University of Zurich[UZH]

INSTITUTE OF MATHEMATICS

Master's Thesis

The Cyclic Sieving Phenomenon

Author:
Marino Gambarara

Supervisor
Prof. Dr. Valentin Féray

July, 2020

Abstract

In this thesis, we survey some of the literature on the cyclic sieving phenomenon and elaborate many results by rewriting some of the existing proofs. We present our idea of how cyclic sieving can be usefully applied in combinatorics. Furthermore, we give proofs for instances of the cyclic sieving phenomenon on binary words and lattice paths. We also provide proofs for two Catalan objects, namely triangulations of convex polygons and non-crossing matchings.

Acknowledgements

I would like to express my sincere gratitude to my supervisor Prof. Dr. Valentin Féray for giving me the opportunity to write my Master's Thesis in algebraic combinatorics and for introducing me to the cyclic sieving phenomenon. He has given me the freedom I wished for and the guidance I needed. I would also like to thank him for correcting many previous drafts, pointing out missing arguments and making me reflect on my way of writing down proofs.

I would like to thank Niklas Gassner, Simon Grüning and Severin Schraven for helping me out with LaTeX and writing style problems.

A special thanks goes to Nathan Brack, Niklas Gassner and Severin Schraven for their willingness to always support me enthusiastically when I encountered mathematical problems.

I would like to thank Myriam Dudli for helping me with the intricacies of the English language.

Moreover, I would like to thank Mariah Blatty for proofreading the thesis.

Finally, I want to thank my fellow students. There has been a great atmosphere in the institute of mathematics and it has always been a pleasure to discuss mathematics with them.

Contents

1 Introduction **4**

2 Preliminaries **6**
2.1 Basic Notions of Combinatorics 6
2.1.1 Group Action and Permutation Groups 6
2.1.2 Q-Binomial Coefficients 9
2.1.3 Permutation Statistics 12
2.2 Representation Theory of Finite Groups 15

3 Fundamental Concept of Cyclic Sieving **18**
3.1 A First Example 19
3.1.1 A Proof by Explicit Evaluation 20
3.1.2 A Proof using Representation Theory 23
3.2 Application of CSP to Problems of Burnside Type 28

4 A Representation Theory Paradigm **32**

5 Pólya's Theory **35**
5.1 The Theorems of Pólya 35
5.2 A Generalization 40

6 Words and Lattice Paths **42**
6.1 Binary Words 42
6.2 Lattice Paths 46
6.2.1 Circular Dyck Paths 47
6.2.2 Möbius Paths 53

7 Catalan Objects **59**
7.1 Triangulations 59
7.2 Non-Crossing Matchings 64
7.3 Non-Crossing Partitions 71

Chapter 1

Introduction

The cyclic sieving phenomenon was defined by V. Reiner, D. Stanton and D. White in 2004 [1]. The phenomenon displays a beautiful interplay between algebra and combinatorics. Three ingredients are used: a finite set X, a cyclic group C acting on X and a polynomial f(q) with non-negative integer coefficients. Then the triple (X, C, f(q)) exhibits the cyclic sieving phenomenon if for all elements $c \in C$

$$|X^c| = f(\omega),$$

where X^c is the fixed point set of c and ω a root of unity chosen to have the same order as c. Many instances of the cyclic sieving phenomenon have since been found.

In the preliminaries, we will develop some basic notions such as q-binomial coefficients and permutation statistics, which will be used in several cases to prove the cyclic sieving phenomenon for a certain triple. Indeed, we will see how omnipresent and powerful q-binomial coefficients are when we discuss the cyclic sieving phenomenon. It is worth to emphasize that there is no real explanation why this phenomenon occurs so often with these q-analogues.

In Chapter 3 we will introduce the fundamental concept of cyclic sieving with its two approaches for proving it. One approach uses representation theory, which is why we will recall the important notions in the preliminaries as well. These proofs rely on showing that two modules are isomorphic and then using the fact that the respective characters coincide. Another way to prove that the cyclic sieving phenomenon holds for a certain triple is by explicitly evaluating both sides of the definition. We will take this approach several times by first evaluating the q-binomial coefficients in the d-th roots of unity and then investigating the number of fixed points of the group elements on the respective set. Furthermore, we will present our idea of how cyclic sieving can be usefully applied in combinatorics.

In Chapter 4 we will provide a useful tool to prove that a certain triple exhibits the cyclic sieving property by using representation theory.

In Chapter 5 we will discuss Pólya's Theory, which allows us to prove a generalization of a result we give in Chapter 3. Moreover, we will make use of the tool presented in Chapter 4.

In Chapter 6 we will prove instances of the cyclic sieving phenomenon on binary words and lattice paths. We will give two different cyclic actions on binary words and show its correspondence to lattice paths. In addition, we will present results on circular Dyck paths and Möbius paths respectively.

Finally, in Chapter 7, we will discuss the cyclic sieving phenomenon on Catalan objects. We will provide proofs for triangulations of convex polygons and non-crossing matchings and present a result on non-crossing partitions, which was given in the original paper.

This thesis is written on the basis of the aforementioned paper from 2004 [1], the survey of B. Sagan from 2011 [2] and the paper on circular dyck paths by P. Alexandersson, S. Linusson and S. Potka published in 2019 [3].

In the following we list our original contributions in this thesis. In section 3.2 we present an idea of how cyclic sieving could be applied in combinatorics and give a proof (3.4) for a result on binary words. We rewrite or elaborate existing proofs and arguments in more detail in Section 3.1.2, Theorem 5.4, Corollary 5.5, Theorem 6.19 and Theorem 7.4. Moreover, we present the results in Section 6.2.1 and Section 6.2.2 in more detail. Finally, we give new proofs for existing results in Theorem 6.2, Theorem 6.7, Theorem 7.1 and Theorem 7.3.

Chapter 2

Preliminaries

In order to discuss the cyclic sieving phenomenon, we need to develop some basic notions from combinatorics and representation theory. As the name suggests, we will work in particular with cyclic groups, where we presume some basic results from algebra.

2.1 Basic Notions of Combinatorics

Most of the notions in section 2.1.1 are very standard and can be found in e.g. [5]. For sections 2.1.2 and 2.1.3 we refer to [2] and [6].

2.1.1 Group Action and Permutation Groups

First of all we define the group action and fixed point set of a permutation, which will be elementary for the cyclic sieving phenomenon.

Definition 2.1. We say that a group $(G, \circ)$ *acts on a set X*, if there is a map

$$* : \begin{cases} G \times X \to X \\ (a, x) \mapsto a * x \end{cases}$$

such that

(1) $e * x = x$ for every $x \in X$ and the neutral element $e \in G$, and

(2) $(a \circ b) * x = a * (b * x)$ for all $a, b \in G$ and $x \in X$.

Definition 2.2. Let $(G, \circ)$ be a group acting on a set X. For an element $g \in G$, we define

$$X^g := \{x \in X \mid g * x = x\}$$

to be the set of points in X, which are fixed by the group element g.

The following elementary definition of stabilizer will be helpful to prove Burnside's Lemma later on.

Definition 2.3. Let $(G, \circ)$ be a group acting on X. For an element $x \in X$, we define $G_x := \{g \in G \mid g * x = x\}$ to be its *stabilizer*.

Note that $(G_x, \circ)$ is a subgroup of $(G, \circ)$. Next, we give the definition of orbits.

Definition 2.4. Let $(G, \circ)$ be a group acting on X. For elements $x_1, x_2 \in X$ we define $x_1 \sim x_2$ if there exists $g \in G$ with $g * x_1 = x_2$. Then $\sim$ is an equivalence relation and the equivalence classes are called *orbits* of X under $(G, \circ)$. For $x \in X$, we call $G * x := \{g * x \mid g \in G\}$ the *orbit* of x under $(G, \circ)$.

Orbits will play a central role in the chapter about Pólya's Theory. To give an idea when they appear, imagine we want to count the number of possible colorings of the vertices of a die. We could for example color the vertices on the top with a color and the vertices on the bottom with a different color. Or we choose two different colors for the vertices on the left side, respectively for the vertices on the right side. However, since we can rotate the die, the latter two colorings should be identified. In this case X is the set of colorings of vertices of a fixed die and $(G, \circ)$ the rotation group of a die. To solve the problem, we then can count the orbits of X under $(G, \circ)$. As we will see, such types of problems can be solved with Burnside's Lemma or Pólya's Theorems.

In the following, we give further important definitions we will need throughout the chapters.

Definition 2.5. Let $\mathbb{N}_n := \{1, \ldots, n\}$. A bijection $\pi : \mathbb{N}_n \to \mathbb{N}_n$ is called a *permutation of degree n*.

Definition 2.6. Let $\mathcal{S}_n := \{\pi \mid \pi : \mathbb{N}_n \to \mathbb{N}_n\}$ be the set of all permutations on $\mathbb{N}_n$. The group $(\mathcal{S}_n, \circ)$, where $\circ$ denotes the composition, is called the *symmetric group*.

Definition 2.7. Let $(G, \circ)$ be a group. If the elements of G are permutations of degree n and $\circ$ denotes the composition, we call $(G, \circ)$ a *permutation group*.

Note that every permutation group is a subgroup of the symmetric group $(\mathcal{S}_n, \circ)$.

Definition 2.8. A permutation π is called a *k-cycle*, if there exist $k \in \mathbb{N}_{>0}$, $i \in \mathbb{N}_n$ such that

(1) k is the smallest positive integer such that $\pi^k(i) = i$, and

(2) π fixes each $j \notin \{i, \pi(i), \ldots, \pi^{k-1}(i)\}$.

A 1-cycle of a permutation π is called a *fixed point*.

We multiply permutations from right to left. Thus $\pi\sigma$ is the bijection obtained by first applying σ, followed by π. We will display a permutation π using *cycle notation*. For example, if $\pi \in \mathcal{S}_6$ is given by

$$\pi(1) = 2, \quad \pi(2) = 1, \quad \pi(3) = 3, \quad \pi(4) = 6, \quad \pi(5) = 4, \quad \pi(6) = 5,$$

the *two-line notation* of the permutation is

$$\pi = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 2 & 1 & 3 & 6 & 4 & 5 \end{pmatrix}.$$

In cycle notation the permutation is given by

$$\pi = (12)(465),$$

where we drop the fixed point 3.

Definition 2.9. Let π be a permutation of degree n. The *cycle type* of π is the sequence $(j_1, \ldots, j_n)$, where $j_k, 1 \leq k \leq n$, denotes the number of k-cycles in π.

If $(j_1, \ldots, j_n)$ is the cycle type of a permutation of degree n, it holds

$$\sum_{k=1}^{n} k j_k = n,$$

since n is the number of elements in $\mathbb{N}_n$. In particular, a vector $(j_1, \ldots, j_n)$ satisfying the above equality represents the cycle type of a permutation in $\mathcal{S}_n$.

It follows a standard fact about the number of permutations given a cycle type.

Proposition 2.10. The number of permutations $\pi \in \mathcal{S}_n$ with cycle type $(j_1, \ldots, j_n)$ is given by

$$h(j_1, \ldots, j_n) = \frac{n!}{1^{j_1} j_1! \cdots n^{j_n} j_n!}.$$

□

Finally, we give the order of a permutation.

Lemma 2.11. Let $\pi \in \mathcal{S}_n$ a permutation with cycles of length $l_1, \ldots, l_k$. The order of π is $\mathrm{lcm}(l_1, \ldots, l_k)$.

Proof. The order of any cycle of π divides the order of π. The least integer n, such that $\pi^n = e$, is exactly $\mathrm{lcm}(l_1, \ldots, l_k)$. □.

2.1.2 Q-Binomial Coefficients

Discussing the cyclic sieving phenomenon, we will frequently use q-binomial coefficients for our polynomial f(q). As a matter of fact, it turns out that they constitute a powerful tool to prove the cyclic sieving phenomenon on many different instances and can be found in a wide range of literature. Firstly, we define the notion of q-analogues.

Definition 2.12. Let n be a non-negative integer. The geometric series $[n]_q := 1 + q + \cdots + q^{n-1}$ is called *q-analogue of n*. We set $[0]_q := 0$.

Note that setting $q = 1$ gives $[n]_1 = n$. Next we define the factorial of $[n]_q$ and the q-binomial coefficients.

Definition 2.13. The *factorial* $[n]_q!$ is $[n]_q! := [1]_q \cdots [n]_q$. We set $[0]_q! := 1$.

Definition 2.14. For $0 \leq k \leq n$, define the *q-binomial coefficients* by

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

There is also a combinatorial approach to define the q-binomial coefficients. The binomial coefficient $\binom{n}{k}$ counts the k-combinations from an n-element set. Assume these n elements denote the different character positions in a word of length n. Then each k-combination corresponds to a word of length n using a binary alphabet, say $\{0, 1\}$, with k copies of the letter 0 and $n - k$ copies of the letter 1. To illustrate, the $\binom{4}{2}$ words on a binary alphabet are

$$0011,\ 0101,\ 0110,\ 1001,\ 1010,\ 1100.$$

To obtain the q-binomial coefficient, it suffices to count each word with a factor q^d, where d is the number of *inversions* of the word. An inversion is a pair of character positions, where we write a pair in ascending order, such that the first position holds a letter 1 and the second position holds a letter 0. The corresponding q-binomial coefficient is then given by

$$\begin{bmatrix} 4 \\ 2 \end{bmatrix}_q = 1 + q + 2q^2 + q^3 + q^4.$$

For example, the monomial $2q^2$ corresponds to the two words 0110 and 1001, which both have two inversions. We will briefly prove that both definitions coincide and in fact, see another interpretation of the q-binomial coefficients.

When we are interested in that a certain triple exhibits the cyclic sieving phenomenon, we want our polynomial to have non-negative integer coefficients. The following lemma [6, pages 21 – 22] shows that this is the case for q-binomial coefficients.

Proposition 2.15. The q-binomial coefficients are polynomials with non-negative integer coefficients.

Proof. We prove the claim by induction on n. For $n = 1$ the claim follows directly by definition. Assume the claim holds for n. We want to show that it also holds for $n + 1$. We prove the identity

$$\begin{bmatrix} n \\ k \end{bmatrix}_q = \begin{bmatrix} n-1 \\ k-1 \end{bmatrix}_q + q^k \begin{bmatrix} n-1 \\ k \end{bmatrix}_q \tag{2.1}$$

for $1 \leq k \leq n-1$ from which the claim will follow, since by assumption both polynomials on the right hand side have non-negative integer coefficients.

Note that for any $1 \leq k \leq n-1$ we have

$$\begin{aligned} [n]_q &= 1 + \cdots + q^{n-1} \\ &= (1 + \cdots + q^{k-1}) + q^k(1 + \cdots + q^{n-k-1}) \\ &= [k]_q + q^k[n-k]_q \end{aligned}$$

and thus

$$\begin{aligned} \begin{bmatrix} n \\ k \end{bmatrix}_q &= \frac{[n]_q!}{[k]_q![n-k]_q!} = \frac{[n-1]_q![n]_q}{[k]_q![n-k]_q!} \\ &= \frac{[n-1]_q!([k]_q + q^k[n-k]_q)}{[k]_q![n-k]_q!} \\ &= \frac{[n-1]_q!}{[k-1]_q![n-k]_q!} + q^k \frac{[n-1]_q!}{[k]_q![n-k-1]_q!} \\ &= \begin{bmatrix} n-1 \\ k-1 \end{bmatrix}_q + q^k \begin{bmatrix} n-1 \\ k \end{bmatrix}_q. \end{aligned}$$

□

To provide another combinatorial interpretation of the q-binomial-coefficients, we introduce the notion of lattice paths.

Definition 2.16. A *lattice path* of length k is a sequence of points $L = \{l_1, \ldots, l_k\}$ in $\mathbb{Z}^2$ with north-east steps in $S = \{(1,0), (0,1)\}$, such that each consecutive difference $l_i - l_{i-1}$ lies in S.

Note that in general the steps could be chosen arbitrarily. However, we will work only with north-east lattice paths.

The number of lattice paths from the origin (0,0) to the point (m,n) is $\binom{m+n}{m}$, since we must take m+n steps from which m are north and n are east. Suppose we want to count the paths by area under the path, which is bounded by the lines

x = m, y = n and the path. We use a generating function approach, so that a path enclosing an area of A units contributes q^A to the overall generating function. Here q is simply a formal variable; the answer is obviously a polynomial in q.

The idea for the following proof can be found in e.g. [7, Theorem 6.2].

Proposition 2.17. The generating function for lattice paths from (0,0) to (m,n) by area under path is $\begin{bmatrix} m+n \\ m \end{bmatrix}_q$.

Proof. We will make use of the identity (2.1). Let Q(n,k) be the sum of the weights of lattice paths from (0,0) to $(n-k, k)$, where the weight of a path is q^A if the area below is A. Clearly Q(n,0) = Q(n,n) = 1.

Consider all latice paths from (0,0) to (n−k, k) and divide them into two classes: those in which the last step is vertical and those in which it is horizontal. In the first case, the last step is from the end of a path counted by $Q(n-1, k-1)$, ending at $(n-k, k-1)$, and adds no area to the path. In the second case, it is from the end of a path counted by $Q(n-1, k)$, ending at $(n-k-1, k)$, and increases the area by k, adding $q^k Q(n-1, k)$ to the sum.

So the numbers Q(n, k) have the same recurrence and boundary conditions as the q-binomial coefficients (2.1), thus must be equal to them. □

For example, consider the q-binomial coefficient

$$\begin{bmatrix} 6 \\ 3 \end{bmatrix}_q = 1 + q + 2q^2 + 3q^3 + 3q^5 + 3q^6 + 2q^7 + q^8 + q^9,$$

which is the generating function for lattice paths from (0,0) to (3,3) by area under path. The monomial $3q^5$ tells us, that there are 3 lattice paths with area 5 from (0,0) to (3,3). These are listed below.

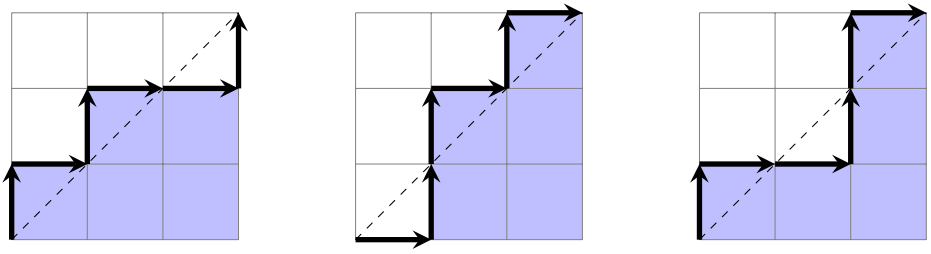

Figure 2.1: All 3 lattice paths with area 5.

Observe that lattice paths correspond to words with a binary alphabet, say $\{0, 1\}$, where 0 denotes an east step and 1 denotes a north step. Further, any inversion of such a word contributes exactly 1 to the area under path. This justifies the alternative definition we gave using inversions of binary words.

2.1.3 Permutation Statistics

In this section we discuss permutation statistics, which are connected to q-binomial coefficients. Moreover, we will need them in Chapter 6, where we will investigate how the cyclic sieving phenomenon appears on different kinds of lattice paths. For a broad overview, see [6]. To begin with, we define statistics and provide several examples.

Definition 2.18. A *statistic* on a finite set X is a function $\mathrm{st} : X \to \mathbb{N}$. The statistic has a corresponding *weight generating function*

$$f^{\mathrm{st}}(X) := \sum_{x \in X} q^{\mathrm{st}(x)},$$

which is a polynomial in q.

Definition 2.19. Let S_n be the symmetric group on $\mathbb{N}_n$ and $\pi \in S_n$ a permutation. We call

(1) $\mathrm{Inv}(\pi) := \{(i,j) \in \mathbb{N}_n \times \mathbb{N}_n \mid i < j \text{ and } \pi(i) > \pi(j)\}$ the set of *inversions* of π,

(2) $\mathrm{Des}(\pi) := \{i \in \mathbb{N}_n \mid \pi(i) > \pi(i+1)\}$ the *descent set* of π,

(3) $\mathrm{Exc}(\pi) := \{i \in \mathbb{N}_n \mid \pi(i) > i\}$ the *set of excedances* of π,

and define the statistics

$$\begin{aligned} \mathrm{inv}(\pi) &:= |\mathrm{Inv}(\pi)|, \\ \mathrm{des}(\pi) &:= |\mathrm{Des}(\pi)|, \\ \mathrm{exc}(\pi) &:= |\mathrm{Exc}(\pi)|, \\ \mathrm{maj}(\pi) &:= \sum_{i \in \mathrm{Des}(\pi)} i. \end{aligned}$$

To illustrate, consider the symmetric group S_3. We get the following table for these four statistics:

π	(1)(2)(3)	(12)(3)	(13)(2)	(23)(1)	(123)	(132)
inv(π)	0	1	3	1	2	2
des(π)	0	1	1	1	1	1
exc(π)	0	1	1	1	2	1
maj(π)	0	1	3	2	2	1

Table 2.1: Statistics table for S_3.

Analogously we can define the statistics above on binary words. To do so, let $\{0,1\}^n$ be the set of binary words and write $b = \{b_1, \ldots, b_n\} \in \{0,1\}^n$. Instead of checking the condition $\pi(i) > \pi(j)$ for an inversion, we then check the condition $b_i > b_j$. Doing this similarly for the other statistics gives the statistics on binary words. We will particularly make use of the major statistic of a binary word later on, when we will prove a cyclic sieving result on lattice paths.

In order to make a connection to the q-analogues, we introduce another statistic on a different set than the permutations of the symmetric group.

Definition 2.20. For each $n \in \mathbb{N}_{\geq 0}$ let SE_n denote the set of *subexcedent* sequences $x = (x_1, \ldots, x_n)$. These are the sequences of integers x_i of length n, that satisfy the inequalities $0 \leq x_i \leq i - 1$ for all $i = 1, \ldots, n$.

The cardinality of SE_n is of course n!.

Definition 2.21. For each sequence $x \in SE_n$ we define the statistic

$$\text{total}(x) := x_1 + \cdots + x_n.$$

We can rewrite the set of subexcedent sequences as $SE_n = SE_{n-1} \times \{0, \ldots, n-1\}$. Using this fact, we can prove the following proposition [6, Proposition 2.1].

Proposition 2.22. For each $n \geq 1$ we have

$$\sum_{x \in SE_n} q^{\text{total}(x)} = [n]_q!.$$

Proof. For $n = 1$ the result is trivial. By induction on n we get

$$\begin{aligned} \sum_{x \in SE_n} q^{\text{total}(x)} &= \sum_{x \in SE_{n-1}} q^{\text{total}(x)} \sum_{0 \leq x_n \leq n-1} q^{x_n} \\ &= [n-1]_q![n]_q \\ &= [n]_q!. \end{aligned}$$

□

To show that an analogous property holds for the statistics inv and maj, we will construct two bijections $\pi \to x$ of S_n onto SE_n having the properties

$$\text{inv}(\pi) = \text{total}(x), \qquad \text{maj}(\pi) = \text{total}(x).$$

The construction of those two bijections makes use of two different codings [6, pages 17–18] of the permutations. The image x of π under each of those bijections is called the inv-coding and the maj-coding respectively.

Proposition 2.23. We have

$$\sum_{\pi\in S_n} q^{inv(\pi)} = [n]_q! = \sum_{\pi\in S_n} q^{maj(\pi)}$$

and in particular $f^{inv}(S_n) = f^{maj}(S_n)$.

Proof. Let $\pi \in S_n$ a permutation where we use the notation $\pi = \pi(1)\cdots\pi(n)$. For each $i = 1, \ldots, n$ define x_i to be the number of terms $\pi(j)$ to the left of $\pi(i)$ which are greater than $\pi(i)$, namely

$$x_i := \sum_{1\le j\le i-1} \mathrm{Ind}(\pi(j) > \pi(i)),$$

where $\mathrm{Ind}(\pi(j) > \pi(i))$ is 1 if the inequality holds and 0 else. Clearly, the defined sequence $x = x_1, \ldots, x_n$ is subexcedent. This coding is bijective, since it has the following inverse. First let $\pi(n) := n - x_n$. Once the elements $\pi(k+1), \ldots, \pi(n)$ have been obtained, eliminate all the terms of the sequence $(n, n-1, \ldots, 2, 1)$ equal to one of the $\pi(l)'$s for a certain $l \ge k+1$. Then, $\pi(k)$ is equal to the $(x_k + 1) - st$ term of the sequence $(n, n-1, \ldots, 2, 1)$, when reading that sequence from left to right. Moreover, by definition the sum total(x) is precisely equal to the inversion number $inv(\pi)$ of the permutation π. Therefore the first equality holds. One can find a suitable bijection that establishes the equality for the major statistic as well. □

To illustrate the inverse of the coding, consider the permutation

$$\pi = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 2 & 1 & 4 & 5 & 3 \end{pmatrix}.$$

The coding gives us the sequence $x = 01002$. To obtain the inverse, we compute $\pi(n) := n - x_n$ and get

$$\pi(5) = 5 - 2 = 3.$$

For $k = 4$ we have $\pi(4+1) = \pi(5)$. Eliminating all the terms of the sequence (5,4,3,2,1) equal to 3 yields the sequence (5, 4, 2, 1). So $\pi(4) = 5$, since $x_4 + 1 = 1$. Iterating this algorithm, we get the following table:

$\mathbf{k}$	$\boldsymbol{\pi(k+1)}$	$\boldsymbol{\pi(l)'s}$	**sieved sequence**	$\mathbf{x_k + 1}$	$\boldsymbol{\pi(k)}$
4	3	3	(5,4,2,1)	1	5
3	5	3, 5	(4,2,1)	1	4
2	4	3, 4, 5	(2,1)	2	1
1	1	1, 3, 4, 5	(2)	1	2

Table 2.2: Iteration table.

2.2 Representation Theory of Finite Groups

One approach for proving the cyclic sieving phenomenon uses representation theory. In the following we introduce the required tools to do so. The notions in this section can be found in e.g. [5].

Let V be a vector space. From now on we assume that all vector spaces have finite dimension and are over the complex numbers $\mathbb{C}$. Further we assume, that all groups G are finite.

Definition 2.24. Let $\mathrm{GL(V)} := \{\mathrm{A} : \mathrm{V} \to \mathrm{V} \mid \mathrm{A \text{ is invertible}}\}$ be the set of all invertible linear tranformations of V to itself.

$(\mathrm{GL(V)}, \circ)$ is a group with $\circ$ being the composition of linear maps.

Definition 2.25. Let V be a vector space and $(\mathrm{G}, \circ)$ be a group. Then V is a *G-module*, if there is a group-homomorphism

$$\rho : \mathrm{G} \to \mathrm{GL(V)}.$$

We call ρ a *representation* of G. Alternatively, we can say that the vector space V carries a representation of G.

Lemma 2.26. Equivalently, V is a G-module if there is a G-action, gv, of elements of V by elements of g such that

(1) $\mathrm{gv} \in \mathrm{V}$,

(2) $\mathrm{g(cv + dw)} = \mathrm{c(gv)} + \mathrm{d(gw)}$,

(3) $\mathrm{(gh)v} = \mathrm{g(hv)}$, and

(4) $\mathrm{ev} = \mathrm{v}$.

for all $\mathrm{g, h} \in \mathrm{G}$, $\mathrm{v, w} \in \mathrm{V}$ and scalars $\mathrm{c, d} \in \mathbb{C}$.

Proof. Assume V is a G-module. Then $\rho(\mathrm{g})\rho(\mathrm{h}) = \rho(\mathrm{gh})$ for all $\mathrm{g, h} \in \mathrm{G}$ and thus (3) holds. Choosing $\mathrm{g} = \mathrm{h} = \mathrm{e}$, we get $\rho(\mathrm{e}) = 1$. This implies (4). (1) and (2) are implied by the fact, that $\rho(\mathrm{g}) \in \mathrm{GL(V)}$ for $\mathrm{g} \in \mathrm{G}$.

Assume now (1) - (4) hold. Let $\mathrm{g, h} \in \mathrm{G}$. Then (3) implies, that there is a multiplication such that we can define $\rho(\mathrm{gh}) = \rho(\mathrm{g})\rho(\mathrm{h})$. Therefore there exists a group-homomorphism $\rho : \mathrm{G} \to \mathrm{GL(V)}$. □

In fact, it is always possible to take a set on which $(\mathrm{G}, \circ)$ acts and turn it into a G-module as follows.

Definition 2.27. Let $S = \{s_1, \dots, s_n\}$ be a set. Then $\mathbb{C}S = \mathbb{C}\{s_1, \dots, s_n\}$ is defined as

$$\mathbb{C}S := \{c_1 s_1 + \cdots + c_n s_n \mid c_i \in \mathbb{C}, 1 \leq i \leq n\}.$$

That is, $\mathbb{C}S$ is the vector space generated by S over $\mathbb{C}$, i.e., $\mathbb{C}S$ consists of all the formal linear combinations.

Notice that s_i should be considered as vectors. Vector addition and scalar multiplication in $\mathbb{C}S$ are defined by

$$(c_1 s_1 + \cdots + c_n s_n) + (d_1 s_1 + \cdots + d_n s_n) = (c_1 + d_1)s_1 + \cdots + (c_n + d_n)s_n$$

and

$$c(c_1 s_1 + \cdots + c_n s_n) = (cc_1)s_1 + \cdots + (cc_n)s_n$$

respectively. Now the action of G on S can be extended to an action on $\mathbb{C}S$ by linearity:

$$g(c_1 s_1 + \cdots + c_n s_n) = c_1(gs_1) + \cdots + c_n(gs_n) \tag{2.2}$$

for all $g \in G$. This makes $\mathbb{C}S$ into a a G-module of dimension $|S|$.

Definition 2.28. If a group G acts on a set S, then the associated module $\mathbb{C}S$ is called *permutation representation* associated with S. Also, the elements of S form a basis of $\mathbb{C}S$ called the *standard basis*.

We will make use of the latter construction several times, where our set S will be $\mathbb{N}_n$. Next we define, when two G-modules are isomorphic and introduce the notions of submodules and irreducibility.

Definition 2.29. Let V, W be two G-modules. Then V and W are *isomorphic*, written $V \cong W$, if there is a linear bijection $\phi : V \to W$ which preserves the action of g, namely

$$\phi(gv) = g\phi(v)$$

for every $g \in G, v \in V$.

Equivalenty, the following diagramm commutes for every $g \in G$, where ρ' and ρ'' are the representations of V and W respectively.

$$\begin{array}{ccc} V & \xrightarrow{\rho'(g)} & V \\ {\scriptstyle\phi}\downarrow & & \downarrow{\scriptstyle\phi} \\ W & \xrightarrow{\rho''(g)} & W \end{array}$$

Definition 2.30. Let V be a G-module. A *submodule* of V is a subspace $W \subseteq V$ which is invariant under the action of $(G, \circ)$, namely

$$gw \in W \text{ for all } g \in G, w \in W.$$

Definition 2.31. Let V be a G-module. Then V is *reducible*, if it contains a non-trivial submodule. Otherwise, it is *irreducible*.

Note that the zero subspace and V itself are the trivial submodules. Finally, we introduce the notion of the character of a representation, which will be essential later on.

Definition 2.32. Let V be a G-module and $\rho : G \to GL(V)$ be a group-homomorphism. For each $g \in G$, put

$$\chi_\rho(g) := \mathrm{Tr}(\rho(g)),$$

where $\mathrm{Tr}(\rho(g))$ is the trace of $\rho(g)$. Then the obtained complex valued function χ_ρ on G

$$\chi_\rho : \begin{cases} G \to \mathbb{C} \\ g \mapsto \mathrm{Tr}(\rho(g)) \end{cases}$$

is called the *character* of ρ.

Chapter 3

Fundamental Concept of Cyclic Sieving

In order to define the concept of cyclic sieving, we need three ingredients. The first is a finite set X. The second is a finite cyclic group, C, which acts on X. The final ingredient is a polynomial $f(q) \in \mathbb{N}[q]$, where

$$\mathbb{N}[q] = \{ \sum_{k=0}^{n} a_k q^k \mid a_k \in \mathbb{N}, n \in \mathbb{N} \}$$

is the set of polynomials in the variable q with non-negative integer coefficients and we assume $0 \in \mathbb{N}$.

Further, with ω_d we denote a primitive d-th root of unity. We should think of an element $c \in C$ and $\omega_{ord(c)}$ as being linked because they have the same order in their respective groups.

Given these ingredients, we can define the cyclic sieving phenomenon [1, page 18].

Definition 3.1. The triple (X, C, f(q)) exhibits the *cyclic sieving phenomenon* (abbreviated CSP) if for all $c \in C$ we have

$$|X^c| = f(\omega_{ord(c)}). \tag{3.1}$$

In words, the triple (X, C, f(q)) exhibits the cyclic sieving phenomenon, if the number of fixed points of any group element of C is equal to the evaluation of the polynomial f(q) in a primitive ord(c)-th root of unity.

Observe that using linear algebra it is always possible to find some polynomial which will satisfy the system of equations given by (3.1). But the point is that f(q) should be a polynomial naturally associated with the set X; we will think of f(q) as a q-enumerator or generating function for X.

At first blush it may seem strange that this result would even count something, but we will briefly see some examples. Most proofs of cyclic sieving phenomena fall into two broad categories: those involving explicit evaluation of both sides of (3.1) and those using representation theory. At first we will consider an example of the CSP and show that (3.1) holds by explicitly evaluating both sides of the equation.

3.1 A First Example

This section follows closely the survey [2, pages 2 – 10], where we use a slightly different approach for the proof using representation theory.

Definition 3.2. A *multiset* on $\mathbb{N}_n$ is an unordered set of elements of $\mathbb{N}_n$ where repetition is allowed.

We define our X to be

$$X = \left(\!\binom{\mathbb{N}_n}{k}\!\right) := \{M \mid M \text{ is a multiset on } \mathbb{N} \text{ with } k \text{ elements}\}.$$

It is a well-known fact that

$$\left|\left(\!\binom{\mathbb{N}_n}{k}\!\right)\right| = \binom{n+k-1}{k}. \tag{3.2}$$

For the group, we take one generated by an n-cycle:

$$C_n = \langle (1 \cdots n) \rangle.$$

If we take for example $n = 3$ and $k = 2$, then

$$X = \{\{1,1\},\{2,2\},\{3,3\},\{1,2\},\{1,3\},\{2,3\}\} \text{ and } C_3 = \{e,(123),(132)\}.$$

The action of $c = (123)$ on X is then

$$\begin{array}{lll} c(\{1,1\}) = \{2,2\}, & c(\{2,2\}) = \{3,3\}, & c(\{3,3\}) = \{1,1\}, \\ c(\{1,2\}) = \{2,3\}, & c(\{1,3\}) = \{1,2\}, & c(\{2,3\}) = \{1,3\}. \end{array}$$

The polynomial for the CSP should be a polynomial naturally associated with the set X. Hence in view of (3.2), a natural choice for our CSP polynomial is

$$f(q) = \begin{bmatrix} n+k-1 \\ k \end{bmatrix}_q.$$

3.1.1 A Proof by Explicit Evaluation

To prove that this triple exhibits the CSP by explicit evaluation, we need some more results. Another way of of expressing a multiset M on $\mathbb{N}_n$ is $M = \{1^{m_1}, \dots, n^{m_n}\}$, where m_i is the multiplicity of i in M. For example:

$$\begin{aligned} N &:= \{1, 1, 2, 2, 2, 5\} \\ &= \{1^2, 2^3, 5\}. \end{aligned}$$

Definition 3.3. Let $L = \{1^{l_1}, \dots, n^{l_n}\}$ and $M = \{1^{m_1}, \dots, n^{m_n}\}$ be two multisets. The *disjoint union* is the multiset

$$L \sqcup M := \{1^{l_1+m_1}, \dots, n^{l_n+m_n}\}.$$

We also want to apply the disjoint union $\sqcup$ to cycles in $\mathcal{S}_n$, in which case we consider each cycle as a set (which is just a multiset with all multiplicities 0 or 1). To illustrate, $(123) \sqcup (124) \sqcup (234) = \{1^2, 2^3, 3^2, 4^2\}$.

Lemma 3.4. Let $\pi \in \mathcal{S}_n$ have disjoint cycle decomposition $\pi = c_1 \cdots c_k$. Then $\pi(M) = M$ if and only if M can be written as

$$M = c_{l_1} \sqcup \cdots \sqcup c_{l_m}$$

for some $1 \le l_1 \le \cdots \le l_m \le k$.

Proof. Assume $M = c_{l_1} \sqcup \cdots \sqcup c_{l_m}$. If c is a cycle of π and $\bar{c}$ its corresponding set, then $\pi(\bar{c}) = \bar{c}$, since π merely permutes the elements of $\bar{c}$ between themselves. Therefore $\pi(M) = M$.

Assume $\pi(M) = M$. Suppose M is not such a disjoint union. Then there must be some cycle c of π and $i, j \in \mathbb{N}_n$ such that $c(i) = j$ but i and j have different multiplicities in M. But then, $\pi(M) \neq M$, because the cycle decomposition is disjoint. □

To illustrate the forward direction, let $\pi = (123)(45)$. If M is not a disjoint union of cycles (123) and (45), then the multiplicities of elements of these cycles must differ in M, say $M = \{4^2, 5\}$. But then, M can not be fixed by π, in contradiction to the assumption.

Now we can evaluate the number of fixed points $|X^c|$ for an element $c \in C_n$. With $d \mid k$ we denote, that d divides k. Recall that if $c \in C_n$ has order d, then by Lagrange's Theorem we have $d \mid n$.

Lemma 3.5. If $X = \binom{\mathbb{N}_n}{k}$ and $c \in C_n$ has order d, then

$$|X^c| = \begin{cases} \binom{n/d+k/d-1}{k/d} & \text{if } d \mid k, \\ 0 & \text{otherwise.} \end{cases}$$

Proof. Since c is a power of $(1 \cdots n)$ with order d, the cycle decomposition of c must consist of n/d cycles each of length d.

Assume d does divide k. Then by Lemma 3.4, the fixed points of c are those multisets obtained by choosing k/d of the n/d cycles of c with repetition allowed, as $|M| = k$ and $k/d \cdot d = k$.

Assume d does not divide k. If M is a multiset, then $|M| = k$ implies that M can not be the disjoint union of cycles of c: This union produces a set whose cardinality is a multiple of d. Then Lemma 3.4 yields that c does not have any fixed points, where a point here is a multiset. □

It remains to evaluate the right side of (3.1), namely $f(\omega_{\mathrm{ord}(c)})$. For this we need the following lemma.

Lemma 3.6. Suppose $m, n \in \mathbb{N}$ satisfy $m \equiv n \pmod d$ and let ω_d be a d-th root of unity. Then

$$\lim_{q \to \omega_d} \frac{[m]_q}{[n]_q} = \begin{cases} \frac{m}{n} & \text{if } n \equiv 0 \pmod d, \\ 1 & \text{otherwise.} \end{cases}$$

Proof. Let $m \equiv n \equiv r \pmod d$ where $0 \leq r < d$. Since

$$\begin{aligned} 1 + \omega_d + \cdots + \omega_d^{d-1} &= \frac{1 - \omega_d^d}{1 - \omega_d} \\ &= 0 \end{aligned}$$

and $m - 1 = dt + r - 1$ for $t \in \mathbb{N}$, we get

$$\begin{aligned} [m]_{\omega_d} &= 1 + \omega_d + \cdots + \omega_d^{m-1} \\ &= \underbrace{1 + \cdots + \omega_d^{d-1}}_{=0} + \underbrace{\omega_d^d + \cdots + \omega_d^{2d-1}}_{=0} + \cdots + \underbrace{\omega_d^{dt} + \cdots + \omega_d^{dt+r-1}}_{1+\cdots+\omega_d^{dt}\omega_d^{r-1}} \\ &= 1 + \omega_d + \cdots + \omega_d^{r-1} \\ &= [n]_{\omega_d}. \end{aligned}$$

Hence if $r \neq 0$, then $[n]_{\omega_d} \neq 0$ and $\frac{[m]_{\omega_d}}{[n]_{\omega_d}} = 1$.

If $r = 0$, then $n = ld$ and $m = kd$ for certain $l, k \in \mathbb{N}$. It follows

$$\begin{aligned} \frac{[m]_q}{[n]_q} &= \frac{1 + q + \cdots + q^{m-1}}{1 + q + \cdots + q^{n-1}} \\ &= \frac{(1 + q + \cdots + q^{d-1})(1 + q^d + q^{2d} + \cdots + q^{(k-1)d})}{(1 + q + \cdots + q^{d-1})(1 + q^d + q^{2d} + \cdots + q^{(l-1)d})} \\ &= \frac{1 + q^d + q^{2d} + \cdots + q^{m-d}}{1 + q^d + q^{2d} + \cdots + q^{n-d}}. \end{aligned}$$

We get

$$\lim_{q\to\omega_d} \frac{[m]_q}{[n]_q} = \frac{m}{n}$$

as desired. □

We will use Lemma 3.6 a lot, since we will work often with q-binomial coefficients; especially when we discuss Catalan objects in Chapter 7.

With the previous lemma we can evaluate the polynomial in our CSP triple.

Lemma 3.7. Let ω_d be a d-th root of unity with $d \mid n$. Then

$$\begin{bmatrix} n+k-1 \\ k \end{bmatrix}_{\omega_d} = \begin{cases} \binom{n/d+k/d-1}{k/d} & \text{if } d \mid k, \\ 0 & \text{otherwise.} \end{cases}$$

Proof. Let's investigate the left hand side:

$$\begin{aligned} \begin{bmatrix} n+k-1 \\ k \end{bmatrix}_{\omega_d} &= \frac{[n+k-1]_{\omega_d}!}{[k]_{\omega_d}![n-1]_{\omega_d}!} \\ &= \frac{[n+k-1]_{\omega_d}\cdots[n]_{\omega_d}}{[k]_{\omega_d}!}. \end{aligned}$$

Since $d \mid n$, $[n]_{\omega_d} = 0$ and so the product $[n]_{\omega_d}\cdots[n+k-1]_{\omega_d}$ starts with a zero factor and has every d-th factor after that also as zero factor, with all other factors being non-zero. The product $[1]_{\omega_d}\cdots[k]_{\omega_d}$ has also every d-th factor a zero factor but starts with $d-1$ non-zero factors. The numerator and denominator have the same amount of factors and it follows that the number of zero factors of the numerator is always greater or equal to the number of zero factors of the denumerator, with equality if and only if d divides k. This gives the "otherwise" case.

If $d \mid k$, using Lemma 3.6 we get

$$\begin{aligned} \begin{bmatrix} n+k-1 \\ k \end{bmatrix}_{\omega_d} &= \lim_{q\to\omega}\left(\frac{[n]_q}{[k]_q}\cdot\frac{[n+1]_q}{[1]_q}\cdot\frac{[n+2]_q}{[2]_q}\cdots\frac{[n+k-1]_q}{[k-1]_q}\right) \\ &= \frac{n}{k}\cdot 1\cdots 1\cdot\frac{n+d}{d}\cdot 1\cdots 1\cdot\frac{n+k-d}{k-d}\cdot 1\cdots 1 \\ &= \frac{n/d}{k/d}\cdot\frac{n/d+1}{1}\cdot\frac{n/d+2}{2}\cdots\frac{n/d+k/d-1}{k/d-1} \\ &= \binom{n/d+k/d-1}{k/d}. \end{aligned}$$

as desired. □

Finally we can state the following theorem.

Theorem 3.8. The cyclic sieving phenomenon is exhibited by the triple

$$\left(\left(\binom{\mathbb{N}_n}{k}\right), \langle(1\cdots n)\rangle, \begin{bmatrix} n+k-1 \\ k \end{bmatrix}_q\right).$$

Proof. We have to check that the equation (3.1) holds. We get the left hand side from Lemma 3.5 and the right hand side from Lemma 3.7. Since they coincide, the claim follows. □

3.1.2 A Proof using Representation Theory

Another way of proving the CSP property (3.1) is using representation theory. First we set up the tools to reprove it, where we will use the notions introduced in Section 2.2.

Definition 3.9. Let V be a vector space. Then $V^{\otimes k}$ denotes the *k-fold tensor product* of V.

If we take $V = \mathbb{C}\{1,\ldots,n\}$ which has basis $B = \{v_i \mid 1 \le i \le n\}$, then $V^{\otimes k}$ has a basis of the form

$$\{v_{j_1} \otimes \cdots \otimes v_{j_k} \mid 1 \le j_1 \le n, \ldots, 1 \le j_k \le n\}.$$

We define a group action of the symmetric group $\mathcal{S}_k$ on $V^{\otimes k}$ as follows. For any $\sigma \in \mathcal{S}_k$ and $x_{i_1} \otimes \cdots \otimes x_{i_k} \in V^{\otimes k}$, we let

$$\sigma(x_{i_1} \otimes \cdots \otimes x_{i_k}) := x_{i_{\sigma(1)}} \otimes \cdots \otimes x_{i_{\sigma(k)}}$$

and extend this linearly to $V^{\otimes k}$. Thus each $\sigma \in \mathcal{S}_k$ defines a linear operator $\sigma : V^{\otimes k} \to V^{\otimes k}$.

Definition 3.10. A k-fold tensor $A \in V^{\otimes k}$ is *symmetric* if

$$\sigma(A) = A$$

for all permutations $\sigma \in \mathcal{S}_k$. The set of symmetric tensors in $V^{\otimes k}$ will be denoted by $\mathrm{Sym}_k(n)$.

Definition 3.11. Let $S : V^{\otimes k} \to \mathrm{Sym}_k(n)$ be the linear operator defined by

$$S := \frac{1}{k!} \sum_{\sigma \in \mathcal{S}_k} \sigma.$$

Note that given any $\sigma \in \mathcal{S}_k$, it holds $\sigma \circ S = S \circ \sigma = S$. Hence for any $\sigma \in \mathcal{S}_k$ we have $\sigma \circ S(A) = S(A)$, so $S(A)$ is a symmetric tensor, which explains the domain of S is $\mathrm{Sym}_k(n)$. Here $\circ$ denotes the composition of the linear operator σ and S. The next lemma allows us to decide if a k-fold tensor is symmetric and shows that the symmetric tensors compose an eigenspace of S.

Lemma 3.12. A k-fold tensor $A \in V^{\otimes k}$ is symmetric if and only if

$$S(A) = \frac{1}{k!} \sum_{\sigma \in \mathcal{S}_k} \sigma(A) = A.$$

Proof. Clearly, if A is symmetric, then

$$S(A) = \frac{1}{k!} \sum_{\sigma \in \mathcal{S}_k} \sigma(A) = \frac{1}{k!} \sum_{\sigma \in \mathcal{S}_k} A = A.$$

Conversely, if $S(A) = A$, then

$$\sigma(A) = \sigma(S(A)) = \sigma \circ S(A) = S(A) = A.$$

for any $\sigma \in \mathcal{S}_k$ and so A is symmetric. □

In other words, a symmetric tensor is an eigenvector of the linear operator S with eigenvalue 1. $\mathrm{Sym}_k(n)$ is the 1-eigenspace of S.

For any $v_{j_1}, \ldots, v_{j_k} \in \mathbb{C}\{1, \ldots, n\}$ with $j_1, \ldots, j_k \in \mathbb{N}$, we write

$$v_{j_1} \cdots v_{j_k} := S(v_{j_1} \otimes \cdots \otimes v_{j_k}) = \frac{1}{k!} \sum_{\sigma \in \mathcal{S}_k} v_{j_{\sigma(1)}} \otimes \cdots \otimes v_{j_{\sigma(k)}}.$$

Since for all $\sigma \in \mathcal{S}_k$ we have $\sigma S = S$, every permutation of the basis tensors $v_{j_1} \otimes \cdots \otimes v_{j_k}$ of $V^{\otimes k}$ yield the same tensor under S, hence the term $v_{j_1} \cdots v_{j_k}$ depends only on the number of times each v_i is in this product and we may write

$$v_{j_1} \cdots v_{j_k} = v_1^{p_1} \cdots v_n^{p_n},$$

where p_i is the multiplicity of the occurrence of v_1 in $v_{j_1} \ldots v_{j_k}$. Note that $p_1, \ldots, p_k$ are non-negative integers satisfying $p_1 + \cdots + p_n = k$, as our tensor is k-fold.

Proposition 3.13. Let $\{v_1, \ldots, v_n\}$ be a basis of $\mathbb{C}\{1, \ldots, n\}$. Then

$$\{v_{j_1} \cdots v_{j_k} \mid 1 \leq j_1 \leq \cdots \leq j_k \leq n\}$$

or, explicitly,

$$\Big\{\frac{1}{k!}\sum_{\sigma\in S_k} v_{j_{\sigma(1)}}\otimes\cdots\otimes v_{j_{\sigma(k)}} \mid 1\le j_1\le\cdots\le j_k\le n\Big\}$$

is a basis of $\mathrm{Sym}_k(n)$. Furthermore,

$$\dim_{\mathbb{C}}(\mathrm{Sym}_k(n)) = \binom{n+k-1}{k}.$$

Proof. Since $B = \{v_{j_1}\otimes\cdots\otimes v_{j_k} \mid 1\le j_1\le n,\dots,1\le j_k\le n\}$ is a basis of $V^{\otimes k}$ and S maps $V^{\otimes k}$ to $\mathrm{Sym}_k(n)\subseteq V^{\otimes k}$, the set

$$S(B) = \{v_{j_1}\cdots v_{j_k} \mid 1\le j_1\le\cdots\le j_k\le n\} = \{v_1^{p_1}\cdots v_k^{p_n} \mid p_1+\cdots+p_n = k\}$$

spans $\mathrm{Sym}_k(n)$.

Let $v_1^{p_1}\cdots v_k^{p_n}$ and $v_1^{q_1}\cdots v_k^{q_n}$ be two tensors in $\mathrm{Sym}_k(n)$ with $(p_1,\dots,p_n)\neq(q_1,\dots,q_n)$. Then these tensors are respectively linear combinations of two non-intersecting subsets of basis elements of $V^{\otimes k}$ and therefore linearly independent.

The cardinality of S(B) is precisely the number of compositions of k into n parts, i.e. $\binom{n+k-1}{k}$. □

The cyclic group $C_n = \langle(1\cdots n)\rangle$ acts on $\mathbb{C}\{1,\dots,n\}$ by (2.2) and so there is an induced action on $\mathrm{Sym}_k(n)$ given by

$$c(v_{j_1}\cdots v_{j_k}) = c(v_{j_1})\cdots c(v_{j_k}).$$

If $c\in C_n$, then let $\rho(c),\rho'(c)$ denote the associated linear transformation on $\mathbb{C}\{1,\dots,n\}$ and $\mathrm{Sym}_k(n)$ respectively. Similarly, let χ_ρ and χ'_ρ be the respective characters of C_n acting on $\mathbb{C}\{1,\dots,n\}$ and $\mathrm{Sym}_k(n)$.

Suppose that there exists a basis $\mathcal{B} = \{b_1,\dots,b_n\}$ for $\mathbb{C}\{1,\dots,n\}$ such that $\rho(c)$ is diagonalizable, namely

$$\rho(c) = \mathrm{diag}(x_1,\dots,x_n), \tag{3.3}$$

where $x_1,\dots,x_n$ are the eigenvalues of the basisvectors $b_1,\dots,b_n$.

In the next chapter we will prove, that such a basis exists. Since $\mathcal{B}$ is a basis for $\mathbb{C}\{1,\dots,n\}$,

$$\mathcal{B}' = \{b_{j_1}\cdots b_{j_k} \mid 1\le j_1\le\cdots\le j_k\le n\}$$

is a basis for $\mathrm{Sym}_k(n)$. This is the crucial property of the space of symmetric tensors which makes us choose to work with them rather than in the original

permutation module. If $\rho(c)$ is diagonalized in a basis $\mathcal{B}$, then every basisvector is an eigenvector for $\rho(c)$. The same is true for $\mathcal{B}'$ and $\rho'(c)$ acting on $\mathrm{Sym}_k(n)$. More precisely,

$$c(b_{j_1}\cdots b_{j_k}) = c(b_{j_1})\cdots c(b_{j_k}) = x_{j_1}\cdots x_{j_k} b_{j_1}\cdots b_{j_k}.$$

Therefore we have

$$\rho'(c) = \mathrm{diag}(x_{j_1}\cdots x_{j_k} \mid 1 \le j_1 \le \cdots \le j_k \le n)$$

and

$$\chi'_\rho(c) = \sum_{1\le j_1\le\cdots\le j_k\le n} x_{j_1}\cdots x_{j_k}.$$

The expression on the right-hand side is called a *complete homogeneous symmetric polynomial* and denoted $h_k(x_1,\ldots,x_n)$. It is called complete homogeneous, because it is the sum of all monomials of degree k in the x_j. It is a symmetric polynomial because it is invariant under permutation of the subscripts of the variables. To make use of it, we need to relate complete homogeneous symmetric functions to q-binomial coefficients. This is done by taking the principal specialization which sets $x_i = q^{i-1}$ for all i.

Lemma 3.14. For $n \ge 1$ and $k \ge 0$ we have

$$h_k(1, q, \ldots, q^{n-1}) = \begin{bmatrix} n+k-1 \\ k \end{bmatrix}_q.$$

Proof. We do a double induction on n and k. For $n = 1$ we have

$$h_k(1) = 1, \text{ and } \begin{bmatrix} k \\ k \end{bmatrix}_q = 1.$$

For $k = 0$ clearly both sides are 1 as well.

Assume $n \ge 2$ and $k \ge 1$. By splitting the sum $h_k(x_1,\ldots,x_n)$ into those terms which do not contain x_n and those which do, we obtain the recursion

$$h_k(x_1,\ldots,x_n) = h_k(x_1,\ldots,x_{n-1}) + x_n h_{k-1}(x_1,\ldots,x_n).$$

Specializing yields

$$h_k(1,\ldots,q^{n-1}) = h_k(1,\ldots,q^{n-2}) + q^{n-1} h_{k-1}(1,\ldots,q^{n-1}).$$

Regarding (2.1), we can prove that it holds

$$\begin{bmatrix} n \\ k \end{bmatrix}_q = \begin{bmatrix} n-1 \\ k \end{bmatrix}_q + q^{n-k} \begin{bmatrix} n-1 \\ k-1 \end{bmatrix}_q .$$

Substituting $n+k-1$ for n, we get the desired result. □

We are ready now to reprove Theorem 3.8.

Proof of Theorem 3.8. Recall that $\rho((1\cdots n))$ is a linear transformation from $\mathbb{C}\{1,\ldots,n\}$ to itself. The map has the characteristic poylnomial x^n-1 with roots (eigenvalues) $1,\omega_n,\ldots,\omega_n^{n-1}$. Since these roots are distinct, by linear algebra there exists a diagonalizing basis $\mathcal{B}$ of $\mathbb{C}\{1,\ldots,n\}$ with

$$\rho((1\cdots n)) = \operatorname{diag}(1,\omega_n,\ldots,\omega_n^{n-1}).$$

But any $c \in C_n$ is of the form $(1\cdots n)^i$ for some i and hence, since we have a diagonal representation,

$$\rho((1\cdots n)^i) = \operatorname{diag}(1^i,\omega_n^i,\ldots,\omega_n^{(n-1)i}) = \operatorname{diag}(1,\omega,\ldots,\omega^{n-1}),$$

where $\omega = \omega_n^i$ is a primitive $\operatorname{ord}((1\cdots n)^i)$-th root of unity. Using the space of k-fold symmetric tensors $\operatorname{Sym}_k(n)$, which has basis $\mathcal{B}'$ as defined before, we get

$$\chi'_\rho(c) = h_k(1,\omega,\ldots,\omega^{n-1}) = \begin{bmatrix} n+k-1 \\ k \end{bmatrix}_\omega$$

by the previous lemma.

Now we make the connection to the C_n-module $\mathbb{C}\binom{\mathbb{N}_n}{k}$, such that we can use its character to conclude the proof. Since $\mathbb{C}\binom{\mathbb{N}_n}{k}$ and $\operatorname{Sym}_k(n)$ are vector spaces over $\mathbb{C}$ with the same dimension, they are isomorphic. Let

$$v = c_1 k_{j_1}\cdots k_{j_k} + \cdots + c_m k_{j_1}\cdots k_{j_k} \in \mathbb{C}\left(\binom{\mathbb{N}_n}{k}\right),$$
$$w = c_1 b_{j_1}\cdots b_{j_k} + \cdots + c_m b_{j_1}\cdots b_{j_k} \in \operatorname{Sym}_k(n),$$

where $c_i \in \mathbb{C}, k_{j_1}\cdots k_{j_k} \in \binom{\mathbb{N}_n}{k}$, $1 \le k_{j_1} \le \cdots \le k_{j_k} \le n$, $1 \le b_{j_1} \le \cdots b_{j_k} \le n$ and $k_{j_i} = b_{j_i}$ for all j_i. Note that in this case the dots in $k_{j_1}\cdots k_{j_k}$ do not corresspond to a multiplication, as $k_{j_1}\cdots k_{j_k}$ denotes a multiset. Take a $c \in C_n$ and consider

the linear bijection ϕ which maps v to w, namely $\phi(\mathrm{v}) = \mathrm{w}$. Then we have

$$\begin{aligned}
\phi(\mathrm{c}(\mathrm{v})) &= \phi(\mathrm{c}_1\mathrm{c}(\mathrm{k}_{\mathrm{j}_1})\cdots\mathrm{c}(\mathrm{k}_{\mathrm{j}_k}) + \cdots + \mathrm{c}_\mathrm{m}\mathrm{c}(\mathrm{k}_{\mathrm{j}_1})\cdots\mathrm{c}(\mathrm{k}_{\mathrm{j}_k})) \\
&= \mathrm{c}_1\phi(\mathrm{k}_{\mathrm{j}_{\mathrm{c}(1)}}\cdots\mathrm{k}_{\mathrm{j}_{\mathrm{c}(\mathrm{k})}}) + \cdots + \mathrm{c}_\mathrm{m}\phi(\mathrm{k}_{\mathrm{j}_{\mathrm{c}(1)}}\cdots\mathrm{k}_{\mathrm{j}_{\mathrm{c}(\mathrm{k})}}) \\
&= \mathrm{c}_1\mathrm{b}_{\mathrm{j}_{\mathrm{c}(1)}}\cdots\mathrm{b}_{\mathrm{j}_{\mathrm{c}(\mathrm{k})}} + \cdots + \mathrm{c}_\mathrm{m}\mathrm{b}_{\mathrm{j}_{\mathrm{c}(1)}}\cdots\mathrm{b}_{\mathrm{j}_{\mathrm{c}(\mathrm{k})}} \\
&= \mathrm{c}_1\mathrm{c}(\mathrm{b}_{\mathrm{j}_1})\cdots\mathrm{c}(\mathrm{b}_{\mathrm{j}_k}) + \cdots + \mathrm{c}_\mathrm{m}\mathrm{c}(\mathrm{b}_{\mathrm{j}_1})\cdots\mathrm{c}(\mathrm{b}_{\mathrm{j}_k}) \\
&= \mathrm{c}_1\mathrm{c}(\mathrm{b}_{\mathrm{j}_1}\cdots\mathrm{b}_{\mathrm{j}_k}) + \cdots + \mathrm{c}_\mathrm{m}\mathrm{c}(\mathrm{b}_{\mathrm{j}_1}\cdots\mathrm{b}_{\mathrm{j}_k}) \\
&= \mathrm{c}_1\mathrm{c}(\phi(\mathrm{k}_{\mathrm{j}_1}\cdots\mathrm{k}_{\mathrm{j}_k})) + \cdots + \mathrm{c}_\mathrm{m}\mathrm{c}(\phi(\mathrm{k}_{\mathrm{j}_1}\cdots\mathrm{k}_{\mathrm{j}_k})) \\
&= \mathrm{c}(\phi(\mathrm{c}_1\mathrm{k}_{\mathrm{j}_1}\cdots\mathrm{k}_{\mathrm{j}_k} + \cdots + \mathrm{c}_\mathrm{m}\mathrm{k}_{\mathrm{j}_1}\cdots\mathrm{k}_{\mathrm{j}_k})) \\
&= \mathrm{c}(\phi(\mathrm{w})).
\end{aligned}$$

and therefore $\mathbb{C}\left(\!\binom{\mathbb{N}_\mathrm{n}}{\mathrm{k}}\!\right) \cong \mathrm{Sym}_\mathrm{k}(\mathrm{n})$ as C_n-modules. Let χ''_ρ be the character of the C_n-module $\mathbb{C}\left(\!\binom{\mathbb{N}_\mathrm{n}}{\mathrm{k}}\!\right)$. Since two isomorphic modules have the same character, with

$$\chi''_\rho(\mathrm{c}) = |\{\mathrm{M} \in \left(\!\binom{\mathbb{N}_\mathrm{n}}{\mathrm{k}}\!\right) \mid \mathrm{c}(\mathrm{M}) = \mathrm{M}\}|$$

the proof is completed. □

We explicate the last step: If an element c of the group C_n acts on the set $\mathbb{C}\left(\!\binom{\mathbb{N}_\mathrm{n}}{\mathrm{k}}\!\right)$, then $\rho''(\mathrm{c})$ is the permutation matrix for c's action. Therefore, only the elements fixed under c contribute to the trace of $\rho''(\mathrm{c})$.

3.2 Application of CSP to Problems of Burnside Type

When discussing the cyclic sieving phenomenon, we essentially present a triple which exhibits the latter. There is however a natural application of the CSP, whenever one is searching for the number of fixed points of an element of a cyclic group that acts on a finite set. Note that this only worthwhile, when we prove the CSP by using representation theory; if we prove the CSP by explicit evaluation, then we will work out the number of fixed points in the first place and so there is no point in using the polynomial. Such an application could be of use when solving problems which are of Burnside Type.

The Lemma of Burnside allows us to count the orbits, respectively the equivalence classes, induced by a permutation group. To do so, it requires to know the number of fixed points of the group elements acting on a given set. Here, the CSP could help to find these fixed points. The Lemma of Burnside can be found in [4,

Lemma 7.2].

There is a natural action on $\mathbb{N}_n$ induced by a permutation group:

$$* : \begin{cases} G \times \mathbb{N}_n \to \mathbb{N}_n, \\ (\pi, i) \mapsto \pi(i). \end{cases}$$

To prove Burnside's Lemma, we need the following lemma. Recall that G_i is the stabilizer of g and $G * i$ the orbit of i under G.

Lemma 3.15. Let $(G, \circ)$ be a permutation group acting on $\mathbb{N}_n$ and $i \in \mathbb{N}_n$. Then it holds

$$|G * i| = [G : G_i],$$

where $[G : G_i]$ is the index of G_i in G.

□

It is a well known fact from algebra that $|G| = [G : G_i]|G_i|$ and thus we get $|G| = |G * i||G_i|$.

Lemma 3.16. (Lemma of Burnside) Let $(G, \circ)$ be a permutation group acting on a set M. Further, let t(G) be the number of orbits induced by $(G, \circ)$ on M. Then

$$t(G) = \frac{1}{|G|} \sum_{\pi \in G} |M^\pi|.$$

Proof. We prove the lemma by double counting. Without loss of generality assume $M = \mathbb{N}_n$. Consider the stabilizers $G_i, i \in \mathbb{N}_n$, as well as the number of fixed points $|\mathbb{N}_n^\pi|$, for each $\pi \in G$. Then the following equality holds:

$$\sum_{\pi \in G} |\mathbb{N}_n^\pi| = \sum_{i=1}^{n} |G_i|.$$

Now instead of taking the sum from i=1 to n on the right hand side, we can identify all i which belong to the same orbit $G * j$. Then the result becomes

$$\sum_{\pi \in G} |\mathbb{N}_n^\pi| = \sum_{j=1}^{t(G)} |G_j||G * j|$$

since instead of summing up all the stabilizers of elements in the same orbit, we can multiply one such stabilizier with the elements in the orbit, as the stabilizers have the same cardinality. Since $|G| = |G * i||G_i|$, the claim follows. □

With Burnside we can now answer questions of the following type.

Question Given a necklace with 6 places for beads. How many different necklaces could we compose, if we have 2 different colors?

If the necklace is fix, there are 2^6 different colorings. However, since the necklace can be rotated, we have to identify all the colorings, which can be rotated in one another. Hence we are searching for the number of orbits the cyclic group $\langle(123456)\rangle$ induces on the set M of colorings, where $|M| = 2^6$.

Answer Working with Burnside, we have to carry out the characters of the elements of $\langle(123456)\rangle$. For example, the identitiy $(1)(2)(3)(4)(5)(6)$ has 2^6 fixed points, since it fixes every coloring. The cycle $(123456)^2 = (135)(246)$ fixes 2^2 elements in M, since we have to color the elements of both cycles with the same color. We get the following table for the fixed points of $C_6 = \langle(123456)\rangle$:

$c \in \mathbf{C_6}$	**Order**	$\mathbf{\lvert X^c \rvert}$
e	1	64
c	6	2
c^2	3	4
c^3	2	8
c^4	3	4
c^5	6	2

Table 3.1: Fixed points table for C_6.

Using Burnside's Lemma we get

$$\begin{aligned} t(G) &= \frac{1}{6}(2 \cdot 2 + 2 \cdot 4 + 8 + 64) \\ &= 14 \end{aligned}$$

orbits. And hence there are 14 different colorings.

We show now, that there is a cyclic sieving phenomenon hidden in this example. In this case, $X = M$ is the set of colorings and $C = \langle(123456)\rangle$ is the cyclic group. It remains to find a polynomial f(q) such that this triple satisfies (3.1).

First note, that the set M is equal to the set of binary words of length 6, namely $M = \{0,1\}^6$. We denote this set as BW(6). Therefore, we can identify our set of necklaces with the set of binary words. Again, as in our first example, the polynomial for the CSP should be a polynomial naturally associated with the set X. Since a binary word $w \in BW(6)$ describes a lattice path

with north-east steps $S = \{(1,0),(0,1)\}$, we can make use of Proposition 2.17. Starting from the origin (0,0), a lattice path of length 6 can have an endpoint in $\{(0,6),(1,5),(2,4),(3,3),(4,2),(5,1),(6,0)\}$. The generating function for lattice paths by area under path of length 6 with north-east steps $S = \{(1,0),(0,1)\}$ is thus

$$f(q) = \sum_{k=0}^{6} \begin{bmatrix} 6 \\ k \end{bmatrix}_q .$$

Computing this sum by working out the binomial coefficients, we get the following polynomial:

$$f(q) = 7 + 5q + 8q^2 + 9q^3 + 11q^4 + 9q^5 + 7q^6 + 4q^7 + 3q^8 + q^9.$$

Now we have to evaluate this polynomial in the d-th roots of unity. Let $\omega_d = e^{\frac{2\pi i}{d}}$ denote these roots. We get the following value table:

ω_d	$f(\omega_d)$
1	64
$e^{\frac{2\pi i}{2}}$	8
$e^{\frac{2\pi i}{3}}$	4
$e^{\frac{2\pi i}{6}}$	2

Table 3.2: Value table for f(q).

Comparing the value table with the fixed point table above, we see that (3.1) holds and hence the CSP is exhibited by the triple

$$(BW(6), \langle(123456)\rangle, \sum_{k=0}^{6} \begin{bmatrix} 6 \\ k \end{bmatrix}_q). \tag{3.4}$$

We are now able to answer the question using the polynomial of our CSP triple. However, as we mentioned, in this case we have no additional value as we proved the CSP property by explicit evaluation; the number of fixed points were already known. We presented the above example to illustrate, how we possibly could apply the cyclic sieving phenomenon to such problems. But to have an additional value, we would have to prove such results by using representation theory.

Of course, (3.4) raises the question of a generalization for binary words BW(n) for any $n \in \mathbb{N}$. We will discuss this later on in the Chapter 6 about words.

Chapter 4

A Representation Theory Paradigm

The goal of this chapter is to provide a tool for proving that a certain triple exhibits the CSP by using representation theory. To do so, we need the following theorem which collects together three standard results from representation theory, see e.g. [8, pages 4 – 10].

Further, we will justify (3.3), where we assumed that there exists a basis for $\mathbb{C}\{1, \ldots, n\}$ such that $\rho(c)$ is diagonalizable. This chapter will follow closely the survey [2, pages 10 – 11].

Theorem 4.1. Let G be a finite group and consider G-modules which are vector spaces over $\mathbb{C}$.

(1) The number of pairwise non-isomorphic irreducible G-modules is finite and equals to the conjugacy classes of G.

(2) Every G-module can be written as a direct sum of irreducible G-modules.

(3) Two G-modules are isomorphic if and only if they have the same character.

□

Note that if G is not finite, these results may not hold. Furthermore, we already used the forward direction of (3) in Section 3.1.2.

We now want to investigate the irreducible representations of a cyclic group C_n, which we assume to have order n. The dimension of a C_n-module V is its usual vector space dimension. If the dimension of V is 1, then V must be irreducible, so we can look for the dimension 1 modules of C_n.

The cyclic group C_n consists of powers $1, c, \ldots, c^{n-1}$ where $c^n = 1$. For any number $h = 0, \ldots, n-1$, we define a map

$$\rho^h(c^k) = e^{\frac{2\pi ikh}{n}}.$$

This gives n non-isomorphic degree 1 representations of the cyclic group C_n. Hence we have found n irreducible G-modules of C_n carrying a representation ρ^h, one for each n-th root of unity: $V^{(h)}, 0 \leq h \leq n-1$.

Let $c^i, c^j \in C_n$. Then

$$c^i c^j = c^{i+j} = c^{j+i} = c^j c^j,$$

so C_n is abelian. Therefore C_n has n conjugacy classes [8, page 14] and thus by (1) of the Theorem 4,1, we have found all the irreducible representations.

Now given any C_n-module, V, part (2) of Theorem 4.1 says we have a module isomorphism

$$V \cong \bigoplus_{i=0}^{n-1} a_i V^{(i)},$$

where $a_i V^{(i)}$ denotes a direct sum of a_i copies of $V^{(i)}$. Consider now the representation $\rho : C_n \to GL(V)$. Since every summand $V^{(i)}$ is one dimensional, the linear transformations $\rho(c), c \in C_n$, are the direct sums of one dimensional linear transformations, and therefore diagonalizable for any basis $\mathcal{B}$. This justifies (3.3). Extend the definition of $V^{(i)}$ to any $i \in \mathbb{N}$ by letting $V^{(i)} = V^{(j)}$ if $i \equiv j \pmod n$. Now given any polynomial $f(q) = \sum_{i \geq 0} m_i q^i$ with non-negative integer coefficients, define a corresponding C_n-module

$$V_f = \bigoplus_{i \geq 0} m_i V^{(i)}.$$

We have the following representation theory paradigm for proving that the CSP holds [2, Theorem 4.2].

Theorem 4.2. The cyclic sieving property holds for the triple $(X, C_n, f(q))$ if and only if one has $\mathbb{C}X \cong V_f$ as C_n-modules.

Proof. Consider the representation $\rho : C_n \to GL(V_f)$. For $c \in C_n$ we have

$$\begin{aligned} \chi_\rho(c) &= \mathrm{Tr}(\rho(c)) \\ &= \sum_{i \geq 0} m_i \rho^i(c) \\ &= f(\omega_{\mathrm{ord}(c)}). \end{aligned}$$

Observe that for any $c \in C_n$, $|X^c|$ is the character value of the module $\mathbb{C}X$. Therefore $|X^c|$ and $f(\omega_{ord(c)})$ are the character values, for a $c \in C_n$, in the modules $\mathbb{C}X$ and V_f, respectively. So the result now follows from Theorem 4.1 (3), since we have that

$$|X^c| = f(\omega_{ord(c)})$$

if and only if $\mathbb{C}X \cong V_f$. □

We will briefly see an application of Theorem 4.2 in the next chapter.

Chapter 5

Pólya's Theory

George Pólya introduced a combinatorial method in 1937 [9] which led to unexpected applications to diverse problems in science such as the enumeration of isomers of chemical compounds. Since then, this method has become a standard tool in algebraic combinatorics. We will use it to find a generalization of Theorem 3.8. Moreover, the representation theory introduced in Chapter 2 and developed further in Chapter 3 will come into play; in addition, we will apply Theorem 4.2 introduced in the previous chapter.

5.1 The Theorems of Pólya

In the following we introduce the notions needed for Pólya's Theorems. The modern version of Pólya's Theorems can be found in [4, pages 82 – 85].

Definition 5.1. Let $(G, \circ)$ be a permutation group of degree n. To each $\pi \in G$ we associate the monomial $z_1^{j_1} \cdots z_n^{j_n}$, where $(j_1, \ldots, j_n)$ is the cycle type of π. Then we call

$$\zeta(G; z_1, \ldots, z_n) := \frac{1}{|G|} \sum_{\pi \in G} z_1^{j_1} \cdots z_n^{j_n}$$

the *cycle index* of $(G, \circ)$.

We give two important examples of cycle indices.

At first we investigate the cycle index of a cyclic group C_n with order n. We can interpret C_n as the permutation group, which acts as rotations on the vertices of a convex n-polygon. If for example $c = (1 \cdots 12)$ is the generator of C_{12}, then

$$c^3 = (1\ 4\ 7\ 10)(2\ 5\ 8\ 11)(3\ 6\ 9\ 12)$$

has 3 cycles of length 4 and thus cycle type (0,0,0,3,0,0,0,0,0,0,0,0). As we have already discussed, every permutation $c \in C_n$ splits into cycles of the same length and has $\frac{n}{d}$ cycles of length d, where with d we denote its order. Therefore we get

$$\zeta(C_n; z_1, \ldots, z_n) = \frac{1}{n} \sum_{d|n} \varphi(d) z_d^{\frac{n}{d}},$$

because in C_n there are $\varphi(d)$ elements of order d, where φ is the Euler's totient function.

In order to investigate the cycle index of the symmetric group, we define $\mathbb{P}_n$ to be the solution set of the diophantine equation $\sum_{k=1}^{n} k j_k = n$. Recall that $h(j_1, j_2, j_3, j_4)$ denotes the number of permutation with cycle type (j_1, j_2, j_3, j_4). By Proposition 2.10 we have

$$\zeta(S_n; z_1, \ldots, z_n) = \frac{1}{n!} \sum_{\mathbb{P}_n} h(j_1, \ldots, j_n) z_1^{j_1} \cdots z_n^{j_n}.$$

To illustrate, we consider the special case $n = 4$:

(j_1, j_2, j_3, j_4)	$h(j_1, j_2, j_3, j_4)$
(4,0,0,0)	1
(2,1,0,0)	6
(1,0,1,0)	8
(0,2,0,0)	3
(0,0,0,1)	6

Table 5.1: Number of permutations with cyclic structure (j_1, j_2, j_3, j_4).

And thus we get

$$\zeta(S_4; z_1, z_2, z_3, z_4) = \frac{1}{24}(z_1^4 + 6z_1^2 z_2 + 8z_1 z_3 + 3z_2^2 + 6z_4). \tag{5.1}$$

To formulate Pólya's Theorems, we need some more definitions. Let $\mathcal{F} = \{\phi_1, \ldots, \phi_r\}$ be a finite set of *figures* and

$$\mathcal{F}^S := \{(\phi_{j_1}, \ldots, \phi_{j_s}) \mid \phi_{j_i} \in \mathcal{F}\}$$

be the set of *configurations* of length s. Let $(G, \circ)$ be a permutation group acting on a set S, with $|S| = s$. Elements of S will be referred to as places. A permutation $\pi \in G$ acts then on $\Gamma \in F^S$ by permuting the places S and with it also the figures

sitting on it. In doing so, a permutation $\pi \in \mathrm{G}$ induces a permutation $\bar{\pi}$ on the set $\mathcal{F}^{\mathrm{s}}$. It is easy to show that for $|\mathcal{F}^{\mathrm{s}}| \geq 2$ the map $\pi \mapsto \bar{\pi}$ is an isomorphism.

As an example, let $\mathcal{F} = \{\circ, \bullet\}$ and $\mathrm{s} = 3$. We have

$$\mathcal{F}^3 = \{(\circ,\circ,\circ), (\circ,\circ,\bullet), (\circ,\bullet,\circ), (\bullet,\circ,\circ), (\circ,\bullet,\bullet), (\bullet,\circ,\bullet), (\bullet,\bullet,\circ), (\bullet,\bullet,\bullet)\}.$$

The permutation $\pi = (231)$ induces on $\mathcal{F}^3$ the permutation $\bar{\pi}$:

$$\begin{aligned}
(\circ,\circ,\circ) &\mapsto (\circ,\circ,\circ),\\
(\circ,\circ,\bullet) &\mapsto (\bullet,\circ,\circ),\\
(\circ,\bullet,\circ) &\mapsto (\circ,\circ,\bullet),\\
(\bullet,\circ,\circ) &\mapsto (\circ,\bullet,\circ),\\
(\circ,\bullet,\bullet) &\mapsto (\bullet,\circ,\bullet),\\
(\bullet,\circ,\bullet) &\mapsto (\bullet,\bullet,\circ),\\
(\bullet,\bullet,\circ) &\mapsto (\circ,\bullet,\bullet),\\
(\bullet,\bullet,\bullet) &\mapsto (\bullet,\bullet,\bullet).
\end{aligned}$$

Let $\bar{\mathrm{G}}$ denote the set of induced permutations of G. Two configurations $\Gamma, \Gamma' \in \mathcal{F}^{\mathrm{s}}$ should be seen as equivalent, if there is a permutation $\bar{\pi} \in \bar{\mathrm{G}}$ such that $\bar{\pi}(\Gamma) = \Gamma'$. We are then interested in the number of orbits (equivalence classes) of $\mathcal{F}^{\mathrm{s}}$ under the action of $(\bar{\mathrm{G}}, \circ)$.

Theorem 5.2. (Pólya's first Theorem) Let $|\mathcal{F}| = \mathrm{r}$. The number of orbits of $\mathcal{F}^{\mathrm{s}}$ under the action of $(\bar{\mathrm{G}}, \circ)$ is

$$\mathrm{t}(\bar{\mathrm{G}}) = \zeta(\mathrm{G}; \mathrm{r}, \ldots, \mathrm{r}),$$

where $\zeta(\mathrm{G}; \mathrm{z}_1, \ldots, \mathrm{z}_{\mathrm{n}})$ is the cycle index of the permutation group $(\mathrm{G}, \circ)$, which acts on the set of places S.

Proof. Since we are searching for the number of orbits, we can use Burnside's Lemma. $|\mathcal{F}^{\mathrm{s}\bar{\pi}}|$ denotes the number of configurations $\Gamma \in \mathcal{F}^{\mathrm{s}}$ that are fixed under $\bar{\pi}$. A configuration Γ is fixed under the permutation of the places, if the permuted places of each cycle of π are all occupied with the same figure. If π has cycle type $(\mathrm{j}_1, \ldots, \mathrm{j}_{\mathrm{n}})$, then $|\mathcal{F}^{\mathrm{s}\bar{\pi}}| = \mathrm{r}^{\mathrm{j}_1 + \cdots + \mathrm{j}_{\mathrm{n}}}$, as we have r different figures to distribute on

the cycles. With Burnside's Lemma it follows

$$\begin{aligned} \mathrm{t}(\bar{\mathrm{G}}) &= \frac{1}{|\mathrm{G}|} \sum_{\bar{\pi} \in \bar{\mathrm{G}}} |\mathcal{F}^{\mathrm{s}\bar{\pi}}| \\ &= \frac{1}{|\mathrm{G}|} \sum_{\pi \in \mathrm{G}} \mathrm{r}^{\mathrm{j}_1 + \cdots + \mathrm{j}_\mathrm{n}} \\ &= \frac{1}{|\mathrm{G}|} \sum_{\pi \in \mathrm{G}} \mathrm{z}_1^{\mathrm{j}_1} \cdots \mathrm{z}_\mathrm{n}^{\mathrm{j}_\mathrm{n}} \big|_{\mathrm{z}_\mathrm{i} = \mathrm{r}} \\ &= \zeta(\mathrm{G}; \mathrm{r}, \ldots, \mathrm{r}). \end{aligned}$$

□

Pólya's first Theorem is a powerful tool to solve many combinatorial problems, but we can provide a refinement of this theorem.

To every figure $\phi_\mathrm{i} \in \mathcal{F}$ we associate a weight $\mathrm{w}(\phi_\mathrm{i}) \in \mathbb{Q}[[\mathrm{z}_1, \ldots, \mathrm{z}_\mathrm{n}]]$, where the latter is the set of formal power series in the variables $\mathrm{z}_1, \ldots, \mathrm{z}_\mathrm{n}$. The weight of a configuration $\Gamma = (\Gamma_1, \ldots, \Gamma_\mathrm{s}) \in \mathcal{F}^\mathrm{s}$ is then defined as the product of all these weights, namely

$$\mathrm{w}(\Gamma) := \prod_{\mathrm{i}=1}^{\mathrm{s}} \mathrm{w}(\Gamma_\mathrm{i}) \in \mathbb{Q}[[\mathrm{z}_1, \ldots, \mathrm{z}_\mathrm{n}]].$$

With $\mathcal{F}^\mathrm{s}/\mathrm{G}$ we denote the set of orbits of $\mathcal{F}^\mathrm{s}$ under the action of $(\bar{\mathrm{G}}, \circ)$. Further we let $\mathbb{C}^\mathrm{s}_\mathrm{w}$ denote the set of configurations in $\mathcal{F}^\mathrm{s}$ with weight w and $\mathbb{W}$ denote the set of weights in $\mathcal{F}^\mathrm{s}$.

Theorem 5.3. (Pólya's second Theorem) The sum of the weights of all orbits in $\mathcal{F}^\mathrm{s}$ induced by a permutation group $(\mathrm{G}, \circ)$, which permutes the set of places S, is given by

$$\mathrm{w}(\mathcal{F}^\mathrm{s}/\mathrm{G}) = \zeta\bigg(\mathrm{G}; \sum_{\phi \in \mathcal{F}} \mathrm{w}(\phi), \ldots, \sum_{\phi \in \mathcal{F}} \mathrm{w}(\phi)^\mathrm{s}\bigg).$$

Proof. First note that two configurations Γ, Γ' in the same orbit have the same weight, since the multiplication is commutative. So given a weight $\mathrm{w} \in \mathbb{W}$, we can find the number of orbits of $\mathcal{F}^\mathrm{s}$ with weight w using Burnside's Lemma:

$$\frac{1}{|\mathrm{G}|} \sum_{\pi \in \mathrm{G}} |\mathbb{C}^{\mathrm{s}\ \bar{\pi}}_\mathrm{w}|.$$

Here $|\mathbb{C}^{\mathrm{s}\ \bar{\pi}}_\mathrm{w}|$ is the cardinality of the set of configurations in $\mathbb{C}^\mathrm{s}_\mathrm{w}$, which are fixed under the permutation $\bar{\pi} \in \bar{\mathrm{G}}$. Therefore, the sum of the weights of all orbits in

$\mathcal{F}^{\mathrm{s}}$ is equal to

$$\begin{aligned} \mathrm{w}(\mathcal{F}^{\mathrm{s}}/\mathrm{G}) &= \sum_{\mathrm{w}\in\mathbb{W}} \mathrm{w}\left(\frac{1}{|\mathrm{G}|}\sum_{\pi\in\mathrm{G}} |\mathbb{C}_{\mathrm{w}}^{\mathrm{s}\ \bar{\pi}}|\right) \\ &= \frac{1}{|\mathrm{G}|}\sum_{\pi\in\mathrm{G}}\sum_{\mathrm{w}\in\mathbb{W}} \mathrm{w}|\mathbb{C}_{\mathrm{w}}^{\mathrm{s}\ \bar{\pi}}|. \end{aligned} \tag{5.2}$$

The term $\sum_{\mathrm{w}\in\mathbb{W}} \mathrm{w}|\mathbb{C}_{\mathrm{w}}^{\mathrm{s}\ \bar{\pi}}|$ denotes the sum of the weights of all configurations that are fixed under $\bar{\pi}$. Let $(\mathrm{j}_1,\ldots,\mathrm{j}_{\mathrm{s}})$ be the cycle type of π and consider the product

$$\mathrm{H}_\pi = \left(\sum_{\phi\in\mathcal{F}} \mathrm{w}(\phi)\right)^{\mathrm{j}_1} \cdots \left(\sum_{\phi\in\mathcal{F}} \mathrm{w}(\phi)^{\mathrm{s}}\right)^{\mathrm{j}_{\mathrm{s}}}.$$

When we expand this product as a sum of monomials $\mathrm{w}(\phi_1)^{\mathrm{k}_1}\cdots\mathrm{w}(\phi_{\mathrm{r}})^{\mathrm{k}_{\mathrm{s}}}$, we get one of these monomials by choosing a term $\mathrm{w}(\phi_{\mathrm{i}})^{\mathrm{j}}$ from each factor of H_π and multiplying these terms together. Choosing $\mathrm{w}(\phi_{\mathrm{i}})^{\mathrm{j}}$ corresponds to associating all the elements of some j-cycle with weight $\mathrm{w}(\phi_{\mathrm{i}})$. Since a factor $(\mathrm{w}(\phi_1)+\cdots+\mathrm{w}(\phi_{\mathrm{r}}))^{\mathrm{j}_{\mathrm{i}}}$ occurs precisely j_{i} times in H_π, choosing a term $\mathrm{w}(\phi_{\mathrm{i}})^{\mathrm{j}}$ from every factor corresponds to associating all elements of the same cycle with the same weight. The product of these terms $\mathrm{w}(\phi_{\mathrm{i}})^{\mathrm{j}}$ will be the monomial $\mathrm{w}(\phi_1)^{\mathrm{k}_1}\cdots\mathrm{w}(\phi_{\mathrm{r}})^{\mathrm{k}_{\mathrm{s}}}$, where we have used weight $\mathrm{w}(\phi_{\mathrm{i}})$ a total of k_{i} times. It follows that the coefficient of $\mathrm{w}:=\mathrm{w}(\phi_1)^{\mathrm{k}_1}\cdots\mathrm{w}(\phi_{\mathrm{r}})^{\mathrm{k}_{\mathrm{s}}}$ in H_π is equal to the number of fixed points of π on the set of configurations with weight w, namely $|\mathbb{C}_{\mathrm{w}}^{\mathrm{s}\ \bar{\pi}}|$. Therefore

$$\mathrm{H}_\pi = \sum_{\mathrm{w}\in\mathbb{W}} \mathrm{w}|\mathbb{C}_{\mathrm{w}}^{\mathrm{s}\ \bar{\pi}}|.$$

Plugging this term back into (5.2), we get the desired result. □

To explicate the proof, we discuss an example. We choose

$$\mathcal{F} = \{\phi_1,\phi_2,\phi_3\}$$

with weights $\mathrm{w}(\phi_1)=\mathrm{x},\mathrm{w}(\phi_2)=\mathrm{y},\mathrm{w}(\phi_3)=\mathrm{z}$ and $\mathrm{s}=5$. Consider the permutation $\pi=(12)(34)(5)\in\mathrm{G}$. For configurations fixed under $\bar{\pi}$ it must hold, that elements in the same cycle must be associated with the same weight. But then, the sum of the weights of all configurations fixed under $\bar{\pi}$ is equal to

$$(\mathrm{x}^2+\mathrm{y}^2+\mathrm{z}^2)(\mathrm{x}^2+\mathrm{y}^2+\mathrm{z}^2)(\mathrm{x}+\mathrm{y}+\mathrm{z}) = (\mathrm{x}^2+\mathrm{y}^2+\mathrm{z}^2)^2(\mathrm{x}+\mathrm{y}+\mathrm{z}).$$

5.2 A Generalization

With Theorem 3.8 we showed a CSP result on the set of multisets $\binom{\mathbb{N}_n}{k}$ with k elements. Using the Theorem's of Pólya, we can find a more general result, of which Theorem 3.8 is a special case. In order to prove this result, we will utilize the introduced tool in Chapter 4, namely Theorem 4.2.

We choose $\mathcal{F} = \mathbb{N}_n$ with weights $w(i) = x_i$. Then by Theorem 5.3 we have

$$\zeta\Big(G; \sum_{i\in\mathbb{N}_n} x_i, \ldots, \sum_{i\in\mathbb{N}_n} x_i^k\Big) = \sum_{G\text{–orbits}} \prod_{i=1}^{n} x_i^{m_i},$$

where m_i denotes the number of occurrences of the figure i in any representative of an orbit. The following proof is modified from [1, Theorem 6.1]. We will set $x_i = q^{i-1}$ or equivalently $w(i) = q^{i-1}$.

Theorem 5.4. Let $X = \mathbb{N}_n^s/G$ denote the set of orbits of $\mathbb{N}_n^s$ induced by $(G, \circ)$, where $(G, \circ)$ permutes the set of places S, and $(C_n, \circ)$ be a cyclic group acting on $\mathbb{N}_n$. For $i \in \mathbb{N}_n$ we choose the weights $w(i) = q^{i-1}$ and define

$$f(q) := \zeta\Big(G; \sum_{i\in\mathbb{N}_n} q^{i-1}, \ldots, \sum_{i\in\mathbb{N}_n} (q^{i-1})^k\Big).$$

Then the triple (X, C_n, f(q)) exhibits the cyclic sieving phenomenon.

Proof. As in the proof of Theorem 3.8, we let $V = \mathbb{C}\{1, \ldots, n\}$ and consider the $|S|$-fold tensor product $V^{\otimes|S|}$, where $(G, \circ)$ acts on the tensor positions. Again, the cyclic group $(C_n, \circ)$ acts on V by (2.2) and so there is an induced action on $V^{\otimes|S|}$. For a group element $c \in C_n$ we denote with $\rho(c)$ and $\rho'(c)$ the associated linear transformation on V and $V^{\otimes|S|}$ respectively, which are diagonalizable as discussed in Chapter 4.

Next we let $U = (V^{\otimes|S|})^G$ be the G-invariant subspace for this action, therefore $gu \in U$ for all $g \in G, u \in U$. Then U is a submodule of $V^{\otimes|S|}$ and still affords a representation $\psi : C_n \to GL(U)$. We consider the G-symmetrized basic tensors:

$$\Big\{\frac{1}{|G|}\sum_{g\in G} v_{j_{g(s_1)}} \otimes \cdots \otimes v_{j_{g(s_{|S|})}} \mid 1 \le j_1 \le \cdots \le j_{|S|} \le n\Big\}.$$

We now make use of the arguments already given in Section 3.1.2.

This set of G-symmetrized basic tensors is a basis for U and clearly indexed by the set of G-orbits having weights $\prod_{i=1}^{n} x_i^{m_i}$: two configurations $\Gamma_1, \Gamma_2 \subseteq \mathbb{N}_n^s$

in the same orbit yield the same symmetrized basic tensor. Since such a basis tensor is an eigenvector for $\psi(c)$ (see the arguments using (3.3)), the eigenvalue is the weight $\prod_{i=1}^{n} x_i^{m_i}$. Therefore the character value of $\psi(c)$ is the sum of these eigenvalues, namely $\chi_\psi(x_1, \ldots, x_n)\big|_{x_i=q^{i-1}} = f(q)$.

Next if C_n acts on $\mathbb{N}_n$ and we consider again the representation ρ^h which assigns to a generator $c \in C_n$ an n-th root of unity ω_n, then the eigenvalues of any $c \in C_n$ are given by the multiset $1, \psi^h(c), \ldots, \psi^h(c)^{n-1}$. Since we substituted x_i for the eigenvalues, the character value of $\psi(c)$ is consequently

$$\chi_\psi(1, q, \ldots, q^{n-1})\big|_{q=\psi^h(c)} = f(\omega_{ord(c)}).$$

But then we get that $U \cong V_f$ as C_n-modules, as they have the same characters. On the other hand, the basis vectors of $\mathbb{C}X$ are exactly the orbits and thus we have $U \cong \mathbb{C}X$. Therefore we can apply Theorem 4.2 and the result follows. □

If we choose S such that $|S| = k$ and $G = \mathcal{S}_k$, we operate on the set of symmetric tensors again and then this theorem specializes to Theorem 3.8. Furthermore, if we choose $n = 2$ we get an interesting result of de Bruijn [10, pages 67 – 69].

Corollary 5.5. Let $X = \mathbb{N}_2^s/G$ denote the set of orbits on $\mathbb{N}_2^s$ induced by $(G, \circ)$, where $(G, \circ)$ permutes the of set places S, and $(C_2, \circ)$ be a cycle group acting on $\mathbb{N}_2$. For $i \in \mathbb{N}_2$ we choose the weights $w(i) = q^{i-1}$.

Then f(-1) counts the self-complementary orbits.

Proof. Since an orbit is self-complementary if it is invariant under the action of the cyclic group C_2, only the orbits with the same number of both colors are self-complementary. Hence the self-complementary orbits are the ones, that are fixed under the (color swapping) permutation of order 2. Since we have proven that the triple $(X, C_2, f(q))$ exhibits the CSP, these orbits are counted by f(-1). □

To illustrate, let $\mathcal{F} = \{\circ, \bullet\}$ and $s = 4$. We choose $(G, \circ)$ to be the symmetric group $(S_4, \circ)$. Then the set of orbits is given by

$$\mathbb{N}_2^s/G = \{(\circ,\circ,\circ,\circ), (\bullet,\circ,\circ,\circ), (\bullet,\bullet,\circ,\circ), (\bullet,\bullet,\bullet,\circ), (\bullet,\bullet,\bullet,\bullet)\}.$$

As discussed before, we have the following cycle index for $(S_4, \circ)$:

$$\zeta(S_4; z_1, z_2, z_3, z_4) = \frac{1}{24}(z_1^4 + 6z_1^2z_2 + 8z_1z_3 + 3z_2^2 + 6z_4).$$

Plugging in $\sum_{\phi\in\mathcal{F}} w(\phi)^i$ into the corresponding z_i and working out the polynomial, we have

$$f(q) = 1 + q + q^2 + q^3 + q^4,$$

which of course counts the orbits according to their weight. Finally f(-1) = 1, coinciding with the observation that $(\bullet, \bullet, \circ, \circ)$ is the only self-complementary orbit.

Chapter 6

Words and Lattice Paths

We will start this chapter by proving a generalization of the CSP result (3.4), which we found when we discussed an application of Burnside's Lemma. Since there is a natural correspondence between words and lattice paths, the first section about binary words forms the basis for the chapter about lattice paths. In addition to the natural cyclic shift on binary words, we will present another cyclic action. The latter will allow us to provide a further CSP result on binary word and moreover, we will make use of it again when we discuss lattice paths. We will also give a CSP result on lattice paths and introduce the notions of different kinds of Dyck paths. Further, we will present a CSP result on circular Dyck paths from the paper [3] of P. Alexandersson, S. Linusson and S. Potka, which was published recently in 2019.

It is particularly remarkable, that in this and the following chapter about Catalan objects we will see how omnipresent and powerful q-binomial coefficients are when we talk about the cyclic sieving phenomenon: Without exception all the following results make use of a polynomial, which is composed of q-binomial coefficients.

6.1 Binary Words

In section 3.2 we gave an idea, how the CSP can be used to help solving combinatorial problems. Now we give a generalization of (3.4), namely that the triple

$$\big(\mathrm{BW}(n), \langle(1 \cdots n)\rangle, \sum_{k=0}^{n} \begin{bmatrix} n \\ k \end{bmatrix}_q\big)$$

exhibits the CSP for any $n \in \mathbb{N}$. To do so, we need the following lemma.

Lemma 6.1. Let ω_d be a d-th root of unity and $n = md$, then

$$\begin{bmatrix} n \\ k \end{bmatrix}_{\omega_d} = \begin{cases} \binom{m}{k/d} & \text{if } d \mid k, \\ 0 & \text{otherwise.} \end{cases}$$

Proof. Let's investigate the left hand side:

$$\begin{aligned} \begin{bmatrix} n \\ k \end{bmatrix}_{\omega_d} &= \frac{[n]_{\omega_d}!}{[k]_{\omega_d}![n-k]_{\omega_d}!} \\ &= \frac{[n]_{\omega_d} \cdots [n-k+1]_{\omega_d}}{[k]_{\omega_d}!}. \end{aligned}$$

The proof is analogous to the one of Lemma 3.7; the "otherwise" case follows by the exactly same argument.

If $d \mid k$, then using Lemma 3.6 again we get

$$\begin{aligned} \begin{bmatrix} n \\ k \end{bmatrix}_{\omega_d} &= \lim_{q \to \omega_d} \left(\frac{[n]_q}{[k]_q} \cdot \frac{[n-1]_q}{[1]_q} \cdot \frac{[n-2]_q}{[2]_q} \cdots \frac{[n-k+1]_q}{[k-1]_q} \right) \\ &= \frac{n}{k} \cdot 1 \cdots 1 \cdot \frac{n-d}{d} \cdot 1 \cdots 1 \cdot \frac{n-2d}{2d} \cdots \\ &= \frac{n/d}{k/d} \cdot \frac{n/d-1}{1} \cdot \frac{n/d-2}{2} \cdots \\ &= \binom{n/d}{k/d}. \end{aligned}$$

From $n = md$ the result follows. □

Using this lemma, we can prove our generalization.

Theorem 6.2. The cyclic sieving phenomenon is exhibited by the triple

$$\big(\mathrm{BW}(n), \langle (1 \cdots n) \rangle, \sum_{k=0}^{n} \begin{bmatrix} n \\ k \end{bmatrix}_q \big).$$

Proof. First we work out the number of fixed points of the elements in the cyclic group. Let $c \in \langle (1 \cdots n) \rangle$ have order d. Recall again that c has $\frac{n}{d}$ cycles of the same length. For a binary word to be fixed under c, the letters permuted by each cycle of c must coincide. Because we can choose for each cycle two different letters, there are $2^{\frac{n}{d}}$ binary words $w \in \mathrm{BW}(n)$ fixed under c. Since $n = md$, the result simplifies to 2^m.

Now we evaluate the polynomial at the d-th roots of unity. Suppose ω_d is a

d-th root of unity with $n = md$. Then by the previous lemma, only the terms with $d \mid k$ contribute to the sum in the polynomial:

$$\begin{aligned}\sum_{k=0}^{n} \begin{bmatrix} n \\ k \end{bmatrix}_{\omega_d} &= \sum_{j=0}^{m} \begin{bmatrix} n \\ jd \end{bmatrix}_{\omega_d} \\ &= \sum_{j=0}^{m} \binom{m}{j}.\end{aligned}$$

By the binomial theorem the last term is equal to 2^m. □

Instead of working with the natural cyclic shift for binary words, we can define other shifts. The remaining results of this section can be found in [3, pages 21–23]; we will describe the arguments in more detail.

Definition 6.3. Let BW(n) denote the set of binary words of length n. We define

$$\eta : \begin{cases} \mathrm{BW}(n) \to \mathrm{BW}(n), \\ (b_1, \ldots, b_n) \mapsto (\hat{b}_{n-1}, \hat{b}_n, b_1, b_2, \ldots, b_{n-2}), \end{cases}$$

where $\hat{b}_i := 1 - b_i$.

Note that the shift is indeed two steps, and that $\eta^n(b) = b$ for all words b of length n. For example:

$$\eta(1000011) = (0010000).$$

Lemma 6.4. The number of words in BW(n) fixed under η^m is given by

$$|\mathrm{BW}(n)^{\eta^m}| = \begin{cases} 2^d & \text{if } \frac{n}{d} \text{ is odd}, \\ 0 & \text{otherwise}, \end{cases}$$

where $d = \gcd(m,n)$.

Proof. At first we claim that both group elements η^d and η^m have the same number of fixed points. First consider a word b which is fixed under η^d. Since $d \mid m$, we have $m = kd$ for a $k \in \mathbb{N}$ and hence

$$\eta^m(b) = \eta^{kd}(b) = (\eta^d)^k(b) = b.$$

On the other hand, since η generates a cyclic group of order n, from algebra we know that $\mathrm{ord}(\eta^m) = \mathrm{ord}(\eta^d)$. This implies $\eta^d \in \langle \eta^m \rangle$, where the latter is the

subgroup generated by η^m. Hence there exists a $k \in \mathbb{N}$ such that $(\eta^m)^k = \eta^d$ and so the words fixed by η^m are also fixed by η^d, from which the claim follows.

Therefore it suffices to show that if $n = kd$, then η^d fixes 2^d elements if k is odd, and 0 elements otherwise.

Let $b \in BW(n)$ and partition b into k contiguous blocks of length d. Note that η^d maps block i onto block $i + 2 \pmod k$. Suppose now b is fixed under η^d and consider the following cases.

Assume k is even. We have that the blocks $1, 3, 5, \ldots, k-1$ must all be equal. However, block $k-1$ and block 1 must also be different, as η^d not only shifts bits 2d steps to the right, but also flips all bits that wrap around. This is impossible, so there cannot be any fixed words in this case.

Assume k is odd. A similar argument as above shows that all odd-indexed blocks must be qual and all even-indexed blocks must be equal. Further, an even-indexed block is given by flipping all bits in an odd block. There are 2^d such possibilities, as there are d bits in a block. □

The previous lemma allows us to prove the following CSP result.

Theorem 6.5. The cyclic sieving phenomenon is exhibited by the triple

$$\big(BW(n), \langle\eta\rangle, \sum_{k=0}^{n} q^{\binom{k}{2}} \begin{bmatrix} n \\ k \end{bmatrix}_q\big).$$

Proof. Again, we need to evaluate our polynomial f(q) at d-th roots of unity. Suppose ω_d is a d-th root of unity with $n = md$. Applying Lemma 6.1, we get

$$\begin{aligned} f(\omega_d) &= \sum_{k=0}^{n} \omega_d^{\binom{k}{2}} \begin{bmatrix} n \\ k \end{bmatrix}_{\omega_d} \\ &= \sum_{j=0}^{m} \omega_d^{\binom{jd}{2}} \binom{m}{j} \end{aligned}$$

since only terms with $d \mid k$ contribute to the sum. For the next step note, that the term $j(jd-1)$ is always even if d is odd and alternating even, and odd if d is

even. Rewriting $\binom{jd}{2} = \frac{jd(jd-1)}{2}$, we have

$$\begin{aligned}\sum_{j=0}^{m} \omega_d^{\binom{jd}{2}} \binom{m}{j} &= \sum_{j=0}^{m} (\omega_d^{\frac{d}{2}})^{j(jd-1)} \binom{m}{j} \\ &= \sum_{j=0}^{m} (-1)^{j(jd-1)} \binom{m}{j} \\ &= \begin{cases} 2^m & \text{if d is odd,} \\ 0 & \text{otherwise.} \end{cases}\end{aligned} \tag{6.1}$$

which completes the proof. □

We will apply the latter theorem later on, when we dicuss Möbius paths.

6.2 Lattice Paths

We focus now on investigating CSP results on lattice paths, where we will make use of the properties of binary words.

With Proposition 2.17 and Lemma 3.7 we can prove an obvious CSP result. To do so, we define the set of north-east lattice paths:

Definition 6.6. We define LE(m,n) to be the set of lattice paths with m east steps and n north steps.

Recall that we can describe lattice paths with north-east steps via binary words, where we choose 0 to be an east and 1 to be a north step. Hence we can interpret this set as a subset of binary words $LE(m, n) \subset BW(m + n)$. For our polynomial we choose of course

$$f(q) = \begin{bmatrix} m+n \\ m \end{bmatrix}_q$$

and let C_{m+n} be the cyclic group with generator $\langle (1 \cdots (m + n)) \rangle$.

Theorem 6.7. The cyclic sieving phenomenon is exhibited by the triple

$$\Big(LE(m, n), C_{m+n}, \begin{bmatrix} m+n \\ m \end{bmatrix}_q\Big).$$

Proof. Let ω_d be a d-th root of unity and m+n = kd. Applying Lemma 3.7, we have

$$f(\omega_d) = \begin{cases} \binom{m/d+n/d}{n/d} & \text{if } d \mid n, \\ 0 & \text{otherwise.} \end{cases}$$

Suppose now $c \in C_{m+n}$ has order d.

First assume that $d \nmid n$. For a binary word to be fixed under c, the letters permuted by each cycle of c must coincide. The permutation c has $\frac{m+n}{d}$ cycles of length d and if each cycle permutes only 0's or 1's, then the corresponding binary word has $k \cdot \frac{m+n}{d}$ 0's (or 1's) for an integer k. But by assumption, there exists no integer k such that n = kd. Hence $k \cdot \frac{m+n}{d}$ can not be an integer and so there is no lattice path that is fixed under c.

Assume now that $d \mid n$. Since $d \mid (m+n)$ then also $d \mid m$. As we have $\frac{m+n}{d}$ cycles in total and each of them have to permute either all 0's or all 1's, we can choose $\frac{n}{d}$ cycles that permute all 1's. Therefore there are exactly $\binom{m/d+n/d}{n/d}$ binary words fixed under c. □

Next we discuss some more specific lattice paths.

6.2.1 Circular Dyck Paths

In this section we present a CSP result from the paper of P. Alexandersson, S. Linusson and S. Potka [3] on circular Dyck paths. To do so, we introduce a display of circular Dyck paths that represents its circular nature. But at first, we give the definition of a Dyck path.

Definition 6.8. Let $n \in \mathbb{N}$. A *Dyck path* of size n is a lattice path from (0,0) to (n,n) that lies strictly below but may touch the diagonal y = x. We denote the set of Dyck paths of size n with DP(n).

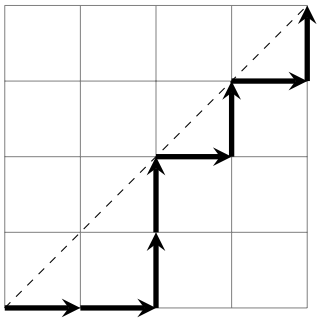

Figure 6.1: A Dyck path of size 4.

It is a well-known fact that the number of Dyck paths of size n is given by the n-th Catalan number $\mathcal{C}at_n$, where

$$\mathcal{C}at_n = \frac{1}{n+1}\binom{2n}{n}.$$

There are many more objects that are counted by the Catalan numbers; we will see a few more in the next chapter. Interestingly these Catalan objects are in bijection to each other but many combinatorial properties do only hold for a few of them. This is also the case here: There is no CSP result known yet on Dyck paths, however, as we will see, there are many CSP results on different Catalan objects.

The following notions can be found in [3, pages 6–9]. We will make an effort to describe circular Dyck paths in more detail and show its correspondence to binary words.

To define circular Dyck paths, we introduce a different approach to describe Dyck paths. In fact, a Dyck path may be described via the area sequence between the diagonal the Dyck path itself.

Definition 6.9. The *area sequence* of a Dyck path is a sequence of numbers, describing the area between the diagonal and the Dyck path itself.

For example, the Dyck path in Figure 6.1 corresponds to the area sequence (0,1,0,0).

Finally, a circular Dyck path is defined via its area sequence.

Definition 6.10. A *circular Dyck path* of size n is a lattice path specified by an area sequence $(a_1, \ldots, a_n)$ such that

(1) $0 \leq a_i \leq n-1$ for $1 \leq i \leq n$,

(2) $a_{i+1} \leq a_i + 1$ for $1 \leq i \leq n$,

where the index is taken mod n in the second condition. We denote the set of circular dyck paths of size n by CDP(n).

Observe that if $a_1 = 0$, the circular Dyck path coincides with a classical Dyck path. We will briefly discuss properties (1) and (2) in the definition of a circular Dyck path.

Circular Dyck paths can also be illustrated as diagrams. For this we use a slightly different display than in the previous figures. Consider the area sequence (2,3,0,1,1,2) that describes the following lattice path:

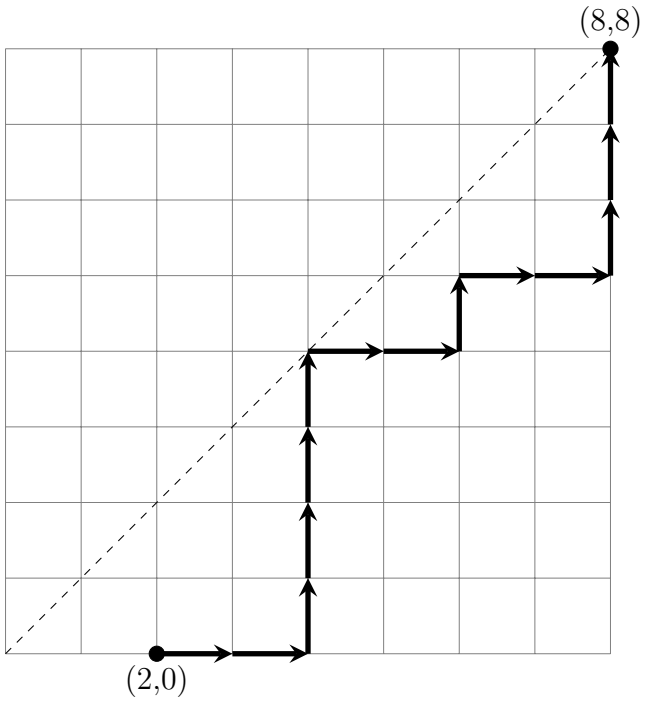

Figure 6.2: A lattice path with area sequence (2,3,0,1,1,2), consisting of 6 east and 8 north steps. The number n defines the number of east steps, whereas the number of north steps is given by $n + a_1$. Observe that if we had $a_1 = 0$, the area sequence would correspond to a Dyck path.

We mirror the lattice path at the diagonal $y = x$. Condition (1) implies that the largest possible area between the diagonal and the lattice path itself is $n - 1$. Thus the largest possible distance between a point on the Dyck path and its perpendicular point on the diagonal is $\sqrt{2}n$, since we have to take each $\frac{n}{2}$ north and east steps to reach it. Therefore this point on the Dyck path has a distance of $2 \cdot \sqrt{2}n$ to its mirrored point, and this is the largest possible distance a point can have to its mirrored point. So the mirrored lattice path stays below but may touch the diagonal $y = x + n$, respectively stays above but may touch the diagonal $y = x$. We change the coordinate system now such that the $x-$axis goes through the start of the mirrored path. Also, we let the path be constricted by the diagonals $y = x$ and $y = x - n$.

Next we remove the east steps in the end of the mirrored path, such that the last step is a north step. Further, we attach so many east steps to the beginning of the mirrored path, until we have n east steps and thus the number of east and north steps coincide. Then the circular Dyck path has a unique starting point $0 \leq x_0 \leq n$ and as we will see, a unique corresponding binary sequence. Note that

the starting point is indeed between 0 and n: After mirroring we have n north steps and $n + a_1$ east steps in the path. In total we remove $a_n + 1$ east steps and add

$$n - (n + a_1 - (a_n + 1)) = a_n + 1 - a_1 \geq 0$$

east steps, because we want to have each n north and east steps and the inequality follows from condition (2). After mirroring, the starting point is at $n - a_1 \leq n$. Adding $a_n + 1 - a_1$ east steps to the start, we get

$$n - a_1 - (a_n + 1 - a_1) = n - a_1 - 1 \geq n - (n-1) - 1 = 0$$

for the starting point, where the inequality follows from condition (1).

The resulting diagram of the circular Dyck path with area sequence (2,3,0,1,1,2) is then as below.

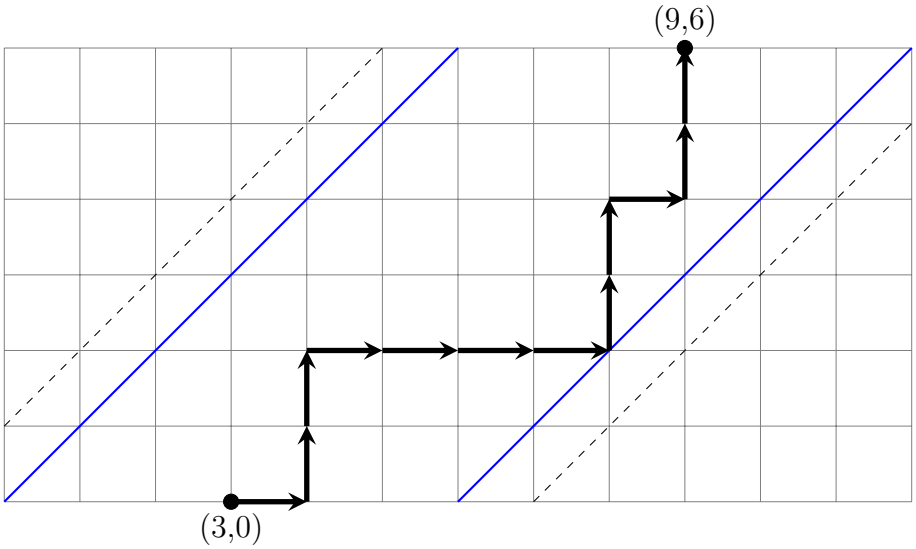

Figure 6.3: A circular Dyck path starting at (3,0) with area sequence (2,3,0,1,1,2). The path corresponds to the binary word 011000011011. The area sequence is determined by the number of (whole) squares to the right of the path (between the path and the blue diagonal) in each row. The two dashed diagonals are never touched by a lattice path corresponding to an area sequence, whereas the blue diagonals $y = x$ and $y = x - n$ may be touched.

As already mentioned, the subset of paths with $a_1 = 0$ correspond to classical Dyck paths DP(n). Condition (1) ensures that the path stays between the diagonals $y = x$ and $y = x - n$. Condition (2) restricts the steps to be either north or east steps. Further, the condition $a_1 \leq a_n + 1$ enables the area sequence to

be shifted and still result in a lattice path with north and east steps; hence the circular nature of the graph, which can be better displayed in the way we did it in Figure 6.3. To illustrate, assume $a_1 = 4 > 3 = a_n + 1$. If we shift the area sequence to the right, we obtain a sequence $(2, 4, \dots)$. But the path corresponding to this area sequence must contain a west step now.

It is often convenient to describe circular dyck paths as paths along the border of the white squares, see Figure 6.3. We denote such a path by (x,b), where $b = (b_1, \dots, b_{2n}) \in \{0,1\}^{2n}$ is a binary sequence with n 0's and 1's, respectively and $x = (x_0, 0)$ the starting point. By the construction of our circular Dyck path, we always have $b_{2n} = 1$. Note that without these restrictions, an area sequence would correspond to several binary sequences.

Given an area sequence $a = (a_1, \dots, a_n)$, the corresponding path (x, b) can be obtained by the following algorithm: At first, we initialize an empty list σ. Every time we add a letter to the start of σ, we shift its elements to the right. We start at the end of the area sequence $a = (a_1, \dots, a_n)$ and compute

$$a_{n-1} - a_n = k \in \mathbb{Z}.$$

Then we add a 1 to the start of σ and afterwards k+1 0's. In doing so, we always get $b_{2n} = 1$. We repeat this process by computing $a_i - a_{i+1}$ for all $1 \leq i \leq n-1$. After these iterations, we add a last 1 to σ, which then has a certain number of elements $|\sigma|$. In a final step we add $2n - |\sigma|$ 0's to the start of σ. This defines the unique starting point $x = (x_0, 0), 0 \leq x_0 \leq n$ and also our binary sequence $b := \sigma$.

We also study circular Dyck paths with a width different from the height, which are defined in an analogous manner.

Definition 6.11. A *circular Dyck path* of heigth n and width w is a lattice path specified by an area sequence $(a_1, \dots, a_n)$ such that

(1) $0 \leq a_i \leq w - 1$ for $1 \leq i \leq n$,

(2) $a_{i+1} \leq a_i + 1$ for $1 \leq i \leq n$,

where the index is taken mod n in the second condition. This set is denoted by CDP(n,w).

Equivalently we can think of the elements in CDP(n,w) as tuples (x,b) where $x = (x_0, 0), 0 \leq x_0 \leq w$ is the starting point and $b = (b_1, \dots, b_{2n}) \in \{0,1\}^{n+w}$ is a binary sequence with n 1's and w 0's such that the corresponding path stays between the diagonals y = x and y = x - w; and it holds $b_{n+w} = 1$.

There is a natural C_n-action on CDP(n,w), where the generator shifts the area sequence cyclically by one step to the right. We let α denote such a cyclic shift and

denote the group by $\langle\alpha\rangle$. For examle, we have $\alpha(2,3,0,1,1,2) = (2,2,3,0,1,1)$ with the following graphs.

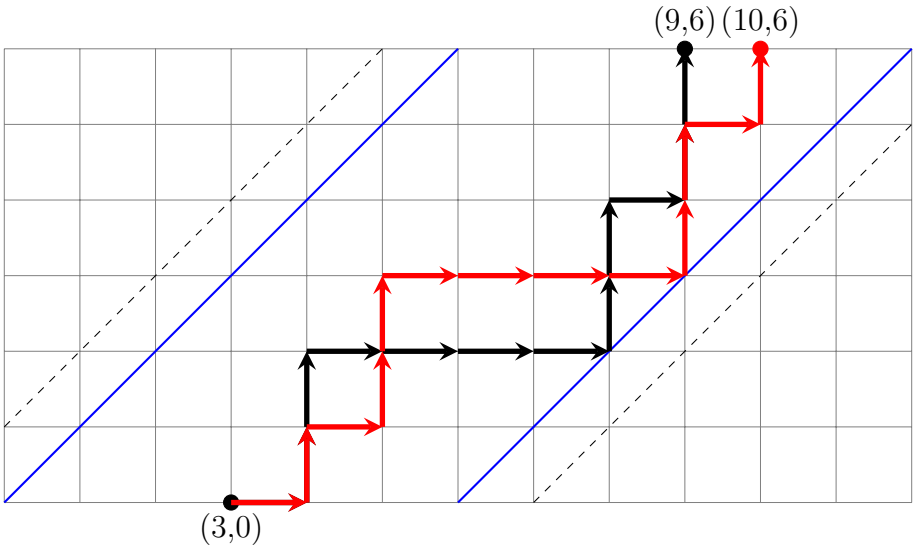

Figure 6.4: A circular Dyck path starting at (3,0) with area sequence (2,3,0,1,1,2) in black and the α shifted circular Dyck path with area sequence (2,2,3,0,1,1) in red.

Recall Definition 2.19: The major index of a word b of length n is the sum of the indices $i \in \mathbb{N}_{n-1}$ such that $b_i > b_{i+1}$. For the last ingredient of our CSP triple, we define the following q-analogue of circular Dyck paths:

$$|\mathrm{CDP}(n,w)|_q := \sum_{(x,b)\in \mathrm{CDP}(n,w)} q^{\mathrm{maj}(b)}. \tag{6.2}$$

In fact, it is possible to express $|\mathrm{CDP}(n,w)|_q$ as a sum of q-binomial coefficients. This is done in [3, pages 10–14] by considering the major index generating function for arbitrary north-east lattice paths starting at the origin with some constraints, which will be used in an inclusion-exclusion argument. We then get the following result [3, Corollary 20]:

Lemma 6.12. We have the q-enumeration

$$|\mathrm{CDP}(n,w)|_q = \sum_{s\in\mathbb{Z}}\sum_{j=1}^{w} q^{s^2\delta+s(j+1)}\left(\begin{bmatrix} 2n-1 \\ n-1-\delta s\end{bmatrix}_q - \begin{bmatrix} 2n-1 \\ n+j+\delta s\end{bmatrix}_q\right),$$

where $\delta = w+2$. □

For the latter lemma, note that the q-binomial coefficients are defined to be 0 if the term below exceeds the term above.

Now we can state the main result on circular Dyck paths [3, Theorem 22]. The proof is very technical and consists of first counting the number of fixed points under cyclic shift by k steps and afterwards evaluating the q-analogue $|\mathrm{CDP}(n, w)|_q$ at $\omega_{n/k}$. This is done by manipulating the q-binomial-coefficients using several identities [3, Lemma 24]. Finally, we have:

Theorem 6.13. Let α act on CDP(n,w) by cyclically shifting the area sequence on step. Then the triple

$$(\mathrm{CDP}(n, w), \langle\alpha\rangle, |\mathrm{CDP}(n, w)|_q)$$

exhibits the cyclic sieving phenomenon. □

6.2.2 Möbius Paths

In the following we discuss so called Möbius paths, which are special circular Dyck paths. Here, a previous CSP result on binary words will come into play again. The definition can be found in [3, page 8].

Definition 6.14. We define CMP(n) to be the subset of circular Dyck paths, such that $b = (b_1, \ldots, b_{2n})$ fulfills the relation

$$b_i = 1 - b_{n+i} \text{ for all } i \in \mathbb{N}_n$$

and $b_n = 0$ corresponds to an east step that ends on the vertical line $x = n$. We refer to such paths as *circular Möbius paths*.

Note that, in particular, $b_n = 0$ as we always have $b_{2n} = 1$. The starting point $x = (x_0, 0)$ is uniquely determined by b since $b_n = 0$ must correspond to an east step that ends on the vertical line $x = n$. So all possible b correspond to exactly one path. This does indeed not have to be the case for circular Dyck paths: Different tuples (x,b) could correspond to different area sequences and hence to different circular Dyck paths, but the binary sequences could coincide. Then, however, the starting points would differ.

Moreover, the second part of a Möbius path is a reflection of the first path. To illustrate, consider the following figure:

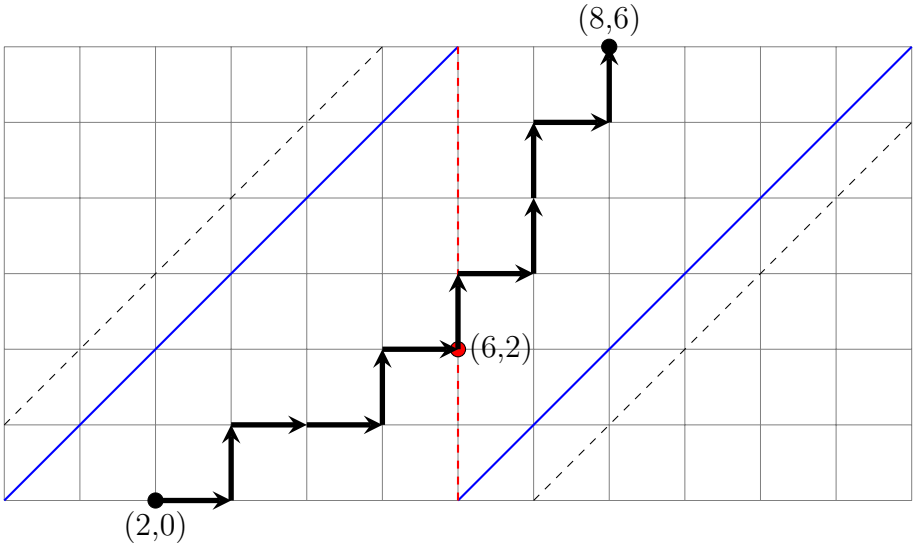

Figure 6.5: A Möbius path starting at x = (2,0) with area sequence (3,2,2,2,3,3) and corresponding binary sequence b = (010010101101). The path is a concatenation of two smaller paths, the second part being a reflection of the first. Hence the "Möbius" name. The red dashed vertical line denotes x = n.

The next result [3, Lemma 12] allows us to define a bijection from Möbius paths to BW(n − 1).

Lemma 6.15. We have that $|\mathrm{CMP}(n)| = 2^{n-1}$.

Proof. As noted above a path in CMP(n) is uniquely determined by the first n−1 steps in b. □

We define the bijection:

$$\mathrm{M} : \begin{cases} \mathrm{BW}(n-1) \to \mathrm{CMP}(n), \\ (b_1, \ldots, b_{n-1}) \mapsto (b_1, \ldots, b_{n-1}, 0, \hat{b}_1, \ldots, \hat{b}_{n-1}, 1). \end{cases}$$

Recall Definition 6.3 of η. This shift η acts on BW(n − 1) and thus induces an action $\tilde{\eta} = \mathrm{M} \circ \eta$ on CMP(n), where $\circ$ denotes the composition.

To illustrate, consider the Möbius path in CMP(6) of Figure 6.5. The first half of the corresponding binary word is given by (010010) which is identified with (01001) ∈ BW(5). Applying M on this word gives exactly the path in CMP(n). The action $\tilde{\eta}$ is now induced by the composition

$$\tilde{\eta}(01001) = \mathrm{M}(\eta(01001)) = \mathrm{M}(10010) = 100100011011.$$

Observe that if a binary word in BW(n − 1) is fixed under η, the corresponding Möbius path in CMP(n) is fixed under $\tilde{\eta}$. Using this fact, we can prove the following result.

Theorem 6.16. The cyclic sieving phenomenon is exhibited by the triple

$$\big(\mathrm{CMP(n)}, \langle\tilde{\eta}\rangle, \sum_{k=0}^{n-1} q^{\binom{k}{2}} \begin{bmatrix} n-1 \\ k \end{bmatrix}_q\big).$$

Proof. By the previous remark, the number of fixed points of an element in $\langle\tilde{\eta}\rangle$ on CMP(n) with order d equals the number of fixed points of an element in $\langle\eta\rangle$ on BW(n − 1) with order d. Applying Theorem 6.5 yields the result. □

For proving a further CSP result, we need the following lemma [3, Lemma 33].

Lemma 6.17. For fixed n, all the expressions

$$(1)\ \sum_{k=0}^{n} q^{\binom{k}{2}} \begin{bmatrix} n \\ k \end{bmatrix}_q, \qquad (2)\ \prod_{j=0}^{n-1}(1+q^j), \qquad (3)\ \sum_{b\in \mathrm{BW(n)}} q^{\mathrm{maj(b)}+\mathrm{maj}(\hat{b})}$$

are equal.

Proof. Identity (1) = (2). This is a consequence of the q-binomial theorem, see e.g. [11, pages 14 – 15]:

$$\prod_{j=0}^{n-1}(1+xq^k) = \sum_{k=0}^{n} q^{\binom{k}{2}} \begin{bmatrix} n \\ k \end{bmatrix}_q x^k.$$

Identity (2) = (3). We do induction over n. The base case n = 1 is clear. Assume now the identity holds for n − 1. Consider a binary word b of length n − 1. We can either append 0 or 1 to make a word b' of length n. If the last bit of b is equal to the appended bit, then

$$\mathrm{maj(b)} + \mathrm{maj}(\hat{b}) = \mathrm{maj}(b') + \mathrm{maj}(\hat{b}')$$

because there are not more descents contributing to the sum. If the last bit of b is not equal to the appended bit, then either maj(b′) or maj($\hat{b}'$) contributes n − 1

more to the sum. We get

$$\begin{aligned}\sum_{b\in BW(n)} q^{maj(b)+maj(\hat{b})} &= \sum_{b\in BW(n-1)} q^{maj(b)+maj(\hat{b})} + \sum_{b\in BW(n-1)} q^{maj(b)+maj(\hat{b})+n-1} \\ &= \sum_{b\in BW(n-1)} q^{maj(b)+maj(\hat{b})}(1+q^{n-1}) \\ &= \prod_{j=0}^{n-2}(1+q^j)(1+q^{n-1}) \\ &= \prod_{j=0}^{n-1}(1+q^j)\end{aligned}$$

which completes the proof. □

Since $CMP(n) \subset CDP(n)$ we can use the same q-analogue as in (6.2):

$$|CMP(n)|_q = \sum_{b\in CMP(n)} q^{maj(b)}.$$

Observe that in contrast to circular Dyck paths, the Möbius paths are uniquely determined by the binary sequences. The proof of the next result is modified from [3, Lemma 36].

Lemma 6.18. We have the following formula for $|CMP(n)|_q, \bmod (q^n-1)$:

$$\sum_{b\in CMP(n)} q^{maj(b)} \equiv \frac{1}{2}\sum_{k=0}^{n} q^{\binom{k}{2}} \begin{bmatrix} n \\ k \end{bmatrix}_q \mod (q^n-1).$$

Proof. First note that by Definition 6.14 we have

$$|CMP(n)|_q = \sum_{b\in CMP(n)} q^{maj(b)} = \sum_{\substack{b\in BW(n) \\ b_n=0}} q^{maj(b\sim\hat{b})},$$

where $\sim$ denotes concatenation and $\hat{b}$ is such that $\hat{b_i} = 1 - b_i$. Now observe that $maj(b\sim\hat{b}) \equiv maj(b)+maj(\hat{b}) \pmod n$, since any descent in the second half of the concatenation contributing to maj can simply be shifted by n. Furthermore, any contribution to maj by a descent between the first and second half must be exactly 0 or n, since we check the relation $b_n > b_{n+1}$. Instead of making the restriction

$b_n = 0$ we can also sum up with the restriction $b_n = 1$ since by symmetry we will get the same sum $\mathrm{maj}(b) + \mathrm{maj}(\hat{b})$. Hence

$$\sum_{\substack{b\in BW(n)\\ b_n=0}} q^{\mathrm{maj}(b\sim\hat{b}) \pmod n} = \sum_{\substack{b\in BW(n)\\ b_n=1}} q^{\mathrm{maj}(b\sim\hat{b}) \pmod n}.$$

Putting everything together, we have

$$\begin{aligned}
|\mathrm{CMP}(n)|_q \bmod (q^n-1) &= \sum_{b\in CMP(n)} q^{\mathrm{maj}(b)} \bmod (q^n-1)\\
&= \sum_{\substack{b\in BW(n)\\ b_n=0}} q^{\mathrm{maj}(b\sim\hat{b}) \pmod n}\\
&= \frac{1}{2}\sum_{b\in BW(n)} q^{\mathrm{maj}(b\sim\hat{b}) \pmod n}\\
&= \frac{1}{2}\sum_{b\in BW(n)} q^{\mathrm{maj}(b)+\mathrm{maj}(\hat{b}) \pmod n}\\
&= \frac{1}{2}\sum_{b\in BW(n)} q^{\mathrm{maj}(b)+\mathrm{maj}(\hat{b})} \bmod (q^n-1)\\
&= \frac{1}{2}\sum_{k=0}^{n} q^{\binom{k}{2}} \begin{bmatrix} n \\ k \end{bmatrix}_q \bmod (q^n-1).
\end{aligned}$$

Where we used Lemma 6.17 in the last equality. □

We are now ready to present another cyclic sieving phenomenon on circular Möbius Dyck paths of size n [Theorem 37].

Theorem 6.19. The cyclic sieving phenomenon is exhibited by the triple

$$\big(\mathrm{CMP}(n), \langle\tilde{\eta}\rangle, |\mathrm{CMP}|_q\big).$$

Proof. First we prove the quality

$$\frac{1}{2}\sum_{k=0}^{n} q^{\binom{k}{2}} \begin{bmatrix} n \\ k \end{bmatrix}_q = \sum_{k=0}^{n-1} q^{\binom{k}{2}} \begin{bmatrix} n-1 \\ k \end{bmatrix}_q$$

such that we can apply Theorem 6.16. Once again we apply Lemma 3.6, assuming $d \mid k$:

$$\begin{aligned}
\begin{bmatrix} n-1 \\ k \end{bmatrix}_{\omega_d} &= \lim_{q \to \omega_d} \frac{[n-1]_q!}{[k]_q![n-k-1]_q!} \\
&= \lim_{q \to \omega_d} \frac{[n-k]_q}{[k]_q} \cdot \frac{[n-k-1]_q}{[k-1]_q} \cdots \frac{[n-d]_q}{[d]_q} \cdots \frac{[n-1]_q}{[1]_q} \\
&= \frac{n-k}{k} \cdot 1 \cdots 1 \cdot \frac{n-k-d}{k-d} \cdot 1 \cdots 1 \cdot \frac{n-d}{d} \cdot 1 \cdots 1 \\
&= \frac{n/d - k/d}{k/d} \cdots \frac{n/d-1}{1} \\
&= \binom{n/d-1}{k/d}.
\end{aligned}$$

Plugging this into (6.1) and taking the sum over $n-1$ instead of n yields the result.

Next, let $p_1(q), p_2(q)$ be two polynomials such that $p_1(q) \equiv p_2(q) \bmod (q^n-1)$. Then by the polynomial remainder theorem we can write

$$\begin{aligned}
p_1(q) &= q_1(q)(q^n-1) + r(q), \text{ and} \\
p_2(q) &= q_2(q)(q^n-1) + r(q)
\end{aligned}$$

for some polynomials $q_1(q)$ and $q_2(q)$, where $r(q)$ is the remainder polynomial. Substituting for $r(q)$ and yields

$$p_1(q) = p_2(q) + (q^n-1)(q_1(q) - q_2(q)).$$

But then, if we evaluate $p_1(q)$ in d-th roots of unity ω_d (and vice versa for p_2) we get $p_1(\omega_d) = p_2(\omega_d)$, as $d \mid n$.

Since we have shown that

$$|\mathrm{CMP}(n)|_q \equiv \sum_{k=0}^{n-1} q^{\binom{k}{2}} \begin{bmatrix} n \\ k \end{bmatrix}_q \bmod (q^n-1)$$

the above argument shows, that both polynomials coincide when evaluated at d-th roots of unity with $d \mid n$. But by Theorem 6.16, such a polynomial together with CMP(n) and $\langle \hat{\eta} \rangle$ exhibits the CSP. □

Chapter 7

Catalan Objects

In the section about Dyck paths, we already encountered the Catan numbers, which are given directly in terms of binomial coefficients by

$$\mathcal{C}at_{\mathrm{n}} = \frac{1}{\mathrm{n}+1}\binom{2\mathrm{n}}{\mathrm{n}}.$$

There are many counting problems in combinatorics whose solution is given by the Catalan numbers. The book [12] by combinatorialist Richard P. Stanley contains a set of exercises which describe 66 different interpretations of the Catalan numbers. In the following, we are going to discuss three of its instances; triangulations, non-crossing matchings and non-crossing partitions.

It is worth to emphasize that we will use the same polynomial, namely

$$\mathrm{f}(\mathrm{q}) = \frac{1}{[\mathrm{n}+1]_{\mathrm{q}}}\begin{bmatrix}2\mathrm{n}\\ \mathrm{n}\end{bmatrix}_{\mathrm{q}},$$

throughout the different instances, whereas the cyclic group will differ. In fact, we will use the cyclic groups $\mathrm{C}_{\mathrm{n}+2}, \mathrm{C}_{2\mathrm{n}}$ and there is also a result [13] using the cyclic group $\mathrm{C}_{\mathrm{n}-1}$, which is quite astounding. On the other hand, although these objects are in bijection to each other, there is no CSP result on Dyck paths known yet.

7.1 Triangulations

In this section we consider convex polygons and define a polygon triangulation to be a decomposition of a convex polygon into a set of triangles. The catalan-numbers $\mathcal{C}at_{\mathrm{n}}$ count the number of triangulations of a n+2-gon.

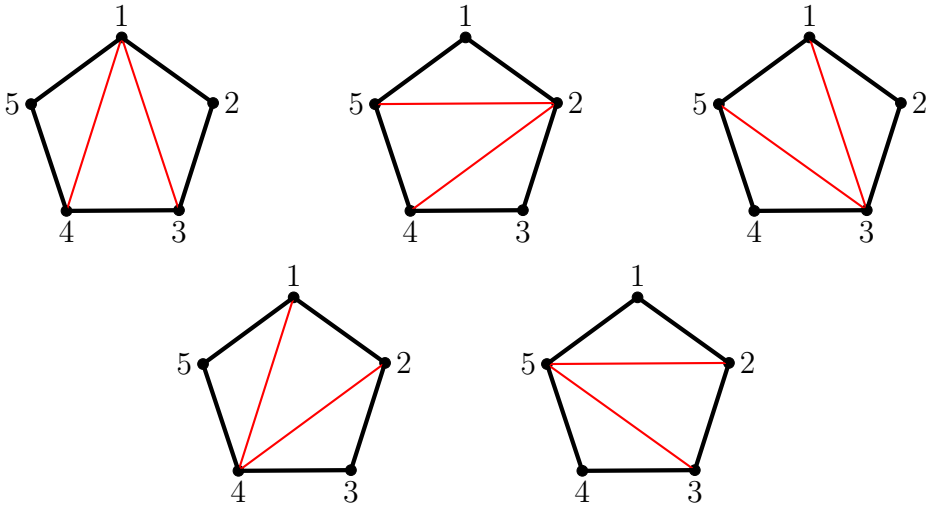

Figure 7.1: List of triangulations for n = 3.

We define $\mathcal{T}(n+2)$ to be the set of triangulations of a $n+2$–gon and C_{n+2} to be the cyclic group acting on $\mathcal{T}(n+2)$ by rotations. The natural q-polynomial for the set $\mathcal{T}(n+2)$ is

$$f(q) = \frac{1}{[n+1]_q} \begin{bmatrix} 2n \\ n \end{bmatrix}_q .$$

In the following, we provide a proof for a CSP result for this triple.

Theorem 7.1. The cyclic sieving phenomenon is exhibited by the triple

$$\left(\mathcal{T}(n+2), C_{n+2}, \frac{1}{[n+1]_q} \begin{bmatrix} 2n \\ n \end{bmatrix}_q\right).$$

Proof. We prove the statement by explicit evaluation. Let ω_d be a d-th root of unity with $d \mid (n+2)$. Writing $f(q)$ explicitly, we have

$$\begin{aligned} f(q) &= \frac{[1]_q \cdots [2n]_q}{[n+1]_q([1]_q \cdots [n]_q)^2} \\ &= \frac{[n+2]_q \cdots [2n]_q}{[1]_q \cdots [n]_q}. \end{aligned}$$

The numerator has $n-1$ factors, whereas the denominator has n factors. Plugging in ω_d, observe that the product $[n+2]_{\omega_d} \cdots [2n]_{\omega_d}$ starts with a zero factor and has every $d-$th factor after that also a zero factor. The product $[1]_{\omega_d} \cdots [n]_{\omega_d}$ has also every $d-$th factor a zero factor but starts with $d-1$ non-zero factors. It

follows that the number of zero factors of the numerator is always greater or equal to the number of zero factors of the denumerator, with equality if and only if d divides $n-1$ or n.

If $d = 1$, clearly $f(\omega_d) = \mathcal{C}at_n$. We assume that $d > 1$ in the following cases.

Case $d \mid n$. Because $d \mid (n+2)$ we have $d \in \{1, 2\}$ if n is even; and $d = 1$ if n is odd.

If $d = 2$, using the fact that $[1]_{\omega_2} = 1$ and applying Lemma 3.6 yields

$$\begin{aligned}\lim_{q\to\omega_2} f(q) &= \lim_{q\to\omega_2}\left(\frac{[n+2]_q}{[2]_q}\cdot\frac{[n+3]_q}{[3]_q}\cdot\ldots\cdot\frac{[2n-1]_q}{[n-1]_q}\cdot\frac{[2n]_q}{[n]_q}\right)\\ &= \frac{n+2}{2}\cdot 1\cdot\frac{n+4}{4}\cdot 1\cdots 1\cdot\frac{2n}{n}\\ &= \frac{n/2+1}{1}\cdot\frac{n/2+2}{2}\cdots\frac{2n/2}{n/2}\\ &= \binom{n}{n/2}.\end{aligned}$$

Case $d \mid (n-1)$. Because $d \mid (n+2)$ we have $d = 3$. Using the fact that $[n]_{\omega_3} = 1$ and applying Lemma 3.6 again, we obtain

$$\begin{aligned}\lim_{q\to\omega_3} f(q) &= \lim_{q\to\omega_3}\left(\frac{[n+2]_q}{[n-1]_q}\cdot\frac{[n+3]_q}{[n-2]_q}\cdots\frac{[2n-2]_q}{[3]_q}\cdot\frac{[2n-1]_q}{[2]_q}\cdot\frac{[2n]_q}{[1]_q}\cdot\frac{1}{[n]_q}\right)\\ &= \frac{n+2}{n-1}\cdot 1\cdot 1\cdot\frac{n+5}{n-4}\cdot 1\cdots 1\cdot\frac{2n-2}{3}\cdot 1\cdot 1\cdot 1\\ &= \frac{n+2}{3}\cdot\frac{n+5}{6}\cdots\frac{2n-2}{n-1}\\ &= \frac{(2n-2)/3!}{(n-1)/3!\cdot(n-1)/3!}\\ &= \binom{(2n-2)/3}{(n-1)/3}.\end{aligned}$$

The second to last equality follows from factoring out and canceling the 3's in the numerator and denominator.

Finally, we have

$$f(\omega_d) = \begin{cases}\frac{1}{n+1}\binom{2n}{n} & \text{if } d = 1,\\ \binom{n}{n/2} & \text{if } d = 2 \text{ and } n \text{ even},\\ \binom{(2n-2)/3}{(n-1)/3} & \text{if } d = 3 \text{ and } n \equiv 1 \bmod 3,\\ 0 & \text{otherwise.}\end{cases} \tag{7.1}$$

Next we need to investigate the fixed points of group elements $c \in C_{n+2}$ acting on $\mathcal{T}(n+2)$. To do so, we give some definitions. We call a straight line segment joining two vertices a *diagonal*. The *diameter* of a polygon is the largest distance between any pair of vertices. In other words, it is the length of the longest diagonal. If n is even and v is a vertex on the polygon, we denote by $\bar{v}$ the vertex opposite to v. The pair $\{v, \bar{v}\}$ is then called an *antipodal pair* of vertices. We now have to distinguish the cases where $c \in C_{n+2}$ has order $d = 1$, $d = 2$, $d = 3$ and $d > 3$.

Case $d = 1$. If $c \in C_{n+2}$ has order 1, it fixes all elements. Therefore we have $|\mathcal{T}(n+2)^c| = \mathcal{C}at_n$.

Case $d = 2$. If $c \in C_{n+2}$ has order 2, then c acts on $\mathcal{T}(n+2)$ as a $\pi-$rotation. This means that the triangulations fixed under c are those, which are centrally symmetric.

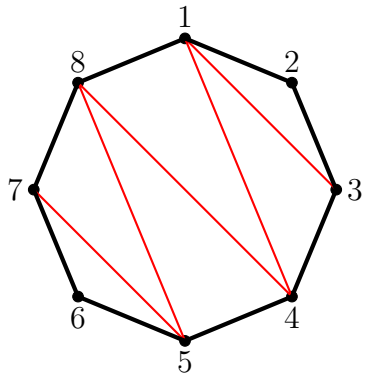

Figure 7.2: A triangulation of a 8-gon which is fixed under a π-rotation.

If n is odd, there is no group element of order 2; so n must be even. Observe that a triangulation is centrally symmetric when it contains diagonal $\{\bar{u}, \bar{v}\}$ as soon as it contains diagonal $\{u, v\}$. Since a triangulation contains $n-1$ diagonals, there must be a unique diameter; namely a diagonal $\{u, \bar{u}\}$. Otherwise the triangulation would contain an even number of diagonals, contradicting the fact that $n-1$ is odd. Note that this only holds for centrally symmetric triangulations; in general, a triangulation must not contain a diameter.

There are $\frac{n+2}{2}$ possibilities for such a diameter, which splits the n+2-gon into two $\frac{n+2}{2}+1$-gons. The number of triangulations of a $\frac{n+2}{2}+1$-gon is counted by the $\frac{n+2}{2}-1$-th Catalan number

$$\mathcal{C}at_{\frac{n+2}{2}-1} = \frac{1}{n/2+1}\binom{n}{n/2}.$$

Summarized there are $\frac{n+2}{2}$ possibilites for a diameter and $\mathcal{C}at_{\frac{n+2}{2}-1}$ different triangulations for one of the split off $\frac{n+2}{2}+1$-gons. For the other $\frac{n+2}{2}+1$-gon

there is only one possibility left, since the n+2-gon has to be centrally symmetric. Therefore there are in total

$$\frac{n+2}{2} \cdot \frac{1}{n/2+1}\binom{n}{n/2} = \binom{n}{n/2}$$

triangulations being fixed, coinciding with (7.1).

Case d = 3. In order to discuss this case, we define the *length of a diagonal* $\{u, v\}$ to be the minimal number of edges on the n+2-gon between u and v. Further, we say that a vertex on the n+2-gon is *covered* by a diagonal $\{u, v\}$, if it lies between the vertices u and v on the polygon that is described by the edges on the n+2-gon and the diagonal $\{u, v\}$.

Let $T \in \mathcal{T}(n+2)$ be a triangulation fixed under a 3-fold rotation. An element $c \in C_{n+2}$ with order 3 acts on a triangulation by rotating every vertex, say clockwise, by $\frac{n+2}{3}$ vertices. Observe that diagonals in T have at most length $\frac{n+2}{3}$. To see this, we suppose there exists a diagonal $\{u, v\}$ with length larger than $\frac{n+2}{3}$ and without loss of generality we assume that $u < v$. This diagonal is rotated into the diagonal $\{u + \frac{n+2}{3}, v + \frac{n+2}{3} \bmod (n+2)\}$, but by assumption $u + \frac{n+2}{3} < v$ and hence $\{u, v\}$ and $\{u + \frac{n+2}{3}, v + \frac{n+2}{3} \bmod (n+2)\}$ would be a set of crossing edges, contradicting the fact that T is a triangulation.

We assume now, T does not have a diagonal with length $\frac{n+2}{3}$. Consider then the diagonal $\{u, v\}$ in T with greatest length. In this case, the vertex u (and also v) is not covered by any diagonal. But then, the vertex $u + \frac{n+2}{3} \bmod (n+2)$, in which the vertex u is rotated to, is neither covered by any diagonal. Therefore, the vertices u and $u + \frac{n+2}{3} \bmod (n+2)$ can be joined by a diagonal, contradicting the fact that T is a triangulation.

So T contains a diagonal $\{u, v\}$ of length $\frac{n+2}{3}$. Since T is 3-fold rotationally symmetric, it contains 3 such diagonals and these compose a triangle.

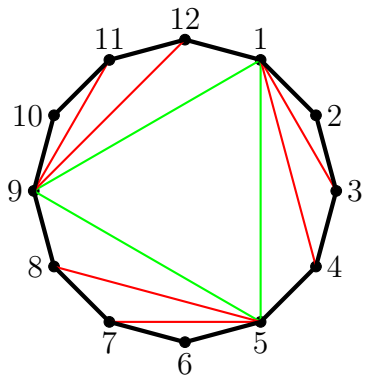

Figure 7.3: A triangulation on 12 vertices that is fixed under a 3-fold rotation. The green triangle consists of polygon diagonals with greatest possible length.

Knowing that a triangulation fixed under a 3-fold rotation must contain a triangle composed by diagonals with length $\frac{n+2}{3}$, we can count how many 3-fold rotationally symmetric triangulations exist. Let $\{a, b, c\}$ denote the vertices of such a triangle. Between a and b, respectively between b and c and also between c and a, there are $\frac{n+2}{3} - 1$ vertices. Therefore there are $\frac{n+2}{3}$ possibilites to choose our triangle. This triangle decomposes the polygon into 3 $\frac{n+2}{3} + 1$-gons, which all must have the same triangulation; otherwise the triangulation would not be fixed. But we know that these triangulations are counted by $\mathcal{C}at_{\frac{n+2}{3}-1}$. So in total we have

$$\begin{aligned}\frac{n+2}{3}\mathcal{C}at_{\frac{n+2}{3}-1} &= \frac{n+2}{3}\frac{1}{(n+2)/3}\binom{(2n-2)/3}{(n-1)/3} \\ &= \binom{(2n-2)/3}{(n-1)/3}\end{aligned}$$

triangulations in $\mathcal{T}(n+2)$ that are fixed under c, coinciding with (7.1).

Case $d > 3$. Applying the exact same argument as in the previous case, we get that a d-fold rotationally symmetric triangulation T must contain d diagonals with length $\frac{n+2}{d}$. These diagonals compose a d-gon. Observe that in this d-gon, only adjacent vertices can be joined by a diagonal: Joining two non-adjacent vertices would require a diagonal with a length larger than $\frac{n+2}{d}$. But this means, that T contains vertices which still could be joined by diagonals; hence T can not be a triangulation. Therefore there is no triangulation that is fixed under a d-fold rotation for $d > 3$, which completes the proof. □

7.2 Non-Crossing Matchings

Having used the cyclic group C_{n+2} in the triple to prove the cyclic sieving phenomenon on triangulations, we will use the cyclic group C_{2n} for non-crossing matchings; the polynomial f(q), however, will be the same.

For the definition of a non-crossing matching, we recall some basic definitions of graph theory. Let $V = \mathbb{N}_n$ be a set of n vertices and $E \subseteq \{\{u, v\} \mid (u, v) \in V \times V \text{ and } u \neq v\}$ be a set of edges. Then we call G = (V,E) a *graph*. A *complete graph* is a graph in which every pair of vertices is connected by an edge. Finally, we give a definition of a non-crossing matching on a convex 2n-polygon.

Definition 7.2. Let G be a complete graph on 2n vertices. A *non-crossing matching* in G is a set of n pairwise non-adjacent edges, such that there are no edges $\{a, b\}$ and $\{c, d\}$ fulfilling the relations

$$a < c < b < d. \tag{7.2}$$

We will denote the set of non-crossing matchings on 2n vertices by NCM(2n).

Note that in general one does not require a matching to have n edges. We will work with this definition, which would be called a *perfect matching* in graph theory. Further, assume the vertices of our graphs to be arranged in a convex 2n-gon in a circular order.

It is a well known fact, that NCM(2n) is counted by the Catalan numbers $\mathcal{Cat}_n$. We let the generator of C_{2n} act on NCM(2n) by a $\frac{\pi}{n}$ rotation.

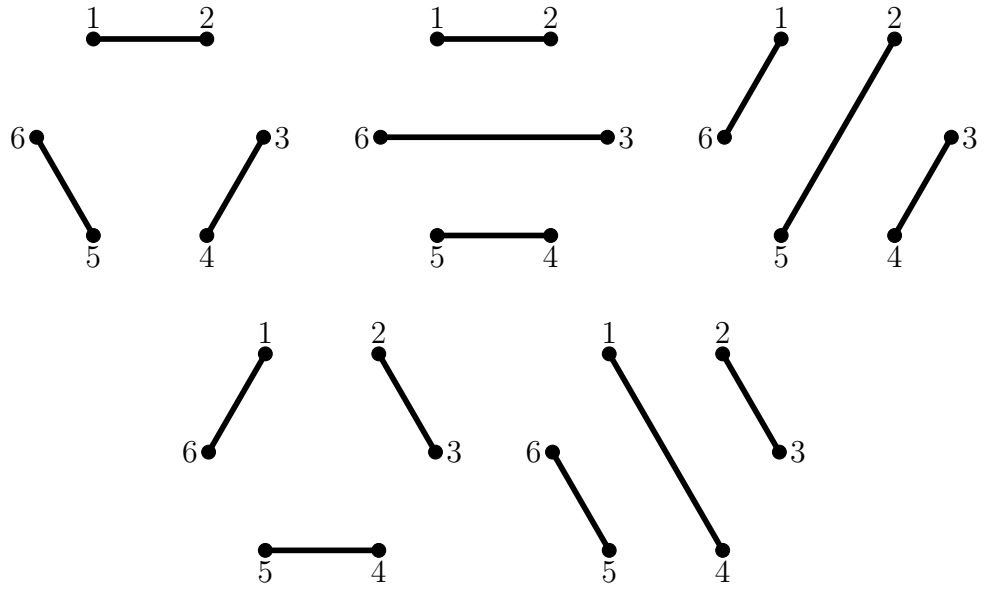

Figure 7.4: List of non-crossing matchings for n = 3.

Theorem 7.3. The cyclic sieving phenomenon is exhibited by the triple

$$\big(\mathrm{NCM}(2n), C_{2n}, \frac{1}{[n+1]_q}\begin{bmatrix}2n\\ n\end{bmatrix}_q\big).$$

Proof. Once again we prove the statement by explicit evaluation. Let ω_d again be a d-th root of unity with $d \mid 2n$. With the exact same argument as in Theorem 7.1, we write

$$\begin{aligned} f(q) &= \frac{[1]_q \cdots [2n]_q}{[n+1]_q([1]_q \cdots [n]_q)^2} \\ &= \frac{[n+2]_q \cdots [2n]_q}{[1]_q \cdots [n]_q} \end{aligned}$$

and observe that the number of zero factor of the numerator and denumerator is equal if and only if if d divides $n-1$ or n.

If $d = 1$, clearly $f(\omega_d) = \mathcal{Cat}_n$. We assume that $d > 1$ in the following cases.

Case $d \mid n$. Because $d \mid 2n$ we have $2n \equiv n \equiv 0 \pmod{d}$. Using the fact that $[1]_{\omega_d} = 1$ and applying Lemma 3.6 yields

$$\begin{aligned}\lim_{q\to\omega_d} f(q) &= \lim_{q\to\omega_d}\left(\frac{[n+2]_q}{[2]_q}\cdot\frac{[n+3]_q}{[3]_q}\cdot\ldots\cdot\frac{[2n-1]_q}{[n-1]_q}\cdot\frac{[2n]_q}{[n]_q}\right)\\ &= 1\cdots 1\cdot\frac{n+d}{d}\cdot 1\cdots 1\cdot\frac{2n-d}{n-d}\cdot 1\cdots 1\cdot\frac{2n}{n}\\ &= \frac{n/d+1}{1}\cdot\frac{n/d+2}{2}\cdots\frac{2n/d}{n/d}\\ &= \binom{2n/d}{n/d}.\end{aligned}$$

Case $d \mid (n-1)$. In this case $d \nmid n$. Since $d \mid 2n$, this implies $d = 2$ and so n is odd. Using the fact that $[1]_{\omega_d} = 1$ and applying Lemma 3.6 yields

$$\begin{aligned}\lim_{q\to\omega_d} f(q) &= \lim_{q\to\omega_d}\left(\frac{[n+2]_q}{[n]_q}\cdot\frac{[n+3]_q}{[2]_q}\cdot\ldots\cdot\frac{[2n-1]_q}{[n-2]_q}\cdot\frac{[2n]_q}{[n-1]_q}\right)\\ &= 1\cdot\frac{n+3}{2}\cdot 1\cdots 1\cdot\frac{2n-2}{n-3}\cdot 1\cdot\frac{2n}{n-1}\\ &= \frac{(n+3)/2}{1}\cdot\frac{(n-1)/2}{(n-3)/2}\cdots\frac{2n/2}{(n-1)/2}\\ &= \binom{n}{(n+1)/2}.\end{aligned}$$

Finally, we obtain

$$f(\omega_d) = \begin{cases}\frac{1}{n+1}\binom{2n}{n} & \text{if } d = 1,\\ \binom{2n/d}{n/d} & \text{if } d > 1 \text{ and } d \mid n,\\ \binom{n}{(n+1)/2} & \text{if } d > 1 \text{ and } d \mid (n-1),\\ 0 & \text{otherwise.}\end{cases} \tag{7.3}$$

In order to evaluate the number of fixed points of an element $c \in C_{2n}$ with order d, we now have to distinguish the cases $d = 1$, $d \mid n$, and $d \mid (n-1)$.

Case $d = 1$. If $c \in C_{2n}$ has order 1, it fixes all elements. Therefore we have $|\mathrm{NCM}(2n)^c| = \mathcal{Cat}_n$. In the following we assume that $d > 1$.

Case d | n. A first observation is, that if $n = md$, for $m \in \mathbb{N}$, then $\frac{2n}{d}$ is always even, since

$$\frac{2n}{d} = \frac{2md}{d} = 2m.$$

The element $c \in C_{2n}$ acts on NCM(2n) by a rotation of $\frac{2\pi}{d}$, which is equal to rotating the vertices by $\frac{2n}{d}$. We let $k := \frac{2n}{d}$ and denote by $\mathrm{NCM}_k(2n)$ the set of non-crossing matchings in NCM(2n), which are invariant under a rotation by k vertices.

We will establish a correspondence[1] between $\mathrm{NCM}_k(2n)$ and the subsets of $\mathbb{N}_k$ of size $\frac{k}{2}$. To do so, we say that the left-endpoint $L\{a, b\}$ of a matched edge $\{a, b\}$, where we write it in the way that $a < b$, is equal to

$$L\{a, b\} = \begin{cases} a & \text{if } b = a + i \text{ for some } 0 \leq i < k, \\ b & \text{else.} \end{cases}$$

To illustrate, look at the following matching.

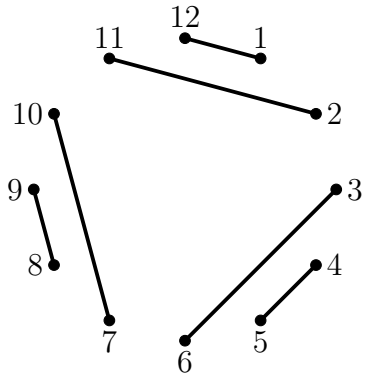

Figure 7.5: A non-crossing matching which is fixed under a rotation by 4 vertices. In the matched edge $\{2, 11\}$ the left-endpoint is 11; whereas in the matched edge $\{7, 10\}$ the left endpoint is 7, since $10 = 7 + 3$ and $3 < 4$.

Consider a subset $S \subseteq \mathbb{N}_k$ of size $\frac{k}{2}$. Such subsets will be referred to as sets of left-endpoints. We construct a circle with k symbols, where the j-th symbol is an arrow pointing clockwise if $j \in S$, respectively an arrow pointing counterclockwise if $j \notin S$. If an clockwise pointing arrow, being the j-th symbol, is followed by a counterclockwise pointing arrow, then j and j+1 are matched to each other. We

[1] We would like to thank Mike Earnest, a contributor to Mathematics Stackexchange, for the idea of this correspondence.

delete the matching arrows, which gives us a smaller circle, and repeat this process again until all elements of $\mathbb{N}_k$ are matched.

We give an example for k = 10 and S = {1,2,4,7,8}.

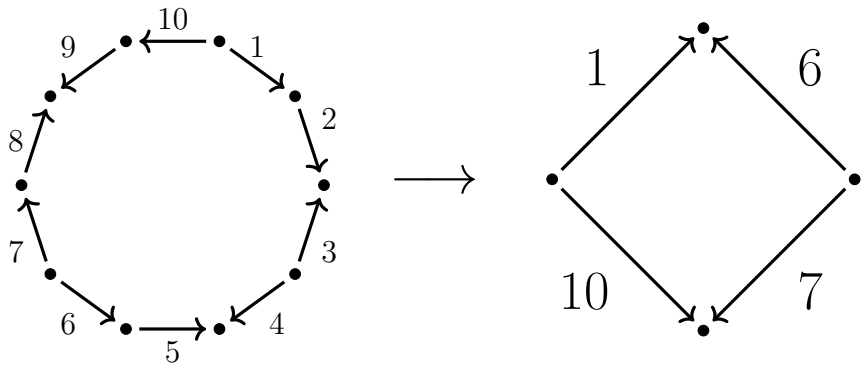

Figure 7.6: Algorithm for k = 10. In the first iteration, the following edges are created by matching the corresponding vertices: $\{2,3\}, \{4,5\}, \{8,9\}$. In the second iteration, the matchings are $\{1,6\}$ and $\{7,10\}$.

The resulting non-crossing matchings are invariant under a k-rotation. Note that with this algorithm the condition (7.2) is automatically fulfilled. The above algorithm must now be extended to the whole 2n-gon, by placing $d = \frac{2n}{k}$ copies of the circle onto a 2n-gon. If j and j+1 are matched to each other, then also j + mk (mod 2n) and j + 1 + mk (mod 2n) are matched to each other, for all $1 \leq m \leq \frac{2n}{k}$. More general, if a and b are matched to each other during the algorithm, then also a + mk (mod 2n) and b + mk (mod 2n) are matched to each other, for all m. Hence the resulting non-crossing matching is indeed invariant under a rotation of k vertices.

The elements of S correspond to left-endpoints. Further we claim that the elements of S, which correspond to a clockwise pointing arrow in the circle, result indeed in left-endpoints with this construction. Since $|S| = \frac{k}{2}$, in every of the constructed copies there are each $\frac{k}{2}$ clockwise and counterclockwise pointing arrows. After placing them circularly onto a 2n-gon, consider an arbitrary clockwise pointing arrow, corresponding to an element $s \in S$. Observe that if we move on clockwise in this circle, there can be at most $\frac{k}{2} - 1$ consecutively clockwise pointing arrows in front of our clockwise pointing arrow. In this case, these arrows are follow by $\frac{k}{2}$ consecutively counterclockwise pointing arrows. Therefore the vertex s will be matched with the vertex $s + (k-1)$. This is the largest possible distance between two matched vertices.

If $s < 2n$ and $s + (k-1) < 2n$, by definition $L\{s, s + (k-1)\} = s$.

If $s < 2n$ and $s+(k-1) > 2n$, we have the matching edge $\{s+(k-1) \pmod{2n}, s\}$.

As $d = \frac{2n}{k}$, observe that

$$\begin{aligned} s - (s + (k-1) \pmod{2n}) &= 2n - (k-1) \\ &= kd - (k-1) \\ &= k(d-1) + 1. \end{aligned}$$

If $d > 1$, we get $k(d-1) + 1 > k + 1 > k - 1$. In this case, by definition s is a left-endpoint again. Observe that if $d = 1$, then $k = 2n$ and we have the matching edge $\{s-1, s\}$. In this case, s is not a left-endpoint and therefore our correspondence only works if we assume $d > 1$ (what we did in the beginning). The same holds for every $0 \leq i \leq k-1$, so the claim follows.

Since our sets S are the set of left-endpoints of its associated matchings, by construction our correspondence is injective.

The correspondence is surjective. Let $M \in NCM_k$ be arbitrary. We follow the 2n-gon clockwise and place an arrow pointing clockwise over a vertex if it is a left-endpoint of a matching edge, respectively an arrow pointing counterclockwise if it is a right-endpoint. Let $\{a, b\}$ and edge in M. Since M is fixed under a rotation of k vertices, this edge is rotated into the edge $\{a+k \pmod{2n}, b+k \pmod{2n}\}$. Hence left- and right-endpoints are rotated into left- and right-endpoints again. But then, the arrow sequence of k arrows is repeated every k vertices. Since there are $\frac{2n}{k}$ such blocks of k arrows and there are n edges, the number $|S|$ of left-endpoints in every block must satisfy the equation

$$\frac{2n}{k} \cdot |S| = n.$$

Therefore $|S| = \frac{k}{2}$.

We show now that if we apply the construction on S, the resulting non-crossing matching is indeed M. For the sake of deriving a contradiction, assume that the resulting matching is not M. Then there exist an edge $\{a, b\}$ in M, that is not matched by this construction. Without loss of generality we suppose that a is the left-endpoint. The construction ensures, however, that the vertex a is a left endpoint in the resulting non-crossing matching. Now if a is not matched with b, then there must be at least either one clockwise pointing arrow (corresponding to a left-endpoint) in front of a, or a counterclockwise pointing arrow (corresponding to a right-endpoint) before b in the constructed circle of arrows. Assume there is a left-endpoint c in front of a that is matched with b. This means, that there is at least one more left-endpoint than right-endpoints between a and b. And one of them has to be joined with a right-endpoint, say d, in M, which has to be positioned after b in the circle.

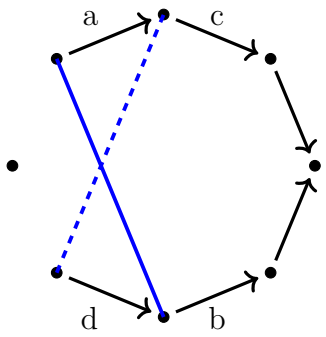

Figure 7.7: The edge $\{a, b\}$ is crossed by the edge with right endpoint d.

But then, the edge $\{a, b\}$ is crossed by another edge; contradicting the fact that M is a non-crossing matching.

Finally, we have that M corresponds to a unique $S \subseteq \mathbb{N}_k$ with size $\frac{k}{2}$, since S is determined by the left-endpoints. Hence the correspondence is surjective and thus bijective. The number of such subsets $S \subseteq \mathbb{N}_k$ is of course

$$\binom{k}{k/2},$$

which coincides with (7.3) as $k = \frac{2n}{d}$.

Case $d \mid (n-1)$. As discussed, in this case we have $d = 2$. This implies that $k = n$ is odd and that the non-crossing matchings fixed under $c \in C_{2n}$ must be centrally symmetric. Then again, there must be a unique diameter since the number of edges n is odd. There are n possibilites to choose the diameter, which cuts the remaining vertices into two halves with each $\frac{2n-2}{2} = n-1$ vertices. For one of this half, there are $\mathcal{Cat}_{\frac{n-1}{2}}$ possible non-crossing matchings; the other half must be exactly be the same, since we have central symmetry. Therefore we get

$$\begin{aligned} n \cdot \mathcal{Cat}_{\frac{n-1}{2}} &= n \cdot \frac{1}{(n-1)/2+1}\binom{n-1}{(n-1)/2} \\ &= \frac{n}{(n+1)/2}\frac{(n-1)!}{((n-1)/2)!^2} \\ &= \frac{n!}{(n+1)/2)!(n-1)/2)!} \\ &= \binom{n}{(n+1)/2} \end{aligned}$$

coinciding with (7.3), which completes the proof. □

It follows the very last section of this thesis.

7.3 Non-Crossing Partitions

Germain Kreweras defined non-crossing partitions in 1972, and they have been intensively studied since. To define them, number the vertices of a convex n-gon by $\mathbb{N}_n$ in a circular order. A *partition* of $\mathbb{N}_n$ is a dissection into pairwise non-empty subsets of $\mathbb{N}_n$, which are called *blocks*. We identify these blocks with the convex hulls of its vertices in the n-gon and call the partition *non-crossing*, if these convex hulls are pairwise disjoint.

This last section will follow [1, pages 34 - 36], where we will elaborate the arguments in more detail. We define the set of non-crossing partitions on n vertices to be NC(n) and say that $N \in NC(n)$ has rank $n - b$, if it has b blocks. The cardinality $|NC(n)|$ is the Catalan number $\mathcal{C}at_n$, and the number of elements at rank k in NC(n), which we denote by $NC(n,k)$, are counted by the *Narayana number*

$$N(n,k) = \frac{1}{n}\binom{n}{k}\binom{n}{k+1}.$$

The formula follows from a stronger result, see [14, Theorem 4]. For a discussion, consider [15, Chapter 4].

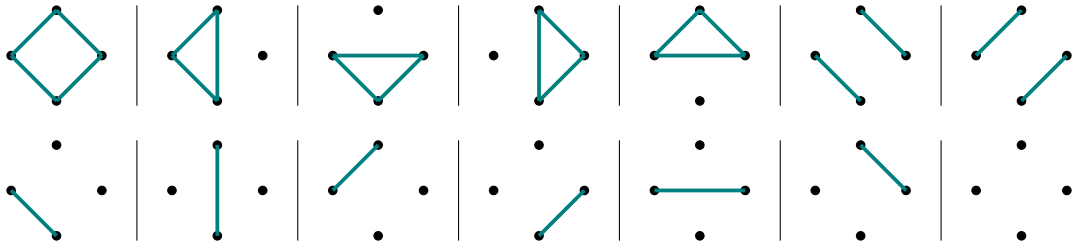

Figure 7.8: List of non-crossing partitions for $n = 4$.

A natural q-analogue of the Narayana number is given by

$$N(n,k)(q) := \frac{1}{[n]_q}\begin{bmatrix} n \\ k \end{bmatrix}_q \begin{bmatrix} n \\ k+1 \end{bmatrix}_q q^{k(k+1)}.$$

Again we let C_n be the group of order n, which acts on NC(n) by cyclic rotations of the n-gon. The following proof is based on [1, Theorem 7.2].

Theorem 7.4. The cyclic sieving phenomenon is exhibited by the triple

$$\Big(NC(n,k), C_n, \frac{1}{[n]_q}\begin{bmatrix} n \\ k \end{bmatrix}_q \begin{bmatrix} n \\ k+1 \end{bmatrix}_q q^{k(k+1)}\Big).$$

Proof. Let ω_d be a d-th root of unity such that $d \mid n$.

Case $d \mid k$. Expanding $N(n,k)(q)$ by $[n-k]_q$, we obtain

$$\frac{1}{[n]_q}\begin{bmatrix} n \\ k \end{bmatrix}_q \begin{bmatrix} n \\ k+1 \end{bmatrix}_q q^{k(k+1)} \cdot \frac{[n-k]_q}{[n-k]_q} = \frac{1}{[n]_q}\begin{bmatrix} n \\ k \end{bmatrix}_q \frac{[n]_q!}{[k+1]_q![n-k-1]_q!} q^{k(k+1)} \cdot \frac{[n-k]_q}{[n-k]_q}$$
$$= \frac{[n-k]_q}{[n]_q[k+1]_q}\begin{bmatrix} n \\ k \end{bmatrix}_q^2 q^{k(k+1)}.$$

We have $[k+1]_{\omega_d} = 1$ and since $n-k \equiv n \equiv 0 \pmod{d}$, Lemma 3.6 implies

$$\lim_{q \to \omega_d} \frac{[n-k]_q}{[n]_q} = \frac{n-k}{n}.$$

When evaluated at $q = \omega_d$, the power $q^{k(k+1)}$ is clearly 1. Further, by Lemma 3.7 we have

$$\begin{bmatrix} n \\ k \end{bmatrix}_q^2 = \binom{n/d}{k/d}^2.$$

Therefore it holds

$$NC(n,k)(\omega_d) = \frac{n-k}{n}\binom{n/d}{k/d}^2.$$

Case $d \mid (k+1)$. Expanding $N(n,k)(q)$ by $[k+1]_q$, we obtain

$$\frac{1}{[n]_q}\begin{bmatrix} n \\ k \end{bmatrix}_q \begin{bmatrix} n \\ k+1 \end{bmatrix}_q q^{k(k+1)} \cdot \frac{[k+1]_q}{[k+1]_q} = \frac{1}{[n]_q}\frac{[n]_q!}{[k]_q![n-k]_q!}\begin{bmatrix} n \\ k+1 \end{bmatrix}_q q^{k(k+1)} \cdot \frac{[k+1]_q}{[k+1]_q}$$
$$= \frac{[k+1]_q}{[n]_q[n-k]_q}\begin{bmatrix} n \\ k+1 \end{bmatrix}_q^2 q^{k(k+1)}.$$

With the same arguments as above we have

$$N(n,k)(\omega_d) = \frac{k+1}{n}\binom{n/d}{(k+1)/d}^2,$$

since $k+1 \equiv n \equiv 0 \pmod{d}$ and $d \mid (n-k-1)$ implies $[n-k]_{\omega_d} = 1$.

Case $d \nmid k$ and $d \nmid (k+1)$. Writing the polynomial explicitly we have

$$N(n,k)(q) = \frac{1}{[n]_q}\frac{[n]_q!}{[k]_q![n-k]_q!}\frac{[n]_q!}{[k+1]_q![n-k-1]_q!} q^{k(k+1)}$$
$$= \frac{[n-1]_q \cdots [n-k+1]_q}{[k]_q!}\frac{[n]_q \cdots [n-k]_q}{[k+1]_q!} q^{k(k+1)}.$$

Observe that the numerator and denominator in the left fraction both start with $d-1$ non-zero factors and then have every d-th factor a zero factor. Since $d \nmid k$ by assumption, we can ignore the last factor $[k]_q$, such that there equally many zero factors in both terms. This means, the number of zero factors coincides in both terms. On the other hand, the numerator in the right fraction starts with a zero factor and has every d-th factor after that also as a zero factor, whereas the denominator starts with $d-1$ non-zero factors. Hence the numerator always has one more zero factor than the denominator, unless $d \mid (k+1)$, which we excluded by assumption. But then, the whole term is zero. Finally, we have

$$N(n,k)(\omega_d) = \begin{cases} \frac{n-k}{n}\binom{n/d}{k/d}^2 & \text{if } d \mid k, \\ \frac{k+1}{n}\binom{n/d}{(k+1)/d} & \text{if } d \mid (k+1), \\ 0 & \text{otherwise.} \end{cases} \tag{7.4}$$

Now we must compute the number of elements in NC(n,k) which are invariant under a d-fold rotation. For this, we introduce some notations.

We write the elements of a block in ascending order, namely $B = \{b_1, \ldots, b_m\}$, such that $b_i < b_{i+1}$ for all $1 < i < m$. A block $B \subseteq \mathbb{N}_n$ is called *central*, if it satisfies

$$b_{i+1} - b_i = \frac{n}{|B|} \bmod n$$

for all i, where $|B|$ denotes the cardinality of B and the indices are taken mod $|B|$. Next we recall that $\bar{b}$ is the vertex opposite to b on the polygon. We call two blocks B_1, B_2 *antipodal*, if $\bar{b} \in B_2$ as soon as $b \in B_1$.

To illustrate, consider the non-crossing partition $\{\{2\},\{4\},\{6\},\{1,3,5\}\}$. By definition, the block $B = \{1,3,5\}$ is central and the partition contains no pair of antipodal blocks.

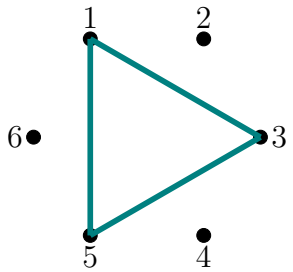

Figure 7.9: A non-crossing partition that contains a central block. Each two vertices of the central block have a difference of 2 (mod 6).

Now observe that when a non-crossing partition is d-fold rotationally symmetric, none of its blocks are fixed under a rotation with order d except for possibly

the central block, if it exists. The orbit of each block must consist of d blocks and hence the number of blocks is congruent either to 0 or 1 modulo d. Since $d \mid n$ and $b = n - k$, this means that there will be no such partitions unless $d \mid k$ or $d \mid (k+1)$, in agreement with (7.4).

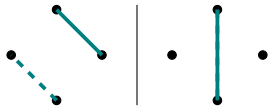

Figure 7.10: Two non-crossing partitions that are 2-fold rotationally symmetric. Observe that in the left non-crossing partition, the block denoted by the thick line is rotated into the dashed line under a 2-fold rotation; thus not fixed. The non-crossing partition in the right however has a central block, which is fixed by a 2-fold rotation.

This leaves the two cases where $d \mid k$ or $d \mid (k+1)$. Here we will utilize a result which can be found in [16, Lemma 4.4].

Lemma 7.5. Let $N \in \mathbb{N}$. There are $\binom{N}{p}^2$ centrally symmetric non-crossing partitions of $\mathbb{N}_{2N}$ that have p antipodal pairs of blocks and among these

- the fraction which have a central block is $\frac{N-p}{N}$, so
- the fraction with no central block is $\frac{p}{N}$.

□

To illustrate, let $N = 2$ and $p = 1$. Then there are $\binom{2}{1}^2 = 4$ centrally symmetric non-crossing partitions of $\mathbb{N}_4$ that have 1 antipodal pair of blocks. Looking at figure 7.7, these are the following:

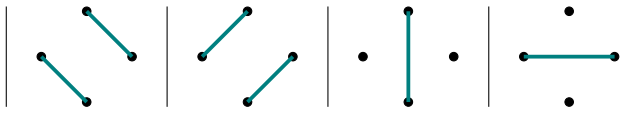

Figure 7.11: Non-crossing partitions on 4 vertices with 1 antipodal pair of blocks.

And the fraction which have a central block, respectively which have no central block, is $\frac{1}{2}$, coinciding with Lemma 7.5.

Case $d \mid k$. Then $b \equiv 0 \pmod{d}$ and there is a bijection [17, Proposition 1] to centrally symmetric non-crossing partitions of $\mathbb{N}_{2n/d}$ having $\frac{2b}{d}$ blocks: Given a non-crossing partition $P \in \mathrm{NCP}(n)$ on n vertices that is d-rotationally symmetric,

there is a set of $\frac{n}{d}$ vertices that uniquely determines P. As P has b blocks, this set must have $\frac{b}{d}$ blocks. We map P to the non-crossing partition on $\frac{2n}{d}$ vertices that arises by concatenating the set of $\frac{n}{d}$ vertices in a circle. Observe that the arised partition is centrally symmetric and has $\frac{2b}{d}$ blocks with $\frac{b}{d}$ antipodal pairs of blocks and no central block.

Therefore, these partitions are counted by the following formula for $N = \frac{n}{d}$, $p = \frac{b}{d}$:

$$\frac{p}{N}\binom{N}{p}^2 = \frac{b/d}{n/d}\binom{n/d}{b/d}^2 = \frac{n-k}{n}\binom{n/d}{k/d}^2.$$

This agrees with (7.4) for $d \mid k$.

Case $d \mid (k+1)$. Then $b \equiv 1 \pmod{d}$ and as in the previous case, there is an obvious bijection to centrally symmetric non-crossing partitions of $\mathbb{N}_{2n/d}$ having $\frac{2(b-1)}{d} + 1$ blocks. The latter will have $\frac{b-1}{d}$ antipodal pairs of non-central blocks and one central block, and so are counted by the following formula with $N = \frac{n}{d}$, $p = \frac{b-1}{d}$:

$$\frac{N-p}{N}\binom{N}{p}^2 = \frac{n/d-(b-1)/d}{n/d}\binom{n/d}{(b-1)/d}^2 = \frac{k+1}{n}\binom{n/d}{(k+1)/d}^2.$$

This agrees with (7.4) for $d \mid (k+1)$, which finishes the proof. □

Bibliography

[1] V. Reiner, D. Stanton and D. White. *The cyclic sieving phenomenon.* Journal of Combinatorial Theory, Series A 108 (2004) 17-50.

[2] B. E. Sagan. *The cyclic sieving phenomenon: a survey.* arXiv:1008.0790v3.

[3] P. Alexandersson, S. Linusson and S. Potka. *The cyclic sieving phenomenon on circular dyck paths.* arXiv:1903.01327v1.

[4] R. P. Stanley. *Algebraic Combinatorics.* Springer, second edition (2018).

[5] B. E. Sagan. *The Symmetric Group.* Springer, second edition (2001).

[6] D. Foata and G. Han. *The q-series in combinatorics; permutation statistics.* Lecture Notes in Mathematics (2011).

[7] T. Kyle Petersen. *Eulerian Numbers.* Springer, first edition (2015).

[8] A. Buryak. *Representation Theory of Finite Groups and in Particular Symmetric Groups.* Lecture Notes in Mathematics (2015).

[9] G. Pólya. *Kombinatorische Anzahlbestimmungen für Gruppen, Graphen und chemische Verbindungen.* Acta mathematica. (1937).

[10] N.G. de Bruijn. *Generalization of Pólya's fundamental theorem in enumerative combinatorial analysis.* Nederl. Akad. Wetensch. Proc. Ser. A 62 = Indag. Math 21 (1959).

[11] V. Kac and P. Cheung. *Quantum Calculus (Universitext).* Springer, (2001).

[12] R. P. Stanley. *Enumerative Combinatorics, Volume 2.* Cambridge University Press, (1999).

[13] M. Thiel. *A new cyclic sieving phenomenon for catalan objects.* arXiv:1601.03999v2.

[14] G. Kreweras. *Sur les partitions non croisées d'un cycle*. Discrete Math. 1 (1972), 333-350.

[15] D. Armstrong. *Generalized Non-Crossing Partitions and Combinatorics of Coxeter Groups*. arXiv:math/0611106v2.

[16] C. A. Athanasiadis and V. Reiner. *Non-crossing partitions for the group* $\mathrm{D_n}$. preprint 2003 (at www.math.umn.edu/ reiner/Papers/papers.html).

[17] V. Reiner. *Non-crossing partitions for classical reflection groups*. Discrete Math. 177 (1997) 195-222.