A Chinese Remainder Theorem for Partitions

A Thesis

submitted to
Indian Institute of Science Education and Research Pune
in partial fulfillment of the requirements for the
BS-MS Dual Degree Programme

by

Seethalakshmi K

Indian Institute of Science Education and Research Pune
Dr. Homi Bhabha Road,
Pashan, Pune 411008, INDIA.

April, 2019

Supervisor: Amritanshu Prasad

Certificate

This is to certify that this dissertation entitled A Chinese Remainder Theorem for Partitions towards the partial fulfilment of the BS-MS dual degree programme at the Indian Institute of Science Education and Research, Pune represents study/work carried out by Seethalakshmi K at The Institute of Mathematical Sciences, Chennai under the supervision of Amritanshu Prasad, Professor, Department of Mathematics , during the academic year 2018-2019.

Amritanshu Prasad

Amritanshu Prasad

Committee:

Amritanshu Prasad

Steven Spallone

This thesis is dedicated to my parents and teachers.

Declaration

I hereby declare that the matter embodied in the report entitled A Chinese Remainder Theorem for Partitions are the results of the work carried out by me at the Department of Mathematics, at The Institute of Mathematical Sciences, Chennai, under the supervision of Amritanshu Prasad and the same has not been submitted elsewhere for any other degree.

Seethalakshmi K

Acknowledgments

I would like to express my deep gratitude to Prof. Amritanshu Prasad and Prof. Steven Spallone for their valuable guidance and support throughout this project. I'm extremely thankful and indebted to them for sharing expertise and for always steering me in the right direction with immense patience.

Special thanks to Dr. Brendan McKay for providing insights on the asymptotic enumeration of integer matrices with constant row and column sum [4]. I also take this opportunity to thank Ragini and Ojaswi for the helpful discussions during the initial stages of this project.

I would like to thank my friends (especially Ni and Chi) for always being there for me. Last but not the least, I thank my parents for the unceasing encouragement and support.

Abstract

Given $s, t \in \mathbb{N}$ such that $\gcd(s,t) = d$, $\mathrm{lcm}(s,t) = m$, an s-core σ, and a t-core τ, we write $N_{\sigma,\tau}(k)$ for the number of m-cores of length no greater than k whose s-core is σ and t-core is τ. In this thesis we prove that, for $k \gg 0$, $N_{\sigma,\tau}(k)$ is a quasi-polynomial of quasi-period m and degree $\frac{1}{d}(s-d)(t-d)$.

Contents

"The unusual nature of these coincidences might lead us to suspect that some sort of witchcraft is operating behind the scene."

- Donald Knuth

Introduction

The study of integer partitions by visualizing them as Young diagrams was first introduced in [14] and has led to many new insights. The concepts of hooks and hook lengths associated to the Young diagram of a partition has been discussed in [8] and used to prove the hook length formula for the degree of an irreducible representation of S_n. The theory of cores has applications in Representation theory of S_n: Character formulas, mod p theory, and Ramanujan congruences. It also has been used to prove an effective upper bound on $p(n)$ using purely combinatorial methods [15].

For a partition λ, there is a notion of 'a remainder of λ upon division by s' called the s-core of λ and an s-quotient whose total number of nodes is equal to the number of s-hooks removed to obtain the s-core. A partition λ can be recovered from its s-core and s-quotient. It is known that

$$|\lambda| = s(|\mathrm{quot}_s\lambda|) + |\mathrm{core}_s\lambda|$$

where the modulus denotes the total number of nodes. This is an analogue of division for partitions and by this we can say that $\mathrm{core}_s\lambda$ is a kind of remainder. So we look at the Chinese remainder theorem for partitions.

In the first Chapter, we give some preliminaries on the theory of cores. Then we count s-cores of given length using an s-abacus. It is much more difficult to count the s-cores of given size [10].

Polytopes are the higher dimensional versions of polygons. Many counting problems can be translated into the language of polytopes. In Chapter 2, we recall the theory of Ehrhart polynomials for counting integer points in a k-dilated polytope. Using this and the concepts of totally unimodular matrices (matrices with sub-determinants +1, -1 or 0), we provide a variant of Ehrhart theory for some special kind of polytopes defined by totally unimodular matrices. This will help us in counting integer points in certain transportation polytopes which are formed by the set of all non-negative real matrices having fixed row sum and column sum.

Let $N_{\sigma,\tau}(k)$ be the number of m-cores of length no greater than k whose s-core is σ and t-core is τ where $m = \operatorname{lcm}(s,t)$. In the third Chapter, we see how finding the asymptotics of $N_{\sigma,\tau}(k)$ translates into the problem of counting integer points in certain transportation polytopes. Then we use the variant of Ehrhart theory developed in Chapter 2 to prove our main result.

A function $f : \mathbb{N} \to \mathbb{N}$ is a quasi-polynomial of degree d and quasi-period p if its restriction to each coset $p\mathbb{N} + j$ is a polynomial of degree d ([13], Section 4.4).

Write $V(\frac{\mathbf{s}}{\mathbf{d}}, \frac{\mathbf{t}}{\mathbf{d}})$ for the relative volume ([13], page 565) of the transportation polytope for row margins $(\underbrace{\frac{s}{d}, \dots, \frac{s}{d}}_{\frac{t}{d}\text{ times}})$ and column margins $(\underbrace{\frac{t}{d}, \dots, \frac{t}{d}}_{\frac{s}{d}\text{ times}})$. We prove that

Theorem 0.0.1. *For $k \gg 0$, $N_{\sigma,\tau}(k)$ is a quasi-polynomial of quasi-period $m = \operatorname{lcm}(s,t)$ and degree $\frac{1}{d}(s-d)(t-d)$, with leading coefficient $(V(\frac{\boldsymbol{s}}{\boldsymbol{d}}, \frac{\boldsymbol{t}}{\boldsymbol{d}}))^d$.*

Chapter 1

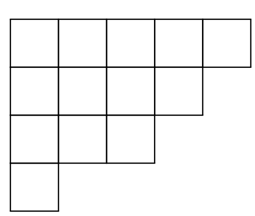
Introduction to Core Partitions

1.1 Preliminaries

For $n \in \mathbb{N}$, a **partition** of n is a non-increasing sequence of positive integers $\lambda = (a_1, a_2, \dots, a_\ell)$ satisfying $a_1 + a_2 + \dots + a_\ell = n$. The positive integers a_i are called the parts of λ and the total number of parts, denoted as $\ell(\lambda)$, is called the length of λ. We write Λ for the set of all partitions.

1.1.1 The Young diagram of a partition

A partition λ of n can be visualized as a **Young diagram** (also known as Ferrers graph), $Y(\lambda)$, consisting of a collection of n boxes arranged in $\ell(\lambda)$ rows which are left justified with a_i boxes in the ith row.
For example, when $\lambda = (5, 4, 3, 1)$, $Y(\lambda)$ is as follows.



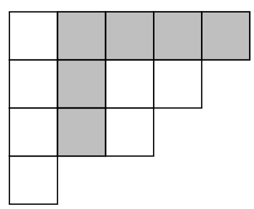
The jth box in the ith row of $Y(\lambda)$ is called the (i,j)-node. We associate a **hook** and a **hook length** to the (i,j)-node. Let

$$Y(\lambda) = \{(i,j) \in \mathbb{N} \times \mathbb{N} \mid 1 \leq i \leq \ell(\lambda), 1 \leq j \leq a_i\}.$$

Then the (i,j)-hook is given by

$$H_{ij}(\lambda) = \{(i',j') \in Y(\lambda) \mid i' = i \ \ and \ \ j' \geq j \ \ or \ \ j' = j \ \ and \ \ i' > i\}$$

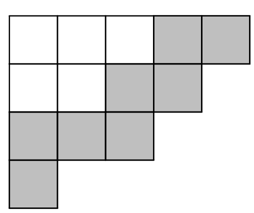
The (i,j)-hook consists of the (i,j)-node and all the nodes to the right and below it. The total number of nodes in the (i,j)-hook is called the hook length of the (i,j)-node. If a hook is of length h_{ij}, then it is also called an h_{ij}-hook.
The $(1,2)$- hook of the partition $(5,4,3,1)$ of hook length six is shown as shaded boxes in the figure below.



An (i,j)-node is called a **rim node** if there is no $(i+1,j+1)$-node in the Young diagram. All such nodes in $Y(\lambda)$ form the **rim** of λ given by

$$R(\lambda) = \{(i',j') \in Y(\lambda) \mid (i'+1, j'+1) \notin Y(\lambda)\}.$$

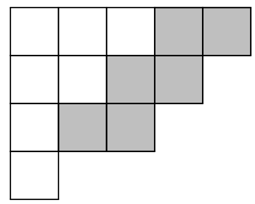
The rim of $(5,4,3,1)$ consists of the shaded boxes in the figure below.



The (i,j)**-rim hook** is a portion of the rim given by

$$R_{ij}(\lambda) = \{(i',j') \in R(\lambda) \mid i' \geq i \ \ and \ \ j' \geq j\}.$$

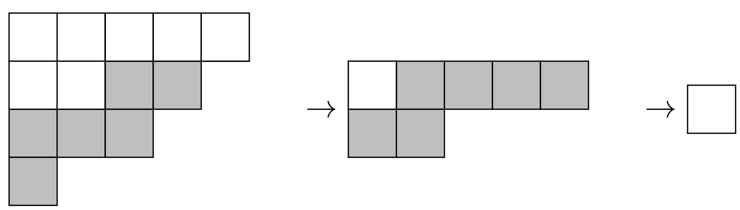
The $(1,2)$-rim hook of $(5,4,3,1)$ is shaded in the figure below.



1.1.2 The s-core of a partition

Rim hooks are removable in the sense that, removal of a rim hook results in another Young diagram. Given $Y(\lambda)$, we remove rim s-hooks successively until no s-hook remains in the Young diagram. It turns out that the resulting Young diagram does not depend on the sequence in which rim s-hooks are removed (this will be clear from the abacus method for finding s-cores which is discussed in section 1.2.4). The resulting partition is called the s-**core** of λ.

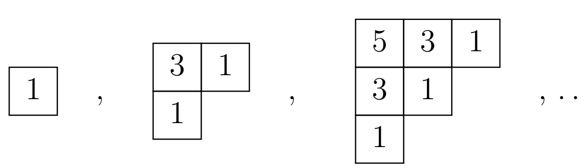
Example 1. Let $\lambda = (5,4,3,1)$ and $s = 6$.



Therefore $\mathrm{core}_6(5,4,3,1) = (1)$.

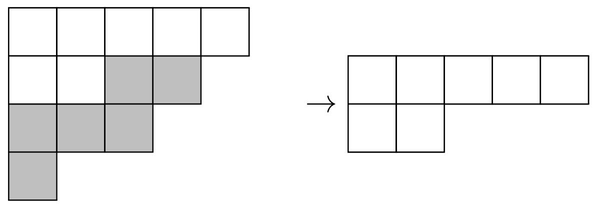
An s-**core** is a partition having no s-hook in its Young diagram. Write C_s for the set of all s-cores and C_s^k for those of length no greater than k. We define the map $\mathrm{core}_s : \Lambda \to C_s$ as $\mathrm{core}_s(\lambda) = \mathrm{core}_s\lambda$ where $\mathrm{core}_s\lambda$ denotes the s-core of λ.

Example 2. The 2-cores are the staircase partitions,

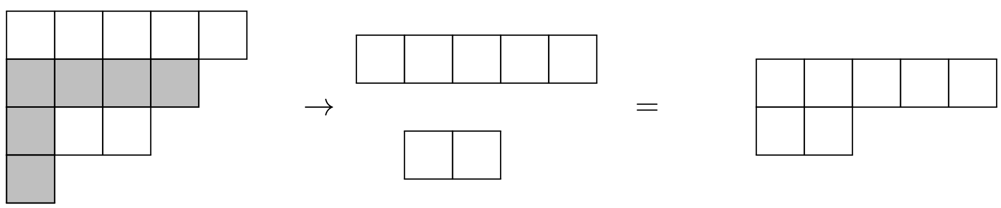


Proposition 1.1.1. *Removing $R_{ij}(\lambda)$ from $Y(\lambda)$ is equivalent to removing $H_{ij}(\lambda)$ and rearranging the nodes accordingly.*

For example, when $\lambda = (5,4,3,1)$, removing the (1,2)-rim hook gives $(5,2)$.



Removing 1,2-hook and rearranging also gives $(5,2)$.



Proposition 1.1.2. *If $d \mid s$,*

$$\mathrm{core}_d \mathrm{core}_s \lambda = \mathrm{core}_d \lambda.$$

Thus a d-core is also an s-core.

1.1.3 Beta sets of a partition

We encode a partition in certain subsets of non-negative integers called beta sets. They can be thought of as a generalization of the set of first column hook lengths of the partition. Beta sets are very useful in characterizing and dealing with the core partitions as we will see in later sections.

The Young diagram of a partition can be reconstructed from its first column hook lengths. Suppose $H(\lambda) = \{h_1, h_2, \ldots, h_\ell\}$ where $h_1 > h_2 > \ldots > h_\ell$ is the set of first column hook lengths of λ. Then the partition λ can be recovered as

$$\lambda = (h_1 - \ell + 1, h_2 - \ell + 2, \ldots, h_\ell). \tag{1.1}$$

Let $\mathcal{H}$ be the set of all finite subsets of $\mathbb{N}$. The map $H : \Lambda \to \mathcal{H}$ taking a partition λ to its first column hook lengths set $H(\lambda)$ is a bijection.

Let $\mathcal{H}^*$ be the set of all finite subsets of $\mathbb{N} \cup \{0\}$. Define the map $S : \mathcal{H}^* \to \mathcal{H}^*$ as

$$\{h_1, h_2, \ldots, h_\ell\} \mapsto \{h_1 + 1, h_2 + 1, \ldots, h_\ell + 1, 0\}.$$

Given $H \in \mathcal{H}^*$, there exists a unique $H_0 \in \mathcal{H}$ and $j \geq 0$ such that $S^j(H_0) = H$. For $j \geq 0$, $S^j(H(\lambda))$ is called the **beta set** of λ of length $\ell(\lambda) + j$. We will use the notation H_λ^k for the beta set of λ of length k. By this notation, $H_\lambda^{\ell(\lambda)} = H(\lambda)$.

Example 3. Let $\lambda = (5, 4, 3, 1)$, $\ell(\lambda) = 4$.

Then $H(\lambda) = \{5 + (4 - 1), 4 + (4 - 2), 3 + (4 - 3), 1 + (4 - 4)\} = \{8, 6, 4, 1\}$.
The next beta set of length 5 is,
$S(H_\lambda^4) = H_\lambda^5 = \{8 + 1, 6 + 1, 4 + 1, 1 + 1, 0\} = \{9, 7, 5, 2, 0\}$.

Now λ can be retrieved from H_λ^5 as,
$H_\lambda^5 = \{9, 7, 5, 2, 0\} \rightsquigarrow \{9 - (5 - 1), 7 - (5 - 2), 5 - (5 - 3), 2 - (5 - 4), 0 - (5 - 5)\} = (5, 4, 3, 1, 0) \rightsquigarrow \lambda = (5, 4, 3, 1)$.

Lemma 1.1.3 ([9, Lemma 2.7.13])**.** *Suppose $H(\lambda) = \{h_1, h_2, \ldots, h_\ell\}$. Then a beta set of the partition $\lambda \setminus R_{ij}$, obtained by removing the (i, j)-rim hook of λ is given by*

$$\{h_1, \ldots, h_{i-1}, h_i - k, h_{i+1}, \ldots, h_\ell\}.$$

1.1.4 Abacus

An s-abacus has s-runners numbered from 0 to $s - 1$. The ith runner is numbered vertically as $i, i + s, i + 2s$ and so on. More details can be found in Section 2.7 of [9].

$$\begin{array}{cccc}
\overline{0} & \overline{1} & \cdots & \overline{s-1} \\
\hline
0 & 1 & \cdots & s-1 \\
s & s+1 & \cdots & 2s-1 \\
\vdots & \vdots & \vdots & \vdots
\end{array}$$

A beta set of a partition can be displayed on an s-abacus by placing beads on the numbers which are elements of the beta set. A bead is shown as $\bullet$ and a space without a bead is shown as $\circ$. For instance, let $s = 3$ and $H(\lambda) = \{8, 6, 4, 1\}$. Then the 3-abacus display of $H(\lambda)$ is as follows.

$$\begin{array}{ccc} \overline{0} & \overline{1} & \overline{2} \\ \hline \circ & \bullet & \circ \\ \circ & \bullet & \circ \\ \bullet & \circ & \bullet \end{array}$$

Finding s-core on s-abacus

The following proposition provides a quick method to find the s-core of a partition using the s-abacus display of its beta set.

Proposition 1.1.4. *[15, page 3] The s-hooks in $Y(\lambda)$ correspond to beads with a space above them in the s-abacus display of a beta set of λ. An abacus display for the partition obtained by removing a given s-hook is achieved by sliding the corresponding bead one position up its runner.*

This follows from Lemma 1.1.3.

Hence, to find the s-core of λ we consider the abacus display of a beta set of λ and move all the beads to their highest possible position. This gives a beta set of $\mathrm{core}_s\lambda$ from which we can retrieve $\mathrm{core}_s\lambda$.

Example 4. Let $\lambda = (5, 4, 3, 1)$ and $s = 6$. Move the beads to their highest possible position on the 6-abacus display of $H(\lambda) = \{8, 6, 4, 1\}$.

$$\begin{array}{cccccc} \overline{0} & \overline{1} & \overline{2} & \overline{3} & \overline{4} & \overline{5} \\ \hline \circ & \bullet & \circ & \circ & \bullet & \circ \\ \bullet & \circ & \bullet & \circ & \circ & \circ \end{array} \quad \rightarrow \quad \begin{array}{cccccc} \overline{0} & \overline{1} & \overline{2} & \overline{3} & \overline{4} & \overline{5} \\ \hline \bullet & \bullet & \bullet & \circ & \bullet & \circ \\ \circ & \circ & \circ & \circ & \circ & \circ \end{array}$$

Therefore $H^4_{core_6\lambda} = \{4, 2, 1, 0\} \rightsquigarrow core_6(5, 4, 3, 1) = (1)$.

1.2 Arithmetic of core partitions

Let λ be a partition of length no greater than k. Then define

$$H^k_{\lambda,s} = \{h \mod s \mid h \in H^k_\lambda\} \in \left(\!\!\binom{\mathbb{Z}/s\mathbb{Z}}{k}\!\!\right)$$

where $\left(\!\binom{\mathbb{Z}/s\mathbb{Z}}{k}\!\right)$ denotes the k element multisets on $\mathbb{Z}/s\mathbb{Z}$.

For $H \in \left(\!\binom{\mathbb{Z}/s\mathbb{Z}}{k}\!\right)$, write $H(r)$ for the multiplicity of r in the multiset H. Note that, $H^k_{\lambda,s}(r)$ is the number of beads on the r^{th} runner when H^k_λ is displayed on an s abacus.

Lemma 1.2.1. *For $i \geq \ell(\lambda)$ and $k \in \mathbb{N}$,*

$$H^{i+sk}_{\lambda,s}(r) = H^i_{\lambda,s}(r) + k$$

Proof. From the definition of a length $i + sk$ beta set of λ it follows that,

$$H^{i+sk}_\lambda = \{h + sk \mid h \in H^i_\lambda\} \cup \{sk-1, sk-2, \ldots, 0\}.$$

Hence, $H^{i+sk}_{\lambda,s} = H^i_{\lambda,s} \cup \{0^k, 1^k, \ldots, (s-1)^k\}$ which implies $H^{i+sk}_{\lambda,s}(r) = H^i_{\lambda,s}(r) + k$. $\square$

Lemma 1.2.2. *Let λ, μ be partitions of length no greater than k. Then* $\mathrm{core}_s(\lambda) = \mathrm{core}_s(\mu)$ *if and only if $H^k_{\lambda,s} = H^k_{\mu,s}$.*

Proof. We know that $\mathrm{core}_s(\lambda) = \mathrm{core}_s(\mu)$ if and only if $H^k_{\mathrm{core}_s(\lambda),s} = H^k_{\mathrm{core}_s(\mu),s}$.

$H^k_{\mathrm{core}_s(\lambda),s} = H^k_{\lambda,s}$ since $H^k_{\lambda,s}(r)$ is the number of beads on the r^{th} runner when H^k_λ is displayed on an s abacus. Similarly, $H^k_{\mathrm{core}_s(\mu),s} = H^k_{\mu,s}$. Thus the result follows. $\square$

Proposition 1.2.3. *The map $\mathscr{A}_s : C^k_s \to \left(\!\binom{\mathbb{Z}/s\mathbb{Z}}{k}\!\right)$ defined as $\sigma \mapsto H^k_{\sigma,s}$ is a bijection.*

Proof. Injectivity of the map follows from Lemma 1.2.1. For surjectivity, given any $H \in \left(\!\binom{\mathbb{Z}/s\mathbb{Z}}{k}\!\right)$ place $H(r)$ beads on the rth runner of an s-abacus. This gives an abacus display of a beta set of some s-core σ such that $H^k_{\sigma,s} = H$, from which we get H^k_σ and thus σ. $\square$

1.2.1 Counting s-core partitions

The s-core partitions of length ℓ can be counted easily on an s abacus. For $a, b \in \mathbb{N}$, we write $\left(\!\binom{a}{b}\!\right)$ for the number of b-tuples of non-negative integers $(x_1, x_2, \ldots, x_b)$ satisfying $x_1 + x_2 + \ldots + x_b = a$.

Proposition 1.2.4 ([16, Theorem 2.3])**.** *The number of s-cores of length ℓ is*

$$\left(\!\binom{\ell}{s-1}\!\right) = \binom{\ell+s-2}{\ell}.$$

Proof. We have that the s-core partitions correspond to s-abacus displays with no beads on the 0th runner and no sliding up possible. The number of beads is the length of the partition. Therefore, the number of s-cores of length ℓ is same as the number of ways to distribute ℓ beads on on $s-1$ runners. By applying "stars and bars" method [2] we get that $\left(\!\binom{\ell}{s-1}\!\right) = \binom{\ell+s-2}{\ell}$. □

Proposition 1.2.5. *The maximum size of an s-core of length ℓ is $(s-1)\binom{\ell+1}{2}$.*

Proof. We will find the maximum size of a beta set of cardinality ℓ, from which we obtain the maximum size of an s-core of length ℓ. We need to place all ℓ beads on the last runner of the s-abacus on their highest possible position to get the beta set with maximum size. Hence, $\{\ell s-1, (\ell-1)s-1, \ldots, s-1\}$ is the beta set of maximum size and the corresponding s-core is, $(\ell s-1, (\ell-1)s-(\ell-1), \ldots, \ell-1)$. Therefore, the maximum size of an s-core of length ℓ is,

$$\sum_{i=1}^{\ell} is - i = (s-1)\binom{\ell+1}{2}.$$

□

1.2.2 Fibres of the map from st-cores to s-cores

As a warm up to the CRT for partitions, let us consider the map $\mathrm{core}_s : C_{st} \to C_s$ taking an st-core to its s-core. Given $\sigma \in C_s$, let

$$N_\sigma(k) = \{\lambda \in C_{st} \mid core_s\lambda = \sigma, \ell(\lambda) \leq k\}.$$

In other words, $N_\sigma(k)$ is the cardinality of the fibre of $\mathrm{core}_s : C^k_{st} \to C^k_s$ over σ. Now we define the map $\mathscr{S}_s : \left(\!\binom{\mathbb{Z}/st\mathbb{Z}}{k}\!\right) \to \left(\!\binom{\mathbb{Z}/s\mathbb{Z}}{k}\!\right)$ as

$$F \mapsto F_s = \{f \mod s \mid f \in F\}.$$

From the definition of the map $\mathscr{S}_s$ it follows that,

$$F_s(a \mod s) = \sum_{m=0}^{t-1} F(a + ms \mod st). \tag{1.2}$$

Proposition 1.2.6. *The following diagram commutes,*

$$\begin{tikzcd} C^k_{st} \arrow[r, "\mathrm{core}_s"] \arrow[d, "\mathscr{A}_{st}"'] & C^k_s \arrow[d, "\mathscr{A}_s"] \\ \left(\!\binom{\mathbb{Z}/st\mathbb{Z}}{k}\!\right) \arrow[r, "\mathscr{S}_s"] & \left(\!\binom{\mathbb{Z}/s\mathbb{Z}}{k}\!\right) \end{tikzcd}$$

Proof. Let $\sigma \in C^k_{st}$, then $\mathscr{A}_{st}(\sigma) = H^k_{\sigma,st}$ and $\mathscr{A}_s(\mathrm{core}_s\sigma) = H^k_{\mathrm{core}_s\sigma,s}$. We will show that

$$\mathscr{S}_s(H^k_{\sigma,st}) = H^k_{\mathrm{core}_s\sigma,s}.$$

We have,

$$H^k_{\sigma,st} = \{h \mod st \mid h \in H^k_\sigma\}.$$

Then

$$\begin{aligned} \mathscr{S}_s(H^k_{\sigma,st}) &= \{g \mod s \mid g \in H^k_{\sigma,st}\} \\ &= \{(h \mod st) \mod s \mid h \in H^k_\sigma\} \\ &= \{h \mod s \mid h \in H^k_\sigma\} \\ &= H^k_{\sigma,s} = H^k_{\mathrm{core}_s\sigma,s}. \end{aligned}$$

□

By Proposition 1.2.6, $N_\sigma(k)$ is also the cardinality of the fibre of $\mathscr{S}_s$ over $H^k_{\sigma,s}$.

Quasi-polynomials

A function $f : \mathbb{N} \to \mathbb{N}$ such that

$$f(x) = c_d(x)x^d + c_{d-1}(x)x^{d-1} + \cdots + c_0(x)$$

where $c_i(x)$ are periodic functions is called a quasi-polynomial. Let p be a common period of $c_0, \cdots, c_d$, then $f(x) = f_i(x)$ for $n \equiv i \mod p$ where f_is are polynomials and p is called a quasi-period of f. In other words, a function $f : \mathbb{N} \to \mathbb{N}$ is a quasi-polynomial of degree d and quasi-period p if its restriction to each coset $p\mathbb{N} + j$ is a polynomial of degree d.

Example 5. For $d \in \mathbb{N}$, $f(k) = \lfloor \frac{k}{d} \rfloor$ is a quasi-polynomial of degree 1 and quasi-period d.

Theorem 1.2.7. *For $k \geq \ell(\sigma)$, $N_\sigma(k)$ is a quasi-polynomial of degree $s(t-1)$ and quasi-period s.*

Proof. Given $F_s \in \left(\!\binom{\mathbb{Z}/s\mathbb{Z}}{k}\!\right)$, by (1.2) the number of $F \in \left(\!\binom{\mathbb{Z}/st\mathbb{Z}}{k}\!\right)$ such that $\mathscr{S}_s(F) = F_s$ is

$$\prod_{j=0}^{s-1} \left(\!\binom{F_s(j)}{t}\!\right)$$

where $\left(\!\binom{F_s(j)}{t}\!\right)$ is the number of ways to distribute $F_s(j)$ beads on t runners.

Therefore for $i \geq \ell(\sigma)$,

$$\begin{aligned} N_\sigma(i+sk) &= \prod_{j=0}^{s-1} \left(\!\binom{H^{i+sk}_{\sigma,s}(j)}{t}\!\right) \\ &= \prod_{j=0}^{s-1} \left(\!\binom{H^{i}_{\sigma,s}(j)+k}{t}\!\right) \end{aligned}$$

Then the theorem follows from the formula for $\left(\!\binom{a}{b}\!\right)$. $\square$

Chapter 2

Introduction to Polytopes

The enumeration of integer points in a bounded region of the Euclidean space is a common problem which appears in various fields of mathematics disguised in different forms. The Frobenius coin exchange problem well explained in [1], Section 1.2, is a beautiful example of this. Our main goal is to enumerate the fibres of the Chinese remainder theorem map. We will see that this is equivalent to counting integer points in certain polytopes. In this Chapter, we develop the necessary machinery required for this task.

2.1 Preliminaries

A polytope is a higher dimensional analogue of a polygon in two dimensions. In this section, we recall some basic concepts and define polytopes more carefully.

Definition 2.1.1. A set X is said to be convex if for every $x, y \in X$, $tx + (1-t)y \in X$ for all $t \in (0, 1)$.

Definition 2.1.2. The convex hull of a set $X = \{x_1, x_2, \dots, x_k\}$ is the smallest convex set which contains X given by

$$\operatorname{conv}(X) = \{\sum_{i=1}^{k} \lambda_i x_i \mid \lambda_i \geq 0, \sum_{i=1}^{k} \lambda_i = 1\}.$$

Now we give the "vertex description" of a polytope.

Definition 2.1.3. A convex polytope P in $\mathbb{R}^n$ is defined as

$$P = \mathrm{conv}(\{v_1, v_2, \ldots, v_m\})$$

for some $\{v_1, v_2, \ldots, v_m\} \subset \mathbb{R}^n$ called the vertices of P.

If all vertices of P are integer points in $\mathbb{R}^n$, then it is called a lattice polytope. The dimension of P is the vector space dimension of the subspace, $\mathrm{span}(\{v_2 - v_1, \ldots, v_m - v_1\})$. A d dimensional polytope is called a d-polytope. We will be considering only convex polytopes in this thesis and henceforth we will refer to them as just polytopes. Polytopes can also be defined as a bounded intersection of finitely many half spaces. We discuss some preliminaries for this drawn from [7].

Hyperplanes are subspaces of dimension one less than its ambient vector space. Let $\mathbf{a} \in \mathbb{R}^{1\times n}$ and $b \in \mathbb{R}$. A hyperplane defined as

$$H = \{\mathbf{x} \in \mathbb{R}^n \mid \mathbf{ax} = b\}$$

separates the ambient vector space into two halfspaces,

$$H^+ = \{\mathbf{x} \in \mathbb{R}^n \mid \mathbf{ax} \geq b\}, \quad H^- = \{\mathbf{x} \in \mathbb{R}^n \mid \mathbf{ax} \leq b\}.$$

These are called the closed halfspaces bounded by H.

Definition 2.1.4. A hyperplane H is called a supporting hyperplane of a closed convex set $K \subset \mathbb{R}^n$ if $K \cap H \neq \emptyset$ and $K \subset H^-$ or $K \subset H^+$.

If $K \subset H^-$, then H^- is called a supporting halfspace of K. Now we are ready to give the "hyperplane description" of a polytope.

Definition 2.1.5. A bounded intersection of k halfspaces given by

$$P = \{\mathbf{x} \in \mathbb{R}^n \mid \mathbf{a}_i\mathbf{x} \leq b_i, 1 \leq i \leq k\},$$

where $\mathbf{a}_i \in \mathbb{R}^{1\times n}$ and $b_i \in \mathbb{R}$ is called a polytope.

Note that, since an equality of the form $\mathbf{a}_i\mathbf{x} = b_i$ can be replaced by two inequalities $\mathbf{a}_i\mathbf{x} \leq b_i$ and $-(\mathbf{a}_i\mathbf{x}) \leq -b_i$, the constraints defining a polytope can include both equalities and inequalities. The equivalence of vertex description and hyperplane description can be found in Appendix A of [1]. If the condition of boundedness is removed from the definition of a polytope then it is called a polyhedron.

2.2 Counting integer points in polytopes

For a polytope P in $\mathbb{R}^n$ let

$$L_P(k) = \#(kP \cap \mathbb{Z}^n),$$

be the number of integer points in the k-dilated polytope of P. Suppose P is a lattice polygon. Then by Pick's theorem

$$L_P(k) = A(P)k^2 + \frac{1}{2}B(P)k + 1,$$

where $A(P)$ is the area of P and $B(P)$ is the number of integer points on the boundary of P ([11], Theorem 5.11). Ehrhart's theorem is an extension of Pick's theorem in higher dimensions.

Theorem 2.2.1 ([11, Theorem 13.4])**.** *Let P be a lattice d-polytope in $\mathbb{R}^n$. Then $L_P(k)$ is a polynomial in k of degree d.*

Let P' be the projection of P on to the d-dimensional space $\mathbb{R}^d$. The volume of P' is said to be the relative volume of P ([13], page 565). For example, the triangle in $\mathbb{R}^3$

$$T = \{(x_1, x_2, x_3) \in \mathbb{R}^3_{\geq 0} \mid x_1 + x_2 + x_3 = 1\}$$

can be projected on to $\mathbb{R}^2$ to get the triangle

$$T' = \{(x_1, x_2) \in \mathbb{R}^2_{\geq 0} \mid x_1 + x_2 \leq 1\}.$$

The relative volume of T is the area of T'.

Proposition 2.2.2 ([13, Proposition 4.6.13])**.** *Let P be a lattice d-polytope in $\mathbb{R}^n$. Then the leading coefficient of $L_P(k)$ is $V(P)$, the relative volume of P.*

There is a more general version of Ehrhart's theorem for counting integer points in polytopes with rational vertices.

Theorem 2.2.3 ([1, Theorem 3.23])**.** *Let P be a d-dimensional polytope with rational vertices. Then $L_P(k)$ is a quasi-polynomial in k of degree d and its quasi-period dividing the least common multiple of the denominators of the vertices of P.*

Example 6. The closed interval $P = \lfloor \frac{a}{b}, \frac{c}{d} \rfloor$ is a one dimensional polytope, where $\frac{a}{b}, \frac{c}{d}$ are in their lowest terms.

$$L_P(k) = \lfloor \frac{kc}{d} \rfloor - \lfloor \frac{ka-1}{b} \rfloor.$$

From example 5 we know that $\lfloor \frac{k}{d} \rfloor$ is a quasi-polynomial of quasi-period d. Hence in this case, $L_P(k)$ is a quasi-polynomial with quasi-period $\mathrm{lcm}(b, d)$.

Ehrhart's theorem is proved using the following lemma which uses the theory of generating functions.

Lemma 2.2.4 ([1, Lemma 3.24])**.** *Suppose the generating function of f is given as,*

$$\sum_{k \geq 0} f(k) x^k = \frac{g(x)}{h(x)}.$$

Then f is a quasi-polynomial of degree d with period dividing p if and only if g and h are polynomials where $\deg(g) < \deg(h)$*, all roots of h are p^{th} roots of unity of multiplicity at most $d+1$, and there is a root of multiplicity equal to $d+1$(assuming $\frac{g}{h}$ is reduced to lowest terms).*

Now we discuss some special kind of polytopes relevant to our problem.

2.3 Polytopes of totally unimodular matrices

Definition 2.3.1. An $m \times n$ matrix A is said to be totally unimodular if the determinant of any square submatrix of A is +1, -1 or 0.

Given a totally unimodular $m \times n$ matrix A and a vector $\mathbf{b} \in \mathbb{R}^m$, suppose

$$P(A, \mathbf{b}) = \{\mathbf{x} \in \mathbb{R}^n \mid A\mathbf{x} \leq \mathbf{b}\}$$

is a bounded closed subset of $\mathbb{R}^n$. Then $P(A, \mathbf{b})$ is said to be the polytope associated to the totally unimodular matrix A and vector $\mathbf{b}$.

Proposition 2.3.1 ([12, Corollary 19.2 a]). *Let A be an integer matrix. Then A is totally unimodular if and only if for each integer vector $\boldsymbol{b}$ the polyhedron $\{\boldsymbol{x} \in \mathbb{R}^n \mid A\boldsymbol{x} \leq \boldsymbol{b}\}$ has integer vertices.*

2.3.1 Transportation polytopes

Let $\mathbf{r} \in \mathbb{R}^s$ and $\mathbf{c} \in \mathbb{R}^t$ be positive real vectors and $\mathbf{x} = (x_{ij})_{1\leq i\leq s, 1\leq j\leq t}$ be an $s \times t$ matrix. The constraints on row sums and column sums of $\mathbf{x}$ are specified as

$$\sum_{j=1}^{t} x_{ij} = r_i, 1 \leq i \leq s, \qquad \sum_{i=1}^{s} x_{ij} = c_j, 1 \leq j \leq t. \tag{2.1}$$

If $\sum\limits_{i=1}^{s} r_i \neq \sum\limits_{j=1}^{t} c_j$, there does not exist a matrix $\mathbf{x}$ satisfying the above conditions. Hence we assume that the vectors $\mathbf{r}$ and $\mathbf{c}$ have equal sums. The feasible solutions of (2.1) forms a polytope, called the transportation polytope for margins $\mathbf{r}$ and $\mathbf{c}$, denoted by $P(\mathbf{r}, \mathbf{c})$. By viewing the $s \times t$ matrix $\mathbf{x}$ as an st-vector the transportation polytope can be given as

$$P(\mathbf{r}, \mathbf{c}) = \{\mathbf{x} \in \mathbb{R}^{st} \mid A\mathbf{x} = \mathbf{b}, \mathbf{x} \geq 0\}$$

for some matrix A and vector b where $A\mathbf{x} = b$ is the constraints (2.1).

Proposition 2.3.2 ([3, Theorem 8.1.1]). *The dimension of the transportation polytope $P(\boldsymbol{r}, \boldsymbol{c})$ is $(s-1)(t-1)$.*

Lemma 2.3.3 ([3, Corollary 8.1.4]). *The transportation polytope $P(\boldsymbol{r}, \boldsymbol{c})$ is a lattice polytope if $\boldsymbol{r} \in \mathbb{Z}^s$ and $\boldsymbol{c} \in \mathbb{Z}^t$.*

Proposition 2.3.4. *The transportation polytope $P(\boldsymbol{r}, \boldsymbol{c})$ is of the form*

$$\{\boldsymbol{x} \in \mathbb{R}^{st} \mid A\boldsymbol{x} = \boldsymbol{b}, \boldsymbol{x} \geq 0\}$$

for some totally unimodular $(s + t) \times st$ matrix A and vector $\boldsymbol{b}$.

Proof. The row and column sum conditions defining $P(\mathbf{r}, \mathbf{c})$ can be given as

$$\sum_{j=1}^{t} x_{ij} = r_i, 1 \leq i \leq s, \qquad \sum_{i=1}^{s} x_{ij} = c_j, 1 \leq j \leq t.$$

These $s + t$ constraints can be written in matrix form as $A\mathbf{x} = \mathbf{b}$ where $\mathbf{x}$ is the column vector $(x_{11}, \ldots, x_{1t}, x_{21}, \ldots, x_{2t}, \ldots, x_{s1}, \ldots, x_{st})$ and $\mathbf{b} = (r_1, r_2, \ldots, r_s, c_1, c_2, \ldots, c_t)$.

The constraint matrix A is the vertex-edge incidence matrix of the complete bipartite graph $K_{s,t}$ ([5], page 3). Hence A is totally unimodular ([12], page 273). $\square$

Since $P(\mathbf{r}, \mathbf{c})$ is an $(s-1)(t-1)$-polytope, it can be projected onto $\mathbb{R}^{(s-1)(t-1)}$. Let the constraints

$$r_i - c_t \leq \sum_{j=1}^{t-1} x_{ij} \leq r_i, \;\; 1 \leq i \leq s-1,$$

$$c_j - r_s \leq \sum_{i=1}^{s-1} x_{ij} \leq c_j, \;\; 1 \leq j \leq t-1.$$

in matrix form be written as $A'\mathbf{x}' \leq \mathbf{b}'$ for some matrix A' and vector $\mathbf{b}'$. Then the polytope

$$P'(\mathbf{r}, \mathbf{c}) = \{\mathbf{x}' \in \mathbb{R}^{(s-1)(t-1)} \mid A'\mathbf{x}' \leq \mathbf{b}', \mathbf{x}' \geq 0\}$$

is the projection of $P(\mathbf{r}, \mathbf{c})$ onto $\mathbb{R}^{(s-1)(t-1)}$. Since each coordinate of $\mathbf{x}'$ is involved in a row and a column sum constraint, A' is totally unimodular by [12], page 274.

2.4 Counting integer points in polytopes of totally unimodular matrices

Proposition 2.4.1. *Let A be an $m \times n$ totally unimodular matrix and $P_k(A, \boldsymbol{b}) = \{\boldsymbol{x} \in \mathbb{R}^n \mid A\boldsymbol{x} \leq \boldsymbol{b}k, \boldsymbol{x} \geq 0\}$ be a polytope where $\boldsymbol{b}$ is an integer vector. Then the number of integer points in $P_k(A, \boldsymbol{b})$ is a polynomial in k of degree equal to $\dim(P_1(A, \boldsymbol{b}))$ and leading coefficient equal to the relative volume of $P_1(A, \boldsymbol{b})$.*

Proof. By Proposition 2.3.1, the polytope $P_1(A, \mathbf{b})$ has integer vertices. Also, $P_k(A, \mathbf{b}) = kP_1(A, \mathbf{b})$. Hence, the result follows by Ehrhart's theorem. $\square$

Lemma 2.4.2. *Let A be an $m \times n$ totally unimodular matrix and a_{ij} be the entry in the ith row and jth column of A. Choose i, j such that $a_{ij} \neq 0$. Perform the following row operations on A sequentially.*
(1) For $t \neq i$, $R_t \to R_t - a_{tj}a_{ij}^{-1}R_i$.
(2) $R_i \to a_{ij}^{-1}R_i$.
(3) $a_{ij} \to 0$.

Then the resulting matrix is totally unimodular.

Proof. Without loss of generality, assume $i = 1$, $j = 1$ and $a_{11} = 1$. First we will show that A remains totally unimodular under the operations (1). Suppose A' is the matrix obtained after performing (1) on A. Let $I \subset \{1, 2, \ldots, m\}$ and $J \subset \{1, 2, \ldots, n\}$ of cardinality r where $1 \leq r \leq \min(m, n)$. Let A_{IJ} denotes the submatrix of A that corresponds to the rows with index in I and columns with index in J. We need to show that $\det(A'_{IJ})$ is $1, -1$ or 0.

Case 1: If $1 \in I$, $\det(A'_{IJ}) = \det(A_{IJ}) = 1, -1$ or 0, since A is totally unimodular and the determinant remains unchanged under a row operation.

Case 2: If $1 \notin I$, $1 \in J$, $\det(A'_{IJ}) = 0$ since the first column of A'_{IJ} is 0.

Case 3: $1 \notin I$, $1 \notin J$, let $\tilde{I} = I \cup \{1\}$ and $\tilde{J} = J \cup \{1\}$. Then $\det(A'_{IJ}) = \det(A'_{\tilde{I}\tilde{J}})$. By Case 1 $\det(A'_{\tilde{I}\tilde{J}})$ is 1, -1 or 0.

It is known that under row operation (2) a matrix remains totally unimodular ([12], page 280, (iii)). Note that the operation (1) takes A to A' such that the first column entries of A' are 0 except a'_{11} (since $a_{t1} \to a_{t1} - a_{11}^2 a_{t1} = 0$). Any submatrix of a totally unimodular matrix is totally unimodular. Hence A' remains totally unimodular under the row operation (3). $\square$

Theorem 2.4.3. *Let A be an $m \times n$ totally unimodular matrix and $P_k(A, \boldsymbol{b}, \boldsymbol{c}) = \{\boldsymbol{x} \in \mathbb{R}^n \mid A\boldsymbol{x} \leq \boldsymbol{b}k + \boldsymbol{c}, \boldsymbol{x} \geq 0\}$ be a polytope where $\boldsymbol{b}$ and $\boldsymbol{c}$ are integer vectors. Then for $k \gg 0$, the number of integer points in $P_k(A, \boldsymbol{b}, \boldsymbol{c})$ is a polynomial in k. If $\dim(P_1(A, \boldsymbol{b}, \boldsymbol{0}))$ is equal to n, then the degree of the polynomial equals $\dim(P_1(A, \boldsymbol{b}, \boldsymbol{0}))$ and the leading coefficient equals the volume of $P_1(A, \boldsymbol{b}, \boldsymbol{0})$.*

Proof. Let $P_k(A, b, c)$ be the polytope defined by the system of m linear inequalities

$$\begin{array}{ccccccccc} a_{11}x_1 & + & a_{12}x_2 & + & \dots & + & a_{1n}x_n & \leq & b_1k + c_1 \\ a_{21}x_1 & + & a_{22}x_2 & + & \dots & + & a_{2n}x_n & \leq & b_2k + c_2 \\ \vdots & & \vdots & & \dots & & \vdots & & \vdots \\ a_{m1}x_1 & + & a_{m2}x_2 & + & \dots & + & a_{mn}x_n & \leq & b_mk + c_m \end{array} \tag{2.2}$$

which is written in short as $A\mathbf{x} \leq \mathbf{b}k + \mathbf{c}$. We will proceed by induction on the number of variables n. Let $n = 1$, the polytope is defined as

$$\{x_1 \in \mathbb{R} \mid a_{i1}x_1 \leq (b_ik + c_i), 1 \leq i \leq m, \quad x_1 \geq 0\}.$$

Let I be the set of indices i for which $a_{i1} = 1$ and J be $\{0\}\cup$ the set of indices j for which $a_{j1} = -1$. Put $b_0 = c_0 = 0$, and switch the signs of b_js and c_js for $j \in J$. Then the polytope can be given by

$$\{x_1 \in \mathbb{R} \mid x_1 \leq (b_ik + c_i), \ \ x_1 \geq (b_jk + c_j), i \in I, j \in J\}.$$

We assume that $b_j \leq b_i$ for all i, j, since otherwise the polytope is eventually empty.

Let $B^- = \max(b_j : j \in J)$, and $B^+ = \min(b_i : i \in I)$. Further, let $C^- = \max(c_j : b_j = B^-)$ and $C^+ = \min(c_i : b_i = B^+)$.

Then for $k \gg 0$, we have

$$L_P(k) = \#\{x \in \mathbb{Z} : B^-k + C^- \leq x \leq B^+k + C^+\} = (B^+ - B^-)k + (C^+ - C^-) + 1.$$

Thus the theorem holds true for $n = 1$.

If all c_is are 0, it reduces to the Ehrhart's theorem and the result follows by Proposition 2.4.1. So without loss of generality assume $c_1 > 0$. The integer solutions of the system (2.1) can be split as integer solutions of

$$\begin{array}{ccccccccc} a_{11}x_1 & + & a_{12}x_2 & + & \dots & + & a_{1n}x_n & \leq & b_1k \\ a_{21}x_1 & + & a_{22}x_2 & + & \dots & + & a_{2n}x_n & \leq & b_2k + c_2 \\ \vdots & & \vdots & & \dots & & \vdots & & \vdots \\ a_{m1}x_1 & + & a_{m2}x_2 & + & \dots & + & a_{mn}x_n & \leq & b_mk + c_m. \end{array} \tag{2.3}$$

and integer solutions of

$$\begin{array}{ccccccccc} a_{11}x_1 & + & a_{12}x_2 & + & \ldots & + & a_{1n}x_n & = & b_1k+j \\ a_{21}x_1 & + & a_{22}x_2 & + & \ldots & + & a_{2n}x_n & \leq & b_2k+c_2 \\ \vdots & & \vdots & & \ldots & & \vdots & & \vdots \\ a_{m1}x_1 & + & a_{m2}x_2 & + & \ldots & + & a_{mn}x_n & \leq & b_mk+c_m. \end{array} \tag{2.4}$$

for $j = 1, 2 \ldots, c_1$.

Let $L_P(k)$ denote the number of integer points in the polytope P. Write $P_k(A, \mathbf{b}, \mathbf{c})$ as P for brevity. Let P_1 and P_{1j} be the regions defined by the systems (2.3) and (2.4) respectively. Since P is a polytope, it is bounded. The regions P_1 and P_{1j} are subsets of the polytope P, hence they are also bounded and are polytopes. Then we have

$$L_P(k) = L_{P_1}(k) + \sum_{j=1}^{c_1} L_{P_{1j}}(k).$$

The polytopes P_{1j} can be projected to an $n-1$ dimensional space as follows.

Let $f_1(x) = a_{11}x_1 + \ldots + a_{1n}x_n$. If all the coefficients a_{1r} are zero, we can safely ignore the 1st inequality from the set of inequalities (2.2) describing the polytope P, since this only gives a bound on k. Thus assume that $a_{11} \neq 0$. Then we get

$$x_1 = a_{11}^{-1}(b_1k + j - \sum_{k \neq 1} a_{1k}x_k).$$

We eliminate the variable x_1 from (2.4) by substituting this equation to get

$$\begin{array}{ccccccc} & a_{11}^{-1}(a_{12}x_2 & + & \ldots & +a_{1n}x_n &) & \leq a_{11}^{-1}(b_1k+j) \\ a_{21}a_{11}^{-1}(b_1k + j - \sum_{k \neq 1} a_{1k}x_k) & + & a_{22}x_2 & + & \ldots & + & a_{2n}x_n \leq b_2k+c_2 \\ \vdots & & \vdots & & \ldots & \vdots & \vdots \\ a_{m1}a_{11}^{-1}(b_1k + j - \sum_{k \neq 1} a_{1k}x_k) & + & a_{m2}x_2 & + & \ldots & + & a_{mn}x_n \leq b_mk+c_m. \end{array} \tag{2.5}$$

for $j = 1, 2 \ldots, c_1$.

These m inequalities can be written as $A'\mathbf{x}' \leq \mathbf{b}'k + \mathbf{c}'$ where $\mathbf{x}' = (x_2, \ldots, x_n)$. There is a bijection between the non-negative integer solutions of (2.4) and (2.5). Hence it is enough to show that A' is totally unimodular. This follows from Lemma 2.4.2. Hence by induction $L_{P_{1j}}(k)$ is a polynomial for $k \gg 0$.

Now assume $c_2 > 0$ and repeat the same splitting process on P_1 to get $L_{P_1}(k)$ as the number of integer solutions of

$$\begin{array}{ccccccccc} a_{11}x_1 & + & a_{12}x_2 & + & \dots & + & a_{1n}x_n & \leq & b_1 k \\ a_{21}x_1 & + & a_{22}x_2 & + & \dots & + & a_{2n}x_n & \leq & b_2 k \\ a_{31}x_1 & + & a_{32}x_2 & + & \dots & + & a_{3n}x_n & \leq & b_3 k + c_3 \\ \vdots & & \vdots & & \dots & & \vdots & & \vdots \\ a_{m1}x_1 & + & a_{m2}x_2 & + & \dots & + & a_{mn}x_n & \leq & b_m k + c_m. \end{array} \tag{2.6}$$

and the integer solutions of

$$\begin{array}{ccccccccc} a_{11}x_1 & + & a_{12}x_2 & + & \dots & + & a_{1n}x_n & \leq & b_1 k \\ a_{21}x_1 & + & a_{22}x_2 & + & \dots & + & a_{2n}x_n & = & b_2 k + j \\ a_{31}x_1 & + & a_{32}x_2 & + & \dots & + & a_{3n}x_n & \leq & b_3 k + c_3 \\ \vdots & & \vdots & & \dots & & \vdots & & \vdots \\ a_{m1}x_1 & + & a_{m2}x_2 & + & \dots & + & a_{mn}x_n & \leq & b_m k + c_m. \end{array} \tag{2.7}$$

for $j = 1, 2 \dots, c_2$. So we have

$$L_{P_1}(k) = L_{P_2}(k) + \sum_{j=1}^{c_2} L_{P_{2j}}(k)$$

where P_2 is the polytope defined by (2.6) and P_{2j} by (2.7). By repeating this process we get

$$L_P(k) = L_{P_m}(k) + \sum_{i=1}^{m} \sum_{j=1}^{c_i} L_{P_{ij}}(k)$$

where $L_{P_m}(k)$ is a k-dilated polytope since all c_is are zero in the inequalities defining P_m. $L_{P_m}(k)$ is a polynomial in k of degree $\dim(P_1(A, \mathbf{b}, \mathbf{0}))$ and leading coefficient volume of $P_1(A, \mathbf{b}, \mathbf{0})$ by Ehrhart's theorem and $L_{P_{ij}}$s are polynomials for $k \gg 0$ by the arguments given above. Hence $L_P(k)$ is a polynomial for $k \gg 0$.

The dimension of a polytope can be no greater than the number of variables used to define it. Hence degrees of $L_{P_{ij}}(k)$s are less than n. So if $\dim(P_1(A, \mathbf{b}, \mathbf{0}))$ is equal to n, then the degree of the polynomial $L_P(k)$ equals n and the leading coefficient equals the volume of $P_1(A, \mathbf{b}, \mathbf{0})$. $\square$

2.4.1 Counting integer points in transportation polytopes

Write $M_{\mathbf{r},\mathbf{c}}$ for the number of non-negative integer points in the transportation polytope $P(\mathbf{r}, \mathbf{c})$, for margins $\mathbf{r}$ and $\mathbf{c}$.

Lemma 2.4.4. *Let $\boldsymbol{r}_k = (p_i k + a_i \mid 1 \leq i \leq s)$ and $\boldsymbol{c}_k = (q_j k + b_j \mid 1 \leq j \leq t)$ where $\sum p_i = \sum q_j$ and $\sum a_i = \sum b_j$ for $p_i, q_j, a_i, b_j \in \mathbb{Z}$. Then for $k \gg 0$, $M_{\boldsymbol{r}_k,\boldsymbol{c}_k}$ is a polynomial in k of degree equal to $(s-1)(t-1)$ and leading coefficient $V(\boldsymbol{p}, \boldsymbol{q})$, the relative volume of the transportation polytope $P(\boldsymbol{p}, \boldsymbol{q})$.*

Proof. The non-negative integer points in $P(\mathbf{r}_k, \mathbf{c}_k)$ are in bijection with the non-negative integer points in its projection onto $\mathbb{R}^{(s-1)(t-1)}$, $P'(\mathbf{r}_k, \mathbf{c}_k)$ defined as solutions of $A'\mathbf{x} \leq \mathbf{b}'k + \mathbf{c}'$ for some totally unimodular matrix A' and vectors $\mathbf{b}'$ and $\mathbf{c}'$ as explained after Proposition 2.3.4. Hence the result follows by Theorem 2.4.3. $\square$

Chapter 3

Chinese Remainder Theorem for Partitions

Analogous to the Chinese remainder theorem map for numbers $\mathbb{Z}/st\mathbb{Z} \to \mathbb{Z}/s\mathbb{Z} \times \mathbb{Z}/t\mathbb{Z}$, we define a map $\mathrm{core}_{s,t} : C_{st} \to C_s \times C_t$ taking an st-core to its s-core and t-core. The fibres of of this map are infinite, but we stratify them by length to get finite sets. In this Chapter, we study the asymptotic growth of these finite strata.

We will see that enumerating fibres of $\mathrm{core}_{s,t}$ of given length is equivalent to counting non-negative integer matrices with prescribed row sum and column sum. Then we use the theory of polytopes developed in Chapter 2 to understand the asymptotics of the cardinality of fibres.

3.1 Co-prime case

Recall from Section 1.2.2 that there are bijections $\mathscr{A}_n : C_n^k \to \left(\!\binom{\mathbb{Z}/n\mathbb{Z}}{k}\!\right)$ for every integer n. Define

$$\mathscr{S}_{s,t} : \left(\!\binom{\mathbb{Z}/st\mathbb{Z}}{k}\!\right) \to \left(\!\binom{\mathbb{Z}/s\mathbb{Z}}{k}\!\right) \times \left(\!\binom{\mathbb{Z}/t\mathbb{Z}}{k}\!\right)$$

as $\mathscr{S}_{s,t}(F) = (\mathscr{S}_s(F), \mathscr{S}_t(F))$, where $\mathscr{S}_s$ and $\mathscr{S}_t$ are as in Section 1.2.2, we have the commutative diagram

$$
\begin{tikzcd}
C^k_{st} \arrow[r, "core_{s,t}"] \arrow[d] & C^k_s \times C^k_t \arrow[d] \\
\left(\!\binom{\mathbb{Z}/st\mathbb{Z}}{k}\!\right) \arrow[r, "\mathscr{S}_{s,t}"] & \left(\!\binom{\mathbb{Z}/s\mathbb{Z}}{k}\!\right) \times \left(\!\binom{\mathbb{Z}/t\mathbb{Z}}{k}\!\right)
\end{tikzcd}
\tag{3.1}
$$

3.1.1 Existence

In this section, we prove the surjectivity of the map $\text{core}_{s,t}$ when s and t are co-prime. We use the notation $\lambda_1 \equiv \lambda_2 \mod s$ for $\text{core}_s(\lambda_1) = \text{core}_s(\lambda_2)$.

Theorem 3.1.1. *Given s, t such that $\gcd(s,t) = 1$, an s-core σ and a t-core τ, there exists a st-core λ such that*

$$
\begin{aligned}
\lambda &\equiv \sigma \mod s, \\
\lambda &\equiv \tau \mod t.
\end{aligned}
$$

Proof. It is enough to prove the surjectivity of the map $\mathscr{S}_{s,t}$. Given $(F_s, F_t) \in \left(\!\binom{\mathbb{Z}/s\mathbb{Z}}{k}\!\right) \times \left(\!\binom{\mathbb{Z}/t\mathbb{Z}}{k}\!\right)$ where $k \in \mathbb{N}$ is the cardinality of F_s and F_t, we will construct $F \in \left(\!\binom{\mathbb{Z}/st\mathbb{Z}}{k}\!\right)$ such that $\mathscr{S}_{s,t}(F) = (F_s, F_t)$.

Let $F_s = \{f_{s1}, f_{s2}, \ldots, f_{sk}\}$ and $F_t = \{f_{t1}, f_{t2}, \ldots, f_{tk}\}$. Then define F as,

$$
F = \{f_1, f_2, \ldots, f_k\}
$$

where f_i is the unique solution modulo st to the congruences $x_i \equiv f_{si} \mod s$ and $x_i \equiv f_{ti} \mod t$, which exists by the Chinese remainder theorem. Then $\mathscr{S}_{s,t}(F) = (F_s, F_t)$. $\square$

The proof of Theorem 3.1.1 gives an algorithm to find an element in each fibre of $\text{core}_{s,t}$.

Example 7. Let $s = 2$, $\sigma = (3,2,1)$ and $t = 3$, $\tau = (1,1)$.

Then $H(\sigma) = \{5,3,1\}$ and $H(\tau) = \{2,1\}$. We need beta sets of equal length to apply the construction as in the proof of Theorem 3.1.1. So we consider $H^3_\sigma = \{5,3,1\}$ and $H^3_\tau = \{3,2,0\}$.

Let $F_s = H^3_{\sigma,2} = \{1,1,1\}$ and $F_t = H^3_{\tau,3} = \{0,2,0\}$.

Now to find F such that $\mathscr{S}_{s,t}(F) = (F_s, F_t)$ we solve the following congruences

$$\begin{aligned} x_1 &\equiv 1 \mod 2,\ x_1 \equiv 0 \mod 3 \\ x_2 &\equiv 1 \mod 2,\ x_2 \equiv 2 \mod 3 \\ x_3 &\equiv 1 \mod 2,\ x_3 \equiv 0 \mod 3 \end{aligned}$$

and get the unique solution modulo 6 as $F = \{3,5,3\}$. The 6-abacus display of F is

$$\begin{array}{cccccc} \bar{0} & \bar{1} & \bar{2} & \bar{3} & \bar{4} & \bar{5} \\ \hline \circ & \circ & \circ & \bullet & \circ & \bullet \\ \circ & \circ & \circ & \bullet & \circ & \circ \end{array}$$

Hence, $H(\lambda) = \{9,5,3\}$ and $\lambda = (7,4,3)$.

3.1.2 Counting fibres

For $\sigma \in C_s$, $\tau \in C_t$ and $k \in \mathbb{N}$ let

$$N_{\sigma,\tau}(k) = \#\{\lambda \in C_{st} \mid \mathrm{core}_s(\lambda) = \sigma, \mathrm{core}_t(\lambda) = \tau, \ell(\lambda) \le k\}.$$

In other words, $N_{\sigma,\tau}(k)$ is the cardinality of the fibre of $\mathrm{core}_{s,t} : C^k_{st} \to C^k_s \times C^k_t$ over (σ,τ). By the commutative diagram (3.1), $N_{\sigma,\tau}(k)$ can also be thought of as the cardinality of the fibre of $\mathscr{S}_{s,t}$ over $(H^k_{\sigma,s}, H^k_{\tau,t})$.

Counting fibres of $(\emptyset,\emptyset)$ with $s=2$ and $t=3$

We first look at an example where $\sigma = \emptyset$ is a 2-core and $\tau = \emptyset$ is a 3-core. We will show that for $k \gg 0$, $N_{\emptyset,\emptyset}(k)$ is a quasi-polynomial of degree 2 and quasi-period 6.

It is trivial that $N_{\emptyset,\emptyset}(1) = 1$, since the only 6-core of length no greater than 1 in the fibre is the empty partition itself.

To find 6-core solutions of length no greater than 2, we consider the 2 and 3 abacus displays of the length 2 beta set of the empty partition, $H^2_\emptyset = \{1, 0\}$.

$$\begin{array}{cc} \overline{0} & \overline{1} \\ \hline \bullet & \bullet \\ \circ & \circ \end{array} \qquad\qquad \begin{array}{ccc} \overline{0} & \overline{1} & \overline{2} \\ \hline \bullet & \bullet & \circ \\ \circ & \circ & \circ \end{array}$$

Therefore $H^2_{\emptyset,2} = \{0, 1\}$ and $H^2_{\emptyset,3} = \{0, 1\}$.

Given a partition λ we find its s-core by displaying its beta set on an s-abacus and moving the beads to their highest possible position. So to get back the beta set of a partition from the abacus display of its core we have to move the beads down. Therefore to find the beta set of a 6-core of length no greater than two whose 2-core and 3-core abacus displays are as given in the figure above, we have to find a bead configuration that can be attained on both abaci by moving the beads down on the runners. This can be done by solving the system of congruences

$$\begin{aligned} x_1 &\equiv 0 \mod 2,\ x_1 \equiv 0 \mod 3 \\ x_2 &\equiv 1 \mod 2,\ x_2 \equiv 1 \mod 3. \end{aligned}$$

This gives the beta set of a 6-core solution as $H^2_{\lambda_1,6} = \{1, 0\} \rightsquigarrow \lambda_1 = \emptyset$.

To get another solution we consider another set of congruences obtained by matching the elements of$H^2_{\emptyset,2}$ and $H^2_{\emptyset,3}$ in a different way.

$$\begin{aligned} x_1 &\equiv 0 \mod 2,\ x_1 \equiv 1 \mod 3 \\ x_2 &\equiv 1 \mod 2,\ x_2 \equiv 0 \mod 3 \end{aligned}$$

Hence the beta set of another solution is $H^2_{\lambda_2,6} = \{4, 3\} \rightsquigarrow \lambda_2 = (3, 3)$.

Here we observe that the number of solutions of length 2 is equal to the number of distinct matchings between the multisets $H^2_{\emptyset,2}$ and $H^2_{\emptyset,3}$. Therefore we come to a conclusion that $N_{\emptyset,\emptyset}(k)$ is equal to the number of distinct matchings between the multisets $H^k_{\emptyset,2}$ and $H^k_{\emptyset,3}$. Now consider 2×3 matrices whose (i, j)th entry a_{ij} is defined as the number of i's in $H^k_{\emptyset,2}$ matched with the number of j's in $H^k_{\emptyset,3}$. The number of distinct matchings between the multisets $H^2_{\emptyset,2}$ and $H^2_{\emptyset,3}$ is equal to the number of such matrices.

The length $6k, 6k+1, 6k+2, \ldots, 6k+5$ beta sets of the empty set modulo 2 and 3 are

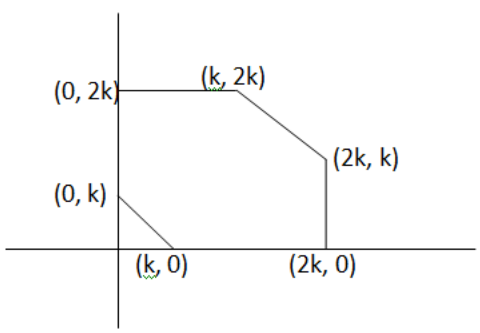
$$\begin{aligned}
H_{\emptyset,2}^{6k} &= \{0^{3k}, 1^{3k}\} & H_{\emptyset,3}^{6k} &= \{0^{2k}, 1^{2k}, 2^{2k}\} \\
H_{\emptyset,2}^{6k+1} &= \{0^{3k+1}, 1^{3k}\} & H_{\emptyset,3}^{6k+1} &= \{0^{2k+1}, 1^{2k}, 2^{2k}\} \\
H_{\emptyset,2}^{6k+2} &= \{0^{3k+1}, 1^{3k+1}\} & H_{\emptyset,3}^{6k+2} &= \{0^{2k+1}, 1^{2k+1}, 2^{2k}\} \\
H_{\emptyset,2}^{6k+3} &= \{0^{3k+2}, 1^{3k+1}\} & H_{\emptyset,3}^{6k+3} &= \{0^{2k+1}, 1^{2k+1}, 2^{2k+1}\} \\
H_{\emptyset,2}^{6k+4} &= \{0^{3k+2}, 1^{3k+2}\} & H_{\emptyset,3}^{6k+4} &= \{0^{2k+2}, 1^{2k+1}, 2^{2k+1}\} \\
H_{\emptyset,2}^{6k+5} &= \{0^{3k+3}, 1^{3k+2}\} & H_{\emptyset,3}^{6k+5} &= \{0^{2k+2}, 1^{2k+2}, 2^{2k+1}\}
\end{aligned}$$

Let $r_{ik} = (H_{\emptyset,2}^{6k+i}(r) \mid r = 0,1)$ and $c_{ik} = (H_{\emptyset,3}^{6k+i}(c) \mid c = 0,1,2)$. Then $N_{\emptyset,\emptyset}(6k+i) = M_{r_{ik},c_{ik}}$.

For example $r_{0k} = (3k, 3k)$ and $c_{0k} = (2k, 2k, 2k)$. $N_{\emptyset,\emptyset}(6k)$ equals the number of 2×3 integer matrices with row sum r_{0k} and column sum c_{0k}. Now we count this as integer points in the transportation polytope for margins r_{0k} and c_{0k}.

Let $A = \begin{bmatrix} x & y & z \\ a & b & c \end{bmatrix}$, the transportation polytope for margins r_{0k} and c_{0k} can be defined as follows.

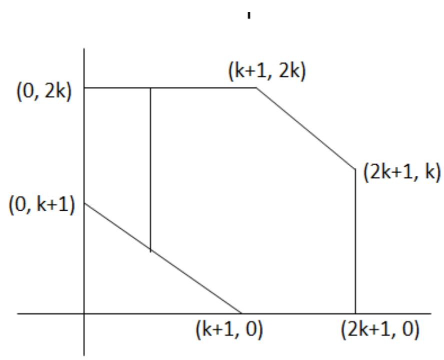
$$\begin{gathered}
k \leq x + y \leq 3k \\
0 \leq x \leq 2k \\
0 \leq y \leq 2k
\end{gathered}$$



By Ehrhart's theorem, $M_{r_{0k},c_{0k}} = 3k^2 + 3k + 1$.

Now for $r_{1k} = (3k+1, 3k)$ and $c_{1k} = (2k+1, 2k, 2k)$, the transportation polytope is defined as

$$\begin{gathered} k+1 \leq x+y \leq 3k+1 \\ 0 \leq x \leq 2k+1 \\ 0 \leq y \leq 2k \end{gathered}$$



Here we can see that coordinates are of the form $ak+b$, hence we apply the variant of Ehrhart's theorem from Lemma 2.4.4 to get $M_{r_{1k},c_{1k}} = 3k^2+4k+1$.

Similarly we get $M_{r_{2k},c_{2k}} = 3k^2+5k+2$, $M_{r_{3k},c_{3k}} = 3k^2+6k+3$, $M_{r_{4k},c_{4k}} = 3k^2+7k+4$, $M_{r_{5k},c_{5k}} = 3k^2+8k+5$. Hence $N_{\emptyset,\emptyset}(k)$ is a quasi-polynomial of degree 2 and quasi-period 6.

Therefore, for $s=2$, $t=3$,

$$N_{\emptyset,\emptyset}(n) = \begin{cases} 3k^2+3k+1, & \text{if } n = 6k \\ 3k^2+4k+1, & \text{if } n = 6k+1 \\ 3k^2+5k+2, & \text{if } n = 6k+2 \\ 3k^2+6k+3, & \text{if } n = 6k+3 \\ 3k^2+7k+4, & \text{if } n = 6k+4 \\ 3k^2+8k+5, & \text{if } n = 6k+5 \end{cases} \tag{3.2}$$

Now we prove the general case using the ideas from this example.

Lemma 3.1.2. *Suppose* $\gcd(s,t)=1$ *and let* $\ell_0=\max\{\ell(\sigma),\ell(\tau)\}$. *We have*

$$N_{\sigma,\tau}(k)=\begin{cases}0 & \text{if } k<\ell_0\\ M_{\boldsymbol{r}_k,\boldsymbol{c}_k} & \text{if } k\geq \ell_0\end{cases}$$

where $\boldsymbol{r}_k=(H^k_{\sigma,s}(r)\mid 0\leq r\leq s-1)$ *and* $\boldsymbol{c}_k=(H^k_{\tau,t}(c)\mid 0\leq c\leq t-1)$.

Proof. The s-core of a partition is obtained by removing s-hooks. Hence the length of $\mathrm{core}_s\lambda$ is definitely no greater than the length of λ itself. So $N_{\sigma,\tau}(k)=0$ for $k<\ell_0$.

For $k\geq\ell_0$, $N_{\sigma,\tau}(k)$ is the number of distinct matchings between the multisets $H^k_{\sigma,s}$ and $H^k_{\tau,t}$. This is equal to the number of non-negative integer matrices with row sum $\mathbf{r}_k=(H^k_{\sigma,s}(r)\mid 0\leq r\leq s-1)$ and column sum $\mathbf{c}_k=(H^k_{\tau,t}(c)\mid 0\leq c\leq t-1)$. □

Write $V(\mathbf{s},\mathbf{t})$ for the relative volume of the transportation polytope for row margins $(\underbrace{s,\dots,s}_{t\text{ times}})$ and column margins $(\underbrace{t,\dots,t}_{s\text{ times}})$. Finding the volume of a transportation polytope is a hard problem. The volume of a special kind of transportation polytope of $n\times n$ doubly stochastic matrices with margins $(1,\dots,1)$ has been much studied [6].

Theorem 3.1.3. *For* $k\gg 0$, $N_{\sigma,\tau}(k)$ *is a quasi-polynomial of degree* $(s-1)(t-1)$ *and quasi-period* st, *with leading coefficient* $V(\boldsymbol{s},\boldsymbol{t})$.

Proof. By Lemma 3.1.2, for $i\geq\ell_0$, $N_{\sigma,\tau}(i+stk)$ is the number of matrices whose margins are $(H^{i+stk}_{\sigma,s}(r)\mid 0\leq r\leq s-1)$ and $(H^{i+stk}_{\tau,t}(c)\mid 0\leq c\leq t-1)$.

For $i\geq\ell_0$, by Lemma 1.2.1 the margins satisfy the property,

$$(H^{i+stk}_{\sigma,s}(r)\mid 0\leq r\leq s-1)=(H^{i}_{\sigma,s}(r)+tk\mid 0\leq r\leq s-1),$$

$$(H^{i+stk}_{\tau,t}(c)\mid 0\leq c\leq t-1)=(H^{i}_{\tau,t}(c)+sk\mid 0\leq c\leq t-1).$$

Hence, for a fixed i the margins are of the form $(tk+a_0,tk+a_1,\dots,tk+a_{s-1})$ and $(sk+b_0,sk+b_1,\dots,sk+b_{t-1})$. By applying Lemma 2.4.4, we get that for each i such that $\ell_0\leq i\leq\ell_0+st-1$, $N_{\sigma,\tau}(i+stk)$ is a polynomial in k for $k\gg 0$ of degree $(s-1)(t-1)$ with leading coefficient $V(\mathbf{s},\mathbf{t})$. □

3.2 Non-coprime case

For $s, t \in \mathbb{N}$ such that $\gcd(s,t) = d$ and $\mathrm{lcm}(s,t) = m$, consider the map

$$\mathrm{core}_{s,t} : C_m \to C_s \times C_t.$$

Given the map $\mathscr{S}_{s,t} : \left(\!\binom{\mathbb{Z}/m\mathbb{Z}}{k}\!\right) \to \left(\!\binom{\mathbb{Z}/s\mathbb{Z}}{k}\!\right) \times \left(\!\binom{\mathbb{Z}/t\mathbb{Z}}{k}\!\right)$ defined as $\mathscr{S}_{s,t}(F) = (\mathscr{S}_s(F), \mathscr{S}_t(F))$, where $\mathscr{S}_s$ and $\mathscr{S}_t$ are as in Section 1.2.2, we have the commutative diagram

$$\begin{tikzcd} C_m^k \arrow[r, "core_{s,t}"] \arrow[d] & C_s^k \times C_t^k \arrow[d] \\ \left(\!\binom{\mathbb{Z}/m\mathbb{Z}}{k}\!\right) \arrow[r, "\mathscr{S}_{s,t}"] & \left(\!\binom{\mathbb{Z}/s\mathbb{Z}}{k}\!\right) \times \left(\!\binom{\mathbb{Z}/t\mathbb{Z}}{k}\!\right) \end{tikzcd} \tag{3.3}$$

3.2.1 Existence

Given s, t such that $\gcd(s,t) = d$, $\mathrm{lcm}(s,t) = m$, an s-core σ and a t-core τ, there exists a m-core λ such that

$$\lambda \equiv \sigma \mod s,$$
$$\lambda \equiv \tau \mod t$$

if and only if $\sigma \equiv \tau \mod d$.

Proof. Suppose there exists an m-core λ such that $\mathrm{core}_s\lambda = \sigma$ and $\mathrm{core}_t\lambda = \tau$. By Proposition 1.1.2,

$$\mathrm{core}_d\mathrm{core}_s\lambda = \mathrm{core}_d\lambda,$$

$$\mathrm{core}_d\mathrm{core}_t\lambda = \mathrm{core}_d\lambda.$$

Hence $\mathrm{core}_d\sigma = \mathrm{core}_d\tau$.

Conversely, given $\sigma \in C_s$, $\tau \in C_t$ where $\mathrm{core}_d\sigma = \mathrm{core}_d\tau$, we will show that there exists $\lambda \in C_m$ such that $\mathrm{core}_s\lambda = \sigma$ and $\mathrm{core}_t\lambda = \tau$. It is enough to show that for $(F_s, F_t) \in \left(\!\binom{\mathbb{Z}/s\mathbb{Z}}{k}\!\right) \times \left(\!\binom{\mathbb{Z}/t\mathbb{Z}}{k}\!\right)$ where $\mathscr{S}_d(F_s) = \mathscr{S}_d(F_t)$, there exists an $F \in \left(\!\binom{\mathbb{Z}/m\mathbb{Z}}{k}\!\right)$ such that $\mathscr{S}_{s,t}(F) = (F_s, F_t)$.

As in co-prime case, we will construct F satisfying this property. Let $F_s = \{f_{s1}, f_{s2}, \dots, f_{sk}\}$ and $F_t = \{f_{t1}, f_{t2}, \dots, f_{tk}\}$. Let

$$\mathscr{S}_d(F_s) = \{f_{sdi} \mid f_{sdi} = f_{si} \mod d, 1 \le i \le k\}$$

and

$$\mathscr{S}_d(F_t) = \{f_{tdi} \mid f_{tdi} = f_{ti} \mod d, 1 \le i \le k\}.$$

Since $\mathscr{S}_d(F_s) = \mathscr{S}_d(F_t)$ we assume $f_{sdi} = f_{tdi}$ for $1 \le i \le k$. Then define

$$F = \{f_1, f_2, \dots, f_k\}$$

where f_i is the solution to the congruence $x_i \equiv f_{si} \mod s$ and $x_i \equiv f_{ti} \mod t$. By CRT we know that this solution exists and is unique modulo m, since $f_{si} \equiv f_{ti} \mod d$. By the definition of F, $\mathscr{S}_{s,t}(F) = (F_s, F_t)$. $\square$

3.2.2 Counting fibres

For $\sigma \in C_s$, $\tau \in C_t$ such that $\sigma \equiv \tau \mod d$ and $k \in \mathbb{N}$ let

$$N_{\sigma,\tau}(k) = \#\{\lambda \in C_m \mid \mathrm{core}_s(\lambda) = \sigma, \mathrm{core}_t(\lambda) = \tau, \ell(\lambda) \le k\}.$$

Then $N_{\sigma,\tau}(k)$ is the cardinality of the fibre of $\mathrm{core}_{s,t} : C_m^k \to C_s^k \times C_t^k$ over (σ, τ). By the commutative diagram (3.3), $N_{\sigma,\tau}(k)$ can also be thought of as the cardinality of the fibre of $\mathscr{S}_{s,t}$ over $(H^k_{\sigma,s}, H^k_{\tau,t})$.

Lemma 3.2.1. *Suppose* $\gcd(s,t) = d$, $\mathrm{lcm}(s,t) = m$ *and let* $\ell_0 = \max\{\ell(\sigma), \ell(\tau)\}$ *and* $\sigma \equiv \tau \mod d$. *We have*

$$N_{\sigma,\tau}(k) = \begin{cases} 0 & \text{if } k < \ell_0 \\ \prod_{j=0}^{d-1} M_{\boldsymbol{r}_{jk}, \boldsymbol{c}_{jk}} & \text{if } k \ge \ell_0 \end{cases}$$

where $\boldsymbol{r}_{jk} = (H^k_{\sigma,s}(j + ad) \mid 0 \le a \le \frac{s}{d} - 1)$ *and* $\boldsymbol{c}_{jk} = (H^k_{\tau,t}(j + bd) \mid 0 \le b \le \frac{t}{d} - 1)$.

Proof. It is obvious that for $k < \ell_0$, $N_{\sigma,\tau}(k) = 0$.

For $k \ge \ell_0$ we know that, $N_{\sigma,\tau}(k)$ is the cardinality of the fibre of $\mathscr{S}_{s,t}$ over $(H^k_{\sigma,s}, H^k_{\tau,t})$

where $\mathscr{S}_d(H^k_{\sigma,s}) = \mathscr{S}_d(H^k_{\tau,t})$. It is equal to the number of distinct matchings between the multisets $H^k_{\sigma,s}$ and $H^k_{\tau,t}$ with the condition that $f \in H^k_{\sigma,s}$ is matched with $g \in H^k_{\tau,t}$ if and only if $f \equiv g \mod d$.

So we split $H^k_{\sigma,s}$ and $H^k_{\tau,t}$ into d sets whose elements can be matched. Let $s = pd$ and $t = qd$. For $0 \leq j \leq d-1$ let,

$$H^k_{\sigma,s,j} = \{j + ad \in H^k_{\sigma,s} \mid 0 \leq a \leq p-1\},$$

$$H^k_{\tau,t,j} = \{j + bd \in H^k_{\tau,t} \mid 0 \leq b \leq q-1\}.$$

Note that, $H^k_{\sigma,s} = \bigcup_{j=0}^{d-1} H^k_{\sigma,s,j}$ and $H^k_{\tau,t} = \bigcup_{j=0}^{d-1} H^k_{\tau,t,j}$.

Hence the number of distinct matchings between the multisets $H^k_{\sigma,s}$ and $H^k_{\tau,t}$ with the restriction given is equal to the product of the number of distinct matchings between the multisets $H^k_{\sigma,s,j}$ and $H^k_{\tau,t,j}$.

As we have have seen earlier, the number of distinct matchings between the multisets $H^k_{\sigma,s,j}$ and $H^k_{\tau,t,j}$ is equal to $M_{\mathbf{r}_{jk},\mathbf{c}_{jk}}$ where $\mathbf{r}_{jk} = (H^k_{\sigma,s}(j+ad) \mid 0 \leq a \leq \frac{s}{d} - 1)$ and $\mathbf{c}_{jk} = (H^k_{\tau,t}(j+bd) \mid 0 \leq b \leq \frac{t}{d} - 1)$. Thus the result follows. □

Lemma 3.2.2. *Suppose* $\gcd(s,t) = d$, $\operatorname{lcm}(s,t) = m$ *and let* $\ell_0 = \max\{\ell(\sigma), \ell(\tau)\}$ *and* $\sigma \equiv \tau \mod d$. *Then for* $k \geq \ell_0$, *there exist* $\frac{s}{d}$ *cores* σ^k_j, $\frac{t}{d}$ *cores* τ^k_j, *and some integers* $\ell_j(k)$ *such that*

$$N_{\sigma,\tau}(k) = \prod_{j=0}^{d-1} N_{\sigma^k_j,\tau^k_j}(\ell_j(k)).$$

Proof. Let $s = pd$, $t = qd$, and let

$$\ell_j(k) = \sum_{a=0}^{p-1} H^k_{\sigma,s}(j+ad) = \sum_{b=0}^{q-1} H^k_{\tau,t}(j+bd).$$

We define σ^k_j by setting its length $\ell_j(k)$ beta set modulo p as,

$$H^{\ell_j(k)}_{\sigma^k_j,p} = \{a \mid j + ad \in H^k_{\sigma,s,j}\}$$

and define τ_j^k by setting its length $\ell_j(k)$ beta set modulo q as,

$$H^{\ell_j(k)}_{\tau_j^k,q} = \{b \mid j + bd \in H^k_{\tau,t,j}\}.$$

From previous Lemma we know that, for $k \geq \ell_0$

$$N_{\sigma,\tau}(k) = \prod_{j=0}^{d-1} M_{\mathbf{r}_{jk},\mathbf{c}_{jk}}$$

where $\mathbf{r}_{jk} = (H^k_{\sigma,s}(j + ad) \mid 0 \leq a \leq \frac{s}{d} - 1)$ and $\mathbf{c}_{jk} = (H^k_{\tau,t}(j + bd) \mid 0 \leq b \leq \frac{t}{d} - 1)$.

Now the result follows since $N_{\sigma_j^k,\tau_j^k}(\ell_j(k)) = M_{\mathbf{r}_{jk},\mathbf{c}_{jk}}$. $\square$

Example 8. $s = 6, \quad t = 9, \quad d = 3, \quad m = 18$

$$\sigma = (5,5,3,2,2) \qquad \tau = (8,8,6,2,2)$$

$$H(\sigma) = \{9,8,5,3,2\} \qquad H(\tau) = \{12,11,8,3,2\}$$

$$\begin{array}{cccccc} \overline{0} & \overline{1} & \overline{2} & \overline{3} & \overline{4} & \overline{5} \\ \hline \circ & \circ & \bullet & \bullet & \circ & \bullet \\ \circ & \circ & \bullet & \bullet & \circ & \circ \end{array} \qquad \begin{array}{ccccccccc} \overline{0} & \overline{1} & \overline{2} & \overline{3} & \overline{4} & \overline{5} & \overline{6} & \overline{7} & \overline{8} \\ \hline \circ & \circ & \bullet & \bullet & \circ & \circ & \circ & \circ & \bullet \\ \circ & \circ & \bullet & \bullet & \circ & \circ & \circ & \circ & \circ \end{array}$$

Now we display $H(\sigma)$ and $H(\tau)$ on the 2 abacus.

$$\begin{array}{ccc} \overline{0} & \overline{1} & \overline{2} \\ \hline \circ & \circ & \bullet \\ \bullet & \circ & \bullet \\ \circ & \circ & \bullet \\ \bullet & \circ & \circ \end{array} \qquad \begin{array}{ccc} \overline{0} & \overline{1} & \overline{2} \\ \hline \circ & \circ & \bullet \\ \bullet & \circ & \circ \\ \circ & \circ & \bullet \\ \circ & \circ & \bullet \\ \bullet & \circ & \circ \end{array}$$

From this we get

$$H^5_{\sigma,6,0} = \{3,3\} \qquad H^5_{\sigma,9,0} = \{3,3\}$$

$$H^5_{\sigma,6,1} = \emptyset \qquad H^5_{\sigma,9,1} = \emptyset$$

$$H^5_{\sigma,6,2} = \{2,2,5\} \qquad H^5_{\sigma,9,2} = \{2,2,8\}$$

We define the number of distinct matchings between the empty sets to be 1.

The number of distinct matchings between $H^5_{\sigma,6,0}$ and $H^5_{\sigma,9,0} = 1$.
The number of distinct matchings between $H^5_{\sigma,6,2}$ and $H^5_{\sigma,9,2} = 2$.
Therefore, $N_{\sigma,\tau}(5) = 2$. The 2 solutions can be obtained by solving the following system of congruences.

$$\begin{gathered}
x_1 \equiv 3 \mod 6 \text{ and } x_1 \equiv 3 \mod 9 \implies x_1 \equiv 3 \mod 18 \\
x_2 \equiv 3 \mod 6 \text{ and } x_2 \equiv 3 \mod 9 \implies x_1 \equiv 3 \mod 18 \\
z_1 \equiv 2 \mod 6 \text{ and } z_1 \equiv 2 \mod 9 \implies z_1 \equiv 2 \mod 18 \\
z_2 \equiv 2 \mod 6 \text{ and } z_2 \equiv 2 \mod 9 \implies z_2 \equiv 2 \mod 18 \\
z_3 \equiv 5 \mod 6 \text{ and } z_3 \equiv 8 \mod 9 \implies z_3 \equiv 17 \mod 18 \\
H(\lambda_1) = \{21, 20, 17, 3, 2\} \rightsquigarrow \lambda_1 = (17, 17, 15, 2, 2).
\end{gathered}$$

$$\begin{gathered}
x_1 \equiv 3 \mod 6 \text{ and } x_1 \equiv 3 \mod 9 \implies x_1 \equiv 3 \mod 18 \\
x_2 \equiv 3 \mod 6 \text{ and } x_2 \equiv 3 \mod 9 \implies x_1 \equiv 3 \mod 18 \\
z_1 \equiv 2 \mod 6 \text{ and } z_1 \equiv 2 \mod 9 \implies z_1 \equiv 2 \mod 18 \\
z_2 \equiv 2 \mod 6 \text{ and } z_2 \equiv 8 \mod 9 \implies z_2 \equiv 8 \mod 18 \\
z_3 \equiv 5 \mod 6 \text{ and } z_3 \equiv 2 \mod 9 \implies z_3 \equiv 11 \mod 18 \\
H(\lambda_2) = \{21, 11, 8, 3, 2\} \rightsquigarrow \lambda_2 = (17, 8, 6, 2, 2).
\end{gathered}$$

Write $V(\frac{\mathbf{s}}{\mathbf{d}}, \frac{\mathbf{t}}{\mathbf{d}})$ for the relative volume of the transportation polytope for row margins $(\underbrace{\frac{s}{d}, \ldots, \frac{s}{d}}_{\frac{t}{d} \text{ times}})$ and column margins $(\underbrace{\frac{t}{d}, \ldots, \frac{t}{d}}_{\frac{s}{d} \text{ times}})$.

Theorem 3.2.3. *For $k \gg 0$, $N_{\sigma,\tau}(k)$ is a quasi-polynomial of quasi-period $m = \operatorname{lcm}(s, t)$ and degree $\frac{1}{d}(s-d)(t-d)$, with leading coefficient $(V(\frac{\mathbf{s}}{\mathbf{d}}, \frac{\mathbf{t}}{\mathbf{d}}))^d$.*

Proof. Let $\frac{s}{d} = p$, $\frac{t}{d} = q$. By Lemma 3.2.1, for $i \geq \ell_0$, $N_{\sigma,\tau}(i + mk)$ is the product of the number of matrices whose margins are $(H^{i+mk}_{\sigma,s}(j + ad) \mid 0 \leq a \leq p-1)$ and $(H^{i+mk}_{\tau,t}(c) \mid 0 \leq c \leq q-1)$.

For $i \geq \ell_0$, by Lemma 1.2.1 the margins satisfy the property,

$$(H^{i+mk}_{\sigma,s}(j + ad) \mid 0 \leq a \leq p-1) = (H^{i}_{\sigma,s}(j + ad) + qk \mid 0 \leq r \leq p-1),$$

$$(H^{i+mk}_{\tau,t}(j + bd) \mid 0 \leq b \leq q-1) = (H^{i}_{\tau,t}(j + bd) + pk \mid 0 \leq b \leq q-1).$$

Hence, for a fixed i the margins are of the form $(qk + a_0, qk + a_1, \ldots, qk + a_{s-1})$ and $(pk + b_0, pk + b_1, \ldots, pk + b_{t-1})$. By applying Lemma 2.4.4, we get that for each i such that $\ell_0 \leq i \leq \ell_0 + m - 1$, $N_{\sigma,\tau}(i + mk)$ is a polynomial in k for $k \gg 0$ of degree $\frac{1}{d}(s-d)(t-d)$ with leading coefficient $(V(\frac{\mathbf{s}}{\mathbf{d}}, \frac{\mathbf{t}}{\mathbf{d}}))^d$. $\square$

Bibliography

[1] M. Beck and S. Robins. *Computing the continuous discretely.* Springer, 2007.

[2] R. Brualdi. *Introductory Combinatorics.* Pearson/Prentice Hall, 2010.

[3] R. A. Brualdi. *Combinatorial matrix classes*, volume 13. Cambridge University Press, 2006.

[4] E. R. Canfield and B. D. McKay. Asymptotic enumeration of integer matrices with constant row and column sums. *arXiv preprint math/0703600*, 2007.

[5] J. A. De Loera and E. D. Kim. Combinatorics and geometry of transportation polytopes: an update. *Discrete geometry and algebraic combinatorics*, 625:37–76, 2014.

[6] J. A. De Loera, F. Liu, and R. Yoshida. A generating function for all semi-magic squares and the volume of the birkhoff polytope. *Journal of Algebraic Combinatorics*, 30(1):113–139, 2009.

[7] G. Ewald. *Combinatorial convexity and algebraic geometry*, volume 168. Springer Science & Business Media, 2012.

[8] J. S. Frame, G. d. B. Robinson, and R. M. Thrall. The hook graphs of the symmetric group. *Canadian Journal of Mathematics*, 6:316–324, 1954.

[9] G. James and A. Kerber. *The Representation Theory of the Symmetric Group.* Encyclopedia of Mathematics and its Applications. Cambridge University Press, 1984.

[10] K. Ono et al. A note on the number of t-core partitions. *Rocky Mountain Journal of Mathematics*, 25:1165–1170, 1995.

[11] J. D. Sally. *Roots to research: a vertical development of mathematical problems.* American Mathematical Soc., 2007.

[12] A. Schrijver. *Theory of linear and integer programming.* John Wiley & Sons, 1998.

[13] R. Stanley. *Enumerative Combinatorics:.* Cambridge Studies in Advanced Mathematics. Cambridge University Press, 2012.

[14] J. J. Sylvester and F. Franklin. A constructive theory of partitions, arranged in three acts, an interact and an exodion. *American Journal of Mathematics*, 5(1):251–330, 1882.

[15] M. Wildon. Counting partitions on the abacus. *The Ramanujan Journal*, 17(3):355–367, 2008.

[16] H. Zhong. Bijections between t-core partitions and t-tuples. *arXiv preprint arXiv:1903.07772*, 2019.