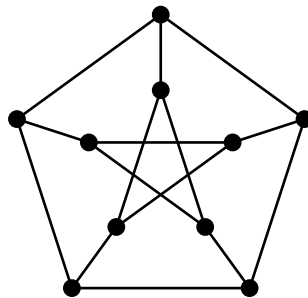
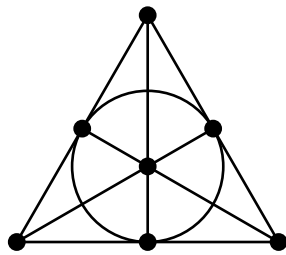


# Combinatorics and Graph Theory



Donald L. Kreher

DRAFT September 26, 2019



# Contents

<b>I</b>	<b>A Taste of Graph Theory</b>	<b>1</b>
<b>1</b>	<b>Basic graph theory</b>	<b>3</b>
1.1	Incidence, adjacency and degree . . . . .	3
1.2	Isomorphisms and Automorphisms . . . . .	6
1.2.1	Exercises . . . . .	7
1.3	Walks, trails, paths and cycles . . . . .	7
1.3.1	Exercises . . . . .	10
1.4	Connectivity . . . . .	10
1.4.1	Exercises . . . . .	13
1.5	Trees and forests . . . . .	14
1.5.1	Exercises . . . . .	16
1.6	Bipartite graphs . . . . .	16
1.6.1	Exercises . . . . .	17
1.7	Euler trails . . . . .	17
<b>2</b>	<b>Planar Graphs</b>	<b>21</b>
2.1	Planar embedding . . . . .	21
2.2	Topology . . . . .	21
2.3	Euler's formula . . . . .	22
2.4	Regular polyhedra . . . . .	24
2.5	Kuratowski's theorem . . . . .	27
2.5.1	Subdivision, contraction and minors . . . . .	27
2.5.2	Blocks and seperable graphs . . . . .	28
2.5.3	Proof of Kuratowski's theorem . . . . .	28
2.5.4	Exercises . . . . .	30
<b>3</b>	<b>Algebraic Graph Theory</b>	<b>33</b>
3.1	Spectrum . . . . .	33
3.2	Regular graphs . . . . .	38
3.3	The matrix tree theorem . . . . .	40
3.4	Notes . . . . .	44
<b>4</b>	<b>Connectivity</b>	<b>45</b>
4.0.1	Exercises . . . . .	46

<b>II</b>	<b>A Taste of Design Theory</b>	<b>47</b>
<b>5</b>	<b>Steiner Triple Systems</b>	<b>49</b>
5.1	Graph decomposition . . . . .	49
5.2	The Bose construction $v \equiv 3 \pmod{6}$ . . . . .	54
5.2.1	Exercises . . . . .	55
5.3	The Skolem construction $v \equiv 1 \pmod{6}$ . . . . .	55
<b>6</b>	<b>Magic Squares</b>	<b>59</b>
6.1	De La Loubère's construction . . . . .	61
6.2	The orthogonal Latin square construction . . . . .	61
6.3	Strachey's construction . . . . .	63
6.4	The Product construction . . . . .	65
6.4.1	Exercises . . . . .	66
<b>7</b>	<b>Mutually Orthogonal Latin Squares</b>	<b>69</b>
7.1	Finite fields . . . . .	69
7.2	Finite projective planes . . . . .	73
7.3	Pairs of orthogonal Latin squares . . . . .	75
7.3.1	Exercises . . . . .	82
<b>III</b>	<b>Miscellaneous Topics</b>	<b>85</b>
<b>8</b>	<b>Alternating Paths and Matchings</b>	<b>87</b>
8.1	Introduction . . . . .	87
8.1.1	Exercises . . . . .	90
8.2	Perfect matchings and 1-factorizations . . . . .	90
8.2.1	Exercises . . . . .	92
8.3	Tutte's theorem . . . . .	93
8.3.1	Exercises . . . . .	95
8.4	The 4-color problem . . . . .	96
8.4.1	Exercises . . . . .	98

## Acknowledgments

I thank the following people for their help in note taking and proof reading: Steve Sy, Kyle Rokos, Dave Torey, Robert Edman, Betsy George, David Clark, Sibel Ozkan, Joshua Ruark, Melissa Keranen.

## Part I

# A Taste of Graph Theory



# Chapter 1

## Basic graph theory

### 1.1 Incidence, adjacency and degree

A (undirected) *graph*  $G = (V, E)$  consists of a set  $V$  of *vertices* and a set  $E$  of pairs of vertices called *edges*.

**Example 1.1.** An example of a graph with 8 vertices and 6 edges is given by

$$\begin{aligned} V &= \{1, 2, 3, 4, 5, 6, 7, 8\} \\ E &= \{\{1, 2\}, \{2, 3\}, \{1, 3\}, \{4, 5\}, \{5, 6\}, \{6, 7\}\} \end{aligned}$$

Every graph has a picture. A picture of the graph in this example is given in Figure 1.1.

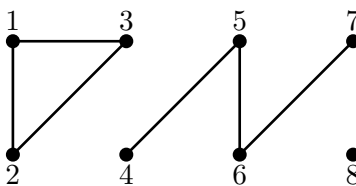


Figure 1.1: A picture of a graph.

If  $x$  and  $y$  are vertices and  $\{x, y\}$  is an edge, then we say that  $x$  is *adjacent* to  $y$ . The graph on  $n$  vertices in which all pairs of vertices are adjacent is called the *complete graph* and it is denoted by  $K_n$ .

$$x \text{ is adjacent to } y: \quad x \bullet \text{---} \bullet y$$

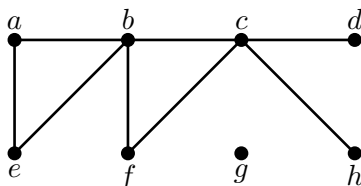
If  $x$  is a vertex, and  $e$  is an edge that contains  $x$ , then we say that  $x$  is *incident* to  $e$ .

$$x \text{ is incident to } e: \quad x \bullet \text{---} \overset{e}{\bullet} \bullet$$

The *degree* of a vertex  $x$  is the number of edges incident to  $x$ . This is denoted by

$$\text{DEG}(x) = |\{e \in E : x \in e\}|$$

**Example 1.2.**



$x$	$a$	$b$	$c$	$d$	$e$	$f$	$g$	$h$	$\sum_x \text{DEG}(x)$
$\text{DEG}(x)$	2	4	4	1	2	2	0	1	16

We now state the fundamental theorem of graph theory.

**Theorem 1.3.** For any graph  $G = (V, E)$ , the sum of the degrees of the vertices is twice the number of edges.

$$\sum_{x \in V} \text{DEG}(x) = 2|E|$$

*Proof.* Every edge is incident to two vertices. Thus the sum counts every edge twice. □

**Corollary 1.4.** In any graph the number of vertices of odd degree is even.

*Proof.* Let  $G = (V, E)$  be a graph and let

$$\begin{aligned} A &= \{x \in V : \text{DEG}(x) \text{ is even}\} \\ B &= \{x \in V : \text{DEG}(x) \text{ is odd}\}. \end{aligned}$$

Then  $A \dot{\cup} B = V$  and thus by Theorem 1.3 we have

$$2|E| = \sum_{x \in V} \text{DEG}(x) = \sum_{x \in A} \text{DEG}(x) + \sum_{x \in B} \text{DEG}(x)$$

All of the summands in  $\sum_{x \in A} \text{DEG}(x)$  are even, we have:

$$0 \equiv \sum_{x \in B} \text{DEG}(x) \equiv |B| \pmod{2},$$

because all of the summands in  $\sum_{x \in B} \text{DEG}(x)$  are odd. □

The *average degree* of a vertex in the graph  $G = (V, E)$  is

$$\text{AVGDEG}(G) = \frac{1}{|V|} \sum_{x \in V} \text{DEG}(x) = \frac{2|E|}{|V|},$$

the *minimum degree* is

$$\delta(G) = \text{MIN}\{\text{DEG}(x) : x \in V\},$$



and the *maximum degree* is

$$\Delta(G) = \text{MAX}\{\text{DEG}(x) : x \in V\}.$$

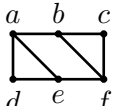

Hence

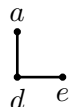
$$\delta(G) \leq \text{AVGDEG}(G) \leq \Delta(G).$$

The *number of edges per vertex* is

$$\epsilon(G) = \frac{|E|}{|V|} = \frac{1}{2} \text{AVGDEG}(G)$$

For any graph  $G$ , we also denote the set of its edges and the set of its vertices by  $E(G)$  and  $V(G)$ , respectively. We say that the graph  $H$  is a *subgraph* of the graph  $G$  if  $V(H) \subseteq V(G)$  and  $E(H) \subseteq E(G)$ . For any  $U \subseteq V(G)$ , the subgraph *induced* by  $U$  is  $H = G[U]$  which has  $V(H) = U$  and  $E(H) = \{\{x, y\} \subseteq U : \{x, y\} \in E(G)\}$ . If  $G$  is a graph and  $x \in V(G)$ , then  $G - x$  is the subgraph induced by  $V(G) \setminus \{x\}$ . It is the subgraph obtained by removing  $x$  and all the edges incident to  $x$ . If  $H$  is a subgraph of  $G$  and  $V(H) = V(G)$ , then  $H$  is called a *spanning subgraph*.

**Example 1.5.** In the graph  $G =$   the subgraph  $G[\{a, d, e\}] =$   is an induced

subgraph of  $G$ , but  $H =$   is a subgraph that is not induced.

An *empty graph* is a graph that contains no edges. A graph that has no vertices is *pointless*.

**Theorem 1.6.** Every non-empty graph  $G$  has a subgraph  $H$  satisfying

$$\delta(H) > \epsilon(H) \geq \epsilon(G)$$

*Proof.* We construct from  $G$  the subgraph  $H$  by deleting vertices without lowering  $\epsilon$  the ratio of the number of edges to the number of vertices. We can delete the vertex  $x$  so long as  $\text{DEG}(x) \leq \epsilon$ . Deleting such  $x$  decreases the number of vertices by 1 and the number of edges by at most  $\epsilon$ . So

$$\begin{aligned} \epsilon(G - x) &\geq \frac{|E| - \epsilon(G)}{|V| - 1} \\ &= \frac{|E| - \frac{|E|}{|V|}}{|V| - 1} \\ &= \frac{|E| \left(1 - \frac{1}{|V|}\right)}{|V| - 1} \\ &= \frac{|E| \left(\frac{|V| - 1}{|V|}\right)}{|V| - 1} \\ &= \frac{|E|}{|V|} \end{aligned}$$

More formally, we construct a sequence of induced subgraphs

$$G = G_0 \supseteq G_1 \supseteq G_2 \supseteq G_3 \supseteq \dots$$

If  $G_i$  has a vertex  $x_i$  with  $\text{DEG}(x_i) \leq \epsilon(G_i)$ , then we set  $G_{i+1} = G_i - x_i$  the subgraph obtained by deleting  $x_i$  and the edges incident to vertex  $x_i$ . If there is no such vertex then we terminate the sequence and set  $H = G_i$ . By the choice of  $x_i$ , we have  $\epsilon(H) \geq \epsilon(G)$ . Furthermore  $H$  has no vertex  $x$  with  $\text{DEG}(x) \leq \epsilon(H)$ . Therefore  $\text{DEG}(x) > \epsilon(H)$  for all  $x \in V$ .  $\square$

## 1.2 Isomorphisms and Automorphisms

Two graphs  $G$  and  $H$  are *isomorphic* if there is a one to one function  $f : V(G) \rightarrow V(H)$  such that

$$\{x, y\} \in E(G) \text{ if and only if } \{f(x), f(y)\} \in E(H).$$

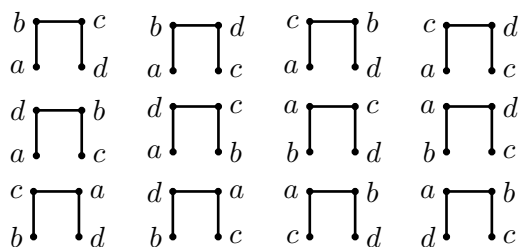
We say that such a function  $f$  is an *isomorphism* from  $G$  to  $H$ . An *automorphism* of a graph  $G$  is an isomorphism from  $G$  to  $G$ . The set of all automorphism of a graph  $G$  form an (algebraic) group under composition of functions that is called the *automorphism group* of  $G$  and is denoted by  $\text{AUT}(G)$ . The automorphism group of the graph in Figure 1.1 is the set of permutations

I (the identity)  
 $(1, 2, 3)$   
 $(1, 3, 2)$   
 $(2, 3)$   
 $(1, 3)$   
 $(1, 2)$   
 $(4, 7)(5, 6)$   
 $(1, 2, 3)(4, 7)(5, 6)$   
 $(1, 3, 2)(4, 7)(5, 6)$   
 $(2, 3)(4, 7)(5, 6)$   
 $(1, 3)(4, 7)(5, 6)$   
 $(1, 2)(4, 7)(5, 6)$

A picture of a graph that contains no vertex labels represents all possible labelings of that picture. It is an isomorphism class or orbit under the action of the symmetric group on the set of vertex labels. For example the picture



represents the 12 labeled graphs



They are all isomorphic.

Table 1.1: The nonisomorphic graphs on 4 vertices.

$ E $	graphs
0	
1	
2	
3	
4	
5	
6	

### 1.2.1 Exercises

- Let  $G$  be a graph on the vertex set  $V = \{x_1, x_2, \dots, x_n\}$ . Let  $d_i = \text{DEG}(x_i)$ , for  $i = 1, 2, \dots, n$  and order the vertices such that  $d_1 \leq d_2 \leq \dots \leq d_n$ . The sequence  $(d_1, d_2, d_3, \dots, d_n)$  is called the *degree sequence* of the graph. If two graphs have different degree sequences, then they are non-isomorphic, but the converse is not true. Find the smallest pair of graphs that are non-isomorphic but have the same degree sequence.
- Draw the nonisomorphic graphs on 5 vertices. (Solution is given in Table 1.2.)
- Find the set of automorphisms of the cube.

## 1.3 Walks, trails, paths and cycles

Let  $G$  be a graph. A *walk* of length  $k$  in  $G$  is an alternating sequence

$$x_0 e_1 x_1 e_2 x_2 e_3 x_3 \cdots e_k x_k$$

of vertices and edges such that  $e_i = x_{i-1}x_i$ . If the walk starts at vertex  $a = x_0$  and ends at vertex  $b = x_k$ . we say that it is a *a-b walk*. We will simplify our notation  $\{x, y\}$  for an edge to just  $xy$ , and use the simpler notation

$$x_0 x_1 x_2 x_3 \cdots x_k$$

to denote the walk. The edges are easily determined:  $e_i = x_{i-1}x_i$ ,  $i = 1, 2, \dots, k$ . If  $x_0 = x_k$ , then we say that the walk is a *closed walk*.

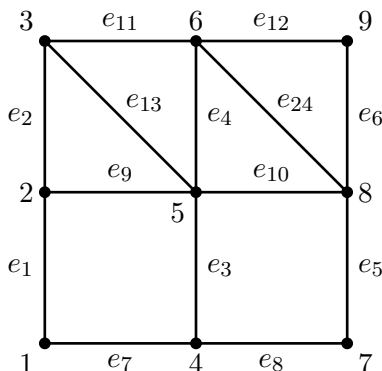


Figure 1.2: a graph for illustrating walks, trails, paths and cycles.

In the graph displayed in Figure 1.2 we see that

$$1e_74e_35e_{13}3e_22e_23e_22e_95e_46e_45e_{10}8e_69$$

is a 1-9 walk of length 11. A *trail* is a walk in which all of the edges are distinct. A 1-9 trail of length 8 in the graph displayed in Figure 1.2 is

$$1e_74e_35e_{13}3e_22e_95e_46e_{14}8e_69.$$

A *path* is a walk in which all of the vertices (and hence the edges) are distinct. A 1-9 path of length 5 in the graph displayed in Figure 1.2

$$1e_74e_35e_46e_{14}8e_69.$$

So, a *path*  $P$  is a subgraph of  $G$  of the form

$$\begin{aligned} V(P) &= \{x_0, x_1, \dots, x_k\} \\ E(P) &= \{x_0x_1, x_1x_2, \dots, x_{k-1}x_k\} \end{aligned}$$

for some subset of distinct vertices  $x_0, x_1, \dots, x_k$ . We write  $P = x_0x_1x_2 \cdots x_k$  to denote this path. In Figure 1.2, 145689 is a path from 1 to 8. It has length 5. We denote a path of with  $n$  vertices by  $P_n$ . ( $P_n$  has length  $n - 1$ .)

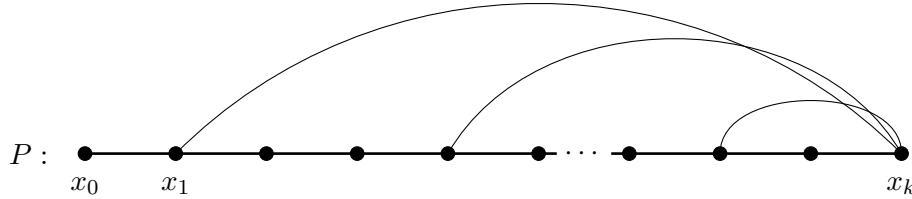
If  $P = x_0x_1x_2 \cdots x_k$  is a path in the graph  $G$  and  $x_kx_0$  is an edge of  $G$ , then

$$C = P + x_kx_0$$

i.e.  $E(C) = E(P) \cup \{x_k, x_0\}$  is a *cycle* (or *circuit*) in  $G$ . A *cycle* is a path from a vertex to itself. We denote a cycle of length  $n$  by  $C_n$ .

**Theorem 1.7.** *Every graph  $G$ , with  $\delta(G) \geq 2$ , contains a path of length  $\delta(G)$  and a cycle of length at least  $\delta(G) + 1$ .*

*Proof.* Let  $P = x_0x_1x_2 \cdots x_k$  be a longest path in the graph  $G$ .



Because  $P$  is a longest path from  $x_0$  to  $x_k$  all of the vertices adjacent to  $x_k$  lie on this path. Thus

$$k \geq \text{DEG}(x_k) \geq \delta(G)$$

Let  $i$  be the smallest index such that  $x_ix_k \in E(G)$ . Then

$$C = x_ix_{i+1}x_{i+2} \cdots x_kx_i$$

is a cycle of length at least  $\delta(G) + 1$ . □

The *distance*  $\text{DIST}(x, y)$  between two vertices  $x, y$  of  $G$  is the length of the shortest  $x$ - $y$  path. If no such path exists, then  $\text{DIST}(x, y) = \infty$ . In Figure 1.2 we see that  $\text{DIST}(1, 9) = 4$ . The greatest distance between any vertices is called the *diameter* of  $G$  which we denote by

$$\text{DIAM}(G) = \text{MAX}\{\text{DIST}(x, y) : x, y \in V(G)\}$$

The graph in Figure 1.2 has diameter 4. Two more examples are given in Figure 1.3. The minimum

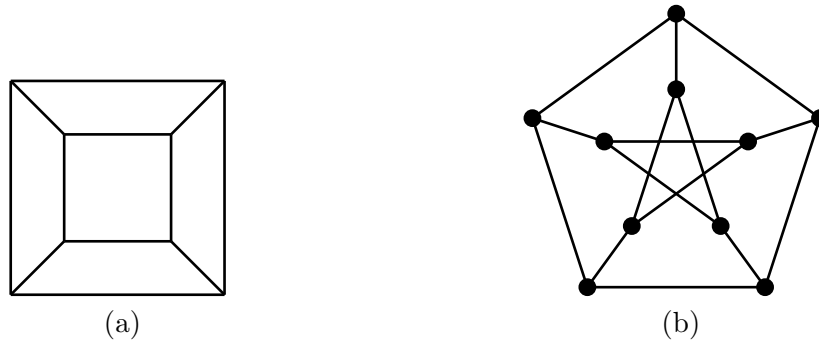


Figure 1.3: Graph (a) is called the *cube*. It has  $|V| = 8$ ,  $\text{DIAM}(G) = 3$ ,  $\delta = \Delta = 3$  and  $g(G) = 4$ . Graph (b) is called the *Petersen graph*. It has  $|V| = 10$ ,  $\text{DIAM}(G) = 2$ ,  $\delta = \Delta = 3$  and  $g(G) = 5$ .

length of a cycle in a graph  $G$  is called the *girth* of  $G$  and is denoted by  $g(G)$ . Examples are given in Figure 1.3.

**Theorem 1.8.** *Every graph  $G$  containing a cycle satisfies  $g(G) \leq 2\text{DIAM}(G) + 1$ .*

*Proof.* Let

$$C = x_0x_1x_2x_3 \cdots x_j \cdots x_{g-1}x_0$$

be a shortest cycle in  $G$  and suppose  $g \geq 2\text{DIAM}(G) + 2$ . Then the length of  $C$  is  $g = g(G) \geq 2\text{DIAM}(G) + 2$ . Let  $j = \text{DIAM}(G) + 1$ . The path

$$x_0x_1x_2 \cdots x_j$$

has length  $\text{DIAM}(G) + 1$  and the path

$$x_jx_{j+1}x_{j+2} \cdots x_0$$

has length at least  $\text{DIAM}(G) + 1$ . The shortest  $x_0$ - $x_j$  path

$$P : x_0 = y_0y_1 \cdots y_\ell = x_j$$

in  $G$  has length  $\ell \leq \text{DIAM}(G)$ . Thus

$$x_0x_1 \cdots x_jy_{\ell-1}y_{\ell-2} \cdots y_2y_1x_0$$

is a closed walk of length

$$j + 1 + \ell - 1 = j + \ell = \text{DIAM}(G) + 1 + \ell \leq 2\text{DIAM}(G) + 1$$

Furthermore not all of the edges of  $P$  are on the cycle  $C$ . Therefore this walk contains a cycle. This cycle has length less than that of the walk, i.e. less than  $2\text{DIAM}(G) + 1$ . This contradicts the choice of  $C$  being the shortest cycle.  $\square$

### 1.3.1 Exercises

1. Show that a closed walk of odd length contains a cycle of odd length.

## 1.4 Connectivity

A non-empty graph  $G$  is connected if any two vertices are joined by a path.

**Lemma 1.9.** *The vertices  $x_1, x_2, \dots, x_n$  of a connected graph  $G$  can be listed so that the induced subgraph*

$$G_i = G[x_1, x_2, x_3, \dots, x_i]$$

*is connected for every  $i$ .*

*Proof.* We inductively construct graphs  $G_i$  as follows. Let  $x_1$  be any vertex of  $G$ . Obviously  $G_1 = G[x_1]$  is connected. Suppose that we have constructed the connected subgraphs  $G_1, G_2, \dots, G_i$  and let  $x$  be any vertex in  $V(G) \setminus \{x_1, x_2, \dots, x_i\}$ . Choose any path

$$P : x_1 = y_0y_1 \cdots y_\ell = x$$

from  $x_1$  to  $x$ . (There exists such a path, because  $G$  is connected.) Let  $j$  be smallest such that  $y_j \notin \{x_1, x_2, \dots, x_i\}$ , and set  $x_{i+1} = y_j$ . Then  $x_{i+1}$  is adjacent to  $y_{j-1}$  and  $y_{j-1} \in V(G_i)$ . Therefore  $G_{i+1} = G[x_1, x_2, x_3, \dots, x_i, x_{i+1}]$  is connected.  $\square$

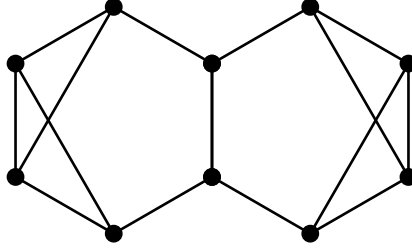


Figure 1.4: A graph  $G$  with  $\kappa(G) = 2$  and  $\delta(G) = 3$ .

Let  $G = (V, E)$  be a graph. If  $A, B \subseteq V$  and  $X \subseteq V \cup E$  is a set of vertices and edges such that every path in  $G$  from a vertex in  $A$  to a vertex in  $B$  contains an edge or vertex in  $X$ , we say that  $X$  separates  $A$  from  $B$  and we call  $X$  a *separating set*. A vertex that separates two other vertices is called a *cut vertex* or an *articulation point*. An edge that separates its ends is called a *bridge*.

A graph  $G = (V, E)$  is said to be  $k$ -connected for  $k \in \mathbb{N}$  if  $|V| > k$  and  $G - X$  is connected for every  $X \subseteq V$ ,  $|X| < k$ . That is *no two vertices are separated by fewer than  $k$  other vertices*. Every non-empty graph is 0-connected. The 1-connected graphs are the non-trivial connected graphs. The largest integer  $k$  such that  $G$  is  $k$ -connected is the (*vertex*) *connectivity* of  $G$ . We denote this integer by  $\kappa(G)$ .

**Example 1.10.** *The connectivity of some graphs.*

1.  $\kappa(G) = 0$  if and only if  $G$  is disconnected or  $G = K_1$ .
2.  $\kappa(K_n) = n - 1$ .
3. The connectivity of the Petersen graph is 3.
4. We can delete all of the vertices adjacent to a given vertex and disconnect the graph. Thus  $\kappa(G) \leq \delta(G)$ .
5. The connectivity of the graph in Figure 1.4 is 2 but the minimum degree is 3.

If  $|V| > 1$  and  $G - F$  is connected for every set  $F \subseteq E$  of fewer than  $\ell$  edges, then  $G$  is called  $\ell$ -edge connected. The greatest integer  $\ell$  such that  $G$  is  $\ell$ -edge connected is called the *edge connectivity* of  $G$  and this integer is denoted by  $\lambda(G)$ . Note that  $\lambda(G) = 0$  if and only if  $G$  is disconnected. For a non-trivial graph  $G$ , it is easy to see that

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

Thus large connectivity implies large minimum degree, but the converse is not true as Figure 1.5 illustrates.

**Theorem 1.11.** Mader (1972). *Every non-trivial graph  $G$  with  $\text{AVGDEG}(G) \geq 4k$  has a  $k$ -connected subgraph.*

*Proof.* If  $k \in \{0, 1\}$  this is trivial. Let  $k \geq 2$  and  $G = (V, E)$ . Set  $n = |V|$  and  $m = |E|$ . We will prove the stronger result:

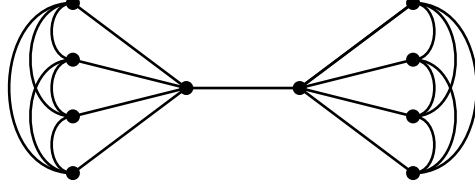


Figure 1.5: A graph with  $\delta(G) = 4$ ,  $\lambda(G) = \kappa(G) = 1$ .

*G has a k-connected subgraph whenever*

1.  $n \geq 2k - 1$ , and
2.  $m \geq (2k - 3)(n - k + 1) + 1$ .

**Remark:** This is indeed stronger. Conditions 1 and 2 follow from our assertion of  $\text{AVGDEG}(G) \geq 4k$  as follows.

If 1 is not true, then we have  $n < 2k - 1$  and

$$m = \frac{1}{2} \text{AVGDEG}(G)n \geq 2kn > (n + 1)n.$$

This is too many edges. A graph can have at most  $\binom{n}{2} = n(n - 1)/2$  edges.

Condition 2 follows from

$$m = \frac{1}{2} \text{AVGDEG}(G)n \geq 2kn$$

because,

$$\begin{aligned} 2kn &= (2k - 3)n + 3n \\ &= (2k - 3)(n - (k - 1)) + (2k - 3)(k - 1) + 3n \\ &= (2k - 3)(n - k + 1) + 1 + (2k - 3)(k - 1) + 3n - 1 \\ &\geq (2k - 3)(n - k + 1) + 1. \end{aligned}$$

The last inequality holds as  $(2k - 3)(k - 1) + 3n - 1 \geq 0$ .

We now prove the stronger result by induction on  $n$ .

If  $n = 2k - 1$ , then  $k = (n + 1)/2$  and hence

$$\begin{aligned} m &\geq \left(2 \left\lfloor \frac{n+1}{2} \right\rfloor - 3\right) \left(n - \left\lfloor \frac{n+1}{2} \right\rfloor + 1\right) + 1 \\ &= (n - 2) \left(\frac{n+1}{2}\right) + 1 \\ &= \frac{n(n-1)}{2} \end{aligned}$$

Thus  $G = K_n$  and  $K_{k+1} \subseteq K_n$ , because  $k + 1 \leq 2k - 1 = n$  for  $k \geq 2$ . The subgraph  $K_{k+1}$  is  $k$  connected.



Suppose  $n > 2k - 1$ . If  $G$  has a vertex  $x$  with  $\text{DEG}(x) \leq 2k - 3$ , then  $G - x$  has  $n' = (n - 1)$  vertices and  $m' \geq m - (2k - 3)$  edges. Thus

$$\begin{aligned} m' &\geq (2k - 3)(n - k + 1) + 1 - (2k - 3) \\ &= (2k - 3)(n - 1 - k + 1) + 1 \\ &= (2k - 3)(n' - k + 1) + 1 \end{aligned}$$

So by induction  $G - x$  and hence  $G$  has a  $k$ -connected subgraph.

So now suppose  $G$  has no such vertex. Then

$$\delta(G) \geq 2k - 2$$

If  $G$  is  $k$ -connected we are done,  $G$  itself is the required subgraph. If  $G$  is not  $k$  connected, then there is a set  $X$  of  $k - 1$ -vertices such that  $G - X = A_1 \cup A_2$ , where  $V(A_1) \cup V(A_2) = V(G - X)$  and  $V(A_1) \cap V(A_2) = \emptyset$ . Let  $G_1 = G[X \cup V(A_1)]$  and  $G_2 = G[X \cup V(A_2)]$ . So  $G = G_1 \cup G_2$ ,  $|V(G_1)|, |V(G_2)| < n$  and  $|V(G_1 \cap G_2)| = |X| = k - 1$ . Furthermore, for every  $x \in V(G_1) \setminus V(G_2)$  we have  $\text{DEG}(x) \geq \delta(G) \geq 2k - 2$  and the vertices adjacent to such  $x$  are in  $V(G_1)$ . Therefore  $|V(G_1)| \geq 2k - 1$ . Similarly  $|V(G_2)| \geq 2k - 1$ . Thus both  $G_1$  and  $G_2$  satisfy Condition 1 of the induction hypothesis. If neither  $G_1$  nor  $G_2$  satisfies Condition 2, then

$$|E(G_1)| \leq (2k - 3)(|V(G_1)| - k + 1)$$

and

$$|E(G_2)| \leq (2k - 3)(|V(G_2)| - k + 1)$$

Hence

$$\begin{aligned} m &\leq |E(G_1)| + |E(G_2)| \\ &\leq (2k - 3)(|V(G_1)| - k + 1) + (2k - 3)(|V(G_2)| - k + 1) \\ &= (2k - 3)(|V(G_1)| + |V(G_2)| - 2k + 2) \\ &= (2k - 3)(n + (k - 1) - 2k + 2) \\ &= (2k - 3)(n - k + 1) \end{aligned}$$

(Recall  $|V(G_1 \cap G_2)| = |X| = k - 1$ .) This contradicts the fact that  $G$  satisfied Condition 2. Consequently at least one of  $G_1$  and  $G_2$  satisfy both conditions of the induction hypothesis and so at least one of  $G_1$  and  $G_2$  contain a  $k$ -connected subgraph. Therefore because these are subgraphs of  $G$  we have that  $G$  contains a  $k$ -connected subgraph.  $\square$

### 1.4.1 Exercises

1. (*The Chekad and Ernie problem.*) Given a connected graph  $G$  let  $T(G)$  be the number of sequences

$$x_1, x_2, \dots, x_n$$

of the vertices of  $G$  such that the induced subgraphs

$$G_i = G[x_1, x_2, \dots, x_i]$$

are connected.

- (a) Compute  $T(G)$  for every connected graph on 5 or less vertices.
- (b) Show that  $T(P_n) = 2^{n-1}$ .
- (c) Show that  $T(C_n) = n2^{n-2}$ .
- (d) Show that  $T(K_{1,n-1}) = 2(n-1)!$ . ( $K_{1,n-1}$  is the graph having one vertex adjacent to each of the other vertices, but no other edges. )
- (e) Show that  $T(K_n) = n!$ .
- (f) If  $H$  is a connected subgraph of  $G$  show that  $T(H) \leq T(G)$ .
- (g) Show that  $T(G)$  is always even.

These are easy except possibly for 1g. The general question of what are the possible values of  $T(G)$  is called the spectrum problem of  $T(G)$  and I believe this to be an open question. It probably will depend heavily on the solution for spanning trees.

- 2. Show that every 2-connected graph contains a cycle.

## 1.5 Trees and forests

A graph  $F$  is *acyclic* if contains no cycles. An acyclic graph is also called a *forest*. A connected acyclic graph is called a *tree*. See Figure 1.6. The vertices of degree 1 in a tree  $T$  are called its leaves.

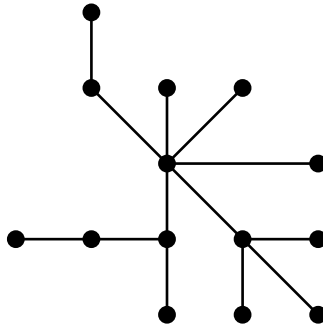


Figure 1.6: A tree

Every non-trivial tree has at least 2 leaves. A characterization of trees is given in Theorem 1.12.

**Theorem 1.12.** *The following are all equivalent for a graph  $T$ .*

1.  $T$  is a tree.
2. Any two vertices of  $T$  are connected by a unique path.
3.  $T$  is minimally connected. That is  $T$  is connected but  $T - e$  is disconnected for every edge  $e \in E(T)$ .
4.  $T$  is maximally acyclic. That is  $T$  contains no cycles, but  $T + xy$  contains a cycle through  $xy$  for any two non adjacent vertices  $x, y \in V(T)$ ,  $x \neq y$ .

*Proof.* Let  $T = (V, E)$  be a graph.

(1 $\Rightarrow$ 2) Suppose  $T$  is a tree and let  $a, b \in V, a \neq b$ . If

$$a = x_0x_1x_2x_3 \dots x_{k-1}x_k = b$$

and

$$a = y_0y_1y_2y_3 \dots y_{\ell-1}y_\ell = b$$

are two different paths from  $a$  to  $b$ . Then

$$a = x_0x_1x_2x_3 \dots x_{k-1}y_\ell y_{\ell-1} \dots y_3y_2y_1y_0 = a$$

is a closed walk in which not all of the  $y_i$ s are  $x_j$ s are the same. It must therefore contain a cycle contradicting  $T$  is a tree.

(2 $\Rightarrow$ 3) Suppose any two vertices of  $T$  are connected by a unique path and let  $e = xy$  be any edge of  $T$ . If  $T - e$  is connected then there is a path  $P$  from  $x$  to  $y$  in  $T - e$ . But then there are two  $x$  to  $y$  paths in  $T$ , namely  $P$  and the edge  $e = xy$ . Thus  $T - e$  is disconnected for every edge  $e$  and so  $T$  is minimally connected.

(3 $\Rightarrow$ 4) Suppose  $T$  is minimally connected and let  $x, y$  be any two non-adjacent vertices of  $T, x \neq y$ . Then there is an  $x$  to  $y$  path

$$x = x_0x_1x_2x_3 \dots x_{k-1}x_k = y$$

in  $T$  and hence there is a cycle in  $T + xy$  and so  $T$  is maximally acyclic.

(4 $\Rightarrow$ 1) Suppose  $T$  is maximally acyclic. Then  $T$  has no cycles and for any pair of non-adjacent vertices  $x$  and  $y$  we have that  $T + xy$  contains a cycle through  $xy$ . Thus  $T$  has a path from  $x$  to  $y$  and so  $T$  is connected. Consequently  $T$  is a tree. □

Applying Theorem 1.12 it is easy to see that every connected graph  $G$  contains a spanning tree. Simply delete edges on cycles of  $G$  until there are no more cycles. Similarly it is easy to see that any minimally connected spanning subgraph of  $G$  is also a tree.

**Corollary 1.13.** *The vertices of a tree can always be listed  $x_1, x_2, \dots, x_n$  so that every  $x_i$  with  $i \geq 2$  has a unique neighbor in  $\{x_1, x_2, \dots, x_{i-1}\}$ .*

*Proof.* Use the listing provided by Lemma 1.9. □

**Corollary 1.14.** *A connected graph with  $n$  vertices is a tree if and only if it has  $n - 1$  edges.*

*Proof.* We leave this as Exercise 3. □

**Corollary 1.15.** *If  $T$  is a tree and  $G$  is any graph with  $\delta(G) \geq |V(T)| - 1$ , then  $G$  has a subgraph isomorphic to  $T$ .*

*Proof.* We leave this as Exercise 4. □

### 1.5.1 Exercises

1. Show that any tree  $T$  has at least  $\Delta(T)$  leaves.
2. Show that every automorphism of a tree fixes a vertex or an edge.
3. Prove Corollary 1.14.
4. Prove Corollary 1.15.

## 1.6 Bipartite graphs

Let  $r \geq 2$  be a positive integer. A graph  $G = (V, E)$  is said to be  $r$ -partite if its vertices can be partitioned into  $r$  blocks

$$V = V_1 \dot{\cup} V_2 \dot{\cup} V_3 \dot{\cup} \dots \dot{\cup} V_r, \quad V_i \cap V_j = \emptyset \text{ for } i \neq j$$

such that every edge has its ends in different blocks. That is if  $xy \in E$ , then  $x \in V_i$  and  $y \in V_j$ , for some  $i \neq j$ . If  $r = 2$ , then an  $r$ -partite graph is said to be *bipartite*. An  $r$ -partite graph in which every pair of vertices belonging to different blocks of the partition are adjacent is said to be *complete*. If the  $r$  blocks of a complete  $r$ -partite graph  $G$  have sizes  $n_1, n_2, \dots, n_r$ , then we denote  $G$  by  $K_{n_1, n_2, \dots, n_r}$ . We abbreviate  $\underbrace{K_{s, s, s, \dots, s}}_r$  with  $K_r^s$ . The bipartite graph  $K_{1, n}$  is called the *star*.

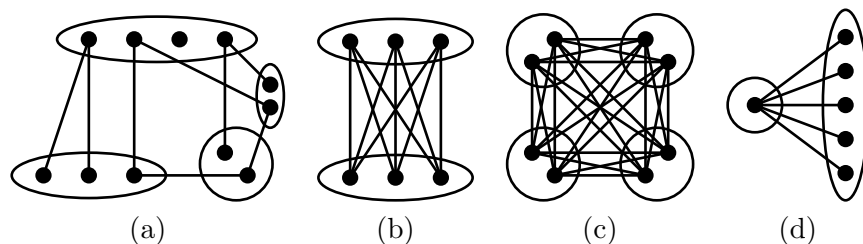


Figure 1.7: Examples of  $r$ -partite graphs: (a) A 4-partite graph. (b) The bipartite graph  $K_{3,3}$ . (c) The 4-partite graph  $K_{2,2,2,2} = K_2^4$ . (d) The star  $K_{1,5}$ .

**Theorem 1.16.** *A graph is bipartite if and only if it contains no odd cycle.*

*Proof.* Clearly a graph  $G = (V, E)$  is bipartite if and only if its connected components are bipartite. So we may assume that  $G$  is connected.

Suppose  $G$  is bipartite with partition  $V = V_0 \dot{\cup} V_1$ , in which every edge has one end in  $V_0$  and the other in  $V_1$  and let  $C = x_0 x_1 x_2 \dots x_{k-1} x_0$  be any cycle. The length of  $C$  is  $k$ .

Without loss  $x_0 \in V_0$ , say. Then  $x_i \in V_0$ , if  $i$  is even and  $x_i \in V_1$  if  $i$  is odd. It follows that  $k$  is even and hence  $C$  has even length. So,  $G$  does not contain an odd cycle.

Conversely suppose  $G$  has no odd cycles. Let  $T$  be a spanning tree in  $G$  and fix any vertex  $r$ . We define a partition  $V = V_0 \dot{\cup} V_1$  as follows. For each  $x \in V$  let  $P_x$  be the unique path in  $T$  from  $r$  to  $x$ .

$$V_0 = \{x \in V : \text{length of } P_x \text{ is even}\}$$

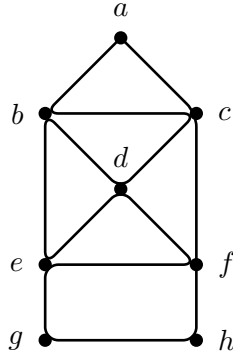


Figure 1.8: An Eulerian graph.  $abcdbedfeghfgca$  is an Euler trail.

and

$$V_1 = \{x \in V : \text{length of } P_x \text{ is odd}\}$$

We now show that every edge  $e = xy$  of  $G$  has one of its ends in  $V_0$  and the other in  $V_1$ .

If  $e$  is an edge of  $T$ , then either  $x$  is on the path  $P_y$  or  $y$  is on the path  $P_x$ . So assume  $x$  is on  $P_y$ , if not switch the roles of  $x$  and  $y$ . Then  $P_y = P_x y$  and so if length of  $P_y$  is even then the length of  $P_x$  is odd and if  $P_y$  is odd then  $P_x$  is even. Hence one of  $x$  and  $y$  are in  $V_0$  and the other is in  $V_1$ .

If  $e$  is not an edge of  $T$ , then  $T + e$  has a unique cycle  $C_e$ , namely the unique path  $P$  from  $x$  to  $y$  in  $T$  together with the edge  $e$ . This cycle has even length by assumption and so  $P$  has odd length. Furthermore the edges of the path  $P$  are edges of  $T$  and so each has one end in  $V_0$  and the other in  $V_1$ . Hence the vertices of  $P$  alternate between  $V_0$  and  $V_1$ . Therefore, because  $P$  has odd length, one of  $x$  and  $y$  is in  $V_0$  and the other is in  $V_1$ .  $\square$

### 1.6.1 Exercises

1. Show that  $G$  is bipartite if and only if every *induced* cycle has even length.

## 1.7 Euler trails

An *Euler trail* in a graph  $G$  is a closed walk that uses every edge of  $G$  exactly once. A graph  $G$  that has an Euler trail is said to be *Eulerian*. An example of an Eulerian graph is given in Figure 1.8.

**Theorem 1.17.** (1736 Euler) *A connected graph is Eulerian if and only if all of its degrees are even.*

*Proof.* Suppose  $G$  is Eulerian and let

$$W = x_0 e_0 x_1 e_1 \cdots x_{\ell-1} e_{\ell-1} x_{\ell} e_{\ell} x_0$$

be an Euler trail in  $G$ . Every occurrence of a vertex  $x$  in the trail accounts for two edges incident to  $x$ , namely the edges immediately preceding and following it in the trail. Thus if  $x$  occurs  $k$  times in the trail it must have degree  $2k$ .

Conversely suppose all the vertices of the graph  $G$  have even degree and let

$$W = x_0 e_0 x_1 e_1 \cdots x_{\ell-1} e_{\ell-1} x_\ell e_\ell$$

be a longest walk in  $G$  that uses each edge at most once. Because  $W$  cannot be extended, all of the edges incident to  $x_\ell$  must appear in  $W$ . Therefore because  $x_\ell$  has even degree, we have  $x_0 = x_\ell$  and  $W$  is closed. If there is an edge of  $G$  outside of  $W$ , then because  $G$  is connected, there must be an edge  $e$  incident to some vertex  $x_i$  of  $W$ , say  $e = ux_i$ . Then

$$ux_i e_i x_{i+1} e_{i+1} \cdots x_{\ell-1} e_{\ell-1} x_0 e_0 x_1 e_1 x_2 e_2 \cdots e_{i-1} x_i$$

is a longer walk than  $W$ . This is a contradiction and therefore  $W$  must include all of the edges of  $G$  and is thus an Euler trail.  $\square$

Table 1.2: The 34 nonisomorphic graphs on 5 vertices.

$ E $	graphs
0	
1	
2	
3	
4	
5	
6	
7	
8	
9	
10	





## Chapter 2

# Planar Graphs

### 2.1 Planar embedding

A graph  $G$  is said to be *embeddable* in the  $XY$ -plane if it can be drawn in the  $XY$ -plane so that edges only intersect at their ends. A graph  $G$  that is embeddable in the  $XY$ -plane is said to a *planar* graph and a *plane* graph is a graph that has been embedded in the  $XY$ -plane.

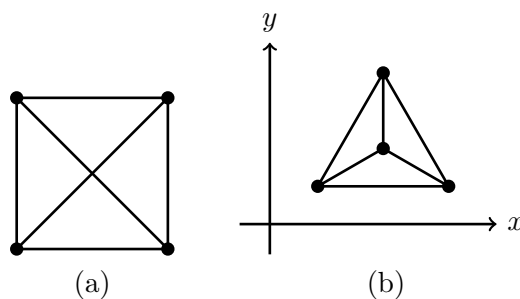


Figure 2.1: (a)  $K_4$ . (b) A planar embedding of  $K_4$ .

### 2.2 Topology

A *Jordan curve* is a continuous non-intersecting curve whose origin and terminus intersect. If  $J$  is a Jordan curve, the rest of the plane is partitioned into two open sets: the interior of  $J$  denoted by  $\text{INT}(J)$ , and the exterior of  $J$  denoted by  $\text{EXT}(J)$ . See Figure 2.2. Let  $\text{INT}(J)$ , and  $\text{EXT}(J)$  be the closures of  $\text{INT}(J)$ , and  $\text{EXT}(J)$  respectively.  $\text{INT}(J) \cap \text{EXT}(J) = J$ .

The *Jordan curve theorem* states that any line joining a point in  $\text{INT}(J)$  to a point in  $\text{EXT}(J)$  must intersect  $J$ . We will use the Jordan curve theorem to prove that  $K_5$  is non-planar.

**Theorem 2.1.**  $K_5$  is non-planar.

*Proof.* Let  $G$  be a planar embedding of  $K_5$  with vertices  $x_1, x_2, x_3, x_4$  and  $x_5$ .  $G$  is complete so  $C = x_1x_2x_3x_1$  is a cycle, i.e.  $C$  is a Jordan curve. The point  $x_4$  is either in  $\text{INT}(C)$  or in  $\text{EXT}(C)$ . Suppose  $x_4$  is in  $\text{INT}(C)$ . ( $x_4 \in \text{EXT}(C)$  is similar.)

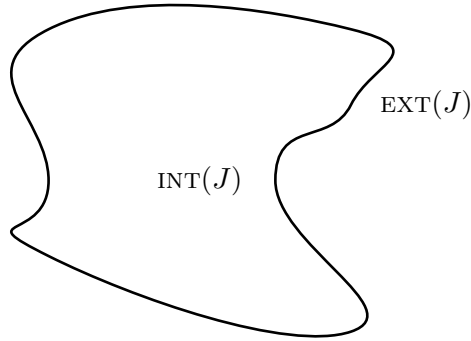


Figure 2.2: A Jordan curve.

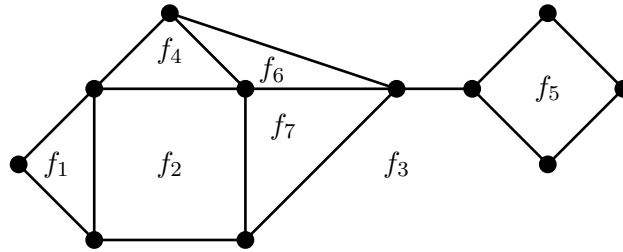


Figure 2.3: A plane graph with 7 faces.

The edges  $x_1x_4$ ,  $x_2x_4$ , and  $x_3x_4$  divide  $\text{INT}(C)$  into 3 regions:  $\text{INT}(C_1)$ ,  $\text{INT}(C_2)$ , and  $\text{INT}(C_3)$ , where  $C_1 = x_1x_4x_2x_1$ ,  $C_2 = x_2x_4x_3x_2$ , and  $C_3 = x_3x_4x_1x_3$ . The vertex  $x_5$  must lie in one of the four regions:  $\text{EXT}(C)$ ,  $\text{INT}(C_1)$ ,  $\text{INT}(C_2)$ , and  $\text{INT}(C_3)$ . If  $x_5 \in \text{EXT}(C)$ , then the edge  $x_5x_4$  must intersect  $C$  by the Jordan curve theorem. If  $x_5 \in \text{INT}(C_1)$ , then the edge  $x_5x_3$  must intersect  $C_1$  by the Jordan curve theorem. If  $x_5 \in \text{INT}(C_2)$ , then the edge  $x_5x_1$  must intersect  $C_2$  by the Jordan curve theorem. If  $x_5 \in \text{INT}(C_3)$ , then the edge  $x_5x_2$  must intersect  $C_3$  by the Jordan curve theorem.  $\square$

A shorter proof of Theorem 2.1.

## 2.3 Euler's formula

A plane graph  $G$  divides the plane into a number of connected regions called the faces (or regions) of  $G$ . See the plane graph in Figure 2.3. Let  $F = F(G)$  be the set of faces of the plane graph  $G$ . We will write  $G = (V, E, F)$  to denote a plane graph with vertex set  $V = V(G)$ , edge set  $E = E(G)$  and face set  $F = F(G)$ . A face  $f \in F$  is incident with its vertices and edges. The degree of a face  $f$  is  $\text{DEG}(f)$  and is the number of edges incident to  $f$ , counting cut edges twice.

**Theorem 2.2.** *In a plane graph  $G = (V, E, F)$  we have*

$$\sum_{f \in F} \text{DEG}(f) = 2|E|$$

*Proof.* Every edge is incident to 2 faces. □

**Theorem 2.3. (Euler's theorem.)** *Let  $G = (V, E, F)$  be a connected plane graph, then*

$$|V| - |E| + |F| = 2$$

*Proof.* (By induction on  $|F|$ .) If  $|F| = 1$ , then  $G$  contains no cycles and hence  $G$  is a tree. Thus  $|E| = |V| - 1$  by Corollary 1.14, and therefore

$$|V| - |E| + |F| = |V| - (|V| - 1) + 1 = 2$$

Now suppose  $|F| > 1$ . Then there is an edge  $e$  on some cycle and so  $G - e$  is connected. Therefore

$$|V(G - e)| - |E(G - e)| + |F(G - e)| = 2$$

But

$$\begin{aligned} |V(G - e)| &= |V| \\ |E(G - e)| &= |E| - 1 \\ |F(G - e)| &= |F| - 1 \end{aligned}$$

Hence,

$$2 = |V| - (|E| - 1) + (|F| - 1) = |V| - |E| + |F|$$

□

**Corollary 2.4.** *Let  $G = (V, E, F)$  be a (simple) planar graph with  $|V| \geq 3$ , then*

$$|E| \leq 3|V| - 6$$

*Proof.* It suffices to do this for connected graphs. Let  $G = (V, E, F)$  be a (simple) connected planar graph, with  $|V| \geq 3$ . Then  $\text{DEG}(f) \geq 3$  and so

$$2|E| = \sum_f \text{DEG}(f) \geq 3|F|$$

Hence,

$$|F| \leq \frac{2}{3}|E|.$$

Applying Euler's formula we have

$$\begin{aligned} 2 &= |V| - |E| + |F| \\ &\leq |V| - |E| + \frac{2}{3}|E| \\ &= |V| - \frac{1}{3}|E|. \end{aligned}$$

So,  $6 \leq 3|V| - |E|$  and thus  $|E| \leq 3|V| - 6$ . □

**Corollary 2.5.**  $K_5$  is non-planar.

*Proof.* If  $K_5$  were planar, then  $10 = |E| \leq 3|V| - 6 = 3 \cdot 5 - 6 = 9$ . A contradiction.  $\square$

**Corollary 2.6.** If  $G = (V, E, F)$  is a (simple) planar graph  $\delta(G) \leq 5$ .

*Proof.* This is trivially true for  $|V| = 1$  and  $|V| = 2$ . So suppose  $|V| \geq 3$ . Then,

$$\delta(G)|V| \leq \sum_{x \in V} \text{DEG}x = 2|E| \leq 6|V| - 12$$

by Corollary 2.4. Therefore  $\delta(G) \leq 6 - \frac{12}{|V|}$  and so  $\delta(G) \leq 5$ , because  $\delta(G)$  is integer.  $\square$

**Corollary 2.7.**  $K_{3,3}$  is non-planar.

*Proof.* Let  $G = (V, E, F)$  be a planar embedding. Now  $K_{3,3}$  is bipartite and so  $G$  contains no odd cycles. Therefore  $\text{DEG}(f) \geq 4$  for each face  $f \in F$ . So,

$$4|F| \leq \sum_{f \in F} \text{DEG}(f) = 2|E| = 2 \cdot 9 = 18$$

Therefore  $|F| \leq 4$ . But, then applying Euler's Formula we have

$$2 = |V| - |E| + |F| \leq 6 - 9 + 4 = 1,$$

a contradiction.  $\square$

## 2.4 Regular polyhedra

Consider the solid cube. (Figure 2.4.) Now picture a sphere with center at the center of the cube

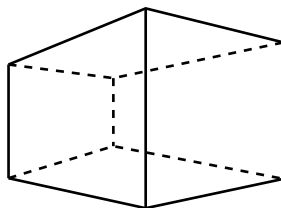


Figure 2.4: The Solid cube

and radius just large enough so that the vertices of the cube lie on its surface. Chose a vertex  $\mathbf{N}$  at the top of the sphere (centered above one of the faces of the cube) and let  $\mathbf{S}$  be the vertex diametrically opposite  $\mathbf{N}$ . Let  $\mathbb{P}$  be the plane tangent to the sphere at the point  $\mathbf{S}$ . If  $v$  is a point on the sphere, then its *stereographic projection* is the point  $\hat{v}$ , where the line  $\mathbf{n} + \lambda(v - \mathbf{n})$ ,  $\lambda \geq 0$  intersects the plane  $\mathbb{P}$ . See Figure 2.5. Thus the stereographic projection of a solid polyhedra is a plane graph. A *platonic solid* is a polyhedron in which all of its faces have the same shape and every vertex is on the same number of edges.

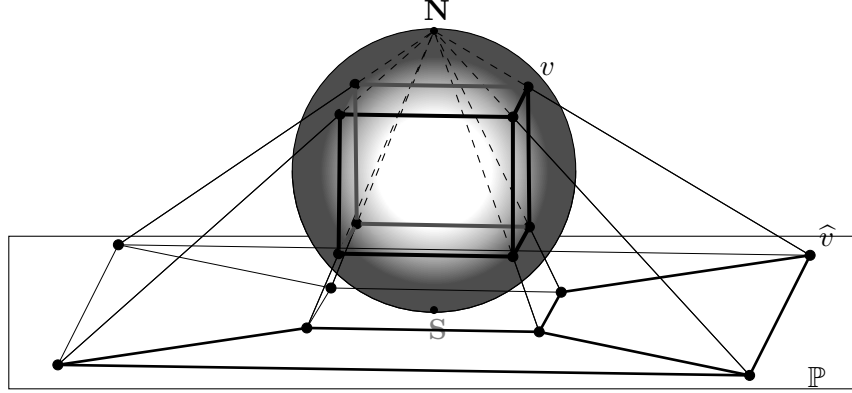


Figure 2.5: Stereographic projection

A plane graph  $G = (V, E, F)$  is a *platonic graph* if there exists constants  $k, \ell > 0$  such that  $\text{DEG}(x) = k$  for all  $x \in V$  and  $\text{DEG}(f) = \ell$  for all  $f \in F$ . Let  $n = |V|$ ,  $m = |E|$  and  $r = |F|$ . Notice that  $k, \ell \geq 3$ . Then by Euler we have

$$n - m + r = 2,$$

by the fundamental theorem of graph theory Theorem 1.3 we have

$$2m = nk,$$

and by Theorem 2.2 we have

$$2m = r\ell$$

Therefore:

$$\frac{2m}{k} - m + \frac{2m}{\ell} = 2$$

So,

$$m\left(\frac{2}{k} - 1 + \frac{2}{\ell}\right) = 2$$

Therefore

$$\left(\frac{2}{k} - 1 + \frac{2}{\ell}\right) > 0,$$

because  $m > 0$  and  $2 > 0$ . Consequently,

$$\begin{aligned} 2\ell - k\ell + 2k &> 0 \\ k\ell - 2\ell - 2k &< 0 \\ (k-2)(\ell-2) - 4 &< 0 \\ (k-2)(\ell-2) &< 4 \end{aligned}$$

There are thus 5 possibilities for the positive integers which we give in Table 2.1. The graphs are drawn in Figure 2.6.

Table 2.1: The 5 platonic graphs.

$k$	$l$	$(k-2)(l-2)$	$n =  V $	$m =  E $	$r =  F $	Name
3	3	1	4	6	4	<i>Tetrahedron</i>
3	4	2	8	12	6	<i>Cube</i>
3	5	3	20	30	12	<i>Dodecahedron</i>
4	3	2	6	12	8	<i>Octahedron</i>
5	3	3	12	30	20	<i>Icosahedron</i>

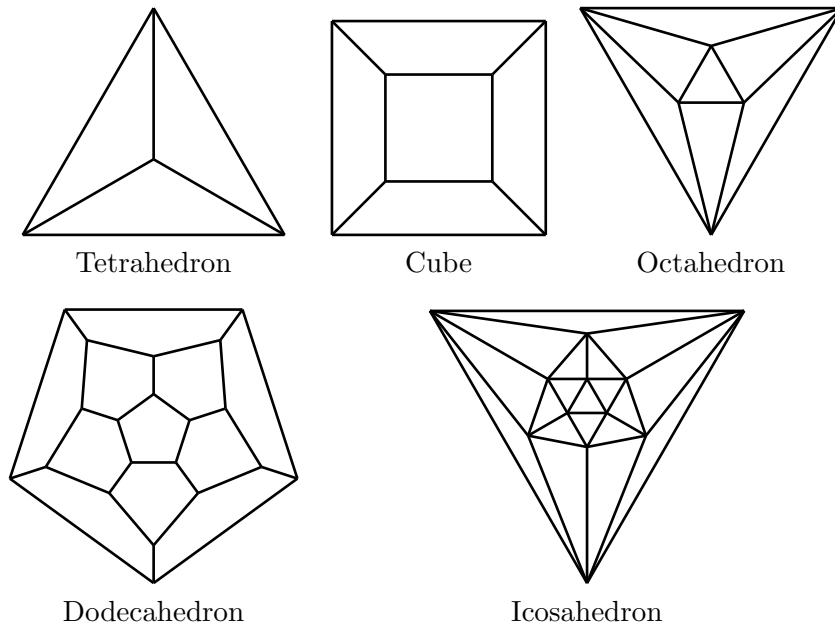


Figure 2.6: The 5 platonic graphs.

## 2.5 Kuratowski's theorem

The goal of this section will be to prove Kuratowski's Theorem which characterizes planar graphs.

### 2.5.1 Subdivision, contraction and minors

The graphs  $K_5$  and  $K_{3,3}$  are special graphs for planarity. If we construct a graph from  $K_5$  by replacing one or more edges with a path of length  $\geq 2$ , we obtain a *subdivision* of  $K_5$ . We say that the edges of  $K_5$  have been *subdivided*.

Given a graph  $G$ , a *subdivision* of  $G$  is any graph obtained from  $G$  by replacing one or more edges by paths of length two or more.

It is clear that any subdivision of  $K_5$  or  $K_{3,3}$  is non-planar, because  $K_5$  and  $K_{3,3}$  are non-planar. It is apparent that vertices of degree two do not affect the planarity of a graph. The inverse operation to subdividing an edge is to *contract* an edge with an endpoint of degree two.

Graphs  $G_1$  and  $G_2$  are *topologically equivalent* or *homeomorphic*, if  $G_1$  can be transformed into  $G_2$  by the operations of subdividing edges and/or contracting edges with an endpoint of degree two.

We will denote by  $TK_5$  any graph that is topologically equivalent to  $K_5$ . Similarly,  $TK_{3,3}$  denotes any graph that is topologically equivalent to  $K_{3,3}$ . In general,  $TK$  denotes a graph topologically equivalent to  $K$ , for any graph  $K$ . If  $G$  is a graph containing a subgraph  $TK_5$  or  $TK_{3,3}$ , then  $G$  must be non-planar. Kuratowski's theorem states that this is a necessary and sufficient condition for a graph to be non-planar.

If  $G$  is a planar graph, and we delete any vertex  $v$  from  $G$ , then  $G - v$  is still planar. Similarly, if we delete any edge  $uv$ , then  $G - uv$  is still planar. Also, if we contract any edge  $uv$  of  $G$ , then  $G \cdot uv$  is still planar. Contracting an edge can create parallel edges or loops. Because parallel edges and loops do not affect the planarity of a graph, loops can be deleted, and parallel edges can be replaced by a single edge, if desired.

Let  $H$  be a graph obtained from  $G$  by any sequence of deleting vertices and/or edges, and/or contracting edges.  $H$  is said to be a *minor* of  $G$ . (We also say  $G$  has minor  $H$ .)

Notice that if  $G$  contains a subgraph  $TK_5$ ,  $K_5$  is a minor of  $G$ , even though  $K_5$  need not be a subgraph of  $G$ . For we can delete all vertices and edges which do not belong to the subgraph  $TK_5$ , and then contract edges to obtain  $K_5$ . Similarly, if  $G$  has a subgraph  $TK_{3,3}$ , then  $K_{3,3}$  is a minor of  $G$ , but need not be a subgraph. Any graph having  $K_5$  or  $K_{3,3}$  as a minor is non-planar. A special case of minors is when a graph  $K$  is subdivided to obtain  $G$ .

**Lemma 2.8.** *Let  $G$  be any graph obtained by splitting a vertex of  $K_5$ . Then  $G$  contains a subgraph  $TK_{3,3}$ .*

*Proof.* Let  $v_1$  and  $v_2$  be the two vertices resulting from splitting a vertex of  $K_5$ . Each has at least degree three. Consider  $v_1$ . It is joined to  $v_2$ . Together,  $v_1$  and  $v_2$  are joined to the remaining four vertices of  $G$ , and each is joined to at least two of these vertices. Therefore we can choose a partition of these four vertices into  $x, y$  and  $w, z$  such that  $v_1$  is adjacent to  $x$  and  $y$  and such that  $v_2$  such that  $w$  and  $z$ . Then  $G$  contains a  $K_{3,3}$  with bipartition  $v_1, w, z$  and  $v_2, x, y$ , as illustrated in Figure 2.7.  $\square$

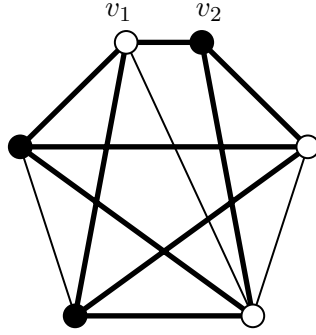


Figure 2.7: Splitting a vertex of  $K_5$

**Theorem 2.9.** *If  $G$  has a minor  $K_{3,3}$ , then  $G$  contains a subgraph  $TK_{3,3}$ . If  $G$  has a minor  $K_5$ , then  $G$  contains a subgraph  $TK_5$  or  $TK_{3,3}$ .*

*Proof.* Suppose that  $G$  has a minor  $K_5$  or  $K_{3,3}$ . If no edges were contracted to obtain this minor, then it is also a subgraph of  $G$ . Otherwise let  $G_0, G_1, \dots, G_k$  be a sequence of graphs obtained from  $G$ , where  $G_0$  is a subgraph of  $G$ , edge  $e_i$  of  $G_{i-1}$  is contracted to obtain  $G_i$ , and  $G_k$  is either  $K_5$  or  $K_{3,3}$ .

If each  $e_i$  has an endpoint of degree two, then we can reverse the contractions by subdividing edges, resulting in a  $TK_5$  or  $TK_{3,3}$  in  $G$ , as required. Otherwise let  $e_i$  be the edge with largest  $i$ , with both endpoints of at least degree three. All edges contracted subsequent to  $G_i$  have an endpoint of degree two, so that  $G_i$  has a subgraph  $TK_5$  or  $TK_{3,3}$ .  $G_{i-1}$  can be obtained by splitting a vertex  $v$  of  $G_i$ . If  $v$  is a vertex of  $TK_5$ , then by Lemma 2.8,  $G_{i-1}$  contains  $TK_{3,3}$ . If  $v$  is a vertex of  $TK_{3,3}$ , then  $G_{i-1}$  also contains  $TK_{3,3}$ . If  $v$  is a vertex of neither  $TK_5$  nor  $TK_{3,3}$ , then  $G_{i-1}$  still contains  $TK_5$  or  $TK_{3,3}$ . In each case we find that  $G_0$  must have a subgraph  $TK_5$  or  $TK_{3,3}$ .  $\square$

### 2.5.2 Blocks and seperable graphs

If a connected graph  $G$  has a cut-vertex  $v$ , then it is said to be *separable*, because deleting  $v$  separates  $G$  into two or more components. A separable graph has  $\kappa = 1$ , but it may have subgraphs which are 2-connected, just as a disconnected graph has connected subgraphs. We can then find the maximal non-separable subgraphs of  $G$ , just as we found the components of a disconnected graph. This is illustrated in Figure 2.8.

The maximal non-separable subgraphs of  $G$  are called the *blocks* of  $G$ . The graph illustrated in Figure 2.8 has eight blocks, held together by cut-vertices.

### 2.5.3 Proof of Kuratowski's theorem

We now prove Kuratowski's theorem. The proof presented is based on the W. Klotz's (1989) proof<sup>1</sup>. It uses induction on  $m = |E(G)|$ .

<sup>1</sup>W. Klotz, A constructive proof of Kuratowski's theorem, *Ars Combin.*, **28** (1989), 51–54.



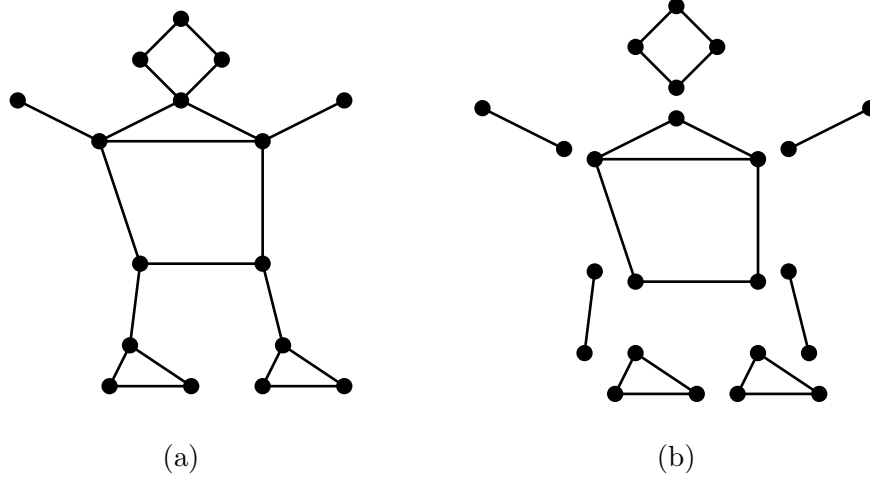


Figure 2.8: A graph (a) and its blocks (b)

If  $G$  is a disconnected graph, then  $G$  is planar if and only if each connected component of  $G$  is planar. Therefore we assume that  $G$  is connected. If  $G$  is a separable graph that is planar, let  $H$  be a block of  $G$  containing a cut-vertex  $v$ .  $H$  is also planar, because  $G$  is. We can delete  $H - v$  from  $G$ , and find a planar embedding of the result. We then choose a planar embedding of  $H$  with  $v$  on the outer face, and embed  $H$  into a face of  $G$  having  $v$  on its boundary. This gives:

**Lemma 2.10.** *A separable graph is planar if and only if all its blocks are planar.*

So there is no loss in generality in starting with a 2-connected graph  $G$ .

**Theorem 2.11. (Kuratowski's theorem)** *A graph  $G$  is planar if and only if it contains no subgraph  $TK_{3,3}$  or  $TK_5$ .*

*Proof.* It is clear that if  $G$  is planar, then it contains no subgraph  $TK_{3,3}$  or  $TK_5$ . To prove the converse, we show that if  $G$  is non-planar, then it must contain  $TK_{3,3}$  or  $TK_5$ . We assume that  $G$  is a simple, 2-connected graph with  $m$  edges. To start the induction, notice that if  $m \leq 6$ , the result is true, as all graphs with  $m \leq 6$  are planar. Suppose that the theorem is true for all graphs with at most  $m - 1$  edges. Let  $G$  be non-planar, and let  $ab \in E(G)$  be any edge of  $G$ . Let  $G' = G - ab$ . If  $G'$  is non-planar, then by the induction hypothesis, it contains a  $TK_{3,3}$  or  $TK_5$ , which is also a subgraph of  $G$ . Therefore we assume that  $G'$  is planar. Let  $\kappa(a, b)$  denote the number of internally disjoint  $ab$ -paths in  $G'$ . Because  $G$  is 2-connected, we know that  $\kappa(a, b) \geq 1$ .

**Case 1.**  $\kappa(a, b) = 1$ .

$G'$  has a cut-vertex  $u$  contained in every  $ab$ -path. Add the edges  $au$  and  $bu$  to  $G'$ , if they are not already present, to get a graph  $H$ , with cut-vertex  $u$ . Let  $H_a$  and  $H_b$  be the blocks of  $H$  containing  $a$  and  $b$ , respectively. If one of  $H_a$  or  $H_b$  is non-planar, say  $H_a$ , then by the induction hypothesis, it contains a  $TK_{3,3}$  or  $TK_5$ . This subgraph must use the edge  $au$ , as  $G'$  is planar. Replace the edge  $au$  by a path consisting of the edge  $ab$  plus a  $bu$ -path in  $H_b$ . The result is a  $TK_{3,3}$  or  $TK_5$  in  $G$ . If  $H_a$  and  $H_b$  are both planar, choose planar embeddings of them with edges  $au$  and  $bu$  on the outer face. Glue them together at vertex  $u$ , remove

the edges  $au$  and  $bu$  that were added, and restore  $ab$  to obtain a planar embedding of  $G$ , a contradiction.

**Case 2.**  $\kappa(a, b) = 2$ .

Let  $P_1$ , and  $P_2$  be two internally disjoint  $ab$ -paths in  $G'$ . Because  $\kappa(a, b) = 2$ , there is a vertex  $u \in P_1$  and  $v \in P_2$  such that all  $ab$ -paths contain at least one of  $\{u, v\}$ , and  $G' - \{u, v\}$  is disconnected. If  $K_a$  denotes the connected component of  $G' - \{u, v\}$  containing  $a$ , let  $G'_a$  be the subgraph of  $G'$  induced by  $K_a \cup \{u, v\}$ . Let  $K_b$  denote the remaining connected components of  $G' - \{u, v\}$ , and let  $G'_b$  be the subgraph of  $G'$  induced by  $K_b \cup \{u, v\}$ , except that  $uv$ , if it is an edge of  $G'$ , is not included (because it is already in  $G'_a$ ). Now add a vertex  $x$  to  $G'_a$ , adjacent to  $u, v$ , and  $a$  to obtain a graph  $H_a$ . Similarly, add  $y$  to  $G'_b$  adjacent to  $u, v$ , and  $b$  to obtain a graph  $H_b$ . Suppose first that  $H_a$  and  $H_b$  are both planar. As vertex  $x$  has degree three in  $H_a$ , there are three faces incident on  $x$ . Embed  $H_a$  in the plane so that the face with edges  $ux$  and  $xv$  on the boundary is the outer face. Embed  $H_b$  so that edges  $uy$  and  $yv$  are on the boundary of the outer face. Now glue  $H_a$  and  $H_b$  together at vertices  $u$  and  $v$ , delete vertices  $x$  and  $y$ , and add the edge  $ab$  within the face created, to obtain a planar embedding of  $G$ . Because  $G$  is non-planar, we conclude that at least one of  $H_a$  and  $H_b$  must be non-planar. Suppose that  $H_a$  is non-planar. It must contain a subgraph  $TK_5$  or  $TK_{3,3}$ . If the  $TK_5$  or  $TK_{3,3}$  does not contain  $x$ , then it is also contained in  $G$ , and we are done. Otherwise the  $TK_5$  or  $TK_{3,3}$  contains  $x$ . Now  $H_b$  is 2-connected (because  $G$  is), so that it contains internally disjoint paths  $P_{bu}$  and  $P_{bv}$  connecting  $b$  to  $u$  and  $v$ , respectively. These paths, plus the edge  $ab$ , can be used to replace the edges  $ux$ ,  $vx$ , and  $ax$  in  $H_a$  to obtain a  $TK_5$  or  $TK_{3,3}$  in  $G$ .

**Case 3.**  $\kappa(a, b) \geq 3$ .

Let  $P_1, P_2$ , and  $P_3$  be three internally disjoint  $ab$ -paths in  $G'$ . Consider a planar embedding of  $G'$ . Each pair of paths  $P_1 \cup P_2$ ,  $P_1 \cup P_3$ , and  $P_2 \cup P_3$  creates a cycle, which embeds as a Jordan curve in the plane. Without loss of generality, assume that the path  $P_2$  is contained in the interior of the cycle  $P_1 \cup P_3$ , as in Figure 2.9. The edge  $ab$  could be placed either in the interior of  $P_1 \cup P_2$  or  $P_2 \cup P_3$ , or else in the exterior of  $P_1 \cup P_3$ . As  $G$  is non-planar, each of these regions must contain a path from an interior vertex of  $P_i$  to an interior vertex of  $P_j$ . Let  $P_{12}$  be a path from  $u_1$  on  $P_1$  to  $u_2$  on  $P_2$ . Let  $P_{13}$  be a path from  $v_1$  on  $P_1$  to  $u_3$  on  $P_3$ . Let  $P_{23}$  be a path from  $v_2$  on  $P_2$  to  $v_3$  on  $P_3$ . If  $u_1 \neq v_1$ , contract the edges of  $P_1$  between them. Do the same for  $u_2, v_2$  on  $P_2$  and  $u_3, v_3$  on  $P_3$ . Adding the edge  $ab$  to the resultant graph then results in a  $TK_5$  minor. By Theorem 2.9,  $G$  contains either a  $TK_5$  or  $TK_{3,3}$ .

□

## 2.5.4 Exercises

1. Show that adding a new edge to a maximal planar graph of order at least 6 always produces both  $K_5$  and  $K_{3,3}$  as topological minors.
2. Show that a 2-connected plane graph is bipartite if and only if every face is bounded by an even cycle.

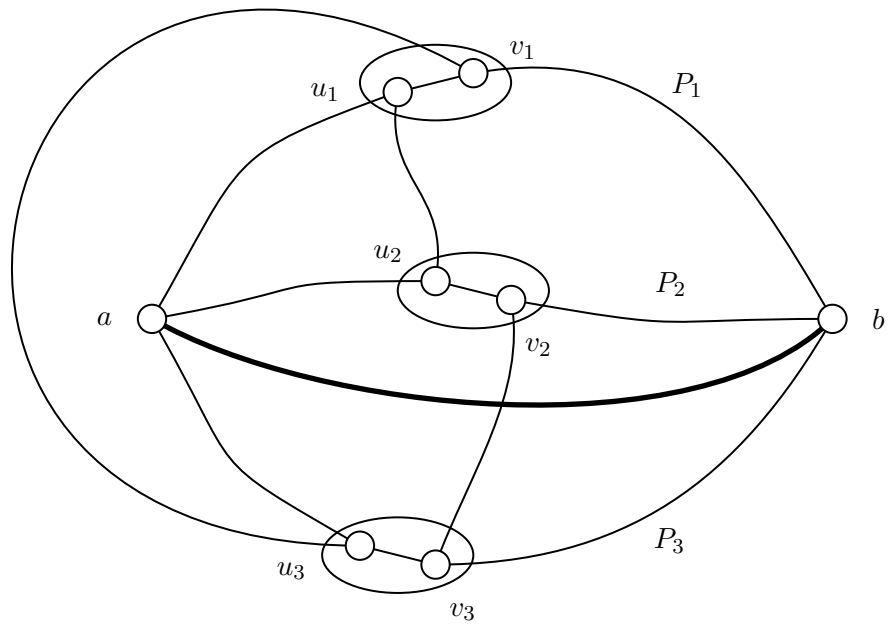


Figure 2.9: A  $K_5$  minor



## Chapter 3

# Algebraic Graph Theory

In algebraic graph theory we study the algebras that can be associated with a graph  $G$ , and try to obtain graphical information from these algebras.

### 3.1 Spectrum

The *adjacency matrix* of a graph  $G = (V, E)$  is the  $V$  by  $V$  matrix  $A = A_G$ , where

$$A[x, y] = \begin{cases} 1 & \text{if } xy \in E \\ 0 & \text{if } xy \notin E. \end{cases}$$

The adjacency matrix is a real symmetric matrix. It follows that the eigen values of  $A$  are real and that  $A$  has a set of  $n$  linearly independent eigen vectors.

**Proposition 3.1.** *The eigen values of  $A$  are real.*

*Proof.* Let  $\lambda$  be an eigen value of  $A$ . Then  $A\vec{u} = \lambda\vec{u}$  for some complex valued vector  $\vec{u}$ . If  $z = a+bi \in \mathbb{C}$ , then let  $\bar{z} = a-bi$ , the complex conjugate of  $z$ . We may also assume  $\vec{u}^T \vec{u} = \|\vec{u}\| = 1$ . For otherwise we can use  $\vec{u}/\|\vec{u}\|$  for our eigen vector with eigen value  $\lambda$ . Thus

$$\lambda = \lambda(\vec{u}^T \vec{u}) = \vec{u}^T (\lambda\vec{u}) = \vec{u}^T (A\vec{u}) = (\vec{u}^T A)\vec{u} = (\vec{u}^T A^T)\vec{u} = (\overline{A\vec{u}})^T \vec{u} = (\overline{\lambda\vec{u}})^T \vec{u} = \overline{\lambda\vec{u}^T} \vec{u} = \bar{\lambda}$$

Consequently  $\lambda$  is a real number. □

Recall that if  $\lambda$  is an eigen value of  $A$ , then  $A\vec{u} = \lambda\vec{u}$  for some nonzero vector  $\vec{u}$ . Hence  $(\lambda I - A)\vec{u} = 0$  and so the columns of  $\lambda I - A$  are linearly dependent and therefore  $\det(\lambda I - A) = 0$ . Consequently the eigen values of  $A$  are the roots of

$$\chi_G(\lambda) = \det(\lambda I_n - A) = \lambda^n + c_1 \lambda^{n-1} + c_2 \lambda^{n-2} + \cdots + c_{n-1} \lambda + c_n$$

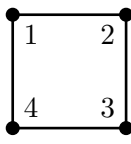
the *characteristic polynomial* of  $A$ . ( $I_n$  is the  $n$  by  $n$  identity matrix.)

The *spectrum* of the graph  $G$  is the list of the eigen values of  $A$ , the adjacency matrix of  $G$ . Let  $\lambda_1 > \lambda_2 > \cdots > \lambda_s$  be the  $s$  distinct eigen values of  $A$ . The number  $m_i$  of times  $\lambda_i$  is a root of  $\chi_G(\lambda)$ , is called the *algebraic multiplicity* of  $\lambda$ . We exhibit the spectrum of  $G$  as follows:

$$\text{SPEC}(G) = \begin{pmatrix} \lambda_1 & \lambda_2 & \cdots & \lambda_s \\ m_1 & m_2 & \cdots & m_s \end{pmatrix}$$

Thus the characteristic polynomial of  $G$  is

$$\chi_G(\lambda) = \det(\lambda I_n - A) = (\lambda - \lambda_1)^{m_1} (\lambda - \lambda_2)^{m_2} \dots (\lambda - \lambda_s)^{m_s}$$

For example the the adjacency matrix of the 4-cycle  $G =$   is  $\begin{bmatrix} 0 & 1 & 0 & 1 \\ 1 & 0 & 1 & 0 \\ 0 & 1 & 0 & 1 \\ 1 & 0 & 1 & 0 \end{bmatrix}$  and thus

$$\text{SPEC}(G) = \left( \begin{array}{ccc} 2 & 0 & -2 \\ 1 & 2 & 1 \end{array} \right).$$

To motivate our study of adjacency matrix eigen values consider the following theorem.

**Theorem 3.2.** *Let  $G = (V, E)$  be a graph with adjacency matrix  $A$  and characteristic polynomial*

$$\chi_G(\lambda) = \lambda^n + c_1 \lambda^{n-1} + c_2 \lambda^{n-2} + \dots + c_{n-1} \lambda + c_n.$$

Then

1.  $c_1 = 0$ ;
2.  $-c_2 = |E|$  the number of edges in  $G$ ;
3.  $-c_3$  is twice the number of triangles in  $G$ .

Thus the coefficients of the characteristic polynomial carry graphical information. This result follows from the computation of the coefficients  $c_k$  as the sum of principle minors. That is

$$c_k = (-1)^k \sum \{ \det A_K : K \subseteq V, |K| = k \}$$

where  $A_K$  is the  $K$  by  $K$  sub-matrix of  $A$  whose rows and columns are indexed by the vertices in  $K$ . The sub-matrix  $A_K$  is called a *principle minor*. We now prove Theorem 3.2.

*Proof.* (of Theorem 3.2)

1. The principle minors with one row and column are the diagonal entries of  $A$  and these are all zero. Hence  $c_1 = 0$ .
2. If  $K = \{x, y\} \subseteq V$ ,  $x \neq y$ . Then either

$$A_K = \begin{bmatrix} 0 & 0 \\ 0 & 0 \end{bmatrix} \text{ or } A_K = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}.$$

The first possibility occurs when  $xy \notin E$  and has determinant 0, while the second occurs when  $xy \in E$  and has determinant  $-1$ ,

3. If  $K = \{x, y, z\} \subseteq V$ ,  $x \neq y \neq z \neq x$ . Then  $A_K$  is

$$\begin{bmatrix} 0 & 0 & 0 \\ 0 & 0 & 0 \\ 0 & 0 & 0 \end{bmatrix}, \begin{bmatrix} 0 & 0 & 0 \\ 0 & 0 & 1 \\ 0 & 1 & 0 \end{bmatrix}, \begin{bmatrix} 0 & 1 & 0 \\ 1 & 0 & 0 \\ 0 & 0 & 0 \end{bmatrix}, \begin{bmatrix} 0 & 1 & 0 \\ 1 & 0 & 1 \\ 0 & 1 & 0 \end{bmatrix}, \begin{bmatrix} 0 & 0 & 1 \\ 0 & 0 & 0 \\ 1 & 0 & 0 \end{bmatrix}, \begin{bmatrix} 0 & 0 & 1 \\ 0 & 0 & 1 \\ 1 & 1 & 0 \end{bmatrix}, \begin{bmatrix} 0 & 1 & 1 \\ 1 & 0 & 0 \\ 1 & 0 & 0 \end{bmatrix} \text{ or } \begin{bmatrix} 0 & 1 & 1 \\ 1 & 0 & 1 \\ 1 & 1 & 0 \end{bmatrix}.$$

Only the last one has non-zero determinant. It has value 2.

□

Here is useful theorem on eigen values that relates the eigen values between two matrices.

**Theorem 3.3.** *Let  $A$  be any  $n$  by  $n$  matrix and let*

$$f(x) = f_0x^n + f_1x^{n-1} + f_2x^{n-2} + \cdots + f_{k-1}x + f_k$$

*be any polynomial. Define the matrix  $f(A)$  by*

$$f(A) = f_0A^n + f_1A^{n-1} + f_2A^{n-2} + \cdots + f_{k-1}A + f_kI$$

*If  $\lambda_1, \lambda_2, \dots, \lambda_n$  are the eigen values of  $A$  then  $f(\lambda), f(\lambda_1), f(\lambda_2), \dots, f(\lambda_n)$  are the eigen values of  $f(A)$ .*

*Proof.* Let  $\vec{u}$  be an eigen vector of  $A$  with eigen value  $\lambda$ . Then  $A\vec{u} = \lambda\vec{u}$  and so,  $A^j\vec{u} = \lambda^j\vec{u}$ . Thus

$$\begin{aligned} f(A)\vec{u} &= (f_0A^n + f_1A^{n-1} + f_2A^{n-2} + \cdots + f_{k-1}A + f_kI)\vec{u} \\ &= f_0A^n\vec{u} + f_1A^{n-1}\vec{u} + f_2A^{n-2}\vec{u} + \cdots + f_{k-1}A\vec{u} + f_k\vec{u} \\ &= f_0\lambda^n\vec{u} + f_1\lambda^{n-1}\vec{u} + f_2\lambda^{n-2}\vec{u} + \cdots + f_{k-1}\lambda\vec{u} + f_k\vec{u} \\ &= (f_0\lambda^n + f_1\lambda^{n-1} + f_2\lambda^{n-2} + \cdots + f_{k-1}\lambda + f_k)\vec{u} \\ &= f(\lambda)\vec{u} \end{aligned}$$

□

For example consider the  $n$  by  $n$  matrix  $J_n$  that has every entry 1. Then

$$\vec{\mathbf{1}} = \underbrace{[1, 1, \dots, 1]^T}_{n \text{ times}}$$

is an eigen vector with eigen value  $n$  and the  $n - 1$  vectors  $u_i, i = 2, 3, \dots, n$  given by

$$\vec{u}_i[j] = \begin{cases} 1 & \text{if } j = 1 \\ -1 & \text{if } j = i \\ 0 & \text{otherwise} \end{cases}$$

are linearly independent eigen vectors with eigen value 0. Thus the eigen values of  $J_n$  are

$$n, \underbrace{0, 0, \dots, 0}_{n-1 \text{ times}}.$$

The adjacency matrix  $A$  of the complete graph  $K_n$  is  $A = J_n - I_n$ . Thus  $A = f(J)$  where  $f(x) = x - 1$ . Therefore the eigen values of  $A$  are

$$n - 1, \underbrace{-1, -1, \dots, -1}_{n-1 \text{ times}}.$$

Hence

$$\text{SPEC}(K_n) = \left( \begin{array}{c} n - 1, -1 \\ 1, n - 1 \end{array} \right)$$

If  $A$  is the adjacency matrix of a graph  $G$ , then the set of polynomials in  $A$  with complex coefficients is an algebra under the usual matrix operations. This algebra is called the *adjacency algebra* and we denote it by

$$\mathcal{Alg}(G) = \{f(A) : f(x) \in \mathbb{C}[x]\}.$$

This algebra has finite dimension as a vector space over the complex numbers  $\mathbb{C}$ . Our next few theorems relates the dimension of  $\mathcal{Alg}(G)$  to  $\text{DIAM}(G)$  the diameter of  $G$ . Recall that

$$\text{DIAM}(G) = \text{MAX}\{\text{DIST}(x, y) : x, y \in V(G)\},$$

where  $\text{DIST}(x, y)$  is the length of the shortest path in  $G$ .

**Theorem 3.4.** *The number of walks of length  $\ell$  in  $G$  from vertex  $x$  to vertex  $y$  is  $A^\ell[x, y]$ .*

*Proof.* ( by induction on  $\ell$ , the length of the walk.) If  $\ell \in \{0, 1\}$ , then the result is obvious. So suppose  $\ell > 1$ , then by induction  $A^{\ell-1}[x, h]$  is the number of walks of length  $\ell - 1$  from  $x$  to  $h$ . Hence  $A^{\ell-1}[x, h]A[h, y]$  is the number of walks of length  $\ell$  from  $x$  to  $y$  whose penultimate vertex is  $h$ . Summing over all vertices  $h$  we have

$$A^\ell[x, y] = \sum_{h \in V(G)} A^{\ell-1}[x, h]A[h, y]$$

is the number of walks from  $x$  to  $y$  that have length  $\ell$ . □

**Theorem 3.5.** *The dimension of  $\mathcal{Alg}(G)$  is at least  $\text{DIAM}(G) + 1$*

*Proof.* Let  $d = \text{DIAM}(G)$  and choose vertices  $x, y$  such that  $\text{DIST}(x, y) = d$ . Let

$$x = x_0x_1x_2, \dots, x_d = y$$

be a path from  $x$  to  $y$  of length  $d$ . Then  $A^d[x_0, x_d] \neq 0$ , but  $A^j[x_0, x_d] = 0$  for all  $j < d$ . Hence  $I, A, A^2, \dots, A^d$  are linearly independent. □

**Proposition 3.6.**  *$A$  has  $n$  linearly independent eigen vectors.*

*Proof.* Let  $\lambda_1$  be an eigen value (there must be at least one) and let  $\vec{u}_1$  be an associated eigen vector of unit length, so  $A\vec{u}_1 = \lambda_1\vec{u}_1$  and  $\|\vec{u}_1\| = 1$ . Furthermore  $\vec{u}_1$  is real valued because  $\lambda$  is real. Using the Gram-Schmidt process extend  $\vec{u}_1$  to an orthonormal basis  $\{\vec{u}_1, \vec{u}_2, \vec{u}_3, \dots, \vec{u}_n\}$ . Let



$R = [\vec{u}_2, \vec{u}_3, \dots, \vec{u}_n]$  and  $U = [\vec{u}_1, R]$  Then  $U^T U = I$ . Consider the matrix  $U^T A U$ .

$$\begin{aligned}
U^T A U &= [\vec{u}_1, R]^T A [\vec{u}_1, R] \\
&= [\vec{u}_1, R]^T [\lambda \vec{u}_1, AR] \\
&= \left[ \begin{array}{c|c} \vec{u}_1^T \lambda \vec{u}_1 & \vec{u}_1^T AR \\ \hline R^T \lambda \vec{u}_1 & R^T AR \end{array} \right] \\
&= \left[ \begin{array}{c|c} \lambda (\vec{u}_1^T \vec{u}_1) & (A \vec{u}_1)^T R \\ \hline \lambda (R^T \vec{u}_1) & R^T AR \end{array} \right] \\
&= \left[ \begin{array}{c|c} \lambda & (\lambda \vec{u}_1)^T R \\ \hline 0 & R^T AR \end{array} \right] \\
&= \left[ \begin{array}{c|c} \lambda & \lambda (\vec{u}_1^T R) \\ \hline 0 & R^T AR \end{array} \right] \\
&= \left[ \begin{array}{c|c} \lambda & 0 \\ \hline 0 & R^T AR \end{array} \right] \\
&= \left[ \begin{array}{c|c} \lambda & 0 \\ \hline 0 & B \end{array} \right]
\end{aligned}$$

where  $B = R^T AR$ . The matrix  $B$  is a real symmetric matrix with one less row and column than  $A$ . We can repeat the process obtaining another eigen value on the diagonal. Continuing we obtain a matrix  $S$  such that  $S^T A S$  is a diagonal matrix of the eigen values of  $A$ , and the columns of  $S$  are an orthonormal basis of eigen vectors.  $\square$

The minimum polynomial  $\mu_A(x)$  of a matrix  $A$  is the monic polynomial of smallest degree such that  $\mu_A(A) = 0$ .

**Proposition 3.7.** *Let  $A$  be the adjacency matrix of a graph  $G$ . Then*

$$\mu_A(\lambda) = (\lambda - \lambda_1)(\lambda - \lambda_2)(\lambda - \lambda_3) \cdots (\lambda - \lambda_s)$$

where  $\lambda_1, \lambda_2, \dots, \lambda_s$  are the distinct eigen values of  $A$ .

*Proof.* Applying Proposition 3.6 we see that there is an  $n$  by  $n$  matrix  $S = [\vec{S}_1, \vec{S}_2, \dots, \vec{S}_n]$  whose columns are linearly independent eigen vectors of  $A$ . Let  $D = \text{DIAG}(\lambda'_1, \lambda'_2, \dots, \lambda'_n)$  be the diagonal matrix in which  $A \vec{S}_i = \lambda'_i \vec{S}_i$ . Then  $A = SDS^{-1}$  and  $\mu_A(\lambda'_i) = 0$ , for all  $i$ . Hence,  $\mu(A) = S\mu(D)S^{-1} = S\text{DIAG}(\mu_A(\lambda'_1), \mu_A(\lambda'_2), \dots, \mu_A(\lambda'_n))S^{-1} = 0$ . Furthermore if  $f(x)$  is any polynomial such that  $f(A) = 0$ , then  $0 = f(A) = Sf(D)S^{-1} = S\text{DIAG}(f(\lambda'_1), f(\lambda'_2), \dots, f(\lambda'_n))S^{-1}$  and consequently  $\lambda'_i$  is a root of  $f(x)$  for each  $i = 1, 2, \dots, s$ . Therefore  $\text{DEG}(f(x)) \geq \text{DEG}(\mu_A(x))$ .  $\square$

**Corollary 3.8.** *A connected graph with  $n$  vertices and diameter  $d$  has at least  $d + 1$  and at most  $n$  distinct eigen values.*

*Proof.* The degree of the minimum polynomial cannot be less than the dimension of the adjacency algebra.  $\square$

## 3.2 Regular graphs

**Theorem 3.9.** *Let  $G$  be a regular graph of degree  $k$ . Then*

1.  $k$  is an eigen value of  $G$ .
2. If  $G$  is connected, then the multiplicity of  $k$  is one.
3. For any eigen value  $\lambda$  of  $G$ , we have  $|\lambda| \leq k$ .

*Proof.* 1. Let

$$\vec{\mathbf{1}} = \underbrace{[1, 1, \dots, 1]}_{n \text{ times}}^T$$

Then  $A\vec{\mathbf{1}} = k\vec{\mathbf{1}}$ , so  $k$  is an eigen value.

2. We compute the eigenspace with eigen value  $k$ . Let  $A\vec{u} = k\vec{u}$  for some non-zero vector  $\vec{u}$ . Choose vertex  $x$  such that  $|\vec{u}[x]|$  is largest. We may assume that  $\vec{u}[x] > 0$ , for otherwise we can take  $-\vec{u}$ . Let  $y_1, y_2, \dots, y_k$  be the  $k$  vertices adjacent to  $x$ . Then

$$k\vec{u}[x] = (A\vec{u})[x] = \vec{u}[y_1] + \vec{u}[y_2] + \dots + \vec{u}[y_k] \leq \vec{u}[x] + \vec{u}[x] + \dots + \vec{u}[x] = k\vec{u}[x]$$

Thus  $\vec{u}[x] = \vec{u}[y]$  for all  $y$  adjacent to  $x$ . Hence, because  $G$  is connected we can repeat their argument until all entries of  $\vec{u}$  have been shown to be equal. Thus  $\vec{u} = \alpha\vec{\mathbf{1}}$  for some  $\alpha$ . Hence the eigen space with eigen value  $k$  is  $\{\alpha\vec{\mathbf{1}} : \alpha \in \mathbb{C}\}$ . Thus  $k$  has multiplicity one.

3. Let  $\lambda$  be any eigen value of  $G$ , and let  $\vec{u}$  be such that  $A\vec{u} = \lambda\vec{u}$ . Let  $x$  be a vertex such that  $|\vec{u}[x]|$  is largest. Let  $y_1, y_2, \dots, y_k$  be the  $k$  vertices adjacent to  $x$ . Then

$$\begin{aligned} |\lambda||\vec{u}[x]| = |A\vec{u}[x]| &= |\vec{u}[y_1] + \vec{u}[y_2] + \dots + \vec{u}[y_k]| \\ &\leq |\vec{u}[y_1]| + |\vec{u}[y_2]| + \dots + |\vec{u}[y_k]| \\ &\leq |\vec{u}[x]| + |\vec{u}[x]| + \dots + |\vec{u}[x]| = k|\vec{u}[x]| \end{aligned}$$

Therefore  $|\lambda| \leq k$

□

**Theorem 3.10.** *(Hoffman 1963) Let  $G$  be a graph. Then  $J \in \text{Alg}(G)$  if and only if  $G$  is a regular connected graph.*

*Proof.* Let  $A$  be the adjacency matrix of the graph  $G$ . Suppose  $J \in \text{Alg}(G)$ . Then  $J = P(A)$  for some polynomial  $P(x) \in \mathbb{C}[x]$ . Thus  $AJ = JA$  and so

$$\text{DEG}(x) = (AJ)[x, y] = (JA)[x, y] = \text{DEG}(y)$$

for all vertices  $x$  and  $y$ . Therefore  $G$  is regular. If  $G$  were disconnected, there would be vertices  $x$  and  $y$  with no walk between them. Hence  $A^\ell[x, y] = 0$  for all  $\ell$  and it therefore impossible for  $J = P(A)$  for any polynomial  $P(x)$ .

Conversely suppose  $G$  is a regular connected graph of degree  $k$ . Then by Theorem 3.9, we know that  $k$  is an eigen value and hence the minimum polynomial of  $A$  is of the form

$$\mu_A(x) = (x - k)P(x)$$

for some  $P(x) \in \mathbb{C}[x]$ . Then

$$0 = \mu_A(A) = (A - kI)P(A),$$

and hence

$$AP(A) = kP(A).$$

Thus each column of  $P(A)$  is an eigen vector with eigen value  $k$ . So by 3.9, each column of  $P(A)$  is a multiple of  $\vec{1}$  and thus  $P(A) = tJ$  for some constant  $t$ , because  $A$  and hence  $P(A)$  is symmetric. Also,  $t$  is not zero, because  $\text{DEG}(P(x)) < \text{DEG}(\mu_A(x))$ . Therefore

$$J = \frac{1}{t}P(A) \in \text{Alg}(G).$$

□

Another matrix associated with a graph  $G = (V, E)$  is *incidence matrix*. This is the  $V$  by  $E$  matrix  $X = X_G$  given by

$$X[x, e] = \begin{cases} 1 & \text{if } x \text{ is incident to } e, \\ 0 & \text{if not.} \end{cases}$$

Observe for vertices  $x$  and  $y$  that the  $[x, y]$ -entry of  $XX^T$  is

$$\begin{aligned} XX^T[x, y] &= \sum_{e \in E} X[x, e]X^T[e, y] \\ &= \sum_{e \in E} X[x, e]X[y, e] \\ &= |\{e \in E : e \text{ is incident to both } x \text{ and } y\}| \\ &= \begin{cases} 1 & \text{if } x \neq y \text{ and } x \text{ is adjacent to } y; \\ 0 & \text{if } x \neq y \text{ and } x \text{ is not adjacent to } y; \\ \text{DEG}(x) & \text{if } x = y. \end{cases} \end{aligned}$$

Thus if  $G$  is regular of degree  $k$ , then

$$XX^T = A + kI_n. \tag{3.1}$$

The line graph  $L(G)$  of a graph  $G$  is constructed by taking as vertices the edges of  $G$  with two being adjacent in  $L(G)$  if they shared a common vertex. See Figure 3.1.

Observe for any pair of edges  $e$  and  $f$  that the  $[e, f]$ -entry of  $X^T X$  is

$$\begin{aligned} X^T X[e, f] &= \sum_{x \in V} X^T[e, x]X[x, f] \\ &= \sum_{x \in V} X[x, e]X[x, f] \\ &= |\{x \in V : x \text{ is incident to both } e \text{ and } f\}| \\ &= \begin{cases} 1 & \text{if } e \neq f \text{ and } e \text{ and } f \text{ share a common vertex;} \\ 0 & \text{if } e \neq f \text{ and } e \text{ and } f \text{ do not share a common vertex;} \\ 2 & \text{if } e = f. \end{cases} \end{aligned}$$

Thus if  $A_L$  is the adjacency matrix of the line graph of  $G$ , then

$$X^T X = A_L + 2I_m \tag{3.2}$$

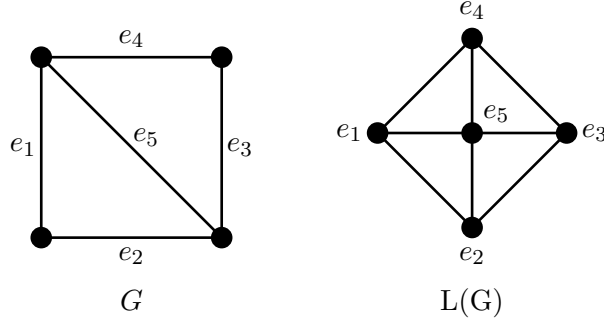


Figure 3.1: A graph  $G$  and its line graph  $L(G)$

**Theorem 3.11.** (Sachs 1967) If  $G = (V, E)$  is a regular graph of degree  $k$  with  $n = |V|$  and  $m = |E|$ , then

$$\chi_{L(G)}(\lambda) = (\lambda + 2)^{m-n} \chi_G(\lambda + 2 - k)$$

*Proof.* Let

$$U = \begin{bmatrix} \lambda I_n & -X \\ 0 & I_m \end{bmatrix} \quad \text{and} \quad V = \begin{bmatrix} I_n & X \\ X^T & \lambda I_m \end{bmatrix}.$$

Then

$$UV = \begin{bmatrix} \lambda I_n - XX^T & 0 \\ X^T & \lambda I_m \end{bmatrix} \quad \text{and} \quad VU = \begin{bmatrix} \lambda I_n & 0 \\ \lambda X^T & \lambda I_m - X^T X \end{bmatrix}.$$

The determinant of  $UV$  equals the determinant of  $VU$ . Thus

$$\lambda^m \det(\lambda I_n - XX^T) = \lambda^n \det(\lambda I_m - X^T X) \tag{3.3}$$

$$\begin{aligned} \chi_{L(G)}(\lambda) &= \det(\lambda I_m - A_L) \\ &= \det(\lambda I_m - (X^T X - 2I_m)) \text{ by Equation 3.2} \\ &= \det((\lambda + 2)I_m - X^T X) \\ &= (\lambda + 2)^{m-n} \det((\lambda + 2)I_n - XX^T) \text{ by Equation 3.3} \\ &= (\lambda + 2)^{m-n} \det((\lambda + 2)I_n - (A + kI_n)) \text{ by Equation 3.1} \\ &= (\lambda + 2)^{m-n} \det((\lambda + 2 - k)I_n - A) \\ &= (\lambda + 2)^{m-n} \chi_G(\lambda + 2 - k) \end{aligned}$$

□

### 3.3 The matrix tree theorem

Let  $G = (V, E)$  be a graph. Arbitrarily orient the edges of  $G$  by replacing the edge  $\{x, y\}$  with either  $(x, y)$  or  $(y, x)$ . We represent this graphically by adding an arrow to the edge of  $G$ . The

incidence matrix  $D$  is the  $V \times E$  matrix  $D$  given by

$$D[x, e] = \begin{cases} +1 & \text{if } e = (x, z) \text{ for some } z \in V \\ -1 & \text{if } e = (z, x) \text{ for some } z \in V \\ 0 & \text{otherwise} \end{cases}$$

An example is provided in Figure 3.2.

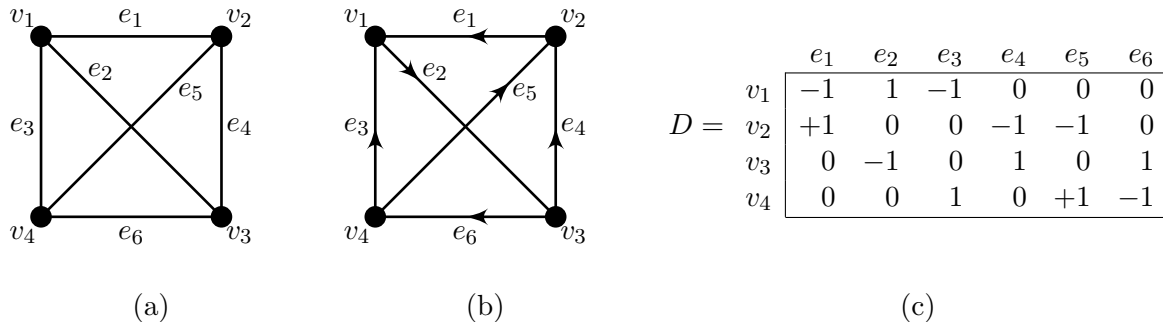


Figure 3.2: (a) The Graph  $K_4$ . (b) An arbitrary orientation of  $K_4$ . (c) The corresponding incidence matrix of  $K_4$ .

**Theorem 3.12.** *Let  $D$  be an incidence matrix of the graph  $G = (V, E)$ . Then  $\text{RANK}(D) = n - c$ , where  $n = |V|$  and  $c$  is number of connected components of  $G$ .*

*Proof.* Let  $D_i = (V_i, E_i)$  be the incidence matrix of the  $i$ -th component of  $G$ . Then

$$D = \begin{bmatrix} D_1 & 0 & \cdots & 0 \\ 0 & D_2 & \cdots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \cdots & D_c \end{bmatrix}$$

by way of a simple relabeling of the vertices. Thus

$$\text{RANK}(D) = \sum_{i=1}^c \text{RANK}(D_i)$$

and consequently we need only show that  $\text{RANK}(D_i) = |V_i| - 1$ . Hence it suffices to assume that  $G$  is connected. Denote the row of  $D$  corresponding to vertex  $x$  by  $\vec{d}_x$ , and recall that every column of  $D$  has the form

$$\begin{bmatrix} 0 \\ +1 \\ \vdots \\ -1 \\ 0 \end{bmatrix}$$

with exactly one 1 and one  $-1$ , because an edge only has 2 ends. Therefore the row sum is

$$\sum_{x \in V} \vec{d}_x = 0.$$

Thus the rows of  $D$  are linearly dependent and hence  $\text{RANK}(D) \leq n - 1$ . Now suppose that we have any dependency

$$\sum_{x \in V} \alpha_x \vec{d}_x = 0,$$

where not all  $\alpha_x = 0$ . Choose a row  $\vec{d}_x$  for which  $\alpha_x \neq 0$ . Because  $G$  is connected there is an edge  $e = \{x, y\}$  such that  $\vec{d}_x[e] = \pm 1$  and  $\vec{d}_y[e] = -\vec{d}_x[e]$ . In particular  $\vec{d}_x[e]$  and  $\vec{d}_y[e]$  are opposite in sign. But we must have

$$\alpha_x \vec{d}_x[e] + \alpha_y \vec{d}_y[e] = 0,$$

so  $\alpha_x = \alpha_y$ . But  $G$  is connected so there is a path from  $x$  to any other vertex  $z \in V$ . Consequently all the  $\alpha_z$ s are equal to some common value say  $\alpha$ . Thus

$$0 = \sum_{x \in V} \alpha \vec{d}_x = \alpha \sum_{x \in V} \vec{d}_x,$$

is the only dependency among the rows of  $D$ . Therefore we can conclude that

Therefore  $\text{RANK}(D) = |V| - 1$  for a connected graph  $D$  and for a graph  $G$  with  $c$  components  $\text{RANK}(D) = |V| - c$ .  $\square$

Let  $C = x_1 x_2 x_3 \cdots x_k x_1$  be any cycle of the graph  $G$ . Independent from any orientation of  $G$  assign to  $C$  the orientation  $\{(x_1, x_2), (x_2, x_3), (x_3, x_4), \dots, (x_{k-1}, x_k), (x_k, x_1)\}$ , and define

$$\vec{C}[e] = \begin{cases} +1 & \text{if } e \in E(C) \text{ and the orientation in } G \text{ and } C \text{ agree on } e, \\ -1 & \text{if } e \in E(C) \text{ and the orientation in } G \text{ and } C \text{ disagree on } e, \\ 0 & \text{Otherwise.} \end{cases}$$

See Figure 3.3 for an example.

Observe that if  $G = (V, E)$  has a cycle  $C$ , then  $\vec{C} \in \text{NULLSPACE}(D)$ . Hence  $\text{DIM}(\text{NULLSPACE}(D)) \geq 1$  and thus  $\text{RANK}(D) \leq \min\{|V|, |E|\} - 1$ .

**Lemma 3.13.** (*Poincare 1901*) *Any square submatrix of  $D$  has determinant either 0, +1, -1.*

*Proof.* (By induction on the number of rows.) Let  $S$  be a square submatrix of  $D$ . If  $S$  has only one row (and column), then  $S = [0]$ ,  $[-1]$  or  $[+1]$ . Hence  $\det(S)$  is either 0, +1, -1. Now suppose  $S$  has more than one row. If every column of  $S$  is either all 0s, or has both a  $+1$  and a  $-1$ . Then the row sum of  $S$  is all 0's and hence  $\det(S) = 0$ . Otherwise there is a column with exactly one nonzero entry, a  $\pm 1$ . Then

$$\det(S) = \pm 1 S',$$

where  $S'$  is the square submatrix obtained by deleting the row and column containing this nonzero entry. By induction  $\det(S')$  is either 0, +1, -1. Therefore  $\det(S)$  is either 0, +1, -1.  $\square$

**Theorem 3.14.** *Let  $G = (V, E)$  be a graph with  $n = |V|$  vertices and incidence matrix  $D$ . Suppose  $U \subset E$ ,  $|U| = n - 1$ , and let  $D_U$  be a  $(n - 1) \times (n - 1)$  submatrix of  $D$  consisting of the intersection of the  $n - 1$  columns of  $D$  and any of the  $n - 1$  rows of  $D$ . Then  $D_U$  is non-singular if and only if the  $(V, U)$  is a spanning tree of  $(V, E)$*

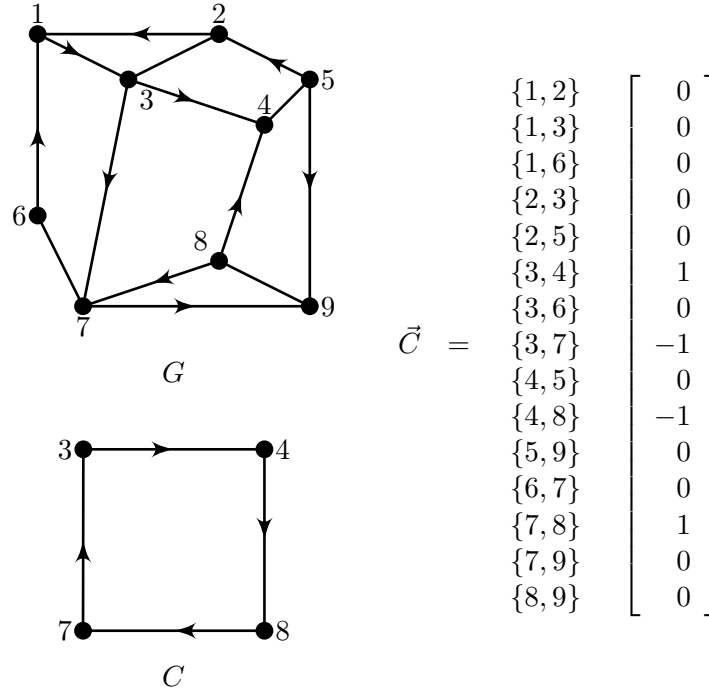


Figure 3.3: An example of  $\vec{C}$ .

*Proof.* Suppose  $(V, U)$  is a spanning tree, then  $D_U$  consists of  $n - 1$  rows of  $D$ , the incidence matrix of  $(V, U)$ .  $G$  is connected so  $\text{RANK}(D) = |V| - 1 = n - 1$ , So the  $n - 1$  rows of  $D_U$  must be linearly independent so  $\det(D_U) \neq 0$ .

Conversely suppose  $\det(D_U) \neq 0$ . Then  $D_U$  has an inverse, in other words  $D$  had a  $(n - 1) \times (n - 1)$  invertible submatrix so  $\text{RANK}(D_U) = n - 1$ . Thus  $(V, U)$  is connected by Theorem 3.12. Also, because  $D_U$  is of full rank we know that  $\text{DIM}(\text{NULLSPACE}(D_U)) = 0$  so  $(V, U)$  can not have a cycle, which means that  $(V, U)$  must be a tree.  $\square$

Consider the function

$$\kappa(G) = \text{the number of spanning trees of } G.$$

Some basic properties of  $\kappa(G)$  are:

1.  $\kappa(G) = 0$  if  $G$  is disconnected,
2.  $\kappa(C_n) = n$ , and
3.  $\kappa(G) = 1$  if and only if  $G$  is a tree.

**Lemma 3.15.** *Let  $D$  be the incidence matrix of  $G = (V, E)$  and let  $Q = DD^T$ . Then the adjoint  $\text{ADJ}(Q) = tJ$  for some  $t$ .*

*Proof.* Let  $n = |V|$ . If  $G$  is disconnected, then  $\text{RANK}(Q) = \text{RANK}(D) < n - 1$ . Hence every cofactor is 0 and thus  $\text{ADJ}(Q) = 0$ .

If  $G$  is connected then  $\text{RANK}(Q) = \text{RANK}(D) = n - 1$  and  $Q\text{ADJ}(Q) = \det(Q)I = 0$  implies each column of  $\text{ADJ}(Q)$  is in the null-space of  $Q$  which is contained in  $\text{NULLSPACE}(D^T) = \text{SPAN}_{\mathbb{C}}([1, 1, 1, \dots, 1]^T)$ . Therefore each column of  $\text{ADJ}(Q)$  is a multiple of  $[1, 1, \dots, 1]^T$  but  $Q$  is symmetric so  $\text{ADJ}(Q)$  is symmetric. Therefore  $\text{ADJ}(Q) = tJ$ .  $\square$

**Theorem 3.16.**  $\text{ADJ}(Q) = \kappa(G)J$

*Proof.* It suffices to show that one of the cofactors of  $Q$  is the number of spanning trees. Let  $D_0$  be  $D$  minus a row, then  $\det D_0 D_0^T$  is a cofactor.

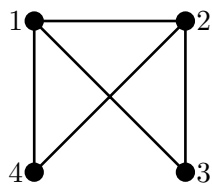
The Cauchy-Binet Theorem says that

$$\det(D_0 D_0^T) = \sum_{|U|=n-1, U \subseteq E} (D_U D_U^T),$$

where  $D_U$  is the  $(n - 1) \times |U|$  submatrix of  $D$  with edges in  $U$ .

Applying Theorem 3.14 we see that  $\det(D_U) \neq 0$  if and only if  $(V, U)$  is a spanning tree and in this case  $\det(D_U) = \pm 1$ . Hence,  $\det(D_U D_U^T) = \det(D_U) \det(D_U^T) = \det(D_U)^2 = 1$  and so from the Cauchy-Binet Theorem we have:  $\det(D_0 D_0^T) = \kappa(G)$   $\square$

**Example 3.17.**



$$D = \begin{array}{c} \begin{array}{cccccc} & 12 & 13 & 14 & 23 & 24 \\ 1 & 1 & 1 & 1 & 0 & 0 \\ 2 & -1 & 0 & 0 & 1 & 0 \\ 3 & 0 & -1 & 0 & -1 & 1 \\ 4 & 0 & 0 & -1 & 0 & -1 \end{array} \end{array} \quad D_0 D^T = \begin{bmatrix} 3 & -1 & 1 \\ -1 & 2 & -1 \\ -1 & -1 & 3 \end{bmatrix}$$

### 3.4 Notes

Two excellent text on algebraic graph theory are

1. N. Biggs, *Algebraic Graph Theory*, Cambridge University Press, (1993).
2. C. Godsil and G. Royale, *Algebraic Graph Theory*, Graduate Texts in Mathematics **207** Springer, (2001).



## Chapter 4

# Connectivity

**Theorem 4.1.** (Menger's Theorem) *Let  $G = (V, E)$  be graph and choose subsets  $A, B \subseteq V$ . The minimum number of vertices separating  $A$  and  $B$  equals the maximum number of disjoint paths from  $A$  to  $B$ .*

*Proof.* (Theorem 4.1) Let  $k$  be the number of vertices separating  $A$  and  $B$ . Clearly  $\ell$ , the number of disjoint paths from  $A$  to  $B$ , cannot be more than  $k$ , for after all deleting one vertex on each such path will separate  $A$  from  $B$ . So,  $\ell \leq k$ . We show by induction on  $|V| + |E|$  that  $\ell \geq k$ . If  $k = 0$ , then  $G$  is a disconnected graph with  $A$  and  $B$  in different components. Hence  $\ell = 0$ . If  $k = 1$ , then there is a vertex  $x$  such that  $A$  and  $B$  are in different components of  $G - x$ . Consequently every path from  $A$  to  $B$  passes through  $x$  and so there is a path from  $A$  to  $B$  through  $x$  and hence  $\ell = 1$ .

Now suppose  $G$ ,  $A$  and  $B$  are given with  $k \geq 2$ . Assume the assertion holds for graphs with fewer vertices or edges.

**Case 0:** (The trivial case.)  $A \cap B \neq \emptyset$ .

Let  $x \in A \cap B$ . Then  $x$  is one in of the paths from  $A$  to  $B$  and so  $x$  is in any set separating  $A$  from  $B$ . Thus  $G - x$  has a set of  $k - 1$  vertices separating  $A \setminus \{x\}$  from  $B \setminus \{x\}$ . Thus by induction  $G - x$  has  $k - 1$  disjoint paths from  $A \setminus \{x\}$  to  $B \setminus \{x\}$ . These paths together with the trivial path  $x$  account for  $k$  disjoint paths from  $A$  to  $B$  in  $G$ . We will therefore assume  $A \cap B = \emptyset$  for the remaining cases.

**Case 1:**  $A$  and  $B$  separated by  $X$ ,  $|X| = k$  and  $X \neq A, B$ .

Let  $C_A$  be all of the components of  $G - X$  hitting  $A$  and let  $C_B$  be all of the components of  $G - X$  hitting  $B$ . Let  $G_A = G[V(C_A) \cup X]$  and  $G_B = G[V(C_B) \cup X]$ . Note  $C_A \neq \emptyset$ , because  $|A| \geq k = |X|$ , but  $A \neq X$ . Similarly  $C_B \neq \emptyset$ . Furthermore  $G_A \cap G_B = \emptyset$ . Thus  $G_A$  and  $G_B$  contain fewer vertices and edges than  $G$  does. Therefore by induction the number of vertices separating  $A$  from  $X$  in  $G_A$  is the same as the number of disjoint paths from  $A$  to  $X$  in  $G_A$ . Every  $A$  to  $B$  path contains a path from  $A$  to  $X$  in  $G_A$  and so we cannot separate  $A$  from  $X$  by fewer than  $k$  vertices. Hence  $G_A$  contains  $k$  disjoint paths from  $A$  to  $X$ . Similarly  $G_B$  contains  $k$  disjoint paths from  $B$  to  $X$ . As  $|X| = k$  we can put these paths together to form  $k$  disjoint paths from  $A$  to  $B$ .

**Case 2:** The minimum set of vertices separating  $A$  and  $B$  is either  $A$  or  $B$ .

Let  $P$  be any path from  $A$  to  $B$ , then because  $A \cap B = \emptyset$ ,  $P$  has an edge  $ab$  with  $a \notin B$  and  $b \notin A$ . Let  $Y$  be a smallest set of vertices separating  $A$  from  $B$  in  $G - ab$ . Then  $Y_a = Y \cup \{a\}$  and  $Y_b = Y \cup \{b\}$  both separate  $A$  from  $B$  in  $G$ . Thus

$$|Y_a| = |Y_b| \geq k.$$

If equality holds, then we're done by Case 1, unless  $Y_a = A$  and  $Y_b = B$ . But then  $Y = A \cap B$ , and so  $|A \cap B| = |Y| = k - 1 \geq 1$ , and we are done by Case 0.

If equality does not hold, then

$$|Y_a| = |Y_b| > k.$$

and so  $|Y| \geq k$ . So by induction  $G - ab$  has  $k$  disjoint paths from  $A$  to  $B$  in  $G - ab$ . These are the required  $k$  disjoint paths in  $G$ .  $\square$

#### 4.0.1 Exercises

1. Let  $k \geq 2$ . Show that in a  $k$ -connected graph any  $k$  vertices lie on a common cycle.

## Part II

# A Taste of Design Theory



# Chapter 5

## Steiner Triple Systems

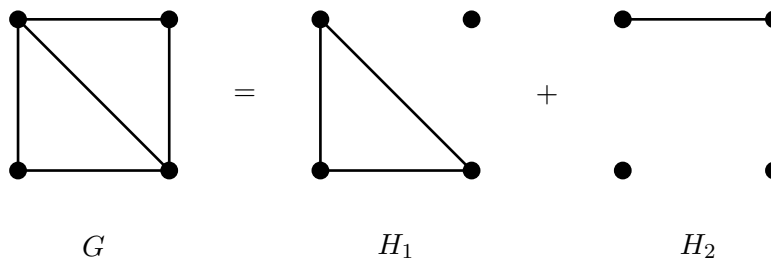
### 5.1 Graph decomposition

Given a graph  $G$  a collection of subgraphs  $\{H_1, H_2, \dots, H_\ell\}$  such that

1.  $E(G) = E(H_1) \cup E(H_2) \cup \dots \cup E(H_\ell)$ , and
2.  $E(H_i) \cap E(H_j) = \emptyset$ , for all  $i \neq j$ .

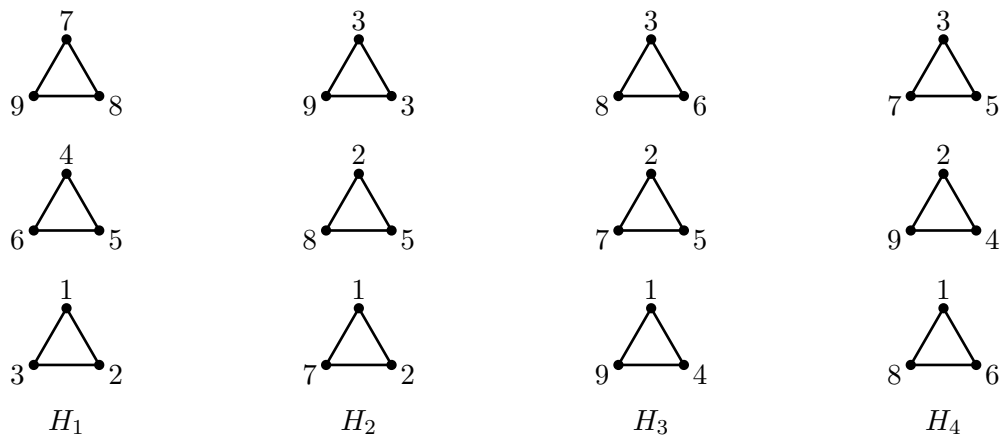
is called a *decomposition* of  $G$ .

**Example 5.1.** A decomposition of a graph  $G$  into subgraphs  $H_1$  and  $H_2$ .



A spanning  $r$ -regular subgraph  $H$  of a graph  $G$  is called an  $r$ -factor of  $G$ . A decomposition of  $G$  into  $r$ -factors is called an  $r$ -factorization.

**Example 5.2.** A 2-factorization of  $K_9$ .



**Theorem 5.3.** *The complete graph  $K_n$  has a one-factorization if and only if  $n$  is even.*

*Proof.* A one-factor is a matching and so if a graph has a one-factor, then the number of vertices must be even. Suppose  $n = 2m$  and let  $V = \mathbb{Z}_{2m-1} \cup \{\infty\}$  be a set of  $n$  vertices. Let  $F_0$  be the one factor with edges

$$\{\{0, \infty\}\} \cup \{\{x, 2m-1-x\} : x = 1, 2, \dots, m-1\}.$$

Clearly  $F_0$  has  $m$  edges and these edges are pairwise disjoint. Hence  $F_0$  is a one-factor. We develop  $F_0$  modulo  $2m-1$  to obtain the one-factorization. That is for  $j = 0, 1, 2, \dots, 2m-2$  define  $F_j$  to have the edges

$$\{\{j, \infty\}\} \cup \{\{x+j, 2m-1-x+j\} : x = 1, 2, \dots, m-1\}$$

The edge  $\{x, \infty\} \in E(F_x)$ , for each  $x = 0, 1, 2, \dots, 2m-2$ . Given an edge  $\{x, y\}$  define  $\Delta(x, y) = \pm d$ , where  $d \equiv x - y \pmod{2m-1}$ ,  $1 \leq d \leq m-1$ . There are  $m-1$  possible values for  $\Delta(x, y)$ . Namely  $\pm 1, \pm 2, \dots, \pm m-1$ . Observe that  $\Delta(x+j, 2m-1-x+j) = \pm 2x$  and  $\{\pm 2x : 1 \leq x \leq m-1\} = \{\pm x : 1 \leq x \leq m-1\}$ . Thus  $F_j$  contains exactly one edge for each possible value of  $\Delta$ . Therefore all edges have been accounted for because the set of edges with  $\Delta = \pm d$  is

$$\{\{x+j, y+j\} : j = 0, 1, 2, \dots, 2m-2\},$$

where  $\{x, y\}$  is any edge with  $\Delta(x, y) = \pm d$ . □

A  $k$ -matching in a graph  $G$  is a set of  $k$  independent edges, that is,  $k$  edges that have no common vertices.

**Lemma 5.4.** *Let  $G$  be a regular graph of order  $n$  and degree 1 or 2. If  $k$  is a proper divisor of  $|E(G)|$ , then  $G$  can be decomposed into  $k$ -matchings except when  $n = 2k$  and at least one component of  $G$  has odd order.*

*Proof.* If  $G$  is regular of degree 1, then  $G$  itself is an  $\frac{n}{2}$ -matching. If  $k$  is a proper divisor of  $|E(G)|$ , then  $k \mid n/2$ . We simply partition the  $\frac{n}{2}$ -matching into  $k$ -matchings.

We move to the degree 2 case. Let

$$C_1, C_2, \dots, C_z$$

be the  $z$  cycles comprising the components of  $G$ . Let the respective orders be  $\ell_1, \ell_2, \dots, \ell_z$ . We know that

$$\sum_{i=1}^z \ell_i = n$$

and that  $k$  is a proper divisor of  $n$ . Thus, we want to find  $d = n/k$   $k$ -matchings that partition  $E(G)$ . We do this by finding a proper edge coloring of  $G$  with  $d$  colors so that each color class contains  $k$  edges.

We dispose of the  $d = 2$  case first. If all the cycles have even length, then each may be properly colored by 2 colors and we are done. If some cycles has odd length, then it is impossible to properly 2-color the edges of the cycle, and this gives rise to the exception in the statement of the lemma.

We assume  $d \geq 3$  for the remainder of the proof. Start with  $C_1$ . Color an arbitrary edge color 1. Next color an edge on  $C_1$  adjacent to the first colored edge color 2. Continue around  $C_1$  coloring successive edges 3, 4 and so on until either all edges are colored or an edge is colored  $d$  and not all edges of  $C_1$  are yet colored. In the latter case, color the next edge 1 and continue as before.

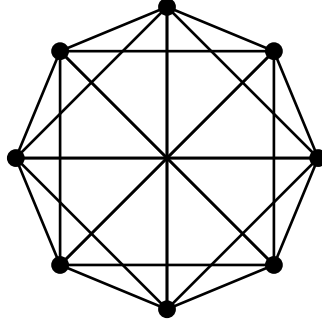


Figure 5.1: The circulant graph  $\text{CIRC}(8; \{1, 2, 4, 6, 7\})$ .

The preceding process either properly colors the edges of  $C_1$  or  $\ell_1 \equiv 1 \pmod{d}$  and the next to last edge has been colored  $d$ . The process then says to color the next edge color 1, but this edge is adjacent to the first colored edge and cannot be colored 1 in a proper edge coloring. So instead of coloring the last colored edge with color  $d$ , give it the color 1 and then color the last edge with color  $d$ . We have properly edge colored  $C_1$ .

Note that the edge coloring of  $C_1$  uses colors  $1, 2, \dots, r$   $i$  times and colors  $r + 1, r + 2, \dots, d$   $i - 1$  times, where  $r \equiv \ell_1 \pmod{d}$ ,  $0 \leq r < d$ . We then move to cycle  $C_2$  and repeat the process used on  $C_1$  starting with color  $r + 1$ . We then continue in this way through all the cycles and clearly obtain a proper edge coloring with  $d$  colors, where each color is used  $k$  times. This completes the proof.  $\square$

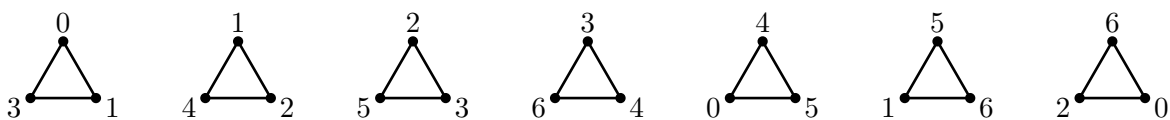
The *circulant graph*  $G = \text{CIRC}(n; S)$  is the graph with vertex set  $\{u_0, u_1, \dots, u_{n-1}\}$ , and an edge joining vertices  $u_i$  and  $u_j$  if and only if  $j - i \in S$ , where  $S \subseteq \mathbb{Z} \setminus \{0\}$  and  $s \in S$  if and only if  $-s \in S$ . We denote an edge joining  $u_i$  and  $u_j$  by  $u_i u_j$ . The set  $S$  is called the *connection set* of  $\text{CIRC}(n; S)$ . For example,  $\text{CIRC}(8; \{1, 2, 4, 6, 7\})$  is given in Figure 5.1. The edge joining  $u_i$  and  $u_j$  is said to have *length* equal to the residue in the range  $1, 2, \dots, \lfloor n/2 \rfloor$  that is congruent to  $j - i$  or  $i - j$  modulo  $n$ .

**Theorem 5.5.** *If  $G = \text{CIRC}(n; S)$  is connected,  $k$  is a proper divisor of  $n$ , and  $k$  divides  $|E(G)|$ , then there is a decomposition of  $G$  into  $k$ -matchings.*

*Proof.* Write  $G$  as the union of circulant subgraphs  $\text{CIRC}(n; \{\pm s\})$ ,  $s \in S$  and use Lemma 5.4 to independently decompose each into  $k$ -matchings. Note that when  $s = n/2$ , if  $k$  divides  $n$  and  $|E(G)|$ , then  $k$  also divides  $n/2$  when  $n/2 \in S$ .  $\square$

An  $F$ -factorization of a graph  $G$  is a decomposition of  $G$  into subgraphs  $\{H_1, H_2, \dots, H_\ell\}$  in which  $H_i \approx F$  for each  $i = 1, 2, \dots, \ell$ .

**Example 5.6.** *A  $K_3$ -factorization of  $K_7$*



A  $K_3$ -factorization of  $K_n$  is also called a *Steiner triple system* of order  $n$ . It is generally more convenient to describe a Steiner triple system as a collection of 3-element subsets. A *Steiner triple system* of order  $v$  is a pair  $(V, T)$  where

1.  $V$  is a  $v$ -element set of *points*,
2.  $T$  is a collection of 3-element subsets called *triples*, and
3. every pair of points is in exactly one triple.

We use  $\text{STS}(n)$  to denote a Steiner triple system of order  $n$ .

An  $\text{STS}(3)$  on  $\{1, 2, 3\}$  consists of only one triple, namely  $\{1, 2, 3\}$ . A more interesting example is given Example 5.7.

**Example 5.7.** *A Steiner triple system of order 7.*

$$\begin{aligned} V &= \{0, 1, 2, 3, 4, 5, 6\} \\ T &= \{\{0, 1, 3\}, \{1, 2, 4\}, \{2, 3, 5\}, \{3, 4, 6\}, \{0, 4, 5\}, \{1, 5, 6\}, \{0, 2, 6\}\} \end{aligned}$$

Observe that the  $\text{STS}(7)$  in Example 5.7 is exactly the same as the  $K_3$ -factorization of  $K_7$  given in Example 5.6.

**Lemma 5.8.** *If a Steiner triple system of order  $v$  exists, then  $v \equiv 1, 3 \pmod{6}$ .*

*Proof.* There are  $\binom{v}{2}$  pairs and each triple contains three of them. Thus the number of triples in an  $\text{STS}(v)$  is

$$\frac{1}{3} \binom{v}{2}.$$

Hence

$$\frac{v(v-1)}{3 \cdot 2} \text{ is an integer.} \tag{5.1}$$

Also, any triple containing a fixed point  $x$  contains two other points. Therefore the number of triples containing a fixed point  $x$  is  $(v-1)/2$  and so

$$\frac{(v-1)}{2} \text{ is an integer.} \tag{5.2}$$

Putting Equations 5.1 and 5.2 we see that  $v \equiv 1, 3 \pmod{6}$ . □

**Theorem 5.9.** (The doubling construction) *If a  $\text{STS}(v)$  exists, then so does an  $\text{STS}(2v+1)$ .*

*Proof.* If an  $\text{STS}(v)$  exists, then  $v \equiv 1, 3 \pmod{6}$  and so  $v$  is odd. Thus there is a one-factorization  $\{F_1, \dots, F_v\}$  on  $\{0, 1, \dots, v\}$ . Let  $x_1, \dots, x_v$  be  $v$  new points and let

$$V = \{0, 1, \dots, v, x_1, \dots, x_v\}$$

be the  $2v+1$  points of our  $\text{STS}(2v+1)$ . The triples are of two types.

**Type 1.** The  $\frac{1}{3} \binom{v}{2}$  triples in an  $\text{STS}(v)$  on  $x_1, \dots, x_v$ .



**Type 2.** The  $\frac{v(v+1)}{2}$  triples defined by

$$\{x_j \cup e : e \in F_j, j = 1, 2, \dots, v\}.$$

This accounts for

$$\frac{1}{3} \binom{v}{2} + \frac{v(v+1)}{2} = \frac{(2v+1)(2v)}{6}$$

triples. The right number. Consider any pair  $\{a, b\}$ . If  $a, b \in \{0, 1, \dots, v\}$ , then  $ab$  is an edge in some one-factor  $F_j$ , and  $\{a, b, x_j\}$  is the triple in  $T$  that contains  $\{a, b\}$ , a type 2 triple. If  $a, b \in \{x_1, \dots, x_v\}$ , then  $a, b$  is contained in exactly one of the type 1 triples. If  $a \in \{0, 1, \dots, v\}$ , and  $b = x_j \in \{x_1, \dots, x_v\}$ , then there is a unique edge  $ac$  in  $F_j$ , that contains  $a$ . Hence  $a, b$  is contained in the type 2 triple  $\{a, b, c\}$ . Therefore every pair is in some triple and there are exactly the right number of triples. Therefore it follows that every pair is in exactly one triple and consequently these triples form a STS( $2v+1$ ).  $\square$

**Theorem 5.10.** (vector space construction) *A Steiner Triple System of order  $2^n - 1$  exists for all  $n \geq 2$ .*

*Proof.* Take as points  $V = \mathbb{Z}_2^n \setminus \vec{0}$  and as triples

$$T = \{\{\vec{a}, \vec{b}, \vec{c}\} : \vec{a} + \vec{b} + \vec{c} = \vec{0}\}$$

Observe that for any pair  $\vec{a}, \vec{b}$ , there is a unique  $\vec{c}$  such that  $\vec{a} + \vec{b} + \vec{c} = \vec{0}$ . Namely,  $\vec{c} = \vec{a} + \vec{b}$ . Furthermore,  $\vec{c} \neq \vec{a}$ , for if so then  $\vec{a} + \vec{b} = \vec{a}$  and thus  $\vec{b} = \vec{0}$  a contradiction. Similarly  $\vec{c} \neq \vec{b}$ . Consequently  $(V, T)$  is an STS( $2^n - 1$ ).  $\square$

**Theorem 5.11.** (multiply construction) *If there is exists an STS( $v$ ) and an STS( $w$ ), then there exists an STS( $vw$ ).*

*Proof.* Let  $(V, T)$  be an STS( $v$ ) and let  $(W, U)$  be an STS( $w$ ). We construct an STS( $vw$ ) on  $V \times W$  by taking the following three types of triples:

**Type 1.**  $\{(a, x), (b, x), (c, x)\}$  for each  $\{a, b, c\} \in T$ , and  $x \in W$ ,

**Type 2.**  $\{(a, x), (a, y), (a, z)\}$  for each  $\{x, y, z\} \in U$ , and  $a \in V$ ,

**Type 3.** The six triples  $\{(a, x), (b, y), (c, z)\}$ ,  $\{(a, y), (b, x), (c, z)\}$ ,  $\{(a, x), (b, z), (c, y)\}$ ,  $\{(a, z), (b, x), (c, y)\}$ ,  $\{(a, y), (b, z), (c, x)\}$  and  $\{(a, z), (b, y), (c, x)\}$  for each  $\{a, b, c\} \in T$  and  $\{x, y, z\} \in U$ .

There is accounts for

$$\frac{v(v-1)w}{6} + \frac{w(w-1)v}{6} + \frac{6v(v-1)w(v-1)}{36} = \frac{vw(vw-1)}{6}$$

triples. The right number. Consider any pair of points  $(a, x), (b, y)$ . If  $x = y$ , then  $(a, x), (b, y)$  is in the Type 1 triple  $\{(a, x), (b, x), (c, x)\}$ , where  $\{a, b, c\}$  is the unique triple in  $T$  that contains  $a, b$ . If  $a = b$ , then  $(a, x), (b, y)$  is in the Type 2 triple  $\{(a, x), (a, y), (a, z)\}$ , where  $\{x, y, z\}$  is the unique triple in  $U$  that contains  $x, y$ . Otherwise,  $(a, x), (b, y)$  is in the Type 3 triple  $\{(a, x), (b, y), (c, z)\}$ , where  $\{a, b, c\}$  is the unique triple in  $T$  that contains  $a, b$  and  $\{x, y, z\}$  is the unique triple in  $U$  that contains  $x, y$ .  $\square$

Applying, these constructions to the STS(3) and STS(7) we constructed earlier we can obtain for example STS( $v$ ) for  $v \in \{3, 7, 9, 15, 19, 21, 27, 31\}$  however we cannot so far construct STS( $v$ ) for  $v \in \{13, 25, 33, 37\}$  among others. In the next two sections we will see that we can construct STS( $v$ ) for all  $v \equiv 1, 3 \pmod{6}$ .

## 5.2 The Bose construction $v \equiv 3 \pmod{6}$

A *Latin square* of order  $n$  is an  $n$  by  $n$  array  $L$  with entries from an  $n$ -element set such that each row and column contain each symbol exactly once. A Latin square  $L$  is *commutative* if  $L[i, j] = L[j, i]$  for all  $i, j$ . The multiplication table of an Abelian group is a commutative Latin square. A Latin square is *idempotent* if  $L[i, i] = i$  for all  $i$ .

**Example 5.12.** *Some Latin squares.*

1	2	3
2	3	1
3	1	2

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

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

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

**Theorem 5.13.** *An idempotent commutative Latin square of order  $2n + 1$  exists for every  $n \geq 0$ .*

*Proof.* The group  $(\mathbb{Z}_{2n+1}, +)$  is a commutative group. Thus its addition table is a commutative Latin square. The entries on the diagonal are  $\{2x : x = 0, 1, 2, 3, \dots, 2n-1\}$  multiplying each entry of the square by  $(n+1)$  the inverse of 2 modulo  $2n+1$ . creates a square that is idempotent and commutative.  $\square$

**Theorem 5.14.** (Bose's construction) *A STS( $v$ ) exists whenever  $v \equiv 3 \pmod{6}$ .*

*Proof.* Let  $v = 3 + 6n$ , set  $Q = \{1, 2, \dots, 2n+1\}$  and let  $L$  be an idempotent commutative Latin square on  $Q$ . We construct an STS( $v$ ) on  $Q \times \mathbb{Z}_3$  by taking the following two types of triples. See Figure 5.2.

**Type 1.**  $\{(x, 0), (x, 1), (x, 2)\}$  for each  $x \in Q$

**Type 2.**  $\{(x, 0), (y, 0), (L[x, y], 1)\}$ ,  $\{(x, 1), (y, 1), (L[x, y], 2)\}$  and  $\{(x, 2), (y, 2), (L[x, y], 0)\}$  for each  $x, y \in Q, x \neq y$ .

The Type 2 triples are well defined, because  $L[x, y] = L[y, x]$  and  $L[x, x] = x$ . There are

$$2n + 1 + 3 \binom{2n + 1}{2} = \frac{(3 + 6n)(2 + 6n)}{6} = \frac{v(v - 1)}{6}$$

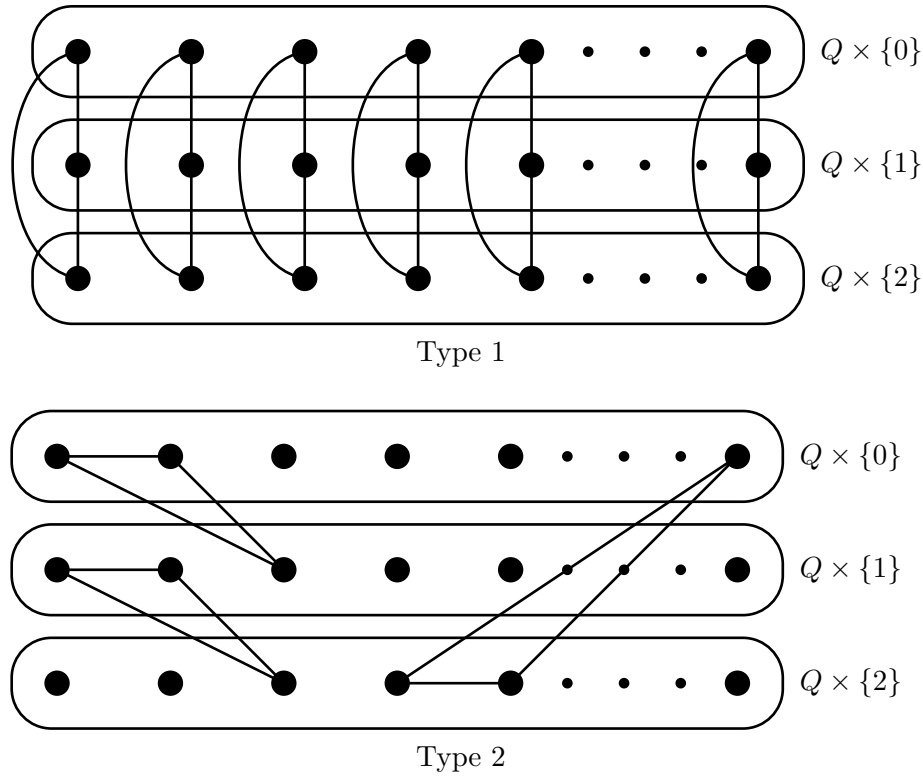


Figure 5.2: The Bose construction

triples. The right number for an STS( $v$ ). Consider any pair of different points  $(p, i), (q, j) \in Q \times \{0, 1, 2\}$ . If  $p = q$ , then they are in the Type 1 triple  $\{(p, 0), (p, 1), (p, 2)\}$ . If  $i = j$ , then the pair of points are in the Type 2 triple  $\{(p, i), (q, i), (L[p, q], i + 1)\}$ . If  $p \neq q$  and  $i \neq j$ , then without loss  $j = i + 1$  and  $(q, i), (p, j)$  are in the Type 2 triple  $\{(p, i), (q, j), (r, k)\}$ , where  $k = -i - j \pmod{3}$  and  $r$  is defined by  $L[p, r] = q$ .  $\square$

### 5.2.1 Exercises

1. Explicitly Construct a Steiner Triple System of order 15, using the vector space construction, the doubling construction and the Bose construction. For a bonus determine if these three STS(15)s are nonisomorphic.

Two Steiner triple systems  $(V, T)$  and  $(W, U)$  of order  $v$  are isomorphic if there is a one to one mapping  $f : V \rightarrow W$  such that

$$\{a, b, c\} \in T \text{ if and only if } \{f(a), f(b), f(c)\} \in U$$

## 5.3 The Skolem construction $v \equiv 1 \pmod{6}$

A Latin square  $L$  of order  $2n$  is said to be *half-idempotent* if cells  $L[i, i]$  and  $L[n + i, n + i]$  both contain  $i$  for  $i = 1, 2, \dots, n$ .

**Example 5.15.** *Examples of commutative half-idempotent Latin Squares.*

1	2
2	1

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

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

**Theorem 5.16.** *There is a half-idempotent commutative Latin square of order  $2n$  for all  $n$ .*

*Proof.* The addition table of  $(\mathbb{Z}_{2n}, +)$  is a commutative Latin square with diagonal entries:

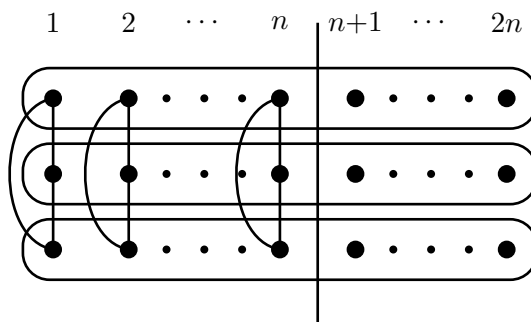
$$\begin{aligned}
 & [0 + 0, 1 + 1, 2 + 2, \dots, (n - 1) + (n - 1), n + n, (n + 1) + (n + 1), \dots, (2n - 1) + (2n - 1)] \\
 = & [0, 2, 4, 6, \dots, 2n - 2, 0, 2, 4, \dots, 2n - 2]
 \end{aligned}$$

So we can relabel the entries in this table to make a half-idempotent commutative Latin Square.  $\square$

**Theorem 5.17.** (The Skolem Construction) *There exists a Steiner triple system of every order  $v \equiv 1 \pmod{6}$ .*

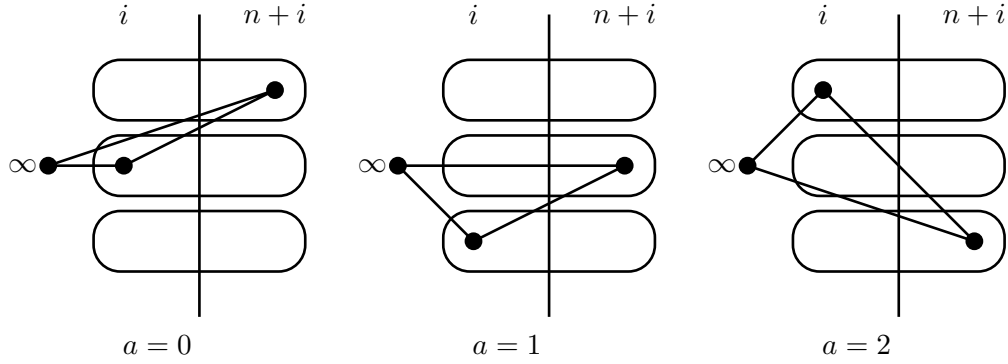
*Proof.* Let  $v = 1 + 6n$ ,  $n \geq 1$ , let  $L$  be a half-idempotent Latin square on  $Q = \{1, 2, \dots, 2n\}$  and let  $V = \{\infty\} \cup Q \times \mathbb{Z}_3$ . Take the following 3 types of triples.

**Type 1:**  $\{(i, 0), (i, 1), (i, 2)\}$ ,  $i = 1, 2, \dots, n$ .



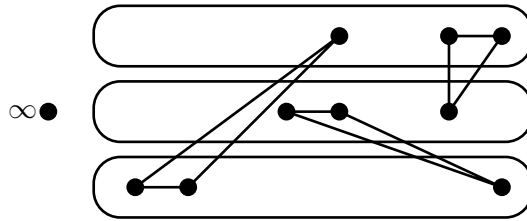
There are  $n$  Type 1 triples.

**Type 2:**  $\{\infty, (n + i, a), (i, a + 1)\}$ ,  $i = 1, 2, \dots, n$ ,  $a \in \mathbb{Z}_3$ .



There are  $3n$  Type 2 triples.

**Type 3:**  $\{(i, a), (j, a), (L[i, j], a + 1)\}, \{i, j\} \subset Q, a \in \mathbb{Z}_3$



There are  $3\binom{2n}{2}$  Type 3 triples.

The total number of triples chosen is

$$\begin{aligned}
 n + 3n + 3\binom{2n}{2} &= 4n + 3 \cdot \frac{2n(2n-1)}{2} \\
 &= 4n + 3n(2n-1) \\
 &= 6n^2 + n \\
 &= \frac{(6n+1)(6n)}{6} \\
 &= \frac{v(v-1)}{6}.
 \end{aligned}$$

It is easy to see that every pair is in exactly one of the chosen triples. Thus the  $\frac{v(v-1)}{6}$  chosen triples form a Steiner triple system of order  $v = 1 + 6n$ .  $\square$

**Example 5.18.** A Steiner triple system of order 13. Here  $n = 2$  and  $v = 1 + 6n = 13$ .

$$L = \begin{array}{|c|c|c|c|} \hline 1 & 3 & 2 & 4 \\ \hline 3 & 2 & 4 & 1 \\ \hline 2 & 4 & 1 & 3 \\ \hline 4 & 1 & 3 & 2 \\ \hline \end{array}$$

**Type 1 triples:**

$$\begin{aligned}
 &\{(1, 0), (1, 1), (1, 2)\} \\
 &\{(2, 0), (2, 1), (2, 2)\}
 \end{aligned}$$

**Type 2 triples:**

$$\begin{aligned} & \{\infty, (3, 0), (1, 1)\} \\ & \{\infty, (4, 0), (2, 1)\} \\ & \{\infty, (3, 1), (1, 2)\} \\ & \{\infty, (3, 1), (2, 2)\} \\ & \{\infty, (4, 2), (1, 0)\} \\ & \{\infty, (4, 2), (2, 0)\} \end{aligned}$$

**Type 3 triples:**

$$\begin{aligned} & \{(1, 0), (2, 0), (3, 1)\} \\ & \{(1, 0), (3, 0), (2, 1)\} \\ & \{(1, 0), (4, 0), (4, 1)\} \\ & \{(2, 0), (3, 0), (4, 1)\} \\ & \{(2, 0), (4, 0), (1, 1)\} \\ & \{(3, 0), (4, 0), (3, 1)\} \\ & \{(1, 1), (2, 1), (3, 2)\} \\ & \{(1, 1), (3, 1), (2, 2)\} \\ & \{(1, 1), (4, 1), (4, 2)\} \\ & \{(2, 1), (3, 1), (4, 2)\} \\ & \{(2, 1), (4, 1), (1, 2)\} \\ & \{(3, 1), (4, 1), (3, 2)\} \\ & \{(1, 2), (2, 2), (3, 0)\} \\ & \{(1, 2), (3, 2), (2, 0)\} \\ & \{(1, 2), (4, 2), (4, 0)\} \\ & \{(2, 2), (3, 2), (4, 0)\} \\ & \{(2, 2), (4, 2), (1, 0)\} \\ & \{(3, 2), (4, 2), (3, 0)\} \end{aligned}$$

1. R. Stong, On 1-factorizability of Cayley graphs, *J. Combin. Theory Ser. B* **39** (1985), 298–307.

## Chapter 6

# Magic Squares

Chapter 1 of H.J. Ryser's book on combinatorial Mathematics begins with:

Combinatorial mathematics also referred to as combinatorial analysis or combinatorics, is a mathematical discipline that began in ancient times. According to legend the Chinese Emperor Yu (c. 2200 B.C.) observed the magic square on the shell of a divine turtle. ...

After years of careful research I have discovered a picture of that famous turtle.



A *magic square* is an  $n$  by  $n$  array of integers with the property that the sum of the numbers in each row, each column and the the main and back diagonals is the same. This sum is the *magic sum*.

A magic square is *n-th order* if the integers  $1, 2, 3, \dots, n^2$  are used

16	3	2	13
5	10	11	8
9	6	7	12
4	15	14	1

$$n = 4 \quad \text{magic sum} = 34$$

The magic sum of an  $n$ -th order magic square is easily determined because we must have the same sum in each of the  $n$  rows. Thus the magic sum is

$$\frac{1}{n} (1 + 2 + \cdots + n^2) = \frac{n^3 + n}{2}.$$

The Statesman Benjamin Franklin writes in his autobiography:

When I disengaged myself, as above mentioned, from private business, I flatter'd myself that, by the sufficient tho' moderate fortune I had acquir'd, I had secured leisure during the rest of my life for philosophical studies and amusements. I purchased all Dr. Spence's apparatus, who had come from England to lecture here, and I proceeded in my electrical experiments with great alacrity; but the publick, now considering me as a man of leisure, laid hold of me for their purposes, every part of our civil government, and almost at the same time, imposing some duty upon me. The governor put me into the commission of the peace; the corporation of the city chose me of the common council, and soon after an alderman; and the citizens at large chose me a burgess to represent them in Assembly. This latter station was the more agreeable to me, as I was at length tired with sitting there to hear debates, in which, as clerk, I could take no part, and which were often so unentertaining that I was induc'd to amuse myself with making **magic squares** or circles, or any thing to avoid weariness; and I conceiv'd my becoming a member would enlarge my power of doing good. I would not, however, insinuate that my ambition was not flatter'd by all these promotions; it certainly was; for, considering my low beginning, they were great things to me; and they were still more pleasing, as being so many spontaneous testimonies of the public good opinion, and by me entirely unsolicited.

Example 6.1 contains an Magic Square of order 8.

**Example 6.1.** *The Franklin Square of order 8.*

52	61	4	13	20	29	36	45
14	3	62	51	46	35	30	19
53	60	5	12	21	28	37	44
11	6	59	54	43	38	27	22
55	58	7	10	23	26	39	42
9	8	57	56	41	40	25	24
50	63	2	15	18	31	34	47
16	1	64	49	48	33	32	17

In this chapter we will determine the values of  $n$  for which a  $n$ -th order magic square exist. Let  $\mathcal{M}$  be the set of all positive integers  $n$  such that an  $n$ -th order magic square exists. So far we know  $3, 4, 8 \in \mathcal{M}$  and it is easy to see that  $2 \notin \mathcal{M}$ .



## 6.1 De La Loubère's construction

In 1693 De La Loubère constructed a magic square of order  $n$  whenever  $n$  is odd. His construction is as follows.

First we place 1 in the middle cell of the first row. The numbers are placed consecutively  $1, 2, 3, \dots, n^2$  in diagonal lines which slope upwards to the right except

1. when the top row is reached the next number is written in the bottom row as if it were the next row after the top;
2. when the right column is reached, the next number is written in the first column as if it followed the right-hand column; and
3. if a cell is reached that is already filled or if the upper right corner is reached then the next cell to be used is the one directly below it.

**Example**

$$\begin{array}{ccccc} 17 & 24 & 1 & 8 & 15 \\ 23 & 5 & 7 & 14 & 16 \\ 4 & 6 & 13 & 20 & 22 \\ 10 & 12 & 19 & 21 & 3 \\ 11 & 18 & 25 & 2 & 9 \end{array}$$

This construction shows that  $2m + 1 \in \mathcal{M}$  for all  $m$ .

The proof that In 1693 De La Loubère construction works is complicated. We offer in the next section another construction for Magic Squares of odd order. This construction uses orthogonal Latin squares.

## 6.2 The orthogonal Latin square construction

Two Latin squares  $A$  and  $B$  of order  $n$  on  $\{0, 1, 2, \dots, n-1\}$  are said to be *orthogonal Latin squares* if the  $n^2$  ordered pairs

$$(A[x, y], B[x, y])$$

$x = 0, 1, 2, 3, \dots, n-1, y = 0, 1, 2, \dots, n-1$  are all distinct.

An  $n$  by  $n$  array is said to be *row magic* if the sum of the entries in any row are the same. We similarly define *column magic*.

If  $A$  and  $B$  are orthogonal Latin squares on  $\{0, 1, 2, \dots, n-1\}$ , then

$$M = J + A + nB,$$

where  $J$  is the matrix of all 1s is row and column magic, because the sum of the entries in any row or column of  $M$  is

$$\begin{aligned} & \underbrace{1 + 1 + \dots + 1}_n + (0 + 1 + 2 + \dots + (n-1)) + n(0 + 1 + 2 + \dots + (n-1)) \\ & = n + \frac{n(n-1)}{2} + n \frac{n(n-1)}{2} \\ & = \frac{n^3 + n}{2}. \end{aligned}$$

**Example 6.2.** *An example of almost constructing a magic square from 2 orthogonal Latin squares.*

$$\begin{bmatrix} 1 & 7 & 13 & 19 & 25 \\ 12 & 18 & 24 & 5 & 6 \\ 23 & 4 & 10 & 11 & 17 \\ 9 & 15 & 16 & 22 & 3 \\ 20 & 21 & 2 & 8 & 14 \end{bmatrix} = \begin{bmatrix} 1 & 1 & 1 & 1 & 1 \\ 1 & 1 & 1 & 1 & 1 \\ 1 & 1 & 1 & 1 & 1 \\ 1 & 1 & 1 & 1 & 1 \\ 1 & 1 & 1 & 1 & 1 \end{bmatrix} + \begin{bmatrix} 0 & 1 & 2 & 3 & 4 \\ 1 & 2 & 3 & 4 & 0 \\ 2 & 3 & 4 & 0 & 1 \\ 3 & 4 & 0 & 1 & 2 \\ 4 & 0 & 1 & 2 & 3 \end{bmatrix} + 5 \begin{bmatrix} 0 & 1 & 2 & 3 & 4 \\ 2 & 3 & 4 & 0 & 1 \\ 4 & 0 & 1 & 2 & 3 \\ 1 & 2 & 3 & 4 & 0 \\ 3 & 4 & 0 & 1 & 2 \end{bmatrix}$$

Unfortunately the front and back diagonals of

$$M = J + A + nB$$

do not necessarily have the magic sum as the above example shows.

Fortunately we can carefully choose the squares  $A$  and  $B$  so that the front and back diagonals have the magic sum. For example consider the squares  $A$  and  $B$  on  $\mathbb{Z}_n$ ,  $n$  odd, defined by

$$\begin{aligned} A[x, y] &= (y - x) + \frac{n-1}{2} \pmod{n} \\ B[x, y] &= 2^{-1}(x + y) \pmod{n} \end{aligned}$$

(Note,  $2^{-1}$  exists, because  $n$  is odd.) First observe that if

$$(A[x_1, y_1], B[x_1, y_1]) = (A[x_2, y_2], B[x_2, y_2]),$$

then

$$y_1 - x_1 + \frac{n-1}{2} \equiv y_2 - x_2 + \frac{n-1}{2} \pmod{n}$$

and

$$2^{-1}(x_1 + y_1) \equiv 2^{-1}(x_2 + y_2) \pmod{n}.$$

Thus,

$$y_1 - x_1 \equiv y_2 - x_2 \pmod{n}$$

and

$$x_1 + y_1 \equiv x_2 + y_2 \pmod{n}.$$

Consequently  $x_1 = x_2$  and  $y_1 = y_2$ , and so  $A$  and  $B$  are orthogonal. Therefore  $M = J + A + nB$  is row and column magic. The forward diagonal of  $A$  is

$$\left[ \frac{n-1}{2}, \frac{n-1}{2}, \dots, \frac{n-1}{2} \right]$$

Thus forward diagonal sum of  $M$  is

$$n + n \frac{n-1}{2} + n(0 + 1 + 2 + \dots + n-1) = \frac{n^3 + n}{2}.$$

The magic sum. The back diagonal of  $B$  is

$$\left[ \frac{n-1}{2}, \frac{n-1}{2}, \dots, \frac{n-1}{2} \right]$$

Thus back diagonal sum of  $M$  is

$$n + (0 + 1 + 2 + \dots + n - 1) + n \frac{n-1}{2} = \frac{n^3 + n}{2}.$$

Again the magic sum. Thus we have shown that there is a magic square for all odd orders  $n$ .

**Example 6.3.** A magic square of order 5 constructed from two orthogonal Latin squares.

$$\begin{bmatrix} 3 & 19 & 10 & 21 & 12 \\ 17 & 8 & 24 & 15 & 1 \\ 6 & 22 & 13 & 4 & 20 \\ 25 & 11 & 2 & 18 & 9 \\ 14 & 5 & 16 & 7 & 23 \end{bmatrix} = \begin{bmatrix} 1 & 1 & 1 & 1 & 1 \\ 1 & 1 & 1 & 1 & 1 \\ 1 & 1 & 1 & 1 & 1 \\ 1 & 1 & 1 & 1 & 1 \\ 1 & 1 & 1 & 1 & 1 \end{bmatrix} + \begin{bmatrix} 2 & 3 & 4 & 0 & 1 \\ 1 & 2 & 3 & 4 & 0 \\ 0 & 1 & 2 & 3 & 4 \\ 4 & 0 & 1 & 2 & 3 \\ 3 & 4 & 0 & 1 & 2 \end{bmatrix} + 5 \begin{bmatrix} 0 & 3 & 1 & 4 & 2 \\ 3 & 1 & 4 & 2 & 0 \\ 1 & 4 & 2 & 0 & 3 \\ 4 & 2 & 0 & 3 & 1 \\ 2 & 0 & 3 & 1 & 4 \end{bmatrix}$$

### 6.3 Strachey's construction

Strachey in 1918, showed how to construct a magic square  $M$  of order  $2(2m + 1)$  from a magic square  $A$  of order  $2m + 1$ . His construction is as follows.

**Step 1.** From  $A$  construct this non-magic square of order  $2u$ :

$$S_1 = \begin{array}{|c|c|} \hline A & A + 2u^2 \\ \hline A + 3u^2 & A + u^2 \\ \hline \end{array} \tag{6.1}$$

**Step 2.** Interchange the indicated cells:

$$S_2 = \begin{array}{|c|c|c|} \hline \overbrace{\text{[Dark Gray Block]}^m} & & \overbrace{\text{[Dark Gray Block]}^{m-1}} \\ \hline \text{Swap} & & \text{Swap} \\ \hline \text{[Dark Gray Block]} & & \text{[Dark Gray Block]} \\ \hline \end{array} \tag{6.2}$$

The result is a magic square of order  $2(2m + 1)$ , So  $2(2m + 1) = 4m + 2 \in \mathcal{M}$  for all  $m$ .

**Example 6.4.** A magic square of order 10, magic sum=505.  $m = 2$ ,  $u = 5$ .

Step 1.

17	24	1	8	15	67	74	51	58	65
23	5	7	14	16	73	55	57	64	66
4	6	13	20	22	54	56	63	70	72
10	12	19	21	3	60	62	69	71	53
11	18	25	2	9	61	68	75	52	59
92	99	76	83	90	42	49	26	33	40
98	80	82	89	91	48	30	32	39	41
79	81	88	95	97	29	31	38	45	47
85	87	94	96	78	35	37	44	46	28
86	93	100	77	84	36	43	50	27	34

Step 2.

92	99	1	8	15	67	74	51	58	40
98	80	7	14	16	73	55	57	64	41
4	81	88	20	22	54	56	63	70	47
85	87	19	21	3	60	62	69	71	28
86	93	25	2	9	61	68	75	52	34
17	24	76	83	90	42	49	26	33	65
23	5	82	89	91	48	30	32	39	66
79	6	13	95	97	29	31	38	45	72
10	12	94	96	78	35	37	44	46	53
11	18	100	77	84	36	43	50	27	59

**Theorem 6.5.** *If there is a magic square of odd order  $u = 2m + 1$ , then there is a magic square of order  $2u$ .*

*Proof.* Let  $A$  be a magic square of order  $u = 2m + 1$  and apply Strachy's construction obtaining the  $2u$  by  $2u$  square  $S_2$  in Equation 6.2. The magic sum of  $A$  is  $\frac{u^3 + u}{2}$ . We will show that  $S_2$  has magic sum  $\frac{(2u)^3 + 2u}{2} = 4u^3 + u$ .

The change from the matrix  $S_1$  in Equation 6.1 to the matrix  $S_2$  in Equation 6.2 does not change the entries in any column only their order. Thus the sum of the entries of columns 1 through  $u$  is

$$\frac{u^3 + u}{2} + \left( \frac{u^3 + u}{2} + u \cdot 3u^2 \right) = 4u^3 + u$$

and the sum of the entries of columns  $u$  through  $2u$  is

$$\left( \frac{u^3 + u}{2} + u \cdot 2u^2 \right) + \left( \frac{u^3 + u}{2} + u \cdot u^2 \right) = 4u^3 + u$$

The sum of the entries of rows 1 through  $u$  is

$$\left( \frac{u^3 + u}{2} + m \cdot 3u^2 \right) + \left( \frac{u^3 + u}{2} + (m + 2) \cdot 2u^2 + (m - 1) \cdot u^2 \right) = 4u^3 + u$$

The sum of the entries of rows  $u$  through  $2u$  is

$$\left( \frac{u^3 + u}{2} + (m + 1) \cdot 3u^2 \right) + \left( \frac{u^3 + u}{2} + (m + 2) \cdot u^2 + (m - 1) \cdot 2u^2 \right) = 4u^3 + u$$

The sum of the entries on the forward diagonal is

$$\left( \frac{u^3 + u}{2} + (m + 1) \cdot 3u^2 \right) + \left( \frac{u^3 + u}{2} + (m + 2) \cdot u^2 + (m - 1) \cdot 2u^2 \right) = 4u^3 + u$$

The sum of the entries on the backward diagonal is

$$\left( \frac{u^3 + u}{2} + m \cdot 3u^2 \right) + \left( \frac{u^3 + u}{2} + (m + 2) \cdot u^2 + (m - 1) \cdot 2u^2 \right) = 4u^3 + u$$

□

## 6.4 The Product construction

Let  $A = [a_{ij}]$  be a magic square of order  $m$  and magic sum  $\alpha$ . Let  $B = [b_{ij}]$  be a magic square of order  $n$  and magic sum  $\beta$ . Then the  $mn$  by  $mn$  square

$$A \otimes B = \begin{bmatrix} (a_{11} - 1)n^2 + B & (a_{12} - 1)n^2 + B & \cdots & (a_{1m} - 1)n^2 + B \\ (a_{21} - 1)n^2 + B & (a_{22} - 1)n^2 + B & \cdots & (a_{2m} - 1)n^2 + B \\ \vdots & & \ddots & \vdots \\ (a_{m1} - 1)n^2 + B & (a_{m2} - 1)n^2 + B & \cdots & (a_{mm} - 1)n^2 + B \end{bmatrix}$$

is a magic square of order  $mn$  and magic sum  $\alpha n^3 - mn^3 + m\beta$ . See Exercise 6.4.1.1. Thus if  $m, n \in \mathcal{M}$ , then  $mn \in \mathcal{M}$ .

**Example 6.6.** The product of a magic square of order 3 with a magic square of order 4

$$\begin{bmatrix} 8 & 1 & 6 \\ 3 & 5 & 7 \\ 4 & 9 & 2 \end{bmatrix} \otimes \begin{bmatrix} 16 & 3 & 2 & 13 \\ 5 & 10 & 11 & 8 \\ 9 & 6 & 7 & 12 \\ 4 & 15 & 14 & 1 \end{bmatrix} = \begin{array}{|cccc|cccc|cccc|} \hline 128 & 115 & 114 & 125 & 16 & 3 & 2 & 13 & 96 & 83 & 82 & 93 \\ \hline 117 & 122 & 123 & 120 & 5 & 10 & 11 & 8 & 85 & 90 & 91 & 88 \\ \hline 121 & 118 & 119 & 124 & 9 & 6 & 7 & 12 & 89 & 86 & 87 & 92 \\ \hline 116 & 127 & 126 & 113 & 4 & 15 & 14 & 1 & 84 & 95 & 94 & 81 \\ \hline 48 & 35 & 34 & 45 & 80 & 67 & 66 & 77 & 112 & 99 & 98 & 109 \\ \hline 37 & 42 & 43 & 40 & 69 & 74 & 75 & 72 & 101 & 106 & 107 & 104 \\ \hline 41 & 38 & 39 & 44 & 73 & 70 & 71 & 76 & 105 & 102 & 103 & 108 \\ \hline 36 & 47 & 46 & 33 & 68 & 79 & 78 & 65 & 100 & 111 & 110 & 97 \\ \hline 64 & 51 & 50 & 61 & 144 & 131 & 130 & 141 & 32 & 19 & 18 & 29 \\ \hline 53 & 58 & 59 & 56 & 133 & 138 & 139 & 136 & 21 & 26 & 27 & 24 \\ \hline 57 & 54 & 55 & 60 & 137 & 134 & 135 & 140 & 25 & 22 & 23 & 28 \\ \hline 52 & 63 & 62 & 49 & 132 & 143 & 142 & 129 & 20 & 31 & 30 & 17 \\ \hline \end{array}$$

**Theorem 6.7.** There exists a magic square for every order except  $n = 2$ .

*Proof.* Let  $M$  be the set of orders  $n$ , for which there exists a magic square of order  $n$ . We have examples that show  $1, 3, 4, 8 \in M$  and constructions showing that:

1.  $2n + 1 \in M$ , for all  $n$ ,
2.  $4n + 2 \in M$ , for all  $n$ ,
3. if  $m, n \in M$ , then  $mn \in M$ .

Thus, by 1 and 2 we see that if  $n \equiv 1, 2, 3 \pmod{4}$ , then  $n \in M$ . If  $n \notin M$ ,  $n \neq 2$ , then there is a smallest  $n = 4k$  that  $n \notin M$ . Then, because  $4, 8 \in M$ , we see that  $k > 2$  and so  $k \in M$ . Consequently, by the product construction,  $4k \in M$ . Therefore  $M = \{n \in \mathbb{Z} : n \neq 2\}$ .  $\square$

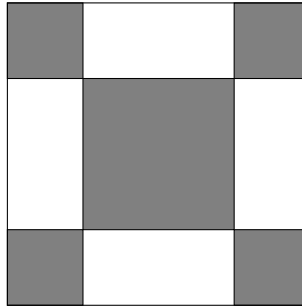
### 6.4.1 Exercises

1. Prove that the production construction given in Section 6.4 does indeed produce a magic square.
2. According to *Mathematical Recreations and Essays* By W. W. Rouse Ball, 1937, printed in Great Britain the following construction was first discovered in 1889 by W. Firth and has been rediscovered by many other authors. It was first related to me by M.S. Keranen.
  - (a) Prove that the following construction forms a normal magic square of order  $n = 4m$  for all  $m \geq 1$ .

**Step 1.** Form a square  $S_1$  by writing the numbers from the set  $\{1, 2, \dots, n^2\}$  in order from left to right across each row in turn, starting from the top left hand corner.

1	2	...	$n$
$n + 1$	$n + 2$	...	$2n$
	⋮		
	⋮		
	⋮		
$(n - 1)n + 1$	$(n - 1)n + 2$	...	$n^2$

**Step 2.** Now fix the shaded entries and interchange each unshaded entry with its diametrically opposite number. The shaded entries are the four  $m$  by  $m$  corner boxes and the center  $(2m)$  by  $(2m)$  box.



**Example:** A normal magic square of order  $n = 8$ , magic sum=260,  $m = 2$ .

**Step 1.**

1	2	3	4	5	6	7	8
9	10	11	12	13	14	15	16
17	18	19	20	21	22	23	24
25	26	27	28	29	30	31	32
33	34	35	36	37	38	39	40
41	42	43	44	45	46	47	48
49	50	51	52	53	54	55	56
57	58	59	60	61	62	63	64

**Step 2.**

1	2	62	61	60	59	7	8
9	10	54	53	52	51	15	16
48	47	19	20	21	22	42	41
40	39	27	28	29	30	34	33
32	31	35	36	37	38	26	25
24	23	43	44	45	46	18	17
49	50	14	13	12	11	55	56
57	58	6	5	4	3	63	64

- (b) Use this construction instead of the product construction to complete the proof that a magic square of order  $n$  exists except when  $n = 2$





## Chapter 7

# Mutually Orthogonal Latin Squares

Two Latin squares  $A$  and  $B$  of order  $n$  are said to be *orthogonal Latin squares* if the  $n^2$  ordered pairs

$$(A[x, y], B[x, y])$$

$x = 1, 2, 3, \dots, n, y = 1, 2, \dots, n$  are all distinct. A set  $A_1, A_2, \dots, A_k$  *mutual orthogonal Latin squares* of order  $n$ , is said to be  $k$  MOLS( $n$ ).

**Theorem 7.1.** *The number of MOLS( $n$ ) is at most  $n - 1$  for any  $n$ .*

*Proof.* Let  $L_1, L_2, \dots, L_t$  be  $t$  MOLS( $n$ ) on the symbols  $\{1, 2, \dots, n\}$ . Relabel the squares so that the first row of each is  $[1, 2, \dots, n]$ . This is always possible. Now consider  $[2, 1]$ -cell of each square. It can not be 1, because 1 is in the  $[1, 1]$ -cell of every square. Furthermore, they all must be different, for if  $L_i[2, 1] = L_j[2, 1] = k$ , then the pair  $(k, k)$  would appear twice as it appears already in row 1, i.e.  $L_i[1, k] = L_j[1, k] = k$ . Thus there are only  $n - 1$  choices for the  $[2, 1]$ -cells of the squares.  $\square$

### 7.1 Finite fields

A *field* is a set of elements  $\mathbb{F}$  with two binary operations defined on  $\mathbb{F}$  called multiplication and addition, such that  $\mathbb{F}$  is an commutative group under addition,  $\mathbb{F} \setminus \{0\}$  is a commutative group under multiplication, and  $a(b + c) = ab + ac$ , for all  $a, b, c \in \mathbb{F}$ . The field is said to be *finite*, if  $|\mathbb{F}|$  is finite.

**Theorem 7.2.** *Let  $\mathbb{F}$  be a finite field.*

1.  $|\mathbb{F}| = p^\alpha$ , for some prime  $p$  and some integer  $\alpha \geq 0$ .
2. For every prime  $p$  and integer  $\alpha \geq 0$ , there is up to isomorphism a unique field of order  $q = p^\alpha$ . We denote this unique field by  $\mathbb{F}_q$ .

3.

$$\mathbb{F}_q \approx \mathbb{Z}_p[X]/(f(X)) = \mathbb{Z}_p[X] \pmod{f(X)}$$

where  $f(X)$  is any irreducible polynomial of degree  $\alpha$  in  $\mathbb{Z}_p[X]$ .

4.  $\mathbb{F}_q \setminus \{0\}$  is a cyclic group of order  $q - 1$ .

*Proof.* A proof can be found in any abstract algebra book. □

**Example 7.3.** The polynomial  $f(X) = X^2 + 1$  is irreducible over  $\mathbb{Z}_3$ , because it is quadratic and has no roots in  $\mathbb{Z}_3$ . Thus

$$\mathbb{F}_9 \approx \mathbb{Z}_3[X]/(X^2 + 1)$$

Let  $g = X + 1$ , then modulo  $(X^2 + 1)$  we see that:

$$\frac{i}{g^i} \begin{array}{c|c|c|c|c|c|c|c|c} 0 & 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ \hline 1 & X + 1 & 2X & 2X + 1 & 2 & 2X + 2 & X & X + 2 \end{array}$$

and  $g^8 = 1$ . Hence  $\mathbb{F}_9 \setminus 0$  is a cyclic group of order 8.

**Theorem 7.4.** Let  $n = p^\alpha$ , where  $p$  is a prime and  $\alpha$  is a positive integer. Then for  $n \geq 3$ , there exists a complete set of  $n - 1$  MOLS( $n$ ).

*Proof.* Let  $\mathbb{F}_n$  be a finite field of order  $n$ . For each  $f \in \mathbb{F}_n$  define the  $\mathbb{F}_n \times \mathbb{F}_n$  matrix  $A_f$  by

$$A_f[x, y] = fx + y,$$

for all  $x, y \in \mathbb{F}_n$ . We claim that the  $n - 1$  squares  $A_f$ ,  $f \in \mathbb{F}_n$ ,  $f \neq 0$  are MOLS( $n$ ).

1. (**Row Latin**) If  $fx + y_1 = fx + y_2$ , then  $y_1 = y_2$ .
2. (**Column Latin**) If  $fx_1 + y = fx_2 + y$ , then  $fx_1 = fx_2$  and so  $x_1 = x_2$ .
3. (**Orthogonal**) Suppose

$$(A_f[x, y], A_\ell[x, y]) = (A_f[x_1, y_1], A_\ell[x_1, y_1])$$

for some  $f \neq \ell$ . Then

$$\begin{aligned} fx + y &= fx_1 + y_1 \\ \ell x + y &= \ell x_1 + y_1 \end{aligned}$$

Subtracting we see that

$$(f - \ell)x = (f - \ell)x_1.$$

Thus  $x = x_1$  and then  $y = y_1$ . □

**Example 7.5.** Four mutually orthogonal Latin squares of order 5. For  $n = 5$ , we have  $\mathbb{F}_5 = \mathbb{Z}_5$ . The four mutually orthogonal Latin squares are defined by the equations:

$$\begin{aligned} A_1[x, y] &= x + y \\ A_2[x, y] &= 2x + y \\ A_3[x, y] &= 3x + y \\ A_4[x, y] &= 4x + y, \end{aligned}$$

where  $x, y \in \mathbb{F}_5$ . The actual squares are:

0	1	2	3	4	0	1	2	3	4	0	1	2	3	4	0	1	2	3	4
1	2	3	4	0	2	3	4	0	1	3	4	0	1	2	4	0	1	2	3
2	3	4	0	1	4	0	1	2	3	1	2	3	4	0	1	2	3	4	0
3	4	0	1	2	1	2	3	4	0	4	0	1	2	3	2	3	4	0	1
4	0	1	2	3	3	4	0	1	2	2	3	4	0	1	1	2	3	4	0
A <sub>1</sub>					A <sub>2</sub>					A <sub>3</sub>					A <sub>4</sub>				

An *orthogonal array* of order  $n$  and size  $k$  is a  $k$  by  $n^2$  array  $A$  with entries from an  $n$ -element set  $S$  such that in any pair of distinct rows  $i$  and  $j$  every ordered pair occurs. That is

$$\{(A[i, h], A[j, h]) : h = 1, 2, 3, \dots, n^2\} = S \times S.$$

We denote an *orthogonal array* of order  $n$  and size  $k$  by  $\text{OA}(k, n)$ .

**Example 7.6.** An  $\text{OA}(4, 3)$ .

1	1	1	2	2	2	3	3	3
1	2	3	1	2	3	1	2	3
1	2	3	3	1	2	2	3	1
1	2	3	2	3	1	3	1	2

**Theorem 7.7.** An  $\text{OA}(k, n)$  is equivalent to  $k - 2$   $\text{MOLS}(n)$ .

*Proof.* Let  $L_1, L_2, \dots, L_{k-2}$  be  $k - 2$   $\text{MOLS}(n)$  on the symbols  $\{1, 2, \dots, n\}$ . Label the rows and columns of the squares by  $1, 2, 3, \dots, n$ . Define the  $k$  by  $n^2$  array  $A$  by:

$$\begin{aligned} A[1, ni + j + 1] &= i + 1 \text{ for } i = 0, 1, 2, \dots, n - 1 \text{ and } j = 0, 1, 2, \dots, n - 1 \\ A[2, ni + j + 1] &= j + 1 \text{ for } i = 0, 1, 2, \dots, n - 1 \text{ and } j = 0, 1, 2, \dots, n - 1 \\ A[h + 2, \ell] &= L_h[A[1, \ell], A[2, \ell]] \text{ for } \ell = 1, 2, \dots, n^2 \text{ and } h = 1, 2, \dots, k - 2 \end{aligned}$$

It is easy to see that  $A$  is an  $\text{OA}(k, n)$ .

Given an  $\text{OA}(k, n)$   $A$  we can define Latin squares  $L_1, L_2, \dots, L_{k-2}$  as follows

$$L_h[A[1, \ell], A[2, \ell]] = A[h, \ell], \quad \ell = 1, 2, \dots, n^2.$$

It is an easy exercise to check that these squares are Latin squares and are pairwise orthogonal.  $\square$

**Example 7.8.** 2  $\text{MOLS}(3)$  is equivalent to  $\text{OA}(4, 3)$

1	2	3	1	2	3	1	1	1	2	2	2	3	3	3
3	1	2	2	3	1	1	2	3	1	2	3	1	2	3
2	3	1	3	1	2	1	2	3	3	1	2	2	3	1
L <sub>1</sub>			L <sub>2</sub>			A								

A *transversal design* with  $k$  groups of size  $n$ , denoted by  $\text{TD}(k, n)$  is a triple  $(X, \mathcal{B}, \mathcal{G})$ , where

1.  $X$  is a set of  $kn$  points,

2.  $\mathcal{B}$  is a collection of  $k$ -element subsets called *blocks*

3.  $\mathcal{G} = \{G_1, G_2, \dots, G_k\}$  is a partition of the  $kn$  points into  $k$  subsets of size  $n$  called *groups*,

such that every pair of points is in exactly one group or one block.

Because the blocks of a transversal design each contain exactly one point from each group, we say that the blocks are *transverse*.

**Example 7.9.** A TD(4, 3).

$$\begin{aligned} X &= \{a_1, a_2, a_3, b_1, b_2, b_3, c_1, c_2, c_3, d_1, d_2, d_3\} \\ \mathcal{G} &= \left[ \underbrace{\{a_1, a_2, a_3\}}_{G_1}, \underbrace{\{b_1, b_2, b_3\}}_{G_2}, \underbrace{\{c_1, c_2, c_3\}}_{G_3}, \underbrace{\{d_1, d_2, d_3\}}_{G_4} \right] \\ \mathcal{B} &= \left\{ \begin{array}{l} \{a_1, b_1, c_1, d_1\} \\ \{a_1, b_2, c_2, d_2\} \\ \{a_1, b_3, c_3, d_3\} \\ \{a_2, b_1, c_3, d_2\} \\ \{a_2, b_2, c_1, d_3\} \\ \{a_2, b_3, c_2, d_1\} \\ \{a_3, b_1, c_2, d_3\} \\ \{a_3, b_2, c_3, d_1\} \\ \{a_3, b_3, c_1, d_2\} \end{array} \right\} \end{aligned}$$

**Theorem 7.10.** A TD( $k, n$ ) is equivalent to an OA( $k, n$ ).

*Proof.* Given an OA( $k, n$ ) on symbols  $\{1, 2, \dots, n\}$ , define the groups  $G_1, G_2, \dots, G_k$  of the corresponding TD( $k, n$ ) as follows:

$$G_i = \{(i, j) : j = 1, 2, \dots, n\}.$$

If the  $\ell$ -th column of the OA( $k, n$ ) is

$$[x_1, x_2, x_3, \dots, x_k]^T$$

choose

$$\{(1, x_1), (2, x_2), (3, x_3), \dots, (k, x_k)\}$$

as a block of the TD( $k, n$ ). It is easy to see that this does indeed construct a TD( $k, n$ ) from an OA( $k, n$ ).

Conversely suppose we are given a TD( $k, n$ )  $(X, \mathcal{B}, \mathcal{G})$ . Define an OA( $k, n$ )  $A$  by choosing a bijection  $f_i : G_i \rightarrow \{1, 2, \dots, n\}$  for each group  $G_i \in \mathcal{G}$ . Let  $\mathcal{B} = \{B_1, B_2, \dots, B_{n^2}\}$ . Then the array is

$$A[i, j] = f_i(G_i \cap B_j)$$

it is an easy exercise to show that  $A$  is indeed an OA( $k, n$ ) □

**Corollary 7.11.** The three objects OA( $k, n$ ), TD( $k, n$ ) and  $(k - 2)$  MOLS( $n$ ) are all equivalent.

## 7.2 Finite projective planes

A *projective plane* is a pair  $(\mathbb{P}, \mathcal{L})$ , where  $\mathbb{P}$  is a finite set of *points* and  $\mathcal{L}$  is a collection of subsets of  $\mathbb{P}$  called *lines*, satisfying the following three axioms

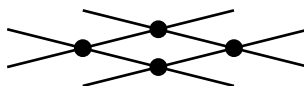
1. *Every 2 points determine a unique line.* That is given points  $x, y \in \mathbb{P}$ ,  $x \neq y$  there is exactly one line  $L \in \mathcal{L}$ , with  $x, y \in L$ .



2. *Every 2 lines determine a unique point.* That is given lines  $L, L' \in \mathcal{L}$ ,  $L \neq L'$  then  $|L \cap L'| = 1$ .



3. *There exist 4 points no 3 of which are collinear.* That is there are at least four distinct points no 3 of which are in the same line.

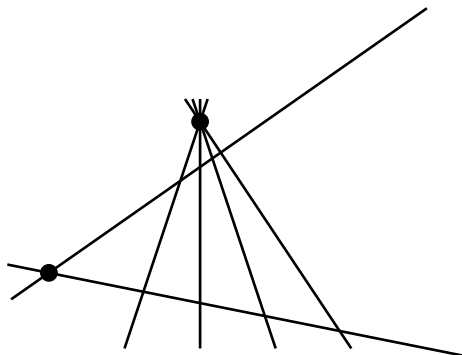


**Theorem 7.12.** *All the lines in a projective plane  $(\mathbb{P}, \mathcal{L})$  have the same number of points.*

*Proof.* Consider any two lines  $L, L' \in \mathcal{L}$ . By axiom 2 they intersect in a unique point  $x$ .

$$L \cap L' = \{x\}.$$

Let  $x_1, x_2, \dots, x_n$  be the remaining points on  $L$ . Thus  $L$  has  $n + 1$  points. By axiom 3 there is point  $y$  that is not on  $L$  or  $L'$ . By axiom 1 there is a unique line  $L_i$  that contains  $y$  and  $x_i$ ,  $i = 1, 2, \dots, n$ . By axiom 2 the line  $L_i$  intersects  $L'$  in a unique point  $x'_i$ . The points  $x'_1, x'_2, \dots, x'_n$  are all distinct because by axiom 1 the lines  $L_i$ ,  $i = 1, 2, \dots, n$ , pairwise intersect only in the point  $y$ . This accounts for  $n + 1$  points on  $L'$ . If  $z$  is on  $L'$ , then there is a line  $\hat{L}$  that contains  $x$  and  $y$ . This line intersects  $L$  in some point  $x_i$  say. But then  $\hat{L} = L_i$  because the two points  $y$  and  $x_i$  determine a unique line. Consequently  $z = x'_i$ . Therefore  $L'$  has exactly  $n + 1$  points the same as  $L$ .



□

A projective plane  $(\mathbb{P}, \mathcal{L})$  in which the number of points on a line is  $n + 1$  is called a projective plane of order  $n$ .

**Theorem 7.13.** *In a projective plane of order  $n$ , every point is on  $n + 1$  lines.*

*Proof.* Let  $y$  be any point. Then by axiom 3 there is a line  $L$  such that  $y \notin L$ . According to Theorem 7.12  $L = \{x_1, x_2, \dots, x_{n+1}\}$  for some set of  $n + 1$  points. By axiom 2, every line containing  $y$  must intersect  $L$ , and by axiom 1 we see that for each  $i = 1, 2, \dots, n + 1$ , There is a unique line  $L_i$ , with  $y, x_i \in L_i$  for each  $i = 1, 2, \dots, n + 1$ . Thus there are exactly  $n + 1$  lines through the point  $y$ .  $\square$

**Theorem 7.14.** *A projective plane of order  $n$  has  $n^2 + n + 1$  points.*

*Proof.* Let  $y$  be any point. If  $x$  is any other point then by axiom 1 there is a line that contains  $x$  and  $y$ . Thus every point is on a line through  $y$ . Applying Theorem 7.13 we see that there are  $n + 1$  lines through  $y$ , and by Theorem 7.12 there are  $n$  points other than  $y$  on each of these lines. There are thus

$$1 + n(n + 1) = n^2 + n + 1$$

points.  $\square$

**Example 7.15.** *The Steiner triple system  $\{ \{0,1,3\} \{1,2,4\} \{2,3,5\} \{3,4,6\} \{0,4,5\} \{1,5,6\} \{0,2,6\} \}$  of order 7 is a projective plane of order 2.*

**Theorem 7.16.** *A projective plane of order  $n$ ,  $n - 1$  MOLS( $n$ ), a OA( $n + 1, n$ ) and a TD( $n + 1, n$ ) are all equivalent.*

*Proof.* We already know from Theorem 7.11 that  $n - 1$  MOLS( $n$ ), a OA( $n + 1, n$ ) and a TD( $n + 1, n$ ) are equivalent. We will first show that from a projective plane of order  $n$  that you can construct OA( $n + 1, n$ ).

Let  $(\mathbb{P}, \mathcal{L})$  be a projective plane of order  $n$ . Choose any line  $L \in \mathcal{L}$  and let  $P_1, P_2, \dots, P_{n+1}$  be the  $n + 1$  points on  $L$ . Through each  $P_i$  there are  $n$  lines other than  $L$ , number them  $1, 2, 3, \dots, n$  arbitrarily. Let  $Q_1, Q_2, \dots, Q_{n^2}$  be the other  $n^2$  points and let  $a_{ij}$  be the number assigned to the line through  $P_i$  and  $Q_j, i = 1, 2, \dots, n + 1$  and  $j = 1, 2, \dots, n^2$ . Then its easily checked that

$$A = [a_{ij}],$$

$i = 1, 2, \dots, n + 1, j = 1, 2, \dots, n^2$  is an OA( $n + 1, n$ ).

Now we will show how to construct a a projective plane of order  $n$  from a TD( $n + 1, n$ ).

Let  $(X, \mathcal{B}, \mathcal{G})$  be a TD( $n + 1, n$ ) and let  $\infty$  be a new point. Set  $\mathbb{P} = X \cup \{\infty\}$  and  $\mathcal{L} = \mathcal{B} \cup \{G \cup \{\infty\} : G \in \mathcal{G}\}$ . Then  $(\mathbb{P}, \mathcal{L})$  is the required projective plane.  $\square$

**Theorem 7.17.** *There exists a projective plane of order  $n$  whenever  $n$  is a prime power.*

*Proof.* If  $n$  is a prime power then we know from Theorem 7.4 that there exist  $n - 1$  MOLS( $n$ ). Thus applying Theorem 7.16 we have the result.  $\square$

### 7.3 Pairs of orthogonal Latin squares

The pair of orthogonal Latin squares time line.

- Euler conjectures that 2 MOLS( $n$ ) exists if and only if  $n \equiv 0,1,3 \pmod{4}$ . He could do these but could not construct any pair of orthogonal Latin squares of order  $2 \pmod{4}$ .
- G. Tarry (1900) In a 33 page journal paper showed that does not exist 2 MOLS(4).
- MacNeise (1922) conjectures that if

$$n = p_1^{r_1} p_2^{r_2} \cdots p_x^{r_x},$$

where  $p_1, p_2, \dots, p_x$  are distinct primes, then the maximum number of MOLS( $n$ ) is

$$M(n) = \text{MIN}\{p_1^{r_1} - 1, p_2^{r_2} - 1, \dots, p_x^{r_x} - 1\}$$

- E.T. Parker (1957) constructs 3 MOLS(21). This disproves MacNeise's conjecture that the maximum number would be  $M(21) = \text{MIN}\{3 - 1, 7 - 1\} = 2$ .
- R.S. Bose and S.S. Shrikande (1958) construct 2 MOLS(22) disproving Euler's conjecture. This result made the New York times.
- E.T. Parker (1959) constructs 2 MOLS(10).
- Bose, Shrikande, and Parker (1960) proves that there exists 2 MOLS( $n$ ) for every  $n$  except for  $n = 2$  or  $n = 6$  when they cannot exist.
- Stinson (1984) Gives a clever 3 page proof that there do not exist 2 MOLS(6).

In this chapter we construct 2 MOLS( $n$ ) for every  $n$  except  $n = 2$  and  $n = 6$ . Let  $N_{\text{MOLS}}(n)$  be the number of mutually orthogonal Latin squares of order  $n$ . Note that  $N_{\text{MOLS}}(1) = \infty$ . Our goal is to show  $N_{\text{MOLS}}(n) \geq 2$  for all positive integers  $n$  except  $n = 2$ , and  $n = 6$ .

**Theorem 7.18. (Finite Field construction)** For each  $p^r$ , where  $p$  is a prime and  $r > 0$  is an integer, there exist  $p^r - 1$  MOLS( $p^r$ ), i.e.  $N_{\text{MOLS}}(p^r) = p^r - 1$ .

*Proof.* We all ready did this in Theorem 7.4. □

**Theorem 7.19. (Direct product construction)** Let  $A$  be a Latin square on  $X$  and let  $B$  be a Latin square on  $Y$ . Define the square  $A \times B$  on  $X \times Y$  by

$$(A \times B)[(x_1, y_1), (x_2, y_2)] = (A[x_1, x_2], B[y_1, y_2]).$$

Then  $A \times B$  is a Latin square.

*Proof.* Exercise 1. □

**Example 7.20.**

$$\begin{array}{|c|c|} \hline X & O \\ \hline O & X \\ \hline \end{array} \times \begin{array}{|c|c|c|} \hline 1 & 2 & 3 \\ \hline 3 & 1 & 2 \\ \hline 2 & 3 & 1 \\ \hline \end{array} = \begin{array}{|c|c|c|c|c|c|} \hline X1 & X2 & X3 & O1 & O2 & O3 \\ \hline X3 & X1 & X2 & O3 & O1 & O2 \\ \hline X2 & X3 & X1 & O2 & O3 & O1 \\ \hline O1 & O2 & O3 & X1 & X2 & X3 \\ \hline O3 & O1 & O2 & X3 & X1 & X2 \\ \hline O2 & O3 & O1 & X2 & X3 & X1 \\ \hline \end{array}$$

**Theorem 7.21.** . If  $A_1, A_2$  are  $\text{MOLS}(x)$  and  $B_1, B_2$  are  $\text{MOLS}(y)$ , then  $A_1 \times B_1$  and  $A_2 \times B_2$  are  $\text{MOLS}(xy)$ ,

*Proof.* Exercise 2. □

**Corollary 7.22.** If  $n = p_1^{r_1} p_2^{r_2} \cdots p_x^{r_x}$ , where  $p_1, p_2, \dots, p_x$  are distinct primes, then

$$N_{\text{MOLS}}(n) \geq \min\{p_1^{r_1} - 1, p_2^{r_2} - 1, \dots, p_x^{r_x} - 1\}.$$

*Proof.* Let  $M(n) = \min\{p_1^{r_1}, p_2^{r_2}, \dots, p_x^{r_x}\} - 1$ . The Finite field construction provides  $p_i^{r_i} - 1$   $\text{MOLS}(p_i^{r_i})$  for  $i = 1, 2, \dots, x$ . So there exists  $M(n)$   $\text{MOLS}(p_i^{r_i})$ , for each  $i$ . Now apply the direct product construction to get  $M(n)$   $\text{MOLS}(n)$ . □

Observe that if  $n \equiv 0, 1$ , or  $3 \pmod{4}$ , then the smallest prime power  $q$  that divides  $n$  is at least 3. Hence applying Corollary 7.22 we may conclude the following.

**Corollary 7.23.** If  $n \equiv 0, 1$ , or  $3 \pmod{4}$ , then  $N_{\text{MOLS}}(n) \geq 2$ .

The rest of this chapter deals with the difficult case, i.e. two  $\text{MOLS}$  of order  $n$ , when  $n \equiv 2 \pmod{4}$ .

**Theorem 7.24.** If there are  $k - 1$   $\text{MOLS}(n)$ , then there are  $k - 2$  idempotent  $\text{MOLS}(n)$ .

*Proof.* Let  $L_0, L_1, \dots, L_{k-2}$  be  $\text{MOLS}(n)$  on  $\{1, 2, \dots, n\}$ . Simultaneously, permute the rows and columns of the all the squares so that the diagonal of  $L_0$  is  $[1, 1, 1, \dots, 1]$ . The remain squares now must have each of the symbols  $1, 2, 3, \dots, n$  on there diagonals in some order. These squares can be simultaneously relabeled so that  $L_1, L_2, \dots, L_{k-2}$  are idempotent. □

Using the alternative language of orthogonal arrays we rewrite Theorem 7.24 into Theorem 7.25. A column is a constant column if all its entries are identical.

**Theorem 7.25.** If there is an  $\text{OA}(k + 1, n)$ , then there is an  $\text{OA}(k, n)$  with  $n$  constant columns.

If  $S$  is any subset of the symbols we denote in the remainder of this chapter the  $k$  by  $|S|$  matrix of constant columns by

$$C(k, S) = \underbrace{[[s, s, s, \dots, s]^T : s \in S]}_{k \text{ times}}$$

An orthogonal array  $\text{OA}(k, n)$  on  $S$  with  $n = |S|$  constant columns can be written as

$$[C(k, S), A]$$

where  $A$  are the remaining  $n^2 - n$  non-constant columns.

**Example 7.26.** 3 idempotent  $\text{MOLS}(5)$  and an  $\text{OA}(5, 5)$  with 5 constant columns

We start with the 4  $\text{MOLS}(5)$  given in Example 7.5:

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



Now simultaneously permute the rows of all the squares so that the first one has a constant diagonal say  $[0, 0, 0, 0, 0]^T$ .

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

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

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

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

Now in each of the remaining squares the diagonal contains each symbol once. Independently permute the symbols in these squares so that their diagonals become  $[0, 1, 2, 3, 4]^T$ . That is use the permutations

$$\begin{pmatrix} 0 & 1 & 2 & 3 & 4 \\ 0 & 4 & 3 & 2 & 1 \end{pmatrix}, \begin{pmatrix} 0 & 1 & 2 & 3 & 4 \\ 0 & 2 & 4 & 1 & 3 \end{pmatrix}, \text{ and } \begin{pmatrix} 0 & 1 & 2 & 3 & 4 \\ 0 & 3 & 1 & 4 & 2 \end{pmatrix}$$

This obtains 3 idempotent MOLS(5).

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

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

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

we can now use Theorem 7.7 to construct  $[C(k, S), A]$  an OA(5, 5) with 5 constant columns,  $S = \{0, 1, 2, 3, 4\}$ .

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

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

$C(k, S)$ 
 $A$

A pairwise balanced design PBD of type  $2-(v, \mathcal{K}, \lambda)$  is a pair  $(X, \mathcal{B})$  where

1.  $X$  is a  $v$ -element set of points,
2.  $\mathcal{B}$  is a collection of subsets of  $X$  called blocks,
3.  $|B| \in \mathcal{K}$  for every block  $B \in \mathcal{B}$ , and
4. every pair of points is in  $\lambda$  blocks.

The parameter  $\lambda$  is called the index. If the index is  $\lambda = 1$  we say that the design is a Steiner pairwise balanced design or a Linear space. If  $\mathcal{K} = \{k\}$ , we write  $2-(v, k, \lambda)$  instead of  $2-(v, \mathcal{K}, \lambda)$ .

**Example 7.27.** • A Steiner triple system of order  $n$ , STS( $n$ ), is a  $2-(n, 3, 1)$ .

- A projective plane of order  $n$  is a  $2-(n^2 + n + 1, n + 1, 1)$ .

- A transversal design,  $\text{TD}(k, n)$  is a  $2-(nk, \{k, n\}, 1)$  with exactly  $k$  blocks of size  $n$ , and they are disjoint.

**Theorem 7.28. (The PBD construction for an  $k$  MOLS( $n$ ))**

Let  $(X, \mathcal{B})$  be a PBD of index 1. Suppose for each  $B \in \mathcal{B}$ , there exists  $k$  idempotent MOLS( $|B|$ ). Then there are  $k$  idempotent MOLS( $|X|$ ).

*Proof.* We will construct an  $\text{OA}(k+2, |X|)$ , with  $|X|$  constant columns. Let  $(X, \mathcal{B})$  be a PBD of index 1 and suppose for each  $B_i \in \mathcal{B} = \{B_1, B_2, \dots, B_b\}$ , there exists  $k$  idempotent MOLS( $|B|$ ) with  $|B|$  constant columns. Then for each  $B_i \in \mathcal{B}$  there is an  $\text{OA}(k+2, |B_i|)$  on  $B_i$

$$[C(k+2, B_i), A_{B_i}]$$

where  $C(k+2, B_i)$  are the constant columns and  $A_{B_i}$  are the remaining non-constant columns. Then

$$[C(k+2, X), A_{B_1}, A_{B_2}, A_{B_3}, \dots, A_{B_b}]$$

is an  $\text{OA}(k+2, |X|)$ , with  $|X|$  constant columns. For consider any pair of rows  $u, v$  and any two symbols  $a, b \in X$ . If  $a = b$ , then  $a, b$  appears on rows  $u, v$  in a unique column of  $C(k+2, X)$ . If  $a \neq b$ , then there is exactly one block  $B_i \in \mathcal{B}$  that contains  $a$  and  $b$  on rows  $u, v$ . Hence there is exactly one column of  $A_{B_i}$  that contains  $a, b$  on rows  $u, v$ . An  $\text{OA}(k+2, |X|)$ , with  $|X|$  constant columns is equivalent to  $k$  idempotent MOLS( $|X|$ )  $\square$

**Example 7.29.** Three MOLS of order 21. We have that  $4 = 2^2$ , is a prime power. So, by Theorem 7.18, there are 3 MOLS(4) and thus by Theorem 7.16 there is a projective plane of order 4, i.e a  $2-(21, 5, 1)$ . Also 5, is a prime power. So, by Theorem 7.18, there are 4 MOLS(5) and thus by Theorem 7.24, there are 3 idempotent MOLS(5). Now applying Theorem 7.28 we have 3 MOLS(21).

**Corollary 7.30.** If there is a PBD of type  $2-(v, \mathcal{K}, 1)$ , then

$$N_{\text{MOLS}}(v) \geq \min\{N_{\text{MOLS}}(k) - 1 : k \in \mathcal{K}\}$$

*Proof.* For each  $k \in \mathcal{K}$ , apply Theorem 7.24 to obtain  $N_{\text{MOLS}}(k)-1$  idempotent MOLS( $k$ ). Now use the construction provided by Theorem 7.28.  $\square$

In a PBD( $X, \mathcal{B}$ ) a collection of blocks

$$B_1, B_2, \dots, B_r$$

that partition the points is called a *parallel class*. A partial parallel class is called *clear set* of blocks.

**Theorem 7.31. (The clear set PBD construction for  $k$  MOLS( $n$ ))**

Let  $(X, \mathcal{B})$  be a PBD with a clear set  $\Pi$  of blocks  $\Pi \subseteq \mathcal{B}$ . Suppose for each  $P \in \Pi$  there are  $k$  MOLS( $|P|$ ) and for each  $B \in \mathcal{B} \setminus \Pi$  there are  $k$  idempotent MOLS( $|B|$ ). Then there are  $k$  MOLS( $|X|$ ).



4. 5 is a prime so there are  $(5 - 1) - 1 = 3$  idempotent  $\text{MOLS}(5)$ .

The clear set PBD construction (Theorem 7.31) yields 2  $\text{MOLS}(22)$ .

**Corollary 7.33.** *If there is a PBD of type  $2-(v, \mathcal{K}, 1)$  and a subset  $\mathcal{K}_0 \subseteq \mathcal{K}$  in which no two blocks with sizes in  $\mathcal{K}_0$  intersect, then*

$$N_{\text{MOLS}}(v) \geq \min \{ \{N_{\text{MOLS}}(k) : k \in \mathcal{K}_0\} \cup \{N_{\text{MOLS}}(k) - 1 : k \in \mathcal{K} \setminus \mathcal{K}_0\} \}$$

*Proof.* Observe that  $\Pi = \{B \in \mathcal{B} : |B| \in \mathcal{K}_0\}$  is a clear set of blocks. For each  $k \in \mathcal{K} \setminus \mathcal{K}_0$ , apply Theorem 7.24 to obtain  $N_{\text{MOLS}}(k)-1$  idempotent  $\text{MOLS}(k)$ . Now use the construction provided by Theorem 7.31.  $\square$

**Example 7.34.** *Consider a projective plane of order 4, i.e. a PBD of type  $2-(21, 5, 1)$  and let  $x, y,$  and  $z$  be any 3 non-collinear points. Referring to Figure 7.1 we see that there are 3 lines containing pair of  $x, y,$  and  $z$ , there are 3 other lines through each of  $x, y,$  and  $z$ , and there are 9 lines not containing any of  $x, y,$  or  $z$ . Deleting  $x, y,$  and  $z$  we obtain a PBD of type  $2-(18, \{3, 4, 5\}, 1)$  in*

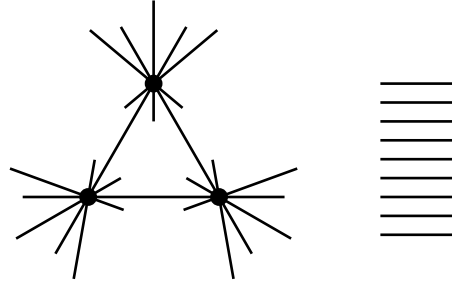


Figure 7.1: The projective plane of order 4 and 3 non-collinear points

which the blocks of size 3 form a clear set. Hence applying Theorem 7.33 we have

$$N_{\text{MOLS}}(18) \geq \min\{N_{\text{MOLS}}(3), N_{\text{MOLS}}(4) - 1, N_{\text{MOLS}}(5) - 1\} = 2.$$

A pairwise balanced design is said to be *resolvable* if its blocks can be partitioned into parallel classes.

**Theorem 7.35.** *If  $N_{\text{MOLS}}(m) \geq k - 1$ , then there is a resolvable PBD of type  $2-(km, \{k, m\}, 1)$  with  $m + 1$  parallel classes in which the blocks of size  $m$  form one of the parallel classes.*

*Proof.* Because  $N_{\text{MOLS}}(m) \geq k - 1$ , there is a  $\text{TD}(k+1, m)$   $(X, \mathcal{G}, \mathcal{B})$ . Let  $\mathcal{G} = \{G_0, G_1, G_2, \dots, G_k\}$  and  $G_0 = \{1, 2, 3, \dots, m\}$ . For each  $i \in G_0$ , i.e. for each  $i = 1, 2, \dots, m$  set

$$\mathbb{P}_i = \{B \setminus \{i\} : B \in \mathcal{B} \text{ and } i \in B\}$$

Let  $\mathbb{P}_0 = \{G_1, G_2, \dots, G_k\}$ . Then  $\mathbb{P}_0, \mathbb{P}_1, \dots, \mathbb{P}_m$  form the parallel classes of the required PBD. of type  $2-(km, \{k, m\}, 1)$ .  $\square$

**Corollary 7.36.** *If  $N_{\text{MOLS}}(m) \geq k - 1$  and  $1 \leq x < m$ , then*

1. *There exists a PBD of type  $2-(km + x, \{x, m, k, k + 1\}, 1)$ , and*

$$2. N_{\text{MOLS}}(km + x) \geq \min\{N_{\text{MOLS}}(x), N_{\text{MOLS}}(m), N_{\text{MOLS}}(k) - 1, N_{\text{MOLS}}(k + 1) - 1\}.$$

*Proof.* Use Theorem 7.35 to obtain a resolvable PBD of type  $2\text{-}(km, \{m, k\}, 1)$  with parallel classes  $\mathbb{P}_0, \mathbb{P}_1, \dots, \mathbb{P}_m$  in which  $\mathbb{P}_0 = \{B_1, B_2, \dots, B_k\}$  is the parallel class formed by the blocks of size  $m$ . For  $i = 1, 2, \dots, x$ , add a new point  $\infty_i$  to each block in  $\mathbb{P}_i$ . Let  $B_0 = \{\infty_1, \infty_2, \dots, \infty_x\}$  be a new block. It is easy to check that this yields a PBD of type  $2\text{-}(km + x, \{x, m, k, k + 1\}, 1)$  in which the blocks  $B_0, B_1, \dots, B_k$  form a clear set. Apply Theorem 7.31.  $\square$

**Example 7.37.**  $N_{\text{MOLS}}(100) = N_{\text{MOLS}}(7 \cdot 13 + 9)$ . So with  $k = 7$ ,  $m = 13$ ,  $x = 9$ , we have

$$N_{\text{MOLS}}(100) \geq \min\{N_{\text{MOLS}}(13), N_{\text{MOLS}}(9), N_{\text{MOLS}}(7) - 1, N_{\text{MOLS}}(8) - 1\} = 5$$

The value of  $k = 4$  in Corollary 7.36 yields the following Theorem.

**Theorem 7.38.** *If  $N_{\text{MOLS}}(m) \geq 3$ ,  $N_{\text{MOLS}}(x) \geq 2$  and  $1 \leq x < m$ , then  $N_{\text{MOLS}}(4m + x) \geq 2$ .*

**Lemma 7.39.**  $N_{\text{MOLS}}(4t) \geq 3$  for all  $t \geq 1$ .

*Proof.* Corollary 7.22 shows that  $N_{\text{MOLS}}(4t) \geq 2$  except possibly when  $3|t$  but  $9 \nmid t$ . Write  $4t = 2^a 3u$ , where  $a \geq 2$  and  $\gcd(u, 6) = 1$ . Then  $N_{\text{MOLS}}(u) \geq 4$  and so  $N_{\text{MOLS}}(4t) \geq \min\{N_{\text{MOLS}}(2^a 3), 4\}$ . Hence we need only show that  $N_{\text{MOLS}}(2^a 3) \geq 3$ . Now  $2^a 3 = 2^b \cdot 12$  or  $2^a 3 = 2^b \cdot 24$ , where either  $b = 0$  or  $b \geq 2$ . So

$$N_{\text{MOLS}}(2^a 3) \geq \min\{3, N_{\text{MOLS}}(12)\} \geq 2$$

or

$$N_{\text{MOLS}}(2^a 3) \geq \min\{3, N_{\text{MOLS}}(24)\} \geq 2$$

Exercises 5 and 4 show that the number of mutually orthogonal Latin squares of orders 12 and 24 is at least 2.  $\square$

**Theorem 7.40.**  $N_{\text{MOLS}}(n) \geq 2$  for all positive integers  $n$ ,  $n \neq 2$  or 6.

*Proof.* Corollary 7.23 tells us that we need only consider  $n \equiv 2 \pmod{4}$ . Write

$$\begin{aligned} n &= 16k + y \\ &= 16(k - 1) + (16 + y). \end{aligned}$$

where  $y = 2, 6, 10$  or  $14$ . We see that  $N_{\text{MOLS}}(16 + y) \geq 2$  for each such  $y$  as follows:

- $N_{\text{MOLS}}(18) \geq 2$ , by Example 7.34.
- $N_{\text{MOLS}}(22) \geq 2$ , by Exercise 3.
- $N_{\text{MOLS}}(26) \geq 2$ , by Exercise 7.
- $N_{\text{MOLS}}(30) \geq \min\{N_{\text{MOLS}}(3), N_{\text{MOLS}}(10)\} = 2$ , by Theorem 7.21 and Exercise 3.

Thus by Theorem 7.38 and Lemma 7.39,

$$N_{\text{MOLS}}(16k + y) = N_{\text{MOLS}}(4 \cdot 4(k - 1) + (16 + y)) \geq 2$$

provided  $k - 1 \geq 1$  and  $16 + y < 4(k - 1)$ , i.e. provided  $k \geq 2$  and  $4k - 4 > 30$ . i.e. provided  $k \geq 9$ . Thus all that remains is to show that  $N_{\text{MOLS}}(n) \geq 2$  for all  $n \equiv 2 \pmod{4}$ , and  $6 < n < 144$ .

The ones with  $n \equiv 1 \pmod{3}$  are taken care of in Exercise 3. For  $n = 14, 26,$  and  $38,$  see Exercises 6, 7 and 8. For  $n = 18,$  see Example 7.34. For the remaining values of  $n$  we write  $n = x \cdot y,$  where  $\min\{N_{\text{MOLS}}(x), N_{\text{MOLS}}(y)\} \geq 2$  and use Theorem 7.21 or we write  $n = k \cdot m + x$  where  $\min\{N_{\text{MOLS}}(x), N_{\text{MOLS}}(m), N_{\text{MOLS}}(k) - 1, N_{\text{MOLS}}(k + 1) - 1\} \geq 2$  and use Corollary 7.36. The values of  $x, y, m,$  and  $k$  are given in the following table.

$30=3 \cdot 10$	$42=3 \cdot 14$	$50=5 \cdot 10$	$54=3 \cdot 18$	$62=4 \cdot 13 + 10$	$66=3 \cdot 22$
$74=4 \cdot 16 + 10$	$78=3 \cdot 66$	$86=4 \cdot 19 + 10$	$90=9 \cdot 10$	$98=7 \cdot 14$	$102=3 \cdot 34$
$110=5 \cdot 22$	$114=3 \cdot 38$	$122=4 \cdot 27 + 14$	$126=9 \cdot 14$	$134=4 \cdot 27 + 26$	$138=3 \cdot 46$

□

### 7.3.1 Exercises

1. Prove Theorem 7.19.
2. Prove Theorem 7.21.
3. Let  $A$  be the following  $4 \times 4m$  array

$$\begin{bmatrix} 0 & 0 & \cdots & 0 & 1 & 2 & \cdots & m & 2m & 2m-1 & \cdots & m+1 & \infty_1 & \infty_2 & \cdots & \infty_m \\ 1 & 2 & \cdots & m & 0 & 0 & \cdots & 0 & \infty_1 & \infty_2 & \cdots & \infty_m & 2m & 2m-1 & \cdots & m+1 \\ 2m & 2m-1 & \cdots & m+1 & \infty_1 & \infty_2 & \cdots & \infty_m & 0 & 0 & \cdots & 0 & 1 & 2 & \cdots & m \\ \infty_1 & \infty_2 & \cdots & \infty_m & 2m & 2m-1 & \cdots & m+1 & 1 & 2 & \cdots & m & 0 & 0 & \cdots & 0 \end{bmatrix}$$

The entries in  $A$  are from the set  $\mathbb{Z}_{2m+1} \cup \{\infty_1, \dots, \infty_m\}.$  Let  $A_i$  be the array obtained from  $A$  by adding  $i$  to each entry, where  $i + \infty_j = \infty_j$  for all  $j = 1, 2, \dots, m.$  Let  $B$  be an  $\text{OA}(4, m),$  which exists if  $N_{\text{MOLS}}(m) \geq 2.$  Let  $C$  be the matrix of constant columns:

$$C = \begin{bmatrix} 0 & 1 & \cdots & 2m \\ 0 & 1 & \cdots & 2m \\ 0 & 1 & \cdots & 2m \\ 0 & 1 & \cdots & 2m \end{bmatrix}$$

Show that the array

$$D = [A_0, A_1, A_2, \dots, A_{2m}, B, C]$$

is an  $\text{OA}(4, 3m + 1).$  Conclude that the following Theorem is true.

**Theorem 7.41.** *If  $N_{\text{MOLS}}(m) \geq 2,$  then  $N_{\text{MOLS}}(3m + 1) \geq 2.$*

Note that in particular  $N_{\text{MOLS}}(10) \geq 2.$  and  $N_{\text{MOLS}}(22) \geq 2.$

4. Take a projective plane of order  $q,$  where  $q$  is a prime power, and delete all the points on a fixed line to obtain a PBD of type  $2-(q^2, q, 1).$  Delete an additional point to obtain a PBD of type  $2-(q^2 - 1, \{q, q - 1\}, 1)$  in which the blocks of size  $q - 1$  form a clear set. Deduce that

$$N_{\text{MOLS}}(q^2 - 1) \geq N_{\text{MOLS}}(q - 1)$$

for all prime powers  $q.$  What does this say about  $N_{\text{MOLS}}(24)?$

5. Let

$$A = \begin{bmatrix} 0 & 1 & 2 & 3 & 4 & 5 \\ 1 & 2 & 3 & 4 & 5 & 0 \\ 2 & 3 & 4 & 5 & 0 & 1 \\ 3 & 4 & 5 & 0 & 1 & 2 \\ 4 & 5 & 0 & 1 & 2 & 3 \\ 3 & 4 & 5 & 0 & 1 & 2 \\ 4 & 5 & 0 & 1 & 2 & 3 \\ 5 & 0 & 1 & 2 & 3 & 4 \end{bmatrix}$$

and  $B = A + 6J$ , where  $J$  is the 6 by 6 matrix of 1s. Define

$$L_1 = \begin{bmatrix} A & B \\ B & A \end{bmatrix}$$

and obtain  $L_2, \dots, L_5$  from  $L_1$  by permuting the columns of  $L_1$  so that

- $L_2$  has first row  $[0, 6, 8, 2, 7, 1, 9, 11, 4, 10, 5, 3]$ ,
- $L_3$  has first row  $[0, 3, 6, 1, 9, 11, 2, 8, 5, 4, 7, 10]$ ,
- $L_4$  has first row  $[0, 8, 1, 11, 5, 9, 3, 10, 2, 7, 6, 4]$ ,
- $L_5$  has first row  $[0, 4, 11, 10, 2, 7, 8, 6, 9, 1, 3, 5]$ .

Show that  $L_1, L_2, L_3, L_4, L_5$  are mutually orthogonal and conclude that  $N_{\text{MOLS}}(12) \geq 5$ .

6. Let

$$\begin{aligned} \vec{w} &= [0, 0, 0, 0] \\ \vec{x} &= [1, 3, 4, 6] \\ \vec{y} &= [x_1, x_2, x_1, 5] \\ \vec{z} &= [9, 4, 6, 2] \end{aligned}$$

and

$$A_0 = \begin{bmatrix} \vec{w} & \vec{z} & \vec{y} & \vec{x} \\ \vec{x} & \vec{w} & \vec{z} & \vec{y} \\ \vec{y} & \vec{x} & \vec{w} & \vec{z} \\ \vec{z} & \vec{y} & \vec{x} & \vec{w} \end{bmatrix}.$$

$A_0$  is a 4 by 16 array. For each  $i \in \mathbb{Z}_{11}$ , let  $A_i$  be the array obtained from  $A_0$  by adding  $i$  to each entry modulo 11, fixing  $x_1, x_2, x_3$ . Let  $B$  be an  $\text{OA}(4, 3)$  on  $\{x_1, x_2, x_3\}$  and let  $C$  be the array of constant columns

$$C = \begin{bmatrix} 0 & 1 & \dots & 10 \\ 0 & 1 & \dots & 10 \\ 0 & 1 & \dots & 10 \\ 0 & 1 & \dots & 10 \end{bmatrix}$$

Show that  $[A_0, A_1, \dots, A_{10}, B, C]$  is an  $\text{OA}(4, 14)$  and conclude that  $N_{\text{MOLS}}(14) \geq 2$ .

**Remark:** The 4 by 176 array  $[A_0, A_1, \dots, A_{10}]$  is an *Incomplete Orthogonal Array* (IOA) of type  $3^1 1^{11}$ . It has 1 hole of size 3 and 11 holes of size 1. We filled the hole of size 3 with an  $\text{OA}(4, 3)$  and the holes of size 1 with  $\text{OA}(4, 1)$ s to complete the IOA to an OA.

7. Let

$$\begin{aligned}\vec{w} &= [x_1, x_2, x_3, x_4, x_5, x_6, x_7, 18] \\ \vec{x} &= [0, 0, 0, 0, 0, 0, 0, 0] \\ \vec{y} &= [15, 10, 7, 8, 12, 9, 6, 2] \\ \vec{z} &= [1, 2, 4, 6, 7, 8, 10, 5]\end{aligned}$$

and

$$A_0 = \begin{bmatrix} \vec{w} & \vec{z} & \vec{y} & \vec{x} \\ \vec{x} & \vec{w} & \vec{z} & \vec{y} \\ \vec{y} & \vec{x} & \vec{w} & \vec{z} \\ \vec{z} & \vec{y} & \vec{x} & \vec{w} \end{bmatrix}.$$

$A_0$  is a 4 by 32 array. For each  $i \in \mathbb{Z}_{19}$ , let  $A_i$  be the array obtained from  $A_0$  by adding  $i$  to each entry modulo 19, fixing  $x_1, x_2, \dots, x_7$ . Let  $B$  be an  $\text{OA}(4, 7)$  on  $\{x_1, x_2, \dots, x_7\}$  and let  $C$  be the array of constant columns

$$C = \begin{bmatrix} 0 & 1 & \dots & 18 \\ 0 & 1 & \dots & 18 \\ 0 & 1 & \dots & 18 \\ 0 & 1 & \dots & 18 \end{bmatrix}$$

Show that  $[A_0, A_1, \dots, A_{18}, B, C]$  is an  $\text{OA}(4, 26)$  and conclude that  $N_{\text{MOLS}}(26) \geq 2$ .

**Remark:** The 4 by 352 array  $[A_0, A_1, \dots, A_{18}]$  is an *Incomplete Orthogonal Array* (IOA) of type  $7^1 1^{19}$ . It has 1 hole of size 7 and 19 holes of size 1. We filled the hole of size 7 with an  $\text{OA}(4, 7)$  and the holes of size 1 with  $\text{OA}(4, 1)$ s to complete the IOA to an OA.

8. Develop the base-blocks  $\{0, 7, 10, 11, 23\}$  and  $\{0, 5, 14, 20, 22\}$  to obtain 82 blocks. Show that these 82 blocks form a PBD of type  $2\text{--}(41, 5, 1)$ . Delete 3 non-collinear points to obtain a  $2\text{--}(38, \{3, 4, 5\}, 1)$  design in which the blocks of size 3 are a clear set. Now use Corollary 7.33 to show that  $N_{\text{MOLS}}(38) \geq 2$ .



**Part III**

**Miscellaneous Topics**



# Chapter 8

## Alternating Paths and Matchings

### 8.1 Introduction

Matchings arise in a variety of situations as assignment problems, in which pairs of items are to be matched together, for example, if people are to be assigned jobs, if sports teams are to be matched in a tournament, if tasks are to be assigned to processors in a computer, whenever objects or people are to be matched on a one-to-one basis.

In a graph  $G$ , a *matching*  $M$  is a set of edges such that no two edges of  $M$  have a vertex in common. Figure 8.1 illustrates two matchings  $M_1$  and  $M_2$  in a graph  $G$ .

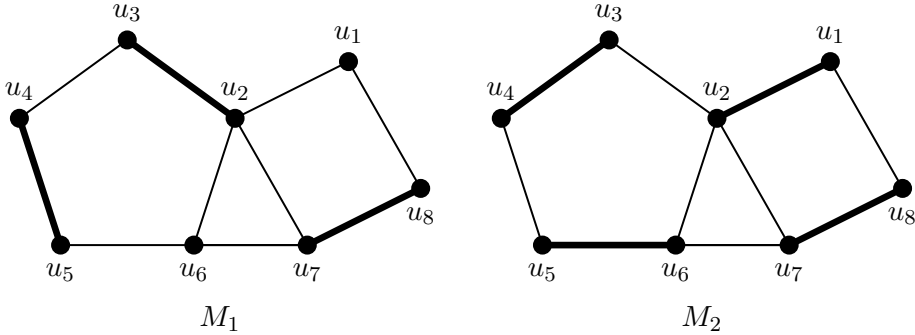


Figure 8.1: Matchings

Let  $M$  have  $m$  edges. Then  $2m$  vertices of  $G$  are matched by  $M$ . We also say that a vertex  $u$  is *saturated* by  $M$  if it is matched, and *unsaturated* if it is not matched. In general, we want  $M$  to have as many edges as possible.  $M$  is a *maximum matching* in  $G$  if no matching of  $G$  has more edges.

For example, in Figure 8.1,  $|M_1| = 3$  and  $|M_2| = 4$ . Since  $|G| = 8$ ,  $M_2$  is a maximum matching. A matching which saturates every vertex is called a *perfect matching*. Obviously a perfect matching is always a maximum matching.  $M_1$  is not a maximum matching, but it is a *maximal matching*; namely  $M_1$  cannot be extended by the addition of any edge  $uv$  of  $G$ . However, there is a way to build a bigger matching out of  $M_1$ . Let  $P$  denote the path  $(u_1, u_2, \dots, u_6)$  in Figure 8.1.

Let  $G$  have a matching  $M$ . An *alternating path*  $P$  with respect to  $M$  is any path whose edges are alternately in  $M$  and not in  $M$ . If the endpoints of  $P$  are unsaturated, then  $P$  is an *augmenting*

path.

So  $P = (u_1, u_2, \dots, u_6)$  is an augmenting path with respect to  $M_1$ . Consider the subgraph formed by the *exclusive or* operation  $M = M_1 \oplus E(P)$  (also called the *symmetric difference*,  $(M_1 - E(P)) \cup (E(P) - M_1)$ ).  $M$  contains those edges of  $P$  which are not in  $M_1$ , namely,  $u_1u_2$ ,  $u_3u_4$ , and  $u_5u_6$ .  $M$  is a bigger matching than  $M_1$ . Notice that  $M = M_2$ .

**Lemma 8.1.** *Let  $G$  have a matching  $M$ . Let  $P$  be an augmenting path with respect to  $M$ . Then  $M' = M \oplus E(P)$  is a matching with one more edge than  $M$ .*

*Proof.* Let the endpoints of  $P$  be  $u$  and  $v$ .  $M'$  has one more edge than  $M$ , since  $u$  and  $v$  are unsaturated in  $M$ , but saturated in  $M'$ . All other vertices that were saturated in  $M$  are still saturated in  $M'$ . So  $M'$  is a matching with one more edge.  $\square$

The key result in the theory of matchings is the following:

**Theorem 8.2. (Berge's theorem)** *A matching  $M$  in  $G$  is maximum if and only if  $G$  contains no augmenting path with respect to  $M$ .*

*Proof.*  $\Rightarrow$ : If  $M$  were a maximum matching and  $P$  an augmenting path, then  $M \oplus E(P)$  would be a larger matching. So there can be no augmenting path if  $M$  is maximum.

$\Leftarrow$ : Suppose that  $G$  has no augmenting path with respect to  $M$ . If  $M$  is not maximum, then pick a maximum matching  $M'$ . Clearly  $|M'| > |M|$ . Let  $H = M \oplus M'$ . Consider the subgraph of  $G$  that  $H$  defines. Each vertex  $v$  is incident on at most one  $M$ -edge and one  $M'$ -edge, so that in  $H$ ,  $\text{DEG}(v) \leq 2$ . Every path in  $H$  alternates between  $M$ -edges and  $M'$ -edges. So  $H$  consists of alternating paths and cycles, as illustrated in Figure 8.2.

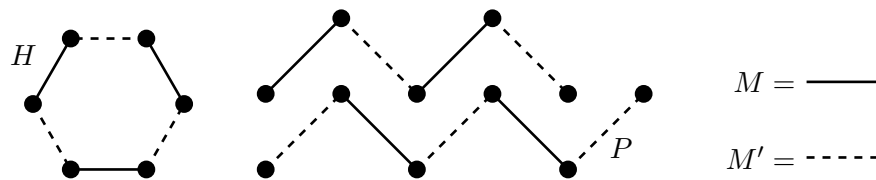


Figure 8.2: Alternating paths and cycles

Each cycle must clearly have even length, with an equal number of edges of  $M$  and  $M'$ . Since  $|M'| > |M|$ , some path  $P$  must have more  $M'$ -edges than  $M$ -edges. It can only begin and end with an  $M'$ -edge, so that  $P$  is augmenting with respect to  $M$ . But we began by assuming that  $G$  has no augmenting path for  $M$ . Consequently,  $M$  was initially a maximum matching.  $\square$

This theorem tells us how to find a maximum matching in a graph. We begin with some matching  $M$ . If  $M$  is not maximum, there will be an unsaturated vertex  $u$ . We then follow alternating paths from  $u$ . If some unsaturated vertex  $v$  is reached on an alternating path  $P$ , then  $P$  is an augmenting  $uv$ -path. Set  $M \leftarrow M \oplus E(P)$ , and repeat. If the method that we have chosen to follow alternating paths is sure to find all such paths, then this technique is guaranteed to find a maximum matching in  $G$ .

In bipartite graphs it is slightly easier to follow alternating paths and therefore to find maximum matchings, because of their special properties. Let  $G$  have bipartition  $(X, Y)$ . If  $S \subseteq X$ , then the *neighbor set* of  $S$  is  $N(S)$ , the set of  $Y$ -vertices adjacent to  $S$ . Sometimes  $N(S)$  is called the *shadow*

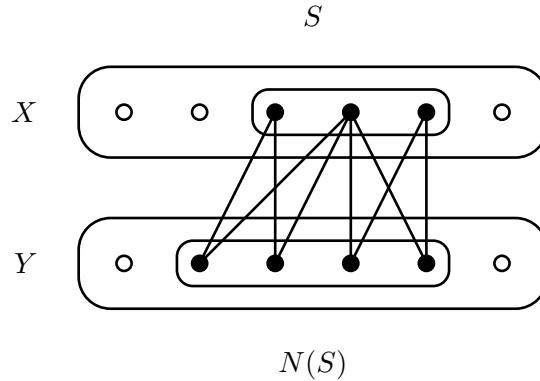


Figure 8.3: The neighbor set

set of  $S$ . If  $G$  has a perfect matching  $M$ , then every  $x \in S$  will be matched to some  $y \in Y$  so that  $|N(S)| \geq |S|$ , for every  $S \subseteq X$ . P. HALL proved that this necessary condition is also sufficient.

**Theorem 8.3. (Hall's theorem)** *Let  $G$  have bipartition  $(X, Y)$ .  $G$  has a matching saturating every  $x \in X$  if and only if  $|N(S)| \geq |S|$ , for all  $S \subseteq X$ .*

*Proof.* We have all ready discussed the necessity of the conditions. For the converse suppose that  $|N(S)| \geq |S|$ , for all  $S \subseteq X$ . If  $M$  does not saturate all of  $X$ , pick an unsaturated  $u \in X$ , and follow all the alternating paths beginning at  $u$ . (See Figure 8.4.)

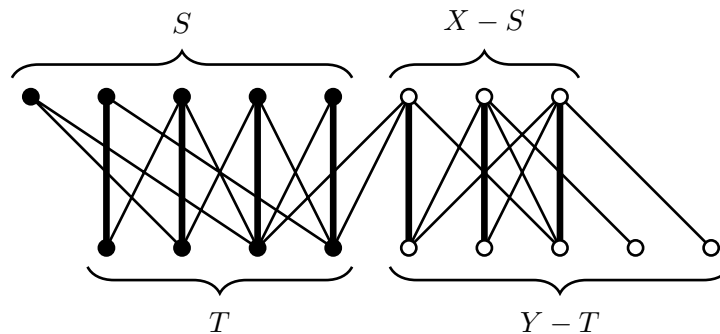


Figure 8.4: Follow alternating paths

Let  $S \subseteq X$  be the set of  $X$ -vertices reachable from  $u$  on alternating paths, and let  $T$  be the set of  $Y$ -vertices reachable. With the exception of  $u$ , each vertex  $x \in S$  is matched to some  $y \in T$ , for  $S$  was constructed by extending alternating paths from  $y \in T$  to  $x \in S$  whenever  $xy$  is a matching edge. Therefore  $|S| = |T| + 1$ .

Now there may be other vertices  $X - S$  and  $Y - T$ . However, there can be no edges  $[S, Y - T]$ , for such an edge would extend an alternating path to a vertex of  $Y - T$ , which is not reachable from  $u$  on an alternating path. So every  $x \in S$  can only be joined to vertices of  $T$ ; that is,  $T = N(S)$ . It follows that  $|S| > |N(S)|$ , a contradiction. Therefore every vertex of  $X$  must be saturated by  $M$ .  $\square$

**Corollary 8.4.** *Every  $k$ -regular bipartite graph has a perfect matching, if  $k > 0$ .*

*Proof.* Let  $G$  have bipartition  $(X, Y)$ . Since  $G$  is  $k$ -regular,  $\varepsilon = k \cdot |X| = k \cdot |Y|$ , so that  $|X| = |Y|$ . Pick any  $S \subseteq X$ . How many edges have one end in  $S$ ? Exactly  $k \cdot |S|$ . They all have their other end in  $N(S)$ . The number of edges with one endpoint in  $N(S)$  is  $k \cdot |N(S)|$ . So  $k \cdot |S| \leq k \cdot |N(S)|$ , or  $|S| \leq |N(S)|$ , for all  $S \subseteq X$ . Therefore  $G$  has a perfect matching.  $\square$

### 8.1.1 Exercises

1. Find a formula for the number of perfect matchings of  $K_{2n}$  and  $K_{n,n}$ .
2. (Hall's theorem.) Let  $A_1, A_2, \dots, A_n$  be subsets of a set  $S$ . A *system of distinct representatives* for the family  $\{A_1, A_2, \dots, A_n\}$  is a subset  $\{a_1, a_2, \dots, a_n\}$  of  $S$  such that  $a_1 \in A_1, a_2 \in A_2, \dots, a_n \in A_n$ , and  $a_i \neq a_j$ , for  $i \neq j$ . Example:

$A_1$  = students taking computer science 421

$A_2$  = students taking physics 374

$A_3$  = students taking botany 464

$A_4$  = students taking philosophy 221

The sets  $A_1, A_2, A_3, A_4$  may have many students in common. Find four distinct students  $a_1, a_2, a_3, a_4$ , such that  $a_1 \in A_1, a_2 \in A_2, a_3 \in A_3$ , and  $a_4 \in A_4$  to represent each of the four classes.

Show that  $\{A_1, A_2, \dots, A_n\}$  has a system of distinct representatives if and only if the union of every combination of  $k$  of the subsets  $A_i$  contains at least  $k$  elements, for all  $k = 1, 2, \dots, n$ . (*Hint:* Make a bipartite graph  $A_1, A_2, \dots, A_n$  versus all  $a_j \in S$ , and use Hall's theorem.)

## 8.2 Perfect matchings and 1-factorizations

Given any graph  $G$  and positive integer  $k$ , a  $k$ -factor of  $G$  is a spanning subgraph that is  $k$ -regular. Thus a perfect matching is a 1-factor. A 2-factor is a union of cycles that covers  $V(G)$ , as illustrated in Figure 8.5.

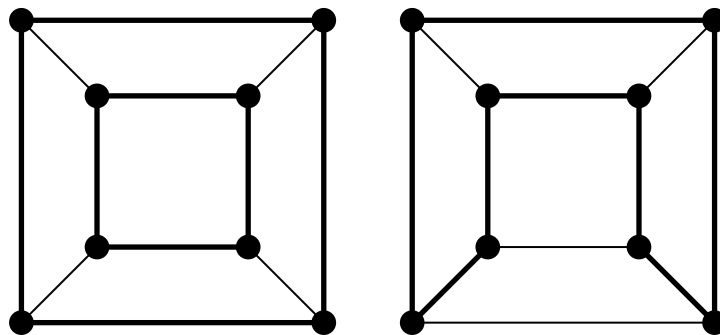


Figure 8.5: 2-factors of the cube

The reason for this terminology is as follows. Associate indeterminates  $x_1, x_2, \dots, x_n$  with the  $n$  vertices of a graph. An edge connecting vertex  $i$  to  $j$  can be represented by the expression  $x_i - x_j$ .

Then the entire graph can be represented (up to sign) by the product  $P(G) = \prod_{ij \in E(G)} (x_i - x_j)$ . For example, if  $G$  is the 4-cycle, this product becomes  $(x_1 - x_2)(x_2 - x_3)(x_3 - x_4)(x_4 - x_1)$ . Since the number of terms in the product is  $\varepsilon(G)$ , when it is multiplied out, there will be  $\varepsilon$   $x$ 's in each term. A 1-factor of  $P(G)$ , for example,  $(x_1 - x_2)(x_3 - x_4)$ , is a factor that contains each  $x_i$  exactly once. This will always correspond to a perfect matching in  $G$ , and so on.

With some graphs it is possible to decompose the edge set into perfect matchings. For example, if  $G$  is the cube, we can write  $E(G) = M_1 \cup M_2 \cup M_3$ , where  $M_1 = \{12, 34, 67, 85\}$ ,  $M_2 = \{23, 14, 56, 78\}$ , and  $M_3 = \{15, 26, 37, 48\}$ , as shown in Figure 8.6. Each edge of  $G$  is in *exactly one* of  $M_1$ ,  $M_2$ , or  $M_3$ .

In general, a  $k$ -factorization of a graph  $G$  is a decomposition of  $E(G)$  into  $H_1 \cup H_2 \cup \dots \cup H_m$ , where each  $H_i$  is a  $k$ -factor, and each  $H_i$  and  $H_j$  have no edges in common. The above decomposition of the cube is a 1-factorization. Therefore we say the cube is 1-factorable.

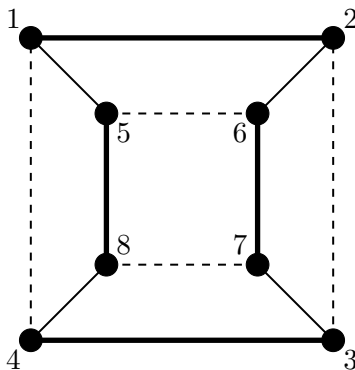


Figure 8.6: A 1-factorization of the cube

**Lemma 8.5.**  $K_{n,n}$  is 1-factorable.

*Proof.* Let  $(X, Y)$  be the bipartition of  $K_{n,n}$ , where  $X = \{x_0, x_1, \dots, x_{n-1}\}$  and  $Y = \{y_0, y_1, \dots, y_{n-1}\}$ . Define  $M_0 = \{x_i y_i \mid i = 0, 1, \dots, n-1\}$ ,  $M_1 = \{x_i y_{i+1} \mid i = 0, 1, \dots, n-1\}$ , etc., where the addition is modulo  $n$ . In general  $M_k = \{x_i y_{i+k} \mid i = 0, 1, \dots, n-1\}$ . Clearly  $M_j$  and  $M_k$  have no edges in common, for any  $j$  and  $k$ , and together  $M_0, M_1, \dots, M_{n-1}$  contain all of  $E(G)$ . Thus we have a 1-factorization of  $K_{n,n}$ .  $\square$

**Lemma 8.6.**  $K_{2n}$  is 1-factorable.

*Proof.* Let  $V(K_{2n}) = \{0, 1, 2, \dots, 2n-2\} \cup \{\infty\}$ . Draw  $K_{2n}$  with the vertices  $0, 1, \dots, 2n-2$  in a circle, placing  $\infty$  in the center of the circle. This is illustrated for  $n = 4$  in Figure 8.7. Take  $M_0 = \{(0, \infty), (1, 2n-2), (2, 2n-3), \dots, (n-1, n)\} = \{(0, \infty)\} \cup \{(i, -i) \mid i = 1, 2, \dots, n-1\}$ , where the addition is modulo  $2n-1$ .  $M_0$  is illustrated by the thicker lines in Figure 8.7.

We can then “rotate”  $M_0$  by adding one to each vertex,  $M_1 = M_0 + 1 = \{(i+1, j+1) \mid (i, j) \in M_0\}$ , where  $\infty + 1 = \infty$ , and addition is modulo  $2n-1$ . It is easy to see from the diagram that  $M_0$  and  $M_1$  have no edges in common. Continuing like this, we have

$$M_0, M_1, M_2, \dots, M_{2n-2},$$

where  $M_k = M_0 + k$ . They form a 1-factorization of  $K_{2n}$ .  $\square$

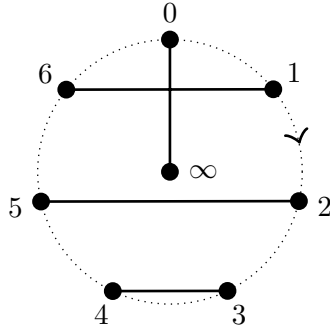


Figure 8.7: 1-factorizing  $K_{2n}$ , where  $n = 4$

We can use a similar technique to find a 2-factorization of  $K_{2n+1}$ .

**Lemma 8.7.**  $K_{2n+1}$  is 2-factorable.

*Proof.* Let  $V(K_{2n+1}) = \{0, 1, 2, \dots, 2n - 1\} \cup \{\infty\}$ . As in the previous lemma, draw the graph with the vertices in a circle, placing  $\infty$  in the center. The first 2-factor is the cycle  $H_0 = (0, 1, -1, 2, -2, \dots, n - 1, n + 1, n, \infty)$ , where the arithmetic is modulo  $2n$ . This is illustrated in Figure 8.8, with  $n = 3$ . We then rotate the cycle to get  $H_1, H_2, \dots, H_{n-1}$ , giving a 2-factorization of  $K_{2n+1}$ .  $\square$

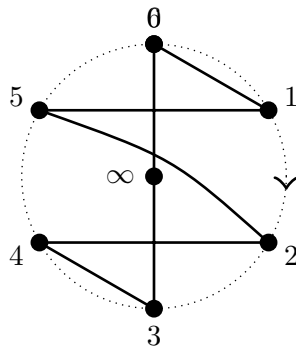


Figure 8.8: 2-factorizing  $K_{2n+1}$ , where  $n = 3$

### 8.2.1 Exercises

1. Find all perfect matchings of the cube. Find all of its 1-factorizations.
2. Find all perfect matchings and 1-factorizations of  $K_4$  and  $K_6$ .
3. Prove that the Petersen graph has no 1-factorization.
4. Prove that for  $k > 0$  every  $k$ -regular bipartite graph is 1-factorable.



5. Describe another 1-factorization of  $K_{2n}$ , when  $n$  is even, using the fact that  $K_{n,n}$  is a subgraph of  $K_{2n}$ .
6. Let  $M_1, M_2, \dots, M_k$  and  $M'_1, M'_2, \dots, M'_k$  be two 1-factorizations of a  $k$ -regular graph  $G$ . The two factorizations are isomorphic if there is an automorphism  $\theta$  of  $G$  such that for each  $i$ ,  $\theta(M_i) = M'_j$ , for some  $j$ ; that is,  $\theta$  induces a mapping of  $M_1, M_2, \dots, M_k$  onto  $M'_1, M'_2, \dots, M'_k$ . How many non-isomorphic 1-factorizations are there of  $K_4$  and  $K_6$ ?
7. How many non-isomorphic 1-factorizations are there of the cube?

### 8.3 Tutte's theorem

Tutte's theorem gives a necessary and sufficient condition for any graph to have a perfect matching.

Let  $S \subseteq V(G)$ . In general,  $G - S$  may have several connected components. Write  $\text{odd}(G - S)$  for the number of components with an odd number of vertices. The following proof of Tutte's theorem is due to LOVÁSZ

**Theorem 8.8. (Tutte's theorem)** *A graph  $G$  has a perfect matching if and only if  $\text{odd}(G - S) \leq |S|$ , for every subset  $S \subseteq V(G)$ .*

*Proof.*  $\Rightarrow$ : Suppose that  $G$  has a perfect matching  $M$  and pick any  $S \subseteq V(G)$ . Let  $G_1, G_2, \dots, G_m$  be the odd components of  $G - S$ . Each  $G_i$  contains at least one vertex matched by  $M$  to a vertex of  $S$ . Therefore  $\text{odd}(G - S) = m \leq |S|$ . See Figure 8.9.

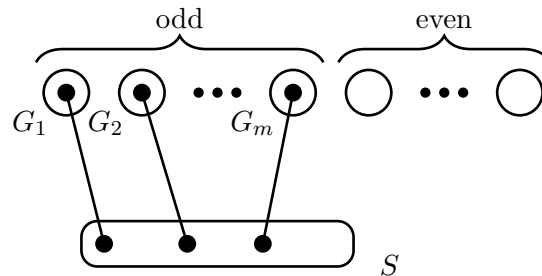


Figure 8.9: Odd and even components of  $G - S$

$\Leftarrow$ : Suppose that  $\text{odd}(G - S) = m \leq |S|$ , for every  $S \subseteq V(G)$ . Taking  $S = \emptyset$  gives  $\text{odd}(G) = 0$ , so  $n = |G|$  is even. The proof is by reverse induction on  $\varepsilon(G)$ , for any given  $n$ . If  $G$  is the complete graph, it is clear that  $G$  has a perfect matching, so the result holds when  $\varepsilon = \binom{n}{2}$ . Let  $G$  be a graph with the largest  $\varepsilon$  such that  $G$  has no perfect matching. If  $uv \notin E(G)$ , then because  $G + uv$  has more edges than  $G$ , it must be that  $G + uv$  has a perfect matching. Let  $S$  be the set of all vertices of  $G$  of degree  $n - 1$ , and let  $G'$  be any connected component of  $G - S$ . If  $G'$  is not a complete graph, then it contains three vertices  $x, y, z$  such that  $x$  adjacent to  $y$ ,  $y$  is adjacent to  $z$ , but  $x$  is not adjacent to  $z$ . Since  $y \notin S$ ,  $\deg(y) < n - 1$ , so there is a vertex  $w$  that is not adjacent to  $y$ . Let  $M_1$  be a perfect matching of  $G + xz$  and let  $M_2$  be a perfect matching of  $G + yw$ , as shown in Figures 8.10 and 8.11. Then  $xz \in M_1$  and  $yw \in M_2$ . Let  $H = M_1 \oplus M_2$ .  $H$  consists of one or more alternating cycles in  $G$ . Let  $C_{xz}$  be the cycle of  $H$  containing  $xz$  and let  $C_{yw}$  be the cycle containing  $yw$ .

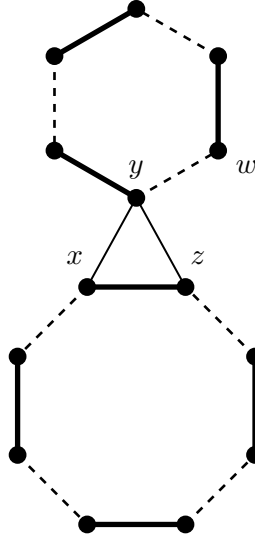


Figure 8.10:  $H = M_1 \oplus M_2$ , case 1

**Case 1.**  $C_{xz} \neq C_{yw}$ .

Form a new matching  $M$  by taking  $M_2$ -edges of  $C_{xz}$ ,  $M_1$ -edges of  $C_{yw}$ , and  $M_1$  edges elsewhere. Then  $M$  is a perfect matching of  $G$ , a contradiction.

**Case 2.**  $C_{xz} = C_{yw} = C$ .

$C$  can be traversed in two possible directions. Beginning with the vertices  $y, w$ , we either come to  $x$  first or  $z$  first. Suppose it is  $z$ . Form a new matching  $M$  by taking  $M_1$ -edges between  $w$  and  $z$ ,  $M_2$ -edges between  $x$  and  $y$ , and the edge  $yz$ . Then take  $M_1$  edges elsewhere. Again  $M$  is a perfect matching of  $G$ , a contradiction.

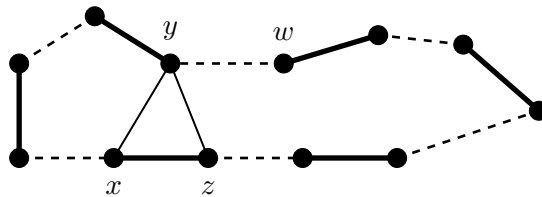


Figure 8.11:  $H = M_1 \oplus M_2$ , case 2

We conclude that every component  $G'$  of  $G - S$  must be a complete graph. But then we can easily construct a perfect matching of  $G$  as follows. Each even component of  $G - S$  is a complete graph, so it has a perfect matching. Every odd component is also a complete graph, so it has a near perfect matching, namely, one vertex is not matched. This vertex can be matched to a vertex of  $S$ , since  $\text{odd}(G - S) \leq |S|$ . The remaining vertices of  $S$  form a complete subgraph, since they have degree  $n - 1$ , so they also have a perfect matching. It follows that every  $G$  satisfying the condition of the theorem has a perfect matching.  $\square$

Tutte's theorem is a powerful criterion for the existence of a perfect matching. For example, the following graph has no perfect matching, since  $G - v$  has three odd components.

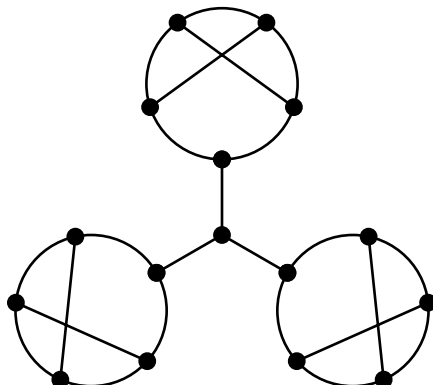


Figure 8.12: A 3-regular graph with no perfect matching

We can use Tutte's theorem to prove that every 3-regular graph  $G$  without cut-edges has a perfect matching. Let  $S \subseteq V(G)$  be any subset of the vertices. Let  $G_1, G_2, \dots, G_k$  be the odd components of  $G - S$ . Let  $m_i$  be the number of edges connecting  $G_i$  to  $S$ . Then  $m_i > 1$ , since  $G$  has no cut-edge. Since  $\sum_{v \in G_i} \text{DEG}(v) = 2\varepsilon(G_i) + m_i = 3|G_i| = \text{an odd number}$ , we conclude that  $m_i$  is odd. Therefore  $m_i \geq 3$ , for each  $i$ . But  $\sum_{v \in S} \text{DEG}(v) = 3|S| \geq \sum_i m_i$ , since all of the  $m_i$  edges have one endpoint in  $S$ . It follows that  $3|S| \geq 3k$ , or  $|S| \geq \text{odd}(G - S)$ , for all  $S \subseteq V(G)$ . Therefore  $G$  has a perfect matching  $M$ .  $G$  also has a 2-factor, since  $G - M$  has degree two.

### 8.3.1 Exercises

1. For each integer  $k > 1$ , find a  $k$ -regular graph with no perfect matching.
2. A *near perfect matching* in a graph  $G$  is a matching which saturates all vertices of  $G$  but one. A *near 1-factorization* is a decomposition of  $E(G)$  into near perfect matchings. Prove that  $K_{2n+1}$  has a near 1-factorization.
3. Find a condition similar to Tutte's theorem for a graph to have a near perfect matching.

## 8.4 The 4-color problem

Given a geographic map drawn in the plane, how many colors are needed such that the map can be colored so that any two regions sharing a common border have different colors? In 1852, it was conjectured by Francis Guthrie that four colors suffice. This simple problem turned out to be very difficult to solve. Several flawed “proofs” were presented. Much of the development of graph theory originated in attempts to solve this conjecture. See AIGNER [?] for a development of graph theory based on the 4-color problem. In 1976, Appel and Haken announced a proof of the conjecture. Their proof was based on the results of a computer program that had to be guaranteed bug-free. A second computer proof by ALLAIRE [?] appeared in 1977. Each of these approaches relied on showing that any planar graph contains one of a number of configurations, and that for each configuration, a proper coloring of a smaller (reduced) graph can be extended to a proper coloring of the initial graph. The computer programs generated all irreducible configurations, and colored them. In the Appel-Haken proof, there were approximately 1800 irreducible configurations. The uncertainty was whether all irreducible configurations had indeed been correctly generated. In 1995, ROBERTSON, SANDERS, SEYMOUR, and THOMAS [?] presented another proof, also based on a computer program, but considerably simpler than the original, requiring only 633 irreducible configurations.

In this section, we present the main ideas of Kempe’s 1879 “proof” of the 4-color theorem.

Given a geographic map drawn in the plane, one can construct a dual graph, by placing a vertex in the interior of each region, and joining vertices by edges if they correspond to adjacent regions. Coloring the regions of the map is then equivalent to coloring the vertices of the dual, so that adjacent vertices are of different colors. Consequently, we shall be concerned with coloring the vertices of a planar graph.

**Theorem 8.9. (4-Color theorem)** *Every planar graph can be properly colored with four colors.*

If  $G$  is any simple planar graph, then it is always possible to extend  $G$  to a simple triangulation, by adding diagonal edges in non-triangular faces. Therefore, if we can prove that all simple planar triangulations are 4-colorable, the result will be true for all planar graphs. Hence we assume that we are given a planar triangulation  $G_n$  on  $n$  vertices. We attempt to prove the 4-color theorem (Theorem 8.9) by induction on  $n$ .

The colors can be chosen as the numbers  $\{1, 2, 3, 4\}$ . Given a coloring of  $G$ , then the subgraph induced by any two colors  $i$  and  $j$  is bipartite. We denote it by  $K^{ij}$ .

**Definition:** Given any 4-coloring of a planar graph  $G$ , each connected component of  $K^{ij}$  is called a *Kempe component*. The component containing a vertex  $x$  is denoted  $K^{ij}(x)$ . A path in  $K^{ij}$  between vertices  $u$  and  $v$  is called a *Kempe chain*.

Notice that if we interchange the colors  $i$  and  $j$  in any Kempe component, we obtain another coloring of  $G$ .

Now let  $G_n$  be a simple triangulation on  $n$  vertices. If  $n = 4$ , then  $G_n = K_4$ . It is clear that Theorem 8.9 is true in this case. Assume that  $n > 4$ . By Corollary 2.6, we know that  $G_n$  has a vertex of degree three, four, or five. Let  $u$  be such a vertex. We reduce  $G_n$  to a simple planar triangulation  $G_{n-1}$  by deleting  $u$  and adding up to two diagonals in the resulting face. Thus we may assume as an induction hypothesis, that  $G_{n-1}$  has a 4-coloring. There are three cases.

**Case 1.**  $\text{DEG}(u) = 3$ .

Let the three adjacent vertices to  $u$  be  $(x, y, z)$ . They all have different colors. Therefore there is a fourth color available for  $v$ , giving a coloring of  $G_n$ .

**Case 2.**  $\text{DEG}(u) = 4$ .

Let the four vertices adjacent to  $u$  in  $G_n$  be  $(w, x, y, z)$ , with a diagonal  $wy$  in  $G_{n-1}$ . It is clear that  $w, x$ , and  $y$  have different colors. If  $x$  and  $z$  have the same color, then a fourth color is available for  $u$ . Otherwise, let  $w, x, y, z$  be colored 1, 2, 3, 4, respectively. There may be a Kempe chain from  $x$  to  $z$ . If there is no Kempe chain, interchange colors in the Kempe component  $K^{24}(x)$ , so that  $x$  and  $z$  now both have color 4. If there is a Kempe chain from  $x$  to  $z$ , there can be no Kempe chain from  $w$  to  $y$ , for it would have to intersect the  $xz$ -Kempe chain. Interchange colors in  $K^{13}(w)$ , so that  $w$  and  $z$  now both have color 3. In each case there is a fourth color available for  $u$ .

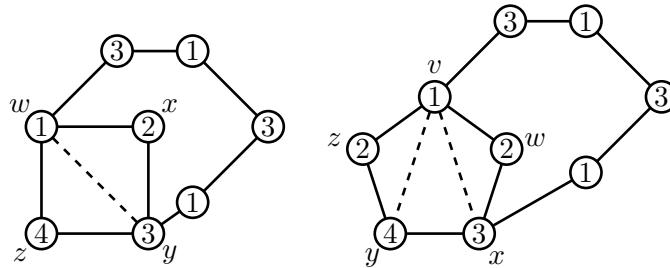


Figure 8.13: Kempe chains

**Case 3.**  $\text{DEG}(u) = 5$ .

Let the five vertices adjacent to  $u$  in  $G_n$  be  $(v, w, x, y, z)$ , with diagonals  $vx$  and  $vy$  in  $G_{n-1}$ . It is clear that  $v, x$ , and  $y$  have different colors. Since we have a 4-coloring of  $G_{n-1}$ , the pentagon  $(v, w, x, y, z)$  is colored in either 3 or 4 colors. If it is colored in three colors, there is a fourth color available for  $u$ . If it is colored in four colors, then without loss of generality, we can take these colors to be  $(1, 2, 3, 4, 2)$ , respectively. If  $K^{13}(v)$  contains no  $vx$ -Kempe chain, then we can interchange colors in  $K^{13}(v)$ , so that  $v$  and  $x$  are now both colored 3. Color 1 is then available for  $u$ . If  $K^{14}(v)$  contains no  $vy$ -Kempe chain, then we can interchange colors in  $K^{14}(v)$ , so that  $v$  and  $y$  are now both colored 4. Color 1 is again available for  $u$ . Otherwise there is a Kempe chain  $P_{vx}$  connecting  $v$  to  $x$  and a Kempe chain  $P_{vy}$  connecting  $v$  to  $y$ . It follows that  $K^{24}(w)$  contains no  $wy$ -Kempe chain, as it would have to intersect  $P_{vx}$  in  $K^{13}(v)$ . Similarly,  $K^{23}(z)$  contains no  $vz$ -Kempe chain, as it would have to intersect  $P_{vy}$  in  $K^{14}(v)$ . If  $P_{vx}$  and  $P_{vy}$  intersect only in vertex  $v$ , then we can interchange colors in both  $K^{24}(w)$  and  $K^{23}(z)$ , thereby giving  $w$  color 4 and  $z$  color 3. This makes color 2 available for  $u$ . The difficulty is that  $P_{vx}$  and  $P_{vy}$  can intersect in several vertices. Interchanging colors in  $K^{24}(w)$  can affect the other Kempe chains, as shown in Figure ??, where the pentagon  $(v, w, x, y, z)$  is drawn as the outer face.

Although this attempted proof of Theorem 8.9 fails at this point, we can use these same ideas to prove the following.

**Theorem 8.10. (5-Color theorem)** *Any planar graph can be colored in five colors.*

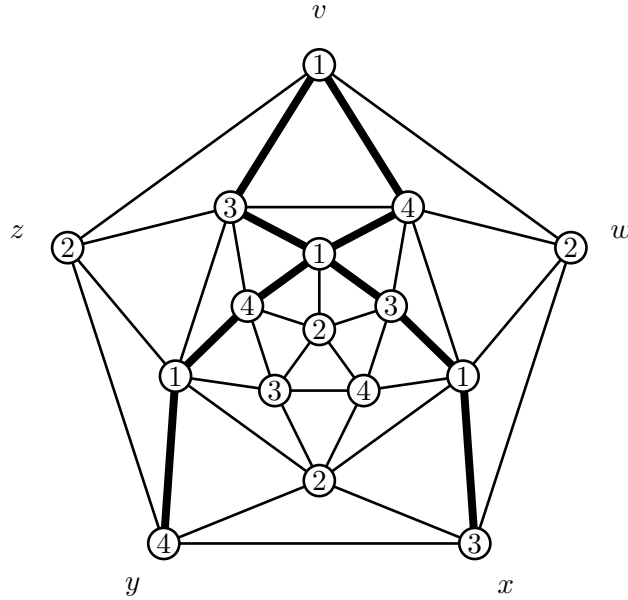


Figure 8.14: Intersecting Kempe chains

*Proof.* See Exercise 8.4.1. □

Appel and Haken's proof of the 4-color theorem is based on the important concept of *reducibility*. Given a graph  $G$ , a *reducible configuration*  $H$  is a subgraph of  $G$  with the property that  $H$  can be reduced to a smaller subgraph  $H'$ , such that a 4-coloring of  $H'$  can be extended to all of  $H$  and  $G$ . If every planar graph contained a reducible configuration, then every planar graph could be 4-colored. Appel and Haken's proof was essentially a computer program to construct all irreducible configurations, and to show that they could be 4-colored. The difficulty with this approach is being certain that the computer program is correctly constructing all irreducible configurations. The reader is referred to SAATY and KAINEN [?] or WOODALL and WILSON [?] for more information on reducibility.

### 8.4.1 Exercises

1. Prove Theorem 8.10, the 5-color theorem.
2. Let  $G$  be a planar triangulation with a separating 3-cycle  $(u, v, w)$ . Let  $H$  and  $K$  be the two connected subgraphs of  $G$  that intersect in exactly  $(u, v, w)$ , such that  $G = H \cup K$ . Show how to construct a 4-coloring of  $G$  from 4-colorings of  $H$  and  $K$ .
3. Let  $G$  be a planar triangulation with a separating 4-cycle  $(u, v, w, x)$ . Let  $H$  and  $K$  be the two connected subgraphs of  $G$  that intersect in exactly  $(u, v, w, x)$ , such that  $G = H \cup K$ . Show how to construct a 4-coloring of  $G$  from 4-colorings of the triangulations  $H + uw$  and  $K + uw$ . *Hint:*  $u$ ,  $v$ , and  $w$  can be assumed to have the same colors in  $H$  and  $K$ . If  $x$  is colored differently in  $H$  and  $K$ , look for an  $xv$ -Kempe chain, try interchanging colors in  $K^{ij}(x)$ , or try coloring  $H + vx$  and  $K + vx$ .

4. All lakes are blue. Usually all bodies of water are colored blue on a map. Construct a planar graph with two non-adjacent vertices that must be blue, such that the graph cannot be colored in four colors subject to this requirement.

# Index

- $A_G$ , 33
- $C_n$ , 8
- $E(G)$ , 5
- $F(G)$ , 22
- $G[U]$ , 5
- $J_n$ , 35
- $L(G)$ , 39
- $P_n$ , 8
- $T(G)$ , 13
- $V(G)$ , 5
- $X_G$ , 39
- $\Delta(G)$ , 5
- EXT( $J$ ), 21
- INT( $J$ ), 21
- STS, 52
- TD( $k, n$ ), 71
- Alg( $G$ ), 36
- AVGDEG( $G$ ), 4
- $\chi_G(\lambda)$ , 33
- DEG( $x$ ), 3
- $\delta(G)$ , 4
- DIAM( $G$ ), 9
- DIST( $x, y$ ), 9
- $\mathbb{F}_q$ , 69
- $\epsilon(G)$ , 5
- EXT( $J$ ), 21
- INT( $J$ ), 21
- $\kappa(G)$ , 11
- $\kappa G$ , 43
- $\lambda(G)$ , 11
- $\mu_A(x)$ , 37
- $\vec{1}$ , 35
- $g(G)$ , 9
- $k$ -factor, 90
- $k$ -factorization, 91
  
- acyclic, 14
- adjacency algebra, 36
  
- adjacency matrix, 33
- adjacent, 3
- algebraic multiplicity, 33
- alternating path, 87
- articulation point, 11
- augmenting path, 88
- automorphism, 6
- automorphism group, 6
- average degree, 4
  
- Berge's theorem, 88
- bipartite, 16
- blocks, 28, 72, 77
- Bose Construction, 54
- bridge, 11
  
- characteristic polynomial, 33
- Chekad and Ernie problem, 13
- circuit, 8
- circulant graph, 51
- clear set, 78
- closed walk, 8
- column magic, 61
- commutative Latin square, 54
- complete, 16
- complete graph, 3
- connectivity, 11
- contract, 27
- Cube, 26
- cube, 9
- cut vertex, 11
- cycle, 8
  
- decomposition, 49
- degree, 3
- degree sequence, 7
- diameter, 9
- distance, 9
- Dodecahedron, 26



doubling construction, 52  
 edge connected, 11  
 edge connectivity, 11  
 edges, 3  
 embeddable, 21  
 empty graph, 5  
 Euler trail, 17  
 Eulerian, 17  
 F-factorization, 51  
 factor, 49  
 factorization, 49  
 field, 69  
 finite field, 69  
 five-color theorem, 97  
 forest, 14  
 four-color theorem, 96  
 girth, 9  
 graph, 3  
 groups, 72  
 half-idempotent Latin Square, 55  
 Hall's theorem, 89  
 homeomorphic, 27  
 Icosahedron, 26  
 idempotent Latin square, 54  
 incidence matrix, 39, 41  
 incident, 3  
 Incomplete Orthogonal Array, 83, 84  
 induced, 5  
 induced subgraph, 5  
 isomorphic graphs, 6  
 isomorphism, 6  
 Jordan curve, 21  
 Jordan curve theorem, 21  
 k-connected, 11  
 k-matching, 50  
 Kempe, 96  
 Kempe chain, 96  
 Kuratowski's theorem, 29  
 Latin square, 54  
 Linear space, 77  
 lines, 73  
 magic square, 59  
 magic sum, 59  
 matching, 87  
 maximal matching, 87  
 maximum degree, 5  
 maximum matching, 87  
 minimum degree, 4  
 minor, 27  
 MOOLS, 69  
 multiply construction, 53  
 mutual orthogonal Latin squares, 69  
 near 1-factorization, 95  
 near perfect matching, 95  
 neighbor set, 88  
 number of edges per vertex, 5  
 Octahedron, 26  
 order, 74  
 orthogonal array, 71  
 orthogonal Latin squares, 61, 69  
 pairwise balanced design, 77  
 parallel class, 78  
 partite, 16  
 path, 8  
 perfect matching, 87  
 Petersen graph, 9  
 planar, 21  
 plane, 21  
 platonic graph, 25  
 platonic solid, 24  
 pointless, 5  
 points, 52, 73, 77  
 principle minor, 34  
 projective plane, 73  
 r-factor, 49  
 r-factorization, 49  
 r-partite, 16  
 reducibility, 98  
 reducible configuration, 98  
 row magic, 61  
 saturated, 87

separable, 28  
separates, 11  
separating set, 11  
shadow set, 89  
spanning subgraph, 5  
spectrum, 33  
star, 16  
Steiner pairwise balanced design, 77  
Steiner triple system, 52  
stereographic projection, 24  
subdivided, 27  
subdivision, 27  
subgraph, 5  
symmetric difference, 88  
system of distinct representatives, 90

Tetrahedron, 26  
topologically equivalent, 27  
trail, 8  
transversal design, 71  
transverse, 72  
tree, 14  
triples, 52  
Tutte's theorem, 93

unsaturated, 87

vector space construction, 53  
vertex connectivity, 11  
vertices, 3

walk, 7