Chapter 2: Matching Theory

Thomas Britz

Hall's Marriage Theorem

The Marriage Theorem
In a little traditional village, some girls are to be married monogamously to some boys.
How many of the girls can get married? A set of girls can get married a boy if and only if each k-subset of these girls together like at least k boys.

Definition. Let $\mathcal{A} = \{A_i\}_{i\in I}$ be a finite family of sets.
A *matching* of $\mathcal{A}$ is a set of distinct elements $\{a_i\}_{i\in I}$ with $a_i \in A_i$ for all $i \in I$.

Notation. Set $\mathcal{A}(J) = \bigcup_{i\in J} A_i$ for all $J \subseteq I$.

Example. Let $\mathcal{A} = \{A_1, A_2\}$, where $A_1 = \{1, 2\}$ and $A_2 = \{2, 4\}$.
Then $\mathcal{A}(\{1\}) = A_1 = \{1, 2\}$ and $\mathcal{A}(\{1, 2\}) = \{1, 2, 4\}$.

This notation allows us to rewrite the Marriage Theorem (also called *Hall's Theorem*) as follows.

Theorem (Frobenius 1917, Hall 1935)
$\mathcal{A}$ has a matching if and only if $|\mathcal{A}(J)| \geq |J|$ for all $J \subseteq I$.

Proof. If $|\mathcal{A}(J)| < |J|$ for some $J \subseteq I$, then $\mathcal{A}$ has no matching.
Suppose therefore that $|\mathcal{A}(J)| \geq |J|$ for all $J \subseteq I$.

If $|A_{i_0}| \geq 2$ for some $i_0 \in I$, then let x and y be distinct elements of A_{i_0}.
Assume that we cannot remove x or y from A_{i_0} without violating the inequality in the theorem.
Then there are subsets I_x, $I_y \subseteq I - i_0$ so that

$$|\mathcal{A}(I_x) \cup (A_{i_0} - \{x\})| \leq |I_x| \text{ and}$$
$$|\mathcal{A}(I_y) \cup (A_{i_0} - \{y\})| \leq |I_y| .$$

Thus,

$$\begin{aligned} |I_x| + |I_y| &\geq |\mathcal{A}(I_x) \cup (A_{i_0} - \{x\})| + |\mathcal{A}(I_y) \cup (A_{i_0} - \{y\})| \\ &\geq |\mathcal{A}(I_x) \cup (A_{i_0} - x) \cup \mathcal{A}(I_y) \cup (A_{i_0} - y)| + |\mathcal{A}(I_x) \cap \mathcal{A}(I_y)| \\ &\geq |\mathcal{A}(I_x \cup I_y \cup \{i_0\})| + |\mathcal{A}(I_x \cap I_y)| \\ &\geq |I_x \cup I_y| + 1 + |I_x \cap I_y| \\ &= |I_x| + |I_y| + 1 , \end{aligned}$$

which is a contradiction.

We can therefore remove elements from the sets A_i while preserving the inequality in the theorem until $A_i = \{a_i\}$ for some a_i for each $i \in I$. Then $|\{a_i\}_{i\in I}| = |\mathcal{A}(I)| \geq |I|$. Hence, the elements a_i are distinct, so $\{a_i\}_{i\in I}$ is a matching of $\mathcal{A}$. □

Definition. A *partial matching* of $\mathcal{A}$ is a matching of some subfamily $\mathcal{B} \subseteq \mathcal{A}$.

Example. $\mathcal{A} = \{\{1\}, \{2\}, \{1,2\}\}$ has no matching.
However, $\mathcal{A}$ does has the following partial matchings:

$$\emptyset, \{1\}, \{2\}, \{1,2\}\,.$$

Theorem (Ore 1955)
$\mathcal{A}$ has a partial matching of size k if and only if, for all $J \subseteq I$, $|\mathcal{A}(J)| \geq |J| - |I| + k$.

Proof. Let D be a set of $|I| - k$ "dummy" elements not in $\mathcal{A}(I)$. Set $\mathcal{B} = \{A_i \cup D\}_{i \in I}$.
Then $\mathcal{A}$ has a partial matching of size k if and only if $\mathcal{B}$ has a matching. For each $J \subseteq I$,

$$|\mathcal{B}(J)| = \left|\bigcup_{i \in J} A_i \cup D\right| = |\mathcal{A}(J)| + |D| = |\mathcal{A}(J)| + |I| - k\,.$$

By the Marriage Theorem, $\mathcal{B}$ has a matching if and only if $|\mathcal{B}(J)| \geq |J|$ for all $J \subseteq I$.
In other words, $\mathcal{A}$ has a partial matching of size k if and only if $|\mathcal{A}(J)| \geq |J| - |I| + k$ for all $J \subseteq I$. □

Theorem (Ore 1955)
A set B contains a partial matching of $\mathcal{A}$ of size k if and only if, for all $J \subseteq I$,

$$|\mathcal{A}(J) \cap B| \geq |J| - |I| + k\,.$$

Proof. Define $\mathcal{B} = \{A_i \cap B\}_{i \in I}$.
Then B contains a partial matching of $\mathcal{A}$ of size k if and only if $\mathcal{B}$ has a partial matching of size k.
By the previous theorem, this is true precisely when $|\mathcal{A}(J) \cap B| = |\mathcal{B}(J)| \geq |J| - |I| + k$ for all $J \subseteq I$. □

Theorem (Ore 1955)
A set B is a partial matching of $\mathcal{A}$ if and only if for all $J \subseteq I$, $|\mathcal{A}(J) \cap B| \geq |J| - |I| + |B|$.

Proof. Set $k = |B|$ in Theorem 2.1.8. □

Theorem
A set B is a partial matching of $\mathcal{A}$ if and only if, for all $A \subseteq B$, $|\{i \in I : A_i \cap A \neq \emptyset\}| \geq |A|$.

Proof. Define $\mathcal{C} = \{C_a\}_B$, where $C_a = \{i \in I : a \in A_i\}$. Now, B is a partial matching of $\mathcal{A}$ if and only if $\mathcal{C}$ has a matching. By Hall's Theorem, this is true precisely when $|\mathcal{C}(A)| \geq |A|$ for all $A \subseteq B$.
But $|\mathcal{C}(A)| = |\{i \in I : A_i \cap A \neq \emptyset\}|$, which concludes the proof. □

Let $\mathcal{A} = \{A_i\}_{i \in I}$ be a finite family of subsets of a finite set E. Consider the family $\mathcal{I}(\mathcal{A})$ of partial matchings of $\mathcal{A}$.

Example. Let $\mathcal{A} = \{\{1\}, \{2,3\}\}$. Then

$$\mathcal{I}(\mathcal{A}) = \{\emptyset, \{1\}, \{2\}, \{3\}, \{1,2\}, \{1,3\}\}\,.$$

Lemma. If $A \in \mathcal{I}(\mathcal{A})$ and $B \subseteq A$, then $B \in \mathcal{I}(\mathcal{A})$.

Definition. Let $\{z_{ai} : a \in E, i \in I\}$ be independent variables.
Define the *formal incidence matrix* $M_{\mathcal{A}} = (m_{ai})$ as follows:

$$m_{ai} := \begin{cases} z_{ai} & \text{if } a \in A_i \\ 0 & \text{if } a \notin A_i \,. \end{cases}$$

Lemma. $B \in \mathcal{I}(\mathcal{A})$ if and only if the rows of $M_{\mathcal{A}}$ indexed by B are linearly independent.

Proof. The rows of $M_{\mathcal{A}}$ indexed by B are linearly independent
if and only if they contain a non-singular square submatrix N of order $|B|$.

Such N is non-singular precisely when $\det N = \ldots + \prod_{a \in B} z_{ai_a} + \ldots \neq 0$.
This happens exactly when there is at least one nonzero term $\prod_{a \in B} z_{ai_a}$ (since the z_{ai_a} are independent variables and cannot cancel each other). This term corresponds to a partial matching B. □

Theorem
The family $\mathcal{I}(\mathcal{A})$ satisfies the following properties:

(I1) $\emptyset \in \mathcal{I}(\mathcal{A})$.

(I2) If $A \in \mathcal{I}(\mathcal{A})$ and $B \subseteq A$, then $B \in \mathcal{I}(\mathcal{A})$.

(I3) If $A, B \in \mathcal{I}(\mathcal{A})$ and $|A| < |B|$, then $A \cup \{a\} \in \mathcal{I}(\mathcal{A})$ for some $a \in B - A$.

Proof. These properties are true for any finite family of finite sets of linearly independent vectors in some vector space. The proof therefore follows from the preceding lemma. □

Since $(E, \mathcal{I}(\mathcal{A}))$ satisfies the properties (I1-3), it is a *matroid* (or *independence structure* or *combinatorial geometry*). In particular, it is a *transversal matroid*. Matroids arise in numerous ways and are very useful in combinatorics. We shall meet them again at the end of this chapter.

Corollary. The maximal partial matchings of $\mathcal{A}$ have equal size.

Proof. This follows by the third matroid property (I3). □

Corollary (Hoffman and Kuhn 1956)
A set M is contained in a matching of $\mathcal{A}$ if and only if
$\mathcal{A}$ has a matching and M is a partial matching of $\mathcal{A}$.

Proof. This also follows from the third matroid property (I3). □

König's Theorem

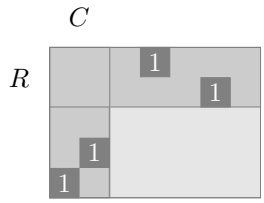
Definition. Let A be a $(0,1)$-matrix. A *line* is a row or a column.
A *partial transversal* is a set of 1-entries with no common line.

König's Theorem (1916)
The maximal size M of partial transversal in A equals
the minimal number m of lines needed to cover all 1-entires of A.

Proof. Note that $M \leq m$. We therefore only need to prove that $M \geq m$.
Let the 1s be covered by rows R and columns C where $|R| + |C| = m$.
Define $\mathcal{A}_R = \{C_i\}_R$, where $C_i = \{j \notin C : a_{ij} = 1\}$, and let $J \subseteq R$. Then $|\mathcal{A}_R(J)| \geq |J|$.
Otherwise, we could replace the rows R by fewer columns, contradicting the minimality of m.

By Hall's Theorem, $\mathcal{A}_R$ has a matching, corresponding to a partial transversal T_R of size $|R|$, that lies in rows R outside of columns C. Similarly, there is a partial transversal T_C of size $|C|$ that lies in columns C outside of rows R.

Then $T_R \cup T_C$ is a partial transversal of size $|R| + |C| = m$. Hence, $M \geq m$. □



Theorem
Hall's Theorem and König's Theorem are equivalent.

Proof. We have shown already that Hall's Theorem implies König's Theorem.
We must then prove that Hall's Theorem follows from König's Theorem.
So, let $\mathcal{A} = \{A_i\}_{i \in I}$ be a finite family of subsets of a finite set E so that $|\mathcal{A}(J)| \geq |J|$ for all $J \subseteq I$.
We now need to show that $\mathcal{A}$ has a matching.

Define $A = (m_{ia})$, where $m_{ia} = 1$ if $a \in A_i$ and $m_{ia} = 0$ otherwise.
Cover the 1s of A with rows indexed by R and columns indexed by C, with $m = |R| + |C|$ minimal.
The 1s in rows $J = I - R$ lie in columns C. Then $|C| \geq |\mathcal{A}(J)| \geq |J| = |I| - |R|$, so $m = |C| + |R| \geq |I|$.

By König's Theorem, A has a partial transversal of size $m = |I|$. That is, $\mathcal{A}$ has a matching. □

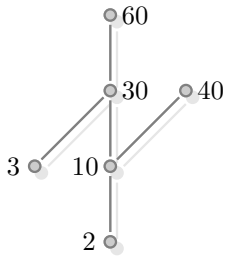
Dilworth's Theorem

Definition. A *partially ordered set* (or *poset*) is a set P with a *partial order* $\preceq$ so that, for all $x, y, z \in P$,

(R)eflexivity: $x \preceq x$.
(A)nti-symmetry: If $x \preceq y$ and $y \preceq x$, then $x = y$.
(T)ransitivity: If $x \preceq y$ and $y \preceq z$, then $x \preceq z$.

Definition. Two elements $x, y \in P$ are *comparable* if either $x \preceq y$ or $y \preceq x$.
A *chain* is a subset of elements of P whose elements are all pairwise comparable.
An *antichain* is a subset of elements of P no two elements of which are comparable.

Example.



The set $\{2, 3, 10, 30, 40, 60\}$ with $x \preceq y$ defined by $x|y$ is a poset P.
Elements 2 and 10 are comparable since $2|10$ and thus $2 \preceq 10$.
In contrast, $2 \not\preceq 3$ and $3 \not\preceq 2$, so 2 and 3 are not comparable.
The subset $\{2, 10, 30, 60\}$ is a chain in P and $\{3, 10\}$ is an antichain in P.

Dilworth's Theorem (1950)
The minimal number m of disjoint chains covering a finite poset P equals the maximal size M of an antichain.

Proof. Note that $m \geq M$. We therefore only need to prove that $m \leq M$.
Assume that the theorem holds for all posets on fewer than $|P|$ elements.
Choose a maximal chain C in P.

If every antichain in $P - C$ has at most $M - 1$ elements, then by the induction assumption, $P - C$ can be covered by $M - 1$ disjoint chains. Together with C, these chains cover P. Hence, $m \leq M$.

Suppose that A is an antichain in $P - C$ with M elements. Set

$$A^- = \{x \in P : x \preceq a \text{ for some } a \in A\}$$
$$A^+ = \{x \in P : a \preceq x \text{ for some } a \in A\}.$$

Since $|A| = M$, $P = A^- \cup A^+$. By the maximality of C, element $\max(C)$ is not in A^-. Hence, $|A^-| < |P|$.
By the induction assumption, A^- is a union of M disjoint chains C_a^- with $\max(C_a^-) = a \in A$.

Similarly, A^+ is a union of M disjoint chains C_a^+ with $\min(C_a^+) = a \in A$.
Then P is the union of the M disjoint chains $C_a^- \cup C_a^+$. Hence $m \leq M$. □

The Dual of Dilworth's Theorem (Mirsky 1971)
The minimal number m of disjoint antichains covering the poset P equals the maximal size M of a chain.

Proof. Note that $m \geq M$. We therefore only need to prove that $m \leq M$.
For each $i = 1, \ldots, M$, define

$$A_i = \{x \in P : i = \text{ the longest length of a chain starting in } x\}.$$

Then $A_1, \cdots, A_M$ are nonempty disjoint antichains that together cover P. Hence $m \leq M$. □

Note that Dilworth's Theorem is harder to prove than its dual!
This means that chains and antichains are not completely interchangeable.

Theorem
Hall's Theorem, König's Theorem, and Dilworth's Theorem are equivalent.

Proof. We have previously shown the equivalence of Hall's and König's Theorems. We must now prove that Dilworth's Theorem is equivalent to these.

Let us begin by showing that Dilworth's Theorem implies Hall's Theorem.
Let $\mathcal{A} = \{A_i\}_{i \in I}$ be a finite family of subsets of a finite set E so that $|\mathcal{A}(J)| \geq |J|$ for all $J \subseteq I$. We must show that $\mathcal{A}$ has a matching. Define the poset $P = E \cup \mathcal{A}$ with partial order $\preceq$ given by $a \prec A$ if and only if $a \in A$ ($a \in E, A \in \mathcal{A}$). Thus the chains in P have length 1 or 2.

Let $F \cup \{A_j\}_{j \in J}$ be an antichain of maximal size in P where $F \subseteq E$. By Dilworth's Theorem, P can be covered by $|F|+|J|$ disjoint chains and each of these must cover an element of $F \cup \{A_j\}_{j \in J}$. In particular, $|J|$ of these chains cover $\{A_j\}_{j \in J}$ and must also cover the elements $\mathcal{A}(J)$. Since $|\mathcal{A}(J)| \geq |J|$, we have equality, and these $|J|$ chains correspond to a matching $B_1 = \{a_j\}_{j \in J}$ of $\{A_j\}_{j \in J}$.

Similarly, $\{A_j\}_{j \in I-J}$ must be covered by chains (a, A_j) where $a \in F$. This corresponds to a matching $B_1 = \{a_j\}_{j \in I-J}$ of $\{A_j\}_{j \in I-J}$. Thus, $B_1 \cup B_2$ is a matching for $\mathcal{A} = \{A_i\}_{i \in I}$.

We now show that König's Theorem implies Dilworth's Theorem. Suppose that P is a finite poset and let $M = (m_{ab})$ be the matrix with $m_{ab} = 1$ if $a \prec b$ and $m_{ab} = 0$ otherwise.

Now, if $a \prec b \prec c \prec \cdots \prec y \prec z$ is a chain of length n in P, then the entries $m_{ab}, m_{bc}, \ldots, m_{yz}$ form a partial transversal of size $n-1$ in M. Thus, a covering of P by j chains corresponds in M to a partial transversal of size $|P| - j$. Conversely, a partial transversal of size $|P| - j$ corresponds to j chains that cover P.

Now, consider m chains that cover P, where m is minimal. This corresponds to a partial transversal in M of maximal size $|P| - m$. By König's Theorem, the 1-entries of M can be covered by $|P| - m$ lines, indexed by at most $|P| - m$ elements of P. There are thus at least m elements no indexed; these form an antichain in P. □

Applications

Definition. Let $M := (m_{ij})$ be a real $n \times n$ matrix.
A *transversal* of M is n nonzero entries with no common line.
A *permutation matrix* is a square $(0,1)$-matrix with one 1-entry in each line.

The Birkhoff-Neumann Theorem (1946, 1953)
The line sums of M all equal t if and only if, for permutation matrices P_i,

$$M = \sum_{i=1}^{m} c_i P_i \,, \qquad \text{where} \qquad \sum_{i=1}^{m} c_i = t \,.$$

Proof. If $M = \sum_i c_i P_i$ with $\sum_i c_i = t$, then all the line sums of M equal t. Therefore, suppose that each line sum of M equals t.

If M has negative entries, then let $a = \min m_{ij}$ and let $M' = M + |a| J_n$, where J_n is all-1 $n \times n$ matrix. Then each entry of M' is nonnegative and each line sum equals $t = |a|n$. Since $|a|J_n$ is a weighted sum of permutation matrices, we can assume without loss of generality, that M is nonnegative.

If $t = 0$, then $M = 0 \times P$ for any permutation matrix P, so assume $t > 0$.

Thus, suppose that $M \geq 0$ and each line sum equals $t > 0$.

We use induction on the number of nonzero entries in M.
Define $\mathcal{A} = \{A_i\}_{i \in I}$, where $A_i = \{j : m_{ij} > 0\}$ and $I = \{1, \ldots, n\}$. Consider any subset $J \subseteq I$. Then

$$|\mathcal{A}(J)|t = \sum_{j \in \mathcal{A}(J)} \sum_{i \in I} m_{ij} \geq \sum_{j \in \mathcal{A}(J)} \sum_{i \in J} m_{ij} \geq \sum_{i \in J} \sum_{j \in A_i} m_{ij} = \sum_{i \in J} t = |J|t \,.$$

Hence, $|\mathcal{A}(J)| \geq |J|$. By Hall's Theorem, $\mathcal{A}$ has a matching, corresponding to a transversal T of M and represented by a permutation matrix P. Let $c > 0$ be the minimal value of the entries T. Then $M' = M - cP$ has all line sums equal to $t - c \geq 0$, and M' has fewer nonzero entries than M.

By induction, $M' = \sum_i c_i P_i$ for permutation matrices P_i and $\sum_i c_i = t - c$. Adding P to M' gives $M = cP + \sum_i c_i P_i$. □

Example. We have the following decompostion, where $t = 4$:

$$\begin{pmatrix} -1 & 4 & 1 \\ 3 & 1 & 0 \\ 2 & -1 & 3 \end{pmatrix} = -\begin{pmatrix} 1 & 0 & 0 \\ 0 & 0 & 1 \\ 0 & 1 & 0 \end{pmatrix} + \begin{pmatrix} 0 & 0 & 1 \\ 0 & 1 & 0 \\ 1 & 0 & 0 \end{pmatrix} + 3\begin{pmatrix} 0 & 1 & 0 \\ 1 & 0 & 0 \\ 0 & 0 & 1 \end{pmatrix} + \begin{pmatrix} 0 & 1 & 0 \\ 0 & 0 & 1 \\ 1 & 0 & 0 \end{pmatrix} .$$

Corollary. M is doubly stochastic (i.e. all line sums equal 1) if and only if $M = \sum_i c_i P_i$ for permutation matrices P_i and $\sum_i c_i = 1$.

(König 1916)
If M is a nonnegative matrix with integer entries and constant line sums, then $M = \sum_i P_i$ for permutation matrices P_i.

Definition. A *Latin rectangle* is a matrix in which no line has repeated entries.
A *Latin square* is a square Latin rectangle.
A Latin rectangle is *incomplete* if it has some empty entries.
We will assume that each $n \times n$ Latin square contains n types of symbols, or fewer if incomplete.

Example.

$$M = \begin{pmatrix} 1 & 3 & 4 & 2 \\ 3 & 1 & 2 & 4 \\ 4 & 2 & 1 & 3 \end{pmatrix} \qquad N = \begin{pmatrix} 1 & 3 & 4 & 2 \\ 3 & 1 & & \\ 4 & & 1 & 3 \\ 2 & 4 & 3 & \end{pmatrix}$$

The above matrix M is a Latin rectangle, and N is an incomplete Latin square.

Theorem (Ryser 1956)
Each $r \times n$ Latin square ($r < n$) can be extended to an $n \times n$ Latin square.

Proof. By induction, we need only show that one row can be added. Let A_i be the set of elements not in the i^{th} column of the rectangle R, and set $\mathcal{A} = \{A_i\}_{i \in I}$ where $I = \{1, \ldots, n\}$. Now that $|A_i| = n - r$.

Consider any subset $J \subseteq I$. Each element appears r times in R and therefore $n - r$ times in the sets A_i. Therefore, each element can appear at most $n - r$ times in the sets A_i, where $i \in J$. Then

$$|J|(n-r) = \sum_{i \in J} |A_i| = \sum_{j \in \mathcal{A}(J)} |\{i \in J : j \in A_i\}| \leq |\mathcal{A}(J)|(n-r)\,.$$

Hence, $|\mathcal{A}(J)| \geq |J|$. By Hall's Theorem, $\mathcal{A}$ has a matching, which gives a new row for R. □

Hall's Theorem can also be used to prove stronger results like the following two celebrated theorems.

Ryser's Theorem (1956)
An $r \times s$ Latin rectangle on n symbols can be extended to an $n \times n$ Latin square if and only if each symbol occurs at least $r + s - n$ times.

Evan's Conjecture (Smetianuk 1981)
An incomplete Latin $n \times n$ square with at most $n - 1$ entries can be completed to a Latin square of order n.

Definition. The *Boolean lattice* $\mathcal{B}_n$ is the poset of subsets of $\{1, \ldots, n\}$ under inclusion.

Algorithm
A *symmetric chain decomposition* of $\mathcal{B}_n$ is given inductively as follows:

① The chain $\emptyset \subset \{1\}$ decomposes $\mathcal{B}_1$ (trivially).
② Suppose that $\mathcal{C}$ decomposes $\mathcal{B}_n$ into disjoint symmetric chains.
③ Replace each chain $P_k \subset P_{k+1} \subset \cdots \subset P_{n-k}$ in $\mathcal{C}$ with $|P_i| = i$ by

$$P_{k+1} \subset \cdots \subset P_{n-k} \qquad \text{and} \qquad P_k \subset P_k \cup \{n+1\} \subset \cdots \subset P_{n-k} \cup \{n+1\}\,.$$

Example.
$\mathcal{B}_2$ decomposes into $\{1\}$ and $\emptyset \subset \{2\} \subset \{1,2\}$.
$\mathcal{B}_3$ decomposes into $\emptyset \subset \{3\} \subset \{2,3\} \subset \{1,2,3\}$, $\{1\} \subset \{1,3\}$, and $\{2\} \subset \{1,2\}$.

Sperner's Theorem (1928)
If $\mathcal{A}$ is a family of subsets of $\{1,\ldots,n\}$ with $A \not\subset B$ for all $A, B \in \mathcal{A}$, then $|\mathcal{A}| \leq \binom{n}{\lfloor n/2 \rfloor}$.

Proof. The family $\mathcal{A}$ is an antichain in $\mathcal{B}_n$. By the trivial direction of Dilworth's Theorem, $|\mathcal{A}| \leq m$, where m is the minimal number of chains to cover $\mathcal{B}_n$. The symmetric chain decomposition algorithm gives a covering of $\mathcal{B}_n$ by disjoint chains that each contain one member of P of size $|P| = \lfloor n/2 \rfloor$. There are $\binom{n}{\lfloor n/2 \rfloor}$ such members. Hence, $|\mathcal{A}| \leq m \leq \binom{n}{\lfloor n/2 \rfloor}$. □

The Erdös-Szemeredi Theorem (1935)
Each sequence $a_1, \ldots, a_{n^2+1}$ of n^2+1 distinct integers has a subsequence with $n+1$ elements that is either increasing or decreasing.

Proof. Define a poset P on the elements $a_1, \ldots, a_{n^2+1}$, where $a_i \preceq a_j$ if and only if $i \leq j$ and $a_i \leq a_j$. The chains in P correspond to the decreasing subsequences.

If there is an increasing subsequence of size $n+1$, then we are done. Suppose then that all increasing subsequences have length at most n. In other words, the chains of P have length at most n.

By the Dual of Dilworth's Theorem, we can cover P by at most n antichains.
Since $|P| > n^2$, at least one antichain must have at least $n+1$ elements.
Thus, there is a decreasing subsequence of size at least $n+1$. □

Example. Consider the following sequence of n^2+1 integers where $n = 3$:

$$7\ 8\ 9\ 4\ 5\ 6\ 1\ 2\ 3\ 0\,.$$

There is no increasing subsequence of size $n+1 = 4$.
However, there is a decreasing subsequence of size $n+1 = 4$.

Generalisations

Recall that $(E, \mathcal{I})$ where $\mathcal{I} \subseteq \mathcal{P}(E)$ is a *matroid* if and only if

(I1) $\emptyset \in \mathcal{I}$.
(I2) If $A \in \mathcal{I}$ and $B \subseteq A$, then $B \in \mathcal{I}$.
(I3) If $A, B \in \mathcal{I}$ and $|A| < |B|$, then $A \cup \{a\} \in \mathcal{I}$ for some $a \in B - A$.

Definition. The *rank function* ρ of M is defined by

$$\rho(A) = \max\{|B| : B \subseteq A, B \in \mathcal{I}\}\,.$$

A subset A is *independent* with respect to M if $\rho(A) = |A|$.

Theorem
For all $A, B \subseteq E$,

$$\rho(A) + \rho(B) \geq \rho(A \cup B) + \rho(A \cap B)\,.$$

Proof. Let $X \subseteq A \cap B$ be an independent subset with $|X| = \rho(A \cap B)$. Then X is in an independent subset $Y \subseteq A \cup B$ with $|Y| = \rho(A \cup B)$. Set $Y_A = Y - B$ and $Y_B = Y - A$ and note that $Y = X \cup Y_A \cup Y_B$. Then $X \cup Y_A$ is an independent subset of A. Also, $X \cup Y_B$ is an independent subset of B. Hence,

$$\rho(A) + \rho(B) \geq |X \cup Y_A| + |X \cup Y_B| = |X| + |Y| = \rho(A \cap B) + \rho(A \cup B)\,. \qquad \square$$

Let $\mathcal{A} = \{A_i\}_{i \in I}$ be a finite family of subsets of a finite set E.
Also, let $(E, \mathcal{I})$ be a matroid, and call each partial matching M of $\mathcal{A}$ *independent* if $M \in \mathcal{I}$.

Rado's Theorem (1942)
$\mathcal{A}$ has an independent matching if and only if $\rho(\mathcal{A}(J)) \geq |J|$ for all $J \subseteq I$.

Proof. If $\rho(\mathcal{A}(J)) < |J|$ for some $J \subseteq I$, then there is no independent matching of $\{A_i\}_{i \in J}$ and thus no independent matching of $\mathcal{A}$. Suppose therefore that $\rho(\mathcal{A}(J)) \geq |J|$ for all $J \subseteq I$.

If $\rho(A_j) \geq 2$ for some $j \in \mathcal{I}$, then let x and y be distinct elements of A_j.
Assume that we cannot remove x or y from A_j without violating the inequality in the theorem.
Then there are subsets $I_x, I_y \subseteq I - j$ so that

$$\rho(\mathcal{A}(I_x) \cup (A_j - \{x\})) \leq |I_x|$$
$$\rho(\mathcal{A}(I_y) \cup (A_j - \{y\})) \leq |I_y|\,.$$

Thus,

$$\begin{aligned}
|I_x| + |I_y| &\geq \rho(\mathcal{A}(I_x) \cup (A_j - x)) + \rho(\mathcal{A}(I_y) \cup (A_j - y)) \\
&\geq \rho(\mathcal{A}(I_x) \cup (A_j - x) \cup \mathcal{A}(I_y) \cup (A_j - y)) + \rho((\mathcal{A}(I_x) \cup (A_j - x)) \cap (\mathcal{A}(I_y) \cup (A_j - y))) \\
&\geq \rho(\mathcal{A}(I_x) \cup (A_j - x) \cup \mathcal{A}(I_y) \cup (A_j - y)) + \rho(\mathcal{A}(I_x) \cap \mathcal{A}(I_y)) \\
&\geq \rho(\mathcal{A}(I_x \cup I_y \cup \{j\})) + \rho(\mathcal{A}(I_x \cap I_y)) \\
&\geq |I_x \cup I_y| + 1 + |I_x \cap I_y| \\
&= |I_x| + |I_y| + 1\,,
\end{aligned}$$

a contradiction. We can thus remove the elements from the sets A_i while preserving the inequality in the theorem, until $A_i = \{a_i\}$ for some a_i for each $i \in I$. Then $|\{a_i\}_{i \in I}| \geq \rho(\{a_i\}_{i \in I}) = \rho(\mathcal{A}(I)) \geq |I|$. Hence, the elements a_i are distinct, so $\{a_i\}_{i \in I}$ is a matching if $\mathcal{A}$. $\square$

Let $\mathcal{A} = \{A_i\}_{i \in I}$ and $\mathcal{B} = \{B_i\}_{i \in I}$ be families of finite sets indexed by I.

Ford and Fulkerson (1962)
$\mathcal{A}$ and $\mathcal{B}$ have a matching in common if and only if, for all $J_A, J_B \subseteq I$,

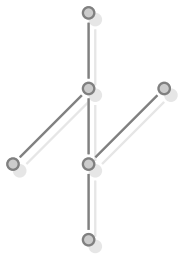
$$|\mathcal{A}(J_A) \cap \mathcal{B}(J_B)| \geq |J_A| + |J_B| - |I|\,.$$

Proof. Let ρ be the rank function of the matroid associated to $\mathcal{I}(\mathcal{A})$. Then a set is a common matching of $\mathcal{A}$ and $\mathcal{B}$ if and only if it is an independent matching of $\mathcal{B}$. By Rado's Theorem, such a set exists if and only if $\rho(\mathcal{B}(J_B)) \geq |J_B|$ for all $J_B \subseteq I$. That is, if and only if $\mathcal{B}(J_B)$ contains a partial matching of $\mathcal{A}$ of size $|J_B|$. By Ore's theorems, this occurs precisely when, for all $J_A \subseteq I$,

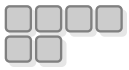
$$\mathcal{A}(J_A) \cap \mathcal{B}(J_B)| \geq |J_A| - |I| + |J_B|\,.$$

$\square$

Example. Consider the poset given by the following graph:



maximal size of 1 chain = 4
maximal size of 2 chains = 6

$\Delta =$ 

maximal size of 1 antichain = 2
maximal size of 2 antichains = 4
maximal size of 3 antichains = 5
maximal size of 4 antichains = 6

$\tilde{\Delta} =$ 

Greene's Duality Theorem (1976)

$$\triangle = \tilde{\triangle}^T$$

Note that Greene's Duality Theorem implies both Dilworth's Theorem and its dual.

Graph Algorithms

Definition. A *graph* $G = (V, E)$ consists of *vertices* V and *edges* $E \subseteq \binom{V}{2}$.
We can draw G as dots (vertices) and lines between the dots (edges).
A graph is *s*imple if no edge is adjacent to just one vertex and no two edges share the same endpoints.
A graph $G = (V, E)$ is *bipartite* if there is a bipartition $V = X \cup Y$ so that all edges go from one part to the other, i.e., $E \cap \binom{X}{2} = E \cap \binom{Y}{2} = \emptyset$).
A *matching* is a set of disjoint edges.
Vertex set $X \subseteq V$ is *matched* if it is covered by a matching.
A *complete matching* (or *1-factor*) is a matching that covers V.
The neighbours of vertices $Z \subseteq V$ are denoted by $N(Z)$.
That is, $N(Z) = \{u \in V : \{u, v\} \in E \text{ for some } v \in Z\}$.
Let $\mathcal{A} = \{A_i\}_{i \in I}$ be a finite family of sets.
Define $B = (V, E_B)$, where $V = \mathcal{A} \cup \mathcal{A}(I)$ and $E_B = \{\{a, A\} : a \in A\}$.
Then $\mathcal{A}$ has a matching if and only if $\mathcal{A}$ is matched in B.
The Marriage Theorem has the following natural bipartite graph expression.

The Marriage Theorem (Frobenius 1917, Hall 1935)
Let $B = (X \cup Y, E_B)$ be a bipartite graph.
Then X is matched in B if and only if for all $A \subseteq X$, $|N(A) \geq |A|$.

Definition. Let $G = (V, E)$ be a graph.
A *walk* in G is a sequence of vertices $v_1, \ldots, v_n$ with $\{v_i, v_{i+1}\} \in E$.
A *path* in G is a walk with no repeated vertex.
A *closed walk* in G is a walk of the form $v_1, \ldots, v_n, v_1$.
A *cycle* in G is a closed walk with no repeated vertex but the first and last.
If a walk exists between each pair of vertices in G, then G is *connected*.
The *maximally connected subgraphs* of G are components of G.
Let $c_0(G)$ denote the number of components in G of odd vertex size.

(Tutte's 1-Factor Theorem 1947)
G has a complete matching if and only if for all $S \subseteq V$, $c_0(G - S) \leq |S|$.

Augmenting Paths

Definition. Let $G = (V, E)$ be a (simple) graph and let M be a matching in G.
An *alternating path* for M is a path where every second edge lies in M.
An alternating path P is *augmenting* if its end-edges lie outside M.
Let $E(P)$ denote the edges along P.

Lemma. The set of edges $M' = M \oplus E(P)$ is a matching of size $|M'| = |M| + 1$.

Proof. The vertices covered by M' are those of P.
Each is in one edge of M', so M' is a matching, and $|M'| = |M| + 1$. □

Theorem
M has maximal size in G if and only if M has no augmenting path.

Proof. We have previously shown that M is not maximal if an augmenting path exists.

Suppose that no such path exists and let M' be a maximal matching in G. Each vertex of $G = M \oplus M'$ is in at most one edge of M and of M'. Thus, D is a disjoint union of cycles and alternating paths.

The edges alternate between M and M', so each cycle has even edge total. By assumption, no path is augmenting, so each path has even edge totals. Therefore, all of the cycles and paths contain the same number of edges from M as from M'. This imples that $|M - M'| = |M' - M|$. Hence,

$$|M| = |M - M'| + |M \cap M'| = |M' - M| + |M \cap M'| = |M'|\,.$$

Thus, M has maximal size. □

Maximal Matching Algorithm

1. Set $M = \emptyset$.
2. Search for an augmenting path P for M.
3. Replace M by $M \oplus E(P)$.
4. Continue until there is no augmenting path.
5. M is a maximal matching.

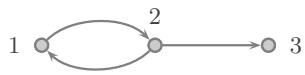
In general, it is difficult to find augmenting paths efficiently but for bipartite graphs it is easy.

Bipartite Augmenting Path Algorithm
Let $B = (X \cup Y, E_B)$ be a bipartite graph and let M be a matching in B.

1. If M covers X, then M is maximal; set $T = \emptyset$; end.
2. Otherwise, set $T = \{v\}$ for some vertex $v \in X - V(M)$.
3. Let $2m$ be the longest path-length from v in T.
4. Consider each $x \in V(T)$ at distance $2m$ from v.
5. If $y \in N(x) - V(T) - V(M)$, then add edge $\{x, y\}$ to T; end.
6. If $y \in N(x) - V(T)$, then add edges $\{x, y\}$ and $\{y, x'\} \in M$ to T.
7. Repeat until $N(x) - V(T) = \emptyset$.
8. Then T contains an augmenting path starting from v if one exists.

Definition. A *directed graph* $D = (V, A)$ consists of vertices V and arcs $A \subseteq V \times V$.
We can draw D as dots and A as arrows between the dots.

Example. Let D be the directed graph (V, A) with $V = \{1, 2, 3\}$ and $A = \{(1, 2), (2, 1), (2, 3)\}$.



Definition. A *network* is a directed graph $D = (V, A)$ with two distinguished vertices, the *source* s and *sink* t (or *terminal*), and a *capacity function* $c : A \to \mathbb{R}_{\geq 0}$.

Definition. A *flow* in D is a function $f : A \to \mathbb{R}_{\geq 0}$ such that

- $0 \leq f(a) \leq c(a)$ for each arc $a \in A$.
- $f^+(v) = f^-(v)$ for each vertex $v \in V - \{s, t\}$, where

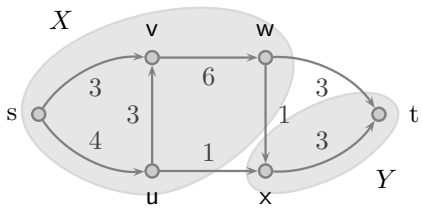
$$f^-(v) = \sum_{u:(u,v)\in A} f(u, v)$$
$$f^+(v) = \sum_{w:(v,w)\in A} f(v, w)\,.$$

The *strength* of f is $|f| = f^+(s) - f^-(s)$.

Definition. A *cut* in D is a bipartition (X, Y) of V with $s \in X$ and $t \in Y$.
The *capacity* of a cut (X, Y) is the sum

$$c(X, Y) = \sum_{u\in X, v\in Y:(u,v)\in A} c(u, v)\,.$$

Example.



The strength of f is $|f| = f^+(s) - f^-(s) = 2 + 3 - 0 = 5$.
The cut (X, Y) has capacity $c(X, Y) = c(u, x) + c(w, x) + c(w, t) = 1 + 1 + 3 = 5$.

Definition. Let (X, Y) be a partition of D and f be a flow on D. Define

$$f(X, Y) := \sum_{u\in X, v\in Y:(u,v)\in A} f(u, v)\,.$$

Theorem
If (X, Y) is a cut of D, then $|f| = f(X, Y) - f(Y, X)$.

Proof. By definition, $f^+(v) - f^-(v) = 0$ for all $v \in X - \{s\}$. Therefore,

$$\begin{aligned}
|f| &= f^+(s) - f^-(s) \\
&= \sum_{u \in X} f^+(u) - \sum_{v \in X} f^-(v) \\
&= \sum_{u \in X} \sum_{v:(u,v)\in A} f(u,v) - \sum_{v \in X} \sum_{u:(u,v)\in A} f(u,v) \\
&= \sum_{\substack{u,v \in X: \\ (u,v)\in A}} f(u,v) + \sum_{\substack{u \in X, v \in Y: \\ (u,v)\in A}} f(u,v) - \sum_{\substack{v,u \in X: \\ (u,v)\in A}} f(u,v) - \sum_{\substack{v \in X, u \in Y: \\ (u,v)\in A}} f(u,v) \\
&= f(X,Y) - f(Y,X).
\end{aligned}$$

□

Theorem
For each flow f and each cut (X, Y) in D, $|f| \leq c(X, Y)$.

Proof. From the previous theorem,

$$|f| = f(X,Y) - f(Y,X) \leq f(X,Y) \leq c(X,Y)\,.$$

□

Corollary. $|f| = f^-(t) - f^+(t)$.

Proof. $|f| = f(V - \{t\}, \{t\}) - f(\{t\}, V - \{t\}) = f^-(t) - f^+(t)$. □

Definition. Let f be a flow on the network $D = (V, A)$. An *augmenting path* P for f is a sequence of vertices $v_0, v_1, \ldots, v_n \in V$ for which either

- $e = (v_i, v_{i+1}) \in A$ and $\alpha_i = c(e) - f(e) > 0$, or
- $e = (v_{i+1}, v_i) \in A$ and $\alpha_i = f(e) > 0$.

Define $\alpha = \min\{\alpha_i\}$ and let $f \oplus P$ denote the function given on A by

$$(f \oplus P)(e) = \begin{cases} f(e) + \alpha, & e = (v_i, v_{i+1}) \in A \\ f(e) - \alpha, & e = (v_{i+1}, v_i) \in A \end{cases}$$

Theorem
If f has an augmenting path P from s to t, then $f \oplus P$ is a flow with $|f \oplus P| > |f|$.

Proof. It is easy to check that $f \oplus P$ satisfies the two flow conditions.
Furthermore, $|f \oplus P| = |f| + \alpha > |f|$ where α is defined as above. □

Corollary. If f is a maximal flow (i.e. has maximal strength $|f|$), then there is no augmenting path for f from s to t.

The Max-Flow Min-Cut Theorem (Ford and Fulkerson 1955)

$$\max |f| = \min c(X,Y)\,.$$

Proof. Let any f be a maximal flow in D and let S be the set of all vertices reachable by an augmenting path for f starting in s. By the corollary above, f has no augmenting path from s to t. Thus, $t \in T$, where $T = V - S$, so (S, T) is a cut. Let $u \in S$ and $v \in T$.

Suppose that $e = (u, v) \in A$. Since v cannot extend any augmenting path ending in u, $f(e) = c(e)$.

Suppose then that $e = (v, u) \in A$. Since v cannot extend any augmenting path ending in u, $f(e) = 0$. Hence, by the corollary above,

$$|f| = f(S,T) - f(T,S) = \sum_{\substack{u\in S, v\in T:\\ (u,v)\in A}} f(u,v) - \sum_{\substack{u\in S, v\in T:\\ (v,u)\in A}} f(u,v) = \sum_{\substack{u\in S, v\in T:\\ (u,v)\in A}} c(u,v) = c(S,T)\,.$$

Hence, $\min c(X, Y) \le c(S, T) \le |f|$.

However, a theorem above states that $|f| \le c(X, Y)$ for any cut (X, Y). Thus, $|f| = \min c(X, Y)$. □

The Ford-Fulkerson Algorithm (1960)

① Set $f = 0$.
② Search for an augmenting path P for f from s to t.
③ Replace f by $f \oplus P$.
④ Continue until there is no augmenting path.
⑤ Then f is a maximal flow.

Theorem
Each network with all-integer capacities has integer-valued maximal flow.

Proof. Starting with the zero flow $f = 0$, augment f with augmenting paths from s to t, until f is a maximal flow. At each step, the values $f(e)$ change by the integers 0 or $\pm\alpha$. □

We now use these ideas to prove König's Theorem (and hence also Hall's and Dilworth's Theorems).

König's Theorem (1916)
The maximal size M of a partial transversal in a $(0, 1)$-matrix N equals
the minimal number m of lines needed to cover all 1-entries of N.

Proof. Let R and C be the row and column indices of N.
Define network $D = (V, A)$ with

$$V = R \cup C \cup \{s, t\}$$
$$A = S \cup B \cup T$$

where
$$S = \{s\} \times R$$
$$B = \{(i, j) \in R \times C : n_{ij} = 1\}$$
$$T = C \times \{t\}$$

with capacities $c(e) = M + 1$ if $e \in B$ and $c(e) = 1$ otherwise. Then there is a maximal flow f with $f(e) \in \{0, 1\}$ for all edges $e \in A$. Therefore, the arcs $e \in B$ with positive flow ($f(e) = 1$) are vertex-disjoint and correspond to a partial transversal of A.

Hence, by the Max-Flow Min-Cut Theorem, $M \ge \min c(X, Y)$.
Let (X, Y) be a minimal edge cut. Since $c(X, Y) = \max |f| < M + 1$, no edge of B is cut by (X, Y), so $c(X, Y) = |C|$, where $U = (R \cap Y) \cup (C \cap X)$ is a set of vertices touching all edges of B.

Thus, U corresponds in N to a set of lines covering of 1-entries. Hence, $m \le |U| = c(X, Y) \le M$. Since $m \ge M$, we have equality. □

Spanning Trees

Definition. A *tree* is a connected graph containing no cycle.
A *spanning tree* of a graph G is a subgraph of G that is a tree containing all vertices of G.

Theorem
Every tree on n vertices has $n-1$ edges.

Proof. We can build up a tree by starting with a single vertex and adding edges to the existing graph. The single vertex has 1 vertex and 0 edges. Each added edge adds just one vertex, so the final tree will have one fewer edges than vertices. □

Theorem
The spanning trees of a connected graph have the same number of edges.

Proof. If G is a connected graph on n vertices, then any spanning tree T of G will contain all n vertices. Hence, T has $n-1$ edges. □

Theorem
Every connected graph contains a spanning tree.

Proof. Let G be a connected graph. If G is a tree, then G is a spanning tree for itself.
If G is not a tree, then G contains at least one cycle. Remove an edge from a cycle in G.
The resulting graph is still connected and contains all vertices of G.

Continue to remove an edge from each cycle until no cycles remain.
The resulting graph is a tree containing all vertices of G. In other words, it is a spanning tree of G. □

Theorem
A connected graph on n vertices is a tree if and only if it has $n-1$ edges.

Proof. Let G be a connected graph with n vertices. If G is a tree, then it has $n-1$ edges.

Conversely, suppose that G has $n-1$ edges. Let T be a spanning tree of G. Then T is contained in G and has as many vertices and edges as G. Therefore, T is in fact equal to G. Hence, G is a tree. □

Definition. A *weighted graph* G is a graph whose edges have been assigned numbers.
The *weight* of an edge e is denoted by $w(e)$.
The *weight* $w(G)$ of G is the sum of edge weights in G.
A *minimal spanning tree* T of G is a spanning tree with minimal weight $w(T)$ among all such trees of G.

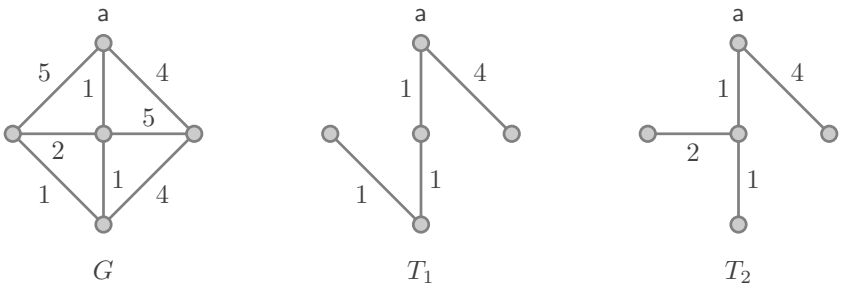
The Greedy Algorithm

① Set $T = \emptyset$.
② Let A be the edges in $E - E(T)$ that form no cycle with edges in T.
③ Choose an edge e from A that has smallest weight.
④ Add e to T.
⑤ Continue until T has $n-1$ edges.
⑥ Then T is a minimal spanning tree for G.

Definition. Let G be a connected graph with positive edge-weights and let $a \in V(G)$.
Consider a shortest path from a to v for each vertex v in G (a shortest path is one with minimal weight).
A *minimal a-path spanning tree* for G is a union of such paths to form a spanning tree.

Remark. A minimal a-path spanning tree is *not* generally a minimal spanning tree.

Example.



The tree T_1 below is a minimal spanning tree in G whereas T_2 is a minimal a-path spanning tree in G.

Dijkstra's Algorithm (1959)

① Set $T = \{a\}$.
② Let A be the edges with one vertex v not in T and the other int T.
③ Choose and edge e from A that gives a shortest path from a to any v.
④ Add e to T.
⑤ Continue until T contains all vertices of G.
⑥ Then T is a minimal a-path spanning tree for G.

Proof. It is easy to see that T is a spanning tree. We must therefore show that the distances given by T from a to each vertex v indeed equal $d(a, v)$ in G, where, for any vertices $w, x \in V(G)$, $d(w, x)$ denotes the shortest distance between them.

Assume that this is not true - that the algorithm fails, and let v be the first vertex for which this happens. Let T' be the tree generated up until this point, and let u be the vertex preceding v in T'. Let P be a shortest path from a to v, and let z be the first vertex along this path that is not in T'.

Also, let y be the preceding vertex in P. Since the algorithm first failed with v and v was chosen to be in T' and z was not, we have

$$\begin{aligned} d(a, v) &< d(a, u) + w(u, v) \\ &\leq d(a, y) + w(y, z) \\ &< d(a, y) + d(y, v) \\ &= d(a, v)\,, \end{aligned}$$

which is clearly a contradiction. □

Traversing Circuits

Definition. The *degree* $\deg(v)$ of a vertex v is the number of edges that contain v.

Handshaking Lemma

$$2|E| = \sum_{v \in V} \deg(v)$$

Proof.

$$2|E| = \sum_{e \in E} 2 = \sum_{e \in E} \sum_{v \in e} 1 = \sum_{v \in V} \sum_{e \in E : v \in e} 1 = \sum_{v \in V} \deg(v). \qquad \square$$

Example. By this lemma, no graph with five vertices can have degrees 3,3,3,2,2.

Lemma. Each vertex degree is at most $n - 1$.

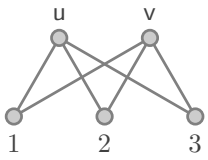
Example. By the above lemma, no graph with five vertices can have degrees 5,4,3,2,1, or 4,3,3,1,1.

Lemma. Suppose that G is connected. Then

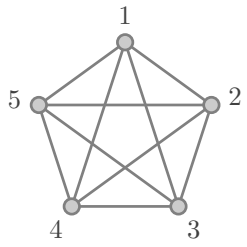
- G is a cycle if and only if each vertex in G has degree 2.
- G is a path if and only if each vertex in G has degree 2, except two with degree 1.

Definition. Let G be a connected graph.
An *Euler trail* in G is a nonclosed walk passing each edge of G exactly once.
An *Euler circuit* in G is a closed walk passing each edge of G exactly once.
A *Hamilton path* in G is a path that passes each vertex of G exactly once.
A *Hamilton cycle* in G is a cycle that passes each vertex of G exactly once.

Example.



$u1v2u3v$ is an Euler trail.
There is no Euler circuit.
$1u2v3$ is a Hamilton path.
There is no Hamilton cycle.



There is no Euler trail.
12345135241 is an Euler circuit.
12345 is a Hamilton path.
123451 is a Hamilton cycle.

Theorem
G has an Euler circuit if and only if each vertex of G has even degree.

Proof. Suppose that G has an Euler circuit C. Each time C passes via a vertex v, it uses 2 edges, one in and one out. Every edge is used exactly one, so $\deg(v)$ is twice the number of times C passes through v. Thus, $\deg(v)$ is even.

Conversely, suppose that each vertex in G has even degree. If G has at least one edge, then some vertex has at least two edges. Let $P = v_1, \ldots, v_k$ be a maximal path in G. Since $\deg(v_k) \geq 2$, there is an edge $\{v_k, v\}$ in G where $v \neq v_{k-1}$. Since P is maximal, v must lie in P - in other words, $v = v_j$ for some j. Then $C = v_j, \ldots, v_k, v_j$ is a cycle in G.

Let G' be the graph obtained from G by removing the edges of C. Then each vertex degree in G' is even. As long as edges remain, we can thus continue to find and remove cycles. Hence, G is a union of edge-disjoint cycles. Since G is connected, no cycle is vertex-disjoint from all other cycles. Hence, we can traverse the cycles recursively to get an Euler circuit. □

Theorem
G has an Euler trail if and only if exactly two vertices have odd degree.

Proof. Suppose that G has an Euler trail $v_1, \ldots, v_k$. Add the edge $\{v_k, v_1\}$ to G.
Now G has an Euler circuit, so each vertex degree is even. Remove the edge $\{v_k, v_1\}$ again.
Then each vertex degree is even, except $\deg(v_1)$ and $\deg(v_k)$.

The converse is proved similarly. □

Algorithm

① Set $C = v_0$ for some vertex v_0 in G.
② Choose a cycle C' with at least one vertex v, but no edge, of C.
③ Replace one of the v's in C by C'.
④ Continue this process until C contains all edges in G.
⑤ Then C is an Euler circuit in G.

In the following theorem, suppose that $G = (V, E)$ is simple with $n = |V| \geq 3$.

Dirac's Theorem (1962)
If $\deg(v) \geq \frac{n}{2}$ for all $v \in V$, then G has a Hamilton cycle.

Proof. Assume that the theorem is false. Since the graph $K_V = \left(V, \binom{V}{2}\right)$ has a Hamilton cycle, G is contained in a graph G' on V that is maximal with respect to having no Hamilton cycle. Without loss of generality, we may assume that $G = G'$.

Since $G \neq K_V$, there are vertices $u, v \in V$ such that $\{u, v\} \notin E$. Let G^+ be the graph obtained by adding the edge $\{u, v\}$ to G. By the maximality of G, G^+ has a Hamilton cycle, and each Hamilton cycle of G^+ must contain $\{u, v\}$. Therefore, G has a Hamilton path $v_1, \ldots, v_n$ from $u = v_1$ to $v = v_n$.

Set $S = \{v_i : \{u, v_{i+1}\} \in E\}$ and $T = \{v_i : \{v_i, v\} \in E\}$. Then, since G is simple, $v \notin S \cup T$, so $|S \cup T| < n$. Assume that $v_i \in S \cap T$. Then $v_1, \ldots, v_i, v_n, v_{n-1}, \ldots, v_{i+1}, v_1$ is a Hamilton cycle in G, a contradiction. Therefore, $|S \cap T| = 0$. Hence,

$$n = \frac{n}{2} + \frac{n}{2} \leq \deg(u) + \deg(v) = |S| + |T| = |S \cup T| + |S \cap T| < n\,,$$

a contradiction. □

Matroids

Theorem (Birkhoff 1912)
The number of ways to colour a map M in λ colours is $P(M;\lambda)$ for some fixed polynomial $P(M;x)$.

Recall that $(E,\mathcal{I})$ where $\mathcal{I} \subseteq \mathcal{P}(E)$ is a *matroid* if and only if

(I1) $\emptyset \in \mathcal{I}$.

(I2) If $A \in \mathcal{I}$ and $B \subseteq A$, then $B \in \mathcal{I}$.

(I3) If $A, B \in \mathcal{I}$ and $|A| < |B|$, then $A \cup \{a\} \in \mathcal{I}$ for some $a \in B - A$.

Example. Given the matrix

$$\begin{pmatrix} 1 & 0 & 1 & 0 & 0 \\ 0 & 1 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 & 1 \end{pmatrix}$$

the set of its columns induce a *vector matroid* determined by linear dependence,
for instance by any of the following representations, where each digit refers to the associated column:

$\mathcal{I}$*ndependent sets*: $\emptyset, 1, 2, 3, 4, 5, 12, 13, 14, 15, 23, 24,\ 25, 34, 35, 124, 125, 134, 135, 234, 235$.

$\mathcal{B}$*ases* (maximal independent sets): $124, 125, 134, 234, 235$.

$\mathcal{C}$*ircuits* (minimally dependent sets): $123, 45$.

Example. The *uniform matroid* $U_{r,n} = (E,\mathcal{I})$ has $|E| = n$ and $\mathcal{I} = \{A \subseteq E : |A| \leq r\}$.

Example. Let $\mathcal{A} = \{A_i\}_{i\in\mathcal{I}}$ be a family of subsets of E.
The partial matching $\mathcal{I}$ of $\mathcal{A}$ form the *transversal matroid* $(E,\mathcal{I})$ (see page 3 for more details).

Example. Let E be the edges of a graph G and let $\mathcal{I}$ be the family of forests of G.
Then $M(G) = (E,\mathcal{I})$ is the *cycle matroid* of G.

Definition. Let E be a finite set and $\mathcal{B} \subseteq \mathcal{P}(E)$ be a family of subsets of E.
The tuple $(E,\mathcal{B})$ is a matroid if and only if

(B1) $\mathcal{B} \neq \emptyset$.

(B2) If $B_1, B_2 \in \mathcal{B}$ and $x \in B_1 - B_2$, then $(B_1 - x) \cup \{y\} \in \mathcal{B}$ for some $y \in B_2 - B_1$.

Example.
$U_{r,n} = (E,\mathcal{B})$ is a uniform matroid, where $\mathcal{B} = \{A \subseteq E : |A| = r\}$.
The maximal partial matchings $\mathcal{B}$ form the transversal matroid $(E,\mathcal{B})$.
The spanning forests $\mathcal{B}$ of a graph G define the cycle matroid $M(G) = (E,\mathcal{B})$ of G.

Definition. Let E be a finite set and $\mathcal{C} \subseteq \mathcal{P}(E)$ be a family of subsets of E.
The tuple $(E,\mathcal{C})$ is a matroid if and only if

(C1) $\emptyset \notin \mathcal{C}$.

(C2) If $C_1, C_2 \in \mathcal{C}$, then $C_1 \not\subset C_2$.

(C3) If $C_1, C_2 \in \mathcal{C}$ are distinct and $e \in C_1 \cap C_2$, then $C \subseteq (C_1 \cup C_2) - e$ for some $C \in \mathcal{C}$.

Example.
$U_{r,n} = (E,\mathcal{C})$ is a uniform matroid, where $\mathcal{C} = \{A \subseteq E : |A| = r+1\}$.
The cycle edge sets $\mathcal{C}$ of a graph G define the cycle matroid $M(G) = (E,\mathcal{C})$ of G.

Theorem
The sets of axioms (I1-3), (B1-2), and (C1-3) are equivalent.

Proof. We will merely prove that (C3) follows from (I1-3).
Let $(E, \mathcal{I})$ be a matroid and let $\mathcal{C}$ be the minimal subsets not in $\mathcal{I}$.
Suppose that $C_1, C_2 \in \mathcal{C}$ are distinct and that $e \in C_1 \cap C_2$, and assume that $(C_1 \cup C_2) - e \in \mathcal{I}$.

By construction, $C_2 - C_1 \neq \emptyset$, so we may choose some $f \in C_2 - C_1$. Now, C_2 is minimally not in $\mathcal{I}$, so $C_2 - f \in \mathcal{I}$. Choose $I \in \mathcal{I}$ to be maximal so that $C_2 - f \subseteq I \subseteq C_1 \cup C_2$. Note that $C_2 \not\subseteq I$, so $f \notin I$.

Similarly, $C_1 \not\subseteq I$, so there exists $g \in C_1 - I$. Since $f \notin C_1$, the elements f and g are distinct, so

$$|I| \leq |(C_1 \cup C_2) - \{f, g\}| = |C_1 \cup C_2| - 2 < |(C_1 \cup C_2) - e| .$$

By (I3), $I \cup \{a\} \in \mathcal{I}$ for some $a \in (C_1 \cup C_2) - e$ not in I, contradicting the maximality of I.
Hence, $(C_1 \cup C_2) - e$ is not in $\mathcal{I}$ and thus contains some $C \subseteq \mathcal{C}$. □

From the theorem above, we see that

- If $(E, \mathcal{I})$ is a matroid, then its *bases* $\mathcal{B}$ (maximal members of $\mathcal{I}$) satisfy (B1-2), and *circuits* $\mathcal{C}$ (or minimal subsets not in $\mathcal{I}$) satisfy (C1-3).
- If $(E, \mathcal{B})$ is a matroid, then its *independent sets* $\mathcal{I}$ (subsets of $\mathcal{B}$'s members) satisfy (I1-3), and its *circuits* $\mathcal{C}$ (or minimal non-subsets of $\mathcal{B}$'s members).
- If $(E, \mathcal{C})$ is a matroid, then its *independent sets* $\mathcal{I}$ (proper subsets of $\mathcal{C}$'s members) satisfy (I1-3), and its *bases* $\mathcal{B}$ (or maximal proper subsets of $\mathcal{C}$'s members) satisfy (B1-2).

Remark. There are a myriad of other equivalent ways in which to define matroids, for instance via the *rank function* $r(A) := \max\{|I| : I \subseteq A, I \in \mathcal{I}\}$.
The tuple (E, r) is a matroid if and only if
(R1) If $A \subseteq E$, then $0 \leq r(A) \leq |A|$.
(R1) If $A \subseteq B \subseteq E$, then $r(A) \leq r(B)$.
(R1) If $A, B \subseteq E$, then $r(A \cup B) + r(A \cap B) \leq r(A) + r(B)$.

Theorem
For a graph $G = (V, E)$, let $\mathcal{C}$ be its cycle edge sets.
Then $M(G) = (E, \mathcal{C})$ is a matroid (the cycle matroid of G).

Proof. The family $\mathcal{C}$ trivially satisfies (C1) and (C2). Let $C_1, C_2 \in \mathcal{C}$ be distinct circuits of G containing a shared edge e. Let P_1 and P_2 be the paths $C_1 - e$ and $C_2 - e$ respectively. Since C_1 and C_2 are distinct, P_1 and P_2 must also be distinct.

Now, P_1 and P_2 have the same endpoints (the vertices of e), so $P_1 \cup P_2$ is a closed walk containing a cycle. The edge set C of this cycle is contained in $(C_1 \cup C_2) - e$. □

The Greedy Algorithm For Matroids (Borvka 1926, Kruskal 1956)
Let $M = (E, \mathcal{I})$ be a matroid with weights $w(e)$ for each $e \in E$:

① Set $B = \emptyset$.
② Let A be all elements e in $E - B$ for which $B \cup \{e\} \in \mathcal{I}$.
③ Choose an edge e from A with smallest weight $w(e)$.
④ Add e to B.
⑤ Continue until $A = \emptyset$.
⑥ Then B is a minimally weighted basis for M.

Proof. By (I3), the algorithm will return a basis $B = \{e_1, \ldots, e_r\}$. Assume that $w(B') < w(B)$ for some basis $B' = \{f_1, \ldots, f_r\}$ of M. We may suppose that $w(e_1) \leq \ldots \leq w(e_r)$ and $w(f_1) \leq \cdots \leq w(f_r)$. Set $i = \min\{j : w(f_j) < w(e_j)\}$.

By (I3), there is some $j \in \{1, \ldots, i\}$ for which $\{e_1, \ldots, e_{i-1}\} \cup \{f_j\} \in \mathcal{I}$. Also, $w(f_j) \leq w(f_i) < w(e_i)$. However, this means that the algorithm would not have chosen e_i at the i^{th} step for B, a contradiction. Thus, B is a basis with minimal weight. □

Let $M = (E, r)$ be a matroid.

Edmond's Matroid Partition Theorem (1970)
The set E can be partitioned into k independent sets if and only if $k \cdot r(A) \geq |A|$ for all $A \subseteq E$.

A special case of this result is Edmonds' Tree Partition Theorem.

Definition. Let $M = (E, r)$ be a matroid on $n = |E|$ elements. For all $A \subseteq E$, define

$$r^*(A) := |A| - r(E) + r(E - A)\,.$$

Then $M^* := (E, r^*)$ is a matroid, called the *dual matroid* of M.
Further, for $k = r(E)$ and all i, j, define

$$f_i = \max\{|A| : r(A) = i\}, \qquad U = \{f_0 + 1, \ldots, f_{k-1} + 1\}$$
$$f_j^* = \max\{|A| : r^*(A) = j\}, \qquad V = \{n - f_{n-k-1}^*, \ldots, n - f_0^*\}\,.$$

Britz et al. (2012)

$$U \cup V = \{1, \ldots, n\} \qquad \text{and} \qquad U \cap V = \emptyset\,.$$

Proof. Assume that the theorem is false.
Then $f_i + 1 = n - f_j^*$ for some i, j.
Choose $A \subseteq E$ so that $|A| = f_j^*$ and $r^*(A) = j$.
Then $|E - A| = n - |A| = n - f_j^* = f_i + 1$, so $r(E - A) \geq i + 1$.
By definition, $-|A| + r^*(A) + r(E) = r(E - A)$; therefore $-f_j^* + j + k \geq i + 1$.
Similarly, $n - f_i + i - k \geq j + 1$. Adding these inequalities gives $1 = n - f_i - f_j^* \geq 2$, a contradiction. □

The above theorem generalises Wei's Duality Theorem [Wei 1991], a celebrated theorem in which similarly defined numbers described the minimal weights of subcodes, by rank, of a linear code and its dual. The theorem also generalises a similar result for graphs proved by [Britz 2007].
(See lecture slides for more details.)

References

[1] M. Aigner, *Combinatorial Theory*, Springer-Verlag, New York, 1979.

[2] J.A. Bondy and U.S.R. Murty, *Graph Theory with Applications*, Macmillan Press, New York, 1976.

[3] T. Britz, Higher support matroids, *Discrete Math.* **307** (2007), 2300–2308.

[4] T. Britz, T. Johnsen, D. Mayhew, and K. Shiromoto, Wei-type duality theorems for matroids, *Des. Codes Cryptogr.* **62** (2012), 331–341.

[5] L.R. Ford, Jr. and D.R. Fulkerson, *Flows in Networks*, Princeton Univ. Press, 1962.

[6] R.L. Graham, M. Grötschel, and L. Lovász (eds.), *Handbook of Combinatorics. I–II*, North-Holland, Amsterdam, 1995.

[7] L. Lovász and M.D. Plummer, *Matching Theory*, Akadémiai Kiadó, North Holland, Budapest, 1986.

[8] J.H. van Lint and R.M. Wilson, *A Course in Combinatorics*, Cambridge University Press, 1992.

[9] R. Rado, A theorem on independence relations, *Quart. J. Math., Oxford Ser.* **13** (1942), 83–89.

[10] V.K. Wei, Generalized Hamming weights for linear codes, *IEEE Trans. Inform. Theory* **37** (1991), 1412–1418.