

Introduction to Combinatorics

Lecture Notes

Hung-Lin Fu

Combinatorics is an area of mathematics primarily concerned with **counting** and **certain properties of finite structures**.

- The study of Combinatorics: Combinatorial Theory
- The scope of Combinatorics: Discrete Mathematics and beyond
- The inside of Combinatorics: Applied Algebra (mainly)
- Topics on Combinatorics:
 1. Graph Theory
 2. Design Theory (Combinatorial Designs)
 3. Enumerative Combinatorics
 4. Algebraic Combinatorics
 5. Additive Combinatorics
 6. Combinatorial Geometry
 7. Combinatorial Optimization
 8. Combinatorial Number Theory
 9. Applications of Combinatorics

Finite Structures

\mathbb{X} : A finite non-empty set

\mathbb{B} : A collection of subsets of \mathbb{X} (repeated subsets are allowed)

Incidence matrix A of a finite structure (\mathbb{X}, \mathbb{B}) :

Let $\mathbb{X} = \{x_1, x_2, \dots, x_v\}$ and $\mathbb{B} = \{B_1, B_2, \dots, B_b\}$,

$$A_{\mathbb{X}, \mathbb{B}} = \begin{matrix} & B_1 & B_2 & \cdots & B_b \\ \begin{matrix} x_1 \\ x_2 \\ \vdots \\ x_v \end{matrix} & \left(\begin{matrix} & & & & \\ & & & & \\ & & a_{i,j} & & \\ & & & & \\ & & & & \end{matrix} \right) & \begin{matrix} \\ \\ \\ \\ \end{matrix} & \begin{matrix} \\ \\ \\ \\ \end{matrix} \\ & & & & v \times b \end{matrix}, \text{ where } a_{i,j} = \begin{cases} 1 & \text{if } x_i \in B_j, \\ 0 & \text{otherwise.} \end{cases}$$

(\mathbb{X}, \mathbb{B}) can be viewed as:

1. a graph where \mathbb{X} is the vertex set and \mathbb{B} is the edge set;
2. a design where \mathbb{X} is the set of varieties (elements) and \mathbb{B} is the set of blocks (experiments);
3. a code of length v where each column of $A_{\mathbb{X}, \mathbb{B}}$ is a codeword;
4. pooling design with v test and b items; and more.

Graphs

- Simple graph : $\mathbb{B} \subseteq \binom{\mathbb{X}}{2}$ (a set not a multi-set)
- Multi-graph : $\mathbb{B} \subseteq \binom{\mathbb{X}}{2}$ (with possible repeated elements)
- Hypergraph : $\mathbb{B} \subseteq 2^{\mathbb{X}}$ (repeated elements are possible)
- Random graph : The existence of an edge is of probability $0 \leq p \leq 1$.

(Revised version: $\forall x, y \in \mathbb{X}, \exists p(x, y)$, i.e., each edge has its own probability.)

- Directed graph : $\mathbb{B} \subseteq \mathbb{X} \times \mathbb{X} = \mathbb{X}^2$

Graph Theory

- Study the structure of graphs and its applications.
- Topics on Graph Theory:

1. Subgraphs:

What kind of subgraphs does a graph contain?

2. Chromatic Theory:
Graph colorings.
3. Topological Graph Theory:
Graph embeddings, proper drawing of a graph on surface.
4. Extremal Graph Theory:
The graph of maximum size which forbids a given graph.
If both G and \bar{G} (or G_1, G_2, \dots, G_t with $\bigcup_{i=1}^t E(G_i) = E(G)$) are concerned, we have Ramsey Theory.
5. Random Graph Theory:
Study the structure of random graphs.
6. Algebraic Graph Theory:
Use the adjacency matrices or Laplacians of a graph G .
7. Graph Labelings:
Label the graph (either the vertices or edges) to satisfy given constraints.
(Many topics/ problems can be converted into labeling graph problems.)
8. Digraphs
The most popular topic is Network.
9. Algorithmic Graph Theory:
Graph algorithms are applied to solve graph optimization problems.

Plan of Lectures

1. Cover chapters 1, 2, 3, 4, 5, 32, 33 (in the textbook) for Graph Theory.
2. Cover chapters 10, 13, 14 for Enumerative Combinatorics.
3. Cover chapters 5, 6, 17, 19 for Design Theory.
4. Introduce Additive Combinatorics; Sum sets.
5. Introduce some topics of Combinatorial Optimization.

Textbook: A course in Combinatorics, Van Lint and Wilson.

Contents

Lecture 1: Subgraphs in Simple Graphs	5
Lecture 2: Eulerian Circuits and Hamilton Cycles	12
Lecture 3: Connectivity	18
Lecture 4: Topological Graph Theory	22
Lecture 5: Vertex Coloring	30
Lecture 6: Ramsey Theory	34
Lecture 7: Edge Coloring	40
Lecture 8: An Introduction of Extremal Set Theory	48
Lecture 9: Latin Square	60
Lecture 10: Critical Sets	71
Lecture 11: BIBD with $k = 3$	82
Lecture 12: Principle of Counting	88
Lecture 13: Generating Function	93
Lecture 14: Sum set in Additive Combinatorics	99
Lecture 15: Probabilistic Method (Graphs)	107
Lecture 16: Combinatorial Optimization	113

Subgraphs in Simple Graphs

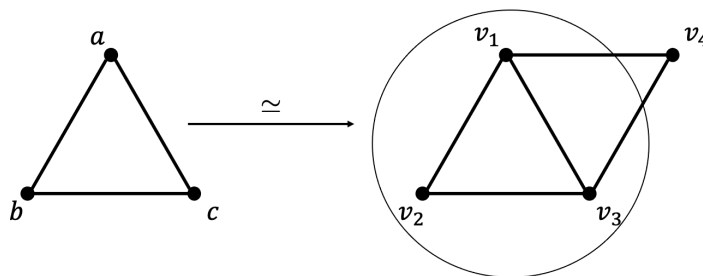
Definition 1.1. A graph G is an ordered pair (V, E) where $V = V(G)$ is the vertex set of G and $E = E(G)$ is the edge set of G .

Definition 1.2. Two vertices u and v in $G(V(G))$ are adjacent, denoted by $u \sim_G v$, if $\{u, v\} = uv$ is an edge of $G(E(G))$ or we say u and v are incident in G . We also say u (and v respectively) is incident to uv .

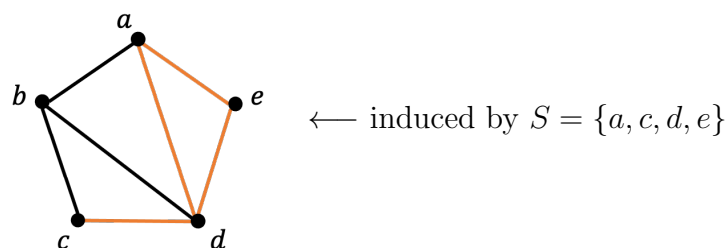
Definition 1.3. Two graphs $G_1 = (V_1, E_1)$ and $G_2 = (V_2, E_2)$ are isomorphic if there exists a bijection φ from V_1 to V_2 such that $u \sim_{G_1} v$ if and only if $\varphi(u) \sim_{G_2} \varphi(v)$, denoted by $G_1 \simeq G_2$.


Definition 1.4. A graph $G' = (V', E')$ is a subgraph of $G = (V, E)$ if $V' \subseteq V$ and $E' \subseteq E$. (Denoted by $G' \leq G$.)

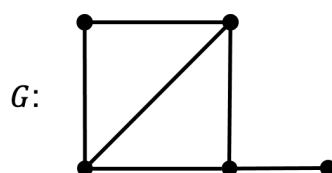
General sense: \tilde{G} is a **subgraph** of G if \tilde{G} is **isomorphic to a subgraph** of G .



Definition 1.5 (Induced subgraph). Let $S \subseteq V(G)$. Then, the subgraph obtained from S and all edges in G which are incident to two vertices of S is called the induced subgraph of G by S , denoted by $\langle S \rangle_G$. (Denoted by $\langle S \rangle_G \preceq G$.)



Remark. A graph may contain a subgraph H but not an induced subgraph H . For example, G contains a subgraph C_4 () but not an induced subgraph C_4 .



Definition 1.6. The set of vertices in G which are incident to a vertex v is called the neighborhood of v , denoted by $N_G(v)$; and $|N_G(v)|$ is known as the degree of v , denoted by $\deg_G(v)$.

Theorem 1.1. For any graph G , $\sum_{v \in V(G)} \deg_G(v)$ is even and the number of vertices with odd degree is also even.

Proof. Each edge contributes two edges. □

Remark. $\sum_{v \in V(G)} \deg_G(v)$ is "known" as the volume of G , which measures how big the graph is.

Definition 1.7. If all degrees of the vertices in G are the same (say k), then G is a regular graph (k -regular). Especially, if k is 3, then we have a cubic graph, and if k is 2, then we have a "2-factor".

Remark.

- The maximum degree (resp. minimum degree) of G is denoted by $\Delta(G)$ (resp. $\delta(G)$). A vertex with the maximum degree is called a major vertex.

- The average degree of G is denoted by $d(G)$.
- $|G|$ is the order of G .
- $\|G\| = |E(G)|$ is the size of G .

Definition 1.8.

- Walk : a sequence of vertices in $V(G)$, $\langle v_1, v_2, \dots, v_m \rangle$, such that for $i = 1, 2, \dots, m - 1$, $v_i v_{i+1} \in E(G)$.
- Path : a walk with all distinct vertices. (P_m ; length $m - 1$)
- Cycle : a walk with distinct vertices except $v_1 = v_m$. (C_m ; length m)
- Trail : a walk with distinct edges.
- Circuit: a walk with distinct edges and $v_1 = v_m$.

The above definitions are also applied to digraph. ($(v_i, v_{i+1}) \in A(D)$, (v_i, v_{i+1}) is an arc of a digraph D .)

Theorem 1.2. *Every graph G contains a path of length $\delta(G)$ and a cycle of length at least $\delta(G) + 1$ provided $\delta(G) \geq 2$.*

Proof. Let $\langle x_0, x_1, \dots, x_k \rangle$ be a longest path we can find in G . Then, $N_G(x_k) \subseteq \{x_0, x_1, \dots, x_{k-1}\}$. For otherwise, we have a longer path. Now, $\deg_G(x_k) \geq \delta(G)$, but $\deg_G(x_k) \leq k$. Hence, $k \geq \delta(G)$ and we have the proof of the first part.

Since $\deg_G(x_k) \geq 2$, x_k is incident to some vertex in $\{x_0, x_1, \dots, x_{k-2}\}$. Let i be the minimum index in $\{0, 1, 2, \dots, k - 2\}$ such that $x_k x_i \in E(G)$. Then, $(x_i, x_{i+1}, \dots, x_k)$ is a cycle in G . By the fact $\deg_G(x_k) \geq \delta(G)$, $i \leq k - \delta(G)$. This implies that the cycle has at least $\delta(G) + 1$ vertices. \square

Theorem 1.3 (Mantel, 1907). *If $|G| = n$ and $\|G\| > \lfloor \frac{n^2}{4} \rfloor$, then G contains a C_3 (or K_3).*

Proof. Let $x \in V(G)$ be a major vertex, i.e., $\deg_G(x) = \Delta(G)$. Assume that $C_3 \not\subseteq G$. This implies that $\langle N_G(x) \rangle_G$ contains no edges. Hence,

$$\begin{aligned} \|G\| &\leq \Delta(G) + \Delta(G) \cdot (n - \Delta(G) - 1) \\ &= \Delta(G) \cdot (n - \Delta(G)) \\ &\leq \lfloor \frac{n}{2} \rfloor \cdot (n - \lfloor \frac{n}{2} \rfloor) \\ &= \lfloor \frac{n}{2} \rfloor \cdot \lceil \frac{n}{2} \rceil \\ &= \lfloor \frac{n^2}{4} \rfloor, \end{aligned}$$

a contradiction. □

Definition 1.9. A graph is called H -free if $H \not\subseteq G$.

Extremal Graph Theory

Research Problem. Given a graph H of order $m \leq n$. Find a graph G of order n which has the maximum number of edges, but G is H -free.

Remark.

- We use $ext(n; H)$ to denote the above mentioned number. The graph which attains this size $ext(n; H)$ is called an extremal graph (which forbids H).
- G is a complete graph of order n if $\|G\| = \binom{n}{2}$, i.e., any two vertices of G are adjacent. We use K_n to denote such graph. K_{n_1, n_2, \dots, n_q} denotes a **complete multipartite graph** with q partite sets, each of size n_1, n_2, \dots, n_q respectively.
- From Theorem 1.3, we have $ext(n; C_3) = \lfloor \frac{n^2}{4} \rfloor$ and $K_{\lfloor \frac{n}{2} \rfloor, \lceil \frac{n}{2} \rceil}$ is an extremal graph of order n which forbids $C_3 (\simeq K_3)$.

Theorem 1.4 (Turán, 1941). Let $n = t(p-1) + r$, $1 \leq r \leq p-1$, and

$$M(n, p) =_{def} \frac{p-2}{2(p-1)} n^2 - \frac{r(p-1-r)}{2(p-1)}.$$

Then, $ext(n; K_p) = M(n, p)$.

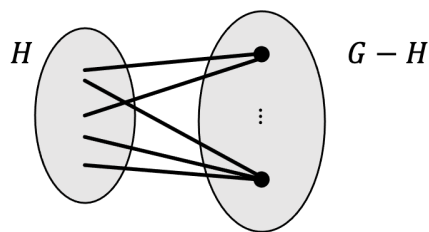
Proof. By induction on t . First, if $t = 0$, then $n = r \leq p-1$, clearly, G does not contain K_p . Moreover,

$$M(n, p) = \frac{(p-2)r^2 - rp + r + r^2}{2(p-1)} = \frac{pr^2 - rp - r^2 + r}{2(p-1)} = \frac{(p-1)(r^2 - r)}{2(p-1)} = \binom{r}{2},$$

$G \simeq K_r$.

Now, consider $t \geq 1$ and let the assertion be true for $t-1$. Let G be the extremal graph which does not contain K_p . So, G contains K_{p-1} . Let $V(K_{p-1}) = H$. Thus, H contains $p-1$ vertices. Since G does not contain K_p , the vertices outside of H are incident to at most $p-2$ vertices of H . This implies that

$$\|G\| \leq \binom{p-1}{2} + (p-2)(n-p+1) + ext(n-p+1; K_p).$$



$$|H| = p - 1, \quad |G - H| = n - p + 1.$$

Now, $n - p + 1 = (t - 1)(p - 1) + r$. By induction, $\text{ext}(n - p + 1; K_p) = M(n - p + 1, p)$.

Hence,

$$\begin{aligned} \|G\| &\leq \binom{p-1}{2} + (p-2)(n-p+1) + \frac{p-2}{2(p-1)}(n-p+1)^2 - \frac{r(p-1-r)}{2(p-1)} \\ &= \frac{p-2}{2(p-1)} [(p-1)^2 + 2(p-1)(n-(p-1)) + (n-(p-1))^2] - \frac{r(p-1-r)}{2(p-1)} \\ &= \frac{p-2}{2(p-1)} n^2 - \frac{r(p-1-r)}{2(p-1)} \\ &= M(n, p). \end{aligned}$$

For the (\geq) direction, let G be the complete multipartite graph $K_{t+1, \dots, t+1, t, \dots, t}$ with r partite sets of size $t+1$ and $p-1-r$ partite sets of size t . Then, $n = r(t+1) + (p-1-r)t = t(p-1) + r$. Now, $\|G\| = M(n, p)$, this concludes the proof.

(G is an extremal graph. In fact, this is the unique extremal graph. (proof?)) \square

Definition 1.10. If G contains a cycle, then the length of a shortest cycle is called the *girth* of G , denoted as $g(G)$, and the length of a longest cycle is called the *circumference* of G , denoted as $c(G)$. Clearly, $g(G) \leq c(G)$.

Definition 1.11. If $c(G) = |G|$, then G is a hamiltonian graph, i.e., G contains a Hamilton cycle.

Remark.

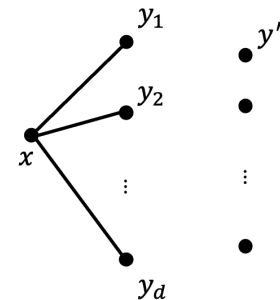
- Determining whether a graph is hamiltonian or not is a very difficult problem. But, for the existence of an Eulerian circuit, it is simpler.
- The problem of forbidding cycles of length larger than 3 is comparatively difficult.

Theorem 1.5. *If a graph G of order n has more than $\frac{n\sqrt{n-1}}{2}$ edges, then $g(G) \leq 4$. (G contains either a C_3 or a C_4 .)*

Proof. Let $g(G) \geq 5$ and $N_G(x) = \{y_1, y_2, \dots, y_d\}$. Then, $\langle N_G(x) \rangle_G$ has no edges (no C_3 's).

For vertices $y' \in V(G) \setminus N_G(x)$, y' is incident to at most one vertex in $N_G(x)$ (no C_4 's). That is, $N_G(y_i) \cap N_G(y_j) = \{x\}$,

for $1 \leq i < j \leq d$. Hence, $\sum_{i=1}^d \deg_G(y_i) \leq n - (d + 1) + d = n - 1$.



Now, consider the volume of G , $vol(G) \leq n(n - 1)$.

$$\begin{aligned} n(n - 1) &\geq \sum_{x \in V(G)} \sum_{y \sim_G x} \deg_G(y) \\ &= \sum_{z \in V(G)} \deg_G^2(z) \quad \text{each } z \text{ of degree } \deg_G(z) \text{ will be counted } \deg_G(z) \text{ times} \\ &\geq \frac{1}{n} \left(\sum_{z \in V(G)} \deg_G(z) \right)^2 \quad \text{by Cauchy's inequality} \\ &= \frac{1}{n} (2\|G\|)^2. \end{aligned}$$

Hence, $\|G\| \leq \frac{1}{2}n\sqrt{n-1}$. □

Corollary 1.6. $ext(n; C_3 \text{ or } C_4) \leq \frac{1}{2}n\sqrt{n-1}$. *Extremal graphs:*

- $n = 5 : C_5$
- $n = 10 : Petersen \text{ graph}$
- $n = 50 : srg(50, 7, 0, 1)$ (*strongly regular graph*)

Corollary 1.7. $ext(n; C_4) \leq \frac{n}{4}(1 + \sqrt{4n - 3})$. (*proof?*)

Eulerian Circuits and Hamilton Cycles

Before we get to the proof of Euler's result on Eulerian circuits, we need more background.

Definition 2.1. A graph G is connected if and only if for any two vertices u and v in $V(G)$, there exists a path connecting u and v .

Remark. If G is connected, then $|G| \leq \|G\| + 1$.

Definition 2.2. G_i is a component of G if G_i is a maximal connected subgraph of G . The number of components of G is denoted by $\omega(G)$.

Definition 2.3. G is a forest if G contains no cycles (G is acyclic), and G is a tree if G is connected and acyclic.

Theorem 2.1. *The following statements are equivalent.*

- G is a tree.
- G is acyclic and $\|G\| = |G| - 1$.
- G is connected and $\|G\| = |G| - 1$.
- Any two vertices of G are connected with a unique path.

Proof. We prove (1) \Rightarrow (2) and leave the others for the readers to verify.

(1) \Rightarrow (2) By definition, G is a tree implies that G is connected and acyclic. The proof is by induction on $|G|$ and it is true for $|G| = 1$ and 2.

Since G is connected, there exist two vertices u and v which are of maximum distance (diameter). Then, v must be of degree 1. For otherwise, v is either adjacent to some

vertex on the path from u to v or v is adjacent to a new vertex. Both of them are not possible.

Hence, $\deg_G(v) = 1$. Now, consider $G - v$. $G - v$ is connected and acyclic. By induction hypothesis,

$$\|G - v\| = |G - v| - 1 \implies \|G\| - 1 = |G| - 1 - 1 \implies \|G\| = |G| - 1.$$

□

Definition 2.4. An Eulerian circuit of a graph G is a circuit passing all the edges of G .

Theorem 2.2. G has an Eulerian circuit if and only if G is connected and each vertex of G is even.

Proof.

(\implies) Since G has a walk passes all vertices, G is connected. If a circuit passes a vertex x h times, then $\deg_G(x) = 2h$.

(\impliedby) By induction on $\|G\|$. Since $\|G\| \geq 1$, $\delta(G) \geq 2$ (G is not a tree!) and thus G contains a cycle. Let Z be a circuit in G with the maximum number of edges. If Z is an Eulerian circuit, then we are done. Suppose not.

Let H be a nontrivial component of $G - E(Z)$. Since G is connected, $V(H) \cap V(Z) \neq \emptyset$. Let $x \in V(H) \cap V(Z)$. (Figure 2.1) Now, H is nontrivial connected graph (even graph). Hence, H contains an Eulerian circuit Y . By using x , we can attach Z and Y together to obtain a larger circuit. This contradicts to the maximality of $|E(Z)|$. Hence, Z must be an Eulerian circuit in G .

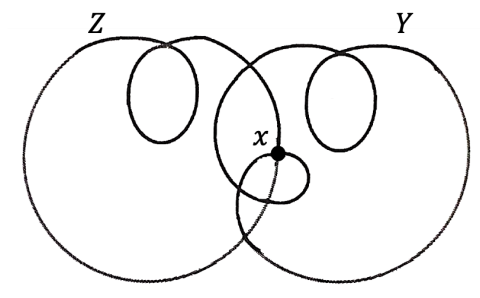



Figure 2.1

□

Open Problem. Find the number of distinct Eulerian circuits of an Eulerian graph G .

Remark.

- The Euler's theorem on circuits is also true for multi-graph, in which we have 2-cycle .
- In a digraph $D = (V, A)$, we use $N_D^+(v)$ (resp. $N_D^-(v)$) to denote the out neighbor (resp. in-neighbor) where $N_D^+(v) = \{u \in V \mid (v, u) \in A\}$ (resp. $N_D^-(v) = \{u \in V \mid (u, v) \in A\}$). $|N_D^+(v)| = \text{deg}_D^+(v)$ and $|N_D^-(v)| = \text{deg}_D^-(v)$.

Definition 2.5. A digraph $D = (V, A)$ is connected if for each ordered pair (a, b) , $a, b \in V$, there exists a directed path from a to b , i.e., there exists a sequence $\langle a = a_1, a_2, \dots, a_t = b \rangle$ where $(a_i, a_{i+1}) \in A$ for $i = 1, 2, \dots, t - 1$.

Theorem 2.3. A connected digraph $D = (V, A)$ has a directed Eulerian circuit if and only if for each v in V , $\text{deg}_D^+(v) = \text{deg}_D^-(v)$.

Proof. By a similar argument as that of Theorem 2.2. □

Surprisingly, if D has a directed Eulerian circuit, then we can find all distinct directed Eulerian circuits. This is different from the case on un-directed graphs.

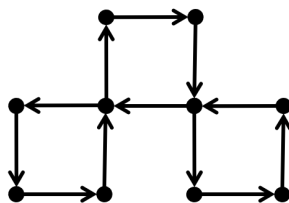


Figure 2.2: A directed eulerian circuit.

Theorem 2.4 (BEST). Let $t_i(D)$ be the number of spanning trees oriented toward v_i in D of order n . Then the number of distinct Eulerian circuits $s(D)$ is equal to

$$t_i(D) \cdot \prod_{j=1}^n (\text{deg}_D^+(v_j) - 1)!$$

Remark.

- Note that in a directed eulerian graph $t_i(D) = t_j(D)$ for any two vertices v_i and v_j .
- This theorem was proved by two independent groups: deBruijn and van Aardenne-Ehrenfest, and Smith and Tutte.

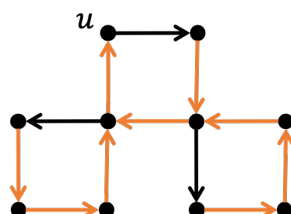


Figure 2.3: A spanning tree oriented toward u .

Definition 2.6. A cycle which contains all vertices of G is called a Hamilton cycle. G is called hamiltonian if G contains a Hamilton cycle.

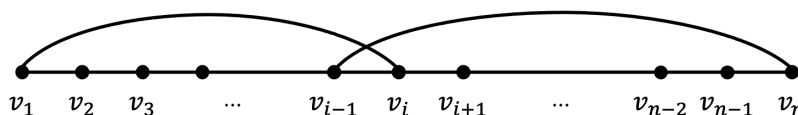
As mentioned earlier, determining whether a graph is hamiltonian or not is a very difficult problem. In fact, determining whether G contains a cycle of length k is also difficult. So, the researchers are interested in finding good sufficient conditions for the existence of Hamilton cycles. The following theorem is a classical one.

Theorem 2.5 (Ore, 1960). *If G is a graph of order $n \geq 3$ such that for all distinct non-adjacent vertices u and v , $\deg(u) + \deg(v) \geq n$, then G contains a Hamilton cycle.*

Proof. (By maximality argument.)

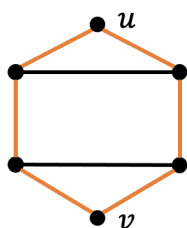
Assume the assertion is false. Then, there exists a nonhamiltonian graph \tilde{G} of order $n \geq 3$ which satisfies the hypothesis of the theorem. Therefore, for any two distinct vertices v_1 and v_2 , $\tilde{G} + v_1v_2$ contains a Hamilton cycle. Furthermore, every Hamilton cycle, if any, of $\tilde{G} + v_1v_2$ contains the edge v_1v_2 .

Now, let u and v be two non-adjacent vertices of G . Since $G + uv$ contains a Hamilton cycle, G contains a Hamilton path $\langle u = v_1, v_2, \dots, v_n = v \rangle$.



By observation, if $v_1v_i \in E(G)$, $2 \leq i \leq n$, then $v_{i-1}v_n \notin E(G)$. (?) For otherwise, we have a Hamilton cycle $(v_1, v_i, v_{i+1}, \dots, v_n, v_{i-1}v_{i-2}, \dots, v_1)$. This implies that if $\deg(v_i) = t$, $\deg(v_n) \leq (n-1) - t$. Hence, $\deg(u) + \deg(v) \leq t + (n-1) - t = n-1$, a contradiction. We conclude that G contains a Hamilton cycle. \square

Remark. There are sufficient conditions (Quite a few!) for the existence of Hamilton cycles in a graph, but so far, none of them is also necessary. For example, the condition in above theorem is not necessary:



$$\deg(u) + \deg(v) = 4 < 6.$$

Weighted Graphs

Definition 2.7 (Weighted graphs). A graph G is weighted if each edge is assigned a weight by using a weighted function $w : E(G) \rightarrow \mathbb{R}$.

Traveling Salesman Problem (TSP)

In a weighted complete graph G , find a minimum Hamilton cycle, i.e., the sum of all weights in the cycle is minimum comparing the sums of all the weighted of the other Hamilton cycles.

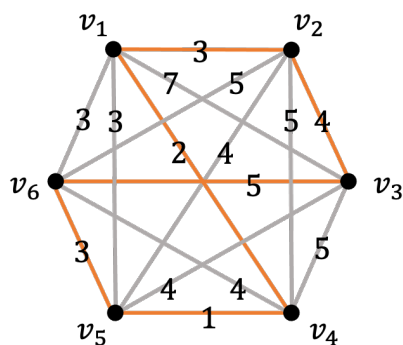


Figure 2.4: A minimum Hamilton cycle.

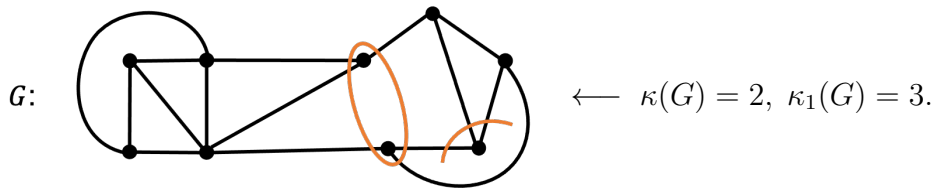
Remark.

- If each weight is a finite number, then a greedy algorithm can provide an answer. (May not be minimum.)
- If we are looking for minimum spanning trees, then it is an easier problem.

Connectivity

Definition 3.1 (Connectivity). The connectivity of a graph G , $\kappa(G)$, is the minimum number of vertices whose removal from G results in a disconnected graphs or a trivial graph (a graph with one vertex).

Definition 3.2 (Edge connectivity). The edge connectivity of a graph G , $\kappa_1(G)$, is the minimum number of edges whose removal from G results in a disconnected graph.



Theorem 3.1. For any graph G ,

$$\kappa(G) \leq \kappa_1(G) \leq \delta(G).$$

Proof. Let $v \in V(G)$ and $\deg(v) = \delta(G)$. Then, the deletion of all edges incident to v results in a disconnected graph. Hence, $\kappa_1(G) \leq \delta(G)$.

Now, consider the other inequality. First, if $\kappa_1(G) = 0$, then the G is already disconnected, hence $\kappa(G) = 0$. Assume that $\kappa_1(G) > 0$ and let E' be a set of $\kappa_1(G)$ edges such that $G - E'$ is disconnected. Let S be a set of vertices chosen from the set of vertices incident to edges in E' such that each edge is incident to S exactly once. Therefore, $|S| \leq |E'|$. Also, $G - S$ is disconnected or a trivial graph since $G - E'$ is disconnected. This implies that $\kappa(G) \leq |S| \leq |E'| = \kappa_1(G)$. \square

Remark.

- G is super-connected if $\kappa(G) = \delta(G)$.

- Let $a \leq b \leq c$ be positive integers. Then, there exists a graph G such that $\kappa(G) = a$, $\kappa_1(G) = b$, and $\delta(G) = c$.

Definition 3.3 (n -connected and n -edge-connected). A graph G is said to be n -connected (resp. n -edge-connected) if $\kappa(G) \geq n$ (resp. $\kappa_1(G) \geq n$).

Remark. A graph is n -edge-connected if it is n -connected.

Definition 3.4 (Separating set). A set S of vertices in G is said to be a separating set of two vertices u and v ((u, v) -separating set) of G if $G - S$ is a disconnected graph in which u and v lie in different components. We also say S separates u and v .

Theorem 3.2 (Manger, 1927). Let u and v be non-adjacent vertices in G . Then, the minimum number of vertices that separates u and v is equal to the maximum number of internally disjoint $u - v$ paths in G .

Proof. Many different versions. We include one here for your reference.

Let the number of vertices separating u and v to be k . Then, it is easy to see that there are at most k independent (vertex-disjoint) paths connecting u and v . Also, if $k = 1$, then we have a path joining u and v . Now, suppose the assertion is not true, i.e., we can find less than k independent $u - v$ paths for certain k . Now, take the minimal k in which we have a counterexample. Then, among all such examples, let G be the one with minimum size (number of edge).

First, we notice that u and v have at most $k - 1$ independent paths and no common neighbors. For otherwise, let ux and xv be edges of G . Then $G - x$ will be a counterexample for ' $k - 1$ ' (smaller than k). Let W be a separating set of u and v and $|W| = k$. Suppose, neither $N_G(u) = W$ nor $N_G(v) = W$. (See Figure 3.1.)

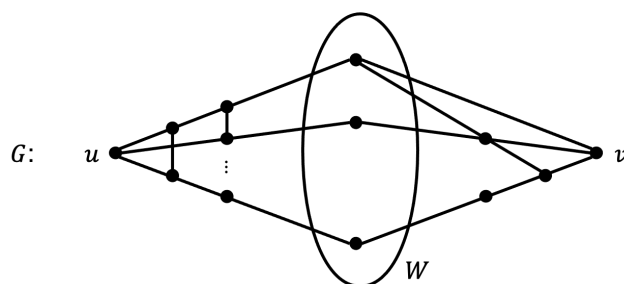


Figure 3.1

Let G_u be obtained by deleting all the vertices to the left of G in Figure 3.1 and adding a replacing u' with edges joining W , see Figure 3.2. Now, G_u has fewer edges than G and thus there are k independent $u' - v$ paths. Hence, we have k $W - v$ independent paths. With the same technique, we derive k $u - W$ independent paths (by changing u to v).

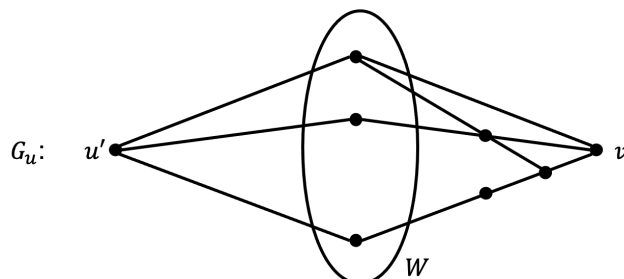


Figure 3.2

So, as a conclusion, either u or v must have their neighbors W . Let $N_G(u) = W$ and $P = \langle u, x_1, x_2, \dots, x_l, v \rangle$ be a shortest $u - v$ path. (Figure 3.3) Then $l \geq 2$. Consider $G - x_1x_2$.

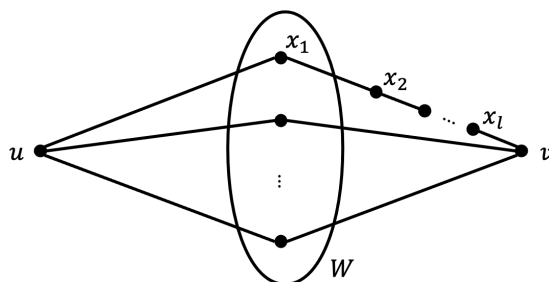


Figure 3.3

In $G - x_1x_2$, there exists a $u - v$ separating set W_0 of size $k - 1$. Then, both $W_1 = W_0 \cup \{x_1\}$ and $W_2 = W_0 \cup \{x_2\}$ are $u - v$ separating sets of G . By the fact that P is a shortest $u - v$ path, u is not adjacent to x_2 and v is not adjacent to x_1 . This implies that $N_G(u) = W_1$ since v is not adjacent to a vertex of the separating set W_1 . Similarly, $N_G(v) = W_2$. Hence, $N_G(u) \cap N_G(v) = W_0$ (u and v have common neighbors), a contradiction.
 ($|W_0| = k - 1 \geq 1$) □

Definition 3.5. In G , given a vertex x and a set U of vertices, an $\langle x, U \rangle$ -fan of size k is a set of k internally disjoint (independent) paths from x to U in G .

Theorem 3.3 (Fan Lemma, Dirac, 1960). *A graph is k -connected if and only if it has at least $k + 1$ vertices and, for every choice of x, U with $|U| \geq k$, it has an $\langle x, U \rangle$ -fan of size k .*

Proof.

(\Rightarrow) If G is k -connected and $U \subseteq V(G)$ with $|U| \geq k$, then the graph $G' = G + \{yu \mid u \in U\}$ where $y \notin V(G)$ is also k -connected. (?) By Menger's Theorem, there are k internally disjoint paths between x and y in G' . Now, clearly, in G we have an $\langle x, U \rangle$ -fan of size k .

(\Leftarrow) It suffices to show that for any two vertices w and z , there are at least k internally disjoint paths. Since an $\langle x, U \rangle$ -fan of size k exists, $\deg_G(x) \geq k$, i.e., $\delta(G) \geq k$. Now, let $U = N_G(z)$. By using $\langle w, U \rangle$ -fan, we obtain the desired paths. \square

Theorem 3.4. *If G is n -connected ($n \geq 2$) and S is a set of n vertices, then there exists a cycle in G which contains S .*

Proof. By induction on n and clearly the case $n = 2$ is true. Assume that the assertion holds for $n - 1$ and G is an n -connected graph. Now, let $|S| = n$ and $x \in S$. Since G is also $(n - 1)$ -connected, $S \setminus \{x\}$ lies on a cycle C (by induction). Furthermore, we have an $\langle x, V(C) \rangle$ -fan of size $n - 1$.

Case 1. $|C| = n - 1$.

The proof follows by finding \tilde{C} which contains all vertices of S , see Figure 3.4.

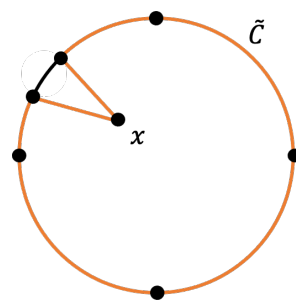


Figure 3.4

Case 2. $|C| > n - 1$.

Since G is n -connected, an $\langle x, V(C) \rangle$ -fan of size n exists. By the fact that $S \setminus \{x\} \subseteq V(C)$, C is partitioned into $n - 1$ paths $\langle V_1, V_2, \dots, V_{n-1} \rangle$. Therefore, the $\langle x, V(C) \rangle$ -fan of size n will contain (at least) two vertices in one V_i by Pigeon-hole principle. Now, we are able to find a cycle which contains S . (?) This concludes the proof. \square

Topological Graph Theory

Definition 4.1 (Proper drawing). A proper drawing on a surface of a graph G with p vertices and q edges follows the rules:

1. There are p points on the surface which corresponds to the set of vertices in G .
2. There are q curves joining points defined above which correspond to the set of edges and they are pairwise disjoint except possibly for the endpoints.

Definition 4.2 (2-manifold). A connected topological space in which every point has a neighborhood homomorphic to the open unit disk defined on \mathbb{R}^2 .

Definition 4.3 (Bound subspace). A subspace M of \mathbb{R}^3 is bounded if $\exists K \in \mathbb{R}^+$ such that $M \subseteq \{(x, y, z) \mid x^2 + y^2 + z^2 \leq K\}$.

Definition 4.4 (Closed). M is closed if its boundary ∂M coincides with M .

Definition 4.5 (Orientable). M is orientable if for every simple closed curve C on M , a clockwise sense of rotation is preserved once around C . Otherwise, M is non-orientable.

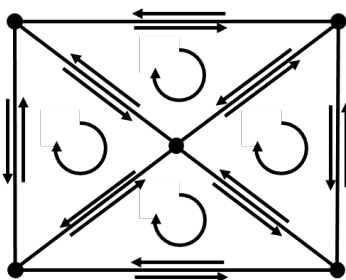


Figure 4.1: Orientable

Definition 4.6 (Orientable surface). A surface S_k is a compact 'orientable' 2-manifold that may be thought of as a sphere on which has been placed (inserted) a number k of 'handles' (holes).

Definition 4.7 (Non-orientable surface). A surface obtained by adding k cross-caps to a sphere (S_0) is a non-orientable surface N_k . (Adding a cross-cap: attach the boundary of a Möbius band to a cycle on S_0 .)

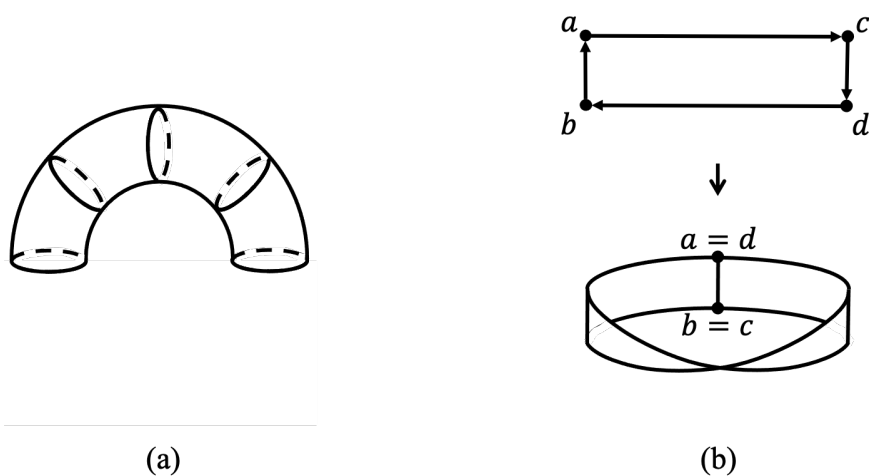


Figure 4.2: (a) A handle. (b) A Möbius band.

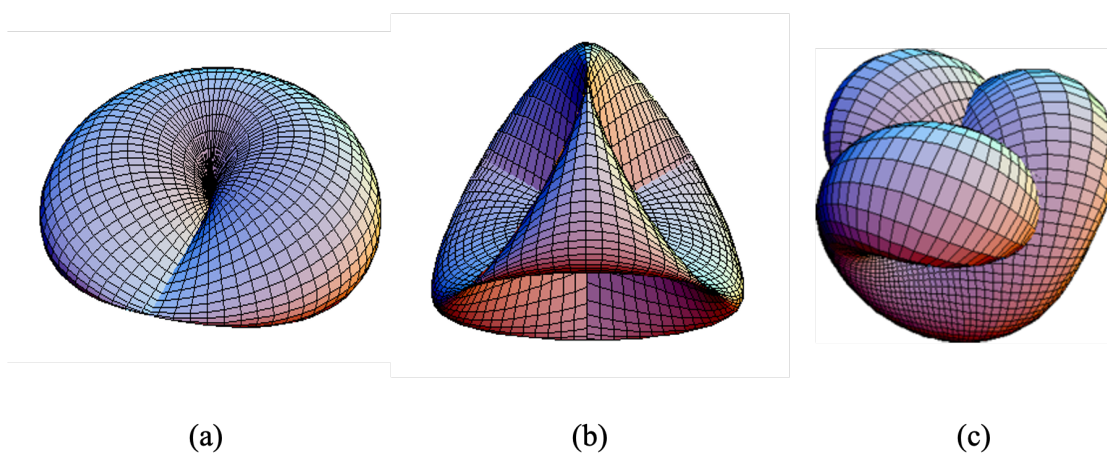


Figure 4.3: (a) The cross-cap. (b) The Roman surface. (c) The Boy's surface.

Definition 4.8 (Embeddable). A (p, q) -graph G is said to be embeddable on a surface if it is possible to draw G *properly* (*drawing without crossings*) on the surface.

Definition 4.9 (Planar graph). A graph is planar if it can be embedded in the plane, equivalently, embedded on the sphere.

Definition 4.10 (2-cell embedding). A region is called a 2-cell if any simple closed curve in that region can be continuously deformed or contracted in that region to a single point, equivalently, a 2-cell is topologically homeomorphic to \mathbb{R}^2 . An embedding of G on a surface is a 2-cell embedding of G if all the regions determined are 2-cells.

Remark.

- S_0 : Sphere
- S_k : a surface obtained by attaching k handles to S_0 .
- $N_0 \simeq S_0$ (Homeomorphic)
- N_h : attach h cross-caps to $N_0(S_0)$.

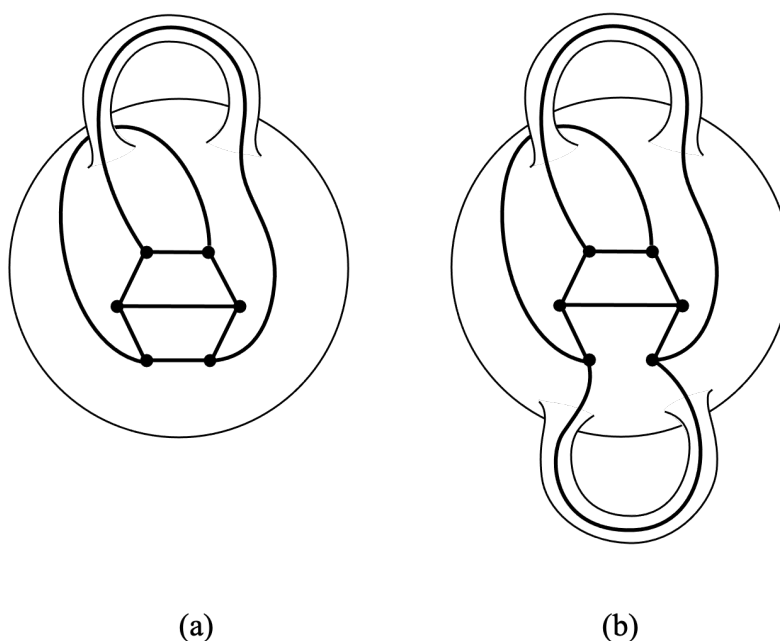


Figure 4.4: Embeddings of $K_{3,3}$ on surfaces S_1 and S_2 respectively.

Definition 4.11 (Genus). The number of handles (resp. cross-caps) (on a surface) is referred to as genus of the orientable surface (resp. non-orientable surface). We use $\gamma(G)$ (resp. $\tilde{r}(G)$) to denote the smallest genus of all orientable surfaces (resp. non-orientable surfaces) on which G can be embedded.

Remark.

- If G is a planar graph, then $\gamma(G)$ (so is $\tilde{r}(G)$) is equal to zero. But, G can also be embedded on a surface with genus larger than '0'.
- Given a graph G , determining $\gamma(G)$ is a difficult problem.

Theorem 4.1 (Euler's formula). *Let G be a connected planar graph with p vertices, q edges and f faces (regions). Then, $p - q + f = 2$.*

Proof. By induction on q . Since G is connected, G has at least $p - 1$ edges. (?) If G has $p - 1$ edges and G is connected, then G is a tree which contains no cycles. This implies that $f = 1$ and thus $p - (p - 1) + 1 = 2$. The assertion is true for 'minimal' graphs. Assume the hypothesis is true for $k = ||G|| \geq p - 1$. Now, consider G with $k + 1$ edges. Clearly, G contains a cycle. Let e be a cycle edge. Since G is connected planar graph (with q faces), $G - e$ is also a connected planar graph. Moreover, $G - e$ has k edges and $q - 1$ faces. By induction, $p - k + (q - 1) = 2$ and thus $p - (k + 1) + q = 2$. This concludes the proof. \square

Theorem 4.2. *If G is a planar graph with largest size, then $||G|| = 3|G| - 6$.*

Proof. By observation, if G has maximum size, then each region of G is a triangle. Since each edge of G is in the boundary of exact two regions, $3f = 2q$ where f is the number of regions and q is the size of G , i.e., $q = ||G||$. Now, by Euler's formula, $p - q + f = 2$, equivalently, $|G| - ||G|| + \frac{2}{3}||G|| = 2$ and thus $3|G| - 6 = ||G||$. (G is a *maximal planar graph!*) \square

Corollary 4.3. *If G is a planar graph, then $||G|| \leq 3|G| - 6$.*

Corollary 4.4. *In any planar graph, there exists at least one vertex of degree smaller than 6. (This corollary is very useful.)*

Corollary 4.5. *The degree sum of a planar graph is at most $6|G| - 12$.*

We can give a more accurate estimation of the above corollary:

Theorem 4.6. *Let G be a maximal planar graph (triangulated) of order p , and let p_i denote the number of vertices of degree i in G for $i = 3, 4, \dots, \Delta(G) = d$. Then,*

$$3p_3 + 2p_4 + p_5 = p_7 + 2p_8 + \dots + (d - 6)p_d + 12.$$

Proof. Since $p = \sum_{i=3}^d p_i$ and $2q = \sum_{i=3}^d i \cdot p_i$, we have $\sum_{i=3}^d i \cdot p_i = 2(3p - 6) = 6 \cdot \sum_{i=3}^d p_i - 12$. This implies the conclusion. \square

Theorem 4.7. *There are exactly five regular polyhedra.*

Proof. Notice that a regular polyhedron is a polyhedron whose faces (regions) are bounded by congruent (全等) regular polygons and whose polyhedral angles are congruent.

First, we convert a polyhedron into a regular planar graph. (See Figure 4.5 for examples.)

Let the number of vertices, edges and faces be p, q and f respectively. By Euler's formula, $p - q + f = 2$. Hence,

$$\begin{aligned} -8 &= 4q - 4p - 4f \\ &= 2q + 2q - 4p - 4f \\ &= \sum_{i \geq 3} i \cdot f_i + \sum_{i \geq 3} i \cdot p_i - 4 \sum_{i \geq 3} p_i - 4 \sum_{i \geq 3} f_i (f_i : \# \text{ of } i\text{-face}) \\ &= \sum_{i \geq 3} (i - 4)f_i + \sum_{i \geq 3} (i - 4)p_i. \end{aligned}$$

Since the polyhedron is regular, all degrees and face sizes are the same, let them be k and h respectively. Therefore,

$$-8 = (h - 4)f_h + (k - 4)p_k.$$

By the fact that every planar graph contains a vertex of degree less than six, we only have nine cases to consider: $3 \leq h \leq 5$ and $3 \leq k \leq 5$. From direct checking, only 5 cases are possible, namely,

- (1) $f_3 = p_3 = 4$ (Tetrahedron, 四面體)
- (2) $f_3 = 8$ and $p_4 = 6$ (Octahedron, 八面體)
- (3) $f_3 = 20$ and $p_5 = 12$ (Icosahedron, 二十面體)
- (4) $f_4 = 6$ and $p_3 = 8$ (Cube, 六面體)
- (5) $f_5 = 12$ and $p_3 = 8$ (Dodecahedron, 十二面體)

See Figure 4.5 for regular polyhedra. □

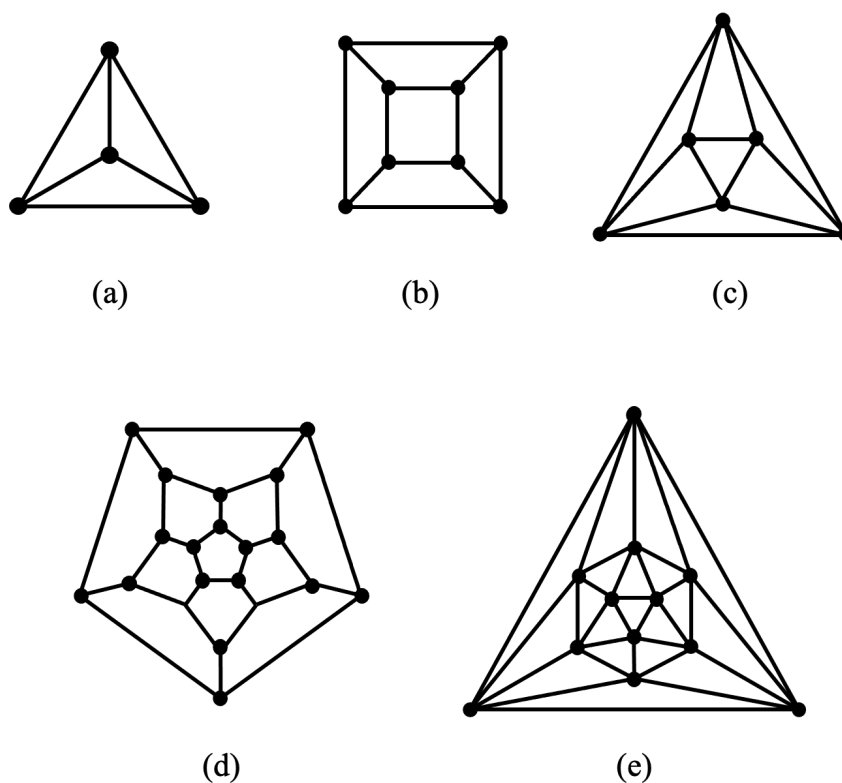


Figure 4.5: (a) Tetrahedron. (b) Cube. (c) Octahedron.
(d) Dodecahedron. (e) Icosahedron.

Theorem 4.8 (Fáry (1948), Wagner (1936)). *A planar graph G can be embedded in the plane so that each edge is a straight line segment.*

Proof. The proof is by induction on the order of G . It suffices to prove that case when G is a connected maximal planar graph. Clearly, it is true for small orders. Assume the hypothesis is true for order k and let G be a connected maximal planar graph of order $k + 1$. Since G is maximal $3 \leq \delta(G) \leq 5$.

Case 1. $\delta(G) = 3$.

Let $v_0 \in V(G)$ such that $\deg_G(v_0) = 3$ and v_0 is adjacent to v_1, v_2 and v_3 . Since G is maximal, $\langle \{v_1, v_2, v_3\} \rangle_G \cong K_3$. This implies that $G - v_0$ is also a maximal planar graph. By induction $G - v_0$ has a straight line segment embedding. Now, put v_0 back to the graph $G - v_0$ such that v_0 is inside the region bounded by $\langle \{v_1, v_2, v_3\} \rangle_G$ and connect v_0 to the three vertices by straight line segment. This concludes the proof this case.

Case 2. $\delta(G) = 4$.

The proof follows by a similar process as above by letting $N(v_0) = \{v_1, v_2, v_3, v_4\}$. Now, $G - v_0 + v_1v_3$ is a maximal planar graph and this it has a straight line segment embedding. The proof follows by placing v_0 back to $G - v_0 + v_1v_3 - v_1v_3$. By consider the drawing of the embedding (Figure 4.6 (a)), we are able to put v_0 back and connected v_0 to its neighbors in G by straight line segment.

Case 3. $\delta(G) = 5$.

Again, we use the same technique and the drawing can be seen in Figure 4.6 (b). \square

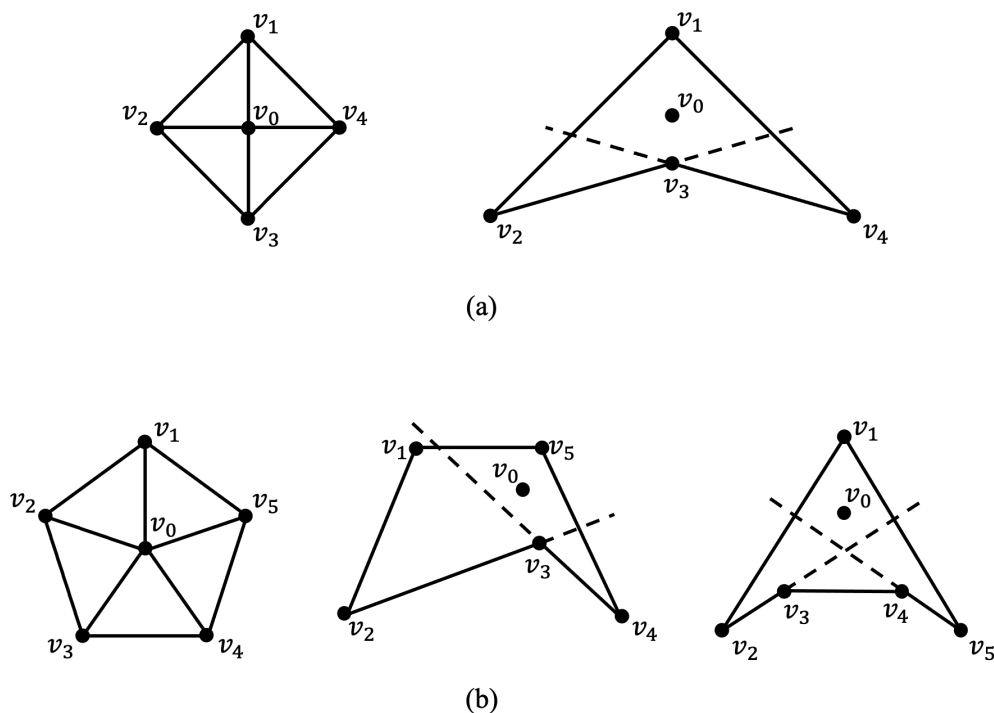


Figure 4.6: Location of v_0 .

The following theorem considers pseudographs, i.e., loops and multiedges are allowed.

Theorem 4.9. *Let G be a (p, q) -pseudograph which has a 2-cell embedding on S_n . Then, $p - q + f = 2 - 2n$ where f is the number of faces in the embedding.*

Proof. By induction on n and it is true when $n = 0$ (by Euler's planar graph formula). Assume that the assertion is true when $n = k \geq 0$ and G is a (p, q) -pseudograph which has a 2-cell embedding on S_{k+1} . Since $k + 1 \geq 1$, there exists a handle in the embedding, see Figure 4.7 (a). It suffices to consider the embedding such that there exists at least one edge which passes through the handle (on the surface). Note that if we can pull back an edge without passing through the handle, then pull it back, see Figure 4.7 (b). Now, we apply the idea of 'cut and past' to obtain a 2-cell embedding of \tilde{G} on S_k .

By using a circle around the handle, we can cut the handle through the circle and obtain \tilde{G} , see Figure 4.7 (c). As a consequence, the graph \tilde{G} is embedded in S_k . If there are t edges passing through the handle, then $|\tilde{G}| = p + 2t$, $||\tilde{G}|| = q + 3t$ and the embedding in S_k has $f + t + 2$ faces. Hence, $(p + 2t) - (q + 3t) + (f + t + 2) = 2 - 2k$. This implies that $p - q + f = 2 - 2(k + 1)$. \square

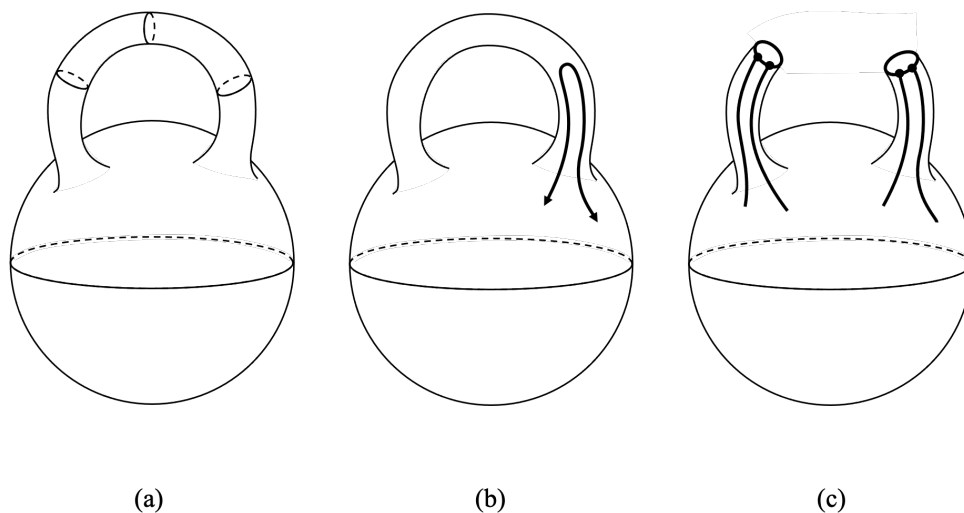


Figure 4.7

Vertex Coloring

Motivated by the well-known 4-color theorem, this topic attracts many researchers to work on. Nowadays, the study of colorings either on vertices, edges or regions was known as the chromatic theory. Besides of its original problem on map colorings, there are quite a few different versions of colorings. We start here with the original coloring which is on vertices of a graph. How many colors do we need to color the vertices of the following graph?

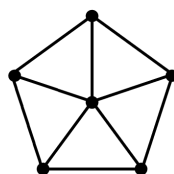


Figure 5.1: Wheel

Definition 5.1.

- k -coloring (proper): $\varphi : V(G) \rightarrow \{1, 2, 3, \dots, k\}$ s.t. $uv \in E(G) \Rightarrow \varphi(u) \neq \varphi(v)$.
- $\chi(G) = \min\{k \mid G \text{ has a } k \text{ coloring}\}$ (Chromatic number of G)
- G is n -critical (chromatically) if $\chi(G - v) < \chi(G)$ for each $v \in V(G)$.

Remark.

- Every graph G has an n -critical induced subgraph H .
- Let $\omega(G)$ denote the order of a maximum clique, i.e., the order of complete subgraphs is maximum. So, $\chi(G) \geq \omega(G)$. When does the equality holds?

Definition 5.2. A graph G is called *perfect* if $\chi(H) = \omega(H)$ for each induced subgraph H of G . Clearly, not every graph is perfect. $\chi(H) - \omega(H)$ can be very large!

Theorem 5.1 (Mycielski). *For every integer n , there exists a triangle-free graph G such that $\chi(G) = n$. ($\chi(G) - \omega(G) = n - 2$.)*

Proof. By induction on n and K_1, K_2, C_5 do have the property respectively for $n = 1, 2$, and 3 . Now, assume that H is a triangle-free k -chromatic graph, i.e., $\mathcal{H} = k$. We construct a graph G based on H such that G is a triangle-free $(k + 1)$ -chromatic graph. Let $V(H) = \{v_1, v_2, \dots, v_p\}$ and $V(G) = V(H) \cup \{u_1, u_2, \dots, u_p, u_0\}$. Let $E(G) = E(H) \cup \{u_0 u_i \mid i = 1, 2, \dots, p\} \cup \{u_i v_j \mid v_j \in N_H(v_i)\}$. See Figure 5.2 for an example when $k = 3$. Since $\langle \{u_1, u_2, \dots, u_p\} \rangle_G$ contains no edges, u_0 is not in any triangle. By assumption, $H \not\cong K_3$. So, the only possibility will be a triangle consists of u_i, v_j and v_k where $u_i v_j$ and $u_i v_k$ are edges of G . If they form a triangle, then $\langle \{v_i, v_j, v_k\} \rangle_H$ is a triangle in H . Hence, G is triangle-free.

Now, we claim $\chi(G) = k + 1$. Let φ be a k -coloring of H . Let $\tilde{\varphi} : V(G) \rightarrow \{1, 2, \dots, k + 1\}$ by letting $\tilde{\varphi}(u_i) = \varphi(v_i)$ and $\tilde{\varphi}(u_0) = k + 1$. Hence, we have a $(k + 1)$ -coloring of G , thus $\chi(G) \leq k + 1$. On the other hand, we show that $\chi(G) \geq k + 1$. Suppose not. Let φ' be a k -coloring of G and the colors used are $1, 2, \dots, k$. First, we assign u_0 the color k , i.e., $\varphi'(u_0) = k$. So, the colors used for u_1, u_2, \dots, u_p must be in $\{1, 2, \dots, k - 1\}$. Since $\chi(H) = k$, k occurs somewhere in H , say v_i . (May have more vertices.) Now, we recolor v_i by using $\varphi'(u_i)$. Since u_i is adjacent to every vertex of $N_H(v_i)$, $\varphi'(u_i) \neq \varphi'(v)$ for each $v \in N_H(v_i)$ and thus we have a proper coloring of H using at most $k - 1$ colors. (?)

A contradiction. □

Remark. This result was generalized later to the graph G with given girth g and $\chi(G)$ can be any larger $n \in \mathbb{N}$ by P. Erdős.

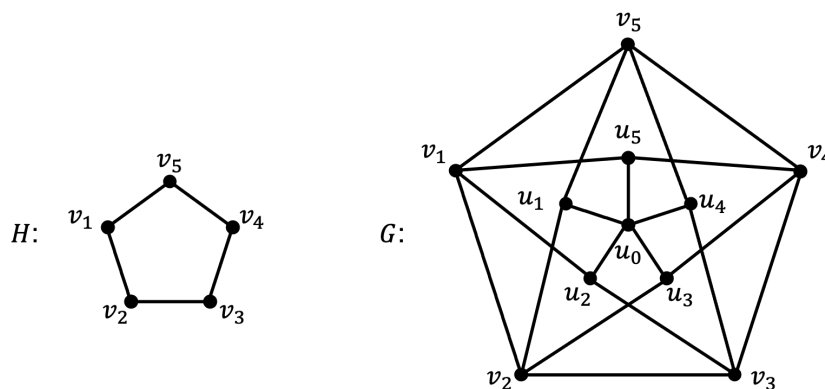


Figure 5.2: Grötzsch graph

Now, we consider the original problem of map coloring. So, we would like to show that if G is planar, then $\chi(G) \leq 4$. Clearly, so far, all proofs include the aid of computer checking. But, the weaker version of showing $\chi(G) \leq 5$ was obtained around 1890.

Theorem 5.2. *If G is a connected planar graph, then $\chi(G) \leq 5$.*

Proof. By induction on $|G|$. For $\delta(G) = 1, 2, 3$ and 4 , the proof can be obtained easily.

(?) Hence, it suffices to consider a planar graph H whose minimum degree is 5 .

Let $v \in V(H)$ such that $\deg_H(v) = 5$. By induction, $\chi(H - v) \leq 5$. Let φ be a 5-coloring of H and we consider the colors assigned on $N_H(v)$. Let them be $\varphi(v_1), \varphi(v_2), \dots, \varphi(v_5)$. Clearly, if any two of them are of the same color, then there is a color for v such that we have a proper 5-coloring of H . So assume that $\varphi(v_i), i = 1, 2, 3, 4, 5$, the vertices are in clockwise order, and join consecutive vertices if they are missing. See Figure 5.3.

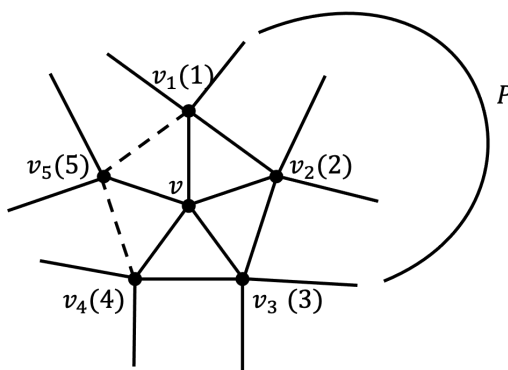


Figure 5.3

Now, consider the induced subgraph $H_{1,3} = \langle \varphi^{-1}(1) \cup \varphi^{-1}(3) \rangle_H$. If v_1 and v_3 are in distinct components, then by changing the colors 1 and 3 in the $\varphi(v_1) = 3$ and $\varphi(v_3) = 3$. Hence, 3 is available for v .

On the other hand, there exists a path P connecting v_1 and v_3 . Hence, $v - v_1 - P - v_3 - v$ is a cycle such that v_2 and v_4 are in different regions. By a similar argument, we may change the color of v_2 to 4. Then 2 is available for v . \square

Theorem 5.3 (4CT). *Every planar graph is 4-colorable.*

Remark.

- The most recent proof was obtained by N. Robertson, D.P. Sanders, P.D. Seymour and R. Thomas (1996): A new proof of the 4CT, Electron. Res. Announc. A.M.S. 2,17-25.
- This first proof was obtained in 1976-1977, by K. Appel and W. Haken.

Open Problem. Characterize the planar graphs which are 3-colorable.

Ramsey Theory

This topic plays an important role in learning the structure of graphs. Moreover, it does have important applications. (?)

Definition 6.1. The Ramsey number $R(s, t)$ is the smallest value "n" for which either a graph G of order n contains K_s or $K_t \leq \bar{G}$ (the complement of G).

Definition 6.2 (Edge-coloring version of Ramsey number). The Ramsey number $R(s, t)$ is the smallest value "n" for which any 2-edge-colored K_n (red and blue), either there exists a red K_s or a blue K_t . (A red K_s is a complete graph of order s such that all its edges are colored red.)

Example. $R(3, 3) = 6$. (Do you know this fact?)

Theorem 6.1. *The following statements are true:*

1. $R(s, 2) = s$ and $R(2, t) = t$,
2. $R(s, t) = R(t, s)$,
3. For $s > 2$ and $t > 2$, $R(s, t) \leq R(s, t - 1) + R(s - 1, t)$, and
4. $R(s, t) \leq \binom{s+t-2}{s-1} = \binom{s+t-2}{t-1}$.

Proof.

1. and 2. are easy to see.

Claim of 3.

Let $n = R(s, t - 1) + R(s - 1, t)$. Then, in K_n , each vertex is of degree $R(s, t - 1) + R(s - 1, t) - 1$. Therefore, if K_n is 2-edge-colored by red and blue, then the edges incident to a fixed vertex $x \in V(K_n)$ are either red edges or blue edges. By Pigeon-hole principle, either there are $R(s, t - 1)$ blue edges or $R(s - 1, t)$ red edges. If the first case holds, then

in $\langle N_{K_n}(x) \rangle_{K_n}$ (a complete graph of order $R(s, t - 1)$), either there exists a red K_s or a blue K_{t-1} . Hence, we have a red K_s or a blue K_t in K_n . The other case can be obtained by a similar argument.

Claim of 4.

By inductive argument. (Or induction.)

$$\begin{aligned}
 R(s, t) &\leq R(s, t - 1) + R(s - 1, t) \\
 &\leq \binom{s + t - 1 - 2}{s - 1} + \binom{s - 1 + t - 2}{t - 1} \\
 &\leq \binom{s + t - 3}{s - 1} + \binom{s + t - 3}{s - 2} \\
 &\leq \binom{s + t - 3 + 1}{s - 1} \\
 &\leq \binom{s + t - 2}{s - 1}
 \end{aligned}$$

□

Theorem 6.2 (Erdős and Szekeres, 1935). *For each $s \geq 2$,*

$$R(s) =_{\text{def}} R(s, s) \leq \frac{2^{2s-2}}{s^{1/2}}.$$

Proof. $R(s, s) \leq \binom{2s-2}{s-1}$. We claim that $\binom{2s-2}{s-1} \leq \frac{2^{2s-2}}{s^{1/2}}$ by induction on s .

First, if $s = 2$, $2 \leq \frac{4}{\sqrt{2}}$, the assertion is true. Assume that the assertion is true for $s = k$, thus $\binom{2k-2}{k-1} \leq \frac{2^{2k-2}}{k^{1/2}}$. Now, we calculate

$$\begin{aligned}
 \binom{2k}{k} &= \frac{(2k)!}{k!k!} \\
 &= \frac{2k \cdot (2k-1) \cdot (2k-2)!}{k^2 \cdot (k-1)! \cdot (k-1)!} \\
 &= \frac{2k(2k-1)}{k^2} \binom{2k-2}{k-1} \\
 &\leq \frac{4k-2}{k} \cdot \frac{2^{2k-2}}{k^{1/2}} \\
 &= \frac{4k-2}{4k} \cdot \frac{2^{2k}}{k^{1/2}}.
 \end{aligned}$$

Since $(k+1)^{1/2} \leq \frac{4k \cdot k^{1/2}}{4k-2}$, we conclude that $\binom{2k}{k} \leq \frac{2^{2k}}{(k+1)^{1/2}}$. □

Remark.

- The result has been there for almost 50 years before the improvement due to Thomason in 1988: $R(s) \leq \frac{2^{2s}}{s}$.
- The original proof by Ramsey shows that $R(s) \leq 2^{2s-3} = \frac{2^{2s-2}}{2}$. (1930)

Theorem 6.3. For $k \geq 3$,

$$R(k) \geq \lceil 2^{k/2} \rceil.$$

Proof. (Probabilistic method)

Consider a random red-blue coloring of the edges of K_n . For a fixed set T of k vertices, let A_T be the event that $\langle T \rangle_{K_n}$ is monochromatic. Hence, $P(A_T) = \left(\frac{1}{2}\right)^{\binom{k}{2}} \cdot 2$ (red or blue) $= 2^{1-\binom{k}{2}}$. Since there are $\binom{n}{k}$ possible sets for T , the probability that at least one of A_T occurs is $\binom{n}{k} \cdot 2^{1-\binom{k}{2}}$. Now, if $\binom{n}{k} \cdot 2^{1-\binom{k}{2}} < 1$, then no event A_T occurs is of positive probability, i.e., there exists a coloring of edges such that no monochromatic K_k occurs. Therefore, for such n , $R(k) > n$.

Let $n = \lfloor 2^{k/2} \rfloor$. It suffices to show that $\binom{n}{k} \cdot 2^{1-\binom{k}{2}} < 1$.

$$\begin{aligned} \binom{n}{k} \cdot 2^{1-\binom{k}{2}} &< \frac{n^k}{k!} \cdot \frac{2^{1+\frac{k}{2}}}{2^{\frac{k^2}{2}}} & (1 - \binom{k}{2}) &= 1 - \frac{k^2}{2} + \frac{k}{2} \\ &\leq \frac{(2^{\frac{k}{2}})^k}{k!} \cdot \frac{2^{1+\frac{k}{2}}}{2^{\frac{k^2}{2}}} \\ &\leq \frac{2^{1+\frac{k}{2}}}{k!} \\ &< 1. & (k \geq 3) \end{aligned}$$

Hence, $R(k) \geq \lceil 2^{k/2} \rceil$. □

Remark. Combining Theorems above we obtain: $2^{s/2} \leq R(s) \leq 2^{2s-3}$ for $s \geq 2$.

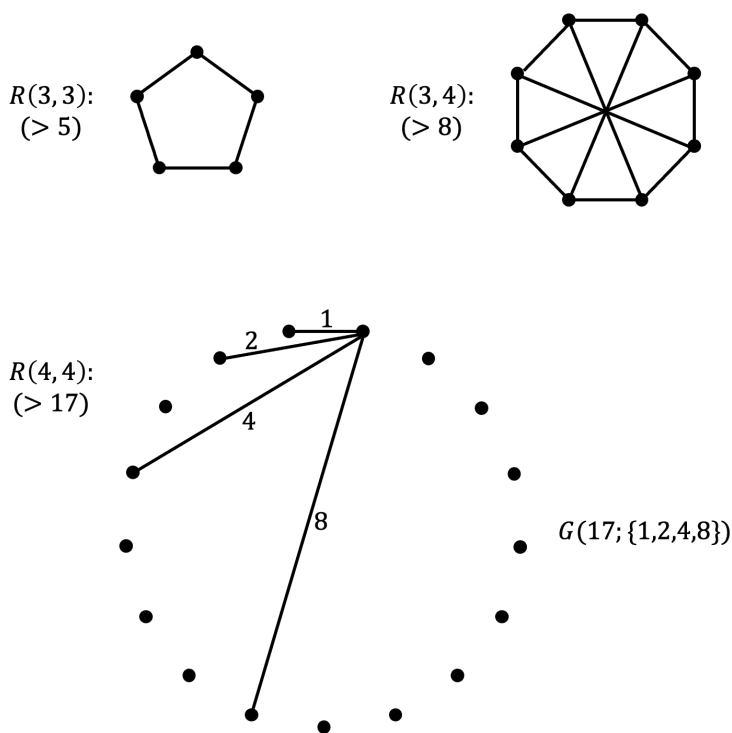
Open Problem. $R(s) = 2^{(c+o(1))s}$ (c may be equal to 1).

Theorem 6.4. *Known results of $R(s, t)$. ($R(t, s) = R(s, t)$)*

t \ s	3	4	5	6	7	8	9
3	6	9	14	18	23	28	36
4		18	25	36-41	49-61	59-84	73-115
5			43-48	58-87	80-143	101-216	133-316
6				102-165	115-298	134-495	183-780
7					205-540	217-1031	252-1713
8						282-1870	329-3583
9							565-6588

Table 6.1

Remark. The result of lower bounds are obtained by "a special edge-coloring" with two colors. Corresponding to the coloring we have G and \bar{G} of order (prescribed).



Research Problem.

- Find as many vertices (n) as possible such that a graph G of order n satisfying $K_5 \not\subseteq G$ and $K_5 \not\subseteq \bar{G}$. (Try 43!)
- Find a better upper bound for $R(s)$. (Do your best!)

We can extend the notion $R(s, t)$ to $R(p_1, p_2, \dots, p_t)$ by using the coloring version. For $R(s, t)$, we consider 2-coloring the edges of K_n for some n . Now, we color the edges of K_n by using t colors. Hence, we are looking for the existence of monochromatic K_{p_i} using color i (the i -th color).

Definition 6.3. $R(p_1, p_2, \dots, p_t) = \min\{n \mid \text{for each } t\text{-coloring of } E(K_n), \text{ there exists a } i\text{-monochromatic } K_{p_i} \text{ for some } 1 \leq i \leq t\}$.

Notice that the order of p_i 's is important since they may not be the same. In case that $p_1 = p_2 = \dots = p_t = s$, we denote it by $R_t(s)$. For example, we will prove that $R_k(3) = \lfloor e \cdot k! \rfloor + 1$. (?) The proof relies on using the generalized Pigeon-hole principle.

Definition 6.4 (Pigeon-hole principle).

- If there are n holes (cages) to hold $n \cdot k - n + 1$ pigeons, then at least one of them will have k pigeons.
- If the n holes are of size a_1, a_2, \dots, a_n , then $n \cdot k$ can be replaced by $\sum_{i=1}^n a_i$ and the i -th hole will have a_i pigeons for some $1 \leq i \leq n$.

Theorem 6.5.

$$R(p_1, p_2, \dots, p_t) \leq R(p_1 - 1, p_2, \dots, p_t) + R(p_1, p_2 - 1, \dots, p_t) + R(p_1, p_2, \dots, p_t - 1) - t + 2.$$

Proof. By a similar argument as the proof $R(s, t) \leq R(s, t - 1) + R(s - 1, t)$. □

Remark.

- $R(3, 3, 3) \leq 6 + 6 + 6 - 3 + 2 = 17$ (Theorem 6.6)
- There exists a 3-edge-coloring of K_{16} such that no monochromatic triangles occur.

Theorem 6.6.

$$R(\underbrace{3, 3, \dots, 3}_{k\text{-tuples}}) =_{\text{def}} R_k(3) \leq \lfloor e \cdot k! \rfloor + 1.$$

Proof. Since $R(3, 3) = 6$, $R(3, 3, 3) = 17$, the assertion is true for $k = 2$ and 3 . Assume that it holds for $k - 1$ when $k > 3$. Hence, $R_{k-1}(3) \leq \lfloor e \cdot (k - 1)! \rfloor + 1$. By Theorem 6.5,

$$\begin{aligned} R_k(3) &\leq k(\lfloor e \cdot (k - 1)! \rfloor + 1) - k + 2 \\ &= k\lfloor e \cdot (k - 1)! \rfloor + 2. \end{aligned}$$

Now,

$$\begin{aligned} k\lfloor e \cdot (k - 1)! \rfloor &= k\lfloor (k - 1)! \cdot (1 + \frac{1}{1!} + \frac{1}{2!} + \dots + \frac{1}{(k - 1)!} + \frac{1}{k!} + \dots) \rfloor \\ &= k\lfloor M + \frac{1}{k} + \frac{1}{k(k + 1)} + \frac{1}{k(k + 1)(k + 2)} + \dots \rfloor \\ &\quad \vdots \\ &= \lfloor e \cdot k! \rfloor - 1. \quad (?) \end{aligned}$$

□

Remark. Instead of $R(s, t)$, we use $R(H_1, H_2)$ to denote the smallest integer n such that any 2-edge-coloring (red, blue) of K_n , either there exists a red H_1 or a blue H_2 .

Edge-coloring

Definition 7.1 (k -edge-coloring). A k -edge-coloring is a mapping $\pi : E(G) \rightarrow \{1, 2, \dots, k\}$ such that incident edges receive distinct images (colors).

Definition 7.2 (Chromatic index). Chromatic index of G $\chi'(G) = \min\{k \mid G \text{ has a } k\text{-edge-coloring}\}$. If $\chi'(G) = k$, then G is h -edge-colorable for each $h \geq k$.

Theorem 7.1 (Vizing, 1964). If G is a simple graph, then $\Delta(G) \leq \chi'(G) \leq \Delta(G) + 1$.

Proof. The left hand inequality is easy to see. We prove the right hand inequality by induction on $\|G\|$. We shall prove that G has a $(\Delta(G) + 1)$ -edge-coloring (coloring in short) for G and the assertion is true for smaller sizes, i.e., for each $e \in E(G)$, $G - e$ has a coloring π .

First, we observe that since each vertex v is of degree at most $\Delta(G)$, a color is missing around v . Second, if α and β are two colors used in the coloring, then α and β induce a subgraph with components either paths or even cycles. Finally, if ' G has no coloring using $\Delta(G) + 1$ colors', then for each edge xy and any coloring of $G - xy$, there exists an $\alpha - \beta$ path from y ends in x provided α is missing at x and β is missing at y . See Figure 7.1 for missing colors.

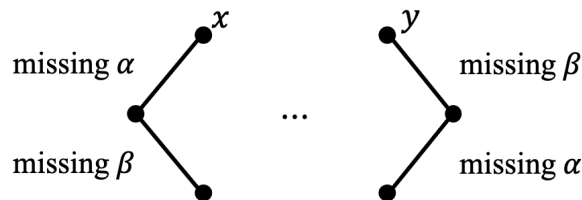


Figure 7.1

Note that if $\alpha - \beta$ path does not connect x and y , then we may recolor one of the path (α, β) to obtain a coloring of G using $\Delta(G) + 1$ colors. Also, if x and y are missing the

same color, then we can use that color to color xy and obtain a $\Delta(G) + 1$ coloring of G . Hence, it suffices to claim that there is a way to recolor some edges in $G - xy$ such that x and y miss the same color.

Proof of claim. (Outline.)

Let $M(y)$ denote the colors missing at y , and $c_1 \in M(y)$. Now, consider $M(x)$. If $c_1 \in M(x)$, then color xy by c_1 results in a $\Delta(G) + 1$ coloring of G . (The claim holds.) Hence, assume $c_1 \notin M(x)$. Let $c_0 \in M(x)$ and $\pi(xy_1) = c_1$, see Figure 7.2. Then, consider $M(y_1)$ and let $c_2 \in M(y_1)$. If $c_2 \in M(x)$, then we let $\pi(xy_1) = c_2$. Thus, c_1 becomes a missing color in $M(x)$, the coloring c_1 is available for xy , $\pi(xy) = c_1$. Hence, assume $c_2 \notin M(x)$. This fact will continue: $c_2 \notin M(x) \Rightarrow \exists y_2$ such that $\pi(xy_2) = c_2$; and then $c_3 \in M(y_2)$, $\pi(xy_3) = c_3$; ...; $c_{i+1} \in M(y_i)$, $\pi(xy_{i+1}) = c_{i+1}$. Since we only have $\Delta(G) + 1$ colors, there exists an l such that $\pi(xy_{l+1}) = c_{l+1} \in \{c_1, c_2, \dots, c_l\}$. W.L.O.G., let $c_{l+1} = c_k$, $k \in \{1, 2, \dots, l\}$. Now, we have several cases to consider depending on whether $c_0 \in M(y_l)$ or $c_0 \notin M(y_l)$.

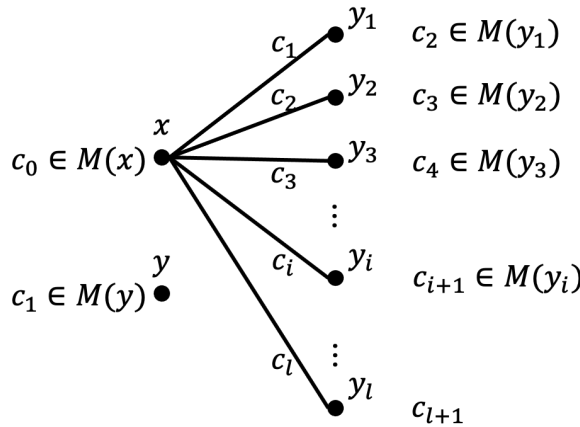


Figure 7.2

Case 1. $c_0 \notin M(y_l)$.

Since $c_{l+1} = c_k$, $c_k \in M(y_l)$. Now, consider $c_k - c_0$ path starting from y_l .

- (i) It is a $y_l - y_k$ path. Since $\pi(xy_k) = c_k$, we may recolor them to a $c_0 - c_k$ path starting from y_k . (Note that c_0 occurs in an edge incident to y_l here. By the fact that the last color is c_k , both c_0 and c_k occur an even number of times.) Now, since $\pi(xy_k) = c_0$, the recoloring of $xy_1, xy_2, \dots, xy_{k-1}$ gives $c_1 \in M(x)$, we have the proof.

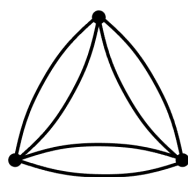
- (ii) It is a $y_l - y_{k-1}$ path. Since $c_k \in M(y_{k-1})$, this path is ended with color c_0 . That is to say c_0 is also available for xy_{k-1} (not only c_{k-1}). Hence, we color xy_{k-1} with c_0 instead of c_{k-1} , the proof follows by a similar recoloring process as above.
- (iii) It is a $y_l - y_i$ path, $i \notin \{k-1, k\}$. Then either c_l or c_0 will be available for xy_i and the proof follows by recoloring process.

Case 2. $c_0 \in M(y_l)$ can be done similarly. □

Base on the same proof technique, we also have a stronger result of Vizing's theorem.

Theorem 7.2 (Vizing, 1964). *If G is a multigraph with multiplicity η , then $\chi'(G) \leq \Delta(G) + \eta$.*

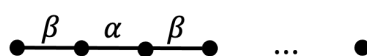
Example. The following graph has $\Delta(G) = 4$ and $\eta = 2$.



Definition 7.3 (Class 1 and Class 2). A graph (simple) is of Class 1 if $\chi'(G) = \Delta(G)$ and of Class 2 if $\chi'(G) = \Delta(G) + 1$.

Theorem 7.3 (König, 1916). *A bipartite graph is of Class 1.*

Proof 1. By induction on $\|G\|$. Let $xy \in E(G)$ and $G - xy$ can be edge-colored with $\Delta(G)$ colors. Now, since $\deg_{G-xy}(x) < \Delta(G)$ and $\deg_{G-xy}(y) < \Delta(G)$, a color is missing at x and also a color is missing at y . Let them be α and β respectively. Clearly, $\alpha \neq \beta$, and β occurs around x and α occurs around y . Now, we adapt the idea in proving Vizing's theorem. Let P be a longest $\alpha - \beta$ path from x :



First, if P is an $x - y$ path and the last edge has color α , then P is a path of even length. Hence, $P \cup \{xy\}$ is an odd cycle. A contradiction to the fact that G is bipartite. Hence,

x and y are in different components induced by the set of edges colored α and β . Now, we recolor all the edges of P by interchanging α and β . This gives a coloring in which β is missing at x and also at y . By coloring xy with β , we obtain a $\Delta(G)$ -edge coloring of G . \square

Proof 2. Let G be a bipartite graph. Then there exists a $\Delta(G)$ -regular bipartite graph $\tilde{G} \geq G$. (Exercise) Since \tilde{G} is a $\Delta(G)$ -regular bipartite graph, \tilde{G} can be decomposed into $\Delta(G)$ perfect matchings by König's theorem. This implies that $\chi'(\tilde{G}) = \Delta(G)$. Since $G \leq \tilde{G}$, $\chi'(G) \leq \chi'(\tilde{G}) = \Delta(G)$. Hence, we conclude the proof. \square

Theorem 7.4. *Petersen graph is of Class 2.*

Proof. If G is the Petersen graph and $\chi'(G) = 3$, then G can be decomposed into three 1-factors: F_1, F_2 and F_3 (three color classes). Now, consider the set of five link-edges e_1, e_2, e_3, e_4 and e_5 , see Figure 7.3.

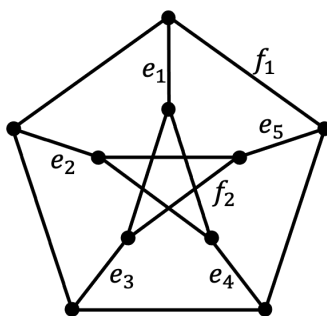


Figure 7.3: Petersen graph.

At least one of F_1, F_2 and F_3 will contain at least two link-edges by Pigeon-hole principle, let it be F_1 . Clearly, F_1 cannot contain all the five link-edges. For otherwise, two C_5 's is the union of F_2 and F_3 which is impossible. So, there are three cases to consider.

Case 1. $|F_1 \cap \{e_1, e_2, \dots, e_5\}| = 4$.

Let e_1 be the edge not in F_1 . But, now all the edges of $G - e_1$ not in $\{e_2, e_3, e_4, e_5\}$ are incident to an edge of $\{e_2, e_3, e_4, e_5\}$. So, no other edge can be chosen for F_1 .

Case 2. $|F_1 \cap \{e_1, e_2, \dots, e_5\}| = 3$.

Let e_1 and e_2 be the edges not in F_1 . Then, other than link-edges, we choose at most

one more edge f_1 . The case e_1 and e_3 are not in F_1 has similar conclusion (only f_2 is available).

Case 3. $|F_1 \cap \{e_1, e_2, \dots, e_5\}| = 2$.

This case comes out that we can find two more edges which are not link-edges. \square

Corollary 7.5. *Petersen graph contains no Hamilton cycles.*

Proof. If G contains a Hamilton cycle C , then $\chi'(G) = 3$ by coloring the cycle with two colors and $G - C$ (1-factor) with another color. \square

Theorem 7.6. *A 3-regular planar graph G is of Class 1.*

Proof. Let G be embedded in S_0 . Then, by 4-color Theorem, G is 4-face-colorable (or 4-map-colorable). Let the 4 colors used be obtained from the group $(\mathbb{Z}_2 \times \mathbb{Z}_2, \oplus)$. Since each edge is in the boundary of two adjacent faces, let the edge be colored by $(a_1, b_1) \oplus (a_2, b_2)$ where (a_1, b_1) and (a_2, b_2) are the colors of these two adjacent faces. As a conclusion, we obtain a 3-edge-coloring of G , since $(0, 0)$ will not be used. The coloring is proper since three adjacent faces will receive three different colors, see Figure 7.4. \square

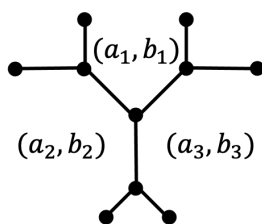


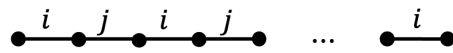
Figure 7.4

Remark. Without using 4CT, the proof is very difficult.

Conjecture 7.1. *If G is planar and $\Delta(G)$ is large enough, then G is of Class 1.*

Theorem 7.7 (Equitable edge-coloring). *If G has a k -edge-coloring f , then G has an equitable edge coloring, i.e., for any two $i, j \in \{1, 2, \dots, k\}$, $\|f^{-1}(i) - f^{-1}(j)\| \leq 1$.*

Proof. If there exist i and j such that $\|f^{-1}(i) - f^{-1}(j)\| \geq 2$, then we consider the graph H induced by the set of edges colored i and j . Then, H is a subgraph of G such that each component of H is either a path or an even cycle. Since i occurs more times than j , there exists an $i - j$ path whose end edges are colored i :



Now, by switching the colors on this path, we obtain a new edge coloring of G such that i occurs one less time and j occurs one more. It turns out that we can obtain an k -edge-coloring such that $\|f^{-1}(i) - f^{-1}(j)\| \leq 1$. As a consequence, we are able to adjust all of them and obtain an equitable k -edge-coloring. \square

Remark. This theorem is not difficult to prove, but very useful.

Definition 7.4 (Overfull). A graph G is said to be overfull if $\|G\| > \lfloor \frac{|G|}{2} \rfloor \cdot \Delta(G)$.

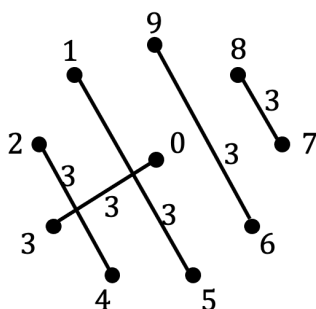
Remark.

- If G is overfull, then G is of Class 2.
- If G is overfull, then $|G|$ is odd.

Theorem 7.8. *The complete graph K_n is of Class 2 if and only if K_n is overfull or equivalently n is odd.*

Proof. First, we claim that for each $m \geq 1$, K_{2m} is of Class 1. It suffices to give a $(2m-1)$ -edge-coloring of K_{2m} . For convenience, let $V(K_{2m}) = \mathbb{Z}_{2m} = \{0, 1, 2, \dots, 2m-1\}$. For each color $i \in \{1, 2, \dots, 2m-1\}$, let the set of edges colored i be $F_i = \{(0, i), (i+1, i-1), (i+2, i-2), \dots, (i+m-1, i-m+1)\} \pmod{2m-1}$. See Figure 7.5 for an example of $m = 5$ and $i = 3$.

Since $\Delta(K_{2m}) = 2m-1$, $\chi'(K_{2m}) = 2m-1$.

Figure 7.5: $\chi'(K_{10}) = 9$.

Now, by deleting 0 in K_{2m} , we obtain a $(2m - 1)$ -edge-coloring of K_{2m-1} . On the other hand, it is not difficult to check that K_{2m-1} is overfull for $m \geq 2$, this concludes that $\chi'(K_{2m-1}) > \Delta(K_{2m-1}) = 2m - 2$. \square

Remark.

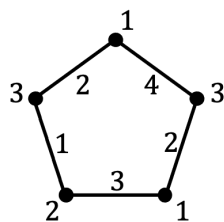
- This theorem is not difficult to prove, but it is very useful in the construction of 'Combinatorial Designs'.
- Equivalently, K_{2m} can be decomposed into $2m - 1$ 1-factors, which is also known as a 1-factorization of K_{2m} .
- If G is an r -regular graph and $\chi'(G) = r$, then G has a 1-factorization.

Conjecture 7.2. *If G is r -regular and $r \geq \frac{|G|}{2}$, then G has a 1-factorization or equivalently $\chi'(G) = r$.*

Theorem 7.9 (D. Hoffman et al.). *A complete multipartite graph G is of Class 2 if and only if G is overfull.*

Definition 7.5 (Total coloring). A k -total coloring of a graph G is a mapping $\varphi : V(G) \cup E(G) \rightarrow \{1, 2, \dots, k\}$ such that

1. adjacent vertices receive distinct images,
2. incident edges receive distinct images, and
3. each vertex has a distinct image with the images of its incident edges.

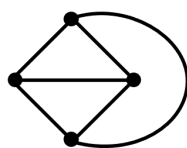
Figure 7.6: A 4-total coloring of C_5 .

Definition 7.6 (Total chromatic number). Total chromatic number of G $\chi''(G) = \min\{k \mid G \text{ has a } k\text{-total coloring}\}$.

Theorem 7.10. $\chi''(K_{2n+1}) = \chi''(K_{2n}) = 2n + 1$.

Proof. $\chi''(K_{2n+1})$ can be obtained by using $\chi'(K_{2n+1}) = 2n + 1$. As to the total coloring of K_{2n} , we claim that $2n$ colors are not enough. (Note that $\chi''(G) \geq \Delta(G) + 1$.) Observe that each color class has at most one vertex and $n - 1$ edges. So, $2n$ color classes will contain at most $2n$ vertices and $2n(n - 1)$ edges. Hence, there are $2n^2$ elements (vertices and edges) in total. But, K_{2n} has $2n + \frac{2n(2n - 1)}{2} = 2n^2 + n$ elements to color. Clearly, $2n$ color is not enough. Since K_{2n+1} is $(2n + 1)$ -total colorable, K_{2n} is also $(2n + 1)$ -total colorable. The proof follows. \square

Example. $\chi''(K_4) = 5$. (?)

Figure 7.7: K_4

Conjecture 7.3 (TCC Conjecture). $\chi''(G) \leq \Delta(G) + 2$.

An Introduction of Extremal Set Theory

Research Problem. Under a constraint or a collection of constraints, find the maximum number of sets satisfying the given constraints.

Clearly, the collection of sets, \mathbb{B} , from \mathbb{X} is also a design (\mathbb{X}, \mathbb{B}) .

Notation.

- $[n] = \{1, 2, \dots, n\}$.
- $\binom{[n]}{k} =_{def}$ the collection of (all) k -subsets of $[n]$.
- $\binom{n}{k} = |\binom{[n]}{k}|$.


Definition 8.1 (Partial ordered set). $\mathbb{X} = \{x_1, x_2, \dots, x_n\}$ is a set of n elements and ' \leq ' is a partial order defined on \mathbb{X} . $\langle \mathbb{X}, \leq \rangle$ is called a partial order set, Poset in short.

Definition 8.2 (Partial order). ' \leq ' is a partial order of \mathbb{X} if

1. Reflexivity: $a \leq a \quad \forall a \in \mathbb{X}$
2. Anti-symmetry: $a \leq b$ and $b \leq a$ imply $a = b \quad \forall a, b \in \mathbb{X}$, and
3. Transitivity: $a \leq b, b \leq c$ imply $a \leq c \quad \forall a, b, c \in \mathbb{X}$.

Definition 8.3 (Total order). ' \leq ' is a total order of Y provided any two distinct elements in Y , y_i and y_j , either $y_i \leq y_j$ or $y_j \leq y_i$. (y_i and y_j are comparable.)

We may use a graph to depict a partial ordered set (Poset), $\langle S, \leq \rangle$. It is known as the Hasse-diagram. Mainly, if $a, b \in S$ and $a \leq b$, then the vertex representing b is higher

than a as: .

For example, $\langle 2^{[4]}, \subseteq \rangle$ can be represented as follows.

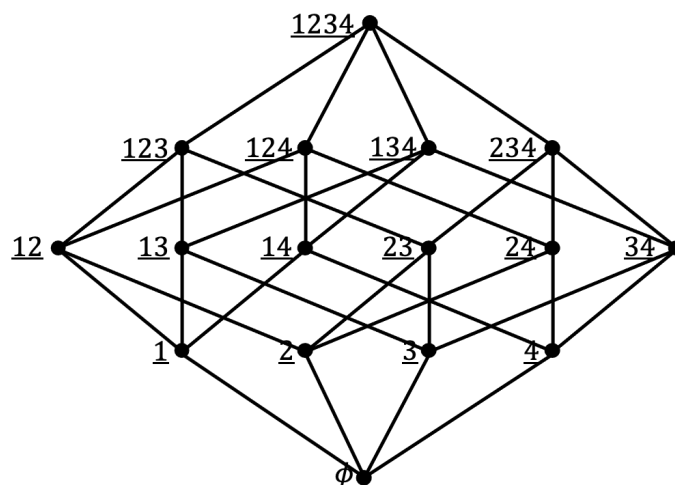


Figure 8.1: Hasse-diagram of $\langle 2^{[4]}, \subseteq \rangle$.

For convenience, this diagram can be considered as a graph (in Figure 8.2) and only the structure will be studied.

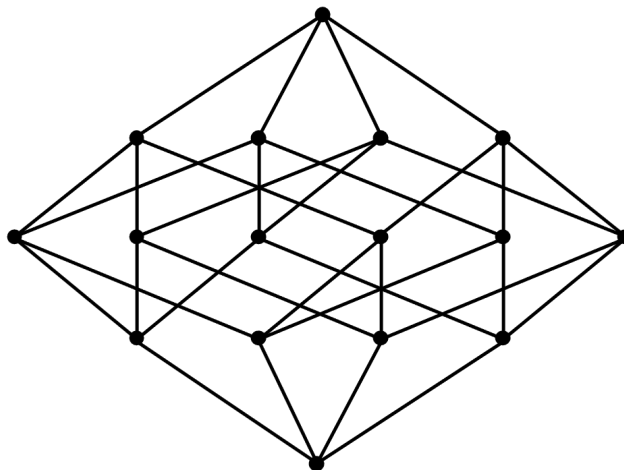


Figure 8.2

Definition 8.4 (Anti-chain, Chain). A subset of a poset in which no two distinct elements are comparable is called an anti-chain. On the other hand, a totally ordered set is called a chain.

Example. The blue vertices are an anti-chain and the orange path is a chain.

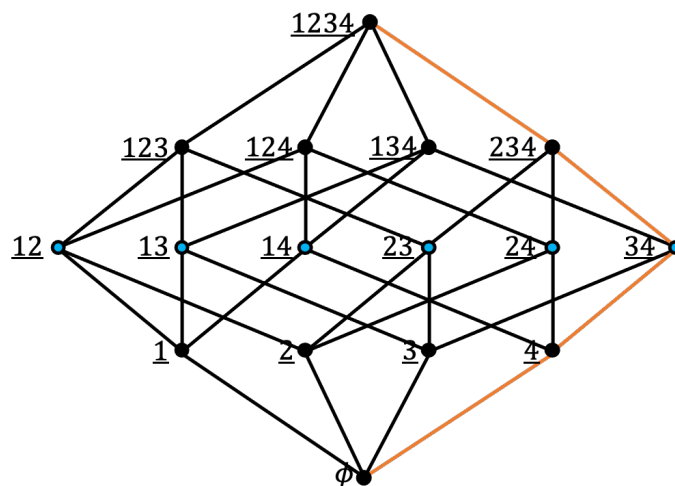


Figure 8.3: Poset with set-containment.

Extremal set problem.

Given a configuration of posets, say $I = P_2 : \begin{matrix} \bullet & x \\ | & \\ \bullet & y \end{matrix}$ ($y \leq x$), find the maximum number of sets in $2^{[n]}$ such that the induced partial ordered set contains no sub-poset which is given, i.e., contains no P_2 .

We can change $I = P_2$ to any kinds of sub-poset. For example, $P_3 : \begin{matrix} \bullet \\ | \\ \bullet \\ | \\ \bullet \end{matrix}$ or S_3 (star of order 3): $\begin{matrix} \bullet & & \bullet \\ & \diagdown & / \\ & \bullet & \\ & | & \\ & \bullet & \end{matrix}$. The result solving case $I = P_2$ is known as the Sperner's theorem.

Theorem 8.1 (Sperner's theorem). *Consider the collection of all subsets of $[n]$. The maximum number of subsets which do not contain each other is equal to $\binom{n}{\lfloor \frac{n}{2} \rfloor}$. (The maximum anti-chain problem.)*

Proof. Let \mathbb{B} be a collection of subsets which do not contain each other and attains the maximum. Furthermore, let a_k be the number of sets in \mathbb{B} whose size is k . Hence, $|\mathbb{B}| = \sum_{k=0}^n a_k$. Note that a_i 's may be zero. Since $\binom{[n]}{\lfloor \frac{n}{2} \rfloor}$ is clearly an anti-chain, $|\mathbb{B}| \geq \binom{n}{\lfloor \frac{n}{2} \rfloor}$.

So, it suffices to prove $|\mathbb{B}| \leq \binom{n}{\lfloor \frac{n}{2} \rfloor}$.

Claim (Lubell-Yamamoto-Meshalkin, LYM inequality). $\sum_{k=0}^n a_k / \binom{n}{k} \leq 1$.

Consider the set of permutations of $[n]$. Clearly, there are $n!$ permutations. Now, for each set $S = \{s_1, s_2, \dots, s_k\}$ in \mathbb{B} , we associate this set with $|S|!(n - |S|)!$ permutations by taking the maximum chain passing $s_1 s_2 \cdots s_k$. ($\emptyset - s'_1 - s'_1 s'_2 - s'_1 s'_2 s'_3 - \cdots - s_1 s_2 \cdots s_k - s_1 s_2 \cdots s_k s'_{k+1} - \cdots - [n]$ where $s'_i \in \{s_1, s_2, \dots, s_k\}$ for $1 \leq i \leq k$.) Note that each permutation can only be associated with a single set in \mathbb{B} . Two sets in \mathbb{B} do not contain each other. Now we have

$$\sum_{S \in \mathbb{B}} |S|!(n - |S|)! = \sum_{k=0}^n a_k \cdot k!(n - k)! \leq n!$$

Hence, $\sum_{k=0}^n a_k \cdot \frac{k!(n - k)!}{n!} \leq 1$.

Since $1 \geq \sum_{k=0}^n a_k / \binom{n}{k} \geq \sum_{k=0}^n a_k / \binom{n}{\lfloor \frac{n}{2} \rfloor}$, $\binom{n}{\lfloor \frac{n}{2} \rfloor} \geq \sum_{k=0}^n a_k = |\mathbb{B}|$. The proof follows. \square

Example. $n = 5$.

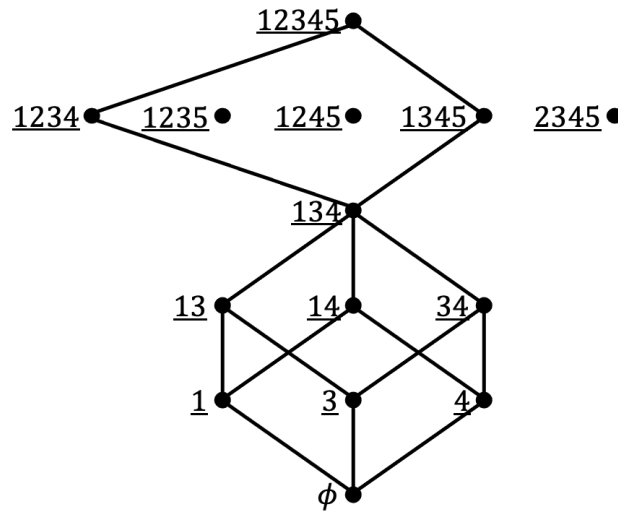


Figure 8.4: $(5 - 3)! \cdot 3!$ maximum chains.

Problem. Find the maximum number of subsets in $2^{[n]}$ such that their induced poset does not contain P_3 . A good guess is $\binom{n}{\lfloor \frac{n}{2} \rfloor} + \binom{n}{\lfloor \frac{n}{2} \rfloor + 1}$. But is it true? Try it!

Problem. Find the maximum collection of sets $B_{n,r}$ of size r which are mutually intersection, that is, $\forall S_1, S_2 \in B_{n,r}, S_1 \cap S_2 \neq \emptyset$. $B_{n,r}$ is called an r -uniform intersection family defined on $[n]$. The following theorem is a beautiful result of this problem.

Theorem 8.2 (Erdős-Ko-Rado, EKR theorem). $|B_{n,r}| = \binom{n-1}{r-1}$ $n \in \mathbb{N}$.

Proof. Let $B = \{S \cup \{n\} \mid S \in \binom{[n-1]}{r-1}\}$. Then, B is an intersection family of $[n]$ since each set contains the element n . Hence, $|B_{n,r}| \geq \binom{n-1}{r-1}$. Next, we prove that $|B_{n,r}| \leq \binom{n-1}{r-1}$.

Observe that if we let (a_1, a_2, \dots, a_n) be a cyclic permutation of $[n]$, then this cycle contains at most r sets of $B_{n,r}$. For example, when $n = 8$ and $r = 3$, let $(3, 1, 8, 2, 7, 5, 6, 4)$ be an arbitrary cyclic permutation. Now, if $\{8, 2, 7\} \in B_{8,3}$, then we have two more possible sets $\{1, 8, 2\}$ and $\{2, 7, 4\}$. So, for general n , we have at most $r \cdot (n-1)!$ sets for intersecting family. By the same idea in Sperner's theorem, each set in $B_{n,r}$ can be associated with $r!(n-r)!$ permutations. Hence, $|B_{n,r}| \cdot r!(n-r)! \leq r \cdot (n-1)!$. Therefore, $|B_{n,r}| \leq \frac{(n-1)!}{(r-1)!(n-r)!} = \binom{n-1}{r-1}$. \square

Example. $|B_{7,3}| = \binom{6}{2} = 15$.

Another good problem to study related to sets.

Let $n = 2t + 1$. We may define a graph G as follows: $V(G) = \binom{[n]}{t}$ and two vertices are adjacent if and only if their intersection is an empty set. The graph G is known as an *odd graph* of order n , denoted by O_n .

Example. O_5 ($n = 5$, $t = 2$). It is in fact the Petersen graph.

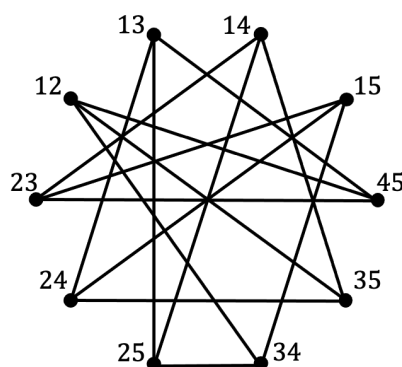


Figure 8.5: O_5 .

Study the structure of O_n is an important problem in both Graph Theory and Design Theory.

If we further require that any two r -sets in $2^{[n]}$ can have at most one element in common, thus exactly one element in common, then the collection of such r -sets, denoted by $B_{n,r}^{(1)}$ has at most $\frac{n(n-1)}{r(r-1)}$ sets.

To see this, we notice that any pair of elements in $[n]$ can occur in at most one r -set of $B_{n,r}^{(1)}$. Hence, the pairs we have in total is $\frac{n(n-1)}{2} = \binom{n}{2}$ and each r -set can use $\binom{r}{2} = \frac{r(r-1)}{2}$ pairs, this implies that $|B_{n,r}^{(1)}| \leq \binom{n}{2} / \binom{r}{2}$.

For some n and r , the equality does hold. For example, $B_{7,3}^{(1)} = \{124, 235, 346, 457, 672, 713\}$ (Fano plane), and $B_{13,4}^{(1)} = \{\{0, 1, 3, 9\} + i \mid i \in \mathbb{Z}_{13}\}$ ($|B_{13,4}^{(1)}| = \frac{13 \times 12}{4 \times 3} = 13$).

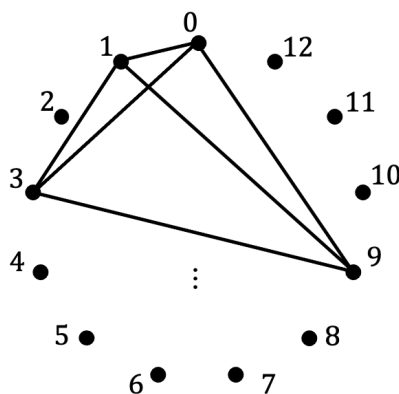


Figure 8.6: $B_{13,4}^{(1)}$

Block Design

The study of the incidence structures between finite sets is one of the most important topics in Combinatorial Theory. There are three basic directions: (1) Finite Geometry, (2) Block Design, and (3) Hypergraph. It is not easy to describe the difference between them. In general, 'Finite Geometry' cares more about the property related to the geometry on a plane, 'Block Design' emphasizes on numerical relationship, and 'Hypergraph' focuses on arbitrarily given edges (finite subsets).

Therefore, to study Block Design, we start with the construction of designs of small order. We also find the necessary conditions for the existence of the kind of designs we would like to obtain. Following that, we then put forth to prove the necessary conditions are also sufficient by constructing all such designs. In general, the part on necessary conditions is comparatively easier. As to construction part, some of the design does not exist even we know the necessary conditions. We shall see that in next section.

Definition 8.5 (Block design). (\mathbb{X}, \mathbb{B}) is a design if \mathbb{X} is a non-empty set and \mathbb{B} is a collection of subsets of \mathbb{X} . If all the subsets are of the same cardinality, then (\mathbb{X}, \mathbb{B}) is called a block design. For convenience, all the sets in \mathbb{B} are referred as blocks in \mathbb{X} .

Definition 8.6 (Simple design). If all the subsets of a design (\mathbb{X}, \mathbb{B}) are all distinct, then it is a simple design. Note that \mathbb{B} can be a multi-set in a design, the blocks with repeated occurrence is known as repeated blocks.

Definition 8.7 (Representation of design). Let $\mathbb{X} = \{x_1, x_2, \dots, x_v\}$ be the set of 'varieties' and $\mathbb{B} = \{B_1, B_2, \dots, B_b\}$ be the set of blocks. Then, we can define a variety-block incidence matrix to represent the design, say \mathbf{A} , and also a bipartite graph to represent (\mathbb{X}, \mathbb{B}) , say $\mathbf{G}_{\mathbb{X}, \mathbb{B}}$. $A = [a_{i,j}]_{v \times b}$ where $a_{i,j} = \begin{cases} 1 & \text{if } x_i \in B_j, \text{ and} \\ 0 & \text{otherwise.} \end{cases}$

Therefore, \mathbf{A} is a $(0, 1)$ -matrix.

Definition 8.8 (Pairwise balanced design, PBD). An (\mathbb{X}, \mathbb{B}) is called a pairwise balanced design (PBD for short) if for any pair of elements in $\binom{\mathbb{X}}{2}$, they occur together in exactly λ blocks of \mathbb{B} . Notice that in PBD, the blocks are not necessarily be of the same. So, it is denoted by $2 - (v, K, \lambda)$ design where $|\mathbb{X}| = v$.

Example.

1. A $2 - (6, \{2, 5\}, 1)$ design: $\mathbb{X} = \mathbb{Z}_6$ and $\mathbb{B} = \{\{0, 1\}, \{0, 2\}, \{0, 3\}, \{0, 4\}, \{0, 5\}, \{1, 2, 3, 4, 5\}\}$.

2. $\mathbb{X} = \mathbb{Z}_v$ and $\mathbb{B} = \binom{\mathbb{Z}_v}{k}$, $k \geq 2$. Then, (\mathbb{X}, \mathbb{B}) is a $2 - (v, k, \lambda)$ design where $\lambda = \frac{r(k-1)}{v-1}$.

Note that $r = \binom{v-1}{k-1} = \frac{(v-1)!}{(k-1)!(v-k)!} = \frac{(v-1)(v-2)\cdots(v-k+1)}{(k-1)!}$,
hence $\lambda = \frac{(v-1)(v-2)\cdots(v-k+1)}{(k-1)!} \cdot \frac{k-1}{v-1} = \binom{v-2}{k-2}$.

Remark. (\mathbb{X}, \mathbb{B}) is also a $t - (v, k, \lambda)$ design for all $2 \leq t \leq k < v$.

The following notions are not related to vector spaces.

Definition 8.9 (Partial linear space, Linear space). An (\mathbb{X}, \mathbb{B}) is called a partial linear space if any two blocks of \mathbb{B} contains at most one common element. If, indeed, any two elements (varieties) of a partial linear space occur together in a block of \mathbb{B} , then (\mathbb{X}, \mathbb{B}) is a linear space with index 1.

Remark. We can use 'Geometry' to refer the above definitions:

- Partial linear space: Any two lines intersect at most one point.
- Linear space: Any two points lie on a line (some line) of a partial linear space.

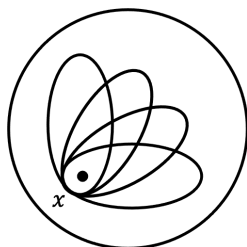
Basic properties of a design.

1. If (\mathbb{X}, \mathbb{B}) is a $2 - (v, k, \lambda)$ design, then we have

(a) for each $x \in \mathbb{X}$, $r_x = r = \frac{\lambda(v-1)}{k-1}$ or $r(k-1) = \lambda(v-1)$.

(b) $b = |\mathbb{B}| = \frac{\lambda v(v-1)}{k(k-1)}$ or $bk = rv$.

Proof. Since x occurs with (each of) all the other $v - 1$ elements exactly in λ blocks, r_x is equal to $\lambda(v - 1)$ possible such pairs divided by the $k - 1$ pairs which can be obtained from a block. (The second equality is a consequence of the above idea by using two-way counting.) This concludes the proof of (a).



As to (b), it is a direct counting of the number of pairs occur in \mathbb{B} via the number of pairs occur in a block. Therefore $|\mathbb{B}| = \frac{\lambda \binom{v}{2}}{\binom{k}{2}}$. The second identity comes from the (total) occurrence of elements. \square

2. (Fisher's inequality) If (\mathbb{X}, \mathbb{B}) is a $2 - (v, k, \lambda)$ design, then $|\mathbb{X}| \leq |\mathbb{B}|$.

Proof. Let A be the incident matrix of (\mathbb{X}, \mathbb{B}) . Then, $AA^T = (r - \lambda)I + \lambda J$, i.e., AA^T is a $v \times v$ matrix such that each entry in the diagonal is r and each entry out side diagonal is λ .

$$AA^T = \begin{matrix} & B_1 & B_2 & \cdots & B_b \\ \begin{matrix} x_1 \\ \vdots \\ x_v \end{matrix} & \left[\begin{array}{cccc} & & & \\ & & & \\ & & & \\ & & & \end{array} \right] & \left[\begin{array}{c} \\ \\ \\ \end{array} \right] \\ & v \times b & & b \times v \end{matrix}$$

Note that $AA^T(i, j)$ is the inner product of the i th row and the j th row. So, if $i = j$, it is the occurrence of x_i ($r_{x_i} = r$) in the blocks of \mathbb{B} , and if $i \neq j$, it is the number of blocks in which x_i and x_j occur together in the blocks, λ .

Now, we can find $\det(AA^T) = k \cdot r \cdot (r - \lambda)^{v-1}$. (Gaussian elimination.) Since $v > k$, $\lambda < r$. This concludes that AA^T is non-singular, i.e., $\text{rank}(AA^T) = v$. Furthermore, $\text{rank}(AA^T) \leq \text{rank}(A) \leq \min\{v, b\}$, hence $b \geq v$.

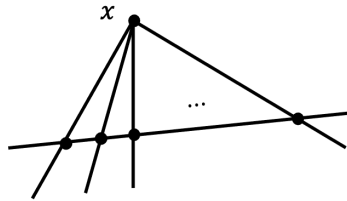
In what follows, we find $\det(AA^T)$ by using its eigenvalues. Since $AA^T = (r - \lambda)I + \lambda J$, an eigenvalue μ satisfies $(AA^T)x = \mu x = (r - \lambda)x + \lambda Jx = (r - \lambda)x + \lambda \mu' x$ where

μ' is an eigenvalue of J . By the fact that J is of rank 1, the set of eigenvalues of J are $\{v, 0, 0, \dots, 0\}$ (0 with multiplicity $v - 1$). Hence, $\mu x = ((r - \lambda) + \lambda\mu')x$. This implies that $\mu = r - \lambda$ ($v - 1$ of them) and $\mu = r - \lambda + \lambda v = r + \lambda(v - 1) = r + (k - 1)r = kr$. Thus, $\det(AA^T) = k \cdot r \cdot (r - \lambda)^{v-1}$.

(Note here that using the spectrum of an adjacency matrix of a graph is one of the main subjects of **Algebraic Graph Theory**.) □

Theorem 8.3. *If (\mathbb{X}, \mathbb{B}) is a linear space, then $|\mathbb{X}| \leq |\mathbb{B}|$.*

Proof. Again, let $|\mathbb{X}| = \{x_1, x_2, \dots, x_v\}$ and $\mathbb{B} = \{B_1, B_2, \dots, B_b\}$. Since (\mathbb{X}, \mathbb{B}) is a linear space, any two elements in \mathbb{X} occur together in a block of \mathbb{B} . Assume that $b \leq v$. Here is an important observation: If $x \notin B_i$, then $r_x \geq |B_i|$ since each element of B_i is going to occur together with x in some other blocks in \mathbb{B} .



Now, we are ready for the following statements.

$$1 = \sum_{B \in \mathbb{B}} \frac{1}{b} = \sum_{B \in \mathbb{B}} \left(\sum_{x \notin B} \frac{1}{b(v - |B|)} \right) \tag{1}$$

$$1 = \sum_{x \in \mathbb{X}} \frac{1}{v} = \sum_{x \in \mathbb{X}} \left(\sum_{B \not\ni x} \frac{1}{v(b - r_x)} \right) \tag{2}$$

$$vr_x \geq b|B| \text{ for each } x \notin B \quad (v \geq b). \tag{3}$$

By (1), (2) and (3),

$$\frac{1}{b} = \sum_{x \notin B} \frac{1}{b(v - |B|)} \leq \sum_{B \not\ni x} \frac{1}{v(b - r_x)} = \frac{1}{v}$$

we have $b \geq v$, a contradiction. Hence, $b \geq v$. □

Remark. The equality $v = b$ also shows that $r_x = |B|$ for each $x \in \mathbb{X}$ and $B \in \mathbb{B}$. The implication of this fact is that any two blocks intersect at exactly one element, i.e., $|B_i \cap B_j| = 1$ for all $1 \leq i \neq j \leq b$.

Definition 8.10 (Projective plane). (\mathbb{X}, \mathbb{B}) is a projective plane if $(|\mathbb{X}| = |\mathbb{B}|)$ and (\mathbb{X}, \mathbb{B}) is a linear space.

Definition 8.11 (SBIBD). A BIBD is a square BIBD, denoted by SBIBD, if $v = b$.

The following Theorem is well-known, we state it and omit the proof here. (It is a 'necessary condition' for the existence of an SBIBD.)

Theorem 8.4 (Bruck-Ryser-Chowla, 1949-1950). *If a $2 - (v, k, \lambda)$ design is a square BIBD, then*

1. $k - \lambda$ is a square of an integer when v is even; and
2. $z^2 = (k - \lambda)x^2 + (-1)^{\frac{v-1}{2}} \cdot \lambda y^2$ has a nonzero integral solution when v is odd.

Remark. (1) is easy to see: $\det(AA^T) = \det(A)^2 = kr(r - \lambda)^{v-1} = k^2(k - \lambda)^{v-1}$ ($v = b$ implies $r = k$). However, the proof of (2) is quite complicate, we omit it.

Special designs related to Geometry.

Definition 8.12 (Projective plane and Affine plane). A Steiner 2-design $S(2, n + 1, n^2 + n + 1)$ is called a projective plane of order n , denoted by $PG(2, n)$. A Steiner 2-design $S(2, n, n^2)$ is an affine plane of order n , denoted by $AG(2, n)$.

Facts.

1. The existence of a $PG(2, n)$ is 'equivalent' to the existence of an $AG(2, n)$.

Proof. (More details will be given later.)

$$\begin{array}{ccc} PG(2, n) & \xrightarrow{\text{deleting a block}} & AG(2, n) \\ AG(2, n) & \xrightarrow{\text{adding a line at infinity}} & PG(2, n) \end{array}$$

□

2. A $PG(2, n)$ does exist for each n when n is a prime power.

3. No other kind of $PG(2, n)$ has been founded.
4. A $PG(2, n)$ does not exist for $n = 1, 2, 6, 10$ and possibly others.
5. We can extend $AG(2, n)$ and $PG(2, n)$ to $AG(d, n)$ and $PG(d, n)$ for $d \geq 3$ respectively. But, the constructions are getting harder.

Example.

$$1. \ n = 2, \ AG(2, 2) : \ \mathbb{X} = \mathbb{Z}_4, \ \mathbb{B} = \underbrace{\{\{0, 1\}, \{2, 3\}, \{1, 2\}, \{0, 3\}, \{1, 3\}, \{0, 2\}\}}_{\text{parallel classes}}.$$

$$2. \ n = 2, \ PG(2, 2) : \ \mathbb{X} = \mathbb{Z}_7, \ \mathbb{B} = \{\{0, 1, 4\}, \{2, 3, 4\}, \{0, 2, 5\}, \{1, 3, 5\}, \{0, 3, 6\}, \{1, 2, 6\}, \{4, 5, 6\}\}.$$

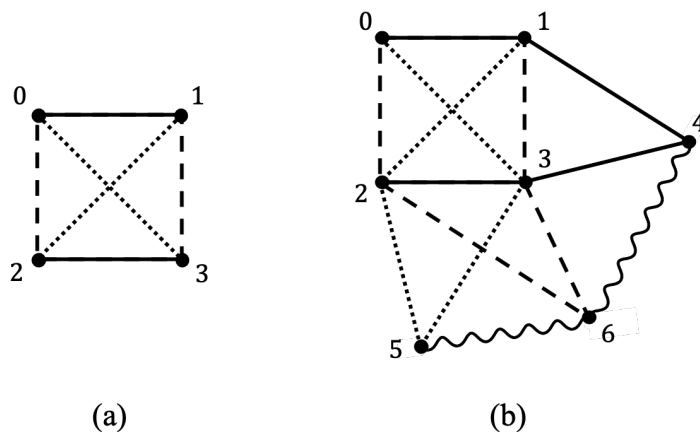


Figure 8.7: (a) $AG(2, 2)$. (b) $PG(2, 2)$.

Remark.

- A $PG(2, n)$ is a symmetric design, i.e., $|\mathbb{X}| = |\mathbb{B}|$.
- An $AG(2, n)$ contains parallel classes, each has n blocks. In fact, there are $n + 1$ parallel classes.
- A parallel class of a design is a collection of blocks B_1, B_2, \dots, B_t such that $\cup_{i=1}^t B_i = \mathbb{X}$.

Latin Square

The notion (concept) of 'Latin Square' probably originated with problems concerning the movement and disposition of pieces on a chess board. Its applications on agricultural design (a special type of experimental design) came out during mid-20 century. So, it is assumed to be a fairly new subject comparing to the other fields of combinational topics.

In fact, the earliest reference to the use of such squares can be dated back to 10 century. At that time, people are placing the sixteen court cards (A, K, Q, J) of a pack of ordinary playing cards in the form of a square so that no row, column, or diagonal should contain more than one card of each suit and one card of each rank. The solution was obtained in 1723. Here is an example.

	A_1	K_2	Q_3	J_4
A		K	Q	J
	1	2	3	4
Q		J	A	K
	4	3	2	1
J		Q	K	A
	2	1	4	3
K		A	J	Q
	3	4	1	2

Figure 9.1

But, the real impact comes from the famous **36 officers problem** proposed by Euler around 10 years later. So, 16 cards are extended to 36 cards. Unfortunately, this plan turns out to be impossible. The proof by 'brute force' was obtained around 1900 by Tarry. A theoretical argument to show that it is not possible came out after around 80 years by D. R. Stinson (1984).

Nowadays, the applications of using Latin Squares have been everywhere.

Definition 9.1 (Latin Square of order n). A Latin square of order n , L , is an $n \times n$ array based on a n -set S (\mathbb{Z}_n for convenience) such that each element of S occurs in each row and each column exactly once.

Example. Latin square of order 3. Note that we can use any n -set for S , say $S = \{\alpha, \beta, \gamma\}$.

	1 st	2 nd	3 rd				
	↓	↓	↓				
1 st →	0	1	2	≅			
2 nd →	1	2	0		α	β	γ
3 rd →	2	0	1		β	γ	α

Figure 9.2: Latin square of order 3.

We use $L_{i,j}$ to denote that (i, j) -entry in L where i (resp. j) is the row (resp. column) number. If L is of order n , then the row (column) numbers are $1, 2, \dots, n$. (Even we use $0, 1, 2, \dots, n-1$ for the number of side line or head line.)

Facts.

1. A Latin square of order n exists for each $n \in \mathbb{N}$.
2. A Latin square of order n can be obtained from the fact $\chi'(K_{n,n}) = n$ (edge coloring of $K_{n,n}$).
3. The existence of a Latin square of order n is equivalent to the existence of $K_3 \mid K_{n,n,n}$ (graph decomposition).
4. Let l_n denoted the number of distinct Latin sequences of order n . Then, $l_1 = 1$, $l_2 = 2$, $l_3 = 12$, $l_4 = 576$, $l_5 = 161280$, ($L \neq L'$ if and only if $L_{i,j} \neq L'_{i,j}$ for some (i, j) .)
5. $l_9 = 9!8!$ (377, 597, 964, 258, 816). Check Wiki for more information!

A Latin square of order n can be obtained from the operation table of a 'quasigroup' of order n . For example, $S = \{0, 1, 2\}$, $\langle S, * \rangle$ is a quasigroup of order 3.

*	0	1	2
0	0	1	2
1	1	2	0
2	2	0	1

Figure 9.3: Quasigroup of order 3.

By using permutations of 0, 1, 2, 3, we can obtain a Latin square of 'standard form':

$3!$	↓					
		0	1	2	3	← $4!$
	{	1				
		2				
		3				

Now, there are 4 ways to finish filling all the other entries by choosing 'typical' entries first (circled entry in Figure 9.4). (Similar to Sudoku.)

0	1	2	3		0	1	2	3		0	1	2	3
1	0	3	2		1	2	3	0		1	3	0	2
2	3	0/1	1/0		2	3	2	1		2	0	1	3
3	2	1/0	0/1		3	0	1	2		3	2	3	1
		↑	↑				↑	↑			↑	↑	
		2 choices	2 choices			1 choice	1 choice			1 choice	1 choice		

Figure 9.4: 4 non-isomorphic Latin squares of order 4.

Basically, this is the idea of counting distinct Latin squares. Hence, $\ell_4 = 4 \times 4! \times 3! = 576$, $\ell_5 = (?) \times 5! \times 4!$, $(?) = 56$. $(?)$

Algebraic Structure

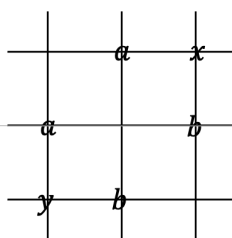
Definition 9.2 (Binary operation). A binary operation defined on A is a mapping $\circ : A \times A \rightarrow A$. For convenience, $\circ((c, b)) = c$ is denoted by $a \circ b = c$.

Remark. For $t \geq 2$, we can define a t -ary operation defined on A as a mapping $f : A^t \rightarrow A$.

Definition 9.3 (Algebraic structure in one operation). An order pair $\langle A, \circ \rangle$ is a *groupoid* if ' \circ ' is a binary operation defined on A .

Besides binary operation, an operation may satisfy more 'laws':

- ① Associative law: $\forall a, b, c \in A, a \circ (b \circ c) = (a \circ b) \circ c$.
- ② Commutative law: $\forall a, v \in A, a \circ b = b \circ a$.
- ③ Identity: e is an identity of $\langle A, \circ \rangle$ if $\forall a \in A, a \circ e = e \circ a = a$.
Right identity: $a \circ e = a$.
Left identity: $e \circ a = a$.
- ④ Inverse: a is an inverse of b (in A) if $a \circ b = b \circ a = e$.
Right inverse: $a \circ b = e$.
Left inverse: $b \circ a = e$.
- ⑤ Row Latin property: $\forall a, b \in A, a \circ x = b$ has a unique solution in A .
- ⑥ Column Latin property: $\forall a, b \in A, y \circ a = b$ has a unique solution in A .



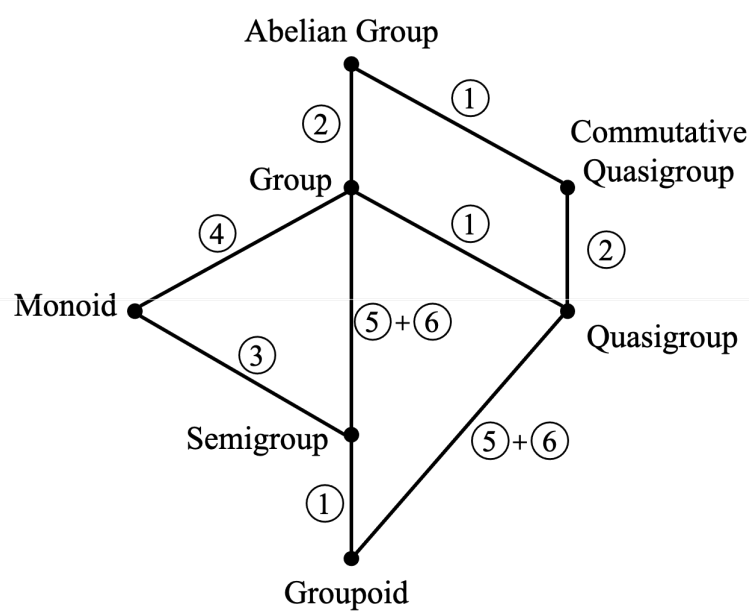
Remark.

- If ⑤ is true, then the row ' a ' has distinct entries, further more, all elements in A occur! (If we have two common entries in a row, then ' x ' is not unique.)
- If ⑥ is true, then the column ' a ' has distinct entries of A . (Similar reason.)

Definition 9.4 (Quasigroup). If $\langle A, \circ \rangle$ satisfies row and column Latin properties, then $\langle A, \circ \rangle$ is a quasigroup. If A is a finite set, then its operation table corresponds to a Latin square of order $|A|$.

Some basic structures. ($\textcircled{0}$: $\langle A, \circ \rangle$ is a groupoid.)

1. $\textcircled{0} + \textcircled{1} = \text{Semigroup}$
2. $\textcircled{0} + \textcircled{1} + \textcircled{3} = \text{Monoid}$
3. $\textcircled{0} + \textcircled{1} + \textcircled{3} + \textcircled{4} = \text{Group}$
4. $\textcircled{0} + \textcircled{1} + \textcircled{2} + \textcircled{3} + \textcircled{4} = \text{Abelian Group}$
5. $\textcircled{0} + \textcircled{5} + \textcircled{6} = \text{Quasigroup}$
6. $\textcircled{0} + \textcircled{1} + \textcircled{5} + \textcircled{6} = \text{Group}$
7. $\textcircled{0} + \textcircled{2} + \textcircled{5} + \textcircled{6} = \text{Commutative Quasigroup}$



Definition 9.5 (Idempotent and Unipotent). A quasigroup $\langle Q, * \rangle$ is idempotent if for each $a \in Q$, $a * a = a$. $\langle Q, * \rangle$ is unipotent if for each $a \in Q$, $a * a = c$ (a constant in Q).

Example.

0	3	1	4	2
3	1	4	2	0
1	4	2	0	3
4	2	0	3	1
2	0	3	1	4

(a)

0	1	2	3
1	0	3	2
2	3	0	1
3	2	1	0

(b)

Figure 9.5: (a) Idempotent and commutative L.S. $\approx \chi'(K_n) = n$ (n is odd).

(b) Unipotent and commutative L.S. $\approx \chi'(K_n) = n - 1$ (n is even).

Remark. To construct an idempotent commutative Latin square for each odd n , we define an abelian group $\langle \mathbb{Z}_n, + \rangle$. For example, $n = 7$. Then, permuting the entries.

+	0	1	2	3	4	5	6
0	0	1	2	3	4	5	6
1	1	2	3	4	5	6	0
2	2	3	4	5	6	0	1
3	3	4	5	6	0	1	2
4	4	5	6	0	1	2	3
5	5	6	0	1	2	3	4
6	6	0	1	2	3	4	5

Figure 9.6: Operation table of $\langle \mathbb{Z}_7, + \rangle$.

Facts.

6. We shall adapt the property of a quasigroup of order n to 'claim' the property of its corresponding Latin square.

For example, if $\langle Q, * \rangle$ is a commutative quasigroup of order n , then its corresponding Latin square is a commutative Latin square or sometimes a 'symmetric' Latin square.

7. Let $\langle Q, * \rangle$ be a quasigroup. Define $\langle Q, \circ \rangle$ where $a \circ c = b$ provided $a * b = c$ for all $a, b, c \in Q$. Then, $\langle Q, \circ \rangle$ is also a quasigroup (conjugate).

Note that $a * b = c \Rightarrow a \circ c = b$, $b \circ' a = c$, $\underline{b \circ'' c = a}$, $c \circ''' a = b$, $c \circ'''' b = a$.

$\forall a, b \in Q$, $a \circ'' x = b$ has unique solution $c \in Q$ since $c * b = a$. Similarly, $y \circ'' a = b$ has a solution c' if $a * b = c'$. They are called conjugate quasigroups and therefore we have conjugate Latin squares of order 3.

\circ	0	1	2
0	0	1	2
1	1	2	0
2	2	0	1

$*$	0	1	2
0	0	1	2
1	2	0	1
2	1	2	0

$0 \circ 0 = 0$	$0 \circ 0 = 0$
$0 \circ 1 = 1$	$0 \circ 1 = 1$
$0 \circ 2 = 2$	$0 \circ 2 = 2$
$1 \circ 0 = 1$	$1 \circ 1 = 0$
$1 \circ 1 = 2$	$1 \circ 2 = 1$
$1 \circ 2 = 0$	$1 \circ 0 = 2$
$2 \circ 0 = 2$	$2 \circ 2 = 0$
$2 \circ 1 = 0$	$2 \circ 0 = 1$
$2 \circ 2 = 1$	$2 \circ 1 = 2$
$\uparrow \quad \uparrow \quad \uparrow$	$\uparrow \quad \uparrow \quad \uparrow$
$a \quad b \quad c$	$a \quad c \quad b$

Figure 9.7: Conjugate quasigroups.

Definition 9.6 (Isotopism). Two quasigroups $\langle Q_1, \circ \rangle$ and $\langle Q_2, * \rangle$ are isotopic if there exist three bijections α , β and γ from Q_1 onto Q_2 such that $\gamma(x \circ y) = \alpha(x) * \beta(y)$ for any two elements $x, y \in Q_1$. If $\alpha = \beta = \gamma$, then $\langle Q_1, \circ \rangle$ and $\langle Q_2, * \rangle$ are isotopic.

Remark.

- If $\langle Q_1, \circ \rangle$ and $\langle Q_2, * \rangle$ are isotopic, then we say there exists an isotopism between $\langle Q_1, \circ \rangle$ and $\langle Q_2, * \rangle$. Check that 'isotopism' is an equivalence relation!
- Since isotopism is an equivalence relation, we can partition the set of distinct Latin squares of order n into isotopic classes. For example, there are two isotopic classes of order 4 and 22 isotopic classes of order 6. (Only one isotopic class for order 1, 2 and 3; and two classes for order 4.)

Partial Latin Square

Over past 30 years, several important progress in solving open problems on Latin squares has been done by applying graph technique. The main idea comes from the following correspondence.

Let $G = (V, E)$ be a graph. A k -edge-coloring π of G is a mapping $\pi : E \rightarrow \{1, 2, \dots, k\}$ such that $\pi(e) \neq \pi(f)$ provided e and f are incident edges in G . The minimum integer k such that G has a k -edge-coloring is called the chromatic index of G , denoted by $\chi'(G)$. The following facts are well-known in Graph Theory.

Facts.

8. If G is a simple graph, then $\Delta(G) \leq \chi'(G) \leq \Delta(G) + 1$.
9. If G is a bipartite graph, then $\chi'(G) = \Delta(G)$.
10. The edge-coloring $\chi'(K - n, n)$ corresponds to a Latin square of order n .

Remark.

- The number of distinct n -edge-colorings of $K_{n,n}$ gives ℓ_n , see Figure 9.8.

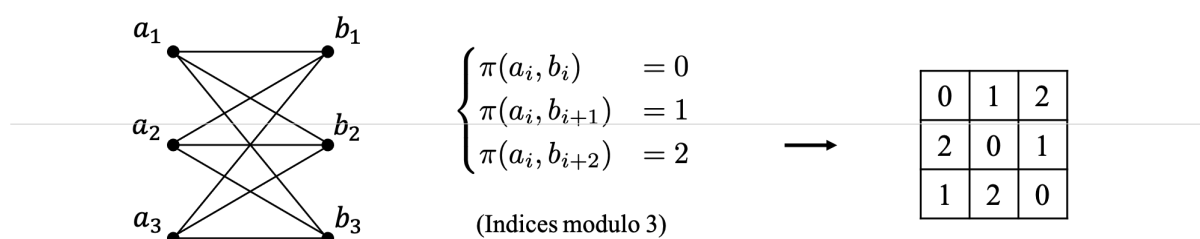
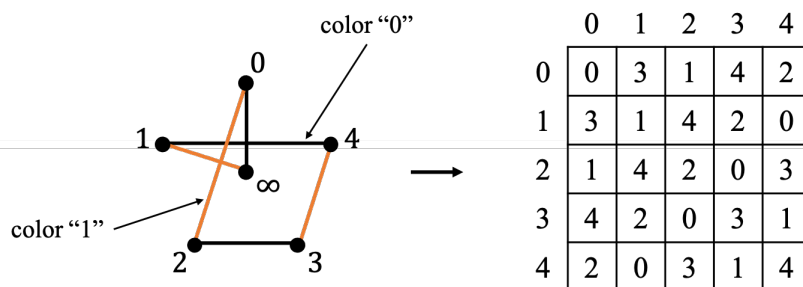


Figure 9.8: $n = 3$.

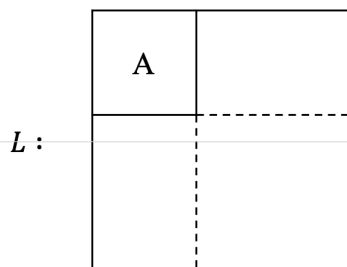
- A unipotent Latin square of order n can be constructed accordingly.
- We can use $\chi'(K_{2m+1}) = 2m + 1$ to construct an idempotent commutative Latin square, see Figure 9.9.
- There does not exist an idempotent commutative Latin square of even order.

Figure 9.9: $m = 2$.

Just like algebraic structures, we have sub-quasigroups and subsquares.

Definition 9.7 (Sub-Latin square). If $Q' \subseteq Q$, $\langle Q', \circ \rangle$ and $\langle Q, \circ \rangle$ are quasigroups, then $\langle Q', \circ \rangle$ is called a sub-quasigroup of $\langle Q, \circ \rangle$. Their corresponding Latin squares are Latin square and Latin subsquare respectively.

Definition 9.8 (Embedding). If A is a sub-Latin square (or Latin subsquare) of L , then A is said to be embedded in L . The standard form is the one with A in the upper left hand corner.



Theorem 9.1. A Latin subsquare of order m can be embedded in a Latin square of order n if and only if $n \geq 2m$.

Facts.

11. If L (of order n) has a Latin subsquare A (of order m), then n may not be a multiple of m . (It is true $m \mid n$ if both L and A are corresponding to a group.)

In what follows, we provide some more insight above having a subsquare.

Proposition 9.2. *If A is embedded in L and $L(i)$ denotes the number of element i occurs in L (respectively A, B, C, D in Figure 9.10), then $A(i) \geq 2m - n$ where A is a Latin square of order m and L is a Latin square of order n .*

Proof. $\forall i \in \mathbb{Z}_n$, since $B(i) + D(i) = n - m$, $B(i) \leq n - m$ and $A(i) + B(i) = m$. Hence, $A(i) = m - B(i) \geq m - (n - m) = 2m - n$. \square

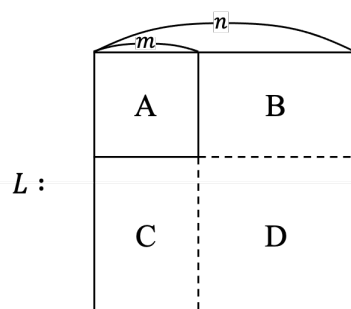


Figure 9.10

Corollary 9.3. *A Latin subsquare of order m can be embedded in a Latin square of order n , then $n \geq 2m$. (The sufficient condition of Theorem 9.1 is true.)*

Proof. If $n < 2m$, then every $i \in \mathbb{Z}_n$ has to occur in A , which is not possible since A is a Latin square of order m . \square

Remark. The subsquare A we consider here can be replaced by Latin rectangle or partial Latin rectangle, denoted as R .

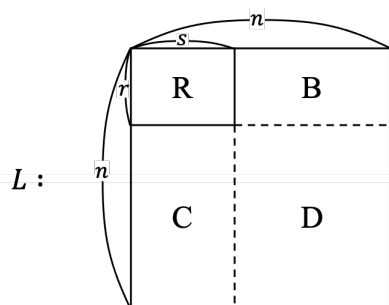


Figure 9.11

Proposition 9.4. *If R is embedded in a Latin square L which is based on S , then $\forall i \in S$, $R(i) \geq r + s - n$.*

Proof. $R(i) + B(i) = r$, $B(i) + D(i) = n - s$ and $B(i) \leq n - s$. Hence, $R(i) = r - B(i) \geq r - (n - s)$. \square

Proposition 9.5. *Let R be a $r \times n$ Latin rectangle based on an n -set S . Then R can be embedded in a Latin square of order n .*

Proof. SDR (system of distinct representatives) or König's Theorem. \square

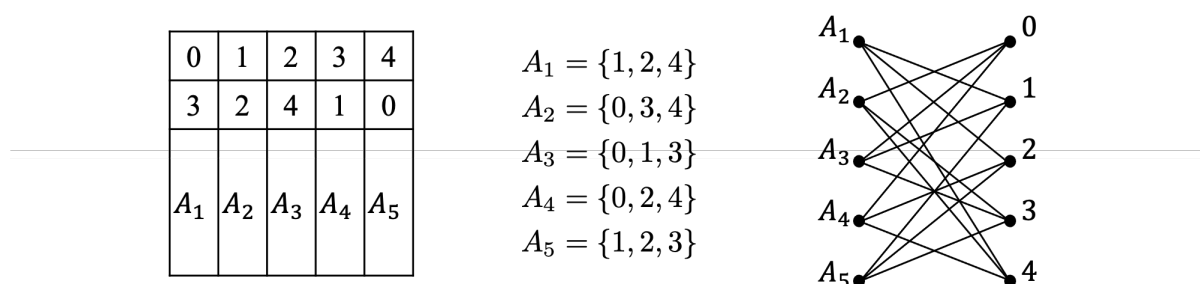


Figure 9.12

Proposition 9.6. *Let R be a $r \times n$ partial Latin rectangle. Then R can be embedded in a Latin square of order n based on S if and only if $R(i) \geq r + s - n \forall i \in S$ ($|S| = n$).*

Proof. (Outline)

Step 1. Fill all the entries in R such that the condition $R(i) \geq r + s - n$ holds.

Step 2. Fill in the entries in B . (Obtain a $n \times n$ Latin rectangle.)

Step 3. Complete the Latin square by extending the rectangle. The details are obtained by using two theorems related to the existence of SDR's. (?) \square

Critical Sets

It is interesting to know whether a $PLS(n)$ can be completed to a Latin square.

Facts.

1. A $PLS(n)$ with at most $n - 1$ filled cells can be completed to a Latin square of order n . (Evan's conjecture)

In fact, the proof of this fact is not very difficult, and was proved by B. Smetaniuk in 1981. You may refer to 'A course in combinatorics' by J.H van Lint and R.M. Wilson, page 189-193.

2. It takes about 50 pages to characterize a $PLS(n)$ with at most $n + 1$ filled cells which is in completable. (L.D. Anderson and A.J.W. Hilton, 1983, LMS.)

0	1	2	
			3

0			
	0		
		0	
			1

Figure 10.1: n filled cells may be too much!

Definition 10.1 (Critical set). A partial Latin square C is called a critical set of a Latin square L if

1. the empty cells of C can be filled to obtain L , and
2. any proper sub-partial square of C can be completed to at least two distinct Latin squares (one of them is L).

Remark.

- A critical set of order n contains at least $n - 1$ distinct elements and covers at least $n - 1$ rows and $n - 1$ columns.
- Sudoku is a special critical set of order 9.

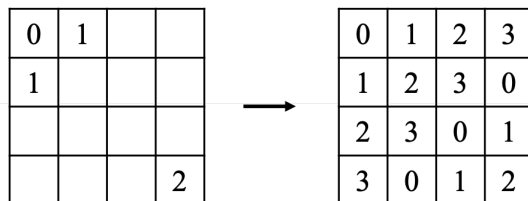


Figure 10.2: A critical set.

Facts.

- 3. We can construct a (strong) critical set C of order n with $|C| = \lfloor \frac{n^2}{4} \rfloor$.

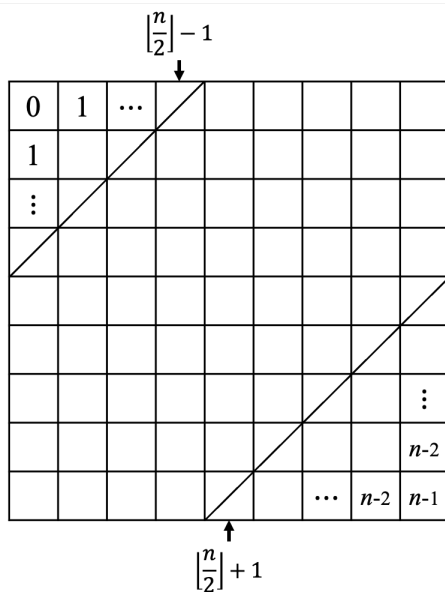
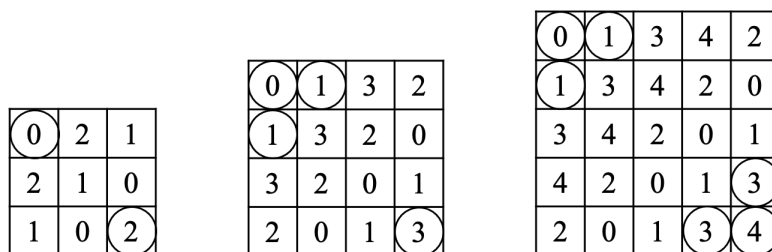


Figure 10.3

Problem. If C is a critical set of order n , then find $\min |C|$ and $\max |C|$.

Conjecture 10.1. $|C| \geq \lfloor \frac{n^2}{4} \rfloor$.

Construction of Latin squares with many subsquares

First, we consider the operation of two Latin squares.

Definition 10.2 (Direct product). Let A and B be two Latin squares based on \mathbb{Z}_m and \mathbb{Z}_n respectively. Then, the direct product of A and B , denoted by $A \otimes B$ is a Latin square of order nm based on $\mathbb{Z}_m \times \mathbb{Z}_n$ such that the entry $A_{i,j} = x$ is replaced by (x, B) where (x, B) is a Latin square of order n where the (i', j') entry is filled by $(x, B_{i',j'})$.

Example.

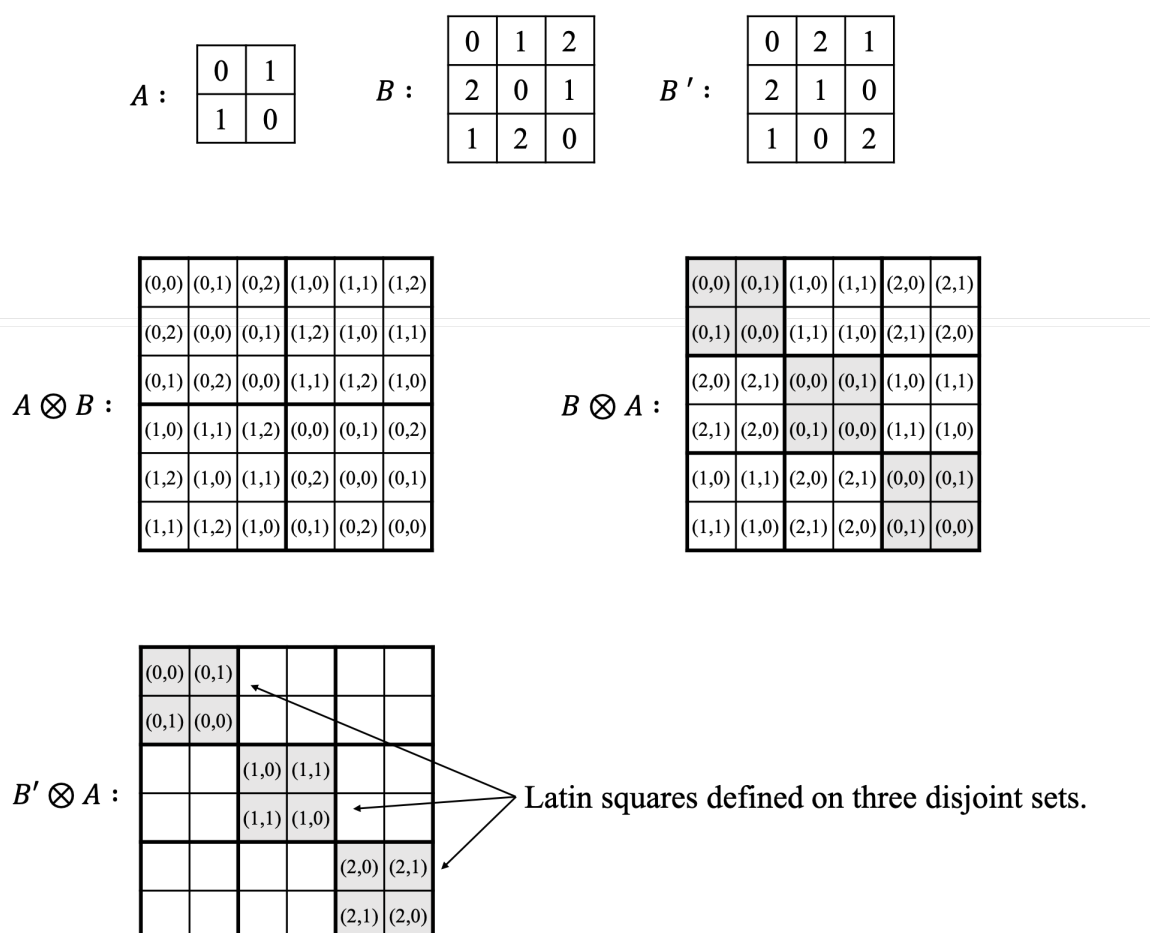


Figure 10.4

Remark.

- $B' \otimes A$ is referred to as a Latin square with 2×2 holes.
- Let $n = h_1 + h_2 + \dots + h_t$. If L is a Latin square of order n with t subsquares of order h_1, h_2, \dots, h_t (as above), then L is a Latin square with holes of type $h_1 \times h_2 \times \dots \times h_t$.

Problem. Construct a Latin square L of order 12 such that L is commutative and also with holes of type 2^6 .

Remark. If m is odd, then L can be constructed by using direct product. But for even m , it takes some effort!

Example. $m = 4$.

1	2	8	5	4	7	6	3
2	1	6	7	8	3	4	5
8	6	4	3	7	2	8	1
5	7	3	4	1	8	2	6
4	8	7	1	6	5	3	2
7	3	2	8	5	6	1	4
6	4	5	2	3	1	8	7
3	5	1	6	2	4	7	8

$2m \times 2m$

Figure 10.5

Orthogonal Latin Squares

Definition 10.3 (Orthogonal Latin squares). Two Latin squares of order n based on \mathbb{Z}_n (We use \mathbb{Z}_n throughout of this lecture), $L = [l_{i,j}]$ and $M = [m_{i,j}]$, are orthogonal if $\{(l_{i,j}, m_{i,j}) \mid 1 \leq i, j \leq n\} = \mathbb{Z}_n^2$, denoted as $L \perp M$.

Example.

0	1	2	\perp	0	1	2
1	2	0		2	0	1
2	0	1		1	2	0
L				M		

Figure 10.6

Proposition 10.1. Let $\alpha(L)$ denote the Latin square which is obtained from L by permuting the entries of L with α (permutation of \mathbb{Z}_n). If $L \perp M$, then $\alpha(L) \perp \beta(M)$ for any two permutation α and β for \mathbb{Z}_n .

Example. Let $\alpha = \begin{pmatrix} 0 & 1 & 2 \\ 1 & 2 & 0 \end{pmatrix}$, $\beta = \begin{pmatrix} 0 & 1 & 2 \\ 0 & 2 & 1 \end{pmatrix}$. Then we have $\alpha(L) \perp \beta(M)$.

1	2	0	\perp	0	2	1
2	0	1		1	0	2
0	1	2		2	1	0
$\alpha(L)$				$\beta(M)$		

Figure 10.7

Proposition 10.2 (Two Finger's rule). $L \perp M$ if and only if $y \neq z$ in M whenever their corresponding entries in L are the same entry, i.e., $l_{i,j} = l_{i',j'} \implies m_{i,j} \neq m_{i',j'}$.

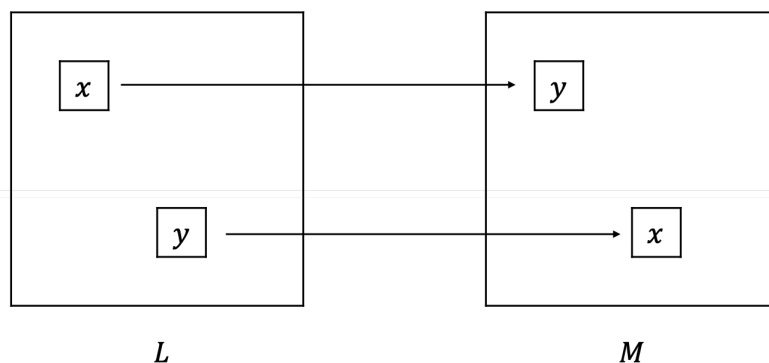


Figure 10.8: Corresponding entries.

Proposition 10.3. *If $L_1 \perp L_2$ (of order m) and $M_1 \perp M_2$ (of order n), then $(L_1 \otimes M_1) \perp (L_2 \otimes M_2)$ (of order mn). ($L_1 \perp L_2$, $M_1 \perp M_2$ and $N_1 \perp N_2 \implies (L_1 \otimes M_1) \otimes N_1 \perp (L_2 \otimes M_2) \otimes N_2$ and more.)*

Proposition 10.4. *If n is a prime power, then there exist $n - 1$ Latin squares of order n , L_1, L_2, \dots, L_{n-1} , which are mutually orthogonal, i.e., $L_i \perp L_j$ for any two $1 \leq i \neq j \leq n - 1$.*

Proof. Since n is a prime power, we have a finite field $GF(n)$, $\langle F, +, \cdot \rangle$. Let $F^* = F \setminus \{0\}$. For convenience, let $F = \{0 = \alpha_0, \alpha_1, \dots, \alpha_{n-1}\}$. Now, for $0 \leq i, j \leq n - 1$, we define $L_{i,j}^{(h)} = \alpha_i + \alpha_h \cdot \alpha_j$ where $h \in F^*$. Since $i \neq i'$ implies that $L_{i,j}^{(h)} \neq L_{i',j}^{(h)}$ and $j \neq j'$ implies that $L_{i,j}^{(h)} \neq L_{i,j'}^{(h)}$ where $L^{(h)}$ is a Latin square. As to the orthogonality of two Latin squares, we can also use two fingers rule.

Assume that for $(i, j) \neq (i', j')$, $L_{i,j}^{(h)} = L_{i',j'}^{(h)}$. Consider $1 \leq k \neq h \leq n - 1$. Suppose that $L_{i,j}^{(k)} \neq L_{i',j'}^{(k)}$. Then we have

$$\begin{cases} \alpha_i + \alpha_h \cdot \alpha_j = \alpha_{i'} + \alpha_h \cdot \alpha_{j'}, \text{ and} \\ \alpha_i + \alpha_k \cdot \alpha_j = \alpha_{i'} + \alpha_k \cdot \alpha_{j'}. \end{cases}$$

$(\alpha_h - \alpha_k)\alpha_j = (\alpha_h - \alpha_k)\alpha_{j'} \implies \alpha_j = \alpha_{j'} \implies \alpha_i = \alpha_{i'}$. A contradiction. Hence, $L^{(h)} \perp L^{(k)}$. \square

Facts on finite fields.

- a. A finite field of order n exists if and only if n is a prime power.
- b. $\langle \mathbb{Z}_n, +, \cdot \rangle$ is a finite field if and only if n is a prime.
- c. Let $n = p^m$ where p is a prime and $m \geq 1$. Then, a finite field of order n can be constructed by using an irreducible polynomial $g(x)$ (over \mathbb{Z}_p) of degree m , i.e., $GF(n) \cong \mathbb{Z}_p[x]/\langle g(x) \rangle$.
- d. All finite fields of the same order are isomorphic.
- e. If $\langle F, +, \cdot \rangle$ is a finite field, then $\langle F^*, \circ \rangle$ is a cyclic group, i.e., $\langle F^*, \circ \rangle \cong \langle \alpha \rangle$, F^* is generated by an element $\alpha \in F^*$ ($= F \setminus \{0\}$).
- f. $x^3 + x + 1$ is irreducible over \mathbb{Z}_2 . $\mathbb{Z}_2[x]/\langle x^3 + x + 1 \rangle$ is a finite field of order 8.

Definition 10.4 (A complete family of MOLS(n)). For order n , $n - 1$ mutually orthogonal Latin squares (MOLS) form a complete family of MOLS(n).

Facts.

4. If n is a prime power, then we have a complete family of MOLS(n).

Remark.

- So far, only for prime power n that we can find a complete family of MOLS(n).
- It is known that there does not exist a complete family of MOLS(n) for $n = 6$ and 10.

Example. Figure 10.9 is a complete family of MOLS(4). (Can we find the 3rd one by using the first two MOLS(4)?) Note that two mutually orthogonal Latin squares of order 4 solve the 16 cards problem!

5. For each n , there are at most $n - 1$ mutually orthogonal Latin squares.

Proof. By Proposition 10.2, we can assume all mutually orthogonal Latin squares do have the same first row $(0, 1, 2, \dots, n - 1)$. Then, consider the $(2, 1)$ cell, no two of the squares have the same entry. (?) Hence, we have at most $n - 1$ distinct Latin squares which are mutually orthogonal. \square

0	1	2	3	\perp	0	1	2	3	\perp	0	1	2	3
2	3	0	1		1	0	3	2		3	2	1	0
3	2	1	0		2	3	0	1		1	0	3	2
1	0	3	2		3	2	1	0		2	3	0	1

Figure 10.9: A complete family of MOLS(4).

Proposition 10.5. *If there exist $n - 2$ MOLS(n), then we can find $n - 1$ MOLS(n).*

Idea of proof.

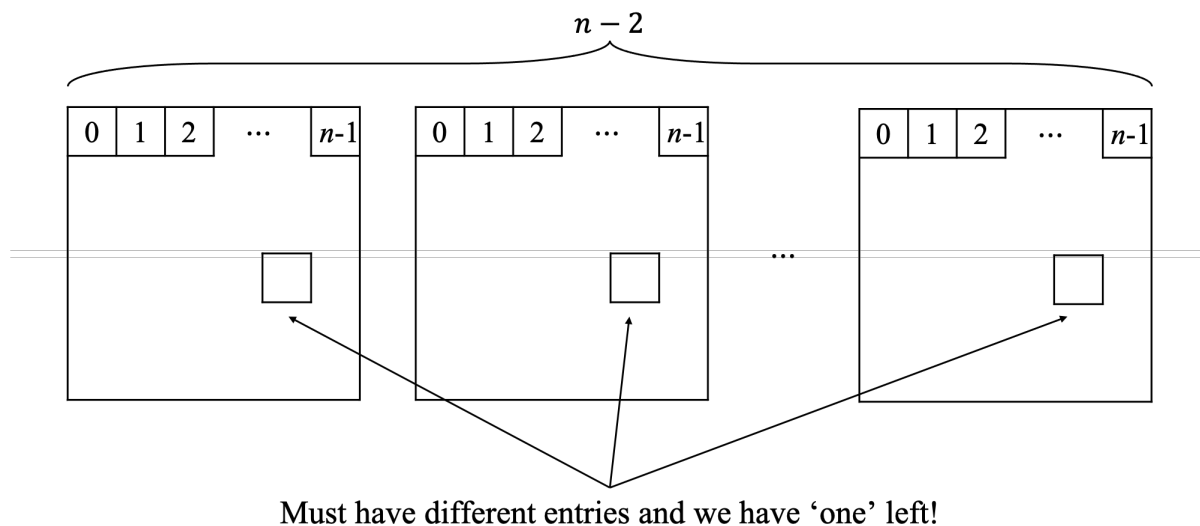


Figure 10.10

Why Euler made the following conjecture?

Conjecture 10.2 (Euler's conjecture on MOLS). *For each $n \equiv 2 \pmod{4}$, there do not exist two mutually orthogonal Latin squares of order n . (If $n > 1$ and $n \not\equiv 2 \pmod{4}$, then either n is a prime or n has a prime factor larger than 2.)*

Facts.

6. Euler's conjecture is true for $n = 2$ and 6 (only!). Also, $n = 1$ is trivial.

7. If $n \not\equiv 2 \pmod{4}$, then we can find at least two MOLS(n).

Proof.

Case 1. $n \equiv 0 \pmod{4}$.

In this case, $n = x^t \cdot m$ where $t \geq 2$ and m is an odd integer. If $m = 1$, then n is a prime power, the proof follows. On the other hand, if $m > 1$, then $m = p_1^{e_1} p_2^{e_2} \cdots p_k^{e_k}$ where p_i 's are distinct odd primes. Now, by using Proposition 10.3, we can construct two MOLS(n) by using direct product of two mutually orthogonal Latin squares of order $2^t, p_1^{e_1}, p_2^{e_2}, \dots, p_k^{e_k}$ respectively.

Case 2. $n \equiv 1$ or $3 \pmod{4}$.

The proof of this case has been include in Case 1. □

Problem. Prove that there do not exist two mutually orthogonal Latin squares of order 6. (Reference: D. R. Stinson, A short proof of the non-existence of a pair of orthogonal Latin squares of order six, J. Combin. Th. A36, 373-376.)

Euler's conjecture was disproved by Parker, Bose and Shrikhande in the year 1959. Figure 10.11 are two MOLS(10) proposed by E. T. Parker. As for $n \equiv 2 \pmod{4}$, $n \geq 10$, we need to apply ideas from pairwise balanced design to prove that two MOLS(n) do exist. (See lecture notes on Combinatorial Designs, Hung-Lin Fu.)

4	0	9	8	3	2	7	5	6	1
2	3	7	5	4	0	9	8	1	6
8	1	6	9	0	4	5	3	2	7
9	8	1	4	5	6	3	2	7	0
0	9	8	6	1	3	2	7	4	5
7	2	3	1	6	5	4	0	9	8
5	4	0	3	2	7	6	1	8	9
6	5	4	2	7	1	8	9	0	3
1	6	5	7	8	9	0	4	3	2
3	7	2	0	9	8	1	6	5	4

5	4	0	1	2	7	8	9	3	6
3	1	6	4	8	5	9	2	0	7
0	9	8	7	3	6	1	4	5	2
2	5	4	3	6	1	7	8	9	0
9	8	7	6	1	0	4	5	2	3
1	6	3	5	9	2	0	7	4	8
8	7	2	9	0	4	5	3	6	1
4	0	9	2	7	8	3	6	1	5
7	2	5	0	4	3	6	1	8	9
6	3	1	8	5	9	2	0	7	4

Figure 10.11: Two MOLS(10).

Definition 10.5 (r -orthogonal). Two Latin squares of order n defined on the same set S are r -orthogonal if when they are superimposed, exactly r different order pairs of S^2 occur among the n^2 ordered pairs of entries.

Example. The two Latin squares is a pair of 34-orthogonal Latin squares of order 6. (3, 4) and (1, 5) are the only two repeated ordered pairs.

0	1	2	3	4	5
1	2	3	5	0	4
2	5	0	4	1	3
3	4	1	2	5	0
4	0	5	1	3	2
5	3	4	0	2	1

0	1	2	3	4	5
5	0	4	2	3	1
3	4	1	5	2	0
4	3	5	1	0	2
2	5	3	0	1	4
1	2	0	4	5	3

Figure 10.12: A pair of 34-orthogonal Latin squares.

Definition 10.6 (Orthogonal array). An orthogonal array of order n with depth k , $OA(k, n)$, is a $k \times n^2$ array $A = [a_{i,j}]$ such that for any two rows, the ordered pairs obtained from the two rows are exactly all ordered pairs of \mathbb{Z}_n^2 ($a_{i,j} \in \mathbb{Z}_n$).

Example. $OA(4,3)$.

$$\begin{bmatrix} 0 & 0 & 0 & 1 & 1 & 1 & 2 & 2 & 2 \\ 0 & 1 & 2 & 0 & 1 & 2 & 0 & 1 & 2 \\ 0 & 1 & 2 & 2 & 0 & 1 & 1 & 2 & 0 \\ 0 & 2 & 1 & 2 & 1 & 0 & 1 & 0 & 2 \end{bmatrix}$$


0	0	0	0	1	2	0	1	2	0	2	1
1	1	1	0	1	2	2	0	1	2	1	0
2	2	2	0	1	2	1	2	0	1	0	2

Figure 10.13: $OA(4,3)$.

Facts.

8. The existence of an $OA(k, n)$ is equivalence to the existence of $k - 2$ $MOLS(n)$.
(This fact comes from that the number of ordered pairs is at most n^2 .)
9. An $OA(k, n)$ has at most n^2 columns and $n + 1$ rows. (This fact is a consequence of the result that there are at most $n - 1$ $MOLS(n)$.)

In applications, regularly a partial orthogonal array uses orthogonal array of order m defined of \mathbb{Z}_n with depth k . In such an array, the ordered pairs are required to be distinct, not necessarily be all pairs in \mathbb{Z}_n^2 . Here, $m \leq n^2$ (as the case in an $OA(k, n)$), but k may be larger than $n + 1$.

Example. $n = 3$, $m = 3$, $k = 5$.

$$\begin{bmatrix} 0 & 0 & 0 \\ 0 & 1 & 2 \\ 0 & 1 & 2 \\ 0 & 2 & 1 \\ 1 & 2 & 0 \end{bmatrix}$$

Three columns represent three orthogonal partial Latin squares.

Remark. If $m = n^2$, then $k \leq n + 1$.

BIBD with $k = 3$ **Facts.**

1. A $2 - (v, 2, \lambda)$ design exists for all $v \geq 2$.

This is a direct consequence of using $\lambda \cdot K_v$.

2. A $2 - (v, 3, 1)$ design exists if and only if $v \equiv 1$ or $3 \pmod{6}$.

This theorem was first proved by T. P. Kirkman in 1847. Later, there are many different proofs for this seeming easy but quite complicate 'fact'. (More details will be given later.)

Kirkman's 15 school girls problem.

Arrange 15 girls to line up in five rows with each row has three girls to walk to school. Can we complete that any two of girls stay in a row for some day in seven days?

We need at least 7 days since each day we use up 15 pairs and in total there are $\binom{15}{2} = 105$ pairs. So, the extra requirement is that every day, the arrangement is in fact a parallel class. Such designs are also known as Kirkman triple systems. Such systems of order v exists if and only if $v \equiv 3 \pmod{6}$. Note that $AG(2, 3)$ is a Kirkman triple system of order 9. Here is an answer of 15 girls problem.

0	1	2	0	3	4	0	5	6	0	7	8	0	9	10	0	11	12	0	13	14
3	7	11	1	7	9	1	8	10	1	11	14	1	12	13	1	3	5	1	4	6
4	9	13	2	12	14	2	11	13	2	4	5	2	3	6	2	8	9	2	7	10
5	10	12	5	8	13	3	9	14	3	10	13	4	8	11	4	10	14	3	8	12
6	8	14	6	10	11	4	7	12	6	9	12	5	7	14	6	7	13	5	9	11

Figure 11.1

Theorem 11.1. A $2 - (v, 3, 1)$ design, known as a Steiner triple system of order v , exists if and only if $v \equiv 1$ or $3 \pmod{6}$.

Proof.

(\Rightarrow) As mentioned earlier, if a $2 - (v, 3, 1)$ design exists, then $r = \frac{v-1}{3-1} = \frac{v-1}{2}$ and $b = \frac{v(v-1)}{6}$ are both integers. This implies that $v \equiv 1$ or $3 \pmod{6}$.

(\Leftarrow) We prove this sufficient condition by constructing a $2 - (v, 3, 1)$ design for each $v \equiv 1$ or $3 \pmod{6}$.

First, we need to construct Steiner triple systems of small orders: $v = 7, 9, 13$ and 15 (defined on \mathbb{Z}_v).

$$v = 7, \mathbb{B} = \{013, 124, 235, 346, 561, 602\} \quad (PG(2))$$

$$v = 9, \mathbb{B} = \{012, 345, 678, 036, 147, 258, 048, 156, 237, 057, 138, 246\} \quad (AG(3))$$

$$v = 13, \mathbb{B} = \{(0, 3, 4) + i, (0, 2, 7) + i \pmod{13} \mid i \in \mathbb{Z}_{13}\} \quad (PG(3))$$

$$v = 15, \mathbb{B} = \{(0, 3, 4) + i, (0, 2, 8) + i, (0, 5, 10) + i \pmod{15} \mid i \in \mathbb{Z}_{15}\}$$

Now, we shall use the following two constructions to construct all the other Steiner triple system of order v , $STS(v)$ in short.

Case 1. $v \equiv 1 \pmod{6}$, $v \geq 19$.

Let $v = 6k + 1$, $k \geq 3$. Let $L^{(i)}$ be the commutative Latin square of order $2k$ defined on $\{(i, j) \mid i \in \mathbb{Z}_3 \text{ and } j \in \mathbb{Z}_{2k}\}$ with holes of size 2, see Figure 11.2.

1	2	5	6	3	4
2	1	6	5	4	3
5	6	3	4	1	2
6	5	4	3	2	1
3	4	1	2	5	6
4	3	2	1	6	5

(a) $2m \times 2m$

1	2	8	5	4	7	6	3
2	1	6	7	8	3	4	5
8	6	4	3	7	2	8	1
5	7	3	4	1	8	2	6
4	8	7	1	6	5	3	2
7	3	2	8	5	6	1	4
6	4	5	2	3	1	8	7
3	5	1	6	2	4	7	8

(b) 8×8

Figure 11.2: Commutative Latin square with 2×2 holes. (a) $m = 3$. (b) $m = 4$.

(If m is odd, then L can be constructed by using direct product. But, for even m , it takes some effort!)

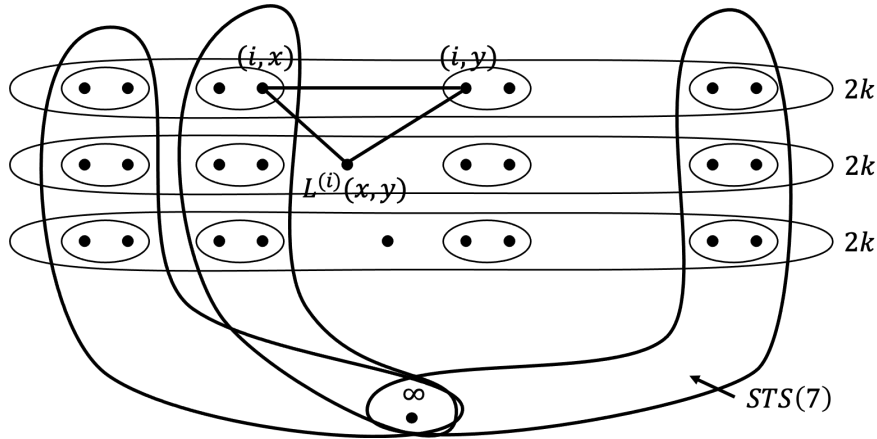


Figure 11.3

Let (\mathbb{X}, \mathbb{B}) be a design with $\mathbb{X} = \{\infty\} \cup (\mathbb{Z}_3 \times \mathbb{Z}_{2k})$, and \mathbb{B} defined as follows:

- (a) $B \in \mathbb{B}$ if B is a block in an $STS(7)$ defined on $\{\infty, (i, 2h), (i, 2h + 1) \mid i \in \mathbb{Z}_3\}$ for each $0 \leq h \leq k - 1$; and
- (b) $\{(i, x), (i, y), (i + 1, L^{(i)}(x, y))\} \in \mathbb{B}$ for all $i \in \mathbb{Z}_3$ and $x, y \in \mathbb{Z}_{2k}$ such that (i, x) and (i, y) are met in a 2×2 hole. (The first component is taking modulo 3 and the second component is taking modulo $2k$.)

It's left to check that (\mathbb{X}, \mathbb{B}) is an $STS(v)$. First, we count $|\mathbb{B}|$. Since each entry outside the hole and in the upper part of $L^{(i)}$ gives a triple (block), we have $3 \cdot \frac{(2k)^2 - 2(2k)}{2} + 7k = \frac{12k^2 - 12k + 14k}{2} = 6k^2 + k = \frac{1}{6}(6k+1)6k = \frac{v(v-1)}{6}$. Hence, if each pair of two elements in \mathbb{X} occurs, then the pair occurs at most once. So, we have to verify each pair of the elements of \mathbb{X} does occur in a block of \mathbb{B} defined above in (a) and (b). Clearly, if one of the elements is ∞ , then $\{\infty, x\}$ occurs in the blocks defined in (a). On the other hand, consider (i_1, x) and (i_2, y) where $i_1, i_2 \in \mathbb{Z}_3$ and $x, y \in \mathbb{Z}_{2k}$. First, if they are in the holes of either $L^{(i_1)}$ or $L^{(i_2)}$ ($= L^{(i)}$), then they occur together in the block of (a). On the other hand, if they are not in the holes of $L^{(i)}$, then we have two cases to consider:

- (1) $i_1 = i_2 = i$.

Clearly, they occur together in $\{(i, x), (i, y), (i + 1, L^{(i)}(x, y))\}$ in (b).

- (2) $i_1 \neq i_2$.

Without loss of generality, let $i_2 \equiv i_1 + 1 \pmod{3}$ and $i_1 = i$. Since there exists a $z \in \mathbb{Z}_{2k}$ such that $L^{(i)}(x, z) = y$, (i_1, x) and (i_2, y) will occur in $\{(i_1, x), (i_1, z), (i_2, y)\}$ in (b).

This concludes the proof. All $STS(v)$ of order $v \equiv 1 \pmod{6}$ have been constructed.

Case 2. $v \equiv 3 \pmod{6}$, $v \geq 21$.

The construction can be obtained similarly. Let $\mathbb{X} = \{\infty_1, \infty_2, \infty_3\} \cup (\mathbb{Z}_3 \times \mathbb{Z}_{2k})$, and \mathbb{B} defined as follows:

- (a) Use $STS(9)$ instead of $STS(7)$ when $\{\infty\}$ is replaced by $\{\infty_1, \infty_2, \infty_3\}$. Moreover, fix $\{\infty_1, \infty_2, \infty_3\}$ as a block for each $STS(9)$.
- (b) Use the same construction.

Hence, $|\mathbb{B}| = 1 + 11k + \frac{3((2k)^2 - 4k)}{2} = 6k^2 + 5k + 1 = (2k+1)(3k+1) = \frac{(6k+3)(6k+2)}{6} = \frac{v(v-1)}{6}$. And the existence of every pair of distinct elements in \mathbb{X} can be checked similarly. \square

Remark. The above construction was obtained not long time ago. There are quite a few methods in construction of Steiner triple systems. One of the most 'popular' one is called 'cyclic construction' method, or, in general, difference method.

Definition 11.1 (Difference). Let $\mathbb{X} = \mathbb{Z}_n$. Then the difference of two distinct element x and y in \mathbb{X} is $\pm(x - y) := \pm|x - y|$ such that $1 \leq |x - y| \leq \lfloor \frac{n}{2} \rfloor$. The difference obtained in a set S is the set of all difference of two distinct elements in S , denoted by $D(S) = \{x - y \pmod{n} \mid x, y \in S\}$.

Example.

1. $n = 7$, $S = \{0, 1, 3\}$, $D(S) = \{\pm 1, \pm 2, \pm 3\} \pmod{7} = \{1, 2, 3, 4, 5, 6\}$.
2. $n = 7$, $S = \{1, 2, 4\}$, $D(S) = \{1, 2, 3, 4, 5, 6\}$.
3. $n = 13$, $S = \{1, 2, 4, 9\}$, $D(S) = \{1, 2, 3, \dots, 12\}$.

Remark.

- If $a, b \in S \subseteq \mathbb{Z}_n$, then $a - b \pmod{n} \in \mathbb{Z}_n^\times$ provided $a \neq b$.
- If $|S| = s$, then $|D(S)| \leq 2 \binom{s}{2}$ (provided $s \leq n$).

Definition 11.2 (Equi-difference set). A set S is called an equi-difference set if the elements of S form an arithmetic progression, i.e., $S = \{a, a + d, \dots, a + (k - 1)d\}$ where $a + (t - 1)d \leq n$ and $d > 0$.

Remark. An equi-difference set could produce the minimum number of distinct differences among all the sets of the same cardinality.

Definition 11.3 (Circular difference). If the difference of a and b is defined as $\min\{|a - b|, n - |a - b|\}$, then it is known as the circular difference of a and b or half difference in short, denoted as $D_2(S)$.

Remark.

- $\{1, 2, 4\}$ in \mathbb{Z}_7 provides three half-difference: 1, 2 and 3. Clearly, in \mathbb{Z}_n , the set of half-difference will be $\{1, 2, \dots, \lfloor \frac{n}{2} \rfloor\}$.
- $|D_2(S)| \leq \binom{|S|}{2}$.
- Again, an equi-difference set S is the set whose $D_2(S)$ is of 'smaller' cardinality. For example, $D(\{1, 2, 3, 4\}) = \{1, 2, 3\}$ and $D(\{0, 2, 4, 6\}) = \{2, 4\}$ in \mathbb{Z}_8 .

Definition 11.4 (Difference set). A set of k elements $D = \{a_1, a_2, \dots, a_k\}$ in \mathbb{Z}_v is called a (v, k, λ) -difference set if $\forall d \in \mathbb{Z}_v^\times$, there are exactly λ ordered pairs (a_i, a_j) , $a_i, a_j \in D$ such that $a_i - a_j \equiv d \pmod{v}$.

Definition 11.5 (Base blocks). A collection of subsets of $\mathbb{X} = \mathbb{Z}_v$ is called a set of base blocks \mathbb{C} of a $2 - (v, k, \lambda)$ design if the following conditions satisfied:

1. Each set of \mathbb{C} is of size k ; and
2. $\cup_{S \in \mathbb{C}} D(S)$ contains each difference in $\pm\{1, 2, \dots, \lfloor \frac{n}{2} \rfloor\}$ exactly λ times.

Constructing design cyclically

Theorem 11.2. *If \mathbb{C} is a set of base blocks of a $2 - (v, k, \lambda)$ design $(\mathbb{X}, \mathbb{B}) = (\mathbb{Z}_v, \mathbb{B})$, then $\mathbb{B} = \{i + S \mid S \in \mathbb{C} \text{ and } i \in \mathbb{Z}_v\}$. (Note that if $S = \{x_1, x_2, \dots, x_k\}$, then $i + S = \{x_1 + i, x_2 + i, \dots, x_k + i\} \pmod{v}$.)*

Example.

1. $\mathbb{X} = \mathbb{Z}_7$, $\mathbb{C} = \{\{0, 1, 3\}\}$ is a set of base block of an $STS(7)$.
2. $\mathbb{X} = \mathbb{Z}_{15}$, $\mathbb{C} = \{\{0, 3, 4\}, \{0, 2, 8\}, \{0, 5, 10\}\}$ is a set of base block of an $STS(15)$.
Note that $\{0, 3, 4\}$ and $\{0, 2, 8\}$ generate 15 blocks respectively, and $\{0, 5, 10\}$ generates 5 blocks.
3. For complete proof, refer to Handbook of Combinatorial Designs.

Principle of Counting

- We consider the sets A which are countable, i.e., A is either a finite set or A has the same cardinality as the set of positive integers \mathbb{N} .
- For convenience, we use $|A|$ to denote the cardinality of A .

Facts

1. If there exists a function f from A into B , then $|A| \leq |B|$, $|A| \geq |B|$ provided f is onto.
2. (Fundamental idea of counting) If $f : A \rightarrow B$ is a bijection, then $|A| = |B|$.
3. The number of k -subsets (distinct) of an n -set is equal to $n \cdot (n-1) \cdots (n-k+1)/k! = \frac{n!}{(n-k)!k!}$, denoted by $\binom{n}{k}$ (n -chooses- k).
4. There are $n!$ permutations on n elements. (It is known as the order of a symmetric group of order n .)
5. If we select k elements from an n -set and the order is en-counted, then there are $n!/k!$ ways to get the job done.

Definition 12.1 (Principle of Inclusion and Exclusion, PIE).

Let A_1, A_2, \dots, A_n be n countable sets. Then

$$\left| \bigcup_{i=1}^n A_i \right| = \sum_{i=1}^n |A_i| - \sum_{1 \leq i < j \leq n} |A_i \cap A_j| + \cdots + (-1)^{n-1} \left| \bigcap_{i=1}^n A_i \right|.$$

Example. For A, B and C , $|A \cup B \cup C| = |A| + |B| + |C| - |A \cap B| - |A \cap C| - |B \cap C| + |A \cap B \cap C|$.

Definition 12.2 (Euler totient function on relative primes).

$$n \in \mathbb{N}, \phi(n) = |\{k | 1 \leq k \leq n, \gcd(n, k) = 1\}|.$$

Example. $\phi(1) = 1, \phi(2) = 1, \phi(3) = 2, \phi(4) = 2, \phi(5) = 4, \phi(6) = 2.$

Proposition 12.1. *By PIE, if $n = p_1^{a_1} p_2^{a_2} \cdots p_r^{a_r}$, then*

$$\begin{aligned} \phi(n) &= n - \sum_{i=1}^r \frac{n}{p_i} + \sum_{1 \leq i < j \leq r} \frac{n}{p_i p_j} - \cdots + (-1)^r \frac{n}{p_1 p_2 \cdots p_r} \\ &= n - \left[\sum_{i=1}^r \frac{n}{p_i} - \sum_{1 \leq i < j \leq r} \frac{n}{p_i p_j} + \cdots + (-1)^{r-1} \frac{n}{p_1 p_2 \cdots p_r} \right] \end{aligned}$$

Proof. Let A_i be the set of integers in $[1, n]$ which are multiple of p_i . Then

$$\phi(n) = n - \left| \bigcup_{i=1}^r A_i \right| = |\overline{A_1} \cap \overline{A_2} \cap \overline{A_3} \cap \cdots \cap \overline{A_r}|. \quad \square$$

Proposition 12.2. *Another famous example of PIE is the derangement. Let \mathbb{D}_n denote the set of permutations σ of $[1, n]$ such that $\sigma(i) \neq i$ for each $i \in [1, n]$. Then,*

$$|\mathbb{D}_n| = D_n = n! \left(1 - \frac{1}{1!} + \frac{1}{2!} - \frac{1}{3!} + \cdots + (-1)^n \frac{1}{n!} \right).$$

Proposition 12.3.

$$\sum_{d|n} \phi(d) = n.$$

Proof. Consider the partition on $[1, n]$ into subsets

$A_d = \{m | m \in [1, n] \text{ and } \gcd(m, n) = d\}$. Since $\gcd(m, n) = d$, $\gcd(\frac{m}{d}, \frac{n}{d}) = 1$. Hence, there are $\phi(\frac{m}{d})$ such $\frac{m}{d}$'s. This implies that $|A_d| = \phi(\frac{n}{d})$. Thus,

$$n = \sum_{d|n} |A_d| = \sum_{d|n} \phi\left(\frac{n}{d}\right) = \sum_{d|n} \phi(d).$$

□

Note that $\forall \bar{m} \in \mathbb{Z}_n$, $\langle \bar{m} \rangle$ generates a subgroup of \mathbb{Z} of order $n/\gcd(m, n)$ and there are $\phi(n/\gcd(m, n))$ m 's. This implies the conclusion as above.

Definition 12.3 (Möbius function). If $m = p_1^{a_1} p_2^{a_2} \cdots p_r^{a_r}$, then

$$\mu(m) = \begin{cases} (-1)^r & \text{if } a_1 = a_2 = \cdots = a_r = 1; \text{ and} \\ 0 & \text{otherwise.} \end{cases}$$

Proposition 12.4. For each $n > 1$,

$$\sum_{d|n} \mu(d) = 0.$$

Proof. Let $n = p_1^{a_1} p_2^{a_2} \cdots p_r^{a_r}$. Hence, $\sum_{d|n} \mu(d) = \sum_d \mu(d)$ where d is a product of distinct primes. Thus

$$\sum_{d|n} \mu(d) = \sum_{i=0}^r \binom{r}{i} (-1)^i = \binom{r}{0} - \binom{r}{1} + \binom{r}{2} - \binom{r}{3} + \cdots + (-1)^r \binom{r}{r} = (1 + (-1))^r = 0.$$

□

Proposition 12.5.

$$\frac{\phi(n)}{n} = \sum_{d|n} \frac{\mu(d)}{d}.$$

Proof. Let $n = p_1^{a_1} p_2^{a_2} \cdots p_r^{a_r}$. By **Proposition 12.1**,

$$\phi(n) = n - \sum_{i=1}^r \frac{n}{p_i} + \sum_{1 \leq i < j \leq r} \frac{n}{p_i p_j} - \cdots + (-1)^r \frac{n}{p_1 p_2 \cdots p_r}.$$

Hence,

$$\frac{\phi(n)}{n} = 1 - \sum_{i=1}^r \frac{1}{p_i} + \sum_{1 \leq i < j \leq r} \frac{1}{p_i p_j} - \cdots + (-1)^r \frac{1}{p_1 p_2 \cdots p_r}.$$

On the other hand, $\sum_{d|n} \frac{\mu(d)}{d} = \sum_d \frac{\mu(d)}{d}$ where d is a product of distinct primes in $\{p_1, p_2, \dots, p_r\}$. This implies that

$$\sum_{d|n} \frac{\mu(d)}{d} = 1 - 1 + \sum_{i=1}^r \frac{1}{p_i} - \sum_{1 \leq i < j \leq r} \frac{1}{p_i p_j} + \cdots + (-1)^r \frac{1}{p_1 p_2 \cdots p_r}.$$

Thus, the proof follows. □

The following formula is known as "Möbius Inversion Formula".

Proposition 12.6 (Möbius Inversion Formula). *If $f(n) = \sum_{d|n} g(d)$, then*

$$g(n) = \sum_{d|n} \mu(d) f\left(\frac{n}{d}\right).$$

Proof.

$$\begin{aligned} \sum_{d|n} \mu(d) f\left(\frac{n}{d}\right) &= \sum_{d'|n} f(d') \mu\left(\frac{n}{d'}\right) \text{ where } d' = \frac{n}{d} \\ &= \sum_{d|n} f(d) \mu\left(\frac{n}{d}\right) \\ &= \sum_{d|n} \mu(d) \cdot \sum_{d''|d} g(d'') \\ &= \sum_{d''|n} g(d'') \cdot \sum_{m|\frac{n}{d''}} \mu(m) \\ &= g(n) \text{ (when } d'' = n) + \left\{ \sum_{d''|n} g(d'') \cdot \sum_{m|\frac{n}{d''}} \mu(m) \text{ with } d'' < n \right\} \\ &= g(n), \text{ since } \sum_{m|\frac{n}{d''}} \mu(m) = 0 \text{ provided } \frac{n}{d''} > 1. \end{aligned}$$

□

Remark. We can use **Proposition 12.3** and **Proposition 12.6** to prove **Proposition 12.5**. Since $n = \sum_{d|n} \phi(d)$, $\phi(n) = \sum_{d|n} \mu(d) \frac{n}{d}$. Hence, we have $\frac{\phi(n)}{n} = \sum_{d|n} \frac{\mu(d)}{d}$.

Möbius Inversion Formula plays an important role in enumeration. We present a good example in what follows.

Review that in order to construct a finite field with p^n elements where p is a prime and $n \geq 1$, we need to find an irreducible polynomial $f(x)$ over \mathbb{Z}_p and the finite field is obtained as $\mathbb{Z}_p[x]/\langle f(x) \rangle$. Therefore, the existence of such polynomials must be verified. In fact, we can enumerate the number of such polynomials which are monic, i.e., the coefficient of x^n is 1.

1. $x^{p^n} - x$ is a product of all monic irreducible polynomials over $\text{GF}(p)$ (or \mathbb{Z}_p) whose degree $d|n$. (Extension field: from p^d elements to p^n elements, $d|n$ is obtained from dimension fact.)
2. Now, let N_d denote the number of monic irreducible polynomial of degree d over \mathbb{Z}_p in the factorization $x^{p^n} - x$. Then, $p^n = \sum_{d|n} d \cdot N_d$ (over \mathbb{Z}_p).
3. Let $f(n) = p^n$, $g(d) = d \cdot N_d$. By Möbius Inversion Formula, $n \cdot N_n = \sum_{d|n} \mu(d) \cdot p^{n/d}$.

Thus,

$$\begin{aligned} N_n &= \frac{1}{n} \sum_{d|n} \mu(d) \cdot p^{n/d} \\ &\geq \frac{1}{n} (p^n - p^{n/2}) > 0 \end{aligned}$$

Generating Function

Definition 13.1 (Generating function).

- $(1+x)^n = \sum_{k=0}^n \binom{n}{k} x^k = \sum_{k=0}^n a_k x^k$.
- $\sum_{k=0}^{\infty} a_k x^k$ is called a generating function of the sequence $\langle a_0, a_1, a_2, \dots, a_k, \dots \rangle$.

Remark. $\binom{n}{k}$ is known as n -choose- k where $n, k \in \mathbb{N} \cap \{0\}$. In fact, we can extend n to

a real number. In that case, $\binom{r}{k} = r^{\underline{k}}/k!$ where $r^{\underline{k}} = r \cdot (r-1) \cdot (r-2) \cdots (r-k+1)$.

For example, let $r = \frac{1}{2}$. Then, $\binom{\frac{1}{2}}{5} = \frac{\frac{1}{2} \cdot (-\frac{1}{2}) \cdot (-\frac{3}{2}) \cdot (-\frac{5}{2}) \cdot (-\frac{7}{2})}{5!}$. Also, $(1+x)^{\frac{1}{2}} =$

$\sum_{k=0}^{\infty} \binom{\frac{1}{2}}{k} x^k$. (Extension of binomial formula) Therefore, we have the geometric series:

$$(1-x)^{-1} = \sum_{k=0}^{\infty} \binom{-1}{k} (-1)^k x^k = \sum_{k=0}^{\infty} x^k,$$

since $(-1)^k \binom{-1}{k} (-1) = (-1)^k \frac{(-1)(-2) \cdots (-k)}{k!} = 1$.

Facts

$$1. \alpha \sum_{k=0}^{\infty} a_k x^k + \beta \sum_{k=0}^{\infty} b_k x^k = \sum_{k=0}^{\infty} (\alpha a_k + \beta b_k) x^k.$$

$$2. \text{ (Convolution of two series) } \left(\sum_{k=0}^{\infty} a_k x^k \right) \left(\sum_{k=0}^{\infty} b_k x^k \right) = \sum_{k=0}^{\infty} \left(\sum_{i=0}^k a_i b_{k-i} \right) x^k = \sum_{k=0}^{\infty} c_k x^k,$$

$$\text{i.e., } c_k = \sum_{i=0}^k a_i b_{k-i}.$$

$$3. \text{ If } F(x) = \sum_{k=0}^{\infty} a_k x^k, \text{ then } F'(x) = \sum_{k=1}^{\infty} k a_k x^{k-1} = \sum_{k=0}^{\infty} (k+1) a_{k+1} x^k.$$

Quite a few counting problems can be solved by using G.F., here we present several examples.

Example 1.

How many different ways are there to make a thousand dollars by using Taiwanese coins, 1 dollar, 5 dollars, 10 dollars and 50 dollars?

Solution. Let the number of coins be e_1, e_2, e_3 and e_4 respectively for 1, 5, 10 and 50 dollars. Then, $e_1 + 5e_2 + 10e_3 + 50e_4 = 1000$, and the G.F. we can use is

$$(1 + x + x^2 + \cdots)(1 + x^5 + x^{10} + \cdots)(1 + x^{10} + x^{20} + \cdots)(1 + x^{50} + x^{100} + \cdots) \\ = \frac{1}{1-x} \cdot \frac{1}{1-x^5} \cdot \frac{1}{1-x^{10}} \cdot \frac{1}{1-x^{50}}.$$

Example 2.

Let h_n denote the number of ways of dividing a convex $(n+1)$ -gon into triangles by inserting diagonals which do not cross each other. Find h_n . (Clearly, $h_1 = 1, h_2 = 1, h_3 = 2, h_4 = 5$ and so on.)

Solution. Let $G(x) = \sum_{k=1}^{\infty} h_k x^k$. Observe that $h_n = \sum_{k=1}^{n-1} h_k \cdot h_{n-k}$.

$$[G(x)]^2 = h_1^2 x^2 + (h_1 h_2 + h_2 h_1) x^3 + (h_1 h_3 + h_2 h_2 + h_3 h_1) x^4 + \cdots = G(x) - h_1 x$$

$$[G(x)]^2 - G(x) + x = 0, \quad G(x) = \frac{1 \pm \sqrt{1-4x}}{2}$$

Since $G(0) = 0$, $G(x) = \frac{1 - \sqrt{1-4x}}{2} = \frac{1}{2} - \frac{1}{2}(1-4x)^{\frac{1}{2}}$. By using Newton's binomial theorem,

$$(1-4x)^{\frac{1}{2}} = 1 - 2 \sum_{n=1}^{\infty} \frac{1}{n} \binom{2n-2}{n-1} x^n, \quad (|x| < \frac{1}{4}).$$

Hence, $G(x) = \sum_{n=1}^{\infty} \frac{1}{n} \binom{2n-2}{n-1} x^n$ and thus $h_n = \frac{1}{n} \binom{2n-2}{n-1}$ ($n \geq 1$).

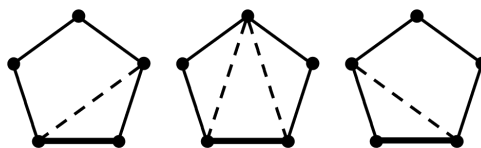


Figure 13.1: Example of $n = 4$. $h_4 = h_1 h_3 + h_2 h_2 + h_3 h_1$.

Remark.

- The number $\frac{1}{n} \binom{2n-2}{n-1}$ is known as the Catalan numbers for various n .
- Many counting problems will have their solutions as this number.

Example 3.

Following from Example 2, if we would like to partition the $(n+1)$ -gon into triangles and one quadrangle, we may use a similar idea to find the number of different ways. (?)

Exponential Generating Functions

Definition 13.2 (Exponential generating function).

- We use the set $\{1, x, x^2, \dots\}$ of monomials to define a generating function such as $\sum_{k=0}^{\infty} a_k x^k$.
- If we consider $\langle a_0, a_1, \dots, a_n, \dots \rangle$ whose terms count permutations, then we shall use monomials $\{1, x, \frac{x^2}{2!}, \dots, \frac{x^n}{n!}, \dots\}$ to define a generating function: $\sum_{k=0}^{\infty} \frac{a_k}{k!} x^k$.

Example 4.

$(1+x)^n$ is an exponential generating function for $\langle p(n,0), p(n,1), \dots, p(n,k), \dots \rangle$ where $p(n,k)$ denotes the number of k -permutations of an n -element set, in fact $p(n,k)$ is equal to $\binom{n}{k} \cdot k!$:

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

G.F. E.G.F.

Note that the E.G.F. of sequence $\langle 1, 1, \dots, 1, \dots \rangle$ is $e^x = \sum_{k=0}^{\infty} x^k / k!$. (This is the reason why we got "exponential".)

For more examples, please refer to the book "Introductory Combinatorics" by R. A. Brualdi.

Recurrence Relations

- One of the famous sequences is known as the Fibonacci sequence $\langle f_0, f_1, \dots, f_n, \dots \rangle$ where $f_0 = 0$, $f_1 = 1$ and $f_n = f_{n-1} + f_{n-2}$ for $n \geq 2$.
- In a sequence, if for each n , $a_n = f(a_1, a_2, \dots, a_{n-1})$, then we have a recurrence relation f . Clearly, if f is quite complicate, then finding a general form for a_n is also difficult. On the other hand, as mentioned above, in case that the relation is comparatively simple, then there is a hope to settle the sequence and use a close form to represent a_n .

Use G.F. to find f_n .

Let $F(x) = \sum_{k=0}^{\infty} f_k x^k$. Since $f_k = f_{k-1} + f_{k-2}$ for $k \geq 2$,

$$\begin{aligned} F(x) &= f_0 + f_1 x + \sum_{k=2}^{\infty} f_k x^k \\ &= x + \sum_{k=2}^{\infty} f_{k-1} x^k + \sum_{k=2}^{\infty} f_{k-2} x^k \\ &= x + x \cdot \sum_{k=2}^{\infty} f_{k-1} x^{k-1} + x^2 \cdot \sum_{k=2}^{\infty} f_{k-2} x^{k-2} \\ &= x + x \cdot (F(x) - f_0) + x^2 \cdot F(x). \end{aligned}$$

$$F(x)(1 - x - x^2) = x, \quad F(x) = \frac{x}{1 - x - x^2} = \frac{x}{(1 - \frac{1+\sqrt{5}}{2}x)(1 - \frac{1-\sqrt{5}}{2}x)} = \frac{a}{1 - \frac{1+\sqrt{5}}{2}x} + \frac{b}{1 - \frac{1-\sqrt{5}}{2}x}.$$

Hence,
$$\begin{cases} a + b = 0 \\ -\frac{1+\sqrt{5}}{2}b - \frac{1-\sqrt{5}}{2}a = 1, \end{cases} \quad , \quad a = \frac{1}{\sqrt{5}}, \quad b = -\frac{1}{\sqrt{5}}.$$

By geometric series,

$$f_n = \frac{1}{\sqrt{5}} \left(\frac{1+\sqrt{5}}{2} \right)^n - \frac{1}{\sqrt{5}} \left(\frac{1-\sqrt{5}}{2} \right)^n.$$

Another idea.

For the Fibonacci number f_n , we may assume that the solution is of the form q^n for some positive real number q . So, $f_n = f_{n-1} + f_{n-2}$ gives $q^n = q^{n-1} + q^{n-2}$, .i.e.,

$q^{n-2}(q^2 - q - 1) = 0$. This yields $q_1 = \frac{1 + \sqrt{5}}{2}$ and $q_2 = \frac{1 - \sqrt{5}}{2}$. Since both q_1 and q_2 provide solutions for f_n , so is their linear combination. The answer is of form $c_1 q_1^n + c_2 q_2^n$ in case that $q_1 \neq q_2$.

Now, we can extend the above idea of a more general linear homogeneous recurrence relation

$$h_n = \sum_{i=1}^k a_i h_{n-i}, \quad a_i \neq 0 \text{ is a constant and } n \geq k.$$

1. If q is a root of $x^k - a_1 x^{k-1} - a_2 x^{k-2} - \dots - a_k = 0$ (*), then $h_n = q^n$ is a solution of the recurrence relation.
2. If (*) has k distinct roots q_1, q_2, \dots, q_n , then $\sum_{i=1}^k c_i q_i^n$ is a general solution of h_n and e_i 's can be determined by using k initial conditions, h_0, h_1, \dots, h_{k-1} .

Remark.

- (*) is known as the characteristic equation of the recurrence relation $h_n = \sum_{i=1}^k a_i h_{n-i}$.
- If (*) has roots which are multiple, then the situation (solutions) will be different.
- If q is a s -multiple set, then we can check that $h_n = q^n, h_n = nq^n, \dots, h_n = n^{s-1}q^n$ as solutions, so is the linear combination of them.

Example 5.

$h_n = -h_{n-1} + 3h_{n-2} + 5h_{n-3} + 2h_{n-4}$, $h_0 = 1, h_1 = 0, h_2 = 1$ and $h_3 = 2$. Then, $x^4 + x^3 - 3x^2 - 5x - 2 = 0$ has roots $-1, -1, -1$ and 2 . So, the general solution for h_n is

$$h_n = c_1(-1)^n + c_2 \cdot n \cdot (-1)^n + c_3 \cdot n^2 \cdot (-1)^n + c_4 \cdot 2^n.$$

By using initial conditions, we obtain

$$h_n = \frac{7}{9}(-1)^n - \frac{1}{3}n(-1)^n + \frac{2}{9}2^n. \quad (c_3 = 0)$$

Note that both of the above two conclusions can be proved, again, see Brualdi's book for reference.

Sum set in Additive Combinatorics

A classical problem dealing with the sum of primes is the well-known Goldbach Conjecture (1742). It was conjectured that for each even positive integer n , n is the sum of two primes. This is a revised version of the original conjecture that all integers larger than 5 can be written as a sum of three primes. Clearly, these two primes are odd integers. In the sense of sum set, we let \mathcal{P} be the set of all primes in \mathbb{N} . The goal is to verify that $\mathcal{P} + \mathcal{P} \supseteq 2\mathbb{N}$ where $2\mathbb{N}$ denotes the set of even positive integers larger than 3. So far, this seeming easy conjecture remains unsettled though there are people who claim that they have verified the trueness of the Goldbach conjecture.

It is worth of noting that for (sufficiently) large odd integer n , n can be written as the sum of three primes. This result was obtained not too long ago. (2013, Harald Helfgott) That is, the weak version of Goldbach's conjecture has been proved. Another idea comes from using product sets. It was proved by 陳景濶 that every integer can be written as the sum " $p_1 + p_2 \cdot p_3$ " where p_1, p_2 and p_3 are odd primes. (This is known as the 1+2 version of Goldbach conjecture.)

The most fundamental problem in additive combinatorics is to find the size of sum set $A + B := \{a + b | a \in A \text{ and } b \in B\}$ where A and B are two given sets in an abelian group with operation " $+$ ". For example, \mathbb{R}, \mathbb{Z} or \mathbb{Z}_n .

Definition 14.1 (Sum set, Difference set).

- $A + B = \{a + b | a \in A \text{ and } b \in B\}$ is called the sum set of A and B . Similarly, $A - B = \{a - b | a \in A \text{ and } b \in B\}$ is called the difference set of A and B .
- The group considered for sum sets or difference sets is called an ambient group.

Remark.

- We shall consider the sum set in what follows, the idea on difference set $A - B$ can be dealt similarly.
- $A + A = 2A$ and $A + A + \cdots + A$ (n copies of A) $= nA$.

Facts.

1. Let Z be an ambient group (may be finite!). $\forall x \in Z$ and $A \subseteq Z$, $|A + x| = |A|$.
2. $\max\{|A|, |B|\} \leq |A + B| \leq |A| \cdot |B|$.
3. Let $A, B \subseteq \mathbb{Z}$ (the set of integers). Then, $|A + B| \geq |A| + |B| - 1$.

Proof. Order the elements of A and B respectively as follows: $A = \{a_1, a_2, \dots, a_n\}$, $a_1 < a_2 < \cdots < a_n$, $B = \{b_1, b_2, \dots, b_m\}$, and $b_1 < b_2 < \cdots < b_m$. Then, in $A + B$, $a_1 + b_1, a_2 + b_1, \dots, a_n + b_1, a_n + b_2, \dots, a_n + b_m$ are $n + m - 1$ distinct integers in \mathbb{Z} . Hence, $|A + B| \geq |A| + |B| - 1$. \square

Note that if A, B are subsets of a finite set (finite additive group), then the size of $A + B$ may be smaller, but still we have $|A + B| \geq \max\{|A|, |B|\}$. (Fact 2)

4. $|A| \leq |A + A| \leq |A| \cdot (|A| + 1)/2 = \binom{|A| + 1}{2}$.
5. $|nA| \leq \binom{|A| + n - 1}{n}$.

Proof. By induction on n . Clearly, it is true when $n = 1$. (The equality holds when the sum of any two elements are different.) On the other hand, if $|A| = 1$, the equality holds. (Both are "1".) So, consider $|A| > 1$ and $n \geq 2$, moreover the assertion is true for $n - 1$.

Let $A = B \cup \{x\}$. $|B| = |A| - 1$. Then, $nA = \cup_{j=0}^n (jB + (n - j)x)$. (j terms in B and $n - j$ x 's) Hence,

$$\begin{aligned} |nA| &= |\cup_{j=0}^n jB| \leq \sum_{j=0}^n |jB| \leq \sum_{j=0}^n \binom{|B| + j - 1}{j} \\ &= \sum_{j=0}^n \binom{|A| + j - 2}{j} \\ &= \binom{|A| - 2}{2} + \binom{|A| - 1}{1} + \binom{|A|}{2} + \binom{|A| + 1}{3} + \cdots + \binom{|A| + n - 2}{n} \end{aligned}$$

$$\begin{aligned}
&= \binom{|A|}{1} + \binom{|A|}{2} + \binom{|A|+1}{3} + \cdots + \binom{|A|+n-2}{n} \\
&= \binom{|A|+1}{2} + \binom{|A|+1}{3} + \cdots + \binom{|A|+n-2}{n} \\
&= \binom{|A|+2}{3} + \cdots + \binom{|A|+n-2}{n} \\
&= \binom{|A|+n-1}{n}.
\end{aligned}$$

□

Remark.

- If $A, B \subseteq \mathbb{Z}$, then $|A + B| \geq |A| + |B| - 1$, furthermore if $|A + B| = |A| + |B| - 1$, then either
 1. $|A| = 1, |B| = 1$ or
 2. both A, B are arithmetic progression integers with a common difference.
- In a finite group, the above conclusion may be wrong. (In \mathbb{Z}_n , $|A| + |B| - 1$ may be larger than n , but $A, B \subseteq \mathbb{Z}_n$ and thus $|A + B| \leq n$.)

Theorem 14.1 (Cauchy-Davenport, 1935). *If p is a prime, $A, B \subseteq \mathbb{Z}_p$ are non-empty, then*

$$|A + B| \geq \min\{p, |A| + |B| - 1\}.$$

Proof. By induction on $|A| \geq 2$. ($|A| = 1$ is trivially true.) Moreover, assume that $|B| \neq p$. Note that $g + A$ is called a shift of A and $g + A = \{g\} + A$. "Shift" does not change the size of a set. By shifting the elements of A to obtain $\{0, g\} \subseteq A$, for some $g \neq 0 \in \mathbb{Z}_p$. Note that $\langle g \rangle \cong \mathbb{Z}_p$. Now, since $|B| \neq p$, we may shift the elements of B to obtain that $0 \in B$ and $g \notin B$. Hence, $A \cap B \neq \emptyset$, and $A \cap B \neq A$.

Let $x \in A \cap B$, $y \in A \cup B$. If $y \in A \setminus B$, then let $x \in B$. If $y \in B$, then let $x \in A$. Thus, $A \cap B + (A \cup B) \subseteq A + B$.

$$\begin{aligned}
|A + B| &\geq |(A \cap B) + (A \cup B)| && (|A \cap B| < |A| \text{ by induction on } |A|) \\
&\geq \min\{p, |A \cap B| + |A \cup B| - 1\} \\
&= \min\{p, |A| + |B| - 1\}.
\end{aligned}$$

□

Question. Is this theorem also true for \mathbb{Z}_n where n is not a prime?

Problem. Given a sequence of $2n - 1$ integers. Can we find an n -term sub-sequence such that the sum of these n terms is a multiple of n ?

We can use Cauchy-Davenport's theorem to answer the problem when n is a prime. Clearly, the problem is equivalent to the following.

Problem. Given a set S of $2n - 1$ elements in \mathbb{Z}_n . Can we find an n -subset of S such that its sum is 0 in \mathbb{Z}_n ?

This is also known as a zero-sum problem.

Proposition 14.2. *If p is a prime and $a_1, a_2, \dots, a_{2p-1} \in \mathbb{Z}_p$, then there is a subsequence with p terms such that the sum is 0.*

Proof. Based on $0, 1, 2, \dots, p - 1$, order the terms as follows: $a_1 \leq a_2 \leq \dots \leq a_{2p-1}$. Now, consider $\{a_1, a_p\}, \{a_2, a_{p+1}\}, \dots, \{a_{p-1}, a_{2p-2}\}, \{a_{2p-1}\}$.

If $a_i \neq a_{p+i}$ for each $i = 1, 2, \dots, p - 1$, then by Theorem 14.1, we conclude that the number of p -term sum in $\{a_1, a_p\} + \{a_2, a_{p+1}\} + \dots + \{a_{p-1}, a_{2p-2}\} + \{a_{2p-1}\}$ has size p . That is, all elements in \mathbb{Z}_p occur in the sum set. 0 is one of them.

If $\exists j, a_j = a_{j+p-1}$, then $a_j = a_{j+1} = \dots = a_{j+p-1}$. Hence, $p \cdot a_j = a_j + a_{j+1} + \dots + a_{j+p-1} = 0$ (in \mathbb{Z}_p). \square

For general n , we need to use the idea of Algebra to show that this proposition can be extended to the case where p is not a prime.

Lemma 14.3. *If G is an abelian group, then there exists a subgroup H such that G/H is of order p where $p|n$.*

Theorem 14.4 (Erdős-Ginzburg-Ziv). *For each positive integer n let $S = \{a_1, a_2, \dots, a_{2n-1}\}$ be a subset of \mathbb{Z}_n . Then, there exists an n -subset of S , S' , such that $\sum_{x \in S'} x = 0$.*

Proof. By induction on n . If n is a prime, then the proof can be obtained by Proposition 14.2. So, assume that $n \geq 2$ and n is a composite integer. Let $p|n$ and p be a prime. For convenience, let $n = p \cdot h$ where $h > 1$. Now, let H be a subgroup of \mathbb{Z}_n and $|H| = h$.

Since $\langle \mathbb{Z}_n, + \rangle$ is an abelian group, \mathbb{Z}_n/H is a cyclic group of order p . Further,

$\mathcal{H} = \{a_1 + H, a_2 + H, \dots, a_{2n-1} + H\}$ is a set of $2n - 1$ cosets. By the fact that $\mathbb{Z}_n/H \cong \mathbb{Z}_p$, and $2n - 1 > 2p - 1$, there exist p cosets in \mathcal{H} whose sum is H . We can

select such p cosets at a time to find a collection of $2h - 1$ sets $\mathcal{H}_1, \mathcal{H}_2, \dots, \mathcal{H}_{2h-1}$ satisfying $\sum_{y \in \mathcal{H}_i} y = H$, $i = 1, 2, \dots, 2h - 1$. ($2n - 1 = 2ph - 1 = p(2h - 1) + p - 1$.) For convenience,

let $\mathcal{H}_i = \{a_{(i-1)p+1}, a_{(i-1)p+2}, \dots, a_{ip}\} + H$ and $\sum_{j=1}^p a_{(i-1)p+j} = b_i$. Since $\sum_{y \in \mathcal{H}_i} y = H$, $b_i \in H$.

By the fact that $|H| < n$ and $\mathbb{B} = \{b_1, b_2, \dots, b_{2h-1}\}$ is a set of $2h - 1$ elements in H , we conclude that there are h elements in \mathbb{B} , $b_{i_1}, b_{i_2}, \dots, b_{i_h}$, with 0 sum. Clearly, 0 in H is also 0 in \mathbb{Z}_n . The proof follows by letting the $ph = n$ elements be obtained from corresponding b_{i_j} 's, i.e., the union $\bigcup_{k=1}^h \{a_{(i_k-1)p+j} \mid j = 1, 2, \dots, p\}$. \square

Definition 14.2 (Doubling constant). The doubling constant of an additive set A (in Z) is $\sigma[A] =_{\text{def}} \frac{|2A|}{|A|} = \frac{|A + A|}{|A|}$.

Facts.

$$6. \quad 1 \leq \sigma[A] \leq \frac{|A| + 1}{2}. \quad (\text{By Fact 4.})$$

Remark.

- The upper bound can be attained by letting $Z = \mathbb{Z}$ (set of integers), $A = \{1, 2, 2^2, \dots, 2^{n-1}\}$.

Now, the sum of any two elements (may be the same) from A are distinct and thus $\sigma[A] = \frac{|A| + 1}{2}$. This kind of sets are known as Sidon sets.

- The lower bound of $\sigma[A]$ can be smaller. Let $A = \{0, d, 2d, \dots, (n - 1)d\}$ where $d \neq 0$ and $d \in \mathbb{Z}$. Then, $\sigma[A] \leq 2 - \frac{1}{n}$. This is by the fact that $\forall x, y \in A$, $x + y \in \{0, d, 2d, \dots, (n - 1)d, \dots, 2(n - 1)d\}$. Hence, $|A + A| \leq 2(n - 1) + 1 = 2n - 1$, thus $\sigma[A] \leq \frac{2n - 1}{n} = 2 - \frac{1}{n}$.

As a matter of fact, since $kd \neq 0$ (in \mathbb{Z}) for any $k \in \mathbb{N}$, we also conclude that $\sigma[A] = 2 - \frac{1}{n}$ for the above set of arithmetic progression.

- If Z is a finite group, then the above equality holds if the order of d in Z is larger than $2(n - 1)$.

Definition 14.3 (Difference constant). Similarly, we can define the difference constant as $\delta[A] = \frac{|A - A|}{|A|}$.

Remark. Again, we have $\delta[A] \geq 1$ and $\delta[A] \leq |A| - 1 + \frac{1}{|A|}$.

Definition 14.4 (Product set). Besides sum set, we can also consider the product set $A \cdot A$ where $A \cdot A := \{ab | a, b \in A\}$.

Remark. Clearly, $|A \cdot A|$ can be as large as the order of $|A|^2$. But, $|A \cdot A|$ can also be small if we take A as the set $\{1, r, r^2, \dots, r^{n-1}\}$, then $|A \cdot A| = 2n - 1$ (provided the multiplication order of r is larger than $2n - 2$ in the multiplication group).

One of the important problems in Additive Combinatorics is to simultaneously estimate $|A + A|$ and $|A \cdot A|$ if both addition and multiplication are operations defined on A . Especially, is that possible to find a set A for which both $|A + A|$ and $|A \cdot A|$ are small.

Conjecture 14.1 (Erdős). For every $\epsilon > 0$, every sufficiently large set $A \subseteq \mathbb{R}$ (or \mathbb{Z}) satisfies $\max\{|A + A|, |A \cdot A|\} \geq |A|^{2-\epsilon}$.

The following theorem provides a good estimation of $\max\{|A + A|, |A \cdot A|\}$.

Theorem 14.5 (Elekes). For any $A \subseteq \mathbb{R}$,

$$|A + A| \cdot |A \cdot A| \geq \frac{1}{64} |A|^{5/2}.$$

To prove Theorem 14.5, we need the following theorems and facts.

Facts.

7. If $cr(G) = 0$ (crossing number of G), then $\|G\| \leq 3|G| - 6$.
8. $cr(G) \geq \|G\| - 3|G| + 6 \leq \|G\| - 3|G|$.

Proof. Let $cr(G) = c$. Convert G into a planar graph G' by letting the crossings be vertices, Hence, $|G'| = |G| + c$, $\|G'\| = \|G\| + 2c$. By using $\|G'\| \leq 3|G'| - 6$, we have $c \geq \|G\| - 3|G| + 6$. □

Theorem 14.6 (Crossing Lemma). *If $\|G\| \geq 4|G|$, then $cr(G) \geq \frac{\|G\|^3}{64|G|^2}$.*

Proof. (Probabilistic method) Set $|G| = v, \|G\| = e$ and $cr(G) = c$. Consider a drawing of G with crossing number $cr(G) = c$. Let $p = \frac{4v}{e} \leq 1$. Choose $V' \subseteq V$ by selecting each vertex independently with probability p . Let $G' = \langle V' \rangle_G$. G' has a drawing from G and let $cr(G') = c'$. Then, $0 \leq c' - e' + 3v'$. Take expectation of them, we have

$$\begin{aligned} 0 &\leq E[c'] - E[e'] + 3E[v'] = p^4 \cdot c - p^2 \cdot e + 3p \cdot v \\ &= p^4 \left(c - \frac{e}{p^2} + \frac{3v}{p^3} \right) = p^4 \left(c - \frac{e^3}{64v^2} \right). \end{aligned}$$

□

Theorem 14.7 (Szemerédi-Trotter). *Let V be a set of points and L be a set of lines in \mathbb{R}^2 . Let $m =_{def} \#\{(p, l) \in V \times L \mid p \sim l\}$. Then,*

$$m \leq 4(|V|^{2/3} \cdot |L|^{2/3} + |V| + |L|).$$

Proof. We may assume that every line contains a point. For each $l \in L$, add an edge between two consecutive pair of points on l , this gives $k - 1$ edges for each line with k points. (Consider a graph $G = (V, E)$.) $|E| = \sum_{l \in L} (\#\text{points on } l - 1)$. $|L|^2 \geq \#\text{crossings}$. Note that if $m - |L| = |E| < 4|V|$, then $m < 4|V| + |L|$. Done. On the other hand, $|E| \geq 4|V|$, $|L|^2 \geq \#\text{crossings} \geq \frac{(m - |L|)^3}{64|V|^2}$ (by Crossing Lemma). Thus,

$$\begin{aligned} (m - |L|)^3 &\leq |L|^2 \cdot 64 \cdot |V|^2 \\ m - |L| &\leq 4|L|^{2/3} \cdot |V|^{2/3} \\ m &\leq 4(|V|^{2/3} \cdot |L|^{2/3} + |V| + |L|). \end{aligned}$$

□

Now, we can prove the theorem of Elekes.

Proof of Theorem 14.5. Let $A \subseteq \mathbb{R}$, define $V = (A + A) \times (A \cdot A)$. For $a, b \in A$, let $l_{a,b}$ be the line given by the equation $y = a(x - b)$. $L = \{l_{a,b} \mid a, b \in A\}$. For every $c \in A$, the point $(c + b, ac) \in V$. So, every $l_{a,b}$ hits at least $|A|$ points.

Since $|L| = |A|^2$,

$$\begin{aligned} |A|^3 &= |A| \cdot |L| \leq \# \text{point-line incident between } V \text{ and } L \\ &\leq 4(|V|^{2/3} \cdot |L|^{2/3} + |V| + |L|) = 4(|V|^{2/3} \cdot |A|^{4/3} + |V| + |A|^2) \\ &\leq 16|V|^{2/3}|A|^{4/3} \text{ (estimation)} \end{aligned}$$

Hence,

$$\begin{aligned} |V|^{2/3} &\geq \frac{1}{16}|A|^{5/3} \\ |V| &\geq \left(\frac{1}{16}|A|^{5/3}\right)^{3/2} = \frac{1}{64}|A|^{5/2}. \end{aligned}$$

□

Probabilistic Method (Graphs)

Definition 15.1 (Random graph with edge probability). $G(n, p)$ or $G(n, P = p)$, where $0 \leq p \leq 1$. The probability of the existence of an edge (independently) is p and the graph induced by using existent edges is G_p .

Definition 15.2 (Discrete Probabilistic Space, D.P.S.). A D.P.S. is an ordered paired pair (S, f) where S is countable set and $f : S \rightarrow \mathbb{R}$ satisfying (i) $0 \leq f(x) \leq 1$ and (ii) $\sum_{x \in S} f(x) = 1$.

Remark. A countable set is either finite set or an infinite set which has the same cardinality as \mathbb{N} .

Definition 15.3. Let (S, f) be a D.P.S.. Then the probability of an event $A \subseteq S$ is $P(A) = \sum_{x \in A} f(x)$.

Definition 15.4 (Independent event). If $P(A \cap B) = P(A)P(B)$, then A and B are independent events.

Definition 15.5 (Random variables). Let (S, f) be a D.P.S.. Then $\mathbb{X} : S \rightarrow \mathbb{R}$ is a random variable where we use $(\mathbb{X} = k) := \{x \in S \mid \mathbb{X}(x) = k\}$ to denote an event.

Example. Let $S = [1, 6]^2$ and $f(x, y) = \frac{1}{36}$ for each $(x, y) \in [1, 6]^2$. $\mathbb{X}((x, y)) = x + y$, $k = 7$. Then, $(\mathbb{X} = 7) = \{(1, 6), (2, 5), (3, 4), (4, 3), (5, 2), (6, 1)\}$.

Definition 15.6 (Expectation). Let \mathbb{X} be a random variable. Then the expectation of \mathbb{X} , $\mathbb{E}(\mathbb{X}) = \sum_k k \cdot P(\mathbb{X} = k)$. (We define $P(\mathbb{X} = h) = 0$ if h is not in the image of $\mathbb{X} : S \rightarrow \mathbb{R}$.)

Example. (Continued) $\mathbb{X} = 7$.

$$\begin{aligned}\mathbb{E}(\mathbb{X}) &= 2 \cdot \frac{1}{36} + 3 \cdot \frac{1}{18} + 4 \cdot \frac{1}{12} + 5 \cdot \frac{1}{9} + 6 \cdot \frac{5}{36} + 7 \cdot \frac{1}{6} \\ &\quad + 12 \cdot \frac{1}{36} + 11 \cdot \frac{1}{18} + 10 \cdot \frac{1}{12} + 9 \cdot \frac{1}{9} + 8 \cdot \frac{5}{36} \\ &= 14 \cdot \left(\frac{1}{36} + \frac{1}{18} + \frac{1}{12} + \frac{1}{9} + \frac{5}{36} + \frac{1}{12} \right) \\ &= 14 \cdot \frac{1+2+3+4+5+3}{36} = 7.\end{aligned}$$

Lemma 15.1 (Pigeon-Hole Principle of Expectation). *Let \mathbb{X} be a random variable of a D.P.S.. Then, there exists a $y \in S$ such that $\mathbb{X}(y) \geq \mathbb{E}(\mathbb{X})$.*

Lemma 15.2 (Linear Property of Expectation). *Let X, X_1, \dots, X_m be random variables such that $X = \sum_{i=1}^m X_i$. Then, $\mathbb{E}(X) = \sum_{i=1}^m \mathbb{E}(X_i)$.*

Definition 15.7 (Indicator Random Variable). An indicator random variable for the event $A \subseteq S$, $I[A]$, is a random variable \mathbb{X} such that $\mathbb{X} : S \rightarrow \{0, 1\}$ (instead of \mathbb{R}).

Remark. A random variable \mathbb{X} can be written as a sum of $|S|$ indicator random variables for an event $A \subseteq S$,

$$x_v = \begin{cases} 1 & \text{if } v \in A, \text{ and} \\ 0 & \text{otherwise.} \end{cases}$$

Here are some examples of probabilistic method.

Theorem 15.3. *If $\binom{n}{k} \cdot 2^{1-\binom{k}{2}} < 1$, then $R(k, k) > n$. Thus,*

$$R(k, k) > \lfloor 2^{\frac{k}{2}} \rfloor, \forall k \geq 3.$$

Proof. Consider a random red-blue coloring of the edges of K_n . For a fixed set T of k vertices, let A_T be the event that $\langle T \rangle_{K_n}$ is monochromatic. Hence, $P(A_T) = \left(\frac{1}{2}\right)^{\binom{k}{2}} \cdot 2 = 2^{1-\binom{k}{2}}$. Since there are $\binom{n}{k}$ possible sets for T , the probability that at least one of the

events A_T occurs is $\binom{n}{k} \cdot 2^{1-\binom{k}{2}}$. By assumption, $\binom{n}{k} \cdot 2^{1-\binom{k}{2}} < 1$. This implies that no event A_T occurs is of positive probability, i.e., there exists a red-blue coloring such that no monochromatic K_k exists. Thus, we have $R(k, k) > n$.

Now, if we take $n = \lfloor 2^{\binom{k}{2}} \rfloor$, then

$$\begin{aligned} \binom{n}{k} \cdot 2^{1-\binom{k}{2}} &< \frac{n^k}{k!} \cdot \frac{2^{1+\frac{k}{2}}}{2^{\frac{k^2}{2}}} & (1 - \binom{k}{2}) &= 1 - \frac{k^2}{2} + \frac{k}{2} \\ &\leq \frac{(2^{\frac{k}{2}})^k}{k!} \cdot \frac{2^{1+\frac{k}{2}}}{2^{\frac{k^2}{2}}} \\ &\leq \frac{2^{1+\frac{k}{2}}}{k!} \\ &< 1. & (k \geq 3) \end{aligned}$$

Hence, $R(k, k) > \lfloor 2^{\frac{k}{2}} \rfloor$, for all $k \geq 3$. This concludes the proof. \square

Theorem 15.4 (Szele, 1943). *There exists a tournament T_n such that T_n has at least $\frac{n!}{2^{n-1}}$ Hamiltonian paths.*

Proof. There are $n!$ possible Hamiltonian (undirected) paths and the probability of a undirected Hamiltonian path is a directed Hamiltonian path is $\frac{1}{2^{n-1}}$. Therefore, $\mathbb{E}(X) = n! \cdot \frac{1}{2^{n-1}}$. This concludes the proof. \square

Theorem 15.5. $\alpha(G) \geq \sum_{v \in V(G)} \frac{1}{1 + \deg_G(v)}$.

Proof. (Greedy Algorithm) In a set of $\deg_G(v) + 1$ vertices we can select one vertex. This concludes the proof by selecting an independent set one vertex at a time. \square

Proof. (Random idea) Use $1, 2, \dots, |G|$ to label the vertices of the set $V(G)$ randomly, call this bijection φ . Let $v_0 \in S$ (an independent set) if $\varphi(v_0) = \min\{\varphi(x) \mid x \in N(v_0) \text{ (neighbor of } v_0)\}$. So, the probability is $\frac{1}{1 + \deg_G(v_0)}$ and the expectation value is

$$\sum_{v \in V(G)} \frac{1}{1 + \deg_G(v)}. \quad \square$$

Theorem 15.6. *If $|G| = n$ and $\|G\| = \frac{nd}{2}$, $d \geq 1$, then $\alpha(G) \geq \frac{n}{2d}$.*

Proof. Let $S \subseteq V(G)$ be a random subset defined by $P[v \in S] = p$. Let $X = |S|$. For each $e = \{v_i, v_j\} \in E(G)$, let Y_e be the indicator random variable for the event $\{v_i, v_j\} \subseteq S$ and $Y = \sum_{e \in E} Y_e$. Now, $\mathbb{E}(Y_e) = P[v_i, v_j \in S] = p^2$ and thus $\mathbb{E}(Y) = \frac{nd}{2} \cdot p^2$. Since

$$\mathbb{E}(X) = np, \quad \mathbb{E}(X - Y) = np - \frac{nd}{2}p^2 = np\left(1 - \frac{d}{2}p\right), \quad p = \frac{1}{d} \text{ gives the maximum. Hence,}$$

$$\mathbb{E}(X - Y) = \frac{n}{2d}.$$

Thus, there exists a specific S for which $|S| - \|\langle S \rangle_G\| \geq \frac{n}{2d}$. Now, select one vertex from each edge of S and delete it to obtain a set S^* with at least $\frac{n}{2d}$ vertices. Since all edges are gone, S^* is an independent set. \square

Definition 15.8. We use n -th space G^n to denote the distribution of graphs of order n . Let q_n be the probability of the existence of "Property Q".

Definition 15.9. If $\lim_{n \rightarrow \infty} q_n = 1$, then we say "Property Q" almost always holds or in this case, almost all graphs have "Property Q".

Theorem 15.7 (Gilbert, 1959). *Let $0 < p \leq 1$ be a constant. Then, almost all graphs are connected.*

Proof. If G is not connected, then there exists a subset $S \subseteq V(G)$ such that $\langle S, V(G) \setminus S \rangle = \emptyset$. This implies that the probability q_n of the existence of disconnected graphs of

order n satisfies $0 \leq q_n \leq \sum_{k=1}^{\lfloor \frac{n}{2} \rfloor} \binom{n}{k} (1-p)^{k(n-k)} \cdot p^x$ where x is fixed. Hence,

$$\begin{aligned} 0 \leq q_n &\leq \sum_{k=1}^{\lfloor \frac{n}{2} \rfloor} n^k \cdot (1-p)^{k(n-k)} \\ &\leq \sum_{k=1}^{\lfloor \frac{n}{2} \rfloor} (n(1-p)^{n-k})^k \\ &\leq \sum_{k=1}^{\lfloor \frac{n}{2} \rfloor} (n(1-p)^{\frac{n}{2}})^k \\ &< \frac{x}{1-x} \quad \text{where } x = n(1-p)^{\frac{n}{2}}. \end{aligned}$$

But $\lim_{n \rightarrow \infty} x = \lim_{n \rightarrow \infty} n(1-p)^{\frac{n}{2}} = 0$. This implies that $\lim_{n \rightarrow \infty} q_n = 0$. \square

Lemma 15.8 (Markov's Inequality). *Let $p_k = P(\mathbb{X} = k)$, $k \geq 0$. Then, $p(\mathbb{X} \geq t) \leq \frac{\mathbb{E}(\mathbb{X})}{t}$. Moreover, if $\mathbb{E}(\mathbb{X}) \rightarrow 0$, then $P(\mathbb{X} = 0) \rightarrow 1$.*

Proof.

$$\mathbb{E}(\mathbb{X}) = \sum_{k \geq 0} kp_k \geq \sum_{k \geq t} kp_k \geq t \cdot \sum_{k \geq t} p_k = tP(\mathbb{X} \geq t).$$

\square

Theorem 15.9. *Let $0 < p \leq 1$ be a constant. Then almost all graphs are of diameter 2.*

Proof. Let $\mathbb{X} = \sum_{i \neq j} \mathbb{X}_{i,j}$ where $\mathbb{X}_{i,j}$ is the indicator random variables such that

$$\mathbb{X}_{i,j} = \begin{cases} 1 & \text{if } v_i \text{ and } v_j \text{ do not have a common neighbor, and} \\ 0 & \text{otherwise.} \end{cases}$$

Note that the probability of " v_i and v_j do not have a common neighbor" is equal to $(1-p^2)^{n-2}$, hence $P(\mathbb{X}_{i,j} = 1) = (1-p^2)^{n-2}$. Thus, $\mathbb{E}(\mathbb{X}) = \sum_{i \neq j} \mathbb{E}(\mathbb{X}_{i,j}) = \binom{n}{2} (1-p^2)^{n-2}$.

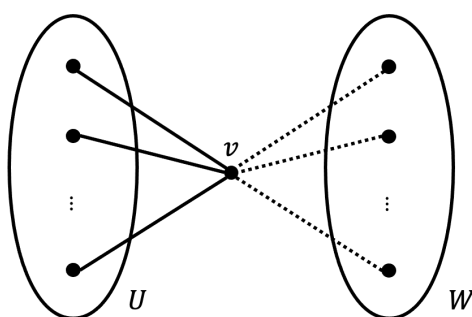
Since $\lim_{n \rightarrow \infty} \binom{n}{2} (1-p^2)^{n-2} = 0$, $\mathbb{E}(\mathbb{X}) \rightarrow 0$. This implies that $P(\mathbb{X} = 0) \rightarrow 1$, i.e., almost every pair of distinct vertices v_i and v_j have a common neighbor. This concludes the proof. \square

Theorem 15.10. *For every constant $p \in (0, 1)$ and every graph H , almost all graphs G^p contains an induced copy of H .*

Proof. Let H be given and $|H| = k$. Let U be a set of k (fixed) vertices of G . Then, $\langle U \rangle_G \cong H$ with a certain probability $r > 0$. (r depends on p , not n . (?)) Now, G contains a collection of $\lfloor \frac{n}{k} \rfloor$ disjoint sets U_i of size k . So, the probability that none of $\langle U_i \rangle_G$ is isomorphic to H is $(1-r)^{\lfloor \frac{n}{k} \rfloor}$. Hence, $P[H \not\subseteq G] \leq (1-r)^{\lfloor \frac{n}{k} \rfloor} \rightarrow 0$ as $n \rightarrow \infty$. \square

Theorem 15.11. Let $P_{i,j}$ be the property that for any disjoint vertex sets U and W with $|U| \leq i$ and $|W| \leq j$, there exists at least one vertex $v \notin U \cup W$ that is adjacent to all the vertices of U but to none of the vertices of W . Then, for every constant $p \in (0, 1)$ and $i, j \in \mathbb{N}$, almost all graphs G^p has property $P_{i,j}$.

Proof. Let $i, j \in \mathbb{N}$ be fixed and $q = 1 - p$. Let U and W be two disjoint vertex sets with $|U| \leq i$ and $|W| \leq j$. The probability that $v \in V(G) \setminus (U \cup W)$ is adjacent to U but not to W is $p^{|U|}q^{|W|} \geq p^i q^j$. Hence, the probability that no suitable v exists for these U and W is $(1 - p^{|U|}q^{|W|})^{n-|U|-|W|} \leq (1 - p^i q^j)^{n-i-j}$. Since the number of $\langle U, W \rangle$ pairs is at most n^{i+j} , the probability that $P_{i,j}$ does not hold is $n^{i+j} \cdot (1 - p^i q^j)^{n-i-j} \rightarrow 0$ as $n \rightarrow \infty$.



□

Corollary 15.12. For every constant $p \in (0, 1)$ and $k \in \mathbb{N}$, almost all graphs are k -connected.

Proof. Let $i = 2$ and $j = k - 1$. Since almost all graphs has property $P_{2,k-1}$, $|G| \geq k + 2$. Let W be an arbitrary set of at most $k - 1$ vertices. Then for all $x, y \in V(G) \setminus W$, either x is adjacent to y or x and y have a common neighbor. ($U = \{x, y\}$) Therefore, W is not a vertex cut. This concludes the proof.

□

Combinatorial Optimization

- "Optimization" plays the most important role in applications.
- If it is not of continuous type, then we refer this type of optimization problems as combinatorial optimization.
- So, we are aiming at minimizing or maximizing combinatorial objects.

Minimizing problems.

1. Chromatic number, Chromatic index of graphs
2. Domination number
3. Vertex cover, Edge cover
4. Genus, Thickness, Crossing number
5. Decycling number
6. Optical index
7. Minimum spanning tree, Traveling salesman problem (TSP)
8. Connectivity, Edge-connectivity
9. Arboricity, Linear arboricity

Maximizing problems.

1. Independence number, Maximum clique
2. Maximum matching
3. Maximum flow in networks
4. Longest cycle in graphs
5. Diameter, Longest path in graphs (hypergraphs)

6. Maximum genus
7. Hamilton cycle problem (Longest cycle, Perimeter of a graph)

Some of the above mentioned problems are solved in the sense of finding an algorithm which uses polynomial time. For example, the minimum spanning tree problem in a weighted connected graph, the maximum matching problem, the longest path problem and the maximum flow problem in a network with rational capacity.

The idea of using algorithm to solve a problem in Graph Theory is known as "Algorithmic Graph Theory". Almost all problems in Graph Theory can be "partially" solved or solved by using algorithm.

If there exists a polynomial time algorithm to find the solution, then we consider the problem is solved. Of course, we are not limited to consider special classes of graphs if we claim the problem is solved in general.

MST-problem.

One of the well-known problem that is solved is "MST-problem", i.e., finding a minimum spanning tree (total weights) in a weighted connected graph with real weights.

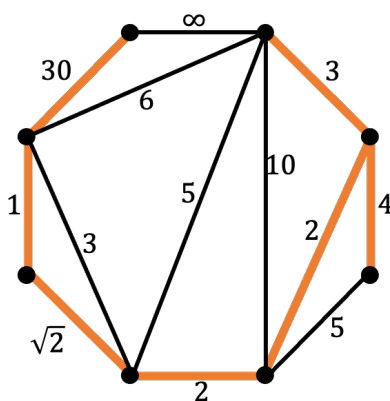


Figure 16.1

The solution can be obtained by selecting edges with minimum weight among the edges left as long as we don't create a cycle.

Maximum matching problem.

Another problem that is solved is finding a "maximum matching" of a graph.

Theorem 16.1. *Let G be a graph and M be a matching in G . Then either M is a matching of maximum cardinality or there exists an M -augmenting path.*

Proof. Clearly, if M is of maximum cardinality, then no M -augmenting paths exist. On the other hand, if M' is a matching with larger cardinality than $|M|$, let $G' = (V, M \cup M')$. Then, $\Delta(G') = 2$. This implies that the components of G' are either a path or a cycle. Since $|M'| > |M|$, at least one component of G' contains more edges from M' than that from M . Such a component is in fact an augmenting path. \square

But, for more problems mentioned above, finding solutions for general graphs are very difficult. From the "algorithm" point of view, they are NP-hard, i.e., so far no polynomial time algorithms have been obtained.

Min-max problems.

A type of problems are called min-max problems. First, we review the well-known Menger's Theorem.

Theorem 16.2 (Menger, 1927). *The maximum number of internally disjoint $s - t$ paths is equal to the minimum size of an $s - t$ cut (or $\langle s, t \rangle$ -separating set).*

Remark.

- We can extend s, t to S, T .
- We can extend the undirected version to directed version.
- We can also extend "vertex-disjoint paths" version to "edge-disjoint paths" version.

Idea of proof.

- The idea can be depicted as Figure 16.2.
- $c \geq n$ (in general): trivial observation.

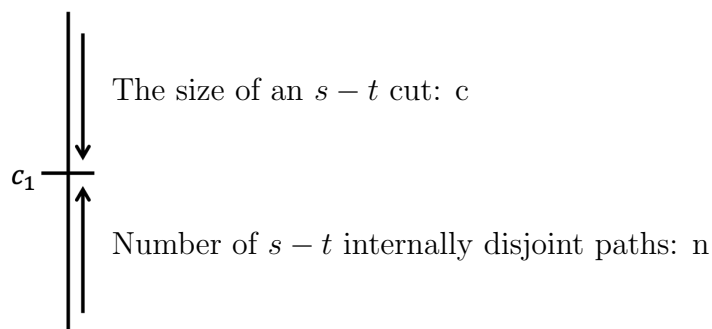


Figure 16.2

- So, the main proof comes from the existence c_1 "paths" and an $s - t$ cut of size " c_1 ". Therefore, c_1 is the answer.
- So, we prove that if c_1 is the minimum size of an $s - t$ cut, then there exist c_1 internally disjoint $s - t$ paths.

This theorem has a beautiful extension to networks.

Definition 16.1 (Flow). Let $D = (V, A)$ be a directed graph and let s (source) and t (sink) be two vertices in V . A function $f : A \rightarrow \mathbb{R}$ is called an $s - t$ flow if

1. $\forall a \in A, f(a) \geq 0$, and
2. $\forall v \in V \setminus \{s, t\}, \sum_{x \in \delta^{in}(v)} f(x) = \sum_{y \in \delta^{out}(v)} f(y)$, where x has head v and y has tail v .

Definition 16.2 (Value of a flow). The value of f , $value(f) =_{def} \sum_{x \in \delta^{out}(s)} f(x) - \sum_{y \in \delta^{in}(s)} f(y)$.

Equivalently, $value(f) = \sum_{x \in \delta^{in}(t)} f(x) - \sum_{y \in \delta^{out}(t)} f(y)$.

($\delta^{in}(U) = \bigcup_{u \in U} \delta^{in}(u)$, $\delta^{out}(U) = \bigcup_{u \in U} \delta^{out}(u)$, and $\delta^{in}(u)$ (resp. $\delta^{out}(u)$) is the set of arcs in A with head u (resp. tail u .)

Definition 16.3 (Capacity). In a network $D = (V, A)$, a capacity function is a mapping $c : A \rightarrow \mathbb{R}_+$. We say that a flow f is subject to c if $f(a) \leq c(a)$ for each $a \in A$.

Definition 16.4 (Cut). A cut in a network is a subset U of V which contains s but not t , i.e., $\langle U, V \setminus U \rangle$.

Definition 16.5 (Capacity of a cut). The capacity of a cut U is defined as

$$c(U) =_{\text{def}} c(\delta^{\text{out}}(U)) = \sum_{a \in \delta^{\text{out}}(U)} c(a)$$

where $\delta^{\text{out}}(U)$ denotes the set of arcs (x, y) with $x \in U$ and $y \in V \setminus U$ (leaving U), and $\delta^{\text{in}}(U)$ denotes the set of arcs (x, y) with $x \in V \setminus U$ and $y \in U$ (entering U).

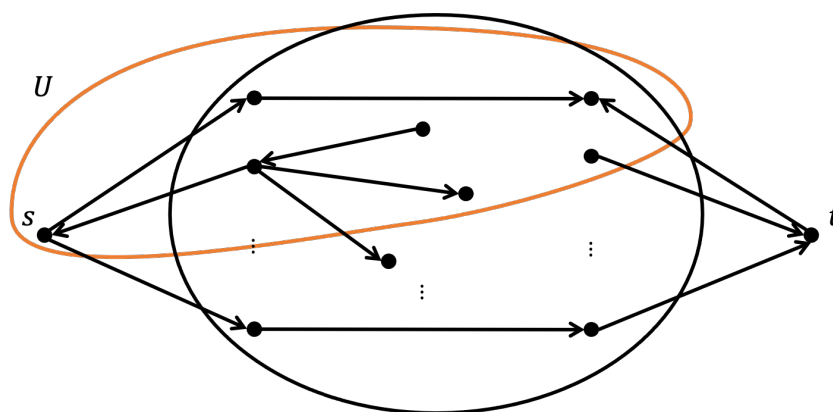


Figure 16.3

Proposition 16.3. In a network $D = (V, A)$, $\text{value}(f) \leq c(\delta^{\text{out}}(U)) = c(U)$, where U is a cut and f is a flow from s to t .

Proof.

$$\begin{aligned} \text{value}(f) &= \left(\sum_{a \in \delta^{\text{out}}(s)} f(a) - \sum_{a \in \delta^{\text{in}}(s)} f(a) \right) + \sum_{v \in U \setminus s} \left(\sum_{a \in \delta^{\text{out}}(v)} f(a) - \sum_{a \in \delta^{\text{in}}(v)} f(a) \right) \\ &= \left(\sum_{a \in \delta^{\text{out}}(s)} f(a) - \sum_{a \in \delta^{\text{in}}(s)} f(a) \right) + \sum_{v \in U \setminus s} 0 \\ &= \sum_{a \in \delta^{\text{out}}(U)} f(a) - \sum_{a \in \delta^{\text{in}}(U)} f(a) \\ &\leq \sum_{a \in \delta^{\text{out}}(U)} f(a) \leq \sum_{a \in \delta^{\text{out}}(U)} c(a) = c(\delta^{\text{out}}(U)) = c(U). \end{aligned}$$

□

Remark. The equality $value(f) = c(U)$ holds if (1) $\forall a \in \delta^{in}(U)$, $f(a) = 0$ and (2) $\forall a \in \delta^{out}(U)$, $f(a) = c(a)$.

Theorem 16.4 (max-flow min-cut theorem). *For any network $D = (V, A)$ with source s and sink t , the maximum flow value f from s to t is equal to the minimum capacity $c : A \rightarrow \mathbb{N}$ of an $s - t$ cut.*

(We consider integral capacity in this theorem. For the case when the capacity is either rational or real can be obtained by more careful arguments.)

Proof. By the edge-version of Menger's theorem, the maximum number of edge-disjoint $s - t$ paths is equal to the minimum size of an $s - t$ edge-cut. Note that this theorem is true for multi-digraph as well.

Now, we define a new digraph D' by letting each arc $a \in A$ be replaced by $c(a)$ arcs (with the same orientation). Thus, we have a directed multi-graph. By Menger's theorem, in D' , the maximum number of $s - t$ edge-disjoint directed paths is equal to an $s - t$ edge-cut E' with minimum size.

Therefore, $D' - E'$ contains no dipaths from s to t . This implies that we have an $s - t$ edge-cut in D with capacity $|E'|$ and also a cut U in D satisfying $\sum_{a \in \delta^{out}(U)} c(a) = |E'|$.

Clearly, this is the maximum number of $s - t$ dipaths by Menger theorem. \square

Remark. U can be obtained by using the arc-induced subgraph of D' by E' .

Finding a maximum flow. (Flow augmenting algorithm)

Idea.

1. First, we start with an "initial flow f " from s to t , say $value(f) = 0$.
2. Then, from s to t we have an $s - t$ path (directed) $P = \langle s = v_0, v_1, v_2, \dots, v_k = t \rangle$ where $a_i = (v_{i-1}, v_i)$, $i = 1, 2, \dots, k$.
3. P is called a flow augmenting path if for each $i = 1, 2, \dots, k$, either $a_i \in A$, $\sigma_i = c(a_i) - f(a_i) > 0$ or $a_i^{-1} \in A$, $\sigma_i = f(a_i^{-1}) > 0$.

(Note that for the initial flow, the second case won't happen.)

4. If for each $i = 1, 2, \dots, k$, $\sigma_i > 0$, then we can increase the current flow value by $\sigma = \min\{\sigma_1, \sigma_2, \dots, \sigma_k\}$. Define a new flow f' .

$$f'(a) = \begin{cases} f(a) + \sigma & \text{if } a = a_i \text{ and } \sigma_i = c(a_i) - f(a_i) > 0; \\ f(a) - \sigma & \text{if } a = a_i^{-1} \text{ and } \sigma_i = f(a_i^{-1}) > 0; \\ f(a) & \text{if } a \notin P. \end{cases}$$

- If there are no flow augmenting paths left, then the flow value is maximum.

The above algorithm was obtained by Ford and Fulberson long time ago and it is known as "maximum flow algorithm" now. There are applications in network by using the above theorem, especially on transportation and networking. Here, we present applications in proving the other theorem in Combinatorics.

Example 1. (Hall's marriage theorem)

Let $G = (X, Y)$ be a bipartite graph. If for each subset $A \subseteq X$, $|N_G(A)| \geq |A|$, then G has a matching saturates A .

Proof. Define a network as follows: Let $D = (V, A)$ be the network where $V = \{s, t\} \cup X \cup Y$, $A = A_1 \cup A_2 \cup A_3 = \{(s, x) \mid x \in X\} \cup \{(y, t) \mid u \in Y\} \cup \{(x, y) \mid xy \text{ is an edge of } G\}$, each arc of $A_1 \cup A_2$ has capacity 1 and each arc of A_3 has capacity $M > |X|$.

Now, we claim that the network contains a flow with value $|X|$. This implies the sufficiency of Hall's theorem. First, let U be a cut with minimum capacity, see Figure 16.4. $U = \{s\} \cup X_1 \cup Y_1$. Then, the capacity of cut $c(U) = |X| - |X_1| + |Y_1|$. Since $c(U)$ is minimum, $N_D(X_1) \subseteq U_1$. By assumption, $|Y_1| \geq N_D(X_1) \geq |X_1|$. Hence, $c(U) \geq |X|$. This concludes the proof. \square

Example 2.

For a bipartite graph $G = (X, Y)$, define the deficiency

$$def(A) =_{def} \begin{cases} |A| - |N_G(A)| & \text{if } |A| > |N_G(A)| \\ 0 & \text{otherwise.} \end{cases}$$

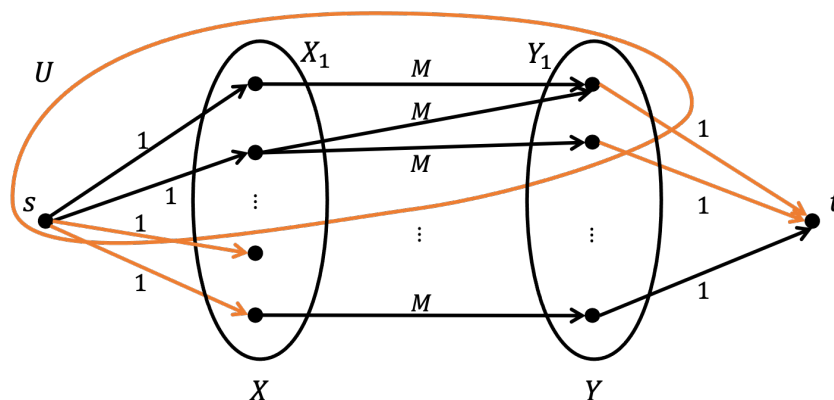


Figure 16.4

Then, $def(G) =_{def} \{def(A) \mid A \subseteq X\}$. The revised version of Hall's marriage theorem is to prove that G contains a matching of size $|X| - def(G)$.

Proof. By using max-flow min-cut theorem, we are able to prove the revised version. Mainly, using the same idea as Example 1 and we are able to find a maximum flow with value $|X| - def(G)$. (Hall's condition shows that $def(G) = 0$.) \square

Example 3.

A $(0, 1)$ -matrix is double stochastic if its row sums and column sums are constant.

e.g.

$$\begin{bmatrix} 0 & 1 & 1 \\ 1 & 0 & 1 \\ 1 & 1 & 0 \end{bmatrix}$$

A double stochastic matrix with row sums and column sums 2.

Prove that a double stochastic matrix can be written as the sum of permutation matrices.

Proof. Let $M = [m_{i,j}]_{n \times n}$ be the matrix we consider, furthermore, let its row sum (resp. column sum) be k . Clearly, $1 \leq k \leq n$ and M can be corresponded to a bipartite graph (A, B) where $|A| = |B| = n$. Similar to Example 1, we can define a network with source s and sink t . Also, the capacities of arcs are defined by the same way.

Now, it is suffices to prove that the minimum cut must be of capacity n (?) and thus we obtain a flow with value n . This shows that M can be the sum of a permutation matrix and a double stochastic matrix M' with row sum and column sum $k - 1$. Hence, the proof follows by induction on k . \square

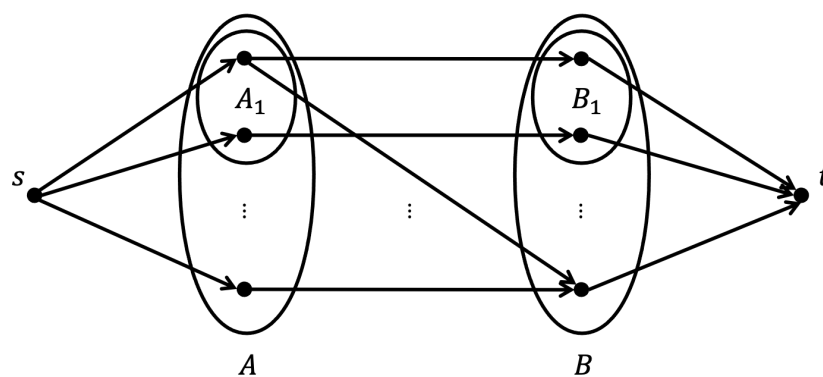


Figure 16.5

Remark. (the (?) part) Let $U = \{s\} \cup A_1 \cup B_1$ be the minimum cut. Since $M > n$, $N(A_1) \subseteq B_1$. By assumption, the degree sum of vertices in A_1 (in (A, B)) is equal to $|A_1| \cdot k$. This implies that the degree sum of vertices of B_1 (in (A, B)) is at least $|A_1| \cdot k$. But, each vertex of B_1 is of degree k (in (A, B)), thus $|B_1| \geq |A_1|$. Now, $c(U) = |A| - |A_1| + |B_1| \geq |A| = n$.

Example 4.

A function $f : A \rightarrow \mathbb{R}$ defined on a directed graph $D = (V, A)$ is called a circulation if for each vertex $v \in V$, we have

$$\sum_{a \in \delta^{in}(v)} f(a) = \sum_{b \in \delta^{out}(v)} f(b).$$

Note that the flow conservation law holds at each vertex v .

The following theorem can be proved by using max-flow min-cut theorem, we omit the details here.

Theorem 16.5 (Hoffman, 1960). *Let $D = (V, A)$ and $d, c : A \rightarrow \mathbb{R}$ satisfying $d(a) \leq c(a)$ for each $a \in A$. Then, there exists a circulation f such that $d(a) \leq f(a) \leq c(a) \forall a \in A$ if and only if for each subset $U \subseteq V$, $\sum_{a \in \delta^{in}(U)} d(a) \leq \sum_{a \in \delta^{out}(U)} c(a)$, i.e., $d(\delta^{in}(U)) \leq c(\delta^{out}(U))$.*

Final words

Combinatorics or Combinatorial Theory play an important role in modern era especially on discrete models. This one semester course can only provide some parts of the topic due to the limit of time. In fact, I am not sure that we are able to cover everything even we are given infinite amount of time. At the time about to finish, there are new topics to occur. Always, new ideas to come and thus new topics to learn. So, we just have to move toward as long as we learn "Combinatorics", the world of counting.