))$. This implies that $C_1(i) = C_1(j)$ and $C_2(i) = C_2(j)$. Since C_1 is a proper coloring of G_1, we can say that $(i, j) \notin E_1$ because i and j have the same color w.r.t C_1 and similarly we can say that $(i, j) \notin E_2$. Hence, $(i, j) \notin E_1 \cup E_2$. Thus, C is a proper coloring of $G_1 \cup G_2$ with at most $\chi(G_1)\chi(G_2)$ many colors.

Problem Set 7b

Released: November 1, 2021

1. **Matching Number.** For a graph G, its *matching number* is the size of a maximum matching in G. For each of the following graphs, compute its matching number: C_5, K_5, W_5, $K_{4,5}$.

   Solution: Suppose a graph G has n vertices. Clearly, the number of independent edges cannot exceed $\frac{n}{2}$; if there are $> \frac{n}{2}$ edges, then by pigeonhole principle, some two of them share a vertex. Therefore the matching number of a graph cannot exceed $\frac{n}{2}$.

   Consider C_5. The matching number cannot exceed 2. Also, if the graph can be written as $v_1v_2v_3v_4v_5$, then the set $\{v_1v_2, v_4v_5\}$ forms an independent set. Therefore the matching number of C_5 is 2. Also, it can be shown that the matching number of C_n is $\lfloor \frac{n}{2} \rfloor$.

   The matching number for K_5 is 2 again; the same subgraph mentioned for C_5 works here too. Also, it can be shown that the matching number of K_n is $\lfloor \frac{n}{2} \rfloor$.

   W_5 is the wheel graph on 6 vertices. The matching number for W_5 is at most 3. Now, if the cycle in W_5 is $v_1v_2 \cdots v_5$, and the central vertex is x, Then $\{xv_1, v_2v_3, v_4v_5\}$ is an independent edge set. So the matching number of W_5 is 3. More generally, W_n, the wheel graph with $n+1$ vertices, has matching number $\lfloor \frac{n+1}{2} \rfloor$.

   Let the 2 vertex sets of $K_{4,5}$ be V_1 and V_2 such that $|V_1| = 4$ and $|V_2| = 5$. We start off by noting that the matching number cannot exceed 4. Now, if the vertices in V_1 are $\{a_1, a_2, a_3, a_4\}$ and the vertices in V_2 are $\{b_1, b_2, b_3, b_4, b_5\}$, then $\{a_1b_1, a_2b_2, a_3b_3, a_4b_4\}$ forms a valid independent edge set. Therefore 4 is the matching number of $K_{4,5}$. In fact, it is easy to show that the matching number of $K_{m,n}$ is $\min(m, n)$.

2. How many different perfect matchings exist in each of the following graphs.

   (a) C_{2n}

   (b) $K_{n,n}$

   (c) K_{2n} *Hint: Any ordering of the $2n$ vertices as $v_1, v_2, \ldots, v_{2n-1}, v_{2n}$ can be interpreted as describing a matching, consisting of all edges of the form $\{v_{2i-1}, v_{2i}\}$. Account for the number of different orderings which result in the same matching.*

   (d) W_{2n-1}

   Solution:

   (a) Pick a vertex v in the cycle. It can be matched to either of its two neighbours. Once this matching is determined, the remaining $2n-2$ vertices form a path, and there is only one possible perfect matching. So the answer to the problem is 2.

   (b) If the vertices in the two partite sets U and V are $u_1, u_2, \cdots, u_n$ and $v_1, v_2, \cdots, v_n$, then any matching corresponds to a permutation σ of the first n elements, where the matching has edges of the form $\{u_i, v_{\sigma(i)}\}$. Conversely, any such permutation σ yields a perfect matching. Therefore, the number of perfect matchings in $K_{n,n}$ is $n!$.

   (c) Suppose we order the $2n$ vertices in some manner; say $v_1, v_2, \cdots, v_{2n-1}, v_{2n}$. Any such ordering acts as a description of a matching $\{v_1, v_2\}, \{v_3, v_4\}, \cdots, \{v_{2n-1}, v_{2n}\}$. This should give $(2n)!$ matchings. However, any matching might be counted multiple times in this scheme.

   More precisely, if we change the ordering among v_{2i-1} and v_{2i}, the matching remains the same. For example, if $n = 3$, then $v_1, v_2, v_3, v_4, v_5, v_6$ and $v_1, v_2, v_4, v_3, v_6, v_5$ both yield the same matching. Furthermore, if we permute the vertices such that the n pairs $\{v_{2i-1}, v_{2i}\}$ remain the same, even then the matching remains the same. For example, $v_1, v_2, v_3, v_4, v_5, v_6$ and $v_3, v_4, v_5, v_6, v_1, v_2$ yield the same matching. In all, the matching remains same by either a permutation of the n sets $\{v_{2i-1}, v_{2i}\}$, or by a permutation within each 2-element set $\{v_{2i-1}, v_{2i}\}$. Therefore, the answer is $\frac{(2n)!}{2^n \cdot n!}$.

   (d) The vertex in the centre can be matched to any of the other $2n-1$ vertices. Once this is decided, there is a path left, which has a unique perfect matching. Therefore, the number of matchings of W_{2n-1} is $2n-1$.

3. A pack of $m \times n$ cards with m *values* and n *colours* consists of one card of each value and colour. The cards are arranged in an array with n rows and m columns, such that no two cards in a column have the same colour. Then, show that there exists a set of m cards, one in each column, such that they all have distinct values.

   Solution: Consider any arrangement of mn cards into n rows, m columns with no two colours in the same column. Since, the total number of distinct colours in the cards is n, every column of the arrangement must contain all the distinct n colours. Otherwise, by PHP, there will be at least two cards with same colour, which is a contradiction. Now, consider cards in the arrangement with a particular colour, say c. Since, there are m cards with this colour and exactly one card of this colour in a column, it follows that they are all in different columns. Also, since all these cards have the same colour c, they must have different values. Thus the desired set of cards exists.

4. A *doubly stochastic matrix* is a square matrix with non-negative real numbers such that the entries in each row adds up to 1, as does the entries in each column. A *permutation matrix* is a square matrix in which each row and each column has a single entry that is *equal to* 1, and all the other entries are 0. Show that any doubly stochastic matrix M can be written as $M = p_1Q_1 + \ldots p_tQ_t$, where $Q_1, \ldots, Q_t$ are permutation matrices and $p_1, \ldots, p_t$ are positive real numbers that add up to 1.

   Hint: It is enough to show that $M = \sum_i p_iQ_i$ for some positive real numbers p_i and permutation matrices Q_i. (Argue separately that $\sum_{i=1}^{t} p_t = 1$ must hold.) A special case of this problem was solved in the lecture, when M was the adjacency matrix of a d-regular bipartite graph (scaled by $1/d$, to make it doubly stochastic). Here, use induction on the number of positive entries in M. As base case, consider an $n \times n$ doubly stochastic matrix with exactly n non-zero entries.

   Solution: We induct on the number of non-zero entries in the doubly stochastic matrix. Note that if the number of non-zero entries is less than n, then some row has no non-zero entry. This would mean that the common sum of the matrix is 0, so all entries of the matrix are 0, which is a contradiction. So we assume that the number of non-zero entries in the matrix is at least n.

   For any doubly-stochastic $n \times n$ matrix M, define the bipartite graph $G_M = (R, C, E)$ where $R = \{r_1, \cdots, r_n\}$, $C = \{c_1, \cdots, c_n\}$ (formally, we may let $R = \{0\} \times [n]$, $C = \{1\} \times [n]$, $r_i = (0, i)$ and $c_j = (1, j)$) and $E = \{\{r_i, c_j\} \mid M_{ij} > 0\}$.

   Claim: For any doubly stochastic matrix M, the graph G_M has a perfect matching.

   Proof: We shall use Hall's theorem to prove that there is a perfect matching in $G_M = (R, C, E)$. Consider any $S \subset R$, and let $T = \Gamma(S)$. We claim that $|T| \geq |S|$.

   Now, let us count the sum of entries $W = \sum_{r_i \in S, c_j \in T} M_{ij}$ in two different ways. Firstly,

$$W = \sum_{r_i \in S, c_j \in C} M_{ij} = |S|$$

   where the first equality follows from the fact that if $c_j \notin T = \Gamma(S)$ then in particular, $\{r_i, c_j\} \notin E$ and hence $M_{ij} = 0$; the second equality follows from stochasticity (specifically, for all r_i, $\sum_{c_j \in C} M_{ij} = 1$).

   On the other hand

$$W \leq \sum_{r_i \in R, c_j \in T} M_{ij} = |T|$$

   where the inequality holds because $S \subseteq R$ and the equality follows from stochasticity. Putting these together, $|S| = W \leq |\Gamma(S)|$, as required. Hence G_M has a perfect matching, as claimed.

   Let us go back to the original question. We wanted to proceed via (strong) induction.

   Base Case: The number of non-zero entries in M is n.

   Clearly, no row and no column has all entries zero, as the common sum is 1. Therefore, each row and each column has exactly one non-zero entry, so M itself is a permutation matrix.

   Induction Step: Let M be a doubly-stochastic matrix with $k > n$ non-zero entries. From the claim, G_M has a perfect matching. This perfect matching corresponds to n entries in M, none of which share a row or a column. Suppose the smallest of these n entries is p. Consider the permutation matrix Q, which has a 1 as an entry wherever these n entries in M reside. Then, the matrix $M - pQ$ has the following properties:

   - All entries of $M - pQ$ are non-negative.
   - The sum of each row and each column of $M - pQ$ is $1 - p$.
   - $M - pQ$ has at least one less non-zero entry than M. This is because p was the smallest entry among the n entries we considered, so $M - pQ$ has a 0 in its place.

If $p = 1$, then we are already done, as then $M = Q$. Otherwise, Consider the doubly stochastic matrix $M' = \frac{M - pQ}{1-p}$, which has at least one non-zero entry less than M. By induction hypothesis,

$$M' = \sum_{i=1}^{t} p_i Q_i$$

for positive reals p_i and permutation matrices Q_i. But then

$$M = pQ + \sum_{i=1}^{t} p_i (1-p) Q_i$$

is also of the required form, because $p > 0$, $p_i(1-p) > 0$ for all i, and

$$p + \sum_{i=1}^{t} p_i (1-p) = p + (1-p) \sum_{i=1}^{t} p_i = p + (1-p) = 1$$

This ends the proof.

5. Let $G = (X, Y, E)$ be a bipartite graph such that $\deg(x) \geq 1 \; \forall \; x \in X$ and $\deg(x) \geq \deg(y) \; \forall \; (x, y) \in E$ where $x \in X$ and $y \in Y$. Show that G has a complete matching from X into Y.

Solution: To every edge $e = \{x, y\}$ in the graph, we assign it a weight $\frac{1}{\deg(x)}$. Consider any subset S of X. We verify Hall's condition on the problem by counting the sum, W, of the weights of the edges across S and $\Gamma(S)$.

To start with, every $x \in S$ has all neighbours in $\Gamma(S)$, by definition of neighbourhood. Therefore

$$\begin{aligned}
W &= \sum_{x \in S, y \in \Gamma(S)} \frac{1}{\deg(x)} \\
&= \sum_{x \in S} \; \sum_{y \in \Gamma(S), xy \in E(G)} \frac{1}{\deg(x)} \\
&= \sum_{x \in S} \; \sum_{xy \in E(G)} \frac{1}{\deg(x)} \\
&= \sum_{x \in S} \deg(x) \cdot \frac{1}{\deg(x)} \\
&= \sum_{x \in S} 1 \\
&= |S|
\end{aligned}$$

On the other hand, it is also true that

$$\begin{aligned}
W &= \sum_{x \in S, y \in \Gamma(S)} \frac{1}{\deg(x)} \\
&= \sum_{y \in \Gamma(S)} \; \sum_{x \in S, xy \in E(G)} \frac{1}{\deg(x)} \\
&\leq \sum_{y \in \Gamma(S)} \; \sum_{xy \in E(G)} \frac{1}{\deg(x)} \\
&\leq \sum_{y \in \Gamma(S)} \; \sum_{xy \in E(G)} \frac{1}{\deg(y)} \\
&= \sum_{y \in \Gamma(S)} \deg(y) \cdot \frac{1}{\deg(y)} \\
&= \sum_{y \in \Gamma(S)} 1 \\
&= |\Gamma(S)|
\end{aligned}$$

Therefore $|S| \leq |\Gamma(S)|$ for all $S \subseteq X$. By Hall's Theorem, there is a complete matching in G from X to Y.

6. Suppose that $G = (X, Y, E)$ is a bipartite graph. For each $S \subseteq X$, define $\text{shrinkage}(S) = \max\{0, |S| - |\Gamma(S)|\}$. Show that the the size of the largest subset of X which has a complete matching into Y is $|X| - \max_{S \subseteq X} \text{shrinkage}(S)$.

Hint: Hall's theorem is a special case when $\text{shrinkage}(S) = 0$ *for all* $S \subseteq X$*. To prove the above general formulation, if the largest subset of* X *which has a complete matching is of size* $|X| - t$*, consider applying Hall's theorem to a larger graph formed by adding* t *new vertices to* Y *which are all connected to every vertex in* X*.*

Solution: Call the maximum among all shrinkages to be the *deficit* d, that is, define

$$d = \max_{S \subseteq X} \text{shrinkage}(S)$$

This means that for every $S \subseteq X$, $|\Gamma(S)| \geq |S| - d$, by definition.

First, we show that there exists a subset of X which has a complete matching into Y with size at least $|X| - d$. For this, consider a new bipartite graph G', that adds d new vertices to Y. Each of these d new vertices is connected to every vertex in X. In this new graph G', it is easy to see that for any $S \subseteq X$, we have

$$|\Gamma_{G'}(S)| = |\Gamma_G(S)| + d \geq (|S| - d) + d = |S|$$

where we add indices G and G' to avoid confusion. By Hall's Theorem, G' has a matching that saturates all vertices of X. In this matching, remove the edges that are joined to any of the d new vertices added. This gives a matching in G of size at least $|X| - d$, as required.

Now, we show that $|X| - d$ is the best we can do. Assume the contrary, that is, suppose the maximum matching has size $|X| - k$ for some $k < d$, and this subset of X belonging to this matching is X'. Now, let S be any subset of X. Write S as $S = (S \cap X') \cup (S - X')$; note that this is a disjoint union. Now, every vertex in $S \cup X'$ is in X', so it has a corresponding matching vertex in Y from the maximum matching. Also, $|S - X'|$ cannot exceed k, because X' has $|X| - k$ elements. Therefore,

$$|\Gamma(S)| \geq |\Gamma(S \cap X')| \geq |S \cap X'| = |S| - |S - X'| \geq |S| - k$$

which means that the deficit is at most $k < d$, a contradiction.

7. Let $G = (X, Y, E)$ be a bipartite graph. Suppose that $S \subseteq X$, $T \subseteq Y$ such that G has a complete matching from S to Y, and also has a complete matching from T to X. Prove that there exists a matching which contains a complete matching from S to Y as well as a complete matching from T to X.

Hint: Start with an arbitrary complete matching from T *to* X*. Can you extend this to a matching which contains a complete matching from* S *to* Y*?*

Solution: Let M_1, M_2 be arbitrary complete matchings from S to Y, T to X respectively. Consider the edges in the graph $G' = M_1 \cup M_2$. Since, each vertex has a degree atmost 1 in either of M_1, M_2, each vertex has a degree of 2 in G'. Now, we will find a matching M in G' covering each vertex in $S \cup T$. It can been seen that if such a matching exists then it contains the required matchings.

Since, each vertex has atmost degree 2 in G', we conclude that G' can be a collection of isolated vertices, isolated edges, cycles or chains and has no other configuration of edges. Let v be any vertex in $S \cup T$. Clearly, it has at least degree 1 in G'. Consider the sub graph of G' containing v. If it is an isolated edge, including it in M covers v. If it is a cycle, it has be an even cycle (as G' is bipartite). Thus, taking alternating edges of the cycle in M cover all the vertices in the sub graph and also v. Similar subgraphs can be constructed for odd-length (edge-wise) chains by taking alternating edges.

The only case where we can't assign an edge is when the sub graph containing v is an even-length chain with both the end points belonging to $S \cup P$. We claim that this can't happen and prove this by contradiction. Suppose, there is a connected-component of G' which is an $2n$ even-length chain $a, c_0, c_1, ..., c_{2*n-2}, b$ with a, b belonging to $S \cup T$. W.l.g, let $a \in S$. Then, the path from a to b must be an alternating sequence between M_1, M_2 starting with M_1 from a and ending with M_2 at b. Since, it is of even length, a, b will be on same bipartite set, hence, $b \in S$. Thus, there will be an edge in M_1 covering b, but this can't be the edge ending in the path as then, two edges from M_1 would have a common vertex, which is a contradiction. Thus, in all cases, we can find a matching M from X to Y , which contains all vertices from $S \cup T$. Hence, proved.

8. Given a graph $G = (V, E)$, its *line graph* (or "edge graph") $L(G)$ is defined as the graph whose vertices are the edges of G, and two such vertices are connected if they share a vertex in G. That is, $L(G) = (E, E')$, where $E' = \{\{e_1, e_2\} \mid e_1, e_2 \in E,\ e_1 \cap e_2 \neq \emptyset\}$.

(a) Describe $L(C_n)$ and $L(K_{1,n})$. What is $L(C_3)$ and $L(K_{1,3})$?

Solution: We can see that $L(C_n)$ is C_n. $L(K_{1,n})$ is K_n. Thus, $L(C_3)$ is triangle C_3 and $L(K_{1,3})$ is also a triangle $K_3 (= C_3)$.

(b) Show that if G is a d-regular bipartite graph, then $L(G)$ has a d-colouring.

Hint: Argue that a colouring of $L(G)$ corresponds to a partition of G into matchings.

Solution: Let G be a d-regular bipartite graph with sets (A, B, E). We know, by repeated applications of Hall's theorem, that E is comprised of d disjoint perfect matching from A to B.
Now, every disjoint set of edges in G corresponds to an independent vertex set in $L(G)$. This is because, if the corresponding vertices in $L(G)$ have an edge in between then the edges must have common vertex, which is a contradiction. Thus, each of d-disjoint perfect matching in G forms an independent vertex set. Since, the perfect matchings cover the entire edge-set, these d-independent vertex sets form a vertex cover. Now, colouring each independent vertex set with a distinct colour gives a valid colouring of $L(G)$. Hence, $L(G)$ has a d-colouring.

(c) Show that the size of the largest matching in G is the same as the size of the largest independent set in $L(G)$.

Solution: From above, we see that disjoint set of edges in G corresponds to an independent set in $L(G)$. By similar reasoning, we have that every independent set in $L(G)$ corresponds to a disjoint set of edges in $L(G)$. Since, every disjoint set of edges in G is a matching, we have that the largest matching in G corresponds to the largest independent set in $L(G)$. Hence, they have same size.

(d) Given the above problem, one may wonder if algorithms for finding the size of the largest matching in a graph can be used to find the size of the largest independent sets in graphs. Unfortunately, this does not always work. (Indeed, finding the size of the largest matching is an "easy" problem, while finding the size of the largest independent set is a "hard" problem.) In particular, there are graphs which are not line graphs for any graph. Show that $K_{1,3}$ (the "claw graph") is not the line graph of any graph.

Solution: Denote the vertices of $K_{1,3}$ as v_1, v_2, v_3, v_4, with degree of $v_1 = 3$. Suppose, G is a graph whose line graph is $K_{1,3}$. Let e_1, e_2, e_3, e_4 be their corresponding edges in G. Then, by edges in $K_{1,3}$, we must have that, e_1 is adjacent to each of e_2, e_3, e_4 and none of them are adjacent to each other. Since, e_1 has only two end-points, by PHP, two of $e_i, i \geq 2$ must have a common end point, which is a contradiction. Thus, $K_{1,3}$ isn't a line graph for any graph.

9. In a graph, if every vertex has degree at least 2, then it must have a cycle (as it has no leaves). Show that if every vertex has degree at least 3, then it must have a cycle of even length.

Hint: Consider a maximal path.

Solution: Let $G = (V, E)$ be a graph with $\deg(v) \geq 3 \; \forall v \in V$. Consider a maximal path in G and call it $P = v_0 v_1 ... v_k$. Clearly, v_1 is a neighbour of v_0 in G because they are consecutive vertices in a path. Consider 2 more neighbours of v_0 - v_i and v_j for $i < j$ (WLOG). It can be seen that both v_i and v_j must be part of P because otherwise we could extend the path.

Consider the cycle $v_0 v_i ... v_j v_0$ where the path from v_i to v_j is obtained from P. If this cycle has even length, then we have proved the claim. If not, we have proved that the path between v_i and v_j in P has odd length. Now consider the cycle $v_1 ... v_i v_0 v_1$. If this cycle has odd length, then we have proved that the path from v_1 to v_i in P is of odd length. From the above 2 results, it is easy to see that the path from v_1 to v_j in P must be of even length. Then the cycle $v_1 ... v_j v_0 v_1$ must be of even length.

10. **An application of Kőnig's theorem.**

(a) Show that every bipartite graph with m edges and maximum degree d has a matching of size at least m/d.

Solution: Consider any subset of vertices S in $G = (V, E)$. Let $E(S) = \{(u, v) | (u, v) \in E \text{ and } u \in S \text{ or } v \in S\}$. Since maximum degree of any vertex is d, it implies that the maximum number of edges of G that can be covered by S are $d|S|$ implying that $|E(S)| \leq d|S|$. If S was a vertex cover, it should cover all edges in G thus implying that $|E(S)| = m$. Hence, $m \leq d|S|$ if S is a vertex cover of G implying that the size of the vertex cover must be at least m/d. From Kőnig's theorem, the size of the maximum matching is same as the size of the minimum vertex cover implying that the maximum matching will have size at least m/d.

(b) Show that a bipartite graph (X, Y, E) with $|X| = |Y| = n$ and $|E| > n(k-1)$ should have a matching of size at least k.

Hint: Use the previous part.

Solution: Apply the above result with $m = n(k-1)+1$ and $d = n$.

11. Give an alternate proof for Hall's Theorem, using Kőnig's theorem.

(In class, we proved Kőnig's theorem using Hall's theorem; so this may appear to be circular reasoning. But it is possible to prove Kőnig's theorem directly, by induction.)

Hint: If a bipartite graph $G = (X, Y, E)$ does not have a complete matching from X to Y, the largest matching has size $< |X|$, and hence, by Kőnig, G has a vertex cover C of that size. Can you show that $X - C$ must be shrinking?

Solution: Suppose for contradiction, a bi-partite graph $G = (A, B, E)$ satisfies Hall's condition but doesn't have a complete matching from X to Y. Thus, by Kőnig's theorem, there exists a vertex cover C with $|C| < |X|$. Let C_A, C_B are the vetices of C in A, B respectively. Consider the set $X - C_A$, which is non-empty. Since, $C = C_A \cup C_B$ is the vertex cover, we must have that, every edge incident on $X - C_A$ must be incident on some vertex in C_B. Thus $\tau(X - C_A) \subseteq C_B$ and hence, $|\tau(X - C_A)| < |C_B| \leq |X| - |C_A| \leq |X - C_A|$. Thus, $X - C_A$ is a shrinking set in G, which is a contradiction. Thus, all bi-partite graphs which satisfy the Hall's condition must have a complete matching. Hence, Hall's theorem is true.

12. A maximal matching can be smaller than a maximum matching. In this problem we explore how much smaller it can be.

(a) Show that for any graph G, a maximal matching is at least half as large as a maximum matching. Prove this directly (by contradicting the maximality of a matching which is less than half the size of the maximum matching), and then repeat the proof using the connections between matchings and vertex cover.

Solution: Suppose $M = \{u_1v_1, \cdots, u_kv_k\}$ is a maximum matching in G. Also, suppose M' is a maximal matching in M of size $k' < k/2$. Consider the set of vertices V' involved in the matching M'. This set has size $|V'| = 2k' < k$, so $|V'| \leq k-1$. Therefore, there exists an index i such that $1 \leq i \leq k$ and neither u_i nor v_i is in V'. But then, adding the edge u_iv_i to M' extends the matching M', contradicting its maximality. Therefore $k' \geq k/2$, as required.

(b) Give examples of graphs which have a maximal matching which is exactly half the size of a maximum matching. Specifically, for any n, describe a connected graph G with $2n$ nodes which has a perfect matching and also a maximal matching of size $\lceil n/2 \rceil$.

Hint: For $n = 2$, consider the "path graph" P_4.

Solution: We distinguish cases for $n = 4k$ and $n = 4k+2$, where k is a natural number (if $n = 2$, just take a P_2). Suppose $n = 4k$ for $k \geq 1$. Here is a formal description of the graph (the graph will be clear once you draw it). Take $4k$ vertices indexed as $u_{i,j}$, where $1 \leq i \leq k$ and $1 \leq j \leq 4$. For each i, join $u_{i,1}$ to $u_{i,2}$, $u_{i,2}$ to $u_{i,3}$, and $u_{i,3}$ to $u_{i,4}$. Also, join $u_{i,2}$ to $u_{i+1,2}$ for all $1 \leq i \leq k-1$. This gives a connected graph G on $4k$ vertices. Note that taking the edges $u_{i,1}u_{i,2}$ for all i and $u_{i,3}u_{i,4}$ for all i gives a perfect matching in G of size $2k$. Also, taking the edges $u_{i,2}u_{i,3}$ for all i gives a maximal matching of size $k = \lceil 2k/2 \rceil$.
The construction for $n = 4k+2$ is similar. Take the graph mentioned above. Now add two new vertices v and w, and join v to w. Also, join v to $u_{n,2}$. Call this graph G. Once again, the edges vw, $u_{i,1}u_{i,2}$ for all i, and $u_{i,3}u_{i,4}$ for all i, give a perfect matching in G of size $2k+1$. Also, the edges vw, and the edges $u_{i,2}u_{i,3}$ for all i, give a maximal matching of size $k+1 = \lceil (2k+1)/2 \rceil$.

(c) What is the size of the smallest maximal matching in C_6? What about in C_n?

Solution: We claim that the smallest maximal matching in C_n has size $\lceil n/3 \rceil$. In particular, the smallest maximal matching in C_6 has size 2. We first show the lower bound, and then construct a maximal matching of that size.

Let the vertices of the graph $C = u_1u_2 \cdots u_n$. Let M' be a maximal matching of C. For notational rigour, we assign a variable $x_i = 1$ if the edge between u_i and u_{i+1} is present in M', and $x_i = 0$ otherwise (here, it is standard to assume that u_{n+1} means u_1). Note that the number of edges in M' is just $x_1 + x_2 + \cdots + x_n$.
Observe that $x_1 + x_2 + x_3 \geq 1$. Indeed, if this is not the case, then neither of u_1, u_2, u_3, u_4 is matched. So adding the edge

u_2u_3 in M' increases the size of the matching, which is a contradiction. Similarly, $x_2+x_3+x_4 \geq 1, \cdots, x_{n-1}+x_n+x_1 \geq 1$, and $x_n + x_1 + x_2 \geq 1$, Adding all these inequalities together, we get

$$3(x_1 + x_2 + \cdots + x_n) \geq n$$

or $x_1 + x_2 + \cdots + x_n \geq n/3$. Therefore M' has at least $n/3$ (and therefore at least $\lceil n/3 \rceil$ edges).

To show this is achieved, we provide a construction. Take the following edges in C: If $n = 3k$, take the edges $u_1u_2, u_4u_5, \cdots, u_{3k-2}u_{3k-1}$. If $n = 3k + 1$ or $n = 3k + 2$, take the edges $u_1u_2, u_4u_5, \cdots, u_{3k-2}u_{3k-1}, u_{3k}u_{3k+1}$.

13. An **edge cover** is a concept closely related to a matching. An edge cover of a graph $G = (V, E)$ is a set of edges such that every vertex in the graph is part of some edge in the set. That is, $L \subseteq E$ is an edge cover if $V = \bigcup_{e \in L} e$.

    (a) What is the condition on a graph $G = (V, E)$ so that E is an edge cover?

    Solution: It is easy to see that E is an edge cover if and only if there are no isolated vertices (with degree 0) in G.

    (b) Suppose $G = (V, E)$ is a graph which has an edge cover. Show that if L is the smallest edge cover for G, then the graph (V, L) is a forest, in which each connected component is a "star graph" – i.e., a tree in which every edge is incident on a leaf.

    Solution: Given that there exists an edge cover for G, let L be the smallest edge cover. We claim that L has no cycles. Because if it is a cycle then removing an edge from this cycle gives a smaller edge cover of G. Also, no edge in L connects two vertices each degree more than 1 in (V, L). Because, if there exists such an edge, dropping it from L still is an edge cover which is smaller. Hence, no edge in (V, L) connects vertices each of degree more than 1.
    From the above two observations on (V, L), we conclude it is a forest with each edge incident on a leaf.

    (c) Suppose G and L are as above. Then describe a matching M in G such that $|M| = |V| - |L|$.

    Hint: How many connected components are there in (V, L)?

    Solution: let k be the number of components in L. Since, it is a forest, it will contain $|V| - k$ edges $= |L|$. Thus, no. of components in $L = k = |V| - |L|$. Now, each component of L contains at least one edge (as G has no isolated vertices). Consider matching M in G as union of arbitrary edges from each component. Since, the components are disjoint, M is a matching. Now, $|M|$ = no. of components in $(V, L) = |V| - |L|$

    (d) Suppose $G = (V, E)$ is a graph which has an edge cover. Also, suppose M is a matching in G. Then show that G has an edge cover L such that $|L| \leq |V| - |M|$.

    Solution: Given a matching M in G with an edge cover. Consider the minimal edge cover set L. We will modify this edge-cover set to L' such that L' is also a forest and contains all edges of M and atmost one edge of M in a component.
    Now, we try to construct such an edge cover L' by modifying L. By (b), L is a forest with every edge on incident on a leaf. For each edge in M, either it is already present in L. In case it is present in L, the component in which it is present has non other edge in M (as each component is a "star"). In case it isn't present, it could be incident with a leaf in L with a non-leaf or between two non-leaves or two leaves. If it is incident between between two non-leaves, include it in L'. If it is incident between a leaf v_f and a non-leaf v_n, remove the connecting edge v_fv_n in L' and remove edge connecting v_f to it's initial component. If the edge connects between two leaves, remove the connecting edges and add this edge to L. If any isolated vertices are formed by these operation, add minimal edges not in M to connect it to some component. This is always possible as, the only edges removed are edges not in M. Because of their minimality, no cycles will formed after their addition hence, L' is still a forest.
    Now the constructed edge cover L' is a forest and every component has atmost one edge from matching M and all edges in M are covered. Hence, no. of components in L' is at least that of size of M. We have $|L'| =$ $|V|$ – no. components in $L' \leq |V| - |M|$. Hence, proved.

    (e) Conclude from the above that if G is a graph which has an edge cover, then the size of a maximum matching and the size of a minimum edge cover add up to the number of nodes in the graph.

    Solution: Let L_{min}, M_{max} are the minimal edge-cover and maximal matching in G. By (c), we have there exists a matching M of size $|V| - |L_{min}|$. Thus, $|M_{max}| \geq |V| - |L_{min}|$.
    By (d), we have by taking M_{max} matching there exists an edge cover L of size $|V| - |M_{max}|$. Thus, $|L_{min}| \leq |V| - |M_{max}| \implies |M_{max}| \leq |V| - |L_{min}|$. Thus, from the inequalities, we conclude that $|M_{max}| = |L_{min}|$.

Problem Set 7c

Released: November 1, 2021

1. Show that a tree has at most one perfect matching.

   Hint: Use induction.

   Solution: We will prove the claim by inducting on the number of vertices n in tree T. For $n \leq 2$, the claim is trivially true because there is at max one edge possible in T and hence one matching. Let us assume that the claim is true for $n \leq k$ where $k \geq 2$. Now consider a tree T with $n = k + 1$ many vertices. Since T has at least 2 vertices, it must have at least 2 leaves. Consider a leaf l and it's neighbour p in T. In a perfect matching of T, l must be mapped to p because that is the only edge that l is a part of. Let us call the subgraph induced by removing l and p from T as F. F is still acylic but may not be connected because other vertices in the subtree of p might have gotten disconnected from the rest of the graph. Therefore, F must be a forest with m many trees $T_1, T_2, ...T_m$ with at most $k-1$ vertices.

   It is easy to see that a perfect matching for T can be obtained by adding edge (l, p) to a perfect matching of F and a perfect matching for F can be obtained by removing the edge (l, p) from a perfect matching for T. Also, a perfect matching for F can only be obtained by combining the perfect matchings of trees $T_1, T_2, ...T_k$. By the induction hypothesis, we can say that each of these trees have at most one perfect matching which implies that the forest F has at most one perfect matching. Thus, T has at most one perfect matching.

2. Show that a tree is a bipartite graph.

   Hint: Consider the distance of each node from a fixed node. The two parts correspond to even and odd distances. Where do you use the fact that the graph is a tree?

   Solution: Consider a node u in G. Let distance(v_1, v_2) denote distance of vertex v_1 from v_2 in G. Now, let's define the following 2 sets -

   $$\text{Odd} = \{\ v \mid v \in V \text{ and distance}(u, v) \text{ is odd}\ \}$$
   $$\text{Even} = \{\ v \mid v \in V \text{ and distance}(u, v) \text{ is even}\ \}$$

   Color the vertices in Odd red and the vertices in Even blue. Color u blue. We need to prove that this is a valid coloring of G. For the sake of contradiction, assume that there is an edge between 2 vertices v_1 and v_2 of the same color. Since these 2 vertices have the same color, they must be at distances d_1 and d_2 from u s.t. $d_2 - d_1$ is even (including 0) or one of v_1 or v_2 must be u. In the second case, it can be shown that distance of the other vertex is 1 from u (because of the edge from v_1 to v_2) which implies that it should have different color from u. In the first case, we can consider the paths P_1 from u to v_1 and P_2 from u to v_2 and then we can get a cycle in the graph by considering $P = u...v_1v_2...u$ by using P_1 and P_2. If no vertex repeats in P, then it is a cycle. Else, the vertex that repeats will give a cycle. Hence, this must represent a valid 2-coloring of the graph which in turn implies that it is a bipartite graph.

3. A *spanning tree* of a graph G is a subgraph G' which has all the nodes in G and is a tree. Show that every connected graph G has a spanning tree.

   Hint: Induct on the number of cycles in G. Use the previous problem.

   Solution: We strong induct on the number of cycles in G.
   Base Case: G has 0 cycles. In this case, G is a tree, so it is its own spanning tree.

   Induction Hypothesis: For a natural number n, it is true that for all $m < n$, if a connected graph has m cycles then it has a spanning tree.

   Induction Step: Suppose G is a spanning tree with n cycles, where n is as above. Since $n \geq 1$, it has at least one cycle C. Let e be an edge of the cycle. Remove this edge e to obtain a graph G'. From the previous problem, G' is connected. Also, G' has strictly less than n cycles, because the cycle C no longer exists. By induction hypothesis, G' has a spanning tree T. Since G' is a subgraph of G with all nodes of G, so T is a spanning tree of G as well. This completes the proof.

4. Prove that for a graph with n vertices, any two of the following imply the third:

(a) G is connected.

(b) G is acyclic.

(c) G has $n-1$ edges.

Solution: (a) & (b) together imply (c): Let G be a connected, acyclic graph with n vertices. We induct on n. If G has only one vertex, then it clearly has $0 = 1-1$ edges, and (c) holds. Otherwise, suppose $n \geq 2$, and the assertion holds for all graphs with less than n vertices. We show first that G has a leaf. Take a maximal path $P = u_1u_2\cdots u_k$ in G. u_1 cannot have a neighbour outside u_is, else P would not be maximal. Also, u_1 cannot have $u_3, u_4, \cdots u_k$ as neighbours, or else a cycle is formed. So u_1 has degree 1, and we found a leaf. So delete u_1 from G. This gives a connected acyclic graph G' on $n-1$ vertices, so this graph G' has $n-2$ edges. Therefore G has $(n-2)+1 = n-1$ edges, as required.

(b) & (c) together imply (a): Let G be an acyclic graph with n vertices and $n-1$ edges. Suppose G has k connected components $G_1, G_2, \cdots, G_k$, with $n_1, n_2, \cdots, n_k$ vertices respectively. Then, each connected component G_i is also acyclic, so from the previous part, G_i has $n_i - 1$ edges. This means G has $(n_1-1)+(n_2-1)+\cdots+(n_k-1) = n-k$ edges, but we know that G has $n-1$ edges. Therefore $k = 1$, so G is connected.

(c) & (a) together imply (b): Let G be a connected graph with n vertices and $n-1$ edges. Suppose G is cyclic. Remove an edge from a cycle; from the previous to previous problem, this new graph G_1 is connected. If G_1 also has a cycle, remove an edge from G_1 to obtain a connected graph G_2, and so on. This process cannot keep going on forever, because the number of cycles strictly decreases every step. Let G' be the final graph obtained. This graph is connected and acyclic, but has strictly less than $n-1$ edges, which contradicts the first part. We infer that our assumption is wrong. Hence, G is acyclic.

5. What is the maximum size of $|S|$ such that there is a poset $(S, \preceq)$ of height h and width w? Construct such a poset.

   Solution: Since the width of the poset is w, by Dilworth's theorem, there is a decomposition into w chains. Since, max. length of chain is h, maximum number of elements in S $= h * w$.

   As an example of a poset which attains the equality, consider, divisibility poset with $S = \cup_{i=0}^{w}\{p_i, p_i^2, .., p_i^h\}$, where $p_i's$ are w prime numbers.

6. Use Dilworth's theorem to show that any set of 5 natural numbers either contains numbers of the form x, xy and xyz, or contains 3 numbers which are mutually indivisible by each other?

   Solution: By Dilworth's theorem, size of largest anti-chain is equal to the smallest chain decomposition in any poset. Given a set of 5 naturals, consider the divisibility poset S on them. If any three of them are mutually indivisible then the required statement is true. Else, the maximal anti-chain in S has size less than or equal to 2. Which means, S can be decomposed into atmost 2 chains. By PHP, since there are 5 numbers in total, in at least of one the chain there must be 3 elements. Since, they form a divisibility chain they must be of the form x, xy, xyz. Hence, the statement is true.