Discrete Mathematics Lecture Notes (2024/2025)

Griffin Reimerink

Contents

Note

The following have been omitted from these notes for conciseness:

- Spanning trees of the fan graph (lecture 8 page 7)
- Counting the number of ways to pay n€ (lecture 8 page 9)
- Planted plane trees (lecture 9 page 4)
- Probabilistic method (lecture 12, lecture 13 page 2, lecture 14 page 2)
- Linear algebra method (lecture 14 page 3, lecture 15)

1 Combinatorics

1.1 Introduction

Notation: $[n] := \{1, 2, \dots, n\}$

Number of ways to choose elements from a set

Number of ways to choose k balls from an urn containing n balls:

- With order, with replacement: n^k
- With order, without replacement: $(n)_k := \frac{n!}{(n-k)!}$ (**falling factorial**)
- Without order, without replacement: $\binom{n}{k} := \frac{n!}{k!(n-k)!}$ (**binomial coefficient**)
- Without order, with replacement: $\binom{n+k-1}{k}$

The number of vectors in $\{0,1\}^k$ with exactly k ones is equal to $\binom{n}{k}$.

A **multiset** is a generalization of a set which allows duplicates.

Binomial notation for sets

$$\binom{V}{k} := \{A \subseteq V : |A| = k\} \qquad \left|\binom{V}{k}\right| = \binom{|V|}{k}$$

Pigeon-hole principle

Pigeon-hole principle:
If p pigeons are divided among $h < p$ pigeon-holes, then some hole has ≥ 2 pigeons.
Advanced pigeon-hole principle:
If p pigeons are divided among h pigeon-holes with $h(t-1) < p$, then some hole has $\geq t$ pigeons.

Theorem *Inclusion-exclusion principle*

Let $V_1, \dots, V_k$ be subsets of a finite set V.

$$|V_1 \cup V_2 \cup \ldots \cup V_k| = \sum_{r=1}^{k} (-1)^{r+1} \left(\sum_{1 \leq i_1 < i_r \leq k} |V_{i_1} \cap \ldots \cap V_{i_k}| \right)$$

$$|V \setminus (V_1 \cup V_2 \cup \ldots \cup V_k)| = |V| + \sum_{r=1}^{k} (-1)^{r} \left(\sum_{1 \leq i_1 < i_r \leq k} |V_{i_1} \cap \ldots \cap V_{i_k}| \right)$$

Derangements

A **derangement** is a permutation with no fixed points. $\quad$ #(derangements of $[n]$) $= \left\lfloor \frac{n!}{e} + \frac{1}{2} \right\rfloor$

1.2 Counting circular words

1.2.1 The Möbius function

Theorem *Prime decomposition theorem*

For every positive integer $n \in \mathbb{N}$ there is precisely one way to write it as

$$n = p_1^{e_1} p_2^{e_2} \dots p_k^{e_k}$$

where $k \in \mathbb{N}$, $p_1, \dots, p_k$ are primes, and $e_1, \dots, e_n \in \mathbb{N}$.

Definition *Möbius function*

$$\mu(n) := \begin{cases} 1 & \text{if } n = 1 \\ 0 & \text{if } n \mid p^2 \text{ for some prime } p \\ (-1)^k & \text{if } n \text{ is the product of } k \text{ distinct primes} \end{cases}$$

Lemma

$$\sum_{d|n} \mu(n) = \mathbf{1}_{\{1\}} \qquad \forall n \in \mathbb{N}$$

Theorem *Möbius inversion theorem*

Let $F, G : \mathbb{N} \to \mathbb{R}$.

$$F(n) = \sum_{d|n} G(d) \quad \forall n \in \mathbb{N} \quad \Longrightarrow \quad G(n) = \sum_{d|n} \mu(d) F\left(\frac{n}{d}\right) \quad \forall n \in \mathbb{N}$$

1.2.2 Words

Definition *Words*

Let A be an **alphabet** (a finite set). A **word** of length n is a sequence of length n of symbols in A.

We can define two maps on words:

Shift map: $\sigma(w_1 \dots w_n) := w_2 \dots w_n w_1$ **Reverse map:** $\tau(w_1 \dots w_n) = w_n w_{n-1} \dots w_2 w_1$

Definition *Period*

A word w is **periodic** if it is made by repeating a shorter word. Otherwise it is **aperiodic**.
The **period** of a periodic word is the length of the shortest word v such that w is a repeat of v.

1.2.3 Necklaces

Definition *Necklace*

Two words are **shift equivalent** (denoted $w \equiv_{nl} v$) if one can be obtained from the other by some number of shifts.
An equivalence class under this relation, denoted $[w]_{nl}$, is called a **necklace**.

Notation

$$N(n, r) := \#\{\text{necklaces of length n over an alphabet of size r}\}$$

$$A(n, r) := \#\{\text{aperiodic necklaces of length n over an alphabet of size r}\}$$

Theorem *(Macmahon)*

$$A(n, r) = \frac{1}{n} \sum_{d|n} \mu(d) \cdot r^{\frac{n}{d}}$$

Definition *Euler totient function*

$$\varphi(n) := \#\{1 \leq i \leq n : \gcd(i,n) = 1\}$$

Theorem *(Moreau)*

$$N(n,r) = \frac{1}{n}\sum_{d|n}\varphi(n/d)\cdot r^d$$

1.2.4 Bracelets

Definition *Bracelet*

Two words are **shift-reverse equivalent** (denoted $w \equiv_{br} v$) if one can be obtained from the other by some sequence of shifts and reverses. An equivalence class under this relation, denoted $[w]_{br}$, is called a **bracelet**.

Definition *Symmetric and constant necklaces*

A **symmetric necklace** is a necklace where the reverse is equal to some number of shifts.
A **constant word** is a word of the form $(x\dots x)$ for some $x \in [r]$.
A **constant necklace** is a necklace that has a representative word which is constant.

Notation

$$B(n,r) := \#\{\text{bracelets of length n over an alphabet of size r}\}$$

$$S(n,r) := \#\{\text{symmetric necklaces of length n over an alphabet of size r}\}$$

Lemma

If n is odd, then for every symmetric necklace s, there is exactly one $v \in s$ such that $\tau(v) = v$.

Lemma

For n even, and every non-constant symmetric necklace s, one of the following holds:

1. There is precisely one $v \in s$ such that $\tau(v) = v$ and precisely one $u \in s$ such that $\tau(u) = \sigma(u)$
2. There are precisely two $v \in s$ such that $\tau(v) = v$ and no $u \in s$ such that $\tau(u) = \sigma(u)$
3. There are no $v \in s$ such that $\tau(v) = v$ and precisely two $u \in s$ such that $\tau(u) = \sigma(u)$

Theorem

$$B(n,r) = \begin{cases} \frac{1}{2}N(n,r) + \frac{1}{2}r^{(n+1)/2} & \text{if } n \text{ is odd} \\ \frac{1}{2}N(n,r) + \frac{1}{4}(r+1)r^{n/2} & \text{if } n \text{ is even} \end{cases}$$

1.3 Counting graphs

Proposition

There are $2^{\binom{n}{2}}$ distinct graphs on the vertex set $[n]$.

1.3.1 Counting trees

Theorem *(Cayley)*

There are n^{n-2} distinct trees with vertex set $[n]$.

Prüfer codes

We can construct the **Prüfer code** $(c_1, c_2, \dots, c_{n-2})$ of a tree T with n vertices as follows:

1. Assign a label (a real number) to each vertex $v \in V$.
2. Repeat the following steps:
   (a) Find the leaf v with the smallest label amongst all leaves.
   (b) This leaf v has a unique neighbor u. Add u to the code.
   (c) Remove v from the tree.
   (d) If there are only 2 vertices left, stop.

Proposition *Properties of the Prüfer code*

1. Leaves of T do not appear in the code.
2. Each vertex v occurs precisely $\deg(v) - 1$ times in the code.
3. If v is the leaf that is first removed and the code for T is $(c_1, c_2, \dots, c_{n-2})$ then $(c_2, \dots, c_{n-2})$ is the code for $T \setminus v$.
4. We can recover the tree T from its Prüfer code $(c_1, c_2, \dots, c_{n-2})$.

1.3.2 Unlabelled graphs

Definition *Graph isomorphism*

The graphs $G = (V, E)$ and $G' = (V', E')$ are **isomorphic**, denoted $G \cong G'$, if there exists a bijection

$$\varphi : V \to V' \quad \text{such that} \quad vw \in E \iff \varphi(v)\varphi(w) \in E'$$

Such a map φ is called an **isomorphism**.
The set of all graphs is partitioned into **isomorphism classes**, which we also call **unlabelled graphs**.
We denote:

$$\mathrm{Isom}(G, H) := \{\text{isomorphisms from } G \text{ to } H\} \qquad \mathrm{isom}(G, H) := \#\,\mathrm{Isom}(G, H)$$

Notation

For two sequences (a_n) and (b_n), we denote $a_n \sim b_n$ if $\lim_{n\to\infty} \frac{a_n}{b_n} = 1$

Theorem *(Pólya)*

The number u_n of unlabelled graphs on n vertices satisfies $u_n \sim \dfrac{2^{\binom{n}{2}}}{n!}$

Definition *Graph automorphism*

An **automorphism** of a graph $G = (V, E)$ is an isomorphism from G to itself.
We denote:

$$\mathrm{Aut}(G) := \{\text{automorphisms of } G\} \qquad \mathrm{aut}(G) := \#\,\mathrm{Aut}(G)$$

Notation

$$\mathscr{G}_n := \{\text{(labelled) graphs with vertex set } [n]\} \qquad \mathscr{U}_n := \{\text{unlabelled graphs on } n \text{ vertices}\}$$

Lemma

$$|\mathscr{G}_G| = \frac{v(G)!}{\mathrm{aut}(G)}$$

Lemma

If π is not the identity map, then there exist $2 \leq k \leq n$ and distinct $i_1, \dots, i_k \in [n]$ such that

$$\pi(i_1) = i_2, \dots, \pi(i_{k-1}) = i_k \qquad \pi(i_k) = i_1$$

Theorem *(Otter)*

The number t_n of unlabelled trees satisfies

$$t_n \sim c \cdot n^{-\frac{5}{2}} \cdot \alpha^n \qquad c \approx 0.534949606\dots \qquad \alpha \approx 2.95576528565\dots$$

2 Recurrences

Definition *Recursive relation*

We say that (a_n) satisfies a **recursion** (or **recursive relation**) of **order** m if we can write

$$a_n = f(a_{n-1}, ..., a_{n-m}, n) \qquad \text{for all } n \geq m$$

where f is some (fixed) function.

Closed-form expression

We usually want to find an explicit solution (i.e. a function f such that $a_n = f(n)$) for a recurrence, which does not contain symbols like $\sum$, $\prod$ or $\dots$. This is sometimes called a **closed-form expression**.

2.1 Linear recurrences with constant coefficients

Definition *Linear recursion with constant coefficients*

A **linear recursion** is of the form

$$a_n = f_1(n) \cdot a_1 + \dots + f_m(n) \cdot a_n + g(n)$$

If the coefficients do not depend on n, then we speak of a **linear recursion with constant coefficients**.
If $g(n) = 0$, the recurrence is **homogeneous**. Otherwise, it is **inhomogeneous**.

2.1.1 Homogeneous recurrences

Proposition

Consider a linear, homogeneous recursion with constant coefficients. Then the set of all sequences that satisfies it:

$$\mathcal{S} := \{(a_n) : a_n + c_1 a_{n-1} + \dots + c_m a_{n-m} = 0 \text{ for all } n \geq m\}$$

is a vector space over $\mathbb{C}$. Provided that $c_m \neq 0$, the dimension of this vector space is m.

Definition *Characteristic polynomial*

Consider a linear, homogeneous recursion with constant coefficients. Its **characteristic polynomial** is:

$$P(z) = z^m + c_1 z^{m-1} + \dots + c_m$$

and its **characteristic equation** is $P(z) = 0$.

Theorem *Fundamental theorem of algebra*

Any complex polynomial $P(z)$ of degree n can be written as:

$$(z - r_1)(z - r_2) \dots (z - r_n) \qquad r_1, \dots, r_n \in \mathbb{C}$$

Lemma

Consider a linear, homogeneous recursion with constant coefficients.
Any $r \neq 0$ is a root of the characteristic polynomial if and only if $a_n := r^n$ is a solution of the recursion.

Proposition

Consider a linear, homogeneous recursion with constant coefficients. Any $r \neq 0$ is a root of the characteristic polynomial of multiplicity $> i$ if and only if the sequence $a_n := n^i r^n$ is a solution of the recursion.

Lemma

Let P be an arbitrary polynomial and $i \in \mathbb{N}$.

1. If P has a root of multiplicity $> i$ at r then its derivative P' has a root of multiplicity $> i - 1$ at r.
2. If P has a root at r, and P' has a root of multiplicity $> i - 1$ at r, then r has multiplicity $> i$ in P.

Theorem

Consider a linear, homogeneous recursion with constant coefficients, and suppose the roots of $P(z)$ are $r_1, \ldots, r_k$ with r_j having multiplicity m_j. Every solution of the recurrence is of the form

$$a_n = P_1(n)r_1^n + \ldots + P_k(n)r_k^n$$

where P_j is a polynomial of degree $\leq m_j - 1$, and every sequence of this form is a solution of the recurrence.
Alternatively:

$$\mathcal{S} = \operatorname{span}\{r_1^n, \ldots, n^{m_1-1}r_1^n, \ldots, r_k^n, \ldots, n^{m_k-1}r_k^n\}$$

2.1.2 Inhomogeneous recurrences

Theorem

Consider a linear, inhomogeneous recursion with constant coefficients.
Let $a_n^{(p)}$ be a (particular) solution of the inhomogeneous recursion.
Then all solutions are of the form $a_n^{(p)} + a_n^{(h)}$ for some solution $a_n^{(h)}$ of the homogeneous case.

Combined with the previous theorem, we have for any linear recursion with constant coefficients:

$$a_n = a_n^{(h)} + P_1(n)r_1^n + \ldots + P_k(n)r_k^n$$

Lemma

Let $c_0, c_1, \ldots, c_m \in \mathbb{R}$ with $c_0 \neq 0$ and let $a_n = n^k r^n$ where k is a nonnegative integer and $r \in \mathbb{C}$. Then

$$c_0 a_n + c_1 a_{n-1} + \ldots + c_m a_{n-m} = R(n) \cdot r^n$$

where R is a polynomial of degree $k + j$, and j is the multiplicity of r if r is a root of

$$P(z) := c_0 z^m + c_1 z^{m-1} + \ldots + c_m$$

and 0 otherwise. Moreover, the coefficient of n^{k-j} in R is

$$\binom{k}{j} \cdot \frac{P^{(j)}(r)}{r^{m-j}}$$

where $P^{(j)}$ denotes the j-th derivative of P.

Theorem

Consider an inhomogeneous recursion with linear coefficients of the following form:

$$a_n + c_1 a_{n-1} + \ldots + c_m a_{n-m} = Q(n) \cdot r^n$$

where $Q(n)$ is a polynomial of degree k. There is a particular solution:

$$a_n^{(p)} = R(n) \cdot r(n)$$

where R is a polynomial of degree $k + j$, and j is the multiplicity of r if r is a root of $P(z)$, and 0 otherwise.

2.2 Ordinary generating functions

Definition *Generating function*

If $a_0, a_1, \ldots$ is a sequence of numbers then its (ordinary) **generating function** is the following power series:

$$A(z) := \sum_{n=0}^{\infty} a_n z^n = a_0 + a_1 z + b_2 z^2 + \ldots$$

We use the notation $[z^n]A(z) := a_n$ for the coefficient of z_n in $A(z)$.

Proposition

Let $A(z)$ and $B(z)$ be generating functions with positive radius of convergence:

$$A(z) = a_0 + a_1 z + b_2 z^2 + \ldots = \sum_{n=0}^{\infty} a_n z^n \qquad B(z) = b_0 + b_1 z + b_2 z^2 + \ldots = \sum_{n=0}^{\infty} b_n z^n$$

Then the the following are also generating functions with positive radius of convergence.

1. $A(z) + B(z) = (a_0 + b_0) + (a_1 + b_1)z + (a_2 + b_2)z^2 + \ldots = \sum_{n=0}^{\infty} (a_n + b_n) z^n$
2. $A(z) \cdot B(z) = a_0 b_0 + (a_0 b_1 + a_1 b_0)z + (a_0 b_2 + a_1 b_1 + a_2 b_0)z^2 = \sum_{n=0}^{\infty} z_n \cdot \left(\sum_{i=0}^{n} a_i b_{n-i} \right)$ **(Convolution formula)**
3. $A'(z) = \sum_{n=0}^{\infty} n a_n z^{n-1} = \sum_{n=0}^{\infty} (n+1) a_{n+1} z^n$
4. $\int_0^z A(t) \, \mathrm{d}t = \sum_{n=0}^{\infty} \frac{1}{n+1} a_n z^{n+1} = \sum_{n=0}^{\infty} \frac{1}{n} a_{n-1} z^n$

Proposition

Suppose (a_n) is a sequence such that $|a_n| < K^n$ for some constant $K > 0$.
Then the power series $A(z)$ has a positive radius of convergence and the derivatives of A of all orders exist at 0, and satisfy:

$$A^{(n)}(0) = n! \cdot a_n$$

where $A^{(n)}$ denotes the n-th derivative of A.

Examples of generating functions

Sequence	Generating function
$a_0, a_1, a_2, \ldots$	$A(z)$
$0, a_0, a_1, \ldots$	$aA(z)$
$a_1, a_2, a_3, \ldots$	$\frac{1}{z} \cdot (A(z) - a_0)$
$a_0, 0, a_1, 0, a_2, \ldots$	$A(z^2)$
$a_0, 0, a_2, 0, a_4, \ldots$	$\frac{1}{2}(A(z) + A(-z))$
Partial sums of (a_n)	$\frac{1}{1-z} \cdot A(z)$
Fibonacci sequence	$\frac{1}{1-z-z^2}$

2.2.1 Generalized binomial coefficient

Definition *Generalized binomial coefficient*

For $\alpha \in \mathbb{R}$ and $n \in \mathbb{N}_0$, the **generalized binomial coefficient** is given by:

$$\binom{\alpha}{n} := \frac{\alpha \cdot (\alpha - 1) \cdot \ldots \cdot (\alpha - n + 1)}{n!}$$

Theorem *Generalized binomial theorem*

For $|z| < 1$ and $\alpha \in \mathbb{R}$ we have

$$(1+z)^\alpha = \sum_{n=0}^{\infty} \binom{\alpha}{n} z^n$$

2.2.2 Catalan numbers

Definition *Catalan numbers*

$$c_n = \frac{1}{n+1}\binom{2n}{n}$$

Definition *Dyck word and path*

A **Dyck word** is a word $w = w_1 w_2 \ldots w_{2n}$ over the alphabet $\{0, 1\}$ of length $2n$ with exactly n zeroes and n ones, such that for each $i \leq 2n$, the number of ones in $w_1 \ldots w_i$ is greater than or equal to the number of zeroes.

A **Dyck path** is a path of length $2n$ in the integer grid $\{0, \ldots, n\} \times \{0, \ldots, n\}$ with the property that the path starts at the origin $(0, 0)$, ends at (n, n), at each step either goes right or up, and is never below the diagonal $y = x$.

Proposition

The following are equal to the Catalan number c_n:

- The number of ways to add non-intersecting line segments between the corner points of a convex n-gon such that the line segments dissect the polygon into triangles.
- The number of Dyck words of length $2n$
- The number of Dyck paths of length $2n$
- The number of planted plane trees (explained further in lecture 9, page 4)

Definition *Pattern-avoiding permutations*

Let $\sigma \in S_k$ be a permutation of $[k]$. A permutation $\pi \in S_n$ of $[n]$ **contains the pattern** σ if:

$$\text{there exist} \quad i_1 < i_2 < \ldots < i_k \quad \text{such that} \quad \pi(i_{\sigma^{-1}(1)}) < \pi(i_{\sigma^{-1}(2)}) < \cdots < \pi(i_{\sigma^{-1}(k)})$$

We say π avoids σ if it does not contain the pattern σ, and for notational convenience we set:

$$\mathrm{Av}(n,\sigma) := \{\pi \in S_n : \pi \text{ avoids } \sigma\} \qquad \mathrm{av}(n,\sigma) := |\,\mathrm{Av}(n,\sigma)|$$

Theorem

$\mathrm{av}(n,\sigma)$ is equal to the Catalan number c_n for all $\sigma \in S_3$.

2.3 Exponential generating functions

Definition *Exponential generating function*

The **exponential generating function** of the sequence $a_0, a_1, a_2, \ldots$ is:

$$\hat{A}(z) := \sum_{n=0}^{\infty} a_n \frac{z^n}{n!}$$

Examples of transformed exponential generating functions

Sequence	EGF
$a_0, a_1, a_2, \ldots$	$\hat{A}(z)$
$1, 1, 1, \ldots$	e^z
$a_1, a_2, a_3, \ldots$	$\hat{A}'(z)$
$0, a_0, a_1, \ldots$	$\int \hat{A}(z)$
$0, a_1, 2a_2, 3a_3, \ldots$	$z\hat{A}(z)$

Proposition *Binomial convolution formula*

$$\hat{A}(z) \cdot \hat{B}(z) = \sum_{n=0}^{\infty} \frac{z^n}{n!} \cdot \left(\sum_{i=0}^{n} \binom{n}{i} \cdot a_i \cdot b_{n-i} \right)$$

Definition *Multinomial coefficient*

$$\binom{n}{n_1, \ldots, n_k} = \frac{n!}{n_1! \cdots n_k!} \quad (\text{provided } n_1 + \cdots + n_k = n)$$

2.3.1 Bernoulli numbers

Definition *Bernoulli numbers*

The **Bernoulli numbers** are defined recursively by:

$$b_0 = 1, \quad \sum_{j=0}^{k} \binom{k+1}{j} \cdot b_j = 0 \quad (k \geq 1)$$

Theorem *Faulhaber's formula*

$$\sum_{i=0}^{n-1} i^k = \frac{1}{k+1} \cdot \left(\binom{k+1}{0} \cdot b_0 \cdot n^{k+1} + \binom{k+1}{1} \cdot b_1 \cdot n^k + \binom{k+1}{2} \cdot b_2 \cdot n^{k-1} + \cdots + \binom{k+1}{k} \cdot b_k \cdot n \right)$$

2.3.2 Stirling numbers

Definition *Stirling numbers of the second kind*

We denote the number of ordered partitions of $[n]$ into k non-empty parts by $o_{n,k}$. The **Stirling numbers of the second kind**, denoted $u_{n,k}$ or $\left\{ n \atop k \right\}$, are the number of unordered partitions of $[n]$ into k non-empty parts.

Partitions of $[n]$ into k non-empty parts

$$o_{n,k} = \sum_{j=0}^{k} \binom{k}{j} j^n (-1)^{k-j} \qquad u_{n,k} = \frac{1}{k!} \cdot o_{n,k} = \frac{1}{k!} \cdot \sum_{j=0}^{k} \binom{k}{j} j^n (-1)^{k-j}$$

Definition *Bell numbers*

The **Bell number** b_n is the total number of unordered partitions of $[n]$, into any number of parts.

Theorem *Dobiński's formula*

$$b_n = \frac{1}{e} \cdot \sum_{k=0}^{\infty} \frac{k^n}{k!}$$

Definition *Stirling numbers of the first kind*

The (unsigned) **Stirling number of the first kind**, denoted $s_{n,k}$ or $\left[n \atop k \right]$, is the number of permutations $\pi \in S_n$ that have exactly k cycles. The **signed Stirling numbers of the first kind** are $(-1)^{n-k} \cdot s_{n,k}$.

Lemma

$$\begin{bmatrix} n+1 \\ k \end{bmatrix} = \begin{bmatrix} n \\ k-1 \end{bmatrix} + n \cdot \begin{bmatrix} n \\ k \end{bmatrix} \qquad \text{for all } n, k \geq 1$$

Proposition

$$(z)_n = \sum_{k=0}^{n} (-1)^{n-k} \begin{bmatrix} n \\ k \end{bmatrix} z^k$$

Corollary

$$\begin{bmatrix} n \\ k \end{bmatrix} = \sum_{0<i_1<\cdots<i_{n-k}<n} i_1 \cdots i_{n-k}$$

Theorem *Stirling inversion*

Let (a_n) and (b_n) be sequences of numbers.

$$b_n = \sum_{k=0}^{n} \left\{ n \atop k \right\} a_k \quad \text{for all } n \qquad \iff \qquad a_n = \sum_{k=0}^{n} (-1)^{n-k} \begin{bmatrix} n \\ k \end{bmatrix} b_k \quad \text{for all } n$$

3 Extremal graph and set theory

3.1 Ramsey theory

Definition *Ramsey numbers*

$$R(s,t) := \inf\{n : \text{in every red-blue colouring of the edges of } K_n \text{ there is either a red } K_s \text{ or a blue } K_t\}$$

Theorem *(Ramsey)*

$R(s,t) < \infty$ for all $s, t \in \mathbb{N}$.

Theorem *(Erdös)*

If n, t satisfy $\binom{n}{t}2^{1-\binom{t}{2}} < 1$, then $R(t,t) > n$.

Theorem *(Erdös-Szekeres)*

$R(s+1,t+1) \leq R(s,t+1) + R(s+1,t)$ for all $s,t \geq 1$

Corollary

$R(s,t) \leq 2^{s+t}$ for all $s,t \geq 1$.

Theorem

$$\sqrt{2}^t \leq R(t,t) \leq 4^t$$

3.2 High girth and chromatic number

Definition *Chromatic number*

A k-**colouring** of a graph G is a map $f : V(G) \to [k]$ with the property that $f(u) \neq f(v)$ whenever $uv \in E(G)$.
The **chromatic number** of G, denoted $\chi(G)$, is the least k for which a k-colouring exists.

Definition *Stable set*

A **stable set** in a graph G is a subset $A \subseteq V(G)$ of the vertices such that $ab \notin E(G)$ for all $a, b \in A$.
The **stability number** or **independence number** of G, denoted $\alpha(G)$, is the cardinality of the largest stable set.

Definition *Girth*

The **girth** of a graph G is the length of the shortest cycle in G.

Theorem *(Erdös)*

For every k, ℓ there exists a graph G with $\chi(G) > k$ and girth$(G) > \ell$.

3.3 Crossing numbers

Definition *Crossing number*

The **crossing number** $\mathrm{cr}(G)$ of a graph G is the least number of crossings in a drawing of G in the plane.
The **rectilinear crossing number** $\mathrm{rcr}(G)$ of G is the minimum number of crossings in a **rectilinear drawing** of G.
A rectilinear drawing is a drawing of a graph where all edges are straight line segments.

Theorem *Crossing number inequality*

$$cr(G) \geq \frac{e(G)^3}{64v(G)^2} \qquad \text{provided } e(G) \geq 4v(G)$$

Theorem *(Euler)*

$$v(G) - e(G) + f(G) = 2$$

Corollary

If G is planar then $e(G) \leq 3v(G)$; if G is planar and $v(G) \geq 3$ then $e(G) \leq 3v(G) - 6$.

Theorem *(Wagner)*

If G is planar then it has a rectilinear drawing that is crossing free.

Theorem *(Bienstock-Dean)*

1. If $\mathrm{cr}(G) \leq 3$ then $\mathrm{rcr}(G) = \mathrm{cr}(G)$
2. For every k, there exists a graph G with $\mathrm{cr}(G) = 4$ and $\mathrm{rcr}(G) > k$.

3.3.1 Point-line incidences and unit distances

Definition *Point-line incidences*

Let $P \subseteq \mathbb{R}^2$ be a set of points and L a set of lines. The number of **point-line incidences** is defined as:

$$I(P, L) := \#\{(p, \ell) : p \in P, \ell \in L, p \in \ell\}$$

Theorem *(Szemerédi-Trotter)*

$$I(P, L) \leq 4(|P||L|)^{2/3} + |L| + 4|P|$$

Definition *Maximum number of unit distances*

$$u(n) := \max_{\substack{P \subseteq \mathbb{R}^2 \\ |P| = n}} \#\{(p, q) : p, q \in P, \|p - q\| = 1\}\}$$

Theorem *(Erdös)*

For n sufficiently large, there exists a constant $c > 0$ such that $u(n) > n^{1 + \frac{c}{\log \log n}}$.

Theorem *(Spencer,Szemerédi,Trotter)*

$$u(n) = \mathcal{O}(n^{4/3})$$

3.4 Extremal set theory

Definition *Intersecting and uniform family*

Let V be a finite set. A **family** $\mathscr{F} \subseteq 2^V$ of subsets of V is **intersecting** if $A \cap B \neq \varnothing$ for all $A, B \in \mathscr{F}$.
A family $\mathscr{F}$ is k-**uniform**, denoted $\mathscr{F} \subseteq \binom{V}{k}$, if all sets in $\mathscr{F}$ have cardinality k.

Proposition

Let V be a finite set with n elements and let $\mathscr{F} \subseteq 2^V$. If $\mathscr{F}$ is intersecting, then $|\mathscr{F}| \leq 2^{n-1}$
(Note: this bound is attained by $\mathscr{F} = \{A \subseteq V : v \in A\}$ for some arbitrary $v \in V$)

Lemma

Let V be a finite set, $\sigma : V \to V$ a permutation and $\mathscr{F} \subseteq \binom{V}{k}$ an intersecting family. Define:

$$A_s := \{s, s+1, \dots, s+k-1\} \qquad A_s^\sigma := \{\sigma(s), \sigma(s+1), \dots, \sigma(s+k-1)\}$$

where addition is modulo n. Then:

- $\mathscr{F}$ contains at most k of the sets $A_0, A_1, \dots, A_{n-1}$
- For every permutation σ, $\mathscr{F}$ contains at most k of the sets $A_0^\sigma, A_1^\sigma, \dots, A_{n-1}^\sigma$

Theorem *(Erdös-Ko-Rado)*

If V is finite, $k \leq \frac{|V|}{2}$ and $\mathscr{F} \subseteq \binom{V}{k}$ is intersecting, then $|\mathscr{F}| \leq \binom{|V|-1}{k-1}$
(Note: this bound is attained by $\mathscr{F} = \{A \subseteq V : |A| = k, v \in A\}$ for some arbitrary $v \in V$)

Theorem

Let $\mathscr{F} \subseteq 2^{[n]}$ be a family of subsets of $[n]$ such that

1. $|F|$ is odd for all $F \in \mathscr{F}$
2. $|F \cap G|$ is even for all for all distinct $F, G \in \mathscr{F}$.

Then $|\mathscr{F}| \leq n$. (Note: this bound is attained by $\mathscr{F} = \{\{1\}, \{2\}, \ldots, \{n\}\}$.)

Theorem *Generalized Fisher inequality*

Let $\mathscr{F} \subseteq 2^{[n]}$ and $1 \leq t \leq n$ be such that $|F \cap G| = t$ for all distinct $F, G \in \mathscr{F}$. Then $|\mathscr{F}| \leq n$

3.5 More extremal graph theory

Theorem

K_n cannot be decomposed into fewer then $n-1$ complete bipartite graphs, for every $n \geq 1$.

Theorem *(Hoffman, Singleton)*

If there exists a graph G with $\operatorname{girth}(G) \geq 5$, all degrees $\geq k$ and $v(G) = k^2 + 1$, then $k \in \{1, 2, 3, 7, 57\}$.

Index