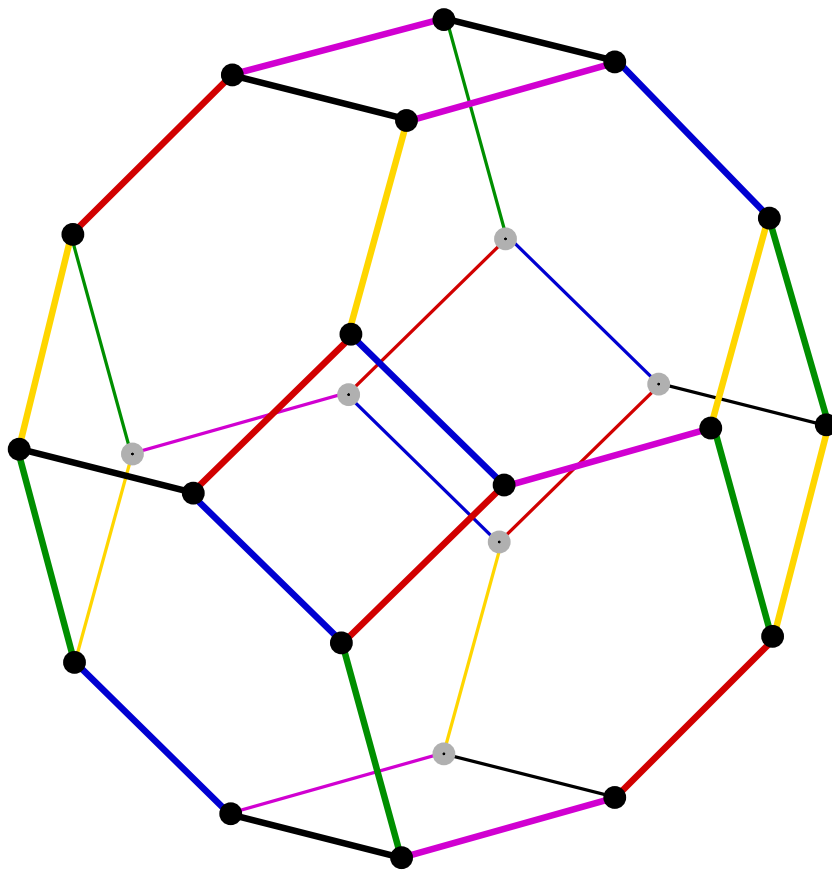


Combinatorics

Diskrete Strukturen I

Students Transcript

of Lectures by **Stefan Felsner**
in the Summer Semester 2021
at Technische Universität Berlin



Preface

At the Math department of TU Berlin I am responsible for the courses in the study focus Discrete Structures (DS). The first course is Combinatorics, it is listed as a *basic course* by the Berlin Mathematical School (BMS) and must therefore be taught in English. The second course in the DS series is Graph Theory, depending on the audience this course is in English or in German. In the winter 2013/14 students from my course Graphentheorie converted their notes into a latex book with lecture notes.

In April 2021 a group of students started a project on overleaf aiming at a similar latex book for the Combinatorics course held in the summer term of 2021. In the order of their final contribution the students are Dario Cavallaro, Heiko Scholz, Leon Ludwig, Melanie Reihl, and Matthias Vogt. Together with my PhD student Felix Schröder who served as a teaching assistant for the course we took the chapters as provided by the students and carefully edited them to get rid of errors, improve layout and the structure of proofs, and add explanations. It took us until winter 2022 to complete the task. The result is a book of 27 chapters and 185 pages which fully covers the content of the course. The text will be valuable to those who attend a combinatorics class at TU in the future. I believe that all those who contributed can be proud on the achievement. My thanks go to Dario, Heiko, Leon, Melanie, and Matthias for their initiative and commitment and to Felix for his support during the copyedit phase.

Stefan Felsner

Berlin, 21/Dec./2022

Contents

1. Derangements	1
2. Introductory Examples II	5
2.1 Derangements (continued)	5
2.2 Euler's officers problem	9
3. Basic Counting	13
3.1 Binomial coefficients	13
3.2 Extended binomial coefficients	18
3.2.1 Extending identities	18
3.3 Counting related to permutations	22
4. Basic Counting II	24
4.1 Counting cycles of permutations (continued)	24
4.2 The expected number of cycles	27
4.3 The twelfefold way	28
4.3.1 Partitions of a set	29
5. Stirling Numbers and Integer Partitions	30
5.1 The twelfefold way (continued)	30
5.2 Stirling inversion	31
5.3 Integer partitions	32
6. Euler's Pentagonal Number Theorem	36
6.1 Fibonacci sequence	42
7. Binet's Formula and Linear Recurrences	44
7.1 Solving linear recurrences	46
8. Formal Power Series and the Symbolic Method	50
8.1 Formal power series	50
8.1.1 Composition of FPS	53
8.2 Generating functions and the symbolic method	54
9. Catalan Numbers and q-Enumeration	56
9.1 q -Enumeration	57
9.1.1 More permutation statistics	59

10. Eulerian Numbers and q-Binomial Coefficients	63
10.1 q -binomial coefficients and q -binomial theorems	65
10.1.1 Another model for q -binomial coefficients	69
11. q-Binomial Coefficients, Finite Sets and Posets	70
11.1 Finite sets and posets	72
12. Sperner's Theorem and Intersecting Families	75
12.1 Finding large intersecting sets	76
12.2 Shadows and intersecting families	79
12.3 Colex order, cascading representation and the Kruskal-Katona theorem	81
13. The Lovász Version of Kruskal-Katona	84
13.1 A second proof of the Erdős-Ko-Rado theorem	88
13.2 Symmetric chains and symmetric chain decompositions	89
14. Symmetric Chain Decompositions and Orthogonal Chain Decompositions	91
14.1 Symmetric chain decompositions	91
14.1.1 A direct construction of an SCD of Boolean lattices	92
14.1.2 Application: An estimate of Dedekind numbers	93
14.2 Orthogonal chain decompositions	96
15. Duality Theorems	98
15.1 Probability of an ordered pairs	98
15.2 Duality theorems	100
15.2.1 Dilworth's theorem	100
15.2.2 Further duality theorems	104
16. Tilings	107
16.1 Tiling boards with dominoes	108
16.2 Criteria for tilings	110
16.3 A homology criterion for the existence of tilings	114
17. Homology and the Aztec Diamond	119
17.1 Tilings with L shapes	119
17.2 The power of homology	121
18. Homotopy and Counting Tilings	125
18.1 Homotopy	125
18.2 Counting Tilings	128
19. Aztec Tiling Continued	132
19.1 Schröder paths and Schröder numbers	132
19.2 Lemma of Lindström Gessel-Viennot	136

20. Binet-Cauchy Formula and Pólya Theory	140
20.1 Pólya Theory	143
20.1.1 Permutation groups and group action	144
21. Pólya Theory (continued)	147
21.1 Lemma of Cauchy-Frobenius-Burnside	147
21.2 The fundamental theorem	150
22. Design Theory	152
22.1 Introduction	152
22.2 Arithmetic conditions	155
22.3 Steiner triple systems	157
23. Steiner Triple Systems and Kirkman's problem	158
23.1 Existence of Steiner Triple Systems	159
23.2 An algebraic construction of designs	160
24. Möbius Inversion	163
24.1 The incidence algebra of a poset	163
24.2 Zeta function and properties of P	164
24.3 Möbius inversion	165
24.4 Computing Möbius functions	165
24.4.1 Chains	165
24.4.2 Products	166
24.4.3 Boolean lattices	167
24.5 Möbius inversion on the Boolean lattice	167
24.6 An algorithmic application of Möbius inversion	168
25. Catalan Families	171
25.1 Catalan families and bijections	171
26. More Catalan Families	178
26.1 Derivations of the Catalan formula	178
26.1.1 Cycle Lemma	179
26.1.2 Reflection Principle	180
26.1.3 Symmetric chain decompositions	181
26.2 Narayana numbers via LGV Lemma	181
27. More Catalan Connections	185
27.1 Tamari lattice	185
27.2 The associahedron	186
27.3 The maule lattice	187
27.4 Final links and references	187

Derangements

In our first lesson we will define derangements and learn some formulas for them, which we will prove in this and subsequent lessons.

Definition 1.1 (Permutation). A *permutation* is a bijection $\pi : X \rightarrow X$ for some finite X , for example $X = [n] := \{1, 2, 3, \dots, n\}$.

We let S_n denote the *set of all permutations* of $[n]$.

From other courses we know that $|S_n| = n!$. The easiest way to write down permutations is in 2 lines:

n	1	2	3	4	5	6	7
$\pi(n)$	5	4	6	7	2	3	1

Table 1.1: 2-line notation: Since the first row is the same for every permutation, the second row determines it uniquely, yielding 1-line notation.

There is a lot you can do with permutations. The *Permutahedron* is a polytope whose vertices are exactly the permutations of S_n , their 1-line notation interpreted as vectors in \mathbb{R}^n . From a vertex we can go with an edge to neighbours by exchanging an adjacent pair of numbers, i.e., by using an adjacent transposition.

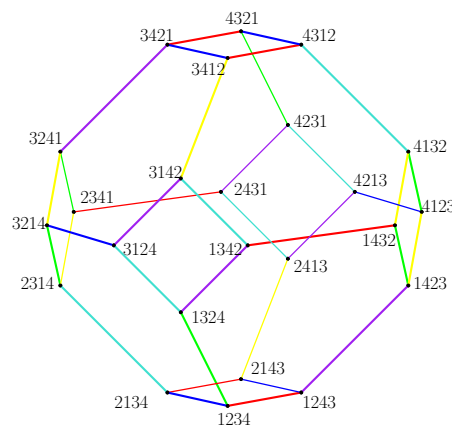


Figure 1.1: The Permutahedron of S_4

In this lecture, we will focus on permutations without fixed points:

Definition 1.2 (Fixed point). We say that $x \in [n]$ is a *fixed point* of $\pi \in S_n$ if $\pi(x) = x$.

Definition 1.3 (Derangement). A derangement is a permutation without a fixed point, and $d(n)$ is defined as the number of derangements in S_n

Example 1 (One-armed bandit). Imagine playing the following game with a machine:

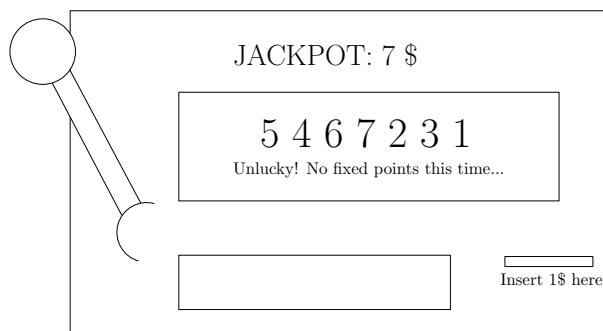


Figure 1.2: One armed bandit game: You get 1\$ for each fixed point of a permutation

Cost: You spend one dollar to the machine.

Benefit: The machine samples a permutation π uniformly at random and then gives you one dollar for each fixed point of π .

Question: What is the expected value? Do you win or lose more money?

Every $i \in [n]$ is a fixed point in $(n-1)!$ permutations. The total number of fixed points therefore is:

$$\sum_{i=1}^n (n-1)! = n(n-1)! = n!$$

Therefore the expected value is 0 dollar, which means that the game is fair.

P.R. Montmort proposed the following variant: You gain x dollar when no fixed point is in the permutation. For which x is the game fair? If you know $d(n)$, then you can calculate $x = \frac{n!}{d(n)}$, so this was Montmort's motivation for examining $d(n)$.

Next we will state several relations on $d(n)$, and dedicate the rest of this section to prove them.

Theorem 1.4. "What is $d(n)$ "?

1. Look up *encyclopedia of integer sequences*¹ and get numbers:

n	1	2	3	4	5	6	7	...
$d(n)$	0	1	2	9	44	265	1854	...

2. Recursion:

a) $d(n) = (n-1) \cdot [d(n-1) + d(n-2)],$

b) $n! = \sum_{k=1}^n \binom{n}{k} d(k).$

¹The On-Line Encyclopedia of Integer Sequences (OEIS) is a great website that gathers information about any kind of integer sequences and a good first resource to look at.

3. *Summation:*

$$d(n) = \sum_{k=1}^n \binom{n}{k} (-1)^{n+k} k!$$

4. *Explicit:*

$$d(n) = \left\lfloor \frac{n!}{e} \right\rfloor = \left\lfloor \frac{n!}{e} + \frac{1}{2} \right\rfloor.$$

5. *Asymptotics:*

$$d(n) \sim \sqrt{2\pi n} \cdot \frac{n^n}{e^{(n+1)}}.$$

6. *Generating function:*

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

Proof. 2.a of $d(n) = (n-1)[d(n-1) + d(n-2)]$ by bijection:

For the proof, we use the cycle decomposition of the permutation:

Let $\pi \in S_n$ without a fixed point, and let $x, y \in \mathbb{N}$ be such that $\pi(n) = y$ and $\pi(x) = n$.

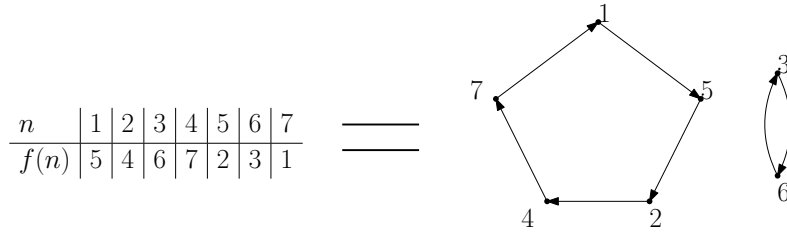


Figure 1.3: Two line representation and cycle decomposition of π .

The cycle decomposition of π has a cycle, where n is one of the vertices. We will use a proof by bijection that maps π to $(x, \tilde{\pi})$, where $x \in [n-1]$ and $\tilde{\pi}$ is a derangement on $n-1$ or $n-2$ elements. We have two cases, see [Figure 1.4](#):

- 1st case $x \neq y$:
 (left and middle of [Figure 1.4](#)).
 We can delete n and get $\tilde{\pi}$ with $\tilde{\pi}(i) = \pi(i)$ for every $i \in [n-1], i \neq x$ and $\tilde{\pi}(x) = y$, since we have $x \neq y$ it is no fixed point. Furthermore, we have to remember $x \in [n-1]$ to know where to insert n for the reverse direction.
- 2nd case $x = y$:
 (middle and right of [Figure 1.4](#)).
 If we proceed like in the 1st case, we get $\tilde{\pi}(x) = y = x$, and so we would have a fixed point (\cancel{x}). To solve this problem, we also delete x and our new $\tilde{\pi}$ is defined in two steps: first we define $a(i) = \pi(i)$ if $\pi(i) < x$ and $a(i) = \pi(i) - 1$ if $\pi(i) > x$ second we let $\tilde{\pi}(i) = a(i)$ for $0 < i < x$, and $\tilde{\pi}(i) = a(i+1)$ for $x \leq i \leq n-2$. This corresponds to deleting the 2-cycle (x, n) and replacing each $i > x$ by $i-1$ in the cycle representation of π . In the reverse direction we are given $x \in [n-1]$, hence we know which vertex is connected to n and can go from $\tilde{\pi}$ to π .

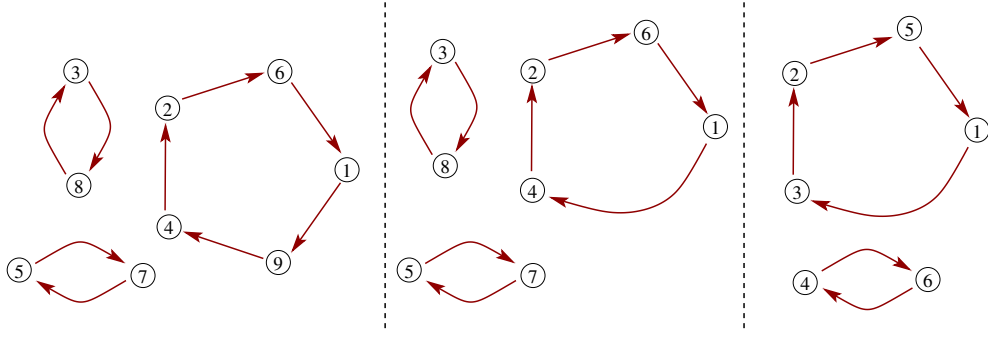


Figure 1.4: The derangement on the left is mapped with case 1 and $n = 9$ to the derangement in the middle which in turn is mapped by case 2 with $n = 8$ and $x = 3$ to the derangement on the right, now $n = 6$.

So we get

$$d(n) = \sum_{x \in [n-1]} (n-1) \cdot \left(d(n-1) + d(n-2) \right)$$

$\tilde{\pi}$ in the 1st case and 2nd case

Proof. 2.b) of $n! = \sum_{k=1}^n \binom{n}{k} d(k)$ by bijection.

Let π be a permutation of $[n]$. We denote $A := \{x \in [n] \mid \pi(x) = x\}$ and $B = [n] \setminus A$, in other words A is the set of fixed points and B contains no fixed point of π .

We define $\tilde{\pi}$ with $\tilde{\pi} : B \rightarrow B$ and $\tilde{\pi}(x) = \pi(x)$. Thus, $\tilde{\pi}$ is a derangement on $|B|$ numbers.

In total there are $\binom{n}{|A|} = \binom{n}{|B|}$ possibilities where the fixed points are, $\tilde{\pi}$ has $d(|B|)$ possibilities. Summing over each possible number k of elements of B this results in:

$$|S_n| = n! = \sum_{k=1}^n \binom{n}{k} d(k)$$

□

Introductory Examples II

In the second lecture we continue to derive the already mentioned expressions and relations for the number of derangements $d(n)$ of S_n and finish by analysing another combinatorial problem posed by Euler.

2.1 Derangements (continued)

Recall that the *derangements* of S_n are exactly the *fixed-point free permutations*. We write $d(n)$ for the number of derangements in S_n given $n \in \mathbb{N}$. In the last lecture we have seen the following relations and expressions for $d(n)$:

$$d(n) = (n-1)(d(n-1) + d(n-2)), \quad (2.1)$$

$$n! = \sum_{k=0}^n \binom{n}{k} d(k) \iff d(n) = \sum_{k=0}^n \binom{n}{k} (-1)^{n+k} k! \quad (2.2)$$

With **Theorem 1.4** we have already proven **Equation (2.1)** and the lefthand side of **Equation (2.2)**. We will continue by proving the equivalence **Equation (2.2)** which follows immediately from the *general inversion formula*.

Proposition 2.1 (General Inversion Formula). *Let $g, f : \mathbb{N} \rightarrow \mathbb{R}$ be two functions, then the following two relations are equivalent*

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

i.e. (1) holds true if and only if (2) holds true.

In order to prove **Proposition 2.1** we will use another lemma. It is convenient to introduce some simplifying notation: given a function $g : \mathbb{N} \rightarrow \mathbb{R}$ and a finite set B we write

$$g(B) := g(|B|).$$

This gives another formulation for the general inversion formula, which will be the one that we prove:

$$g(B) = \sum_{A \subseteq B} (-1)^{|A|} f(A) \iff f(B) = \sum_{A \subseteq B} (-1)^{|A|} g(A). \quad (\text{IF})$$

Lemma 2.2 (Fundamental lemma). *Let B be any finite set, then*

$$\sum_{A \subseteq B} (-1)^{|A|} = \begin{cases} 1, & B = \emptyset \\ 0, & \text{else.} \end{cases}$$

Proof. If $B = \emptyset$ the equation is trivially satisfied since $(-1)^0 = 1$, so assume $B \neq \emptyset$. Note that we may as well prove that the number of odd subsets of B is equal to the number of even subsets of B ; that is what the lemma states after all. We will prove the latter by giving a bijection between the odd and even subsets of B . To this extent fix $b \in B$ and write

$$A \boxtimes b := \begin{cases} A + b, & b \notin A \\ A - b, & b \in A. \end{cases}$$

By construction A and $A \boxtimes b$ have cardinality of different parity, and clearly for every fixed b , $A \rightarrow A \boxtimes b$ is a bijective function (since $A = (A \boxtimes b) \boxtimes b$)^{II}. Now for every even $A \subseteq B$ there is exactly one odd subset $A \boxtimes b$, giving a bijection between the even and odd subsets of B and thus proving the lemma. \square

Remark. In the case that B is of odd parity we get a bijection already from the fact that $\binom{n}{k} = \binom{n}{n-k}$ and if k is even then $n - k$ is odd, using a bijection between the k -subsets and $(n - k)$ -subsets.

We are now ready to prove **Proposition 2.1**.

Proof of Proposition 2.1. As mentioned above we will prove the theorem using the alternate formulation given in **Equation (IF)**, that is we prove

$$g(B) = \sum_{A \subseteq B} (-1)^{|A|} f(A) \Rightarrow f(C) = \sum_{B \subseteq C} (-1)^{|B|} g(B)$$

which follows from a chain of equations, that we will break up into pieces and analyse step by step.

$$\begin{aligned} \sum_{B \subseteq C} (-1)^{|B|} g(B) &= \sum_{B \subseteq C} \left((-1)^{|B|} \sum_{A \subseteq B} (-1)^{|A|} f(A) \right) \\ &= \sum_{A \subseteq C} \left((-1)^{|A|} f(A) \sum_{B: A \subseteq B \subseteq C} (-1)^{|B|} \right), \end{aligned} \tag{1}$$

where the first equality follows using our assumption on g and (1) follows by keeping track of the summed subsets. A fixed $A \subseteq C$ is counted in $(-1)^{|B|} \sum_{A \subseteq B} (-1)^{|A|} f(A)$ for each $B \subseteq C$ with $A \subseteq B$, so all in all we add up $(-1)^{|A|} f(A)$ a total of $\sum_{B: A \subseteq B \subseteq C} (-1)^{|B|}$

^{II}This shows that $A \rightarrow A \boxtimes b$ is self-inverse, i.e., an *involution*

times. If we can prove that $(1) = f(C)$ we are done. To do so we continue by examining that last term.

$$\sum_{B: A \subseteq B \subseteq C} (-1)^{|B|} = (-1)^{|A|} \sum_{B' \subseteq C \setminus A} (-1)^{|B'|} = \begin{cases} (-1)^{|C|}, & \text{if } A = C, \\ 0, & \text{else.} \end{cases}$$

The first equation follows from keeping track of the subsets we sum over, using that for fixed $A \subseteq B$ we get $(-1)^{|B|} = (-1)^{|A|}(-1)^{|B \setminus A|}$ and switching to $B' := B \setminus A \subseteq C \setminus A$ as the sum's index. The last equation follows using [Lemma 2.2](#).

Finally plugging our results into (1) we conclude that

$$(1) = \sum_{A \subseteq C} \left((-1)^{|A|} f(A) \sum_{B: A \subseteq B \subseteq C} (-1)^{|B|} \right) = 0 + \dots + 0 + (-1)^{|C|} f(C) (-1)^{|C|} = f(C),$$

and hence the proof. \square

Using part (2b) of [Theorem 1.4](#) (that is the left hand side of [Equation \(2.2\)](#)) we can deduce part (3) of [Theorem 1.4](#). For convenience we state it here again as a corollary.

Corollary 2.3. *The number of derangements $d(n)$ on S_n satisfies*

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

Next we continue to establish the explicit and asymptotical relations for $d(n)$ that were mentioned in [Theorem 1.4](#) (4, 5), that is

$$d(n) = \left\lfloor \frac{n!}{e} \right\rfloor \quad \text{and} \quad d(n) \sim \sqrt{2\pi n} \frac{n^n}{e^{n+1}}.$$

Plugging $\binom{n}{k} = \frac{n!}{k!(n-k)!}$ into our expression [Equation \(2.2\)](#) for $d(n)$ we get

$$\begin{aligned} d(n) &= \sum_{k=0}^n \binom{n}{k} (-1)^{n+k} k! = n! \sum_{k=0}^n \frac{(-1)^{n+k}}{(n-k)!} = n! \sum_{k=0}^n \frac{(-1)^{n-k}}{(n-k)!} \\ &= n! \sum_{k=0}^n \frac{(-1)^k}{k!} \longrightarrow n! e^{-1}, \end{aligned}$$

where the third equation follows since $n+k$ and $n-k$ have the same parity. One can now easily show that $d(n) = \left\lfloor \frac{n!}{e} \right\rfloor$ using the known fast convergence behavior of the exponential series. The asymptotic relation now follows from Stirling's formula for the asymptotic behaviour of the factorial, which we will not prove here:

$$n! \sim \sqrt{2\pi n} \left(\frac{n}{e}\right)^n \Rightarrow d(n) \sim \sqrt{2\pi n} \frac{n^n}{e^{n+1}}$$

The last relation on $d(n)$ that we will prove ([Theorem 1.4](#) (6)) regards its *generating function* $\sum_{k=0}^{\infty} \frac{d(n)}{n!} z^n$.

Proposition 2.4. *The exponential generating function induced by $d(n)$ satisfies*

$$\sum_{n=0}^{\infty} \frac{d(n)}{n!} z^n = \frac{e^{-z}}{1-z}.$$

Proof. Let $D(z) := \sum_{n=0}^{\infty} \frac{d(n)}{n!} z^n$ be the generating function. We can differentiate it yielding

$$D'(z) = \sum_{n=1}^{\infty} \frac{d(n)}{(n-1)!} z^{n-1} = \sum_{n=0}^{\infty} \frac{d(n+1)}{n!} z^n,$$

where the latter equality comes from an index-shift. Using a trick that turns out to be very effective we find

$$\begin{aligned} (1-z)D'(z) &= (1-z) \sum_{n=0}^{\infty} \frac{d(n+1)}{n!} z^n \\ &= \sum_{n=0}^{\infty} \frac{d(n+1)}{n!} z^n - \frac{d(n+1)}{n!} z^{n+1} \\ &= \frac{d(1)}{1} z^0 + \sum_{n=1}^{\infty} \left(\frac{d(n+1)}{n!} - \frac{d(n)}{(n-1)!} \right) z^n \\ &= 0 + \sum_{n=1}^{\infty} \left(\frac{d(n+1)}{n!} - \frac{d(n)}{(n-1)!} \right) z^n. \end{aligned} \tag{1}$$

Recalling the recursion formula [Equation \(2.1\)](#) for $d(n)$ we get

$$\frac{d(n+1)}{n!} = \frac{d(n)}{(n-1)!} + \frac{d(n-1)}{(n-1)!}.$$

Plugging this back into (1) we find

$$(1) = \sum_{n=1}^{\infty} \frac{d(n-1)}{(n-1)!} z^n = z \sum_{n=1}^{\infty} \frac{d(n-1)}{(n-1)!} z^{n-1} = z \sum_{n=0}^{\infty} \frac{d(n)}{n!} z^n = zD(z).$$

All in all this proves that $D(z)$ satisfies the differential equation

$$(1-z)D'(z) = zD(z),$$

where defined. It is a known fact that $D(z) = \frac{e^{-z}}{1-z}$ is the unique solution of this equation with start value $D(0) = 1$, concluding the proof. \square

2.2 Euler's officers problem

The following problem was posed by Euler around 1782 and conjectured to be impossible.

EULER'S OFFICER PROBLEM

Input: we are given 36 officers of 6 ranks coming from 6 different countries, such that each pair of country/rank is represented exactly once.

Question: can we place them in a table of 6 rows and 6 columns, such that every row and every column contains each country and each rank?

In 1900, Tarry proved that this problem is indeed not solvable. The question becomes more interesting when leaving the number of officers variable, that is for $k \in \mathbb{N}$ we formulate the problem as

GENERAL OFFICER PROBLEM

Input: we are given k^2 officers of k ranks coming from k different countries, such that each pair of country/rank is represented exactly once.

Question: Can we place them in a table of k rows and k columns, such that every row and every column contains each country and each rank?

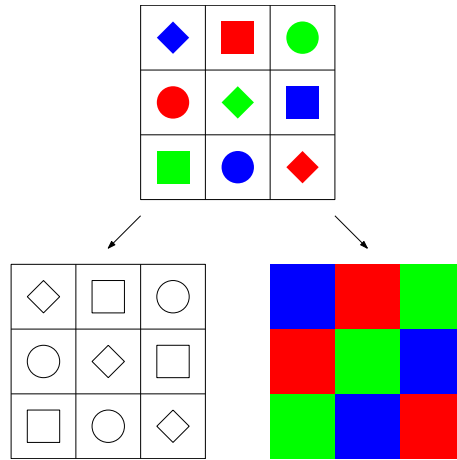


Figure 2.1: The officers and how to make orthogonal latin squares out of them: the rank is shown by the form, the countries are distinguished by color

Euler conjectured that this problem is not solvable for $k \equiv 2 \pmod{4}$. This was however disproven in 1960 by Bose, Parker and Shrikhande. To state the theorem we first develop definitions that transform our problem into mathematical language:

Definition 2.5 (Latin Square). A *latin square of order n* is a filling of an $n \times n$ table with elements of $[n]$ such that each row and each column is a permutation $\sigma \in S_n$.

Latin squares give exactly the different possible placements for the countries or ranks.

Definition 2.6 (Orthogonal latin squares). Two latin squares L_1, L_2 are said to be *orthogonal* if each of the n^2 pairs $(i, j) \in [n]^2$ appears in a cell of the tables.

What we mean here by being in a cell of the tables is that the two latin squares L_1, L_2 ought to be seen as fillings of the same table, so as an entry of the table we get a pair of elements, one from each latin square.

One easily sees that pairs of orthogonal latin squares are solutions to our previously defined officer problem.

Theorem 2.7 (Bose, Parker, Shrikhande, 1960). *For every $k \in \mathbb{N}$ with $k \neq 2, 6$ there is a pair of orthogonal latin squares, and thus a solution to the officer problem.*

We will not prove this theorem but a weaker version dealing only with odd k . To do this (although you might not see the connection yet) we can use the following algebraic lemma.

Lemma 2.8. *Let (G, \odot) be a group of odd order. Then $x \mapsto x^2$ is a bijection, i.e. we have unique square roots.*

Proof. Let $z \in G$. Since the group has odd order, there is a $k \in \mathbb{N}$ such that $z^{2k+1} = e_G$. This implies that $(z^{k+1})^2 = z^{2k+2} = z$, proving that every $z \in G$ can be written as a square. Thus $z \mapsto z^2$ maps G to G surjectively. Since G is finite, it is even a bijection. \square

We are now ready to prove the theorem for odd n .

Theorem 2.9. *For odd $n \in \mathbb{N}$ there is a pair of orthogonal latin squares.*

Proof. Let (G, \odot) be any group of odd order $n \in 2\mathbb{N} + 1$. Let the $n \times n$ table be indexed by the elements of G and define two maps (i.e. fillings of the $n \times n$ table)

$$L_1(g, h) := g \odot h, \quad L_2(g, h) := g^{-1} \odot h.$$

We will prove that L_1, L_2 are orthogonal latin squares hence for each odd $n \in \mathbb{N}$ there is an instance of orthogonal latin squares because there is a group of order n .

- 1 L_1 and L_2 are latin squares. For every $a \in G$ the maps $g \mapsto a \odot g$ and $g \mapsto g \odot a$ and $g \mapsto a^{-1} \odot g$ as well as $g \mapsto g^{-1} \odot a$ are bijections on G . This yields the claim, since then each columns and rows (given by $L_1(a, \cdot), L_1(\cdot, a), L_2(a, \cdot)$ and $L_2(\cdot, a)$) are indeed permutations.
- 2 L_1 and L_2 are orthogonal. This follows from the previous lemma. We will show that for any $(a, b) \in G^2$ there are $g, h \in G$ such that

$$L_1(g, h) = a = g \odot h \quad \text{and} \quad L_2(g, h) = b = g^{-1} \odot h.$$

Having proven this we see that any pair $(a, b) \in G^2$ is represented in a cell of the tables filled by L_1 and L_2 (in the cell (g, h)).

To see that the claim holds, let $g := (a \odot b^{-1})^{k+1}$, where $2k+1$ is the order of the group G . Using [Lemma 2.8](#) this yields $g^2 = a \odot b^{-1}$.

It remains to find an h satisfying the following two equations:

$$\begin{array}{ccc} a = g \odot h & \text{and} & b = g^{-1} \odot h \\ \iff & & \\ g^{-1} \odot a = h & \text{and} & g \odot b = h. \end{array}$$

This amounts to verifying that

$$\begin{array}{c} g^{-1} \odot a = g \odot b \\ \iff a \odot b^{-1} = g^2, \end{array}$$

which we already know to hold, so we can find the desired h by setting it to be $h = g^{-1} \odot a$ proving this last part. □

Having thought about orthogonal latin squares it is natural to ask whether there are sometimes more than 2 pairwise orthogonal latin squares, and if so, how many?

Definition 2.10 (Mutually orthogonal latin squares). Let L_1, \dots, L_k be latin squares of order $n \in \mathbb{N}$ for some $k \in \mathbb{N}$. They are *MOLS* (*mutually orthogonal latin squares*) of order n if every pair L_i, L_j with $i \neq j$ is orthogonal.

Proposition 2.11. *For every $n \in \mathbb{N}$ the number of latin squares in a MOLS of order n is at most $n - 1$.*

Proof. Assume that L_1, \dots, L_k are MOLS. The first thing we claim, is that by permuting the entries of L_i by the same $\pi_i \in S_n$ we still get a latin square $L_i^{\pi_i}$ and the latin squares $L_1^{\pi_1}, \dots, L_k^{\pi_k}$ are again MOLS.

1. The fact that $L_i^{\pi_i}$ is again a latin square follows immediately from the fact that the composition of two permutations is a permutation.
2. The fact that $L_i^{\pi_i}$ and $L_j^{\pi_j}$ are still mutually orthogonal follows from permutations being bijections: let $(\ell, m) \in [n]^2$ be any pair. Since permutations are bijections, there are $\ell', m' \in [n]$ such that $\pi_i(\ell') = \ell$ and $\pi_j(m') = m$. Then since L_i, L_j are orthogonal we have (ℓ', m') as an entry of the $n \times n$ table implying that (ℓ, m) is in the table given by the squares $L_i^{\pi_i}$ and $L_j^{\pi_j}$. Since $(\ell, m) \in [n]^2$ was arbitrary we are done.

Thus (after normalising via the right permutations π_1, \dots, π_k) we may assume that L_1, \dots, L_k have $(1, 2, \dots, n)$ as a first row.

We now claim that by setting

$$a_i := L_i(2, 1), \text{ for all } i \in \{1, \dots, k\}$$

we get

$$\begin{cases} a_i \neq 1, & \text{for all } i \\ a_i \neq a_j, & \text{for } i \neq j. \end{cases} \quad (\star)$$

Assuming (\star) , this then implies that $a_i \in [n] \setminus \{1\}$ so by the orthogonality assumption we get $n - 1$ distinct possibilities for a_i . If $k \geq n$ then (by the pigeonhole principle) we find i, j such that $a_i = a_j$ so L_i, L_j cannot be orthogonal, since then $(a_i, a_j) = (a_i, a_i)$ appears twice in the table (the first time comes from their first rows being identical).

So we are left with proving (\star) . This follows easily from the definition of latin squares and orthogonality: a_i cannot be 1 as the first column already contains a 1 and must be a permutation; $a_i \neq a_j$ as discussed previously since otherwise (a_i, a_i) would be twice in the table but we need n^2 many different pairs in n^2 many cells so no doubles are allowed. \square

We conclude this lecture with an application to geometry linking projective planes over finite fields to MOLS. Recall that a *projective plane of order n* is a collection of $n^2 + n + 1$ points and $n^2 + n + 1$ lines such that

1. each line contains exactly $n + 1$ points.
2. each point lies on exactly $n + 1$ lines.
3. any two points lie on a common line.
4. any two lines cross in a single point.

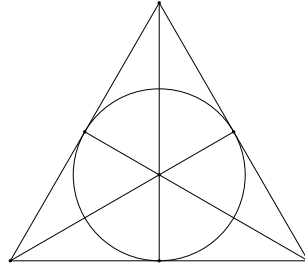


Figure 2.2: The projective plane of order 2, it is known as the *Fano-plane*

Theorem 2.12. *Let $n \in \mathbb{N}$ be fixed, then there is a MOLS of $(n - 1)$ squares of order n if and only if there is a projective plane of order n .*

Proof. Exercise. Hint: Given a MOLS of $n - 1$ squares, add two squares, one with constant rows and one with constant columns to make it $n + 1$ squares. \square

Basic Counting

3.1 Binomial coefficients

Today, we are starting with the basics of counting. A lot of the following rules are quite obvious but it is important to realize that they are sitting in the background of almost every single tool in combinatorics.

Theorem 3.1. *Let A, B be sets. Then the following rules hold:*

$$A, B \text{ finite and disjoint} \implies |A \cup B| = |A| + |B| \quad (\text{Rule of sum})$$

$$A, B \text{ finite} \implies |A \times B| = |A| \cdot |B| \quad (\text{Rule of product})$$

$$A, B \text{ finite} \implies |A^B| = |A|^{|B|} \quad (\text{Rule of componentiation})$$

$$\text{There exists a bijection } f: A \rightarrow B \implies |A| = |B| \quad (\text{Rule of bijection})$$

where $A^B := \{f \mid f: B \rightarrow A\}$.

Proof. (Exercise) □

Definition 3.2 (Binomial Coefficient). We write $\binom{n}{k}$ for the number of k -element subsets (k -subsets) of an n -element set. We set this to 0 if $k < 0$ or $k > n$.

Proposition 3.3. *It holds that*

$$\binom{n}{k} = \frac{n!}{k!(n-k)!}$$

for all $n, k \in \mathbb{N}$ with $k \leq n$.

For the proof, we will use the k -profiles of a permutation:

Definition 3.4 (k -profile). For a given permutation $\pi = (\pi_1, \dots, \pi_n) \in S_n$, the k -profile of π is a vector $p(\pi) = (b_1, \dots, b_n) \in \{0, 1\}^n$ where

$$b_i = \begin{cases} 1, & \text{if } \pi_i \leq k \\ 0, & \text{else.} \end{cases}$$

So it is a boolean vector with k many entries equal to 1.

Proof of Proposition 3.3. In many proofs, instead of considering an arbitrary finite set $X = \{x_1, \dots, x_n\}$, we will just consider $[n] := \{1, \dots, n\}$ for some $n \in \mathbb{N}$. This is without loss of generality, because if $X \neq [n]$, we can just use the bijection $[n] \rightarrow X$, $i \mapsto x_i$ where $i \in [n]$ to prove our claim.

So let us consider $[n]$ and the k -profile mapping

$$p : S_n \rightarrow B_k^n := \{b \in \{0, 1\}^n \mid \sum_{i=1}^n b_i = k\}, (\pi_1, \dots, \pi_n) \mapsto (b_1, \dots, b_n),$$

mapping π to its k -profile. This mapping is by no means injective, since two different permutations can have the same k -profile. However it is surjective on the boolean vectors which have k entries equal to one. So let us look at the pre-image of such a boolean vector. If $b \in B_k^n$, it holds that

$$|p^{-1}(b_1, \dots, b_n)| = k!(n-k)!.$$

This is because, for a given permutation $\pi \in S_n$, its k -profile (b_1, \dots, b_n) is invariant when we permute

- the entries π_i where $b_i = 1$, which gives $k!$ new permutations.
- the entries π_i where $b_i = 0$, which gives $(n-k)!$ new permutations.

So ultimately, we get $k!(n-k)!$ different permutations that have the same k -profile.

Moreover, we can write $S_n = \bigcup_{b \in B_k^n} p^{-1}(b)$. Also note that $|B_k^n| = \binom{n}{k}$, since it is the number of possible choices to choose k of the 1 entries in an n -vector.

Ultimately, with the rule of sum, we get

$$n! = |S_n| = \left| \bigcup_{b \in B_k^n} p^{-1}(b) \right| = \underbrace{(n-k)!k! + \dots + (n-k)!k!}_{\binom{n}{k} \text{ summands}} = \binom{n}{k} (n-k)!k!.$$

□

For an alternative motivation of the binomial coefficient, consider [1].

Now let us prove some more properties of the binomial coefficient.

Theorem 3.5. *For all $n, m, k \in \mathbb{N}$, the following identities for binomial coefficients hold. Identity 1 is the recursion, 3 is symmetry and 5 is the Vandermonde identity.*

- | | |
|---|--|
| 1. $\binom{n}{k} = \binom{n-1}{k} + \binom{n-1}{k-1}$ | 4. $\binom{n}{m} \binom{m}{k} = \binom{n}{k} \binom{n-k}{m-k}$ |
| 2. $\binom{n}{k} \cdot k = n \cdot \binom{n-1}{k-1}$ | 5. $\sum_{l=0}^k \binom{n}{l} \binom{m}{k-l} = \binom{n+m}{k}$ |
| 3. $\binom{n}{k} = \binom{n}{n-k}$ | 6. $\sum_{k=0}^m \binom{n+k}{k} = \binom{n+m+1}{m}$ |

Proof of 1. Let A be the set of k -subsets of $[n]$.

Fix $x \in [n]$.

Define $A_x := \{A' \in A \mid x \notin A'\}$ and $A^x := \{A' \in A \mid x \in A'\}$

- It holds that $|A_x| = \binom{n-1}{k}$ because for each $A' \in A_x$, we have $n-1 = |[n]-x|$ elements left to choose from for our k -subset.

We also get $|A^x| = \binom{n-1}{k-1}$ because for each subset $A' \in A^x$, we can choose from $n-1$ elements which $k-1$ elements other than x we want to have in our subset.

- Moreover, it holds that $A = A_x \dot{\cup} A^x$.

Ultimately, we conclude with the rule of sum that

$$\binom{n}{k} = |A| = |A_x| + |A^x| = \binom{n-1}{k} + \binom{n-1}{k-1}. \quad \square$$

Based on this recursion, we can arrange the binomial coefficients in *Pascal's Triangle* where any entry is the sum of the two entries directly above it:

$$\begin{array}{c} \binom{0}{0} \\ \binom{1}{0} \quad \binom{1}{1} \\ \binom{2}{0} \quad \binom{2}{1} \quad \binom{2}{2} \\ \vdots \\ \binom{n-1}{k-1} \quad \binom{n-1}{k} \\ + \\ \binom{n}{k} \\ \vdots \end{array} = \begin{array}{c} 1 \\ 1 \quad 1 \\ 1 \quad 2 \quad 1 \\ 1 \quad 3 \quad 3 \quad 1 \\ 1 \quad 4 \quad 6 \quad 4 \quad 1 \\ 1 \quad 5 \quad 10 \quad 10 \quad 5 \quad 1 \\ \vdots \end{array}$$

Figure 3.1: Pascal's Triangle

Proof of 2. We prove this using bijection.

Let A be a k -subset of $[n]$ and let $a \in A$. Then there are $\binom{n}{k}$ possibilities to choose A and k possibilities to choose a .

On the other hand, let A' be a $(k-1)$ -subset of $[n] - a$. Likewise, there are $\binom{n-1}{k-1}$ possibilities to choose A' but there are also n possible values for a .

Then we have the bijection

$$\begin{array}{ccc} (A, a) & \xleftrightarrow{(A', a) = (A-a, a)} & (A', a) \\ \uparrow & & \uparrow \\ k \text{ subset} & & (k-1)\text{-subset} \\ \text{of } [n] & & \text{of } [n] - a \end{array}$$

□

3. Basic Counting

Proof of 3. We prove this using bijection.

Let A be a k -subset of $[n]$.

Then its complement A^c is an $(n - k)$ subset of $[n]$.

So with the map $A \mapsto A^c$, we have a bijection between the k -subsets and the $(n - k)$ -subsets of $[n]$, which proves our result. \square

Proof of 4. We prove this using bijection.

For the left hand side, we define three sets

$$\begin{array}{ccccc} \text{size } n & & \text{size } m & & \text{size } k \\ \downarrow & & \downarrow & & \downarrow \\ A & \supseteq & B & \supseteq & C. \end{array}$$

For choosing these sets we have $\binom{n}{m}\binom{m}{k}$ possibilities.

For the right hand side, we define the set B' of size $m - k$ and let

$$\begin{array}{ccc} \text{size } n-k & & \text{size } m-k \\ \underbrace{} & & \downarrow \\ A - C & \supseteq & B' \end{array}$$

For choosing B' , we have $\binom{n-k}{m-k}$ possibilities.

Finally, we have the bijection

$$(B, C) \xleftrightarrow{B=C+B'} (C, B')$$

which means the number of possibilities is equal, so we get

$$\binom{n}{m}\binom{m}{k} = \binom{n}{k}\binom{n-k}{m-k}.$$

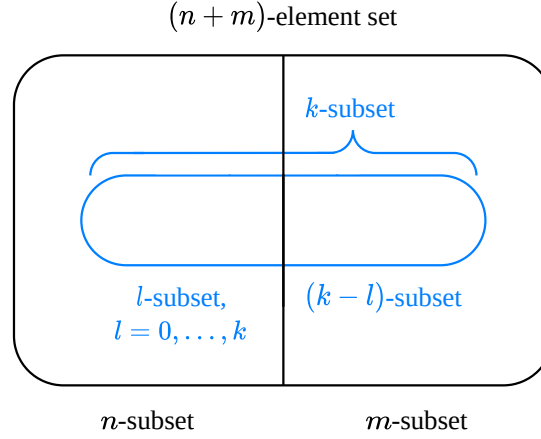
\square

Proof of 5. An $(n + m)$ -element set can be partitioned into an n -element set and an m element set.

If we take a k -subset of our $(n + m)$ -element set, this subset can thus also be partitioned into subsets

$$\underbrace{\{x_1, \dots, x_l\}}_{\subseteq \text{size } n \text{ set}} \dot{\cup} \underbrace{\{x_{l+1}, \dots, x_k\}}_{\subseteq \text{size } m \text{ set}}.$$

as shown in Figure 3.2.


 Figure 3.2: Partitioning our k -subset.

We notice that

1. There are multiple possibilities of how our set could be partitioned: one possibility for each $l = 0, \dots, k$.
2. There are $\binom{n}{l}$ possibilities for the contents of the l -subset and $\binom{m}{k-l}$ possibilities for contents of the $(k-l)$ -subset.

Ultimately, we conclude that

$$\binom{n+m}{k} = \sum_{l=0}^k \binom{n}{l} \binom{m}{k-l}. \quad \square$$

Proof of 6. Consider the boolean Vectors of length $n+m+1$ with m entries equal to 1, the other $n+1$ entries are 0. These form a set we call B .

We want $B = B_0 \dot{\cup} B_1 \dot{\cup} \dots \dot{\cup} B_n$ for some sequence of B_k . For this we choose

$$B_k := \{b \in B \mid b = (\overbrace{b_1, \dots, b_{n+k}}^{n+m+1}, \underbrace{0, 1, \dots, 1}_{m-k})\}.$$

By definition, each boolean vector is in a unique B_k depending on its suffix. For $b \in B_k$, we especially know that b has $m-k$ entries equal to 1. Thus, there must still be k entries equal to 1 among (b_1, \dots, b_{n+k}) . For this, there are $\binom{n+k}{k}$ possibilities, so $|B_k| = \binom{n+k}{k}$.

By the rule of the sum, we finally get

$$\binom{n+m+1}{m} = |B| = |B_0| + |B_1| + \dots + |B_n| = \sum_{k=0}^n \binom{n+k}{k}. \quad \square$$

3.2 Extended binomial coefficients

Definition 3.6 (Falling factorials). We write $(r)_k := r(r-1)(r-2)\cdots(r-k+1)$ for the k -th falling factorial of r , where $r \in \mathbb{N}$ or $r \in \mathbb{C}$ and $1 \leq k \leq r$. Notably, $(r)_r = r!$ so this is a generalization of factorials.

With falling factorials, we can rewrite the binomial coefficient as

$$\binom{n}{k} = \frac{n!}{(n-k)!} \cdot \frac{1}{k!} = \frac{(n)_k}{k!}.$$

Further, $(r)_k$ can be viewed as a polynomial with the variable r . It even makes sense for $r \in \mathbb{C}$. Thus, our rewritten binomial coefficient also makes sense for $n \in \mathbb{C}$ and $k \in \mathbb{N}$.

Example 2. We have

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

An interesting special case is

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

3.2.1 Extending identities

Let $x \in \mathbb{C}$. Let us see if we can extend the previously proven identities to the complex numbers:

- | | |
|---|--|
| 1. $\binom{x}{k} = \binom{x-1}{k} + \binom{x-1}{k-1}$ (✓) | 4. $\binom{x}{m} \binom{m}{k} = \binom{x}{k} \binom{x-k}{m-k}$ (✓) |
| 2. $\binom{x}{k} \cdot k = x \cdot \binom{x-1}{k-1}$ (✓) | 5. $\sum_{l=0}^k \binom{x}{l} \binom{y}{k-l} = \binom{x+y}{k}$ (✓) |
| 3. $\binom{x}{k} = \binom{x}{x-k}$ (✗) | 6. $\sum_{k=0}^m \binom{x+k}{k} = \binom{x+m+1}{m}$ (✓) |

Identity 3 only makes sense if $(x-k) \in \mathbb{N}$, so it is not extendable.

Let us consider Identity 4. The two terms can be seen as polynomials with variable $x \in \mathbb{C}$. Both polynomials have rational coefficients and degree m , which we can see with $\deg \binom{x}{k} = k$ for all $k \in \mathbb{N}$ with $1 \leq k \leq x$. Because they both have degree m , it suffices to show that they agree for at least m distinct points (i.e. they have the same value in at least m distinct points) to show that they are the same polynomials. But we already know they agree for all $x \in \mathbb{N}$, so surely for at least m points. Thus the two terms must indeed be equal as polynomials in $x \in \mathbb{C}$.

Likewise, we can see that both sides of the Identities 1 and 2 have degree k and that both sides of Identity 6 have degree m . With the same criterion as above, we conclude that these identities are extendable over the complex numbers. This proof technique is commonly referred to as *polynomial extension*.

For the Vandermonde Identity (5.), we cannot use our previous technique as we now have a polynomial in two variables $x, y \in \mathbb{C}$. But for this case, we also have an almost as simple criterion that we will formulate as a proposition.

Proposition 3.7. *Let $p, q \in K[x, y]$ be polynomials over some field K in the variables x and y . Further, let $\deg p, \deg q \leq m$ for some $m \in \mathbb{N}$.*

Then if p, q agree on $S \times T$ with $S, T \subseteq K$ and $|S| = |T| = m + 1$, it follows that $p = q$.

Proof. Let $S = \{s_0, \dots, s_m\} \subseteq K$ and $T = \{t_0, \dots, t_m\} \subseteq K$.

Further, let $\mathcal{V} = \text{Span}\{x^k y^l \mid 0 \leq l, k \leq m\}$.

Then \mathcal{V} is a subvectorspace of $K[x, y]$ with dimension $(m + 1)^2$. This is because $x^k y^l$ for $0 \leq l, k \leq m$ build a basis. We also know that $p, q \in \mathcal{V}$ because their degree is at most m . It would be helpful to have another basis for \mathcal{V} to express p, q .

For this, we consider the polynomials p_{kl} with the property

$$p_{kl}(s_i, t_j) = \begin{cases} 1, & (i, j) = (k, l) \\ 0, & \text{otherwise.} \end{cases}$$

where $0 \leq i, j, k, l \leq m$. It holds that

- Our polynomials p_{kl} must be of the form

$$p_{kl}(x, y) = \prod_{i \neq k} (x - s_i) \prod_{j \neq l} (y - t_j).$$

and by multiplying this out, we get $p_{kl} \in \mathcal{V}$.

- Moreover, there are $(m + 1)^2 = \dim \mathcal{V}$ of these p_{kl} in total.

Ultimately, if we can show their linear independence, $\{p_{kl} \mid 0 \leq k, l \leq m\}$ would form a basis of \mathcal{V} .

So let us assume

$$\sum_{0 \leq k, l \leq m} \mu_{kl} \cdot p_{kl}(x, y) = 0$$

for some $\mu_{ij} \in K$. We want to show that all $\mu_{ij} = 0$. If we evaluate our polynomials at (s_i, t_j) , each polynomial evaluates to 0, except for p_{ij} , which evaluates to 1. Thus we have

$$0 = \sum_{0 \leq k, l \leq m} \mu_{kl} \cdot p_{kl}(s_i, t_j) = \mu_{ij} \cdot \underbrace{p_{ij}(s_i, t_j)}_{= 1} = \mu_{ij},$$

which shows the linear independence.

3. Basic Counting

Now we know that $\{p_{kl} \mid 0 \leq k, l \leq m\}$ is a basis of \mathcal{V} , which means we can express our p and q as a linear combination of our p_{kl} polynomials. But to show that $p = q$, we will consider the polynomial $p - q$ instead (which is also in \mathcal{V} since \mathcal{V} is a vector space) and show that it is 0.

It holds that

$$p - q = \sum_{0 \leq k, l \leq m} \lambda_{kl} p_{kl}.$$

for some $\lambda_{ij} \in K$. Moreover, we know that p and q agree on $S \times T$. So we can evaluate them at all $(s_i, t_j) \in S \times T$ and ultimately obtain

$$0 = p(s_i, t_j) - q(s_i, t_j) = \lambda_{ij} \underbrace{p_{ij}}_{=1} = \lambda_{ij}$$

Thus $\lambda_{ij} = 0$ for all $0 \leq i, j \leq m$ and we get

$$p - q = \sum_{0 \leq k, l \leq m} \underbrace{\lambda_{kl}}_{=0} p_{kl} = 0.$$

So we conclude that $p = q$. □

Corollary 3.8. *Vandermonde's identity*

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

holds for all $(x, y) \in \mathbb{C}$.

Proof. We obtain this with the previous proposition since we know that Vandermonde's identity holds for all $x, y \in \mathbb{N}$. □

We can also rewrite the Vandermonde's identity with falling factorials. It holds that

$$\frac{(x+y)_k}{k!} = \binom{x+y}{k} = \sum_{l=0}^k \binom{x}{l} \binom{y}{k-l} = \sum_{l=0}^k \frac{1}{l!} \cdot \frac{1}{(k-l)!} \cdot (x)_l \cdot (y)_{k-l},$$

so multiplying by $k!$ we get

$$(x+y)_k = \sum_{l=0}^k \binom{k}{l} (x)_l (y)_{k-l}.$$

This is a nice identity for falling factorials and surprisingly similar to the binomial theorem.

Theorem 3.9 (Binomial theorem). *It holds that*

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

for all $x, y \in \mathbb{R}$, $k \in \mathbb{N}$.

Typically, the binomial theorem is proven as an exercise using induction. But here are two nicer combinatorial proofs.

Proof 1 of Theorem 3.9. For the left hand side, we have

$$(x + y)^k = \overbrace{(x + y)(x + y) \cdots (x + y)}^{k \text{ factors}}$$

We will now expand this by multiplying out all the terms together. While doing so, we choose for each $(x + y)$ term whether we multiply out using x or y . Say we choose x during this expansion exactly k times (and y the remaining $n - k$ times). Then the resulting term after this specific expansion will be of the form $x^k y^{n-k}$. But there are $\binom{n}{k}$ possibilities to choose at which $(x + y)$ term we choose the x variable instead of y . So our term $x^k y^{n-k}$ is actually summed $\binom{n}{k}$ times, resulting in the term $\binom{n}{k} x^k y^{n-k}$ when multiplying out by choosing x exactly k times. Summing over all possibilities for k , we get

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

□

Proof 2 of Theorem 3.9. For finite sets X , Y and K , we can find a bijection

$$(X \cup Y)^K \xleftrightarrow{\text{bijection}} \bigcup_{L \subseteq K} (X^L \times Y^{K \setminus L})$$

because for every map $f: K \rightarrow (X \cup Y)$, there is a subset $L := f^{-1}(X) \subseteq K$ that it maps to X such that the rest $L \setminus K$ maps to Y . So for a given map, we account for all possibilities of $L \subseteq K$ and then consider all possible pairs of maps $L \rightarrow X$ and $K \setminus L \rightarrow Y$, where a given pair uniquely determines f .

If we take $|X| = a$, $|Y| = b$, $|K| = k$, with our basic rules of counting this yields

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

which is the binomial theorem for $a, b \in \mathbb{N}$. Since the polynomials agree on sufficiently many integers, with **Proposition 3.7**, the result also holds over the reals. □

3.3 Counting related to permutations

A permutation $\pi \in S_n$ can be expressed in multiple ways, as seen in Table 3.2.

Two-line notation	One-line notation	Cycle notation
$\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 5 & 4 & 7 & 2 & 3 & 6 & 8 & 1 \end{pmatrix}$	$(5\ 4\ 7\ 2\ 3\ 6\ 8\ 1)$	$(4\ 2)(6)(8\ 1\ 5\ 3\ 7)$

Table 3.2: Different Representations of an example permutation

The cycle notation stems from considering the cycles in the permutation. For our example, this looks as in Figure 3.3.

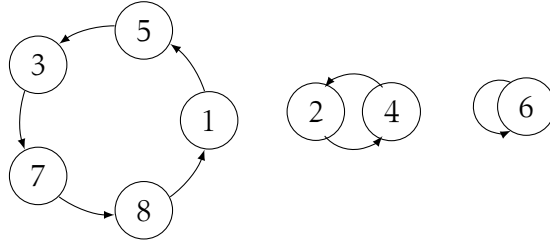


Figure 3.3: Cycles in our permutation

The cycle notation is not unique; the order of the cycles in the notation is arbitrary, as is which of the numbers in a cycle is the first one. As a convention, we make the notation unique by

- starting each cycle with its largest number (the *cycle leader*), as well as
- sorting the cycles by their first entry ascending.

With this convention, we can even leave out the parentheses in the cycle notation. But the cycles can still be uniquely identified, because the cycle leaders are the *left-to-right maxima*, that is, they are larger than all numbers left of them. So the permutation can be uniquely identified as well:

$$(42)(6)(81537) \rightsquigarrow \underline{4}\underline{2}\underline{6}\underline{8}1537 \quad (3.3)$$

The underlined elements are the left-to-right maxima.

Let us now derive some statistics about the cycle structure of a given permutation.

Definition 3.10 (Cycle properties of a permutation). Let $\pi \in S_n$. We write

- $c_i(\pi) \in \mathbb{N}$ for the *number of cycles of length i in π* .
- $\text{type}(\pi) := (c_1(\pi), \dots, c_n(\pi)) \in \mathbb{N}^n$ for the *type of π* .
- $c(\pi) := \sum_{i=1}^n c_i(\pi)$ for the *number of cycles of π* .

Proposition 3.11. For $c = (c_1, \dots, c_n) \in \mathbb{N}^n$ with $\sum_{k=1}^n k \cdot c_k = n$, there are

$$\frac{n!}{1^{c_1} \cdot c_1! \cdot 2^{c_2} \cdot c_2! \cdot \dots \cdot n^{c_n} \cdot c_n!}$$

permutations of type c .

Proof. We define

$$f: S_n \rightarrow S_n, \pi \mapsto f(\pi)$$

where $f(\pi)$ is a permutation of type $c = (c_1, \dots, c_n) \in \mathbb{N}^n$. Let us consider an example to see how this map can be defined.

Example 3. Let $c = (1, 2, 1, 0, \dots, 0)$, then the size of permutation π is $n = 1 + 2 \cdot 2 + 1 \cdot 3 = 8$. We interpret π as a word (one-line notation) and add parentheses according to c to get a permutation in cycle notation:

$$\pi = (3 \ 7 \ 1 \ 5 \ 4 \ 6 \ 8 \ 2) \mapsto f(\pi) = (3)(7 \ 1)(5 \ 4)(6 \ 8 \ 2)$$

Now f produces every permutation π' of type c , but it is not injective. But we can ask ourselves “How many π does f map to π' ?” . The cycle notation is invariant under

1. permutation of cycles and the
2. choice of the first element for each cycle.

For the former, we have to keep in mind that f only maps to cycle notations with increasing size of cycles, so we can only permute cycles of the same length. If we apply these permutations to π while keeping $f(\pi)$ invariant, from 1 and 2, we get $\prod_{k=0}^n c_k!$ and $\prod_{k=0}^n k^{c_k}$ possible pre-images under f respectively. So if $\text{type}(\pi') = c$, ultimately

$$|f^{-1}(\pi')| = \prod_{k=0}^n k^{c_k} c_k!,$$

so all of these pre-images have the same size, which only depends on c . And the number m of permutations of type c which we are looking for, is the same as the number of pre-images under f of our type c permutations. Since f hits all type c permutations, their pre-images also partition S_n . Thus

$$n! = |S_n| = \left| \bigcup_{\pi' \in S_n} f^{-1}(\pi') \right| = m \cdot \prod_{k=0}^n k^{c_k} c_k!,$$

and we conclude that

$$m = \frac{n!}{\prod_{k=0}^n k^{c_k} c_k!}.$$

□

Bibliography

- [1] DorFuchs. Kombinatorik (Mathe-Song).
youtube.com/watch?v=JoETgJS1oWE.

Basic Counting II

4.1 Counting cycles of permutations (continued)

We continue on the topic of counting cycles of permutations and therefore let $c(n, k) := \#(\text{permutations in } S_n \text{ with } k \text{ cycles})$ and remark that $s(n, k) = (-1)^{n-k} c(n, k)$ are the stirling numbers of 1st kind.

Lemma 4.1. *With the convention*

$$c(n,k) = \begin{cases} 0 & n \leq 0 \text{ or } k \leq 0 \text{ but not } n = k = 0, \\ 1 & n = k = 0. \end{cases}$$

we get the recursion

$$c(n, k) = c(n-1, k-1) + (n-1)c(n-1, k). \quad (4.4)$$

Before we get to the proof we observe, that we can write in a triangular table as seen in [Figure 4.1](#). We further observe that $c(n, 1) = (n - 1)!$, because if we fix a 'starting' element of the cycle we can arrange the remaining elements in $(n - 1)!$ ways. It's also true that $c(n, n) = 1$, because every element has to be in a 1-cycle (a fixed point), and that $c(n, n - 1) = \binom{n}{2}$, because in this case all but 2 elements have to be fixed points and there are $\binom{n}{2}$ choices for the 2 elements that are in the 2-cycle.

Figure 4.1: triangular table of $c(n, k)$ for $n, k \in [5]$

Proof of Lemma 4.1. Let $\pi \in S_n$ and let k be the number of cycles in π . We now want to remove n from π :

- If n is a fixed point (1-cycle of itself), removing n yields a permutation $\pi' \in S_{n-1}$ with $k - 1$ cycles. That corresponds to the first summand in the right hand side of Equation (4.4).
- If n is not a fixed point, let p be its predecessor ($\pi(p) = n$). Removing n as in Figure 4.2 yields a permutation $\pi' \in S_{n-1}$ with k cycles, but we also have to memorize p as the place where we have to put in n if we want to determine π again, which corresponds to the second summand in the right hand side of Equation (4.4).

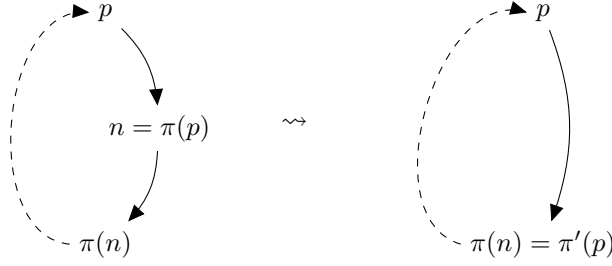


Figure 4.2: permutation π left and π' right

□

With the help of Lemma 4.1 we can prove the the following Theorem:

Theorem 4.2. Let $n, k \in \mathbb{N}$ and $x \in \mathbb{C}$, then

$$\sum_{k=1}^n c(n, k) x^k = x(x+1)(x+2) \dots (x+n-1).$$

Proof I. With $F_n(x) = \sum_{k=1}^n c(n, k) x^k$ we get

$$\begin{aligned} F_n(x) &\stackrel{(4.4)}{=} \sum_{k=1}^n \left(c(n-1, k-1) + (n-1)c(n-1, k) \right) x^k \\ &= \sum_{k=1}^n c(n-1, k-1) x^k + (n-1) \sum_{k=1}^n c(n-1, k) x^k \\ &= x F_{n-1}(x) + (n-1) F_{n-1}(x) \\ &= (x+n-1) F_{n-1}(x) \end{aligned}$$

By induction with the induction conditions

$$F_1(x) = x \quad \text{and} \quad F_2(x) = x + x^2 = x(x+1)$$

we complete the proof.

□

In the second proof we will only show the statement for $x \in \mathbb{N}$. Since two distinct polynomials of degree n have at most $n-1$ common evaluations we obtain the statement for all $x \in \mathbb{C}$.

Proof II. On the right hand side we count vectors (b_1, \dots, b_n) with $1 \leq b_i \leq x + i - 1$. On the left hand side we count pairs (π, f) with $\pi \in S_n$ and $f : \{\text{cycles of } \pi\} \rightarrow [x]$.

We now want to build a bijective map $(b_1, \dots, b_n) \rightarrow (\pi, f)$ by taking b_1, \dots, b_n in that order and placing $n, n-1, \dots, 1$ in a partial permutation in that order. If k is placed at the very left, we fix a value of f , because it will become a cycle leader in the canonical cycle notation ([Equation \(3.3\)](#)):

Assume i elements $(n, \dots, n-i+1)$ have been placed and consider b_{i+1} :

Case I: $1 \leq b_{i+1} \leq x$

Place $n-i$ at the front of the partial permutation.

$n-i$ will be a new left-to-right maximum creating a new cycle γ .

Set $f(\gamma) = b_{i+1}$.

Case II: $x < b_{i+1} = x+k \quad (1 \leq k \leq i)$

Place $n-i$ behind k of the already placed elements. Since larger elements are before $n-i$, there are the same number of cycles now, and the k -th cycle has now become larger by one.

Given a tuple (π, f) we can determine the vector easily by assigning $b_{n-i+1} = f(\gamma(i))$ for all cycle leaders i , where $\gamma(i)$ is its cycle and

$$b_{n-i+1} = x + \#(\text{elements larger than } i \text{ that are placed left of } i),$$

for example given $x = 3$ and

$$\begin{array}{cccccccc} \pi = & 3 & 6 & 1 & 4 & 8 & 7 & 2 & 5 \\ f = & 2 & 3 & & & 2 & & & \end{array}$$

we get

$$\begin{array}{cccccccc} b_1 & b_2 & b_3 & b_4 & b_5 & b_6 & b_7 & b_8 \\ 2 & 3+1 & 3 & 3+3 & 3+1 & 2 & 3+5 & 3+2 \end{array}$$

□

As we will make further use of the expression x^n , we will define it here.

Definition 4.3 (Raising factorial). Let $x \in \mathbb{C}$ and $n \in \mathbb{N}$, then the *raising factorial* x^n is defined as

$$x^n := x(x+1)(x+2)\dots(x+n-1).$$

4.2 The expected number of cycles

Throughout the entire section we are considering the uniform distribution on S_n .

Definition 4.4. Let A be a k -subset of $[n]$. We define a random variable

$$X_A(\pi) = \begin{cases} 1 & \pi \text{ has a } k\text{-cycle whose elements are the elements of } A, \\ 0 & \text{otherwise.} \end{cases}$$

We can easily observe that in the canonical cycle notation of π , A has to appear consecutively, but the order of its elements except the largest element, as well as the order of elements not in A does not matter, thus

$$\begin{aligned} \Pr(X_A = 1) &= \frac{1}{n!} \#(\text{permutations having } A \text{ as a cycle}) \\ &= \frac{1}{n!} (k-1)!(n-k)! \\ &= \frac{1}{k} \binom{n}{k}^{-1} \end{aligned}$$

Definition 4.5.

$$Z_k(\pi) := c_k(\pi) := \#(k\text{-cycles of } \pi)$$

Observation.

$$\begin{aligned} Z_k(\pi) &= \sum_{A \in \binom{[n]}{k}} X_A(\pi) \\ \implies \mathbf{E}(Z_k) &= \mathbf{E} \left(\sum_{A \in \binom{[n]}{k}} X_A(\pi) \right) = \sum_{A \in \binom{[n]}{k}} \mathbf{E}(X_A) = \sum_{A \in \binom{[n]}{k}} \Pr(X_A = 1) = \sum_{A \in \binom{[n]}{k}} \frac{1}{k} \binom{n}{k}^{-1} = \frac{1}{k} \end{aligned}$$

Definition 4.6.

$$Z(\pi) := \sum_{k=1}^n Z_k(\pi) = \#(\text{cycles of } \pi)$$

Observation.

$$\mathbf{E}(Z) = \mathbf{E} \left(\sum_{k=1}^n Z_k \right) = \sum_{k=1}^n \mathbf{E}(Z_k) = \sum_{k=1}^n \frac{1}{k} = H_n$$

with H_n being the n -th harmonic number.

We can bound the n -th harmonic number by $\ln(n+1) \leq H_n \leq \ln(n) + 1$ using

$$H_n = \int_1^{n+1} \sum_{k=1}^n \frac{1}{k} \mathbb{1}_{[k, k+1]}(x) dx \geq \int_1^{n+1} \frac{1}{x} dx = \ln(n+1)$$

and

$$H_n = 1 + \int_1^n \sum_{k=2}^n \frac{1}{k} \mathbb{1}_{[k-1, k]}(x) dx \leq 1 + \int_1^n \frac{1}{x} dx = \ln(n) + 1$$

4.3 The twelfefold way

In this chapter we want to count functions

$$f : N \rightarrow M,$$

where N is a set of n balls and M is a set of m boxes. We can restrict f to be

- injective (when $m \geq n$),
- surjective (when $n \geq m$),
- arbitrary.

Furthermore we can count up to equivalence: Balls and boxes can both be distinguishable (D) or indistinguishable (I). For indistinguishable boxes we have

$$f \sim g \Leftrightarrow \exists \pi \in S_M \text{ such that } \pi \circ f = g$$

For indistinguishable balls we have

$$f \sim g \Leftrightarrow \exists \tau \in S_N \text{ such that } f \circ \tau = g$$

We will now work out the solutions to this counting problems, which are summarized in Table 4.3.

balls	boxes	arbitrary	injective	surjective
D	D	(1) m^n	(2) $(m)_n$	(3) $m!S(n, m)$
I	D	(4) $\binom{n+m-1}{m-1}$	(5) $\binom{m}{n}$	(6) $\binom{n-1}{m-1}$
D	I	(7) $\sum_{t=0}^m S(n, t)$	(8) 1	(9) $S(n, m)$
I	I	(10) $\sum_{t=0}^m P_t(n)$	(11) 1	(12) $P_m(n)$

Table 4.3: solutions to the counting problems

The entries 1 and 2 are easily obtained by looking at how many options we have for each element inserting them one by one.

Entries 8 and 11 follow from the fact, that there is at most 1 ball in each box and the boxes are indistinguishable. Therefore all we know is that n boxes have a ball and the rest doesn't.

Entry 5 just chooses n out of m boxes to contain one of the indistinguishable balls.

Entry 4 is obtained by inserting $m - 1$ separations in a sequence of n balls, that's $m - 1$ separations out of $n + m - 1$ elements. See Figure 4.3.

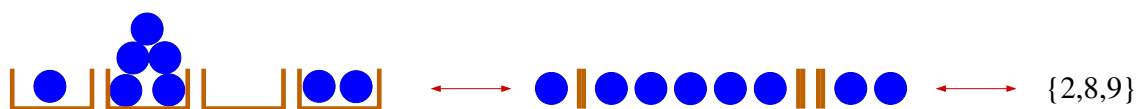


Figure 4.3: Left: 8 balls in 4 boxes. Middle: 8 balls and 3 separators. Right: The positions of the separators as a 3-subset of $[11]$.

In entry 6 instead of separations we select a last ball for each box except the last box, that is $m - 1$ out of $n - 1$ balls, the n -th ball is known to be the last ball of the last box.

In the following, we will learn theory about Stirling numbers and integer partitions. This will lay the basis to understand the more complicated entries.

Stirling Numbers and Integer Partitions

In this lecture we complete our dissection of the twelvefold way from last lecture and discuss some properties of Stirling numbers and integer partition.

5.1 The twelvefold way (continued)

Recall: $S(n, m) = \#(\text{partitions of the set } [n] \text{ into } m \text{ parts})$ are the Stirling numbers of the 2nd kind. The entries 9, 7 and 3 of the twelvefold way all include Stirling numbers.

We get entry 9, which is $S(n, m)$, by placing n distinguishable balls into m indistinguishable boxes, such that there is no empty box. The order of the boxes doesn't matter to us and we get blocks B_1, B_2, \dots, B_m in the boxes, which is exactly $S(n, m)$.

$$\{ \underline{B_1} \quad \underline{B_2} \quad \cdots \quad \underline{B_m} \}$$

For entry 7, $\sum_{t \leq m} S(n, t)$, we have a function that is surjective onto t boxes, where t can range from 1 to m and the number of empty boxes is between $m - 1$ and 0.

$$\{ \underline{B_1} \quad \underline{B_2} \quad \cdots \quad \underline{B_t} \} \quad \underline{\quad} \quad \underline{\quad}$$

Entry 3, $m!S(n, m)$ can be derived from 9, since for distinguishable boxes we can order them in $m!$ ways.

Theorem 5.1. Let $k, n \in \mathbb{N}$ and $x \in \mathbb{C}$. Then

$$x^n = \sum_{k=0}^n S(n, k)(x)_k,$$

where $(x)_k = x(x-1)\dots(x-k+1)$ is a falling factorial.

Proof. We prove this for $x \in \mathbb{N}$ by bijection and then extend it to \mathbb{C} as in Section 3.2. The left-hand side is simply the number of functions $f : [n] \rightarrow [x]$. For the right-hand side consider $A \subseteq [x]$ and let $F_A = \{f : [n] \rightarrow [x] \mid \text{Im}(f) = A\}$. Then $|F_A| = |A|!S(n, |A|)$ as

in entry 3 of the twelvefold way, since the functions in F_A are surjective onto A . Now for each unique A the functions $f : [n] \rightarrow [x]$ will be in a unique F_A and so we get

$$x^n = \sum_{A \subseteq [x]} |F_A| = \sum_{A \subseteq [x]} |A|! S(n, |A|) = \sum_{k=0}^x k! S(n, k) \binom{x}{k} = \sum_{k=0}^n k! S(n, k) \binom{x}{k} = \sum_{k=0}^n S(n, k) (x)_k.$$

In the third equality we can replace the upper summation boundary by n , because if n is larger than x the binomial coefficient will be 0 for the $k > x$, and if n is smaller than x then the $S(n, k)$ will be 0 for $k > n$. \square

5.2 Stirling inversion

Let $c(n, k) = \#(\pi \in S_n \text{ with } k \text{ cycles})$. We have shown in [Theorem 4.2](#) that $x^n = \sum_{k=0}^n c(n, k) x^k$, where x^n is a raising factorial.

Definition 5.2 (Stirling numbers of the 1st kind). Let $n, k \in \mathbb{N}$. Then

$$\hat{s}(n, k) = (-1)^{n-k} c(n, k)$$

are called the *Stirling numbers of the 1st kind*.

Rasing and falling factorials are related as follows:

$$\begin{aligned} x^n &= (x)(x+1)\dots(x+n-1) \\ &= (-1)^n (-x)(-x-1)\dots(-x-n+1) = (-1)^n (-x)_n. \end{aligned}$$

Using this we get

$$\begin{aligned} (-1)^n (x)_n &= (-x)_n = \sum_{k=0}^n c(n, k) (-x)^k = \sum_{k=0}^n c(n, k) (-1)^k x^k \\ \implies (x)_n &= \sum_{k=0}^n \hat{s}(n, k) x^k, \end{aligned}$$

where the last implication follow from $c(n, k) = (-1)^{n-k} \hat{s}(n, k)$ and division by $(-1)^n$.

Consider now the matrices $S = (S(n, k))_{n, k \leq N}$, $\hat{S} = (\hat{s}(n, k))_{n, k \leq N}$. Further let $R_{\leq N}[x]$ be the vector space of polynomials of degree $\leq N$ in x . Then $B = \{x^k\}_{k=0}^N$ and $\hat{B} = \{(x)_k\}_{k=0}^N$ are both bases of this vector space and S and \hat{S} are transformation matrices for basis exchange $B \rightarrow \hat{B}$ and $\hat{B} \rightarrow B$ respectively.

We conclude that because these two matrices are inverse to one another we get

$$\sum_{i \geq 0} S(m, i) \hat{s}(i, k) = \delta_{[m=k]}.$$

Since S and \hat{s} are inverse matrices we get that for sequences (a_n) and (b_n) :

$$b_n = \sum_{k=0}^n S(n, k) a_k \iff a_n = \sum_{k=0}^n \hat{s}(n, k) b_k.$$

This identity is what we call the *Stirling inversion*. This is similar to a prior identity, which we called the binomial inversion given by

$$b_n = \sum_{k=0}^n \binom{n}{k} (-1)^k a_k \iff a_n = \sum_{k=0}^n \binom{n}{k} (-1)^k b_k.$$

5.3 Integer partitions

Definition 5.3 (Integer partition). A partition of $n \in \mathbb{N}$ is a sorted vector $\lambda = (\lambda_1, \lambda_2, \dots, \lambda_k)$ with $\lambda_1 \geq \lambda_2 \geq \dots \geq \lambda_k > 0$ and $\sum_{i=1}^k \lambda_i = n$. We write $\lambda \vdash n$ to denote that λ is a partition of n .

Let $p(n) = \#(\text{partitions of } n)$.

Example 4. $\lambda = (5, 5, 2, 1, 1, 1)$ is a partition of 15, i.e., $\lambda \vdash 15$. This partition can also then be represented by

$$5^2 2^1 1^3 \quad \text{or} \quad 5^2 2 1^3.$$

We will also use the Ferrers diagram $F(\lambda)$ or F_λ , it consists of a stack/column of λ_i boxes for each entry of $\lambda = (\lambda_1, \lambda_2, \dots, \lambda_k)$.

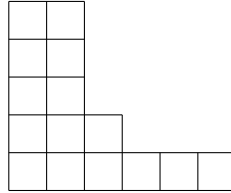


Figure 5.1: Ferrers Diagram F_λ
when $\lambda = (5, 5, 2, 1, 1, 1)$.

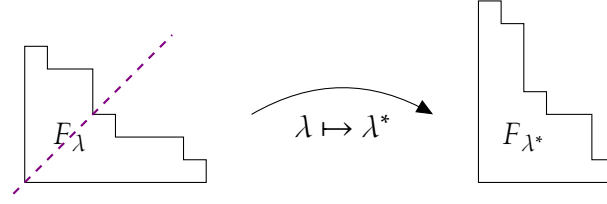
Next we come to restricted classes of partitions

Proposition 5.4.

$$\#(\text{partitions of } n \text{ into parts of size } \leq k) = \#(\text{partitions of } n \text{ into at most } k \text{ parts})$$

Proof. Let λ be a partition with parts of size $\leq k$. Then reflecting the Ferrers diagram along its diagonal gives us a partition λ^* that has $\leq k$ parts. The partition λ^* is called the conjugate of λ .

Because the reflection is an involution this is a bijection between the two types of partitions. \square



Now we come to the remaining 2 entries of the twelvefold way. For entry 12 let $p_k(n) = \#(\text{partitions of } n \text{ into exactly } k \text{ parts})$. We first sort our indistinguishable boxes by the number of balls they contain. We can then represent these boxes by the columns in the Ferrers diagram, where each square is a ball contained in the box. Entry 10 we get by once again considering the t boxes onto which the function maps surjectively and summing over each possible $t \leq m$, analogously to getting entry 7 from entry 9. This completes the discussion of the twelvefold way.

Going back to the discussion of partitions we get the following recursion:

Proposition 5.5. $p_k(n) = p_{k-1}(n-1) + p_k(n-k)$

Proof. Let $\lambda \vdash n$, $\lambda = (\lambda_1, \dots, \lambda_k)$ be an integer partition of n . We do the proof by bijection and considering two cases.

Case 1 ($\lambda_k = 1$): Consider $\lambda' = (\lambda_1, \dots, \lambda_{k-1})$ which is an integer partition of $n-1$, i.e. $\lambda' \vdash n-1$.

Case 2 ($\lambda_k > 1$): Consider $\lambda'' = (\lambda_1 - 1, \lambda_2 - 1, \dots, \lambda_k - 1)$ which is an integer partition of $n-k$, i.e. $\lambda'' \vdash n-k$. \square

Note that $p(n) = \sum_{k=1}^n p_k(n)$. This allows to compute $p(n)$ by first computing $p_k(m)$ for all $k, m \leq n$ with the proposition. Thus the complexity of this approach is $O(n^2)$.

Next we look at the generating function for $(p(n))_{n \geq 0}$.

Theorem 5.6 (Euler). *Let $x \in \mathbb{C}$, then*

$$\sum_{n=0}^{\infty} p(n)x^n = \prod_{k=1}^{\infty} \frac{1}{1-x^k}.$$

Proof. We recall the geometric series $\frac{1}{1-x^k} = 1 + x^k + x^{2k} + x^{3k} + \dots$

We then interpret the factors of the product on the right-hand side, through the geometric series, as infinite sums which we multiply and then collect the terms that together yield x^n . Note that the k here counts the size of the parts. So the x 's coming from $\frac{1}{1-x}$ count the number of parts of size 1 and the ones from $\frac{1}{1-x^2}$ count the number of parts of size 2. Despite having an infinite product, the coefficient $p(n)$ of x^n only depends on those $x^{s \cdot k}$ from the geometric series which have $s \cdot k \leq n$, i.e., we only have to look on finite initial parts of a finite number of factors in the infinite product on the right side to compute $p(n)$.

A generic term contributing to the coefficient of x^n is of the form

$$x^{a_1 \cdot 1} x^{a_2 \cdot 2} x^{a_3 \cdot 3} \dots x^{a_m \cdot m} = x^n$$

5. Stirling Numbers and Integer Partitions

this term corresponds to the partition $m^{a_m}(m-1)^{a_{m-1}}\dots 1^{a_1}$ where we can omit entries for which $a_i = 0$.

Example: the term $x^{3 \cdot 1} x^{3 \cdot 2} x^{1 \cdot 3}$ corresponds to the partition $1^3 2^3 3$ of 12. \square

Remark. The Hardy-Ramanujan-Rademacher expansion gives the precise asymptotic behaviour of $p(n)$:

$$p(n) \sim \frac{1}{4n\sqrt{3}} e^{\pi\sqrt{2n/3}}.$$

Another result about different classes of partitions is given by the following theorem.

Theorem 5.7. *It holds*

$$\#(\text{partitions of } n \text{ into distinct parts}) = \#(\text{partitions of } n \text{ into odd parts}).$$

A partition into distinct parts means that in the representation with exponents all the exponents will be 1, e.g. $5^1 2^1 1^1$.

Proof I. Using the same ideas as for the generating function from Euler's theorem we get

$$\sum_{n=0}^{\infty} p_{\text{dist}}(n) x^n = \prod_{k=1}^{\infty} (1 + x^k).$$

To see this note that for each term x^m appearing in the expansion of the product on the right we get an expression of m as sum of different summands. For example the term of x^4 in the expansion of $(1+x)(1+x^2)(1+x^3)(1+x^4)$, is obtained as $x \cdot x^3$ and $1 \cdot x^4$. So in the simplification of the expansion of the product we get $2x^4$ which corresponds to $p_{\text{dist}}(4) = 2$.

As in Euler's Theorem we use geometric series to obtain

$$\sum_{n=0}^{\infty} p_{\text{odd}}(n) x^n = \prod_{k=1}^{\infty} \frac{1}{1 - x^{2k+1}}.$$

Now we use $(1 - x^{2k}) = (1 - x^k)(1 + x^k)$, which implies $(1 + x^k) = \frac{(1 - x^{2k})}{1 - x^k}$. This gives us

$$\begin{aligned} \sum_{n=0}^{\infty} p_{\text{dist}}(n) x^n &= \prod_{k=1}^{\infty} (1 + x^k) = \frac{(1 - x^2)(1 - x^4)(1 - x^6)(1 - x^8) \dots}{(1 - x)(1 - x^2)(1 - x^3)(1 - x^4) \dots} \\ &= \frac{1}{(1 - x)(1 - x^3)(1 - x^5) \dots} = \prod_{k=0}^{\infty} \frac{1}{1 - x^{2k+1}} = \sum_{n=0}^{\infty} p_{\text{odd}}(n) x^n \end{aligned}$$

To get from the first to the second line just cancel equal factors in numerator and denominator. \square

Next we will see a bijective proof of the same theorem.

Proof II. Let $d \vdash n$ be an integer partition of n into distinct parts, so $d = (d_1, d_2, \dots, d_k)$, $d_1 > d_2 > \dots > d_k$, $\sum_{i=1}^k d_i = n$. Then each d_i can be written as $d_i = 2^{a_i} m_i$ for some unique $a_i \in \mathbb{N}$ and odd $m_i \in \mathbb{N}$. Next we consider a reordering of the m_i , namely let $\{m_1, \dots, m_k\} = \{\mu_1, \dots, \mu_l\}$ with $\mu_1 > \mu_2 > \dots > \mu_l$ where we delete repetitions of m_i , thereby only keeping l out of k values.

Using the sum for n we get

$$\begin{aligned} n &= 2^{a_1} m_1 + 2^{a_2} m_2 + \dots + 2^{a_k} m_k \\ &= (2^{\alpha_1} + 2^{\alpha_2} + \dots) \mu_1 + (2^{\beta_1} + 2^{\beta_2} + \dots) \mu_2 + \dots \\ &= r_1 \mu_1 + r_2 \mu_2 + \dots + r_l \mu_l \end{aligned}$$

which yields the partition $\mu_1^{r_1} \mu_2^{r_2} \dots \mu_l^{r_l}$ of n into odd parts. One has to be a little careful to prove the other direction or showing that the map is indeed injective. \square

Example 5. An example for the second proof

$$\begin{aligned} 6 &= 3 + 2 + 1 && \text{partition into distinct parts} \\ &= 2^0 \cdot 3 + 2^1 \cdot 1 + 2^0 \cdot 1 \\ &= (2^0)3 + (2^1 + 2^0)1 = 3^1 1^3 \vdash 6 && \text{this gives us an odd partition} \end{aligned}$$

Euler's Pentagonal Number Theorem

The main goal of this lecture is to prove Euler's pentagonal number theorem and mention a faster method for computing $p(n)$ as an application. We then continue by introducing the Fibonacci sequence and discussing some identities involving these numbers.

Theorem 6.1 (Euler's pentagonal number theorem). *Let $x \in \mathbb{C}$. Then*

$$\prod_{k=1}^{\infty} (1 - x^k) = \sum_{k=-\infty}^{\infty} (-1)^k x^{\frac{(3k-1)k}{2}} \quad \left(= 1 + \sum_{k=1}^{\infty} (-1)^k \left(x^{\frac{(3k-1)k}{2}} + x^{\frac{(3k+1)k}{2}} \right) \right)$$

We will use a very similar technique as in the proofs of [Theorem 5.6](#) and [Theorem 5.7](#), that is we will relate the product to a generating function with coefficients given by an even and odd variation of $p_{\text{dist}}(n)$, i.e.

$$\begin{aligned} p_d^o(n) &:= p_{\text{dist}}^{\text{odd}}(n) := \#(\text{partitions of } n \text{ having an odd number of distinct parts}), \\ p_d^e(n) &:= p_{\text{dist}}^{\text{even}}(n) := \#(\text{partitions of } n \text{ having an even number of distinct parts}). \end{aligned}$$

Remark. It is crucial to note that p_d^o is *different* from p_{odd} from Lecture 5: here we look at the partitions of n into an odd number of distinct parts while in lecture 5 we focused on partitions into parts of odd cardinality.

In the proof we use the following definitions related to the Ferrers diagram of a partition.

Definition 6.2 (The slope and front of a partition). Look at a generic partition into $k+1$ distinct parts of $n \in \mathbb{N}$, and write it as $\lambda = (\lambda_k, \lambda_{k-1}, \dots, \lambda_1, \lambda_0)$, where $\lambda_0 < \lambda_1 < \dots < \lambda_{k-1} < \lambda_k$ such that $\sum_{i=0}^k \lambda_i = n$. Then we call $\text{front}(\lambda) := \lambda_0$ *the front* of the partition.

The slope of the partition is given by the largest integer m , such that $\lambda_i - \lambda_{i-1} = 1$ for all $i \in \{k-m+1, \dots, k\}$. We will denote this by $\text{slope}(\lambda) = m \in \mathbb{N}$.

The definitions are illustrated on the left side of [Figure 6.1](#).

Next we introduce a "move" to transform an odd partition (a partition with an odd number of parts) into an even partition.

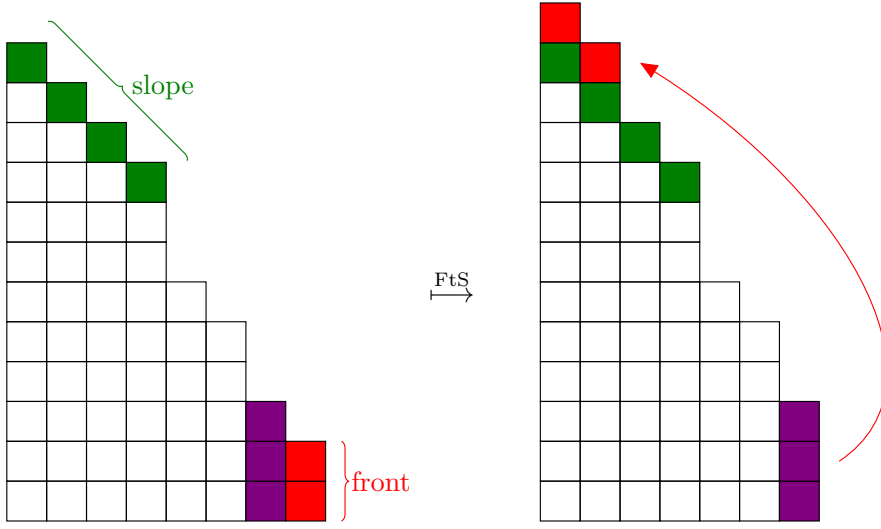


Figure 6.1: The diagram on the left side highlights the slope in green and the front in red. The purple blocks are the successor of the front. The right hand side shows the partition obtained by moving the front over the slope.

Definition 6.3 ("Moving the front over the slope"). Let $\lambda = (\lambda_k, \dots, \lambda_0)$ be a partition of $n \in \mathbb{N}$ and let $\lambda_0 = m \in \mathbb{N}$ be its front, also assume that $m \leq k$. Then we define

$$\text{FtS}(\lambda) := (\lambda_k + 1, \dots, \lambda_{k-m+1} + 1, \lambda_{k-m}, \dots, \lambda_1).$$

On the diagram side this corresponds to removing the front part and redistribute its m squares one by one from the biggest part on until there are none left. ^{III}

Remark. An example application of FtS is shown in Figure 6.1. Note that if $\lambda \vdash n$ is an odd/even partition into distinct parts, then by construction $\text{FtS}(\lambda) \vdash n$ is an even/odd partition into distinct parts.

Now we are ready for the proof of Theorem 6.1. For reasons of readability the proof will be split into several propositions.

Proposition 6.4.

$$\prod_{k=1}^{\infty} (1 - x^k) = \sum_{n=0}^{\infty} (p_d^e(n) - p_d^o(n)) x^n.$$

Proof. As in the proof of Theorem 5.6 and the other results involving generating functions we compare coefficients. We have seen that $\prod_{k=1}^{\infty} (1 + x^k) = \sum_{n=0}^{\infty} p_{\text{dist}} x^n$. Now we have to track the signs. A summand from the expanded product on the left has a minus sign if it is composed of an odd number of nontrivial factors, otherwise the sign is plus. Hence, the coefficient of x^n is exactly $p_d^e(k) - p_d^o(k)$.

^{III}The notation FtS is a shortcut for for *Front to Slope*.

For example the coefficient of x^7 in the product $(1-x)\cdots(1-x^7)$ is $3-2$, i.e., 1, because 7 has three even partitions $1+6$, $2+5$ and $3+4$ into distinct parts and two odd partitions 7 and $1+2+4$ into distinct parts. \square

The next lemma shows that $p_d^e(n) - p_d^o(n)$ is zero for most cases of n , actually it is non-zero only for pentagonal numbers.

Lemma 6.5.

$$p_d^e(n) - p_d^o(n) = (-1)^k \delta \left[n = \frac{(3k \pm 1)k}{2} \right].$$

Proof. We start by assigning another parameter Δ to a partition λ with distinct parts. Given the Ferrers diagram of $\lambda = (\lambda_k, \dots, \lambda_0)$ we distinguish two cases.

If the front and the slope of λ share a square we set $\Delta(\lambda) = 1$, this is illustrated on the left side of [Figure 6.2](#). Note that this case is characterized by $\text{slope}(\lambda) = k+1$. Otherwise, we set $\Delta(\lambda) = 0$, this is illustrated on the right side of [Figure 6.2](#) and corresponds to $\text{slope}(\lambda) < k+1$.

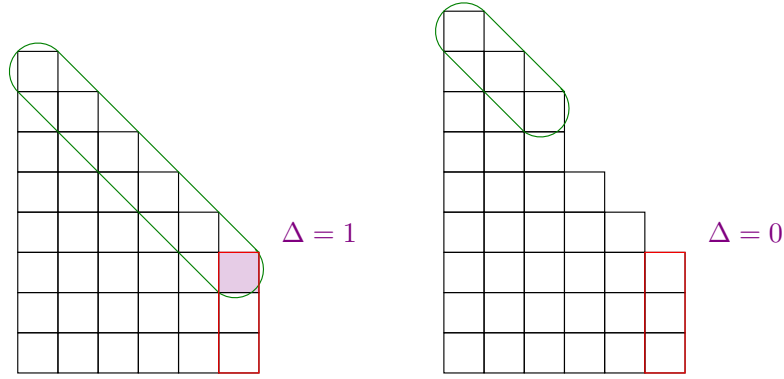


Figure 6.2: The two cases: $\Delta(\lambda) = 1$ and $\Delta(\lambda) = 0$

We partition the set of all partitions $\lambda \vdash n$ with distinct parts into three classes as follows:

Type I: $\text{slope}(\lambda) \geq \text{front}(\lambda) + \Delta(\lambda)$,

Type II: $\text{slope}(\lambda) < \text{front}(\lambda) - \Delta(\lambda)$,

Type III: neither of the other types.

The key to the proof of the lemma will be a sign reverting bijection between the partitions of Type I and Type II. Let us, however, first look at *Type III*. From the definition of the other two types we directly see that a Type III partition λ has $\Delta(\lambda) = 1$. Using this it follows that

$$\text{slope}(\lambda) \in \{\text{front}(\lambda) - 1, \text{front}(\lambda)\}.$$

We distinguish the two cases.

Case 1: $k = \text{slope}(\lambda) = \text{front}(\lambda)$.

The number of boxes of a Ferrers diagram sum up to the n of the corresponding partition. Figure 6.3 indicates a partition of the Ferrers diagram into three "triangles". The number of boxes in each of the blue and the orange triangle is $1+2+\dots, k-1 = \binom{k}{2}$ and the number of boxes in the purple triangle is $1+2+\dots, k = \binom{k+1}{2}$. In total this makes

$$n = 2\binom{k}{2} + \binom{k+1}{2} = k^2 - k + \frac{k^2 + k}{2} = \frac{3k^2 - k}{2},$$

hence, in this case n is a pentagonal number.

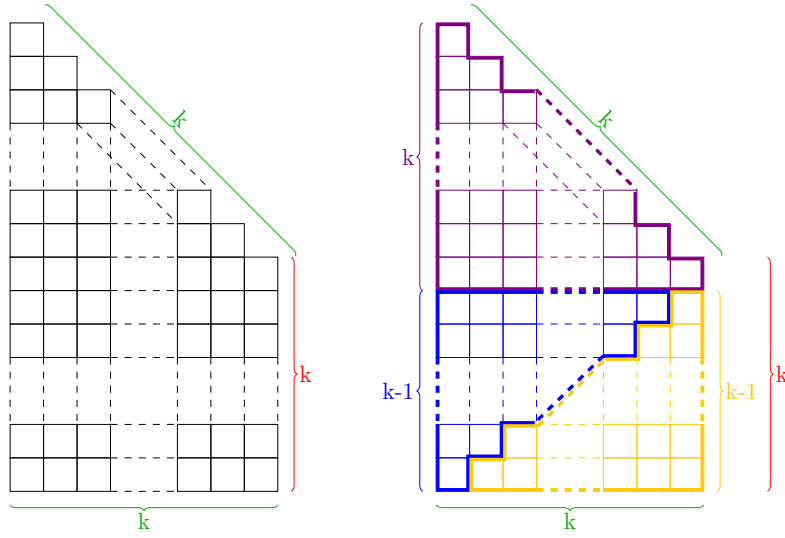


Figure 6.3: On the left there is a schematic representation of the first case. The right side shows how to partition the shape into three triangles.

Case 2: $k = \text{slope}(\lambda) = \text{front}(\lambda) - 1$.

In this case we use the partition of the Ferrers diagram indicated in Figure 6.4. We obtain

$$n = \binom{k}{2} + 2\binom{k+1}{2} = \frac{k^2 - k}{2} + k^2 + k = \frac{3k^2 + k}{2},$$

hence again n is a pentagonal number.

Together the two cases show that for every pentagonal number there is a unique Type III partition. These partitions contribute $(-1)^k$ to the difference $p_d^e(n) - p_d^o(n)$ whenever $n = \frac{(3k \pm 1)k}{2}$.

A bijection between Type I and Type II.

Let $\lambda \vdash n$ be a partition into distinct parts of Type I, so $\text{slope}(\lambda) \geq \text{front}(\lambda) + \Delta(\lambda)$, in particular $\text{front}(\lambda) \leq \text{slope}(\lambda) - \Delta(\lambda) \leq k$. Therefore, we can transform λ into λ' by moving the front over the slope, i.e., $\lambda' = \text{FtS}(\lambda)$. We simplify notation by letting: $S = \text{slope}(\lambda)$, $F = \text{front}(\lambda)$, $S' = \text{slope}(\lambda')$, and $F' = \text{front}(\lambda')$.

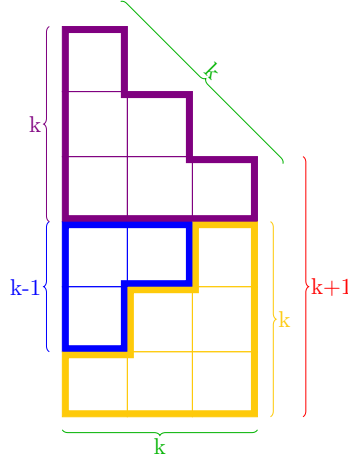


Figure 6.4: A partition of the Ferrers Diagram into three triangles for Case 2.

By construction of λ' via $\text{FtS}(\lambda)$ we have $S' = F$ and $F' \geq F + 1$ whence $S' \leq F' - 1$. If $\Delta(\lambda') = 0$, this show that $S' < F' - \Delta(\lambda')$ so that λ' is Type II. If, however, $\Delta(\lambda') = 1$, then the FtS operation has added a box to the smallest part of λ' which used to be the second to largest part of λ , therefore $F' \geq F + 2$ in this case and again $S' < F' - \Delta(\lambda')$ so that λ' is Type II.

If $\lambda \vdash n$ is a partition into distinct parts of *Type II*, then we can apply a *slope to front* operation, i.e., the inverse of FtS . By construction of λ' we have $F' = S$ and $S' \geq S$ whence $S' \geq F'$. If $\Delta(\lambda') = 0$ we have $S' \geq F' + \Delta(\lambda')$ so that λ' is Type I. If $\Delta(\lambda') = 1$ we note that since S' reaches the front S' is equal to the number of parts in λ' . Since the new partition λ' has one part more than λ we have $S' \geq S + 1 = F' + 1$, i.e., $S' \geq F' + \Delta(\lambda')$ so that λ' is Type I.

We have proven that the *Type I* and *Type II* partitions are in bijection via a bijective map that changes the parity, hence, for $n \neq \frac{3k+1}{2}$ we get $p_d^e(n) - p_d^o(n) = 0$. Together with the analysis of the *Type III* partitions this concludes the proof of the lemma. \square

Finally we prove Eulers pentagonal numbers theorem.

Proof of Theorem 6.1. Using Proposition 6.4 and Lemma 6.5 we get

$$\prod_{k=0}^{\infty} (1 - x^k) = \sum_{k=0}^{\infty} (p_d^e(k) - p_d^o(k)) x^k = 1 + \sum_{k=1}^{\infty} (-1)^k \left(x^{\frac{(3k-1)k}{2}} + x^{\frac{(3k+1)k}{2}} \right) = \sum_{k=-\infty}^{\infty} (-1)^k x^{\frac{(3k-1)k}{2}}.$$

\square

Where does the name *pentagonal number* come from? The number $c_k = \frac{(3k-1)k}{2}$ is the number of dots in a collection of k nested pentagons as in Figure 6.5. Each side of the largest pentagon in the nesting corresponding to c_k has k dots, hence, $c_k - c_{k-1} = 3k - 2$. This recursion together with the initial condition $c_1 = 1$ yields the formula for c_k .

The following proposition is a consequence of the pentagonal number theorem.

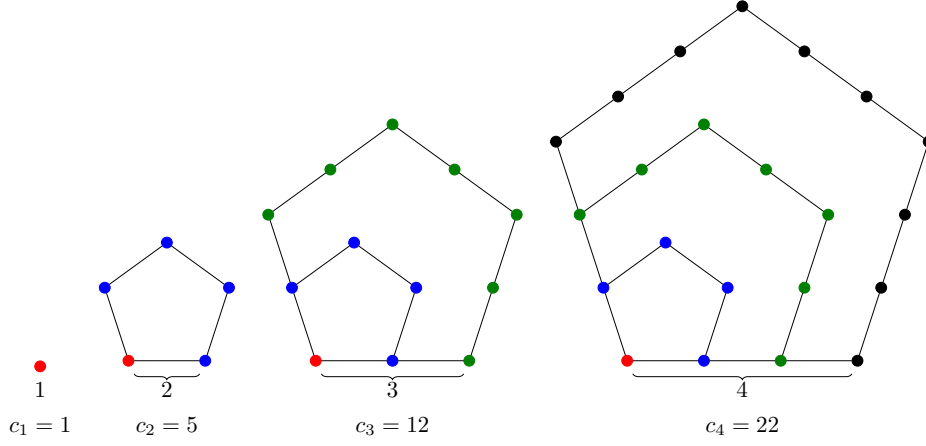


Figure 6.5: The nested pentagons corresponding to c_1 , c_2 , c_3 and c_4 .

Proposition 6.6. *The partition numbers satisfy the recursion*

$$\begin{aligned} p(n) &= p(n-1) + p(n-2) - p(n-5) - p(n-7) + p(n-12) + \dots \\ &= \sum_{k \geq 1} (-1)^k \left(p\left(n - \frac{(3k-1)k}{2}\right) + p\left(n - \frac{(3k+1)k}{2}\right) \right). \end{aligned}$$

Proof. Recall that the generating function of partitions satisfies

$$\sum_{n=0}^{\infty} p(n)x^n = \prod_{k \geq 1} \frac{1}{1-x^k}.$$

This then yields that

$$\sum_{n=0}^{\infty} p(n)x^n \prod_{k \geq 1} (1-x^k) = 1.$$

Using the pentagonal number theorem we have another way to write $\prod_{k \geq 1} (1-x^k)$. This allows to rewrite the equation:

$$\left(\sum_{n=0}^{\infty} p(n)x^n \right) \left(\sum_{k=-\infty}^{\infty} (-1)^k x^{\frac{(3k-1)k}{2}} \right) = 1.$$

The coefficient of x^n in this product is $p(n) - p(n-1) - p(n-2) + p(n-5) + p(n-7) - \dots$. The coefficient of x^n on the right side is zero for all $n > 0$. This concludes the proof. \square

Remark. Since there are $\mathcal{O}(\sqrt{n})$ pentagonal numbers $\leq n$ we can compute $p(n)$ in $\mathcal{O}(\sqrt{n})$ steps if $p(m)$ for all $m < n$ is already known. This shows that $p(n)$ can be computed in $\mathcal{O}(n\sqrt{n})$.

6.1 Fibonacci sequence

The Fibonacci sequence was introduced in the renaissance by Leonardo de Pisa to model the growth of a populations of rabbits. .

Definition 6.7. The *Fibonacci sequence* is the sequence $(F_n)_{n \in \mathbb{N}}$ satisfying the recursion:

$$F_0 := 0, F_1 := 1, \quad F_{n+1} := F_n + F_{n-1}.$$

There are many other models or problems that can be described by the Fibonacci sequence.

Example 6 (Counting with 1's and 2's). Let $f(n) := \#(\text{ways of writing } n \text{ as a sum of 1 and 2})$, then $f(n)$ is given by the $(n+1)$ -th Fibonacci number F_{n+1} . To see this note that clearly $f(1) = 1$ and $f(2) = 2$. Now given $f(n-1)$ and $f(n-2)$, we find $f(n) = f(n-1) + f(n-2)$, by either adding a 1 to a composition of $n-1$ ($f(n-1)$ ways) or adding a 2 to a composition of $n-2$ ($f(n-2)$ ways).

Remark. Instead of compositions of n as sums of 1s and 2s we can equivalently think of tilings of a $1 \times n$ -board with monominoes and dominoes.

Example 7 (Reflections in two glass layers). Take two glass layers and stack them on top of each other. A light-ray can either pass through it or reflect at the top, the middle (where the two layers meet) or the bottom of the stacked glass layers. Then the number of possibilities for the light ray to pass through the glass and be reflected n times—call it g_n —adheres to the Fibonacci recursion with $g_0 = 1$ and $g_1 = 2$, i.e. $g_n = g_{n-1} + g_{n-2}$, since the last reflection was either at the boundary (g_{n-1} possibilities) or the middle of the glass, at which point its second to last reflection has to be at the boundary (g_{n-2} possibilities).

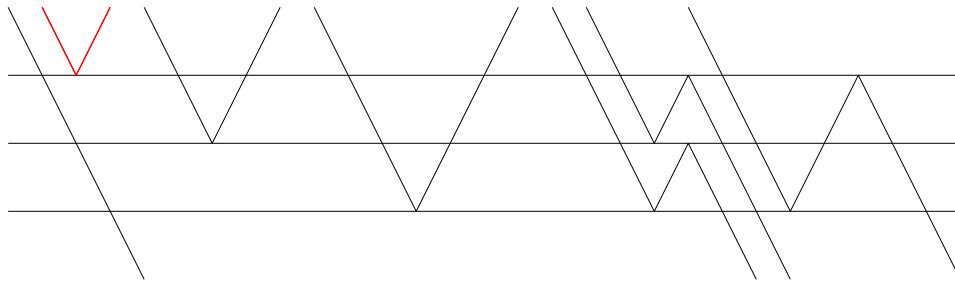


Figure 6.6: The different ways a light ray can be reflected up to 3 times. The red reflected light ray does not count, because it does not pass through the glass

There are many nice identities involving Fibonacci numbers. The following proposition collects a few of them.

Proposition 6.8 (Identities for $f(n)$). (A) $1 + f(1) + f(2) + \dots + f(n) = f(n+2)$,

(B) $f(0) + f(2) + \dots + f(2n) = f(2n+1)$,

$$(C) f(m+n) = f(m) \cdot f(n) + f(m-1) \cdot f(n-1),$$

$$(D) \binom{n}{0} + \binom{n-1}{1} + \dots + \binom{n-\lfloor n/2 \rfloor}{\lfloor n/2 \rfloor} = f(n).$$

$$(E) f(n)^2 = f(n-1) \cdot f(n+1) + (-1)^n$$

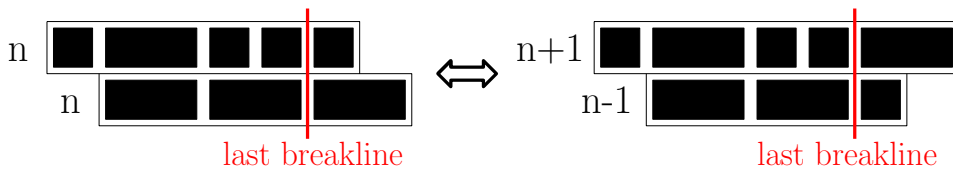
Proof. (A) Given a monomino-domino tiling (m/d-tiling) of an $1 \times (n+2)$ board, delete the last domino that appeared in the tiling from left to right and the chain of monominoes directly after it, e.g. $(2, 1, 2, 1, 1, 1, [2], 1, 1, 1) \rightarrow (2, 1, 2, 1, 1, 1)$. Then this gives a bijection between F_{n+2} and $1 + F_0 + \dots + F_n$. For the inverse just add a sequence $2, 1, 1, 1, \dots$ with $n-m$ 1s to a tiling in F_m ($m \leq n$) to make it a tiling in F_{n+2} .

(B) This is very similar to [A], this time we look for the rightmost monomino (it exists because $2n+1$ is odd!) and remove it together with the dominoes to its right. The result is a tiling of an even m .

(C) Take the $m+n$ -board and split it into two boards of size m and n respectively. Either the splitting is at a break line (no domino overlapped both parts) then we get $F_m \cdot F_n$ possibilities to tile the parts independently; or a domino was sitting where we split, so we keep this domino and have $F_{m-1} \cdot F_{n-1}$ possibilities to tile the left and right part.

(D) Let \mathcal{F} be the set of all tilings of an $1 \times n$ -board, so $|\mathcal{F}| = F_n$. Let $\mathcal{F}_k \subset \mathcal{F}$ be the subset of those tilings which consist of $n-k$ pieces, i.e., k of the pieces are dominoes. It follows that $|\mathcal{F}_k| = \binom{n-k}{k}$ and \mathcal{F} is the disjoint union of the \mathcal{F}_k with $0 \leq k \leq \lfloor n/2 \rfloor$.

(E) We use the monomino-domino tiling again and show a bijection between the two sides. If a rightmost breakline exists, then swapping the upper and lower halves



to the right of the breakline is a bijection. Thus, we have a bijection for pairs of tilings with a breakline. If there is no breakline, then the monomino-domino tiling representation consists of dominoes only. This is only possible if both boards are of even length. Depending on whether n is even or odd there is exactly one such tiling on the left respectively right side. This tiling is accounted for by the $(-1)^n$ term.

□

Binet's Formula and Linear Recurrences

In the previous lecture we met Fibonacci numbers and proved some nice formulas involving them. We start this lecture with the derivation of an explicit formula for F_n .

Proposition 7.1 (Binet's Formula).

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

Proof. Consider the *generating function* of the Fibonacci sequence:

$$F(z) := \sum_{n \geq 0} F_n z^n.$$

We claim that this generating function satisfies the functional equation

$$F(z) \cdot (1 - z - z^2) = z.$$

To see this we multiply $F(z)$ with z and z^2 :

$$zF(z) = \sum_{n \geq 1} F_{n-1} z^n \quad \text{and} \quad z^2 F(z) = \sum_{n \geq 2} F_{n-2} z^n.$$

Using this we get $F(z) \cdot (1 - z - z^2) = F(z) - zF(z) - z^2 F(z) =$

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

Now recall that $F_0 = 0$, $F_1 = 1$ and $F_n = F_{n-1} + F_{n-2}$ for all $n \geq 2$. This proves the claim.

For the following we use partial fraction decomposition as a black box. It tells us that

$$\frac{1}{1-x-x^2} = \frac{1}{(1-\Phi x)(1-\bar{\Phi} x)} = \frac{a}{1-\Phi x} + \frac{b}{1-\bar{\Phi} x}$$

With Φ and $\bar{\Phi}$ being the roots of $1-x-x^2$ and a, b being appropriate constants. A standard computation shows that $\Phi = \frac{1+\sqrt{5}}{2} \approx 1,61803$, $\bar{\Phi} = \frac{1-\sqrt{5}}{2} \approx -0,61803$, $a = \frac{\Phi}{\sqrt{5}}$

and $b = \frac{\bar{\Phi}}{\sqrt{5}}$. We thus get:

$$\begin{aligned} \sum_{n \geq 1} F_n z^n &= F(z) = \frac{z}{1 - z - z^2} = z \cdot \left(\frac{a}{1 - \Phi z} + \frac{b}{1 - \bar{\Phi} z} \right) \\ &= z \cdot \left(\frac{\frac{\Phi}{\sqrt{5}}}{1 - \Phi z} + \frac{\frac{\bar{\Phi}}{\sqrt{5}}}{1 - \bar{\Phi} z} \right) = \frac{z}{\sqrt{5}} \cdot \left(\frac{\Phi}{1 - \Phi z} + \frac{\bar{\Phi}}{1 - \bar{\Phi} z} \right) \\ &\stackrel{\text{geom. series}}{=} \frac{z}{\sqrt{5}} \cdot \left(\Phi \cdot \sum_{n \geq 0} (\Phi z)^n - \bar{\Phi} \cdot \sum_{n \geq 0} (\bar{\Phi} z)^n \right) = \sum_{n \geq 1} \left(\frac{\Phi^n - \bar{\Phi}^n}{\sqrt{5}} \right) z^n \end{aligned}$$

Comparing the coefficients of z^n and plugging in the values of Φ and $\bar{\Phi}$ we now get Binet's formula:

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

□

We next give a second proof of the proposition which is using some linear algebra instead of generating functions.

Proof. We first note that Fibonacci Numbers can be generated by iterated matrix multiplication:

$$\text{Let } A := \begin{pmatrix} 1 & 1 \\ 1 & 0 \end{pmatrix} \text{ then } \begin{pmatrix} F_{n+1} \\ F_n \end{pmatrix} = A \cdot \begin{pmatrix} F_n \\ F_{n-1} \end{pmatrix} = A^n \cdot \begin{pmatrix} F_1 \\ F_0 \end{pmatrix} = A^n \cdot \begin{pmatrix} 1 \\ 0 \end{pmatrix}$$

The characteristic polynomial of A is $P_A(x) = (1 - x)(-x) - 1 = x^2 - x - 1$. This factors as $P_A(x) = (x - \Phi) \cdot (x - \bar{\Phi})$ with Φ and $\bar{\Phi}$ being the same numbers as in the first proof. In particular Φ is the *golden ratio*. Since Φ and $\bar{\Phi}$ are distinct we know that A can be diagonalized. Associated to the roots of $P_A(x)$, i.e., the eigenvalues, we find the following eigenvectors.

$$v_\Phi = \begin{pmatrix} 2 \\ -1 + \sqrt{5} \end{pmatrix} \quad \text{and} \quad v_{\bar{\Phi}} = \begin{pmatrix} 2 \\ -1 - \sqrt{5} \end{pmatrix}$$

From linear algebra we know that $A = Q \cdot D \cdot Q^{-1}$ where the diagonal matrix D and the transformation matrices are given as follows:

$$D = \begin{pmatrix} \Phi & 0 \\ 0 & \bar{\Phi} \end{pmatrix} \quad Q = [v_\Phi \ v_{\bar{\Phi}}] = \begin{pmatrix} 2 & 2 \\ -1 + \sqrt{5} & -1 - \sqrt{5} \end{pmatrix} \quad Q^{-1} = \begin{pmatrix} 1 + \sqrt{5} & 2 \\ -1 + \sqrt{5} & 2 \end{pmatrix} \cdot \frac{1}{4 \cdot \sqrt{5}}$$

The good news is that $A^n = Q \cdot D^n \cdot Q^{-1}$ where D^n is diagonal with diagonal entries Φ^n and $\bar{\Phi}^n$. A standard computation yields $(A^n)_{2,1} = F_n = \frac{1}{\sqrt{5}}(\Phi^n - \bar{\Phi}^n)$. □

From Binet's formula we get the growth rate of the Fibonacci numbers: $\lim_{n \rightarrow \infty} \frac{F_{n+1}}{F_n} = \Phi$, i.e., the growth rate is the golden ratio. One of the nice properties of this number is that its continued fraction expansion consists of an infinite sequence of 1s. A proof can be given by an induction which shows:

$$\frac{F_{n+1}}{F_n} = 1 + \frac{1}{1 + \frac{1}{1 + \frac{1}{\ddots}}} \left\} n \text{ times}$$

7.1 Solving linear recurrences

In the first part of this lecture we found an explicit formula for Fibonacci numbers. These numbers are given by a specific linear recurrence. Now we look at a sequence given by a general linear recurrence and study how to obtain an explicit formula for the entries of the sequence.

A typical linear recurrence is given by

$$f_{n+k} = b_1 f_{n+k-1} + \cdots + b_k f_n \quad (7.6)$$

and initial conditions: $f_0 = c_0, f_1 = c_1, \dots, f_{k-1} = c_{k-1}$

For convenience we write $f_{n+k} + a_1 f_{n+k-1} + \cdots + a_k f_n = 0$ with $a_k = -b_k$. We will work with the generating function $F(x) := \sum_{n \geq 0} f_n x^n$ of the sequence. The following four steps are a high level description of our approach:

1. Write $F(x)$ as a rational function $F(x) = Q(x)/P(x)$.
2. Let $\hat{P}(x)$ be the reflected polynomial of $P(x)$ and determine the roots of $\hat{P}(x)$.
3. Use the roots to find the partial fraction decomposition of $F(x)$.
4. Expand the terms of the partial fraction decomposition as geometric series and collect terms belonging to x^n to find f_n .

1. Define $Q(x) := F(x) + a_1 x F(x) + \cdots + a_k x^k F(x)$ and note that due to the recurrence coefficients of x^n in $Q(x)$ are 0 for all $n \geq k$. Therefore $Q(x)$ is a polynomial of degree $\leq k-1$. In fact we can write $Q(x)$ explicitly as $Q(x) = c_0 + (c_1 + a_1 c_0)x + (c_2 + a_1 c_1 + a_2 c_0)x^2 + \cdots + (\sum_{i=0}^{k-1} c_i a_{k-1-i})x^{k-1}$ with $a_0 = 1$ in the last term. We can thus write $F(x)$ as a rational function:

$$F(x) = \frac{Q(x)}{1 + a_1 x + a_2 x^2 + \cdots + a_k x^k} =: \frac{Q(x)}{P(x)} \quad (7.7)$$

2. Let $\hat{P}(x) = x^k + a_1 x^{k-1} + \cdots + a_k$ be the reflected polynomial of $P(x) = 1 + a_1 x + \cdots + a_k x^k$. Suppose that we know the factorization $\hat{P}(x) = (x - \alpha_1)^{m_1} \cdots (x - \alpha_s)^{m_s}$ with $\sum m_i = k$ of $\hat{P}(x)$. A simple calculation shows that $P(x) = x^k \hat{P}(\frac{1}{x})$. Hence, we have the following expression for $P(x) = x^k \hat{P}(\frac{1}{x}) = (1 - \alpha_1 x)^{m_1} \cdots (1 - \alpha_s x)^{m_s}$.

3. Next we will be looking for the partial fraction decomposition of $F(x)$.

Theorem 7.2 (Partial fraction decomposition). *If*

$$P(x) = x^k \hat{P}\left(\frac{1}{x}\right) = (1 - \alpha_1 x)^{m_1} \cdots (1 - \alpha_s x)^{m_s}$$

is a polynomial of degree $k = \sum_i m_i$, then there exist constants $\gamma_{11}, \gamma_{12}, \dots, \gamma_{1m_1}, \gamma_{21}, \dots, \gamma_{2m_2}, \dots, \gamma_{s1}, \dots, \gamma_{sm_s}$ such that :

$$\frac{1}{P(x)} = \sum_{j=1}^s \sum_{i=1}^{m_j} \frac{\gamma_{ij}}{(1 - \alpha_j x)^i} \quad (7.8)$$

Next we show how to rewrite a generic term of the partial fraction decomposition by using the binomial theorem for negative exponents and $(-i)_n = (-1)^n (n + i - 1)_n$;

$$\frac{1}{(1 - \alpha x)^i} = \sum_{n \geq 0} \binom{-i}{n} (-\alpha x)^n = \sum_{n \geq 0} \binom{n + i - 1}{n} (\alpha x)^n = \sum_{n \geq 0} \binom{n + i - 1}{i - 1} (\alpha x)^n \quad (7.9)$$

4. From $F(x) = Q(x)/P(x)$ together with 7.8 and 7.9 we find that^{IV}

$$f_n = [x^n] \left(Q(x) \sum_{j=1}^s \sum_{i=1}^{m_j} \sum_{t \geq 0} \gamma_{ij} \binom{t + i - 1}{i - 1} \alpha_j^t x^t \right) \quad (7.10)$$

If $Q(x) = \sum_{i=0}^{k-1} d_i x^i$ and the polynomial $P(x)$ has no multiple root ($m_j = 1 \forall j$) then:

$$\begin{aligned} f_n &\stackrel{(7.8)}{=} [x^n] \left(Q(x) \sum_{j=1}^k \gamma_j \frac{1}{1 - \alpha_j x} \right) = [x^n] \left(Q(x) \sum_{j=1}^k \gamma_j \sum_{t \geq 0} \alpha_j^t x^t \right) \\ &= \sum_{i=0}^{k-1} d_i \left(\sum_{j=1}^k \gamma_j \alpha_j^{n-i} \right) = \sum_{j=1}^k \left(\sum_{i=0}^{k-1} d_i \frac{\gamma_j}{\alpha_j^i} \right) \alpha_j^n \end{aligned}$$

hence, $f_n = \sum_{j=1}^k g_j \alpha_j^n$.

Claim: In the general case we get

$$f_n = \sum_{j=1}^s g_j(n) \alpha_j^n, \quad \text{where } g_j(n) \text{ is a polynomial in } n \text{ of degree } < m_j \quad (7.11)$$

Proof of claim 7.11. Recall from 7.10 that $f_n = [x^n] \left(\sum_{j=1}^s Q(x) \sum_{i=1}^{m_j} \sum_{t \geq 0} \gamma_{ij} \binom{t + i - 1}{i - 1} \alpha_j^t x^t \right)$. To prove the claim it is thus enough to show that for a fixed j :

$$[x^n] \left(Q(x) \sum_{i=1}^{m_j} \sum_{t \geq 0} \gamma_{ij} \binom{t + i - 1}{i - 1} \alpha_j^t x^t \right) = g_j(n) \alpha_j^n$$

^{IV}The notation $[x^n]A(x)$ is used to refer to the coefficient of x^n in the power series or polynomial $A(x)$.

where $g_j(n)$ is a polynomial in n of degree $\leq m-1$.

Using $Q(x) = \sum_{l=0}^{k-1} d_l x^l$ and letting $m = m_j$ and $\alpha = \alpha_j$ and $\gamma_i = \gamma_{ij}$ we get:

$$\begin{aligned}
 [x^n] & \left(Q(x) \sum_{i=1}^m \sum_{t \geq 0} \gamma_i \binom{t+i-1}{i-1} \alpha^t x^t \right) \\
 &= d_0 \sum_{i=1}^m \gamma_i \binom{n+i-1}{i-1} \alpha^n + d_1 \sum_{i=1}^m \gamma_i \binom{n+i-2}{i-1} \alpha^{n-1} + \cdots + d_{k-1} \sum_{i=1}^m \gamma_i \binom{n+i-k}{i-1} \alpha^{n-k+1} \\
 &= d_0 \sum_{i=1}^m \frac{\gamma_i}{(i-1)!} (n+i-1)_{i-1} \alpha^n + d_1 \sum_{i=1}^m \frac{\gamma_i}{(i-1)!} \frac{1}{\alpha} (n+i-2)_{i-1} \alpha^n \\
 & \quad + \cdots + d_{k-1} \sum_{i=1}^m \frac{\gamma_i}{(i-1)!} \frac{1}{\alpha^{k-1}} (n+i-k)_{i-1} \alpha^n \\
 &= g(n) \alpha^n
 \end{aligned}$$

To see that $g(n)$ is indeed a polynomial in n of degree $\leq m-1$ note that only the falling factorials depend on n and that $(n-s)_r$ is a polynomial in n of degree r .

Applying this to each of the roots α_j of $\hat{P}(x)$ in 7.10 we get $f_n = \sum_{j=1}^s g_j(n) \alpha_j^n$. \square

The following example shows that in practical situations we can simplify the calculation by treating the coefficients of the polynomials $g_j(n)$ as unknowns of a $k \times k$ system of linear equations.

Example 8. Consider the linear recursion $a_n = 4a_{n-1} - 5a_{n-2} + 2a_{n-3}$ with initial conditions: $a_0 = 2$, $a_1 = 6$, and $a_2 = 11$. The generating function $A(x) = \sum a_n x^n$ satisfies $(1 - 4x + 5x^2 - 2x^3)A(x) = P(x)A(x) = Q(x)$. Since $\hat{P}(x) = x^3 - 4x^2 + 5x - 2 = (x-1)^2(x-2)$ there are coefficients a , b and c such that $\frac{Q(x)}{P(x)} = \frac{a}{(1-x)^2} + \frac{b}{1-x} + \frac{c}{1-2x}$. From the theory 7.11 we know, that there are polynomials $f(n)$ of degree one and $g(n)$ of degree zero such that

$$a_n = f(n)1^n + g(n)2^n = (An + B)1^n + C2^n.$$

With the initial conditions and the coefficients A , B , C as variables we get:

$$\begin{aligned}
 a_0 &= 2 = B + C \\
 a_1 &= 6 = A + B + 2C \\
 a_2 &= 11 = 2A + B + 4C
 \end{aligned}$$

This is a linear system, with the unique solution $A = 3$, $B = 1$ and $C = 1$. Hence, $a_n = (3n+1)1^n + 1 \cdot 2^n = 1 + 3n + 2^n$.

We close the lecture by hinting at another way of obtaining Binet's Formula (Proposition 7.1) and formulas for more general linear recurrences. The exponential generating

function of the Fibonacci numbers is given by $G(z) = \sum_{n \geq 0} F_n \frac{z^n}{n!}$. From the recursion $F_{n+2} = F_{n+1} + F_n$ we get

$$\sum_{n \geq 0} F_{n+2} \frac{z^n}{n!} = \sum_{n \geq 0} F_{n+1} \frac{z^n}{n!} + \sum_{n \geq 0} F_n \frac{z^n}{n!}, \quad \text{hence} \quad G''(z) = G'(z) + G(z).$$

The initial conditions $F_0 = 0$ and $F_1 = 1$ yield evaluations $G(0) = 0$ and $G'(0) = 1$. Altogether we obtain a linear differential equation. The theory of linear differential equations tells us how to solve such a system. We omit the details and just state the solution $G(z) = \frac{1}{\sqrt{5}} \left(e^{\frac{1+\sqrt{5}}{2}z} - e^{\frac{1-\sqrt{5}}{2}z} \right)$. Expanding this function as a power series we get $G(z) = \sum_{n \geq 0} \frac{1}{\sqrt{5}} \left(\frac{1+\sqrt{5}}{2}^n + \frac{1-\sqrt{5}}{2}^n \right) \frac{z^n}{n!}$. Extracting the coefficient of $z^n/n!$ we again obtain Binet's Formula.

Formal Power Series and the Symbolic Method

In the last chapter, we have seen that the generating function can be a useful tool, when dealing with (integer) sequences. The theory of power series developed in Analysis I is not always helpful in this context though. For example, the convergence of a series, while a big part of the theory in Analysis, is not really relevant in this context. On the other hand, while in Analysis we tried to deal with infinite sums, here we will make sure that calculating any element in the sequence requires only finitely many steps. We will therefore have a look at the theoretical foundations for the power series used in combinatorics in this chapter.

8.1 Formal power series

Example 9.

$$\sum_{k \geq 0} k! x^k$$

is an important series in Combinatorics, it is the sequence of factorials. It would be a pity not to consider it, just because its convergence radius in classical analysis is 0. It might also seem that

$$\prod_{k \geq 0} \frac{1}{1 - x^k} = \prod_{k \geq 0} \sum_{i \geq 0} x^{ki}$$

is not finitely computable, but it actually is, because for any n , we can truncate the product and the sum to only consider the first n elements. We know that if we do not choose x^0 in any of the later factors of the infinite product, then the exponent of x will be higher than n .

We will however make use of some results from Analysis in the form of shortcut notation:

$$\sum_{k \geq 0} x^k =: \frac{1}{1 - x}$$

$$\sum_{k \geq 0} \frac{x^k}{k!} =: e^x$$

Definition 8.1. A *Formal Power Series* (FPS) is an integer sequence, but instead of writing it in the form $(a_k)_{k \in \mathbb{N}}$, we write it as

$$\sum_{k \geq 0} a_k x^k$$

Remark. x is not really a variable from any space whatsoever, it just helps us preserve the order of the elements of the integer sequence.

Definition 8.2. We define addition, multiplication and scalar multiplication on these power series as expected:

$$\begin{aligned} \sum_{k \geq 0} a_k x^k + \sum_{k \geq 0} b_k x^k &= \sum_{k \geq 0} (a_k + b_k) x^k \\ \left(\sum_{k \geq 0} a_k x^k \right) \cdot \left(\sum_{k \geq 0} b_k x^k \right) &= \sum_{n \geq 0} \sum_{k=0}^n a_k b_{n-k} x^n \\ c \cdot \left(\sum_{k \geq 0} a_k x^k \right) &= \sum_{k \geq 0} c a_k x^k \end{aligned}$$

Fixing an underlying ring, e.g. \mathbb{C} (or \mathbb{Z}), we can write the space of formal power series as $\mathbb{C}[[x]]$.

Remark. With these operations, the set of formal power series is a commutative ring with $0 = (0)_{n \in \mathbb{N}}$ and $1 = (1, 0, 0, 0, 0, \dots)$. It is actually even an integral domain (if the chosen ring is one), since there are no zero divisors and it forms a module over the chosen ring.

Proposition 8.3. A formal power series has a multiplicative inverse if and only if $a_0 \neq 0$.

Proof. From the definition of the product, in order to have

$$1 = \left(\sum_{k \geq 0} a_k x^k \right) \cdot \left(\sum_{k \geq 0} b_k x^k \right) = \sum_{n \geq 0} \sum_{k=0}^n a_k b_{n-k} x^n = a_0 b_0 + (a_1 b_0 + a_0 b_1) x + (a_2 b_0 + a_1 b_1 + a_0 b_2) x^2 + \dots$$

we need to have $a_0 b_0 = 1$, so $a_0 \neq 0$ is necessary. If $a_0 \neq 0$, we know $b_0 = \frac{1}{a_0}$. From $a_1 b_0 + a_0 b_1 = 0$, we can then deduce $b_1 = -\frac{a_1 b_0}{a_0} = -\frac{a_1}{a_0^2}$ and so on, the precise recursive formula for b_n is

$$b_n = -\frac{\sum_{k=1}^n a_k b_{n-k}}{a_0}$$

By choosing the b_n appropriately, we can therefore make all of the coefficients the same on both sides. \square

Remark. Similarly to \mathbb{Z} , we can still divide by other elements of the ring sometimes and this division is well-defined. For example

$$\frac{\sum_{k \geq 1} x^k}{x} = \sum_{k \geq 0} x^k \Leftrightarrow \sum_{k \geq 1} x^k = x \cdot \left(\sum_{k \geq 0} x^k \right)$$

The well-definition of this operation comes from the fact that $\mathbb{C}[[x]]$ is an integral domain.

Example 10. The series from Example 9 has an inverse. Its inverse can be computed just like we did it in the above proof:

$$\left(\sum_{k \geq 0} k! x^k \right)^{-1} = 1 - x - x^2 - 3x^3 - 13x^4 - 71x^5 - \dots$$

Some other interesting inverse is the inverse of the following power series:

$$f(x) = \frac{e^x - 1}{x} = \sum_{k \geq 0} \frac{x^k}{(k+1)!} \Rightarrow B(x) := f(x)^{-1} = \frac{x}{e^x - 1} = 1 - \frac{x}{2} + \frac{x^2}{12} - \frac{x^4}{90} + \dots$$

The series $B(x)$ is the exponential generating function of the *Bernoulli numbers* that start $b_0 = 1, b_1 = -\frac{1}{2}, b_2 = \frac{1}{6}, b_3 = 0, \dots$ The Bernoulli numbers are a sequence of rational numbers which can also be found as values of Bernoulli polynomials at 0 and 1. Because of the above they are subject to a nice combinatorial identity:

$$\begin{aligned} \sum_{k=0}^n \frac{1}{(k+1)!} \frac{b_{n-k}}{(n-k)!} &= 0 \\ \sum_{k=0}^n \binom{n+1}{n-k} b_{n-k} &= 0 \\ \sum_{k=0}^n \binom{n+1}{k} b_k &= 0 \\ \sum_{k=0}^n \binom{n}{k} b_k &= b_n \end{aligned}$$

Bernoulli and Sums You certainly know the sum $\sum_{k=0}^{n-1} k^1 = \binom{n}{2}$. We will now derive a closed form for $\sum_{k=0}^{n-1} k^s$ in terms of Bernoulli numbers:

$$\begin{aligned} P(x, n) &= \sum_{s \geq 0} \left(\sum_{k=0}^{n-1} k^s \right) \frac{x^s}{s!} = \sum_{s \geq 0} \sum_{k=0}^{n-1} \frac{(kx)^s}{s!} = \sum_{k=0}^{n-1} \sum_{s \geq 0} \frac{(kx)^s}{s!} = \sum_{k=0}^{n-1} e^{kx} = \frac{e^{nx} - 1}{e^x - 1} \\ \Rightarrow xP(x, n) &= B(x) \cdot (e^{xn} - 1) \end{aligned}$$

Now the coefficients from the left hand side can be determined using the right hand side

$$\begin{aligned} xP(x, n) &= \sum_{s \geq 0} \left(\sum_{k=0}^{n-1} k^s \right) \frac{x^{s+1}}{s!} = \left(\sum_{l \geq 0} b_l \frac{x^l}{l!} \right) \left(\sum_{m \geq 1} \frac{(xn)^m}{m!} \right) \\ \Rightarrow \sum_{k=0}^{n-1} k^s &= s! \sum_{l=0}^s \frac{b_l}{l!} \frac{n^{s+1-l}}{(s+1-l)!} = \frac{1}{s+1} \sum_{l=0}^s \binom{s+1}{l} b_l n^{s+1-l} \end{aligned} \quad (8.12)$$

This shows that $\sum_{k=0}^{n-1} k^s$ is a polynomial in n of degree $s+1$.

Example 11.

$s = 3$:

$$\sum_{k=1}^{n-1} k^3 = \frac{1}{4} \sum_{l=0}^3 \binom{4}{l} b_l n^{4-l} = \frac{1}{4} (b_0 n^4 + 4b_1 n^3 + 6b_2 n^2 + 4b_3 n) = \frac{n^4}{4} - \frac{n^3}{2} + \frac{n^2}{4} = \binom{n}{2}^2$$

8.1.1 Composition of FPS

Observation. If $f(x)$ and $g(x)$ are formal power series and $g(0)=0$ (this is another way of saying the constant part is 0), then $f(g(x))$ is well-defined.

Proof.

$$f(x) = \sum_{k \geq 0} a_k x^k, \quad g(x) = \sum_{k \geq 0} b_k x^k$$

$$f(g(x)) = \sum_{n \geq 0} a_n (g(x))^n$$

What is the coefficient of x^n ? It is given by

$$\sum_{k=1}^n a_k \left(\sum_{\substack{i_1 + \dots + i_k = n \\ i_j \geq 1}} b_{i_1} \dots b_{i_k} \right)$$

The fact that $i_j \geq 1$ is only true because $g(x) = 0$, otherwise we would have to deal with an unbounded number of summands, which makes no sense in our world, because the elements of the sequence (coefficient of the FPS) would not be finitely computable. \square

Example 12.

$$f(x) = e^x - 1, \quad g(x) = \ln(1+x) = \sum_{k \geq 1} (-1)^{k+1} \frac{x^k}{k}$$

$$\Rightarrow f(g(x)) = x$$

Example 13.

$$f(x) = e^x, \quad g(x) = 1+x$$

$$\Rightarrow f(g(x)) = e^{x+1}??$$

This actually doesn't make sense in FPS theory, for the constant coefficient you would need to add up

$$\sum_{k \geq 0} \frac{1}{k!}$$

Interestingly, e^{x+y} again makes sense, but we will not go into details here.

Taking roots

$$f(x) = \sqrt{g(x)} \Leftrightarrow f(x)^2 = g(x)$$

Example 14. Consider $f(x) = (1+x)^{-\frac{1}{2}} = \frac{1}{\sqrt{1+x}}$ then $f^2(x) = \frac{1}{1+x}$ or equivalently $f(x)^2 \cdot (1+x) = 1$. We claim that the Binomial Theorem holds in this situation, i.e., $f(x) = (1+x)^{-\frac{1}{2}} = \sum_{k \geq 0} \binom{-\frac{1}{2}}{k} x^k$. To verify the claim we need a little computation:

$$\begin{aligned} f^2(x) &= \left(\sum_{k \geq 0} \binom{-\frac{1}{2}}{k} x^k \right)^2 = \sum_{n \geq 0} \sum_{k=0}^n \binom{-\frac{1}{2}}{k} \binom{-\frac{1}{2}}{n-k} x^n \\ &\stackrel{!}{=} \sum_{n \geq 0} \binom{-1}{n} x^n = \sum_{n \geq 0} (-1)^n x^n = \sum_{n \geq 0} (-x)^n = \frac{1}{1+x} \end{aligned}$$

The third equality is a special instance of the Vandermonde identity. Here we use that this identity holds for values in \mathbb{C} , see Lecture 3.

8.2 Generating functions and the symbolic method

Let \mathcal{A} be a family of "combinatorial objects" of a certain "size". Let further $a_n = \#(\text{members of size } n \text{ in } \mathcal{A})$. The generating function of \mathcal{A} is

$$F_{\mathcal{A}}(x) = A(x) = \sum_{k \geq 0} a_k x^k = \sum_{a \in \mathcal{A}} x^{|a|}$$

Note that $\emptyset \in \mathcal{A}$, $|\emptyset| = 0$. Now for two different families \mathcal{A} and \mathcal{B} , we can write $\mathcal{A} + \mathcal{B}$ for their disjoint union with generating function

$$F_{\mathcal{A}+\mathcal{B}} = F_{\mathcal{A}}(x) + F_{\mathcal{B}}(x)$$

If the elements of some family are composed of one element of \mathcal{A} and one element of \mathcal{B} and their length is defined as the combined length, then this is the equivalent of the cartesian product, so we write this as $\mathcal{A} \times \mathcal{B}$.

$$F_{\mathcal{A} \times \mathcal{B}} = F_{\mathcal{A}}(x) \cdot F_{\mathcal{B}}(x)$$

Finally let \mathcal{A}^* denote the family of finite sequences of objects of \mathcal{A} with length defined as

$$|(a_1, \dots, a_n)| = \sum_{k=0}^n |a_k| \Rightarrow F_{\mathcal{A}^*}(x) = \frac{1}{1 - A(x)}$$

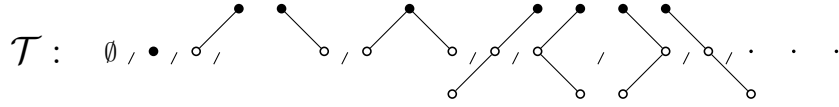
Example 15. Let \mathcal{F} be the set of finite strings of 0s and 1s, but with no consecutive 0s where the size is the length of the string, i.e. the number of bits:

$$\mathcal{F} = \{\emptyset, 0, 1, 01, 10, 11, 010, \dots\}$$

$$\mathcal{F} = \emptyset + \{0\} + \{1, 01\} \times \mathcal{F} \Rightarrow F(x) = 1 + x + (x + x^2)F(x) \Rightarrow F(x) = \frac{1+x}{1-x-x^2}$$

We obtain the generating function of the Fibonacci numbers f_n .

Example 16. \mathcal{T} : binary trees, where the size is given by the number of nodes.



$$\begin{aligned} \mathcal{T} &= \emptyset + \{\cdot\} \times \mathcal{T} \times \mathcal{T} \\ \Rightarrow T(x) &= 1 + xT(x)^2 \end{aligned}$$

This is a Catalan family, which gives rise to the Catalan numbers, maybe the most famous integer sequence in Combinatorics.

Catalan Numbers and q -Enumeration

We continue with the discussion of the results we got from the symbolic method for generating functions, only this time we take a more pedestrian approach to computing these. One important example for this are the *Catalan numbers* $C_n = \#(\text{rooted binary trees of } n \text{ nodes})$. They are defined by the initial conditions $C_0 = C_1 = 1$ and the recursion

$$C_{n+1} = \sum_{k=0}^n C_k C_{n-k}.$$

The recursion formula is based on the fact that for a tree with $n+1$ nodes if there are k nodes in the left subtree of the root, then there must be $n-k$ in the right subtree. The generating function is given by

$$T(x) = \sum_{n=0}^{\infty} C_n x^n$$

and its square by

$$T^2(x) = \sum_{n \geq 0} \underbrace{\left(\sum_{k=0}^n C_k C_{n-k} \right)}_{=C_{n+1}} x^n = \sum_{n=1}^{\infty} C_n x^{n-1}.$$

The last equality sign is due to an index shift. Based on this we again get the equation which was obtained using the symbolic method in the previous lecture, namely

$$xT^2(x) = T(x) - 1.$$

This can be rewritten as

$$T^2(x) - \frac{1}{x}T(x) + \frac{1}{x} = 0$$

if we treat $T(x)$ as a variable while thinking of x as fixed we can use the p - q -formula to get

$$T(x) = \frac{1 \pm \sqrt{1-4x}}{2x}.$$

To see which of the two signs has to be used for $T(x)$ we consider $2xT(x) = 1 \pm \sqrt{1-4x}$ and look at $x=0$. For equality we have to use the $-$ sign, hence, we are left with

$$2xT(x) = 1 - \sqrt{1-4x}.$$

The Generalized Binomial Theorem

$$(1+y)^\alpha = \sum_{k \geq 0} \binom{\alpha}{k} y^k$$

is valid for $0 < \alpha \leq 1$ (In Analysis this is shown via Taylor expansion). Actually the case $\alpha = 1/2$ needed here has been verified in [Example 14](#). We get

$$2xT(x) = 1 - (1-4x)^{1/2} = 1 - \sum_{k \geq 0} \binom{1/2}{k} (-4x)^k, \quad \text{i.e.,} \quad T(x) = \frac{1}{2} \left(1 + \sum_{k \geq 0} \binom{1/2}{k} 4^k (-x)^{k-1} \right)$$

by looking at $k = 0$ this simplifies to $T(x) = \frac{1}{2} \sum_{k \geq 1} \binom{1/2}{k} 4^k (-x)^{k-1}$.

Comparing coefficients we then get:

$$\begin{aligned} C_n &= \frac{1}{2} (-1) \binom{1/2}{n+1} (-4)^{n+1} = \left(\frac{-1}{2} \right) \frac{(1/2)_{n+1}}{(n+1)!} (-4)^{n+1} \\ &= \frac{-1}{2} \frac{2^{n+1}}{(n+1)!} \prod_{k=0}^n \left(\left(\frac{1}{2} - k \right) \cdot (-2) \right) \\ &= (-1) \frac{2^n}{(n+1)!} (-1) 1 \cdot 3 \cdot \dots \cdot (2n-1) \\ &= \frac{2^n}{(n+1)!} \frac{(2n)!}{2 \cdot 4 \cdot \dots \cdot 2n} = \frac{2^n}{(n+1)!} \frac{(2n)!}{2^n \cdot n!} \\ &= \frac{1}{n+1} \binom{2n}{n} \end{aligned}$$

This is the closed form of the Catalan numbers.

9.1 q -Enumeration

We introduce q -Enumeration, which is an approach similar to generating functions which gives us refined identities. An example of this will be the q -binomial theorems which we will get to later. It can also be thought of as a way of more refined counting. Given a set S of combinatorial objects that can be partitioned into k parts $S = \bigcup_{i \in [k]} S_i$ and a natural ordering S_1, \dots, S_k then we write the q -polynomial as

$$S(q) = \sum_{i=1}^k |S_i| q^i,$$

where the q helps us to distinguish between the sets S_i . In the following, we will distinguish between permutations by partitioning them into groups having the same parameter, for different kinds of parameters that we will define one by one.

First though, we introduce some useful notation, the so called q -bracket:

$$[n]_q = q^0 + q^1 + q^2 + \dots + q^{n-1} = \frac{1 - q^n}{1 - q}.$$

Mostly we omit the q subscript from the q -bracket because the meaning of the bracket is unambiguous from the context.

Definition 9.1 (Inversion of a permutation). Let $\pi = (\pi_1, \dots, \pi_n) \in S_n$ be a permutation. An *inversion* of π is a pair (π_i, π_j) with $i < j$ and $\pi_i > \pi_j$. For the number of inversions of π we adopt the notation: $\text{inv}(\pi) = \#(\text{inversions of } \pi)$.

Remark. Inversions appear in the Leibniz formula for determinants, since

$$\text{sgn}(\pi) = (-1)^{\text{inv}(\pi)}$$

Example 17. $\pi = 23154$ has inversions $(2,1)$, $(3,1)$, and $(5,4)$

Theorem 9.2. For fixed $n \in \mathbb{N}$ it holds that

$$\sum_{\pi \in S_n} q^{\text{inv}(\pi)} = [n]_q [n-1]_q \dots [1]_q =: [n]_q!$$

Proof. The proof is based on a bijection between the two sets

$$S_n \quad \text{and} \quad A_n = \{(a_1, \dots, a_n) \mid 0 \leq a_i < i \ \forall i\}.$$

Specifically we want to find a bijective function $\varphi : A_n \rightarrow S_n$, such that

$$\text{inv}(\varphi(a_1, \dots, a_n)) = a_1 + a_2 + \dots + a_n.$$

Given $\pi \in S_n$ let $a_k(\pi) = \#(\text{inversions } (k, \ell) \text{ in } \pi)$, that is $\ell < k$ and k is to the left of ℓ . For fixed k this means $0 \leq a_k(\pi) < k$. From the inversion sequence $(a_1(\pi), a_2(\pi), \dots, a_n(\pi))$ we can reconstruct π uniquely, which is best seen when going through a specific example:

Let

$$a = \overset{1}{(0,} \overset{2}{1,} \overset{3}{1,} \overset{4}{0,} \overset{5}{4,} \overset{6}{3,} \overset{7}{6,} \overset{8}{2})$$

Then we can reconstruct π in the following manner

1	(1 has no numbers smaller to its right)
21	(2 has one smaller number to its right)
231	(3 has one smaller number to its right)
2314	(4 has no smaller numbers to its right)
52314	(5 has four smaller numbers to its right)
526314	(6 has three smaller numbers to its right)
7526314	(7 has six smaller numbers to its right)
75263814	(8 has two smaller numbers to its right)

So $\phi((0, 1, 1, 0, 4, 3, 6, 2)) = (75263814)$.

Now that we have the bijection we compute

$$\begin{aligned} \sum_{\pi \in S_n} q^{\text{inv}(\pi)} &= \sum_{a \in A_n} q^{\|a\|_1} = \sum_{a_1=0}^0 \sum_{a_2=0}^1 \sum_{a_3=0}^2 \dots \sum_{a_n=0}^{n-1} q^{a_1+a_2+a_3+\dots+a_n} \\ &= \left(\sum_{a_1=0}^0 q^{a_1} \right) \left(\sum_{a_2=0}^1 q^{a_2} \right) \dots \left(\sum_{a_n=0}^{n-1} q^{a_n} \right) \\ &= (q^0)(q^0 + q^1)(q^0 + q^1 + q^2) \dots (q^0 + \dots + q^{n-1}) \\ &= [1][2][3] \dots [n] = [n]! \end{aligned}$$

□

9.1.1 More permutation statistics

Let $\pi = (\pi_1, \dots, \pi_n)$ be a permutation.

Definition 9.3. The set of *descents* of a permutation is given by

$$D(\pi) = \{j \mid \pi_j > \pi_{j+1}\}.$$

Major Percy MacMahon, a British officer and mathematician, introduced this concept in 1913 alongside the *major index* of a permutation:

$$\text{maj}(\pi) = \sum_{j \in D(\pi)} j$$

We will now look at an example for the group S_3 of permutations to see the major index and number of inversions, and how they relate.

n=3	<i>maj</i>	<i>inv</i>
1 2 3	0	0
1 3↓2	2	1
3↓1 2	1	2
3↓2↓1	3	3
2 3↓1	2	2
2↓1 3	1	1

Table 9.4: using ↓ where there is a descent

While the major-index and the inversions are not the same, we note that the same values seem to appear in both columns. This is actually always the case. With the following theorem we show that "the statistics *inv* and *maj* are equidistributed".

Theorem 9.4. For all $n \in \mathbb{N}$ it holds

$$\sum_{\pi \in S_n} q^{\text{inv}(\pi)} = \sum_{\pi \in S_n} q^{\text{maj}(\pi)}$$

Proof. We prove this through a generating function argument as well as a bijection. Let

$$M_n(z) = \sum_{\pi \in S_n} z^{\text{maj}(\pi)}$$

We claim that

$$\left(\frac{1}{1-z}\right)^n = M_n(z) \cdot \prod_{k=1}^n \frac{1}{1-z^k} \quad (9.13)$$

The claim implies the statement of the theorem as follows:

$$\sum_{\pi \in S_n} q^{\text{maj}(\pi)} = M_n(q) = \prod_{k=1}^n \frac{1-q^k}{1-q} = \prod_{k=1}^n [k]_q = [n]_q! = \sum_{\pi \in S_n} q^{\text{inv}(\pi)}$$

So it remains to prove the claim. This is done by bijection. The left-hand side $(\frac{1}{1-z})^n$ can be interpreted as a generating function: $(\frac{1}{1-z})^n = \sum a_m z^m$. From

$$\left(\frac{1}{1-z}\right)^n = \left(\sum_{q \in \mathbb{N}} z^q\right)^n = \sum_{(q_1, \dots, q_n) \in \mathbb{N}^n} z^{q_1 + q_2 + \dots + q_n}.$$

we see that a_m is the number of vectors of n nonnegative integers (q_1, \dots, q_n) with $\sum_{i=1}^n q_i = m$.

The second factor of the right hand side of equation (9.13) is recognized as the generating function of integer partitions with parts of size at most n , so we can use Proposition 5.4:

$$\prod_{k=1}^n \left(\frac{1}{1-z^k}\right) = \sum_{\substack{\lambda \text{ partition into} \\ \text{pieces of size } \leq n}} z^{|\lambda|} \stackrel{5.4}{=} \sum_{\substack{\lambda \text{ partition} \\ \text{into } \leq n \text{ pieces}}} z^{|\lambda|} = \sum_{\substack{p_1, \dots, p_n \in \mathbb{N}^n \\ p_1 \geq \dots \geq p_n}} z^{p_1 + \dots + p_n}$$

Therefore, our bijection will be between a vector of nonnegative integers $(q_1, \dots, q_n) \in \mathbb{N}^n$ and the pair of vectors $(\pi_1, \dots, \pi_n) \in S_n$ and $(p_1, \dots, p_n) \in \mathbb{N}^n$ with $p_1 \geq p_2 \geq \dots \geq p_n \geq 0$, such that

$$\sum_{i=1}^n q_i = \text{maj}(\pi) + \sum_{i=1}^n p_i.$$

" \rightarrow ": Given (q_1, \dots, q_n) there is a unique *stable* sorting of the entries $q_{\pi_1} \geq q_{\pi_2} \geq \dots \geq q_{\pi_n}$ where by stable we mean that when $q_{\pi_i} = q_{\pi_j}$ for $i < j$ then $\pi_i < \pi_j$. This gives us a unique $\pi = (\pi_1, \dots, \pi_n)$. Next for every $j \in D(\pi)$, that is if $\pi_j > \pi_{j+1}$, we get that

$q_{\pi_j} > q_{\pi_{j+1}}$, and we subtract 1 from each $q_{\pi_1}, \dots, q_{\pi_j}$, meaning we subtract j in total. After having done this for every $j \in D(\pi)$ we are left with $p_1 \geq p_2 \geq \dots \geq p_n$ as our resulting sequence, and it holds that

$$\sum_{i=1}^n q_i = \sum_{j \in D(\pi)} j + \sum_{i=1}^n p_i = \text{maj}(\pi) + \sum_{i=1}^n p_i$$

" \leftarrow ": Given $\pi \in S_n$ and $p \in \mathbb{N}^n$ with $p_1 \geq \dots \geq p_n$ we can get back to q in a similar manner as above. First for every $j \in D(\pi)$ we add 1 to p_1, \dots, p_j adding j in total, which results in $q_{\pi_1}, \dots, q_{\pi_n}$. Then we can just reorder this using π^{-1} to get q_1, \dots, q_n . \square

Example 18. Now for a short example that illustrates the bijection used in the proof. Given $q = (5, 7, 2, 7, 2)$ we consider the stable reordering by size $(7, 7, 5, 2, 2)$ and the reordering permutation $\pi = 2 \ 4 \downarrow 1 \ 3 \ 5$. Since $D(\pi) = \{2\}$ we subtracting 1 from the first two numbers of the reordered vector and get $p = (6, 6, 5, 2, 2)$.

Even more permutation statistics

Recall $D(\pi) = \{j \mid \pi_j > \pi_{j+1}\}$ is the set of descents.

Definition 9.5. Define $\text{des}(\pi) = |D(\pi)|$ to be the number of descents.

Further define $E(\pi) := \{j \mid \pi_j > j\}$ to be the set of *exceedances* of π and $\text{exc}(\pi) := |E(\pi)|$.

Proposition 9.6.

$$\sum_{\pi \in S_n} q^{\text{des}(\pi)} = \sum_{\pi \in S_n} q^{\text{exc}(\pi)}$$

Proof. by bijection: Given $\pi \in S_n$ in one-line notation interpret π as the canonical cycle decomposition of $\hat{\pi}$, then look at $\hat{\pi}^{-1}$. We then claim that

$$\text{des}(\pi) = \text{exc}(\hat{\pi}^{-1}).$$

A short example will illustrate this

$$\begin{array}{ll} \pi = 4 \downarrow 3 \downarrow 1 \ 7 \ 9 \downarrow 5 \downarrow 2 \ 8 \downarrow 6 & \text{des}(\pi) = 5 \\ \hat{\pi} = (431)(7)(95286) & \text{interpreted as canonical cycle decomp.} \\ \hat{\pi}^{-1} = (413)(7)(96825) & \text{which in two-line notation is} \\ \hat{\pi}^{-1} = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 \\ \underline{3} & \underline{5} & \underline{4} & 1 & \underline{9} & \underline{8} & 7 & 2 & 6 \end{pmatrix} & \text{where the exceedances are underlined} \end{array}$$

So $\text{exc}(\hat{\pi}^{-1}) = 5$ and as can be seen from the example there is a clear one-to-one relation between descents in π and exceedances in $\hat{\pi}^{-1}$. We omit a formal proof which can be extracted quite easily from the example. \square

Definition 9.7 (Eulerian polynomial). The Eulerian polynomial is given by

$$A_n(q) = \sum_{\pi \in S_n} q^{des(\pi)} = \sum_{k=0}^{n-1} \left\langle n \atop k \right\rangle q^k$$

where $\left\langle n \atop k \right\rangle$ are called Eulerian numbers.

Some more equidistribution results which can be found (and are defined) in the literature relate a pair of permutation statistics with another pair:

$$(maj, des) \sim (den, exc) \quad [\text{Foata and Zeilberger 1990, } \textit{Stud. in Appl. Math.}]$$

$$(maj, exc) \sim (aid, des) \quad [\text{Linusson, Shareshian and Wachs 2012, } \textit{J. Comb.}]$$

When given a pair of statistics we talk about bivariate polynomials in the form $\sum_{\pi} a^{i_1(\pi)} b^{i_2(\pi)}$. Note that the fact that des and exc are equidistributed does not imply $(maj, des) \sim (maj, exc)$. The inverse implication would hold, but in fact, the latter is not true:

π	maj	des	exc
123	0	0	0
132	2	1	1
213	1	1	1
231	2	1	2
312	1	1	1
321	3	2	1

Table 9.5: Distribution of maj , des and exc on S_3

Lecture 10

Eulerian Numbers and q -Binomial Coefficients

In the last lecture we met Eulerian numbers in the definition of the Eulerian polynomial (Definition 9.7). They are defined as $\langle n \rangle_k := \#(\pi \in S_n : \text{des}(\pi) = k)$, where $\text{des}(\pi)$ is the cardinality of the descent set $D(\pi) = \{j \mid \pi_j > \pi_{j+1}\}$ (Definition 9.3). We will now go on and study Eulerian numbers in more depth.

- Symmetry:

$$\langle n \rangle_k = \langle n \rangle_{n-1-k}$$

this is due to the simple bijection $\pi \leftrightarrow \pi^{\text{rev}}$, i.e., revert π in one-line notation.

- Recursion:

$$\langle n \rangle_k = (k+1) \langle n-1 \rangle_k + (n-k) \langle n-1 \rangle_{k-1}$$

which is obtained by looking at $\pi \in S_{n-1}$ and inserting n at each of the n possible positions:

- if n is placed between a descending pair or at the end, the number of descents remains the same (left summand).
 - otherwise the number of descents increases by 1 (right summand)
- with that recursion and the obvious initial conditions at $n = 0$ or $n = 1$ for all k we can fill the following table:

		k					
		0	1	2	3	4	5
n	0	1	0	0	0	0	0
	1	1	0	0	0	0	0
	2	1	1	0	0	0	0
	3	1	4	1	0	0	0
	4	1	11	11	1	0	0
	5	1	26	66	26	1	0
	6	1	57	302	302	57	1

- Generating function (Eulerian polynomial)

$$A_n(q) = \sum_{\pi \in S_n} q^{\text{des}(\pi)} = \sum_{k=0}^{n-1} \left\langle n \atop k \right\rangle q^k$$

The recursion can be used to establish a functional equation for Eulerian polynomials:

$$A_{n+1}(q) = (1 + nq)A_n(q) + q(1 - q)A'_n(q)$$

Proof. Exercise. □

We go on to show an identity involving Eulerian Numbers.

Theorem 10.1 (Worpitzky's Identity).

$$x^n = \sum_{k=0}^{n-1} \left\langle n \atop k \right\rangle \binom{x+k}{n} \quad (10.14)$$

Proof. This is a polynomial identity. We will show it for $x \in \mathbb{N}$; it extends to all of \mathbb{C} . We interpret $x^n = \#(\text{vectors } (x_1, x_2, \dots, x_n) \text{ with } x_i \in [x])$. There is a unique *stable sorting permutation* $\pi \in S_n$ such that

$$x_{\pi_1} \geq x_{\pi_2} \geq \dots \geq x_{\pi_n} \quad \text{and} \quad x_{\pi_j} = x_{\pi_{j+1}} \implies \pi_j > \pi_{j+1}$$

Let ℓ denote the number of cases of equality in the sorted sequence. Then by definition π has at least ℓ descents and $Z = \{x_i : i = 1, \dots, n\}$ has $n - \ell$ values. We obtain the following bijection

$$(x_1, \dots, x_n) \longleftrightarrow [Z, \pi, A]$$

where π is the stable sorting permutation and A is a subset of $D(\pi)$ of size ℓ which contains exactly the descents that came from an equality in the sorted sequence.

To show that this is a bijection we have to establish the inverse map. We do this only by example. Let $n = 6$ and consider $[Z, \pi, A]$ where

$$Z = \{2, 4, 5, 7\} \quad \pi = 315642 \quad A = \{1, 5\}$$

Let us first check that the three tuple conforms to the requirements: Since $D(\pi) = \{1, 4, 5\}$ we have $A \subseteq D(\pi)$ and also know $\ell = |A| = 2$ which is consistent with $|Z| = n - \ell = 6 - 2$.

From Z and A we get the sorted sequence 7, 7, 5, 4, 2, 2. Using π we directly get the vector (7, 2, 7, 2, 5, 4).

Given the bijection $(x_1, \dots, x_n) \leftrightarrow [Z, \pi, A]$ let us think about the number of pairs (Z, A) which are consistent with π , i.e., which appear with π in a triple in the image. Since $x_i \in [x]$ these pairs depend on x , indeed the conditions are $Z \subseteq [x]$ and $A \subseteq D(\pi)$

and $|Z| + |A| = n$. Hence Z and A can be obtained by choosing an n -element subset of $[x] \cup D(\pi)$. This shows that:

$$x^n = \sum_{\pi \in S_n} \binom{x + \text{des}(\pi)}{n}$$

Now we can partition the permutations according to the size of their descent set and obtain:

$$x^n = \sum_{\pi \in S_n} \binom{x + \text{des}(\pi)}{n} = \sum_{k=0}^{n-1} \langle n \rangle_k \binom{x+k}{n}$$

□

Using Worpitzky's Identity we can derive a connection between Bernoulli numbers (see [Section 8.1](#)) and Eulerian numbers:

$$\begin{aligned} \frac{1}{s+1} \sum_{\ell=0}^s \binom{s+1}{\ell} b_{\ell} (n+1)^{s+1-\ell} &\stackrel{(8.12)}{=} \sum_{k=1}^n k^s \\ &\stackrel{(10.14)}{=} \sum_{k=1}^n \sum_{m=0}^{s-1} \langle s \rangle_m \binom{k+m}{s} \\ &= \sum_{m=0}^{s-1} \langle s \rangle_m \sum_{k=1}^n \binom{k+m}{s} \\ &= \sum_{m=0}^{s-1} \langle s \rangle_m \binom{n+m-1}{s+1} \end{aligned}$$

This again proves that $\sum_1^n k^s$ is a polynomial of degree $s+1$ in n .

10.1 q -binomial coefficients and q -binomial theorems

We have learned about the generalization $[n]!$ of $n!$, where $n!$ counts permutations and $[n]!$ counts permutations with a weight expressed in terms of q . In this chapter we want to look at q -binomial coefficients $\begin{bmatrix} n \\ k \end{bmatrix}$ defined by

$$\begin{bmatrix} n \\ k \end{bmatrix} := \frac{[n]!}{[k]![n-k]!}$$

We know that

$$\begin{aligned} \binom{n}{k} &= \#(k\text{-subsets of } \{1, \dots, n\}) \\ &= \#((w_1, \dots, w_n) : w_i \in \{0, 1\}, \sum w_i = k) \end{aligned}$$

and for such vectors (w_1, \dots, w_n) we can talk about inversions. In the following theorem we use the notation $\{0, 1\}_k^n := \{(w_1, \dots, w_n) : w_i \in \{0, 1\}, \sum w_i = k\}$.

Theorem 10.2.

$$\sum_{w \in \{0,1\}_k^n} q^{\text{inv}(w)} = \begin{bmatrix} n \\ k \end{bmatrix}$$

Proof. We will define a bijection between S_n and $\{0,1\}_k^n \times S_k \times S_{n-k}$ such that if π maps to (w, σ_1, σ_2) , then $\text{inv}(\pi) = \text{inv}(w) + \text{inv}(\sigma_1) + \text{inv}(\sigma_2)$. This yields

$$\begin{aligned} \sum_{\pi \in S_n} q^{\text{inv}(\pi)} &= \sum_{w \in \{0,1\}_k^n} q^{\text{inv}(w)} \cdot \sum_{\sigma_1 \in S_k} q^{\text{inv}(\sigma_1)} \cdot \sum_{\sigma_2 \in S_{n-k}} q^{\text{inv}(\sigma_2)} \\ \iff [n]! &= \sum_{w \in \{0,1\}_k^n} q^{\text{inv}(w)} \cdot [k]! \cdot [n-k]! \\ \iff \begin{bmatrix} n \\ k \end{bmatrix} &= \sum_{w \in \{0,1\}_k^n} q^{\text{inv}(w)} \end{aligned}$$

The bijection for given π and k works as follows:

- w is 1 in the positions of the k largest elements in π and 0 otherwise.
- σ_1 takes the largest k elements from π in their order and normalizes them by subtracting $n-k$ from every element.
- σ_2 takes the $n-k$ smallest elements from π in their order.

Example.

$$\begin{array}{ll} \pi = \underline{7} \, 5 \, 2 \, \underline{6} \, 3 \, \underline{8} \, 1 \, 4 & k = 3 \\ w = 1 \, 0 \, 0 \, 1 \, 0 \, 1 \, 0 \, 0 \\ \sigma_1 = 7 \, 6 \, 8 \mapsto 2 \, 1 \, 3 \\ \sigma_2 = 5 \, 2 \, 3 \, 1 \, 4 \end{array}$$

□

A word $w \in \{0,1\}_k^n$ can also be interpreted as a lattice path from $(0,0)$ to $(n-k,k)$ where a '0' corresponds to a step $(1,0)$ and a '1' corresponds to a step $(0,1)$, see [Figure 10.1](#). Note that inversions of w correspond to squares below the path and vice versa, hence, $\text{inv}(w) = \text{area below the path}$.

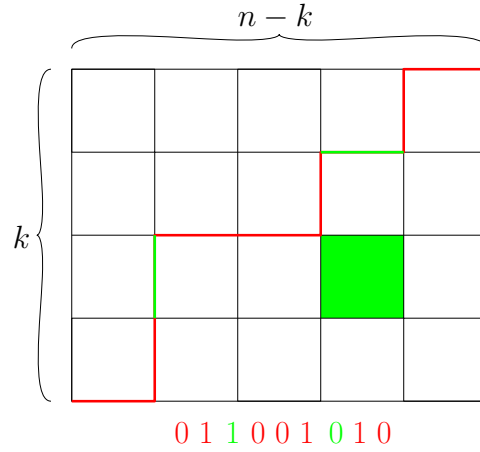


Figure 10.1: A lattice path and its corresponding word $w \in \{0, 1\}_4^9$. An inversion of w and the corresponding square below the path are highlighted in green

Using the path and area model for inversions we can give easy proofs of the following properties:

- Recursion:

$$\left[\begin{matrix} n \\ k \end{matrix} \right]_{w \in \{0,1\}_k^n} = \left[\begin{matrix} n-1 \\ k \end{matrix} \right]_{w_1=0} + q^{n-k} \left[\begin{matrix} n-1 \\ k-1 \end{matrix} \right]_{w_1=1}$$

- Symmetry:

$$\left[\begin{matrix} n \\ k \end{matrix} \right] = \left[\begin{matrix} n \\ n-k \end{matrix} \right]$$

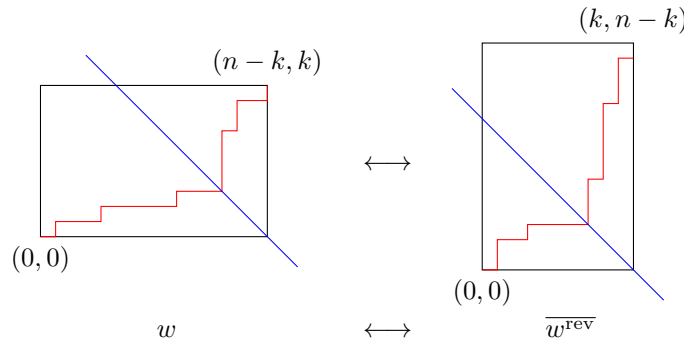


Figure 10.2: Bijection between $\{0, 1\}_k^n$ and $\{0, 1\}_{n-k}^n$ which shows the symmetry of q -binomial coefficients

- putting these two together we get

$$\left[\begin{matrix} n \\ n-k \end{matrix} \right] = \left[\begin{matrix} n-1 \\ n-1-k \end{matrix} \right] + q^{n-k} \left[\begin{matrix} n-1 \\ n-k \end{matrix} \right]$$

we substitute $\ell = n - k$ and get

$$\left[\begin{matrix} n \\ \ell \end{matrix} \right]_{w \in \{0,1\}_\ell^n} = \left[\begin{matrix} n-1 \\ \ell-1 \end{matrix} \right]_{w_n=1} + q^\ell \left[\begin{matrix} n-1 \\ \ell \end{matrix} \right]_{w_n=0}$$

Theorem 10.3 (first binomial theorem).

$$(1 + qx)(1 + q^2x) \dots (1 + q^nx) = \sum_{k=0}^n \left[\begin{matrix} n \\ k \end{matrix} \right] q^{\binom{k+1}{2}} x^k$$

Remark. This is a generalization of $(1 + x)^n = \sum_{k=0}^n \binom{n}{k} x^k$

Proof of Theorem 10.3.

$$\prod_{i=1}^n (1 + q^i x) = \sum_{k=0}^n b_k(q) x^k$$

with

$$b_k(q) = \sum_{1 \leq i_1 < i_2 < \dots < i_k \leq n} q^{i_1 + i_2 + \dots + i_k} = \sum_{\lambda \in P(n,k)} q^{|\lambda|}$$

where $P(n, k) = \{\lambda = (\lambda_1, \dots, \lambda_k) : 1 \leq \lambda_1 < \lambda_2 < \dots < \lambda_k \leq n\}$ denotes the set of partitions into k pairwise distinct parts of size at most n . We claim that

$$b_k(q) = \sum_{\lambda \in P(n,k)} q^{|\lambda|} \stackrel{!}{=} \sum_{w \in \{0,1\}_{n-k}^n} q^{\binom{k+1}{2} + \text{area}(w)} = \left[\begin{matrix} n \\ k \end{matrix} \right] q^{\binom{k+1}{2}}.$$

We prove the claim using a bijection

$$\lambda \in P(n,k) \longleftrightarrow w_\lambda \in \{0,1\}_{n-k}^n$$

with $|\lambda| = \binom{k+1}{2} + \text{area}(w_\lambda)$ constructed the following way:

- Take the Ferrers diagram of λ and reflect it vertically, this yields piles $\lambda_1 < \lambda_2 < \dots < \lambda_k$.
- Shift λ_i down such that i squares of $\lambda_i \geq i$ are below the base line.
- The upper boundary of the piles which remains above the baseline can be extended with vertical steps to a path corresponding to a $w_\lambda \in \{0,1\}_{n-k}^n$.

Example. Let $\lambda = (7, 4, 3, 1) \in P(9, 4)$. The mapping to w_λ is illustrated in [Figure 10.3](#). Since the number of squares below the baseline is $\sum_{i=1}^k j = \binom{k+1}{2}$ this completes the proof of [Theorem 10.3](#). \square

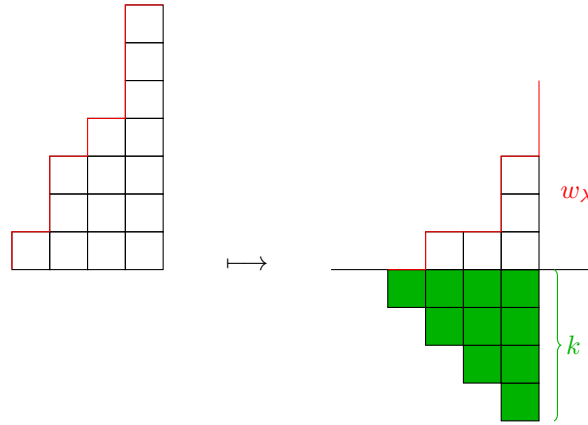


Figure 10.3: The reflected Ferrers diagram of λ on the left hand side and on the right hand side the path of w_λ marked in red and the area below the baseline in green.

10.1.1 Another model for q -binomial coefficients

In order to get to a second q -binomial theorem, we take look at the categories of sets and vectorspaces and note some analogies:

sets	vectorspaces
$f : S \rightarrow T$ maps	$\phi : V \rightarrow w$ linear maps
subsets	subspaces
$S \cap T = \emptyset$	$U \cap W = \{0\}$
cardinality	dimension
$ S \cap T + S \cup T = S + T $	$\dim(U \cap W) + \dim(U + W) = \dim(U) + \dim(W)$

Consider a finite field $\text{GF}(q)$ with q elements (note that this is just another notation for \mathbb{F}_q). Let $V_n(q)$ be an n -dimensional vectorspace over $\text{GF}(q)$. Then $|V_n(q)| = q^n$ since elements of $V_n(q)$ can be regarded as vectors of length n with entries in $\{0, \dots, q-1\}$. How many k -dimensional subspaces does $V_n(q)$ have? The answer will be $\begin{bmatrix} n \\ k \end{bmatrix}$ – here q is the order of the field and hence a fixed number. However, if in this context we find polynomial identities (polynomials in the variable q), then, since there are infinitely many primes resp. prime powers q , these identities also hold over \mathbb{N} and \mathbb{C} .

q -Binomial Coefficients, Finite Sets and Posets

At the end of the previous chapter we have announced a second model for q -binomial coefficients. We now prove the announced proposition.

Proposition 11.1. *The number of k -dimensional subspaces for the n -dimensional vector space $V_n(q)$ over $\text{GF}(q)$ is $\begin{bmatrix} n \\ k \end{bmatrix}$.*

Proof. We start by studying the number of ordered bases of a k -dimensional vector space $V_k(q)$ i.e., the number of k -tuples (b_1, \dots, b_k) of linear independent vectors in $V_k(q)$. Constructing the tuple element by element we find:

possible choices for b_1 :	each vector $v \neq 0$ of $V_k(q)$	$q^k - 1$
possible choices for b_2 :	each $v \in V_k(q)$ with $v \notin \langle b_1 \rangle$	$q^k - q$
possible choices for b_3 :	each $v \in V_k(q)$ with $v \notin \langle b_1, b_2 \rangle$	$q^k - q^2$
\vdots	\vdots	\vdots
possible choices for b_k :	each $v \in V_k(q)$ with $v \notin \langle b_1, b_2, \dots, b_{k-1} \rangle$	$q^k - q^{k-1}$

In total there are $\prod_{i=1}^k (q^k - q^{i-1})$ ordered bases (b_1, \dots, b_k) . We can use a similar calculation to find the number of k -tuples (v_1, \dots, v_k) of linearly independent vectors in $V_n(q)$:

possible choices for v_1 :	each vector $v \neq 0$ of $V_n(q)$	$q^n - 1$
possible choices for v_2 :	each $v \in V_n(q)$ with $v \notin \langle v_1 \rangle$	$q^n - q$
possible choices for v_3 :	each $v \in V_n(q)$ with $v \notin \langle v_1, v_2 \rangle$	$q^n - q^2$
\vdots	\vdots	\vdots
possible choices for v_k :	each $v \in V_n(q)$ with $v \notin \langle v_1, v_2, \dots, v_{k-1} \rangle$	$q^n - q^{k-1}$

In total there are $\prod_{i=1}^k (q^n - q^{i-1})$ such k -tuples (v_1, \dots, v_k) .

Now every k -tuple of linearly independent vectors in $V_n(q)$ is the basis of some k -dimensional subspace and we know exactly how many times each such subspace is counted this way. So for the number of subspaces we get:

$$\frac{\prod_{i=1}^k (q^n - q^{i-1})}{\prod_{i=1}^k (q^k - q^{i-1})} = \prod_{i=1}^k \frac{q^{n-i+1} - 1}{q^{k-i+1} - 1} = \prod_{i=1}^k \frac{q^{n-i+1} - 1}{q^{k-i+1} - 1} = \frac{\prod_{i=1}^k [n - i + 1]}{\prod_{i=1}^k [k - i + 1]} = \begin{bmatrix} n \\ k \end{bmatrix}$$

Hence, the number of number of k -dimensional subspaces for $V_n(q)$ is $\begin{bmatrix} n \\ k \end{bmatrix}$. □

The next theorem is our second q -generalization of the Binomial theorem. In the proof we will use q -vectorspaces.

Theorem 11.2.

$$x^n = \sum_{k=0}^n \begin{bmatrix} n \\ k \end{bmatrix} (x-1) \cdot (x-q) \cdot \dots \cdot (x-q^{n-k-1})$$

Remark. For $q = 1$ we get: $x^n = \sum_{k=0}^n \binom{n}{k} (x-1)^{n-k}$ which is true, because

$$x^n = ((x-1) + 1)^n \stackrel{\text{Theorem 3.9}}{=} \sum_{k=0}^n \binom{n}{k} (x-1)^{n-k} \cdot 1^k = \sum_{k=0}^n \binom{n}{k} (x-1)^{n-k}$$

With the Theorem we prove it for every q .

Proof. Let X be a vector space over $\text{GF}(q)$ with $|X| = x$. We will count linear maps $\varphi : V_n(q) \rightarrow X$ in two different ways.

1st count: Let $\{b_1, \dots, b_n\}$ be a fixed basis of $V_n(q)$. For each b_i we can independently choose its image x_i in X . Such a choice of (x_1, \dots, x_n) uniquely determines a linear map φ . Hence $\#\text{maps} = |X|^n = x^n$

2nd count: Let U be a subspace of $V_n(q)$. We want to count the linear maps φ from $V_n(q) \rightarrow X$ with $U = \text{Ker}(\varphi)$. Let (w_1, \dots, w_k) be an ordered basis of U . It can be extended to an ordered basis $(w_1, \dots, w_k, v_1, \dots, v_{n-k})$ of $V_n(q)$. Since the kernel U has dimension k the image of φ will have to be of dimension $n-k$ (This is due to the dimension formula $\dim(\text{Ker}(\varphi)) + \dim(\text{Im}(\varphi)) = \dim(V_n(q))$). Consider the images of v_1, \dots, v_{n-k} :

possible choices for v_1 :	each vector $v \in X$ with $v \neq 0$	$x-1$
possible choices for v_2 :	each vector $v \in X$ with $v \notin \langle \varphi(v_1) \rangle$	$x-q$
possible choices for v_3 :	each vector $v \in X$ with $v \notin \langle \varphi(v_1), \varphi(v_2) \rangle$	$x-q^2$
\vdots	\vdots	\vdots
possible choices for v_{n-k} :	each vector $v \notin \langle \varphi(v_1), \varphi(v_2), \dots, \varphi(v_{n-k-1}) \rangle$	$x-q^{n-k-1}$

This shows that $|\{\varphi \in \text{Lin}(V_n(q), X) : \text{Ker}(\varphi) = U\}| = \prod_{i=1}^{n-k} (x-q^{i-1})$. We now put things together to complete the proof:

$$\begin{aligned} x^n &= \sum_{U \text{ subspace of } V_n(q)} |\{\varphi \in \text{Lin}(V_n(q), X) : \text{Ker}(\varphi) = U\}| \\ &= \sum_{k=0}^n \begin{bmatrix} n \\ k \end{bmatrix} \prod_{i=1}^{n-k} (x-q^{i-1}) = \sum_{k=0}^n \begin{bmatrix} n \\ k \end{bmatrix} (x-1) \cdot (x-q) \cdot \dots \cdot (x-q^{n-k-1}) \end{aligned}$$

□

11.1 Finite sets and posets

We begin this section with a little extremal problem regarding families of sets.

Given a set N with $|N| = n$, let $\mathcal{A} \subseteq \text{Pot}(N)$ be an *intersecting family*, i.e., any two elements of \mathcal{A} intersect.

The question is: how large can \mathcal{A} be?

It is easily seen that $|\mathcal{A}| \leq \frac{1}{2}|\text{Pot}(N)| = 2^{n-1}$. Indeed, if we pair the elements of $\text{Pot}(N)$ into pairs $\{A, \bar{A}\}$, where $\bar{A} = N - A$, then \mathcal{A} can only contain one set from each pair. Therefore, $|\mathcal{A}| \leq \frac{1}{2}|\text{Pot}(N)| = 2^{n-1}$.

Actually the inequality is tight. An example attaining equality is the star family $\mathcal{A}_x := \{A \in \text{Pot}(N) : x \in A\}$. Since x is contained in every set in \mathcal{A}_x the family is intersecting. Clearly $|\mathcal{A}| = 2^{n-1}$.

Here is another construction which works for odd n : $\mathcal{A} := \{A \in \text{Pot}(n) : |A| > \frac{n}{2}\}$. For n even the same idea of just taking large sets can be used. However, additional care is needed because the sets of cardinality $\frac{n}{2}$ chosen for \mathcal{A} have to be an intersecting family.

Example. For $N = \{1, 2, 3\}$ the first proof ($x = 1$) gives $\mathcal{A}_1 = \{\{1\}, \{1, 2\}, \{1, 3\}, \{1, 2, 3\}\}$ and the second proof gives us $\mathcal{A} = \{\{2, 3\}, \{1, 2\}, \{1, 3\}, \{1, 2, 3\}\}$.

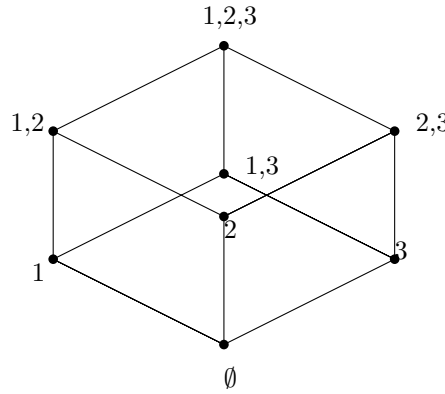


Figure 11.1: drawing (diagram) of the Boolean lattice B_3

Definition 11.3 (Poset). $P = (X, \leq)$ is a *partially ordered set* (or *poset* for short) if X is some ground set and \leq a *partial order*, i.e., a binary relation on X with:

- reflexivity: $\forall x \in X : x \leq x$
- transitivity: $\forall x, y, z \in X : x \leq y, y \leq z \Rightarrow x \leq z$
- asymmetry: $\forall x, y \in X : x \leq y, y \leq x \Rightarrow x = y$

Any partial order comes with a strict order relation $<$ defined by $x < y \Leftrightarrow x \leq y \wedge x \neq y$. This relation can be equivalently defined by *transitivity* and *irreflexivity*, the opposite of reflexivity.

Remark. Talking about *partial* orders means that there may be elements $x, y \in X$ which are *incomparable* with the respective order \leq or $<$. We denote this as $x \parallel y$. If the elements are comparable but we do not want to specify their order, we write $x \sim y$.

Example 19.

- A set of distinct points on the real line can be ordered from left to right. This is a *total order* or *linear order*, because any two elements are comparable.

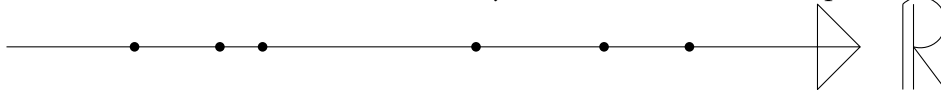


Figure 11.2: Points on the real line

- A set of intervals on the real line induces an *interval order*. The order relation is given by $I < J$ if and only if $\sup(I) < \inf(J)$.

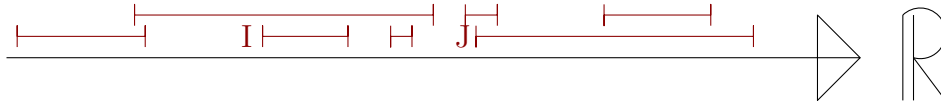


Figure 11.3: I and J are comparable intervals on the real line.

- A family $\mathcal{A} \subseteq \text{Pot}(N)$ comes with a *containment order*, i.e., the order relation $A \leq B \Leftrightarrow A \subseteq B$. In fact containment orders are universal in the following sense: For every $P = (X, \leq)$ with finite X there is a family \mathcal{A} so that (X, \leq) and (\mathcal{A}, \subseteq) are isomorphic.

Definition 11.4 (Lattice). A poset $P = (X, \leq)$ is a lattice if $\forall x, y$ there is a z such that $x \leq z$ and $y \leq z$ and $\forall \tilde{z}$ with $x \leq \tilde{z}$ and $y \leq \tilde{z}$ we have $z \leq \tilde{z}$. The element z is the *join* (*supremum*) of x and y . Dually $\forall x, y$ there is a z such that $z \leq x$ and $z \leq y$ and $\forall \tilde{z}$ with $\tilde{z} \leq x$ and $\tilde{z} \leq y$ we have $\tilde{z} \leq z$. The element z is the *meet* (*infimum*) of x and y .

Example 20.

- **Boolean Lattice \mathcal{B}_N :** The elements of the Boolean lattice \mathcal{B}_N are all subsets of N , with the containment order. Here $\text{join}(A, B) = A \cup B$ and $\text{meet}(A, B) = A \cap B$.
- **Divisor Lattice \mathcal{D}_n :** The elements of the divisor lattice \mathcal{D}_n are the integers that divide n , the order relation is given by division, i.e., $a \leq b$ if and only if a divides b . The lattice operations are: $\text{join}(a, b) = \text{least common multiple of } a \text{ and } b$ and $\text{meet}(a, b) = \text{greatest common divisor of } a \text{ and } b$.

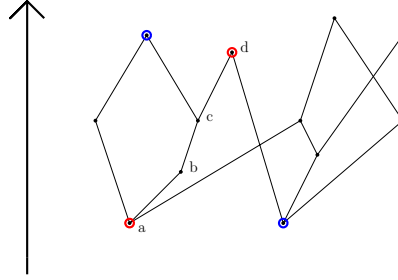
Visualizing posets:

The drawing of the Boolean Lattice given in Figure 11.1 has the property that subsets A and B of $\{1, 2, 3\}$ are in the order relation $A \subseteq B$ if there is an upward path from A to B in the drawing. For example $A = \{\emptyset\} \subseteq B = \{2, 3\}$, and $\{\emptyset\} \rightarrow \{2\} \rightarrow \{2, 3\}$ is an upward path. For these upward paths to exist, only a certain subset of relations is important to draw as an upward edge:

Definition 11.5. A pair (x, y) in a poset $P = (X, \leq)$ is a *cover* if $x < y$ and there are no elements in between ($\forall z : (x \leq z \leq y \Rightarrow z = x \text{ or } z = y)$). Being a cover is denoted as $x < y$.

The typical visual representation of posets is the *Hasse diagram*. The diagram of $P = (X, \leq)$ has a point (bullet) representing each element of X and for each cover relation $a < b$ there is an upward edge, this means that $a_y < b_y$ when a_y and b_y are the y -coordinates of a and b respectively.

Note that $x \leq y$ in P if and only if there is an upward path from x to y in the diagram of P .



In the poset given by the diagram in the figure we have $a < b < c < d$, hence, $a \leq d$. Between the two blue points there is no upward path, hence, they are incomparable.

We continue with some important definitions. Let $P = (X, \leq)$ be a poset:

Definition 11.6. $F \subseteq X$ is a *filter* (up-set) if $x \in F$ and $x \leq y \Rightarrow y \in F$

Definition 11.7. $I \subseteq X$ is a *ideal* (down-set) if $x \in I$ and $y \leq x \Rightarrow y \in I$

Definition 11.8. $A \subseteq X$ is a *antichain* if $\forall x \neq y \in A$ neither $x \leq y$ nor $y \leq x$, i.e., $x \parallel y$.

Definition 11.9. $C \subseteq X$ is a *chain* if $\forall x, y \in A : x \leq y \text{ or } y \leq x$, i.e., $x \sim y$.

If A is an antichain, then $F_A = \{y \in X : \exists a \in A \text{ with } a \leq y\}$ is a filter. Conversely, if F is a filter, then $A = \text{Min}(F)$ is an antichain with $F_A = F$, where we define the set of minima of a filter as $\text{Min}(F) = \{x \in F \mid \nexists y \in F : y < x\}$. A dual situation is true for ideals: If A is an antichain, then $I_A = \{y \in X : \exists a \in A \text{ with } y \leq a\}$ is a ideal. Conversely, if I is an ideal, then $A = \text{Max}(I)$ is an antichain with $I_A = I$. Here $\text{Max}(I) = \{x \in I \mid \nexists y \in I : y > x\}$.

We continue with some easy observations:

- If A is an antichain and C a chain of P , then $|A \cap C| \leq 1$. This follows from the definition, because for any two elements x, y of P either $x \parallel y$ or $x \sim y$.
- If C is a chain in \mathcal{B}_n then $|C| \leq n + 1$
- The Boolean lattice \mathcal{B}_n has an antichain of size $\binom{n}{\lfloor \frac{n}{2} \rfloor}$. An example of such an antichain is $\mathcal{A} = \{A \subset [n] : |A| = \lfloor \frac{n}{2} \rfloor\}$, the family \mathcal{A} has $\binom{n}{\lfloor \frac{n}{2} \rfloor}$ elements and any two sets in \mathcal{A} are incomparable, because they have the same size.

Theorem 11.10 (Sperner 1928). If \mathcal{A} is an antichain in \mathcal{B}_n , then $|\mathcal{A}| \leq \binom{n}{\lfloor \frac{n}{2} \rfloor}$.

In future lectures we will see various proofs of this theorem.

Sperner's Theorem and Intersecting Families

We will start this lecture by proving Sperner's theorem mentioned in lecture 11, and then continue by investigating intersecting families further with the help of *shadows*.

Theorem 12.1 (Sperner's theorem). *Let \mathcal{A} be an antichain in \mathcal{B}_n , then*

$$|\mathcal{A}| \leq \binom{n}{\lfloor n/2 \rfloor}$$

Proof. Let $\pi = (\pi_1, \dots, \pi_n) \in S_n$ be a permutation. Let $A_k := \{\pi_1, \dots, \pi_k\}$ be the set given by the initial segment of π of length $k \in \mathbb{N}$, then we say that π *meets* A_k .

Given $A \subseteq [n]$ with $|A| = k$ we count the number of permutations that meet A .

$$\#(\pi \in S_n, \pi \text{ meets } A) = \sum_{\pi \in S_n} \delta_{\{\pi \text{ meets } A\}} = k!(n-k)!$$

where the $k!$ comes from the possibilities of arranging the initial segment of length k using the elements of A and the $(n-k)!$ comes from arranging the remainder.

Now let \mathcal{A} be an antichain. For every $\pi \in S_n$ the sets met by π form a chain $\emptyset = A_0 \subsetneq A_1 \subsetneq \dots \subsetneq A_n = \{\pi_1, \dots, \pi_n\}$. Since a chain and an antichain can share at most one element we obtain that every $\pi \in S_n$ meets at most one $A \in \mathcal{A}$. This implies

$$\sum_{A \in \mathcal{A}} |A|!(n-|A|)! = \sum_{A \in \mathcal{A}} \#(\pi \in S_n : \pi \text{ meets } A) = \sum_{\pi \in S_n} \#(A \in \mathcal{A} : \pi \text{ meets } A) \leq n! \quad (12.15)$$

Define

$$p_k := p_k(\mathcal{A}) := \#(k\text{-sets in } \mathcal{A})$$

then from Equation (12.15) we get

$$\sum_{k=0}^n p_k k!(n-k)! \leq n! \iff \sum_{k=0}^n \frac{p_k}{\binom{n}{k}} \leq 1 \quad (\text{LYM})$$

The second formula in the previous line (LYM) is known as the LYM-inequality, which is short for Lubell, Yamamoto and Meshalkin, three researchers who discovered

the inequality independently from each other in the 1950-60s. Using the fact that $\binom{n}{k} \leq \binom{n}{\lfloor n/2 \rfloor}$ for every $k \in [n]$ we conclude that

$$\sum_{k=0}^n \frac{p_k}{\binom{n}{\lfloor n/2 \rfloor}} \leq 1 \iff \sum_{k=0}^n p_k \leq \binom{n}{\lfloor n/2 \rfloor}$$

The definition of p_k implies that $\sum_{k=0}^n p_k = |\mathcal{A}|$, concluding the proof. \square

We continue by investigating the case of equality in Sperner's theorem. For the last inequality $|\mathcal{A}| = \sum_{k=0}^n p_k \leq \binom{n}{\lfloor n/2 \rfloor}$ to be tight, we need $p_k = 0$ for all k with $\binom{n}{k} < \binom{n}{\lfloor n/2 \rfloor}$ because otherwise

$$\sum_{k=0}^n \frac{p_k}{\binom{n}{\lfloor n/2 \rfloor}} < \sum_{k=0}^n \frac{p_k}{\binom{n}{k}} \leq 1.$$

n is even: There is a unique maximal binomial coefficient $\binom{n}{n/2}$. Hence, $p_k = 0$ for all $k \neq \frac{n}{2}$. This implies that the maximum antichain \mathcal{A} is just the "middle rank" of \mathcal{B}_n .

n is odd: Then $n = 2s + 1$, so \mathcal{A} lives in the two middle ranks, i.e. $p_k = 0$ except for $k \in \{s, s+1\}$ for the aforementioned reasons. Suppose that it would live in both, i.e. we have $X \in \mathcal{A}$ in the s -rank and $Y \in \mathcal{A}$ in the $(s+1)$ -rank. Then we get a path in the boolean lattice from X to Y by alternately removing and adding elements to the sets X and Y . But then no two consecutive sets on that path can be contained in \mathcal{A} as they would form a two-chain. Now our path from X to Y has odd length as we move from the s -rank to the $(s+1)$ -rank by alternating between them. Thus there will be two consecutive vertices – i.e. intermediary sets – on this path that are both not contained in \mathcal{A} . Since they are consecutive vertices in the path, there is a $\pi \in S_n$ that meets both of them which is part of the $n!$ permutations but which is not covered by the sum $\sum_{A \in \mathcal{A}} |A|!(n-|A|)!$ and thus we get a strict inequality in Equation (12.15). Therefore, in the odd case the only maximum antichains are $\binom{[n]}{\lfloor n/2 \rfloor}$ and $\binom{[n]}{\lceil n/2 \rceil}$.

12.1 Finding large intersecting sets

Next we try to find large intersecting sets in $\binom{[n]}{k}$. Only the case $k \leq n/2$ is of interest since for $k > n/2$ any two k -element subsets of $[n]$ intersect.

Theorem 12.2 (Erdős-Ko-Rado). *For any intersecting family $\mathcal{F} \subseteq \binom{[n]}{k}$ with $n \geq 2k$,*

$$|\mathcal{F}| \leq \binom{n-1}{k-1}$$

The proof of this theorem relies on counting cyclic permutations, so for the sake of readability we define two new notions needed for the proof beforehand.

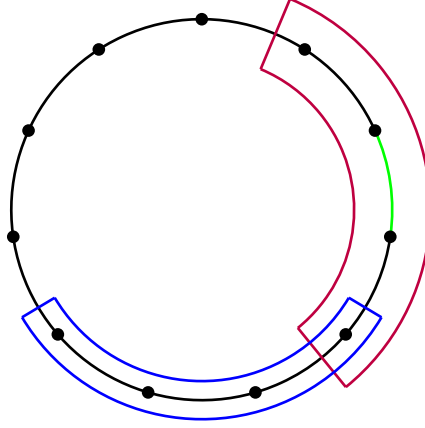


Figure 12.1: A cyclic representation of a permutation $\sigma \in S_{11}$ marked by the 11 vertices and edges between them. Two overlapping 4-arcs are drawn in purple and blue and a gap is highlighted in green.

Definition 12.3 (k -arc and gap of a cyclic permutation). Let $\sigma \in S_n$ be a cyclic permutation of $[n]$, that is $\sigma = (\sigma_1, \dots, \sigma_n)$ in cycle notation. Then a k -arc τ_k^j of σ is a k -tuple given by $(\sigma_j \bmod n, \dots, \sigma_{(j+k) \bmod n})$ for some $j \in [n]$.

A gap of τ_k^j is a pair of two consecutive vertices in τ_k^j .

The definition is best understood by looking at [Figure 12.1](#), where one can see a cyclic permutation as vertices $\sigma_1, \dots, \sigma_n$ cyclically arranged along a circle with respect to the cyclic permutation. A k -arc can be thought of as a bent interval covering k consecutive vertices along the circle, and a gap can be thought of as an edge between two consecutive vertices.

Proof of Theorem 12.2. Let $\mathcal{F} \subseteq \binom{[n]}{k}$ be an intersecting family of k -sets with $n \geq 2k$. Note that there are $(n-1)!$ cyclic permutations of $[n]$ permutations: just fix 1 as the first element of the cycle and consider rearrangements of the others. Let $\sigma \in S_n$ be a cyclic permutation of $[n]$ and let \mathcal{A} be the family of k -arcs of σ that belong to \mathcal{F} .

We claim that

$$|\mathcal{A}| \leq k$$

To see this fix a set $A \in \mathcal{A}$, then for any other $B \in \mathcal{A}$ with $B \neq A$ we have that $|B| = k = |A|$ as well as $A \cap B \neq \emptyset$ since they come from an intersecting family, i.e. the k -arcs overlap. A and B cannot start in the same vertex because they have the same size so they would be equal. Thus one of the two, say B , must start in a gap of the other. But A only has $k-1$ gaps and as we have just seen each gap can have at most one set of \mathcal{A} starting in it. This implies that $|\mathcal{A}| \leq k$, since $A \in \mathcal{A}$ with at most $k-1$ more sets, proving the claim.

We will count the pairs (A, σ) where σ is a cyclic permutation and $A \in \mathcal{F}$ is a k -arc of σ . We count them in two ways:

$$\begin{aligned}
 (1) \quad & \sum_{\sigma \text{ cyclic permutation}} \sum_{A \in \mathcal{F}} \delta_{\{A \text{ } k\text{-arc in } \sigma\}} \leq \sum_{\sigma \text{ cyclic permutation}} k = (n-1)!k \\
 (2) \quad & \sum_{A \in \mathcal{F}} \sum_{\sigma \text{ cyclic permutation}} \delta_{\{A \text{ } k\text{-arc in } \sigma\}} = \sum_{A \in \mathcal{F}} k!(n-k)! = |\mathcal{F}| k!(n-k)!
 \end{aligned}$$

For (2), we used that we can assume that the first element of the cyclic permutation is also the first one of A and therefore the first k elements and also the last $n-k$ elements are determined by A but the order within each of the two sets can be chosen. Combining (1) and (2) we get

$$|\mathcal{F}| \leq \frac{(n-1)!}{(k-1)!(n-k)!} = \binom{n-1}{k-1}$$

proving the theorem. □

Remark. The upper bound from [Theorem 12.2](#) is tight since for $x \in [n]$ we have a star-family $\mathcal{F}_x := \{A \in \binom{[n]}{k} \mid x \in A\}$, which by construction is an intersecting family with $|\mathcal{F}_x| = \binom{n-1}{k-1}$.

On our journey through the world of combinatorics we will often look for families of maximum size with a certain property as well as for maximal families with a certain property, making a distinction between *maximum* and *maximal* objects.

Definition 12.4 (Maximum and maximal). The *maximum* family with a certain property is the biggest family with this property by cardinality. A *maximal* family with some property, is a family with this property, such that adding any object to the family will cause it to lose the property.

The Erdős-Ko-Rado Theorem [12.2](#) talks about *maximum* intersecting families of k -sets. They are the largest *maximal* intersecting families as well. On the other end, it is interesting to construct small maximal intersecting families of k -sets.

Example 21 (Maximal intersecting family from projective planes). Let k be some prime power, then there exists a finite projective plane of order k . This plane has $n = k^2 + k + 1$ points. Denote by \mathcal{P} the set of points and by \mathcal{L} the set of lines of such a projective plane. We know that $|\mathcal{P}| = n = |\mathcal{L}|$, each line $L \in \mathcal{L}$ contains $k+1$ points and each point $p \in \mathcal{P}$ belongs to $k+1$ lines.

We claim that \mathcal{L} is a *maximal* $(k+1)$ -intersecting family. To see this let $E \notin \mathcal{L}$ be a collection of points with $|E| = k+1$. We will show that $\mathcal{L} \cup E$ is not an intersecting family. Let $x, y \in E$ be two distinct points. In \mathcal{L} there is a line L_{xy} containing both. Since $E \notin \mathcal{L}$ there is some $z \in L_{xy} \setminus E$. There are $(k+1)$ lines passing through z so k of these are not L_{xy} . Since two lines cross in exactly one point these lines are disjoint in $\mathcal{P} \setminus \{z\}$. Now if $E \cup \mathcal{L}$ would be intersecting, E would have at least one point in common with each of these k lines, plus the two initial points $x, y \in L_{xy}$. Thus $|E| \geq k+2$ which is a contradiction.

12.2 Shadows and intersecting families

Inspired by the illustration with different ranks of \mathcal{B}_n , we now introduce the notion of *shadows* that will lead to a second proof of Sperner's [Theorem 12.1](#). In essence this is the original proof of Sperner.

Definition 12.5 (Up- and Down-shadows). Let $\mathcal{B} \subseteq \binom{[n]}{k}$ for some $n, k \in \mathbb{N}$. Then we define the *down-shadow* of \mathcal{B} – denoted $\Delta\mathcal{B}$ – as

$$\Delta\mathcal{B} := \{A \mid |A| = k - 1, \exists B \in \mathcal{B} \text{ with } A \subseteq B\}$$

The *up-shadow* of \mathcal{B} – denoted $\nabla\mathcal{B}$ – is defined as

$$\nabla\mathcal{B} := \{A \mid |A| = k + 1, \exists B \in \mathcal{B} \text{ with } B \subseteq A\}$$

Remark. Think of the triangle in the notation as a light-source once shining down and once up to get the respective shadows.

Unsurprisingly the size of the up- and down-shadows is related to the size of \mathcal{B} .

Lemma 12.6. Let $n, k \in \mathbb{N}$ and $\mathcal{B} \subseteq \binom{[n]}{k}$, then the up- and down-shadow satisfy the following inequalities:

$$\begin{aligned} (1) \quad |\Delta\mathcal{B}| &\geq \frac{k}{n - (k - 1)} |\mathcal{B}|, \\ (2) \quad |\nabla\mathcal{B}| &\geq \frac{n - k}{k + 1} |\mathcal{B}| \end{aligned}$$

Proof. We double count the pairs (A, B) with $B \in \mathcal{B}$ and A in its respective shadow.

So assume that A is in the down-shadow of B . For each $B \in \mathcal{B}$ we can remove any of the k elements of B to get an A in the shadow. This shows that the number of pairs (A, B) is

$$\#(A, B) = k|\mathcal{B}|$$

To a given set A of size $k - 1$ which belongs to $\Delta\mathcal{B}$ we can add $n - (k - 1)$ different elements to get a k set containing A . Each of these k -sets may belong to \mathcal{B} . Hence,

$$\#(A, B) \leq (n - (k - 1)) |\Delta\mathcal{B}|$$

Putting things together we get

$$k|\mathcal{B}| = \#(A, B) \leq (n - (k - 1)) |\Delta\mathcal{B}| \iff \frac{k|\mathcal{B}|}{n - (k - 1)} \leq |\Delta\mathcal{B}|$$

An analogous argument counting the pairs (A, B) with A in the up-shadow by removing/adding elements to A and B respectively in the same fashion as we just did, we get that

$$(n - k)|\mathcal{B}| = \#(A, B) \leq (k + 1) |\nabla\mathcal{B}|.$$

This then implies that $\frac{n - k}{k + 1} |\mathcal{B}| \leq |\nabla\mathcal{B}|$, finishing the proof. \square

Corollary 12.7. For $k \geq \frac{n+1}{2}$ we get $|\Delta\mathcal{B}| \geq |\mathcal{B}|$ and for $k \leq \frac{n-1}{2}$ we get $|\nabla\mathcal{B}| \geq |\mathcal{B}|$.

Proof. Plug the values for k into the inequality of Lemma 12.6. \square

We are now ready for the proof of Sperner's theorem.

Proof 2 of Theorem 12.1. Let \mathcal{A} be an antichain in \mathcal{B}_n and denote by $\mathcal{A}_i := \mathcal{A} \cap \binom{[n]}{i}$ the elements of \mathcal{A} from the i -th rank. Fix j_1, j_2 to be minimal and maximal respectively such that $\mathcal{A}_{j_k} \neq \emptyset$. We analyse two cases for the values of j_k , in order to prove that we can assume $j_1 = j_2$ to be the middle rank, which for odd n comes back to choosing either $\frac{n-1}{2}$ or $\frac{n+1}{2}$ which are both equally valid. In the cases we will refer to j_k as j since it is clear what we mean.

If $j = j_1 \leq \frac{n-1}{2}$ define

$$\mathcal{A}' := \mathcal{A} - \mathcal{A}_j + \nabla\mathcal{A}_j$$

See Figure 12.2 for a schematic representation. The up-shadow $\nabla\mathcal{A}_j$ contains at least as many elements as \mathcal{A}_j for $j < \frac{n-1}{2}$ (Corollary 12.7). Moreover, \mathcal{A} contains no sets which are proper supersets of elements of \mathcal{A}_j in particular $\mathcal{A} \cap \nabla\mathcal{A}_j = \emptyset$. Hence \mathcal{A}' is an antichain and $|\mathcal{A}'| \geq |\mathcal{A}|$.

So we found an antichain \mathcal{A}' with $\mathcal{A}'_i := \mathcal{A}' \cap \binom{[n]}{i} = \emptyset$ for all $i \leq j$ that is at least as large as \mathcal{A} , hence we can assume that $j > \frac{n-1}{2}$.

If $j = j_2 \geq \frac{n+1}{2}$ we consider

$$\mathcal{A}' := \mathcal{A} - \mathcal{A}_j + \Delta\mathcal{A}_j$$

again this is an antichain and $|\mathcal{A}'| \geq |\mathcal{A}|$

Together this shows that there is a maximum antichain which is a subset of rank $\lfloor \frac{n}{2} \rfloor$, i.e., for every antichain \mathcal{A} we have $|\mathcal{A}| \leq \binom{[n]}{\lfloor \frac{n}{2} \rfloor}$. This was the claim of the theorem. \square

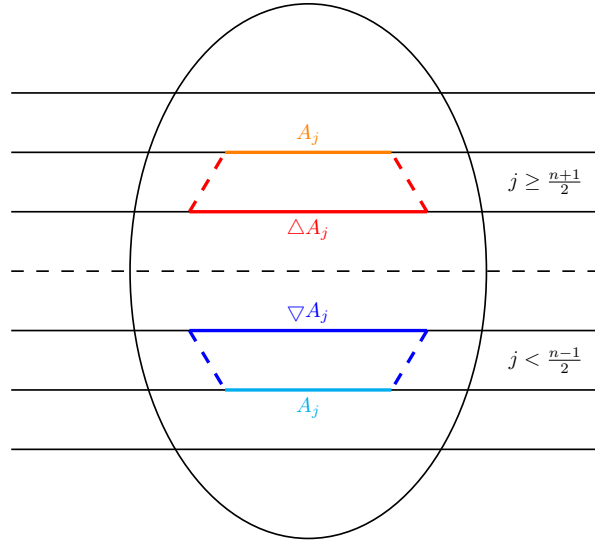


Figure 12.2: A schematic representation of the \mathcal{A}_j and the respective shadows.

12.3 Colex order, cascading representation and the Kruskal-Katona theorem

In this section we prepare for the formulation of the Kruskal-Katona theorem which gives a precise lower bound on the size of the downshadow of a family of k -sets.

Definition 12.8 (Colex order). Let $A, B \subset \mathbb{N}$ be two finite sets. In the *colex order* A precedes B , denoted $A < B$ if and only if $\max(A \Delta B) \in B$. Here $A \Delta B := (A \setminus B) \cup (B \setminus A)$ is the *symmetric difference*.

Observation. With a finite subset $A \subset \mathbb{N}$ we associate its characteristic vector, this is an infinite boolean vector filled with 0's, having a one at the i -th position if $i \in A$. For example the set $A = \{1, 2, 6\}$ will be represented by $(0, 1, 1, 0, 0, 0, 1, 0, 0, \dots)$. Using this representation it is easy to determine whether $A < B$ or not: just write them both as their respective boolean vectors and compare their 1-entries from right to left, where 1's at the same position in both vectors are ignored and the one having the rightmost remaining 1 is colex larger. For example let

$$\begin{aligned} A &= (1, \mathbf{0}, 0, \underline{1}, \underline{1}, \underline{1}, 0, \dots) &= \{0, 3, 4, 5\} \\ B &= (0, \mathbf{1}, 0, \underline{1}, \underline{1}, \underline{1}, 0, \dots) &= \{1, 3, 4, 5\}, \end{aligned}$$

then $A < B$ since they share the underlined 1's and the bold 1 in B is the at the rightmost position where they disagree.

One immediately observes that determining $A < B$ using this representation comes back to determine whether the binary number encoded by the boolean vector representing B is bigger than the one representing A , i.e.

$$A = (1, \mathbf{0}, 0, \underline{1}, \underline{1}, \underline{1}, 0, \dots)_2 = 57 < 58 = (0, \mathbf{1}, 0, \underline{1}, \underline{1}, \underline{1}, 0, \dots)_2 = B.$$

So to get the colex order we can use the standard order for numbers $0 < 1 < 2 < 3 < \dots$, convert them to their binary representation and use the binary representation to get the subsets of \mathbb{N} back:

$$\begin{aligned} 0 &< 1 < 2 < 3 < \dots \\ \iff (0, 0, 0, 0, \dots)_2 &< (1, 0, 0, 0, \dots)_2 < (0, 1, 0, 0, \dots)_2 < (1, 1, 0, 0, \dots)_2 < \dots \\ \iff \emptyset &< \{0\} < \{1\} < \{0, 1\} < \dots \end{aligned}$$

For us, the colex order on k -subsets of \mathbb{N} for some fixed $k \in \mathbb{N}$ will be of special relevance; that is binary numbers having exactly k nonzero entries. The colex order on k -subsets can be used to determine the *k-cascade representation* of numbers.

Proposition 12.9. For every $k, m \in \mathbb{N}$ there exists a unique strictly monotone sequence $a_k > a_{k-1} > \dots > a_s \geq s \geq 1$ for some $s < k$ and $a_i \in \mathbb{N}$ such that

$$m = \binom{a_k}{k} + \binom{a_{k-1}}{k-1} + \dots + \binom{a_s}{s}$$

This is called the *k-cascading representation* of m .

Proof. The proof is by induction over m . If $m = 1$, then $\binom{k}{k}$ does the trick for any $k \in \mathbb{N}$. This is also the only possibility, since each summand of the wanted sum is at least 1.

Given $m > 1, k \in \mathbb{N}$, we can define

$$a_k = \max \left\{ t : \binom{t}{k} \leq m \right\}, \text{ and } m' = m - \binom{a_k}{k}$$

If $m' = 0$, we are done. Otherwise since $m' < m$, it has a unique $(k-1)$ -cascading representation using the numbers $a_{k-1} > \dots > a_s \geq s \geq 1$:

$$m' = \binom{a_{k-1}}{k-1} + \dots + \binom{a_s}{s} \Rightarrow m = \binom{a_k}{k} + \dots + \binom{a_s}{s}$$

To prove that this sum is a k -cascading representation of m , we just need to show $a_k > a_{k-1}$. But if $a_k \leq a_{k-1}$, we would get

$$m \geq \binom{a_k}{k} + \binom{a_{k-1}}{k-1} \geq \binom{a_k}{k} + \binom{a_k}{k-1} = \binom{a_k+1}{k}$$

This contradicts the choice of a_k .

For uniqueness of this representation, we just have to prove that we cannot choose any other value for a_k , because once it is chosen, the values for the rest of the sum m' are unique by induction. Assume therefore we would choose a_k not maximal but smaller. Then

$$\begin{aligned} m &\geq \binom{a_k+1}{k} = \binom{a_k}{k} + \binom{a_k}{k-1} = \binom{a_k}{k} + \binom{a_k-1}{k-1} + \binom{a_k-1}{k-2} = \dots = \sum_{i=0}^{k-1} \binom{a_k-i}{k-i} + \binom{a_k-k+1}{0} \\ &> \sum_{i=0}^{k-1} \binom{a_{k-i}}{k-i} \end{aligned}$$

This is the largest sum that can be built though if a_k is its largest value, so no k -cascading representation of m exists that starts with $\binom{a_k}{k}$. \square

The idea behind determining the k -cascading representation for m from the colex order is the following: Write the first $m+1$ subsets of \mathbb{N} of size k in binary representation in the colex order into a table from left to right, such that each binary number is written in one column from top to bottom as seen in [Example 22](#). Note that for any t the first $\binom{t}{k}$ entries that the table contain exactly k ones out of the first t bits. The idea is to successively choose blocks of the form $\binom{a_r}{r}$ for $r = k$ down to 1 up to the position m : We look for the lowest one in the $(m+1)$ -th column. We go back left from this 1 until we see a zero and then jump to the next higher row say row t . This determines a block of size $\binom{t}{k}$ as there are k ones distributed among t bits in every possible way. Then we continue with the other ones in the representation of $m+1$, choosing blocks with $(k-1)$ ones from among the columns after the previously chosen block and proceed with $k-2$, etc. Since the $(m+1)$ th column is larger than all previous ones in colex order,

every column is put in one of the up to k blocks, namely in the one corresponding to the downmost 1 of column $m+1$ which it does not have as well. The ordering by colex order also assures, that the row left of one of these ones consists of only zeros then only ones from the end of the last chosen block towards the right end at column m .

Example 22 (3-cascading representation). The following figure represents a table of the 3-subsets of \mathbb{N} in binary notation written in columns with respect to their colex order. Let us look at $m = 15$ for example.

1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16
1	1	1	0	1	1	0	1	0	0	1	1	0	1	0	0
1	1	0	1	1	0	1	0	1	0	1	0	1	0	1	0
1	0	1	1	0	1	1	0	0	1	0	1	1	0	0	1
0	1	1	1	0	0	0	1	1	1	0	0	0	1	1	1
0	0	0	0	1	1	1	1	1	1	0	0	0	0	0	0
0	0	0	0	0	0	0	0	0	0	1	1	1	1	1	1

$15 = 10 + 3 + 2 = \binom{5}{3} + \binom{3}{2} + \binom{2}{1}$

Figure 12.3: Determining the 3-cascading representation of $m = 15$ using the colex order. The boxes coming from the respective ones in the $m+1 = 16$ th column are marked by the same color. The n -th column represents the n -th 3-subset in the colex order.

We finish this lecture by stating the *Kruskal-Katona theorem*. We will give no proof of this theorem but in the next lecture we will see a proof of a slightly weaker version of the theorem due to Lovász.

Theorem 12.10 (Kruskal-Katona). Let $k \in \mathbb{N}$ and choose a family $\mathcal{F} \subset \binom{\mathbb{N}}{k}$. Let the unique k -cascading representation for $|\mathcal{F}|$ use $a_k > a_{k-1} > \dots > a_s \geq s \geq 1$, i.e.

$$|\mathcal{F}| = \binom{a_k}{k} + \binom{a_{k-1}}{k-1} + \dots + \binom{a_s}{s}.$$

Then the size of the down-shadow of \mathcal{F} satisfies the following inequality:

$$|\Delta\mathcal{F}| \geq \binom{a_k}{k-1} + \binom{a_{k-1}}{k-2} + \dots + \binom{a_s}{s-1}.$$

Remark. We indicate by example how to show that the lower bound for the down-shadows is tight for every k and $|\mathcal{F}|$: For $k = 3$ and $\mathcal{F} = \{\{0, 1, 2\}, \{0, 1, 3\}, \dots, \{1, 3, 5\}\}$ which is the union of the first 15 sets in colex order (that is up to position $m = 15$ in Figure 12.3), we have $15 = \binom{5}{3} + \binom{3}{2} + \binom{2}{1}$ as seen. For this example we get

$$|\Delta\mathcal{F}| = |\{\{0, 1\}, \{0, 2\}, \dots, \{3, 5\}\} \cup \{\{1, 6\}, \{2, 6\}, \{3, 6\}\} \cup \{\{4, 6\}\}| = \binom{5}{2} + \binom{3}{1} + \binom{2}{0} = 14$$

The Lovász Version of Kruskal-Katona

In this lecture we prove the simplified version of the Kruskal-Katona theorem due to Lovász as mentioned at the end of the last lecture.

Theorem 13.1 (Lovász version of Kruskal-Katona). *Let $k \in \mathbb{N}$ and let \mathcal{F} be a family of k -sets. Let $|\mathcal{F}| = \binom{x}{k}$ for $x \in \mathbb{R}$, $x \geq k$, where*

$$\binom{x}{k} = \frac{x(x-1)\dots(x-k+1)}{k!}$$

Then the down-shadow of \mathcal{F} satisfies the following inequality:

$$|\Delta\mathcal{F}| \geq \binom{x}{k-1} \quad (13.16)$$

Remark. One might want to check whether we can always find an $x \in \mathbb{R}$ such that $|\mathcal{F}| = \binom{x}{k}$ holds. This is the case, since the roots of the polynomial $\frac{x(x-1)\dots(x-k+1)}{k!}$ are given by $0, 1, \dots, k-1$ and the polynomial is strictly monotonically increasing for values of x larger than $k-1$. So for any value of $|\mathcal{F}|$ we find a unique value of $x \geq k-1$ such that $|\mathcal{F}| = \binom{x}{k}$. Since $\binom{k}{k} = 1$ it makes sense to look at $x \geq k$.

The proof will require some understanding of a technique called *shifting*. The idea of shifting is to reduce the largest colex order number of a set in the family of k -sets. The formal definition of shifting is as follows:

Given a family $\mathcal{F} \subseteq \binom{\mathbb{N}}{k}$ of k -sets and $i \in \mathbb{N}$, the i -shift of $F \in \mathcal{F}$ is given by

$$S_i(F) = \begin{cases} F - i + 1 & \text{if } i \in F, \quad 1 \notin F, \quad F - i + 1 \notin \mathcal{F} \\ F & \text{otherwise} \end{cases}$$

The i -shift of the family \mathcal{F} is obtained by applying the shift operator to each of its members:

$$S_i(\mathcal{F}) = \{S_i(F) \mid F \in \mathcal{F}\}.$$

In the case that $S_i(F) = F - i + 1$ we say that the shift was successful, and in the case of $S_i(F) = F$ we say that it was not. For example if $F = \{2, 4, 6\} \in \mathcal{F}$ then $S_6(F) = \{1, 2, 4\}$ if this set is not already in \mathcal{F} , otherwise $S_6(F) = F$.

Remark. In the original proof of Kruskal-Katona a more general shift S_{ij} is used which tries to replace F by $F - j + i$.

Observation. $|S_i(\mathcal{F})| = |\mathcal{F}|$, since we do not introduce duplications and therefore gain as many sets as we lose.

Lemma 13.2.

$$\Delta S_i(\mathcal{F}) \subseteq S_i(\Delta \mathcal{F})$$

In other words, the size of the down-shadow is not increasing when shifting, and by repeating this again and again we get a smaller and smaller set, for which we will then show the inequality in Equation (13.16).

Proof of Lemma 13.2. Consider $E \in \Delta S_i(\mathcal{F})$. Then there exists $F \in \mathcal{F}$ such that $E = S_i(F) - x$, where x is the element that was "deleted" when going from $S_i(F)$ to its down-shadow $\Delta S_i(\mathcal{F})$. Now we consider four different cases depending on whether i and 1 belong to $S_i(F)$.

- $1, i \notin S_i(F)$: Then $S_i(F) = F$, since if $S_i(F)$ and F are different, then 1 is in $S_i(F)$. So $E = F - x \subseteq F$, which means $E \in \Delta F$. Also $i \notin E$, so $S_i(E) = E$. This implies $E \in S_i(\Delta \mathcal{F})$.
- $1, i \in S_i(F)$: Then $i \in S_i(F)$ implies that $S_i(F) = F$, because a successful shift would have removed i . So $E = F - x \subseteq F$, which means $E \in \Delta F$, now we look at two subcases:
 - if $x \neq 1$: Then $1 \in E$ which means $S_i(E) = E$ and then as before $E \in S_i(\Delta \mathcal{F})$.
 - if $x = 1$: Then $E' = E - i + 1 \in \Delta F$ blocks a successful shift of E , therefore, $E \in S_i(\Delta \mathcal{F})$.
- $i \in S_i(F), 1 \notin S_i(F)$: Again 1 not being in $S_i(F)$ immediately implies $S_i(F) = F$. But then we get $i \in F$ and $1 \notin F$ which are two of the conditions that should allow a shift. This means that F was blocked by $F' = F - i + 1 \in \mathcal{F}$. Now $E = F - x \subset F$ which implies $E \in \Delta F$. Again we look at two subcases:
 - if $x = i$: Then $i \notin E$ which implies $S_i(E) = E$ which means $E \in S_i(\Delta \mathcal{F})$.
 - if $x \neq i$: Then E is a candidate for shifting, since $i \in E$ and $1 \notin E$. However $E' = E - i + 1 \in \Delta F'$ blocks E from being shifted. So $S_i(E) = E$ which means $E \in S_i(\Delta \mathcal{F})$.
- $i \notin S_i(F), 1 \in S_i(F)$: Then $i \notin E$ and therefore $S_i(E) = E$. Thus it is enough to prove $E \in \Delta F$ because then $E \in S_i(\Delta \mathcal{F})$ as required. We look at some subcases
 - if F did not shift: Then $S_i(F) = F$ and by definition $E \in \Delta F$.
 - if F did shift: Then $S_i(F) = F - i + 1$.
 If $x = 1$ then we get E by removing i from F , which implies $E \in \Delta F$.
 If $x \neq 1$ we consider $E' = E - 1 + i = F - x$ so $E' \in \Delta F, i \in E', 1 \notin E'$. Then S_i tries to map E' to E . If it succeeds then $E \in S_i(\Delta \mathcal{F})$, since $E' \in \Delta F$. However if it fails then because it is blocked by $E \in S_i(\Delta \mathcal{F})$.

In all four cases we have shown that every $E \in \Delta S_i(\mathcal{F})$ is also in $S_i \Delta(\mathcal{F})$, this concludes the proof. \square

Despite the length and technicality of the proof the important takeaway is the statement of the lemma itself. We wish to apply this shifting repeatedly, but not indefinitely, so we need a definition for the point, where we can stop.

Definition 13.3. A family \mathcal{F} is called *stable* if $S_i(\mathcal{F}) = \mathcal{F}$ for all $i \geq 2$.

Lemma 13.4. Given a finite family $\mathcal{F} \subseteq \binom{[n]}{k}$ we can convert \mathcal{F} into a stable family \mathcal{G} via shifting. These will have the properties that

$$|\mathcal{F}| = |\mathcal{G}| \quad \text{and} \quad |\Delta \mathcal{G}| \leq |\Delta \mathcal{F}|$$

Proof. The two stated properties follow from the above observation and Lemma 13.2, respectively. We have to show that we reach a stable family: Each successful shifting operation increases the number of sets containing 1 by at least 1. Meaning that we can only do a finite number of shifts and thus reach a stable family. \square

From now on we assume that \mathcal{F} is stable. We partition \mathcal{F} into two sets $\mathcal{F} = \mathcal{F}_0 \cup \mathcal{F}_1$:

$$\mathcal{F}_0 = \{F \in \mathcal{F} \mid 1 \notin F\}$$

$$\mathcal{F}_1 = \{F \in \mathcal{F} \mid 1 \in F\}$$

Also we define

$$\mathcal{F}_1' := \{F - 1 \mid F \in \mathcal{F}_1\}$$

this is a subset of the down-shadow of \mathcal{F}_1 and hence of \mathcal{F} .

Lemma 13.5.

$$\Delta \mathcal{F}_0 \subseteq \mathcal{F}_1'$$

Proof. Let $E \in \Delta \mathcal{F}_0$, so E will be of the form $E = F - x$ with $F \in \mathcal{F}_0$ and $x \neq 1$. Since \mathcal{F} is stable $S_x(F) = F$. But since $x \in F$ and $1 \notin F$ then $S_x(F)$ is blocked by $F - x + 1 \in \mathcal{F}$. By definition $F - x + 1 \in \mathcal{F}_1$ and we conclude that $E = F - x \in \mathcal{F}_1'$. \square

Lemma 13.6.

$$|\Delta \mathcal{F}| = |\mathcal{F}_1'| + |\Delta \mathcal{F}_1|$$

Proof. Since \mathcal{F} is a union of \mathcal{F}_0 and \mathcal{F}_1 the same holds for the down shadows:

$$\Delta \mathcal{F} = \Delta \mathcal{F}_0 \cup \Delta \mathcal{F}_1$$

By Lemma 13.5

$$\Delta \mathcal{F}_0 \subseteq \mathcal{F}_1' \subseteq \Delta \mathcal{F}_1$$

Hence $\Delta \mathcal{F} = \Delta \mathcal{F}_1$.

We introduce a new set $\mathcal{F}_1'' := \{D + 1 \mid D \in \Delta \mathcal{F}_1'\}$ which essentially removes an element and then puts the 1 back in, making the elements the same size as those in \mathcal{F}_1' .

$$\text{Claim: } \Delta \mathcal{F}_1 = \mathcal{F}_1' \dot{\cup} \mathcal{F}_1''$$

This is a disjoint union of sets in \mathcal{F}_1' which do not contain a 1, and sets in \mathcal{F}_1'' which do contain a 1. To prove equality we look at the two inclusions:

" \supseteq ": $\mathcal{F}_1' \subseteq \Delta\mathcal{F}_1$ by definition. Let $E \in \mathcal{F}_1''$ this means that $E = D + 1$ for some $D \in \Delta\mathcal{F}_1'$ and therefore there is an $F \in \mathcal{F}_1$ such that $E = D + 1 = (F - 1) - x + 1 = F - x \in \Delta\mathcal{F}_1$ for some $x \neq 1$. So \mathcal{F}_1' and \mathcal{F}_1'' are subsets of $\Delta\mathcal{F}_1$ and so is their union.

" \subseteq ": Let $E = F - x \in \Delta\mathcal{F}_1$. If $x = 1$ then $E \in \mathcal{F}_1'$. Now if $x \neq 1$ then $F \in \mathcal{F}_1$ implies $F - 1 \in \mathcal{F}_1'$ and then further removing the x we get $F - 1 - x \in \Delta\mathcal{F}_1'$. Finally reintroducing the 1 yields $E = F - x \in \mathcal{F}_1''$. So E is either in \mathcal{F}_1' or in \mathcal{F}_1'' .

Now that we have proved the claim, the rest of the proof follows immediately from the fact that $|\Delta\mathcal{F}_1'| = |\mathcal{F}_1''|$. \square

Finally we get to the proof of **Theorem 13.1** which, briefly summarized, states that

$$\mathcal{F} \subseteq \binom{\mathbb{N}}{k}, \quad |\mathcal{F}| = \binom{x}{k}, \quad x \geq k \quad \implies \quad |\Delta\mathcal{F}| \geq \binom{x}{k-1}$$

Proof. We do the proof by induction over $k \in \mathbb{N}$. For $k = 1$ we get

$$|\mathcal{F}| = m = \binom{m}{1} \quad \text{so } x = m \quad \implies \quad \Delta\mathcal{F} = \{\emptyset\} \text{ and } |\Delta\mathcal{F}| = 1 = \binom{m}{0}.$$

Now for the induction step assume the statement is true for $k - 1$. Then we have

$$|\mathcal{F}| = m = \binom{x}{k}.$$

We can assume without loss of generality that \mathcal{F} is stable, due to **Lemma 13.4**. From **Lemma 13.6** we get

$$|\Delta\mathcal{F}| = |\mathcal{F}_1'| + |\Delta\mathcal{F}_1'|.$$

We claim that that $|\mathcal{F}_1'| \geq \binom{x-1}{k-1}$ (this claim will be shown later) then we can find $y \geq x - 1$, such that $|\mathcal{F}_1'| = \binom{y}{k-1}$. We can apply the induction hypothesis to the above equation to get

$$|\Delta\mathcal{F}_1'| \geq \binom{y}{k-2} \geq \binom{x-1}{k-2}$$

where the second inequality follows from the monotonicity of the polynomial $\binom{y}{k-2}$ for $y \geq k - 2$. All this implies that

$$|\Delta\mathcal{F}| \geq \binom{x-1}{k-1} + \binom{x-1}{k-2} = \binom{x}{k-1}$$

which is what we want to show.

It remains verify the above claim: $|\mathcal{F}_1'| \geq \binom{x-1}{k-1}$. We know that

$$|\mathcal{F}| = |\mathcal{F}_0| + |\mathcal{F}_1| = |\mathcal{F}_0| + |\mathcal{F}_1'|$$

Assume that $|\mathcal{F}'_1| < \binom{x-1}{k-1}$, then since $|\mathcal{F}| = \binom{x}{k}$ we get

$$\binom{x}{k} = |\mathcal{F}_0| + |\mathcal{F}'_1| < |\mathcal{F}_0| + \binom{x-1}{k-1},$$

rearrange this to get

$$|\mathcal{F}_0| > \binom{x}{k} - \binom{x-1}{k-1} = \binom{x-1}{k} + \binom{x-1}{k-1} - \binom{x-1}{k-1} = \binom{x-1}{k}$$

By [Lemma 13.5](#) $|\mathcal{F}'_1| \geq |\Delta \mathcal{F}_0|$. So

$$|\mathcal{F}'_1| \geq |\Delta \mathcal{F}_0| \stackrel{\text{induction}}{>} \binom{x-1}{k-1} \quad \text{!}$$

but this is in contradiction to $|\mathcal{F}'_1| < \binom{x-1}{k-1}$. So we have proved the claim which then completes the proof. \square

Remark. Did you notice that the induction step in the last displayed formula of the proof was on x and not on k ? This observation asks for an induction basis for this second induction. We should show that if $|\mathcal{F}|$ is m and $m < k+1$ (this implies $x < k+1$) we have $|\Delta \mathcal{F}| \geq \binom{x}{k-1}$. While this is true we only have long and ugly proofs. In fact in the literature this gap is ubiquitous.

Now that we have completed this proof we look at an application of the theorem:

13.1 A second proof of the Erdős-Ko-Rado theorem

Recall the statement of [Theorem 12.2 \(Erdős-Ko-Rado\)](#): Suppose that $n \geq 2k$, then for an intersecting family $\mathcal{A} \subseteq \binom{[n]}{k}$ it holds true that

$$|\mathcal{A}| \leq \binom{n-1}{k-1}$$

Second proof using Kruskal-Katona. For \mathcal{A} with the given properties, let $\bar{\mathcal{A}}$ be the family of complements of \mathcal{A} . Consider the down-set of $\bar{\mathcal{A}}$ its elements on the k -th rank (the one \mathcal{A} belongs to) will be disjoint from \mathcal{A} . Suppose that $A \in \mathcal{A}$ is also in the down-set of $\bar{\mathcal{A}}$. Then there is a $B \in \mathcal{A}$ with $A \subset B$. This, however, implies that A and B are disjoint which contradicts the intersection property of \mathcal{A} .

Since $\bar{\mathcal{A}}$ is a family of $n-k$ -sets the $(n-2k)$ -fold application of the shadow operator brings the sets in the family down to the intersection of the down-set of $\bar{\mathcal{A}}$ and rank k . From the above considerations we get $\Delta^{n-2k}(\bar{\mathcal{A}}) \cap \mathcal{A} = \emptyset$.

Now suppose that $|\mathcal{A}| > \binom{n-1}{k-1}$, then since $|\mathcal{A}| = |\bar{\mathcal{A}}|$ and by the symmetry of the binomial coefficients we get

$$|\bar{\mathcal{A}}| > \binom{n-1}{k-1} = \binom{n-1}{n-k}.$$

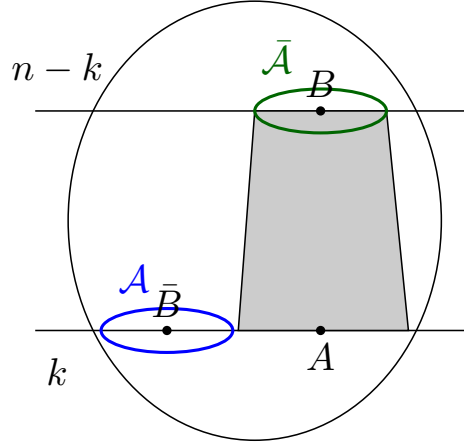


Figure 13.1: The downset of \bar{A} is disjoint from \mathcal{A} in the boolean lattice

And from applying the Lovász version of Kruskal-Katona $(n-2k)$ times to \bar{A} we get that there are at least $\binom{n-1}{(n-k)-(n-2k)} = \binom{n-1}{k}$ sets in $\Delta^{n-2k}(\bar{A})$, i.e., in the intersection of the down-set of \bar{A} with the k -th rank of the Boolean lattice. This implies

$$|\mathcal{A}| + |\Delta^{n-2k}(\bar{A})| > \binom{n-1}{k-1} + \binom{n-1}{(n-k)-(n-2k)} = \binom{n-1}{k-1} + \binom{n-1}{k} = \binom{n}{k} \quad \text{!}$$

The contradiction is because the size of two disjoint sets which both lie on the k -th rank of the Boolean lattice cannot exceed the total size of the k -th rank, which is $\binom{n}{k}$. Therefore $|\mathcal{A}| \leq \binom{n-1}{k-1}$. \square

In the next section we will introduce concepts, which will be extensively used in the next lecture. They can be used to prove **Theorem 12.1** (Sperner's Theorem), but we will also use them to investigate the Boolean lattice even more thoroughly.

13.2 Symmetric chains and symmetric chain decompositions

The concept of a symmetric chain only makes sense in a subclass of posets called *graded* posets:

Definition 13.7 (Graded poset, rank). A poset is *graded* (or *ranked*) if all maximal chains have the same length. The *rank* of an element of a graded poset is its position in any maximal chain (we start with position 0).

It is a good exercise to check that the rank of an element is well-defined as above. If the maximal chains have length h , then the element ranks form a partition of the poset into h antichains R_0, \dots, R_{h-1} .

Definition 13.8 (Saturated chain, symmetric chain). A chain $C \subset P$ is *saturated*, if no element $x \in P \setminus C$ with $\min(C) < x < \max(C)$ exists, such that $C + x$ is a chain.

A saturated chain $C \subset P$ is *symmetric* if

$$\text{rank}(\min(C)) + \text{rank}(\max(C)) = h - 1$$

Note that the minimum and maximum of a chain are well-defined, unique elements of the chain since any two elements are comparable. Saturated chains are paths in the diagram of a poset. Maximal chains and singleton elements are examples of saturated chains. In a graded poset, the diagram can be drawn in a way such that the y -coordinate of any element of rank r is r . In such a diagram, a symmetric chain contains the same number of elements from above the middle line given by $y = \frac{h-1}{2}$ as below it. Some examples can be seen in Figure 13.2:

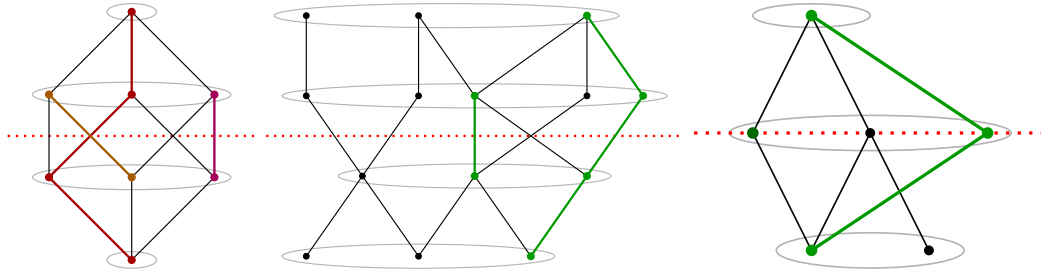


Figure 13.2: Some examples of graded posets with their rank antichains and some symmetric chains: The leftmost example is a symmetric chain decomposition of \mathcal{B}_3

If we can partition a poset into symmetric chains we get a *symmetric chain decomposition* which we will discuss further in the next lecture.

Symmetric Chain Decompositions and Orthogonal Chain Decompositions

At the end of the last lecture we defined symmetric chains. We will use them now to get towards symmetric chain decompositions and later in this lecture talk about orthogonal chain decompositions.

14.1 Symmetric chain decompositions

Definition 14.1 (symmetric chain decomposition). For a poset (P, \leq) a *symmetric chain decomposition* (SCD) is a partition of P into symmetric chains.

We let $\text{rk}(x)$ denote the rank of element x , i.e., its position in any maximal chain where we start with position 0 and let $\text{rk}(P)$ be the maximum rank in P . We also define the *width* $w(P)$ of P as the size of a maximum antichain, i.e., $w(P) = \max(|\hat{A}| : \hat{A} \text{ antichain in } P)$.

Proposition 14.2. Let \mathcal{C} be an SCD of P . It holds that

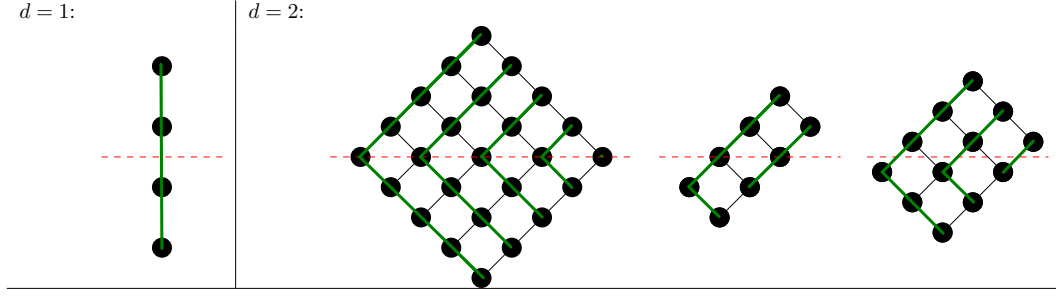
- $|\mathcal{C}| = w(P)$
- $A = \{x : \text{rk}(x) = \lfloor \frac{1}{2} \text{rk}(P) \rfloor\}$ is a maximum antichain.

Proof. Since every chain in \mathcal{C} is symmetric and saturated, it contains an element of A and therefore $|\mathcal{C}| \leq |A| \leq w(P)$. Also each chain in \mathcal{C} contains at most one element from an antichain \hat{A} which implies $w(P) \leq |\mathcal{C}|$. These two inequalities together yield $|\mathcal{C}| \leq |A| \leq w(P) \leq |\mathcal{C}|$ which means $|\mathcal{C}| = |A| = w(P)$ whence A is a maximum antichain. \square

We further observe that for a poset (P, \leq) with $r = \text{rk}(P)$ and ρ_i being the size of rank i , the existence of an SCD implies $\rho_i = \rho_{r-i}$ and that the sequence $\rho_0, \rho_1, \dots, \rho_r$ is *unimodular*, i.e., it increases up to its maximum, then decreases:

$$\rho_0 \leq \rho_1 \leq \dots \leq \rho_{\lfloor \frac{r}{2} \rfloor} = \rho_{\lceil \frac{r}{2} \rceil} \geq \dots \geq \rho_{r-1} \geq \rho_r$$

For the following theorem we need to define the *product* $P \times Q$ of posets $P = (X, \leq_P)$ and $Q = (Y, \leq_Q)$, it has ground set $X \times Y$ and the componentwise order relation \leq_{PQ} , i.e., $(x, y) \leq_{PQ} (x', y') \iff x \leq_P x' \text{ and } y \leq_Q y'$.


 Figure 14.1: Some SCDs for small d

Theorem 14.3. Let K_1, \dots, K_d be chains and

$$P = K_1 \times K_2 \times \dots \times K_d$$

Then P has an SCD.

Proof. Induction on d : For $d = 1, 2$ there is an easy SCD as seen in Figure 14.1

$d - 1 \rightarrow d$: Let $\mathcal{C} = \{C_1, \dots, C_w\}$ be an SCD of $K_1 \times \dots \times K_{d-1}$. We observe that for $Q_i = C_i \times K_d$ we have a partition Q_1, \dots, Q_w of P . The union of the SCDs of $C_i \times K_d$ as in the $d = 2$ case (Figure 14.1) is a chain decomposition of P . But we also know that the product with K_d raises the middle line by $\frac{|K_d|-1}{2}$. From this it can be seen that all the constructed chains are symmetric in $K_1 \times K_2 \times \dots \times K_d$. \square

Corollary 14.4. • Boolean lattices have an SCD since they are products of 2-chains.

- Divisor lattices and therefore multiset lattices have an SCD since the lattice of $m = p_1^{a_1} \cdot p_2^{a_2} \cdot \dots \cdot p_k^{a_k}$ is (isomorphic to)

$$C_{a_1} \times C_{a_2} \times \dots \times C_{a_k}$$

where C_k is the chain with $k + 1$ elements.

- The width of \mathcal{B}_n is $\binom{n}{\lfloor \frac{n}{2} \rfloor}$. (Sperner's Theorem: Theorem 12.1)

14.1.1 A direct construction of an SCD of Boolean lattices

We have seen an inductive construction of symmetric chain decompositions for products of chains. We now aim for a direct construction of an SCD for the Boolean lattice. We will use a clever encoding of the elements of the symmetric chains. To describe this we use an example with $A = \{1, 3, 4, 7, 8\} \subseteq [10]$ (so $n = 10$).

1. Let c_A be the characteristic vector of A , in our example $c_A = (1011001100)$.
2. We replace ones with closing parentheses ')' and zeros with opening parentheses '(' and define the set M_A to contain all the elements corresponding to matching parenthesis. In our example, the parenthesis expression would be $)_1(2)_3)_4(5(6)_7)8(9(10$ (indices indicate the positions) the matched pairs are $(2)_3$, $(5)_8$, and $(6)_7$, therefore $M_A = \{2, 3, 5, 6, 7, 8\}$

3. Define $F_A = [n] - M_A$ and $I_A = M_A \cap A$. In the example $F_A = \{1, 4, 9, 10\}$ and $I_A = \{3, 7, 8\}$.
4. For $F_A = \{x_1 < x_2 < \dots < x_k\}$ and for $i = 0, \dots, k$ let $A_i = I_A \cup \{x_1, x_2, \dots, x_i\}$. Then A_0, \dots, A_k is a saturated chain. From

$$|A_0| = \frac{|M_A|}{2} \quad \text{and} \quad |A_k| = \frac{|M_A|}{2} + |F_A| = \frac{|M_A|}{2} + n - |M_A| = n - \frac{|M_A|}{2}$$

we see that the chain is also symmetric. In our example we get

$$\begin{aligned} A_0 &= \{3, 7, 8\} \\ A_1 &= \{1, 3, 7, 8\} \\ A_2 &= \{1, 3, 4, 7, 8\} \\ A_3 &= \{1, 3, 4, 7, 8, 9\} \\ A_4 &= \{1, 3, 4, 7, 8, 9, 10\} \end{aligned}$$

We claim, that starting the construction with any $A \in \{A_0, \dots, A_k\}$ yields the same chain. This claim is true, because all these sets yield the same set of matched parenthesis P_A (in the example $P_A = \{(2, 3), (5, 8), (6, 7)\}$) and no other element yields this set. That also means that the chain containing A is the set of all B with $P_B = P_A$. The union of all chains that can be obtained by this procedure is an SCD of B_n .

14.1.2 Application: An estimate of Dedekind numbers

Definition 14.5. $D_n = \#(\text{antichains in } B_n)$ are called *Dedekind numbers*. These antichains are exactly the elements of the *free distributive lattice*, which together with the order relation on antichains A and B given by

$$A \leq_F B \Leftrightarrow \forall a \in A \exists b \in B : a \subseteq b$$

is a lattice. Hence Dedekind numbers can also be defined as

$$D_n = \#(\text{elements of the free distributive lattice } F_n)$$

In [Figure 14.2](#) one can see the Hasse diagram for the Boolean lattices and the free distributive lattices for $n = 0, \dots, 3$. Information about Dedekind numbers is collected in the On-Line Encyclopedia of Integer Sequences (entry A000372), see <http://oeis.org/A000372>. From there we have taken the known values:

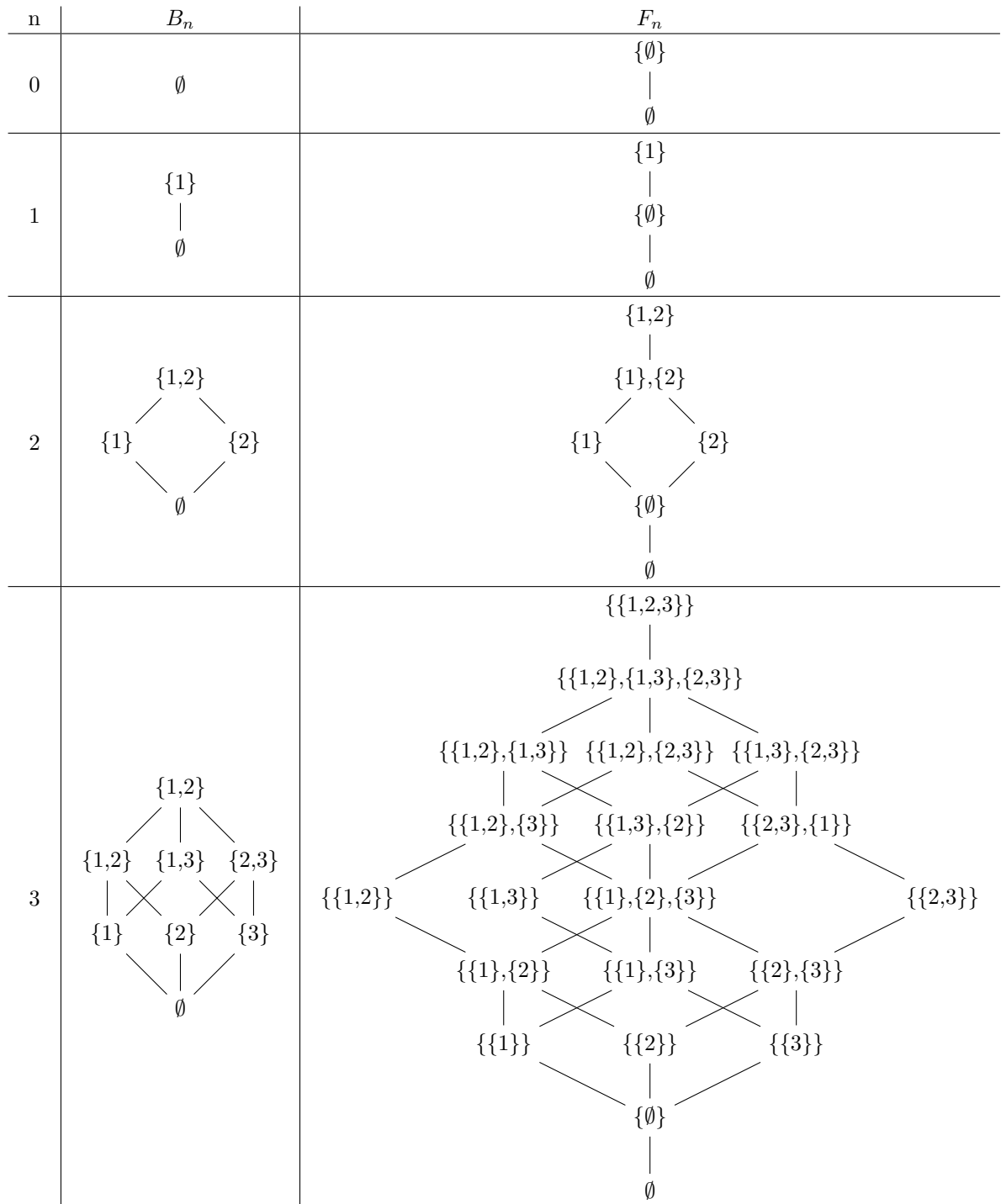


Figure 14.2: Diagrams of the Boolean lattices and the free distributive lattices for $n = 0, \dots, 3$

n	D_n
0	2
1	3
2	6
3	20
4	168
5	7581
6	7828354
7	2414682040998
8	56130437228687557907788

Since there is no easy way known to compute these numbers, we are interested in estimating them. Kleitman and Markowsky showed in 1975 that

$$\binom{n}{\lfloor \frac{n}{2} \rfloor} \leq \log_2(D_n) \leq \binom{n}{\lfloor \frac{n}{2} \rfloor} \left(1 + \mathcal{O}\left(\frac{\log n}{n}\right)\right)$$

In this lecture we prove a weaker theorem:

Theorem 14.6.

$$2^{\binom{n}{\lfloor \frac{n}{2} \rfloor}} \leq D_n \leq 3^{\binom{n}{\lfloor \frac{n}{2} \rfloor}}$$

Proof. The left inequality follows from the fact, that there are $\binom{n}{\lfloor \frac{n}{2} \rfloor}$ elements on rank $\lfloor \frac{n}{2} \rfloor$ on the Boolean lattice and each subset of these is an antichain.

For the right inequality we want to find an estimate on the number of monotone functions (that's all $f : 2^{[n]} \rightarrow \{0, 1\}$ with $f(B) = 1 \implies f(A) = 1$ whenever $A \subseteq B$) which are the characteristic vectors of downsets. Downsets are in bijection with antichains via $D_A = \{b : \exists a \in A \text{ with } b \leq a\}$ and $A_D = \text{Max}(D)$.

The idea is to use the SCD obtained by the parenthesis method (Section 14.1.1) to encode the monotone functions. Given f we look at the chains of the SCD in a fixed order of the chains by increasing size. For chains of size 1 or 2, there are at most 3 possibilities for the evaluation of a monotone f on the elements of the chain, the evaluation $(f(a), f(b)) = (0, 1)$ on a chain $(a < b)$ conflicts with the monotonicity.

Suppose we have encoded the values of f for all elements in chains of length $\leq k$. Now we look at a chain A_0, \dots, A_k of length $k + 1$. The sets in this chain can be written

$$\begin{aligned} A_k &= X_0)X_1)X_2)\dots)X_k \\ &\vdots \\ A_1 &= X_0)X_1(X_2(\dots(X_k \\ A_0 &= X_0(X_1(X_2(\dots(X_k \end{aligned}$$

where X_0, \dots, X_k represent –possibly empty– blocks of matched parenthesis. For each i we can write the set A_i as $Y)X_i(Z$ with appropriate Y and Z . Now define $B_i = Y(X_i)Z$. Note that B_i has an additional pair of matched parenthesis, hence, it belongs to a chain of length at most k and $f(B_i)$ is known. Now observe that $A_{i-1} \subset B_i \subset A_{i+1}$. Therefore

- if $f(B_i) = 0$, then $f(A_j) = 0$ for all $j \geq i + 1$
- if $f(B_i) = 1$, then $f(A_j) = 1$ for all $j \leq i - 1$

Consider the sequence $f(B_1)f(B_2)\dots f(B_{k-1})$ and set $i = \max\{j : f(B_j) = 1\}^V$. From $(f(B_i), f(B_{i+1})) = (1, 0)$ we can conclude that $f(A_0) = \dots = f(A_{i-1}) = 1$ and $f(A_{i+2}) = \dots = f(A_k) = 0$. Hence only $f(A_i)$ and $f(A_{i+1})$ are not determined and we have at most 3 possibilities to choose values for $f(A_i)$ and $f(A_{i+1})$.

The number of chains in the SCD is given by the width of the Boolean lattice, that is we have $\binom{n}{\lfloor \frac{n}{2} \rfloor}$ chains. We have seen that we can encode f by recording one of three possible values for each chain, hence there can be at most 3 to the power of $\binom{n}{\lfloor \frac{n}{2} \rfloor}$ monotone functions. \square

14.2 Orthogonal chain decompositions

Definition 14.7. Two chain decompositions $\mathcal{C}_1, \mathcal{C}_2$ of the same poset are called *orthogonal* if $|C_1 \cap C_2| \leq 1$ for all $C_1 \in \mathcal{C}_1, C_2 \in \mathcal{C}_2$.

It is an open question, how many pairwise orthogonal chain decompositions (OCDs) can be found in Boolean lattices:

- A pair of OCDs can be constructed as follows: Let \mathcal{C}_1 be the SCD obtained from the parenthesis construction. Recall that this construction was based using the replacement $0 \leftrightarrow ($ and $1 \leftrightarrow)$. Construct \mathcal{C}_2 with the same method but based on $0 \leftrightarrow)$ and $1 \leftrightarrow ($. It can be shown that $C_1 \in \mathcal{C}_1$ and $C_2 \in \mathcal{C}_2$ have at most one element in common unless both contain \emptyset and $[n]$. This can be avoided by moving \emptyset to another chain in \mathcal{C}_2 that is disjoint of C_1 .
- It is conjectured that $\lceil \frac{n+1}{2} \rceil$ OCDs exist in the Boolean lattice \mathcal{B}_n .
- In 2018 it was shown with computer assistance that for $n \geq 60$ always 4 OCDs exist.

Pairs of orthogonal chain decompositions have a nice application to estimating the probability of being comparable. Given a probability distribution ϕ on P , what can we say about $\Pr(x \leq y)$ when x and y are chosen independently with respect to ϕ ? If ϕ is concentrated on a single element $\Pr(x \leq y) = 1$ and if ϕ is the uniform distribution on a maximum antichain, then $\Pr(x \leq y) = 1/w(P)$. We are thus interested in lower bounds.

Theorem 14.8. Let P be a poset with a pair of orthogonal chain decompositions $\mathcal{C}_1, \mathcal{C}_2$ and let $k = |\mathcal{C}_1|, l = |\mathcal{C}_2|$. Given a probability distribution on P , for x, y chosen independently with respect to that distribution, it holds, that

$$\Pr(x \leq y) \geq \frac{1}{2} \left(\frac{1}{k} + \frac{1}{l} \right)$$

^VFor the proof we assume $1 \leq i \leq k - 1$ and leave the case that there is no j with $f(B_j) = 1$ to the reader.

Remark. • For $k = l = w(P)$ this implies $\Pr(x \leq y) \geq \frac{1}{w(P)}$.

- If C is an n -chain then C has no pair of orthogonal chain partitions each consisting of one chain, but $w(C) = 1$. Still, for the uniform distribution

$$\Pr(x \leq y) = \frac{\binom{n}{2} + n}{n^2} = \frac{n+1}{2n} \sim \frac{1}{2} < \frac{1}{w(C)} = 1$$

- The pair $\mathcal{C}_1, \mathcal{C}_2$ of orthogonal chain decompositions of the Boolean lattice has the property that their numbers of chains equal $\binom{n}{\lfloor \frac{n}{2} \rfloor}$. Hence because we can concentrate the probability on a maximum antichain we get $1/\binom{n}{\lfloor \frac{n}{2} \rfloor} \leq 1/w$ and hence $w \leq \binom{n}{\lfloor \frac{n}{2} \rfloor}$. This is yet another proof of Sperner's Theorem.

For the proof of the theorem we need a few lemmata:

Lemma 14.9. *Let X be a set, $|X| = n$ and $p : X \rightarrow [0, 1]$ a probability distribution. Let further x, y be chosen independently from (X, p) . Then*

$$\Pr(x = y) \geq \frac{1}{n}$$

Proof. First consider the following:

$$0 \leq \sum_{\alpha \in X} (p_\alpha - \frac{1}{n})^2 = \sum_{\alpha \in X} p_\alpha^2 - \frac{2p_\alpha}{n} + \frac{1}{n^2} = \left(\sum_{\alpha \in X} p_\alpha^2 \right) - \frac{2}{n} + \frac{1}{n}$$

This shows that the quantity of interest $\Pr(x = y) = \sum_{\alpha \in X} p_\alpha^2$ has to be at least $1/n$. \square

Lemma 14.10. *Let $P = (X, \leq)$ be a poset, $p : X \rightarrow [0, 1]$ a probability distribution, and $\mathcal{C} = (C_1, \dots, C_k)$ be a chain decomposition of P . If x, y are chosen independently from (X, p) , then*

$$\Pr(x, y \text{ belong to the same chain}) \geq \frac{1}{k}$$

Proof. Interpret \mathcal{C} as k element set with the probability distribution $q(\mathcal{C}) = \sum_{x \in \mathcal{C}} p(x)$ and apply **Lemma 14.9** to (\mathcal{C}, q) . \square

We will finish the proof of **Theorem 14.8** in the next lecture.

Duality Theorems

We will start this lecture with the proof of **Theorem 14.8**. Then we start a new section on *duality theorems*. The first results will be *Dilworth's theorem* and its dual which deal with chains and antichains in posets. We then continue with duality theorems on graphs.

15.1 Probability of an ordered pairs

For the sake of readability we restate **Theorem 14.8** below as **Theorem 15.1**. the proof of the theorem will critically depend on **Lemma 14.9** and **Lemma 14.10** from the previous lecture.

Theorem 15.1. *Let P be a poset with a pair of orthogonal chain partitions $\mathcal{C}_1, \mathcal{C}_2$ and let $k = |\mathcal{C}_1|$, $l = |\mathcal{C}_2|$. Given a probability distribution on P , for x, y chosen independently with respect to that distribution, it holds, that*

$$\Pr(x \leq y) \geq \frac{1}{2} \left(\frac{1}{k} + \frac{1}{l} \right).$$

Proof. Let $P = (X, \leq)$ and let $p : X \rightarrow [0, 1]$ be a probability distribution. Let x and y be drawn independently from this distribution. then

$$\Pr(x \leq y) = \sum_{\alpha \in X} p_\alpha^2 + \sum_{\alpha < \beta, \alpha \beta \in X} p_\alpha p_\beta, \quad (15.17)$$

The first sum gives the probability for $x = y$ and the second sum the probability for $x < y$. Now consider the two orthogonal chain decompositions $\mathcal{C}_1, \mathcal{C}_2$ and ask for the probability that $x < y$ with x and y belonging to the same chain $C \in \mathcal{C}_1 \cup \mathcal{C}_2$. Since the chain decompositions are orthogonal this event is the disjoint union of two events, one for \mathcal{C}_1 the other for \mathcal{C}_2 . Therefore we have:

$$\sum_{\alpha < \beta: \alpha \beta \in P} p_\alpha p_\beta \geq \sum_{\substack{C \in \mathcal{C}_1, \alpha < \beta: \\ \alpha \beta \in C}} p_\alpha p_\beta + \sum_{\substack{C \in \mathcal{C}_2, \alpha < \beta: \\ \alpha \beta \in C}} p_\alpha p_\beta.$$

Combining this inequality with Equation (15.17) and subsequently using Lemma 14.10 we conclude

$$\begin{aligned}
 \Pr(x \leq y) &\geq \sum_{\alpha \in X} p_\alpha^2 + \sum_{\substack{C \in \mathcal{C}_1, \alpha < \beta: \\ \alpha \beta \in C}} p_\alpha p_\beta + \sum_{\substack{C \in \mathcal{C}_2, \alpha < \beta: \\ \alpha \beta \in C}} p_\alpha p_\beta, \\
 &= \frac{1}{2} \left(\sum_{\alpha \in X} p_\alpha^2 + 2 \sum_{\substack{C \in \mathcal{C}_1, \alpha < \beta: \\ \alpha \beta \in C}} p_\alpha p_\beta \right) + \frac{1}{2} \left(\sum_{\alpha \in X} p_\alpha^2 + 2 \sum_{\substack{C \in \mathcal{C}_2, \alpha < \beta: \\ \alpha \beta \in C}} p_\alpha p_\beta \right) \\
 &= \frac{1}{2} \Pr(C_1(x) = C_1(y)) + \frac{1}{2} \Pr(C_2(x) = C_2(y)) \\
 &\geq \frac{1}{2} \left(\frac{1}{k} + \frac{1}{\ell} \right)
 \end{aligned}$$

In the third line $C_i(x) = C_i(y)$ denotes the event that x and y are elements of the same chain $C \in \mathcal{C}_i$, for $i \in \{1, 2\}$. The equation between line two and three is based on the following reasoning. With the factor 2 in front the $\sum_{C \in \mathcal{C}_i, \alpha < \beta: \alpha \beta \in C} p_\alpha p_\beta$ can be seen as the probability of the event that $x \neq y$ belong to the same chain of \mathcal{C}_i . The last inequality follows from Lemma 14.10. \square

Remark. The lower bound in Theorem 14.8 is *tight*. To see this we provide examples of equality instances.

Example 23. Let P be the product of two chains $P = C_2 \times C_3$. This is a poset with six elements. We assign probabilities as shown in the following figure.

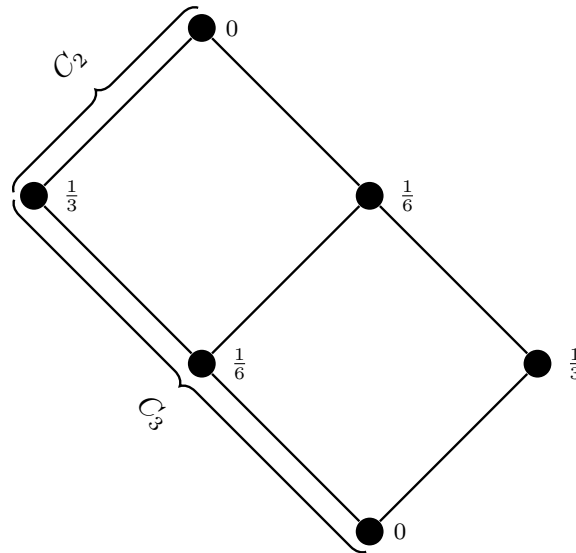


Figure 15.1: The poset $P = C_2 \times C_3$ with respective probabilities.

We immediately see that $\Pr(x \leq y) = 2\left(\frac{1}{3}\right)^2 + 2\left(\frac{1}{6}\right)^2 + \frac{1}{3}\frac{1}{6} + \frac{1}{6}\frac{1}{3} + \frac{1}{6}\frac{1}{6} = \frac{1}{2}\left(\frac{1}{2} + \frac{1}{3}\right)$.

Example 24. Now let $P = C_5 \times C_6$, this is a poset with thirty vertices. Assign probabilities as given by in following figure.

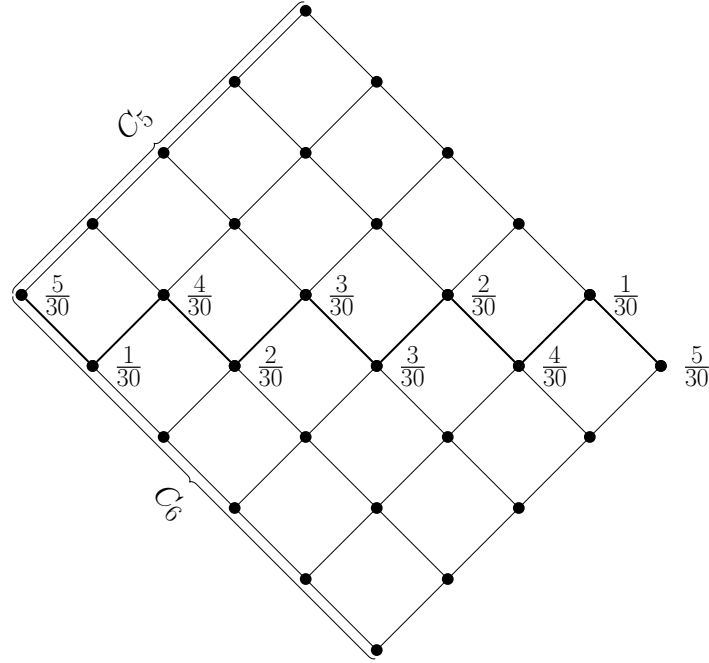


Figure 15.2: The $C_5 \times C_6$ poset with respective probabilities.

It is a little tedious but easy to verify that this again marks an equality instance.

The examples provide an idea on how to continue this construction for arbitrary product posets $C_k \times C_\ell$: if $k = \ell$ assign probability $1/k$ to the elements of the unique maximum antichain. Otherwise assume that $\ell < k$, start by assigning probability $1/\ell$ to the left extreme element and then assign probabilities one-by-one along a zigzag path such that in each step one of the $k + \ell$ chains becomes saturated in the sense that it has its intended probability. The intended probability of a chain C parallel to C_ℓ is $\Pr(x, y \in C \text{ and } x \leq y) = 1/k$ and of a chain parallel to C_k is $\Pr(x, y \in C \text{ and } x \leq y) = 1/\ell$.

15.2 Duality theorems

We start this chapter by proving a theorem due to Dilworth. We then continue with investigating several other duality theorems and making connections between them.

15.2.1 Dilworth's theorem

Before stating and proving Dilworth's theorem, we start by proving its dual which is more obvious. To get to the statement let us first consider the *comparability graph* of a partially ordered set.

Definition 15.2. Let $P = (X, \leq)$ be a poset. The *comparability graph* $\text{Comp}(P) = (X, E)$ is a graph on the same ground set with edges $xy \in E \iff (x < y \text{ or } x > y)$, that is $xy \in E$ if and only if x and y are comparable in P .

Example 25. We give an example of a Poset P together with its comparability graph $\text{Comp}(P)$.

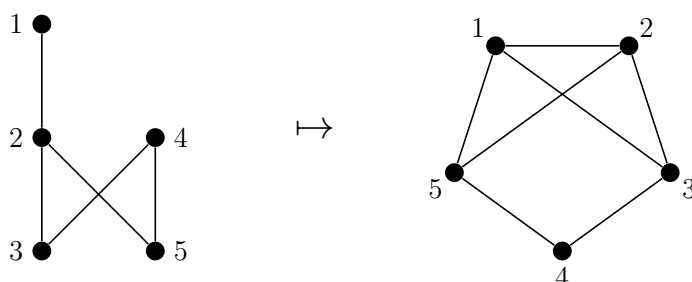


Figure 15.3: A poset on five vertices on the lefthand side, together with its comparability graph on the righthand side.

Definition 15.3 (Coloring of a graph). A *coloring* of a graph $G = (V, E)$ is a map $\gamma : V \rightarrow \mathbb{N}$ (where elements of \mathbb{N} are considered to be colors) such that the two vertices of any edge $xy \in E$ are colored differently $\gamma(x) \neq \gamma(y)$.

We denote by $\chi(G)$ the *chromatic number* of G , that is the minimal number $n \in \mathbb{N}$ such that there is a coloring $\chi : \{1, \dots, n\} \rightarrow V$ of G .

Observation. It turns out that the color classes of the comparability graph of P correspond to antichains in P . Hence, a coloring of the comparability graph induces a decomposition of X into antichains.

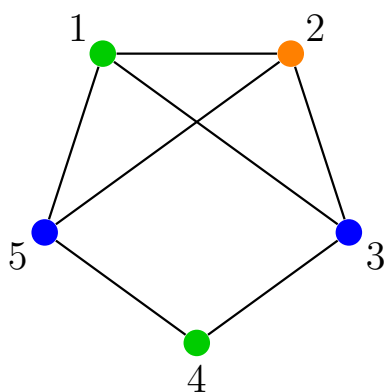


Figure 15.4: A 3-coloring of a comparability graph, related to the previous example.

For every graph G we have $\chi(G) \geq \omega(G)$, where $\omega(G)$ is the *clique number* of G , i.e. the largest integer n such that G contains a K_n (complete graph on n vertices) as a subgraph. This is true because in a K_n any two vertices need to be colored differently.

We are ready for the dual of Dilworth's theorem, which essentially states that for comparability graphs we have $\omega(G) = \chi(G)$.

Proposition 15.4. *Let $P = (X, \leq)$ be a poset. Then*

$$\max(|C| : C \text{ is a chain in } P) = \min(|\mathcal{A}| : \mathcal{A} \text{ is an antichain partition of } P).$$

Proof. First note that for every antichain partition \mathcal{A} of P and for every chain C in P it holds true that

$$|\mathcal{A}| \geq |C|. \quad (15.18)$$

This is true since every element in the chain C has to be in a different antichain of the antichain partition. It remains to construct a pair (\mathcal{A}, C) with equality.

We iteratively construct an antichain partition: Let $P_1 := P$. Given P_i , let $A_i := \min(P_i)$ be the antichain of minimal elements of P_i , then set $P_{i+1} := P_i - A_i$. Since the poset is finite and at each step at least one element is removed from the previous P_i , this iterative procedure terminates. The result is an antichain partition $\mathcal{A} = \{A_1, \dots, A_k\}$. We claim that there is a chain C in P of the same size, i.e. $|C| = k$.

To extract a chain let $x_k \in A_k$ be arbitrary. Since x_k did not belong to A_{k-1} it was not minimal in P_{k-1} , hence there is an $x_{k-1} \in A_{k-1}$ with $x_{k-1} < x_k$. This element x_{k-1} must have a predecessor $x_{k-2} \in A_{k-2}$ with $x_{k-2} < x_{k-1}$. The iteration stops with $x_1 \in A_1$, it yields:

$$C := x_1 < x_2 < \dots < x_k, \quad \text{for } x_i \in A_i.$$

This is a chain of length k , hence we found an equality instance $|\mathcal{A}| = |C|$. This concludes the proof. \square

Remark. For the comparability graph G of P we get $\omega(G) = \chi(G)$ because $\omega(G) = \max(|C| : C \text{ is a chain in } P)$

and $\chi(G) = \min(|\mathcal{A}| : \mathcal{A} \text{ is an antichain partition of } P)$.

We will now state and prove Dilworth's theorem, which we reverses the roles of chain and antichain in the previous proposition. **Theorem 15.5** and **Proposition 15.4** are dual to each other.

Theorem 15.5 (Dilworth's theorem). *Let $P = (X, \leq)$ be a poset. Then*

$$\max(|\mathcal{A}| : \mathcal{A} \text{ an antichain in } P) = \min(|C| : C \text{ a chain partition of } P).$$

Proof. Since a chain and an antichain can share at most one element we directly obtain the *trivial* inequality $|C| \geq |\mathcal{A}|$, hence, we only have to prove the existence of a pair with equality.

The proof is via induction on the number of elements in X . Assume the statement for posets of at most n elements and consider $P = (X, \leq)$ with $|X| = n + 1$.

Let A be an antichain such that $|A|$ is maximal. We define

$$\begin{aligned} U[A] &:= \{x \in X \mid \exists a \in A \text{ such that } x \geq a\}, \\ D[A] &:= \{x \in X \mid \exists a \in A \text{ such that } x \leq a\}, \end{aligned}$$

these are the *upset* and the *downset* of A respectively. Note that A belongs to both parts, in fact $A = \min(U[A])$ and $A = \max(D[A])$. Since antichains of $U[A]$ and $D[A]$ are also antichains in P we see that A is an antichain of maximum size in both parts.

If $|U[A]| < |X|$ and $|D[A]| < |X|$, then we can apply induction to obtain chain partitions \mathcal{C}_U and \mathcal{C}_D of $U[A]$ and $D[A]$ respectively with $|\mathcal{C}_U| = |A| = |\mathcal{C}_D|$. Now for each $a \in A$ let $C_a \in \mathcal{C}_U$ and $C'_a \in \mathcal{C}_D$ be the chains containing a . Since a is the minimal element of C_a and the maximal element of C'_a we can glue the chains together at a to obtain a chain D_a covering $C_a \cup C'_a$. The collection $\mathcal{C} = \{D_a \mid a \in A\}$ is a chain partition of P and $|\mathcal{C}| = |A|$.

If there is no antichain in P such that the above construction can be used, then $|U[A]| = |X|$ or $|D[A]| = |X|$ for every maximum antichain A . The only remaining candidates for a maximum antichain are $\text{Min}(P)$ and $\text{Max}(P)$, i.e. the antichains given by the minimal or maximal elements. We assume that $A = \text{Max}(P)$ is a maximum antichain. Pick $x \in \text{Max}(P)$ and $y \in \text{Min}(P)$ such that $x \geq y$, i.e. they are comparable or equal. Then $\{x, y\}$ is a chain and the maximum size of an antichain in $P \setminus \{x, y\}$ is less than $|A|$. By induction we get a chain partition of $P \setminus \{x, y\}$ by $\mathcal{C}' := \{C_1, \dots, C_k\}$ with $k < |A|$. Adding the chain $\{x, y\}$ to \mathcal{C}' yields a chain partition \mathcal{C} of P with at most $|A|$ chains. Clearly $|\mathcal{C}| = |A|$ and we are done. \square

Definition 15.6 (Height of a poset). We define the *height of a poset* P , written $h(P)$ via $h(P) := \max\{|\mathcal{C}| : \mathcal{C} \text{ is a chain in } P\}$.

Definition 15.7 (Width of a poset). We define the *width of a poset* P , written $w(P)$ via $w(P) := \max\{|A| : A \text{ is an antichain in } P\}$.

A direct corollary to Dilworth's theorem and its dual reads as follows.

Corollary 15.8. *Let $P = (X, \leq)$ be a Poset. Then we get the following bound on the number of elements in P :*

$$|X| \leq h(P)w(P).$$

Getting back to comparability graphs, Dilworth's theorem and its dual can be stated as follows.

Corollary 15.9. *Let P be a Poset, and $G := \text{Comp}(P)$ its comparability graph. Then $\omega(G) = \chi(G)$, and $\alpha(G) = \Theta(G)$.*

Remark. Recall that $\omega(G) = h(P)$ and $\alpha(G) = w(P)$, where $\omega(G)$ denotes the clique number and $\alpha(G)$ the independence number. Also recall that $\chi(G)$ is the chromatic number and $\Theta(G)$ is the minimum number of cliques needed to cover the graph.

Definition 15.10 (ω -perfect graphs). A graph is called ω -perfect if for every induced subgraph $H \subseteq G$ we have $\omega(H) = \chi(H)$.

Proposition 15.4 implies that every comparability graph is ω -perfect.

Definition 15.11 (α -perfect graphs). A graph is called α -perfect if for every induced subgraph $H \subseteq G$ we have $\alpha(H) = \Theta(H)$.

Dilworth's theorem implies that every comparability graph is α -perfect. We state but do not prove an important result on perfect graphs. For a detailed proof visit the lectures on graph theory (discrete mathematics II).

Theorem 15.12 (weak perfect graph theorem). *The following are equivalent for G :*

- G is ω -perfect,
- G is α -perfect,
- G is product-perfect, that is for every induced subgraph $H \subseteq G$ it holds true that $|V_H| \leq \alpha(H)\omega(H)$.

15.2.2 Further duality theorems

There are several duality theorems with a similar flavor as Dilworth's theorem and its dual. An example is the result by Ford and Fulkerson and Ford known as the *Max-Flow Min-Cut theorem*. It states that the flow value of a maximum s - t flow in a capacitated network equals the minimum capacity of an s - t cut. Another example of a duality theorem is *Menger's theorem*. It says that in a graph $G = (V, E)$ with two subsets $A, A' \subseteq V$, the maximum number of pairwise disjoint A - A' paths in G equals a minimum size of a separator separating A from A' . We will focus on yet another duality result, the *bipartite matching theorem*, and prove that it equivalent to Dilworth's theorem.

Recall that a *matching* in a graph G is a subset of edges $M \subseteq E(G)$ such that no two edges $e, e' \in M$ share a vertex. A *vertex cover* of a graph G is a collection of vertices $U \subseteq V(G)$ such that every edge $e \in E(G)$ is incident to at least one vertex in U .

Theorem 15.13 (Bipartite matching theorem (König-Egerváry)). *Let $G = (V, E)$ be a bipartite graph. The minimum size of a vertex cover in G equals a maximum size of a matching in G .*

We show that Dilworth's theorem implies the bipartite matching theorem and conversely.

Dilworth's theorem implies the bipartite matching theorem:

Let $B = (X, Y; E)$ be a bipartite graph. Note that if M is a matching and U is a vertex cover, then $|U| \geq |M|$ because different edges of M have to be covered by different vertices of U . Hence, to prove the theorem we only need such a pair with $|U| = |M|$.

We can interpret B as a poset $P = (S, <)$ with $S = X \cup Y$ and $x < y$ whenever $(x, y) \in E$. Note that the height of P is 2. Therefore a minimum chain partition \mathcal{C} of P consists of chains of size one and two only. The two element chains of \mathcal{C} are a matching M of B . Counting the elements of P via the chains of \mathcal{C} we obtain: $|\mathcal{C}| + |M| = |S| = |X| + |Y|$.

Let A be a maximum antichain in P and let $U = S \setminus A$ be its complement. We claim that U is a vertex cover in B . Otherwise there would be an edge e in the complement

of U , this edge e , however, corresponds to a comparability among elements of A , but A is an antichain. Clearly $|A| + |U| = |S| = |X| + |Y|$.

From Dilworth's theorem, we know that $|C| = |A|$. Together with $|C| + |M| = |S| = |A| + |U|$ this implies $|M| = |U|$. This concludes the proof.

The bipartite matching theorem implies Dilworth's theorem:

Let $P = (S, \leq)$ be a poset, we construct a bipartite graph B_P as follows:

$$B_P = (S', S''; E) \quad \text{here } S' \text{ and } S'' \text{ are two copies of } S, \\ x'y'' \in E \iff x < y \text{ in } P$$

Clearly x' and y'' refer to the elements corresponding to x and y in S' and S'' respectively. The construction of B_P is illustrated in Figure 15.5.

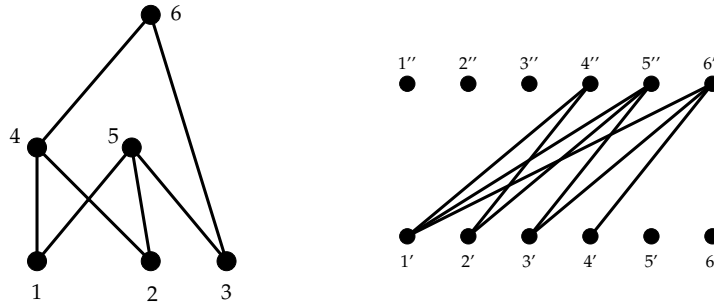


Figure 15.5: The poset P on the left induces the bipartite B_P on the right.

Let M be a maximum matching in B_P . The edges of M correspond to a set C_M of comparabilities in P . Each element y of P participates in at most two comparabilities from C_M . This is because M is a matching and there are only two copies y', y'' of y in B_P , moreover, if y participates in two comparabilities then we have edges $x'y''$ and $y'z''$ in M and get the comparabilities $x < y < z$ in P . Hence the comparabilities in C_M fit together to form a collection of chains. This collection can be extended by one-element chains to form a chain partition C_M of P . The number of chains in C_M is easily seen to be $|S| - |M|$: Start with the trivial chain partition into $|S|$ one-element chains and add the edges of M one by one each added edge glues two chains together thus reducing the number of chains in the partition by one.

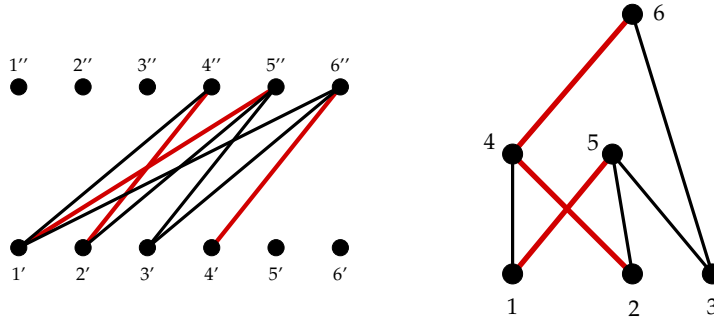


Figure 15.6: On the left a matching of B_P marked in red. On the right the corresponding chain partition of P .

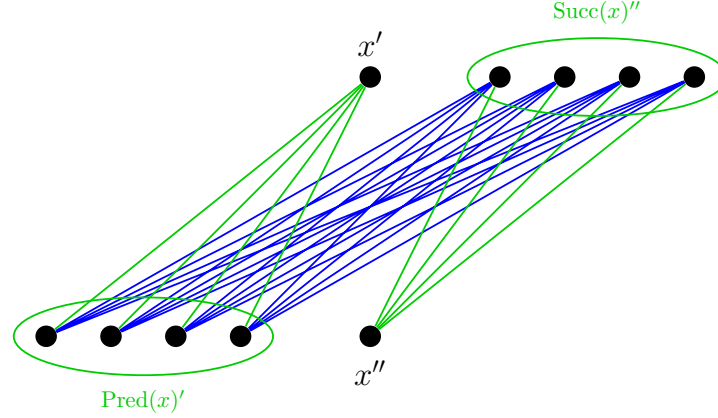


Figure 15.7: The sets $\text{Pred}(x)'$ and $\text{Succ}(x)''$ have been marked in green.

Now consider a minimum vertex cover U in B_P and define

$$A := \{x \mid U \cap \{x', x''\} = \emptyset\}.$$

Since the elements of U cover all the edges of B_P the set A is an antichain of P . We claim that $|A| = |S| - |U|$. If this is shown we can use $|U| = |M|$ to obtain the equality needed for the proof of Dilworth's theorem:

$$|A| = |S| - |U| = |S| - |M| = |\mathcal{C}_M|$$

To prove the equation $|A| = |S| - |U|$ we show that for all x in S the vertex cover U contains at most one of x' and x'' . Consider $\text{Pred}(x)' := \{z' \mid z'x'' \in E\}$ and $\text{Succ}(x)'' := \{z'' \mid x'z'' \in E\}$ as illustrated in **Figure 15.7**.

By transitivity $v < w$ for every $v \in \text{Pred}(x)$ and $w \in \text{Succ}(x)$. This implies $v'w'' \in E$ and the two sets $\text{Pred}(x)'$ and $\text{Succ}(x)''$ form a complete bipartite graph in B_P . To cover this bipartite graph U must contain one of $\text{Pred}(x)'$ and $\text{Succ}(x)''$. If $\text{Pred}(x)' \subset U$ then all the edges incident to x'' are covered, whence, $x'' \notin U$ by minimality of U . In the other case $x' \notin U$. This concludes the proof.

We finish this lecture with a pretty result that has accompanied many math students on their journey throughout a variety of disciplines

Lemma 15.14 (Lemma of Erdős-Szekeres). *Let (a_1, \dots, a_{n^2+1}) be a sequence of real numbers. The sequence contains an increasing or a decreasing subsequence of length $n + 1$.*

Proof. Define a poset $P_A = (X, \leq)$ via

$$(i, a_i) \in X, \tag{15.19}$$

$$(i, a_i) \leq (j, a_j) \iff i \leq j \text{ and } a_i \leq a_j. \tag{15.20}$$

Then a chain in P_A is a weakly increasing subsequence whereas an antichain is a strictly decreasing subsequence. Now $|P_A| = n^2 + 1 \leq h(P_A)w(P_A)$ implying that either $h(P_A)$ or $w(P_A)$ have to exceed n . This concludes the proof. \square

Tilings

This chapter is devoted to *tilings*. We have seen the special case of monomino/domino-tilings of a $1 \times n$ board when discussing fibonacci numbers. Tilings are part of what is called *geometric coverings*, that is we try to cover some geometric regions using only designated patches (in this case called *tiles*).

We will omit a general definition of *tiling* and *tiles* and just introduce the concept of checkerboard tilings: A *region* or a *board* is to be thought of as a subset of the infinite grid. An example for a board would be the 8×8 -board which is a checkerboard when colored accordingly. Tiles are as well subsets of the grid, however, because tiles can be translated and typically we have many copies of a tile it may be better to think of them as connected collections of squares.

Now given a board B and a set of tiles T a *tiling of B with T* is given by a placement of tiles on the board such that they cover the whole board and do not overlap.

Example 26 (Tiling a region). Let B be a 4×3 board and T the set of dominoes. The following figure shows B a single tile and a tiling of B with dominoes.

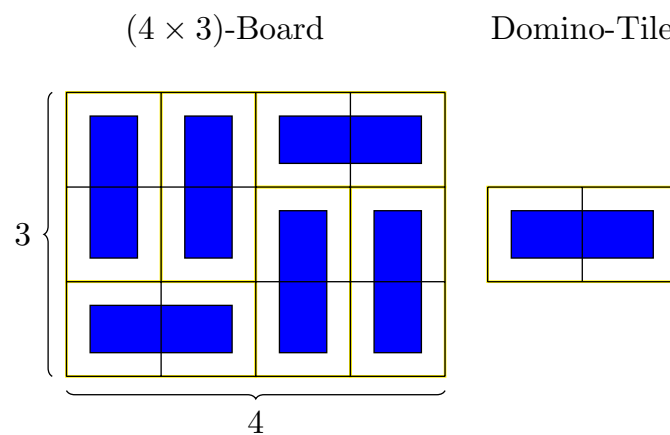


Figure 16.1: A (4×3) -board with a domino-tiling.

Given a board B and a collection T of tiles a combinatorialist may ask the following questions:

- Does a tiling exist, i.e., can B be tiled with tiles from T ?
- How many tilings of B with tiles from T exist?

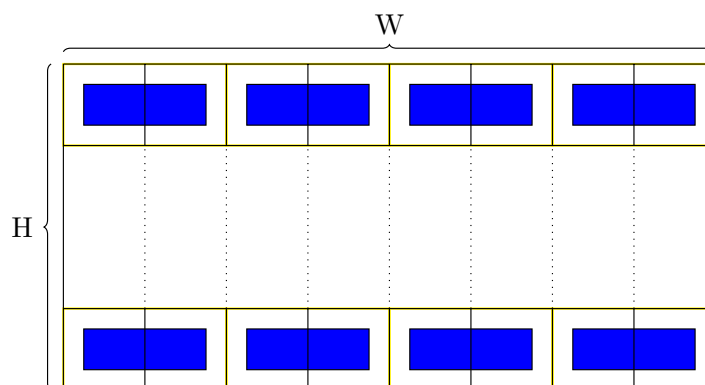


Figure 16.2: A tiling of an $H \times W$ -board with H identical rows.

- What are properties of the tilings? e.g. what is the probability that a given cell of B is covered by a horizontal/vertical domino?

In this lecture we will focus on existence, i.e., on the first question and answer it for several combinations of boards and tiles.

16.1 Tiling boards with dominoes

We start by considering tilings of rectangular and almost rectangular boards using domino tiles.

Proposition 16.1. *Let $H, W \in \mathbb{N}$ then the $(H \times W)$ -board has a domino tiling if and only if $H \cdot W \equiv 0 \pmod{2}$.*

Proof. \Rightarrow : Consider a checkerboard coloring of the $(H \times W)$ -board. Each domino placed on the board will cover a white cell and a black cell. A tiling provides a bijection between black and white cells. Hence, if B can be tiled its cells can be partitioned into two parts of equal size, i.e., the number of cells is even.

\Leftarrow : Assume that $H \cdot W \equiv 0 \pmod{2}$, hence, one of H and W is even, say W is even. We can cover the $(1 \times W)$ -board with domino tiles by putting them side by side. Repeating this tiling for each of the $|H|$ rows on the $H \times W$ board giving a tiling for this board see Figure 16.2. \square

Next we look at *almost rectangular* boards, that is $(n \times m)$ -boards where some cells have been deleted.

Proposition 16.2. *Given an $(H \times W)$ -board with H even and $W \geq 2$, if we delete one black and one white cell the remaining board admits a tiling.*

Proof. Since H is even we know from the previous proposition that the $(H \times W)$ -board admits a tiling. Thinking of the board as a graph, we next consider its *dual graph* which has a vertex for each cell of the board and an edge between two vertices if

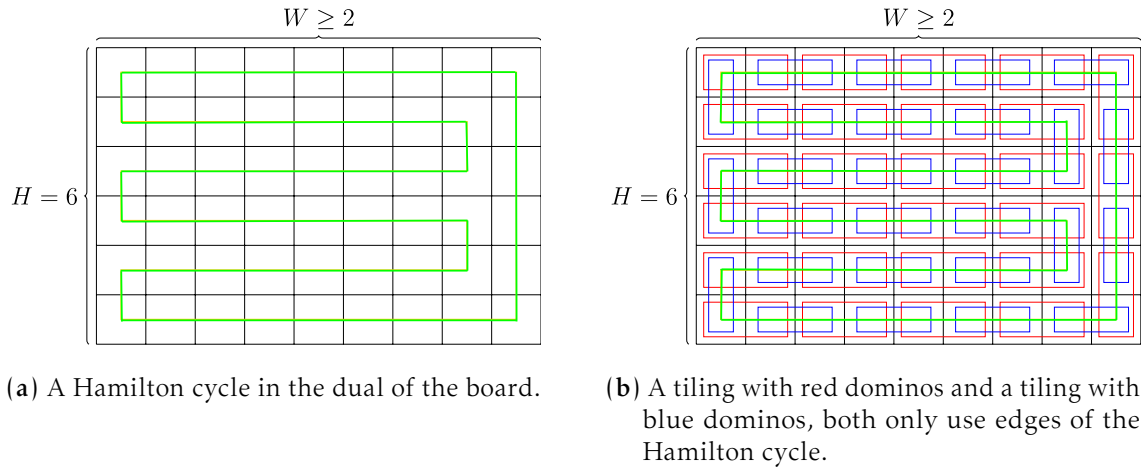


Figure 16.3: A Hamilton cycle and its two tilings for a $(H \times W)$ -board.

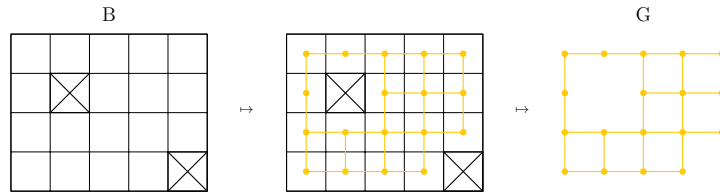


Figure 16.4: An example showing the dual graph G of a region B .

the corresponding cells are adjacent. Then this dual graph contains a *Hamilton cycle*, which is a cycle visiting all the cells exactly once, see the left hand side of [Figure 16.3](#).

Now we have two possible tilings along this cycle, where the second can be obtained from the first by simply shifting all the dominoes by one cell, see the right hand side of [Figure 16.3](#).

If we delete a black and a white cell on the board, we split the Hamilton cycle into at most two paths. Each path can be tiled with one of the two tilings: for when we deleted a white cell we can take the tiling that starts after it on the black cell and thus this one must end in a white cell which implies that it does end before the other deleted black cell and thus is a valid tiling of the path. The other case is similar. \square

We show next, that for every board consisting of unit squares it is efficiently decidable whether there is a domino tiling or not.

Theorem 16.3. *Let B be any board consisting only of unit squares. Then it can be decided in polynomial time (in the input) whether there is a domino-tiling of B .*

Proof. Given a board B we look at the respective dual graph G , see [Figure 16.4](#) for an example. Then a tiling of B corresponds to a perfect matching in G , since no two tiles overlap and each tile connects two cells, i.e. is an edge in G . It is known that the existence of a perfect matching can be decided in polynomial time. In the given case G

is bipartite, hence, we are interested in perfect matchings of bipartite graphs. This is an easy special case of the matching problem. \square

16.2 Criteria for tilings

In this section we will see some examples of boards and tiles where no tiling exists and discuss criteria for tileability. We start with an example that leads us to the so-called *Hall condition* on domino tilings.

Example 27. We give a board that cannot be tiled with domino tiles. The circled area gives a subboard forcing a certain tiling pattern which however cannot lead to a tiling of the board. That is any tiling that covers the cell (3,5) marked in orange, must cover the black cell (3,4). But then the cells (1,3) and (2,4) must be covered by dominos which both also use (2,3). This is impossible.

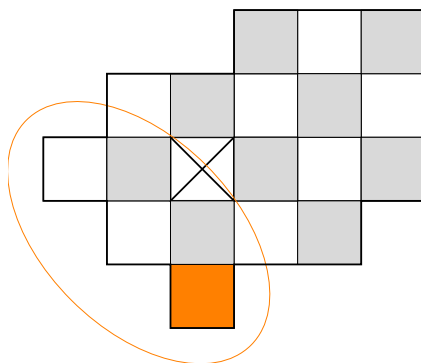


Figure 16.5: The mentioned graph that is not tileable, where the problematic zone has been circled and the square (3,5) has been marked in orange.

The board given in [Example 27](#) violates the *Hall condition* which is necessary for the existence of a domino tiling.

Theorem 16.4 (Hall). *Let $G = (X, Y; E)$ be a bipartite graph with $|X| \leq |Y|$ then there is a matching covering all of X if and only if for every $S \subset X$ it holds that $|N(S)| \geq |S|$, where $N(S)$ denotes the neighbourhood of S .*

Remark. To see that the Hall condition cannot be violated by a domino tiling recall that a domino tiling is equivalent to a perfect matching in the dual graph.

Let us now look at another sort of tiles, namely *V-tiles*, as given in figure [Figure 16.6](#).

Proposition 16.5. *A $(2^n \times 2^n)$ -board cannot be tiled using *V-tiles*.*

This is a direct consequence of the following observation that will be one of our criteria to check tileability.

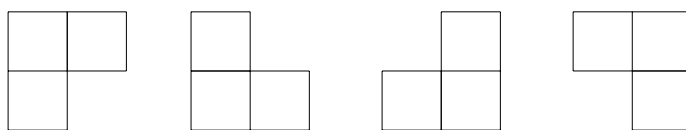


Figure 16.6: The V -tile in its four orientations.

Observation (Criterion 1). Given a region R (in unit squares) and a single type of tile T , then for R to be tileable with T we need that *the size of T is a divisor of the size of R* . This is obvious, since once we have a tiling for R we have used some number $m \in \mathbb{N}$ of tiles T of size $k \in \mathbb{N}$ to completely cover the region R without overlapping tiles. Thus the size of the region must be $k \cdot m$.

Proof of Proposition 16.5. The $(2^n \times 2^n)$ -board has size 4^n which is not divisible by 3, the size of the V -shaped tiles. \square

However, when removing a single cell from the board, it becomes tileable.

Theorem 16.6. *A $(2^n \times 2^n)$ -board where a single cell has been deleted, can be tiled using V -shaped tiles.*

Proof. We prove this by induction. For $n = 1$ the statement is clear as the remaining board can be covered using a single V -tile.

Assume the theorem to hold for $(2^n \times 2^n)$ -boards. Next we look at a $(2^{n+1} \times 2^{n+1})$ -board with a single cell deleted. First split the board into 4 quadrants with width and height 2^n (see Figure 16.7). Then the deleted cell must be from one of the four

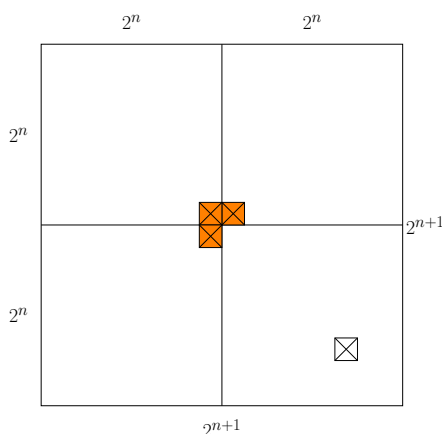


Figure 16.7: A $(2^{n+1} \times 2^{n+1})$ -board that has been split into four quadrants of size $(2^n \times 2^n)$ missing one cell in the lower right quadrant. The three cells around C forming a V -shape highlighted in orange have been removed for the induction step.

quadrants, without loss of generality assume that it is the bottom right quadrant. The center where the four quadrants touch is denoted by C . Now delete the tile that is adjacent to C from each of the other three quadrants, so that on the whole board we get a V -shaped hole around C , see Figure 16.7. Now the four quadrants of the board

are $(2^n \times 2^n)$ -boards each missing exactly one cell, and thus they can be tiled using the induction hypothesis. Finally, since the three deleted cells around C have a V -shape, we can fill this with a single V -tile to obtain a tiling of the $(2^{n+1} \times 2^{n+1})$ -board with one cell deleted. \square

With criterion 1 we directly get the following corollary.

Corollary 16.7. *Let $n \in \mathbb{N}$ be arbitrary, then $(4^n - 1)$ is divisible by 3.*

Our next criterion is based on colorings.

Observation (Criterion 2). Given a region R that is a subset of the infinite grid and a coloring of the infinite grid (for example an extension of the chessboard coloring), we can look at the induced coloring of R . Given a single tile T , it is also a subset of the infinite grid with an induced coloring. Now if R can be tiled using tiles of T , then the number of cells of R of every single color must match the number of cells of that color used by the tiles of T . For example, if some linear equation or inequality holds for the number of cells of different colors for every tile in T , then this relation holds for R as well.

This criterion is most easily understood using examples.

Example 28 (Using criterion 2 with dominoes). Given a (4×4) -board where two opposite corners – which have to be of the same color, say white – are deleted, we have 8 black and 6 white cells left.

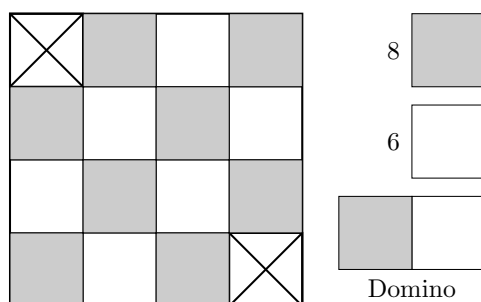


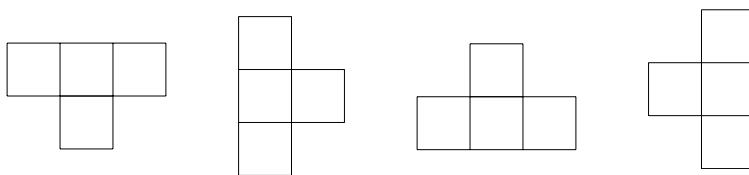
Figure 16.8: A (4×4) -board without the two opposite white corners

Any domino tile covers exactly one black and one white cell, thus if we could tile the board using dominoes, it must have the same number of black and white cells, which is not the case. This means we cannot tile this board using dominoes.

Example 29 (Using Criterion 2 with t -shaped tiles). We are given a (10×10) -board and want to tile it using only T -shaped tiles, see [Figure 16.9](#).

By Criterion 1 we need 25 of these. Each t -shaped tile covers either 3 white and 1 black cell or 3 black and 1 white cell. Suppose we use a tiles of the first type and b of the second type for a tiling, then the following two linear equations for a and b must be valid:

$$\begin{aligned} a + b &= 25 \\ 3a + b &= 50, \end{aligned}$$

Figure 16.9: The orientations of the T -tile

where $3a + b = 50$ comes from counting the number of covered white tiles. These two equations lead to $2a = 25$ which is an obvious contradiction to a being an integer. We conclude that the (10×10) -board admits no tiling with T -tiles.

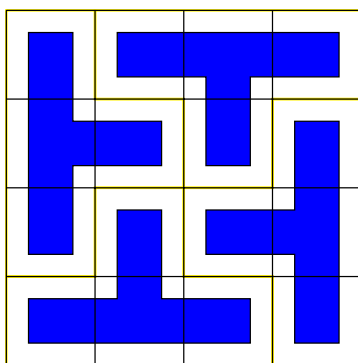
We ask next: *When can we tile a square board using T -tiles?*

Proposition 16.8. *An $(n \times n)$ -board is tileable with T -shaped tiles if and only if 4 divides n .*

Proof. Let a and b as before, i.e., we assume a tiling exists which uses a tiles which cover 3 white and 1 black cell and b tiles which cover 3 black and 1 white cell.

If n is odd, then $n^2 \in 2\mathbb{N} + 1$ and since T -tiles have size 4 there is no tiling by Criterion 1.

If $n = 2m$ for odd m the board has size $4m^2$ and we get $a + b = m^2$. By looking at the white cells: $3a + b = 2m^2$. These two equations lead to $2a = m^2$ which is a contradiction since m^2 is an odd integer. (Note that a special case of this argument was used in the previous example).

Figure 16.10: Tiling a (4×4) -board with T -tiles.

If $n = 4m$ then we are given a $(4m \times 4m)$ -board, that is m^2 copies of a (4×4) -board. The (4×4) -board admits a tiling with T -tiles, see Figure 16.10. We can use m^2 copies of this tiling to tile the $(n \times n)$ -board with T -tiles. \square

Next we look at tilings with 4-sticks, that is the tiles have shape 1×4 or 4×1 . We will refer to 4-sticks using the letter S .

Example 30 (Combining the criteria for S -tiles). We show that the (10×10) -board admits no tiling with S tiles. To see this take the first row and color every 4-th cell red, that is the cells $(1, 4), (1, 8)$. The red cells in the second row are $(2, 3), (2, 7)$. The

red cells in the third row are $(3,2), (3,6), (3,10)$. Continuing that way the red cells form diagonals on the board such that horizontally and vertically there is exactly three non-red cells between two red cells, see Figure 16.11.

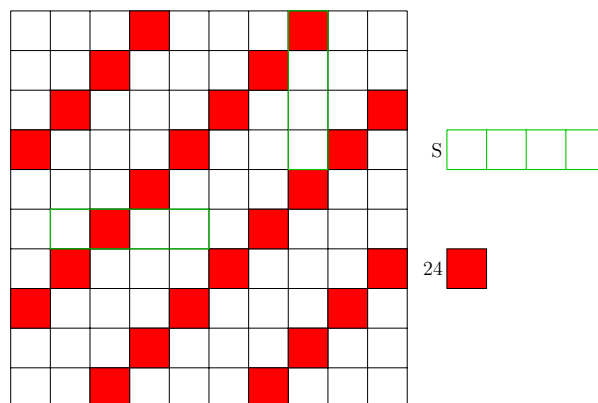


Figure 16.11: A (10×10) -board with red diagonals and an S -tile.

When tiling the board with S -tiles, every tile covers exactly one red cell: it cannot cover two since horizontally and vertically they are 4 cells apart from each other, and it must cover at least one since there are at most three consecutive non-red cells on the board. Counting the red cells on the board, we see that we have 24 red cells thus we can use at most 24 S -tiles. By criterion 1 however, given a board of size 100, we need 25 tiles thus proving that we cannot tile the board using S -tiles.

Remark. A $(n \times n)$ -board admits a tiling with S -tiles if and only if 4 divides n . The proof is similar to the proof of Proposition 16.8 and generalizes the previous example for the case of $n \equiv 2 \pmod{4}$.

The rest of this lecture (the following subsection) is devoted to establishing *Criterion 3*:

Observation (Criterion 3). Let R be a region and T be a tile. Denote by \mathcal{A} the free abelian group over the infinite board generated by its cells, and denote by \mathcal{T} the characteristic elements of all placements of tiles T , and by $\langle \mathcal{T} \rangle \subseteq \mathcal{A}$ the subgroup generated by \mathcal{T} . Then if R has a tiling with T tiles, we have that the characteristic element for R is contained in $\langle \mathcal{T} \rangle$.

Don't panic just yet, the statement will (hopefully) make sense after a few pages.

16.3 A homology criterion for the existence of tilings

First, we define the object of study, an infinite group which contains all possible boards and tiles.

Definition 16.9 (Free abelian group over the infinite board). A free abelian group given

by some set of generators S is the group of formal sums

$$\left\{ \sum_{s \in I} a_s s \mid a_s \in \mathbb{Z}, I \subset S \text{ finite} \right\}$$

with the componentwise sum. We denote by \mathcal{A} the free abelian group with generators $\{e_{i,j} \mid i, j \in \mathbb{Z}\}$.

We can imagine $\mathbb{Z}^2 \equiv \{e_{i,j} \mid i, j \in \mathbb{Z}\}$ as the set of cells of the infinite board B_∞ where we mark some cell as the 0-cell which corresponds to $e_{0,0}$. These single cells of B_∞ are the generators of \mathcal{A} , that is any element $a \in \mathcal{A}$ can be written as

$$a = \sum_{k=1}^n a_k \cdot e_{i_k, j_k}, \quad n \in \mathbb{N}, a_i \in \mathbb{Z}, \{e_{i_k, j_k} : k = 1, \dots, n\} \text{ a subset of the cells.}$$

Now \mathcal{A} is indeed a group, where addition works componentwise, that is given two elements, say $a = 2e_{1,1} + (-1)e_{7,8} + 7e_{2,2}$ and $b = 3e_{1,1} + (-2)e_{1,2} + e_{7,8} + (-3)e_{2,2}$ we get

$$a + b = 5e_{1,1} + (-2)e_{1,2} + 4e_{2,2}.$$

The neutral element is zero. Inverse elements of generators are their negatives, i.e., $e_{i,j}^{-1} = (-1)e_{i,j}$. The group is *abelian* because the ring of coefficients (\mathbb{Z}) is abelian.

Elements of \mathcal{A} can be visualized as shown in Figure 16.12, as an infinite board where the multiplicity a_k of e_{i_k, j_k} is written in the respective cell.

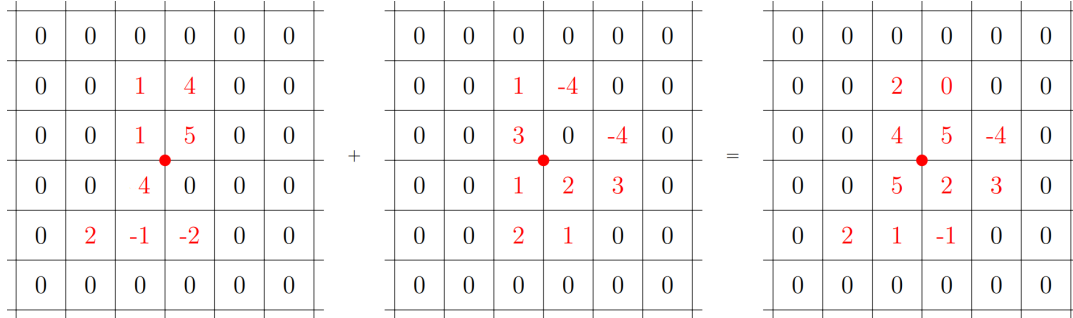


Figure 16.12: Two elements of \mathcal{A} as well as their sum are represented on the grid, where $e_{0,0}$ is the cell whose lower left corner is marked with a red dot. The sum is $2e_{-1,1} + 4e_{-1,0} + 5e_{0,0} - 4e_{1,0} + 5e_{-1,-1} + 2e_{0,-1} + 3e_{1,-1} + 2e_{-2,-1} + e_{-1,-2} - e_{0,-2}$

Having understood the group \mathcal{A} , the free abelian group over B_∞ , we can define *characteristic elements*.

Definition 16.10 (Characteristic element). Let R be a region of B_∞ , that is a selection of cells of B_∞ and let $R_C := \{e_{i,j} \mid R \text{ covers } e_{i,j}\}$ be the cells contained in R . Then the characteristic element for R is given by $\chi_R := \sum_{e \in R_C} 1 \cdot e$.

Remark. The characteristic element χ_R can be visualized having a 1 in every cell covered by R and a 0 in every other cell. If it does not cause confusion we will (somewhat ambiguously) write R for the characteristic element of R .

Tile placements of a tile T can have characteristic elements as well: After placing a tile, that tile covers a region R on B_∞ . So for a tile we get infinitely many possible placements, which we collect in a set of characteristic elements called \mathcal{T} .

Example 31. For the domino tile D , the set \mathcal{D} of possible placements of D consists of all possible elements of the form $e_{i,j} + e_{i+1,j}$ and $e_{i,j} + e_{i,j+1}$ for $i, j \in \mathbb{Z}$.

Given the set of characteristic elements \mathcal{T} we define the last missing piece for Criterion 3:

Definition 16.11. Let T be a tile and \mathcal{T} the corresponding set of characteristic elements of all tile placements. Then we write $\langle \mathcal{T} \rangle \subset \mathcal{A}$ for the subgroup generated by \mathcal{T} .

Remark. Elements of $\langle \mathcal{T} \rangle$ are of the form $\sum_{i=1}^n a_i \cdot T_i$ where $T_i \in \mathcal{T}$ and $a_i \in \mathbb{Z}$.

We continue by giving some example regions in $\langle \mathcal{D} \rangle$ in the case of domino tiles.

Example 32. Let $\langle \mathcal{D} \rangle$ be the subgroup generated by domino placements on B_∞ . **Figure 16.13** shows two elements of $\langle \mathcal{D} \rangle$ and indicates how they are obtained from generators, i.e., from weighted domino placements.

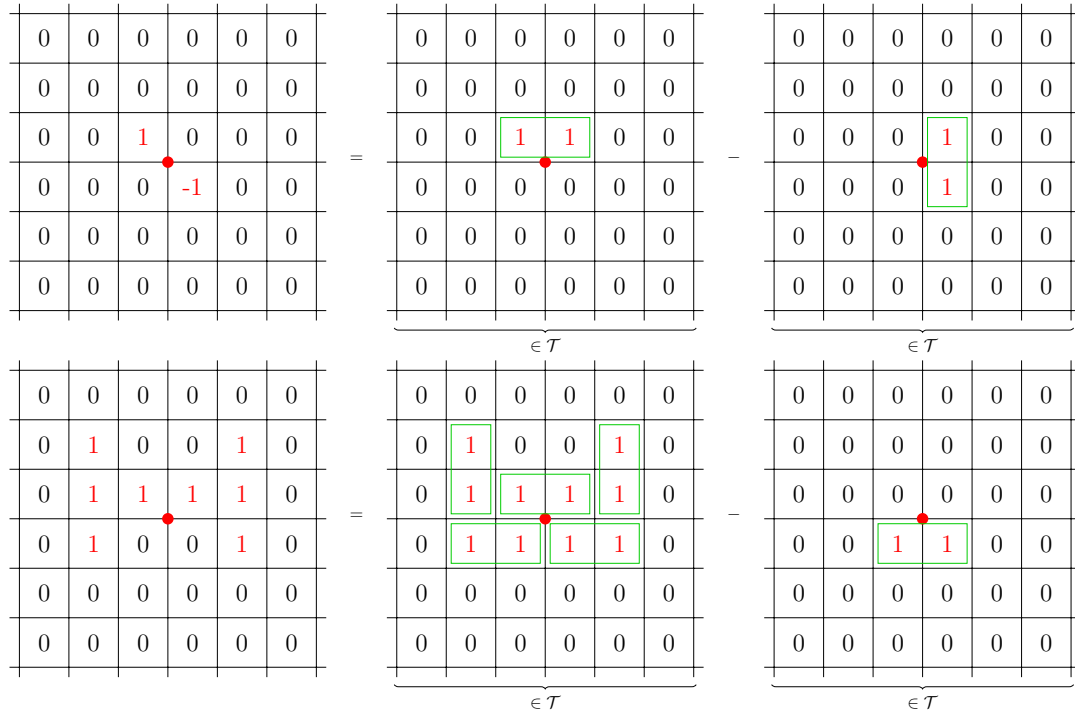


Figure 16.13: Examples of elements in $\langle \mathcal{D} \rangle$ we get by subtracting one characteristic element, i.e. domino placement (highlighted in green) from another.

Remark. Given some $A \in \mathcal{A}$ we can place tiles T on the board in order to reduce its *support*, that is, the set of cells with a non-zero value: Let $e_{i,j} \in \mathcal{A}$ be the cell such that $\max(|i|, |j|)$ is maximal, then after several tile placements this maximum is reduced, thus the cells in the resulting formal sum are closer to the origin O . Formally this means, we can add elements of \mathcal{T} – characteristic elements of placements – to the formal sum A in order to decrease the support, as you can see in Figure 16.14.

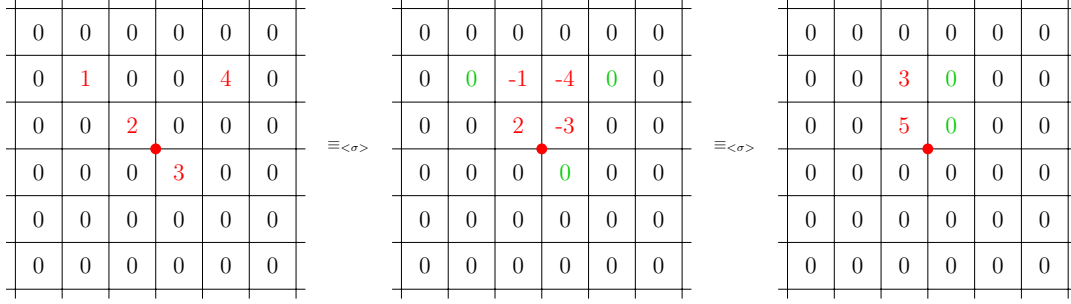


Figure 16.14: A $\langle \mathcal{T} \rangle$ -equivalence chain of elements in \mathcal{A} with shrinking support, where new zeroes are marked in green.

With the domino tile, you can reduce the support to just one cell:

Proposition 16.12. *Let $A \in \mathcal{A}$ and let \mathcal{D} be the subgroup generated by the domino tile placements. Then there exists $r \in \mathbb{Z}$ such that*

$$A \equiv r \cdot e_{0,0} \pmod{\langle \mathcal{D} \rangle},$$

From the proposition we get a criterion for $A \in \langle \mathcal{D} \rangle$:

$$r = 0 \implies A \equiv 0 \pmod{\langle \mathcal{D} \rangle} \iff A \in \langle \mathcal{D} \rangle$$

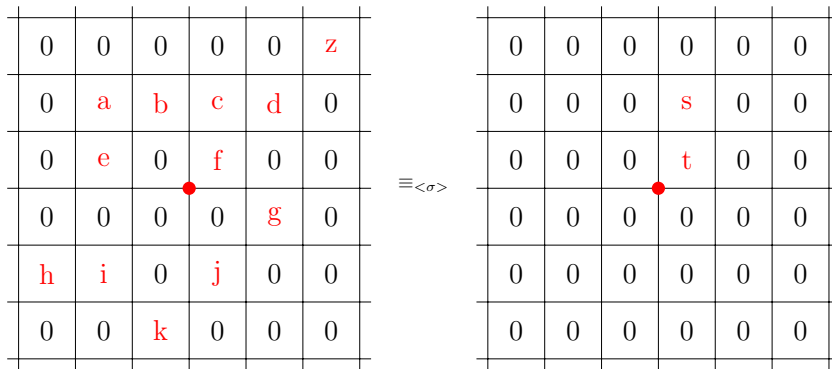


Figure 16.15: An element of \mathcal{A} brought to almost normal form via $\langle \mathcal{D} \rangle$ -equivalences. With just one additional step we reduce it to $(t - s)e_{0,0}$.

We claim that the first implication is indeed an equivalence, i.e., if $A \equiv r' \cdot e_{0,0} \pmod{\langle \mathcal{D} \rangle}$, then $A \in \langle \mathcal{D} \rangle \iff r' = 0$. We have already seen " \Leftarrow ". Given A we define

$s(A) = \sum_{(i,j) \text{ white}} a_{ij} - \sum_{(i,j) \text{ black}} a_{ij}$. Since every domino placement covers a white and a black cell we get that $A \equiv B \pmod{\langle D \rangle}$ implies $s(A) = s(B)$. In particular (assuming that $e_{0,0}$ is a white cell) we find that $r' = s(A)$.

Remark. With regard to tilings we get a *necessary* condition. If R admits a tiling with tiles from T then $R \equiv 0 \pmod{\langle T \rangle}$.

This condition is not incorporating the disjointness of tiles in a tiling and can thus not be expected to be sufficient. In fact the element of \mathcal{A} shown on the lower left of [Figure 16.13](#) is the characteristic element H of an H shaped region. As shown in the figure H belongs to $\langle D \rangle$ but clearly, the region admits no domino tiling.

In the case of dominos the new necessary condition is not stronger than Criterion 2 (coloring). In fact $s(R) = 0$ if and only if R has as many white as black cells.

Proposition 16.13. *Let \mathcal{A} the free abelian group over the infinite board and let $\langle D \rangle$ be the subgroup generated by domino placements, then*

$$\mathcal{A} / \langle D \rangle \cong \mathbb{Z}.$$

The set $\mathcal{A} / \langle T \rangle$ is of special interest and thus gets its own name, whose definition marks the end of this lecture.

Definition 16.14 (Homology group of T). Given a set T of tiles and let $\langle T \rangle$ be the subgroup of \mathcal{A} generated by placements of tiles. The quotient group

$$H(T) := \mathcal{A} / \langle T \rangle$$

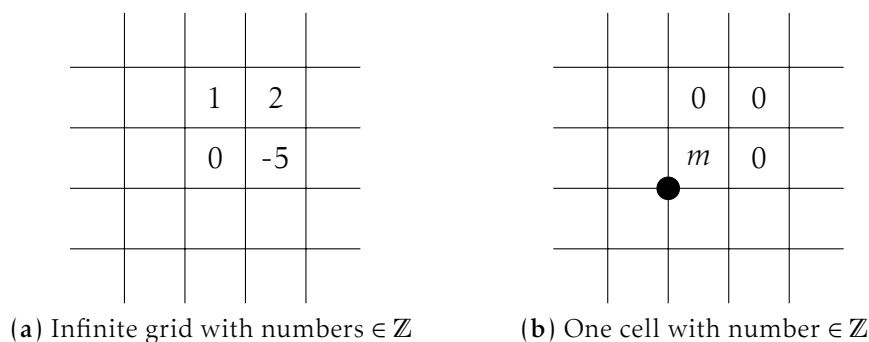
is called the *homology group of T* .

Remark. Criterion 3 reduces to checking whether a region R is the 0-element in the homology group $H(T)$.

In the next lecture we will see cases where the homology criterion provides non-tileability results which could not be obtained with counting or coloring arguments.

Homology and the Aztec Diamond

In the last lecture we saw that the homology group of dominoes on the grid is isomorphic to \mathbb{Z} . Technically: if we have an infinite grid with integers in a finite number of cells, we can reduce it by some rules, depending on the tile, in this case the dominoes, to a smaller grid (the other fields of the grid are 0), in this case only one cell with a number $\in \mathbb{Z}$. To standardize the placement of the small grid we have added an origin in the second image.



In the case of the dominoes, we know from the proof of the last lecture that for any region (even with holes), if we colour the grid like a chessboard, m is the number of white cells minus the number of black cells.

17.1 Tilings with L shapes

Let us have a look at a second example of a homology group related to tilings using a certain single tile:

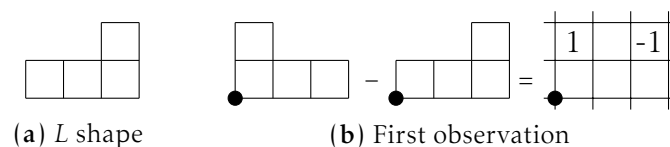


Figure 17.1: A first observation about the L shape

Example 33. Consider the case of tilings where the tiles are all rotations and reflections of an L shape, a tetromino with three cells in a straight line and one in a right angle to the other three (see [Figure 17.1a](#)). What is the homology group of these tiles? A first observation (illustrated in [Figure 17.1b](#)) can be used to prove the following proposition:

Proposition 17.1. Every $A \in \mathcal{A}$ is congruent to some element of type:

$$\begin{array}{|c|c|} \hline a & b \\ \hline c & d \\ \hline \bullet & \\ \hline \end{array}$$

Proof. If we have an s somewhere in the grid, then we can move it two steps into any direction by the observation in [Figure 17.1b](#). Thus we can move it to this small grid as illustrated in [Figure 17.2](#). \square

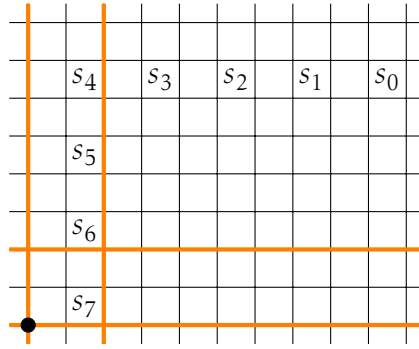


Figure 17.2: Path to move element s into the 2×2 -Box, s_i is the position of s in the i -th step.

With the observation we also know, that

$$\begin{array}{|c|c|c|} \hline 1 & & \\ \hline 1 & 1 & 1 \\ \hline \end{array} \equiv 0 \quad \Rightarrow \quad \begin{array}{|c|c|} \hline 1 & \\ \hline 2 & 1 \\ \hline \end{array} \equiv 0$$

With all rotations and reflections, we get:

$$V := \begin{array}{|c|c|} \hline 1 & \\ \hline 2 & 1 \\ \hline \end{array} \quad W := \begin{array}{|c|c|} \hline & 1 \\ \hline 1 & 2 \\ \hline \end{array} \quad X := \begin{array}{|c|c|} \hline 2 & 1 \\ \hline 1 & \\ \hline \end{array} \quad Y := \begin{array}{|c|c|} \hline 1 & 2 \\ \hline & 1 \\ \hline \end{array}$$

So $V \equiv W \equiv X \equiv Y \equiv 0$, and one can also see, that $Y = W + X - V$. It is easy to see using the observation in [Figure 17.1b](#) that no matter where the L shape lies, it can be shifted to the small 2×2 grid, and then it is congruent to V , W , X or Y .

Proposition 17.2. For all $A \in \mathcal{A}$ there exists an $s \in \mathbb{Z}$ and $t \in \{0, 1, 2, 3\}$ such that

$$A \equiv \begin{array}{|c|c|} \hline 0 & 0 \\ \hline s & t \\ \hline \bullet & \\ \hline \end{array}$$

Proof. Observe that

$$A \equiv \begin{array}{|c|c|} \hline a & b \\ \hline c & d \\ \hline \end{array} - aV - bW = \begin{array}{|c|c|} \hline 0 & 0 \\ \hline s' & t' \\ \hline \end{array} \quad \text{and} \quad 2V + W - X = \begin{array}{|c|c|} \hline 0 & 0 \\ \hline 4 & 4 \\ \hline \end{array}$$

and so it holds:

$$A \equiv \begin{array}{|c|c|} \hline 0 & 0 \\ \hline s' & t' \\ \hline \end{array} \equiv \begin{array}{|c|c|} \hline 0 & 0 \\ \hline s' & t' \\ \hline \end{array} - \left\lfloor \frac{t'}{4} \right\rfloor \begin{array}{|c|c|} \hline 0 & 0 \\ \hline 4 & 4 \\ \hline \end{array} \equiv \begin{array}{|c|c|} \hline 0 & 0 \\ \hline s & t \\ \hline \end{array}$$

with $s \in \mathbb{Z}$ and $t \in \{0, 1, 2, 3\}$, and so we have shown that the homology group is isomorphic to a subgroup of $\mathbb{Z} \times \mathbb{Z}_4$. \square

Theorem 17.3.

$$H(\mathcal{L}) \cong \mathbb{Z} \times \mathbb{Z}_4$$

Proof. We have to show, that for $s \in \mathbb{Z}$ and $t \in \{0, 1, 2, 3\}$ it holds that

$$\begin{array}{|c|c|} \hline s & t \\ \hline \end{array} \equiv \begin{array}{|c|c|} \hline 0 & 0 \\ \hline \end{array} \pmod{\langle \mathcal{L} \rangle} \iff s = t = 0$$

" \Leftarrow " is clear.

" \Rightarrow ": Let $\begin{array}{|c|c|} \hline s & t \\ \hline \end{array} \in \langle \mathcal{L} \rangle$. Then there exists a family of L shapes placed in the grid whose sum is $\begin{array}{|c|c|} \hline s & t \\ \hline \end{array}$. Each of these L shapes is congruent to one of V , W , X , or Y , where $Y = X + W - V$ which means

$$\begin{array}{|c|c|} \hline 0 & 0 \\ \hline s & t \\ \hline \end{array} = a_v V + a_w W + a_x X$$

This yields the following equation system:

$$\begin{array}{ll} \text{(left top)} & 2a_x + a_v = 0 \end{array} \tag{17.21}$$

$$\begin{array}{ll} \text{(right top)} & a_x + a_w = 0 \end{array} \tag{17.22}$$

$$\begin{array}{ll} \text{(right bottom)} & 2a_w + a_v = t \end{array} \tag{17.23}$$

$$\begin{array}{ll} \text{(left bottom)} & 2a_v + a_x + a_w = s \end{array} \tag{17.24}$$

$$\begin{array}{ll} (17.21) - 2(17.22) & a_v - 2a_w = 0 \end{array} \tag{17.25}$$

$$(17.23) - (17.25) \quad 4a_w = t \quad \Rightarrow 4|t \Rightarrow t = 0$$

$$(17.24) - (17.22) - 2(17.25) \quad 4a_w = s \quad \Rightarrow s = t = 0$$

\square

17.2 The power of homology

As we have seen in the previous lecture (Figure 16.13), there are regions congruent to zero in the homology group, that are not tileable by the corresponding tiles. In this section we will see another family of such regions, this time untileable by Z tiles (see Figure 17.3):

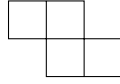


Figure 17.3: The Z tile

Definition 17.4. The Aztec Diamond $A(k)$ of size k is the region of cells having a corner at most $k - 1$ horizontal and/or vertical steps away from the origin.

Observation. The Aztec Diamond $A(k)$ covers $\binom{k+1}{2}$ cells in each quadrant, that is $2k(k + 1)$ cells in total.

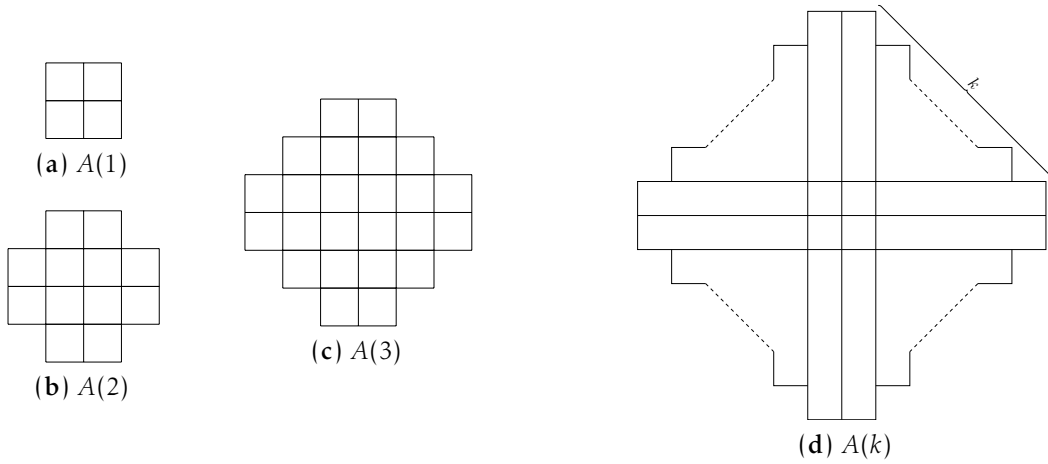
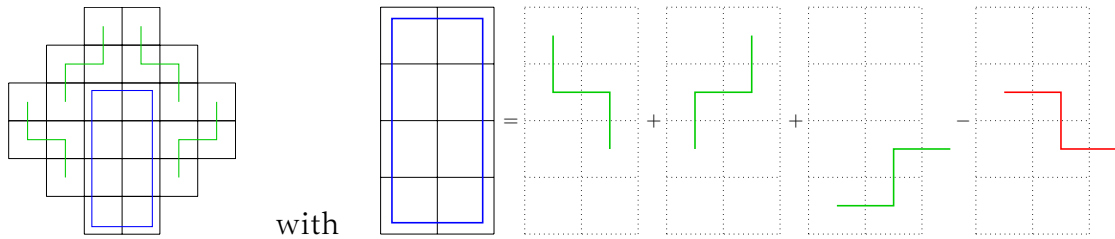


Figure 17.4: Aztec Diamonds of size 1, 2 and 3 and a schematic drawing of an Aztec Diamond of size k

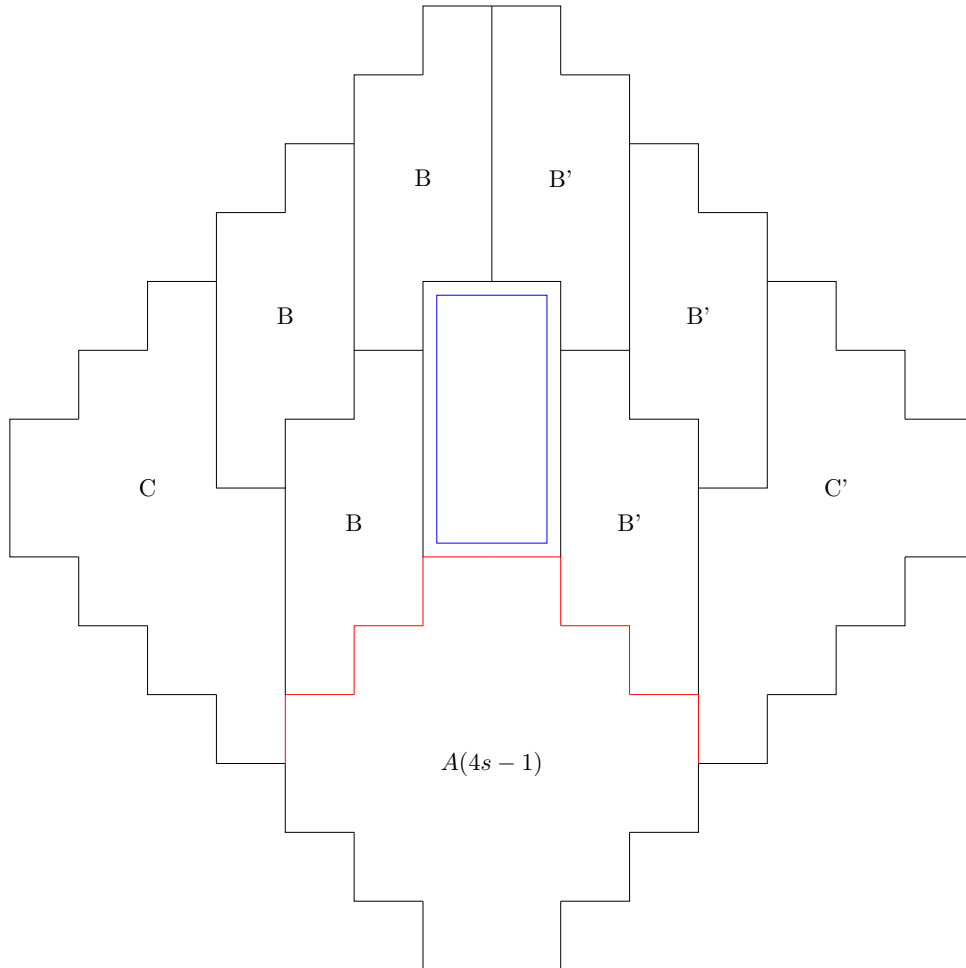
For an illustration of the Aztec Diamonds, see Figure 17.4 We will now state a theorem and try to prove as much of it as possible using homology.

Theorem 17.5. For all $k \in \mathbb{N}$ there is no tiling of $A(k)$ by Z tiles.

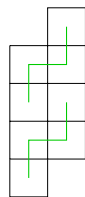
At first we look at $k = 3$ and see that $A(3) \equiv 0 \pmod{\langle Z \rangle}$, because we have



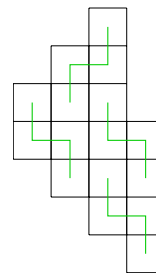
Starting from this example we can extend the construction to go from the Aztec Diamond of size $4s + 3$ to size $4(s + 1) + 3$ for all $s \in \mathbb{N}$ as illustrated in Figure 17.5 and from the Aztec Diamond of size $2n + 1$ to size $2(n + 1)$ as pictured in Figure 17.6. Together this implies that $A(k) \equiv 0 \pmod{\langle Z \rangle}$ for all $k \equiv 0, 3 \pmod{4}$. Hence, the cases $k \equiv 0, 3 \pmod{4}$ of Theorem 17.5 are not provable via homology.



(a) A schematic expansion from an Aztec Diamond of size $4s - 1$ to size $4s + 3$



(b) Tiling of a B-region



(c) Tiling of a C-region

Figure 17.5: Scheme of expanding an Aztec Diamond of size $4s - 1$ to size $4s + 3$ using a single tiling of a C-region, $4s - 1$ tilings of B-regions, and their mirror images B' and C'

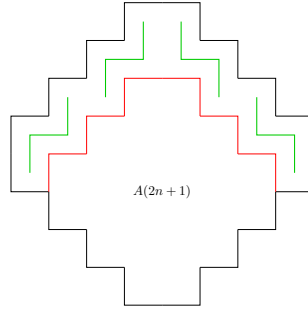


Figure 17.6: Scheme of expanding an Aztec Diamond of size $2n+1$ to size $2(n+1)$

With the following proposition we show that the remaining cases of the theorem can, in contrast, even be proven with a coloring argument.

Proposition 17.6. $A(k)$ has no tiling with Z tiles for $k \equiv 1, 2 \pmod{4}$.

Proof. We color the 4 center squares and then every other 2×2 -block green in a chessboard manner as seen in Figure 17.7. Since $k \equiv 1, 2 \pmod{4}$, this results in all green blocks being completely inside the Aztec Diamond whereas some of the white blocks at the boundary might be partially contained.

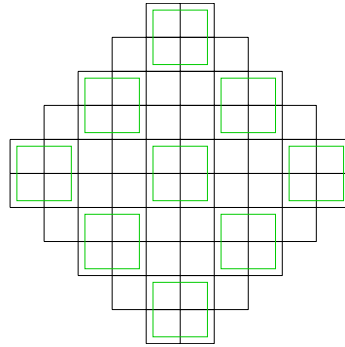


Figure 17.7: Green-white colored Aztec Diamond of size 5

Now suppose that there is a tiling. We distinguish two types of Z tiles in the tiling, one type is covering 1 white and 3 green cells and the other is covering 1 green and 3 white cells. We denote the number of Z tiles of the two types in the tiling by a and b respectively:

$$\begin{aligned}
 a + b &= \#(\text{tiles}) = \frac{\#(\text{cells of the Aztec Diamond})}{4} = \binom{k+1}{2} \\
 3a + b &= \#(\text{green cells}) \equiv 0 \pmod{4} \\
 \implies \binom{k+1}{2} &= \#(\text{green cells}) - 2a \equiv 0 \pmod{2} \\
 \implies k &\equiv 0, 3 \pmod{4} \quad \nexists
 \end{aligned}$$

□

The existence of a proof using the coloring criterion implies the existence of a proof using homology. It is a good exercise to transfer the proof to this setting.

Homotopy and Counting Tilings

In the last lectures we saw 3 criteria for untileability of regions. In this lecture we will see a 4th criterion. We then move on to tiling problems where the focus is on counting.

18.1 Homotopy

To explain the concept of homotopy we again use tiles which are unions of grid-cells. Given a tile T and a starting point s on its boundary we get a boundary word ω by walking counter-clockwise around its boundary as seen in an example in [Figure 18.1](#), where x marks a step to the right (on the x -axis) and y a step up (on the y -axis). The left and down steps are \bar{x} and \bar{y} respectively, they are the inverse elements of x and y in the (non-abelian) free group $\langle x, y \rangle$ generated by x and y .

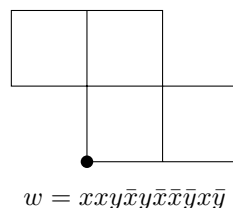


Figure 18.1: a z-shaped tile and its boundary word. The starting point is marked.

Given a point s_0 in $\mathbb{Z} \times \mathbb{Z}$ and a word α representing a $s \rightarrow s_0$ path. Then the conjugate $\alpha\omega\alpha^{-1}$ of ω is a boundary word for the tile T placed such that its starting point is at s_0 . Hence, if we want to identify all translates of a tile in a plane with fixed starting point we can consider conjugate words to be equal. This equivalence/equality will be used in the sequel.

Theorem 18.1. *Let R be a region with simple boundary (no holes) and with boundary word ω_R . If R has a tiling with translates of tiles K_1, \dots, K_r with boundary words $\omega_1, \dots, \omega_r$. Then there are conjugates $\tilde{\omega}_i$ of ω_i for $i \in [r]$ such that*

$$\omega_R = \tilde{\omega}_1 \dots \tilde{\omega}_r$$

holds in the free group $\langle x, y \rangle$ with the equivalence given by conjugation.

Proof. Recall that changing the starting point corresponds to a conjugation. Also note that if $q\omega\bar{q} = \tilde{\omega}_1 \dots \tilde{\omega}_s$, then $\omega = \bar{q}\tilde{\omega}_1q \dots \bar{q}\tilde{\omega}_sq$. Now we are ready for the inductive proof of the theorem.

Induction step: Color the tiles of the existing tiling of R with colors 1 and 2 such that the tiles of each color form a connected region and both color classes contain a part of the boundary of R . Let c be the word representing the boundary between the two regions R_1 and R_2 . Figure [Figure 18.2](#) illustrates the situation.

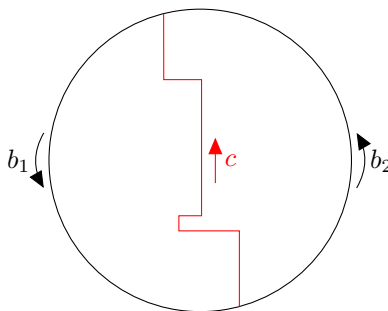


Figure 18.2: The path c splits R into two smaller regions R_1 and R_2 .

$$\begin{aligned}\omega_{R_1} &= cb_1 = \tilde{\omega}_1 \dots \tilde{\omega}_s \\ \omega_{R_2} &= b_2 \bar{c} = \tilde{\omega}_{s+1} \dots \tilde{\omega}_r\end{aligned}$$

$$\omega_{R_2} = b_2 \bar{c} = \tilde{\omega}_{s+1} \dots \tilde{\omega}_r$$


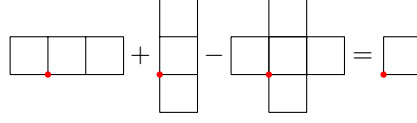
☐
$$\omega_R \neq 1_G \quad \implies \quad R \text{ has no tiling.}$$


Figure 18.3: The two tiles called triomino and cross.

126



We claim that an $n \times m$ rectangle is untileable if $3 \nmid nm$. If we can show the claim for $n \equiv m \equiv 1 \pmod{3}$, then it implies the claim for all $3 \nmid nm$: we can combine copies of an $n \times m$ rectangle to get an $n' \times m'$ rectangle with $n' \equiv m' \equiv 1 \pmod{3}$.

The idea is to use a homomorphism from $\langle x, y \rangle$ to the symmetric group S_5 . The homomorphism is defined by the images of the generators, we use $x \rightarrow (1\ 2\ 3)(4)(5)$ and $y \rightarrow (1)(2)(3\ 4\ 5)$. Then boundary words of all tiles are the identity in the subgroup G of S_5 which is the image of $\langle x, y \rangle$, see Figure 18.4. Since the images of x and y are permutations of order 3 we get $xy^3\bar{x}\bar{y}^3 = x\bar{x} = 1_G$, to verify the claim for the cross is more tedious.

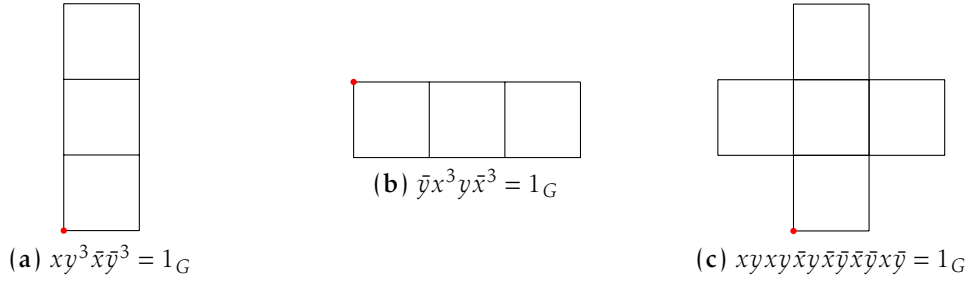


Figure 18.4: The tiles and their boundary words.

The boundary word of the $n \times m$ rectangle is not the identity, since for $n = 3k + 1$ and $m = 3l + 1$ we get

$$x^{3k+1}y^{3l+1}\bar{x}^{k+1}\bar{y}^{3l+1} = xy\bar{x}\bar{y} \neq 1_G$$

To show the power of homotopy arguments we now restate and prove Theorem 17.5:

Theorem 18.2. For all $k \in \mathbb{N}$ there is no tiling of $A(k)$ by Z s.

Proof. There are eight different placements of the tile Z with different boundary words, one of them is $\omega_{Z_1} = x^2y\bar{x}y\bar{x}^2\bar{y}x\bar{y}$, the others are obtained by exchanging $x \leftrightarrow y$ and/or $x \leftrightarrow \bar{x}$ and/or $y \leftrightarrow \bar{y}$. The boundary word of the Aztec diamond is $\omega_{A(n)} = (xy)^n(y\bar{x})^n(\bar{x}\bar{y})^n(\bar{y}x)^n$. We look at this word in a different grid $\Gamma^\#$ shown in Figure 18.5. Consider a ray with a starting point in a side a cell c which contains a point p which is moving along the boundary of a region R in counter-clockwise direction. The winding number of the region R and cell c is the number of times this ray winds around c in a counter-clockwise way minus the number of times it does so in a clockwise way. We now consider winding numbers of boundary paths with respect to all cells of the grid $\Gamma^\#$:

$$w(Z_i, c) = \begin{cases} +1 & \text{for a unique cell } c_i^1 \\ -1 & \text{for a unique cell } c_i^2 \\ 0 & \text{for all the other cells} \end{cases}, \quad w(A(n), c) = \begin{cases} \lfloor \frac{n}{2} \rfloor & \text{for the 4 cells} \\ & \text{of a } 2 \times 2 \text{ square} \\ 0 & \text{for all the other cells.} \end{cases}$$

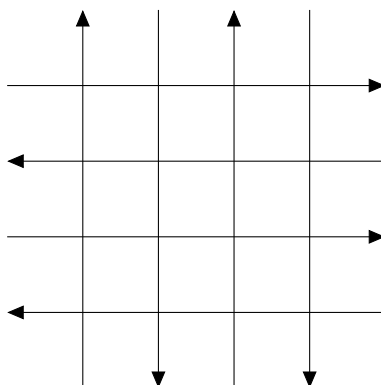


Figure 18.5: The second grid $\Gamma^\#$

Let G° be the subgroup of words in $\langle x, y \rangle$ which correspond to closed walks in $\Gamma^\#$. Note that if $\omega \in G^\circ$, then conjugates of ω also belong to G° . Now consider the map ϕ from G° to \mathbb{Z} which sends ω to the sum of winding numbers of all cells, i.e., $\phi(\omega_R) = \sum_c w(R, c)$. Note that ϕ is a homomorphism. Now $\phi(\omega_{Z_i}) = +1 - 1 = 0$ for all placements of the tile Z while $\phi(\omega_{A(n)}) = 4\lfloor \frac{n}{2} \rfloor \neq 0$. Hence $A(n)$ has no tiling with Z tiles. \square

18.2 Counting Tilings

In many cases the existence of a tiling is rather obvious, e.g., for domino tilings of a $n \times m$ board with even $n \cdot m$. In such cases it is of interest to study *how many* tilings there are. Indeed the question was investigated since the 60s by researchers in statistical physics. The following theorem is due to Elkies, Kuperberg, Larsen and Propp, 1992.

Theorem 18.3 (Aztec Diamond Theorem). $A(n)$ has $2^{\binom{n+1}{2}}$ domino tilings.

Several proofs of the theorem have been given by Elkies et al. later additional proof have been published. We will see complete proofs later but now we start with a sketch of a proof using a technique called *domino shuffling*.

Proof. We color the cells of the plane black and white in chessboard fashion. We also color points with coordinates (x, y) red if $x + y$ is even. Assuming that the cell spanned by $(0, 0)$ and $(1, 1)$ is white the *even points* at the cells are as in Figure 18.6.

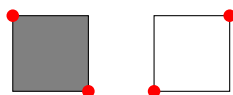


Figure 18.6: The red (even) points at a black and a white cell.

For dominos we define the shuffling directions as shown in Figure 18.7.

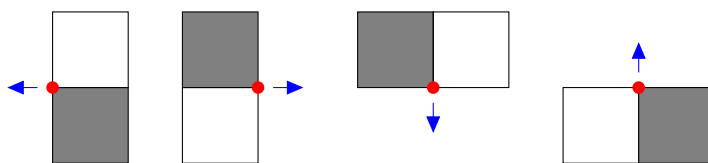


Figure 18.7: shuffling direction for each kind of domino

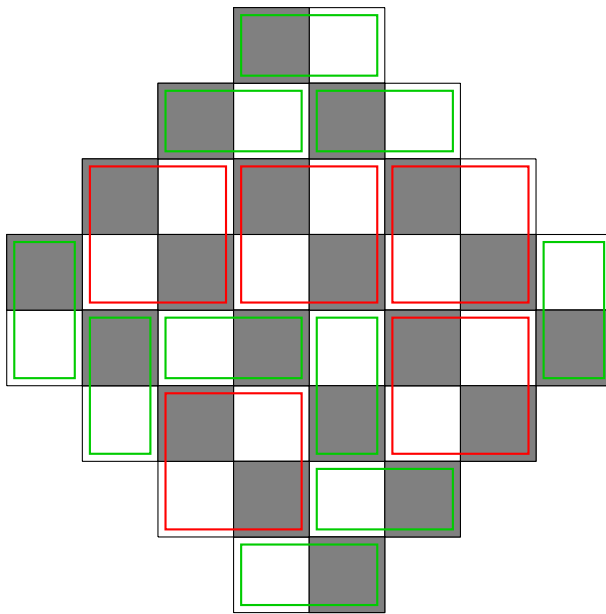


Figure 18.8: The green dominoes form a reduced partial tiling.

A *blank block/bad box/BB* is a 2×2 -block with even center. Call a partial tiling of $A(n)$ *reduced* if (1) it has no BB covered by two dominoes and (2) the free room can be tiled by BBs. Figure 18.8 shows an example of a reduced partial tiling.

Now *shuffling* means to move every domino of a reduced partial tiling one step in the shuffling direction. The following main Lemma will be partially proved later.

Lemma 18.4 (Shuffling Lemma). *Shuffling is an involution on reduced tilings of the whole plane $\mathbb{Z} \times \mathbb{Z}$.*

The lemma is crucial in the proof of the following proposition.

Proposition 18.5.

$$\# \text{ Domino tilings of } A(n) = 2^n \cdot \# \text{ Domino tilings of } A(n-1)$$

Remark. This implies the theorem because

$$\# \text{ Domino tilings of } A(n) = 2^n 2^{n-1} \dots 2^2 \#(\text{Domino tilings of } A(1)) = 2^{\binom{n+1}{2}}$$

Proof of Proposition 18.5. we extend the partial tiling of $A(n)$ to a partial tiling of $\mathbb{Z} \times \mathbb{Z}$ as seen in Figure 18.9, the extension consists of two walls in the upper and lower halfplane and a slab of height two separating them which can be covered by BBs. Apply the shuffle to each domino of this partial tiling, this yields a partial tiling of $A(n-1)$ with as many dominoes as in the preimage, the partial tiling of $A(n)$. Hence because the total area decreased by $2(n+1)n - 2n(n-1) = 4n$, the number of BBs in the area of the Aztec diamond has been reduced by n .

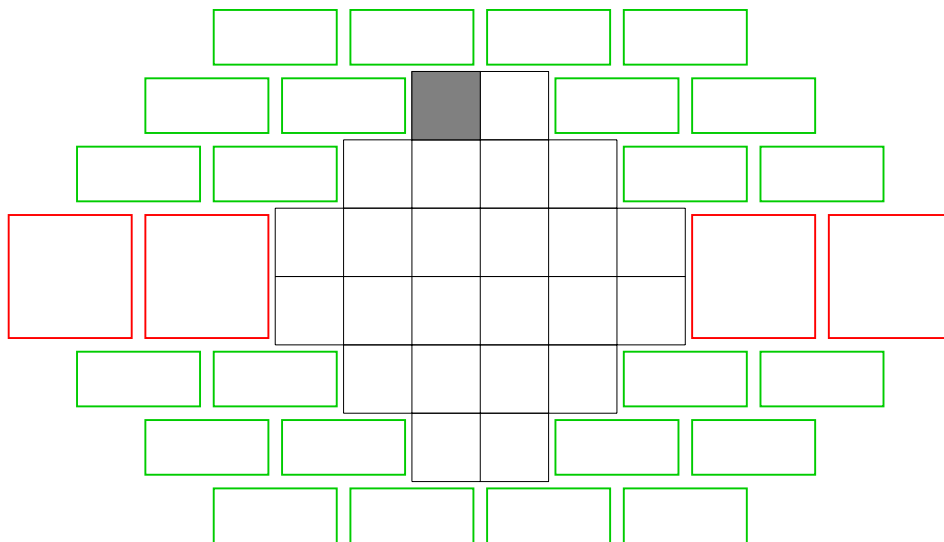


Figure 18.9: The extension of $A(3)$.

Now given a reduced tiling $T(n)$ of $A(n)$ with k BB's we can extend it to 2^k different complete tilings by filling in the BB's using the two possible orientations of the dominos filling a BB. On the other hand, from every complete tiling we can determine which reduced tiling it came from by just deleting any adjacent pair of dominos that shares an even vertex in the middle. This concludes the claim since reduced tilings in $A(n)$ are in bijection with reduced tilings in $A(n-1)$ and the shuffling reduces the number of BBs inside the Aztec diamond by n . \square

Partial proof of Lemma 18.4. Let T be a reduced partial tiling and let S be the shuffling operation. We then have to show

1. $S(T)$ is a partial tiling (no dominoes overlap)
2. $S(T)$ covers no BB with parallel dominoes
3. the free space of $S(T)$ can be covered by BBs
4. $S(S(T)) = T$

Items 1,2, and 3 imply that $S(T)$ is a reduced partial tiling, while 4 says that S is an involution. We will indicate the proofs of 1,2, and 4, the proof of 3 is more involved. We refer to M. Aigner "A course in enumeration" (pages 44–50) for a complete proof.

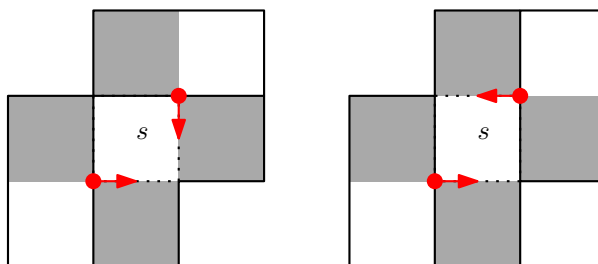


Figure 18.10: Proof of Item 1 of [Lemma 18.4](#): The domino covering s would complete a BB.

Item 4 is easy to see from the definition. Item 2 follows directly, too: Assume there is a BB covered by a pair of dominoes, then that BB was covered by a pair of dominoes in the preimage. For Item 1, suppose a cell s is covered by the shuffles of two dominoes. Then both of these dominoes share a (different) middle red vertex with s , which has two such vertices. Without loss of generality s is white (otherwise rotate the image by $\pi/2$) and the domino at the left red vertex is vertical (otherwise reflect along the line through the two red vertices). There are 2 cases left, see [Figure 18.10](#). In each of them the initial tiling cannot have been reduced. □

□

Aztec Tiling Continued

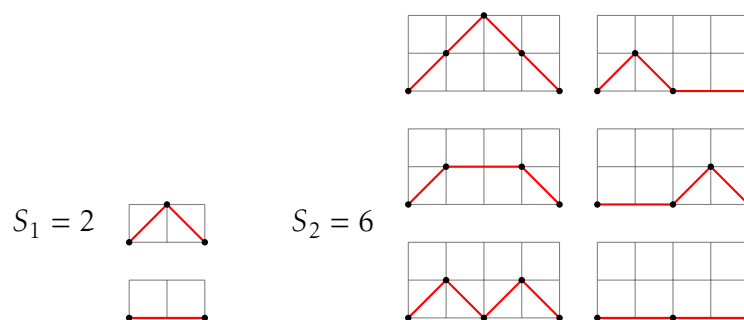
Recall the Aztec diamond Theorem ([Theorem 18.3](#)). We begin the lecture by restating it and then continue with a complete proof. For the use in the proof we will need the Lemma of Lindström-Gessel-Viennot which is an extremely nice piece of combinatorics in its own right.

Theorem 19.1 (Aztec diamond theorem). $\# \text{domino tilings of } A(n) = 2^{\binom{n+1}{2}}$

We lay the basis of our proof with something seemingly unrelated.

19.1 Schröder paths and Schröder numbers

Definition 19.2. A *Schröder path* is a path composed of steps $(1, 1)$, $(1, -1)$ and $(2, 0)$. The starting point is $(0, 0)$ and the path is confined to the upper half-plane. The *Schröder number* S_n is given by $S_n = \# \text{Schröder paths from } (0, 0) \text{ to } (2n, 0)$.



$$S_3 = 22, \quad S_4 = 90, \quad S_5 = 394, \dots$$

Proposition 19.3. The Schröder numbers S_n for $n \in \mathbb{N}$ satisfy the recursion

$$S_n = S_{n-1} + \sum_{k=0}^{n-1} S_k S_{n-k-1}$$

Proof. Given a Schröder path from $(0,0)$ to $(2n,0)$ we look at two cases, depending on whether the first step is a horizontal step $(2,0)$ or a diagonal upwards step $(1,1)$. In the first case the remaining path will be a Schröder path from $(2,0)$ to $(2n,0)$ for which there are S_{n-1} possibilities. In the second case we start with a diagonal upwards step $(1,1)$, which means we are now at height 1 on our path. The path has to go down to height 0 eventually. Look at the first point where the path is at height 0 again. This happens with a diagonal downwards step $(1,-1)$.

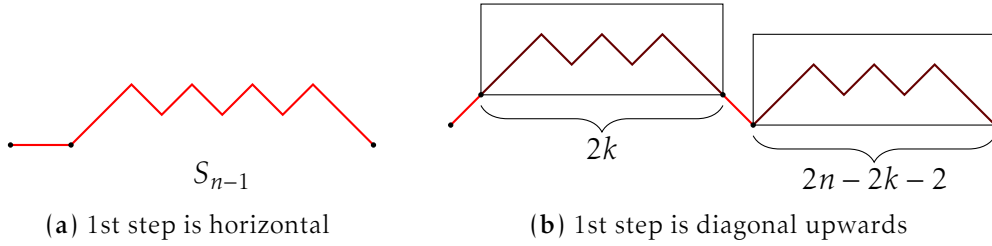


Figure 19.1: the two cases for the recursion.

As indicated in [Figure 19.1](#) we can decompose the path into two Schröder paths, one above height 1 of length $2k$ for some $k \in \{0, 1, \dots, n-1\}$ and the second which is just the original path after the zero, its length is $2n - 2k - 2$. For fixed k there are S_k possibilities for the first and S_{n-k-1} possibilities for the second part. Summing over k and adding this to the options for the first case yields the recursion. \square

A related family of paths is given by the following definition.

Definition 19.4. A *small Schröder path* is a Schröder path without horizontal steps on the x -axis. We let $\hat{s}_n = \# \text{small Schröder paths from } (0,0) \text{ to } (2n,0)$.

$$\hat{s}_1 = 1, \quad \hat{s}_2 = 3, \quad \hat{s}_3 = 11, \quad \hat{s}_4 = 45, \quad \hat{s}_5 = 197, \dots$$

Proposition 19.5. *The number of small Schröder paths is half the number of Schröder paths, i.e.*

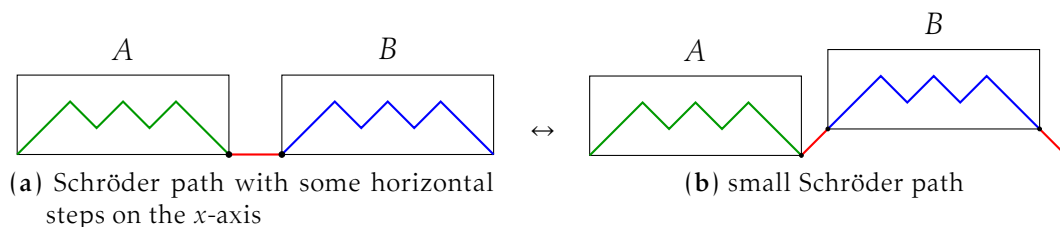
$$S_n = 2\hat{s}_n \quad \forall n > 0$$

There are several proofs of this, for example with the help of generating functions, we will give a simple bijective proof.

Proof. We will find a bijection for fixed n between Schröder paths with some horizontal steps on the x -axis and small Schröder paths. Now the first set has size $S_n - \hat{s}_n$ and the second set has size \hat{s}_n , hence, if there is such a bijection the claimed identity holds.

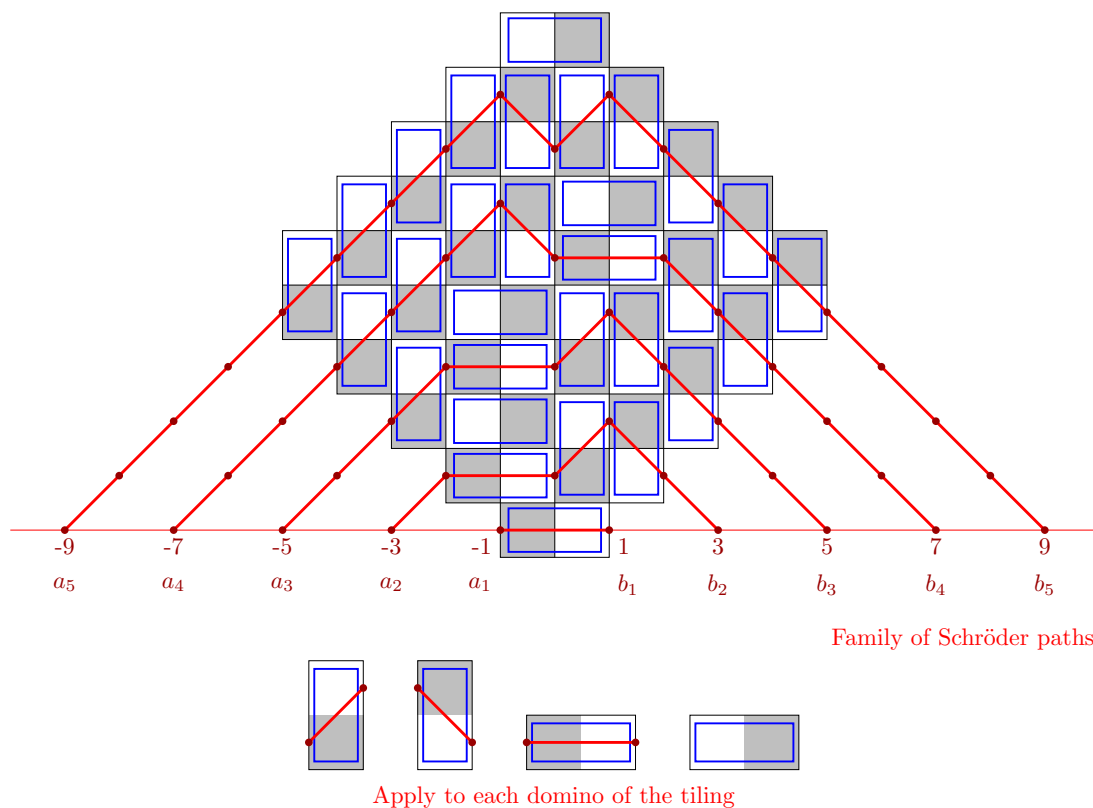
Given a Schröder path with some horizontal steps on the x -axis we look at the first horizontal step H and separate the Schröder path into paths A which is everything before H and B which is everything after H . Then A has by definition no horizontal steps on the x -axis, while B could still have some. To get a small Schröder path we take A , add a diagonal upwards step after A , put B after that step (essentially raising B

by 1), then a diagonal downwards step after B . This gives us a small Schröder paths from $(0,0)$ to $(2n,0)$, since H was deleted and replaced by a diagonal upwards and downwards step which now surround a raised B , leaving no horizontal steps on the x -axis.



On the other hand, given a small Schröder path we can go back to a Schröder path with some horizontal steps on the x -axis by looking at the last zero of the path before $(2n,0)$, which will be $(2k,0)$ for some $k \in \{0, 1, \dots, n-1\}$. Then A will be the path from $(0,0)$ to $(2k,0)$ and B the path from $(2k+1,1)$ to $(2n-1,1)$. Taking A , adding a horizontal step after, and a lowered B after that gives the intended map. Actually, the two maps are inverse to each other, so we have the claimed bijection. \square

Next we make a connection between families of non-intersecting Schröder paths and domino tilings of the aztec diamond. We claim that domino tilings of $A(n)$ are in bijection with the families of n non-intersecting Schröder paths p_1, \dots, p_n where $p_i : a_i \rightarrow b_i$ with $a_i = (-2i + 1, 0)$ and $b_i = (2i - 1, 0)$. Here is an example of a tiling of $A(5)$ illustrating the mapping.



To get from an Aztec diamond tiling to a family of non-intersecting Schröder paths we draw red segments in dominoes as shown in the figure above. Note that the paths do not end inside the tiling: every horizontal contact of two dominoes such that the left cell is white gives rise to a connection of two segments while no other contact of dominoes does. We then extend the paths diagonally down to the base line (x -axis). In a tiling of $A(n)$ we have one path entering the diamond in each of the black cells of the lower left slope and a path leaving the diamond in each white cell on the lower right slope. Therefore this gives us paths a_i to b_i for $i \in \{1, 2, \dots, n\}$. The Schröder paths will not intersect, since they don't do that while just going down outside and inside, each domino only contains a single segment.

Starting from a collection of disjoint Schröder paths, we add vertical dominoes and horizontal black-white dominoes to reflect the steps of the Schröder paths. If a horizontal contact of a left white and right black cell does not take part in any path, we cover it by a white-black horizontal domino. This completes the proof that there is a bijection $T \longleftrightarrow p_1, \dots, p_n$ as claimed.

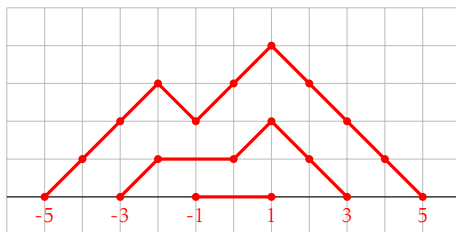
Let $FS(n) = \#$ families of non-intersecting Schröder paths (p_1, \dots, p_n) with $p_i : (a_i, 0) \rightarrow (b_i, 0)$. Then the bijection from above tells us that

$$FS(n) = \# \text{ domino tilings of } A(n).$$

Next let $\widehat{FS}(n) = \#$ families of non intersecting small Schröder paths (q_1, \dots, q_n) with $q_i : (a_i, 0) \rightarrow (b_i, 0)$.

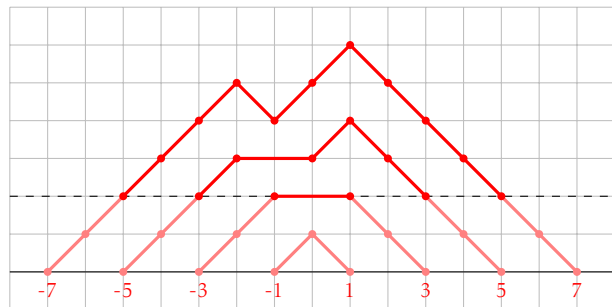
Claim: $FS(n) = \widehat{FS}(n+1)$

Proof. Given a family of non intersecting Schröder paths (p_1, \dots, p_n) we find a bijection to a non intersecting family of small Schröder paths (q_1, \dots, q_{n+1}) by first raising, and then extending the paths p_i to the paths q_{i+1} so that they no longer have a horizontal step on the x -axis. First each path p_i will be raised by 2, so it now goes from $(a_i, 2) \rightarrow$



(a) Family of 3 nonintersecting Schröder paths

\longleftrightarrow



(b) Family of 4 nonintersecting small Schröder paths

$(b_i, 2)$. Then each path will be extended diagonally to the x -axis, so two diagonal upwards steps are added before each path, and two diagonal downwards steps are added after each path. The path q_{i+1} obtained from p_i goes from $(a_i - 2, 0) \rightarrow (b_i + 2, 0)$,

which means $q_{i+1} : (a_{i+1}, 0) \rightarrow (b_{i+1})$. It remains to introduce a path q_1 which will be the path from $a_1 = -1$ to $b_1 = 1$ given by an upwards step followed by a downwards step. To get back from the family of small Schröder paths (q_1, \dots, q_{n+1}) to the paths we had before, we just delete the bottom two layers of nodes at height 0 and 1, and shift all the paths down by 2, and rename the shortened q_{i+1} to p_i . The removal of the bottom two layers also gets rid of q_1 in the process. \square

We have seen a relation between S_n and \hat{s}_n now we come to a relation between families of non-intersecting paths of Schröder and small Schröder paths. Using this we will complete the proof of [Theorem 19.1](#).

We use a result which comes from the Lemma of Lindström Gessel-Viennot, which we will be shown in the next subsection. The lemma tells us that we can express the respective numbers of families of non-intersecting path as determinants as follows:

$$FS(n) = \det \begin{pmatrix} S_1 & S_2 & S_3 & \dots & S_n \\ S_2 & S_3 & S_4 & \dots & S_{n+1} \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ S_n & S_{n+1} & S_{n+2} & \dots & S_{2n-1} \end{pmatrix} \quad \widehat{FS}(n) = \det \begin{pmatrix} \hat{s}_1 & \hat{s}_2 & \hat{s}_3 & \dots & \hat{s}_n \\ \hat{s}_2 & \hat{s}_3 & \hat{s}_4 & \dots & \hat{s}_{n+1} \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ \hat{s}_n & \hat{s}_{n+1} & \hat{s}_{n+2} & \dots & \hat{s}_{2n-1} \end{pmatrix}$$

Recalling that $S_n = 2\hat{s}_n$ we get that the matrix for $FS(n)$ is twice that of $\widehat{FS}(n)$ in every entry. Since the determinant is linear in each column we get $FS(n) = 2^n \widehat{FS}(n)$. This is the key equation in the following chain of equations:

$$\#DT \text{ of } A(n) = FS(n) = 2^n \widehat{FS}(n) = 2^n FS(n-1) = 2^n \#DT \text{ of } A(n-1)$$

$$\text{Now } \#DT \text{ of } A(n) = 2^n \#DT \text{ of } A(n-1) = 2^{n+(n-1)+\dots+2} \#DT \text{ of } A(1) = 2^{\binom{n+1}{2}}.$$

19.2 Lemma of Lindström Gessel-Viennot

We need to set up some terminology before we get to the statement of the lemma.

Let $G = (V, E)$ be a directed acyclic graph with a weight function $\omega : E \rightarrow \mathbb{R}$. We consider two sets of vertices $A = a_1, \dots, a_n$ and $B = b_1, \dots, b_n$, and define $\mathcal{P}(i, j)$ = set of all paths $a_i \rightarrow b_j$ in G . From this data we associate a *path matrix*, which is an $n \times n$ -matrix $M = (m_{i,j})$, with

$$m_{i,j} = \omega(\mathcal{P}(i, j)) = \sum_{P \in \mathcal{P}(i, j)} \omega(P),$$

where

$$\omega(P) = \prod_{e \in P} \omega(e).$$

So we multiply the edge weights along a path to get the weight of the path. Then summing over the weights of the paths going from a_i to b_j gives us the entry $m_{i,j}$ of the path matrix.

Let $\pi \in S_n$ and $\mathcal{P}^\pi(A, B)$ be the set of path systems (P_1, \dots, P_n) where $P_i : a_i \rightarrow b_{\pi(i)}$ is a path from a_i to $b_{\pi(i)}$. We define $\mathcal{P}(A, B) = \bigcup_{\pi \in S_n} \mathcal{P}^\pi(A, B)$, as the collection of all path systems from A to B , and \mathcal{P}_{VD} as the subset of vertex disjoint path systems, i.e. path systems (P_1, \dots, P_n) where the paths are pairwise vertex disjoint.

The weight of a path system (P_1, \dots, P_n) is given by

$$\prod_{i=1}^n \omega(P_i)$$

and the sign of a path system is defined as $\text{sgn}(P_1, \dots, P_n) = \text{sgn}(\pi)$ (recall that each path system is in a unique $\mathcal{P}^\pi(A, B)$ for some $\pi \in S_n$).

Lemma 19.6 (Lindström Gessel-Viennot). *Using the above definitions above*

$$\det(M) = \sum_{P \in \mathcal{P}_{VD}(A, B)} \text{sgn}(P) \omega(P).$$

Proof. By the Leibniz formula for determinants

$$\det(M) = \sum_{\pi \in S_n} \text{sgn}(\pi) \prod_{i=1}^n m_{i, \pi(i)}.$$

Expanding the product we get

$$\prod_{i=1}^n m_{i, \pi(i)} = \prod_{i=1}^n \left(\sum_{P_i \in \mathcal{P}(i, \pi(i))} \omega(P_i) \right) = \sum_{\substack{P \in \mathcal{P}^\pi(A, B) \\ P = (P_1, \dots, P_n)}} \left(\prod_{i=1}^n \omega(P_i) \right) = \sum_{P \in \mathcal{P}^\pi(A, B)} \omega(P).$$

From this we get

$$\det(M) = \sum_{P \in \mathcal{P}(A, B)} \text{sgn}(P) \omega(P).$$

This is already quite close to what we want to show in the Lemma. However the sum still contains intersecting paths systems. We will use an involution on the set of intersecting path systems to show that their contribution to $\det(M)$ is zero. The clue is that the involution is sign reversing and weight preserving. This will have the effect that intersecting path systems will be paired up by the involution, one with the negative weight of the other so that they cancel each other in the sum.

Given an intersecting path system $(P_1, \dots, P_n) \in \mathcal{P}^\pi(A, B)$ for some π there exist $i \neq j$ such that $P_i \cap P_j \neq \emptyset$. Let i_0 be the minimum index such that there exists a j so that $P_{i_0} \cap P_j \neq \emptyset$. Then let x be the first vertex along P_{i_0} which also belongs to some other P_j and let j_0 be the smallest index such that P_{j_0} meets P_{i_0} in x . This makes sure that

the indices of i_0 and j_0 are uniquely defined because $((i_0, x, j_0))$ is lexicographically minimal). The involution $P = (P_1, \dots, P_n) \rightarrow \tilde{P} = (\tilde{P}_1, \dots, \tilde{P}_n)$ is defined as follows:

$$\begin{aligned}\tilde{P}_{i_0} &= P_{i_0} \Big|_{\text{init. piece up to } x} \cup P_{j_0} \Big|_{\text{from } x \text{ to } b_{\pi(j_0)}} \\ \tilde{P}_{j_0} &= P_{j_0} \Big|_{\text{init. piece up to } x} \cup P_{i_0} \Big|_{\text{from } x \text{ to } b_{\pi(i_0)}}\end{aligned}$$

and the remaining paths stay the same

$$\tilde{P}_i = P_i \quad \forall i \notin \{i_0, j_0\}.$$

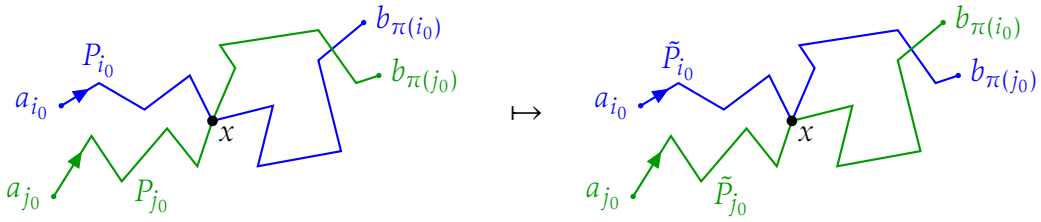


Figure 19.2: Sketch of how the involution applies to paths P_{i_0} and P_{j_0}

This is an involution, because after applying it the index i_0 is still the smallest index of a path that intersects some other path of the family \tilde{P} , vertex x is still the same and j_0 is still the smallest index of a path through x (other than i_0). So applying it again makes $\tilde{\tilde{P}}_{i_0} = P_{i_0}$ and $\tilde{\tilde{P}}_{j_0} = P_{j_0}$.

It remains to argue that the involution is sign-reversing and weight-preserving. The sign is dependent on the sign of the permutation, and applying our involution swaps the endpoints of two of the paths, which means that we apply a transposition to swap $\pi(i_0)$ and $\pi(j_0)$ so the sign of the path system will be reversed. And the weight stays the same, because the weight of a path system is just the product of the weights of all the edges in it (with multiplicities). The multiset of edges in $P_{i_0} \cup P_{j_0}$ did not change.

The involution shows that the intersecting path systems cancel out in the Leibniz expansion of $\det(M)$. This leaves only the vertex disjoint path systems, whence

$$\det(M) = \sum_{P \in \mathcal{P}_{VD}(A, B)} \text{sgn}(P) \omega(P).$$

□

We stated earlier that we can use the lemma of Lindström Gessel-Viennot to get that

$$FS(n) = \det \begin{pmatrix} S_1 & S_2 & S_3 & \dots & S_n \\ S_2 & S_3 & S_4 & \dots & S_{n+1} \\ S_n & S_{n+1} & S_{n+2} & \dots & S_{2n-1} \end{pmatrix}$$

and similarly for $\widehat{FS}(n)$. We consider the directed triangular grid graph consisting of all possible steps, see Figure 19.3. This will give us the number of Schröder paths from a_i to b_j . To argue for that assign a weight of 1 to each edge. Then the entry m_{ij} of the path matrix will just count the number of paths from a_i to b_j . Each path system will then also have a weight of 1. Further, any permutation other than the identity does not appear in the sum, since there is no way for any other permutation to give a set of non-intersecting paths. So the left side counts $FS(n)$, the number of non-intersecting path families.

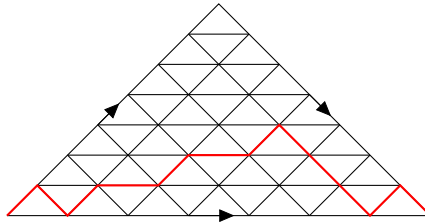


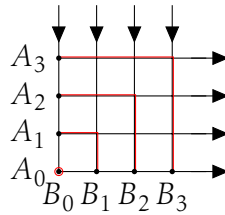
Figure 19.3: The directed acyclic graph on which the Schröder paths live

We conclude the lecture with another application of the lemma. The LGV lemma can be used in two ways. We can compute a determinant to understand combinatorial counting functions (this was done above) or can use combinatorial insights to evaluate a determinant (this is done below).

Theorem 19.7.

$$\det \left(\binom{i+j}{i} \right)_{0 \leq i, j \leq n-1} = 1$$

Proof. We look at the directed grid graph of the first quadrant, where orientations of edges imply that a path can only go right or down. The number of paths from $A_i = (0, i)$ to $B_j = (j, 0)$ is $\binom{i+j}{i}$, since there are $i+j$ steps in total and i of those are downward steps. If we assign each edge a weight of 1 this gives us the entries of our path matrix. The



Lemma of Lindström Gessel-Viennot tells us that the determinant of the path matrix is equal to the number of non-intersecting path systems from $A = \{A_0, \dots, A_{n-1}\}$ to $B = \{B_0, \dots, B_{n-1}\}$. By the planarity of the graph vertex disjoint path systems can only exist for $\pi = id$, i.e., with paths connecting A_i to B_i for all i . It is evident that there is only one choice for the path $A_0 \rightarrow B_0$ having fixed this path there is only one choice for the path $A_1 \rightarrow B_1$ and so on. In effect the path family is unique. \square

Binet-Cauchy Formula and Pólya Theory

We start this lecture by proving the Binet-Cauchy formula which is another application of the Lindström-Gessel-Viennot Lemma, and then start with a new chapter on *Pólya theory*.

Theorem 20.1 (Cauchy-Binet formula). *Given two matrices $P, Q \in \mathbb{R}^{r \times s}$ with $r \leq s$ it holds true that*

$$\det(PQ^T) = \sum_{C \subset [s], |C|=r} \det(P_C) \det(Q_C),$$

where M_C denotes the restriction of a Matrix M to the columns selected by C .

Proof. First construct a directed graph G as follows: there are three disjoint sets of vertices $\{A_1, \dots, A_r\}$, $\{I_1, \dots, I_s\}$, and $\{B_1, \dots, B_r\}$. The edges are the edges of complete bipartite subgraph between $\{A_1, \dots, A_r\}$ and $\{I_1, \dots, I_s\}$ and of a second complete bipartite subgraph between $\{I_1, \dots, I_s\}$ and $\{B_1, \dots, B_r\}$, the edges are oriented as illustrated in Figure 20.1.

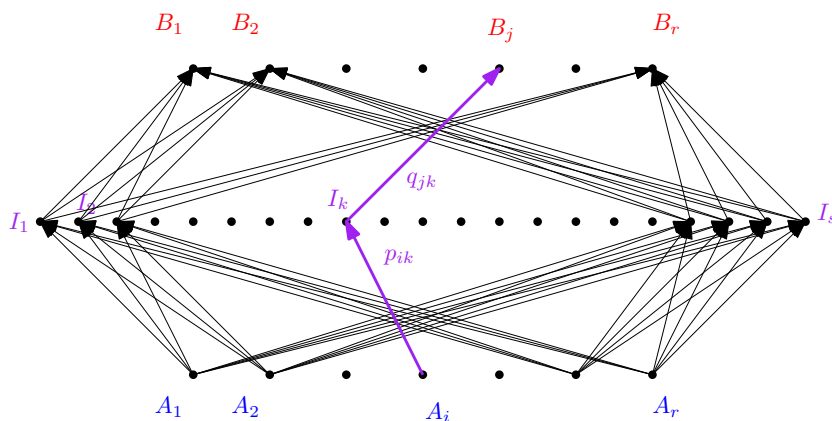


Figure 20.1: The directed graph on the vertices A, B and I , where the subgraph spanned by the vertices in A, I and B, I respectively forms a complete bipartite graph. The edges $A_i I_k$ and $I_k B_j$ are highlighted, their respective weights are $p_{i,k}$ and $q_{j,k}$.

The weight of edges is as follows: $w(A_i I_k) := p_{i,k}$ and $w(I_k B_j) := q_{j,k} = q_{k,j}^T$, where $p_{i,k}$ and $q_{j,k}$ are the respective entries of P, Q .

We construct a path-matrix $M = (m_{i,j})$ for $i, j \in [r]$ where

$$m_{i,j} := \sum_{P: A_i \rightarrow B_j} w(P) = \sum_{k=1}^s p_{i,k} q_{j,k} = (PQ^T)_{i,j}.$$

Hence $M = PQ^T$. Recall that for a path-system \mathcal{P} the weight $w(\mathcal{P})$ is the product of the weights of all the paths in \mathcal{P} .

Using the Lemma of Lindström-Gessel-Viennot ([Lemma 19.6](#)), we get

$$\det(PQ^T) = \det(M) = \sum_{\mathcal{P} \in \mathcal{P}_{VD}(A,B)} \text{sgn}(\mathcal{P}) w(\mathcal{P}), \quad (20.26)$$

where $\mathcal{P}_{VD}(A,B)$ denotes the vertex disjoint path systems from the vertices $\{A_1, \dots, A_r\}$ to the vertices in $\{B_1, \dots, B_r\}$ in the graph G . Given a permutation π , the path $P_i : A_i \rightarrow B_{\pi(i)}$ of a path system \mathcal{P} in $\mathcal{P}^\pi(A,B)$ contains a middle vertex from $\{I_1, \dots, I_s\}$. Every tuple of r distinct vertices from I corresponds to a disjoint path system $\mathcal{P} \in \mathcal{P}^\pi(A,B)$. For $R \subset [s]$, let I_R denote the corresponding subset of vertices of I . Given a path system $\mathcal{P} \in \mathcal{P}^\pi(A,B)$ using the vertices of I_R as middle vertices we can view the permutation π as a product of two permutations π_1 and π_2 , where $\pi_1 : [r] \rightarrow R$ tells us which edges from A to I_R are used and $\pi_2 : R \rightarrow [r]$ which edges from I_R to B . For instance, if $r = 3$ and $s = 17$ we could have $R = \{7, 8, 15\}$ and paths

$$A_1 \rightarrow I_8 \rightarrow B_3, \quad A_2 \rightarrow I_{15} \rightarrow B_1, \quad A_3 \rightarrow I_7 \rightarrow B_2,$$

then we see that $\pi = \pi_1 \cdot \pi_2$ with

$$\pi_1 := \begin{pmatrix} 1 & 2 & 3 \\ 8 & 15 & 7 \end{pmatrix}, \quad \pi_2 = \begin{pmatrix} 8 & 15 & 7 \\ 3 & 1 & 2 \end{pmatrix}.$$

Using this idea we can rewrite the right hand side of [Equation \(20.26\)](#):

$$\begin{aligned} \sum_{\mathcal{P} \in \mathcal{P}_{VD}(A,B)} \text{sgn}(\mathcal{P}) w(\mathcal{P}) &= \sum_{R \subset [s], |R|=r} \sum_{\pi_1, \pi_2} \text{sgn}(\pi_1 \cdot \pi_2) w(\mathcal{P}_1) w(\mathcal{P}_2) \\ &= \sum_{R \subset [s], |R|=r} \left(\sum_{\pi_1} \text{sgn}(\pi_1) w(\mathcal{P}_1) \sum_{\pi_2} \text{sgn}(\pi_2) w(\mathcal{P}_2) \right) \\ &= \sum_{R \subset [s], |R|=r} \left(\sum_{\pi_1} \text{sgn}(\pi_1) w(\mathcal{P}_1) \right) \left(\sum_{\pi_2} \text{sgn}(\pi_2) w(\mathcal{P}_2) \right) \\ &= \sum_{R \subset [s], |R|=r} \det(P_R) \det(Q_R), \end{aligned}$$

where \mathcal{P}_1 are the respective path systems of subpaths $A \rightarrow I_R$, that is $\mathcal{P}^{\pi_1}(A, I_R)$ and \mathcal{P}_2 the respective path systems of subpaths $I_R \rightarrow B$ i.e. $\mathcal{P}^{\pi_2}(B, I_R)$. \square

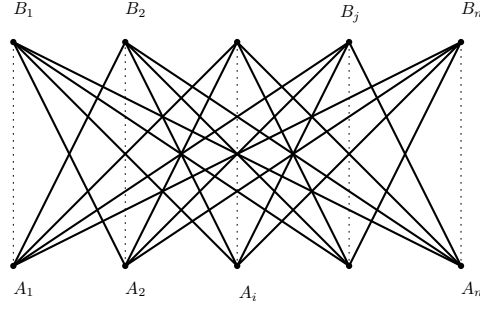


Figure 20.2: The bipartite graph on the vertices A_1, \dots, A_n and B_1, \dots, B_n .

We conclude this chapter with a few remarks.

Remark (Application to derangements). Consider the bipartite graph $G = (A, B; E)$ where $A = \{A_1, \dots, A_n\}$, $B = \{B_1, \dots, B_n\}$ and $E = K_{n,n} \setminus \{(A_i, B_i) \mid i \in \{1, \dots, n\}\}$, as depicted in 20.2. The vertex disjoint pathsystems in this graph correspond to derangements, as there is no path $A_i \rightarrow B_i$ which would be fixed point of the respective permutation. So the pathmatrix here is given by

$$M = \begin{bmatrix} 0 & 1 & 1 & 1 & \dots & 1 \\ 1 & 0 & 1 & 1 & \dots & 1 \\ 1 & 1 & 0 & 1 & \dots & 1 \\ \vdots & \vdots & & \ddots & & \vdots \\ 1 & 1 & 1 & 1 & \dots & 0 \end{bmatrix}$$

Next we can use standard transformations to bring the matrix M into a more suitable form to determine its determinant via the following operations.

$$\begin{bmatrix} 0 & 1 & 1 & 1 & \dots & 1 \\ 1 & 0 & 1 & 1 & \dots & 1 \\ 1 & 1 & 0 & 1 & \dots & 1 \\ \vdots & \vdots & & \ddots & & \vdots \\ 1 & 1 & 1 & 1 & \dots & 0 \end{bmatrix} \rightarrow \begin{bmatrix} 0 & 1 & 1 & 1 & \dots & 1 \\ 1 & -1 & 0 & 0 & \dots & 0 \\ 1 & 0 & -1 & 0 & \dots & 0 \\ \vdots & \vdots & & \ddots & & \vdots \\ 1 & 0 & 0 & 0 & \dots & -1 \end{bmatrix} \rightarrow \begin{bmatrix} (n-1) & 1 & 1 & 1 & \dots & 1 \\ 0 & -1 & 0 & 0 & \dots & 0 \\ 0 & 0 & -1 & 0 & \dots & 0 \\ \vdots & \vdots & & \ddots & & \vdots \\ 0 & 0 & 0 & 0 & \dots & -1 \end{bmatrix}$$

In the first step the first column has been subtracted from each subsequent column. In the second step columns 2 to n have been added to column 1. From the diagonal of the resulting matrix we see that $\det(M) = (n-1)(-1)^{n-1}$. On the other hand the Lemma of Lindström Gessel-Viennot (Lemma 19.6) implies that $\det(M) = \sum_{\pi \in S_n, \pi \text{ derangement}} \text{sgn}(\pi)$. Together this yields:

$$(n-1)(-1)^{n-1} = \#(\text{even derangements in } S_n) - \#(\text{odd derangements in } S_n).$$

For the next remark we need a definition

Definition 20.2. The *permanent* of a matrix $A \in \mathbb{F}^{n \times n}$ is given by

$$\text{per}(A) = \sum_{\pi \in S_n} a_{1,\pi(1)} \cdot a_{2,\pi(2)} \cdot \dots \cdot a_{n,\pi(n)}.$$

Remark. Note that the definition of the permanent resemble Leibniz formula for the determinant, the difference is that the sign of the permutation is missing in the products.

From the considerations above we see that that $\text{per}(J - I) = \#(\text{derangements in } S_n)$ where J is the all-one matrix and I the identity.

We know that \det can be computed in $\mathcal{O}(n^3)$; in contrast computing per is $\#P$ -complete, this means that unless unexpected things happen no polynomial algorithm for the evaluation of permanents exist.

20.1 Pólya Theory

Pólya theory is all about *counting with symmetries*. It is best understood using some examples.

Example 35 (Necklaces). Let $N(m, k)$ denote the number of necklaces with m beads of k colors. One can think of a necklace as a cyclic arrangement of its beads. It is easily verified that $N(1, 2) = 2$, $N(2, 2) = 3$, $N(3, 2) = 4$, $N(4, 2) = 6$, $N(5, 2) = 8$, and $N(6, 2) = 14$. We do not differ between rotations of the necklace. In other words the symmetry group (acting on the necklaces) is the cyclic group C_m . Note that the symmetry group can also be the dihedral group if turning over (reflecting) the necklace is not considered to change the necklace either, with this group of symmetries $ND(6, 2) = 13$.

The general idea is as follows: if you consider the number of ways to color 6 distinguishable beads of a necklace with 3 colors we would get 3^6 possibilities. But if you look at it like a necklace then $RGBRGB = GBRGBR$ would be the same coloring just rotated. Counting with symmetries thus becomes the enumeration of *orbits* – equivalence classes – of the relevant group actions; informally said we factor out the symmetries that we want to count as equal. So if turning the necklace results in the same coloring, we have to look at the orbits of the action of the cyclic group on the 3^6 colorings of the necklace.

For example the $RRRRRR$ coloring only appears once while $RGBRRB$ occurs 12 times when we consider symmetric colorings with respect to the dihedral group—rotations and reflections—to be equal.

We will get into more detail later.

Example 36 (Cube). Given a cube one can ask for the number of colorings of its six faces with k colors up to rigid transformations of the cube. For $k = 2$ we get the following results:

# red faces	0	1	2	3	4	5	6
# colorings	1	1	2	2	2	1	1

The group of the cube can be thought of as all possible rotations of the cube. Now it turns out that a group element is uniquely determined by looking at the image of a *flag*. There are three types of flags given by either (v, e) , $v \in e$ or (v, f) , $v \in \partial f$ or (e, f) , $e \in \partial f$, where each type leads to exactly 24 flags. For example for the (v, e) flags we have 8 vertices each incident to 3 edges giving 24 flags. Thus the group has 24 elements, that is 24 symmetries.

As an abstract group the 24 symmetries of the cube are isomorphic to S_4 . In our context however we will view it as a subgroup of S_6 giving the actions on the faces, and a subgroup of S_8 for actions on the vertices and also as a subgroup of S_{12} for the actions on edges. We will get back to this later.

We start with formally introducing some of the concepts already mentioned in the examples.

20.1.1 Permutation groups and group action

We start with the formal definition of a group action on a set.

Definition 20.3 (Group action). Let (G, \odot) be a group and let X be some set, then we say that G acts on X if there is a map $\alpha : G \times X \rightarrow X$ such that

$$(1) \quad \alpha(e, x) = x,$$

$$(2) \quad \alpha(g \odot h, x) = \alpha(g, \alpha(h, x)).$$

For readability we will write $g(x) := \alpha(g, x)$ which then yields the more concise notation $(g \odot h)(x) = g(h(x))$.

Remark. Note that we can also let a group act on another group or on itself.

Observation. Let G be a group acting on a set X . Then for every $g \in G$ the map $g : X \rightarrow X$, $x \mapsto g(x)$ is a bijection on X .

Proof. Suppose that $g(x) = g(y)$ this implies that $g^{-1}(g(x)) = g^{-1}(g(y))$ which in turn, using the concatenation of actions of a group, implies that $x = e(x) = e(y) = y$. This gives injectivity of the map, where surjectivity immediately follows from the fact that $x = e(x) = g(g^{-1}(x))$. \square

Remark. This implies that one can view the group G as a subgroup of S_X – the symmetry group of X . In fact every $g \in G$ acts as a bijection of X , i.e., as a permutation $\pi_g \in S_X$. from $(g \odot h)(x) = g(h(x))$ it follows that $\pi_g \cdot \pi_h = \pi_{g \odot h}$, i.e., the images of G form a subgroup of S_X .

For what comes next we will need the *type of a permutation* that was already introduced in one of the first lectures. For convenience we repeat the definition.

Definition 20.4 (type of a permutation). Let $\pi \in S_n$ for some $n \in \mathbb{N}$. Then the *type of* π is given by

$$\text{type}(\pi) := (b_1, \dots, b_n),$$

where b_i denotes the number of cycles of length i in π .

Observation. If π has type (b_1, \dots, b_n) then $\sum_{k=1}^n kb_k = n$.

Now we can define the *cycle index* of G . We will need it later for the Lemma of Frobenius-Cauchy-Burnside.

The idea behind the cycle index will be to capture fixpoints of the group actions on color classes. The reflection taking (123456) to (654321) is part of the dihedral group and as a permutation it can be written as $r := (16)(25)(34)$. Now this permutation has 3 cycles of length 2 that will be remembered as x_2^3 . Later we will need to ask ourselves: *how many colorings of the six beads will be fixpoints of r if we use 3 colors?* The answer now is obvious: 3^3 : for each 2-cycle we can freely choose a color but we have to color both beads with that same color. Similarly if we would color the necklace with k colors this would amount to k^3 fixpoints under r . The cycle index polynomial will capture exactly these cycles for the different actions.

Definition 20.5 (Cycle index of a group). Let G be a finite group acting on an m -set, i.e., $G \subseteq S_m$. The cycle index of G (in this action) is defined as

$$P_G(x_1, \dots, x_m) := \frac{1}{|G|} \sum_{g \in G} x_1^{b_1(g)} \cdot \dots \cdot x_m^{b_m(g)},$$

where $(b_1(g), \dots, b_m(g))$ is the type of g as a permutation.

Having these definitions at hand we will revisit the cube group.

Example 37. We give a table analysing the action of elements of G (depending on their nature) on the faces, vertices and edges of the cube.

# of maps	element of G		action on f.	action on v.	action on e.
1	e (identity)		$b_1 = 6$	$b_1 = 8$	$b_1 = 12$
9	fix a face	6 order 4	$b_1 = 2, b_4 = 1$	$b_4 = 2$	$b_4 = 3$
		3 order 2	$b_1 = 2, b_2 = 2$	$b_2 = 4$	$b_2 = 6$
8	fix a vertex, order 3		$b_3 = 2$	$b_1 = 2, b_3 = 2$	$b_3 = 4$
6	fix an edge, order 2		$b_2 = 3$	$b_2 = 4$	$b_1 = 2, b_2 = 5$

So for example the second row of the table gives insight on the actions that fix a face. There is a total of 9 such actions where 6 of these are of order 4, that is the permutation has a maximum cycle of four. The actions for the cube are rotations and compositions thereof. Every action that fixes one face will also fix the opposite face giving us two one-cycles, i.e $b_1 = 2$. Fixing two opposite faces we can rotate the cube by 90° once left or once right to get a 4-cycle for the faces, rotating twice in one direction would give two 2-cycles since we would simply swap the non-fixed opposite faces. Thus fixing two opposite faces we can either rotate the cube around the fixed axis to the left or right giving 2 maps with $b_1 = 2$ and $b_4 = 1$. In total we have 3 different axes that we can fix and around which we can rotate giving the 6 maps. A similar argument gives the three order two maps: we fix opposite faces and swap the remaining opposite faces.

Looking at the order 4 maps the action on the vertices becomes quite clear, since fixing two faces we also fix the vertices lying on that face, thus the map can only interchange vertices lying on a common face of the two fixed faces. Looking into the action of these maps (rotation around the fixed axis) we get $b_4 = 2$. Similarly we get $b_4 = 3$ for the edges.

All in all we get a total of 24 maps which coincides with the 24-element group G .

Given this table we can compute the cycle index of G acting on the faces given by

$$P_{G_{\text{faces}}}(x_1, \dots, x_6) = \frac{1}{24}(x_1^6 + 6x_1^2x_4 + 3x_1^2x_2^2 + 8x_3^2 + 6x_2^3).$$

We continue with more examples.

Example 38 (symmetric group S_m). For the symmetric group acting on itself the cycle index can be rewritten as follows.

$$\begin{aligned} P_{S_m}(\mathbf{x}) &= \frac{1}{m!} \sum_{(b_1, \dots, b_m), \sum k b_k = m} \#(\text{perm. of type } \mathbf{b}) \mathbf{x}^{\mathbf{b}} \\ &= \frac{1}{m!} \sum \left(\frac{m!}{b_1! 1^{b_1} \dots b_m! m^{b_m}} \right) \mathbf{x}^{\mathbf{b}} \\ &= \sum \prod_{k=1}^m \frac{x_k^{b_k}}{b_k! k^{b_k}} \\ &= \text{coefficient of } z^m \text{ in } \prod_{k=1}^m \sum_{n \geq 0} \frac{x_k^n}{n! k^n} z^{kn} \\ &= \text{coefficient of } z^m \text{ in } \prod_{k=1}^m \sum_{n \geq 0} \frac{1}{n!} \left(\frac{x_k z^k}{k} \right)^n \\ &= \text{coefficient of } z^m \text{ in } \prod_{k=1}^m \exp\left(\frac{x_k}{k} z^k\right), \\ &= \text{coefficient of } z^m \text{ in } \exp\left(x_1 z + \frac{x_2}{2} z^2 + \frac{x_3}{3} z^3 + \dots\right), \end{aligned}$$

where \mathbf{x}, \mathbf{b} are vectors, and $\mathbf{x}^{\mathbf{b}}$ is shorthand for $x_1^{b_1} \dots x_m^{b_m}$.

We conclude this lecture with a last example.

Example 39 (The cyclic group C_n). For the cyclic group the order of each group element is a divisor d of n and its type is given by $b_d = \frac{n}{d}$, so the element decomposes into cycles of the same length.

We get

$$P_{C_n}(x) = \frac{1}{n} \sum_{d|n} \varphi(d) x_d^{n/d},$$

where $\varphi(d) = \#(\text{of group elements of order } d \text{ in } C_n)$ is also known as *Euler's Phi-function*. One can show that $\varphi(d) = \#(s < d \mid \gcd(s, d) = 1)$.

Pólya Theory (continued)

We continue with Pólya Theory. Last lecture we discussed the cycle index polynomial P_G of a group G acting on a set.

The first lemma will give us an efficient way to determine the number of orbits of a group acting on a set; that is we get an efficient way to determine the number of color classes with respect to symmetries given by G (recall the Necklace example from last lecture).

21.1 Lemma of Cauchy-Frobenius-Burnside

Given a group G acting on a set X , this induces an obvious equivalence relation given by

$$x \sim y \Leftrightarrow \exists g \in G \quad g(x) = y.$$

Reflexivity comes from the identity $1_G \in G$, symmetry from the inverse $g^{-1} \in G$ and transitivity by the fact that $(g \circ h)(x) = g(h(x))$ and $g, h \in G$ implies that $g \circ h \in G$.

The equivalence classes of this relation are the **orbits of the action**. We write

$$O_G(X) = \{\text{orbits of the action of } G \text{ on } X\} = \{[x]_{\sim} \mid x \in X\}$$

If we fix $x \in X$ there is a **stabilizer** subgroup

$$G_x = \{g \in G \mid g(x) = x\}.$$

For $g \in G$ there is the set of fixed points

$$\text{Fix}(g) = \{x \in X \mid g(x) = x\}$$

Lemma 21.1 (Cauchy-Frobenius-Burnside). *The number of orbits of the action of G on the set X is given by*

$$|O_G(X)| = \frac{1}{|G|} \sum_{g \in G} |\text{Fix}(g)|$$

Proof. We double count the pairs (g, x) with $g(x) = x$. We can express this number in two ways, this yields the identity:

$$\sum_{x \in X} |G_x| = \sum_{g \in G} |\text{Fix}(g)|,$$

We will focus on the left side of the equation.

Define $G_{x \rightarrow y} = \{g \in G \mid g(x) = y\}$ for some x, y in X . Now observe that either $G_{x \rightarrow y} = \emptyset$ or $G_{x \rightarrow y} = hG_x$ for some h with $h(x) = y$. For the second case $G_{x \rightarrow y}$ is a coset of the stabilizer subgroup. In particular $|G_{x \rightarrow y}| = |G_x|$, and we are in the second case if and only if $y \in \text{Orbit}(x) = \{g(x) \mid g \in G\}$. From this we see that for each x the size of the group is the size of the stabilizer times the size of the orbit

$$|G| = |G_x| \cdot |\text{Orbit}(x)| \quad \forall x \in X.$$

Then we get

$$\sum_{g \in G} |\text{Fix}(g)| = \sum_{x \in X} |G_x| = |G| \sum_{x \in X} \frac{1}{|\text{Orbit}(x)|} = |G| \cdot |O_G(X)|.$$

In the last equality we use the fact that every orbit of G on X contributes 1 to the sum, and the set of orbits of the action of G form a partition of X . \square

Applications of the lemma: Colouring edges of the cube with 3 colours.

Two colourings are considered the same, if they belong to the same orbit, in our case if they can be transformed by a rigid motion into each other. Conversely colourings are different if and only if they belong to different orbits.

$$\begin{aligned} \# \text{colourings} &= \# \text{orbits} = \frac{1}{|G|} \sum_{g \in G} |\text{Fix}(g)| \\ &= \frac{1}{24} \sum_{\text{type } b} (\# \text{perm. } g \text{ of type } b) \underbrace{(\# \text{colourings fixed by perm. } g \text{ of type } b)}_{3^{\# \text{cycles}} = 3^{\sum b_i}} \\ &= \frac{1}{24} (1 \cdot 3^{12} + 6 \cdot 3^3 + 3 \cdot 3^6 + 8 \cdot 3^4 + 6 \cdot 3^7) \\ &= 22815 \end{aligned}$$

see [Example 37](#) for the values used for the computation.

Example 40. Necklaces with 2 types of beads with rotational symmetry correspond to orbits of $[2]^{[n]}$ (note that when we take one set raised to another it is defined as the set of functions from the raised set to the ground set, so in this case we get the set of functions from $[n] \rightarrow [2]$ which can be represented as 0,1-vectors of size n) under action of C_n (cyclic group).

$$\begin{aligned} \# \text{necklaces} &= \frac{1}{n} \sum_{g \in C_n} |\text{Fix}(g)| \\ &= \frac{1}{n} \sum_{\text{type } b} (\# \text{perm. } g \text{ of type } b) (\# \text{elem. of } [2]^{[n]} \text{ fixed}) \\ &= \frac{1}{n} \sum_{d|n} \varphi(d) 2^{\frac{n}{d}} \end{aligned}$$

Recall that $\varphi(d) = |\{s \leq d \mid \gcd(s, d) = 1\}|$ is Euler's Phi-function from last lecture.

Definition 21.2. In general we are given a group G acting on a set D , and a "set of colors" R . Two colorings $f_1, f_2 \in R^D$ of the elements in D are G -indistinguishable if there exists a $g \in G$ such that $f_1 \circ g = f_2$.

This yields a G action on R^D . Applying the C-F-B Lemma again we get

$$\begin{aligned} \# \text{classes} &= \frac{1}{|G|} \sum_{g \in G} |\text{Fix}(g)| = \frac{1}{|G|} \sum_{g \in G} |R|^{\# \text{orbits}(g)} \\ &= \frac{1}{|G|} \sum_{g \in G} |R|^{\sum b_i} = \frac{1}{|G|} \sum_{b \text{ type of some } g \in G} (\#g \text{ of type } b) \cdot |R|^{\sum b_i} \\ &= P_G(|R|, |R|, \dots, |R|) \end{aligned}$$

The following theorem is the abstraction of what we have seen in the examples of colorings of the faces of a cube and of necklaces.

Theorem 21.3. If we have G acting on D , then

$$\#(G \text{ indistinguishable } r\text{-colourings of } D) = P_G(r, r, \dots, r)$$

We are going to generalize the theory by looking at Pólya counting with weights. Consider a weight function $\omega : R \rightarrow A$ for some ring A and let $\omega(R) = \sum_{r \in R} \omega(r)$. For a colouring $f : D \rightarrow R$ we let $\omega(f) = \prod_{x \in D} \omega(f(x))$.

Lemma 21.4 (weight distribution on R^D). With notation as above we get

$$\sum_{f \in R^D} \omega(f) = \omega(R)^{|D|}$$

Proof. Let $R = \{r_1, r_2, \dots, r_k\}$, then

$$\omega(R)^{|D|} = (\omega(r_1) + \omega(r_2) + \dots + \omega(r_k))^{|D|} = \prod_{x \in D} (\omega(r_1) + \omega(r_2) + \dots + \omega(r_k))$$

and for each $f : D \rightarrow R$ we get that $\omega(f)$ is a unique summand of the expanded product. So we get

$$\omega(R)^{|D|} = \sum_{f \in R^D} \omega(f)$$

□

Observation. If f_1, f_2 belong to the same orbit of the G action ($f_1 \circ g = f_2$) then this implies $\omega(f_1) = \omega(f_2)$. Hence for an orbit F we can define $\omega(F) := \omega(f)$ for any $f \in F$.

The goal is to find $\sum_{F \text{ Orbit}} \omega(F)$.

Let Λ be a partition of D and let S_Λ be the set of all $f \in R^D$ which are constant on blocks of Λ and let $\omega^{\lambda_i}(R) := \sum_{r \in R} \omega(r)^{\lambda_i}$.

Lemma 21.5. *If Λ consists of k blocks with sizes $\lambda_1, \lambda_2, \dots, \lambda_k$, then*

$$\sum_{f \in S_\Lambda} \omega(f) = \prod_{i=1}^k \left(\sum_{r \in R} \omega(r)^{\lambda_i} \right) = \prod_{i=1}^k \omega^{\lambda_i}(R)$$

21.2 The fundamental theorem

We are ready to state the main result.

Theorem 21.6 (Pólya's Fundamental Theorem).

$$\sum_{\substack{F \text{ orbits of} \\ G \text{ action on } R^D}} \omega(F) = P_G(\omega(R), \omega^2(R), \dots, \omega^{|D|}(R))$$

Remark. If $\omega(r) = 1 \quad \forall r \in R$, then $\omega(F) = 1$ and $\omega^k(R) = \sum_{r \in R} \omega(r)^k = |R|$. So we get $\# \text{orbits} = P_G(|R|, |R|, \dots, |R|)$, which we saw previously in [Theorem 21.3](#) making the Pólya Fundamental Theorem a generalization thereof.

Proof. Consider $f \in R^D$ and let $\omega = \omega(f)$ and

$$S_\omega = \{f' \in R^D \mid \omega(f') = \omega\}$$

We observe that

- S_ω contains all f' in $\text{orbit}(f)$, since if two functions are in the same orbit they have the same weight
- S_ω is a union of orbits
- S_ω is invariant under the action of G on R^D

We now look at the action of G on S_ω . By the Lemma of C-F-B ([Lemma 21.1](#)) we get that

$$\# \text{orbits}(G, S_\omega) = \frac{1}{|G|} \sum_g \#(f \in S_\omega : f \circ g = f).$$

Then

$$\begin{aligned}
 \sum_{F \text{ orbit}} \omega(F) &= \sum_{\omega} \# \text{orbits}(G, S_{\omega}) \cdot \omega \\
 &= \frac{1}{|G|} \sum_g \#(f \in S_{\omega} : f \circ g = f) \cdot \omega \\
 &= \frac{1}{|G|} \sum_g \sum_{f \in \text{Fix}(g)} \omega(f) \\
 &= \frac{1}{|G|} \sum_g \prod_{k=1}^m [\omega^k(R)]^{b_k} = P_G(|R|, |R|, \dots, |R|).
 \end{aligned}$$

For the equation leading to the last line we used that if f is fixed by g , then this implies that f is constant on every cycle of g , and if further g has type (b_1, \dots, b_m) we get by [Lemma 21.5](#)

$$\sum_{f \in \text{Fix}(g)} \omega(f) = \prod_{k=1}^m [\omega^k(R)]^{b_k}$$

For the last equation recall the definition of the cycle index polynomial:

$$P_G(x_1, \dots, x_m) = \frac{1}{|G|} \sum_{g \in G} x_1^{b_1(g)} x_2^{b_2(g)} \dots x_m^{b_m(g)}.$$

□

Question: How many edge 3-colourings of the cube with 2 red, 4 green, and 6 blue edges exist?

Approach: Our set of colours contains $R = \{r, g, b\}$. We define a weighting $\omega : R \rightarrow A$, by

$$\omega(r) = X, \quad \omega(g) = Y, \quad \omega(b) = Z, \quad \text{therefore} \quad \omega(R) = X + Y + Z$$

The prior theorem implies that the number is the coefficient of $X^2 Y^4 Z^6$ of

$$P_{G_{\text{edge}}}(X + Y + Z, X^2 + Y^2 + Z^2, \dots, X^{12} + Y^{12} + Z^{12})$$

The answer we get, although we don't compute this by hand, is 600.

Design Theory

22.1 Introduction

Design theory talks about *set systems*. A known set system is for example a *graph* $G = (V, E)$ which is a system of vertices V and edges $E \subseteq \binom{V}{2}$. An extension of this notion and another example for set systems are so called *hypergraphs*.

Definition 22.1 (Hypergraph). A *hypergraph* $\mathcal{K} = (V, \mathcal{B})$ is given by a set of vertices V and a set of hyperedges $\mathcal{B} \subseteq \text{Pot}(V)$.

Remark. The set of edges for a graph are just binary relations which are either symmetric in the case of non-directed edges or not necessarily symmetric in the case of directed graphs. For hypergraphs, the edges are replaced by larger subsets of vertices.

Design theory studies very special hypergraphs. In this context it is common to view hypergraphs as incidence structures (P, I, \mathcal{B}) here P is a set of points, \mathcal{B} is a set of blocks and $I \subseteq P \times \mathcal{B}$ is the incidence structure which can be described by a matrix.

Definition 22.2 (Flag). Given an incidence structure (P, I, \mathcal{B}) a *flag* is a pair (p, B) with pIB . If (P, \mathcal{B}) is just a hypergraph a flag is a pair (p, B) with $p \in B$.

Definition 22.3 (Design). A hypergraph (P, \mathcal{B}) is a *design* with parameters λ, t, k, v if

- $|P| = v$,
- $\forall B \in \mathcal{B}$ we have $|B| = k$,
- $\forall T \in \binom{P}{t}$ there are exactly λ blocks $B_1, \dots, B_\lambda \in \mathcal{B}$ with $T \subseteq B_i$ for all $i \in \{1, \dots, \lambda\}$.

Such a pair (P, \mathcal{B}) is a *Steiner system* with parameter set λ, t, k, v or simply a $S_\lambda(t, k, v)$.

Remark. Given an incidence structure (P, I, \mathcal{B}) we may also suppress the incidence relation and write (P, \mathcal{B}) if I is clear from context.

Example 41. The complete k -uniform hypergraph $\mathcal{L} = \left(V, \binom{V}{k}\right)$ is a $S_\lambda(t, k, v)$ for every $t \leq k$ and $\lambda = \binom{v-t}{k-t}$. This is one of the so-called *trivial designs*.

Example 42 (Projective plane). The Fano plane is the projective plane of order 2. It has 7 points ($|P| = 7$) and 7 lines ($|\mathcal{B}| = 7$) and 3 points on each line ($k = 3$). Any two distinct points determine a unique line containing them. The Fano plane is an $S_1(2, 3, 7)$.

In general a finite projective plane of order q forms an $S_1(2, q+1, q^2+q+1)$.

Example 43 (Projective plane put differently). Let $P = \mathbb{F}_2^3$, so $|P| = 8$. We let the blocks be defined via $\mathcal{B} := \{\{x, y, z, x + y + z\} \mid x, y, z \in \mathbb{F}_2^3 \text{ different}\}$ giving $k = 4$. As an observation we see that every block is uniquely determined by each of its triples since we get the remaining element via addition as we work over \mathbb{F}_2 . This makes it an $S_1(3, 4, 8)$ which is an *affine geometry*.

Fix $(0, 0, 0) \in \mathbb{F}_2^3$ and consider

$$\mathcal{B}' := \{B \setminus (0, 0, 0) \mid B \in \mathcal{B} \text{ and } (0, 0, 0) \in B\}.$$

We call (P, \mathcal{B}') the residual design of (P, \mathcal{B}) . The blocks are of size three and every pair of points together with $(0, 0, 0)$ determines a unique block. So for example if we are given $(1, 0, 0)$ and $(1, 0, 1)$ then we know that these form a block together with $(0, 0, 1)$. This shows that $(\mathbb{F}_2^3 \setminus (0, 0, 0), \mathcal{B}')$ form an $S_1(2, 3, 7)$.

This construction can be generalised to get an $S_1(3, 4, 2^n)$ which can be transformed in the same fashion to a residual design $S_1(2, 3, 2^n - 1)$.

Having visited several examples we may pose the main question of Design Theory:

Question: Given (λ, t, k, v) does there exist an $S_\lambda(t, k, v)$, and if so, how many of them do exist?

Observation. The existence of a $S_\lambda(t, k, v)$ given some parameters (λ, t, k, v) can be reduced to an integer program. Take a matrix $\binom{P}{t} \times \binom{P}{k}$ matrix T which has a 1 if the t -element subset is contained in the k -element subset and a 0 otherwise. Then we ask for an integer vector x with entries ≥ 0 such that $Tx = \lambda \mathbf{1}$. The selection vector x selects a multiset of sets of size k that form the block such that every t -subset of $|P|$ is covered by exactly λ many blocks.

These matrices can be rather big and solving the IP impossible: this motivates to look for systems with large automorphism groups as for these we can rely on the help of group actions to reduce the size of the matrix and solve the existence question more efficiently.

Example 44 (Existence of $S_6(3, 5, 10)$). First we need a ground set with 10 elements. We take the edges of a K_5 giving $\binom{5}{2} = 10$ edges. The group S_5 is acting on K_5 and its edges. We define the blocks to be the orbits of

- 5-cycles and
- triangles with two legs, i.e., a 3-cycle with two additional independent edges to the remaining vertices

under the action of S_5 .

A block corresponding to the edges of a 5-cycle is fixed by a dihedral subgroup of S_5 . The dihedral group D_5 has 10 elements, hence there are $|S_5|/|D_5| = 120/10 = 12$ blocks of the first type.

For the triangle with legs we have $\binom{5}{3} = 10$ options for the triangle. The first of the remaining vertices can have a leg with each of the three vertices of the triangle, the second only has two options. Hence, we have $\binom{5}{3} \cdot 3 \cdot 2 = 60$ blocks of this type.

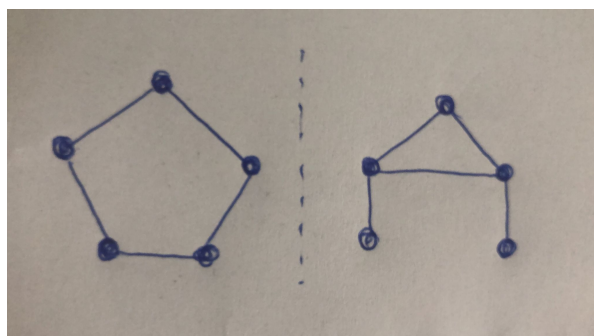


Figure 22.1: A 5-cycle and a triangle with two legs.

We are left to check the properties for $t = 3$ and $\lambda = 6$.

Let us look at 3-element sets of edges—or more rigorous the orbits thereof under the action of S_5 on K_5 . There are four different types as illustrated in Figure 22.2.

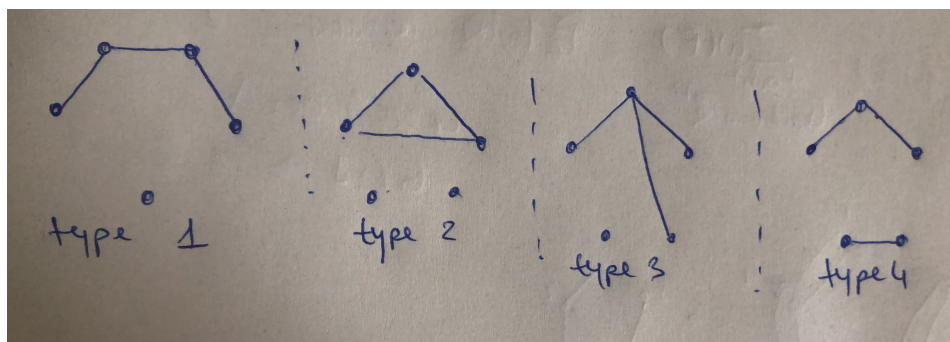


Figure 22.2: The four different types for 3 edges in K_5 .

Each such type comes with a labeling of the vertices/edges and thus we have to check to how many blocks/orbits it can be extended. For the first type there is only one choice to make it a 5-cycle: we have to connect the two vertices of degree one with the missing vertex to make it an element of an orbit of the 5-cycles. There are 5 different choices however to extend it to a triangle with two legs. Thus all in all it is "a subset" of 6 blocks. The following picture shows the extensions.

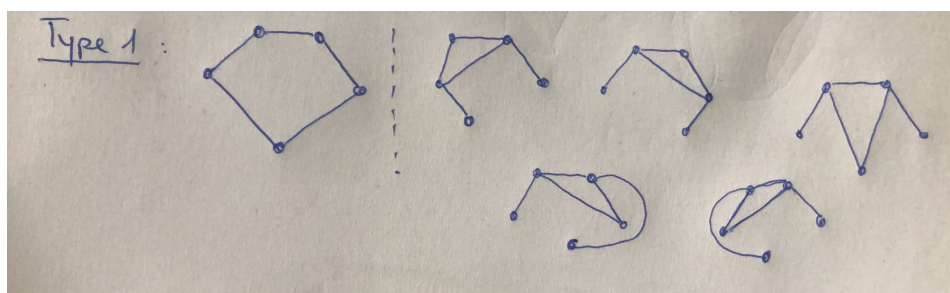


Figure 22.3: The 6 different orbits of type 1.

For the second type – the triangle – there are 6 way for adding the two legs. The third one allows three options of adding one edge to make it a triangle with one leg, in each case there are two options for the second leg, i.e., $3 \cdot 2 = 6$ ways of completing it to a block. Finally type 4 can be completed in 2 ways to a 5-cycle and in 4 ways to a triangle with legs.

Concluding we have seen that any 3-set of edges in K_5 is part of exactly 6 orbits making our set system an $S_6(3, 5, 10)$.

Example 45 (Existence of an $S_1(3, 4, 10)$). We again use the edges of K_5 as the ground set. In this case \mathcal{B} will be the orbits of $K_3 \cup K_2$, S_4 (a star with 4 edges) and $C_4 \cup \{v\}$ a 4-cycle with a singleton

Now for the first one we get $|S_3 \times S_2| = 12$ elements in the stabilizer group giving an orbit of size $120/12 = 10$. The star has automorphism group S_4 giving an orbit of size $120/24 = 5$. For the 4-cycle we get the dihedral group on 4 elements giving an orbit of size $120/8 = 15$. Thus in total we have $|\mathcal{B}| = 30$ blocks. In this case the 3-sets of all types shown in [Figure 22.2](#) allow exactly one completion to a block, this shows that the system is an $S(3, 4, 10)$.

22.2 Arithmetic conditions

The first thing we ask here is *how many blocks does an $S_\lambda(t, k, v)$ have?*

Observation. The idea is to double count pairs (T, B) where $|T| = t$, $B \in \mathcal{B}$ and $T \subseteq B$.

$$\binom{v}{t} \lambda = \sum_T \lambda = \sum_T \sum_{B: T \subseteq B} 1 = \sum_{B \in \mathcal{B}} \sum_{T: T \subseteq B} 1 = \sum_{B \in \mathcal{B}} \binom{k}{t} = b \binom{k}{t},$$

where $b = |\mathcal{B}|$ gives the number of blocks. Thus

$$b = \lambda \frac{\binom{v}{t}}{\binom{k}{t}}.$$

This directly gives a necessary condition for the existence of Steiner systems.

Corollary 22.4. *There is no $S_\lambda(t, k, v)$ for given λ, t, k, v if $\lambda \binom{v}{t} / \binom{k}{t} \notin \mathbb{N}$.*

Let $J \subseteq P$ with $|J| = j < t$ and define $\lambda(J) = \#(B \in \mathcal{B} : J \subset B)$. We count pairs (T, B) again with $|T| = t$, $B \in \mathcal{B}$ and the extra condition $J \subseteq T \subseteq B$.

$$\lambda \binom{v-j}{t-j} = \sum_{T: J \subseteq T} \sum_{B: T \subseteq B} 1 = \sum_{B: J \subseteq B} \sum_{T: J \subseteq T \subseteq B} 1 = \sum_{B: J \subseteq B} \binom{k-j}{t-j} = \lambda(J) \binom{k-j}{t-j}.$$

This implies that $\lambda(J)$ is independent of the choice of J as long as j is fixed. We summarize our observations in the following theorem.

Theorem 22.5 (Arithmetic conditions). *An $S_\lambda(t, k, v)$ can exist only if*

$$\lambda \binom{v-j}{t-j} \equiv 0 \pmod{\binom{k-j}{t-j}},$$

for all $j = 0, \dots, t-1$.

Corollary 22.6. *An $S_1(2, k, v)$ can only exist if*

$$\begin{aligned} v(v-1) &\equiv 0 \pmod{k(k-1)} \\ v-1 &\equiv 0 \pmod{k-1}. \end{aligned}$$

Example 46. If $k = 3$ then $v-1 \equiv 0 \pmod{2}$ implies that v is odd and from the first relation we get that $v(v-1)$ is divisible by 6. Both together imply that $v \equiv 1, 3 \pmod{6}$.

Systems of the form $S(2, 3, v)$ are called *Steiner triple systems* which will be written as $STS(v)$.

Corollary 22.7. *Given $v \in \mathbb{N}$, if a Steiner Triple System $STS(v)$ exists, then $v \equiv 1, 3 \pmod{6}$.*

It turns out that this condition is also sufficient for the existence. We will dedicate part of the next lecture to an in depth analysis of $STS(v)$, but for now we will focus on another result for set systems: *Fisher's inequality*.

Theorem 22.8 (Fisher's inequality). *If an $S_\lambda(t, k, v)$ exists for $t \geq 2$, then the number of blocks exceeds the number of points, i.e. $b \geq v$.*

Proof. Let A be the incidence matrix with v rows and b columns:

$$A_{p,B} = \begin{cases} 1, & p \in B \\ 0, & \text{otherwise} \end{cases}.$$

We look at the $v \times v$ matrix given by AA^T . Then

$$(AA^T)_{p,q} = \#(B : p \in B \text{ and } q \in B) = \begin{cases} \lambda_1, & \text{if } p \neq q, \\ \lambda_2, & \text{if } p = q. \end{cases}$$

So AA^T has λ_1 on the diagonal and else it has λ_2 as entries. We observe that $\lambda_1 > \lambda_2$.

Next we will show that AA^T is regular, i.e., it has a non-vanishing determinant and its rank is v . This then implies that $\text{rank}(A) \geq v$ and finally

$$b \geq \text{rank}(A) \geq v.$$

There is several ways to check the regularity of AA^T , one being the Gauß elimination procedure and verify that $\det(AA^T) = (\mu + v\lambda_2)\mu^{v-1} > 0$ for $\mu = \lambda_1 - \lambda_2$.

Another way is to write $AA^T = \lambda_2 J + \mu I$, where J is the all-one matrix and I the identity. The claim now is that AA^T is positive definite. To this extent let $x \neq 0$ then

$$xAA^T x^T = x(\lambda_2 J)x^T + x(\mu I)x^T = \lambda_2 \sum_{i,j} x_i x_j + \mu \sum x_i^2 = \lambda_2 \left(\sum x_i \right)^2 + \mu \sum x_i^2 > 0.$$

□

Corollary 22.9. *Steiner systems $S(2, 6, 16)$, $S(2, 6, 21)$ and $S_3(2, 10, 25)$ do not exist even though the parameters fulfill the arithmetic condition.*

22.3 Steiner triple systems

We start this section with an old problem known as *Kirkman's schoolgirls problem* dating back to 1850.

Kirkman's Problem: 15 schoolgirls walk each day in 5 groups of 3. Arrange the girls walk for a week such that each pair of girls walks together in a group just once.

Thinking of set systems we have a groundset of size $v = 15$ and blocks of size $k = 3$, and each pair is in exactly one block so we look at $S_1(2, 3, 15)$. By the arithmetic conditions we get $b = \lambda \binom{v}{2} / \binom{k}{2} = 35$ many blocks. So we get $5 \cdot 7$ blocks. Our quest is then to give an $STS(15)$ with the additional property that $\mathcal{B} = \mathcal{B}_1 \dot{\cup} \dots \dot{\cup} \mathcal{B}_7$ with \mathcal{B}_i being an $S(1, 3, 15)$: every girl belongs to exactly one block.

This condition is often summarised by saying that we want the design to be *resolvable*.

Example 47 (Resolvable $STS(9)$). We need $b = \frac{9 \cdot 8}{3 \cdot 2} = 12$ blocks. Arrange the 9 points on a (3×3) -grid. Then the rows and the columns form 6 blocks. The remaining six blocks are the diagonals in a "Sarrus style" as given by [Figure 22.4](#). Then every pair of

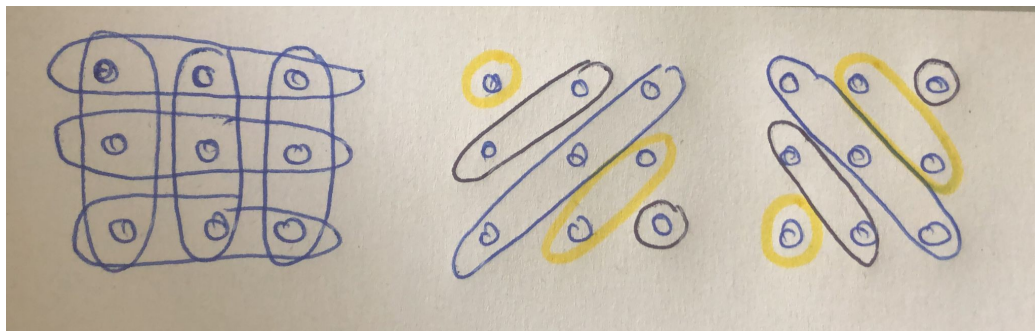


Figure 22.4: The four different partitions of blocks.

vertices is part of exactly one block and we can regroup the blocks into four partitions of the groundset.

Steiner Triple Systems and Kirkman's problem

Last lecture we introduced designs and Steiner Triple Systems (STS) – $S_1(2, 3, v)$ designs – as a special case thereof. We finished the lecture by mentioning Kirkman's problem which we will discuss more thoroughly today. For readability we restate the problem.

Kirkman's Problem: 15 schoolgirls walk each day in 5 groups of 3. Arrange the girls walk for a week such that each pair of girls walks together in a group just once.

We have already seen that Kirkman asks for a $S(2, 3, 15)$ (Steiner triple system on 15 points) which is resolvable, i.e., the set of blocks admits a partition $\mathcal{B} = \mathcal{B}_1 \dot{\cup} \dots \dot{\cup} \mathcal{B}_7$ such that each \mathcal{B}_i forms a $S(1, 3, 15)$: every girl belongs to exactly one block.

Solution to Kirkman's problem. We already know that there is an $S(3, 4, 2^n)$ with points in \mathbb{F}_2^n and blocks $\{x, y, z, x + y + z\}$ as well as residual designs $S(2, 3, 2^n - 1)$. In particular we have an $S(3, 4, 16)$.

Fix $0 \in \mathbb{F}_2^4$ and consider the residual design from last lecture: only look at blocks containing 0 and remove it from the blocks, that is we get an $S(2, 3, 15) = \text{STS}(15)$. So our points are in \mathbb{F}_2^4 and the blocks are of type $\{x, y, x + y\}$. We are left to prove that this design is *resolvable*. To this extent we restrict our attention to the 7 points p_0, \dots, p_6 with 4th coordinate 0

p_0	p_1	p_2	p_3	p_4	p_5	p_6
1	0	0	1	0	1	1
0	1	0	1	1	1	0
0	0	1	0	1	1	1
0	0	0	0	0	0	0

If B is a block containing two of these points (p_i, p_j) , then the third point $p_i + p_j$ also has 4th coordinate 0. Hence the 7 points form a $S(2, 3, 7)$ (this is the projective plane of order 2, compare the example from the previous lecture). The blocks of $S(2, 3, 7)$ are $B_i := \{p_i, p_{i+1}, p_{i+3}\}$ with $i = 0, \dots, 6$ (addition of indices is taken modulo 7).

Remark. The construction of the $S(2, 3, 7)$ above shows that the system is *cyclic*, this means that there is an action of the cyclic group on the points such that the blocks are a collection of orbits of the induced group action on k -sets.

Back to the $STS(15)$; the remaining eight points of the groundset can be labeled as $q_i := p_i + \mathbb{1}$ together with the all-one vector $\mathbb{1}$. We define four additional groups of 7 blocks: $B_i^1 := \{p_i, q_{i+1}, q_{i+3}\}$, and $B_i^2 := \{q_i, p_{i+1}, q_{i+3}\}$, and $B_i^3 := \{q_i, q_{i+1}, p_{i+3}\}$, and $\bar{B}_i = \{p_i, q_i, \mathbb{1}\}$. All these blocks belong to the $STS(15)$ because they are of the type $\{x, y, x + y\}$. In total this yields $5 \cdot 7 = 35$ blocks, i.e., all the blocks of the $STS(15)$.

For $i = 0, \dots, 6$ let

$$\mathcal{B}_i := \{B_i, B_{i+4}^1, B_{i+1}^2, B_{i+2}^3, \bar{B}_{i+6}\}.$$

We easily verify that \mathcal{B}_0 is an $S(1, 3, 15)$ by checking that every point is covered exactly once. And finally conclude that this is a solution to *Kirkman's problem*.

23.1 Existence of Steiner Triple Systems

Using the insights gained from last lecture on arithmetic conditions we already know that $n \equiv 1, 3 \pmod{6}$ is necessary for the existence of an $STS(n)$. It has been shown that this necessary condition is also sufficient. We only show the easy ‘half’ of this.

Theorem 23.1. *If $n \equiv 3 \pmod{6}$ then there is a $STS(n)$.*

Proof. We can write $n = 6s + 3 = 3(2s + 1)$ for some s . Let $m := 2s + 1$ and $P = \{a_i, b_i, c_i \mid i \in \mathbb{Z}_m\}$. Next we define the blocks \mathcal{B} coming in four flavours namely

- (i) set of all (a_i, b_i, c_i) ,
- (ii) set of all (a_i, a_j, b_k) , where $i + j = 2k$ in \mathbb{Z}_m ,
- (iii) set of all (b_i, b_j, c_k) , where $i + j = 2k$ in \mathbb{Z}_m ,
- (iv) set of all (c_i, c_j, a_k) , where $i + j = 2k$ in \mathbb{Z}_m .

It is easily seen that every pair of elements is covered by some unique type of blocks. For example (a_3, b_3) is covered by a type (i) block while (a_2, b_7) must be covered by a type (ii) block and (b_3, b_6) must be covered by a type (iii) block. We claim, that every pair of $\{i, j, k\}$ uniquely determines the third element, this then implies that every pair of points is covered by exactly one block. Now given $\{i, k\}$ or $\{j, k\}$ we get a unique j or i respectively by looking at $2k - i$ or $2k - j$. The interesting case is when we are given $\{i, j\}$ then we know $2k$ but we have to show that we can extract k uniquely (the preimage under $2x$ is unique) which holds true if 2 is a unit in \mathbb{Z}_m so that we can take its inverse.

Claim: the map $x \mapsto 2x$ in \mathbb{Z}_m is a bijection. Let $x, y \in \mathbb{Z}_m$, let $2x = 2y \pmod{m}$ and suppose $x > y$, then $2x = 2y + m$ in \mathbb{Z} which is impossible since $2x$ is even but $2y + m$ is odd. This concludes the proof. \square

23.2 An algebraic construction of designs

Let q be a primepower and consider $X := \mathbb{F}_q \cup \{\infty\}$, this will be our ground set. This set can be thought of as a finite projective line. Then

$$\mathrm{PGL}(2, q) = \{x \mapsto \frac{ax+b}{cx+d} \mid a, b, c, d \in \mathbb{F}_q, ad-bc \neq 0\}$$

is a group acting on X (it is known as a group of Möbius transformations). To deal with ∞ which is not an element of the field \mathbb{F}_q We set some rules:

- $a \neq 0 \implies a \cdot \infty + b = \infty$,
- $0 \cdot \infty = 0$ and $\frac{0}{0} = 1$,
- $\frac{a\infty}{c\infty} = \frac{a}{c}$,
- $\frac{a}{0} = \infty$ and $\frac{a}{\infty} = 0$.

Remark. Recall that $\mathrm{GL}(2, q) = \left\{ \begin{bmatrix} a & b \\ c & d \end{bmatrix} \mid a, b, c, d \in \mathbb{F}_q, ad-bc \neq 0 \right\}$ is acting on \mathbb{F}_q^2 via

$$\begin{bmatrix} x_1 \\ x_2 \end{bmatrix} \mapsto \begin{bmatrix} a & b \\ c & d \end{bmatrix} \begin{bmatrix} x_1 \\ x_2 \end{bmatrix} = \begin{bmatrix} ax_1 + bx_2 \\ cx_1 + dx_2 \end{bmatrix}.$$

If we look at 1-dimensional subspaces of \mathbb{F}_q^2 as points, we can switch to *homogeneous coordinates*: that is for a subspace

$$U_{x,y} := \left\{ \lambda \begin{bmatrix} x \\ y \end{bmatrix} \mid \lambda \in \mathbb{F}_q \right\}$$

with given $x, y \in \mathbb{F}_q$ we can choose the representant for the vectorspace to have a 1 as second entry, i.e. $\{\lambda \begin{bmatrix} x \\ y \end{bmatrix} \mid \lambda \in \mathbb{F}_q\} = \{\lambda \begin{bmatrix} xy^{-1} \\ 1 \end{bmatrix} \mid \lambda \in \mathbb{F}_q\}$ as long as $y \neq 0$. Thus every subspace except for the one spanned by $\begin{bmatrix} 1 \\ 0 \end{bmatrix}$ can be uniquely identified with a single point xy^{-1} in \mathbb{F}_q . This is the reason why we identify $\begin{bmatrix} 1 \\ 0 \end{bmatrix}$ with ∞ , going hand in hand with our new rules: $\frac{1}{0} = \infty$.

Proposition 23.2. *The cardinality of $\mathrm{PGL}(2, q)$ is $q^3 - q = (q+1)q(q-1)$.*

Proof. First note that

$$|\mathrm{GL}(2, q)| = \#(\text{pairs of lin. ind. vectors in } \mathbb{F}_q^2) = (q^2 - 1)(q^2 - q).$$

We also note that all matrices of the form $\begin{bmatrix} a & 0 \\ 0 & a \end{bmatrix}$ map to the identity in PGL and there are $(q-1)$ such maps. In general two matrices that differ by some multiplicative factor

are mapped to the same map in $\text{PGL}(2, q)$. This observation is easily extended to prove that the (quotient)map $\text{GL}(2, q) \rightarrow \text{PGL}(2, q)$ has Kernel of size $(q - 1)$, which proves

$$|\text{PGL}(2, q)| = \frac{|\text{GL}(2, q)|}{q - 1} = (q + 1)(q^2 - q).$$

□

Next we look at a special property of the projective general linear group.

Proposition 23.3. *The group $\text{PGL}(2, q)$ acts sharply transitive on ordered triples of distinct elements of $X := \mathbb{F}_q \cup \{\infty\}$.*

Acting sharply transitive on ordered triples means that for any two triples $(a, b, c), (a', b', c')$ of distinct elements ($a \neq b \neq c$ and $a' \neq b' \neq c'$) there is exactly one $A \in \text{PGL}(2, q)$ mapping (a, b, c) to (a', b', c') . The term *sharply* imposes the uniqueness on A .

Proof. Let $G := \text{PGL}(2, q)$, then the stabilizer $G_\infty := \{g \in G \mid g(\infty) = \infty\}$ of ∞ in G is given by

$$G_\infty = \{x \mapsto ax + b, a \neq 0\},$$

which is an easy conclusion after thorough examination of our new rules for ∞ . In G_∞ only the identity $x \mapsto x$ maps $0 \mapsto 0$, $1 \mapsto 1$ and $\infty \mapsto \infty$. So the stabilizer of $(\infty, 0, 1)$ under the action of G on ordered triples is the identity. Moreover,

$$|\text{orbit}(T)| \cdot |\text{Stab}(T)| = |G| = (q + 1)q(q - 1),$$

for ordered triples T . Since for $(\infty, 0, 1)$ the stabilizer contains only the identity thus $|\text{Stab}((\infty, 0, 1))| = 1$ we deduce that $\text{orbit}((\infty, 0, 1))$ consists of all ordered triples of distinct elements. □

We conclude this section with a rather technical theorem.

Theorem 23.4. *Let q be a prime power, then this implies that $S(3, q + 1, q^n + 1)$ exists.*

Proof. There exists a field \mathbb{F}_q of order q and an extension field \mathbb{F}_{q^n} whose elements are the polynomials of degree $< n$ with coefficients in \mathbb{F}_q . Then $\mathbb{F}_q \subseteq \mathbb{F}_{q^n}$ is a subfield consisting of the constant polynomials.

This implies that $\text{PGL}(2, q) < \text{PGL}(2, q^n) := \Gamma$ is a subgroup. Let $X := \mathbb{F}_{q^n} \cup \{\infty\}$ and define $B := \mathbb{F}_q \cup \{\infty\}$, this is the initial block, its size is $q + 1$. We know that Γ acts transitively on ordered triples of distinct elements which implies that $\text{orbit}_\Gamma(B)$ is a 3-design for some λ this is because the number of appearances of an ordered triple in the orbit is independent of the triple: Every triple can be found in an element of the orbit, since $0, 1, \infty$ belong to B and Γ is 3-transitive. Consider all the blocks containing $(0, 1, \infty)$ and a unique $g \in \Gamma$ which maps $(0, 1, \infty)$ to (a, b, c) . Now g maps each block containing $(0, 1, \infty)$ to a block containing (a, b, c) .

It remains to verify that $\lambda = 1$.

From the choice of B it follows that $\text{Stab}_\Gamma(B)$ contains $\text{PGL}(2, q)$. Hence,

$$|\text{orbit}_\Gamma(B)| = \frac{|\Gamma|}{|\text{Stab}_\Gamma(B)|} \leq \frac{(q^n + 1)q^n(q^n - 1)}{(q + 1)q(q - 1)}.$$

Since we know that the elements of the orbit form the blocks of the design we can use our arithmetic conditions for the number of blocks $b = |\text{orbit}_\Gamma(B)|$. That is

$$|\text{orbit}_\Gamma(B)| = b = \lambda \frac{\binom{q^n+1}{3}}{\binom{q+1}{3}} = \lambda \frac{(q^n + 1)q^n(q^n - 1)}{(q + 1)q(q - 1)},$$

which with our previous inequality yields $\lambda = 1$. □

After all these technicalities let's get back to the fundamental question about the existence of Steiner systems. In the case of Steiner Triple Systems the arithmetic conditions are precisely the conditions that characterise the existence. In 2014 Keevash has proven the following very general existence result.

Theorem 23.5. *For given λ, t, k there exists some $v_0(\lambda, t, k)$ such that for every $v \geq v_0$ if λ, t, k, v satisfy the arithmetic conditions, then there exists an $S_\lambda(t, k, v)$.*

Remark. This implies that for each fixed λ, t, k there are only finitely many v for which one needs to check existence since existence is guaranteed as long as v is "big enough".

Möbius Inversion

24.1 The incidence algebra of a poset

Let $P = (X, \leq)$ be a poset and \mathbb{F} be a field. The set of all functions $F : X \times X \rightarrow \mathbb{F}$ with the property that $F(x, y) = 0$ for all x, y with $x \not\leq y$ is called the *incidence algebra* of poset P . The incidence algebra is equipped with two operations:

$$(F + G)(x, y) = F(x, y) + G(x, y) \quad (\text{pointwise addition})$$

$$(F \cdot G)(x, z) = \sum_{y: x \leq y \leq z} F(x, y)G(y, z) \quad (\text{convolution})$$

Proposition 24.1. *The incidence algebra together with pointwise addition and convolution is a ring with 0 and 1.*

Proof. The zero with respect to addition is the constant 0 map. The neutral element with respect to convolution maps all pairs (x, x) to 1 and all the other pairs to 0.

Let L be a linear extension of P , i.e., $L = (x_1, \dots, x_n)$ is a permutation of the set X such that $x_i < x_j \implies i < j$. Having fixed L we can write an element F of the incidence algebra as an upper triangular matrix $M_F = (F(x_i, x_j))_{i, j \in [n]}$, see Figure 24.1. Note that

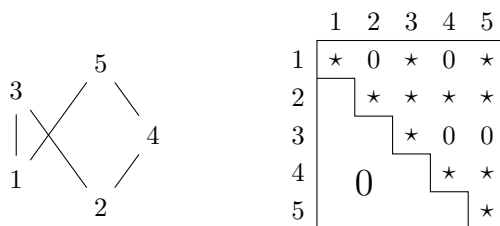


Figure 24.1: A poset with implied linear extension on the left hand side and the corresponding matrix on the right hand side

convolution corresponds to matrix multiplication and the one of the incidence algebra to the identity matrix. We claim that F has an inverse if and only if $F(x, x) \neq 0$ for all $x \in X$: This is easy to see by a determinant argument. We can, however, calculate the inverse explicitly. We need $G \cdot F = \text{id}$ for some G and therefore

$$F(x, x)G(x, x) = 1 \iff G(x, x) = \frac{1}{F(x, x)}$$

For $x \neq z$ we further need

$$0 = (G \cdot F)(x, z) = \sum_{y: x \leq y \leq z} G(x, y)F(y, z)$$

If we solve these by increasing differences in the indices of the linear extension, we know all summands on the right hand side but $y = z$ and therefore get

$$G(x, z) = \frac{-1}{F(z, z)} \sum_{y: x \leq y < z} G(x, y)F(y, z)$$

□

24.2 Zeta function and properties of P

Definition 24.2. The *zeta function* of a poset P is given by

$$z(x, y) = \begin{cases} 1 & x \leq y, \\ 0 & \text{otherwise.} \end{cases}$$

We immediately get

$$\begin{aligned} z^2(x, z) &= \sum_{y: x \leq y \leq z} z(x, y)z(y, z) = \sum_{y: x \leq y \leq z} 1 = \text{size of the interval } [x, z] \text{ in } P \\ &= \#(3\text{-element multichains from } x \text{ to } z \text{ in } P) \end{aligned}$$

and

$$z^k(x, z) = \sum_{x=y_0 \leq y_1 \leq \dots \leq y_k=z} 1 = \#(k+1\text{-element multichains from } x \text{ to } z \text{ in } P)$$

We further have

$$\begin{aligned} (z-1)(x, y) &= \begin{cases} 1 & x < y, \\ 0 & \text{otherwise.} \end{cases} \\ (z-1)^k(x, y) &= \#(k\text{-chains from } x \text{ to } y \text{ in } P) \end{aligned}$$

and

$$\begin{aligned} \#(\text{chains}) &= \left[\sum_{k \geq 0} (z-1)^k \right] = \frac{1}{1 - (z-1)} \\ &= (2-z)^{-1} \end{aligned}$$

24.3 Möbius inversion

Definition 24.3. Let Z be the matrix corresponding to the zeta function of P . Let $M = (\mu(x, y))$ be the inverse of Z . The function μ is called the *Möbius function* of P .

We observe that

$$\sum_{y: x \leq y \leq z} \mu(x, y) Z(y, z) = \delta_{x=z}$$

Hence:

$$(M_1) \quad \mu(x, x) = 1 \text{ for all } x \in X$$

$$(M_2) \quad \mu(x, z) = -\sum_{y: x \leq y < z} \mu(x, y) \text{ if } x < z$$

$$(M_3) \quad \mu(x, z) = 0 \text{ if } x \not\leq z$$

Theorem 24.4 (Möbius Inversion). For any two functions $f_=: f_{\leq} : X \rightarrow \mathbb{F}$

$$f_{\leq}(y) = \sum_{x \leq y} f_=(x) \iff f_=(y) = \sum_{x \leq y} f_{\leq}(x) \mu(x, y)$$

Proof. Consider $f_=: f_{\leq}$ as row vectors:

$$f_{\leq} = f_=: \cdot Z \xLeftrightarrow{ZM=1} f_{\leq} \cdot M = f_=:$$

□

24.4 Computing Möbius functions

24.4.1 Chains

We get

- | | |
|---|---|
| 6

5

4

3

2

1 | <ul style="list-style-type: none"> • $\mu(a, a) = 1$, this follows from (M_1). • $\mu(a, a+1) = -1$, this follows from (M_2) and $\mu(a, a) = 1$. • $\mu(a, a+2) = 0$, this follows from (M_2) and the previous items. • $\mu(a, a+k) = 0$ for all $k \geq 2$ |
|---|---|

By taking \mathbb{N} as chain and $f, g : \mathbb{N} \rightarrow \mathbb{F}$ we therefore get the following corollary of Möbius Inversion:

$$g(n) = \sum_{i=1}^n f(i) \iff f(n) = g(n) - g(n-1)$$

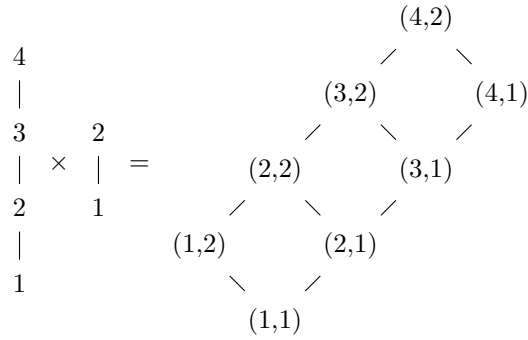
24.4.2 Products

Let $P = (X_P, \leq_P)$ and $Q = (X_Q, \leq_Q)$ be posets. We define

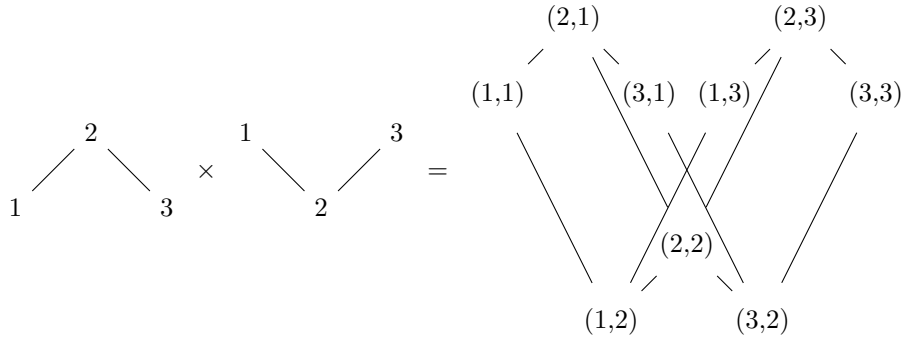
$$P \times Q := (X_P \times X_Q, (x_1, x_2) \leq_{P \times Q} (y_1, y_2) \iff x_1 \leq_P y_1, x_2 \leq_Q y_2)$$

Example 48. Here are some examples of products of posets

- Here is a product of two chains of length 4 and 2 respectively:



- Here is a product of two more complex posets:



- Here is the construction of the boolean lattice as product of 2-chains:

$$\underbrace{\begin{array}{c} 2 \\ | \\ 1 \end{array} \times \begin{array}{c} 2 \\ | \\ 1 \end{array} \times \cdots \times \begin{array}{c} 2 \\ | \\ 1 \end{array}}_{n \text{ factors}} = B_n$$

Proposition 24.5. *The Möbius function of $P \times Q$ is given by*

$$\mu_{P \times Q}((x_1, x_2), (y_1, y_2)) = \mu_P(x_1, y_1) \mu_Q(x_2, y_2)$$

Proof. $(M_1) \checkmark$. $(M_3) \checkmark$. For (M_2) we need a little calculation. Let $(x_1, x_2) < (z_1, z_2)$

$$\begin{aligned} \sum_{(x_1, x_2) \leq (y_1, y_2) \leq (z_1, z_2)} \mu((x_1, x_2), (y_1, y_2)) &= \sum_{\substack{x_1 \leq y_1 \leq z_1 \\ x_2 \leq y_2 \leq z_2}} \mu_P(x_1, y_1) \mu_Q(x_2, y_2) = \\ \left(\sum_{x_1 \leq y_1 \leq z_1} \mu_P(x_1, y_1) \right) \left(\sum_{x_2 \leq y_2 \leq z_2} \mu_Q(x_2, y_2) \right) &= 0, \quad \text{since } x_1 < z_1 \text{ or } x_2 < z_2. \end{aligned}$$

□

24.4.3 Boolean lattices

For a 2-element chain we have $\mu(0, 0) = \mu(1, 1) = 1$ and $\mu(0, 1) = -1$ and $\mu(1, 0) = 0$. In the following we think of elements A, B of \mathcal{B}_n as sets or characteristic vectors interchangeably. Using that \mathcal{B}_n is a power of 2-chains we obtain:

$$\mu(A, B) = \prod_i \mu(A_i, B_i) = \begin{cases} \prod (-1)^{|B_i - A_i|} = (-1)^{|B - A|} & A \subseteq B \\ 0 & \text{otherwise} \end{cases}$$

24.5 Möbius inversion on the Boolean lattice

For the Boolean lattice we get

$$N_{\geq}(A) = \sum_{B \supseteq A} N(B) \iff N(A) = \sum_{B \supseteq A} (-1)^{|B - A|} N_{\geq}(B)$$

Remark. In particular this yields

$$N(\emptyset) = \sum_B (-1)^{|B|} N_{\geq}(B)$$

which implies the inclusion-exclusion-formula.

To exemplify the connection we again derive a formula for the number of derangements on $[n]$.

Example 49. We first define $\text{fix}(\pi) = \{i : \pi(i) = i\}$. We further define

$$N(A) = \#(\pi : \text{fix}(\pi) = A) \quad \text{and} \quad N_{\geq}(A) = \#(\pi : \text{fix}(\pi) \supseteq A).$$

It is easy to see that $N_{\geq}(A) = (n - |A|)!$. It follows that

$$\#(\text{derangements}) = N(\emptyset) = \sum_B (-1)^{|B|} (n - |B|)! = \sum_k \binom{n}{k} (-1)^k (n - k)! = n! \sum_{k=0}^n \frac{(-1)^k}{k!}.$$

24.6 An algorithmic application of Möbius inversion

In this section we aim for an *exact exponential algorithm* for the k -cover problem. As input we get a family \mathcal{F} of subsets of N with $|N| = n$ and want to know how many k -covers exist, that is how many k -subsets $\{F_1, \dots, F_k\}$ of \mathcal{F} with $N = \bigcup F_i$ exist.

Remark. This counting problem is #P-complete and the corresponding existence problem is NP-complete.

A trivial algorithm consists of checking each k -subset of \mathcal{F} . Each such check can be done in $\mathcal{O}(n \cdot k)$. Overall the complexity of this algorithm is $n \cdot k \cdot \binom{|\mathcal{F}|}{k} \sim n|\mathcal{F}|^k$ but the size of the family \mathcal{F} can be large, in fact as large as 2^n . In such a case the complexity of the algorithm is in $\mathcal{O}^*((2^n)^k)$. If k is large as well this yields $\mathcal{O}^*(2^{n^2})$.

In this lecture we will see that counting k -covers can be done in $\mathcal{O}^*(2^n)$ by *fast zeta transform*, a technique relying on the Möbius function, where $\mathcal{O}^*(f(n))$ denotes a function of the form $p(n)f(n)$ for some polynomial p .

Let N be some groundset with $|N| = n$ and let $\mathcal{F} \subset 2^N$ be a family of subsets of N . A k -cover is a subset $\{F_1, \dots, F_k\} \subset \mathcal{F}$ with $N = \bigcup_{i=1}^k F_i$.

Let $X \subseteq N$, then we denote by

$$N_{\geq}(X) := \#\left((F_1, \dots, F_k) \text{ such that } \bigcup F_i \cap X = \emptyset\right).$$

Further let

$$A(X) := \#\{F \in \mathcal{F} \text{ with } F \cap X = \emptyset\}.$$

We observe that $N_{\geq}(X) = A^k(X)$, since the former is just a k -fold choice of $F \in \mathcal{F}$ having no intersection with X .

The key claim is then as follows.

Lemma 24.6. *The value of $A(X)$ can be computed for all $X \subseteq N$ in overall $\mathcal{O}^*(2^n)$ time.*

We begin by describing how to use **Lemma 24.6**. Define

$$N_{=}(X) := \#\{k\text{-tuples } (F_1, \dots, F_k) \text{ such that } \bigcup F_i = \overline{X}\}.$$

From the definitions we get

$$N_{\geq}(X) = \sum_{Y: X \subseteq Y} N_{=}(Y) \quad \text{and} \quad N_{=}(\emptyset) = \#\{k\text{-tuples which are } k\text{-covers}\}.$$

As our notation already suggests we will use Möbius inversion to derive an expression of $N_{=}(\emptyset)$ in terms of $N_{\geq}(X)$. Using our knowledge about the Möbius function of the Boolean lattice and in particular $\mu(\emptyset, X) = (-1)^{|X|}$ we get:

$$N_{=}(\emptyset) = \sum_{X \subseteq N} (-1)^{|X|} N_{\geq}(X) = \sum_{X \subseteq N} (-1)^{|X|} A(X)^k. \quad (24.27)$$

This means in order to compute $N_=(\emptyset)$ it suffices to compute the values of $A(X)$ for all X . Assuming [Lemma 24.6](#) this can be done in $\mathcal{O}^*(2^n)$. The evaluation of each summand on the right side of [Equation 24.27](#) can be done in time polynomial in n whence the evaluation of the sum is in $\mathcal{O}^*(2^n)$. So we are left with proving [Lemma 24.6](#).

Proposition 24.7. *Let $f : 2^{[n]} \rightarrow \{0, 1\}$ be the characteristic function of \mathcal{F} . Then f can be computed in $\mathcal{O}^*(2^n)$ even if \mathcal{F} is implicitly given with a polynomial test.*

Remark. An example for such an implicitly given family would be: given a graph $G = (V, E)$ we define \mathcal{F} to be the family of independent sets. Then for each subset of vertices one can test in polynomial time whether this set vertices is an independent set, i.e. part of the family \mathcal{F} .

Proof. Just check for each of the 2^n subsets of N whether they belong to \mathcal{F} . By assumption the test only takes polynomial time so that the whole computation can be done in $\mathcal{O}^*(2^n)$. \square

Having computed f we get

$$A(X) = \sum_{Y \subseteq \bar{X}} f(Y).$$

For a given X this can be computed in $\mathcal{O}^*(2^n)$ since $|\bar{X}| \leq 2^n$. So we can naively compute $A(X)$ for all X which would need $2^n \mathcal{O}^*(2^n)$ computations which is unfortunately too much. We show next how to use the fast zeta transform to reduce the complexity of these computations to $\mathcal{O}^*(2^n)$.

Fast Zeta Transform:

Suppose that $f : N \rightarrow \mathbb{F}$ is given. We want to compute the function $g(X) = \sum_{Y: X \subseteq Y} f(Y)$ for every $X \subseteq N$ "efficiently".

Note that $g(X)$ needs $2^{n-|X|}$ values of f whence in total

$$\sum_X 2^{n-|X|} = \sum_X 2^{|\bar{X}|} = \sum_k \binom{n}{k} 2^k = (1+2)^n = 3^n.$$

This is already a slight computational improvement, but the basis for the exponential should be 2 and not 3.

Define $g_0(X) = f(X)$ and inductively set

$$g_i(X) := \begin{cases} g_{i-1}(X) + g_{i-1}(X \cup \{i\}) & i \notin X, \\ g_{i-1}(X) & \text{otherwise.} \end{cases}$$

Proposition 24.8. *For every $X \subseteq N$ it holds true that*

$$g_i(X) = \sum_{Y: X \subseteq Y \subseteq X \cup \{1, \dots, i\}} f(Y).$$

Proof. By induction on i . This is clear for $g_0 = f$. So assume it is true for $i - 1$. We distinguish two cases for X :

($i \notin X$) The idea is to split the sum defining g_i in two parts. The first has those Y with $i \notin Y$ and the second has the Y with $i \in Y$:

$$\begin{aligned} g_i(X) &= \sum_{Y: X \subseteq Y \subseteq X \cup \{1, \dots, i\}} f(Y) = \sum_{X \subseteq Y \subseteq X \cup \{1, \dots, i-1\}} f(Y) + \sum_{X+i \subseteq Y \subseteq (X+i) \cup \{1, \dots, i-1\}} f(Y) \\ &= g_{i-1}(X) + g_{i-1}(X+i), \end{aligned}$$

($i \in X$) It is clear that in this case $X \subseteq Y$ implies $i \in Y$ and thus the $Y \subseteq N$ satisfying $X \subseteq Y \subseteq X \cup \{1, \dots, i-1\}$ are the same as those satisfying $X \subseteq Y \subseteq X \cup \{1, \dots, i\}$, i.e., $g_i(X) = g_{i-1}(X)$. \square

Clearly $g_n(X) = g(X)$. The proposition shows that when g_{i-1} is known we can compute g_i with a constant number of operations for each X , hence, overall in $\mathcal{O}(2^n)$ complexity. Now $g_n = g$ can be computed in n rounds where each round is in $\mathcal{O}(2^n)$, hence, g_n is computed in $\mathcal{O}^*(2^n)$.

To actually prove [Lemma 24.6](#) it remains to show that $A(\cdot)$ can be computed using the fast zeta transform. We leave the details as an exercise.

Catalan Families

25.1 Catalan families and bijections

We have already seen *Catalan numbers* in Lectures 8 and 9. There we used the interpretation of the Catalan number C_n as the number of rooted binary trees on n nodes. In the exercises we have seen that they also count the number of triangulations of a convex $(n + 2)$ -gon. The first six Catalan numbers are

$$C_1 = 1, \quad C_2 = 2, \quad C_3 = 5, \quad C_4 = 14, \quad C_5 = 42, \quad C_6 = 132.$$

Using generating functions we found a closed formula for C_n :

$$C_n = \frac{1}{n+1} \binom{2n}{n}.$$

In this chapter we will look at several combinatorial families that are counted by Catalan numbers, we call them *Catalan families*. To show that two families are equinumerous we will give bijections between the families. In the case of Catalan families we can use triangulations of an $(n + 2)$ -gon as the initial family since we already know that they are counted by Catalan numbers.

Remark. There is a book by Richard Stanley from 2015 called *Catalan numbers* containing 214 different combinatorial interpretations of Catalan numbers all enumerated via letter combinations. We will start by looking at the families a, c, d, e, i .

The family (a) is given by the triangulations of $(n + 2)$ -gons.

Definition 25.1 (Catalan families a, c, d, e, i). The families are given as follows

- (a) triangulations of $(n + 2)$ -gons.
- (c) rooted binary trees on n vertices.
- (d) rooted full binary trees with $(n + 1)$ leaves.
- (e) rooted plane trees on $n + 1$ vertices.
- (i) Dyck paths of length n , i.e., paths from $(0, 0)$ to $(2n, 0)$ using diagonal up or down steps which never go below the x -axis.

Proposition 25.2 (Bijections between the families). *There are bijections between the families a, c, d, e, i .*

Proof. Here we give bijections for $c \leftrightarrow d$, $a \leftrightarrow d$, $e \leftrightarrow i$ and $d \leftrightarrow e$.

[$c \leftrightarrow d$] A rooted full binary tree T with $n + 1$ leaves has n non-leaf nodes, i.e. the inner nodes. Map T to the tree T' of non-leaf nodes. Now let T' be a rooted binary tree with n nodes. Each node could accommodate a left and a right descendant. Only $n - 1$ out of these $2n$ positions are occupied by the non-root nodes of T' . Map T' to the tree T where a leaf is added at each free descendant position of the original nodes. This yields a one-to-one correspondence between rooted binary trees on n nodes and rooted full binary trees with $n + 1$ leaves.

[$a \leftrightarrow d$] Let D be an $(n + 2)$ -gon with a marked edge e . Given a triangulation Δ of D we consider the interior dual graph Δ^* of Δ , then we delete the vertex of degree $n + 2$ from the dual. For each edge of D except e we add a leaf to the dual vertex of the incident triangle. This yields the green tree shown on the left of [Figure 25.1](#). The root of the tree is the unique vertex of degree 2, this is the dual of the triangle incident to e .

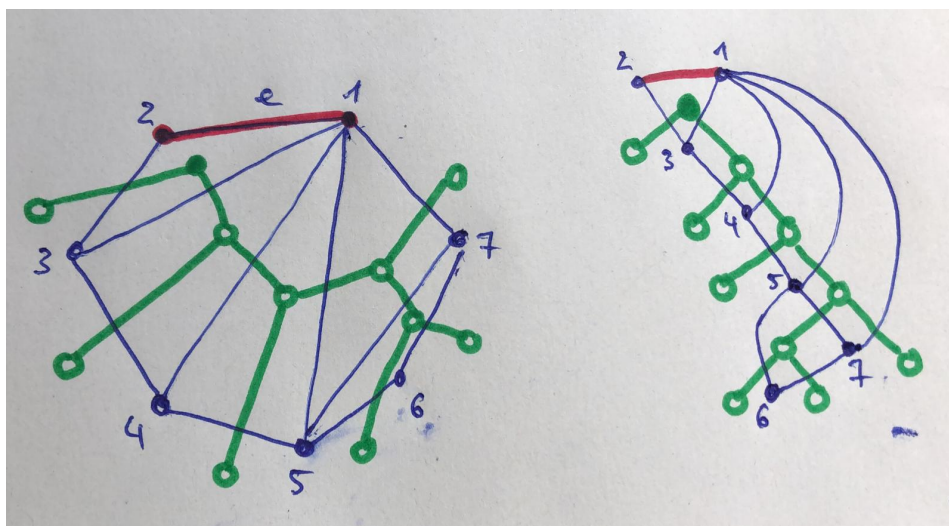


Figure 25.1: The left hand side shows Δ and the corresponding full binary dual tree. The right hand side shows how to obtain a triangulation from a full binary tree.

Conversely given a full binary rooted tree on $n + 1$ leaves we get a unique triangulation of an $n + 2$ -gon with a designated edge e , as illustrated in [Figure 25.1](#), by again taking the dual of the graph obtained by merging all leaves into a single vertex that is also made adjacent to the root.

[$e \leftrightarrow i$] Given a Dyck path think of adding glue on the bottom side of each step. Then push from left and right such that each edge is glued to its partner edge. This yields a tree as shown in [Figure 25.2](#). A more formal description would make each maximal horizontal segment at an integer coordinate below the path a node and define partners

as the pairing of a step $(a, k), (a + 1, k + 1)$ and step $(b, k + 1), (b + 1, k)$ such that between $a + 1$ and b the y -coordinate of the Dyck path is larger than k .

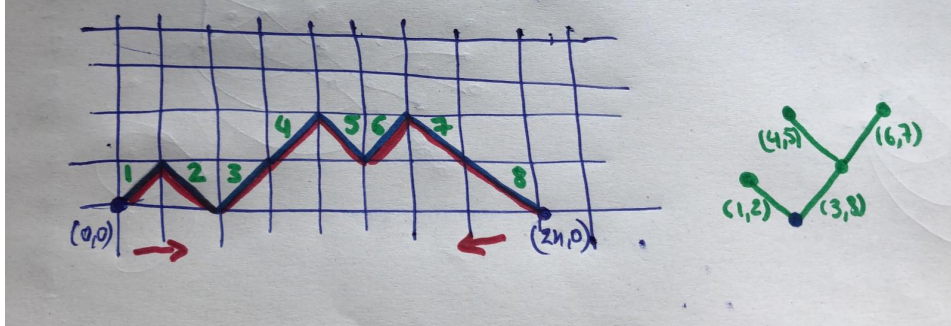


Figure 25.2: On the left we have a Dyck path of length 8 where the glue is marked as red on the lower side of the edges. The numbers next to the edges help to visualise which edges have been glued together to form the tree depicted on the right.

Conversely given a plane tree we get a Dyck path by walking around the tree starting from the root and take a step of slope $+1$ when going visiting a tree edge for the first time and a step of -1 at the second visit of an edge. See [Figure 25.3](#)

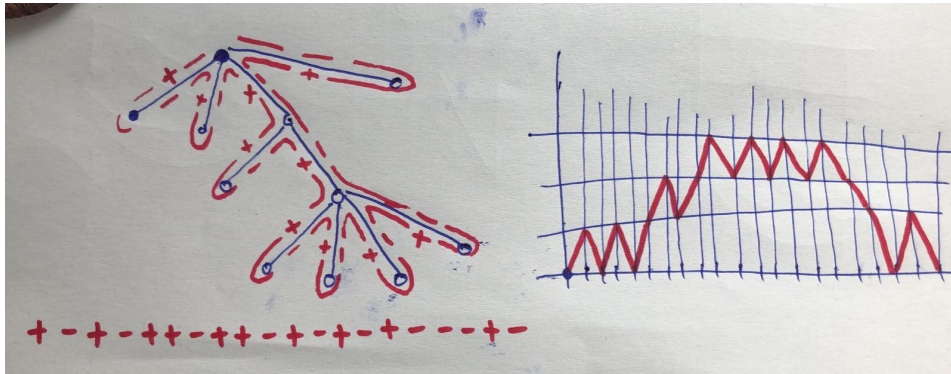


Figure 25.3: On the left we have a plane tree on 11 vertices where we mark the "up-step" with a $(+)$ and the "down-steps" with a $(-)$. We can use these steps to produce the Dyck path on the right.

$[d \leftrightarrow e]$ Given a rooted plane tree T on $n + 1$ vertices we will draw it as an alternating tree, that is we draw all of its vertices on the x -axis and count them through by $0, \dots, n$ from left to right. We start at the root and look at its subtrees, if the first subtree has size k we draw an edge from vertex 0 (the root) to k , and then if the second subtree has size j we draw an edge from 0 to $k + j$ so we count j vertices starting from k . If we are done we continue to look at the subtrees say the subtree of size k . If its first subtree of size m and there is a second subtree, then we draw an edge from k to 1, i.e., the root of the first subtree, and a second edge to $0 + m$ for the second subtree. If the second subtree has ℓ nodes, then either $k = m + \ell + 1$ or there is a third subtree and

we add an edge to $0 + m + \ell$. The full drawing is obtained by iterating this, such that the edge to the root of a subtree always spans the interval where the vertices of the subtree will be placed.

An example is given by the following figure.

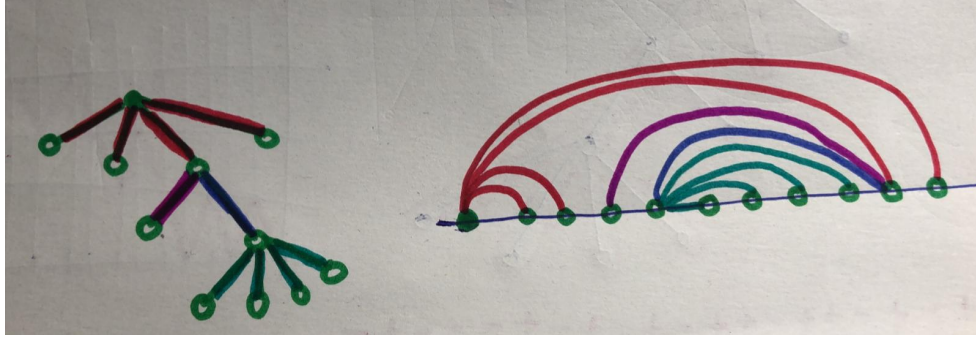


Figure 25.4: On the left we have a plane tree where by taking care of the subtree structures we get the righthand embedding of the tree (known as an alternating tree).

During this construction we can trace whether a vertex has been connected via an edge going to the right or going to the left. Color the root blue, and then inductively color vertices red if they have been connected using a right edge and blue if they have been connected using an edge to the left, as for our previous example these colors have been added in [Figure 25.5](#).

To obtain a full binary tree on $(n + 1)$ leaves, draw all the colored vertices on the x -axis in the same order as for the alternating tree, they will be the leaves. For each edge draw a wedge consisting of an increasing segment of slope $+1$ and a decreasing segment of slope -1 connecting the two nodes, i.e, if the nodes are at $n_l = (a, 0)$ and $n_r = (b, 0)$ with $a < b$, then the wedge consists of the segment n_l, t and the segment t, n_r , where $t = (\frac{a+b}{2}, \frac{b-a}{2})$. Superinposing all these wedges yields a tree, the inner nodes of the tree are the tips of the wedges. This construction is illustrated in [Figure 25.5](#)

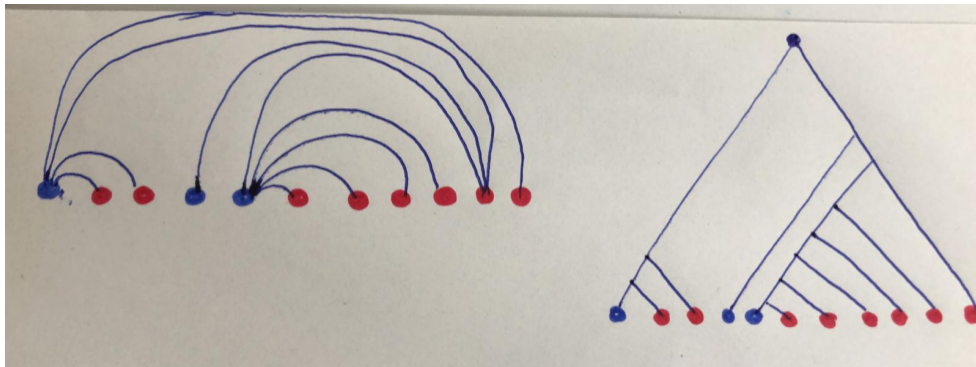


Figure 25.5: On the left we have an alternating tree with correspondingly colored vertices. On the right we get the corresponding full binary tree with $(n + 1)$ -leaves.

The converse is given by converting inner nodes into edges connecting the leftmost

and the rightmost descendent leaf. This makes an alternating tree and hence a plane tree. \square

Next we look at five more families.

Definition 25.3 (Catalan families aaa, ddd, ii, pp, ℓ). The families are given as follows

(aaa) linear extensions of the $2 \times n$ poset

(ddd) semi-orders with n elements.

(ii) permutations $\pi \in S_n$ that can be sorted on a stack.

(pp) non-crossing partitions of $[n]$.

(ℓ) pairs of internally disjoint lattice paths of length $n + 1$ starting in $(0, 0)$, taking only steps upwards and to the right and ending at the same point.

We first have to define some of these objects.

The poset $\mathbf{a} \times \mathbf{b}$ is the product of a chain with a elements and a chain with b elements, it has $a \cdot b$ elements and a grid like diagram.

A *semi-order* is a partial order on intervals of length one where for interval $I_1 = [a, a + 1]$ and $I_2 = [b, b + 1]$ we have $I_1 < I_2$ if and only if $a + 1 < b$.

Sorting a permutation on a stack means given a permutation $\pi = (\pi_1, \dots, \pi_n)$ we can only use the stack operations **push** and **pop** in order to output (**pop**) the elements in sorted order. It is known that a permutation is stack-sortable if and only if it is 231-free. This means that there is no triple $i < j < k$ of indices with $\pi_k < \pi_i < \pi_j$. For example $\pi = (1, 7, 8, 4, 9, 10, 2, 6, 3, 5)$ is not 231-free since it contains the subsequence 8, 10, 3. Note that the permutation $(2, 3, 1)$ is not sortable on a stack. The elements 2 and 3 have to be pushed to allow the 1 pass them towards the output. Then, however, 2 is blocked by 3.

A partition $P = \{X_1, \dots, X_j\}$ of $[n]$ is visually represented by the elements $1, \dots, n$ as points on the x -axis and for each block X_i of the partition a path connecting the elements in increasing order where the edges are circular arcs in the upper halfplane. The partition is *non-crossing* if the resulting family of paths does not cross. An example of the non-crossing partition $P = \{\{1, 5, 7\}, \{2\}, \{3, 4\}, \{6\}, \{8\}\}$ of $[8]$ with the corresponding family of paths is shown in [Figure 25.6](#).

We briefly sketch bijections to the family of Dyck paths:

$[(aaa) \leftrightarrow (i)]:$ We get the bijection by looking at the two canonical n -chains of the ladder poset $2 \times n$. We mark the chain containing the minimal element as red and the other as blue and say that red corresponds to a $(+)$ and blue corresponds to a $(-)$. Then given a linear extension, that is an ordering of the vertices, we interpret it as a sequence of $(+)$ and $(-)$ signs which give us exactly a Dyck path as their sum is 0 and at every

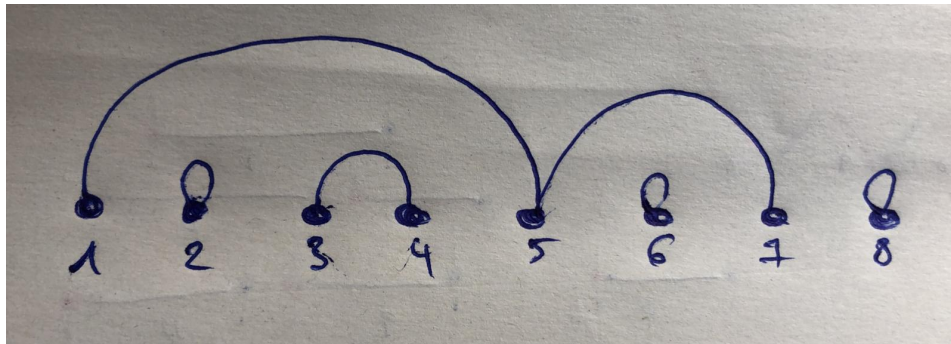


Figure 25.6: An example of a noncrossing partition of $[8]$

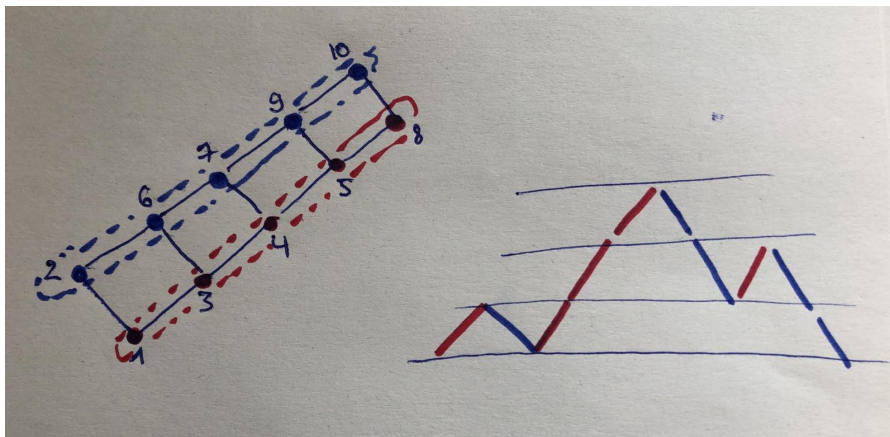


Figure 25.7: On the left we have a linear extension of the 2×5 Poset, where we marked the respective chains in red and blue. On the right we get the Dyck path corresponding to the linear extension.

step the sum of the signs remains positive. The converse is analogous via interpreting ups and downs as numberings in the respective chains.

$[(ddd) \leftrightarrow (i) :]$ Mark the left ends of the intervals red and the right ends blue. Drawing the intervals on a line using the order of the endpoints we simply sweep from left to right and seeing a red point we go up in the Dyck path and if we see a blue one we go down. This can also be reversed to get a semi-order from a Dyck path, where the unit length of the intervals is crucial in order to know which down step closes which interval.

We will continue our analysis of Catalan families and their bijective relations in the next lecture.

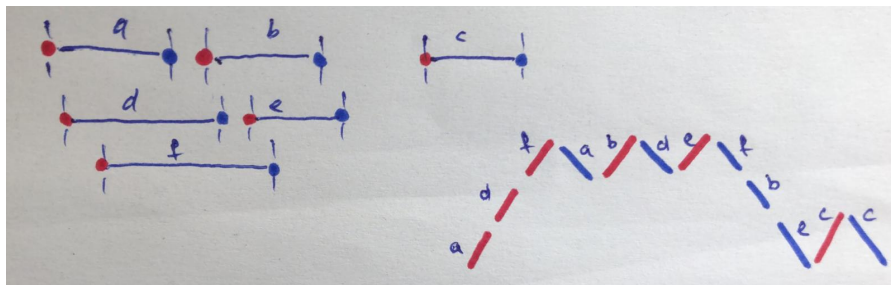


Figure 25.8: On the left we have a semi-order and on the right the corresponding Dyck path.

More Catalan Families

We start the lecture by showing showing two bijections between the family of non-crossing partitions (pp) and the family of Dyck-paths (i):

1. In the first bijection we draw an interval for each i , the interval starts at i and ends at the last element of the block X_j containing i , see [Figure 26.1](#). When sweeping the family of intervals from left to right we insert a step up for each interval start and a step down for each interval end. This yields a Dyck path. The non-crossing property is crucial in order revert the mapping, i.e., to know which down step closes which interval.

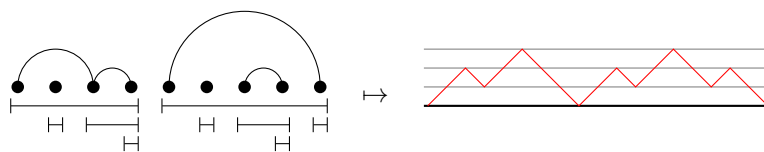


Figure 26.1: First bijection between non-crossing partitions and Dyck paths.

2. In the second bijection associate each i with two steps: a singleton with a step up and then a step down, an internal element with a step down and a step up, the first element of a part with two steps up and the last element with two steps down. In [Figure 26.2](#) one can see the corresponding Dyck path to the partition in [Figure 26.1](#).

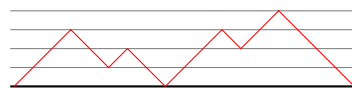


Figure 26.2: second bijection between non-crossing partitions and Dyck paths

26.1 Derivations of the Catalan formula

In Lecture 9 we already learned about a explicit formula for Catalan numbers. In this section we will show that the explicit formula for Catalan numbers can be obtained in several ways.

26.1.1 Cycle Lemma

We look at strings consisting of $n + 1$ times $+1$ and n times -1 . The number of such strings is $\binom{2n+1}{n+1}$. We then let the cyclic group act on these strings which yields orbits. The orbits are equivalence classes.

Lemma 26.1. *Every orbit has length $2n + 1$.*

Corollary 26.2. *This implies*

$$\#(\text{classes}) = \frac{1}{2n+1} \binom{2n+1}{n+1} = \frac{1}{n+1} \binom{2n}{n}.$$

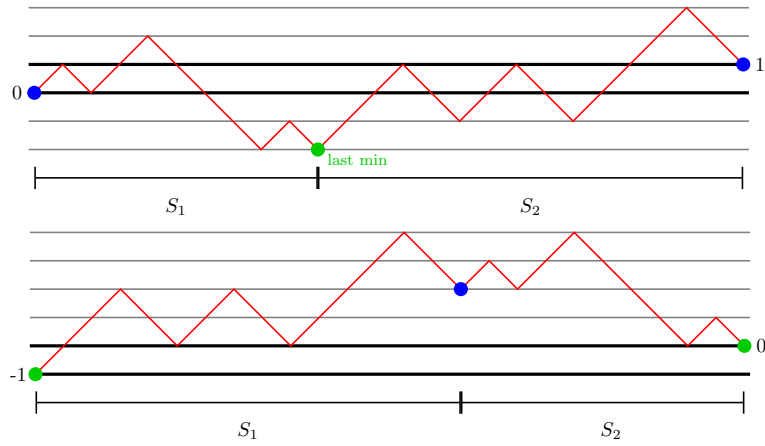


Figure 26.3: Top: some element of an orbit. Bottom: the Dyck path in the orbit.

Proof of Lemma 26.1. Suppose the class of a string S has size $< 2n + 1$. This means there is some $k < 2n + 1$ such that after k rotations string S is mapped to S , we will write this as $S^k = S$. The main idea is that in this case we can break S into t equal pieces which will give a contradiction on the numbers of ± 1 in S . We know that $S = S^k = S_1 S_2 = S_2 S_1$ with $|S_1| = k$ where S_1 is the substring consisting of the first k elements in S . Further we get $S = S^{ak}$ for all $k \in \mathbb{Z}$ by repeatedly rotating k times in either direction. Let further $\ell = \gcd(k, 2n + 1)$. Then it is known that $\ell = ak + b(2n + 1)$ for some $a, b \in \mathbb{Z}$ and hence $S^\ell = S^{ak+b(2n+1)} = S^{ak} = S$.

With that knowledge we can write $S = \underbrace{S' S' \dots S'}_{t \text{ copies of } S'}$ with S' some substring satisfying

$|S'| = \ell$ and $t = \frac{2n+1}{\ell}$. Then

$$1 = \sum S = t \sum S' \neq 1,$$

concluding the proof. \square

We further claim that each class has a unique string $(+1, D)$ such that D is equivalent to a Dyck path.

Proof. Existence: by making the last minimum the first element we get such a string as seen in Figure 26.3.

Uniqueness: Suppose there are $S = S_1, S_2$, $S' = S_2 S_1$. Then $\sum S_1 \geq 1$, $\sum S_2 \geq 1$, but $1 = \sum S = \sum S_1 + \sum S_2 \geq 2$. \square

26.1.2 Reflection Principle

Next we will look at $\binom{2n}{n}$ grid path from $(0,0)$ to (n,n) taking steps $(1,0)$ and $(0,1)$. The paths that stay above the main diagonal correspond to tilted Dyck path and therefore to a Catalan family. We now want to count the bad paths, that is, paths which go below the diagonal. Going below the diagonal is equivalent to touching the subdiagonal, i.e., the line $y = x - 1$. They are in bijection with grid paths $(0,0)$ to $(n+1, n-1)$ by reflection of the suffix at the first touching point with the subdiagonal as seen in Figure 26.4.

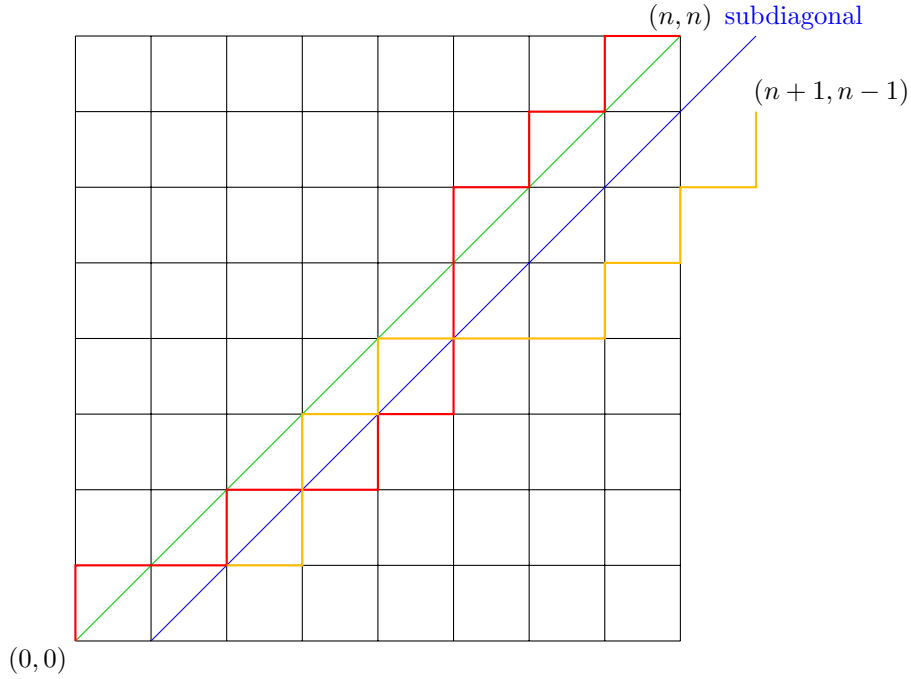


Figure 26.4: An example for $n = 8$ where the subdiagonal is marked in blue, the original path is marked in red and the reflected suffix is marked in orange

This yields

$$C_n = \binom{2n}{n} - \binom{2n}{n-1} = \left(1 - \frac{n}{n+1}\right) \binom{2n}{n} = \frac{1}{n+1} \binom{2n}{n}.$$

26.1.3 Symmetric chain decompositions

Let $A \subseteq [2n]$. As in Section 14.1.1 we associate a sequence of '('s and ')'s with A and call the chain \mathcal{C}_A . We further interpret that sequence as possible Dyck path by taking a step up for an opening parenthesis and a step down for a closing parenthesis. This is a Dyck path if and only if \mathcal{C}_A is a singleton. The number of singleton chains in a symmetric chain decomposition is given by the difference between the two largest ranks:

$$\binom{2n}{n} - \binom{2n}{n-1}.$$

26.2 Narayana numbers via LGV Lemma

Narayana numbers are a two parameter refinement of Catalan numbers, more precisely: $C_n = \sum_k N_k(n)$. We now study these numbers and derive an explicit number for them.

For the start we again look at the Catalan family (d): rooted full binary trees with $n+1$ leaves. With such a tree we associate two binary sequences, the *fingerprint* α and the *bodyprint* β . For the fingerprint we look at the leaves of the tree from left to right and write a 1 for a left leaf and a 0 for a right leaf. This yields the sequence α of length $n+1$ which starts with a 1 and ends with a 0. For the bodyprint we consider the inner nodes of the tree in in-order and write a 0 if the node is a left child and a 1 if it is a right child, for the root we write a 1. This yields the sequence β of length n which ends with a 1. Figure 26.5 shows a tree with fingerprint and bodyprint.

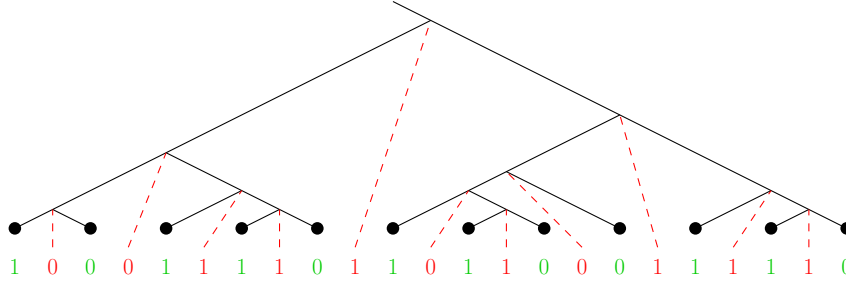


Figure 26.5: Fingerprint α in green and bodyprint β in red

The sequence α always starts with 1 and ends with 0. The sequence β always ends with 1. We call these entries the *trivial bits* and define $\hat{\alpha}$ and $\hat{\beta}$ as α and β by removing the trivial bits from α and β , respectively.

Lemma 26.3. *Let T be a full binary tree with $n+1$ leaves, k of them being left leaves. Then*

$$\sum_{i=1}^{n-1} \hat{\alpha}_i = \sum_{i=1}^{n-1} \hat{\beta}_i = k - 1 \quad \text{and} \quad \sum_{i=1}^j \hat{\alpha}_i \geq \sum_{i=1}^j \hat{\beta}_i \quad \forall j$$

Proof. Bijection between 1s of $\hat{\alpha}$ and 1s of $\hat{\beta}$: As seen in Figure 26.5 the sequences α and β are interleaved in a natural way. Each inner right node (1 in β) has a associated leftmost leaf (1 in α). This yields a bijection between the 1s in α and β . If $(\beta_i, \alpha_j) = (1, 1)$ is pair of the bijection, then $i \leq j$. \square

Lemma 26.4. *Full binary trees with $n + 1$ leaves such that k of them are left-leaves, are in bijection to pairs $(\hat{\alpha}, \hat{\beta})$ of 0,1-strings with*

$$\sum_{i=1}^{n-1} \hat{\alpha}_i = \sum_{i=1}^{n-1} \hat{\beta}_i = k - 1 \quad \text{and} \quad \sum_{i=1}^j \hat{\alpha}_i \geq \sum_{i=1}^j \hat{\beta}_i \quad \forall j$$

Proof. We have already seen the map $T \mapsto (\hat{\alpha}, \hat{\beta})$. We construct the map $(\hat{\alpha}, \hat{\beta}) \mapsto T$ by induction on the number of inversions of $\hat{\alpha}$:

- if $\hat{\alpha}$ has no inversion, then it is easy to find the unique associated tree, see Figure 26.6.

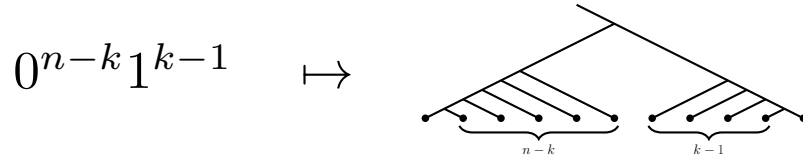


Figure 26.6: mapping for inversion free $\hat{\alpha}$

- if there is an inversion, then there is an adjacent inversion: $(\hat{\alpha}_{i-1}, \hat{\alpha}_i) = (1, 0)$. The two leaves contributing these values to the fingerprint are children of a common internal node t which contributes the value $\hat{\beta}_i$ to the bodyprint. Removing the two leaves makes node t a leaf. This leaf contributes the complement $\overline{\hat{\beta}_i}$ of $\hat{\beta}_i$ to the fingerprint of the reduced tree. With this idea in mind we can give a formal inductive proof. Let $(\hat{\alpha}, \hat{\beta})$ be a pair of 0,1 strings with the properties stated in the lemma and let $(\hat{\alpha}_{i-1}, \hat{\alpha}_i) = (1, 0)$ be an inversion of $\hat{\alpha}$. Let $\hat{\alpha}' = (\hat{\alpha}_1, \dots, \hat{\alpha}_{i-2}, \overline{\hat{\beta}_i}, \hat{\alpha}_{i+1}, \dots, \hat{\alpha}_{n-1})$ and $\hat{\beta}' = (\hat{\beta}_1, \dots, \hat{\beta}_{i-1}, \hat{\beta}_{i+1}, \dots, \hat{\beta}_{n-1})$. It is easy to see that $(\hat{\alpha}', \hat{\beta}')$ obey the conditions for n and either k or $k - 1$. By induction there is a corresponding tree T' . Let t be i th leaf of T' , this is the leaf contributing the value $\overline{\hat{\beta}_i}$ to the fingerprint. Add two leaves to t to obtain T and note that the reduced fingerprint and bodyprint of T are $\hat{\alpha}$ and $\hat{\beta}$ respectively.

\square

From a pair $(\hat{\alpha}, \hat{\beta})$ obeying the conditions of the lemma we build binary strings $\alpha^+ = 1\hat{\alpha}0$ and $\beta^+ = 0\hat{\beta}1$. Note that $\sum_{i=1}^{n+1} \alpha_i^+ = \sum_{i=1}^{n+1} \beta_i^+ = k$ for some k and $\sum_{i=1}^j \alpha_i^+ \geq \sum_{i=1}^j \beta_i^+$ for all $j < n + 1$. We can interpret these binary strings as paths starting in $(0, 0)$ and taking a unit horizontal step to the right for a 0 and a unit vertical step up for a 1. The

conditions imply that the α^+ -path and the β^+ -path end at the same point $(n - k + 1, k)$ and that α^+ is strictly above β^+ except at the endpoints, see Figure 26.7. The bijection between full binary trees and pairs (α^+, β^+) of paths is the bijection $(d) \leftrightarrow (\ell)$ between Catalan families.

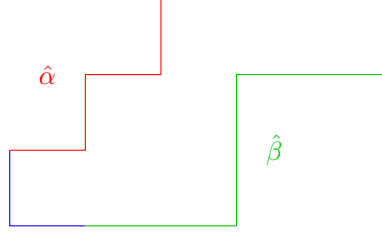


Figure 26.7: The α^+ -path and the β^+ -path obtained from $\hat{\alpha}, \hat{\beta}$.

The Catalan family (ℓ) of internally disjoint path of length $n + 1$ is naturally partitioned into classes $\mathcal{N}_k(n)$ for $k = 1, \dots, n$. The class \mathcal{N}_k consists of the pairs of paths ending in $(n - k + 1, k)$. The cardinality $N_k(n) = |\mathcal{N}_k(n)|$ is a *Narayana number*. A pair of paths in $\mathcal{N}_k(n)$ can be seen as a pair of disjoint paths from the starting points $(0, 1)$ and $(1, 0)$ to the endpoints $(n - k, k)$ and $(n - k + 1, k - 1)$. The Narayana number $N_k(n)$ can be computed with an easy application of the LGV-Lemma (Lemma 19.6).

$$N_k(n) = \det \begin{pmatrix} \binom{n-1}{k-1} & \binom{n-1}{k-2} \\ \binom{n-1}{k} & \binom{n-1}{k-1} \end{pmatrix} = \frac{1}{n} \binom{n}{k} \binom{n}{k-1}.$$

This yields a new formula for the Catalan number

$$C_n = \sum_{k=1}^n N_k(n) = \sum_{k=1}^n \frac{1}{n} \binom{n}{k} \binom{n}{k-1}$$

and allows to define a q -analogue of C_n by

$$C_n(q) = \sum_{k=1}^n N_k(n) q^k.$$

Dyck path areas, and another q -analog. As in Section 26.1.2 we interpret a Dyck path as a path with horizontal and vertical unit steps from $(0, 0)$ to (n, n) . The *region below* a Dyck path D is the region between the path and the diagonal $x = y$. We can define an order relation: $D_1 \leq D_2$ if the region below D_2 is contained in the region below D_1 . A cover relation $D < D'$ in this poset corresponds to a flip where a pair 01 (valley) of D is replaced by a 10 (peak) in D' . In particular the poset is ranked and the set of Dyck path at rank k is exactly the set of Dyck path where the area of the region below the path is $k + \frac{n}{2}$, here k takes the values 0 to $\binom{n}{2}$. If $F_k(n) = \#(\text{Dyck path with area } \frac{n}{2} + k)$. Then

$$\sum_{k=0}^{\binom{n}{2}} F_k(n) = C_n.$$

This refined expression for C_n allows to define a second q -analogue

$$\tilde{C}_n(q) = \sum_{k=0}^{\binom{n}{2}} F_k(n) q^k.$$

The recursion formula of the Catalan numbers nicely generalizes for $\tilde{C}_n(q)$:

$$\tilde{C}_n(q) = \sum_{k=1}^n \tilde{C}_{k-1}(q) \tilde{C}_{n-k}(q) q^{n-k-1}.$$

More Catalan Connections

In this lecture we hint on deeper connections between Catalan families and other objects which are of interest in Discrete Mathematics and beyond.

27.1 Tamari lattice

- Rotations on binary trees and diagonal flips on triangulations of an n -gon correspond to each other under the bijection $(a \leftrightarrow c)$ of Catalan families.
- On binary trees we define $T < T'$ if T can be obtained by a sequence of left-rotations from T' . This is the *Tamari lattice*.
- The *rotation distance* between two binary trees with the same number of nodes is the minimum number of tree rotations needed to reconfigure one tree into another. Sleator, Tarjan and Thurston (1988) proved that for infinitely many values of n , the maximum rotation distance is exactly $2n - 6$. Pournin (2014) gave a purely combinatorial proof for this bound.

Rotation distance and hyperbolic geometry Sleator et al. use the interpretation of rotation distance in terms of flips of triangulations of convex polygons. They interpret the starting and ending triangulation of a flip sequence as the upper and lower convex hull of a convex polyhedron while the convex polygon itself is a Hamiltonian circuit in this polyhedron (consisting of all edges obtained by intersecting the polyhedron with vertical planes. Under this interpretation, a sequence of flips from one triangulation to the other can be translated into a collection of tetrahedra that triangulate the given three-dimensional polyhedron. They find a family of polyhedra with the property that (in three-dimensional hyperbolic geometry) the polyhedra have large volume, but all tetrahedra inside them have much smaller volume, implying that many tetrahedra are needed in any triangulation.

- D. Sleator, R.E. Tarjan and W. Thurston, *Rotation distance, triangulations, and hyperbolic geometry*, J. Am. Math. Soc., 3 (1988) 647–681.
- L. Pournin, *The diameter of associahedra*, Adv. Math. 259 (2014) 13–42.

27.2 The associahedron

The associahedron A_n is an $(n - 2)$ -dimensional convex polytope in which each vertex corresponds to a triangulation of an $(n + 1)$ -gon and the edges correspond to diagonal flips. Associahedra are also called Stasheff polytopes.

- The associahedron can be obtained as the fiber polytope of an $(n + 1)$ -gon. In fact the polytopes $\Sigma(P)$ of [Theorem 27.1](#) below are associahedra.
- The associahedron can be obtained as a hypergraphic polytope. You can find out about this in a lecture of J. Cardinal: <https://youtu.be/rScL2rVvka4>

The associahedron as a fiber polytope Let T be a triangulation of a point set \mathcal{P} in convex position in the plane. Let Δ be a triangle of T , by $\text{vol}(\Delta)$ we denote the area of Δ . For a point $p \in \mathcal{P}$ let

$$\varphi(p) = \sum_{p \in \Delta \in T} \text{vol}(\Delta).$$

be the sum of the areas of triangles having p as a vertex. The *volume vector* of T is the vector

$$\varphi(T) = (\varphi(p_1), \varphi(p_2), \dots, \varphi(p_n)) \in \mathbb{R}^n.$$

The *fiber polytope* $\Sigma(\mathcal{P})$ of is the convex span of the volume vectors of all triangulations \mathcal{P} .

Theorem 27.1. *Let $\mathcal{P} = \{p_1, \dots, p_n\}$ be a set of points in convex position and $\Sigma(\mathcal{P})$ be the fiber polytope.*

- (1) *The dimension of $\Sigma(\mathcal{P})$ is $n - 3$.*
- (2) *The vertices of $\Sigma(\mathcal{P})$ are the volume vectors of triangulations of \mathcal{P} .*
- (3) *Faces of $\Sigma(\mathcal{P})$ correspond to subdivisions of \mathcal{P} , in particular the edges of $\Sigma(\mathcal{P})$ correspond to diagonal flips.*

References There is a book published in 2012 which contains chapters about all kind of mathematics related to associahedra and Tamari lattices but also recollections about the life and mathematical work of Dov Tamari:

Associahedra, Tamari lattices and related structures. Tamari memorial Festschrift Editors F. Müller-Hoissen, J.M. Pallo, and J. Stasheff. Progress in Mathematics Vol. 299, Birkhäuser (2012).

Here is a selection of chapters from the book which I find particularly interesting:

- *Dov Tamari (formerly Bernhard Teitler)*, Folkert Müller-Hoissen, Hans-Otto Walther.
- *Realizing the Associahedron: Mysteries and Questions*, Cesar Ceballos, Günter M. Ziegler.

- *From the Tamari Lattice to Cambrian Lattices and Beyond*, Nathan Reading.
- *Catalan Lattices on Series Parallel Interval Orders*, Filippo Disanto, Luca Ferrari, Renzo Pinzani, Simone Rinaldi.

27.3 The maule lattice

In the final 15 minutes of the lecture I presented some ideas about the maule lattice and its connections to the Tamari lattice and other lattices.

This I learned from lectures of Xavier Viennot which are part of his video-book *The Art of Bijective Combinatorics*, see www.viennot.org/abjc.html. Two lectures about the maule lattice can be found as Lec. 14 (<https://youtu.be/U1x7aS9jroA>) and Lec. 15 (<https://youtu.be/UihstHHmPTw>) of Part III.

27.4 Final links and references

The web page of the combinatorics course 2021 is

<https://page.math.tu-berlin.de/~felsner/Lehre/dsI21.html>.

From this page some additional material related to the course is accessible. You can find **links** to 14 exercise sheets and a link to a page with “detailed content” of the individual lectures. On this page you find a description of the content of the lecture in few lines and **links** to the recordings of the individual lecture on YouTube.

References

Below you find the list of books from the web page of the course. To me these have been the most valuable books about combinatorics.

- M. Aigner: *A Course in Enumeration*; Springer, 2007.
- I. Anderson: *Combinatorics of Finite Sets*; Dover 2002 (reprint of the 1985 edition).
- R. Graham, D. Knuth, O. Patashnik: *Concrete Mathematics*; Addison-Wesley, 1989.
- S. Jukna: *Extremal Combinatorics*; Springer, 2001.
- J.H. van Lint and R.M. Wilson: *A Course in Combinatorics* (2nd ed.); Cambridge Univ. Press, 2001.
- R. Stanley: *Enumerative Combinatorics, Volume I*; Cambridge Univ. Press, 1997.
- R. Stanley: *Enumerative Combinatorics, Volume II*; Cambridge Univ. Press, 1999.
- D.B. West: *Combinatorial Mathematics*; Cambridge Univ. Press, 2021.