

Combinatorics, Graphs, Matroids

August 25, 2026
14:22

Continuous updates of these lecture notes can be found on the eCampus web page of the lecture course “Combinatorics, Graphs, Matroids” from the winter term 2025/2026.

Table of Contents

1	Introduction	4
1.1	Fundamental Counting Rules	4
1.2	Elementary Counting Coefficients	5
1.3	Assignments	8
1.4	Generalized Counting Coefficients	9
1.5	Permutations	11
1.6	Further Combinatorial Techniques	14
2	Computation of Sums	18
2.1	Sums: Direct Methods	18
2.2	Difference and Sum Operators	20
2.3	Inversions	25
3	Solving Recursions	28
3.1	Linear Recursions of Depth 1	28
3.2	Generating Functions	30
3.3	Using Generating Functions to Solve Recursions	31
3.4	Exponential Generating Functions	36
4	Planar Graphs	38
4.1	Basic Definitions and Results	38
4.2	Kuratowski-Wagner Theorem	43
5	Colorings of Graphs	47
5.1	Vertex Colorings	47
5.2	Chromatic Polynomials	54
5.3	List-Colorings	57
5.4	Edge Colorings	59
6	Matroids	64

6.1	Independence Systems and Matroids	64
6.2	Dual Independence Systems	74
6.3	The Greedy Algorithm	76
6.4	Matroid Intersection	81
6.5	Matroid Partitioning	87

I Combinatorics

This part of the notes is more or less a summary of the corresponding chapters in Aigner [2007] (with some contributions from Steger [2007]).

1 Introduction

Combinatorics is a mathematical area dealing with finite or at least countably infinite discrete sets and structures. In particular, our main goal is to “count” things, i.e. to determine the number of elements in specified (typically finite) sets. To this end, we will consider several approaches and methods for counting.

The following counting rules are completely obvious but very useful.

1.1 Fundamental Counting Rules

- (I) For pairwise disjoint finite sets $U_1, \dots, U_n$, we have $|\bigcup_{i=1}^n U_i| = \sum_{i=1}^n |U_i|$.
- (II) For finite sets $U_1, \dots, U_n$, we have $|U_1 \times \dots \times U_n| = \prod_{i=1}^n |U_i|$.
- (III) If there is a bijection between two finite sets S and T , then $|S| = |T|$.

Examples:

We call a set an n -set if it is a finite set with $n \in \mathbb{N}$ elements (where $\mathbb{N}$ includes 0).

Proposition 1 *For two n -sets A and B , the number of bijections from A to B is $n!$.*

Proof: Let U be the set of bijections from A to B . Apply induction on n . The case $n = 0$ is trivial because then $0! = 1 = |U|$. Let $n > 0$ and $x \in A$. For $i \in B$, let U_i be the set of all bijections f from A to B with $f(x) = i$. Then by induction $|U_i| = (n-1)!$ for $i \in B$. Moreover, we have $U = \dot{\bigcup}_{i \in B} U_i$, so by (I) we get $|U| = \sum_{i \in B} |U_i| = n \cdot (n-1)! = n!$. $\square$

Corollary 2 *The number of permutations of an n -set is $n!$.* $\square$

Proposition 3 *The number of mappings from a k -set A to an n -set B is n^k .*

Proof: There is a bijection between the set of all mappings from A to B and the set $\underbrace{B \times \dots \times B}_{k \text{ times}}$. Thus by (III) and (II), the number of such mappings is $|B|^k = n^k$. $\square$

Notation: We denote the set of all mappings from A to B by B^A .

Proposition 4 *The number of subsets of an n -set is 2^n .*

Proof: For an n -set A , there is a bijection between its power set (i.e. the set of its subsets) and the set of mappings from A to $\{0, 1\}$: For each $B \subseteq A$ define a mapping $f_B : A \rightarrow \{0, 1\}$ by setting $f_B(x) = 1$ if and only if $x \in B$. Then, $B \mapsto f_B$ is clearly a bijection. Thus, the statement follows from (III) and the previous proposition. $\square$

Notation: We denote the power set of a set A by 2^A .

What does counting mean? Possible answers can be:

- (i) direct, closed formula,
- (ii) sum,
- (iii) recursive formula.

Example: Consider the number y_n of 0-1-2-strings of length n with an even number of 1s and an odd number of 2s. Then, one easily gets an answer of type (ii): $y_n = \sum_{i=0}^{\lfloor \frac{n-1}{2} \rfloor} \binom{n}{2i+1} 2^{2i}$. Also a recursive solution can be found easily: $y_n = 3^{n-1} - y_{n-1}$ for $n \in \mathbb{N} \setminus \{0\}$ (see exercises for the correctness of the formulas). We will examine methods to transform such sum and recursive formulas into a closed formula.

1.2 Elementary Counting Coefficients

The most important counting coefficient is the **binomial coefficient** $\binom{n}{k}$ which is defined as the number of k -subsets of an n -set (for $k, n \in \mathbb{N}$).

Proposition 5 *Let $n, k \in \mathbb{N}$ with $k \leq n$. Then:*

- (a) $\binom{n}{k} = \binom{n}{n-k}$.
- (b) $\binom{n}{k} = \binom{n-1}{k-1} + \binom{n-1}{k}$ for $k \geq 1$.
- (c) $\binom{n}{k} = \frac{n!}{k!(n-k)!}$.

Proof:

- (a) Trivial.

(b) Let M be an n -set and let $x \in M$ be an arbitrary element. Then

$$\begin{aligned}
\binom{n}{k} &= |\{N \in 2^M \mid |N| = k\}| \\
&= |\{N \in 2^M \mid |N| = k, x \in N\} \cup \{N \in 2^M \mid |N| = k, x \notin N\}| \\
&= |\{N \in 2^M \mid |N| = k, x \in N\}| + |\{N \in 2^M \mid |N| = k, x \notin N\}| \\
&= \binom{n-1}{k-1} + \binom{n-1}{k}.
\end{aligned}$$

(c) Induction on n . The case $n = 0$ is trivial, so assume $n > 0$. If $k = 0$ or $k = n$ then both sides of the equation are 1. Thus, we can assume $0 < k < n$. Then

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

□

		k						
		0	1	2	3	4	5	6
n	0	1						
	1	1	1					
	2	1	2	1				
	3	1	3	3	1			
	4	1	4	6	4	1		
	5	1	5	10	10	5	1	
	6	1	6	15	20	15	6	1

Table 1: Pascal's triangle with the entries $\binom{n}{k}$.

Arranged in a table, the binomial coefficients form Pascal's triangle (see Table 1). Using Proposition 5 (b), every entry here is simply the sum of the entry above it and the entry diagonally left above it (if available). We consider three sums in Pascal's triangle. The following statements can be proven easily by induction but we will show them by "combinatorial arguments".

- Row sums: $\sum_{k=0}^n \binom{n}{k} = 2^n$.

This is quite obvious as both terms denote the number of all subsets of an n -set.

- Column sums: $\sum_{m=0}^n \binom{m}{k} = \binom{n+1}{k+1}$ for $n, k \in \mathbb{N}$.

For $m \in \{0, \dots, n\}$, $\binom{m}{k}$ is the number of ways to choose $k+1$ numbers from the set $\{1, \dots, m+1\}$ under the condition that $m+1$ is the largest chosen number.

- Diagonal sums: $\sum_{k=0}^n \binom{m+k}{k} = \binom{m+n+1}{n}$ for $m, n \in \mathbb{N}$.
For $k \in \{0, \dots, n\}$, $\binom{m+k}{k}$ is the number of ways to choose n numbers from the set $\{1, \dots, m+n+1\}$ under the condition that $m+k+1$ is the largest number that is not chosen.

Proposition 6 (*Binomial theorem*): For $x, y \in \mathbb{R}$ and $n \in \mathbb{N}$, we have:

$$(x + y)^n = \sum_{k=0}^n \binom{n}{k} x^k y^{n-k}.$$

Proof: The coefficient of $x^k y^{n-k}$ in the sum is the number of ways to choose the term x from k of the n factors $(x + y) \cdots (x + y)$. $\square$

Definition 1 For $n, k \in \mathbb{N}$ let $S_{n,k}$ be the number of ways to partition an n -set into k non-empty sets (where we set $S_{0,0} = 1$). The numbers $S_{n,k}$ are called **Stirling numbers of the second kind**.

In particular for $n > 0$: $S_{n,0} = 0$, $S_{n,1} = 1$, $S_{n,2} = 2^{n-1} - 1$.

Proposition 7 For $n, k \in \mathbb{N} \setminus \{0\}$ we have

$$S_{n,k} = S_{n-1,k-1} + kS_{n-1,k}.$$

Proof: Let M be an n -set and $x \in M$. The set of partitions of M into k non-empty subsets can be decomposed in the set of partitions with the set $\{x\}$ (there are $S_{n-1,k-1}$ of them) and the set of partitions where x is an element in a set with more than one element (there are $kS_{n-1,k}$ of them). $\square$

Of course, this recursion formula can be used to fill a table with Stirling's numbers of the second kind in a way similar to Pascal's triangle (see Aigner [2007], p. 21, for a small part of this table).

Definition 2 For $n, k \in \mathbb{N}$, let $P_{n,k}$ be the number of ways to write n as the sum of k positive integers (without considering the order of the summands). In addition, we set $P_{0,0} = 1$.

For example, $P_{6,3} = 3$ because $6 = 4 + 1 + 1 = 3 + 2 + 1 = 2 + 2 + 2$ can be written in three different ways as a sum of three positive integers.

For $n > 0$, we have $P_{n,0} = 0$, $P_{n,1} = 1$, $P_{n,2} = \lfloor \frac{n}{2} \rfloor$.

Observation: For $n, k \in \mathbb{N} \setminus \{0\}$ with $n \geq k$, we have $P_{n,k} = P_{n-k,k} + P_{n-1,k-1}$. The proof of this recursion is left as an exercise.

We can also consider *ordered* partitions of numbers. For example, there are 6 ordered 3-partitions of 5: $3 + 1 + 1$, $1 + 3 + 1$, $1 + 1 + 3$, $2 + 2 + 1$, $2 + 1 + 2$, and $1 + 2 + 2$.

Theorem 8 For $1 \leq k \leq n$, the number of ordered partitions of a positive integer n into k positive summands is $\binom{n-1}{k-1}$.

Proof: Any positive integer number n can be written as a sum of n ones, and these ones can be partitioned into subsequences with lengths $x_1, \dots, x_k$:

$$n = \underbrace{1 + \dots + 1}_{x_1} \oplus \underbrace{1 + \dots + 1}_{x_2} \oplus \dots \oplus \underbrace{1 + \dots + 1}_{x_k}$$

There is a one-to-one correspondence between the partitionings of the sequence of ones into subsequences and the ordered k -partitions of n . Thus, each ordered k -partition of n is given by the choice of the $\oplus$ -signs. There are $\binom{n-1}{k-1}$ ways to choose the $k-1$ $\oplus$ -signs, which implies that also the number of ordered k -partitions of n is $\binom{n-1}{k-1}$. $\square$

1.3 Assignments

Observations:

- The number of *surjective* mappings from an n -set to an r -set is $r!S_{n,r}$. To see this, note that there are $S_{n,r}$ ways to partition an n -set into r preimages, and for each such partition we get $r!$ ways to assign the preimages to the elements of an r -set.
- The number of *injective* mappings from an n -set to an r -set is

$$r^{\underline{n}} := r(r-1) \dots (r-n+1).$$

We call $r^{\underline{n}}$ the n -th **falling factorial** of r .

Analogously, we define the n -th **rising factorial** of r as

$$r^{\overline{n}} := r(r+1) \dots (r+n-1).$$

Definition 3 A k -**multiset** over an n -set A is a mapping $f : A \rightarrow \mathbb{N}$ such that $\sum_{a \in A} f(a) = k$.

We can consider multisets as a generalization of sets that can contain the same element more than once. The mapping f denotes how often an element occurs (but note that $f(a) = 0$ is possible). Thus we write a k -multiset as $\{a_1, \dots, a_k\}$ but in this case there can be numbers $i, j \in \{1, \dots, k\}$ with $i \neq j$ but $a_i = a_j$.

Proposition 9 *The number of k -multisets over an n -set is $\frac{n^{\bar{k}}}{k!} = \binom{n+k-1}{k}$.*

Proof: There is a bijection f between the set of all k -multisets over $\{1, \dots, n\}$ and the set of all k -subsets of $\{1, \dots, n+k-1\}$: For a k -multiset $\{a_1, \dots, a_k\}$ with $a_1 \leq a_2 \leq \dots \leq a_k$ define $f(\{a_1, \dots, a_k\})$ as $\{a_1, a_2+1, a_3+2, \dots, a_k+k-1\}$. It is easy to check that this is indeed a bijection between the two sets. Since there are $\frac{n^{\bar{k}}}{k!} = \binom{n+k-1}{k}$ k -subsets of $\{1, \dots, n+k-1\}$, this proves the proposition. $\square$

Proposition 10 *For $n, r \in \mathbb{N}$, we have*

$$r^n = \sum_{k=0}^n S_{n,k} r^{\bar{k}}.$$

Proof: For two sets A and B , let $\text{Surj}(A, B)$ be the set of surjective mappings from A to B . Let N be an n -set and R an r -set. Then the number of mappings from N to R is r^n , so

$$r^n = \sum_{A \subseteq R} |\text{Surj}(N, A)| = \sum_{k=0}^r \sum_{A \subseteq R, |A|=k} |\text{Surj}(N, A)| = \sum_{k=0}^r \binom{r}{k} k! S_{n,k} = \sum_{k=0}^r S_{n,k} r^{\bar{k}} = \sum_{k=0}^n S_{n,k} r^{\bar{k}}$$

For the last equation, we made use of the fact that $S_{n,k} = 0$ for $k > n$ and $r^{\bar{k}} = 0$ for $k > r$. $\square$

Assume that we want to count the ways to assign a set of n balls to r bins. We may or may not be able to distinguish the balls and we may or may not be able to distinguish the bins. Table 2 gives an overview of the number of assignments.

Remarks on Table 2: Most of the entries are easy consequences of previous results. Assume that we can distinguish the elements of R but not the elements of N . Then, the number of all mappings from N to R is $\frac{r^{\bar{n}}}{n!}$ because this is the number of n -multisets over an r -set. The number of surjective mappings from N to R is the number of ordered partitions of the number n into r summands, hence it is $\binom{n-1}{r-1}$.

1.4 Generalized Counting Coefficients

We generalize the definitions of the rising and falling factorials by setting for $r \in \mathbb{C}$ and $k \in \mathbb{N}$:

$$r^{\bar{k}} := r(r-1)(r-2) \dots (r-k+1)$$

elements distinguishable N R		Mapping $f : N \rightarrow R$			
		arbitrary	injective	surjective	bijective
Yes	Yes	r^n	$r^{\underline{n}}$	$r!S_{n,r}$	$\begin{matrix} 0 & (n \neq r) \\ n! & (n = r) \end{matrix}$
No	Yes	$\frac{r^{\bar{n}}}{n!}$	$\binom{r}{n}$	$\binom{n-1}{r-1}$	$\begin{matrix} 0 & (n \neq r) \\ 1 & (n = r) \end{matrix}$
Yes	No	$\sum_{k=1}^r S_{n,k}$	$\begin{matrix} 0 & (r < n) \\ 1 & (r \geq n) \end{matrix}$	$S_{n,r}$	$\begin{matrix} 0 & (n \neq r) \\ 1 & (n = r) \end{matrix}$
No	No	$\sum_{k=1}^r P_{n,k}$	$\begin{matrix} 0 & (r < n) \\ 1 & (r \geq n) \end{matrix}$	$P_{n,r}$	$\begin{matrix} 0 & (n \neq r) \\ 1 & (n = r) \end{matrix}$

Table 2: Number of mappings from an n -set N to an r -set R with and without additional constraints.

and

$$r^{\bar{k}} := r(r+1)(r+2) \dots (r+k-1)$$

We also generalize the binomial coefficients, by setting for $r \in \mathbb{C}$ and $k \in \mathbb{Z}$:

$$\binom{r}{k} := \begin{cases} \frac{r^{\bar{k}}}{k!} & \text{for } k \geq 0 \\ 0 & \text{for } k < 0 \end{cases}$$

The recursive formula from Proposition 5(b) can now be generalized to $r \in \mathbb{C}$ and $k \in \mathbb{Z}$:

$$\binom{r}{k} = \binom{r-1}{k-1} + \binom{r-1}{k} \quad (1)$$

For a proof, we can simply use the definition of $\binom{r}{k}$, but we can also apply the “polynomial method”: For fixed $k > 0$ (the case $k \leq 0$ is easy), both sides of equation (1) are polynomials in r of degree k . Since we have proved (1) for any positive integer r , we know that both polynomials have the same values at an infinite number of values of r . This means they must be identical. This proves (1).

Proposition 11 (*Vandermonde identity*): For $x, y \in \mathbb{C}$ and $n \in \mathbb{N}$, we have:

$$\binom{x+y}{n} = \sum_{k=0}^n \binom{x}{k} \binom{y}{n-k}$$

Proof: Again, we can use the polynomial method: For $x, y \in \mathbb{N}$, this is true because both terms describe the number of n -subsets of an $(x+y)$ -set. For general values of x and y , the statement follows because both terms are polynomials of degree n and are identical on the infinite grid $\mathbb{N} \times \mathbb{N}$. $\square$

Proposition 12 For $r \in \mathbb{C}$ and $k \in \mathbb{Z}$:

$$\binom{-r}{k} = (-1)^k \binom{r+k-1}{k}.$$

Proof: We have $(-r)^{\overline{k}} = (-r)(-r-1)\dots(-r-k+1) = (-1)^k r(r+1)\dots(r+k-1) = (-1)^k r^{\overline{k}}$. Dividing this equation by $k!$ proves the claim. $\square$

Remark: Together with the equation $\sum_{k=0}^n \binom{m+k}{k} = \binom{m+n+1}{n}$ (see the remark concerning Pascal's triangle), we get

$$\sum_{k=0}^m (-1)^k \binom{n}{k} = \sum_{k=0}^m \binom{k-n-1}{k} = \binom{m-n}{m} = (-1)^m \binom{n-1}{m}.$$

Hence, we have a formula for the alternating sum of a row in Pascal's triangle. Moreover, the equation has a combinatorial interpretation: both sides count the number of m -subsets of $\{1, \dots, n-1\}$ if m is even (or minus this number if m is odd).

1.5 Permutations

An n -permutation is a bijection $\pi : \{1, \dots, n\} \rightarrow \{1, \dots, n\}$.

For a permutation π , a **cycle** is a set $\{i_1, i_2, \dots, i_t\} \subseteq \{1, \dots, n\}$ such that $\pi(i_j) = i_{j+1}$ for $j \in \{1, \dots, t-1\}$ and $\pi(i_t) = i_1$. It is often written as $(i_1, i_2, \dots, i_t)$ (with t possible choices of the first element i_1). In particular, a fixed point corresponds to a cycle of length 1.

Definition 4 For $n, k \in \mathbb{N}$ let $s_{n,k}$ be the number of n -permutations with k cycles (where we set $s_{0,0} = 1$). The numbers $s_{n,k}$ are called **Stirling numbers of the first kind**.

Obviously, for $n > 0$ we have: $s_{n,0} = 0$, $s_{n,1} = (n-1)!$. As for the Stirling numbers of the second kind, we get a recursion formula.

Proposition 13 For $n, k \in \mathbb{N} \setminus \{0\}$ we have:

$$s_{n,k} = s_{n-1,k-1} + (n-1)s_{n-1,k}.$$

Proof: There are $s_{n-1,k-1}$ n -permutations with k cycles where n is a fixed point, and there are $(n-1)s_{n-1,k}$ n -permutations with k cycles where n is not a fixed point (n can be inserted into one of the $n-1$ possible positions in the cycle notation of an $(n-1)$ -permutation with k cycles). $\square$

For the Stirling numbers of the second kind, also the number $S_{n,2}$ (for $n > 1$) was easy to compute. To do this for the Stirling numbers of the first kind, we need the harmonic numbers.

Definition 5 For $n \in \mathbb{N}$ we define $H_n := \sum_{i=1}^n \frac{1}{i}$. We call H_n the n -th **harmonic number**.

It is a well-known fact (that can easily be proved by using the fact that the derivative of $x \mapsto \ln x$ is $\frac{1}{x}$) that $H_n \in \Theta(\ln n)$. More precisely, we have for positive integers n :

$$\ln n + \frac{1}{n} \leq H_n \leq \ln n + 1.$$

Proposition 14 For $n \in \mathbb{N} \setminus \{0\}$ we have $s_{n,2} = (n-1)!H_{n-1}$.

Proof: Induction on n . For $n = 1$ we have 0 on both sides of the equation, so let $n > 1$. Then:

$$\frac{s_{n,2}}{(n-1)!} \stackrel{\text{Prop. 13}}{=} \frac{s_{n-1,1}}{(n-1)!} + \frac{(n-1)s_{n-1,2}}{(n-1)!} = \frac{(n-2)!}{(n-1)!} + \frac{s_{n-1,2}}{(n-2)!} = \frac{1}{n-1} + H_{n-2} = H_{n-1}.$$

□

There is a surprising connection between the two kinds of Stirling numbers: they are coefficients that allow to switch between the bases $\{r^0, r^1, r^2, \dots\}$ and $\{r^{\underline{0}}, r^{\underline{1}}, r^{\underline{2}}, \dots\}$ of the vector space of the polynomials. We know already the following equation for $n, r \in \mathbb{N}$

$$r^n = \sum_{k=0}^n S_{n,k} r^{\underline{k}}.$$

By the polynomial method we can generalize this result to $r \in \mathbb{C}$. For the other direction (i.e. for writing $r^{\underline{n}}$ as a linear function of the polynomials r^k), we can use the Stirling numbers of the first kind:

Proposition 15 For $n \in \mathbb{N}$ and $r \in \mathbb{C}$, we have:

$$r^{\underline{n}} = \sum_{k=0}^n (-1)^{n-k} s_{n,k} r^k.$$

Proof: Induction on n . For $n = 0$, both sides of the equation equal 1. Hence assume $n > 0$. We generalize the definition of $s_{n,k}$ to negative values of k by setting $s_{n,k} = 0$ for $k < 0$. Then, it is easy to see that Proposition 13 still holds for $n \in \mathbb{N} \setminus \{0\}$ and $k \in \mathbb{Z}$. Therefore, we get:

$$r^{\underline{n}} = (r - n + 1)r^{\underline{n-1}}$$

$$\begin{aligned}
&= (r - n + 1) \sum_{k=0}^{n-1} (-1)^{n-1-k} s_{n-1,k} r^k \\
&= \sum_{k=0}^{n-1} (-1)^{n-1-k} s_{n-1,k} r^{k+1} + \sum_{k=0}^{n-1} (-1)^{n-k} (n-1) s_{n-1,k} r^k \\
&= \sum_{k=1}^n (-1)^{n-k} s_{n-1,k-1} r^k + \sum_{k=0}^n (-1)^{n-k} (n-1) s_{n-1,k} r^k \\
&= \sum_{k=0}^n (-1)^{n-k} (s_{n-1,k-1} r^k + (n-1) s_{n-1,k} r^k) \\
&= \sum_{k=0}^n (-1)^{n-k} s_{n,k} r^k
\end{aligned}$$

□

We categorize permutations not only by the number of cycles but also by the number of cycles of a certain length.

Notation: For an n -permutation π , let $b_i(\pi)$ be the number of cycles of length i (for $i \in \{1, \dots, n\}$), and let $b(\pi) := \sum_{i=1}^n b_i(\pi)$ be the total number of cycles. The **type of a permutation** π is the formal expression $t(\pi) = 1^{b_1(\pi)} 2^{b_2(\pi)} \dots n^{b_n(\pi)}$ where we skip the numbers i with $b_i(\pi) = 0$.

Observation: $\sum_{i=1}^n i b_i(\pi) = n$ holds for any n -permutation π .

Proposition 16 For $n \in \mathbb{N} \setminus \{0\}$, there are $\sum_{k=0}^n P_{n,k}$ types of n -permutations.

Proof: For every type $1^{b_1(\pi)} 2^{b_2(\pi)} \dots n^{b_n(\pi)}$ we find a representation of n as a sum of $b(\pi)$ positive integers where the number i occurs $b_i(\pi)$ times as a summand. This leads to a bijection between the set of types of n -permutations and the set of partitions of n . □

Proposition 17 There are

$$\frac{n!}{b_1! \dots b_n! 1^{b_1} 2^{b_2} \dots n^{b_n}}$$

n -permutations of type $1^{b_1} 2^{b_2} \dots n^{b_n}$.

Proof: First consider empty cycles:

$$\underbrace{(\cdot)(\cdot) \dots (\cdot)}_{b_1 \text{ times}} \underbrace{(\cdot\cdot)(\cdot\cdot) \dots (\cdot\cdot)}_{b_2 \text{ times}} \underbrace{(\cdot\cdot\cdot)(\cdot\cdot\cdot) \dots (\cdot\cdot\cdot)}_{b_3 \text{ times}} \dots$$

There are $n!$ ways to fill these cycles with numbers from $\{1, \dots, n\}$ (without repeating numbers) if $\sum_{i=1}^n i b_i = n$. Moreover, each such assignment yields an n -permutation of type $1^{b_1} 2^{b_2} \dots n^{b_n}$.

However, for each $i \in \{1, \dots, n\}$, all assignments that differ just in the order of the b_i cycles lead to the same permutation. And for each cycle of length i there are i assignments giving the same permutation because there are i ways to choose the first element in the cycle. Hence, for each n -permutation π , there are $b_1! \dots b_n! 1^{b_1} 2^{b_2} \dots n^{b_n}$ assignments that encode π . $\square$

In particular, we have

$$s_{n,k} = \sum_{(b_1, \dots, b_n)} \frac{n!}{b_1! \dots b_n! 1^{b_1} \dots n^{b_n}}$$

where we sum over all vectors $(b_1, \dots, b_n)$ with $\sum_{i=1}^n i b_i = n$ and $\sum_{i=1}^n b_i = k$.

Similarly:

$$n! = \sum_{(b_1, \dots, b_n)} \frac{n!}{b_1! \dots b_n! 1^{b_1} \dots n^{b_n}}$$

where we sum over all vectors $(b_1, \dots, b_n)$ with $\sum_{i=1}^n i b_i = n$.

1.6 Further Combinatorial Techniques

Inclusion-exclusion principle:

Proposition 18 (*Inclusion-exclusion principle*) Let $A_1, \dots, A_n$ be finite sets. Then:

$$\left| \bigcup_{i=1}^n A_i \right| = \sum_{r=1}^n (-1)^{r-1} \sum_{1 \leq i_1 < \dots < i_r \leq n} \left| \bigcap_{j=1}^r A_{i_j} \right|.$$

Proof: For each $a \in \bigcup_{i=1}^n A_i$, we have to show that a is counted on the right-hand side of the equation exactly once. Let $k := |\{i \in \{1, \dots, n\} \mid a \in A_i\}|$. Then a is counted $\binom{k}{r}$ times in the sum $\sum_{1 \leq i_1 < \dots < i_r \leq n} |\bigcap_{j=1}^r A_{i_j}|$ (for $r \in \{1, \dots, n\}$). Hence in total, a is counted $\sum_{r=1}^k (-1)^{r-1} \binom{k}{r}$ times. By the binomial theorem, we have

$$0 = (-1 + 1)^k = \sum_{r=0}^k \binom{k}{r} (-1)^r 1^{k-r} = 1 - \sum_{r=1}^k (-1)^{r-1} \binom{k}{r}.$$

Thus, $\sum_{r=1}^k (-1)^{r-1} \binom{k}{r} = 1$, which means that a is counted exactly once in the sum on the right-hand side. $\square$

Proposition 19 The number of fixed-point-free n -permutations is $D_n := n! \sum_{r=0}^n \frac{(-1)^r}{r!}$.

Proof: Let A_i be the set of all n -permutations π with $\pi(i) = i$. Thus, the number of

fixed-point-free n -permutations is

$$n! - \left| \bigcup_{i=1}^n A_i \right| = n! - \sum_{r=1}^n (-1)^{r-1} \sum_{1 \leq i_1 < \dots < i_r \leq n} \left| \bigcap_{j=1}^r A_{i_j} \right|.$$

For $1 \leq i_1 < \dots < i_r \leq n$, we obviously have $|\bigcap_{j=1}^r A_{i_j}| = (n-r)!$. Moreover, there are $\binom{n}{r}$ ways to choose integers $i_1, \dots, i_r$ with $1 \leq i_1 < \dots < i_r \leq n$ (for $r \in \{1, \dots, n\}$). Thus the number of fixed-point-free n -permutations is

$$\begin{aligned} n! - \sum_{r=1}^n \binom{n}{r} (-1)^{r-1} (n-r)! &= \sum_{r=0}^n \binom{n}{r} (-1)^r (n-r)! = \sum_{r=0}^n \frac{n!}{r!(n-r)!} (-1)^r (n-r)! \\ &= n! \sum_{r=0}^n \frac{(-1)^r}{r!} \end{aligned}$$

□

The numbers D_n are called the **derangement numbers**. We have $\lim_{n \rightarrow \infty} \sum_{r=0}^n \frac{(-1)^r}{r!} = \frac{1}{e}$, so for large n the fraction of the fixed-point-free n -permutations among all n -permutations is approximately $\frac{1}{e}$.

The following proposition is another application of the inclusion-exclusion principle:

Proposition 20 *For $n \in \mathbb{N}$, the number of ways to write n as a sum of odd natural numbers is the number of ways to write n as a sum of different positive integers.*

Proof: For $n \in \mathbb{N} \setminus \{0\}$ let $p(n) = \sum_{k=1}^n P_{n,k}$ be the number of ways to write n as a sum of positive integers. For non-positive integers n , we set $p(n) = 0$. Then, for $n \in \mathbb{N} \setminus \{0\}$ and numbers $1 \leq i_1 < \dots < i_r \leq n$, the number of partitions where these numbers occur twice is $p(n - 2 \sum_{j=1}^r i_j)$. However, this is also the number of partitions where the even numbers $2i_1, \dots, 2i_r$ occur. Hence, both for the number of partitions in odd summands and for the number of partitions in different summands we get:

$$p(n) - \sum_{r=1}^n (-1)^{r-1} \sum_{1 \leq i_1 < \dots < i_r \leq n} p\left(n - 2 \sum_{j=1}^r i_j\right).$$

□

Doubly counting:

The **principle of doubly counting** is based on the following simple observation that, for a relation $R \subseteq S \times T$, we can count the pairs in R in two different ways and get:

$$\sum_{s \in S} |\{t \in T \mid (s, t) \in R\}| = \sum_{t \in T} |\{s \in S \mid (s, t) \in R\}|$$

Examples:

- We want to compute the average number of divisors of the integers in $\{1, \dots, n\}$. To this end, we set $S = T = \{1, \dots, n\}$ and define the relation $R \subseteq S \times T$ by $(s, t) \in R :\Leftrightarrow t|s$. Then, the average number of divisors is

$$\begin{aligned}
\frac{1}{n} \sum_{s \in S} |\{t \in \{1, \dots, n\} : t|s\}| &= \frac{1}{n} \sum_{s \in S} |\{t \in T : (s, t) \in R\}| \\
&= \frac{1}{n} \sum_{t \in T} |\{s \in S : (s, t) \in R\}| \\
&= \frac{1}{n} \sum_{t \in T} |\{s \in \{1, \dots, n\} : t|s\}| \\
&= \frac{1}{n} \sum_{t \in T} \left\lfloor \frac{n}{t} \right\rfloor \in \left[\left(\sum_{i=1}^n \frac{1}{i} \right) - 1, \sum_{i=1}^n \frac{1}{i} \right]
\end{aligned}$$

Hence, the average number of divisors of the numbers in $\{1, \dots, n\}$ is approximately $H_n = \sum_{i=1}^n \frac{1}{i}$ which is $\Theta(\ln n)$.

- Let G be an undirected graph. For $S = V(G)$ and $T = E(G)$ we define the relation $R \subseteq V(G) \times E(G)$ by $(v, e) \in R :\Leftrightarrow v \in e$. Then doubly counting proves $\sum_{e \in E(G)} |\{v \in V(G) \mid v \in e\}| = \sum_{v \in V(G)} |\{e \in E(G) \mid v \in e\}|$, so $2|E(G)| = \sum_{v \in V(G)} |\delta_G(v)|$ (for $u \in V(G)$, $\delta_G(u)$ denotes the set of edges incident to u).
- Claim: A simple undirected graph G that does not contain a cycle of length 4 has at most $\lfloor \frac{n}{4}(1 + \sqrt{4n-3}) \rfloor$ edges (where $n = |V(G)|$).
Proof of the claim: For $S = V(G)$ and $T = \{\{v, w\} \subseteq V(G) \mid v \neq w\}$ we define the relation $R \subseteq S \times T$ by

$$(u, \{v, w\}) \in R :\Leftrightarrow \{u, v\} \in E(G) \text{ and } \{u, w\} \in E(G).$$

Then, doubly counting leads to:

$$\sum_{u \in V(G)} \binom{|\delta_G(u)|}{2} = \sum_{s \in S} |\{t \in T \mid (s, t) \in R\}| = \sum_{t \in T} |\{s \in S \mid (s, t) \in R\}| \leq |T| = \binom{n}{2}$$

where the inequality follows from the fact that each two distinct nodes v, w can have at most one common neighbor (otherwise we would have a cycle of length 4 in G). Thus, $\sum_{u \in V(G)} \frac{|\delta_G(u)|^2 - |\delta_G(u)|}{2} \leq \frac{n(n-1)}{2}$ and hence

$$\sum_{u \in V(G)} |\delta_G(u)|^2 \leq n(n-1) + \sum_{u \in V(G)} |\delta_G(u)|$$

Moreover, with $\alpha(u) := \frac{2m}{n} - |\delta_G(u)|$ for $u \in V(G)$ (where $m = |E(G)|$) we get

$$\sum_{u \in V(G)} |\delta_G(u)|^2 = \sum_{u \in V(G)} \left(\frac{2m}{n} - \alpha(u) \right)^2 = \sum_{u \in V(G)} \left(\frac{2m}{n} \right)^2 - \frac{4m}{n} \sum_{u \in V(G)} \alpha(u) + \sum_{u \in V(G)} \alpha(u)^2 \geq \frac{4m^2}{n}$$

because $\sum_{u \in V(G)} \alpha(u) = 0$. Hence, $\frac{4m^2}{n} \leq n(n-1) + 2m$, which proves the claim.

(Generalized) pigeonhole principle:

For an n -set N and an r -set R with $n > r$ and a mapping $f : N \rightarrow R$ there is an $a \in R$ with $|f^{-1}(a)| \geq \lfloor \frac{n-1}{r} \rfloor + 1$. In particular there must be an $a \in R$ with $|f^{-1}(a)| \geq 2$.

This principle is obviously true because otherwise we would have $n = \sum_{a \in R} |f^{-1}(a)| \leq r \lfloor \frac{n-1}{r} \rfloor < n$.

Simple Applications: Let $a_1, \dots, a_n$ (with $n \geq 1$) be a finite sequence of positive integers.

- **Claim:** There are numbers $k, l \in \{1, \dots, n\}$ such that $\sum_{i=k}^l a_i$ is an integral multiple of n .

Proof: Let $N = \{\sum_{i=1}^l a_i \mid l \in \{0, \dots, n\}\}$ and $R = \{0, \dots, n-1\}$. We define $f(m)$ to be the remainder of m upon division by n . Since $|N| = n+1 > n = |R|$, there are numbers $m, l \in \{0, \dots, n\}$ with $m < l$ and $f(\sum_{i=1}^m a_i) = f(\sum_{i=1}^l a_i)$. Thus, $\sum_{i=m+1}^l a_i$ is an integral multiple of n .

- **Claim:** If $\{a_1, \dots, a_n\} \subseteq \{1, \dots, 2n-2\}$, then there are numbers $i, j \in \{1, \dots, n\}$ with $i \neq j$ such that a_i is an integral multiple of a_j .

Proof: If there are $i, j \in \{1, \dots, n\}$ with $i \neq j$ and $a_i = a_j$, we are done. Hence assume that the numbers a_i are pairwise distinct. Let $N = \{a_1, \dots, a_n\}$ and $R = \{2i-1 \mid i \in \{1, \dots, n-1\}\}$. We can write each number a_i in a unique way as $a_i = 2^{k_i} b_i$ where b_i is an odd number. We define $f : N \rightarrow R$ by $f(a_i) = b_i$. Then, by the pigeonhole principle, there are numbers a_i and a_j with $i \neq j$ and $f(a_i) = f(a_j)$, i.e. $a_i = 2^{k_i} b_i$ and $a_j = 2^{k_j} b_i$. W.l.o.g. assume $k_i \geq k_j$. Then a_i is an integral multiple of a_j .

- **Claim:** If the numbers a_i are pairwise distinct and $n > k \cdot l$ for some positive integers l, k , then there is an increasing subsequence $a_{i_1} < a_{i_2} < \dots < a_{i_{k+1}}$ ($i_1 < i_2 < \dots < i_{k+1}$) of length $k+1$ or a decreasing subsequence $a_{i_1} > a_{i_2} > \dots > a_{i_{l+1}}$ ($i_1 < i_2 < \dots < i_{l+1}$) of length $l+1$.

Proof: Assume that there is no increasing subsequence of length $k+1$. For $i \in \{1, \dots, n\}$ we define t_i to be the length of the longest increasing subsequence starting with a_i . Hence, by setting $f(a_i) = t_i$, we get a mapping $f : \{a_1, \dots, a_n\} \rightarrow \{1, \dots, k\}$. Thus there must be a $j \in \{1, \dots, k\}$ with $|f^{-1}(j)| > l$. Obviously, the elements of $f^{-1}(j)$ form a decreasing subsequence.

The following theorem can be considered as a generalization of the pigeonhole principle. Here the set of edges of a complete graph on n nodes is mapped to a 2-set determining if the edge is contained in a specific graph G with $|V(G)| = n$ or not. The theorem not only states that there will be “many” edges inside the graph G or “many” edges outside the graph G but also specifies that there must be “large” complete graphs in G or its complement. In a graph G , we call a **clique** a set of nodes that are pairwise connected by edges and a **stable set** a set of nodes such that no two nodes in this set are connected by an edge.

Theorem 21 (*Ramsey's Theorem, Ramsey [1930]*): For $k, l \in \mathbb{N} \setminus \{0\}$, there is a smallest number $R(k, l)$ such that any graph with at least $R(k, l)$ nodes contains a clique of size k or a stable set of size l .

Proof: Induction on $k + l$. If $k = 1$ or $l = 1$, then obviously $R(k, l) = 1$. Hence, we assume $k > 1$ and $l > 1$.

Claim: $R(k, l) \leq R(k - 1, l) + R(k, l - 1)$.

Proof of the claim: Let G be a graph with at least $R(k - 1, l) + R(k, l - 1)$ nodes, and let $v \in V(G)$ be a node of G . Let X be the set of neighbors of v in G and $Y := V(G) \setminus (X \cup \{v\})$. Thus, $|X| \geq R(k - 1, l)$ or $|Y| \geq R(k, l - 1)$. If $|X| \geq R(k - 1, l)$, then X contains a stable set of size l (so we are done) or a clique of size $k - 1$. Since all elements of X are neighbors of v , such a clique can be extended by adding v to a clique of size k , so, again, we are done. The case $|Y| \geq R(k, l - 1)$ can be handled analogously. $\square$

The numbers $R(k, l)$ are called **Ramsey numbers**.

In particular for $m > 1$: $R(2, m) = R(m, 2) = m$.

Theorem 22 For $k, l \in \mathbb{N} \setminus \{0\}$ we have $R(k, l) \leq \binom{k+l-2}{k-1}$.

Proof: For $k = 1$, we have $R(1, l) = 1$, and for $l = 1$, we have $R(k, l) = 1$. For $k, l > 1$, we get:

$$R(k, l) \leq R(k - 1, l) + R(k, l - 1) \leq \binom{k + l - 3}{k - 2} + \binom{k + l - 3}{k - 1} = \binom{k + l - 2}{k - 1}.$$

$\square$

In general, the exact values $R(k, l)$ are difficult to compute. But, for example, it is easy to see that $R(3, 3) = 6$. The inequality $R(3, 3) \leq \binom{4}{2} = 6$ follows from the previous theorem. Moreover, the graph C_5 which is the cycle of length 5, shows that $R(3, 3) > 5$ since it contains neither a clique nor a stable set of size 3.

2 Computation of Sums

2.1 Sums: Direct Methods

Induction:

Most induction proofs of formulas computing sums are more or less trivial, and we have already seen several examples. As an example for an induction that requires (at least to simplify the

proof) an additional idea, we prove the arithmetic-geometric mean inequality, though this is not really a statement about sums. The arithmetic-geometric mean inequality says that for non-negative real numbers $a_1, \dots, a_n$, we have

$$\sqrt[n]{a_1 a_2 \dots a_n} \leq \frac{a_1 + \dots + a_n}{n}.$$

Equivalently, we show the following statement that we call (P_n) : For non-negative real numbers $a_1, \dots, a_n$, we have

$$a_1 a_2 \dots a_n \leq \left(\frac{a_1 + \dots + a_n}{n} \right)^n.$$

The case (P_1) is trivial but we also show the statement explicitly for $n = 2$. It is equivalent to $4a_1 a_2 \leq a_1^2 + 2a_1 a_2 + a_2^2$, which in turn is equivalent to $0 \leq a_1^2 - 2a_1 a_2 + a_2^2 = (a_1 - a_2)^2$, so it is true.

For the induction step, we avoid showing directly that (P_{n+1}) follows from (P_n) . Instead, we show the following two statements (which is sufficient):

- (a) $(P_n) \Rightarrow (P_{n-1})$,
- (b) $((P_n) \wedge (P_2)) \Rightarrow (P_{2n})$.

For (a), we compute for non-negative real numbers $a_1, \dots, a_{n-1}$:

$$\begin{aligned} \left(\prod_{k=1}^{n-1} a_k \right) \sum_{k=1}^{n-1} \frac{a_k}{n-1} &\stackrel{(P_n)}{\leq} \left(\frac{\sum_{k=1}^{n-1} a_k + \sum_{k=1}^{n-1} \frac{a_k}{n-1}}{n} \right)^n = \left(\frac{n \sum_{k=1}^{n-1} a_k}{n(n-1)} \right)^n \\ &= \left(\frac{1}{n-1} \right)^n \left(\sum_{k=1}^{n-1} a_k \right)^n \end{aligned}$$

and thus

$$\prod_{k=1}^{n-1} a_k \leq \left(\frac{1}{n-1} \right)^{n-1} \left(\sum_{k=1}^{n-1} a_k \right)^{n-1}$$

For (b), we compute for non-negative real numbers $a_1, \dots, a_{2n}$:

$$\begin{aligned} \prod_{k=1}^{2n} a_k &= \left(\prod_{k=1}^n a_k \right) \left(\prod_{k=n+1}^{2n} a_k \right) \stackrel{(P_n)}{\leq} \left(\sum_{k=1}^n \frac{a_k}{n} \right)^n \left(\sum_{k=n+1}^{2n} \frac{a_k}{n} \right)^n = \left(\sum_{k=1}^n \frac{a_k}{n} \sum_{k=n+1}^{2n} \frac{a_k}{n} \right)^n \\ &\stackrel{(P_2)}{\leq} \left(\left(\frac{\sum_{k=1}^n \frac{a_k}{n} + \sum_{k=n+1}^{2n} \frac{a_k}{n}}{2} \right)^2 \right)^n = \left(\frac{\sum_{k=1}^{2n} a_k}{2n} \right)^{2n} \end{aligned}$$

Index transformation:

Make use of the observation that sums can be computed in many different ways:

$$\sum_{k=m}^n a_k = \sum_{k=m+i}^{n+i} a_{k-i} = \sum_{k=m-i}^{n-i} a_{k+i} = \sum_{k=0}^{n-m} a_{m+k} = \sum_{k=0}^{n-m} a_{n-k}$$

For example, assume that we want to compute $S_n = \sum_{k=0}^n ka$ for some constant a . Then, $S_n = \sum_{k=0}^n (n-k)a$, so $2S_n = \sum_{k=0}^n ka + \sum_{k=0}^n (n-k)a = \sum_{k=0}^n na = (n+1)na$, which implies $S_n = \frac{n(n+1)}{2}a$.

Isolating terms:

For a sum $S_n = \sum_{k=0}^n a_k$, isolate the first and the last terms from S_{n+1} : $S_{n+1} = S_n + a_{n+1} = a_0 + \sum_{k=1}^{n+1} a_k = a_0 + \sum_{k=0}^n a_{k+1}$

Examples:

- Consider the (finite) geometric sum $S_n = \sum_{k=0}^n a^k$. We get

$$S_{n+1} = S_n + a^{n+1} = 1 + \sum_{k=0}^n a^{k+1} = 1 + a \sum_{k=0}^n a^k = 1 + aS_n.$$

Thus, $S_n + a^{n+1} = 1 + aS_n$, so $S_n = \frac{a^{n+1}-1}{a-1}$ if $a \neq 1$ (for $a = 1$, we simply get $S_n = n+1$).

- Let $S_n = \sum_{k=0}^n k2^k$. Then,

$$S_{n+1} = S_n + (n+1)2^{n+1} = 0 + \sum_{k=0}^n (k+1)2^{k+1} = 2 \sum_{k=0}^n k2^k + 2 \sum_{k=0}^n 2^k = 2S_n + 2^{n+2} - 2,$$

$$\text{so } S_n = (n-1)2^{n+1} + 2.$$

2.2 Difference and Sum Operators

Our goal in this section is again to solve sums. Sums can be seen as integrals over step functions. Therefore, we will apply techniques from integral calculus to the computations of sums. In order to develop a discrete analogue to integrals, we first have to develop a discrete analogue to the differential calculus.

Definition 6 For $a \in \mathbb{Z}$ the **translation operator** $E^a : \mathbb{R}^{\mathbb{Z}} \rightarrow \mathbb{R}^{\mathbb{Z}}$ maps $f \in \mathbb{R}^{\mathbb{Z}}$ to $E^a f$ where $E^a f(x) = f(x+a)$ for all $x \in \mathbb{Z}$.

Hence $I := E^0$ is the identity.

For two operators $P, Q : \mathbb{R}^{\mathbb{Z}} \rightarrow \mathbb{R}^{\mathbb{Z}}$, we can define their sum by $(P + Q)f = Pf + Qf$ and a multiplication by a scalar α by setting $(\alpha P)f = \alpha(Pf)$. We denote their composition by QP , so $(QP)f = Q(Pf)$.

Moreover, we define $\Delta : \mathbb{R}^{\mathbb{Z}} \rightarrow \mathbb{R}^{\mathbb{Z}}$ as $\Delta = E^1 - I$, so for $f : \mathbb{Z} \rightarrow \mathbb{R}$ we have $\Delta f(x) = f(x+1) - f(x)$. This is the **forward difference operator**. Similarly, we define $\nabla : \mathbb{R}^{\mathbb{Z}} \rightarrow \mathbb{R}^{\mathbb{Z}}$ as $\nabla = I - E^{-1}$, so for $f : \mathbb{Z} \rightarrow \mathbb{R}$ we have $\nabla f(x) = f(x) - f(x-1)$. This is the **backward difference operator**.

Examples: For $n \in \mathbb{N}$:

$$\Delta x^n = (x+1)^n - x^n = (x+1)x^{n-1} - (x-n+1)x^{n-1} = nx^{n-1}$$

and

$$\nabla x^{\bar{n}} = x^{\bar{n}} - (x-1)^{\bar{n}} = (x+n-1)x^{\overline{n-1}} - (x-1)x^{\overline{n-1}} = nx^{\overline{n-1}}$$

We generalize the falling and rising factorials to negative exponents by setting (for $n \in \mathbb{N} \setminus \{0\}$):

$$x^{-n} := \frac{1}{(x+1) \dots (x+n)},$$

and

$$x^{\overline{-n}} := \frac{1}{(x-1) \dots (x-n)}.$$

Theorem 23 For $n \in \mathbb{Z}$, we have:

$$\Delta x^n = nx^{n-1}$$

and

$$\nabla x^{\bar{n}} = nx^{\overline{n-1}}$$

Proof: For $n \geq 0$ we have already proved the statement. The rest follows from

$$\begin{aligned} \Delta x^{-n} &= (x+1)^{-n} - x^{-n} \\ &= \frac{1}{(x+2) \dots (x+n+1)} - \frac{1}{(x+1) \dots (x+n)} \\ &= \frac{x+1}{(x+1) \dots (x+n+1)} - \frac{x+n+1}{(x+1) \dots (x+n+1)} \\ &= (x+1)x^{-n-1} - (x+n+1)x^{-n-1} \\ &= -nx^{-n-1} \end{aligned}$$

and

$$\begin{aligned}
\nabla x^{-n} &= x^{-n} - (x-1)^{-n} \\
&= \frac{1}{(x-1)\dots(x-n)} - \frac{1}{(x-2)\dots(x-n-1)} \\
&= \frac{x-n-1}{(x-1)\dots(x-n-1)} - \frac{x-1}{(x-1)\dots(x-n-1)} \\
&= (x-n-1)x^{-n-1} - (x-1)x^{-n-1} \\
&= -nx^{-n-1}
\end{aligned}$$

□

Definition 7 For two mappings $f, g : \mathbb{Z} \rightarrow \mathbb{R}$, we call f a **(discrete) antiderivative** of g , if $\Delta f = g$. We write $f = \sum g$ and call f an **indefinite sum**.

Thus:

$$\Delta f = g \Leftrightarrow f = \sum g.$$

Note that as in the differential calculus, the antiderivative is defined only up to some additive constant. We will ignore that fact and consider $\sum : \mathbb{R}^{\mathbb{Z}} \rightarrow \mathbb{R}^{\mathbb{Z}}$ as a well-defined operator.

Theorem 24 If f is an antiderivative of g then for all $a, b \in \mathbb{Z}$ with $a \leq b$:

$$\sum_{k=a}^b g(k) = f(b+1) - f(a).$$

Proof: Since $\Delta f = g$, we have $f(k+1) - f(k) = g(k)$ for all $k \in \mathbb{Z}$. Thus,

$$\sum_{k=a}^b g(k) = \sum_{k=a}^b (f(k+1) - f(k)) = f(b+1) - f(a).$$

□

Notation: For $f = \sum g$ and $a, b \in \mathbb{Z}$ with $a \leq b$, we write $\sum_a^{b+1} g(x) := f(x)|_a^{b+1} := f(b+1) - f(a)$. Hence:

$$\sum_a^{b+1} g(x) = \sum_{k=a}^b g(k).$$

Note that on the left-hand side of this equation “ $\sum$ ” denotes an indefinite sum, evaluated at a and $b+1$, while on the right-hand side “ $\sum$ ” just denotes the sum $g(a) + g(a+1) + \dots + g(b)$.

Observation: Both Δ and $\sum$ are linear operators, i.e. $\Delta(\alpha f + \beta g) = \alpha \Delta f + \beta \Delta g$ and $\sum(\alpha f + \beta g) = \alpha \sum f + \beta \sum g$ for scalars α and β and functions f and g .

Proposition 25 For $n \in \mathbb{Z}$, we have:

$$\sum x^n = \begin{cases} \frac{x^{n+1}}{n+1} & \text{if } n \neq -1 \\ H_x & \text{if } n = -1 \end{cases}$$

Proof: Since $\Delta x^{n+1} = (n+1)x^n$, we have $\sum x^n = \frac{x^{n+1}}{n+1}$ if $n \neq -1$. It remains to find $\sum x^{-1}$. A function f with $f' = \sum x^{-1}$ satisfies $\frac{1}{x+1} = x^{-1} = \Delta f = f(x+1) - f(x)$. Thus $H_x = \sum_{i=1}^x \frac{1}{i}$ is an antiderivative of x^{-1} . This proves the proposition. $\square$

Application: Compute $\sum_{k=0}^n k^2$: We have $x^2 = x(x-1) + x = x^2 + x^{-1}$, so

$$\begin{aligned} \sum_{k=0}^n k^2 &= \sum_0^{n+1} x^2 = \sum_0^{n+1} x^2 + \sum_0^{n+1} x^{-1} = \frac{x^3}{3} \Big|_0^{n+1} + \frac{x^2}{2} \Big|_0^{n+1} \\ &= \frac{(n+1)^3}{3} + \frac{(n+1)^2}{2} = \frac{(n+1)n(n-1)}{3} + \frac{(n+1)n}{2} = \frac{n(2n+1)(n+1)}{6} \end{aligned}$$

More general: $x^m = \sum_{k=0}^m S_{m,k} x^k$. Therefore:

$$\begin{aligned} \sum_{k=0}^n k^m &= \sum_0^{n+1} x^m = \sum_0^{n+1} \left(\sum_{k=0}^m S_{m,k} x^k \right) = \sum_{k=0}^m S_{m,k} \sum_0^{n+1} x^k = \sum_{k=0}^m S_{m,k} \frac{x^{k+1}}{k+1} \Big|_0^{n+1} \\ &= \sum_{k=0}^m S_{m,k} \frac{(n+1)^{k+1}}{k+1}. \end{aligned}$$

Further examples:

- For $c \in \mathbb{R} \setminus \{0\}$, we have $\Delta c^x = c^{x+1} - c^x = (c-1)c^x$. Hence, for $c \neq 1$: $\sum c^x = \frac{c^x}{c-1}$. In particular, for $c = 2$ we get $\Delta 2^x = 2^x$ and $\sum 2^x = 2^x$, so we get an analogue to e^x in the differential calculus.
- For $x \in \mathbb{R}$ and $m \in \mathbb{Z}$ we have $\binom{x+1}{m+1} = \binom{x}{m} + \binom{x}{m+1}$. Thus $\Delta \binom{x}{m+1} = \binom{x}{m}$ and $\sum \binom{x}{m} = \binom{x}{m+1}$.

For a function $f : \mathbb{Z} \rightarrow \mathbb{R}$, we have

$$\Delta^n f(x) = (E - I)^n f(x) = \sum_{k=0}^n (-1)^{n-k} \binom{n}{k} E^k f(x) = \sum_{k=0}^n (-1)^{n-k} \binom{n}{k} f(x+k)$$

In particular, for $x = 0$:

$$\Delta^n f(0) = \sum_{k=0}^n (-1)^{n-k} \binom{n}{k} f(k) \quad (2)$$

Theorem 26 (*Newton representation of polynomials*): For a polynomial f of degree n , we have

$$f(x) = \sum_{k=0}^n \frac{\Delta^k f(0)}{k!} x^{\underline{k}}$$

Proof: Since the polynomials $x^{\underline{k}}$ are a basis of the space of polynomials, we can write f in a unique way as $f(x) = \sum_{k=0}^n b_k x^{\underline{k}}$. It remains to show that $b_k = \frac{\Delta^k f(0)}{k!}$ (for $k \in \{0, \dots, n\}$).

We have $\Delta^k x^{\underline{i}} = i(i-1) \dots (i-k+1) x^{\underline{i-k}} = i^{\underline{k}} x^{\underline{i-k}}$. Hence:

$$\Delta^k f(x) = \Delta^k \sum_{i=0}^n b_i x^{\underline{i}} = \sum_{i=0}^n b_i i^{\underline{k}} x^{\underline{i-k}}$$

Thus $\Delta^k f(0) = \sum_{i=0}^n b_i i^{\underline{k}} 0^{\underline{i-k}} = b_k k^{\underline{k}}$ because $i^{\underline{k}} = 0$ for $i < k$ and $0^{\underline{i-k}} = 0$ for $i > k$. Since $k^{\underline{k}} = k!$, this proves the theorem. $\square$

Corollary 27 For $n, k \in \mathbb{N}$, we have:

$$S_{n,k} = \frac{1}{k!} \sum_{i=0}^k (-1)^{k-i} \binom{k}{i} i^n$$

Proof: We know that $x^n = \sum_{k=0}^n S_{n,k} x^{\underline{k}}$, so by the previous theorem we have, with $f(x) = x^n$:

$$S_{n,k} = \frac{\Delta^k f(0)}{k!} = \frac{1}{k!} \sum_{i=0}^k (-1)^{k-i} \binom{k}{i} i^n.$$

For the last equation, we applied (2). $\square$

Theorem 28 (*Partial summation*) For functions $u, v : \mathbb{Z} \rightarrow \mathbb{R}$, we have:

$$\sum (u \Delta v) = uv - \sum ((Ev) \Delta u)$$

Proof: We have

$$\begin{aligned} \Delta uv(x) &= u(x+1)v(x+1) - u(x)v(x) \\ &= u(x)(v(x+1) - v(x)) + v(x+1)(u(x+1) - u(x)) \\ &= u(x)\Delta v(x) + Ev(x)\Delta u(x), \end{aligned}$$

so $\Delta uv = u\Delta v + (Ev)\Delta u$. Applying the operator $\sum$ to this equation proves the statement of the theorem. $\square$

Applications:

- Compute $\sum_{k=0}^n k2^k$.

Thus, we want to compute $\sum x2^x$. We apply the theorem with $u(x) = x$ and $\Delta v(x) = 2^x$, so $\Delta u(x) = 1$ and $v(x) = 2^x$. This leads to:

$$\begin{aligned}\sum_{k=0}^n k2^k &= \sum_0^{n+1} x2^x = x2^x \Big|_0^{n+1} - \sum_0^{n+1} 2^{x+1} = x2^x \Big|_0^{n+1} - 2 \cdot 2^x \Big|_0^{n+1} \\ &= (n+1)2^{n+1} - 2 \cdot 2^{n+1} + 2 = (n-1)2^{n+1} + 2\end{aligned}$$

- Compute $\sum_{k=1}^n H_k$.

Apply the theorem with $u(x) = H_x$ and $\Delta v(x) = 1$, so $\Delta u(x) = \frac{1}{1+x}$ and $v(x) = x$. This implies:

$$\begin{aligned}\sum_{k=1}^n H_k &= \sum_1^{n+1} H_x x^0 = H_x x \Big|_1^{n+1} - \sum_1^{n+1} (x+1) \frac{1}{1+x} = H_{n+1}(n+1) - 1 - x \Big|_1^{n+1} \\ &= H_{n+1}(n+1) - 1 - (n+1) + 1 = (n+1)(H_{n+1} - 1)\end{aligned}$$

- Compute $\sum_{k=1}^n \binom{k}{m} H_k$ (for $m \in \mathbb{N} \setminus \{0\}$).

Apply the theorem with $u(x) = H_x$ and $\Delta v(x) = \binom{x}{m}$, so $\Delta u(x) = \frac{1}{1+x}$ and $v(x) = \binom{x}{m+1}$. This leads to:

$$\begin{aligned}\sum_{k=1}^n \binom{k}{m} H_k &= \sum_1^{n+1} \binom{x}{m} H_x = H_x \binom{x}{m+1} \Big|_1^{n+1} - \sum_1^{n+1} \binom{x+1}{m+1} \frac{1}{1+x} \\ &= H_{n+1} \binom{n+1}{m+1} - H_1 \binom{1}{m+1} - \frac{1}{m+1} \sum_1^{n+1} \binom{x}{m} \\ &= H_{n+1} \binom{n+1}{m+1} - \frac{1}{m+1} \binom{x}{m+1} \Big|_1^{n+1} \\ &= H_{n+1} \binom{n+1}{m+1} - \frac{1}{m+1} \left(\binom{n+1}{m+1} - \binom{1}{m+1} \right) \\ &= \binom{n+1}{m+1} \left(H_{n+1} - \frac{1}{m+1} \right)\end{aligned}$$

2.3 Inversions

Definition 8 A **basis sequence** is a sequence of polynomials $(p_i)_{i \in \mathbb{N}} = p_0(x), p_1(x), \dots$ where p_i is a polynomial of degree i (for $i \in \mathbb{N}$).

Examples of basis sequences are $(x^n)_{n \in \mathbb{N}}$ and $(x^n)_{n \in \mathbb{N}}$.

It is easy to check that if $p_0(x), p_1(x), \dots$ is a basis sequence and $p(x)$ is a polynomial of degree n then there are unique numbers $a_0, \dots, a_n$ such that $p(x) = \sum_{k=0}^n a_k p_k(x)$.

Now let $(p_n)_{n \in \mathbb{N}}$ and $(q_n)_{n \in \mathbb{N}}$ be two basis sequences. Then there are unique numbers $a_{n,k}$ and $b_{n,k}$ for $k \leq n$ with

$$q_n(x) = \sum_{k=0}^n a_{n,k} p_k(x)$$

and

$$p_n(x) = \sum_{k=0}^n b_{n,k} q_k(x)$$

For $k > n$ we set all numbers $a_{n,k}$ and $b_{n,k}$ to 0. The numbers $a_{n,k}$ and $b_{n,k}$ are called **connection coefficients**.

We have

$$q_n(x) = \sum_{k=0}^n a_{n,k} p_k(x) = \sum_{k=0}^n a_{n,k} \sum_{m=0}^k b_{k,m} q_m(x) = \sum_{m=0}^n q_m(x) \sum_{k=m}^n a_{n,k} b_{k,m}$$

Hence

$$\sum_{k=m}^n a_{n,k} b_{k,m} = \sum_{k=1}^n a_{n,k} b_{k,m} = \begin{cases} 1 & \text{if } n = m \\ 0 & \text{if } n \neq m \end{cases}$$

Therefore, for $A_n = (a_{i,j})_{0 \leq i,j \leq n}$ and $B_n = (b_{i,j})_{0 \leq i,j \leq n}$, we have $A_n B_n = I_n$ where I_n is the $(n+1) \times (n+1)$ -identity matrix.

Theorem 29 *Let $(p_n)_{n \in \mathbb{N}}$ and $(q_n)_{n \in \mathbb{N}}$ be two basis sequences with connection coefficients $a_{n,k}$ and $b_{n,k}$. Then for two sequences $(u_n)_{n \in \mathbb{N}}$ and $(v_n)_{n \in \mathbb{N}}$, the following statements are equivalent:*

$$\forall n \in \mathbb{N} \quad v_n = \sum_{k=0}^n a_{n,k} u_k$$

and

$$\forall n \in \mathbb{N} \quad u_n = \sum_{k=0}^n b_{n,k} v_k$$

Proof: Let $n \in \mathbb{N}$. The matrices A_n and B_n are inverse to each other, so for any two vectors $u = (u_0, \dots, u_n)$ and $v = (v_0, \dots, v_n)$, we have

$$v = A_n u \quad \Leftrightarrow \quad u = B_n v.$$

□

Examples:

- **Stirling numbers:**

Consider the basis sequences $(x^n)_{n \in \mathbb{N}}$ and $(x^n)_{n \in \mathbb{N}}$. We know from Proposition 10 and Proposition 15 that

$$x^n = \sum_{k=0}^n S_{n,k} x^k.$$

and

$$x^n = \sum_{k=0}^n (-1)^{n-k} s_{n,k} x^k.$$

Thus the numbers $S_{n,k}$ and $(-1)^{n-k} s_{n,k}$ are the connection coefficients of the basis sequences $(x^n)_{n \in \mathbb{N}}$ and $(x^n)_{n \in \mathbb{N}}$. This gives us

$$\sum_{k \geq 0} S_{n,k} (-1)^{k-m} s_{k,m} = \begin{cases} 1 & \text{if } n = m \\ 0 & \text{if } n \neq m \end{cases}$$

Moreover, for any sequences $(u_n)_{n \in \mathbb{N}}$ and $(v_n)_{n \in \mathbb{N}}$ we have

$$\left(\forall n \in \mathbb{N} \quad v_n = \sum_{k=0}^n S_{n,k} u_k \right) \Leftrightarrow \left(\forall n \in \mathbb{N} \quad u_n = \sum_{k=0}^n (-1)^{n-k} s_{n,k} v_k \right)$$

This equivalence is called **Stirling inversion**.

- **Binomial coefficients:**

For $n \in \mathbb{N}$, we have by Proposition 6:

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

and

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

Therefore, the numbers $\binom{n}{k}$ and $(-1)^{n-k} \binom{n}{k}$ are the connection coefficients of the basis sequences $((x-1)^n)_{n \in \mathbb{N}}$ and $(x^n)_{n \in \mathbb{N}}$.

This implies

$$\sum_{k \geq 0} \binom{n}{k} (-1)^{k-m} \binom{k}{m} = \begin{cases} 1 & \text{if } n = m \\ 0 & \text{if } n \neq m \end{cases}$$

Moreover, for any sequences $(u_n)_{n \in \mathbb{N}}$ and $(v_n)_{n \in \mathbb{N}}$ we have

$$\left(\forall n \in \mathbb{N} \quad v_n = \sum_{k=0}^n \binom{n}{k} u_k \right) \Leftrightarrow \left(\forall n \in \mathbb{N} \quad u_n = \sum_{k=0}^n (-1)^{n-k} \binom{n}{k} v_k \right)$$

This equivalence is called **binomial inversion**. By replacing u_n by $(-1)^n u_n$, we get a more symmetric version:

For any sequences $(u_n)_{n \in \mathbb{N}}$ and $(v_n)_{n \in \mathbb{N}}$ we have

$$\left(\forall n \in \mathbb{N} \quad v_n = \sum_{k=0}^n (-1)^k \binom{n}{k} u_k \right) \Leftrightarrow \left(\forall n \in \mathbb{N} \quad u_n = \sum_{k=0}^n (-1)^k \binom{n}{k} v_k \right)$$

Application: We consider again the derangement numbers D_n . We have

$$n! = \sum_{k=0}^n \binom{n}{k} D_k$$

because $\binom{n}{n-k} D_k = \binom{n}{k} D_k$ is the number of n -permutations with exactly $n-k$ fixed points. By applying the first version of the binomial inversion (with $v_n = n!$ and $u_k = D_k$), we get

$$D_n = \sum_{k=0}^n (-1)^{n-k} \binom{n}{k} k! = n! \sum_{k=0}^n \frac{(-1)^{n-k}}{(n-k)!} = n! \sum_{k=0}^n \frac{(-1)^k}{k!}.$$

3 Solving Recursions

3.1 Linear Recursions of Depth 1

Theorem 30 *Let $T_0, T_1, \dots$ be a sequence that is given by numbers β and a_n, b_n with $a_n \neq 0$ ($n \in \mathbb{N} \setminus \{0\}$) and the following recursion:*

- $T_0 = \beta$,
- $T_n = a_n T_{n-1} + b_n$ for $n \geq 1$.

Then, for all $n \in \mathbb{N}$:

$$T_n = \prod_{k=1}^n a_k \left(\sum_{k=1}^n \frac{b_k}{\prod_{i=1}^k a_i} + T_0 \right).$$

Proof: Induction on n . For $n = 0$ the statement obviously holds, so assume $n \geq 1$. Then

$$\begin{aligned} T_n &= a_n T_{n-1} + b_n = a_n \prod_{k=1}^{n-1} a_k \left(\sum_{k=1}^{n-1} \frac{b_k}{\prod_{i=1}^k a_i} + T_0 \right) + b_n \\ &= \prod_{k=1}^n a_k \left(\sum_{k=1}^{n-1} \frac{b_k}{\prod_{i=1}^k a_i} + T_0 \right) + b_n = \prod_{k=1}^n a_k \left(\sum_{k=1}^n \frac{b_k}{\prod_{i=1}^k a_i} + T_0 \right). \end{aligned}$$

□

Remark: The recursion in the theorem above is a linear inhomogeneous recursion (where the term “inhomogeneous” refers to the fact that the numbers b_n may be non-zero).

Corollary 31 *Let $T_0, T_1, \dots$ be a sequence that is given by numbers a, b and β with $a \neq 1$ and the following recursion:*

- $T_0 = \beta$,
- $T_n = aT_{n-1} + b$ for $n \geq 1$.

Then, for all $n \in \mathbb{N}$:

$$T_n = a^n T_0 + b \frac{a^n - 1}{a - 1}.$$

Proof: For $a = 0$, we have $T_0 = \beta$ and $T_n = b$ for all $n \in \mathbb{N} \setminus \{0\}$, so the statement holds. For $a \neq 0$, the statement follows from the previous theorem and the fact that

$$\sum_{k=1}^n \frac{1}{a^k} = -1 + \sum_{k=0}^n \frac{1}{a^k} = -1 + \frac{\left(\frac{1}{a}\right)^n - a}{1 - a} = \frac{1 - \left(\frac{1}{a}\right)^n}{a - 1},$$

so $a^n b \sum_{k=1}^n \frac{1}{a^k} = b \frac{a^n - 1}{a - 1}$. □

As an application, we again consider the derangement numbers. For $n \geq 2$, we have

$$D_n = (n - 1)(D_{n-1} + D_{n-2})$$

because the set of fixed-point-free n -permutations can be decomposed into $(n - 1)D_{n-2}$ permutations where 1 is contained in a cycle of length 2 and $(n - 1)D_{n-1}$ permutations where 1 is contained in a cycle of length at least 3.

Thus (for $n \geq 3$)

$$D_n - nD_{n-1} = -(D_{n-1} - (n - 1)D_{n-2}) = D_{n-2} - (n - 2)D_{n-3}$$

and so on. Hence

$$D_n - nD_{n-1} = (-1)^{n-1}(D_1 - D_0) = (-1)^n,$$

which is also true for $n = 1$. Therefore, for $n \in \mathbb{N} \setminus \{0\}$:

$$D_n = nD_{n-1} + (-1)^n$$

This leads once again to

$$D_n = n! \left(\sum_{k=1}^n \frac{(-1)^k}{k!} + 1 \right) = n! \sum_{k=0}^n \frac{(-1)^k}{k!}$$

3.2 Generating Functions

Definition 9 A generating function of a sequence $(a_n)_{n \in \mathbb{N}}$ is the formal expression $\sum_{n \geq 0} a_n z^n$.

Let $\sum_{n \geq 0} a_n z^n$ and $\sum_{n \geq 0} b_n z^n$ be two generating functions. Then, their sum is $\sum_{n \geq 0} (a_n + b_n) z^n$, and (for $c \in \mathbb{R}$) $c \sum_{n \geq 0} a_n z^n$ is $\sum_{n \geq 0} (ca_n) z^n$. The product of $\sum_{n \geq 0} a_n z^n$ and $\sum_{n \geq 0} b_n z^n$ is given by the so-called **convolution** of the sequences $(a_n)_{n \in \mathbb{N}}$ and $(b_n)_{n \in \mathbb{N}}$:

$$\left(\sum_{n \geq 0} a_n z^n \right) \left(\sum_{n \geq 0} b_n z^n \right) = \sum_{n \geq 0} \left(\sum_{k=0}^n a_k b_{n-k} \right) z^n$$

Obviously, $\sum_{n \geq 0} a_n z^n = 0$ (i.e. all coefficients are 0) is the additive identity and $\sum_{n \geq 0} a_n z^n = 1$ (i.e. $a_0 = 1$, and all other coefficients are 0) is the multiplicative identity. The (multiplicative) **inverse** of a generating function $\sum_{n \geq 0} a_n z^n$ is a generating function $\sum_{n \geq 0} b_n z^n$ such that $(\sum_{n \geq 0} a_n z^n) (\sum_{n \geq 0} b_n z^n) = 1$.

Proposition 32 $\sum_{n \geq 0} a_n z^n$ has an inverse if and only if $a_0 \neq 0$.

Proof: “ $\Rightarrow$ ”: Obvious, because if $\sum_{n \geq 0} b_n z^n$ is an inverse of $\sum_{n \geq 0} a_n z^n$, then $b_0 = \frac{1}{a_0}$.
“ $\Leftarrow$ ”: Assume that $a_0 \neq 0$. By setting $b_0 = \frac{1}{a_0}$ and $b_n = -\frac{1}{a_0} \sum_{k=1}^n a_k b_{n-k}$ for $n \in \mathbb{N} \setminus \{0\}$ we get that $\sum_{k=0}^n a_k b_{n-k} = 1$ if $n = 0$ and $\sum_{k=0}^n a_k b_{n-k} = 0$ if $n \in \mathbb{N} \setminus \{0\}$. Thus $(\sum_{n \geq 0} a_n z^n) (\sum_{n \geq 0} b_n z^n) = 1$. $\square$

When considering generating functions, we do not care about the radius of convergence of the power series. However, in all our applications, the generating functions $\sum_{n \geq 0} a_n z^n$ have the property, that there is a constant $M > 0$ such that $|a_n| \leq M^n$, so at least for values $z \in \mathbb{C}$ with $z < \frac{1}{M}$, the series will converge. We always assume that z is small enough such that the series converges.

Examples: The following ways to compute generating functions are simply a consequence of the standard formula for the geometric sum:

- $\sum_{n \geq 0} z^n = \frac{1}{1-z}$.
- $\sum_{n \geq 0} a^n z^n = \frac{1}{1-az}$ for a constant a .
- $\sum_{n \geq 0} z^{2n} = \frac{1}{1-z^2}$.

The binomial theorem implies for $m \in \mathbb{N}$:

- $\sum_{n \geq 0} \binom{m}{n} z^n = (1+z)^m.$

By computing products of generating functions, we can get more closed formulas for generating functions. For example:

$$\frac{1}{(1-z)^2} = \left(\sum_{n \geq 0} z^n \right) \left(\sum_{n \geq 0} z^n \right) = \sum_{n \geq 0} (n+1) z^n = \sum_{n \geq 1} n z^{n-1}.$$

This leads to:

$$\sum_{n \geq 0} n z^n = \frac{z}{(1-z)^2}$$

and

$$\sum_{n \geq 0} (n+1) c^n z^n = \frac{1}{(1-cz)^2}.$$

More generally, we get for $m \in \mathbb{N}$:

$$\left(\frac{1}{1-z} \right)^m = \left(\sum_{n \geq 0} z^n \right)^m = \sum_{n \geq 0} \binom{m+n-1}{n} z^n$$

because $\binom{m+n-1}{n}$ is the number of ways to choose n non-distinguishable objects from m distinguishable bins.

3.3 Using Generating Functions to Solve Recursions

As an example, we consider the **Fibonacci numbers** $(F_n)_{n \in \mathbb{N}}$ which can be defined recursively by $F_0 = 0$, $F_1 = 1$ and $F_n = F_{n-1} + F_{n-2}$ (for $n \in \mathbb{N} \setminus \{0, 1\}$). We will show how such a homogeneous linear recursion can be solved (where “homogeneous” means that F_n is just a weighted sum of the previous numbers of the sequence without any additive term).

Excursion: Before we show how to find a formula for computing F_n directly, we want to note that even by just applying the recursion $F_n = F_{n-1} + F_{n-2}$, we can compute F_n with just $O(\log(n))$ instead of $\Theta(n)$ arithmetic operations. Consider the matrix $M = \begin{pmatrix} 1 & 1 \\ 1 & 0 \end{pmatrix}$. For $n \geq 2$, we have

$$\begin{pmatrix} F_n \\ F_{n-1} \end{pmatrix} = M \begin{pmatrix} F_{n-1} \\ F_{n-2} \end{pmatrix} = M^{n-1} \begin{pmatrix} F_1 \\ F_0 \end{pmatrix}.$$

Thus, we just have to compute M^{n-1} , which can be done by repeated squaring of matrices. For $k \in \{1, \dots, \lfloor \log_2(n-1) \rfloor\}$, we compute the matrix M^{2^k} . There are $O(\log(n))$ such matrices, and each matrix M^{2^k} can be computed from $M^{2^{k-1}}$ with a constant number of operations (for $k > 1$). Now, write $n-1 = 2^{k_1} + 2^{k_2} + \dots + 2^{k_t}$ for natural numbers $k_1 < k_2 < \dots < k_t$. Then, $M^{n-1} = M^{2^{k_1}} \cdot M^{2^{k_2}} \cdot \dots \cdot M^{2^{k_t}}$, so M^{n-1} can be computed by $O(\log(n))$ additional arithmetic operations.

Note that this trick can be applied to any homogeneous linear recursion of length k , i.e. any sequence $(a_n)_{n \in \mathbb{N}}$ which is defined by an equation $a_n = c_1 a_{n-1} + \dots + c_k a_{n-k}$ for $n \geq k$ (with constants $c_1, \dots, c_k$ and explicitly given values for $a_0, \dots, a_{k-1}$).

After this excursion, we return to the question for a direct formula for the Fibonacci numbers. There are five steps to solve such a recursion:

1. State the generating function $F(z) = \sum_{n \geq 0} F_n z^n$ and rewrite it using the recursion:

$$F(z) = F_0 + F_1 z + \sum_{n \geq 2} F_n z^n = z + \sum_{n \geq 0} F_{n+2} z^{n+2} = z + \sum_{n \geq 0} (F_{n+1} + F_n) z^{n+2}$$

2. Replace all infinite sums on the right-hand side by $F(z)$:

$$\begin{aligned} F(z) &= z + \sum_{n \geq 0} F_{n+1} z^{n+2} + \sum_{n \geq 0} F_n z^{n+2} = z + z \sum_{n \geq 0} F_{n+1} z^{n+1} + z^2 \sum_{n \geq 0} F_n z^n \\ &= z + z \sum_{n \geq 1} F_n z^n + z^2 F(z) = z + z(F(z) - F_0 z^0) + z^2 F(z) \\ &= z + zF(z) + z^2 F(z). \end{aligned}$$

3. Solve the equation for $F(z)$:

$$F(z) = \frac{z}{1 - z - z^2}.$$

4. Write the right-hand side as a formal power series.

The approach is the **partial fraction decomposition**. We search for numbers A, B, α , and β such that

$$\frac{z}{1 - z - z^2} = \frac{A}{1 - \alpha z} + \frac{B}{1 - \beta z}$$

We can find a solution of this equation by computing a solution of the following system of equations:

$$(i) \quad (1 - \alpha z)(1 - \beta z) = 1 - z - z^2$$

$$(ii) \quad A(1 - \beta z) + B(1 - \alpha z) = z$$

By equating the coefficients (i) leads to $\alpha + \beta = 1$ and $\alpha \cdot \beta = -1$. By combining these equations we get $\alpha^2 - \alpha - 1 = 0$, so $\alpha \in \{\frac{1}{2} + \frac{\sqrt{5}}{2}, \frac{1}{2} - \frac{\sqrt{5}}{2}\}$. We can choose $\alpha = \frac{1}{2} + \frac{\sqrt{5}}{2}$ which implies $\beta = \frac{1}{2} - \frac{\sqrt{5}}{2}$.

Equation (ii) gives $A = -B$ and $-A\left(\frac{1}{2} - \frac{\sqrt{5}}{2}\right) - B\left(\frac{1}{2} + \frac{\sqrt{5}}{2}\right) = 1$. Therefore, we get $A = \frac{1}{\sqrt{5}}$ and $B = -\frac{1}{\sqrt{5}}$.

Since these numbers A, B, α , and β solve the equations (i) and (ii), we get (by applying the formula for the geometric sum):

$$F(z) = \frac{\frac{1}{\sqrt{5}}}{1 - \left(\frac{1+\sqrt{5}}{2}\right)z} + \frac{-\frac{1}{\sqrt{5}}}{1 - \left(\frac{1-\sqrt{5}}{2}\right)z} = \sum_{n \geq 0} \frac{1}{\sqrt{5}} \left(\left(\frac{1+\sqrt{5}}{2}\right)^n - \left(\frac{1-\sqrt{5}}{2}\right)^n \right) z^n.$$

5. Now, we get the sequence by comparing the coefficients:

$$F_n = \frac{1}{\sqrt{5}} \left(\left(\frac{1+\sqrt{5}}{2} \right)^n - \left(\frac{1-\sqrt{5}}{2} \right)^n \right). \quad (3)$$

Remarks:

- Equation (3) is called Binet's formula.
- The number $\Phi = \frac{1+\sqrt{5}}{2} \approx 1.618$ is called **golden ratio**.

General approach for solving linear recursions: Consider a (homogeneous) linear recursion of length k :

$$\begin{aligned} a_n &= c_1 a_{n-1} + \cdots + c_k a_{n-k} & (n \geq k) \\ a_i &= b_i & (i \in \{0, \dots, k-1\}) \end{aligned}$$

1./2. Generating function is $A(z) = \sum_{n \geq 0} a_n z^n$. Application of the recursion:

$$\begin{aligned} A(z) &= \sum_{n=0}^{k-1} b_n z^n + \sum_{n \geq k} (c_1 a_{n-1} + \cdots + c_k a_{n-k}) z^n \\ &= \sum_{n=0}^{k-1} b_n z^n + c_1 z \left(A(z) - \sum_{i=0}^{k-2} a_i z^i \right) \\ &\quad + c_2 z^2 \left(A(z) - \sum_{i=0}^{k-3} a_i z^i \right) + \cdots + c_{k-1} z^{k-1} (A(z) - a_0) + c_k z^k A(z) \end{aligned}$$

3. Solve the equation for $A(z)$:

$$A(z) = \frac{d_0 + d_1 z + \cdots + d_{k-1} z^{k-1}}{1 - c_1 z - c_2 z^2 - \cdots - c_k z^k} \quad \text{for appropriate } d_0, \dots, d_{k-1}$$

4. Partial fraction decomposition:

$$A(z) = \sum_{i=1}^r \frac{g_i(z)}{(1 - \alpha_i z)^{m_i}}$$

where $g_i(z)$ is a polynomial of degree at most $m_i - 1$ ($i = 1, \dots, r$).

5. Computation of the coefficients. Let $g_i(z) = \sum_{j=0}^{m_i-1} g_{ij} z^j$ ($i = 1, \dots, r$). Then:

$$A(z) = \sum_{i=1}^r \sum_{j=0}^{m_i-1} g_{ij} \sum_{n \geq 0} \binom{n + m_i - 1}{n} \alpha_i^n z^{n+j}.$$

Computing the partial fraction decomposition boils down to computing zeros of a polynomial. Let $p(z) = 1 + e_1z + e_2z^2 + \cdots + e_kz^k$ be a polynomial with coefficient 1 of z^0 . $p^R(z) = z^k + e_1z^{k-1} + e_2z^{k-2} + \cdots + e_kz^0$ is called the **reflected polynomial** of p . This implies $p(z) = z^k p^R(\frac{1}{z})$. Let $\alpha_1, \dots, \alpha_k$ be the (complex) zeros of p^R , so

$$p^R(z) = (z - \alpha_1) \cdots (z - \alpha_k)$$

Thus

$$p(z) = z^k \left(\frac{1}{z} - \alpha_1 \right) \cdots \left(\frac{1}{z} - \alpha_k \right) = (1 - \alpha_1 z) \cdots (1 - \alpha_k z)$$

Therefore, the zeros of the reflected polynomial give us the denominators of the partial fraction decomposition.

The numerators can be computed by comparing coefficients of the polynomials. This leads to an equation system with k variables and k equations.

The following section on simultaneous recursions was not covered by the lecture.

Simultaneous Recursions

We can also use generating functions to solve **simultaneous recursions** of two sequences $(a_n)_{n \in \mathbb{N}}$ and $(b_n)_{n \in \mathbb{N}}$ where a_n may depend on $b_1, \dots, b_{n-1}$ and b_n on $a_1, \dots, a_{n-1}$. We consider an example that is motivated by the following question: What is the digit immediately to the right of the decimal point in the decimal representation of $(\sqrt{2} + \sqrt{3})^{1980}$?

The approach to solve this problem is to consider more generally the numbers $(\sqrt{2} + \sqrt{3})^{2n}$ for $n \in \mathbb{N}$. For small value of n , we get the following numbers:

$$\begin{aligned} (\sqrt{2} + \sqrt{3})^0 &= 1 \\ (\sqrt{2} + \sqrt{3})^2 &= 5 + 2\sqrt{6} \\ (\sqrt{2} + \sqrt{3})^4 &= (5 + 2\sqrt{6})^2 = 49 + 20\sqrt{6} \end{aligned}$$

Claim: There are sequences $(a_n)_{n \in \mathbb{N}}$ and $(b_n)_{n \in \mathbb{N}}$ with $a_n, b_n \in \mathbb{N}$ for $n \in \mathbb{N}$ such that $(\sqrt{2} + \sqrt{3})^{2n} = a_n + b_n\sqrt{6}$.

Proof of the Claim: Apply induction: The case $n = 0$ is trivial (set $a_0 = 1$ and $b_0 = 0$). For $n \in \mathbb{N} \setminus \{0\}$, we get:

$$\begin{aligned} (\sqrt{2} + \sqrt{3})^{2n} &= (\sqrt{2} + \sqrt{3})^{2n-2} (\sqrt{2} + \sqrt{3})^2 \\ &= (a_{n-1} + b_{n-1}\sqrt{6}) (5 + 2\sqrt{6}) \\ &= (5a_{n-1} + 12b_{n-1}) + (2a_{n-1} + 5b_{n-1})\sqrt{6} \end{aligned}$$

This proves the claim. □ **Claim**

The proof also yields recursion formulas for a_n and b_n for $n \geq 1$:

$$\begin{aligned} a_n &= 5a_{n-1} + 12b_{n-1} \\ b_n &= 2a_{n-1} + 5b_{n-1} \end{aligned}$$

Moreover, we have $a_0 = 1$ and $b_0 = 0$.

We can solve this recursion by using the generating function $A(z) = \sum_{n \geq 0} a_n z^n$ and $B(z) = \sum_{n \geq 0} b_n z^n$. This gives us

$$A(z) = a_0 z^0 + \sum_{n \geq 1} a_n z^n = a_0 + \sum_{n \geq 1} (5a_{n-1} + 12b_{n-1}) z^n = 1 + 5zA(z) + 12zB(z)$$

and

$$B(z) = b_0 z^0 + \sum_{n \geq 1} b_n z^n = \sum_{n \geq 1} (2a_{n-1} + 5b_{n-1}) z^n = 2zA(z) + 5zB(z).$$

The latter equation implies $B(z) = \frac{2zA(z)}{1-5z}$, and together with the previous equation, we get $A(z) = 1 + 5zA(z) + \frac{24z^2A(z)}{1-5z}$, so

$$A(z) = \frac{1 - 5z}{1 - 10z + z^2}$$

We use the equation

$$1 - 10z + z^2 = (1 - (5 + 2\sqrt{6})z) (1 - (5 - 2\sqrt{6})z)$$

to get a partial fraction decomposition

$$A(z) = \frac{1 - 5z}{1 - 10z + z^2} = \frac{\frac{1}{2}}{1 - (5 + 2\sqrt{6})z} + \frac{\frac{1}{2}}{1 - (5 - 2\sqrt{6})z}.$$

Thus

$$a_n = \frac{1}{2} \left((5 + 2\sqrt{6})^n + (5 - 2\sqrt{6})^n \right). \quad (4)$$

Now, we can use this result to answer the initial question.

We have $(5 + 2\sqrt{6})^n = (\sqrt{2} + \sqrt{3})^{2n} = a_n + b_n\sqrt{6}$. Therefore, (4) implies:

$$a_n = \frac{1}{2} \left(a_n + b_n\sqrt{6} + (5 - 2\sqrt{6})^n \right),$$

which leads to

$$a_n = b_n\sqrt{6} + (5 - 2\sqrt{6})^n.$$

Since a_n is integral, this yields $\{b_n\sqrt{6}\} + \{(5 - 2\sqrt{6})^n\} = 1$ (where $\{x\} := x - \lfloor x \rfloor$ for $x \in \mathbb{R}$). However, $5 - 2\sqrt{6} < 0.11$, so for $n = 990$, the first digits after the decimal point in the decimal representation of $(5 - 2\sqrt{6})^n$ are 0. Therefore, the first digits after the decimal point in the decimal representation of $b_{990}\sqrt{6}$ must be 9. Since $a_{990} \in \mathbb{N}$, the same is true for $(\sqrt{2} + \sqrt{3})^{1980} = a_{990} + b_{990}\sqrt{6}$, so the answer is “9”.

3.4 Exponential Generating Functions

Definition 10 For a sequence $(a_n)_{n \in \mathbb{N}}$ we call $\hat{A}(z) = \sum_{n \geq 0} \frac{a_n}{n!} z^n$ the **exponential generating function** of $(a_n)_{n \in \mathbb{N}}$.

Thus the exponential generating function of $(a_n)_{n \in \mathbb{N}}$ is simply the generating function of $(\frac{a_n}{n!})_{n \in \mathbb{N}}$, so we can make use of all results for the generating functions. In particular, for the **product of the exponential generating functions** $\hat{A}(z) = \sum_{n \geq 0} \frac{a_n}{n!} z^n$ and $\hat{B}(z) = \sum_{n \geq 0} \frac{b_n}{n!} z^n$ we get the exponential generating function $\hat{C}(z) = \sum_{n \geq 0} \frac{c_n}{n!} z^n$ of the sequence $(c_n)_{n \in \mathbb{N}}$ with

$$\frac{c_n}{n!} = \sum_{k=0}^n \frac{a_k}{k!} \frac{b_{n-k}}{(n-k)!}$$

because $(\frac{c_n}{n!})_{n \in \mathbb{N}}$ must be the convolution of $(\frac{a_n}{n!})_{n \in \mathbb{N}}$ and $(\frac{b_n}{n!})_{n \in \mathbb{N}}$.

Therefore, $\hat{C}(z) = \hat{A}(z)\hat{B}(z)$ holds if and only if for all $n \in \mathbb{N}$:

$$c_n = \sum_{k=0}^n \binom{n}{k} a_k b_{n-k}. \quad (5)$$

This equivalence is called **binomial convolution**.

Applications:

- By writing the Taylor series for the exponential function, we get $e^{az} = \sum_{n \geq 0} \frac{a^n}{n!} z^n$. Moreover, $e^{az} \cdot e^{bz} = e^{(a+b)z}$. Hence, by using (5) and comparing the coefficients of z^n in $e^{az} \cdot e^{bz}$ and $e^{(a+b)z}$ we get again the binomial theorem:

$$(a+b)^n = \sum_{k=0}^n \binom{n}{k} a^k b^{n-k}.$$

- We have $(1+z)^a = \sum_{n \geq 0} \binom{a}{n} z^n = \sum_{n \geq 0} \frac{a^n}{n!} z^n$, so $(1+z)^a$ is the exponential generating function of $(\frac{a^n}{n!})_{n \in \mathbb{N}}$. Since we have $(1+z)^a (1+z)^b = (1+z)^{a+b}$, we get by (5) and equating the coefficients

$$(a+b)^n = \sum_{k=0}^n \binom{n}{k} a^k b^{n-k}$$

By dividing this equation by $n!$ we get the Vandermonde identity:

$$\binom{a+b}{n} = \sum_{k=0}^n \binom{a}{k} \binom{b}{n-k}.$$

- For the derangement numbers D_n , we have already proved the formula $n! = \sum_{k=0}^n \binom{n}{k} D_k$. This means that $(n!)_{n \in \mathbb{N}}$ is the convolution of $(D_n)_{n \in \mathbb{N}}$ and the sequence $1, 1, 1, \dots$ whose exponential generating function is $\sum_{n \geq 0} \frac{1}{n!} z^n = e^z$. Thus, with $\hat{D}(z) = \sum_{n \geq 0} \frac{D_n}{n!} z^n$ the function $\hat{D}(z) \cdot e^z$ is the exponential generating function of $(n!)_{n \in \mathbb{N}}$, so

$$\hat{D}(z) \cdot e^z = \sum_{n \geq 0} \frac{n!}{n!} z^n = \sum_{n \geq 0} z^n = \frac{1}{1-z}.$$

This implies

$$\hat{D}(z) = \frac{e^{-z}}{1-z}. \quad (6)$$

We can consider $e^{-z} = \sum_{n \geq 0} \frac{1}{n!} (-1)^n z^n$ and $\frac{1}{1-z} = \sum_{n \geq 0} z^n$ as (standard) generating functions. By comparing coefficients in (6), this gives us once again the equation

$$\frac{D_n}{n!} = \sum_{k=0}^n \frac{1}{k!} (-1)^k.$$

- For $n \in \mathbb{N}$, let a_n be the number of mappings f from $\{1, \dots, n\}$ to $\{1, \dots, n\}$ for which there is a $j \in \{1, \dots, n\}$ with $\text{image}(f) = \{1, \dots, j\}$ (where we set $a_0 = 1$). So, for $n = 2$, we get $a_2 = 3$ (one mapping where both 1 and 2 are mapped to 1 and the two 2-permutations).

Let $\hat{A}(z) = \sum_{n \geq 0} \frac{a_n}{n!} z^n$ be the exponential generating function of $(a_n)_{n \in \mathbb{N}}$.

For a mapping with this property, let k be the number of elements mapped to 1. The k elements can be chosen in $\binom{n}{k}$ ways and the remainder can be mapped in a_{n-k} ways to $\{2, \dots, n\}$. Therefore, for $n \in \mathbb{N} \setminus \{0\}$, we have

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

and for $n \in \mathbb{N}$, we have

$$2a_n = \sum_{k=0}^n \binom{n}{k} a_{n-k} + \begin{cases} 1 & \text{if } n = 0 \\ 0 & \text{if } n \neq 0. \end{cases}$$

Thus, by the binomial convolution, we get

$$2\hat{A}(z) = e^z \hat{A}(z) + 1$$

and hence

$$\hat{A}(z) = \frac{1}{2 - e^z} = \frac{1}{2} \cdot \frac{1}{1 - \frac{e^z}{2}} = \frac{1}{2} \sum_{k \geq 0} \left(\frac{e^z}{2} \right)^k = \sum_{k \geq 0} \frac{1}{2^{k+1}} \sum_{n \geq 0} \frac{k^n z^n}{n!}.$$

By comparing coefficients, this implies

$$a_n = \sum_{k \geq 0} \frac{k^n}{2^{k+1}}.$$

In particular, this shows that the expression $\sum_{k \geq 0} \frac{k^n}{2^{k+1}}$ is always a natural number.

II Graphs

We assume that the reader is familiar with basic facts on graphs as they are, e.g., taught in the lecture course “Algorithmische Mathematik I” (see Hougardy and Vygen [2016]). For an introduction, we also refer to Korte and Vygen [2018], and in particular we use the notation from the latter book.

4 Planar Graphs

This section largely follows the presentation in Korte and Vygen [2018], with some deviations.

In this section, all graphs are undirected but (unless stated otherwise) they may contain loops, i.e. edges connecting a node with itself, and also parallel edges are allowed. Nevertheless, we will use the notation $e = \{v, w\}$ to denote that e is an edge connecting the nodes v and w .

4.1 Basic Definitions and Results

Intuitively, graphs are called planar if they can be drawn into the plane without any crossing of the edges. To formalize this, we need the following definition.

Definition 11 *A simple Jordan curve is the image of a continuous injective function $\phi : [0, 1] \rightarrow \mathbb{R}^2$. Its endpoints are $\phi(0)$ and $\phi(1)$. A closed Jordan curve is the image of a continuous function $\phi : [0, 1] \rightarrow \mathbb{R}^2$ with $\phi(0) = \phi(1)$ and $\phi(\tau) \neq \phi(\tau')$ for $0 \leq \tau < \tau' < 1$.*

A polygonal arc is a simple Jordan curve which is the union of finitely many intervals (straight line segments). A polygon is a closed Jordan curve which is the union of finitely many intervals.

*Let $R = \mathbb{R}^2 \setminus J$ where J is the union of finitely many intervals. We define the **connected regions** of R as equivalence classes of points in R where two points are equivalent if they can be joined by a polygonal arc within R .*

We use this definition to formalize what it means to draw a graph into the plane.

Definition 12 A **planar embedding** of a graph G consists of an injective mapping $\psi : V(G) \rightarrow \mathbb{R}^2$ and for each edge $e = \{x, y\}$ either a polygonal arc J_e with endpoints $\psi(x)$ and $\psi(y)$ (if $x \neq y$) or a polygon J_e with $\psi(x) \in J_e$ (if $x = y$) such that for each $e = \{x, y\} \in E(G)$:

$$(J_e \setminus \{\psi(x), \psi(y)\}) \cap \left(\{\psi(v) \mid v \in V(G)\} \cup \bigcup_{e' \in E(G) \setminus \{e\}} J_{e'} \right) = \emptyset.$$

A graph is called **planar** if it has a planar embedding.

Definition 13 Let G be a planar graph with some planar embedding $\Phi = (\psi, (J_e)_{e \in E(G)})$. Then the set

$$\mathbb{R}^2 \setminus \left(\{\psi(v) \mid v \in V(G)\} \cup \bigcup_{e \in E(G)} J_e \right)$$

splits into open connected regions, called **faces** of Φ .

Note that exactly one of the faces in the definition above is unbounded, the **outer face**.

The following theorem gives us some topological basis for our planar embeddings. It seems to be obvious but it has to be proved.

Theorem 33 (Jordan curve theorem) If J is a polygon then $\mathbb{R}^2 \setminus J$ splits into exactly two connected regions, each of which has J as its boundary. If J is a polygonal arc then $\mathbb{R}^2 \setminus J$ has only one connected region.

Proof: See the proof of Theorem 2.30 in Korte and Vygen [2018]. □

Corollary 34 Let G be a simple connected planar graph with planar embedding $\Phi = (\psi, (J_e)_{e \in E(G)})$. The set $R := \mathbb{R}^2 \setminus \left(\{\psi(v) \mid v \in V(G)\} \cup \bigcup_{e \in E(G)} J_e \right)$ is connected if and only if G is a tree.

Proof: “ $\Rightarrow$ ”: If G is not a tree, it contains a cycle C , and the embedding of the cycle splits $\mathbb{R}^2$ into two regions. Both regions have a non-empty intersection with R , so R is not connected.

“ $\Leftarrow$ ”: Assume that G is a tree, we show the statement by induction on $|V(G)|$. If $|V(G)| = 1$, the statement is trivial. Let $|V(G)| > 1$. Let v be a leaf in G (i.e. a node of degree 1) and w be the

neighbor of v , $\tilde{e} = \{v, w\} \in E(G)$. Consider $\tilde{R} := \mathbb{R}^2 \setminus \left(\{\psi(v) \mid v \in V(G) \setminus \{v\}\} \cup \bigcup_{e \in E(G) \setminus \{\tilde{e}\}} J_e \right)$. By induction hypothesis, $\tilde{R}$ is connected. Now, let $p, q \in R$. Since $\tilde{R}$ is connected, there is a polygonal arc connecting p and q in $\tilde{R}$. If this arc does not cross or touch $J_{\tilde{e}}$, it also connects p and q in R . Otherwise both p and q are connected via polygonal arcs to points arbitrarily close to $J_{\tilde{e}}$, which implies that they can also be connected by polygonal arcs to any ball around $\psi(v)$ (by following a curve sufficiently close to $J_{\tilde{e}}$). Since any sufficiently small ball around $\psi(v)$ is connected, this shows that also R is connected. $\square$

Definition 14 Let G be a planar graph and $\Phi = (\psi, (J_e)_{e \in E(G)})$ a planar embedding of G . The **planar dual** G^* is the graph whose vertices are the faces of Φ and whose edge set is $\{e^* \mid e \in E(G)\}$ where e^* connects the faces that are adjacent to J_e (if e is incident to only one face then e^* is a loop).

Observation: The graph G^* is again planar and there is a planar embedding $(\psi^*, (J_{e^*})_{e^* \in E(G^*)})$ of G^* such that $\psi^*(F) \in F$ for all faces F of Φ and, for each $e \in E(G)$,

$$J_{e^*} \cap \left(\{\psi(v) \mid v \in V(G)\} \cup \bigcup_{f \in E(G) \setminus \{e\}} J_f \right) = \emptyset,$$

and $|J_{e^*} \cap J_e| = 1$, and if e^* is a loop then the face bounded by J_{e^*} contains exactly one endpoint of e . Such an embedding is called **standard embedding** of G^* .

Note that the dual graph G^* indeed depends on the embedding and not just on G .

Proposition 35 Let G be a simple connected planar graph with planar embedding $\Phi = (\psi, (J_e)_{e \in E(G)})$, and let G^* be its planar dual with standard embedding. Let T be a spanning tree in G . Let $F = E(G) \setminus E(T)$ and let F^* be the dual edges of the edges in F . Then $(V(G^*), F^*)$ is a spanning tree of G^* .

Proof: Since T is a tree and thus does not contain a cycle, Corollary 34 implies that the set $\mathbb{R}^2 \setminus \left(\{\psi(v) \mid v \in V(G)\} \cup \bigcup_{e \in E(T)} J_e \right)$ is connected, which implies that $(V(G^*), F^*)$ is a connected graph.

Now, assume that $(V(G^*), F^*)$ contains a cycle C . Then the standard embedding of the cycle C splits $\mathbb{R}^2$ into two regions. Let e^* be an edge in C and let $e = \{v, w\}$ be the corresponding edge of G . Then, the embedding of e crosses the standard embedding of e^* exactly once, so $\psi(v)$ and $\psi(w)$ are in different regions of the standard embedding of the dual graph. This means that v and w are in different connected components of $(V(G), E(G) \setminus F)$ because if P was a path between v and w in $(V(G), E(G) \setminus F)$, the embedding of P would be a polygonal arc outside the embedding of C connecting $\psi(v)$ and $\psi(w)$. This is a contradiction to the assumption that

T is connected. Therefore, $(V(G^*), F^*)$ cannot contain a cycle C .

Thus, $(V(G^*), F^*)$ is connected and does not contain a cycle, so it is a (spanning) tree. $\square$

Corollary 36 (*Euler's formula*): For any planar connected graph G with any embedding, the number of faces is $|E(G)| - |V(G)| + 2$.

Proof: Let T be a spanning tree of G . For a fixed planar embedding of G , let G^* be the planar dual of G with standard embedding. Let $F = E(G) \setminus E(T)$ and let F^* be the dual edges of the edges in F . Then, by Proposition 35, $(V(G^*), F^*)$ is a spanning tree of G^* . Since the number of edges in a spanning tree is by one smaller than the number of nodes, we have $|E(T)| = |V(G)| - 1$ and $|F^*| = |V(G^*)| - 1$. Moreover, we have $|E(T)| + |F^*| = |E(G)|$, so we get $|E(G)| = |V(G)| + |V(G^*)| - 2$. Since the number of faces is $|V(G^*)|$, this proves the corollary. $\square$

Definition 15 Let $k \in \mathbb{Z}_{\geq 2}$. A graph is **k -connected** if it has more than k nodes and it stays connected even if we remove any $k - 1$ nodes. A graph is **k -edge-connected** if it has at least two nodes and it stays connected even if we remove any $k - 1$ edges.

Notation: For two graphs G and H we denote by $G + H$ a graph with node set $V(G) \cup V(H)$ and edge set $E(G) \cup E(H)$.

Definition 16 Let G be a graph. An **ear-decomposition** of G is a sequence $r, P_1, P_2, \dots, P_k$ with $G = (\{r\}, \emptyset) + P_1 + \dots + P_k$ such that each P_i is either a path where exactly the endpoints belong to $\{r\} \cup V(P_1) \cup \dots \cup V(P_{i-1})$ or a circuit where exactly one of its vertices belongs to $\{r\} \cup V(P_1) \cup \dots \cup V(P_{i-1})$ (for $i \in \{1, \dots, k\}$). The graphs $P_1, \dots, P_k$ are called **ears**. The ear-decomposition is called **proper** if

- $k \geq 1$
- P_1 is a circuit of length at least three, and
- $P_2, \dots, P_k$ are paths.

Proposition 37 (*Whitney [1932]*) A graph without loops is 2-connected if and only if it has a proper ear-decomposition.

Proof: “ $\Leftarrow$ ”: A circuit of length at least three is 2-connected. Moreover, if G is 2-connected and P is an x - y -path with $x, y \in V(G)$ and $x \neq y$, then obviously $G + P$ is 2-connected, too. By induction on the number of ears, we can conclude that every graph with a proper

ear-decomposition is 2-connected.

“ $\Rightarrow$ ”: Let G be a 2-connected graph. Let G' be a maximal simple subgraph of G . Then, evidently, G' is also 2-connected. Thus, G' contains a circuit of length at least three (otherwise G' was a tree, which is not 2-connected). Hence G contains a subgraph H that has a proper ear-decomposition. Let H be maximal with that property.

Suppose that H is not spanning, i.e. that $V(G) \setminus V(H) \neq \emptyset$. Since G is connected, this implies that there is an edge $e = \{x, y\} \in E(G)$ with $x \in V(H)$ and $y \notin V(H)$. Let z be a vertex in $V(H) \setminus \{x\}$. Since $G - x$ is connected, there is a path P from y to z in $G - x$. Let z' be the first vertex on this path, when traversed from y , that belongs to $V(H)$. Then $P_{[y, z']} + e$ (where $P_{[y, z']}$ is the sub-path of P from y to z') can be added as an ear, contradicting the maximality of H .

Therefore, H is spanning. Since any edge of $E(G) \setminus E(H)$ can be added as an ear, we conclude that $H = G$. $\square$

Proposition 38 *In a 2-edge-connected planar graph every edge is on the boundary of two faces.*

Proof: Obviously an edge e cannot be on the boundary of more than two faces. If e is on the boundary of just one region then e^* would be a loop, so it cannot be contained in any dual spanning tree. Thus, e must be contained in every primal spanning tree. This means that e is a bridge, i.e. its removal would make the graph disconnected. This is a contradiction to the condition that G is 2-edge-connected. $\square$

Proposition 39 *Let G be a 2-connected planar graph without loops. Let Φ be a planar embedding of G . Then, every face of Φ is bounded by a polygon that is the embedding of a circuit.*

Proof: We apply induction on $|E(G)|$ using a proper ear-decomposition of G . If G is a circuit, the statement follows from Theorem 33. If G is not a circuit then let P be the last ear of some proper ear-decomposition of G . Denote the end nodes of P by x and y . Let G' be the graph before adding P , and let Φ' be the restriction of Φ to G' . Let $\Phi = (\psi, (J_e)_{e \in E(G)})$, and let F' be the face of Φ' containing $\bigcup_{e \in E(P)} J_e \setminus \{\psi(x), \psi(y)\}$. By induction, we know that F' is bounded by a circuit C . This circuit contains x and y , so C is the union of two x - y -paths Q_1 and Q_2 in G' . We can apply Theorem 33 to $Q_1 + P$ and $Q_2 + P$. Thus, we get $F' \cup \{\psi(x), \psi(y)\} = F_1 \dot{\cup} F_2 \dot{\cup} \bigcup_{e \in E(P)} J_e$ where F_1 and F_2 are two faces of G bounded by the circuits $Q_1 + P$ and $Q_2 + P$. Since the other faces of Φ' are exactly the faces of Φ , this proves the statement. $\square$

Definition 17 The **girth** $g(G)$ of a graph G is the length of a shortest circuit (here including loops) in G . If G does not contain a circuit we set $g(G) = \infty$.

Corollary 40 Let G be a 2-connected simple planar graph with girth k . Then, G has at most $(n-2)\frac{k}{k-2}$ edges. Any simple planar graph with $n \geq 3$ vertices has at most $3n-6$ edges.

Proof: First assume that G is 2-connected. Let Φ be a planar embedding of G , and let r be the number of faces. By Euler's formula we know $r = |E(G)| - |V(G)| + 2$. Moreover, each face is bounded by a circuit, i.e. by at least k edges. And (since G is also 2-edge-connected), each edge is on the boundary of exactly two faces. Thus, we get $kr \leq 2|E(G)|$. Together with Euler's formula, this leads to $|E(G)| - |V(G)| + 2 \leq \frac{2}{k}|E(G)|$ and $|E(G)| \leq (n-2)\frac{k}{k-2}$.

If G is not 2-connected, we add edges between non-adjacent vertices while preserving planarity until the graph becomes 2-connected. Therefore, even after adding these edges, we have at most $(n-2)\frac{3}{3-2} = 3n-6$ edges. $\square$

Notation: For $n \in \mathbb{N} \setminus \{0\}$ we denote by K_n the complete graph on n nodes. And for $k, l \in \mathbb{N} \setminus \{0\}$ denote by $K_{k,l}$ the complete bipartite graph with bipartition sizes k and l .

Corollary 41 Neither K_5 nor $K_{3,3}$ is planar.

Proof: K_5 has 5 nodes but $10 > 3 \cdot 5 - 6 = 9$ edges, so it cannot be planar. $K_{3,3}$ has 6 nodes and is 2-connected with girth 4 (as a bipartite graph, it does not contain any odd circuit) but has $9 > (6-2)\frac{4}{4-2} = 8$ edges. $\square$

4.2 Kuratowski-Wagner Theorem

Notation:

- Two graphs G and H are **isomorphic** if there are bijections $\Phi_V : V(G) \rightarrow V(H)$ and $\Phi_E : E(G) \rightarrow E(H)$ such that $\Phi_E(\{v, w\}) = \{\Phi_V(v), \Phi_V(w)\}$ for all $\{v, w\} \in E(G)$.
- For a graph G and $X \subseteq V(G)$, by **contracting** X we mean deleting the vertices in X and the edges in $G[X]$, adding a new vertex x and replacing each edge $\{v, w\}$ with $v \in X$ and $w \notin X$ by an edge $\{x, w\}$ (parallel edges may arise). We denote the resulting graph by G/X .

Definition 18 Let G and H be two graphs. G is a **minor** of H if there is a subgraph H' of H and a partition $V(H') = V_1 \dot{\cup} \dots \dot{\cup} V_k$ of its vertex set into connected subsets such that contracting each of the sets $V_1, \dots, V_k$ yields a graph which is isomorphic to G .

Observation: For two graphs G and H where G does not contain loops, G is a minor of H if and only if it can be obtained from H by a series of operations of the following types:

- delete a vertex,
- delete an edge,
- contract an edge.

Note that any minor of a planar graph is planar. Thus, if a graph contains K_5 or $K_{3,3}$ as a minor, it cannot be planar. We will show the other direction, i.e. that if a graph is not planar, it contains K_5 or $K_{3,3}$ as a minor.

Lemma 42 (Tutte [1961], Thomassen [1980]) Let G be a 3-connected graph with at least five vertices. Then, there is an edge e such that G/e is also 3-connected.

Proof: Suppose there is no such edge. Then for each edge $e = \{v, w\}$, the graph G/e is at most 2-connected, i.e. there are two nodes whose removal makes the graph G/e disconnected. One of these nodes must be the node created by contracting e (otherwise G was not 3-connected). In other words, for each edge $e = \{v, w\}$ there is a vertex x such that $G - \{x, v, w\}$ is disconnected, i.e. has a connected component C with $|V(C)| < |V(G)| - 3$. Choose e, x and C such that $|V(C)|$ is minimum.

The node x has a neighbor y in C because otherwise C is a connected component of $G - \{v, w\}$, contradicting the 3-connectivity of G . By our assumption, $G/\{x, y\}$ is not 3-connected, i.e. there is a vertex z such that $G - \{x, y, z\}$ is disconnected. Since $\{v, w\} \in E(G)$, there is a connected component D of $G - \{x, y, z\}$ which contains neither v nor w .

But D contains a neighbour d of y , since otherwise D is a connected component of $G - \{x, z\}$ (again contradicting 3-connectivity of G). So $d \in V(D) \cap V(C)$, and thus D is a subgraph of C . Since $y \in V(C) \setminus V(D)$, we have a contradiction to the minimality of $|V(C)|$. $\square$

Theorem 43 (Kuratowski [1930], Wagner [1937]) A 3-connected graph is planar if and only if it contains neither K_5 nor $K_{3,3}$ as a minor.

Proof: “ $\Rightarrow$ ”: Since the minor of a planar graph is planar and K_5 and $K_{3,3}$ are not planar, a 3-connected planar graph cannot contain K_5 or $K_{3,3}$ as a minor.

“ $\Leftarrow$ ”: We prove by induction on the number of nodes that any 3-connected graph G with no K_5 or $K_{3,3}$ minor is planar. Since a 3-connected graph has to have at least 4 nodes, we start with $|V(G)| = 4$. But then the statement is trivial because K_4 is planar. Thus, assume $|V(G)| \geq 5$. We can assume that G does not contain loops. Lemma 42 implies that there is an edge $e = \{v, w\}$ such that G/e is 3-connected. By induction, we know that G/e is planar, so let $\Phi = (\psi, (J_{e'})_{e' \in E(G/e)})$ be a planar embedding of G/e . Let x be the vertex in G/e which arises by contracting e . Consider $(G/e) - x$ with the restriction of Φ as a planar embedding. Since $(G/e) - x$ is 2-connected, Proposition 39 implies that every face is bounded by the embedding of a circuit. Let C be the circuit whose embedding bounds the face containing the point $\psi(x)$.

Let $y_1, \dots, y_k \in V(C)$ be the neighbors of v different from w , numbered in cyclic order, and partition C into edge-disjoint paths P_i ($i \in \{1, \dots, k\}$) such that P_i is a y_i - y_{i+1} -path, where $y_{k+1} := y_1$ (see Fig. 1 (a)).

Denote by $Z = \{y \in V(G) \mid \{w, y\} \in E(G)\}$ the set of neighbors of w in G .

Claim: There is an index $i \in \{1, \dots, k\}$ such that $Z \subseteq \{v\} \cup V(P_i)$.

Proof of the Claim: We distinguish 3 cases.

Case 1: w has three neighbors among $y_1, \dots, y_k$.

Then, after contracting the paths between the neighbors of w on C to one edge each, we get a K_5 -minor, which is a contradiction (see Fig. 1 (b)).

Case 2: $Z = \{v, y_i, y_j\}$ for some $i < j$.

Then, if $i + 1 = j$ or $(i, j) = (1, k)$ then $Z \subseteq \{v\} \cup V(P_i)$ or $Z \subseteq \{v\} \cup V(P_k)$, and we are done. Thus, assume $i + 1 < j$ and $(i, j) \neq (1, k)$. Since there is a neighbor of v on the y_i - y_j path on C and a neighbor on the y_j - y_i path on C , and both neighbors are different from y_i and y_j , we get a $K_{3,3}$ -minor, which is a contradiction (see Fig. 1 (c)).

Case 3: There is a neighbor z of w in $V(P_i) \setminus \{y_i, y_{i+1}\}$ for some i and another neighbor $z' \notin V(P_i)$.

In this case, we again get a $K_{3,3}$ minor (see Fig. 1 (d)), which is a contradiction.

So, all 3 cases lead to a contradiction. However, if none of the 3 cases applies then it is easy to check that all neighbors of w except v must be contained in $V(P_i)$ for some $i \in \{1, \dots, k\}$. This proves the claim. $\square$ **Claim**

Since all neighbors of w are contained in $\{v\} \cup V(P_i)$ the embedding of $(G/e) - x$ can be easily extended to an embedding of G by setting $\psi(v) := \psi(x)$ and by placing w somewhere in the face of Φ bounded by the embeddings of P_i , $\{v, y_i\}$, and $\{v, y_{i+1}\}$. $\square$

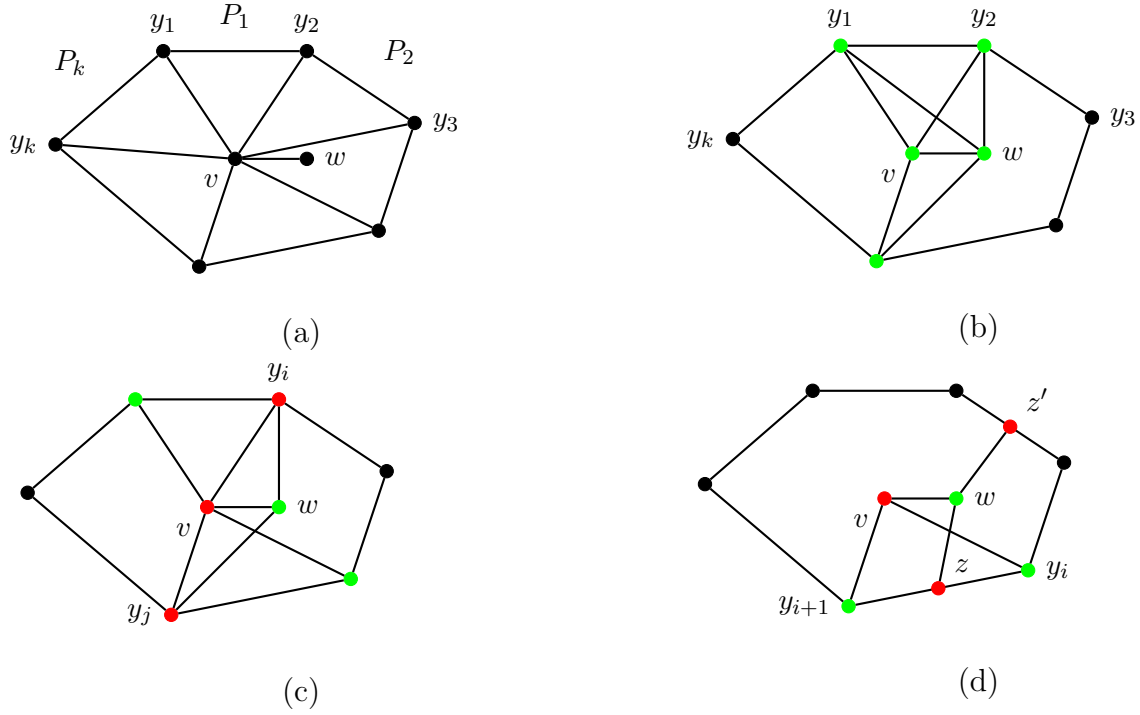


Figure 1: Proof of Theorem 43

Lemma 44 (Thomassen [1980]) *Let G be a graph with at least five vertices which is not 3-connected and which contains neither K_5 nor $K_{3,3}$ as a minor. Then there are two non-adjacent vertices $v, w \in V(G)$ such that adding an edge between v and w leads to a graph that does not contain a K_5 or $K_{3,3}$ minor either.*

Proof: See the proof of Lemma 2.38 in Korte and Vygen [2018]. □

Theorem 45 (Kuratowski-Wagner Theorem, Kuratowski [1930], Wagner [1937]) *A graph is planar if and only if it contains neither K_5 nor $K_{3,3}$ as a minor.*

Proof: “ $\Rightarrow$ ”: Since the minor of a planar graph is planar and K_5 and $K_{3,3}$ are not planar, a planar graph cannot contain K_5 or $K_{3,3}$ as a minor.

“ $\Leftarrow$ ”: Let G be a graph containing neither K_5 nor $K_{3,3}$ as a minor. If $|V(G)| \leq 4$ then the statement is trivial, so assume $|V(G)| \geq 5$. If G is 3-connected then by Theorem 43, G is planar. Otherwise apply Lemma 44 and add edges in such a way that the graph still does not contain K_5 or $K_{3,3}$ as a minor until the graph is 3-connected. By Theorem 43, the graph with the additional edges is planar, so G is planar as well. □

Remark: This version of the result is due to Wagner [1937]. Kuratowski [1930] formulated a

version that used the notion of subdivisions instead of minors (see exercises).

Proposition 46 *Let G be a planar connected graph with a fixed planar embedding. Let G^* be its planar dual with standard embedding. Then $(G^*)^*$ and G are isomorphic.*

Proof: For $|V(G)| = 1$, the statement is trivial, so we assume $|V(G)| > 1$. Let $\Phi = (\psi, (J_e)_{e \in E(G)})$ be the fixed planar embedding and $\Phi^* = (\psi^*, (J_{e^*})_{e^* \in E(G^*)})$ be a standard embedding of G^* . Let F be a face of the standard embedding Φ^* of G^* . The boundary of F contains J_{e^*} for at least one edge e^* , so F must contain $\psi(v)$ for one endpoint v of e . Thus, every face of Φ^* contains at least one vertex of G .

Euler's formula, applied to G^* and G , implies that the number of faces of G^* is

$$|E(G^*)| - |V(G^*)| + 2 = |E(G^*)| - (|E(G)| - |V(G)| + 2) + 2 = |V(G)|.$$

Therefore, every face of G^* contains exactly one vertex of G . This implies that G and $(G^*)^*$ are isomorphic. $\square$

5 Colorings of Graphs

In this section, all graphs will be simple (and as usual undirected).

5.1 Vertex Colorings

Definition 19 *For a graph G , a **vertex coloring** of G is a mapping $c : V(G) \rightarrow \mathbb{N} \setminus \{0\}$ such that $c(v) \neq c(w)$ for every $\{v, w\} \in E(G)$. A vertex coloring c is called a **k -vertex coloring** if $c(v) \leq k$ for all $v \in V(G)$. If there is a k -vertex coloring of G , then we call G **k -(vertex-)colorable**. If c is a k -vertex coloring of G , then the sets $\{v \in V(G) \mid c(v) = i\}$ are called **color classes** of c ($i = 1, \dots, k$). The **chromatic number** $\chi(G)$ of G is the smallest number k such that G is k -colorable. If $k = \chi(G)$, the graph G is called **k -chromatic**.*

In the following, we want to prove bounds on the chromatic number of graphs.

Remark: For a graph G let $\alpha(G)$ be the size of a largest stable set in G and $\omega(G)$ the size of a largest clique in G . We immediately get the following lower bounds on $\chi(G)$.

- In a vertex coloring, all color classes are stable sets, and $\chi(G)$ is the smallest number of stable sets into which $V(G)$ can be partitioned. Since each of the color classes has at

most $\alpha(G)$ elements, we get a lower bound of

$$\chi(G) \geq \frac{|V(G)|}{\alpha(G)}.$$

- Since all vertices in a clique must get different colors in a vertex coloring, we get the following bound

$$\chi(G) \geq \omega(G).$$

Notation: For a graph G let $\Delta(G) := \max\{|\delta_G(v)| \mid v \in V(G)\}$ be its maximum degree.

Proposition 47 *For every graph G , we have:*

$$\chi(G) \leq \Delta(G) + 1.$$

Proof: The following greedy algorithm computes a coloring with $\Delta(G) + 1$ colors: Traverse the vertices of G in an arbitrary order and color each vertex v with the first color that has not yet been used at a neighbor of v . $\square$

Of course, the proof of the previous proposition yields an algorithm to compute a vertex coloring with $\Delta(G) + 1$ colors. However the chromatic number of a graph can be much smaller than $\Delta(G)$, see for example the graph $K_{1,n-1}$ where $\chi(K_{1,n-1}) = 2$ but $\Delta(K_{1,n-1}) = n - 1$.

Examples of graphs G with $\chi(G) = \Delta(G) + 1$ are complete graphs and odd cycles. For all other connected graphs we get a better bound on $\chi(G)$:

Theorem 48 (*Brooks' Theorem, Brooks [1941]*) *Let G be a connected graph that is neither a complete graph nor a cycle of odd length. Then:*

$$\chi(G) \leq \Delta(G).$$

Proof: Assume that the statement is false. Let G be a smallest (with respect to the number of vertices) counterexample, so in particular G is connected but neither a complete graph nor a cycle of odd length, and we have $\chi(G) = \Delta(G) + 1$. This implies $\Delta(G) > 2$ because G cannot be a cycle of even length or a path (in that case, we would have $\chi(G) = \Delta(G) = 2$).

Choose a vertex v with $|\delta_G(v)| = \Delta(G)$. Since G is not a complete graph, there must be two neighbors u and w of v that are not connected by an edge in G . To see this, note that otherwise v together with its neighbors formed a clique. Since G is connected but not complete, some neighbor of v would have degree larger than $\Delta(G)$, which is impossible.

We distinguish two cases:

Case 1: $G[V(G) \setminus \{u, w\}]$ is connected.

Then $G[V(G) \setminus \{u, w\}]$ contains a spanning tree T . Color u and w with color 1. Afterwards perform the following steps $(|V(G)| - 3)$ times:

- (1) Choose a leaf x of T with $v \neq x$.
- (2) Color x with the smallest color not used at the neighbors of x in G .
- (3) Remove x from T .

After these steps all vertices except v have been colored. For this coloring we need at most $\Delta(G)$ colors since by the choice of x step (1) the vertex x always has an uncolored neighbor (namely its neighbor in T). Thus, when x is colored, at most $\Delta(G) - 1$ of its neighbors have already been colored.

Finally, we have to assign a color to v . All of its $\Delta(G)$ neighbors have already been colored but at least two of them (u and w) got the same color, so also for v we can choose one of the colors in $\{1, \dots, \Delta(G)\}$.

Case 2: $G[V(G) \setminus \{u, w\}]$ is not connected.

Let A_1 be a connected component of $G[V(G) \setminus \{u, w\}]$. Set $V_1 := V(A_1) \cup \{u, w\}$ and $V_2 := V(G) \setminus V(A_1)$.

Then $\chi(G[V_i]) \leq \Delta(G)$ because $G[V_i]$ is not complete (there is no edge between u and w) and $\Delta(G) \geq 3$ ($i \in \{1, 2\}$). If, for both $G[V_1]$ and $G[V_2]$, there is a vertex coloring with $\Delta(G)$ colors such that u and w get different colors then we can choose these two colorings in such a way that u gets in both of them color 1 and w gets in both of them color 2. This way, we receive a vertex coloring of G with $\Delta(G)$ colors. Thus, we can assume that there is a $j \in \{1, 2\}$ such that every $\Delta(G)$ -vertex coloring of $G[V_j]$ colors u and w with the same color. Then both u and w have degree at least $\Delta(G) - 1$ in $G[V_j]$. Hence in $G[V_{3-j}]$ they have degree at most 1. Thus, as $\Delta(G) \geq 3$, also $G[V_{3-j}]$ has a vertex coloring with $\Delta(G)$ colors where u and w get the same color. Therefore G is $\Delta(G)$ -colorable. $\square$

Theorem 49 (Heawood [1890]) *For every planar graph G , we have $\chi(G) \leq 5$.*

Proof: We apply induction on $n = |V(G)|$. For $n \leq 5$, the statement is trivial, so assume $n > 5$. Since G is planar, it has at most $3n - 6$ edges. Therefore, there must be a node $v_0 \in V(G)$ of degree at most 5 (otherwise, we had $2|E(G)| = \sum_{v \in V(G)} |\delta_G(v)| \geq 6n$). By induction hypothesis, there must be a 5-vertex-coloring c of $G - v_0$. Let $v_1, \dots, v_k$ be the neighbors of v_0 (so in particular $k \leq 5$). If less than 5 colors are used by c for the neighbors of v_0 , we can simply color v_0 with an unused color out of $\{1, \dots, 5\}$. Thus, assume that all colors $\{1, \dots, 5\}$ occur among the neighbors of v_0 . This implies $k = 5$. As G is planar, there must be two non-adjacent neighbors v_i and v_j of v_0 (otherwise the nodes $\{v_1, \dots, v_5\}$ would be a 5-clique). The graph $G - v_0$ stays planar if we add an edge e between v_i and v_j (as there is a path via v_0 between v_i and v_j in G). And $(G - v_0)/e$ is also planar (where we ignore possible parallel edges), so by induction hypothesis, it has a 5-coloring. This corresponds to a 5-coloring

of $G - v_0$ in which v_i and v_j get the same color. But then, again, at least one color in $\{1, \dots, 5\}$ is left for v_0 . $\square$

The above proof is due to Kainen [1974].

Remark: By the famous **Four Color Theorem**, even four colors suffice to color planar graphs, so $\chi(G) \leq 4$ for any planar graph G . The first proof of this theorem was given in 1977 by Appel and Haken (Appel and Haken [1977a], Appel and Haken [1977b]). The proof is quite involved and cannot be shown here. The proof is based on the analysis of so-called *configurations*. A configuration is a connected subgraph of a graph G where we are given in addition degrees of the vertices of the subgraph in G . A set M of configurations is called *unavoidable* if every planar graph contains a configuration in M . We know for example that the set M^* consisting of 6 copies of K_1 , where we set the degree of the vertex in the i -th copy to i ($i = 0, \dots, 5$), is unavoidable because every planar graph has a vertex of degree at most 5.

A configuration is called *reducible* if no smallest counter example to the Four Color Theorem contains it. For example, the configuration which consists of the graph K_1 where we demand a vertex degree of 3 is obviously reducible. Now the goal is to find an unavoidable set of reducible configurations. For the Five Color Theorem (i.e. Theorem 49) we have seen that the elements of M^* are reducible. For the Four Color Theorem, Appel and Haken could find an unavoidable set of reducible configurations that consists of 1936 elements. To check this set of configurations they had to use a computer. Later on, they could reduce the number of configurations to 1476. A somewhat shorter proof that needed only 633 configurations (but nevertheless needed the help of a computer) was given by Robertson et al. [1997]. The ideas of the proof of the Four Color Theorem are summarized by Woodall and Wilson [1978] (see also Bollobás [1979]).

Definition 20 *The complement $\bar{G}$ of a graph G is the graph that is defined by the vertex set $V(\bar{G}) := V(G)$ and the edge set $E(\bar{G}) := \binom{V(\bar{G})}{2} \setminus E(G)$.*

The following proposition shows that the chromatic numbers of a graph G and its complement $\bar{G}$ cannot be both “very large” (i.e. in the range of $|V(G)|$) nor both “very small” (for example constant).

Proposition 50 (Nordhaus and Gaddum [1956]) *For every graph G with $|V(G)| = n$ we have:*

$$\begin{aligned} (a) \quad 2\sqrt{n} &\leq \chi(G) + \chi(\bar{G}) \leq n + 1, \\ (b) \quad n &\leq \chi(G)\chi(\bar{G}) \leq \left(\frac{n+1}{2}\right)^2. \end{aligned}$$

Proof: (i) Let $c : V(G) \rightarrow \{1, \dots, \chi(G)\}$ be a vertex coloring of G with $\chi(G)$ colors. Let n_i be the number of vertices of G colored with i ($i = 1, \dots, \chi(G)$). Then, $\max_{i \in \{1, \dots, \chi(G)\}} n_i \geq n/\chi(G)$. Since all vertices of a color class of c have to have different colors in a vertex coloring of $\bar{G}$, we get $\chi(\bar{G}) \geq \max_{i \in \{1, \dots, \chi(G)\}} n_i$. This implies $\chi(\bar{G}) \geq n/\chi(G)$ and thus $\chi(G)\chi(\bar{G}) \geq n$.

(ii) The inequality $(\chi(G) - \chi(\bar{G}))^2 \geq 0$ implies $(\chi(G) + \chi(\bar{G}))^2 \geq 4\chi(G)\chi(\bar{G})$, and hence we get $\chi(G) + \chi(\bar{G}) \geq 2(\chi(G)\chi(\bar{G}))^{\frac{1}{2}} \stackrel{(i)}{\geq} 2\sqrt{n}$.

(iii) We show $\chi(G) + \chi(\bar{G}) \leq n + 1$ by induction on $n = |V(G)|$.

For $n = 1$, the statement is trivial.

Let $n > 1$ and $v \in V(G)$. By induction hypothesis we have $\chi(G - v) + \chi(\bar{G} - v) \leq n$. Moreover

$$\chi(G) \leq \chi(G - v) + 1$$

and

$$\chi(\bar{G}) \leq \chi(\bar{G} - v) + 1.$$

If at least one of the last two inequalities is a strict inequality, then the statement follows directly. Hence assume that $\chi(G) = \chi(G - v) + 1$ and $\chi(\bar{G}) = \chi(\bar{G} - v) + 1$. This gives $|\delta_G(v)| \geq \chi(G - v)$ and $|\delta_{\bar{G}}(v)| (= n - 1 - |\delta_G(v)|) \geq \chi(\bar{G} - v)$. Since $|\delta_G(v)| + |\delta_{\bar{G}}(v)| = n - 1$, we get $\chi(G - v) + \chi(\bar{G} - v) \leq n - 1$ and finally $\chi(G) + \chi(\bar{G}) \leq n + 1$.

(iv) The inequality $\chi(G)\chi(\bar{G}) \leq \left(\frac{n+1}{2}\right)^2$ follows from the inequality shown in step (iii) and the inequality $(\chi(G) + \chi(\bar{G}))^2 \geq 4\chi(G)\chi(\bar{G})$. $\square$

If we are asked to construct graphs with large chromatic numbers, an easy solution would be to choose graphs with large cliques. However, the following proposition shows that there are also graphs with very small clique numbers but large chromatic numbers. This means that the clique number can be a very weak lower bound for the chromatic number.

Proposition 51 *For every $k \in \mathbb{N} \setminus \{0\}$ there is a graph G_k with $\chi(G_k) = k$ and $\omega(G_k) \leq 2$.*

Proof: The graphs G_k can be built recursively. For $k = 1$, this is trivial.

Hence, let $k > 1$. We assume that the graphs $G_1, \dots, G_{k-1}$ have already been built. G_k contains a copy of each of the graphs $G_1, \dots, G_{k-1}$ as a subgraph. In addition, G_k contains a vertex set A_k consisting of $|V(G_1)| \cdot |V(G_2)| \cdot \dots \cdot |V(G_{k-1})|$ vertices. Choose a bijection $\tau_k : A_k \rightarrow \{(v_1, \dots, v_{k-1}) \mid v_1 \in V(G_1), \dots, v_{k-1} \in V(G_{k-1})\}$. Then G_k contains (apart from the edges in the subgraphs $G_1, \dots, G_{k-1}$) for each vertex $v \in A_k$ an edge from v to the elements of the $(k-1)$ -tuple $\tau_k(v)$. By construction, the graph G_k does not contain any cycles of length three (provided that the graphs $G_1, \dots, G_{k-1}$ do not contain any 3-cycle).

Under the assumption that each G_i with $i \in \{1, \dots, k-1\}$ can be colored with i colors, the graph G_k can be colored with k colors: for the coloring of all subgraphs $G_1, \dots, G_{k-1}$ we need in total $k-1$ colors and the vertices in A_k (which is a stable set) can get the same color.

On the other hand, G_k is not $(k-1)$ -colorable if none of the G_i ($i = 1, \dots, k-1$) is $(i-1)$ -colorable. To prove this, assume that there was a $k-1$ -coloring of G_k . Then choose a vertex v_1 in G_1 with color c_1 . There must be a vertex v_2 in G_2 with color $c_2 \neq c_1$ because G_2 cannot be colored with just one color. Since G_3 is not 2-colorable there must be a vertex v_3 in G_3 with color $c_3 \notin \{c_1, c_2\}$. We can continue this and get for each $i \in \{1, \dots, k-1\}$ a vertex

v_i in G_i whose color c_i is not contained in $\{c_1, \dots, c_{i-1}\}$. But there is a vertex $v \in A_k$ with $\tau_k(v) = (v_1, \dots, v_{k-1})$. Thus, v is in G_k connected by an edge to all vertices in $\{v_1, \dots, v_{k-1}\}$, so it cannot be colored with any color from $c_1, \dots, c_{k-1}$. Therefore, we need k colors for a vertex coloring of G_k . $\square$

Remark: For any $k \in \mathbb{N}$ there are graphs G with $\chi(G) \geq k$ that do not contain any cycle of length less than k (see Nešetřil and Rödl [1979] or Diestel [2017] for proof of this statement).

Notation: We call a subgraph H of G an **induced subgraph** if $E(H) = E(G[V(H)])$.

Definition 21 An undirected graph G is called **perfect** if $\chi(H) = \omega(H)$ holds for every induced subgraph H of G .

There are several *NP*-hard problems that can be solved in polynomial-time if we restrict the instances to perfect graphs (see chapter 15 of Korte and Vygen [2018] for an introduction to *NP*-hardness). For example, one can compute maximum stable sets, maximum cliques and optimum vertex coloring in perfect graphs in polynomial time (see Grötschel, Lovász and Schrijver [1984]).

Proposition 52 (Lovász [1972b]) A graph is perfect if and only if $\alpha(H)\omega(H) \geq |V(H)|$ holds for every induced subgraph H .

Proof: The proof is taken from Schrijver [2003].

“ $\Rightarrow$ ”: Let G be perfect and H an induced subgraph of G . Then $\chi(H) = \omega(H)$, and since $\alpha(H)\chi(H) \geq |V(H)|$, this implies $\alpha(H)\omega(H) \geq |V(H)|$.

“ $\Leftarrow$ ”: Assume that there is a non-perfect graph G such that $\alpha(H)\omega(H) \geq |V(H)|$ for each induced subgraph H of G . We can assume that G is a smallest graph with this property, so in particular any proper induced subgraph of G (i.e. any induced subgraph different from G) is perfect.

Let $V(G) = \{1, \dots, n\}$, $\alpha = \alpha(G)$ and $\omega = \omega(G)$.

We first show that there are stable sets $S_0, S_1, \dots, S_{\alpha\omega}$ in G such that every vertex is contained in exactly α of these sets.

Let S_0 be a stable set of size α . For every $v \in S_0$, the graph $G - v$ is perfect, so $\chi(G - v) = \omega(G - v) \leq \omega(G)$. Thus $V(G) \setminus \{v\}$ can be decomposed in ω stable sets. By doing this for every $v \in S_0$, we get the sets $S_0, S_1, \dots, S_{\alpha\omega}$.

For each set S_i ($i = 0, \dots, \alpha\omega$) there is a clique C_i of size ω with $C_i \cap S_i = \emptyset$, because otherwise we would have $\omega(G) \geq \omega(G - S_i) + 1 = \chi(G - S_i) + 1 \geq \chi(G)$, which means that G is perfect.

Every clique C_i and every stable set S_j have at most one vertex in common, but in total every

C_i intersects $\alpha\omega$ of the sets S_j , because each of the ω elements of C_i is contained in α of the stable sets. Therefore, $|C_i \cap S_j| = 1$ for $i \neq j$.

Consider two $(\alpha\omega + 1) \times n$ -incidence matrices M and N with entries 0 and 1. Let $M = (M_{ij})_{(i,j) \in \{0, \dots, \alpha\omega\} \times \{1, \dots, n\}}$ with $M_{ij} = 1 \Leftrightarrow j \in S_i$ and $N = (N_{ij})_{(i,j) \in \{0, \dots, \alpha\omega\} \times \{1, \dots, n\}}$ with $N_{ij} = 1 \Leftrightarrow j \in C_i$.

Then, $MN^t = J - I$ where J is an $(\alpha\omega + 1) \times (\alpha\omega + 1)$ -matrix consisting of ones only, and I is the $(\alpha\omega + 1) \times (\alpha\omega + 1)$ -identity matrix. The matrix $J - I$ has rank $\alpha\omega + 1$, which implies $n \geq \alpha\omega + 1$. This is a contradiction to our assumption that $\alpha(H)\omega(H) \geq |V(H)|$ for each induced subgraph H of G . $\square$

Corollary 53 (*Weak perfect graph theorem*) (Lovász [1972a], Lovász [1972b]) *A graph G is perfect if and only if $\bar{G}$ is perfect.*

Proof: Follows directly from the previous theorem. $\square$

Thus, the following graphs and their complements are perfect:

- bipartite graphs,
- line graphs of bipartite graphs (we will prove this when we consider edge colorings, see Theorem 65),
- interval graphs (see exercises).

Theorem 54 (*Strong perfect graph theorem*) (Chudnovsky et al. [2006]) *A graph G is perfect if and only if it contains neither an odd cycle of length at least 5 nor the complement of an odd cycle with length at least 5 as an induced subgraph.*

For a proof we refer to Chudnovsky et al. [2006].

Of course, the strong perfect graph theorem directly implies the weak perfect graph theorem.

Theorem 55 *It can be checked in time $O(|V(G)|^9)$ if a given graph G is perfect.*

For a proof see Chudnovsky et al. [2005]. Note that this proof has been published before the proof of the strong perfect graph theorem. In fact, the authors described their algorithms only as a test for whether a given graph is a *Berge graph*, i.e. a graph that does not contain an odd cycle with length at least 5 nor the complement of an odd cycle with length at least 5 as an induced subgraph.

5.2 Chromatic Polynomials

So far, we have only considered the question of whether a valid coloring with a certain number of colors exists at all. In this section, we want to consider the number of different colorings that are possible with a given number of colors.

Definition 22 Let G be an undirected graph. For $t \in \mathbb{N}$, let $p_G(t)$ be the number of distinct valid vertex colorings of G with the colors $\{1, \dots, t\}$. The mapping $p_G : \mathbb{N} \rightarrow \mathbb{N}$ is called the **chromatic polynomial** of G .

The following theorem ensures that chromatic polynomials deserve their name:

Theorem 56 Let G be a simple undirected graph with n vertices and m edges. Then p_G is a polynomial of degree n . Moreover, with the representation $p_G(t) = \sum_{k=0}^n a_k t^k$ the following statements hold:

- (a) All a_i are integers.
- (b) $a_n = 1$.
- (c) $a_{n-1} = -m$ if $n \geq 1$.
- (d) $a_{n-2} = \binom{m}{2} - N_3(G)$ if $n \geq 2$, where $N_3(G)$ is the number of triangles in G .
- (e) $a_i \geq 0$ if $n - i$ is even.
- (f) $a_i \leq 0$ if $n - i$ is odd.
- (g) $|a_i| > 0 \Leftrightarrow i \geq l$, where l is the number of connected components of G .

Proof: We prove the statement by induction on the number of edges of G . Let $n := |V(G)|$. If $E(G) = \emptyset$, then we can choose any color for each vertex, so $p_G(t) = t^n$. The statements (a)–(g) are clearly true in this case. So let $E(G) \neq \emptyset$. Let $e = \{v, w\} \in E(G)$.

Claim: We have $p_{G-e}(t) = p_G(t) + p_{G/e}(t)$.

Proof of the Claim: The set of colorings of $G - e$ with t colors can be decomposed into the set of colorings in which v and w are colored differently (of which there are $p_G(t)$), and into the set of colorings in which v and w have the same color (of which there are $p_{G/e}(t)$). This proves the claim. $\square$ **Claim**

Let H be a maximal simple subgraph of G/e . This means, in H we replace all sets of parallel edges in G/e that may arise by contracting e by a single edge. Then, obviously, $p_{G/e}(t) = p_H(t)$. However, we have $|E(H)| = m - 1 - (N_3(G) - N_3(G - e))$ because any triangle in G that is not contained in $G - e$ creates a pair of parallel edges in G/e , and this is the only way how

parallel edges in G/e can occur.

Let $p_{G-e}(t) = \sum_{k=0}^n b_k t^k$ (with $b_n = 1$) and $p_{G/e}(t) = \sum_{k=0}^n c_k t^k$ (with $c_n = 0$ and $c_{n-1} = 1$). Then $p_G(t) = \sum_{k=0}^n (b_k - c_k) t^k$, and the statements (a)–(g), whose validity we can assume for $G - e$ and H , are thereby also transferred to G . For statement (d), we compute

$$\begin{aligned} b_{n-2} - c_{n-2} &= \binom{m-1}{2} - N_3(G-e) + |E(H)| \\ &= \binom{m-1}{2} - N_3(G-e) + m-1 - (N_3(G) - N_3(G-e)) \\ &= \binom{m}{2} - N_3(G). \end{aligned}$$

□

The question of whether a graph G can be colored with k colors thus reduces to the question of whether p_G has a zero at k . For example, a graph G is bipartite (i.e., 2-vertex-colorable) if and only if its chromatic polynomial cannot be written in the form $p_G(t) = (t-2)f(t)$ for a polynomial f .

In general, determining the chromatic polynomial of a graph is NP-hard. If the chromatic polynomial is known, one can easily determine the chromatic number of the graph in polynomial time since the a_i from the above theorem are integers and satisfy $|a_i| \leq \binom{|V(G)|}{|E(G)|-i}$ (see Meredith [1972] for a proof of this statement).

In some cases, however, the chromatic polynomial is known.

Theorem 57 *Let G be a graph consisting of the connected components $G_1, \dots, G_k$. Then $p_G(t) = \prod_{i=1}^k p_{G_i}(t)$.*

Proof: For every valid vertex coloring c of G with t colors, we associate the vector $(c_1, \dots, c_k)$ with $c_i := c|_{V(G_i)}$ ($i = 1, \dots, k$). Every mapping c_i is then a valid vertex coloring of G_i (for $i = 1, \dots, k$), and this mapping is a bijection from the set of all vertex colorings of G to the set of all vectors of vertex colorings of the G_i . □

Theorem 58 *A graph G is a tree if and only if $p_G(t) = t(t-1)^{n-1}$ holds.*

Proof: “ $\Rightarrow$ ”: Let G be a tree. We prove the claim by induction on the number of vertices. For $n = 1$, there are exactly t ways to color G with colors from $\{1, \dots, t\}$. So $n > 1$. Let v be a leaf in G . Then, by the induction hypothesis, there are exactly $t(t-1)^{n-2}$ colorings of $G - v$. However, for each of these colorings, there are exactly $t-1$ colorings of G , since for v the $t-1$ colors remain that were not used on the neighbor of v . Thus, there are in total $t(t-1)^{n-1}$ colorings.

“ $\Leftarrow$ ”: Let G be a graph with n vertices and the chromatic polynomial $p_G(t) = t(t-1)^{n-1}$. In p_G the coefficient of the linear term is $(-1)^{n-1}$, so G is connected by Theorem 56(g). Furthermore, the coefficient of t^{n-1} is $-(n-1)$, so G must have exactly $n-1$ edges and is therefore a tree. $\square$

A surprising property of chromatic polynomials has been discovered by Stanley [1973].

Theorem 59 (Stanley [1973]) *For a graph G , let $\sigma(G)$ be the number of ways to orient its edges such that no directed cycle is formed. Then $\sigma(G) = (-1)^n p_G(-1)$.*

Proof: We prove $\sigma(G) = (-1)^n p_G(-1)$ (with $n = |V(G)|$) by induction on the number of edges. If G has no edges, then $\sigma(G) = 1$ and $p_G(t) = t^n$, so $(-1)^n p_G(-1) = (-1)^{2n} = 1$.

Otherwise, let $e = \{v, w\}$ be an edge of G . Then $\sigma(G) = \sigma(G \setminus e) + \sigma(G/e)$, because: Every acyclic orientation of $G \setminus e$ can be extended to at least one acyclic orientation of G , and precisely those acyclic orientations of $G \setminus e$ that also induce an acyclic orientation in G/e can be extended in two ways to an acyclic orientation of G .

Thus,

$$\begin{aligned} \sigma(G) &= \sigma(G \setminus e) + \sigma(G/e) = (-1)^n p_{G \setminus e}(-1) + (-1)^{n-1} p_{G/e}(-1) \\ &= (-1)^n p_{G \setminus e}(-1) - (-1)^n p_{G/e}(-1) = (-1)^n p_G(-1). \end{aligned}$$

$\square$

Theorem 60 *A graph G with $n \geq 3$ vertices is isomorphic to C_n if and only if $p_G(t) = (t-1)^n + (-1)^n(t-1)$.*

Proof: “ $\Rightarrow$ ”: We will prove the statement by induction on n . For $n = 3$, $p_{C_3} = t(t-1)(t-2)$, which is the same as $(t-1)^3 - (t-1)$.

So let $n > 3$. For every edge $e \in E(C_n)$, we have $p_{C_n}(t) = p_{C_n-e}(t) - p_{C_{n-1}}(t) = t(t-1)^{n-1} - ((t-1)^{n-1} + (-1)^{n-1}(t-1)) = (t-1)^n + (-1)^n(t-1)$, since $C_n - e$ is a tree.

“ $\Leftarrow$ ”: If $p_G(t) = (t-1)^n + (-1)^n(t-1)$ holds, then G must have n vertices and n edges. Furthermore, G must be connected, since all these properties are determined by the chromatic polynomial according to Theorem 56 and C_n has these properties.

Thus, G contains exactly one cycle. If l is the length of the cycle, there are $2^n - 2 \cdot 2^{n-l}$ ways to orient G acyclically (since there are $2 \cdot 2^{n-l}$ ways to orient the edges on the cycle in the same direction and all other edges arbitrarily). According to Theorem 59, this number must be equal to $(-1)^n ((-2)^n + (-1)^n(-2)) = 2^n - 2$. Thus, $l = n$ must hold, and the graph is therefore isomorphic to C_n . $\square$

Theorem 58 shows in particular that there are different graphs with the same chromatic polynomial, while the previous theorem shows that cycles are chromatically unique. For further

families of chromatically unique graphs, see Chao and Whitehead [1979].

5.3 List-Colorings

Definition 23 Let G be a graph. Assume that for every vertex $v \in V(G)$ we are given a set C_v (the **color-list** of v). A (feasible) **vertex-list-coloring** is a mapping $c : V(G) \rightarrow \cup_{v \in V(G)} C_v$ such that $c(v) \in C_v$ for every vertex $v \in V(G)$ and $c(v) \neq c(w)$ for every edge $\{v, w\} \in E(G)$. The **list-chromatic number** $\chi_l(G)$ of G is the smallest number k such that for any choice of color-lists of length at least k , a vertex-list-coloring exists.

Observation: For every graph G we have $\chi(G) \leq \chi_l(G)$.

Proposition 61 For $k \in \mathbb{N} \setminus \{0\}$ we have $\chi_l(K_{k,k^k}) > k$.

Proof: Let $V(K_{k,k^k}) = A_k \dot{\cup} B_k$ with $|A_k| = k$, $|B_k| = k^k$ and $E(K_{k,k^k}) = \{\{a, b\} \mid a \in A_k, b \in B_k\}$. We choose all colors for the lists C_v (for $v \in V(G)$) from a set $\{1, \dots, k^2\}$. Let $A_k = \{a_1, \dots, a_k\}$. Set $C_{a_i} = \{(i-1)k+1, (i-1)k+2, \dots, (i-1)k+k\}$ (for $i \in \{1, \dots, k\}$). Thus, the sets C_{a_i} are pairwise disjoint. Choose a bijection

$$\phi : \{1, \dots, k^k\} \rightarrow \left\{ X \subseteq \{1, \dots, k^2\} \mid |X| = k, |X \cap C_{a_i}| = 1 \text{ for all } i \in \{1, \dots, k\} \right\}.$$

With $B_k = \{b_1, \dots, b_{k^k}\}$ we set $C_{b_j} = \phi(j)$ ($j \in \{1, \dots, k^k\}$). If we color each vertex $a_i \in A_k$ with a color $c_i \in C_{a_i}$ ($i \in \{1, \dots, k\}$), then for b_j with $\phi(j) = \{c_1, \dots, c_k\}$ there is no color left. Hence there is no vertex-list-coloring of K_{k,k^k} for these color lists and therefore $\chi_l(K_{k,k^k}) > k$. $\square$

Note that $\chi(K_{k,k^k}) = 2$, so the above proposition yields an example of a graph where the list-chromatic number is much larger than the chromatic number.

Proposition 62 For every graph G , we have:

$$\chi_l(G) \leq \Delta(G) + 1.$$

Proof: Such a coloring can be found using the same greedy procedure as in the proof of Proposition 47. $\square$

Remark: Vizing [1976] and (independently) Erdős, Rubin and Taylor [1979] showed that Brooks' theorem (Theorem 48) also applies to list colorings, i.e., for a connected graph G that

is neither a cycle of odd length nor a complete graph, we have $\chi_l(G) \leq \Delta(G)$. We will not prove this result here.

Theorem 63 (Thomassen [1994]) *For every planar graph G we have $\chi_l(G) \leq 5$.*

Proof: We can assume that G is connected and that there is a planar embedding of G such that all boundaries of regions are cycles and that for all regions with the possible exception of the unbounded region these cycles have length 3 (we call such graphs *nearly triangulated*). If these conditions are not met we can add edges until they are met (and adding edges can only increase the list chromatic number).

We show the theorem by proving the following statement by induction on the number of vertices:

Let G be a nearly triangulated planar graph with fixed planar embedding. Let B be the cycle on the boundary of the unbounded region. We are given color lists C_v ($v \in V(G)$) with the following properties:

- *There are two vertices x and y that are neighbors on B and two different colors α and β such that $C_x = \{\alpha\}$ and $C_y = \{\beta\}$.*
- *For all other vertices v on B we have $|C_v| \geq 3$.*
- *For the vertices v not contained in B we have $|C_v| \geq 5$.*

Then, there is a list coloring of G for these color lists.

We apply induction on the number of vertices. First, assume $|V(G)| = 3$. Then the statement is valid because apart from x and y there is only one vertex v in G , and for this vertex we have $|C_v| \geq 3$, so the color list C_v of v contains a color that is different from α and β .

For $|V(G)| > 3$ we distinguish two cases:

Case 1: G contains an edge that is a chord of B , i.e. an edge connecting two vertices u and v on B such that u and v are not adjacent on B .

Then, B contains two different u - v -paths B_1 and B_2 . For $i \in \{1, 2\}$ let G_i be the subgraph of G that is bounded by the embedding of B_i and $\{u, v\}$. Thus, G_1 and G_2 have exactly u and v as common vertices. W.l.o.g. we can assume that B_1 contains the vertices x and y . Now we apply the induction hypothesis to G_1 and get a list coloring of G_1 . Then, in particular, u and v have been colored. G_2 (with the color lists of u and v reduced to one element each) fulfills all conditions of the statement and we have $|V(G_2)| < |V(G)|$. Hence we can also apply the induction hypothesis to G_2 and extend the list coloring of G_1 to a list coloring of G .

Case 2: G does not contain a chord of B .

Let v be the neighbor of x on B that is different from y . Let w be the neighbor of v on B that is different from x . Thus B contains the edges $\{w, v\}$, $\{v, x\}$, and $\{x, y\}$ ($w = y$ is possible).

Let X be the set of neighbors of v . Since G is nearly triangulated, the graph $G' := G - v$ is nearly triangulated, too. As $|C_v| \geq 3$, the set C_v contains at least two colors γ and δ that are different from α . Now, for each vertex $z \in X \setminus \{w, x\}$, remove the colors γ and δ from the color list C_z . Since all elements of $X \setminus \{w, x\}$ are on the outer boundary of G' but not on the outer boundary of G (otherwise G would contain a chord of B), G' meets all conditions of the statement that we want to prove. We can apply the induction hypothesis to G' and get a list coloring of G' where, among the vertices in X , at most w is colored with one of the colors γ or δ . Thus we can extend this coloring to a list coloring of G by assigning to v one of the colors γ and δ that has not been used for w . $\square$

Remark: This bound on the list-chromatic number of planar graphs G is best possible since there are planar graphs G with $\chi_l(G) = 5$ (see the exercises).

Thomassen [2003] showed (with an approach similar to the one in the proof above) that $\chi_l(G) \leq 3$ holds for any planar graph G with girth at least 5.

5.4 Edge Colorings

Definition 24 Let G be a graph. A (feasible) **k -edge coloring** of G is a mapping $c : E(G) \rightarrow \{1, \dots, k\}$ such that $c(e_1) \neq c(e_2)$ for every two edges $e_1, e_2 \in E(G)$ with $e_1 \cap e_2 \neq \emptyset$. If there is a feasible k -edge coloring then G is called **k -edge-colorable**. The sets $\{e \in E(G) \mid c(e) = i\}$ are called **color classes** of the edge coloring c ($i = 1, \dots, k$). The **chromatic index** (also called edge-chromatic number) $\chi'(G)$ of G is the smallest number k such that G is k -edge-colorable.

An edge coloring of a graph G can be seen as a vertex coloring of the line graph L_G of G with $V(L_G) = E(G)$ and $E(L_G) = \{\{e, e'\} \subset E(G) \mid e \cap e' \neq \emptyset\}$. This way, all results concerning vertex colorings can be translated to edge colorings. However, for the chromatic index, very good upper and lower bounds are known, which are shown in the next theorem.

Theorem 64 (Vizing's Theorem)(Vizing [1964]) For every graph G we have $\Delta(G) \leq \chi'(G) \leq \Delta(G) + 1$.

Proof: The inequality $\Delta(G) \leq \chi'(G)$ is trivial.

We prove $\chi'(G) \leq \Delta(G) + 1$ by induction on the number of edges. The statement is trivial if $E(G) = \emptyset$. So let $E(G) \neq \emptyset$, and let $e = \{x, y\}$ be an edge of G . By induction hypothesis, there is an edge coloring c of $G - e$ with $\Delta(G) + 1$ colors. Now choose for each vertex $v \in V(G)$ a color $\lambda(v) \in \{1, \dots, \Delta(G) + 1\}$ that is missing at v , i.e. a color with $\lambda(v) \notin \{c(e') \mid e' \in \delta_{G-e}(v)\}$.

Determine a maximal sequence $y_0, \dots, y_t$ of distinct neighbors of x with the following properties:

- $y_0 = y$.
- $\lambda(y_{i-1}) = c(\{x, y_i\})$ ($i = 1, \dots, t$).
- If there is a neighbor z of x with $\lambda(y_t) = c(\{x, z\})$ then $z \in \{y_0, \dots, y_t\}$.

Case 1: There is no neighbor z of x with $\lambda(y_t) = c(\{x, z\})$. The edge coloring c' arises from c as follows: Set $c'(\{x, y_{i-1}\}) := c(\{x, y_i\})$ ($i = 1, \dots, t$) and $c'(\{x, y_t\}) = \lambda(y_t)$.

Case 2: There is an $s \in \{1, \dots, t-1\}$ with $\lambda(y_t) = c(\{x, y_s\})$. Let $H := (V(G), \{e \in E(G) \mid c(e) \in \{\lambda(x), \lambda(y_t)\}\})$. Then we have $\Delta(H) \leq 2$, and y_t has degree at most 1 in H . Consider in H a maximal (i.e. by inclusion) path P that starts in y_t .

We distinguish three subcases.

Subcase 2.1: P ends in y_{s-1} . Then the last edge of P has the color $\lambda(x)$, since the color $\lambda(y_t) = c(\{x, y_s\}) = \lambda(y_{s-1})$ is missing at y_{s-1} . c' arises from c as follows: Swap $\lambda(x)$ and $\lambda(y_t)$ on P , and set $c'(\{x, y_{i-1}\}) := c(\{x, y_i\})$ ($i = 1, \dots, s-1$) and $c'(\{x, y_{s-1}\}) := \lambda(x)$.

Subcase 2.2: P ends in x . Then $\{y_s, x\}$ is the last edge in P , since $\lambda(x)$ is missing at x and $\{y_s, x\}$ is the only edge incident to x with color $\lambda(y_t)$. c' arises from c by swapping $\lambda(y_t)$ and $\lambda(x)$ on P and $c'(\{x, y_{i-1}\}) := c(\{x, y_i\})$ ($i = 1, \dots, s$).

Subcase 2.3: P ends neither in x nor in y_{s-1} . Then we get c' from c as follows: Swap $\lambda(x)$ and $\lambda(y_t)$ on P , and set $c'(\{x, y_{i-1}\}) := c(\{x, y_i\})$ ($i = 1, \dots, t$) and $c'(\{x, y_t\}) := \lambda(x)$.

In all cases, it is easy to check that c' is indeed a feasible edge coloring of G . $\square$

Graphs G with $\chi'(G) = \Delta(G)$ are called **graphs of class 1**, and graphs G with $\chi'(G) = \Delta(G) + 1$ are called **graphs of class 2**. In the following, we determine the classes of some groups of graphs.

Theorem 65 (*Kőnig's Theorem*) (*Kőnig [1916]*) *For every bipartite graph G we have $\chi'(G) = \Delta(G)$.*

Proof: We prove the statement by induction on $m = |E(G)|$. For $m = 0$, the statement is trivial.

Thus, let $m > 0$ and let $e = \{v, w\} \in E(G)$ be an edge. By induction hypothesis, $G - e$ has an edge coloring $c : E(G) \setminus \{e\} \rightarrow \{1, \dots, \Delta(G)\}$. In $G - e$ the vertices v and w have at most $\Delta(G) - 1$ neighbors, so there are numbers $\lambda(v), \lambda(w) \in \{1, \dots, \Delta(G)\}$ such that $\lambda(v) \neq c(e')$ for all edges $e' \in (\delta_G(v) \setminus \{e\})$ and $\lambda(w) \neq c(e')$ for all edges $e' \in (\delta_G(w) \setminus \{e\})$. If $\lambda(v) = \lambda(w)$, we can color $\{v, w\}$ with the color $\lambda(v)$ and are done. Hence assume $\lambda(v) \neq \lambda(w)$. Consider the subgraph $H = (V(G), \{e' \in E(G) \mid c(e') \in \{\lambda(v), \lambda(w)\}\})$. All vertices in H have degree at most 2, and v has degree at most 1. Consider a longest path P in H starting in v . The edges of the path are alternately colored with $\lambda(w)$ and $\lambda(v)$. The path P cannot end in w , because

in that case its last edge was an $\lambda(v)$ -edge and P together with the edge $\{v, w\}$ would be a cycle of odd length (in contradiction to the assumption that G is bipartite). Hence, we can swap the colors $\lambda(v)$ and $\lambda(w)$ on P and color the edge $\{v, w\}$ with the color $\lambda(w)$. $\square$

Proposition 66 *For $n > 1$ we have $\chi'(K_n) = 2\lfloor \frac{n+1}{2} \rfloor - 1 = \begin{cases} n & : n \text{ odd} \\ n-1 & : n \text{ even} \end{cases}$.*

Proof: Let $n > 1$. We have $\Delta(K_n) = n - 1$, so (by Theorem 64) $\chi'(K_n) \in \{n - 1, n\}$.

Let n be odd. Every color class of an edge coloring of K_n can have at most $\frac{n-1}{2}$ edges. Thus, $\chi'(K_n) \geq \binom{n}{2} \frac{2}{n-1} = \frac{n(n-1)}{2} \frac{2}{n-1} = n$ and hence $\chi'(K_n) = n$.

In an edge coloring c of K_n with n colors, every color class must have exactly $\frac{n-1}{2}$ elements, and for each node $v \in V(K_n)$ there is a color $\lambda(v) \in \{1, \dots, n\}$ with $\lambda(v) \notin \{c(e) \mid e \in \delta_{K_n}(v)\}$. And we have $\lambda(v) \neq \lambda(w)$ for each two different nodes v and w .

Now let n be even. We have to show that there is an edge coloring with $n - 1$ colors. Remove a node v from K_n . The resulting graph K_{n-1} has an odd number of nodes, so it has an edge coloring with $n - 1$ colors. Now color for each $w \in V(K_{n-1})$ the edge $\{v, w\}$ with the color $\lambda(w)$ missing at w . This gives a coloring of K_n with $n - 1$ colors. $\square$

Corollary 67 *Let G be a connected graph. If $|V(G)| = 1$ or G is a complete graph with even number of nodes then $\chi(G) = \chi'(G) + 1$. In all other cases, we have $\chi(G) \leq \chi'(G)$.*

Proof: The first part follows directly from the previous proposition. If G is a cycle of odd length or a complete graph with odd number of nodes then $\chi(G) = \Delta(G) + 1 = \chi'(G)$. If G is neither an odd cycle nor a complete graph then Brooks' Theorem (Theorem 48) together with Vizing's Theorem (Theorem 64) imply $\chi(G) \leq \Delta(G) \leq \chi'(G)$. $\square$

Lemma 68 *Let G be a graph with n nodes and $m > \Delta(G)\lfloor \frac{n}{2} \rfloor$ edges. Then $\chi'(G) = \Delta(G) + 1$.*

Proof: Every color class of an edge coloring can have at most $\lfloor \frac{n}{2} \rfloor$ elements, so $\chi'(G) \geq \frac{m}{\lfloor \frac{n}{2} \rfloor} > \Delta(G)$, and therefore $\chi'(G) = \Delta(G) + 1$. $\square$

Notation: Let G be a graph. For $k \in \mathbb{N}$, we call G **k -regular** if all vertices in G are of degree k . It is called **regular** if there is a $k \in \mathbb{N}$ such that it is k -regular.

Corollary 69 *Let G be a regular graph with odd number of nodes. Then, we have:*

(a) $\chi'(G) = \Delta(G) + 1$.

(b) *If H arises from G by deleting at most $\frac{\Delta(G)}{2} - 1$ edges, we have $\chi'(H) = \Delta(H) + 1$.*

Proof: We have $|E(G)| \geq |E(H)| \geq \frac{\Delta(G)}{2}n - \frac{\Delta(G)}{2} + 1 > \Delta(G)\frac{n-1}{2} = \Delta(G)\lfloor \frac{n}{2} \rfloor$. Thus, G and H satisfy the condition of Lemma 68. $\square$

Notation: For a graph G , we call an edge $e \in E(G)$ a **bridge** if $G - e$ contains more connected components than G .

Theorem 70 *Let G be a 3-regular planar graph without bridges. Then $\chi'(G) = 3$.*

Proof: Since $\chi'(G) \geq 3$ is trivial, we only have to show $\chi'(G) \leq 3$.

W.l.o.g. we can assume that G is connected (otherwise consider the connected components of G).

Consider a fixed planar embedding of G . The Four Color Theorem implies that we can color the faces of the embedding with four colors such that neighboring faces get different colors. Since G does not contain a bridge, every edge is on the boundary of exactly two faces. For an edge e let C_e be the set of the (two) colors of the faces that are bounded by e . Then we set

$$c(e) := \begin{cases} 1 & : C_e = \{1, 2\} \text{ or } C_e = \{3, 4\} \\ 2 & : C_e = \{1, 3\} \text{ or } C_e = \{2, 4\} \\ 3 & : C_e = \{1, 4\} \text{ or } C_e = \{2, 3\} \end{cases}$$

Every vertex touches exactly three faces, so by this assignment no two edges that are incident to the same vertex can get the same color. $\square$

We applied the Four Color Theorem to prove the previous theorem. On the other hand, the Four Color Theorem can be proven easily by using the previous theorem. First of all, observe that for proving the Four Color Theorem it is sufficient to prove that for any planar embedding of a planar graph G the faces of the embedding can be colored with four colors such that neighboring faces get different colors. Moreover we can assume that G is connected, does not contain any bridges and is 3-regular. By the previous theorem such a graph has a feasible edge coloring $c : E(G) \rightarrow \{1, 2, 3\}$. In order to color the faces of a planar embedding of G with four colors, it is sufficient to assign to each face A of the embedding of G an ordered pair (α_A, β_A) with $\alpha_A, \beta_A \in \{1, 2\}$ such that for each two neighboring faces A and B we have $(\alpha_A, \beta_A) \neq (\alpha_B, \beta_B)$. The numbers α_A and β_A can be found in the following way. For $i, j \in \{1, 2, 3\}$, let $H_{i,j} := (V(G), \{e \in E(G) \mid c(e) \in \{i, j\}\})$. For every two colors i and j from $\{1, 2, 3\}$, the graph $H_{i,j}$ is a 2-regular graph for which we are given a planar embedding by the planar embedding of G . Obviously, there is a feasible coloring $\tilde{c}_{i,j}$ of the faces of the

planar embedding of $H_{i,j}$ with two colors. Any face A of the embedding of G is contained in exactly one face $A_{1,2}$ of the embedding of $H_{1,2}$ and in one face $A_{1,3}$ of the embedding of $H_{1,3}$ (see Fig. 2). We set $\alpha_A := \tilde{c}_{1,2}(A_{1,2})$ and $\beta_A := \tilde{c}_{1,3}(A_{1,3})$. It is easy to check that the pairs (α_A, β_A) have the desired properties.

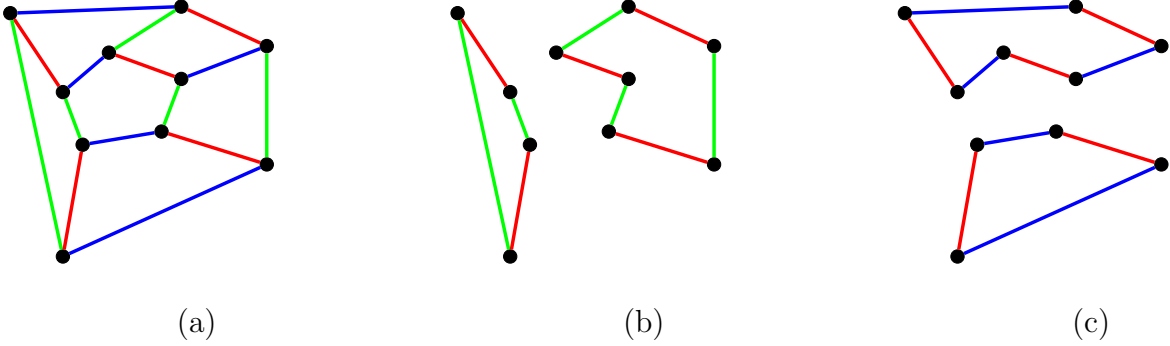


Figure 2: A 3-regular planar graph with a 3-edge coloring (a). Pictures (b) and (c) show the graphs $H_{1,2}$ and $H_{1,3}$ where color red means “1”, color green means “2” and color blue means “3”.

Remark: The equivalence of the Four Color Theorem and Theorem 70 was known before the Four Color Theorem has been proved.

We can also define the *list-chromatic index* $\chi'_l(G)$ of a graph G , which is the list-chromatic number of the line graph of G . Obviously, for any graph we have $\chi'(G) \leq \chi'_l(G)$. It is an open question whether there are graphs G with $\chi'(G) < \chi'_l(G)$. The *list-chromatic conjecture* says that we have $\chi'(G) = \chi'_l(G)$ for all graphs, but so far it has been proved only for special classes of graphs. For example, Galvin [1995] proved the list-chromatic conjecture for bipartite graphs.

III Matroids

This part is mainly based on Chapter 13 of Korte and Vygen [2018], with some contributions from Schrijver [2003]. Other recommendable introductions to matroid theory are the books by Oxley [1992] and Welsh [1976].

6 Matroids

6.1 Independence Systems and Matroids

Matroids describe families of sets that generalize, among others, the following families of sets:

- linearly independent vectors in a vector space,
- edge sets of forests in graphs.

The name matroid (which is due to H. Whitney) is derived from the vector sets, which can be considered as columns in a matrix. Thus matroids are “matrix-like” structures.

Definition 25 A **set system** is a pair $(E, \mathcal{F})$ where E is a nonempty finite set and $\mathcal{F}$ is a family of subsets of E . It is called **independence system** if the following two conditions are satisfied:

(M1) $\emptyset \in \mathcal{F}$,

(M2) If $X \subseteq Y$ and $Y \in \mathcal{F}$ then $X \in \mathcal{F}$.

The elements of $\mathcal{F}$ are called **independent**, the elements of $2^E \setminus \mathcal{F}$ are called **dependent**. Minimal dependent sets are called **circuits**, maximal independent sets are called **bases**. For $X \subseteq E$, the maximal independent subsets of X are called **bases of X** .

Definition 26 Let $(E, \mathcal{F})$ be an independence system. For $X \subseteq E$, we define the **rank of X** by $r(X) = \max\{|Y| \mid Y \subseteq X, Y \in \mathcal{F}\}$. Moreover, we define the **closure of X** by $\sigma(X) = \{y \in E \mid r(X \cup \{y\}) = r(X)\}$.

We mainly consider two kinds of optimization problems on independence systems.

MAXIMIZATION PROBLEM FOR INDEPENDENCE SYSTEMS

Instance: An independence system $(E, \mathcal{F})$ and $c : E \rightarrow \mathbb{R}$.

Task: Find an $X \in \mathcal{F}$ such that $c(X) := \sum_{e \in X} c(e)$ is maximum.

MINIMIZATION PROBLEM FOR INDEPENDENCE SYSTEMS

Instance: An independence system $(E, \mathcal{F})$ and $c : E \rightarrow \mathbb{R}$.

Task: Find a basis B such that $c(B)$ is minimum.

Note that in both cases the weights of the elements can be arbitrary real numbers. But if all weights are positive then in the maximization problem all optimum solutions will be bases while in the minimization problem we have to enforce that we get a basis as otherwise we would simply get the empty set as an optimum solution.

For both problems the instances are typically not complete lists of all elements of $\mathcal{F}$. Instead we specify the independence systems e.g. by an oracle that decides, given a set $X \subset E$, if $X \in \mathcal{F}$.

Examples:

MAXIMUM WEIGHT STABLE SET PROBLEM

Instance: A graph G and weights $c : V(G) \rightarrow \mathbb{R}$.

Task: Find a stable set of maximum weight.

Here $E = V(G)$ and $\mathcal{F} = \{F \subseteq E \mid F \text{ is stable in } G\}$.

SHORTEST PATH PROBLEM

Instance: A graph G , weights $c : E(G) \rightarrow \mathbb{R}$ and $s, t \in V(G)$ such that t is reachable from s .

Task: Find a shortest s - t -path in G with respect to c .

Here $E = E(G)$ and $\mathcal{F} = \{F \subseteq E \mid F \text{ is a subset of the edge set of an } s\text{-}t\text{-path in } G\}$.

MINIMUM SPANNING TREE PROBLEM

Instance: A connected graph G and weights $c : E(G) \rightarrow \mathbb{R}$.

Task: Find a spanning tree in G of minimum weight.

Here $E = E(G)$ and $\mathcal{F} = \{F \subseteq E \mid (V(G), F) \text{ is a forest}\}$.

MAXIMUM-WEIGHT FOREST PROBLEM

Instance: A graph G and weights $c : E(G) \rightarrow \mathbb{R}$.

Task: Find a forest in G of maximum weight.

Here (as in the MINIMUM SPANNING TREE PROBLEM), $E = E(G)$ and $\mathcal{F} = \{F \subseteq E \mid (V(G), F) \text{ is a forest}\}$.

MAXIMUM-WEIGHT MATCHING PROBLEM

Instance: A graph G and weights $c : E(G) \rightarrow \mathbb{R}$.

Task: Find a matching in G of maximum weight.

Here $E = E(G)$ and $\mathcal{F} = \{F \subseteq E \mid F \text{ is a matching in } G\}$.

Definition 27 *An independence system is a **matroid** if the following condition holds:*

(M3) *If $X, Y \in \mathcal{F}$ and $|X| > |Y|$ then there is an $x \in X \setminus Y$ with $Y \cup \{x\} \in \mathcal{F}$.*

Proposition 71 *The following independence systems $(E, \mathcal{F})$ are matroids.*

(a) *E is the set of columns of a matrix A over some field K , and*

$$\mathcal{F} = \{F \subseteq E \mid \text{the columns in } F \text{ are linearly independent over } K\}$$

(b) *E is the set of edges of some graph G , and*

$$\mathcal{F} = \{F \subseteq E \mid (V(G), F) \text{ is a forest}\}$$

(c) *E is a finite set, $k \in \mathbb{N}$, and*

$$\mathcal{F} = \{F \subseteq E \mid |F| \leq k\}$$

(d) *E is the set of edges of some graph G , S is a stable set in G , $k_s \in \mathbb{N}$ (for $s \in S$), and*

$$\mathcal{F} = \{F \subseteq E \mid |\delta_F(s)| \leq k_s \text{ for } s \in S\}$$

(e) *E is the set of edges of some directed graph G , $S \subseteq V(G)$, $k_s \in \mathbb{N}$ (for $s \in S$), and*

$$\mathcal{F} = \{F \subseteq E \mid |\delta_F^-(s)| \leq k_s \text{ for } s \in S\}$$

Proof: In all cases, it is obvious that $(E, \mathcal{F})$ is an independence system. We show that (M3) holds.

(a) This is a well-known fact from linear algebra. The proof can be found in any linear algebra textbook.

- (b) Let $X, Y \in \mathcal{F}$ with $|X| > |Y|$. Then $(V(G), X)$ contains $|V(G)| - |X|$ connected components and $(V(G), Y)$ contains $|V(G)| - |Y|$ connected components. Thus, there must be a connected component C of $(V(G), X)$ that is not completely contained in any connected component of $(V(G), Y)$. Hence, $G[C]$ must contain an edge e with end nodes in different connected components of $(V(G), Y)$. This implies that $(V(G), Y \cup \{e\})$ is also a forest, so $Y \cup \{e\} \in \mathcal{F}$.
- (c) Here, (M3) holds trivially.
- (d) Let $X, Y \in \mathcal{F}$ with $|X| > |Y|$. Let $S' := \{s \in S \mid |\delta_Y(s)| = k_s\}$. As $|X| > |Y|$ and $|\delta_X(s)| \leq k_s$ for all $s \in S'$, there is an $e \in X \setminus Y$ with $e \notin \delta(s)$ for all $s \in S'$. Thus, $Y \cup \{e\} \in \mathcal{F}$.
- (e) The proof is identical to (d) except for replacing δ by δ^- . □

Notation: Some of the matroids in the previous proposition have special names:

- (a) The matroid in (a) is called **vector matroid** of A . If for a matroid $(E, \mathcal{F})$ a matrix A over a field K exists such that $(E, \mathcal{F})$ is the vector matroid of A then $(E, \mathcal{F})$ is called **representable over K** .
- (b) The matroid in (b) is called **cycle matroid** of G . A matroid that is the cycle matroid of some graph (possibly with loops) is called **graphic matroid**.
- (c) These matroids are called **uniform matroids**.

Note that representable matroids formally are just isomorphic to a vector matroid, where two matroids $(E, \mathcal{F})$ and $(\tilde{E}, \tilde{\mathcal{F}})$ are isomorphic if there is a bijection $\phi : E \rightarrow \tilde{E}$ such that for any $X \subseteq E$ the set X is independent if and only if $\{\phi(x) \mid x \in X\}$ is independent. An analogous statement holds for graphic matroids.

Theorem 72 *Let $(E, \mathcal{F})$ be an independence system. Then the following statements are equivalent:*

- (M3) *If $X, Y \in \mathcal{F}$ and $|X| > |Y|$ then there is an $x \in X \setminus Y$ with $Y \cup \{x\} \in \mathcal{F}$.*
- (M3') *If $X, Y \in \mathcal{F}$ and $|X| = |Y| + 1$ then there is an $x \in X \setminus Y$ with $Y \cup \{x\} \in \mathcal{F}$.*
- (M3'') *For each $X \subseteq E$, all bases of X have the same cardinality.*

Proof: (M3) $\Leftrightarrow$ (M3'): trivial.

(M3) $\Rightarrow$ (M3''): also trivial.

(M3'') $\Rightarrow$ (M3): Let $X, Y \in \mathcal{F}$ with $|X| > |Y|$. By (M3''), Y cannot be a basis of $X \cup Y$. Thus, there is an $x \in (X \cup Y) \setminus Y = X \setminus Y$ such that $Y \cup \{x\} \in \mathcal{F}$. □

Definition 28 Let $(E, \mathcal{F})$ be an independence system. For $X \subseteq E$, we define the **lower rank** by

$$\rho(X) := \min\{|Y| \mid Y \text{ is a basis of } X\}.$$

The **rank quotient** of $(E, \mathcal{F})$ is defined by

$$q(E, \mathcal{F}) := \min_{F \subseteq E} \frac{\rho(F)}{r(F)}$$

where we set $\frac{0}{0} := 1$.

Proposition 73 Let $(E, \mathcal{F})$ be an independence system. Then $q(E, \mathcal{F}) \leq 1$. Moreover, $(E, \mathcal{F})$ is a matroid if and only if $q(E, \mathcal{F}) = 1$.

Proof: The inequality $q(E, \mathcal{F}) \leq 1$ holds by definition for any independence system. And $q(E, \mathcal{F}) = 1$ is equivalent to (M3"). $\square$

Theorem 74 Let $(E, \mathcal{F})$ be an independence system. If for any $A \in \mathcal{F}$ and $e \in E$, the set $A \cup \{e\}$ contains at most p circuits (with $p \geq 1$) then $q(E, \mathcal{F}) \geq \frac{1}{p}$.

Proof: Let $F \subseteq E$ and let J, K be two bases of F . We show $\frac{|J|}{|K|} \geq \frac{1}{p}$. Let $J \setminus K = \{e_1, \dots, e_t\}$. We construct a sequence $K = K_0, K_1, \dots, K_t$ of independent subsets of $J \cup K$ such that for $i \in \{1, \dots, t\}$ we have

- (a) $J \cap K \subseteq K_i$,
- (b) $K_i \cap \{e_1, \dots, e_t\} = \{e_1, \dots, e_i\}$, and
- (c) $|K_{i-1} \setminus K_i| \leq p$.

Assume that we have already constructed the sets $K_0, K_1, \dots, K_i$. Since $K_i \cup \{e_{i+1}\}$ contains at most p circuits and each such circuit has a non-empty intersection with $K_i \setminus J$ (because J is independent), there is a set $X \subseteq K_i \setminus J$ such that $|X| \leq p$ and $(K_i \setminus X) \cup \{e_{i+1}\} \in \mathcal{F}$. We set $K_{i+1} := (K_i \setminus X) \cup \{e_{i+1}\}$. It is easy to see that the sequence $K_0, K_1, \dots, K_t$ that we get by this definition satisfies the conditions (a), (b), and (c) above.

We have $J = (J \cap K) \cup \{e_1, \dots, e_t\} \subseteq K_t \in \mathcal{F}$. Since J is a basis of F , this implies $J = K_t$. We conclude that

$$|K \setminus J| = \sum_{i=1}^t |K_{i-1} \setminus K_i| \leq pt = p|J \setminus K|.$$

This implies $|K| = |K \cap J| + |K \setminus J| \leq |K \cap J| + p|J \setminus K| \leq p|J|$. $\square$

Theorem 75 *Let E be a finite nonempty set and $\mathcal{B} \subseteq 2^E$. $\mathcal{B}$ is the set of bases of some matroid $(E, \mathcal{F})$ if and only if*

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

(B2) For any $B_1, B_2 \in \mathcal{B}$ and $x \in B_1 \setminus B_2$ there is a $y \in B_2 \setminus B_1$ with $(B_1 \setminus \{x\}) \cup \{y\} \in \mathcal{B}$.

Proof: “ $\Rightarrow$ ”: Let $\mathcal{B}$ be the set of bases of some matroid $(E, \mathcal{F})$. Then, (B1) is satisfied because by (M1) we have $\mathcal{F} \neq \emptyset$. To prove (B2), let $B_1, B_2 \in \mathcal{B}$ and $x \in B_1 \setminus B_2$. Then $B_1 \setminus \{x\}$ is independent. Since $|B_2| > |B_1 \setminus \{x\}|$, (M3) implies that there is some $y \in B_2 \setminus B_1$ such that $(B_1 \setminus \{x\}) \cup \{y\}$ is independent. It is, in fact, a basis since all bases have the same cardinality.

“ $\Leftarrow$ ”: Let $\mathcal{B} \subseteq 2^E$ satisfy (B1) and (B2).

Claim 1: All elements of $\mathcal{B}$ have the same cardinality.

Proof of Claim 1: Suppose that there are $B_1, B_2 \in \mathcal{B}$ with $|B_1| > |B_2|$. Choose B_1 and B_2 with these properties such that $|B_1 \cap B_2|$ is maximum. Let $x \in B_1 \setminus B_2$. By (B2) there is a $y \in B_2 \setminus B_1$ with $B'_1 := (B_1 \setminus \{x\}) \cup \{y\} \in \mathcal{B}$. But then B'_1 and B_2 are elements of $\mathcal{B}$ with $|B'_1| > |B_2|$ and $|B'_1 \cap B_2| > |B_1 \cap B_2|$, which is a contradiction to the choice of $|B_1|$ and $|B_2|$. This proves the claim. $\square$ **Claim 1**

Now let

$$\mathcal{F} := \{F \subseteq E \mid \text{there is a } B \in \mathcal{B} \text{ with } F \subseteq B\}.$$

Then, $(E, \mathcal{F})$ is obviously an independence system, and $\mathcal{B}$ is the family of its bases. We have to show that $(E, \mathcal{F})$ satisfies (M3). Let $X, Y \in \mathcal{F}$ with $|X| > |Y|$. Let $X \subseteq B_1 \in \mathcal{B}$ and $Y \subseteq B_2 \in \mathcal{B}$, where B_1 and B_2 are chosen such that $|B_1 \cap B_2|$ is maximum

Claim 2: $B_2 \cap (X \setminus Y) \neq \emptyset$.

Proof of Claim 2: Suppose that $B_2 \cap (X \setminus Y) = \emptyset$. Then $B_1 \cap B_2$ and $X \setminus Y$ are disjoint subsets of B_1 . Thus, we get

$$|B_1 \cap B_2| + |Y \setminus B_1| + |(B_2 \setminus B_1) \setminus Y| = |B_2| = |B_1| \geq |B_1 \cap B_2| + |X \setminus Y|.$$

This implies

$$|(B_2 \setminus B_1) \setminus Y| \geq |X \setminus Y| - |Y \setminus B_1| \stackrel{|X| > |Y|}{>} |Y \setminus X| - |Y \setminus B_1| \geq 0,$$

so $(B_2 \setminus B_1) \setminus Y \neq \emptyset$. Let $y \in (B_2 \setminus B_1) \setminus Y$. By (B2), there is an $x \in B_1 \setminus B_2$ with $B'_2 := (B_2 \setminus \{y\}) \cup \{x\} \in \mathcal{B}$. Then $Y \subseteq B'_2$ and $|B_1 \cap B'_2| > |B_1 \cap B_2|$, which is a contradiction to the choice of B_1 and B_2 . $\square$ **Claim 2**

The claim implies (M3) since for any element $y \in B_2 \cap (X \setminus Y)$, we have $Y \cup \{y\} \subseteq B_2$, so $Y \cup \{y\} \in \mathcal{F}$. $\square$

Theorem 76 Let E be a finite nonempty set and $r : 2^E \rightarrow \mathbb{N}$. Then the following statements are equivalent:

(a) r is the rank function of a matroid $(E, \mathcal{F})$.

(b) For all $X, Y \subseteq E$:

$$(R1) \quad r(X) \leq |X|;$$

$$(R2) \quad \text{If } X \subseteq Y \text{ then } r(X) \leq r(Y);$$

$$(R3) \quad r(X \cup Y) + r(X \cap Y) \leq r(X) + r(Y).$$

(c) For all $X, Y \subseteq E$ and $x, y \in E$:

$$(R1') \quad r(\emptyset) \leq 0;$$

$$(R2') \quad r(X) \leq r(X \cup \{x\}) \leq r(X) + 1;$$

$$(R3') \quad \text{If } r(X \cup \{x\}) = r(X \cup \{y\}) = r(X) \text{ then } r(X \cup \{x, y\}) = r(X).$$

Proof: “(a) $\Rightarrow$ (b)”: If r is the rank function of an independence system then (R1) and (R2) obviously hold. Now, let r be the rank function of a matroid. Then we will show (R3). Let $X, Y \subseteq E$, and let A be a basis of $X \cap Y$. By (M3), the set A can be extended to a basis $A \dot{\cup} B$ of X and to a basis $(A \dot{\cup} B) \dot{\cup} C$ of $X \cup Y$. Thus, $A \cup C \subseteq Y$ and $A \cup C \in \mathcal{F}$, which implies $r(Y) \geq |A \cup C|$. Therefore:

$$r(X) + r(Y) \geq |A \cup B| + |A \cup C| = 2|A| + |B| + |C| = |A \cup B \cup C| + |A| = r(X \cup Y) + r(X \cap Y).$$

“(b) $\Rightarrow$ (c)”: Let $r : 2^E \rightarrow \mathbb{N}$ satisfy (R1) to (R3). We will show that r satisfies (R1') to (R3').

(R1') This follows directly from (R1).

(R2') The inequality $r(X) \leq r(X \cup \{y\})$ follows from (R2). And we have

$$r(X \cup \{y\}) \stackrel{(R3)}{\leq} r(X) + r(\{y\}) - r(X \cap \{y\}) \leq r(X) + r(\{y\}) \stackrel{(R1)}{\leq} r(X) + 1.$$

This implies (R2').

(R3') The condition is trivial for $x = y$. And for $x \neq y$, we have

$$2r(X) \stackrel{(R2)}{\leq} r(X) + r(X \cup \{x, y\}) \stackrel{(R3)}{\leq} r(X \cup \{x\}) + r(X \cup \{y\}).$$

Thus, if $r(X \cup \{x\}) = r(X \cup \{y\}) = r(X)$ then $r(X \cup \{x, y\}) = r(X)$, which shows (R3').

“(c) $\Rightarrow$ (a)”: Let $r : 2^E \rightarrow \mathbb{N}$ be a function satisfying (R1'), (R2'), and (R3'). Let

$$\mathcal{F} := \{F \subseteq E \mid r(F) = |F|\}.$$

Claim: $(E, \mathcal{F})$ is a matroid.

Proof of the claim: We show that $(E, \mathcal{F})$ satisfies (M1), (M2), and (M3').

(M1): (M1) follows directly from (R1').

(M2): (R1') and (R2') imply $r(X) \leq |X|$ for all $X \subseteq E$. If $Y \in \mathcal{F}$, $y \in Y$ and $X := Y \setminus \{y\}$, we have

$$|X| + 1 = |Y| = r(Y) = r(X \cup \{y\}) \stackrel{(R2')}{\leq} r(X) + 1 \leq |X| + 1,$$

so $X \in \mathcal{F}$. This implies (M2).

(M3'): Let $X, Y \in \mathcal{F}$ with $|X| = |Y| + 1$. Let $X \setminus Y = \{x_1, \dots, x_k\}$. Suppose that (M3') is violated, i.e. $r(Y \cup \{x_i\}) = |Y|$ for $i \in \{1, \dots, k\}$. Then by (R3'), we have $r(Y \cup \{x_1, x_i\}) = r(Y)$ for $i \in \{2, \dots, k\}$. Repeated application of this argument yields $r(Y) = r(Y \cup \{x_1, \dots, x_k\}) = r(X \cup Y) \geq r(X)$, a contradiction. This proves (M3') and the claim. $\square$ **Claim**

We will show that r is the rank function of the matroid $(E, \mathcal{F})$. Thus, we have to prove that

$$r(X) = \max\{|Y| \mid Y \subseteq X, r(Y) = |Y|\}$$

for all $X \subseteq E$. So let $X \subseteq E$ and Y a maximum subset of X with $r(Y) = |Y|$. For all $x \in X \setminus Y$, we have $r(Y \cup \{x\}) < |Y| + 1$, so by (R2'), we have $r(Y \cup \{x\}) = |Y|$. Repeated application of (R3') implies $r(X) = |Y|$. $\square$

Notation: A function $r : 2^E \rightarrow \mathbb{N}$ with $r(X \cup Y) + r(X \cap Y) \leq r(X) + r(Y)$ for all $X, Y \subseteq E$ is called **submodular**.

Theorem 77 *Let E be a finite nonempty set. A function $\sigma : 2^E \rightarrow 2^E$ is the closure operator of a matroid $(E, \mathcal{F})$ if and only if the following conditions hold for all $X, Y \subseteq E$ and $x, y \in E$:*

(S1) $X \subseteq \sigma(X)$;

(S2) If $X \subseteq Y$ then $\sigma(X) \subseteq \sigma(Y)$;

(S3) $\sigma(X) = \sigma(\sigma(X))$;

(S4) If $y \notin \sigma(X)$ and $y \in \sigma(X \cup \{x\})$ then $x \in \sigma(X \cup \{y\})$.

Proof: “ $\Rightarrow$.” Let σ be the closure operator of a matroid. We show (S1) – (S4).

(S1) Follows directly from the definition of the closure.

(S2) Let $X, Y \subseteq E$ with $X \subseteq Y$ and $z \in \sigma(X)$. Then, we have

$$\begin{aligned} r(X) + r(Y) &\stackrel{z \in \sigma(X)}{=} r(X \cup \{z\}) + r(Y) \stackrel{(R3)}{\geq} r((X \cup \{z\}) \cap Y) + r(X \cup \{z\} \cup Y) \\ &\stackrel{(R2)}{\geq} r(X) + r(Y \cup \{z\}), \end{aligned}$$

and thus $r(Y) = r(Y \cup \{z\})$. This implies $z \in \sigma(Y)$, so $\sigma(X) \subseteq \sigma(Y)$, which implies (S2).

(S3) Let $X \subseteq E$. Then $\sigma(X) \subseteq \sigma(\sigma(X))$ follows from (S1) and (S2). Moreover, by repeated application of (R3') we get $r(\sigma(X)) = r(X)$ for all $X \subseteq E$. Now let $x \in \sigma(\sigma(X))$, i.e. $r(\sigma(X) \cup \{x\}) = r(\sigma(X))$. Then

$$r(X) \stackrel{(R2)}{\leq} r(X \cup \{x\}) \stackrel{(R2)}{\leq} r(\sigma(X) \cup \{x\}) = r(\sigma(X)) = r(X).$$

Hence we have $r(X) = r(X \cup \{x\})$ and thus $x \in \sigma(X)$. This implies (S3).

(S4) Suppose there are a set $X \subseteq E$ and two elements $x, y \in E$ with $y \notin \sigma(X)$, $y \in \sigma(X \cup \{x\})$ and $x \notin \sigma(X \cup \{y\})$. These three conditions imply $r(X \cup \{y\}) = r(X) + 1$, $r(X \cup \{x, y\}) = r(X \cup \{x\})$ and $r(X \cup \{x, y\}) = r(X \cup \{y\}) + 1$. Putting these three equations together we get

$$r(X \cup \{x\}) = r(X \cup \{x, y\}) = r(X \cup \{y\}) + 1 = r(X) + 2.$$

This is a contradiction to the right inequality of (R2').

“ $\Leftarrow$ ” Let $\sigma : 2^E \rightarrow 2^E$ satisfy (S1)-(S4). Let

$$\mathcal{F} := \{X \subseteq E \mid x \notin \sigma(X \setminus \{x\}) \text{ for all } x \in X\}.$$

We will prove that $(E, \mathcal{F})$ is a matroid by showing (M1)-(M3).

(M1) is trivial. And for $X \subseteq Y \in \mathcal{F}$ and $x \in X$, we have $x \notin \sigma(Y \setminus \{x\})$ and $\sigma(X \setminus \{x\}) \subseteq \sigma(Y \setminus \{x\})$, so $x \notin \sigma(X \setminus \{x\})$. Since this is true for all $x \in X$, we have $X \in \mathcal{F}$, and (M2) holds.

For (M3), we need the following claim

Claim: For $X \in \mathcal{F}$ and $Y \subseteq E$ with $|X| > |Y|$, we have $X \not\subseteq \sigma(Y)$.

Proof of the Claim: Induction on $|Y \setminus X|$.

Assume $|Y \setminus X| = 0$, so $Y \subseteq X$. Let $x \in X \setminus Y$. Then $Y \subseteq X \setminus \{x\}$, and by (S2), we have $\sigma(Y) \subseteq \sigma(X \setminus \{x\})$. Moreover (since $X \in \mathcal{F}$), $x \notin \sigma(X \setminus \{x\})$, and hence $x \notin \sigma(Y)$. Therefore $x \in X \setminus \sigma(Y)$, which implies $X \not\subseteq \sigma(Y)$.

Now assume $|Y \setminus X| > 0$. Let $y \in Y \setminus X$. By the induction hypothesis there is an $x \in X \setminus \sigma(Y \setminus \{y\})$. If $x \notin \sigma(Y)$ then $X \not\subseteq \sigma(Y)$ and we are done. Otherwise, we have $x \in \sigma(Y) = \sigma((Y \setminus \{y\}) \cup \{y\})$. Since we also have $x \notin \sigma(Y \setminus \{y\})$, (S4) implies

$$y \in \sigma((Y \setminus \{y\}) \cup \{x\}). \tag{7}$$

By (S1), we have $Y \setminus \{y\} \subseteq \sigma((Y \setminus \{y\}) \cup \{x\})$, so together with (7), we get $Y \subseteq \sigma((Y \setminus \{y\}) \cup \{x\})$. Therefore, by (S2) and (S3), we get $\sigma(Y) \subseteq \sigma((Y \setminus \{y\}) \cup \{x\})$. Since $x \in X$ and $y \in Y \setminus X$, we have $x \neq y$, and hence we can apply the induction hypothesis to X and $(Y \setminus \{y\}) \cup \{x\}$. This implies $X \not\subseteq \sigma((Y \setminus \{y\}) \cup \{x\})$, thus (since $\sigma(Y) \subseteq \sigma((Y \setminus \{y\}) \cup \{x\})$) we have $X \not\subseteq \sigma(Y)$, which proves the claim. $\square$ **Claim**

Now, we will prove (M3). Let $X, Y \in \mathcal{F}$ with $|X| > |Y|$. By the claim, there is an $x \in X \setminus \sigma(Y)$. We will show that $Y \cup \{x\} \in \mathcal{F}$. To this end, let $z \in Y \cup \{x\}$. We have to show that

$z \notin \sigma((Y \cup \{x\}) \setminus \{z\})$. If $z \in Y$ then $z \notin \sigma(Y \setminus \{z\})$ because $Y \in \mathcal{F}$. But if $z = x$ then $z \notin \sigma(Y \setminus \{z\})$ because $x \notin \sigma(Y)$ and $\sigma(Y \setminus \{x\}) \subseteq \sigma(Y)$ by (S2). Hence, in any case, $z \notin \sigma(Y \setminus \{z\})$. By (S4), $z \notin \sigma(Y \setminus \{z\})$ and $x \notin \sigma(Y)$ imply $z \notin \sigma((Y \setminus \{z\}) \cup \{x\})$. As $\sigma((Y \cup \{x\}) \setminus \{z\}) \subseteq \sigma((Y \setminus \{z\}) \cup \{x\})$, this proves $z \notin \sigma((Y \cup \{x\}) \setminus \{z\})$ and hence $Y \cup \{x\} \in \mathcal{F}$.

Therefore, we have proved that $(E, \mathcal{F})$ is a matroid. Denote its rank function by r and its closure operator by σ' . It remains to prove that $\sigma = \sigma'$.

By definition, for all $X \subseteq E$, we have $\sigma'(X) = \{y \in E \mid r(X \cup \{y\}) = r(X)\}$ and

$$r(X) = \max\{|Y| \mid Y \subseteq X, y \notin \sigma(Y \setminus \{y\}) \text{ for all } y \in Y\}.$$

Let $X \subseteq E$. We will show $\sigma(X) = \sigma'(X)$.

“ $\sigma'(X) \subseteq \sigma(X)$ ”: Let $z \in \sigma'(X)$. If $z \in X$ then, by (S1), $z \in \sigma(X)$. Thus assume that $z \notin X$. Let Y be a basis of X . Since $r(Y \cup \{z\}) \leq r(X \cup \{z\}) = r(X) = |Y| < |Y \cup \{z\}|$, we have $Y \cup \{z\} \notin \mathcal{F}$. Thus, by the definition of $\mathcal{F}$ there must be a $y \in Y \cup \{z\}$ with $y \in \sigma((Y \cup \{z\}) \setminus \{y\})$. If $z = y$ then $z \in \sigma(Y)$, and we are done. Otherwise, we have $y \in \sigma((Y \setminus \{y\}) \cup \{z\})$ and $y \notin \sigma(Y \setminus \{y\})$ (because $Y \in \mathcal{F}$), so by (S4) we get $z \in \sigma((Y \setminus \{y\}) \cup \{y\}) = \sigma(Y)$. By (S2), we get $z \in \sigma(X)$. This shows $\sigma'(X) \subseteq \sigma(X)$.

“ $\sigma(X) \subseteq \sigma'(X)$ ”: Let $z \notin \sigma'(X)$, i.e. $r(X \cup \{z\}) > r(X)$. Let Y be a basis of $X \cup \{z\}$. Then $z \in Y$ and $|Y \setminus \{z\}| = |Y| - 1 = r(X \cup \{z\}) - 1 = r(X)$. Therefore $Y \setminus \{z\}$ is a basis of X , implying $X \subseteq \sigma'(Y \setminus \{z\}) \subseteq \sigma(Y \setminus \{z\})$, and thus (by (S2) and (S3)) $\sigma(X) \subseteq \sigma(Y \setminus \{z\})$. As $Y \in \mathcal{F}$ and thus $z \notin \sigma(Y \setminus \{z\})$, we conclude that $z \notin \sigma(X)$. $\square$

Theorem 78 *Let E be a finite nonempty set. A family $\mathcal{C} \subseteq 2^E$ of sets is the set of circuits of an independence system $(E, \mathcal{F})$, where $\mathcal{F} = \{F \subseteq E \mid \text{there is no } C \in \mathcal{C} \text{ with } C \subseteq F\}$ if and only if the following conditions hold:*

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

(C2) For any $C_1, C_2 \in \mathcal{C}$: $C_1 \subseteq C_2$ implies $C_1 = C_2$.

Moreover, if $\mathcal{C}$ is the set of circuits of an independence system $(E, \mathcal{F})$ then the following statements are equivalent.

(a) $(E, \mathcal{F})$ is a matroid.

(b) For any $X \in \mathcal{F}$ and $e \in E$, the set $X \cup \{e\}$ contains at most one circuit.

(C3) For any $C_1, C_2 \in \mathcal{C}$ with $C_1 \neq C_2$ and $e \in C_1 \cap C_2$ there is a $C_3 \in \mathcal{C}$ with $C_3 \subseteq (C_1 \cup C_2) \setminus \{e\}$.

(C3') For any $C_1, C_2 \in \mathcal{C}$ with $C_1 \neq C_2$, $e \in C_1 \cap C_2$ and $f \in C_1 \setminus C_2$ there is a $C_3 \in \mathcal{C}$ with $f \in C_3 \subseteq (C_1 \cup C_2) \setminus \{e\}$.

Proof: The family of circuits of an independence system obviously satisfies (C1) and (C2).

On the other hand, if $\mathcal{C}$ satisfies (C1) then $(E, \mathcal{F})$ is an independence system. Moreover, if $\mathcal{C}$ also satisfies (C2) it is the set of circuits of this independence system.

“(a) $\Rightarrow$ (C3)’”: Let $\mathcal{C}$ be the family of circuits of a matroid, and let $C_1, C_2 \in \mathcal{C}$, $e \in C_1 \cap C_2$ and $f \in C_1 \setminus C_2$. Then

$$\begin{aligned}
|C_1| - 1 + r((C_1 \cup C_2) \setminus \{e, f\}) + |C_2| - 1 &= r(C_1) + r((C_1 \cup C_2) \setminus \{e, f\}) + r(C_2) \\
&\stackrel{(R3)}{\geq} r(C_1) + r((C_1 \cup C_2) \setminus \{f\}) + r(C_2 \setminus \{e\}) \\
&\stackrel{(R3)}{\geq} r(C_1 \setminus \{f\}) + r(C_1 \cup C_2) + r(C_2 \setminus \{e\}) \\
&= |C_1| - 1 + r(C_1 \cup C_2) + |C_2| - 1,
\end{aligned}$$

which implies $r((C_1 \cup C_2) \setminus \{e, f\}) \geq r(C_1 \cup C_2)$ and thus $r((C_1 \cup C_2) \setminus \{e, f\}) = r(C_1 \cup C_2)$. Now, let B be a basis of $(C_1 \cup C_2) \setminus \{e, f\}$. Then B is also a basis of $C_1 \cup C_2$, so $B \cup f$ is dependent, i.e. it contains a circuit C_3 with $f \in C_3 \subseteq (C_1 \cup C_2) \setminus \{e\}$.

“(C3’) $\Rightarrow$ (C3)” : This implication is trivial.

“(C3) $\Rightarrow$ (b)” : If $X \in \mathcal{F}$ and $X \cup \{e\}$ contains two circuits C_1 and C_2 then (C3) implies $(C_1 \cup C_2) \setminus \{e\} \notin \mathcal{F}$, which is a contradiction since $(C_1 \cup C_2) \setminus \{e\} \subseteq X$.

“(b) $\Rightarrow$ (a)” : If (b) is satisfied then (by Theorem 74) $q(E, \mathcal{F}) = 1$. This implies (by Proposition 73) that $(E, \mathcal{F})$ is a matroid. $\square$

Notation: For a matroid $(E, \mathcal{F})$, $X \in \mathcal{F}$ and $e \in E$ such that $X \cup \{e\} \notin \mathcal{F}$, we denote by $C(X, e)$ the unique circuit in $X \cup \{e\}$. If $X \cup \{e\} \in \mathcal{F}$, we write $C(X, e) = \emptyset$.

6.2 Dual Independence Systems

Definition 29 Let $(E, \mathcal{F})$ be an independence system. We define the **dual** of $(E, \mathcal{F})$ by $(E, \mathcal{F}^*)$ where

$$\mathcal{F}^* = \{F \subseteq E \mid \text{there is a basis } B \text{ of } (E, \mathcal{F}) \text{ such that } F \cap B = \emptyset\}.$$

Observation: The dual of an independence system is again an independence system.

Proposition 79 $(E, \mathcal{F}^{**}) = (E, \mathcal{F})$ holds for every independence system $(E, \mathcal{F})$.

Proof: We have

$$\begin{aligned}
F \in \mathcal{F}^{**} &\Leftrightarrow \text{There is a basis } B^* \text{ of } (E, \mathcal{F}^*) \text{ such that } F \cap B^* = \emptyset \\
&\Leftrightarrow \text{There is a basis } B \text{ of } (E, \mathcal{F}) \text{ such that } F \cap (E \setminus B) = \emptyset \\
&\Leftrightarrow F \in \mathcal{F}.
\end{aligned}$$

□

Theorem 80 *Let $(E, \mathcal{F})$ be an independence system, $(E, \mathcal{F}^*)$ its dual, and r and r^* the corresponding rank functions. Then*

- (a) *$(E, \mathcal{F})$ is a matroid if and only if $(E, \mathcal{F}^*)$ is a matroid.*
- (b) *If $(E, \mathcal{F})$ is a matroid then*

$$r^*(F) = |F| + r(E \setminus F) - r(E)$$

for $F \subseteq E$.

Proof: By the previous proposition, we only have to prove one direction for (a). So let $(E, \mathcal{F})$ be a matroid, and we will show that $(E, \mathcal{F}^*)$ is a matroid.

Define $q : 2^E \rightarrow \mathbb{N}$ by $q(F) = |F| + r(E \setminus F) - r(E)$ for all $F \subseteq E$.

Claim: q satisfies (R1), (R2), and (R3).

Proof of the Claim: (R1): We have $r(E) \geq r(E \setminus F)$, so $q(F) \leq |F|$ for all $F \subseteq E$.

(R2): Let $X \subseteq Y \subseteq E$. Since $(E, \mathcal{F})$ is a matroid, we get:

$$r(E \setminus X) + 0 = r((E \setminus Y) \cup (Y \setminus X)) + r(\emptyset) \stackrel{(R3)}{\leq} r(E \setminus Y) + r(Y \setminus X).$$

Thus, we have $r(E \setminus X) - r(E \setminus Y) \leq r(Y \setminus X) \stackrel{(R1)}{\leq} |Y \setminus X| = |Y| - |X|$, which implies $q(X) \leq q(Y)$.

(R3): Let $X, Y \subseteq E$. Then:

$$\begin{aligned}
q(X \cup Y) + q(X \cap Y) &= |X \cup Y| + |X \cap Y| + r(E \setminus (X \cup Y)) + r(E \setminus (X \cap Y)) - 2r(E) \\
&= |X| + |Y| + r((E \setminus X) \cap (E \setminus Y)) + r((E \setminus X) \cup (E \setminus Y)) - 2r(E) \\
&\stackrel{(R3)}{\leq} |X| + |Y| + r(E \setminus X) + r(E \setminus Y) - 2r(E) \\
&= q(X) + q(Y)
\end{aligned}$$

This proves the claim.

□ **Claim**

Therefore, q is the rank function of some matroid. And we have $q(F) = |F|$ if and only if $r(E \setminus F) = r(E)$, which is equivalent to $F \in \mathcal{F}^*$. This shows both (a) and (b). □

Notation: For a graph G , we denote by $\mathcal{M}(G)$ the corresponding cycle matroid, i.e. the matroid $(E, \mathcal{F})$ with $E = E(G)$ and $\mathcal{F} = \{F \subseteq E \mid (V(G), F) \text{ is a forest}\}$.

Theorem 81 *Let G be a connected planar graph with an arbitrary planar embedding and let G^* be the planar dual. Then*

$$\mathcal{M}(G^*) = (\mathcal{M}(G))^*.$$

Proof: Follows directly from Proposition 35. □

The dual of a graphic matroid $(E, \mathcal{F})$ is not necessarily a graphic matroid. In fact, this is only the case if $(E, \mathcal{F})$ is the cycle matroid of a planar graph. In particular, the duals of the cycle matroids of K_5 and $K_{3,3}$ are not graphic (see exercises).

Note that for a connected planar graph G and the corresponding cycle matroid $\mathcal{M}(G)$, the formula in Theorem 80 (b) applied to $F = E(G)$ implies Euler's formula. If f is the number of faces of the embedding (and $m = |E(G)|$ and $n = |V(G)|$) then

$$f - 1 = r^*(E(G)) = |E(G)| + r(\emptyset) - r(E(G)) = m - n + 1.$$

6.3 The Greedy Algorithm

In this section, we will examine two greedy algorithms. We will first formulate them for the MAXIMIZATION PROBLEM for $(E, \mathcal{F}, c)$ where $(E, \mathcal{F})$ is an independence system and $c : E \rightarrow \mathbb{R}_{\geq 0}$.

Whenever we talk about algorithms on independence systems, we have to specify how the input is given. It is in general very inefficient to explicitly list all elements of the set $\mathcal{F}$. Instead, independence systems will be given by so-called oracles that answer questions on the input. For the first version of the greedy algorithm we assume that we are given an **independence oracle**, i.e. an oracle that decides for a given set $F \subseteq E$ if $F \in \mathcal{F}$.

Algorithm 1: BEST-IN-GREEDY ALGORITHM

Input: An independence system $(E, \mathcal{F})$ given by an independence oracle.

Weights $c : E \rightarrow \mathbb{R}_{\geq 0}$.

Output: A set $F \in \mathcal{F}$;

- 1 Sort $E = \{e_1, \dots, e_n\}$ such that $c(e_1) \geq c(e_2) \geq \dots \geq c(e_n)$;
 - 2 Set $F := \emptyset$;
 - 3 **for** $i = 1, \dots, n$ **do**
 - 4 **if** $F \cup \{e_i\} \in \mathcal{F}$ **then**
 - 5 $F := F \cup \{e_i\}$;
-

For the second algorithm, we assume that we have a **basis-superset oracle** that decides for a given set $F \subseteq E$ if F contains a basis.

Algorithm 2: WORST-OUT-GREEDY ALGORITHM

Input: An independence system $(E, \mathcal{F})$ given by a basis-superset oracle.

Weights $c : E \rightarrow \mathbb{R}_{\geq 0}$.

Output: A set $F \in \mathcal{F}$;

1 Sort $E = \{e_1, \dots, e_n\}$ such that $c(e_1) \leq c(e_2) \leq \dots \leq c(e_n)$;

2 Set $F := E$;

3 **for** $i = 1, \dots, n$ **do**

4 **if** $F \setminus \{e_i\}$ *contains a basis* **then**

5 $F := F \setminus \{e_i\}$;

Independence systems can be specified by several other oracles:

- The **rank oracle**: Given a set $F \subseteq E$, return the rank of F .
- The **closure oracle**: Given a set $F \subseteq E$, return $\sigma(F)$.
- The **basis oracle**: Given a set $F \subseteq E$, decide if F is a basis of E .
- The **circuit oracle**: Given a set $F \subseteq E$, decide if F is a circuit.

All these oracles can be used to specify an independence system. However, from an algorithmic point of view, it can make a huge difference by which oracle an independence system is given. We call two oracles **polynomially equivalent** if each one can be simulated by a polynomial-time oracle algorithm using the other one. There are pairs of oracles that are not polynomially equivalent. For example, if $P \neq NP$ then the independence oracle and the basis-superset oracle are, in general, not polynomially equivalent:

- Consider $(E, \mathcal{F})$ where $E = E(K_n)$ is the edge set of the complete graph and

$$\mathcal{F} = \{F \subseteq E \mid F \text{ is a subset of edges of a Hamilton circuit of } K_n\}.$$

Here, the independence oracle solves an easy problem (we just have to check if a given set of edges is either a Hamilton circuit or consists of paths only) but the basis-superset oracle solves an *NP*-complete problem.

- Consider $(E, \mathcal{F})$ where $E = E(G)$ is the edge set of a graph G with two nodes s and t such that t is reachable from s , and

$$\mathcal{F} = \{F \subseteq E \mid F \text{ is a subset of an } s\text{-}t\text{-path}\}.$$

Here the basis-superset oracle is easy (we just have to check if t is reachable from s in a given graph) while the independence oracle has to solve an *NP*-complete problem. (see Korte and Monma [1979]).

However, note that the independence oracle and the basis-superset oracle are polynomially equivalent for matroids (see exercises).

Of course, both greedy algorithms can be formulated for the MINIMIZATION PROBLEM for $(E, \mathcal{F}, c)$. Then, the BEST-IN-GREEDY ALGORITHM for the MAXIMIZATION PROBLEM for $(E, \mathcal{F}, c)$ corresponds to the WORST-OUT-GREEDY ALGORITHM for the MINIMIZATION PROBLEM for $(E, \mathcal{F}^*, c)$ because adding an element to F in the BEST-IN-GREEDY ALGORITHM means removing an element from the complement of F .

Theorem 82 (*Jenkyns [1976], Korte and Hausmann [1978]*) *Let $(E, \mathcal{F})$ be an independence system. For $c : E \rightarrow \mathbb{R}_{\geq 0}$, we denote by $G(E, \mathcal{F}, c)$ the cost of some solution found by the BEST-IN-GREEDY ALGORITHM for the MAXIMIZATION PROBLEM, and by $OPT(E, \mathcal{F}, c)$ the cost of an optimum solution. Then*

$$q(E, \mathcal{F}) \leq \frac{G(E, \mathcal{F}, c)}{OPT(E, \mathcal{F}, c)} \leq 1$$

(where $\frac{0}{0} := 1$) for all $c : E \rightarrow \mathbb{R}_{\geq 0}$. There is a cost function for which the lower bound is attained by some output of the BEST-IN-GREEDY ALGORITHM.

Proof: Let $E = \{e_1, \dots, e_n\}$, $c : E \rightarrow \mathbb{R}_{\geq 0}$, and $c(e_1) \geq c(e_2) \geq \dots \geq c(e_n)$. Let G_n be the solution found by the BEST-IN-GREEDY ALGORITHM (with this order of the elements of E), and let O_n be an optimum solution. Define $E_j := \{e_1, \dots, e_j\}$, $G_j := G_n \cap E_j$, and $O_j := O_n \cap E_j$ for $j \in \{0, \dots, n\}$. Moreover, set $d_n := c(e_n)$ and $d_j := c(e_j) - c(e_{j+1})$ for $j \in \{1, \dots, n-1\}$.

Since $O_j \subseteq O_n \in \mathcal{F}$ and thus $O_j \in \mathcal{F}$, we have $|O_j| \leq r(E_j)$ for $j \in \{1, \dots, n-1\}$. And since G_j is a basis of E_j , we have $|G_j| \geq \rho(E_j)$ for $j \in \{1, \dots, n-1\}$. This implies

$$\begin{aligned} c(G_n) &= \sum_{j=1}^n (|G_j| - |G_{j-1}|)c(e_j) = \sum_{j=1}^n |G_j|d_j \geq \sum_{j=1}^n \rho(E_j)d_j \geq q(E, \mathcal{F}) \sum_{j=1}^n r(E_j)d_j \\ &\geq q(E, \mathcal{F}) \sum_{j=1}^n |O_j|d_j = q(E, \mathcal{F}) \sum_{j=1}^n (|O_j| - |O_{j-1}|)c(e_j) = q(E, \mathcal{F})c(O_n). \end{aligned}$$

To show that the lower bound is tight, choose $F \subseteq E$ and bases B_1 and B_2 of F such that $\frac{|B_1|}{|B_2|} = q(E, \mathcal{F})$. Define

$$c(e) = \begin{cases} 1 & \text{for } e \in F \\ 0 & \text{for } e \in E \setminus F \end{cases}$$

and sort $e_1, \dots, e_n$ such that $c(e_1) \geq c(e_2) \geq \dots \geq c(e_n)$ and $B_1 = \{e_1, \dots, e_{|B_1|}\}$. Then $G(E, \mathcal{F}, c) = |B_1|$ and $OPT(E, \mathcal{F}, c) = |B_2|$, so $\frac{G(E, \mathcal{F}, c)}{OPT(E, \mathcal{F}, c)} = q(E, \mathcal{F})$. $\square$

Note that by slightly perturbing the weights in the construction at the end of the proof, we can enforce that any run of the BEST-IN-GREEDY ALGORITHM finds a solution whose value is arbitrarily close to $q(E, \mathcal{F})\text{OPT}(E, \mathcal{F}, c)$.

Theorem 83 (*Edmonds-Rado Theorem, Rado [1957], Edmonds [1971]*) An independence system $(E, \mathcal{F})$ is a matroid if and only if the BEST-IN-GREEDY ALGORITHM finds an optimum solution for the MAXIMIZATION PROBLEM for $(E, \mathcal{F}, c)$ for all cost functions $c : E \rightarrow \mathbb{R}_{\geq 0}$.

Proof: By the previous theorem, we have $q(E, \mathcal{F}) < 1$ if and only if there is a cost function $c : E \rightarrow \mathbb{R}_{\geq 0}$ for which the BEST-IN-GREEDY ALGORITHM does not find an optimum solution. By Proposition 73, $q(E, \mathcal{F}) < 1$ holds if and only if $(E, \mathcal{F})$ is not a matroid. $\square$

Theorem 84 Let $(E, \mathcal{F})$ be a matroid, $c : E \rightarrow \mathbb{R}$, $k \in \mathbb{N}$, and $X \in \mathcal{F}$ with $|X| = k$. Then $c(X) = \max\{c(Y) \mid Y \in \mathcal{F}, |Y| = k\}$ if and only if the following two conditions hold:

- (a) For all $y \in E \setminus X$ with $X \cup \{y\} \notin \mathcal{F}$ and for all $x \in C(X, y)$, we have $c(x) \geq c(y)$.
- (b) For all $y \in E \setminus X$ with $X \cup \{y\} \in \mathcal{F}$ and for all $x \in X$, we have $c(x) \geq c(y)$.

Proof: “ $\Rightarrow$ ” This is trivial, since if one of the conditions is violated, an element of X could be replaced by the element y from the condition.

“ $\Leftarrow$ ” Let $\mathcal{F}' := \{F \in \mathcal{F} \mid |F| \leq k\}$ and $c'(e) = c(e) + M$ for all $e \in E$ where $M = \max\{|c(e)| \mid e \in E\}$. Sort $E = \{e_1, \dots, e_n\}$ such that $c'(e_1) \geq c'(e_2) \geq \dots \geq c'(e_n)$ and such that for $i \in \{1, \dots, n-1\}$ with $c'(e_i) = c'(e_{i+1})$ and $e_{i+1} \in X$ we also have $e_i \in X$. This means that the elements are sorted such that, among all elements with the same weight, the elements of X come first.

Let X' be the solution found by the BEST-IN-GREEDY ALGORITHM for the MAXIMIZATION PROBLEM for $(E, \mathcal{F}', c')$ if the elements are sorted as above. Since $(E, \mathcal{F}')$ is a matroid (see the exercises) the previous theorem implies

$$c(X') + kM = c'(X') = \max\{c'(Y) \mid Y \in \mathcal{F}'\} = \max\{c(Y) \mid Y \in \mathcal{F}, |Y| = k\} + kM.$$

Claim: $X' = X$

Proof of the claim: We have $|X| = k = |X'|$. Suppose that $X \neq X'$, and let $e_i \in X' \setminus X$ with i minimum. Thus $X \cap \{e_1, \dots, e_{i-1}\} \supseteq X' \cap \{e_1, \dots, e_{i-1}\}$. Moreover, there cannot be an element in $(X \setminus X') \cap \{e_1, \dots, e_{i-1}\}$ because the BEST-IN-GREEDY ALGORITHM would have added this element to X' . Therefore, $X \cap \{e_1, \dots, e_{i-1}\} = X' \cap \{e_1, \dots, e_{i-1}\}$.

Now if $X \cup \{e_i\} \notin \mathcal{F}$ then (a) implies $C(X, e_i) \subseteq X'$, a contradiction. If $X \cup \{e_i\} \in \mathcal{F}$ then (b) implies $X \subseteq X'$, which is also impossible. This proves the claim and thus the theorem. $\square$

We can also apply the **BEST-IN-GREEDY ALGORITHM** to the **MINIMIZATION PROBLEM** for $(E, \mathcal{F}, c)$, where $(E, \mathcal{F})$ is an independence system. In this case, we use the order $c(e_1) \leq c(e_2) \leq \dots \leq c(e_n)$ of the elements. However, this does not lead to any positive upper bound on $\frac{G(E, \mathcal{F}, c)}{\text{OPT}(E, \mathcal{F}, c)}$ (of course 1 is a lower bound). To see this, consider the independence system $(E, \mathcal{F})$ where E is the node set of some graph G and the bases of $(E, \mathcal{F})$ are the **vertex covers** of G , i.e. sets $X \subseteq V(G)$ of nodes such that every edge of $E(G)$ is incident to at least one node in X . Then if $V(G) = \{x, y, z\}$ and $E(G) = \{\{x, y\}, \{y, z\}\}$ and the weights are given by $c(x) = 1$, $c(y) = 2$, $c(z) = 1000$ then the **BEST-IN-GREEDY ALGORITHM** would first pick x and then has to pick z while the optimum solution just contains y .

Theorem 85 (*Korte and Monma [1979]*) *Let $(E, \mathcal{F})$ be an independence system. For $c : E \rightarrow \mathbb{R}_{\geq 0}$, we denote by $G(E, \mathcal{F}, c)$ the cost of some solution found by the **WORST-OUT-GREEDY ALGORITHM** for the **MINIMIZATION PROBLEM** (i.e. using the order $c(e_1) \geq c(e_2) \geq \dots \geq c(e_n)$ of the elements) and by $\text{OPT}(E, \mathcal{F}, c)$ the cost of an optimum solution. Let $\rho^* : 2^E \rightarrow \mathbb{N}$ and $r^* : 2^E \rightarrow \mathbb{N}$ be the lower rank function and the rank function of $(E, \mathcal{F}^*)$, respectively. Then*

$$1 \leq \frac{G(E, \mathcal{F}, c)}{\text{OPT}(E, \mathcal{F}, c)} \leq \max_{F \subseteq E} \frac{|F| - \rho^*(F)}{|F| - r^*(F)}$$

(again with $\frac{0}{0} := 1$) for all $c : E \rightarrow \mathbb{R}_{\geq 0}$. There is a cost function for which the upper bound is attained by some output of the **WORST-OUT-GREEDY ALGORITHM**.

Proof: Let $E = \{e_1, \dots, e_n\}$, $c : E \rightarrow \mathbb{R}_{\geq 0}$, and $c(e_1) \geq c(e_2) \geq \dots \geq c(e_n)$. Let G_n be the solution found by the **WORST-OUT-GREEDY ALGORITHM** (with this order of the elements of E), and let O_n be an optimum solution. Define $E_j := \{e_1, \dots, e_j\}$, $G_j := G_n \cap E_j$, and $O_j := O_n \cap E_j$ for $j \in \{0, \dots, n\}$. Moreover, set $d_n := c(e_n)$ and $d_j := c(e_j) - c(e_{j+1})$ for $j \in \{1, \dots, n-1\}$.

By construction, $G_j \cup (E \setminus E_j)$ contains a basis of E but for $e \in G_j$ the set $(G_j \cup (E \setminus E_j)) \setminus \{e\}$ does not contain a basis of E (for $j \in \{1, \dots, n\}$). Therefore, $E_j \setminus G_j$ is a basis of E_j with respect to $(E, \mathcal{F}^*)$, so $|E_j| - |G_j| \geq \rho^*(E_j)$.

On the other hand, $O_n \subseteq E \setminus (E_j \setminus O_j)$ and O_n is a basis, $E_j \setminus O_j$ is independent in $(E, \mathcal{F}^*)$, so $|E_j| - |O_j| \leq r^*(E_j)$.

Thus, for $j \in \{0, \dots, n\}$ we have

$$\begin{aligned} |G_j| &\leq |E_j| - \rho^*(E_j) \quad \text{and} \\ |O_j| &\geq |E_j| - r^*(E_j). \end{aligned}$$

Now, let $\Gamma = \max_{F \subseteq E} \frac{|F| - \rho^*(F)}{|F| - r^*(F)}$. Then, we get

$$\begin{aligned} c(G_n) &= \sum_{j=1}^n (|G_j| - |G_{j-1}|)c(e_j) = \sum_{j=1}^n |G_j|d_j \leq \sum_{j=1}^n (|E_j| - \rho^*(E_j))d_j \\ &\leq \Gamma \sum_{j=1}^n (|E_j| - r^*(E_j))d_j \leq \Gamma \sum_{j=1}^n |O_j|d_j = \Gamma \sum_{j=1}^n (|O_j| - |O_{j-1}|)c(e_j) = \Gamma c(O_n). \end{aligned}$$

To show that the upper bound can be attained, let $F \subseteq E$ be a set with $\frac{|F| - \rho^*(F)}{|F| - r^*(F)} = \Gamma$. Then, we set

$$c(e) = \begin{cases} 1 & \text{for } e \in F \\ 0 & \text{for } e \in E \setminus F \end{cases}$$

Let B_1 be a basis of F with respect to $(E, \mathcal{F}^*)$, with $|B_1| = \rho^*(F)$. If we sort $e_1, \dots, e_n$ such that $c(e_1) \geq c(e_2) \geq \dots \geq c(e_n)$ and $B_1 = \{e_1, \dots, e_{|B_1|}\}$, we have $G(E, \mathcal{F}, c) = |F| - |B_1| = |F| - \rho^*(F)$ and $\text{OPT}(E, \mathcal{F}, c) = |F| - r^*(F)$. $\square$

We can also apply the WORST-OUT-GREEDY ALGORITHM to the MAXIMIZATION PROBLEM for $(E, \mathcal{F}, c)$, where $(E, \mathcal{F})$ is an independence system. However, this does not lead to any positive lower bound on $\frac{G(E, \mathcal{F}, c)}{\text{OPT}(E, \mathcal{F}, c)}$ (of course 1 is an upper bound). To see this, consider the independence system $(E, \mathcal{F})$ where E is the node set of some graph G and $\mathcal{F} = \{F \subseteq V(G) \mid F \text{ is a stable set}\}$. We can use again the graph G with $V(G) = \{x, y, z\}$ and $E(G) = \{\{x, y\}, \{y, z\}\}$ and set again the weights to $c(x) = 1$, $c(y) = 2$, $c(z) = 1000$. Then the WORST-OUT-GREEDY ALGORITHM would first remove x and then have to remove z .

6.4 Matroid Intersection

Definition 30 Given k independence systems $(E, \mathcal{F}_1), \dots, (E, \mathcal{F}_k)$ we define their **intersection** by $(E, \mathcal{F}_1 \cap \dots \cap \mathcal{F}_k)$.

Obviously, the intersection of independence systems is again an independence system.

Proposition 86 Any independence system $(E, \mathcal{F})$ is the intersection of a finite number of matroids.

Proof: Each circuit C of an independence system $(E, \mathcal{F})$ defines a matroid $(E, \{F \subseteq E \mid C \not\subseteq F\})$. The intersection of all these matroids is $(E, \mathcal{F})$. $\square$

Proposition 87 If $(E, \mathcal{F})$ is the intersection of p matroids then $q(E, \mathcal{F}) \geq \frac{1}{p}$.

Proof: Let $(E, \mathcal{F})$ be the intersection of p matroids $(E, \mathcal{F}_1), \dots, (E, \mathcal{F}_p)$. By Theorem 78, for any $X \in \mathcal{F}$ and $e \in E$, the set $X \cup \{e\}$ can contain at most one circuit with respect to $(E, \mathcal{F}_i)$ (for $i \in \{1, \dots, p\}$). Thus, $X \cup \{e\}$ can contain at most p circuits with respect to $(E, \mathcal{F})$. By Theorem 74, this implies $q(E, \mathcal{F}) \geq \frac{1}{p}$. $\square$

Example: Matchings in a bipartite graph $G = (A \dot{\cup} B, E)$ can be modeled as the intersection of two matroids. Let $\mathcal{F} := \{F \subseteq E \mid F \text{ is a matching in } G\}$. Then $(E, \mathcal{F})$ is the intersection of the two matroids $(E, \mathcal{F}_1)$ and $(E, \mathcal{F}_2)$ with

$$\begin{aligned}\mathcal{F}_1 &:= \{F \subseteq E \mid |\delta_F(x)| \leq 1 \text{ for all } x \in A\} \text{ and} \\ \mathcal{F}_2 &:= \{F \subseteq E \mid |\delta_F(x)| \leq 1 \text{ for all } x \in B\}.\end{aligned}$$

As a consequence of the previous proposition, we have $q(E, \mathcal{F}) \geq \frac{1}{2}$ for this independence system. And a path consisting of three edges is a bipartite graph for which $q(E, \mathcal{F}) = \frac{1}{2}$.

MATROID INTERSECTION PROBLEM

Instance: Two matroids $(E, \mathcal{F}_1)$ and $(E, \mathcal{F}_2)$, given by independence oracles.

Task: Find a set $F \in \mathcal{F}_1 \cap \mathcal{F}_2$ such that $|F|$ is maximum.

We will see that there is a polynomial-time algorithm for the MATROID INTERSECTION PROBLEM. Its main idea is as follows. We start with $X = \emptyset$, and in each iteration we augment the set X by one element in such a way that it is always independent with respect both to $(E, \mathcal{F}_1)$ and $(E, \mathcal{F}_2)$. In general, we cannot just add an element to X but we have to exchange sets of elements.

The following lemma will specify conditions that allow us to exchange not only single elements in independent sets but whole sets.

Lemma 88 (Frank [1981]) *Let $(E, \mathcal{F})$ be a matroid and $X \in \mathcal{F}$. Let $x_1, \dots, x_s \in X$ and $y_1, \dots, y_s \in E \setminus X$ with*

(a) $x_k \in C(X, y_k)$ for $k = 1, \dots, s$ and

(b) $x_j \notin C(X, y_k)$ for $1 \leq j < k \leq s$.

Then $(X \setminus \{x_1, \dots, x_s\}) \cup \{y_1, \dots, y_s\} \in \mathcal{F}$.

Proof: For $r \in \{0, \dots, s\}$, let $X_r = (X \setminus \{x_1, \dots, x_r\}) \cup \{y_1, \dots, y_r\}$. We show by induction on r that $X_r \in \mathcal{F}$ for $r \in \{0, \dots, s\}$. For $r = 0$, this is trivial. For $r > 0$, we assume that $X_{r-1} \in \mathcal{F}$, and we want to show $X_r \in \mathcal{F}$. If $X_{r-1} \cup \{y_r\} \in \mathcal{F}$ then $X_r \in \mathcal{F}$ since $X_r \subseteq X_{r-1} \cup \{y_r\}$. Otherwise $X_{r-1} \cup \{y_r\}$ contains a unique circuit C . By condition (b), we have $C(X, y_r) \subseteq X_{r-1} \cup \{y_r\}$, and thus $C = C(X, y_r)$. By condition (a), we have $x_r \in C(X, y_r) = C$, so $X_r = (X_{r-1} \cup \{y_r\}) \setminus \{x_r\} \in \mathcal{F}$. $\square$

To find the elements that we want to exchange for augmenting a set $X \in \mathcal{F}_1 \cap \mathcal{F}_2$, we define an auxiliary graph G_X :

$$\begin{aligned} A_X^{(1)} &:= \{(x, y) \mid y \in E \setminus X, x \in C_1(X, y) \setminus \{y\}\} \\ A_X^{(2)} &:= \{(y, x) \mid y \in E \setminus X, x \in C_2(X, y) \setminus \{y\}\} \\ G_X &:= (E, A_X^{(1)} \cup A_X^{(2)}) \end{aligned}$$

Moreover, we set

$$\begin{aligned} S_X &:= \{y \in E \setminus X \mid X \cup \{y\} \in \mathcal{F}_1\} \\ T_X &:= \{y \in E \setminus X \mid X \cup \{y\} \in \mathcal{F}_2\} \end{aligned}$$

In particular, if $S_X \cap T_X \neq \emptyset$, we could simply augment X by adding an arbitrary element from $S_X \cap T_X$. In general, we ask for a shortest path from S_X to T_X that enables us to augment X .

Lemma 89 *Let $(E, \mathcal{F}_1)$ and $(E, \mathcal{F}_2)$ be two matroids, and let $X \in \mathcal{F}_1 \cap \mathcal{F}_2$. Let $y_0, x_1, y_1, \dots, x_s, y_s$ be the vertices of a shortest y_0 - y_s -path in G_X (in this order), with $y_0 \in S_X$ and $y_s \in T_X$. Then*

$$X' := (X \cup \{y_0, \dots, y_s\}) \setminus \{x_1, \dots, x_s\} \in \mathcal{F}_1 \cap \mathcal{F}_2.$$

Proof: We first show that $X \cup \{y_0\}$, $x_1, \dots, x_s$ and $y_1, \dots, y_s$ satisfy the conditions of the previous lemma with respect to $\mathcal{F}_1$. We have $X \cup \{y_0\} \in \mathcal{F}_1$ because $y_0 \in S_X$. Condition (a) is satisfied because $(x_j, y_j) \in A_X^{(1)}$ for all j and (b) is satisfied because otherwise the path could be shortcut. Therefore, by the lemma, $X' \in \mathcal{F}_1$.

Now, we show that $X \cup \{y_s\}$, $x_s, x_{s-1}, \dots, x_1$ and $y_{s-1}, \dots, y_1, y_0$ satisfy the conditions of the previous lemma with respect to $\mathcal{F}_2$. We have $X \cup \{y_s\} \in \mathcal{F}_2$ because $y_s \in T_X$. Condition (a) is satisfied because $(y_{j-1}, x_j) \in A_X^{(2)}$ for all j and (b) is satisfied because otherwise the path could be shortcut. Therefore, by the lemma, $X' \in \mathcal{F}_2$. $\square$

Proposition 90 *Let $(E, \mathcal{F}_1)$ and $(E, \mathcal{F}_2)$ be two matroids with rank functions r_1 and r_2 . Then, for any $F \in \mathcal{F}_1 \cap \mathcal{F}_2$ and any $Q \subseteq E$, we have*

$$|F| \leq r_1(Q) + r_2(E \setminus Q).$$

Proof: Since $F \cap Q \in \mathcal{F}_1$, we have $|F \cap Q| \leq r_1(Q)$, and since $F \setminus Q \in \mathcal{F}_2$, we have $|F \setminus Q| \leq r_2(E \setminus Q)$. Adding these two inequalities proves the lemma. $\square$

Lemma 91 *Let $(E, \mathcal{F}_1)$ and $(E, \mathcal{F}_2)$ be two matroids. A set $X \in \mathcal{F}_1 \cap \mathcal{F}_2$ is maximum if and only if there is no S_X - T_X -path in G_X .*

Proof: “ $\Rightarrow$.” If there is an S_X - T_X -path we can augment along a shortest S_X - T_X -path and get a set $X' \in \mathcal{F}_1 \cap \mathcal{F}_2$ with $|X'| = |X| + 1$.

“ $\Leftarrow$.” Assume that there is no S_X - T_X -path in G_X . Let R be the set of nodes reachable from S_X in G_X . Thus, by assumption, $R \cap T_X = \emptyset$. Let r_1 and r_2 be the rank functions of $\mathcal{F}_1$ and $\mathcal{F}_2$, respectively.

Claim 1: $r_2(R) = |X \cap R|$

Proof of the claim: Suppose that $r_2(R) > |X \cap R|$. Then there is a $y \in R \setminus X$ with $(X \cap R) \cup \{y\} \in \mathcal{F}_2$. Since $X \cup \{y\} \notin \mathcal{F}_2$ (because $y \in R$, so $y \notin T_X$), the circuit $C_2(X, y)$ must contain an element $x \in X \setminus R$. But then $(y, x) \in A_X^{(2)}$, which means that there is an edge leaving R . Since this is a contradiction, this proves the claim. $\square$ **Claim 1**

Claim 2: $r_1(E \setminus R) = |X \setminus R|$

Proof of the claim: Suppose that $r_1(E \setminus R) > |X \setminus R|$. Then there is a $y \in (E \setminus R) \setminus X$ with $(X \setminus R) \cup \{y\} \in \mathcal{F}_1$. Since $X \cup \{y\} \notin \mathcal{F}_1$ (because $y \notin R$, so $y \notin S_X$), the circuit $C_1(X, y)$ must contain an element $x \in X \cap R$. But then $(x, y) \in A_X^{(1)}$, which means that there is an edge leaving R . Since this is a contradiction, this proves the claim. $\square$ **Claim 2**

The two claims imply that $|X| = r_2(R) + r_1(E \setminus R)$. By the previous proposition, this implies that X has maximum cardinality. $\square$

Theorem 92 (Edmonds [1970]) *Let $(E, \mathcal{F}_1)$ and $(E, \mathcal{F}_2)$ be two matroids with rank functions r_1 and r_2 . Then*

$$\max\{|X| \mid X \in \mathcal{F}_1 \cap \mathcal{F}_2\} = \min\{r_1(Q) + r_2(E \setminus Q) \mid Q \subseteq E\}.$$

$\square$

Theorem 93 EDMONDS’ MATROID INTERSECTION ALGORITHM *correctly solves the MATROID INTERSECTION PROBLEM in time $O(|E|^3\theta)$, where θ is the maximum complexity of the two independence oracles.*

Proof: Correctness has already been proved. The computation of the sets $C_i(X, y)$ can be done in time $O(|E|^2\theta)$ for each iteration, and the shortest-path computation can be done in time $O(|E|^2)$ (note that the edges are unweighted, so breadth-first search is sufficient). Since there are at most $|E|$ augmentations, we get a running time of $O(|E|^3\theta)$. $\square$

Faster algorithms are known for the MATROID INTERSECTION PROBLEM. The algorithm

Algorithm 3: EDMONDS' MATROID INTERSECTION ALGORITHM

Input: Two matroids $(E, \mathcal{F}_1)$ and $(E, \mathcal{F}_2)$ given by independence oracles.

Output: A set $X \in \mathcal{F}_1 \cap \mathcal{F}_2$ of maximum cardinality;

```
1 Set  $X := \emptyset$ ;  
2 for  $y \in E \setminus X$  and  $i \in \{1, 2\}$  do  
3    $\lfloor$  Compute  $C_i(X, y) := \{x \in X \cup \{y\} : X \cup \{y\} \notin \mathcal{F}_i \text{ and } (X \cup \{y\}) \setminus \{x\} \in \mathcal{F}_i\}$ ;  
4 Compute  $S_X, T_X$  and  $G_X$ ;  
5 if  $T_X$  is not reachable from  $S_X$  in  $G_X$  then  
6    $\lfloor$  return  $X$ ;  
7 Compute a shortest  $S_X$ - $T_X$ -path  $P$  in  $G_X$ ;  
8 Set  $X := X \Delta V(P)$ ;  
9 goto 2;
```

presented by Cunningham [1986] has a running time of $O(|E|^{2.5}\theta)$, Lee et al. [2015] reach a running time of $O(|E|^2 \log(|E|)\theta + |E|^3 \log^{O(1)}(|E|))$, and Chakrabarty et al. [2019] a running time of $O(|E|^2 \log(|E|)\theta)$. There are also algorithms that need less than a quadratic number of oracle calls (see Blikstad [2021] and Blikstad et al. [2021]).

If $P \neq NP$ then there is no polynomial-time algorithm that computes a largest set in the intersection of three (or more) matroids. To see this, consider the *NP*-complete HAMILTON-PATH PROBLEM: Given a directed graph G and two nodes $s, t \in V(G)$ we want to decide if there is an s - t -path in G visiting all nodes. Consider the three matroids $(E(G), \mathcal{F}_1)$, $(E(G), \mathcal{F}_2)$, and $(E(G), \mathcal{F}_3)$ with

$$\begin{aligned}\mathcal{F}_1 &= \{F \subseteq E(G) \mid |\delta_F^-(v)| \leq 1 \text{ for all } v \in V(G) \setminus \{s\} \text{ and } |\delta_F^-(s)| = 0\}, \\ \mathcal{F}_2 &= \{F \subseteq E(G) \mid |\delta_F^+(v)| \leq 1 \text{ for all } v \in V(G) \setminus \{t\} \text{ and } |\delta_F^+(t)| = 0\}, \\ \mathcal{F}_3 &= \{F \subseteq E(G) \mid \text{The underlying undirected graph of } (V(G), F) \text{ is a forest}\}.\end{aligned}$$

Then, a set $F \in \mathcal{F}_1 \cap \mathcal{F}_2 \cap \mathcal{F}_3$ with size $|V(G)| - 1$ corresponds to a Hamilton path $(V(G), F)$, and vice versa.

The following corollaries are applications of Theorem 92.

Corollary 94 *Let $(E, \mathcal{F}_1)$ and $(E, \mathcal{F}_2)$ be two matroids with rank functions r_1 and r_2 such that $r_1(E) = r_2(E)$. Then $(E, \mathcal{F}_1)$ and $(E, \mathcal{F}_2)$ have a common basis if and only if $r_1(Q) + r_2(E \setminus Q) \geq r_1(E)$ for all $Q \subseteq E$. $\square$*

Notation: Let $(E, \mathcal{F})$ be an independence system with rank function r . A set $F \subseteq E$ is **spanning** if $r(F) = r(E)$.

Corollary 95 *Let $(E, \mathcal{F}_1)$ and $(E, \mathcal{F}_2)$ be two matroids with rank functions r_1 and r_2 . Then, the minimum size of a common spanning set of $(E, \mathcal{F}_1)$ and $(E, \mathcal{F}_2)$ is equal to*

$$\max_{F \subseteq E} (r_1(E) - r_1(F) + r_2(E) - r_2(E \setminus F)).$$

Proof: The minimum size of a common spanning set of both matroids is

$$\begin{aligned} & \min \{ |B_1 \cup B_2| \mid B_1 \text{ basis of } (E, \mathcal{F}_1), B_2 \text{ basis of } (E, \mathcal{F}_2) \} \\ &= r_1(E) + r_2(E) - \max \{ |B_1 \cap B_2| \mid B_1 \text{ basis of } (E, \mathcal{F}_1), B_2 \text{ basis of } (E, \mathcal{F}_2) \} \\ &= r_1(E) + r_2(E) - \min_{F \subseteq E} (r_1(F) + r_2(E \setminus F)) \\ &= \max_{F \subseteq E} (r_1(E) - r_1(F) + r_2(E) - r_2(E \setminus F)). \end{aligned}$$

□

Corollary 96 *Let G be an undirected graph and $c : E(G) \rightarrow \{1, \dots, k\}$. There is a spanning tree T in G such that $c(e) \neq c(e')$ for all $e, e' \in E(T)$ with $e \neq e'$ (a so-called rainbow tree) if and only if for any set $I \subseteq \{1, \dots, k\}$ the graph*

$$(V(G), \{e \in E(G) \mid c(e) \notin I\})$$

has at most $|I| + 1$ connected components.

Proof: Let $(E(G), \mathcal{F}_1)$ be the cycle matroid of G and $(E(G), \mathcal{F}_2)$ be the matroid given by

$$\mathcal{F}_2 = \{F \subseteq E(G) \mid c(e) \neq c(e') \text{ for all } e, e' \in F\}.$$

It is easy to see that $(E(G), \mathcal{F}_2)$ is indeed a matroid. Let r_1 and r_2 be the rank functions of $(E(G), \mathcal{F}_1)$ and $(E(G), \mathcal{F}_2)$, respectively. A rainbow tree exists if and only if there is a set $X \in \mathcal{F}_1 \cap \mathcal{F}_2$ with $|X| \geq |V(G)| - 1$. This is the case if and only if for all $F \subseteq E(G)$, we have

$$r_1(E(G) \setminus F) + r_2(F) \geq |V(G)| - 1. \quad (8)$$

Let $F \subseteq E(G)$. We have $r_1(E(G) \setminus F) = |V(G)| - \kappa(G - F)$ where $\kappa(G - F)$ is the number of components in $(V(G), E(G) \setminus F)$. Moreover, $r_2(F) = |\{i \in \{1, \dots, k\} \mid \exists e \in F : c(e) = i\}|$. Let $I = \{i \in \{1, \dots, k\} \mid \exists e \in F : c(e) = i\}$. We can assume that $F = \{e \in E(G) \mid c(e) \in I\}$. Then (8) is equivalent to

$$|V(G)| - \kappa(G - F) + |I| \geq |V(G)| - 1,$$

which is equivalent to $\kappa(G - F) \leq |I| + 1$.

□

6.5 Matroid Partitioning

Definition 31 Let $(E, \mathcal{F}_1), \dots, (E, \mathcal{F}_k)$ be matroids. A set $X \subseteq E$ is called **partitionable** if there exists a partition $X = X_1 \dot{\cup} \dots \dot{\cup} X_k$ with $X_i \in \mathcal{F}_i$ for $i \in \{1, \dots, k\}$. Let $\mathcal{F}$ be the set of partitionable subsets of E . Then $(E, \mathcal{F})$ is called the **union** or **sum** of $(E, \mathcal{F}_1), \dots, (E, \mathcal{F}_k)$.

Note that some authors do not demand that the k matroids have the same ground set E but each matroid has its own set E_i ($i \in \{1, \dots, k\}$). In that case, the ground set of the union is $\bigcup_{i=1}^k E_i$.

MATROID PARTITIONING PROBLEM

Instance: Matroids $(E, \mathcal{F}_1), \dots, (E, \mathcal{F}_k)$, given by independence oracles.

Task: Find a partitionable set $F \subseteq E$ such that $|F|$ is maximum.

Theorem 97 (Nash-Williams [1967]): Let $(E, \mathcal{F}_1), \dots, (E, \mathcal{F}_k)$ be matroids with rank functions $r_1, \dots, r_k$ and let $(E, \mathcal{F})$ be their union. Then $(E, \mathcal{F})$ is a matroid, and its rank function is given by

$$r(X) = \min_{A \subseteq X} \left(|X \setminus A| + \sum_{i=1}^k r_i(A) \right)$$

for all $X \subseteq E$.

Proof: $(E, \mathcal{F})$ is obviously an independence system.

Claim: For all $X \subseteq E$ we have $r(X) = \min_{A \subseteq X} \left(|X \setminus A| + \sum_{i=1}^k r_i(A) \right)$.

Proof of the claim: “ $\leq$ ” Let $X \subseteq E$. For any $Y \subseteq X$ such that Y is partitionable, i.e. $Y = Y_1 \dot{\cup} \dots \dot{\cup} Y_k$ with $Y_i \in \mathcal{F}_i$ ($i \in \{1, \dots, k\}$), and any $A \subseteq X$ we have

$$|Y| = |Y \setminus A| + |Y \cap A| \leq |X \setminus A| + \sum_{i=1}^k |Y_i \cap A| \leq |X \setminus A| + \sum_{i=1}^k r_i(A),$$

so $r(X) \leq \min_{A \subseteq X} \left(|X \setminus A| + \sum_{i=1}^k r_i(A) \right)$.

“ $\geq$ ” Let $X' := X \times \{1, \dots, k\}$. We define two matroids on X' . For $Q \subseteq X'$ and $i \in \{1, \dots, k\}$, let $Q_i := \{e \in X \mid (e, i) \in Q\}$. Moreover let

$$\mathcal{G}_1 := \{Q \subseteq X' \mid Q_i \in \mathcal{F}_i \text{ for all } i \in \{1, \dots, k\}\}$$

and

$$\mathcal{G}_2 := \{Q \subseteq X' \mid Q_i \cap Q_j = \emptyset \text{ for all } i, j \in \{1, \dots, k\} \text{ with } i \neq j\}.$$

It is easy to see that $(X', \mathcal{G}_1)$ and $(X', \mathcal{G}_2)$ are matroids, and their rank functions are given by $s_1(Q) = \sum_{i=1}^k r_i(Q_i)$ and $s_2(Q) = |\bigcup_{i=1}^k Q_i|$ for $Q \subseteq X'$. Then the family of partitionable subsets of X can be written as

$$\{A \subseteq X \mid \text{there is a function } f : A \rightarrow \{1, \dots, k\} \text{ with } \{(e, f(e)) \mid e \in A\} \in \mathcal{G}_1 \cap \mathcal{G}_2\}.$$

So the maximum cardinality of a partitionable set is the maximum cardinality of a set in $\mathcal{G}_1 \cap \mathcal{G}_2$. By Theorem 92, we have

$$\max\{|Y| \mid Y \in \mathcal{G}_1 \cap \mathcal{G}_2\} = \min\{s_1(Q) + s_2(X' \setminus Q) \mid Q \subseteq X'\}.$$

Let $Q \subseteq X'$ be a set where the minimum in this inequality is attained. Then for $A := Q_1 \cap \dots \cap Q_k$, we have

$$r(X) = s_1(Q) + s_2(X' \setminus Q) = \sum_{i=1}^k r_i(Q_i) + \left| X \setminus \bigcap_{i=1}^k Q_i \right| \geq \sum_{i=1}^k r_i(A) + |X \setminus A|.$$

So we have found a set $A \subseteq X$ with $r(X) \geq |X \setminus A| + \sum_{i=1}^k r_i(A)$. $\square$ **Claim**

Finally, we show that r is submodular. By Theorem 76, this implies that $(E, \mathcal{F})$ is a matroid. To show the submodularity, let $X, Y \subseteq E$ and $A \subseteq X$, $B \subseteq Y$ with $r(X) = |X \setminus A| + \sum_{i=1}^k r_i(A)$ and $r(Y) = |Y \setminus B| + \sum_{i=1}^k r_i(B)$. Then, by using submodularity of the rank function $r_1, \dots, r_k$, we get

$$\begin{aligned} r(X) + r(Y) &= |X \setminus A| + |Y \setminus B| + \sum_{i=1}^k (r_i(A) + r_i(B)) \\ &\geq |(X \cup Y) \setminus (A \cup B)| + |(X \cap Y) \setminus (A \cap B)| + \sum_{i=1}^k (r_i(A \cup B) + r_i(A \cap B)) \\ &\geq r(X \cup Y) + r(X \cap Y). \end{aligned}$$

$\square$

Theorem 98 *There is a polynomial-time algorithm for the MATROID PARTITIONING PROBLEM, provided that there are polynomial-time independence oracles for the input matroids $(E, \mathcal{F}_1), \dots, (E, \mathcal{F}_k)$.*

Proof: The matroid $(X', \mathcal{G}_1)$ from the previous proof has a polynomial-time independence oracle if the single matroids $(E, \mathcal{F}_1), \dots, (E, \mathcal{F}_k)$ have one. And for the matroid $(X', \mathcal{G}_2)$, there is a trivial polynomial-time independence oracle. Therefore, the corresponding MATROID INTERSECTION PROBLEM can be solved in polynomial time and thus also the MATROID PARTITIONING PROBLEM. $\square$

We used a polynomial algorithm for the MATROID INTERSECTION PROBLEM to solve the MATROID PARTITIONING PROBLEM. The following proposition shows that it would also be

possible to use any polynomial algorithm for the MATROID PARTITIONING PROBLEM to solve the MATROID INTERSECTION PROBLEM in polynomial time.

Proposition 99 *Let $(E, \mathcal{F}_1)$ and $(E, \mathcal{F}_2)$ be two matroids. And let X be a maximum partitionable set with respect to $(E, \mathcal{F}_1)$ and $(E, \mathcal{F}_2^*)$, so in particular we have $X = X_1 \dot{\cup} X_2$ with $X_1 \in \mathcal{F}_1$ and $X_2 \in \mathcal{F}_2^*$. Moreover, let $B_2^* \supseteq X_2$ be a basis of $\mathcal{F}_2^*$. Then $X \setminus B_2^*$ is a maximum-cardinality set in $\mathcal{F}_1 \cap \mathcal{F}_2$.*

Proof: We have $B_2^* \subseteq X$ since any element of $B_2^* \setminus X$ could have been added to X_2 , which would have increased X .

We have $X \setminus B_2^* \subseteq X_1$, so $(X \setminus B_2^*) \in \mathcal{F}_1$. Moreover, since $(E \setminus B_2^*) \in \mathcal{F}_2$, we also have $X \setminus B_2^* \in \mathcal{F}_2$. Therefore, we have $X \setminus B_2^* \in \mathcal{F}_1 \cap \mathcal{F}_2$.

Let $S \in \mathcal{F}_1 \cap \mathcal{F}_2$, and let $B \supseteq S$ be a basis of $\mathcal{F}_2$. In addition, let $B^* = E \setminus B$ and $Z = S \dot{\cup} B^*$. By the maximality of X , we have $|Z| \leq |X|$ and thus

$$|S| = |Z| - |B^*| = |Z| - |B_2^*| \leq |X| - |B_2^*| = |X \setminus B_2^*|. \quad \square$$

WEIGHTED MATROID PARTITIONING PROBLEM

Instance: Matroids $(E, \mathcal{F}_1), \dots, (E, \mathcal{F}_k)$, given by independence oracles.

Weights $c : E \rightarrow \mathbb{R}_{\geq 0}$.

Task: Find a partitionable set $X \subseteq E$ such that $c(X) := \sum_{e \in X} c(e)$ is maximum.

Theorem 100 *There is a polynomial-time algorithm for the WEIGHTED MATROID PARTITIONING PROBLEM, provided that there are polynomial-time independence oracles for the input matroids $(E, \mathcal{F}_1), \dots, (E, \mathcal{F}_k)$.*

Proof: Since the union $(E, \mathcal{F})$ of the matroids $(E, \mathcal{F}_1), \dots, (E, \mathcal{F}_k)$ is again a matroid, we can apply the BEST-IN-GREEDY ALGORITHM to solve the WEIGHTED MATROID PARTITIONING PROBLEM. It has polynomial running time if there is an independence oracle for $(E, \mathcal{F})$. However, this is the case because in the proof of Theorem 97 we have seen that we can compute the rank of a set $F \subseteq E$ (with respect to $(E, \mathcal{F})$) using the algorithm for matroid intersection. But if we know the rank of a set, we can also decide if it is independent. $\square$

Corollary 101 *Let $(E, \mathcal{F})$ be a matroid with rank function r , and let $k \in \mathbb{N} \setminus \{0\}$. Then the maximum size of the union of k independent sets is equal to*

$$\min_{A \subseteq E} (|E \setminus A| + k \cdot r(A)).$$

Proof: Follows directly from Theorem 97 with $(E, \mathcal{F}_1) = \dots = (E, \mathcal{F}_k) = (E, \mathcal{F})$. $\square$

Corollary 102 (*Matroid covering theorem*) Let $(E, \mathcal{F})$ be a matroid with rank function r , and let $k \in \mathbb{N} \setminus \{0\}$. Then, E can be covered by k independent sets if and only if

$$k \cdot r(A) \geq |A|$$

for all $A \subseteq E$.

Proof: The set E can be covered by k independent sets if and only if there is a union of k independent sets of size $|E|$. By the previous corollary, this is the case if and only if

$$\min_{A \subseteq E} (|E \setminus A| + k \cdot r(A)) \geq |E|$$

which holds if and only if $k \cdot r(A) \geq |A|$ holds for all $A \subseteq E$. $\square$

Corollary 103 (*Matroid base packing theorem*) Let $(E, \mathcal{F})$ be a matroid with rank function r , and let $k \in \mathbb{N} \setminus \{0\}$. Then there exist k disjoint bases if and only if

$$k \cdot (r(E) - r(A)) \leq |E \setminus A|$$

for all $A \subseteq E$.

Proof: There are k disjoint bases if the rank of E in the union of k copies of $(E, \mathcal{F})$ (i.e. the union of $(E, \mathcal{F}_1), \dots, (E, \mathcal{F}_k)$ where $\mathcal{F}_i = \mathcal{F}$ for all $i \in \{1, \dots, k\}$) is $k \cdot r(E)$. By Theorem 97, this is the case if and only if for all $A \subseteq E$ we have $(|E \setminus A| + k \cdot r(A)) \geq k \cdot r(E)$, which is equivalent to the statement of the corollary. $\square$

Now, we consider a weighted version of the MATROID INTERSECTION PROBLEM.

WEIGHTED MATROID INTERSECTION PROBLEM

Instance: Matroids $(E, \mathcal{F}_1)$ and $(E, \mathcal{F}_2)$, given by independence oracles.

Weights $c : E \rightarrow \mathbb{R}$.

Task: Find a set $X \in \mathcal{F}_1 \cap \mathcal{F}_2$ such that $c(X) := \sum_{e \in X} c(e)$ is maximum.

We will show that there is a polynomial-time algorithm for the WEIGHTED MATROID INTERSECTION PROBLEM. To this end, we will adapt Lemma 88 to a setting with weights on the elements.

Lemma 104 (Frank [1981]) Let $(E, \mathcal{F})$ be a matroid, $c : E \rightarrow \mathbb{R}$, and $X \in \mathcal{F}$. Let $x_1, \dots, x_l \in X$ and $y_1, \dots, y_l \in E \setminus X$ with

(a) $x_j \in C(X, y_j)$ and $c(x_j) = c(y_j)$ for $j = 1, \dots, l$, and

(b) $x_i \notin C(X, y_j)$ or $c(x_i) > c(y_j)$ for $1 \leq i < j \leq l$, and

(c) $x_i \notin C(X, y_j)$ or $c(x_i) \geq c(y_j)$ for $1 \leq j < i \leq l$.

Then $(X \setminus \{x_1, \dots, x_l\}) \cup \{y_1, \dots, y_l\} \in \mathcal{F}$.

Proof: We apply induction on l . For $l = 1$, the statement follows from condition (a).

For $l > 1$, let $\mu = \min\{c(x_i) \mid i \in \{1, \dots, l\}\}$, and $h = \min\{i \in \{1, \dots, l\} \mid c(x_i) = \mu\}$. Let $X' := (X \setminus \{x_h\}) \cup \{y_h\}$. Then, by (a), $X' \in \mathcal{F}$.

Claim: $C(X', y_j) = C(X, y_j)$ for all $j \in \{1, \dots, l\} \setminus \{h\}$.

Proof of the claim: Assume that there is a $j \in \{1, \dots, l\} \setminus \{h\}$ with $C(X', y_j) \neq C(X, y_j)$. Then $x_h \in C(X, y_j)$. If $h < j$ then

$$\mu = c(x_h) \stackrel{(b)}{>} c(y_j) \stackrel{(a)}{=} c(x_j),$$

which contradicts the definition of μ . If $h > j$ then

$$\mu = c(x_h) \stackrel{(c)}{\geq} c(y_j) \stackrel{(a)}{=} c(x_j),$$

which contradicts the definition of h . $\square$ **Claim**

The claim implies that the conditions (a), (b), and (c) also hold for X' , and the indices $\{1, \dots, l\} \setminus \{h\}$. Thus, the statement follows by induction. $\square$

The main strategy of the algorithm works as follows. Starting with an empty set X_0 , we compute a sequence $X_0, \dots, X_m$ with $m = \max\{|F| \mid F \in \mathcal{F}_1 \cap F_2\}$ such that $|X_k| = k$ and $X_k \in \mathcal{F}_1 \cap F_2$ for all $k \in \{0, \dots, m\}$. Moreover, we always guarantee that

$$c(X_k) = \max\{c(F) \mid F \in \mathcal{F}_1 \cap F_2, |F| = k\}. \quad (9)$$

Then, we only have to find an index $k \in \{0, \dots, m\}$ with $c(X_k) = \max\{c(X_j) \mid j \in \{0, \dots, m\}\}$. The question is how we can enforce Eq. (9). We want to use Theorem 84 but this only holds for a single matroid. Therefore, we split up the weight function $c : E \rightarrow \mathbb{R}$ into two functions $c_1 : E \rightarrow \mathbb{R}$ and $c_2 : E \rightarrow \mathbb{R}$ such that $c(e) = c_1(e) + c_2(e)$ for all $e \in E$. If we now can enforce that we have

$$c_i(X_k) = \max\{c_i(F) \mid F \in \mathcal{F}_i, |F| = k\} \quad (10)$$

for all $k \in \{0, \dots, m\}$ and $i \in \{1, 2\}$, then this implies Eq. (9) for all $k \in \{0, \dots, m\}$. Of course for arbitrary weights c_1 and c_2 there is, in general, no set X_k with 10, but we are allowed to modify c_1 and c_2 in each iteration (as long as we guarantee $c(e) = c_1(e) + c_2(e)$ for all $e \in E$).

Algorithm 4: Weighted Matroid Intersection Algorithm

Input: Matroids $(E, \mathcal{F}_1), (E, \mathcal{F}_2)$ (by indep. oracles), weights $c : E \rightarrow \mathbb{R}$.

Output: A set $X \in \mathcal{F}_1 \cap \mathcal{F}_2$ of maximum weight.

1 Set $k := 0$ and $X_0 := \emptyset$. Set $c_1(e) := c(e)$ and $c_2(e) := 0$ for all $e \in E$

2 **for** $y \in E \setminus X_k$ **and** $i \in \{1, 2\}$ **do**

$\perp$ Compute $C_i(X_k, y) := \{x \in X_k \cup \{y\} \mid X_k \cup \{y\} \notin \mathcal{F}_i, (X_k \cup \{y\}) \setminus \{x\} \in \mathcal{F}_i\}$.

3 Compute

$$A^{(1)} := \{(x, y) \mid y \in E \setminus X_k, x \in C_1(X_k, y) \setminus \{y\}\},$$

$$A^{(2)} := \{(y, x) \mid y \in E \setminus X_k, x \in C_2(X_k, y) \setminus \{y\}\},$$

$$S := \{y \in E \setminus X_k \mid X_k \cup \{y\} \in \mathcal{F}_1\},$$

$$T := \{y \in E \setminus X_k \mid X_k \cup \{y\} \in \mathcal{F}_2\}.$$

4 Compute

$$m_1 := \max\{c_1(y) \mid y \in S\},$$

$$m_2 := \max\{c_2(y) \mid y \in T\},$$

$$\bar{S} := \{y \in S \mid c_1(y) = m_1\},$$

$$\bar{T} := \{y \in T \mid c_2(y) = m_2\},$$

$$\bar{A}^{(1)} := \{(x, y) \in A^{(1)} \mid c_1(x) = c_1(y)\},$$

$$\bar{A}^{(2)} := \{(y, x) \in A^{(2)} \mid c_2(x) = c_2(y)\},$$

$$\bar{G} := (E, \bar{A}^{(1)} \cup \bar{A}^{(2)}).$$

5 Compute (with BFS) the set R of nodes reachable from $\bar{S}$ in $\bar{G}$.

6 **if** $R \cap \bar{T} \neq \emptyset$ **then**

$\perp$ find an $\bar{S}$ - $\bar{T}$ -path P in $\bar{G}$ with minimum number of edges, set $X_{k+1} := X_k \Delta V(P)$ and
 $k := k + 1$ and **goto** 2

7 Compute

$$\varepsilon_1 := \min\{c_1(x) - c_1(y) \mid (x, y) \in \delta_{A^{(1)}}^+(R)\},$$

$$\varepsilon_2 := \min\{c_2(x) - c_2(y) \mid (y, x) \in \delta_{A^{(2)}}^+(R)\},$$

$$\varepsilon_3 := \min\{m_1 - c_1(y) \mid y \in S \setminus R\},$$

$$\varepsilon_4 := \min\{m_2 - c_2(y) \mid y \in T \cap R\},$$

$$\varepsilon := \min\{\varepsilon_1, \varepsilon_2, \varepsilon_3, \varepsilon_4\}.$$

8 **if** $\varepsilon < \infty$ **then**

$\perp$ set $c_1(x) := c_1(x) - \varepsilon$ and $c_2(x) := c_2(x) + \varepsilon$ for all $x \in R$. **goto** 4.

if $\varepsilon = \infty$ **then**

$\perp$ let X be a maximum-weight set among $X_0, X_1, \dots, X_k$.

9 **return** X .

Theorem 105 (*Frank [1981]*) *The WEIGHTED MATROID INTERSECTION ALGORITHM solves the WEIGHTED MATROID INTERSECTION PROBLEM in time $O(|E|^4 + |E|^3\theta)$, where θ is the maximum running time of the two independence oracles.*

Proof: See the proof of Theorem 13.36 in Korte and Vygen [2018]. □

Remark: The running time can be improved to $O(|E|^3\theta)$. To see this, note that between two consecutive augmentations of the set X_k , in all iterations of the loop of the steps 4 to 8, the set R can only get larger. This means we don't have to run a new graph scan in each iteration. Instead, we only have to check which elements are added to R in each iteration. If $\epsilon = \epsilon_3$ then in the next iteration, we have $R \cap \bar{T} \neq \emptyset$, so we will augment X_k to X_{k+1} . In any other case, R grows by at least one element. In order to find the elements that have to be added to R , we store for each $x \in X \setminus R$, the value $\gamma(x) = \min\{c_2(x) - c_2(y) \mid (y, x) \in \delta_{A(2)}^+(R)\}$, and for each $y \in (E \setminus X) \setminus R$, the value $\gamma(y) = \min\{c_1(x) - c_1(y) \mid (x, y) \in \delta_{A(1)}^+(R)\}$. When the weights are modified in step 8, these additional values can be updated in linear time. Moreover, we can find in linear time all nodes that have to be added to R (of course, we also check if we have to add elements from $S \setminus R$ to $\bar{S}$ and thus to R). And when we add an element to R we can scan all its outgoing edges in linear time to check if they modify the γ -values of any node. For this purpose, we only have to check each edge at most once between two augmentations. Therefore, the whole computation of the set R between two augmentations can be done in time $O(|E|^2)$. And when $R \cap \bar{T} \neq \emptyset$, we can simply run a BFS search to find a shortest $\bar{S}$ - $\bar{T}$ -path (and we know that there exists one).

Bibliography

- Aigner, M. [2007]: *Discrete Mathematics*. Vieweg, 2007.
- Allenby, R.B.J.T., Slomson, A. [2011]: *How to count. An Introduction to Combinatorics*. CRC Press. Second edition, 2011.
- Appel, K., Haken, W. [1977a]: *Every planar map is four colorable. Part I. Discharging*. Illinois J. Math. 21, 429–490, 1977.
- Appel, K., Haken, W. [1977b]: *Every planar map is four colorable. Part II. Reducibility*. Illinois J. Math. 21, 491–567, 1977.
- Appel, K., Haken, W. [1989]: *Every planar map is four colorable*. Contemporary Math. 98, 1989.
- Beeler, R.A. [2015]: *How to Count. An Introduction to Combinatorics and Its Applications*. Springer, 2015.
- Bickle, A. [2020]: *Fundamentals of Graph Theory*. American Mathematical Society, 2020.
- Blikstad, J. [2021]: *Breaking $O(nr)$ for Matroid Intersection*. 48th International Colloquium on Automata, Languages, and Programming (ICALP 2021), 31, 1-17, 2021.
- Blikstad, J., van den Brand, J., Mukhopadhyay, S., Nanongkai, D. [2021]: *Breaking the quadratic barrier for matroid intersection*. 53rd Annual ACM SIGACT Symposium on Theory of Computing (STOC), 421–432, 2021.
- Bollobás, B. [1979]: *Graph Theory – An Introductory Course*. Springer, 1979.
- Brooks, R.L. [1941]: *On coloring the nodes of a network*. Proceedings of the Cambridge Philosophical Society 37, 194–197, 1941.
- Chakrabarty, D., Lee, Y.T., Sidford, A., Singla, S., Wong, S.C.-W. [2019]: *Faster Matroid Intersection*. IEEE 60th Annual Symposium on Foundations of Computer Science (FOCS), 1146–1168, 2019.
- Chao, C.-Y., Whitehead, Jr., E.G., [1979]: *Chromatically unique graphs*. Discrete Mathematics 27 (1979), 171–177.
- Chudnovsky, M., Cornuéjols, G., Liu, X., Seymour, P., Vušković, K. [2005]: *Recognizing Berge graphs*. Combinatorica, 25 (2), 143–186, 2005.
- Chudnovsky, M., Robertson, N., Seymour, P., Thomas, R. [2006]: *The strong perfect graph theorem*. Annals of Mathematics, 164, 51–229, 2006.
- Cunningham, W.H. [1986]: *Improved Bounds for Matroid Partition and Intersection Algorithms*. SIAM Journal on Computing, 15 (4), 948–957, 1986.
- Diestel, R. [2017]: *Graph Theory*. Fifth edition, Springer, 2017.

- Edmonds, J. [1970]: *Submodular functions, matroids, and certain polyhedra*. In: Combinatorial Structures and Their Applications; Proceedings of the Calgary International Conference on Combinatorial Structures and Their Applications 1969 (R. Guy, H. Hanani, N. Sauer, J. Schenheim, eds.), Gordon and Breach, New York, 69–87, 1970.
- Edmonds, J. [1971]: *Matroids and the greedy algorithm*. Mathematical Programming 1, 127–136, 1971.
- Erdős, P., Rubin, A.L., Taylor, H. [1979]: *Choosability in graphs*. West Coast Conference on Combinatorics, Graph Theory and Computing, Arcata, CA, 125–157, 1979.
- Frank, A. [1981]: *A weighted matroid intersection algorithm*. Journal of Algorithms 2, 328–336, 1981.
- Galvin, F. [1995]: *The list chromatic index of a bipartite multigraph*. Journal of Combinatorial Theory, Series B, 63, 353–358, 1995.
- Grötschel, M., Lovász, L., Schrijver, A. [1984]: *Polynomial algorithms for perfect graphs*. Annals of Discrete Mathematics, 21, 325–356, 1984.
- Heawood, P. [1890]: *Map-Colour Theorem*. Quarterly Journal of Pure and Applied Mathematics, Oxford, volume 24, 332–338, 1890.
- Hougardy, S., Vygen, J. [2016]: *Algorithmic Mathematics*. Springer, 2016.
- Jacobs, K., Jungnickel, D. [2004]: *Einführung in die Kombinatorik*. 2nd edition. De Gruyter, 2004.
- Jenkyns, T.A. [1976]: *The efficiency of the greedy algorithm*. Proceedings of the 7th S-E Conference on Combinatorics, Graph Theory, and Computing, Utilitas Mathematica, Winnipeg, 341–350, 1976.
- Kainen, P. [1974]: *A generalization of the 5-color theorem*. Proceedings of the American Mathematical Society, volume 45, 95–98, 1974.
- König, D. [1916]: *Über Graphen und ihre Anwendung auf Determinantentheorie und Mengenlehre*. Mathematische Annalen, 77, 453–465, 1916.
- Korte, B., Hausmann, D. [1978]: *An analysis of the greedy algorithm for independence systems*. In: Algorithmic Aspects of Combinatorics; Annals of Discrete Mathematics 2 (B. Alspach, P. Hell, D.J. Miller, eds.), North-Holland, Amsterdam, 65–74, 1978.
- Korte, B., Monma, C.L. [1979]: *Some remarks on a classification of oracle-type algorithms*. In: Numerische Methoden bei graphentheoretischen und kombinatorischen Problemen; Band 2 (L. Collatz, G. Meinardus, W. Wetterling, eds.), Birkhäuser, Basel, 195–215, 1979.
- Korte, B., Vygen, J. [2018]: *Combinatorial Optimization. Theory and Algorithms*. 6th edition. Springer, 2018.

- Krumke, S.O., Noltemeier, H. [2005]: *Graphentheoretische Konzepte und Algorithmen*. Teubner, 2005.
- Kuratowski, K. [1930]: *Sur le problème des courbes gauches en topologie*. *Fundamenta Mathematicae*, 15, 271–283, 1930.
- Lee, Y.T., Sidford, A., Wong, S.C.-W. [2015]: *A faster cutting plane method and its implications for combinatorial and convex optimization*. 2015 IEEE 56th Annual Symposium on Foundations of Computer Science (FOCS), 1049–1065, 2015.
- Lovász, L. [1972a]: *Normal hypergraphs and the perfect graph conjecture*. *Discrete Mathematics*, 2 (3): 253–267, 1972.
- Lovász, L. [1972b]: *A characterization of perfect graphs*. *Journal of Combinatorial Theory, Series B*, 13 (2): 95–98, 1972.
- Loehr, N.A. [2011]: *Bijjective Combinatorics*. CRC Press, 2011.
- Matoušek, J., Nešetřil, J. [2008]: *Invitation to Discrete Mathematics*. 2nd edition. Oxford University Press, 2008.
- Mazur, D.R. [2010]: *Combinatorics. A Guided Tour*. Mathematical Association of America, 2010.
- Meredith, G.H.J. [1972]: *Coefficients of chromatic polynomials*. *Journal of Combinatorial Theory (B)* 13, 14–17, 1972.
- Nash-Williams, C.S.J.A. [1967]: *An application of matroids to graph theory*. In: *Theory of Graphs; Proceedings of an International Symposium in Rome 1966* (P. Rosenstiehl, ed.), Gordon and Breach, New York, 263–265, 1967.
- Nešetřil, J., Rödl, V. [1979]: *A short proof of the existence of highly chromatic hypergraphs without short cycles*. *Journal of Combinatorial Theory, Series B*, 27, 225–227, 1979.
- Nordhaus, E.A., Gaddum, J.W. [1956]: *On complementary graphs*. *The American Mathematical Monthly*, Vol. 63, 3, 175–177, 1956.
- Oxley, J. [1992]: *Matroid Theory*. Oxford University Press, 1992.
- Rado, R. [1957]: *Note on independence functions*. *Proceedings of the London Mathematical Society* 7, 300–320, 1957.
- Ramsey, F.P. [1930]: *On a problem of formal logic*. *Proceedings of the London Mathematical Society* 2, volume 30, 264–286, 1930.
- Robertson, N., Sanders, D., Seymour, P., Thomas, R. [1997]: *The four-color theorem*. *Journal of Combinatorial Theory, Series B*, 70, 2–44, 1997.
- Schrijver, A. [2003]: *Combinatorial Optimization. Polyhedra and Efficiency*. Springer, 2003.

- Stanley, R.P. [1973]: *Acyclic orientations of graphs*. Discrete Mathematics, 5, 171–178, 1973.
- Steger, A. [2007]: *Diskrete Strukturen. Band 1. Kombinatorik – Graphentheorie – Algebra*. 2nd edition. Springer, 2007.
- Thomassen, C. [1980]: *Planarity and duality of finite and infinite graphs*. Journal of Combinatorial Theory B, 29, 244–271, 1980.
- Thomassen, C. [1994]: *Every planar graph is 5-choosable*. Journal of Combinatorial Theory, Series B, 62, 180–181, 1994.
- Thomassen, C. [2003]: *A short list color proof of Grötzsch’s theorem*. Journal of Combinatorial Theory, Series B, 88, 189–192, 2003.
- Tittmann, P. [2014]: *Einführung in die Kombinatorik*. 2nd edition, Springer Spektrum, 2014.
- Tutte, W. [1961]: *A theory of 3-connected graphs*. Proceedings of the Koninklijke Nederlandse Akademie van Wetenschappen A, 64, 441–455, 1961.
- Vizing, V.G. [1964]: *On an estimate of the chromatic class of a p -graph*. (in Russian) Metody Discret Analiz., 3, 25–30, 1964.
- Vizing, V.G. [1976]: *Coloring the vertices of a graph with prescribed colours*. (in Russian) Metody Discret Analiz., 29, 3–10, 1976.
- Wagner, K. [1937]: *Über eine Eigenschaft der ebenen Komplexe*. Mathematische Annalen, 114, 570–590, 1937.
- Welsh, D.J.A. [1976]: *Matroid Theory*. Academic Press, London, 1976.
- Woodall, D.R., Wilson, R.J. [1978]: *The Appel-Haken proof of the four-color theorem*. In: Beineke, L.W., Wilson, R.J. (eds.): Selected Topics in Graph Theory, Academic Press, 1978, 83–101.
- Whitney, H. [1932]: *Non-separable and planar graphs*. Transactions of the American Mathematical Society, 34, 339–362, 1932.

Index

- Antiderivative, 22
- Backward difference operator, 21
- Basis, 64
- Basis of a set, 64
- Basis oracle, 77
- Basis sequence, 25
- BEST-IN-GREEDY ALGORITHM, 76
- Binet's formula, 33
- Binomial coefficient, 5, 10
- Binomial convolution, 36
- Binomial inversion, 28
- Binomial theorem, 7
- Bridge, 62
- Brooks' Theorem, 48
- Chromatic index, 59
- Chromatic number, 47
- Chromatic polynomial, 54
- Circuit, 64
- Circuit oracle, 77
- Class 1 of graphs, 60
- Class 2 of graphs, 60
- Clique, 17
- Closed Jordan curve, 38
- Closure, 64
- Closure oracle, 77
- Color-list, 57
- Complement of a graph, 50
- Configuration, 50
- Connected region, 38
- Connection coefficient, 26
- Contracting sets of nodes, 43
- Convolution, 30
- Cycle matroid, 67
- Cycle of a permutation, 11
- Dependent set, 64
- Derangement number, 15
- Dual, 74
- Ear, 41
- Ear-decomposition, 41
- Edge coloring, 59
- Edge-chromatic number, 59
- EDMONDS' MATROID INTERSECTION ALGORITHM, 84
- Edmonds-Rado Theorem, 79
- Euler's formula, 41
- Exponential generating function, 36
- Face, 39
- Falling factorial, 8, 9
- Fibonacci number, 31
- Forward difference operator, 21
- Four Color Theorem, 50
- Generating function, 30
- Girth, 43
- Golden Ratio, 33
- Graphic matroid, 67
- HAMILTON-PATH PROBLEM, 85
- Harmonic number, 12
- Inclusion-exclusion principle, 14
- Indefinite sum, 22
- Independence oracle, 76
- Independence system, 64
- Independent set, 64
- Index transformation, 20
- Induced subgraph, 52
- Intersection of matroids, 81
- Inverse of a generating function, 30
- Isolating terms, 20
- Isomorphic graphs, 43
- Isomorphic matroids, 67
- Jordan curve theorem, 39
- k -chromatic graph, 47
- k -connected graph, 41
- k -edge-connected graph, 41
- k -regular graph, 61
- König's Theorem, 60

Kuratowski-Wagner Theorem, 46
 Line graph, 59
 List-chromatic conjecture, 63
 List-chromatic index, 63
 List-chromatic number, 57
 Loop, 38
 Lower rank, 68
 Matroid, 66
 MATROID INTERSECTION PROBLEM, 82
 MATROID PARTITIONING PROBLEM, 87
 MAXIMIZATION PROBLEM FOR INDEPENDENCE SYSTEMS, 65
 MAXIMUM WEIGHT STABLE SET PROBLEM, 65
 MAXIMUM-WEIGHT FOREST PROBLEM, 65
 MAXIMUM-WEIGHT MATCHING PROBLEM, 66
 MINIMIZATION PROBLEM FOR INDEPENDENCE SYSTEMS, 65
 MINIMUM SPANNING TREE PROBLEM, 65
 Minor, 44
 Multiset, 8
 n -set, 4
 Nearly triangulated graphs, 58
 Newton representation of polynomials, 24
 Oracle, 76
 Ordered number partition, 8
 Outer face, 39
 Partial fraction decomposition, 32
 Partial summation, 24
 Partitionable set, 87
 Pascal's triangle, 6
 Perfect graphs, 52
 Pigeonhole principle, 17
 Planar dual, 40
 Planar embedding, 39
 Planar graph, 39
 Polygon, 38
 Polygonal arc, 38
 Polynomially equivalent, 77
 Power set, 5
 Principle of doubly counting, 15
 Proper ear-decomposition, 41
 Ramsey numbers, 18
 Ramsey's Theorem, 18
 Rank, 64
 Rank oracle, 77
 Rank quotient, 68
 Reducible configuration, 50
 Reflected polynomial, 34
 regular graph, 61
 Representable matroid, 67
 Rising factorial, 8, 9
 Set system, 64
 SHORTEST PATH PROBLEM, 65
 Simple Jordan curve, 38
 Simultaneous recursion, 34
 Spanning set, 85
 Stable set, 17
 Standard embedding, 40
 Stirling inversion, 27
 Stirling number of the first kind, 11
 Stirling number of the second kind, 7
 Strong perfect graph theorem, 53
 Submodular function, 71
 Sum of matroids, 87
 Translation operator, 20
 Type of a permutation, 13
 Unavoidable set of configurations, 50
 Uniform matroid, 67
 Union of matroids, 87
 Vandermonde identity, 10
 Vector matroid, 67
 Vertex coloring, 47
 Vertex cover, 80
 Vertex-list-coloring, 57
 Vizing's Theorem, 59
 Weak perfect graph theorem, 53
 WEIGHTED MATROID INTERSECTION PROBLEM, 90

WEIGHTED MATROID PARTITIONING PROBLEM, 89
WORST-OUT-GREEDY ALGORITHM, 77, 85