SCHOOL OF OPERATIONS RESEARCH
AND INDUSTRIAL ENGINEERING
COLLEGE OF ENGINEERING
CORNELL UNIVERSITY
ITHACA, NY 14853-3801

TECHNICAL REPORT NO. 1025

August 1992

DISCRETE GEOMETRY, GROUP REPRESENTATIONS AND COMBINATORIAL OPTIMIZATION: AN INTERPLAY

by

Shmuel Onn[1]

[1]Research partially supported by NSF grants IRI-8710858, DMS-8706133, and DMS-8920550, and a Mathematical Sciences Institute Cornell Fellowship.

Table of Contents

1 Introduction **1**

1.1 Overview 2
1.2 Permutation polytopes 6
1.3 Modules from representations 8
1.4 Integral Radon partitions 10
1.5 Approximating oracle machines 11

2 Geometry, Complexity, and Combinatorics of Permutation Polytopes **12**

2.1 Introduction 12
2.2 Young representations and combinatorial optimization 16
2.3 On the graph of the assignment polytope 20
2.4 Neighborliness degree of Young polytopes 24
2.5 Orbit stratifications and a problem of Kozen 29
2.6 Discussion 33

3 Graded Modules and Hilbert Series of Group Representations **35**

3.1 Introduction 35
3.2 Preliminaries 38
3.3 The graded module of a linear representation 39
3.4 Generic modules and canonical decompositions 43
3.5 Initial modules and the Hilbert series of a linear representation . . . 47
3.6 Multiplicity-free representations 49
3.7 Determinantal ideals and Gröbner bases 51

4 On the Geometry and Computational Complexity of Radon Partitions in the Integer Lattice **53**

4.1 Introduction 53
4.2 A lower bound 56
4.3 An upper bound 57
4.4 Stable sets in polytopes 59
4.5 The two-dimensional case 64
4.6 Computational complexity aspects 66

4.7 Remaining questions 70

5 Approximating Oracle Machines for Combinatorial Optimization 72
5.1 Introduction 72
5.2 Approximating machines 73
5.3 Discussion 76

6 Further Questions 78

Bibliography 82

List of Figures

4.1 Five points in the plane 57
4.2 Bicycle wheel with 8 spokes 63
4.3 The hexagon lemma 65
4.4 The dodecahedron 71

is equipped with a basis $\{e_1, \cdots, e_d\}$, so the space V is identified with $\mathcal{K}^d$ and the linear transformations assigned to group elements are identified with the corresponding $d \times d$ matrices over $\mathcal{K}$, and will be often regarded simply as points in affine space $\mathcal{K}^{d \times d}$. The representation then becomes a *matrix representation.* We will often not distinguish between the group G and its image under the representation. Given a point $v \in \mathcal{K}^d$, its *orbit* is the set $Gv = \{gv : \ g \in G\} \subset \mathcal{K}^d$. We will be primarily concerned with the case in which $\mathcal{K}$ is an ordered field, typically one of the fields $\mathbb{R}$ and $\mathbb{Q}$ of real and rational numbers, respectively. In this situation the space is equipped with the usual convexity operator. We use $conv(S)$ to denote the convex hull of a subset $S \subset \mathcal{K}^d$.

The *representation polytope* is defined to be $conv(G) \subset \mathcal{K}^{d \times d}$. The *orbit polytope* of a point $v \in \mathcal{K}^d$ is the convex hull of its orbit $conv(Gv) \subset \mathcal{K}^d$. These are studied in Chapter 2 for representations of the symmetric group S_n. It is of great interest to consider the entire bundle $\{conv(Gv) : \ v \in \mathcal{K}^d\}$ of orbit polytopes and the stratification of the representation space $\mathcal{K}^d$ by the combinatorial type of the orbit polytopes. Such a study is within the realm of semialgebraic geometry, and oriented matroids provide a suitable framework for our investigation.

The consideration of sequences of representations $\pi_n : G_n \longrightarrow GL(\mathcal{K}^{d(n)})$ gives rise to asymptotic and computational questions. One can then ask, for example, for the $\mathcal{K}$-dimension of the span of $\pi_n(G_n)$ in $\mathcal{K}^{d(n) \times d(n)}$ as a function of n, and whether it is a polynomial time computable function. This question will be touched upon in Chapter 6, while other asymptotic questions are discussed in Chapter 2.

The general problem of *combinatorial optimization* is that of maximizing a rational linear functional $v \in \mathbb{Q}^n$ - the dual space $(\mathbb{Q}^n)^*$ is identified with $\mathbb{Q}^n$ via the standard inner product - over a given set $S \subseteq \{0,1\}^n \subset \mathbb{Q}^n$. More restrictively, the *combinatorial optimization problem over a language* $L \subseteq \{0,1\}^* = \cup_{n \geq 0} \{0,1\}^n$ is that of maximizing $v \in \mathbb{Q}^n$ over $L_n = L \cap \{0,1\}^n$. The input for an algorithm for this problem consists of n and v only, and the number of bits $n + b(v)$ in its binary

encoding is the input size taken for the computational complexity estimation of such an algorithm. The representations studied in Chapter 2 are *permutation representations*, so a sequence of such gives rise to a language $\cup_{n\geq 0}\pi_n(G_n) \subset \{0,1\}^*$, over which the optimization problem is defined. As observed in [BV88] and described in Chapter 2, many combinatorial optimization problems over languages of interest, e.g., over Hamiltonian cycles in complete graphs, are naturally polynomial time reducible to an optimization problem of that type, by choosing an appropriate sequence of permutation representations.

Other interesting objects associated with an orbit Gv are the *orbit matroid* $M(G,v)$ and *orbit oriented matroid* $O(G,v)$ defined by affine dependencies on the orbit. The stratification of the representation space by the oriented matroid type refines both stratifications by polytope type and matroid type, so the three are related. Indeed, in Chapter 2 the consideration of orbit matroids turns out to be helpful in resolving a problem on the polytope stratification.

In the case $\mathcal{K} = \mathbb{R}$, orbits of generic points are of special interest ($v \in \mathbb{R}^n$ is *generic* if its coordinates are algebraically independent over $\mathbb{Q}$). All generic points have the same orbit matroid, which we call the *generic matroid* of the representation. Exploring this matroid, more refined commutative algebraic questions arise. In particular, we are led to consideration of a new type of module arising from each matrix representation in the following way. Let $\mathcal{A} = \mathcal{K}[x_1, \cdots, x_d]$ be the ring of polynomials over $\mathcal{K}$ with d indeterminates, and $\mathcal{F} = \mathcal{K}(x_1, \cdots, x_d)$ its field of fractions. The action of G naturally extends to an action on the free $\mathcal{A}$-module $\mathcal{A}^d$. A generic point is in some sense represented by the element $x = (x_1, \cdots, x_d) \in \mathcal{A}^d \subset \mathcal{F}^d$. We consider both the $\mathcal{A}$-submodule of $\mathcal{A}^d$ and the $\mathcal{F}$-subspace of $\mathcal{F}^d$ generated by its orbit Gx. The generic matroid then coincides with the matroid of $\mathcal{F}$-linear dependencies on the orbit of x. Alternatively, a d-subset of the orbit Gx is a basis of the generic matroid if and only if the $\mathcal{A}$- submodule it generates is free of rank d.

As a step towards understanding these submodules, in Chapter 3, we study the submodule generated by the entire orbit Gx. We define an $\mathbb{N}$-graded module $M(\pi)$ for every linear representation $\pi : G \longrightarrow GL(V)$ (where V is some finite dimensional $\mathcal{K}$-space and $\mathcal{K}$ is any field), which is invariant under equivalence of representations. Its Hilbert series $H(\pi, t) = H(M(\pi), t)$ is an interesting invariant of the linear representation, which could be computed using symbolic computations, providing an interesting tie between representation theory and computer algebra. In the case of an algebraically closed $\mathcal{K}$ with $char(\mathcal{K}) \not| |G|$, and in some cases such as representations of the symmetric group over any subfield $\mathcal{K}$ of $\mathbb{C}$ with $char(\mathcal{K}) = 0$, we provide a canonical decomposition of $M(\pi)$ as a direct sum of certain graded *generic modules*, so $H(\pi, t)$ turns out to be a weighted sum of Hilbert series of generic modules. While the construction of Gröbner bases for these generic modules and the explicit evaluation of their Hilbert series is a continuing project, the case of multiplicity-free representations is entirely resolved here, and it is shown that the dimensions of the irreducible summands of π could be recovered from $H(\pi, t)$.

A rich and important class of theorems in affine geometry over an ordered field is formed by the so-called *Helly-type theorems.* An important subclass has emerged from the fundamental theorem of Tverberg [Tve66], asserting that any set of $(k-1)(d+1)+1$ points in real affine space $\mathbb{R}^d$ may be k-partitioned so that the convex hulls of the parts intersect. This theorem has been quite recently proved to hold more generally for oriented matroids, and an appropriate abstraction of it has long been conjectured to hold for an arbitrary space with a closure operator. In Chapter 4 we study these notions for the lattice of integer points $\mathbb{Z}^d \subset \mathbb{R}^d$. As is often the case, the study of geometric properties of lattices - known as geometry of numbers - tends to be much more difficult than the study of their rational counterparts. This is most transparent for algorithmic questions, where the complexity of many problems, which are trivial in the rational case, is unknown. In Chapter 4 we

address the algorithmic question of deciding the partitionability of a given set of points, and investigate its computational complexity.

Recently, there has been more progress in this area, initiated by a new algebraic proof of Tverberg's theorem by K. Sarkaria (private communication) and a multilinear-algebraic simplification of it due to the author. This raises further questions which are currently being investigated by the author.

Whereas it is customary to consider combinatorial optimization in a restrictive setting such as over a single language as discussed above, it is also important to study the general problem of optimizing linear functionals $v \in \mathbb{Q}^n$ over an arbitrary set $S \subseteq \{0,1\}^n$. A major contribution in this direction was given recently in [LS91]. A setting which makes it possible to let the input consist of (n, v) only, while still attempting to handle an arbitrary set $S \subseteq \{0,1\}^n$, is that of an oracle Turing machine [HU79]. Here one trades off accuracy for generality, and the goal is to maximize in polynomial time over an *approximation* of S, which we define to be a polytope P contained in the unit cube $[0,1]^n$ and satisfying $P \cap \{0,1\}^n = S$. This is the subject of study in Chapter 5.

1.2 Permutation polytopes

In Chapter 2 we concentrate on representations of the symmetric group S_n. The starting point here was, in fact, the broader construction of polytopes from subgroups of S_n without appealing to representations, but the treatment from a representation theoretical point of view provides a systematic construction of important subgroups. Identifying S_d with the subgroup of $GL(\mathbb{R}^d)$ of permutation matrices, for a subgroup G of S_d we have the *permutation polytope* $conv(G)$, and for $v \in \mathbb{R}^d$, the *orbit polytope* $P(G, v) = conv(Gv)$.

In the case $G = S_d$, both the permutation polytope and the orbit polytopes are well-understood. The *assignment polytope* $conv(S_d)$ is the set of bistochastic $d \times d$

matrices [HLP29], [Bir46]. The *permutohedron* introduced by Rado [Rad52] in the context of inequalities is the generic $P(S_d, v)$.

The study of these polytopes for an arbitrary subgroup has, over the years, "turned out to be unexpectedly difficult" (Mirsky, [Mir63]) and little is still known about them. This is no surprise in view of the close connection with hard combinatorial optimization problems which will be demonstrated in this chapter.

In this chapter we concentrate on *Young representations* of S_n (see [Jam78]). While these will be defined in detail in Chapter 2, it is enough here to recall that they are in $1-1$ correspondence with partitions $\lambda = (\lambda_1, \cdots, \lambda_k) \vdash n$ of of positive integers. The λ-Young representation turns S_n into a subgroup S_n^* of S_{d_λ}, where $d_\lambda = \frac{n!}{\prod_{i=1}^{k} \lambda_i!}$. The λ-*Young polytope*, denoted $P(\lambda)$, is the corresponding representation (or permutation) polytope $conv(S_n^*)$, and the corresponding orbit polytopes are denoted by $P(\lambda, v)$.

The 1-skeletons of convex polytopes and their graph theoretical invariants are of great interest in combinatorics. An important such invariant is the *stability number*, the size of a largest set of mutually nonadjacent vertices. Viewing the classical assignment polytope $conv(S_n) = P((n-1,1))$ in the framework of Young polytopes, we show that for any nontrivial partition $\lambda \vdash n$, the subgroup S_n^* gives rise to a stable set of vertices in the 1-skeleton of $P(S_{d_\lambda})$. This enables us to show that the stability number $\alpha(n) = \alpha(conv(S_n))$ is $2^{\Omega(\sqrt{n}logn)}$, which comes as a surprise in view of the density of these graphs. In contrast, for any partition λ as above, the Young polytope $P(\lambda)$ itself turns out to be 2-neighborly.

Another important invariant of the 1-skeleton of a polytope is its combinatorial diameter, which is important in the context of *linear programming* and path following algorithms for optimizing linear functionals over the polytope. Encouraging results on the polynomiality of diameters were obtained recently for $\{0,1\}$ polytopes [Nad89] and for more general lattice polytopes by P. Kleinschmidt and the author [KO92]. However, our 2-neighborliness result mentioned above implies

that the design of efficient algorithms (say, randomized) in a general path following setting may be impossible. Indeed, the graph of $P((n-2,2))$ is a clique, yet deciding the optimal value of a linear functional over this polytope is NP-complete. This implication, though, does not hold in the concrete case of linear programming, since our polytopes usually have exponentially many facets and the problem of optimizing over them does not fit into the linear programming framework.

We go on to discuss higher dimensional skeletons of Young polytopes. Letting m be the largest integer for which $P(\lambda)$ is m-neighborly, we show that under some restrictions on a partition λ with k positive parts, $\lfloor \frac{k^2}{2} \rfloor \leq m < \frac{1}{2}(k+1)!$. A sufficient condition for $P(\lambda)$ to be m-neighborly is derived and reduced to a graph theoretical statement on vertex coloring, and computational complexity aspects are discussed.

In the case S_d, all generic points have the same combinatorial type for the orbit polytope $P(S_d, v)$. D. Kozen (private communication) asked whether the same is true for an arbitrary subgroup G of S_d. We show that the answer to this question is negative. The polytope, matroid and oriented matroid stratifications of $\mathbb{R}^d$ are examined. For each subgroup G, a generic matroid $M(G)$ is defined, and it is shown that, although all generic points have the same orbit matroid $M(G)$, different generic points may have nonisomorphic polytopes and different f-vectors (face enumerators).

1.3 Modules from representations

A matrix $T \in GL_n(\mathcal{K})$ acts on the graded $\mathcal{A}$-module $\mathcal{A}^n$ by sending the n-tuple (or column vector) of polynomials $p = (p_1, \cdots, p_n) \in \mathcal{A}^n$ to the matrix product Tp. Given a matrix representation $\rho : G \longrightarrow GL_n(\mathcal{K})$, we then get an induced action on $\mathcal{A}^n$, and are interested in the graded $\mathcal{A}$ submodule of $\mathcal{A}^n$ generated by the orbit Gx of $x = (x_1, \cdots, x_n)$ under the representation. This module arises in

the study of the generic matroid of a representation as described in Section 1.1.

In Chapter 3 we define an $\mathbb{N}$-graded module $M(\pi)$ for every linear representation $\pi : G \longrightarrow GL(V)$, where V is an n-dimensional $\mathcal{K}$-space, which is invariant under equivalence of representation. In particular, its Hilbert series $H(\pi,t) = H(M(\pi),t)$ turns out to be an interesting invariant of π. For every choice of basis for V, the submodule of $\mathcal{A}^n$ generated by the orbit of x under the resulting matrix realization of π, as described in the paragraph above, could be identified with $M(\pi)$.

We provide a canonical decomposition of $M(\pi)$ into a direct sum of certain graded *generic* modules $M(r,c)$, $(r,c \in \mathbb{N})$, based on the decomposition of π into irreducible representations. The proof is based on the appropriate choice of basis for V and the investigation of the matrix space of the resulting matrix representation. An expression for the Hilbert series $H(\pi,t)$ is then obtained as a certain weighted sum of Hilbert series of generic modules. The field $\mathcal{K}$ is assumed to be algebraically closed, but in some cases, such as for representations of the symmetric group, this decomposition is valid over the reals and rationals as well.

The generic modules, which were studied in a homological context in [BE75], are of special interest. The author conjectures, and currently investigates, certain sets to be Gröbner bases for these modules. These bases will provide an easy way of computing the Hilbert series of generic modules, resulting in an explicit formula for $H(\pi,t)$ for an arbitrary π.

Here, the case in which π is a *multiplicity-free* representation is entirely resolved. An explicit formula for $H(\pi,t)$ is given, and it is shown that the Hilbert series could be used to recover other invariants of π, such as the dimensions of its irreducible components. An interesting consequence is the following. Given a multiplicity-free matrix representation ρ, the decomposition into irreducible components of which is unknown, one could use symbolic computation to determine its Hilbert series $H(\rho,t)$, from which, by the result above, the dimensions of the irreducible

components could be obtained.

1.4 Integral Radon partitions

Convexity spaces - those equipped with a closure operator assigning to each subset its abstract convex hull- form a general framework for abstracting convexity in real spaces and studying Helly-type properties.

A main course of study in this area is the determination of typical invariants for important models. Important models are in abundance, e.g., real affine spaces equipped with various metrics, and oriented matroids.

A particularly important invariant is the *Radon number*, the smallest positive integer n such that any subset of the space with at least n points admits a *Radon partition* - a 2-partition such that the closures of the two parts intersect. Radon partitions are fundamental objects in such a space: in the case of real affine point configurations the collection of Radon partitions encodes the entire combinatorial information. More generally, an oriented matroid is entirely determined by the setwise minimal Radon partitions, which are exactly its oriented circuits. Tverberg's partitions mentioned in Section 1.1 are a natural generalization of Radon partitions.

In Minkowski's "Geometry of numbers", geometric properties of the lattice of integer points $\mathbb{Z}^d \subset \mathbb{R}^d$ are investigated [GL87]. A particularly vital branch is that of algorithmic theory of numbers [Lov86], having important applications in integer programming and offering many problems whose computational complexity is unknown.

In Chapter 4, we relate the two areas above by studying Radon partitions in the lattice $\mathbb{Z}^d$. We call a partition (S, T) of a set of integer points in $\mathbb{R}^d$ an *integral Radon partition* if the convex hulls of S and T (in $\mathbb{R}^d$) have a common integer point. We study geometrical properties of lattice polytopes and introduce a useful

construction on stable sets in polytopes. We are then able to prove that if V is the set of vertices of a lattice d-polytope and $S \subset V$ is a stable set (in the 1-skeleton of $conv(V)$) of size $|S| = 2^d + 1$, then $(S, V \setminus S)$ is an integral Radon partition of V.

Next, we prove rather tight lower and upper bounds on the Radon number $r(d)$ of the integer lattice. We show that $r(d)$ is $\Omega(2^d)$ and $O(d2^d)$. We also settle the two-dimensional case $r(2) = 6$.

Finally, we consider algorithmic questions, and show that deciding whether a given set of n points in $\mathbb{Z}^d$ has an integral Radon partition is NP-complete, whereas in fixed dimension d it can be done in polynomial time.

1.5 Approximating oracle machines

Motivated by the recent work of Lovász and Schrijver [LS91], in this chapter we study the general combinatorial optimization problem using the setting of oracle Turing machines. By an *approximation* of a set $S \subseteq \{0,1\}^n$, we mean a convex polytope $P \subseteq [0,1]^n$ such that $P \cap \{0,1\}^n = S$. In [LS91], an operator $\mathcal{N}$ was introduced that produces from a given approximation P of $S \subseteq \{0,1\}^n$ another one $\mathcal{N}(P)$, with the property $P \supseteq \mathcal{N}(P) \supseteq \mathcal{N}^2(P) \supseteq \cdots \supseteq \mathcal{N}^n(P) = conv(S)$. Furthermore, a polynomial time oracle machine was given that converts maximization over P to maximization over $\mathcal{N}(P)$.

The question arises whether an oracle machine M and approximations $P(S)$ for every $S \subseteq \{0,1\}^n$ exist, such that M^S (the machine M equipped with the set S as oracle) maximizes rational linear functionals over $P(S)$ in polynomial time. In this chapter, we construct such a machine and the corresponding approximations. This enables a systematic application of the results of [LS91] to the combinatorial optimization problem over an arbitrary $S \subseteq \{0,1\}^n$.

Chapter 2

Geometry, Complexity, and Combinatorics of Permutation Polytopes

2.1 Introduction

Let $\pi : S_d \to GL(\mathbb{R}^d)$ be the *standard representation* of S_d, the symmetric group on d elements, assigning to each $\sigma \in S_d$ the corresponding permutation matrix with respect to the standard basis of $\mathbb{R}^d$. For a subgroup G of S_d, we define the *permutation polytope* of G to be $P(G) = conv(\{\pi(\sigma) : \sigma \in G\})$, and for $x \in \mathbb{R}^d$, the *orbit polytope* of x to be the convex hull of its orbit $P(G,x) = conv(\{\pi(\sigma)(x) : \sigma \in G\})$, which is a projection of $P(G)$.

In the case $G = S_d$, both the permutation polytope and the orbit polytopes are well understood. Hardy, Littlewood and Pólya [HLP29], and Birkhoff [Bir46] have shown that the so-called *assignment polytope* $P(S_d)$ is exactly the set of bistochastic $d \times d$ matrices, whereas Rado [Rad52], in the context of inequalities, essentially determined the combinatorial structure of the so-called *permutohedron* $P(S_d, x)$.

Little, however, is known in general, though already in [Rad52] orbit polytopes

were defined for an arbitrary subgroup, and Mirsky [Mir63] posed the question of determining a facial description of the general permutation polytope, indicating that this problem "turns out to be unexpectedly difficult".

As was observed by A. I. Barvinok and A. M. Vershik [BV88], permutation polytopes are closely related to the study of many combinatorial optimization problems. On one hand, this relation provides evidence that the combinatorial structure of these polytopes is probably intractable in general, and justifies Mirsky's claim about the difficulty of investigating them. On the other hand, studying them in a unified way might illuminate computational complexity aspects of combinatorial optimization.

It should be noted that permutation polytopes are $\{0,1\}$-polytopes, and as such, possess some special properties. In particular, Naddef and Pulleyblank [NP84], generalizing results of Brualdi and Gibson for the assignment polytope [BG77], showed that the 1-skeleton of such a polytope is always either a hypercube or Hamilton connected. Also, the diameter of such a polytope is at most its dimension (see [Nad89] for a proof and [KO92] for a generalization). At this point, however, the problem of efficiently characterizing the 1-skeletons of $\{0,1\}$-polytopes, raised in [NP84], remains unsettled.

In the next section we recall the definition of the fundamental class of Young representations of the symmetric group from the combinatorial point of view taken in [Jam78]. With any partition $\lambda = (\lambda_1, \cdots, \lambda_k) \vdash n$ into k positive parts, there is associated a λ-*Young representation* of the symmetric group, which turns S_n into a subgroup S_n^* of S_{d_λ}, where $d_\lambda = \frac{n!}{\prod_{i=1}^{k} \lambda_i!}$. We refer to the corresponding permutation polytope $P(S_n^*)$ as the λ-*Young polytope*, and denote it by $P(\lambda)$, and a corresponding orbit polytope is denoted by $P(\lambda, x)$. Also in Section 2.2, following [BV88], [Bar92], we demonstrate how many interesting combinatorial optimization problems can be embedded in this framework. For example, the problem of deciding the isomorphism of two k-uniform hypergraphs with n vertices, is reduced to the

problem of optimizing a linear functional over the Young polytope $P((n-k,k))$. Another example is provided by the *symmetric traveling salesman polytope*, which is an orbit polytope $P((n-2,2),h_n)$ for an appropriate $h_n \in \mathbb{R}^{\binom{n}{2}}$.

In Section 2.3 we investigate the assignment polytope, the study of which goes back to [HLP29]. In particular, its 1-skeleton has been extensively studied, see for example [BR74] and the second of a series of three papers devoted to the assignment polytope [BG77], where many interesting properties are established.

Viewing the assignment polytope $P(S_n) = P((n-1,1))$ in the framework of Young polytopes, we show that for any nontrivial partition $\lambda \vdash n$, the subgroup S_n^* gives rise to a stable set of vertices in the 1-skeleton of $P(S_{d_\lambda})$. In particular, the stability number $\alpha(n) = \alpha(P(S_n))$ is $2^{\Omega(\sqrt{n}logn)}$, which somewhat contrasts its strong connectivity properties (its diameter is at most 2 [BR74] and it is Hamilton connected [NP84]). We also discuss the computational complexity of recognizing these large stable sets.

In contrast, for any partition λ as above, the Young polytope $P(\lambda)$ itself turns out to be 2-neighborly. In Section 2.4 we study the neighborliness degree of Young polytopes. Letting l be the largest integer for which $P(\lambda)$ is l-neighborly, it is shown that under some restrictions on a partition λ with k positive parts, $\lfloor \frac{k^2}{2} \rfloor \leq l < \frac{1}{2}(k+1)!$. A sufficient condition for $P(\lambda)$ to be l-neighborly is derived and reduced to a graph theoretical statement on vertex coloring, and computational complexity aspects are discussed. It is interesting, in the context of path following algorithms for optimizing linear functionals over convex polytopes, that the associated decision problem on the sequence $P((n-2,2))$ is NP-complete, while the graph of $P((n-2,2))$ has diameter 1. It is also interesting that, while the adjacency relation of the sequence $P((n-2,2))$ is trivial, it is known to be NP-complete for the projected sequence $P((n-2,2),h_n)$ of traveling salesman polytopes [Pap78].

Given a subgroup G of S_d, the orbit polytopes form a polytope bundle $\{P(G,x) : \quad x \in \mathbb{R}^d\}$ (see [BS92]), and their combinatorial type induces the

polytope stratification of the base space $\mathbb{R}^d$, i.e., $\mathbb{R}^d$ is partitioned into equivalence classes with x, y in the same class when the polytopes $P(G,x), P(G,y)$ are of the same combinatorial type. A sequence of partitions, such as $(n-2,2)$, $n \geq 4$, yields a sequence $\{P((n-2,2),x): \ x \in \mathbb{R}^{\binom{n}{2}}\}$ of polytope bundles, and for each specified sequence of vectors $x_n \in \mathbb{R}^{\binom{n}{2}}$ we obtain a sequence of polytope fibers $P((n-2,2),x_n)$, on which the linear optimization-related decision problem is considered. It turns out that for some $\{0,1\}$-valued sequences, the decision problem belongs to the computational complexity class P, while in other cases it is NP-complete. This observation, made in [BV88], motivates the study of the polytope stratification. A first step is to restrict attention to orbits of generic points, i.e., points whose coordinates are algebraically independent over the rationals. Indeed, Rado's work [Rad52] implies that for any generic point, $P(S_d,x)$ is the permutohedron. This naturally leads to the following question suggested by D. Kozen (private communication). Is it true that, for an arbitrary subgroup G of S_d, the combinatorial type of the orbit polytope is the same for any generic point?

In Section 2.5 we show that the answer to this question is negative. We study the polytope stratification of $\mathbb{R}^d$ and the related stratifications induced by the affine matroid and oriented matroid of an orbit. For each subgroup G, a generic matroid $M(G)$ is defined, and it is shown that, while any two generic points have the same orbit matroid $M(G)$, different generic points may have nonisomorphic orbit polytopes. This shows that the polytope stratification is nontrivial even on the set of generic points, and thus provides a negative answer to Kozen's question. In our construction, G is the $(2,2)$-Young representation of S_4 in $GL(\mathbb{R}^6)$, and we establish the existence of generic points $x, y \in \mathbb{R}^6$ for which the polytopes $P(G,x)$ and $P(G,y)$ have different numbers of faces of the same dimension.

2.2 Young representations and combinatorial optimization

We start by establishing some notation. Given a finite set A, we denote by S_A the group of permutations of elements of A, and by $\mathbb{R}^A$ the vector space of real-valued functions on A, with the standard basis $\{e_a : a \in A\}$ of Kronecker functions, $e_a(b) = \delta_{a,b}$ $(a, b \in A)$. Similarly, we denote by $mat(A, \mathbb{R})$ the algebra of real matrices with the standard basis $\{e_{a,b} : a, b \in A\}$. Given a point $x \in \mathbb{R}^A$, its *support* is $supp(x) = \{a : x_a \neq 0\} \subseteq A$, and for a point $x \in mat(A, \mathbb{R})$, let $supp(x) = \{(a, b) : x_{(a,b)} \neq 0\} \subseteq A \times A$. For a subset X of any real space, we let $supp(X) = \cup\{supp(x) : x \in X\}$. We can identify, by means of the standard basis, the algebra $L(\mathbb{R}^A)$ of linear transformations from $\mathbb{R}^A$ to itself, with $mat(A, \mathbb{R})$. These two are also identified with the tensor product $\mathbb{R}^A \otimes \mathbb{R}^A$, by sending a matrix $M \in mat(A, \mathbb{R})$ to the tensor $\sum_{a,b \in A} M_{a,b} e_a \otimes e_b$. The standard representation of S_A is the group homomorphism $\pi : S_A \to GL(\mathbb{R}^A) \subseteq L(\mathbb{R}^A)$ given by $\pi(\sigma)(e_a) = e_{\sigma(a)}$ $(a \in A)$. When $A = [d] = \{1, \cdots, d\}$, we use the abbreviated notation S_d, $\mathbb{R}^d$, and $\mathbb{R}^{d \times d}$.

We now describe the class of Young representations of the symmetric group. For a thorough discussion of this theory the reader is referred to [Jam78]. We remark that this class is complete in the sense that the characters of Young representations form a $\mathbb{Z}$-basis for the lattice of characters of the symmetric group.

Given a partition $\lambda = (\lambda_1, \cdots, \lambda_k)$ of $n \in \mathbb{N}$ into k positive integers $\lambda_1 \geq \cdots \geq \lambda_k$, a *$\lambda$-diagram* is a set $D = \{(i, j) : 1 \leq i \leq k,\ 1 \leq j \leq \lambda_i\}$. A *$\lambda$-tableau* is a bijection from D onto $[n]$. Thinking of a pair $(i, j) \in D$ as the (i, j)th entry of an $n \times n$ matrix, we arrive at the more pictorial way, attributed to A. Young, of viewing a λ-diagram as a table having k left justified rows, where the ith row has λ_i entries. A λ-tableau is then a λ-diagram filled with the numbers $1, \cdots, n$, each appearing exactly once. Define now an equivalence relation on λ-tableaux, where two tableaux

are related if they have the same set of numbers in each row. An equivalence class t is called a λ-*tabloid.* When dealing with partitions with large number k of parts, it will be convenient to think of a tabloid t simply as an ordered list of subsets forming a partition of $[n]$, where the ith subset, denoted by $t[i]$, is the λ_i-set (set of size λ_i) constituting the ith row. For example, $t = (\{1,3,6\}, \{2,4\}, \{5,7\})$ is a $(3,2,2)$-tabloid. The permutation group S_n acts naturally on λ-tableaux, where a permutation $\sigma \in S_n$ sends a given tableau to the one obtained from it by applying σ to its entries. This action clearly induces a well-defined action on the set $T(\lambda)$ of λ-tabloids. When the partition λ is clear from the context, we will denote by σ^* the permutation on $T(\lambda)$ induced from $\sigma \in S_n$. Thus, $* : S_n \longrightarrow S_{T(\lambda)}$ is a group homomorphism, and the image S_n^* of S_n is a subgroup of $S_{T(\lambda)}$. Note that the number of λ-tabloids is $\binom{n}{\lambda} = \frac{(\sum_{i=1}^k \lambda_i)!}{\prod_{i=1}^k \lambda_i!}$.

Now, let $\{e_t : t \in T(\lambda)\}$ be the standard basis of Kronecker functions of the space $\mathbb{R}^{T(\lambda)}$. The λ-*Young representation* of the symmetric group, $\pi_\lambda : S_n \rightarrow GL(\mathbb{R}^{T(\lambda)})$, is defined by $\pi_\lambda(\sigma)(e_t) = e_{\sigma^*(t)}$ for all $\sigma \in S_n$, $t \in T(\lambda)$. We then have the *Young permutation polytope*

$$P(\lambda) = conv(\{\pi_\lambda(\sigma) : \sigma \in S_n\}) = conv(\{\pi(\sigma^*) : \sigma^* \in S_n^*\}) = P(S_n^*) \subseteq \mathbb{R}^{T \times T},$$

and, for $x \in \mathbb{R}^T$, the *Young orbit polytope*

$$\begin{aligned} P(\lambda, x) &= conv(\{\pi_\lambda(\sigma)(x) : \sigma \in S_n\}) \\ &= conv(\{\pi(\sigma^*)(x) : \sigma^* \in S_n^*\}) = P(S_n^*, x) \subseteq \mathbb{R}^T. \end{aligned}$$

Example 2.2.1 Let $\lambda = (n-1, 1)$. Then, identifying a tabloid $t \in T(\lambda)$ with the number $i \in [n]$ such that $t[2] = \{i\}$, we can identify in that case S_n^* with S_n, so $P((n-1,1)) = P(S_n)$ is the assignment polytope.

We now demonstrate the connection between Young polytopes and combinatorial optimization. The discussion below is similar to [BV88], [Bar92] and is included for the completeness of the exposition. Consider a sequence of rational polytopes

$P_n \subseteq \mathbb{R}^{d(n)}$, $n \in \mathbb{N}$, specified in some uniform way. The *optimization problem* on this sequence is the problem of obtaining, given $n \in \mathbb{N}$ and a rational vector $c_n \in \mathbb{Q}^{d(n)}$, the value $z = max\{\langle c_n, x\rangle : x \in P_n\}$. The *decision problem* on the sequence is, given $n \in \mathbb{N}$ and $c_n \in \mathbb{Q}^{d(n)}$ as above, and a rational number $q \in \mathbb{Q}$, to decide whether $z \geq q$. The size of an input instance (n, c_n, q) will be taken as $n + size(c_n) + size(q)$ (see [Sch86]).

Now, any $k-1$ positive integers $\lambda_2 \geq \lambda_3 \geq \cdots \geq \lambda_k$ yield a sequence

$$\lambda(n) = (n - \sum_{i=2}^{k} \lambda_i, \lambda_2, \cdots, \lambda_k), \qquad n \geq \lambda_2 + \sum_{i=2}^{k} \lambda_i$$

of partitions of n, and this yields a sequence of permutation polytopes $P(\lambda(n))$. If, in addition, a sequence $x_n \in \mathbb{R}^{T(\lambda(n))}$ of vectors is specified, then we also have a sequence of orbit polytopes $P(\lambda(n), x_n)$. We remark that this way of producing a sequence of partitions appears implicitly in many contexts, e.g., in [Kal90], where the asymptotics of the rank function of a compatible series of symmetric matroids on $T((n-k,k))$ is addressed.

Example 2.2.2 Let k be a positive integer and $\lambda(n) = (n-k, k)$. A tabloid t can then be identified with the k-set, or hyperedge $t[2]$ of the complete k-uniform hypergraph on the set of vertices $[n]$. Thus, a vector $x \in \mathbb{R}^{T((n-k,k))}$ could be identified with a weighted k-uniform hypergraph, having set of hyperedges $supp(x)$, where the weight of an edge $t \in supp(x)$ is x_t. If x is $\{0,1\}$-valued, then x is an (unweighted) k-uniform hypergraph. If $k = 2$, it is simply an abstract graph. Given two k-uniform hypergraphs $h, g \in \mathbb{R}^{T((n-k,k))}$, having $q = |supp(h)| = |supp(g)|$ hyperedges each, and letting $c = h \otimes g$, the decision problem on $P(\lambda(n))$ with input (n, c, q) is exactly the decision question of whether or not g and h are isomorphic as hypergraphs. Note also that the collection of maximal simplices of a $(k-1)$-dimensional pure simplicial complex is a k-uniform hypergraph, so the isomorphism of pure simplicial complexes could be decided in the same way.

Example 2.2.3 Let $h_n \in \mathbb{R}^{T((n-2,2))}$ be a graph which is an n-cycle. For instance, let $n = 5$, let $t_1 = (\{3,4,5\},\{1,2\}),\cdots,t_4 = (\{1,2,3\},\{4,5\})$, and $t_5 = (\{2,3,4\},\{5,1\})$. Then h_5 could be taken as $h_5 = \sum_{i=1}^{5} e_{t_i}$. The sequence of orbit polytopes $P((n-2,2),h_n)$, $n \in \mathbb{N}$ is the sequence of *symmetric traveling salesman polytopes*, for which the decision problem is NP-complete. More precisely, given a graph $c \in \mathbb{R}^{T((n-2,2))}$, the decision problem on $P((n-2,2),h_n)$ with input (n,c,n) is exactly the decision problem of whether or not c has a Hamiltonian cycle.

Similarly, taking $k(n) \leq n$ and a complement of a $k(n)$-clique $s_n = K_n \setminus K_{k(n)}$, the decision problem on $P((n-2,2),s_n)$ with input (n,c,q), where $c \in \mathbb{R}^{T((n-2,2))}$ is a graph and $q = |supp(c)|$, is the decision problem of whether or not c has a stable set of size at least $k(n)$.

For some nontrivial orbits, however, the optimization and decision problems can be solved in polynomial time. Let m_n be an $\lfloor \frac{n}{2} \rfloor$-matching. Then, the solution for the optimization problem on $P((n-2,2),m_n)$ with input (n,c), where $c \in \mathbb{R}^{T((n-2,2))}$, is the maximum weight of a matching in the weighted graph c.

Thus, as observed in [BV88], the decision problem on the orbit polytopes is NP-complete in general. Observing that for any matrix $A \in \mathbb{R}^{d\times d}$ and vectors $x,c \in \mathbb{R}^d$ we have $\langle c, Ax\rangle = \langle c\otimes x, A\rangle$, it is clear that the optimization problem for any orbit polytope $P(G,x)$ on input c, could be solved by solving the optimization problem on the corresponding permutation polytope $P(G)$ on input $c\otimes x$. This implies that various decision problems that can be associated with the determination of the combinatorial structure of Young polytopes and their orbit counterparts are probably intractable. For example, in [Pap78] it was proved that deciding vertex adjacency for the class $P((n-2,2),h_n)$ of symmetric traveling salesman polytopes is NP-complete. Nevertheless, in Section 2.4 we establish some statements on the combinatorial structure of Young polytopes.

2.3 On the graph of the assignment polytope

Given a convex polytope P with a set of vertices $V = ext(P)$, we will refer to a subset $F \subseteq V$ as a *face* of P if for some face G of P we have $F = G \cap V$. The 1-*skeleton*, or *graph*, of P, is the abstract graph on V in which the edges are the 1-faces of P. A subset $S \subseteq V$ is *stable* in P if it is stable in the graph of P; i.e., no two vertices $u, v \in S$ form an edge (1-face) of P.

In this section, we study the assignment polytope $P(S_n)$, and show that subgroups induced by Young representations give rise to large stable sets of vertices in its 1-skeleton. In particular, letting $\alpha(n) = \alpha(P(S_n))$ be the *stability number* of $P(S_n)$, i.e., the largest size of a stable set of $P(S_n)$, we show that $\alpha(n) = 2^{\Omega(\sqrt{n}logn)}$. This is somewhat surprising, since the graph of $P(S_n)$ is Hamilton connected [NP84] and its diameter is 2 for all $n \geq 4$ [BR74].

Before going on, we recall some definitions and properties of convex polytopes and oriented matroids. For the theory of convex polytopes, consult, for example, [Grü67], [Brø83], and for oriented matroids [BLVS+92].

A convex polytope P is *k-neighborly* if every k-subset of its vertices is a $(k-1)$-face of P. If P is k-neighborly, then it is i-neighborly for $i = 0, 1, \cdots, k$. We define the *neighborliness degree* of P to be the largest k for which it is k-neighborly.

Given a set of points in affine space, $V \subseteq \mathbb{R}^d$, a *Radon partition* of V is a partition (S, T) of V such that $conv(S) \cap conv(T) \neq \emptyset$. A pair (S, T) of sets of points in $\mathbb{R}^d$ is a *minimal Radon partition* if it is a Radon partition of $S \cup T$, and no proper subset of $S \cup T$ admits a Radon partition. Note that, in the language of oriented matroids (see [BLVS+92]), given a finite set $V \subseteq \mathbb{R}^d$ and a pair (S, T) of subsets of V, the pair is a minimal Radon partition exactly when it is an oriented circuit of the affine oriented matroid on V. We will therefore call a pair (S, T) an *oriented circuit* of V if (S, T) is a minimal Radon partition and $S, T \subseteq V$.

We need the following statement from [LV80] (see also [BLVS+92, Prop. 9.1.2]).

Proposition 2.3.1 *Let $P \subseteq \mathbb{R}^d$ be a convex polytope and $V = ext(P)$. A subset $F \subseteq V$ is not a face of P if and only if there exists an oriented circuit (S,T) of V such that $S \subseteq F$ and $T \not\subseteq F$.*

For polytopes contained in the nonnegative orthant $\mathbb{R}^d_+$, we can deduce the following sufficient condition for being a face.

Proposition 2.3.2 *Let $P \subseteq \mathbb{R}^d_+$ be a convex polytope, $V = ext(P)$, and $F \subseteq V$. If for all $v \in V \setminus F$ we have $supp(v) \not\subseteq supp(F)$, then F is a face of P.*

Proof. Let $F \subseteq V$ satisfy the hypothesis of the proposition. Assume indirectly that it is not a face of P, and let (S,T) be an oriented circuit of V as is guaranteed by Proposition 2.3.1. Now, (S,T) is a Radon partition, so there exists a point $x \in conv(S) \cap conv(T)$. Writing x as a convex combination of elements of T, the coefficient of each $t \in T$ is positive, since (S,T) is a minimal Radon partition. But $T \subseteq V \subseteq \mathbb{R}^d_+$, so $supp(T) = supp(x) \subseteq supp(S) \subseteq supp(F)$, which by hypothesis implies $T \subseteq F$, a contradiction. □

Next, we introduce some notation. We denote by e the identity element in S_n. By a *proper cycle* of a permutation, we mean a cycle of length at least two. Given a permutation $\sigma \in S_d$, we denote by $\bar{\sigma} = \pi(\sigma)$ the corresponding matrix assigned to it by the standard representation, regarded as a point in affine space $\mathbb{R}^{d \times d}$, and by $\bar{\sigma}_{i,j}$ its (i,j)th entry $(i,j \in [d])$. Similarly, when $\sigma \in S_n$ and $\sigma^* \in S_{T(\lambda)}$ is the induced permutation, where the partition $\lambda \vdash n$ is understood, we have $\bar{\sigma}^* \in \mathbb{R}^{T \times T}$, and for tabloids $s,t \in T(\lambda)$, its (s,t)th entry is $\bar{\sigma}^*_{s,t}$.

We now turn to discuss the graph of the assignment polytope. Recall the following proposition from [PR74], which can be derived from Proposition 2.3.2.

Proposition 2.3.3 *A 2-subset $F = \{\bar{\sigma}, \bar{\tau}\} \subseteq \{\bar{\sigma} : \sigma \in S_n\} = ext(P(S_n))$ is an edge of $P(S_n)$ if and only if $\sigma^{-1}\tau$ has exactly one proper cycle.*

By means of the identification given in Example 2.2.1, we have $P((n-1,1)) = P(S_n)$, and so Proposition 2.3.3 implies that, for $n \geq 4$, the permutation polytope

$P((n-1,1))$ is not 2-neighborly. It will become evident in the next section that, in contrast, for all $\lambda \vdash n$ other than $(n), (n-1,1)$, the Young polytope $P(\lambda)$ is 2-neighborly, that is, any two vertices in $V(\lambda) = \{\bar{\sigma}^* : \sigma \in S_n\} = ext(P(\lambda))$ form an edge of $P(\lambda)$. It is interesting to note that, in contrast to this last statement, no two vertices in $V(\lambda)$ form an edge in the assignment polytope $P(S_{T(\lambda)})$. This is the content of the following.

Theorem 2.3.4 *Let $\lambda \vdash n$ be any partition other than $(n), (n-1,1)$. The subset*

$$V(\lambda) = \{\bar{\sigma}^* : \sigma \in S_n\} \subseteq \{\bar{\sigma} : \sigma \in S_{T(\lambda)}\} = ext(P(S_{T(\lambda)}))$$

is stable in $P(S_{T(\lambda)})$.

Proof. Let $\sigma \in S_n$, $\sigma \neq e$, and without loss of generality, assume that $C = (1, 2, \cdots, l)$ is a cycle of σ of largest length $l \geq 2$. We will exhibit tabloids $s, t \in T(\lambda)$ that belong to distinct proper cycles of σ^*.

Assume first that $\lambda_1 \geq 2$. Let s be a tabloid satisfying $\{1,3\} \subseteq s[1]$ and $2 \in s[2]$.

If $l \geq 3$ then choose $t \in T(\lambda)$ such that $t[1]$ consists of the smallest elements in $[n] \setminus \{l-1, l\}$, and $\{l-1, l\} \subseteq t[2] \cup t[3]$. Now, $2 \in s[2] \cap \sigma^*(s)[1]$, so $\sigma^*(s) \neq s$ and s belongs to a proper cycle of σ^*. Similarly, $1 \in t[1] \setminus \sigma^*(t)[1]$, so t belongs to a proper cycle of σ^* as well. By construction, $t[1] \cap C = [m]$ for some $m \leq l-2$. Consider the tabloid $(\sigma^*)^i(t)$ in the cycle of t. Reducing i modulo l if necessary, assume $0 \leq i < l$. We need to show that $s \neq (\sigma^*)^i(t)$. This is true for $i = 0$, since it is easy to see that $s \neq t$. For $i = 1, \cdots, l-m$, we have $(\sigma^*)^i(t)[1] \cap C = \sigma^i([m])$, so $1 \in s[1] \setminus (\sigma^*)^i(t)[1]$. For $i = l+1-m \geq 3$, we have $3 \in s[1] \setminus (\sigma^*)^i(t)[1]$. Finally, if $l+2-m \leq i < l$, we have $2 \in (\sigma^*)^i(t)[1] \cap s[2]$. We conclude that s is not in the cycle of t, so σ^* has at least two proper cycles.

If $l = 2$ then choose $t \in T(\lambda)$ such that $1 \in t[1]$ and $\{2,3\} \subseteq t[2] \cup t[3]$.

If, however, $\lambda_1 = 1$ (so $\lambda = (1, 1, \cdots, 1)$), choose $s, t \in T(\lambda)$ such that $1 \in s[1] \cap t[1]$, $2 \in s[2] \cap t[3]$, and $3 \in s[3] \cap t[2]$.

It is left for the reader to verify that s and t belong to different proper cycles of σ^* in these cases as well.

Thus, given any $\bar{\sigma}^*, \bar{\tau}^* \in V(\lambda)$, we have that, in $S_{T(\lambda)}$, $(\sigma^*)^{-1}\tau^* = (\sigma^{-1}\tau)^*$ is either the identity or has more than one proper cycle, and so, by Proposition 2.3.3, $\{\bar{\sigma}^*, \bar{\tau}^*\}$ is not a 1-face of $P(S_{T(\lambda)})$. □

We conclude that, in general, the graph of the assignment polytope $P(S_n)$ contains large stable sets. In particular, we have the following.

Corollary 2.3.5 *Let $\alpha(n) = \alpha(P(S_n))$ denote the stability number of the nth assignment polytope. Then $\alpha(n) = 2^{\Omega(\sqrt{n}logn)}$.*

Proof. Given $n \in \mathbb{N}$, $n \geq 4$, let d be the largest integer such that $D = \binom{d}{2} \leq n$, and let $H = S_{[D]} \times S_{\{D+1\}} \times S_{\{D+2\}} \times \cdots \times S_{\{n\}}$. Identify $T((d-2,2))$ with $[D]$, say, by sending a tabloid t with $t[2] = \{i,j\}$ $(i < j)$ to $d(i-1) - \frac{i}{2}(i+1) + j \in [D]$. Then, the $(d-2,2)$ Young representation turns S_d into a subgroup S_d^* of $S_{[D]}$, and by the theorem, the set

$$STABLE_n = \{\bar{\sigma} : \sigma \in S_d^* \times S_{\{D+1\}} \times S_{\{D+2\}} \times \cdots \times S_{\{n\}}\} \subset mat(n, \mathbb{R})$$

is stable in $conv\{\bar{\sigma} : \sigma \in H\} \subseteq P(S_n)$, and so is stable in $P(S_n)$ as well. Thus, $\alpha(n) \geq d! \geq \sqrt{n}! = 2^{\Omega(\sqrt{n}logn)}$. □

Thus, for every $n \geq 4$ we have the set $STABLE_n$ of $n \times n$ permutation matrices, which is stable in $P(S_n)$. Let $STABLE = \cup_{n \geq 4} STABLE_n$. We now show that (membership in) $STABLE$ can be efficiently decided. First, consider the following question. Given a partition $\lambda = (\lambda_1, \cdots, \lambda_k) \vdash n$ with $n \geq 2\lambda_k$ and a permutation $\sigma \in S_{T(\lambda)}$, is σ induced by the λ-Young representation, i.e., is $\sigma = \tau^*$ for some $\tau \in S_n$? The following procedure decides this question. Construct a candidate τ as follows. For each $i \in [n]$, choose two disjoint $(\lambda_k - 1)$-subsets $S, T \subset [n] \setminus \{i\}$, and tabloids $s, t \in T(\lambda)$ such that $s[k] = S \cup \{i\}$ and $t[k] = T \cup \{i\}$. If $|\sigma(s)[k] \cap \sigma(t)[k]| \neq 1$ then σ is not induced. If $\sigma(s)[k] \cap \sigma(t)[k] = \{j\}$ then let $\tau(i) = j$. If τ was constructed successfully and is a permutation, then σ is induced if and only if

$\sigma = \tau^*$. Using this procedure for the special case $\lambda = (n-2,2)$, we get the following.

Proposition 2.3.6 *Membership in STABLE is decidable in polynomial time.*

Proof. Given $A \in mat(n, \mathbb{R})$, one finds a maximal d such that $D = \binom{d}{2} \leq n$, and verifies that A is a permutation matrix having the form

$$A = \begin{bmatrix} B & 0 \\ 0 & I_{n-D} \end{bmatrix},$$

where I_{n-D} is the identity in $mat(n-D, \mathbb{R})$. Applying the procedure described above, one verifies that the permutation in $S_{T((d-2,2))} = S_D$ corresponding to the permutation matrix $B \in mat(D, \mathbb{R})$ is induced from some permutation in S_d. The matrix A is in $STABLE$ if and only if all verifications are true, and clearly this task can be performed in time polynomial in $size(A)$, in fact, polynomial in n. □

2.4 Neighborliness degree of Young polytopes

In this section we establish lower and upper bounds on the neighborliness degree of Young polytopes, in terms of their defining partition λ.

Given a finite set A and a permutation $\sigma \in S_A$, it will be convenient to denote by $move(\sigma) = \{a \in A : \sigma(a) \neq a\}$ the subset of A moved by σ.

Lemma 2.4.1 *Let $\lambda \vdash n$ be any partition, and l such that $1 \leq l < n!$. If for every l distinct permutations other than the identity, $\sigma_1, \cdots, \sigma_l \in S_n \setminus \{e\}$, there exists a tabloid $t \in T(\lambda)$ such that $\sigma_i^*(t) \neq t \ \ (i = 1, \cdots, l)$, then $P(\lambda)$ is l-neighborly.*

Proof. Let $F = \{\sigma_1, \cdots, \sigma_l\} \subseteq S_n$, and $\bar{F} = \{\bar{\sigma}^* : \sigma \in F\} \subseteq ext(P(\lambda))$. Let $\tau \in S_n \setminus F$. Then $e \notin \{\sigma\tau^{-1} : \sigma \in F\}$, so by the hypothesis there exists a tabloid t such that $(\sigma_i\tau^{-1})^*(t) \neq t \ \ (i = 1, \cdots, l)$. Let $s = (\tau^{-1})^*(t)$. Then,

$$\tau^*(s) = \tau^*(\tau^{-1})^*(t) = (\tau\tau^{-1})^*(t) = t,$$

yet

$$\sigma_i^*(s) = \sigma_i^*(\tau^{-1})^*(s) = (\sigma_i\tau^{-1})^*(t) \neq t \quad (i = 1, \cdots, l).$$

Thus, we have $\bar{\tau}^*_{t,s} = 1$ while $(\bar{\sigma}_i^*)_{t,s} = 0$ $(i = 1, \cdots, l)$. Hence $supp(\bar{\tau}^*) \not\subseteq supp(\bar{F})$. Since τ was an arbitrary permutation not in F, we conclude from Proposition 2.3.2 that $\bar{F}$ is a face of $P(\lambda)$, and since F was an arbitrary l-subset of S_n, it follows that $P(\lambda)$ is indeed l-neighborly. □

We conclude our first lower bound.

Corollary 2.4.2 *If $\lambda \vdash n$ is a partition with $k+1$ parts $(k \geq 1)$ and $\lambda_1 \geq k$, then $P(\lambda)$ is k-neighborly.*

Proof. We prove that the hypothesis of Lemma 2.4.1 holds for $l = k$. Let $\sigma_1, \cdots, \sigma_k \in S_n \setminus \{e\}$ be k distinct permutations. Choose $j_i \in move(\sigma_i)$, $(i = 1, \cdots, k)$, and denote $S = \{j_1, \cdots, j_k\} = \{s_1, \cdots, s_m\}$ for some $m \leq k$ and distinct $s_1, \cdots, s_m$. Now, let $t \in T(\lambda)$ be a tabloid satisfying $s_i \in t[i+1]$ $(i = 1, \cdots, m)$ and $\{\sigma_1(j_1), \cdots, \sigma_k(j_k)\} \setminus S \subseteq t[1]$. It is clear that such tabloid exists and that $\sigma_i^*(t) \neq t$ $(i = 1, \cdots, k)$. The corollary follows from Lemma 2.4.1. □

Behind this proof lies the more general observation that the hypothesis of Lemma 2.4.1 holds for a partition λ and a positive integer l if and only if a certain graph theoretical property on vertex coloring holds for λ and l. Recall that, given a (simple) graph $H = (V, E)$, a function $\chi : V \to [k]$ is a *k-coloring* of H if $\{u, v\} \in E$ implies $\chi(u) \neq \chi(v)$. Given $\lambda = (\lambda_1, \cdots, \lambda_k)$ with $\lambda_1 \geq \cdots \geq \lambda_k \geq 0$, we say that $\chi : V \to [k]$ is a *λ-coloring* if it is a k-coloring and $|\chi^{-1}(i)| \leq \lambda_i$ $(i = 1, \cdots, k)$. The sufficient condition for $P(\lambda)$ to be l-neighborly given in Lemma 2.4.1, translates to a statement on λ-colorings.

Lemma 2.4.3 *Let $\lambda = (\lambda_1, \cdots, \lambda_k) \vdash n$ be any partition, and l such that $1 \leq l \leq \frac{n}{2}$. For every l distinct permutations $\sigma_1, \cdots, \sigma_l \in S_n \setminus \{e\}$ there exists a tabloid $t \in T(\lambda)$ such that $\sigma_i^*(t) \neq t$ $(i = 1, \cdots, l)$, if and only if every graph with l edges admits a λ-coloring.*

Proof. Given distinct permutations $\sigma_1, \cdots, \sigma_l \in S_n \setminus \{e\}$, choose $j_i \in move(\sigma_i)$ $(i = 1, \cdots, l)$, and define the graph $H = (V, E)$, where

$$V = \{j_1, \cdots, j_l\} \cup \{\sigma_1(j_1), \cdots, \sigma_l(j_l)\}, \quad E = \{\{j_1, \sigma_1(j_1)\}, \cdots, \{j_l, \sigma_l(j_l)\}\}.$$

Since $|E| \leq l$, there exists a λ-coloring χ of H. Choose a tabloid $t \in T(\lambda)$ such that $\chi^{-1}(i) \subseteq t[i]$ $(i = 1, \cdots, k)$. It is clear that $\sigma_i^*(t) \neq t$ $(i = 1, \cdots, l)$. Conversely, consider any graph $H = (V, E)$ with l edges. Its set of vertices can be taken as $V = [m]$ for some $m \leq 2l \leq n$. For $i = 1, \cdots, l$, define from the ith edge $f_i = \{u_i, v_i\}$ a transposition $\sigma_i = (u_i, v_i)$. Let $t \in T(\lambda)$ such that $\sigma_i^*(t) \neq t$ $(i = 1, \cdots, l)$, and let $\chi : [m] \to [k]$ be the unique function satisfying $\chi^{-1}(i) = [m] \cap t[i]$ $(i = 1, \cdots, k)$. It is clear that χ is a λ-coloring of H. □

The following graph theoretical proposition is easy ([Ber73, Cor.1, p.336]).

Proposition 2.4.4 *If at most p vertices in a graph H have degree at least p, then H admits a p-coloring.*

Proof. Let H have the set of vertices $[m]$, let the degree of i be denoted by d_i, and assume $d_1 \geq d_2 \cdots \geq d_m$. For $i = 1, \cdots, p$, set $\chi(i) = i$, and for $i > p$ choose $\chi(i) \in [p]$ which has not been assigned to any of the (at most $p - 1$) neighbors of i already colored. □

A second lower bound follows.

Corollary 2.4.5 *Let l be a positive integer, and $\lambda \vdash n$ be any partition with $k \geq \sqrt{2l}$ parts such that $\lambda_1 \geq \cdots \geq \lambda_{\lceil\sqrt{2l}\rceil} \geq 2l$. Then $P(\lambda)$ is l-neighborly.*

Proof. Any graph with l edges satisfies the hypothesis of Proposition 2.4.4 with $p = \lceil\sqrt{2l}\rceil \leq k$, and has at most $2l$ vertices. It therefore has a p-coloring χ, and $|\chi^{-1}(i)| \leq 2l \leq \lambda_i$ $(i = 1, \cdots, p)$, so χ is a λ-coloring as well. The claim follows from Lemma 2.4.3 and Lemma 2.4.1. □

Next, we give an upper bound on the neighborliness degree of Young polytopes.

Lemma 2.4.6 *Let $\lambda \vdash n$ be a partition with $k \geq 2$ parts such that $n > k$. Let H be the subgroup*

$$H = \{\sigma \in S_n : \ move(\sigma) \subseteq [k+1]\} = S_{[k+1]} \times S_{\{k+2\}} \times S_{\{k+3\}} \times \cdots \times S_{\{n\}},$$

and let S be the subgroup of the even permutations in H.

Then the $\frac{1}{2}(k+1)!$-set $\bar{S}^* = \{\bar{\sigma}^* : \ \sigma \in S\} \subseteq ext(P(\lambda))$ is not a face of $P(\lambda)$.

Proof. Let $T = H \setminus S$ be the set of odd permutations in H, and let $\bar{T}^* = \{\bar{\sigma}^* : \sigma \in T\}$. We will show that $\sum\{\bar{\sigma}^* : \ \sigma \in S\} = \sum\{\bar{\sigma}^* : \ \sigma \in T\}$, which, since $|S| = |T|$, shows that $conv(\bar{S}^*) \cap conv(\bar{T}^*) \neq \emptyset$, so $\bar{S}^*$ is not a face.

So, we have to show that, for any two tabloids $t, s \in T(\lambda)$, we have $\sum\{\bar{\sigma}^*_{s,t} : \sigma \in S\} = \sum\{\bar{\sigma}^*_{s,t} : \ \sigma \in T\}$. Since $\bar{\sigma}^*_{s,t} = 1$ if $\sigma^*(t) = s$ and is zero otherwise, this amounts to showing that $|C_{s,t} \cap S| = |C_{s,t} \cap T|$, where $C_{s,t} = \{\sigma \in S_n : \ \sigma^*(t) = s\}$. Now $C_{s,t}$ is a left coset of the *row stabilizer*

$$R_t = \{\sigma \in S_n : \ \sigma^*(t) = t\} = S_{t[1]} \times S_{t[2]} \times \cdots \times S_{t[k]}$$

of t, say $C_{s,t} = \sigma R_t$.

It suffices to show, then, that the set $R_t \cap \sigma^{-1}H$ contains the same number of odd and even permutations. Let $\pi \in \sigma^{-1}H$. Then for $i \geq k+2$ we have $\pi(i) = \sigma^{-1}(i)$, and $\pi([k+1]) = \{\sigma^{-1}(1), \cdots, \sigma^{-1}(k+1)\}$. Let

$$I_i = t[i] \cap [k+1], \quad J_i = t[i] \cap \{\sigma^{-1}(1), \cdots, \sigma^{-1}(k+1)\} \quad (i = 1, \cdots, k).$$

For $\pi \in \sigma^{-1}H$ to be in R_t, both i and $\sigma^{-1}(i)$ must be in the same row of t for $i \geq k+2$, and we must have $|I_j| = |J_j| \quad (j = 1, \cdots, k)$. If this is not the case, then $R_t \cap \sigma^{-1}H = \emptyset$ and we are trivially done, so assume the tabloid t satisfies these conditions. Then, the set $R_t \cap \sigma^{-1}H$ consists exactly of those permutations π satisfying $\pi(i) = \sigma^{-1}(i) \ \ (i \geq k+2)$ and $\pi(I_i) = J_i \ \ (i = 1, \cdots, k)$, and is therefore a left coset of the subgroup

$$K = S_{I_1} \times \cdots \times S_{I_k} \times S_{\{k+2\}} \times S_{\{k+3\}} \times \cdots \times S_{\{n\}}.$$

Since $\cup_{i=1}^{k} I_i = [k+1]$, there exists some I_m such that $|I_m| \geq 2$, and so it is clear that K contains the same number of even and odd permutations. This completes the proof. □

Combining Corollary 2.4.5 and Lemma 2.4.6, we have the following.

Theorem 2.4.7 *Let $\lambda = (\lambda_1, \cdots, \lambda_k)$ such that $k \geq 2$ and $\lambda_1 \geq \cdots \geq \lambda_k \geq k^2$. Let l denote the largest positive integer for which the Young polytope $P(\lambda)$ is l-neighborly. Then $\lfloor \frac{k^2}{2} \rfloor \leq l < \frac{1}{2}(k+1)!$.*

It is very probable that the set $\{(\lambda, l) : P(\lambda) \text{ is } l\text{-neighborly}\}$ does not admit an efficient decision procedure. It is not even clear if it belongs to the computational complexity class NP or its complement $co - NP$. However, for a fixed k and $\lambda_2, \cdots, \lambda_k$, the following holds.

Proposition 2.4.8 *Let $k \geq 2$ and $\lambda_2 \geq \cdots \geq \lambda_k > 0$, and for $n \geq \lambda_2 + \sum_{i=2}^{k} \lambda_i$, let $\lambda(n) = (n - \sum_{i=2}^{k} \lambda_i, \lambda_2, \cdots, \lambda_k)$.*
Then the set $A = \{(n, l) : P(\lambda(n)) \text{ is } l\text{-neighborly}\}$ is in $co - NP$.

Proof. The crucial observation is that the affine dimension of $P(\lambda(n))$ is bounded from above by $d(n)^2$, where $d(n) = \binom{n}{\lambda} \leq n^{(\sum_{i=2}^{k} \lambda_i)}$. For a pair $(n, l) \notin A$, there exists an l-subset $F \subset S_n$ such that $\bar{F} = \{\bar{\sigma}^* : \sigma \in F\}$ is not a face of $P(\lambda(n))$. Then, by Proposition 2.3.1, there exist $S, T \subset S_n$ such that $S \subseteq F$, $T \not\subseteq F$ and $(\bar{S}, \bar{T})$ is a minimal Radon partition, where $\bar{S} = \{\bar{\sigma}^* : \sigma \in S\}$ and $\bar{T} = \{\bar{\sigma}^* : \sigma \in T\}$. By definition of a minimal Radon partition, $|S \cup T| \leq d(n)^2 + 2$. Also, a matrix $M \in mat(d(n), \mathbb{R})$ exists such that $size(M)$ is bounded by a polynomial function in $d(n)$ and $M \in conv(\bar{S}) \cap conv(\bar{T})$, since the matrices in $\bar{S}, \bar{T}$ are $\{0,1\}$-valued (see [Sch86]). Thus, given $F, S, T \subseteq S_n$ and $M \in mat(d(n), \mathbb{R})$ as above, one can verify that $S \subseteq F$ and $T \not\subseteq F$, construct the corresponding sets of matrices $\bar{S}, \bar{T} \subseteq mat(d(n), \mathbb{R})$, and check that $M \in conv(\bar{S}) \cap conv(\bar{T})$ in time polynomial in $n + l$. □

Finally, we characterize those partitions $\lambda \vdash n$ for which $P(\lambda)$ is 2-neighborly.

Proposition 2.4.9 *For any partition $\lambda \vdash n$ other than (n) and $(n-1,1)$, the Young polytope $P(\lambda)$ is 2-neighborly.*

Proof. The polytope $P((1,1,1))$ being a simplex, we may assume $n \geq 4$. By Lemma 2.4.3, it is enough to exhibit λ-colorings χ_1 and χ_2 for the only two nonisomorphic simple graphs with two edges, $H_1 = ([3], \{\{1,2\},\{1,3\}\})$ and $H_2 = ([4], \{\{1,2\},\{3,4\}\})$, respectively. If $\lambda_1 = 1$, then set $\chi_1(i) = i \ \ (i = 1,2,3)$ and $\chi_2(i) = i \ \ (i = 1, \cdots, 4)$. If $\lambda_1 \geq 2$, set $\chi_i(1) = 2$, $\chi_i(2) = \chi_i(3) = 1 \ \ (i = 1,2)$, and, if $\lambda_2 = 1$ set $\chi_2(4) = 3$, whereas if $\lambda_2 \geq 2$ set $\chi_2(4) = 2$. □

We conclude, in particular, that for $n \geq 4$ the graph of $P((n-2,2))$ is a clique, which is interesting in two respects. First, it provides an example of a sequence of 2-neighborly polytopes on which the linear optimization related decision problem is NP-complete. Second, while the adjacency relation is trivial for this sequence, it is NP-complete for the projected sequence $P((n-2,2), h_n)$ of symmetric traveling salesman polytopes [Pap78].

2.5 Orbit stratifications and a problem of Kozen

We now fix an arbitrary subgroup G of S_d. For any point $x \in \mathbb{R}^d$ we have its orbit $Gx = \{\pi(\sigma)(x) : \ \sigma \in G\}$ under the standard representation $\pi : S_d \to GL(\mathbb{R}^d)$. With each $x \in \mathbb{R}^d$ we associate the polytope $P(G,x) = conv(Gx)$ as before, and the matroid $M(G,x)$ and oriented matroid $O(G,x)$ defined by affine dependencies on the orbit Gx. In order to simplify the discussion, we concentrate on the set $\mathcal{D}(\mathbb{R}^d_+)$ of points in the nonnegative orthant with pairwise distinct coordinates. The orbit of any $x \in \mathcal{D}(\mathbb{R}^d_+)$, which is the underlying set of any of the three structures above, can then be indexed simply by the group G. We say that two polytopes P and Q, having their vertices indexed by G, are (combinatorially) *isomorphic*, written $P \simeq Q$, if there exists a bijection $\varphi : G \to G$ such that a subset $F \subseteq G$ is a face of P if and only if $\varphi(F) = \{\varphi(\sigma) : \ \sigma \in F\}$ is a face of Q.

If this bijection is the identity on G, we use the equality sign $P = Q$. Matroid and oriented matroid isomorphisms are defined in a similar manner.

For $x \in \mathcal{D}(\mathbb{R}^d_+)$, we observe that the orbit Gx lies on an affine hyperplane in $\mathbb{R}^d$, so $M(G,x)$ is also the matroid of *linear* dependencies on the orbit, and similarly for the oriented matroid $O(G,x)$.

The isomorphism type of each of these three structures induces a stratification of affine space $\mathbb{R}^d$. Specifically, two points $x, y \in \mathbb{R}^d$ are in the same *polytope stratum* induced by G when $P(G,x) \simeq P(G,y)$, and are in the same *matroid stratum* (respectively, *oriented matroid stratum*) when $M(G,x) \simeq M(G,y)$ (respectively, $O(G,x) \simeq O(G,y)$). Note that the oriented matroid stratification is a refinement of both of the other two (the face lattice could be read off from the oriented matroid, see [LV80]). One can also consider the stratifications induced by the labeled isomorphism type of each of the three structures.

We say that a point $x = (x_1, \cdots, x_d) \in \mathbb{R}^d$ is *generic*, if $x_1, \cdots, x_d \in \mathbb{R}$ are algebraically independent over the field $\mathbb{Q}$ of rational numbers. The following motivating question was raised by D. Kozen. Is it true that any two generic points $x, y \in \mathbb{R}^d$ lie in the same polytope stratum? It will become evident below that it is natural to restrict attention to generic points.

Let $\mathcal{K} = \mathbb{Q}(X_1, \cdots, X_d)$ be the field of rational functions on the variables $X_1, \cdots, X_d$ with rational coefficients. Define the *generic matroid* $M(G)$ of the subgroup G as the matroid of $\mathcal{K}$-linear dependencies on the set of points $\{(X_{\sigma(1)}, \cdots, X_{\sigma(d)}) : \sigma \in G\} \subseteq \mathcal{K}^d$, indexed, as the orbit matroids, by G. Given a point $x = (x_1, \cdots, x_d) \in \mathcal{D}(\mathbb{R}^d_+)$, the specialization map $\varphi : \mathcal{K} \to \mathbb{Q}(x_1, \cdots, x_d) : X_i \mapsto x_i$ induces a weak map of matroids (see [Kun86]). This can be rephrased as follows.

Proposition 2.5.1 *For any point $x \in \mathcal{D}(\mathbb{R}^d_+)$, the orbit matroid $M(G,x)$ is a* weak image *of the generic matroid $M(G)$; i.e., if $F \subseteq G$ is an independent set of $M(G,x)$, then it is also an independent set of $M(G)$.*

The following corollary is useful in deciding when the orbit matroid of a point $x \in \mathbb{R}^d$ is the generic matroid.

Corollary 2.5.2 *Given a point $x \in \mathcal{D}(\mathbb{R}^d_+)$, if $M(G,x)$ and $M(G)$ have the same number of bases, then $M(G,x) = M(G)$.*

If $x \in \mathbb{R}^d$ is a generic point, then the specialization map above is a field isomorphism. Hence, the induced map of matroids is an isomorphism, yielding the following.

Proposition 2.5.3 *For any generic point $x \in \mathbb{R}^d$ we have $M(G,x) = M(G)$.*

Thus, all generic points lie in the same matroid stratum, and the motivation for considering generic points becomes apparent.

We need to recall a few facts about oriented matroids (see [BLVS+92]). Let O be an oriented matroid of rank r, defined on a finite set G. Its *chirotope* is the signed base map $\chi_O : \binom{G}{r} \to \{-1, 0, 1\}$ on the collection of r-subsets of G, which entirely determines the oriented matroid. In particular, an r-set $F \subseteq G$ is a basis of O if and only if $\chi_O(F) \neq 0$. Now, for $x \in \mathcal{D}(\mathbb{R}^d_+)$ and $F \subseteq G \subseteq S_d$, let $F(x) \in \mathbb{R}^{d \times d}$ be the matrix having column set $\{(x_{\sigma(1)}, \cdots, x_{\sigma(d)}) : \sigma \in F\}$. If $rank(O(G,x)) = d$, then its chirotope is given by

$$\chi_x(F) = \chi_{O(G,x)}(F) = sign(det(F(x))).$$

Finally, we need the following.

Observation 2.5.4 *For any $x \in \mathbb{R}^d$, the orbit polytope $P(G,x)$ is G-symmetric; i.e., for any permutation $\sigma \in G$, the bijection $\sigma : G \to G : \tau \mapsto \sigma\tau$ gives an automorphism of $P(G,x)$. Similarly, $M(G,x)$ and $O(G,x)$ are G-symmetric.*

This is true since the linear transformation $\pi(\sigma) : \mathbb{R}^d \to \mathbb{R}^d$ maps every orbit of G bijectively onto itself. Thus, each of the structures is entirely determined by the *vertex figure* of the identity $e \in G$. For example, the list of those subsets

$F \subseteq G$ containing e which are faces of $P(G,x)$ determines the entire face lattice of $P(G,x)$.

We are now in a position to provide the negative answer to Kozen's question.

Theorem 2.5.5 *There exists a subgroup G of S_6, isomorphic to S_4, and two generic points $x, y \in \mathbb{R}^6$ for which $M(G,x) = M(G,y)$, yet $P(G,x) \not\cong P(G,y)$ and $O(G,x) \not\cong O(G,y)$.*

Proof. Let $\lambda = (2,2) \vdash 4$, and let $G = S_4^*$ be the subgroup of $S_{T(\lambda)}$ induced by the λ-Young representation of S_4. Identifying $T(\lambda)$ with $[6] = \{1, \cdots, 6\}$ by sending a tabloid t with $t[2] = \{i,j\}$ $(i < j)$ to $4(i-1) - \frac{i}{2}(i+1) + j \in [6]$, we turn G into a subgroup of S_6.

Using symbolic computation, it was verified for the generic matroid that $rank(M(G)) = 6$, and that 679 of the 6-subsets of G containing the identity $e \in G$ are not bases of $M(G)$.

Similarly, for $u = (1, 10, 11, 30, 70, 90)$ and $v = (19, 5, 83, 29, 67, 37)$, it was verified that $rank(M(G,u)) = rank(M(G,v)) = 6$ and each of these two matroids has 679 nonbasic 6-subsets containing e as well.

It follows from Observation 2.5.4 and Corollary 2.5.2 that $M(G,u) = M(G) = M(G,v)$. Now, consider the chirotope χ_u of $O(G,u)$. If a 6-subset $F \subseteq G$ is a basis of $M(G)$, it is also a basis of $M(G,u)$, so $\chi_u(F) \neq 0$, implying $det(F(u)) \neq 0$. Thus, by continuity of the determinant function, and since the set of generic points is dense in $\mathbb{R}^6$, we can perturb u slightly to get a generic point $x \in \mathbb{R}^6$ such that, for any $F \in \binom{G}{6}$ which is a basis of $M(G)$, we have $\chi_x(F) = sign(det(F(x))) = sign(det(F(u))) = \chi_u(F)$. If $F \in \binom{G}{6}$ is not a basis of $M(G)$, then by Proposition 2.5.1 it is neither a basis of $M(G,u)$ nor of $M(G,x)$, so $\chi_x(F) = 0 = \chi_u(F)$. Thus, the chirotopes χ_x, χ_u are identical, showing that $O(G,x) = O(G,u)$. Similarly, we can perturb v to obtain a generic point $y \in \mathbb{R}^6$ such that $O(G,y) = O(G,v)$.

It follows that $P(G,x) = P(G,u)$ and $P(G,y) = P(G,v)$, as well.

Now, the facets of $P(G,u)$ and $P(G,v)$ containing the identity e were obtained. In $P(G,u)$ there are 4 such facets containing 8 vertices each, 17 facets containing 6 vertices each, and 20 facets containing 5 vertices each. Appealing to Observation 2.5.4 and recalling $|G| = 24$, by counting vertex-facet incidences separately for facets containing 8, 6 or 5 vertices each, we get that $P(G,u)$ has $\frac{24\cdot 4}{8}+\frac{24\cdot 17}{6}+\frac{24\cdot 20}{5} = 176$ facets.

Similarly, $P(G,v))$ has 6 such facets containing 8 vertices each, 8 facets containing 6 vertices each, and 5 facets containing 5 vertices each, and it turns out to have 74 facets.

Thus, $P(G,x) \not\cong P(G,y)$ and hence also $O(G,x) \not\cong O(G,y)$ and, furthermore, even the number of faces of the same dimension of $P(G,x)$ and $P(G,y)$ are not the same. □

Thus, in general, both the polytope and oriented matroid stratifications of $\mathbb{R}^d$ induced by G, are nontrivial on the set of generic points.

We remark that the $(2,2)$-Young representation $\pi_{(2,2)} : S_4 \to S_6$ is the direct sum of three mutually nonisomorphic irreducible representations of S_4, so our example shows that these stratifications are nontrivial even if the underlying representation is multiplicity-free.

2.6 Discussion

This chapter raises many questions, and much work remains to be done. It would be nice to obtain a more complete characterization of pairs (λ, l) for which $P(\lambda)$ is l-neighborly. Surely, using the sufficient condition derived through Proposition 2.3.2 and Lemmas 2.4.1 and 2.4.3 would not be enough. Yet, even obtaining the most to be gained from this condition, namely, characterizing those pairs (λ, l) for which every graph with l edges is λ-colorable, seems a challenging graph theoretical question. A first step might be to consider the computational complexity of the

set $\{(\lambda, l) :\ P(\lambda)$ is l-neighborly$\}$, which at first glance seems to be neither in NP nor in $co - NP$.

The polytope stratifications induced by Young representations are far from being understood. It is particularly interesting to consider sequences of polytope fibers for which the associated decision problems have different computational complexities, arising from the same sequence of polytope bundles, such as $P((n-2,2), m_n)$ and $P((n-2,2), h_n)$, $n \geq 4$. It would be very interesting to understand more fully the way in which the polytopes in the first, tractable sequence, continuously deform into the corresponding polytopes in the second, intractable sequence, when following a uniformly specified sequence of paths $p_n : [0,1] \to [m_n, h_n]$ in the base spaces.

Another interesting direction is to investigate the generic matroid $M(G)$ associated with each subgroup G of S_n.

The general problem is the study of the representation polytope $P(\rho) = conv(\{\rho(g) :\ g \in G\})$ and the orbit polytopes $P(\rho, x) = conv(\{\rho(g)(x) :\ g \in G\})$, $x \in \mathbb{R}^d$, where $\rho : G \to GL(\mathbb{R}^d)$ is any real representation of any finite group G. We have shown that, in order for such a representation to have a trivial polytope stratification on the set of generic points, being multiplicity-free is not sufficient. The next question is, obviously, whether or not the representation being *irreducible* does suffice.

Chapter 3

Graded Modules and Hilbert Series of Group Representations

3.1 Introduction

Given a matrix representation $\rho \longrightarrow GL_d(\mathcal{K})$ of a finite group G over a field $\mathcal{K}$, the orbit of an element $v \in \mathcal{K}^d$ under G is $Gv = \{\rho(g)v : g \in G\}$. There is a variety of categories from which objects could be naturally assigned to points via their orbits. The space $\mathcal{K}^d$ is then stratified into the equivalence classes of points which are assigned isomorphic objects in the category considered.

In the previous chapter, $\mathcal{K}$ was the field $\mathbb{R}$ of real numbers, and the category considered was that of finite partially ordered sets with order preserving maps among them. The object assigned to a point was the face lattice of the convex hull of its orbit $conv(Gv)$, resulting in the *polytope stratification* of $\mathbb{R}^d$. Also, the group was specialized to the symmetric group $G = S_n$. The resulting stratifications of $\mathbb{R}^d$ are of special interest from a computational complexity point of view, as many combinatorial optimization problems could be formulated in terms of these orbit polytopes.

In the study of the polytope stratifications, other stratifications induced by

assigning oriented matroids and matroids to points, are useful. In the matroid stratification, all generic points lie in the same class. As it turns out, their common *generic* orbit matroid could be defined in the following way. Let $x = (x_1, \cdots, x_n)$ and $\mathcal{A} = \mathcal{K}[x_1, \cdots, x_n]$. Let $\mathcal{A}^n$ be the $\mathcal{A}$-module of n-tuples (column vectors) of polynomials $p = (p_1, \cdots, p_n)$ in $\mathcal{A}$. A matrix $T \in GL_n(\mathcal{K})$ acts on $\mathcal{A}^n$ by sending the vector of polynomials $p = (p_1, \cdots, p_n) \in \mathcal{A}^n$ to the matrix product Tp. Given a matrix representation $\rho : G \longrightarrow GL_n(\mathcal{K})$, we then get an induced action on $\mathcal{A}^n$. For each $p \in \mathcal{A}^n$ we have its orbit $Gp = \{\rho(g)p : \ g \in G\}$. The generic matroid is the matroid on the orbit Gx of $x \in \mathcal{A}^n$, where a k-subset of Gx is independent if the $\mathcal{A}$-submodule of $\mathcal{A}^n$ it generates is free of rank k.

A first step in studying these submodules, is to understand the submodule generated by the entire orbit Gx. This is the subject of this chapter. As it turns out, these objects provide a new and interesting link between computer algebra and representation theory, with possible applications.

In studying these objects, it is very helpful to be able to change the basis of the representation space at will, resulting in an equivalent matrix representation. To show that our modules are invariant under such a basis change, it is best to define in an invariant way a graded module $M(\pi)$ for any *linear* representation $\pi : G \longrightarrow GL(V)$. It is then shown that, for any choice of basis of V, the submodule of $\mathcal{A}^n$ generated by the orbit of x under the resulting matrix realization of π could be identified with $M(\pi)$.

Our module $M(\pi)$ is $\mathbb{N}$-graded, and we will be most interested in its Hilbert series $H(\pi, t) = H(M(\pi), t)$, which turns out to be an interesting invariant of the linear representation, and may be used, via symbolic computation, to recover other invariants of the representation as follows. Suppose a matrix representation ρ is given, the representation theoretical properties of which are unknown. Having as little information as an explicit list of matrices in $\rho(G) \subset GL_n(\mathcal{K}) \subset \mathcal{K}^{n \times n}$ which span the matrix space $span_{\mathcal{K}}(\rho(G))$ of ρ, its Hilbert series could be evaluated using

symbolic computation. Comparing it with the general expression for the Hilbert series of a representation derived in this work, part of the desired information could be obtained. If, in addition, ρ is known to be multiplicity-free, then the dimensions of all of its irreducible components could be recovered in this way.

Our results hold over algebraically closed fields. In some cases of interest, such as representations of the symmetric group, these results hold over the reals and rationals as well, since it is known [Jam78] that all irreducible complex representation of S_n could be rationally coordinatized.

The rest of this chapter is organized as follows. After some preliminaries, the symmetric algebra $\mathcal{S}(V^*)$ is considered and the module $M(\pi)$ of a linear representation π is defined as a graded $\mathcal{S}(V^*)$-module in Section 3.3. It is shown that for each choice of basis of V, turning π into a matrix representation, the submodule of $\mathcal{A}^n$ generated by the resulting orbit of x could be identified with $M(\pi)$.

In Section 3.4, we provide a canonical decomposition of $M(\pi)$ into a direct sum of certain graded *generic* modules $M(r,c)$, $(r,c \in \mathbb{N})$, based on the decomposition of π into irreducible representations. The proof is based on the appropriate choice of basis of V and the investigation of the matrix space of the resulting matrix representation. The Hilbert series $H(\pi,t)$ is then a certain weighted sum of Hilbert series of generic modules. This expression is worked out in Section 3.5 using some fundamentals of the theory of Gröbner bases. In Section 3.6, an explicit formula for $H(\pi,t)$ is derived when π is a multiplicity-free representation, and it is proved that in this case the dimensions of the irreducible components of π could be uniquely recovered from $H(\pi,t)$.

The generic modules, which were studied in a homological context in [BE75], are of special interest. In Section 3.7, we raise a conjecture, currently being investigated by the author, of certain sets being Gröbner bases for these modules. These bases will provide an easy way of computing the Hilbert series of generic modules, resulting in an explicit formula for $H(\pi,t)$ for an arbitrary π.

3.2 Preliminaries

As general references on graded algebras and modules, we mention [AM69], [Fed69], and [Sta83], but most relevant definitions and properties will be given here. For representations of finite groups consult [Vin89] and [CR62].

Throughout this chapter $\mathcal{K}$ is an algebraically closed field and G is a finite group whose order is not divisible by $char(\mathcal{K})$. Also, $\mathcal{A} = \mathcal{K}[x_1, \cdots, x_n]$ is the $\mathcal{K}$-algebra of polynomials in n indeterminates, and $x = (x_1, \cdots, x_n)$. A monomial in $\mathcal{A}$ with *exponent vector* $a = (a_1, \cdots, a_n) \in \mathbb{N}^n$ is an element $x^a = \Pi_{i=1}^n x_i^{a_i} \in \mathcal{A}$. The set of monomials forms a $\mathcal{K}$-vector space basis for $\mathcal{A}$. As a $\mathcal{K}$-space, $\mathcal{A}$ admits a direct sum decomposition $\mathcal{A} = \oplus_{d\in\mathbb{N}}\mathcal{A}_d$, where $\mathcal{A}_d$ is the subspace of homogeneous polynomials of degree d, which we call *d-forms* for brevity. This decomposition satisfies $\mathcal{A}_0 = \mathcal{K}$ and $\mathcal{A}_i\mathcal{A}_j \subseteq \mathcal{A}_{i+j}$ $(i, j \in \mathbb{N})$, turning $\mathcal{A}$ into a *graded $\mathcal{K}$-algebra.* Analogously, an $\mathcal{A}$-module M is a *graded $\mathcal{A}$-module* if it has a $\mathcal{K}$-space decomposition $M = \oplus_{d\in\mathbb{N}}M_d$, with the property $\mathcal{A}_iM_j \subseteq M_{i+j}$ $(i, j \in \mathbb{N})$. The elements in M_d are called *homogeneous of degree d.* Given two graded $\mathcal{A}$-modules M^1 and M^2, a map $\Phi : M^1 \longrightarrow M^2$ is *graded* if $\Phi(M_d^1) \subseteq M_d^2$ for all $d \in \mathbb{N}$. If Φ is an $\mathcal{A}$-module homomorphism and is graded, then it is a *map of graded $\mathcal{A}$-modules*, and if it has an inverse which is also a map of graded $\mathcal{A}$-modules, then it is an *isomorphism of graded $\mathcal{A}$-modules.* We denote by $Aut(M)$ the subgroup of $Hom_{\mathcal{A}}(M, M)$ consisting of all isomorphisms of graded $\mathcal{A}$-modules from M onto itself. A submodule N of M is *graded* if it is generated by homogeneous elements in M, in which case it inherits the grading $N_d = N \cap M_d$. If N is a graded submodule of M then its quotient is also graded by letting $(M/N)_d$ be the quotient of $\mathcal{K}$-spaces M_d/N_d. If M^1, M^2 are graded $\mathcal{A}$-modules, then their direct sum is graded by letting $(M^1 \oplus M^2)_d$ be the $\mathcal{K}$-space direct sum $M_d^1 \oplus M_d^2$.

The *Hilbert series* of a graded module M (or a graded $\mathcal{K}$-algebra) is the dimension generating function $H(M, t) = \sum_{d\in\mathbb{N}} dim_{\mathcal{K}}(M_d)t^d \in \mathbb{Z}[[t]]$. For example, the Hilbert series of $\mathcal{A}$ itself is $H(\mathcal{A}, t) = \frac{1}{(1-t)^n}$, where $\frac{1}{(1-t)^n}$ denotes the in-

verse of $(1-t)^n$ in the ring of power series $\mathbb{Z}[[t]]$. By definition of the gradings of a quotient and a direct sum, if M^1 and M^2 are two graded $\mathcal{A}$-modules then $H(M^1 \oplus M^2, t) = H(M^1, t) + H(M^2, t)$ and if N is a graded submodule of M then $H(N,t) = H(M,t) - H(M/N,t)$. It is clear that the Hilbert series is invariant under isomorphism of graded $\mathcal{A}$-modules.

Let $\mathcal{K}^n$ be the space of n-tuples of elements in $\mathcal{K}$. We denote by $U = \{u_1, \cdots, u_n\}$ its standard basis of unit column vectors. The group $GL(\mathcal{K}^n)$ of invertible linear transformations of $\mathcal{K}^n$ is identified with the group of invertible $n \times n$ matrices $GL_n(\mathcal{K})$, so the image of $v \in \mathcal{K}^n$ under $T \in GL_n(\mathcal{K})$ is the matrix product Tv.

A *matrix representation* of a group G (over $\mathcal{K}$) is a homomorphism $\rho : G \longrightarrow GL_n(\mathcal{K})$. A *linear representation* of a group G is a homomorphism $\pi : G \longrightarrow GL(V)$ where V is some $\mathcal{K}$-vector space. The *dimension* of π is $dim(\pi) = dim_{\mathcal{K}}(V)$. If V is finite dimensional with $dim(V) = n$, then any choice of basis of V identifies V with $\mathcal{K}^n$ and $GL(V)$ with $GL_n(\mathcal{K})$, turning π into a matrix representation.

3.3 The graded module of a linear representation

Let $U = \{u_1, \cdots, u_d\}$ be the standard basis of $\mathcal{K}^d$ as above, and let $\mathcal{A}^d$ be the free $\mathcal{A}$-module of rank d generated formally by U. Thus,

$$\mathcal{A}^d = \{\textstyle\sum_{i=1}^d p_i u_i = (p_1, \cdots, p_d) : \ p_1, \cdots, p_d \in \mathcal{A}\}$$

is the $\mathcal{A}$-module consisting of d-tuples of polynomials in $\mathcal{A}$. It is graded naturally by $\mathcal{A}_s^d = \{\sum_{i=1}^d p_i u_i : \ p_1, \cdots, p_d \in \mathcal{A}_s\}$. In particular, $\mathcal{A}_0^d = span_{\mathcal{K}}(U) = \mathcal{K}^d$ is the vector space we started with. A *monomial* in $\mathcal{A}^d$ is an element of the form $x^a u_i$ where $a \in \mathbb{N}^n$ and $i \in [d]$. The set of monomials forms a $\mathcal{K}$-space basis for $\mathcal{A}^d$.

Each invertible matrix $T \in GL_d(\mathcal{K})$ gives an isomorphism of graded $\mathcal{A}$-modules $T : \mathcal{A}^d \longrightarrow \mathcal{A}^d : u_i \mapsto Tu_i$, the inverse being provided by T^{-1}. Given an arbitrary $p = \sum_{j=1}^d p_j u_j \in \mathcal{A}^d$, its image under T

$$Tp = \sum_{j=1}^d p_j T u_j = \sum_{j=1}^d p_j \sum_{i=1}^d T_{i,j} u_i = \sum_{i=1}^d (\sum_{j=1}^d T_{i,j} p_j) u_i$$

is the matrix product of T and the d-tuple (column vector) $p = (p_1, \cdots, p_d)$. Given a matrix representation $\rho : G \longrightarrow GL_d(\mathcal{K})$ of a finite group G, we get an induced representation $\rho : G \longrightarrow Aut(\mathcal{A}^d)$.

We now let $d = n$. For each $p \in \mathcal{A}^n$ we let $M(\rho, p)$ be the $\mathcal{A}$-submodule of $\mathcal{A}^n$ generated by its orbit $Gp = \{\rho(g)p : \ g \in G\}$. If p is a homogeneous element of degree s in $\mathcal{A}^n$ then $Gp \subset \mathcal{A}_s^n$ and $M(\pi, p)$ is graded. Now, regarding $x = (x_1, \cdots, x_n)$ as the vector $\sum_{i=1}^n x_i u_i \in \mathcal{A}_1^n$, we define the graded $\mathcal{A}$-module of the matrix representation ρ to be $M(\rho) = M(\rho, x)$.

Two matrix representations $\rho_1, \rho_2 : G \longrightarrow GL_n(\mathcal{K})$ are *equivalent* if there exists a matrix $T \in GL_n(\mathcal{K})$ such that for all $g \in G$ we have $\rho_2(g) = T^{-1}\rho_1(g)T$. We would like to show that equivalent matrix representations give equivalent modules. For this, we now redefine the module of a linear representation in an invariant way.

Let V be an n-dimensional $\mathcal{K}$-vector space. Recall that its *dual* is the n-dimensional $\mathcal{K}$-space V^* of linear functions from V to $\mathcal{K}$. For each basis $E = \{e_1, \cdots, e_n\}$ of V there is a unique *dual basis* $E^* = \{e_1^*, \cdots, e_n^*\}$ of V^* such that $e_i^*(e_j) = \delta_{i,j}$ (Kronecker function). For each map $T \in GL(V)$ there is a dual map $T^* \in GL(V^*)$ defined by $(T^*(e_i^*))(e_j) = e_i^*(T(e_j))$. If T^E is the matrix of $T \in GL(V)$ with respect to the basis E, then its transpose $(T^E)'$ is the matrix of the dual map T^* with respect to the dual basis E^*. If E and F are two bases of V and $T \in GL(V)$ is the base-changing map from E to F, then $(T^{-1})^* \in GL(V^*)$ is the base-changing dual map from the dual basis E^* to F^*.

Let $\mathcal{S}(V^*) = \oplus_{d \in \mathbb{N}} \mathcal{S}_d(V^*)$ be the graded *symmetric algebra* of the space V^* (see [Fed69]). Thus, any basis $E^* = \{e_1^*, \cdots, e_n^*\}$ of V^* generates $\mathcal{S}(V^*)$ freely as a $\mathcal{K}$-algebra, and the dth summand $\mathcal{S}_d(V^*)$ is the $\mathcal{K}$-span of formal monomials

$\Pi_{i=1}^{n} e_i^{*a_i}$ of degree d. In particular $\mathcal{S}_1(V^*) = V^*$ and $\mathcal{S}_0(V^*) = \mathcal{K}$. Let $\mathcal{M} = \mathcal{S}(V^*) \otimes V$ (tensor products are over $\mathcal{K}$ unless otherwise indicated). This is a graded $\mathcal{S}(V^*)$-module, with scalar multiplication given by $s(t \otimes v) = (st) \otimes v$ for $s, t \in \mathcal{S}(V^*)$ and $v \in V$, and grading $\mathcal{M}_d = \mathcal{S}_d(V^*) \otimes V$. Any basis $E = \{e_1, \cdots, e_n\}$ of V gives an $\mathcal{S}(V^*)$-basis $\{1 \otimes e_1, \cdots, 1 \otimes e_n\}$ of $\mathcal{M}$, hence $\mathcal{M}$ is free of rank n.

Given a map $T \in GL(V)$, we claim that the map

$$\mathbf{1} \otimes T : \mathcal{M} \longrightarrow \mathcal{M} : p \otimes v \mapsto p \otimes T(v)$$

is an isomorphism of graded $\mathcal{S}(V^*)$-modules. Indeed, it is clear that it is graded and has the graded inverse $\mathbf{1} \otimes T^{-1}$, and, given an element $p \otimes v \in \mathcal{M}$ and $q \in \mathcal{S}(V^*)$, we have

$$\begin{aligned} (\mathbf{1} \otimes T)(q(p \otimes v)) &= (\mathbf{1} \otimes T)((qp) \otimes v) \\ &= (qp) \otimes T(v) = q(p \otimes T(v)) = q((\mathbf{1} \otimes T)(p \otimes v)). \end{aligned}$$

Thus, given a linear representation $\pi : G \longrightarrow GL(V)$, we get a representation

$$\mathbf{1} \otimes \pi : G \longrightarrow Aut(\mathcal{M}) : g \mapsto \mathbf{1} \otimes \pi(g).$$

For each $y \in \mathcal{M}$ we let $M(\pi, y)$ be the $\mathcal{S}(V^*)$-submodule of $\mathcal{M}$ generated by its orbit $G(y) = \{(\mathbf{1} \otimes \pi(g))(y) : \ g \in G\}$. If y is a homogeneous element of degree d in $\mathcal{M}$ then $G(y) \subset \mathcal{M}_d$ and $M(\pi, y)$ is graded.

We now show that there exists a distinguished element $e \in \mathcal{M}_1 = V^* \otimes V$ which will make it possible to define invariantly the graded module of π as $M(\pi) = \mathcal{M}(\pi, e)$. Note that, viewing $V^* \otimes V$ as the space of bilinear functions from $V^* \times V$ to $\mathcal{K}$, we have an isomorphism of $\mathcal{K}$-spaces $\Psi : Hom_{\mathcal{K}}(V, V) \longrightarrow V^* \otimes V$ sending $T \in Hom_{\mathcal{K}}(V, V)$ to $\Psi(T) : V^* \times V \longrightarrow \mathcal{K} : (u^*, v) \mapsto u^*(T(v))$; the distinguished element e is then the image under Ψ of the identity map in $Hom_{\mathcal{K}}(V, V)$.

Proposition 3.3.1 *There exists a distinguished nonsimple tensor $e \in \mathcal{M}_1$ which, for any basis $E = \{e_1, \cdots, e_n\}$ of V and its dual basis $E^* = \{e_1^*, \cdots, e_n^*\}$ of V^*, equals $\sum_{j=1}^{n} e_j^* \otimes e_j$.*

Proof. Let $E = \{e_1, \cdots, e_n\}$ and $F = \{f_1, \cdots, f_n\}$ be two arbitrary bases of V and let E^* and F^* be the corresponding dual bases of V^*. Let $T \in GL(V)$ be the base-changing map from E to F, so that the base changing dual map from E^* to F^* is $(T^{-1})^*$. Let $T^E = (T^E_{i,j})$ be the matrix of T with respect to E. Then $(T^E)^{-1}$ is the matrix of T^{-1} with respect to E, and $((T^E)^{-1})'$ is the matrix of $(T^{-1})^*$ with respect to E^*. Then

$$\begin{aligned}
\sum_{j=1}^{n} e_j^* \otimes e_j &= \sum_{j=1}^{n} e_j^* \otimes (TT^{-1})(e_j) = \sum_{j=1}^{n} e_j^* \otimes T(\sum_{i=1}^{n} (T^E)^{-1}_{i,j} e_i) \\
&= \sum_{j=1}^{n} e_j^* \otimes \sum_{i=1}^{n} (T^E)^{-1}_{i,j} T(e_i) = \sum_{i=1}^{n} \sum_{j=1}^{n} (T^E)^{-1}_{i,j} e_j^* \otimes f_i \\
&= \sum_{i=1}^{n} \sum_{j=1}^{n} ((T^E)^{-1})'_{j,i} e_j^* \otimes f_i = \sum_{i=1}^{n} (T^{-1})^*(e_i^*) \otimes f_i \\
&= \sum_{i=1}^{n} f_i^* \otimes f_i,
\end{aligned}$$

and we are done. □

The following definition is now justified.

Definition 3.3.2 The *graded module* $M(\pi)$ of a linear representation $\pi : G \longrightarrow GL(V)$, where G is a finite group and V is a finite dimensional $\mathcal{K}$-space, is the graded $\mathcal{S}(V^*)$-submodule $M(\pi, e)$ of $\mathcal{M}$. The *Hilbert series* $H(\pi, t)$ of π is $H(M(\pi), t)$.

Now, any choice of basis $E = \{e_1, \cdots, e_n\}$ of V turns the linear representation $\pi : G \longrightarrow GL(V)$ into a matrix representation $\rho : G \longrightarrow GL_n(\mathcal{K})$. Let $M(\pi)$ be the graded $\mathcal{S}(V^*)$-submodule of $\mathcal{M}$ as above, and let $M(\rho)$ be the graded $\mathcal{A}$-submodule of $\mathcal{A}^n$ generated by the orbit Gx of x under ρ as in the beginning of this section. We have a unit preserving isomorphism of graded $\mathcal{K}$-algebras

$$\phi : \mathcal{S}(V^*) \longrightarrow \mathcal{A} : e_i^* \mapsto x_i$$

turning $\mathcal{A}^n$ into a graded $\mathcal{S}(V^*)$-module with the scalar multiplication $p(v) = \phi(p) \cdot v$ for $p \in \mathcal{S}(V^*)$ and $v \in \mathcal{A}^n$. We then have an isomorphism of

graded $\mathcal{S}(V^*)$-modules $\Phi : \mathcal{A}^n \longrightarrow \mathcal{M} : u_i \mapsto 1 \otimes e_i$. The following proposition establishes the desired connection between $M(\rho)$ and $M(\pi)$.

Proposition 3.3.3 *The module $M(\rho)$, regarded as a graded $\mathcal{S}(V^*)$-module via the map $\phi : \mathcal{S}(V^*) \longrightarrow \mathcal{A}$ above, is isomorphic as a graded $\mathcal{S}(V^*)$-module to $M(\pi)$.*

Proof. Let T be an arbitrary map in $GL(V)$, and let T^E be its matrix with respect to the basis E. Recall that $x = \sum_{j=1}^n x_j u_j \in \mathcal{A}^n$ and $e = \sum_{j=1}^n e_j^* \otimes e_j \in \mathcal{M}$. Then

$$\begin{aligned}
\Phi(T^E x) &= \Phi(\sum_{i=1}^n (\sum_{j=1}^n T_{i,j}^E x_j) u_i) = \Phi(\sum_{i=1}^n \phi^{-1}(\sum_{j=1}^n T_{i,j}^E x_j)(u_i)) \\
&= \Phi(\sum_{i=1}^n (\sum_{j=1}^n T_{i,j}^E e_j^*)(u_i)) = \sum_{i=1}^n (\sum_{j=1}^n T_{i,j}^E e_j^*)(\Phi(u_i)) \\
&= \sum_{i=1}^n (\sum_{j=1}^n T_{i,j}^E e_j^*)(1 \otimes e_i) = \sum_{i=1}^n (\sum_{j=1}^n T_{i,j}^E e_j^*) \otimes e_i \\
&= \sum_{j=1}^n e_j^* \otimes \sum_{i=1}^n T_{i,j}^E e_i = \sum_{j=1}^n e_j^* \otimes T(e_j) \\
&= (\mathbf{1} \otimes T)(\sum_{j=1}^n e_j^* \otimes e_j) = (\mathbf{1} \otimes T)(e).
\end{aligned}$$

Thus, the set of generators $\{\rho(g)x : g \in G\}$ of $M(\rho)$ is mapped under Φ onto the set of generators $\{(\mathbf{1} \otimes \pi(g))(e) : g \in G\}$ of $M(\pi)$. Since Φ is an isomorphism of graded $\mathcal{S}(V^*)$-modules, this ends the proof. □

3.4 Generic modules and canonical decompositions

Our assumption throughout that G is a finite group whose order is not divisible by the characteristic of the field $\mathcal{K}$ implies (see [CR62, Maschke's Theorem]) that any linear representation π of G over $\mathcal{K}$ is *completely reducible*, i.e., can be written as a direct sum of irreducible representations of G. Let $\pi : G \longrightarrow GL(V)$ be a linear representation with decomposition $\pi = \oplus_{i=1}^k \pi_i$ into isotypic components

$\pi_i = m_i\chi_i$. Thus, the χ_i are pairwise nonisomorphic irreducible representations of G, and we let $dim(\chi_i) = n_i$. We will now choose a basis for V in a way that will make it easy to study the matrix space of π and provide a canonical decomposition of our module into a direct sum of certain *generic* modules. From here on, we regard π also as a matrix representation under this choice of basis, and $M(\pi)$ also as the $\mathcal{A}$-submodule of $\mathcal{A}^n$ generated by the orbit Gx. We remark that the discussion below could alternatively be carried on in the invariant language of Section 3.3, leaving the choice of basis for the stage of analyzing the generic modules defined below.

We choose a basis of V so that, identifying V with $\mathcal{K}^n$ via the standard basis U of $\mathcal{K}^n$, we get a decomposition into π-invariant subspaces

$$\mathcal{K}^n = \oplus_{i=1}^{k} \oplus_{j=1}^{m_i} span_{\mathcal{K}}\{u_s : \ s \in I_{i,j}\},$$

where the $I_{i,j}$ form a partition of $[n]$ and $|I_{i,j}| = n_i$ for each $i \in [k]$ and $j \in [m_i]$. Each matrix $T = \pi(g)$ has a corresponding block decomposition, where the (i,j)th block $T^{i,j}$ is the restriction of T to the rows and columns indexed by $I_{i,j}$, and is the matrix assigned to g under the jth copy of χ_i. Letting $I_{i,j} = \{r_{i,j}^1, \cdots, r_{i,j}^{n_i}\}$, we have for any $i \in [k]$ and $j_1, j_2, \in [m_i]$ a bijection between I_{i,j_1} and I_{i,j_2}. This induces a bijection between the rows and columns of T^{i,j_1} and those of T^{i,j_2}, and we specialize the choice of basis further so that $T^{i,j_1} = T^{i,j_2}$.

Having $\pi(G) \subset GL_n(\mathcal{K}) \subset \mathcal{K}^{n\times n}$ (the space of $n \times n$ matrices), the *matrix space* of π is the subspace $span_{\mathcal{K}}(\pi(G))$ of $\mathcal{K}^{n\times n}$. The following representation theoretical fact is crucial [Vin89, §4.5, Corollaries 1, 5], [CR62, Theorem of Frobenius and Schur (27.8)].

Proposition 3.4.1 *Let π be a matrix representation with decomposition as above. Then the dimension of the matrix space of π is*

$$dim_{\mathcal{K}}(\pi(G)) = \sum_{i=1}^{k} dim^2(\chi_i) = \sum_{i=1}^{k} n_i^2.$$

We call an $\mathcal{A}$-module M *standard* if it is graded and generated by elements in M_1. The module $M(\pi)$ is a standard submodule of $\mathcal{A}^n$. If M is standard then $M_0 = 0$, so any generating set of M must contain a $\mathcal{K}$-basis of M_1. On the other hand, any basis of M_1 already generates the standard module M. We summarize this below.

Observation 3.4.2 *A subset S of a standard $\mathcal{A}$-module M minimaly generates M as an $\mathcal{A}$-module if and only if it is a $\mathcal{K}$-space basis of M_1.*

Let $\{w_{i,j} : 1 \leq i,j \leq n\}$ be the standard basis of the space $\mathcal{K}^{n\times n}$ of matrices, and note that $\{x_i u_j : 1 \leq i,j \leq n\}$ is a $\mathcal{K}$-basis for $\mathcal{A}_1^n$. Thus, we have a $\mathcal{K}$-isomorphism $\psi : \mathcal{A}_1^n \longrightarrow \mathcal{K}^{n\times n} : x_j u_i \mapsto w_{i,j}$. We can already obtain some information on the Hilbert series of π.

Proposition 3.4.3 *Let π be a representation with decomposition as above. A subset $S \subset M(\pi)$ minimally generates $M(\pi)$ as an $\mathcal{A}$-module if and only if $S \subset \mathcal{A}_1^n$ and $\psi(S)$ is a $\mathcal{K}$-basis for the matrix space $span_{\mathcal{K}}(\pi(G))$ in $\mathcal{K}^{n\times n}$. In particular, the minimum number of generators of $M(\pi)$ is*

$$\frac{d}{dt}H(\pi,t)\mid_{t=0} = dim_{\mathcal{K}}(M(\pi)_1) = \sum_{i=1}^{k} n_i^2.$$

Proof. Consider a matrix $T \in GL_n(\mathcal{K})$ and recall $x = (x_1, \cdots, x_n) \in \mathcal{A}^n$. Then

$$\psi(Tx) = \psi(\sum_{i=1}^{n}\sum_{j=1}^{n} T_{i,j}x_j u_i) = \sum_{i=1}^{n}\sum_{j=1}^{n} T_{i,j}\psi(x_j u_i) = \sum_{i=1}^{n}\sum_{j=1}^{n} T_{i,j}w_{i,j} = T.$$

Thus, ψ maps the set $\{\pi(g)x : g \in G\}$, which is a $\mathcal{K}$-spanning set of $M(\pi)_1$, onto the set $\{\pi(g) : g \in G\}$ spanning the matrix space of π in $\mathcal{K}^{n\times n}$. Hence $M(\pi)_1$ and $span_{\mathcal{K}}(\pi(G))$ are $\mathcal{K}$-isomorphic. By Observation 3.4.2, a subset $S \subset M(\pi)$ minimally generates $M(\pi)$ if and only if it is a $\mathcal{K}$-basis of $M(\pi)_1$, which is true if and only if its image $\psi(S)$ is a basis of the matrix space of π in $\mathcal{K}^{n\times n}$. In particular, the minimum number of generators of $M(\pi)$ as an $\mathcal{A}$-module equals the $\mathcal{K}$-dimension of the matrix space of π, which is given by Proposition 3.4.1. □

Having chosen the basis for V as described above, it follows from Proposition 3.4.1 that the matrix space of π in $\mathcal{K}^{n\times n}$ has the basis

$$\{\textstyle\sum_{j=1}^{m_i} w_{r_{i,j}^s, r_{i,j}^t} : \ i \in [k],\ s,t \in [n_i]\}.$$

By Proposition 3.4.3, a minimal generating set for $M(\pi)$ is its inverse image under ψ, that is, the set

$$\{\textstyle\sum_{j=1}^{m_i} x_{r_{i,j}^t} u_{r_{i,j}^s} : \ i \in [k],\ s,t \in [n_i]\}.$$

For $i \in [k]$ and $s \in [n_i]$, let $V_{i,s} = \{\sum_{j=1}^{m_i} x_{r_{i,j}^t} u_{r_{i,j}^s} : \ t \in [n_i]\}$. The elements in $V_{i,s}$ involve only basis elements in the set $\{u_{r_{i,1}^s}, \cdots, u_{r_{i,m_i}^s}\}$, so $V_{1,1}, \cdots, V_{k,n_k}$ involve pairwise disjoint sets of elements from the basis $\{u_1, \cdots, u_n\}$. It follows that $M(\pi) = \oplus_{i=1}^{k} \oplus_{s=1}^{n_i} M_{i,s}$, a direct sum of graded $\mathcal{A}$-modules, where $M_{i,s}$ is the standard $\mathcal{A}$-module generated by $V_{i,s}$.

Now, consider any $V_{i,s}$. Assume that $r_{i,j}^s = j$ for $j = 1, \cdots, m_i$, and for $j \in [m_i]$ and $t \in [n_i]$ let $x_{j,t} = x_{r_{i,j}^t}$ be another labeling of the involved indeterminates. Under this notation $V_{i,s} = \{\sum_{j=1}^{m_i} x_{j,t} u_j : \ 1 \leq t \leq n_i\}$. Thus, $V_{i,s}$ is the set of columns of the generic $m_i \times n_i$ matrix $(x_{j,t})_{1 \leq j \leq m_i,\ 1 \leq t \leq n_i}$ (see below). This leads to the following definition.

Definition 3.4.4 For $r, c \in \mathbb{N}$ let $\mathcal{B} = \mathcal{B}(r,c) = \mathcal{K}[x_{1,1}, \cdots, x_{r,c}]$. The *generic* $r \times c$ *module* $M(r,c)$ is the standard $\mathcal{B}$-submodule of $\mathcal{B}^r$ generated by the set $\{\sum_{i=1}^{r} x_{i,j} u_i : \ 1 \leq j \leq c\}$ of columns of the generic $r \times c$ matrix

$$\begin{bmatrix} x_{1,1} & \cdots & x_{1,c} \\ \vdots & \ddots & \vdots \\ x_{r,1} & \cdots & x_{r,c} \end{bmatrix}.$$

Its Hilbert series will be denoted by $H(r,c;t)$.

If $rc \leq n$, letting $x_{i,j} = x_{(j-1)r+i}$ $(1 \leq i \leq r,\ 1 \leq j \leq c)$ be another labeling of the first rc indeterminates in $\mathcal{A} = \mathcal{K}[x_1, \cdots, x_n]$, we have an inclusion algebra map $\mathcal{B}(r,c) \longrightarrow \mathcal{A}$, and we obtain from $M(r,c)$ by extension of scalars (see [AM69]) the $\mathcal{A}$-module

$$\mathcal{A} \otimes_{\mathcal{B}(r,c)} M(r,c).$$

We now have a canonical decomposition of the representation module $M(\pi)$ and a convenient expression for its Hilbert series.

Theorem 3.4.5 *The representation module of a linear representation π with decomposition as above is the direct sum of scalar extensions of generic modules*

$$M(\pi) = \oplus_{i=1}^{k} n_i(\mathcal{A}\otimes_{\mathcal{B}(m_i,n_i)} M(m_i,n_i)).$$

Its Hilbert series is

$$H(\pi,t) = \sum_{i=1}^{k} n_i H(\mathcal{A}\otimes_{\mathcal{B}(m_i,n_i)} M(m_i,n_i),t).$$

Proof. We have seen above that $M(\pi) = \oplus_{i=1}^{k} \oplus_{s=1}^{n_i} M_{i,s}$. But $M_{i,s}$ is the $\mathcal{A}$-module generated by $V_{i,s}$, hence is isomorphic to $\mathcal{A}\otimes_{\mathcal{B}(m_i,n_i)} M(m_i,n_i)$ proving the first statement of the theorem. The second statement follows from the additivity of Hilbert series with respect to direct sums. □

3.5 Initial modules and the Hilbert series of a linear representation

The study of *monomial submodules* of $\mathcal{A}^d$, i.e., those generated by monomials, turns out simpler than the study of arbitrary ones. We start by reviewing some material from the theory of Gröbner bases. A simple use of basic terminology from this theory will make it easy to deduce statements on Hilbert series of arbitrary graded submodules of $\mathcal{A}^d$ from similar statements on monomial submodules. As a reference we mention [Buc85], and for the analogous theory for modules [Eis89, Chapter 6].

A total order on the set of monomials in $\mathcal{A}$ is called *monomial order* if $1 = x^0$ is the minimal monomial and for all monomials x^a, x^b, x^c we have that $x^a < x^b$ implies $x^{a+c} = x^a x^c < x^b x^c = x^{b+c}$. The monomials in $\mathcal{A}^d$ could be totally ordered by setting $x^a u_i > x^b u_j$ if $x^a > x^b$ or $a = b$ and $i < j$. We now concentrate on

$\mathcal{A}$-modules, but all the notions and properties specialize to the polynomial algebra $\mathcal{A} = \mathcal{A}^1$ regarded as an $\mathcal{A}$-module itself. We say that a monomial $x^a u_i$ *appears* in an element $y \in \mathcal{A}^d$ if it appears with nonzero coefficient in the unique expression of y as a $\mathcal{K}$-linear combination of monomials. The *initial monomial* $in(y)$ of y is then the largest (under $<$) monomial $x^a u_i$ appearing in y. Given a submodule M of $\mathcal{A}^d$, its *initial module* $in(M)$ is the submodule generated by the set $\{in(y) : y \in M\}$ of initial monomials in M. The monomials which are not in $in(M)$ are called *standard* and are not in M either. Macaulay (see [Sta78]) proved that the set of (residue classes of) standard monomials forms a $\mathcal{K}$-space basis for the quotient module $\mathcal{A}^d/M$. Since $in(in(M)) = in(M)$, these same monomials form a basis for $\mathcal{A}^d/(in(M))$. Thus, if M is graded, then $H(\mathcal{A}^d/M, t) = H(\mathcal{A}^d/(in(M)), t)$, so

$$\begin{aligned} H(M,t) &= H(\mathcal{A}^d, t) - H(\mathcal{A}^d/M, t) \\ &= H(\mathcal{A}^d, t) - H(\mathcal{A}^d/(in(M)), t) = H(in(M), t). \end{aligned}$$

Now $in(M)$ is a monomial submodule so $dim_{\mathcal{K}}(in(M)_d)$ is given simply by the number of monomials of degree d in $in(M)$. Thus, the computation of $H(M,t)$ is reduced to such a counting. Further, letting $I(M)^i$ be the ideal of $\mathcal{A}$ generated by all monomials x^a such that $x^a u_i \in in(M)$, we have a direct sum of graded $\mathcal{A}$-modules $in(M) = \oplus_{i=1}^{d} I(M)^i u_i$; hence the Hilbert series satisfies

$$H(M,t) = H(in(M), t) = \textstyle\sum_{i=1}^{d} H(I(M)^i, t).$$

As a side remark, we note that usually a generating set for $in(M)$ is needed to carry out this counting. Being a finitely generated module over a Noetherian ring, $\mathcal{A}^d$ is Noetherian, so all its submodules are finitely generated, in particular $in(M)$. Thus, there exists a finite set of elements $S = \{y_1, \cdots, y_t\} \subset M$ such that $\{in(y_1), \cdots, in(y_t)\}$ generates $in(M)$. Any such set S is a *Gröbner basis* for M. In [Buc85] a simple algorithmic criterion for a finite subset S of M to be a Gröbner basis was given, which makes these objects easily recognizable.

Now, let $\mathcal{F} = \mathcal{K}[x_1, \cdots, x_n, y_1, \cdots, y_m]$. We have an inclusion algebra map $\mathcal{A} \longrightarrow \mathcal{F}$, and from each $\mathcal{A}$-module M we can obtain by extension of scalars (see [AM69]) an $\mathcal{F}$-module $\overline{M} = \mathcal{F} \otimes_{\mathcal{A}} M$. If M is an $\mathcal{A}$-submodule of $\mathcal{A}^d$, then, having the inclusion $\mathcal{A}^d \subset \mathcal{F}^d$, $\overline{M}$ could be identified with the $\mathcal{F}$-submodule of $\mathcal{F}^d$ generated by M.

Now, suppose that M is a monomial submodule of $\mathcal{A}^d$, and let S_k be the set of monomials in M_k. Then the set of monomials in $\overline{M}_k$ is

$$T_k = \cup_{r+t=k} \{y^a s : \ y^a \in \mathcal{F}_r, \ s \in S_t\}.$$

Since S_k forms a $\mathcal{K}$-basis for M_k and T_k forms a $\mathcal{K}$-basis for $\overline{M}_k$, the Hilbert series are related by

$$H(\overline{M}, t) = H(\mathcal{K}[y_1, \cdots, y_m], t) H(M, t) = \frac{H(M,t)}{(1-t)^m}.$$

Now let M be an arbitrary submodule of $\mathcal{A}^d$. Then $in(\overline{M}) = \overline{in(M)}$, so

$$H(\overline{M}, t) = H(in(\overline{M}), t) = H(\overline{in(M)}, t) = \frac{H(in(M),t)}{(1-t)^m} = \frac{H(M,t)}{(1-t)^m},$$

as well.

Let $\mathcal{B} = \mathcal{K}[x_{1,1}, \cdots, x_{r,c}]$ with $rc \leq n$, and recall our notation (Definition 3.4.4) $H(r, c; t) = H(M(r, c), t)$. Applying the above relation to the extension of scalars $\mathcal{A} \otimes_{\mathcal{B}(r,c)} M(r, c)$ of the generic module $M(r, c)$, we get the relation

$$H(\mathcal{A} \otimes_{\mathcal{B}(r,c)} M(r, c), t) = \frac{H(r,c;t)}{(1-t)^{n-rc}}.$$

We can therefore refine the expression for the Hilbert series of a representation provided in Theorem 3.4.5.

Theorem 3.5.1 *Let $\pi : G \longrightarrow GL(V)$ be a linear representation with decomposition $\pi = \sum_{i=1}^{k} m_i \chi_i$, where $dim(\chi_i) = n_i$, and let $n = \sum_{i=1}^{k} m_i n_i$. Then the Hilbert series of π is*

$$H(\pi, t) = \frac{1}{(1-t)^n} \sum_{i=1}^{k} n_i (1-t)^{m_i n_i} H(m_i, n_i; t).$$

3.6 Multiplicity-free representations

A representation π is *multiplicity-free* if it has a decomposition $\pi = \sum_{i=1}^{k} \chi_i$ where the χ_i are pairwise nonisomorphic irreducible representations. Letting $n = \sum_{i=1}^{k} n_i$ where $dim(\chi_i) = n_i$, we get from Theorem 3.5.1 that

$$H(\pi, t) = \frac{1}{(1-t)^n} \sum_{i=1}^{k} n_i (1-t)^{n_i} H(1, n_i; t).$$

Now, the generic $1 \times n$ module $M(1,n)$ is simply the ideal in $\mathcal{A}$ generated by $\{x_1, \cdots, x_n\}$, so $M(1,n) = \oplus_{k \geq 1} \mathcal{A}_k$, and thus

$$H(1, n; t) = H(M(1,n), t) = H(\mathcal{A}, t) - 1 = \frac{1}{(1-t)^n} - 1.$$

We have the following theorem.

Theorem 3.6.1 *The Hilbert series of a multiplicity-free representation π with decomposition as above is*

$$H(\pi, t) = \frac{1}{(1-t)^n} \sum_{i=1}^{k} n_i (1 - (1-t)^{n_i}) = \frac{1}{(1-t)^n} (n - \sum_{i=1}^{k} n_i (1-t)^{n_i}).$$

The dimensions $n_1, \cdots, n_k$ of the irreducible components of π can be recovered from $H(\pi, t)$.

Proof. The first statement is obtained by substituting $H(1, n; t)$ in the expression for $H(\pi, t)$ above. For the second, let $n_{i_1} < n_{i_2} < \cdots < n_{i_m}$ be all distinct values taken by the n_i, and for $j = 1, \cdots, m$ let m_j be the multiplicity of n_{i_j} in $\{n_1, \cdots, n_k\}$. It suffices to show that the m_j and n_{i_j} can be recovered. Now, n is determined as the smallest positive integer for which $(1-t)^n H(\pi, t)$ is a polynomial in t. Then, letting $s = 1 - t$, we have

$$\sum_{j=1}^{m} m_j n_{i_j} s^{n_{i_j}} = n - s^n H(\pi, 1-s),$$

and it is clear that the m_j and n_{i_j} can be recovered. □

Example 3.6.2 Let $\pi_{(n-2,2)} : S_n \longrightarrow GL(\mathbb{R}^{\binom{n}{2}})$ be the $(n-2, 2)$ Young representation of the symmetric group (see [Jam78] and Chapter 2). It is well-known that it decomposes as

$$\pi_{(n-2,2)} = \chi_{(n)} \oplus \chi_{(n-1,1)} \oplus \chi_{(n-2,2)},$$

and the dimensions, which can be computed by the *Hook formula* [Jam78], are 1, $n-1$, and $\frac{n(n-3)}{2}$, in the corresponding order. Thus, the Hilbert series is

$$H(\pi_{(n-2,2)}, t) = \frac{1}{(1-t)^{\binom{n}{2}}}\left(\binom{n}{2} - ((1-t) + (n-1)(1-t)^{n-1} + \frac{n(n-3)}{2}(1-t)^{\frac{n(n-3)}{2}})\right).$$

3.7 Determinantal ideals and Gröbner bases

Let $\mathcal{A} = \mathcal{K}[x_{1,1}, \cdots, x_{r,c}]$ and let $M = M(r,c)$ be the generic $r \times c$ submodule of $\mathcal{A}^r$ (Definition 3.4.4) generated by the columns of the matrix

$$X = \begin{bmatrix} x_{1,1} & \cdots & x_{1,c} \\ \vdots & \ddots & \vdots \\ x_{r,1} & \cdots & x_{r,c} \end{bmatrix}.$$

For k-tuples $I = (i_1, \cdots, i_k)$ of elements in $[r]$ and $J = (j_1, \cdots, j_k)$ of elements in $[c]$, we denote by $X_{I,J}$ the corresponding square submatrix of X and by $det(X_{I,J})$ its determinant. By convention, if I and J are empty, we set $det(X_{I,J}) = 1$. If $I = \{i_1, \cdots, i_k\}$ is a set of positive integers with $i_1 < \cdots < i_k$, then we denote by $I^<$ the k-tuple $(i_1, \cdots, i_k)$.

We order the monomials in $\mathcal{A}$ by the *degree lexicographic order*, where $x^a > x^b$ if either its degree $deg(x^a) = \sum_{i=1}^n a_i > deg(x^b)$ or the degrees are the same and the leftmost nonzero coordinate of $a - b$ is positive, where

$$a = (a_{1,1}, a_{2,1}, \cdots, a_{r,1}, a_{1,2}, \cdots, a_{r,2}, \cdots, a_{1,c}, \cdots, a_{r,c}).$$

Now, fix an integer $k \in [r]$, $k \leq c$. For any k-subset $K \in \binom{[c]}{k}$, let

$$x_K = \sum_{j \in K} det(X_{[k-1]^<,(K\setminus\{j\})^<})(\sum_{i=1}^r x_{i,j} u_i).$$

Being an $\mathcal{A}$-linear combination of the columns of X indexed by K, we see that $x_K \in M$. We conjecture that the set

$$\{x_K : \ K \subseteq [c], \ 1 \leq |K| \leq r\}$$

is a Gröbner basis for $M = M(r,c)$. The validation of this conjecture is a continuing project.

Writing $x_K = \sum_{i=1}^{r} p_i u_i$, we have

$$p_i = \sum_{j \in K} det(X_{[k-1]<,(K\setminus\{j\})<}) x_{i,j} = det(X_{(1,\cdots,k-1,i),K<}).$$

In particular, $p_1 = p_2 = \cdots = p_{k-1} = 0$ and $p_k = det(X_{[k]<,K<})$. Thus, the initial monomial of x_K is $in(x_K) = in(det(X_{[k]<,K<}))u_k$. Recall our notation from Section 3.4 that $I(M)^k$ is the ideal of $\mathcal{A}$ generated by all monomials x^a such that $x^a u_k \in in(M)$. If the above conjecture is true, then for $k = 1, \cdots, min\{r,c\}$, we have that $I(M)^k$ is the initial ideal of the ideal I^k in $\mathcal{A}$ generated by $\{det(X_{[k]<,K<}) : K \in \binom{[c]}{k}\}$, and $I(M)^k = 0$ for larger values of k. Now, letting $I(r,c)$ be the ideal in $\mathcal{K}[x_{1,1}, \cdots, x_{k,c}]$ generated by the same set as above, i.e., the determinantal ideal of maximal minors of the generic $k \times c$ matrix $X_{[k],[c]}$, we have (see Section 3.4) that

$$H(I(M)^k, t) = H(I^k, t) = \frac{1}{(1-t)^{(r-k)c}} H(I(r,c), t).$$

The ideal $I(r,c)$ has been extensively studied; in particular, see [Stu90], [SZ92], [BZ92] for a Gröbner basis theoretical point of view. Its Hilbert series $H(I(r,c),t)$ is well-known (A. Zelevinsky, private communication; see [Stu90]). In fact, being generated by square-free monomials, $in(I(r,c))$ is the so-called *Stanley-Reisner ideal* (see [Sta83]) of a certain simplicial complex $\Delta(r,c)$. This complex turns out to be ([BCS88], [Stu90]) *shellable* and one could use it, via the theory of face rings [Sta83] to compute $H(I(r,c),t)$. This will be discussed in more detail in a forthcoming paper by the author.

If our conjecture above is valid, then the Hilbert series of the generic $r \times c$ module could be expressed as

$$H(r,c;t) = H(M,t) = \sum_{i=1}^{min\{r,c\}} H(I(M)^k, t) = \sum_{i=1}^{min\{r,c\}} \frac{1}{(1-t)^{(r-k)c}} H(I(r,c),t),$$

and, substituting this into the expression for the Hilbert series $H(\pi,t)$ of a representation π given in Theorem 3.5.1, an explicit formula for $H(\pi,t)$ is obtained.

Chapter 4

On the Geometry and Computational Complexity of Radon Partitions in the Integer Lattice

4.1 Introduction

We study the following integer analogue of a Radon partition in affine space $\mathbb{R}^d$: A partition (S, T) of a set of integer points in $\mathbb{R}^d$ is an *integral Radon partition* if the convex hulls of S and T have an integer point in common. The Radon number $r(d)$ of an appropriate convexity space on the integer lattice $\mathbb{Z}^d$, to be defined below, is then the infimum over those natural numbers n such that any set of n points or more in $\mathbb{Z}^d$ has an integral Radon partition.

As the study of Radon partitions has a natural setting in the context of convexity spaces, we recall a few basic definitions from that theory.

Definition 4.1.1 *Convexity space.* A convexity space is a pair (X, C), where X is a set, $C \subseteq 2^X$, and the following hold.

(1) $\emptyset \in C,\ X \in C,$

(2) $F \subseteq C \Rightarrow (\cap_{A \in F} A) \in C.$

The members of C are called *convex*, and the C-hull of a set $A \subseteq X$ is

$$C(A) = \cap\{B :\ A \subseteq B \in C\}.$$

The classic example is $(\mathbb{R}^d, conv)$, where

$$conv = \{A : A \subseteq \mathbb{R}^d \text{ and } A \text{ is convex}\}.$$

Definition 4.1.2 *Radon partition.* A partition (S,T) of a given subset of X, where (X,C) is a convexity space, is called a Radon partition, if the C-hulls of S and T intersect.

Finally, we give the following slightly extended definition.

Definition 4.1.3 *Radon number.* Given a convexity space (X,C) and $F \subseteq 2^X$, we define the F-Radon number $r(F)$ as the infimum over those natural numbers n such that any set $A \in F$ with n elements or more has a Radon partition,

$$\begin{aligned} r(F) \ &= \ \inf\{n \in N :\ \forall A \in F\ [[|A| \geq n] \\ &\qquad \rightarrow [\exists S \exists T\ [S \cup T = A] \wedge [S \cap T = \emptyset] \wedge [C(S) \cap C(T) \neq \emptyset]]]\}. \end{aligned}$$

When $F = 2^X$, this reduces to the usual definition of the Radon number, which is denoted simply by r. When the underlying set of the space is a Cartesian product $X = K^d$, we will use the notation $r(d,F)$, and for $F = 2^X$ we will use $r(d)$.

The classical Radon theorem, which follows easily from the affine structure of $\mathbb{R}^d$, says that the Radon number of the space $(\mathbb{R}^d, conv)$ is r(d)=d+2.

The convexity space which is studied in this chapter is the restriction of $(\mathbb{R}^d, conv)$ to the integer lattice, and will be denoted by $(\mathbb{Z}^d, C_d)$. Thus, the C_d-hull of a set $A \subseteq \mathbb{Z}^d$ is $C_d(A) = conv(A) \cap \mathbb{Z}^d$, and the collection of convex sets is $C_d = \{C_d(A) : A \subseteq \mathbb{Z}^d\}$. It follows that the Radon partitions and the

Radon number $r(d)$ of that space coincide with those defined in the beginning of this section.

There are several papers discussing convexity spaces and their Radon number and Helly, Carathéodory, and exchange numbers (to be defined in Section 4.3), see e.g., [DGK63], [Eck68], [Ham65], [Lev51], and [Tve66]. In particular, the Helly number of our space $(\mathbb{Z}^d, C_d)$ had been studied before by Doignon [Doi73]. Also, some recent investigations motivated by integer programming were concerned with Helly properties of the integer lattice ([Bel77], [Sca77], see [Sch86, p. 234]), and Carathéodory properties of it [CFS86].

In contrast with the linear growth rate, as a function of the dimension, of the Radon number of the reals given above, we show in Section 4.2 an $\Omega(2^d)$ lower bound on the Radon number $r(d)$ of the integer lattice. It is interesting to note that this lower bound is also in contrast with a linear upper bound on the Radon number of the product space $(\mathbb{Z}, C_1)^d$ (defined on the same ground set $\mathbb{Z}^d$, but having only the collection $\{A_1 \times A_2 \times \cdots \times A_d : A_i \subseteq \mathbb{Z},\ 1 \leq i \leq d\}$ of d-boxes as its family of convex sets), which follows from an upper bound on Radon numbers of product convexity spaces given in [Eck68].

On the other hand, we show in Section 4.3 an $O(d2^d)$ upper bound on the Radon number of the integer lattice.

Throughout this chapter, by a "polytope" we mean a real convex polytope, i.e., a set $P = conv(V) \subseteq \mathbb{R}^d$ such that V is finite. If $V \subseteq \mathbb{Z}^d$, then P is called a "lattice polytope". It is easy to see that, in the definition of the Radon number, it is enough to consider subsets $A \subseteq X$ such that $|A| < \infty$ and $A = ext(P)$, the set of vertices of P, where P is some lattice polytope. Thus, the question about $r(d)$ is in fact a question about the existence of Radon partitions of sets of vertices of lattice polytopes, and we can ask the same question about subclasses of lattice polytopes. This is the subject of Section 4.4, in which we study some properties of polytopes having a large stable set of vertices (in the graph theoretical sense),

and establish the existence of a Radon partition for such polytopes. This result is also useful for the proof, given in Section 4.5, that $r(2) = 6$, and leads to a simpler and more direct proof, for simple lattice polytopes, of the upper bound.

Finally, in Section 4.6, we discuss the computational complexity of deciding whether a given set of points in $\mathbb{Z}^d$ has a Radon partition, and show that if d is fixed, then this problem is in P, while if d is part of the input, it is NP-complete.

Before going on, we note that the Radon number of the integer lattice is invariant under affine transformations. More precisely, we have the following observation.

Observation 4.1.4 *Consider a set $S \subseteq \mathbb{Z}^d$ such that $dim(aff(S)) = k \leq d$. If $|S| \geq r(k)$, then S has a Radon partition.*

The proof is based on the fact that, given such a set, there is an affine bijection from $aff(S)$ to $\mathbb{R}^k$ which preserves integrality (this is a result, say, of Theorem 3 in [GL87, p. 19] or Corollary 4.3b in [Sch86]).

4.2 A lower bound

We have the following proposition.

Proposition 4.2.1 *For $d \geq 1$ we have*

$$r(d+1) \geq 2r(d) - 1.$$

Proof. Assume indirectly that $r(d+1) \leq 2r(d) - 2$. Let $A \subseteq \mathbb{Z}^d$, $|A| = r(d) - 1$ be a set that admits no Radon partition. Let

$$X_i = \{(a, i) : a \in A\} \qquad (i = 0, 1).$$

Then $X_0 \cup X_1 \subseteq \mathbb{Z}^{d+1}$ and $|X_0 \cup X_1| = 2(r(d) - 1) \geq r(d+1)$, so there exists a Radon partition of $X_0 \cup X_1$ into two sets Y_0, Y_1. Let $p \in C_{d+1}(Y_0) \cap C_{d+1}(Y_1)$. Then $p \in \mathbb{Z}^{d+1}$, and $C_{d+1}(Y_0) \cap C_{d+1}(Y_1) \subseteq \{(x_1, \cdots, x_{d+1}) : 0 \leq x_{d+1} \leq 1\}$,

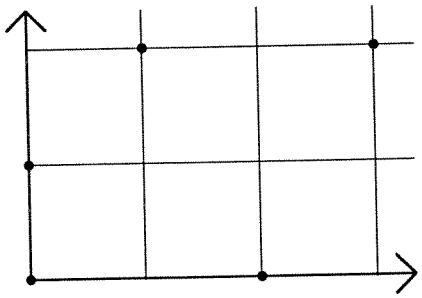

Figure 4.1: Five points in the plane

so $p_{d+1} \in \{0,1\}$. Assume, without loss of generality, that $p_{d+1} = 0$. Then, for $i = 0,1$, let $Z_i = Y_i \cap \{(x_1, \cdots, x_{d+1}) : x_{d+1} = 0\}$. We then have that $p \in C_{d+1}(Z_0) \cap C_{d+1}(Z_1)$. Thus, the sets $\{a : (a,0) \in Z_0\}$ and $\{a : (a,0) \in Z_1\}$ form a Radon partition of A, a contradiction. □

The following set of points shows that $r(2) \geq 6$ (see Fig. 1).

$$\{(0,0),(2,0),(0,1),(1,2),(3,2)\}.$$

This, together with Proposition 4.2.1, yield the following.

Corollary 4.2.2 *For $d \geq 2$, $r(d) \geq 2^d + 2^{d-2} + 1 = 5 \cdot 2^{d-2} + 1$.*

Proof. By induction on d. for $d = 2$ this is true since $r(2) \geq 6$. Now,

$$r(d+1) \geq 2r(d) - 1 \geq 2 \cdot (2^d + 2^{d-2} + 1) - 1 = 2^{d+1} + 2^{(d+1)-2} + 1,$$

as required. □

4.3 An upper bound

In the current section, we need to recall a few more invariants of a convexity space (X, C).

Definition 4.3.1 *Carathéodory number.* The Carathéodory number c is the infimum over those natural numbers n such that the C-hull of any set $S \subseteq X$ is the union of the C-hulls of subsets $T \subseteq S$ with $|T| \leq n$,

$$c = \inf\{n \in N : \forall S \subseteq X \ [C(S) = \cup\{C(T) : [T \subseteq S] \wedge [|T| \leq n]\}]\}.$$

Definition 4.3.2 *Helly number.* The Helly number h is the infimum over those natural numbers n such that any finite family $L \subseteq 2^X$ with the property that the intersection of the C-hulls of all its members, $\cap\{C(A) : A \in L\}$, is empty, has a subfamily $M \subseteq L$ of size $|M| \leq n$ with the same property,

$$\begin{aligned} h = \inf\{n \in N : \ & \forall L \subseteq 2^X \ [[[|L| < \infty] \wedge [\cap\{C(A) : A \in L\} = \emptyset]] \\ & \rightarrow [\exists M \subseteq L \ \ [|M| \leq n] \wedge [\cap\{C(A) : A \in M\} = \emptyset]]]\}. \end{aligned}$$

Definition 4.3.3 *Exchange number.* The exchange number e is the infimum over those natural numbers n such that for every point $p \in X$ and finite set $A \subseteq X$, if $|A| \geq n$ then the C-hull of A is contained in the union of the C-hulls of sets obtained from A by replacing a point $a \in A$ by the point p,

$$\begin{aligned} e = \inf\{n \in N : \ & \forall p \in X \ \forall A \subseteq X \ [[n \leq |A| < \infty] \\ & \rightarrow [C(A) \subseteq \cup\{C(p \cup (A - a)) : a \in A\}]]\}. \end{aligned}$$

As with the Radon number, when the underlying set of the space is a Cartesian product $X = K^d$, we will use $c(d)$, $h(d)$, $e(d)$. It is well known that for $(\mathbb{R}^d, conv)$, $c(d) = h(d) = e(d) = d + 1$.

The following was proved in [Doi73].

Proposition 4.3.4 *The Helly number of the convexity space* $(\mathbb{Z}^d, C_d)$ *is* $h(d) = 2^d$.

The following proposition is an immediate consequence of the definitions.

Proposition 4.3.5 *Let (X, C) be a convexity space with Carathéodory number c and exchange number e, and let $Y \subseteq X$. Then $(Y, \{A \cap Y : A \in C\})$ is a convexity space (the restriction to Y) with Carathéodory number $c' \leq c$, and exchange number $e' \leq e$.*

From the proof of Theorem 3 in [Sie77] we immediately obtain the following proposition.

Proposition 4.3.6 *Let (X, C) be a convexity space with finite Carathéodory, Helly and exchange numbers c, h, e. Let a be a nonnegative integer such that $e \leq a$ and $c \leq a$. Then the Radon number satisfies*

$$r \leq (a-1)(h-1) + 3.$$

We now give an upper bound on the Radon number $r(d)$ of the convexity space $(\mathbb{Z}^d, C_d)$.

Corollary 4.3.7 $r(d) \leq d(2^d - 1) + 3$.

Proof. It is known that for $(\mathbb{R}^d, conv)$ the Carathéodory number and the exchange number are both equal to $d+1$. By Proposition 4.3.5, we then have, for $(\mathbb{Z}^d, C_d)$, that $c(d) \leq d+1$ and $e(d) \leq d+1$. By Proposition 4.3.4, we have $h(d) = 2^d$, and so by Proposition 4.3.6 we get

$$r(d) \leq ((d+1)-1)(h(d)-1) + 3 = d(2^d - 1) + 3.$$

□

4.4 Stable sets in polytopes

In this section we study in detail some elementary properties of stable sets of vertices of polytopes. We establish the existence of a Radon partition of the set of extreme points (vertices) of a lattice polytope having a large stable set (in the

sense defined below) of vertices. As a byproduct, this result yields a simpler and more direct proof of an upper bound for $r(d, SP)$, where $SP = \{A \subseteq \mathbb{Z}^d : A = ext(P),\ P \text{ a simple polytope}\}$, which is asymptotically the same as the one given in Corollary 4.3.7 (recall that a d-polytope is called "simple" if each one of its vertices is contained in exactly d 1-faces). It is also helpful in proving, in the next section, that $r(2) = 6$.

We start with some notation. By the "graph" of a polytope we mean the abstract graph having as vertices and edges the 0-faces and 1-faces of the polytope, respectively. For two points $x, y \in \mathbb{R}^d$ we denote by $[x, y] = conv(\{x, y\})$ the closed line segment joining them. For a vertex $s \in ext(P)$, we denote its set of neighbors by $N_P(s) = \{v \in ext(P) : [s, v] \text{ is a 1-face of } P\}$.

We will need the following proposition (see [Brø83, Thm. 11.8]).

Proposition 4.4.1 *Let P be a d-polytope, v a vertex of P and H a hyperplane separating v from $N_P(v)$. Then H separates v from $ext(P) \setminus \{v\}$.*

By a (real) "Minimal Radon Partition" (MRP for short) we will mean a pair (S, T) constituting a real Radon partition of $S \cup T \subseteq \mathbb{R}^d$ (i.e., $S \cap T = \emptyset$ and $conv(S) \cap conv(T) \neq \emptyset$), such that no proper subset of $S \cup T$ admits a real Radon partition. The following is easy to derive from the affine structure on $\mathbb{R}^d$, and in fact, is just the circuit elimination axiom in the more general setting of oriented matroids (for a general reference to oriented matroids, see the forthcoming book [BLVS+92]).

Proposition 4.4.2 *Let (S_1, T_1) and (S_2, T_2) be two MRP such that $S_1 \neq S_2$, $S_1 \neq T_2$, and $x \in S_1 \cap T_2$. Then there exists an MRP (S_3, T_3) such that $x \notin S_3 \cup T_3$, $S_3 \subseteq S_1 \cup S_2$, and $T_3 \subseteq T_1 \cup T_2$.*

The following is an elementary fact, formulated in terms of MRP.

Proposition 4.4.3 *Let P be a d-polytope, $V = ext(P)$, $u, v \in V$. Then $[u, v]$ is not an edge of P if and only if there exists an MRP $(\{u, v\}, T)$, $T \subseteq V \setminus \{u, v\}$.*

We will now establish some properties of polytopes which will lead to the proof of the main result of this section.

Lemma 4.4.4 *Let P be a d-polytope, $u \in V = ext(P)$, $P' = conv(V \setminus \{u\})$, and $v \in V \setminus (\{u\} \cup N_P(u))$. If $w \in V \setminus \{u, v\}$ is such that $[v, w]$ is not an edge of P, then it is also not an edge of P'.*

Proof. If $[v, w]$ is not an edge of P then, by Proposition 4.4.3, there exists $T_1 \subseteq V \setminus \{v, w\}$ such that $(\{v, w\}, T_1)$ is an MRP. If $u \notin T_1$, then $T_1 \subseteq ext(P')$ and so the claim follows by Proposition 4.4.3. Suppose then, that $u \in T_1$. Now, $[u, v]$ is not an edge of P, and so there exists $T_2 \subseteq V \setminus \{u, v\}$ such that $(\{u, v\}, T_2)$ is an MRP. Now, eliminating $u \in \{u, v\} \cap T_1$ using Proposition 4.4.2, we find an MRP (S, T) with $S \subseteq \{v, w\}$ and $T \subseteq T_1 \cup T_2 \setminus \{u\}$. But v, w are vertices of P, so we must have $S = \{v, w\}$, and $T \subset ext(P')$, so by Proposition 4.4.3 again $[v, w]$ is not an edge of P'. □

Lemma 4.4.5 *Let P be a d-polytope, $u \in V = ext(P)$, $P' = conv(V \setminus \{u\})$, $v \in P \setminus (\{u\} \cup P')$ and $P'' = conv(V \cup \{v\} \setminus \{u\})$. If $w \in V \setminus \{u\}$ is such that $[u, w]$ is not an edge of P, then $[v, w]$ is not an edge of P''.*

Proof. First, it is clear that $ext(P'') = V \cup \{v\} \setminus \{u\}$. Now, if $[u, w]$ is not an edge of P, then there exists $T_1 \subseteq V \setminus \{u, w\}$ such that $(\{u, w\}, T_1)$ is an MRP. Also, $v \in P$ implies that there exists $T_2 \subseteq V$ such that $(\{v\}, T_2)$ is an MRP, and since $v \notin P'$, it must be that $u \in T_2$. Eliminating u via Proposition 4.4.2, we obtain an MRP (S, T) with $S \subseteq \{v, w\}$ and $T \subseteq T_1 \cup T_2 \setminus \{u\}$. Now, w is a vertex of P, $T \subseteq ext(P')$, and $v \notin P'$, so it must be that $S = \{v, w\}$, and so by Proposition 4.4.3, $[v, w]$ is not an edge of P''. □

Lemma 4.4.6 Stable set exchange lemma. *Let P be a d-polytope, $V = ext(P)$ and $S \subset V$ a stable subset of vertices (i.e., no two vertices in S lie on a common 1-face). Let $x \in conv(S) \setminus (S \cup conv(V \setminus S))$. Then there exists a vertex $s \in S$ such*

that in the polytope $P' = conv(V \cup \{x\} \setminus \{s\})$, *we have* $ext(P') = V \cup \{x\} \setminus \{s\}$ *and* $S' = S \cup \{x\} \setminus \{s\}$ *is a stable set.*

Proof. Let H be a hyperplane separating x from $V \setminus S$. Since $x \in conv(S)$, there is a vertex $s \in S$ which is also separated from $V \setminus S$ by H. But S is stable, so $N_P(s) \subseteq V \setminus S$, and so H separates s from $N_P(s)$. Then, by Proposition 4.4.1, it separates s, and hence x, from $V \setminus \{s\}$. Thus $ext(P') = V \cup \{x\} \setminus \{s\}$.

Now, if $t \in S \setminus \{s\}$, then $[s,t]$ is not an edge of P, and so by Lemma 4.4.5, $[x,t]$ is not an edge of P'. If $u \in S \setminus \{s,t\}$, then $[t,u]$ is not an edge of P, and so by Lemma 4.4.4, $[t,u]$ is not an edge of $conv(V \setminus \{s\}) \subseteq P'$, hence not an edge of P' either. So S' is a stable set in P', as claimed. □

We can now prove the following.

Theorem 4.4.7 *Let* P *be a* d*-lattice polytope such that* $S \subset V = ext(P)$ *is a stable set of vertices and* $|S| = 2^d + 1$. *Then* $(S, V \setminus S)$ *is a Radon partition of* V, *i.e.,* $C_d(S) \cap C_d(V \setminus S) \neq \emptyset$.

Proof. S is a set of integer points in $\mathbb{Z}^d$ of size $2^d + 1$, so there are two points $y, z \in S$ having the same parity on all coordinates. The point $x = (y+z)/2$ is an integer point in $conv(S) \setminus S$. If $x \in conv(V \setminus S)$, then we are done. If not, then let the point $s \in S$, the polytope P', and the set S' be as defined in Lemma 4.4.6. Then, by the lemma, P' and S' satisfy the hypothesis of the current theorem and we can repeat the argument above. Now $|conv(S') \cap \mathbb{Z}^d| < |conv(S) \cap \mathbb{Z}^d|$ because $s \in conv(S) \setminus conv(S')$, and $|conv(S) \cap \mathbb{Z}^d| < \infty$, so after finitely many applications of the argument above, we obtain a polytope P'' and a set S'' such that $(S'', V \setminus S)$ is a partition of $ext(P'')$ such that there exists an integer point $x'' \in conv(S'') \cap conv(V \setminus S)$. But, by the construction, $conv(S'') \subseteq conv(S)$, so in fact we have $x'' \in C_d(S) \cap C_d(V \setminus S)$. □

Example 4.4.8 Consider, for $k \geq 3$, the graph $G(k) = (V(k), E(k))$, which is the union of two homeomorphs of the k-wheel (see Fig. 2 for $k = 4$), defined as follows

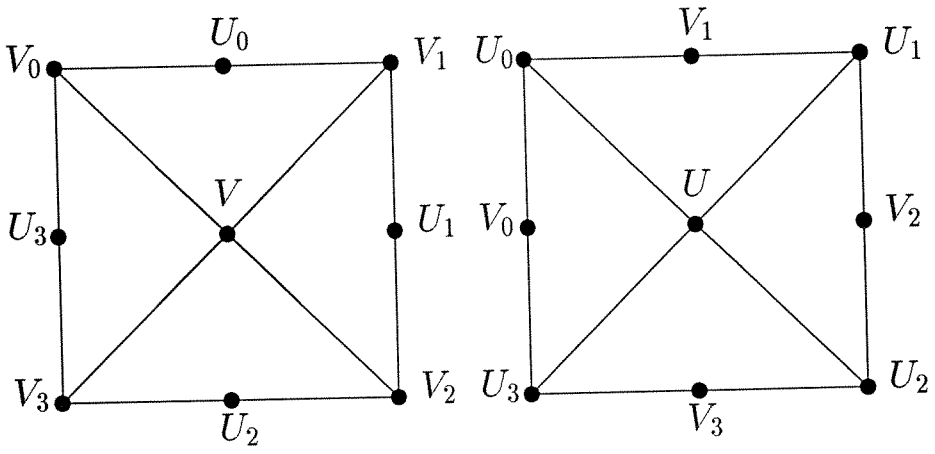

Figure 4.2: Bicycle wheel with 8 spokes

(we call it the "Bicycle wheel with $2k$ alternating spokes"):

$$\begin{aligned} V(k) &= \{v, v_0, \cdots, v_{k-1}, u, u_0, \cdots, u_{k-1}\}, \\ E(k) &= \{\{v_i, u_i\} : 0 \le i \le k-1\} \cup \{\{u_i, v_{i+1 \ (mod\ k)}\} : 0 \le i \le k-1\} \\ &\cup \{\{v, v_i\} : 0 \le i \le k-1\} \cup \{\{u, u_i\} : 0 \le i \le k-1\}. \end{aligned}$$

The graph $G(k)$ is planar and 3-connected, so by Steinitz's theorem (see [Grü67, §13.2]) there exists a (convex) lattice 3-polytope $P(k)$ having $G(k)$ as its graph. Note, for example, that the 3-cube C^3 has $G(3)$ as its graph. Now, for $k \ge 9$ and $d \ge 3$, each one of the polytopes $P(k) \times C^{d-3} \subseteq \mathbb{R}^d$ satisfies the hypothesis of Theorem 4.4.7, and so admits a Radon partition. Note that for $k = 9$ or 10 we cannot deduce this from Corollary 4.3.7.

As a corollary to Theorem 4.4.7 we get again the upper bound, for simple polytopes, and so we have the following corollary.

Corollary 4.4.9 $2^d + 2^{d-2} + 1 \le r(d, SP) \le d2^d + 2$.

Proof. The lower bound is the same as the one given in Corollary 4.2.2, as the proof in Section 2 remains valid for simple polytopes. For the upper bound, recall

that the graph of a simple polytope is d-regular, so if the polytope has at least $d2^d + 2$ vertices, it has a stable set of size at least $\lceil((d2^d + 2) - 1)/d\rceil = 2^d + 1$. Then, by Theorem 4.4.7, the set $ext(P)$ has a Radon partition. □

4.5 The two-dimensional case

In Section 4.2 we have shown that $r(2) \geq 6$. We shall now prove the converse. Recall our notation that, for $S \subseteq \mathbb{Z}^2$, $C_2(S) = conv(S) \cap \mathbb{Z}^2$. We will use the following simple fact (see [GL87, Thm. 4, p. 20]).

Proposition 4.5.1 *Let v_1, v_2 be two linearly independent points in $\mathbb{Z}^2$. If*

$$C_2(\{(0,0), v_1, v_2\}) = \{(0,0), v_1, v_2\},$$

then the set $\{v_1, v_2\}$ is a lattice basis of $\mathbb{Z}^2$.

Lemma 4.5.2 *Let $V \subseteq \mathbb{Z}^2$ be such that $|V| = 6$ and $P = conv(V)$ is a convex hexagon. Let $S \subseteq V$ be a stable subset with $|S| = 3$. Then $C_2(S) \setminus S \neq \emptyset$.*

Proof. Without loss of generality we may assume that $S = \{(0,0), v_1, v_2\}$. Consider the two lines $l_i = lin(v_i)$ $(i = 1, 2)$. Denote the four connected components of $\mathbb{R}^2 \setminus (l_1 \cup l_2)$ by $c_{i,j}$ $(i, j = 0, 1)$ (see Fig. 3).

There must be two points in $V \setminus S$ lying on adjacent components, say $w_1 \in c_{1,0}$, $w_2 \in c_{0,0}$.

Now, suppose indirectly that $C_2(S) = S$. Then, by Proposition 4.5.1, $\{v_1, v_2\}$ is a basis of the lattice $\mathbb{Z}^2$. Now for $i = 1, 2$, $w_i \in \mathbb{Z}^2$, and hence lies on the line $l_1 + k_i v_2$ for some integer $k_i \geq 1$. But then we have $v_2 \in conv(\{(0,0), w_1, w_2\})$, a contradiction. □

Theorem 4.5.3 $r(2) = 6$.

Proof. Let $U \subseteq \mathbb{Z}^2$ be such that $|U| \geq 6$. We may assume that there is a subset $V \subseteq U$ such that $|V| = 6$ and $P = conv(V)$ is a convex hexagon. It is

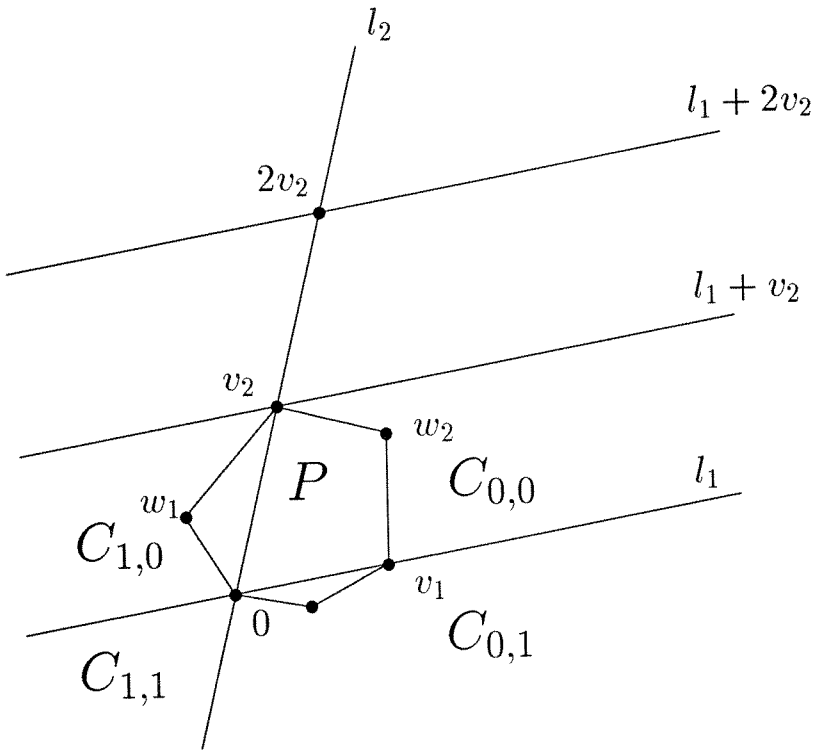

Figure 4.3: The hexagon lemma

enough to show that V admits a Radon partition. Let $S \subseteq V$ be a stable set with $|S| = 3$. By Lemma 4.5.2, $C_2(S) \setminus S \neq \emptyset$. Then either $C_2(S) \cap C_2(V \setminus S) \neq \emptyset$, in which case we are done, or there exists a point $x \in C_2(S) \setminus (S \cup conv(V \setminus S))$. In that case, a stable set exchange yields a new set S' and polytope P' as defined in Lemma 4.4.6, and in particular $C_2(S') \subset C_2(S)$. Repeating the same argument as above, we eventually get, as in the proof of Theorem 4.4.7, a set S'' such that $|S''| = 3$, $P'' = conv((V \setminus S) \cup S'')$ is a convex hexagon, S'' is stable in P'', and $C_2(S'') \cap C_2(V \setminus S) \neq \emptyset$. But then we are done, since $conv(S'') \subseteq conv(S)$ and so $(S, V \setminus S)$ is a Radon partition of V. □

4.6 Computational complexity aspects

Consider the following decision problems.

RADON(d):

Instance: $n \in N$ and $A \subseteq \mathbb{Z}^d$ such that $|A| = n$.

Question: Does A admit an (integral) Radon partition?

RADON:

Instance: $d, n \in N$ and $A \subseteq \mathbb{Z}^d$ such that $|A| = n$.

Question: Does A admit an (integral) Radon partition?

Note that in RADON(d), the dimension d is fixed and is not part of the input. We show that RADON(d) is decidable in polynomial time while, in contrast, RADON is NP-complete.

Proposition 4.6.1 *RADON(d) is decidable in polynomial time.*

Proof. Given an input to RADON(d), if $n \geq r(d)$ then there exists a Radon partition. Otherwise, consider all possible pairs (S, T) of disjoint nonempty subsets of the input set A such that $|S|, |T| \leq d + 1$ and the points in S (respectively T) are affinely independent in $aff(S)$ (respectively $aff(T)$). Since the Carathéodory number of the reals $c(d) \leq d + 1$, there will be such a pair with $C_d(S) \cap C_d(T) \neq \emptyset$

if and only if the input set A has a Radon partition. The number of such pairs is bounded by a polynomial function of n, and in fact, $n < r(d) < \infty$ (the second inequality from Corollary 4.3.7), so it is bounded by a finite constant which depends on d only. For each pair (S,T) with $|S| \leq d+1, |T| \leq d+1$, do the following. Find a system of linear equalities defining $aff(S)$, and check affine independence; i.e., $|S| = 1+dim(aff(S)$ (otherwise, move on to the next pair). Next, add inequalities to this system to get a description of $conv(S)$. This is easy, as $conv(S)$ is a simplex in $aff(S)$, so any $(|S|-1)$-subset of S spans a facet of $conv(S)$ in $aff(S)$.

It is easily verified that the bit size of such a description is bounded above by a polynomial function in the bit size of the input, and so this step can be done in polynomial time.

Similarly, find a description of $conv(T)$ via linear inequalities and equalities.

Now, let L be the union of the collections of linear equalities and inequalities describing $conv(S)$ and $conv(T)$. Apply to it an algorithm that checks whether its solution set contains an integer point, e.g., the integer programming algorithm in [Len83], which runs in polynomial time when the dimension d is not a part of the input. Since the solution set of L is $conv(S) \cap conv(T)$, this algorithm checks if $C_d(S) \cap C_d(T) \neq \emptyset$, which is what we require. □

Next, we show that, in contrast, RADON is NP-complete. The following problem is known to be NP-complete (see [GJ79, p. 223]).

PARTITION:

Instance: $n \in N$ and a set of nonnegative integers $B = \{a_1, \cdots, a_{2n}\}$.

Question: Is there a balanced partition of $[2n] = \{1, \cdots, 2n\}$, namely a partition (I,J) such that $|I| = |J| = n$ and $\sum_{i \in I} a_i = \sum_{j \in J} a_j$?

Theorem 4.6.2 *RADON is NP-complete.*

Proof. To show that RADON is in NP, suppose the instance in question has a Radon partition (S,T). Then there exists $x \in C_d(S) \cap C_d(T)$, and so the triple

(x, S, T) is a witness of size bounded by a polynomial in the size of the input, to the existence of a Radon partition, which can be checked in polynomial time.

We now show that PARTITION is polynomial time reducible to RADON. Given an input (n, B) to PARTITION, let $d = 2\binom{2n}{2}+1, k = n + n^2$. We construct a set A of $2n + 2\binom{2n}{2}$ distinct points in $\mathbb{Z}^d$ such that A has a Radon partition if and only if there exists a balanced partition for (n, B). For convenience, we index the first coordinate of a point by 0, and for each pair i, j such that $1 \leq i < j \leq 2n$, a point will have two coordinates, one indexed by $1, i, j$ and the other by $2, i, j$, so a point will be written as

$$x = (x_0, x_{1,1,2}, x_{2,1,2}, x_{1,1,3}, x_{2,1,3}, \cdots, x_{1,2n-1,2n}, x_{2,2n-1,2n}).$$

Now, for each $i \in [2n]$, we will have one point x^i, and for each pair i, j such that $1 \leq i < j \leq 2n$ we will have two points $y^{i,j}, z^{i,j}$, so

$$A = \{x^1, \cdots, x^{2n}, y^{1,2}, z^{1,2}, \cdots, y^{2n-1,2n}, z^{2n-1,2n}\},$$

where the points are defined as follows.

$\forall i \in [2n]$, let $x^i_0 = ka_i$.

$\forall i, j \in [2n]$ such that $i < j$, let

$$x^i_{1,i,j} = y^{i,j}_{1,i,j} = -1, \quad x^j_{1,i,j} = z^{i,j}_{1,i,j} = 1, \quad y^{i,j}_{2,i,j} = z^{i,j}_{2,i,j} = k.$$

All other entries of all points will be set to zero. Clearly the set A defined in this way can be constructed from B in polynomial time.

Now, suppose first that (I, J) is a balanced partition for (n, B). Define $S, T \subseteq A$ as follows.

$$\begin{aligned} S &= \{x_i : i \in I\} \cup \{z_{i,j} : 1 \leq i < j \leq 2n, i \in I, j \in J\} \\ &\quad \cup \{y_{i,j} : 1 \leq i < j \leq 2n, i \in J, j \in I\}, \\ T &= \{x_i : i \in J\} \cup \{y_{i,j} : 1 \leq i < j \leq 2n, i \in I, j \in J\} \\ &\quad \cup \{z_{i,j} : 1 \leq i < j \leq 2n, i \in J, j \in I\}. \end{aligned}$$

It is easy to see that $S \cap T = \emptyset$ and $|S| = |T| = k$, and that

$$\sum_{s\in S}\tfrac{1}{k}s = \sum_{t\in T}\tfrac{1}{k}t \in \mathbb{Z}^d,$$

so $C_d(S)\cap C_d(T)\neq\emptyset$; hence, for instance, $(S, A\setminus S)$ is a Radon partition.

Conversely, suppose (S,T) is a Radon partition of A; i.e., for every point $x\in A$ there exists a real number $c(x)$, $0\le c(x)\le 1$, such that

$$\sum_{s\in S} c(s)s = \sum_{t\in T} c(t)t \in \mathbb{Z}^d \text{ and } \sum_{s\in S} c(s) = \sum_{t\in T} c(t) = 1.$$

Let $1\le i<j\le 2n$, and consider the $(2,i,j)$th coordinate. It is clear then, that if $c(y^{i,j})>0$ or $c(z^{i,j})>0$, then in fact $c(y^{i,j}) = c(z^{i,j})$ and $y^{i,j}, z^{i,j}$ are on opposite sides of the partition. If both coefficients above are zero then, moving $y^{i,j}$ to the other side if necessary, we may assume again that it is on the opposite side of $z^{i,j}$. So, we may assume that for all $1\le i<j\le 2n$ we have $c(y^{i,j}) = c(z^{i,j})$ and $y^{i,j}, z^{i,j}$ are on opposite sides of the partition.

Now let $1\le i<j\le 2n$. We have the following.

CLAIM. If the points x^i and x^j are on the same side of the partition, then $c(y^{i,j}) = c(z^{i,j}) = 0$ and $c(x^i) = c(x^j)$, whereas if they are on opposite sides of the partition, then $c(x^i) = c(x^j) = c(y^{i,j}) = c(z^{i,j})$.

Proof of claim. Consider the $(1,i,j)$th coordinate. Four cases arise, according to whether x^i and x^j lie on the same or opposite side of the partition, and whether x^i and $y^{i,j}$ lie on the same or opposite side of the partition. We demonstrate the proof in the case where both x^j and $y^{i,j}$ appear on the opposite side of the partition from x^i. In that case, we have

$$-c(x^i) + c(z^{i,j}) = c(x^j) - c(y^{i,j}) \in \mathbb{Z}.$$

If $c(y^{i,j}) = 0$, then

$$c(z^{i,j}) = 0 \Longrightarrow 0 \ge -c(x^i) = c(x^j) \ge 0 \Longrightarrow c(x^i) = c(x^j) = 0.$$

If $c(y^{i,j}) = 1$, then

$$c(z^{i,j}) = 1 \Longrightarrow 0 \le 1 - c(x^i) = c(x^j) - 1 \le 0 \Longrightarrow c(x^i) = c(x^j) = 1.$$

Otherwise, $|c(x^j) - c(y^{i,j})| < 1$ and $c(x^j) - c(y^{i,j}) \in \mathbb{Z}$, so

$$c(x^j) - c(y^{i,j}) = 0 \Longrightarrow -c(x^i) + c(z^{i,j}) = 0 \Longrightarrow c(x^i) = c(z^{i,j}) = c(y^{i,j}) = c(x^j),$$

as claimed. The other cases are simpler and are left for the reader to verify.

The claim implies that, for all $1 \leq i < j \leq 2n$, we have $c(x^i) = c(x^j)$, so for all $i \in [2n]$ we get $c(x^i) = c$ for some number $c \geq 0$. If $c = 0$ then, by the claim again, for all i, j such that $1 \leq i < j \leq 2n$ we also have $c(y^{i,j}) = c(z^{i,j}) = 0$; but then all coefficients are zero, which is impossible. So $c > 0$.

Now, let $I = \{i : x^i \in S\}$, $J = \{j : x^j \in T\}$. We have shown in the beginning of the proof that, for any $1 \leq i < j \leq 2n$, we have $c(y^{i,j}) = c(z^{i,j})$ and $y^{i,j}$, $z^{i,j}$ are on opposite sides of the partition. Thus we have

$$0 = \sum_{s \in S} c(s) - \sum_{t \in T} c(t) = c|I| - c|J|,$$

implying $|I| = |J|$, and so (I, J) is a partition of $[2n]$ such that $|I| = |J| = n$.

Finally, consider the 0th coordinate. We have

$$\sum_{i \in I} cka_i = \sum_{i \in I} cx_0^i = \sum_{s \in S} c(s)s_0 = \sum_{t \in T} c(t)t_0 = \sum_{j \in J} cx_0^j = \sum_{j \in J} cka_j,$$

which implies that $\sum_{i \in I} a_i = \sum_{j \in J} a_j$, so (I, J) is a balanced partition for (n, B).

□

4.7 Remaining questions

Computing the lower and upper bounds given in Corollary 4.2.2 and Corollary 4.3.7, we obtain $11 \leq r(3) \leq 24$. For simple polytopes we can do a little better.

Proposition 4.7.1 $11 \leq r(3, SP) \leq 21$.

Proof. Let P be a simple 3-polytope, and let f_i be the number of i-faces of P $(i = 0, 1, 2)$. Suppose $f_0 \geq 21$. Let g_i be the number of vertices of P contained in

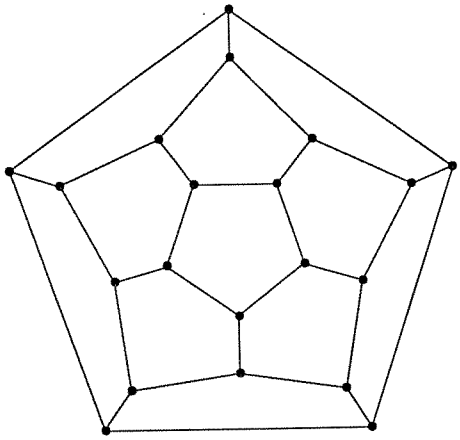

Figure 4.4: The dodecahedron

its ith facet ($i = 1, \cdots, f_2$). We claim that there exists a facet having $g_i \geq r(2) = 6$. Now $f_1 = 3f_0/2$ (P simple), so Euler's formula implies $f_0 = 2(f_2 - 2)$. Counting incidences of vertices and facets, we get $\sum_{i=1}^{f_2} g_i = 3f_0 = 6f_2 - 12$. Now $f_0 \geq 21$, so $f_2 \geq (3 \cdot 21 + 12)/6 > 12$. Thus, the average number of vertices on a facet is $(6f_2 - 12)/f_2 = 6 - 12/f_2 > 5$, so there must be a facet containing at least six vertices, proving the claim. But then the set of vertices of this facet has a Radon partition, by Observation 4.1.4, so the set $ext(P)$ has a Radon partition as well. □

It will be interesting to find tighter lower and upper bounds for $r(d)$ and $r(d, SP)$, or at least the exact values of $r(3)$ and $r(3, SP)$. Even more specifically, does the set of extreme points of any lattice 3-polytope realization of the dodecahedron (see Fig. 4) always admit a Radon partition?

Chapter 5

Approximating Oracle Machines for Combinatorial Optimization

5.1 Introduction

Combinatorial Optimization is the problem of maximizing a rational linear functional $x \in \mathbb{Q}^n$ over a given set $S \subseteq \{0,1\}^n \subset \mathbb{Q}^n$. Typically, S is not listed explicitly, and the natural input size for the problem is $n + b(x)$, where $b(x)$ is the number of bits encoding x. A setting which makes it possible to let the input consist of (n, x) only, is that of an oracle Turing machine (see [HU79]). We would like such a machine M, equipped with the set of interest $S \subseteq \{0,1\}^n$ as an oracle, denoted M^S, to maximize x over S. While time complexity $O(2^n b(x))$ is easily obtained by an exhaustive search of S, it is unlikely that such a general machine will run in time polynomial in $n + b(x)$.

A fruitful approach, taken in much of the literature on combinatorial optimization, is to restrict the set S to come from a specified class $\mathcal{F} \subseteq \cup_{n \geq 0} 2^{\{0,1\}^n}$, say restrict S to be the set of characteristic vectors of stable sets in some bipartite graph. However, even in this setting, efficient machines are often unlikely to exist. Motivated by the recent work of Lovász and Schrijver [LS91], we take here

an alternative approach, where the set S could be arbitrary, but M^S is allowed to maximize over a certain approximation for S rather than S. Appealing to the embedding of $S \subseteq \{0,1\}^n \subset \mathbb{Q}^n$ in rational affine space, an *approximation* of S is a rational convex polytope P contained in the unit cube $[0,1]^n$ and satisfies $P \cap \{0,1\}^n = S$. In [LS91], an operator $\mathcal{N}$ was introduced that produces from a given approximation P of $S \subseteq \{0,1\}^n$ another one $\mathcal{N}(P)$, with the property $P \supseteq \mathcal{N}(P) \supseteq \mathcal{N}^2(P) \supseteq \cdots \supseteq \mathcal{N}^n(P) = conv(S)$. Furthermore, a polynomial time oracle machine was given that converts maximization over P to maximization over $\mathcal{N}(P)$. This naturally raises the following question. Do there exist approximations $P(S)$ for all n and $S \subseteq \{0,1\}^n$, and a single oracle machine M, such that M^S maximizes linear functionals over $P(S)$ in polynomial time? In the following section, we provide a positive answer by constructing a family of such machines. As a result, the operator introduced in [LS91] could be systematically applied to any combinatorial optimization problem.

5.2 Approximating machines

In [GLS81] (see [Lov86]), a certain algorithmic equivalence was established between the problem of maximizing linear functionals over a rational polytope P and the following *separation* problem over P: given $x \in \mathbb{Q}^n$, decide whether $x \in P$ and, if not, provide a vector $y \in \mathbb{Q}^n$ separating x from P, i.e., satisfying $\langle y, z \rangle < \langle y, x \rangle$ for all $z \in P$. We shall start by studying separation, rather than maximization, over our approximations. An oracle machine M will be called *approximating*, if M^S solves the separation problem over some approximation $P(S)$ of S for every n and every $S \subseteq \{0,1\}^n$.

For every positive integer k, we construct an approximation $P_k(S)$ of S for every S, and a related approximating oracle machine M_k. Our approximations have the property $P_1(S) \supseteq P_2(S) \cdots \supseteq P_n(S) \supseteq conv(S)$, and $P_n(S)$ is the smallest

intersection of $[0,1]^n$ and a polytope whose facet normals are in $\{-1,1\}^n$, which contains S. Our machines run in *strongly polynomial time* (see [Lov86], [Tar86]), that is, M_k^S runs in time polynomial in the size $n + b(x)$ of the input (n, x) and performs a number of arithmetic operations bounded by a polynomial in n only.

We need some notation. Throughout the rest of the note, a, b, c denote elements (or variables) of the unit cube $[0,1]^n$, u, v, w denote elements of $\{0,1\}^n$, x, y, z elements of $\mathbb{Q}^n$, and n, m, k positive integers. The inner product of two vectors x, y will be abbreviated $\langle x, y\rangle = xy$. We let $e = (1, \cdots, 1)$, and, for any x we let $\bar{x} = 2x - e$ and $|x| = ||x||_1 = \sum_{i=1}^n |x_i|$. Finally, for any v and m (to be interpreted as "for any $v \in \{0,1\}^n$ and any $m \in \mathbb{N}$") we let $B(v, m) = \{u : \ |u - v| < m\}$.

Now, let k, n, and $S \subseteq \{0,1\}^n$ be arbitrary. For any v, let $k_v = min\{inf_{u \in S}|u - v|, \ k\}$. Define $P_k(S) = \cap_v\{a : \ |a - v| \geq k_v\}$. It is easy to check that $S = \cap_v\{u : |u - v| \geq k_v\}$, so that $P_k(S) \cap \{0,1\}^n = S$. The observation below is easy to verify (but does not hold in general for rational vectors outside the unit cube).

Observation 5.2.1 *For every a and v we have $|a - v| = |a| + |v| - 2av = |v| - \bar{v}a$.*

It follows that $P_k(S) = \cap_v\{x : \ \bar{v}x \leq |v| - k_v\} \cap [0,1]^n$ is a convex polytope, so $P_k(S)$ is indeed an approximation of S.

For any a let $[a]$ be the *rounding* of a, i.e. the vector having $[a]_i = 0$ if $a_i < \frac{1}{2}$ and $[a]_i = 1$ if $a_i \geq \frac{1}{2}$. We have the following proposition.

Proposition 5.2.2 *A point a does not belong to $P_k(S)$ if and only if there exists $v \in B([a], 2k)$ for which $|a - v| < k_v$.*

Proof. By definition of $P_k(S)$, if such v exists then $a \notin P_k(S)$. To prove the converse, note first that for every a and v we have $|a - [a]| \leq |a - v|$. Now, if $a \notin P_k(S)$ then there exists some v for which $|a - v| < k_v$, but then $|a - [a]| \leq |a - v| < k_v$ as well, so by the triangle inequality $|v - [a]| \leq |v - a| + |a - [a]| < 2k_v \leq 2k$, so $v \in B([a], 2k)$. □

Theorem 5.2.3 *For every k, there exists a strongly polynomial time oracle machine M_k such that, for all n and $S \subseteq \{0,1\}^n$, M_k^S solves the separation problem over $P_k(S)$.*

Proof. It is easy to check whether $x \in [0,1]^n$, and if not provide a vector separating x from $[0,1]^n$, hence from $P_k(S)$. So, we may assume that $x = a \in [0,1]^n$, and obtain $[a]$. By the proposition above, $a \in P_k(S)$ unless there exists $v \in B([a], 2k)$ for which $|a - v| < k_v$, in which case the vector $\bar{v}$ separates a from $P_k(S)$, since $\bar{v}y \leq |v| - k_v < \bar{v}a$ for all $y \in P_k(S)$. Thus, we have to compute k_v and check if $|a - v| < k_v$ for no more than $|B([a], 2k)| = \sum_{i=0}^{2k-1} \binom{n}{i} < n^{2k}$ elements v. Now, clearly $k_v = min\{inf\{|u - v| : u \in S \cap B(v,k)\}, k\}$, so for any v we can compute k_v by querying whether $u \in S$ for no more than $|B(v,k)| < n^k$ elements u, and doing $O(n^k)$ comparisons. Thus, the overall time required for carrying out this procedure is polynomial in $n + b(x)$, and the number of arithmetic operations is of order n^{3k}. □

Using the terminology of [Lov86], the *facet complexity* of a rational polytope is the maximum number of bits needed to encode any of its facets. It is easy to see that for all k, our $P_k(S)$ has facet complexity of order n. Thus, by [Lov86, Thm. 2.3.3], our machine M_k could be converted into a polynomial time oracle machine that will maximize linear functionals over our approximations. Combining this with the results of [LS91], we obtain the following corollary.

Corollary 5.2.4 *For every k and m, a polynomial time oracle machine $N_{k,m}$ exists such that, for all n and $S \subseteq \{0,1\}^n$, $N_{k,m}^S$ maximizes rational linear functionals over $\mathcal{N}^m(P_k(S))$, providing an approximate solution to the maximization problem over S. When $n \leq m$, $N_{k,m}^S$ solves the maximization problem over S itself.*

5.3 Discussion

One can restrict the class of admissible sets $S \subseteq \{0,1\}^n$ by studying a machine M designed to maximize over a specified language $L \subseteq \{0,1\}^* = \cup_{n \geq 0}\{0,1\}^n$, i.e., require M^S to maximize only for $S = L_n = L \cap \{0,1\}^n$. Yet, even such a specialized machine is often unlikely to run in polynomial time, as demonstrated by the language L of characteristic vectors of Hamiltonian cycles in complete graphs. Indeed, if it existed, a polynomial time oracle machine maximizing over L could be converted into a polynomial time Turing (non-oracle) machine M, simulating the oracle by a polynomial time decision procedure for L. But then M would solve the *Traveling salesman problem*, implying the unlikely equality between deterministic and nondeterministic polynomial time (see [HU79]).

When maximization over such a single language L is desired, one can alternatively study Turing (non-oracle) machines having L built into them, so that on input (n, x) the machine should maximize x over the built-in L_n. In this setting it is easy to demonstrate languages for which no polynomial time maximizing machine exists. Indeed, for any language L and any $v \in \{0,1\}^n$, the maximum value of $x = \bar{v}$ over L_n is $|v|$ if and only if $v \in L$. Thus, if a maximizing Turing machine for L has time complexity $T(m)$, then L can be decided in time $T(m) + O(m)$. Hence, for example, no polynomial time Turing machine exists for maximizing over the *first order theory of reals with addition*, a language whose decision procedure is known to require nondeterministic exponential time [HU79].

As noted before, for all n and $S \subseteq \{0,1\}^n$, our $P_n(S)$ is the smallest intersection of $[0,1]^n$ and a polytope whose facet normals are in $\{-1,1\}^n$, which contains S. It is interesting to ask whether another family of approximations $Q_k(S)$ could be found, with algorithmic properties similar to our $P_k(S)$, and the stronger geometric property that $Q_n(S) \subseteq P_n(S)$ be the smallest polytope whose facet normals are in $\{-1,0,1\}^n$ which contains S.

It is easy to see that when $n > 2k$, the polytope $P_k(S)$ is full-dimensional

for all $S \subseteq \{0,1\}^n$. If $conv(S)$ is not full-dimensional, it is desirable to use our approximations intersected with the affine hull of S which is often known, that is, to modify our machines M_k so that M_k^S will solve the separation problem over $P_k(S) \cap aff(S)$ rather than $P_k(S)$. In particular, if a language $L \subseteq \{0,1\}^*$ admits a polynomial time algorithm that solves the separation problem over $aff(L_n)$ for all n, then indeed, both M_k and $N_{k,m}$ could be modified so that in polynomial time $M_k^{L_n}$ will solve the separation problem over $P_k(L_n) \cap aff(L_n)$, and $N_{k,m}^{L_n}$ will maximize over $\mathcal{N}^m(P_k(L_n) \cap aff(L_n))$. A typical example is provided again by the language of Hamiltonian cycles above, where a polynomial time separation algorithm for the affine hulls does exist.

Chapter 6

Further Questions

In this concluding chapter, we emphasize some of the questions raised in previous chapters, and mention more related questions which are being investigated by the author.

In Chapter 1, we mentioned the following fundamental question. Given a sequence of representations $\pi_n : G_n \longrightarrow GL(\mathcal{K}^{d(n)})$, what is the $\mathcal{K}$-dimension of the span of $\pi_n(G_n)$ in $\mathcal{K}^{d(n)\times d(n)}$? The key to the answer is provided by the decompositions of the representations into irreducible components. As discussed in Chapter 3 and is well-known (see [Vin89]), if a representation $\pi : G \longrightarrow GL(\mathcal{K}^d)$ has a decomposition $\pi = \oplus_{i=1}^m \pi_i$ into isotypic components over $\mathcal{K}$, that is, each π_i is a direct sum of several copies of a single irreducible representation χ_i of G over $\mathcal{K}$ and no two distinct χ_i and χ_j are isomorphic, then $dim(\pi(G)) = \sum_{i=1}^m dim^2(\chi_i)$. The isotypic decompositions of Young representations are well-understood [Jam78], and for each sequence of Young representations as in Chapter 2 indexed by a sequence of partitions $(n - \sum_{i=2}^k \lambda_i, \lambda_2, \cdots, \lambda_k)$ one can write a constant-length-formula for the dimension $dim_{\mathcal{K}}(\pi_n(S_n))$ as a function of n. In the case $\mathcal{K} = \mathbb{R}$ or $\mathbb{Q}$, this dimension is also the affine dimension of the representation polytope $P(\lambda)$ and is of special interest to us. However, for an arbitrary λ-Young representation, the size of the sum-of-squares-formula above for the dimension can grow exponentially. It

is an interesting question whether a nicer formula, say of length which depends on the number of parts of λ only, or at least a polynomial time procedure for computing $dim(P(\lambda))$ - the input being λ - exists.

The polytope and oriented matroid stratifications of real affine space induced by Young representations are still not very well understood. A more thorough understanding may be at hand for the standard representation of S_n. While much information about the polytope stratification in this case is provided by Rado's theorem - which implies, for example, that there is only one polytope stratum with nonempty interior, the one containing all generic points - the oriented matroid stratification gives rise to many questions. One important goal is to understand the combinatorial-topological structure of the stratification in the following sense. A well-known theorem [Hir75] says that a real semialgebraic set is always a polytope, i.e. the realization space of some finite simplicial complex. It would be very satisfactory, but probably hard, to find a simplicial complex representation of each stratum, together with the partial order on them defined by setting $\Delta_1 < \Delta_2$ whenever Δ_1 is contained in the boundary of Δ_2.

Another project, mentioned in Chapter 2, is to investigate the change in the computational complexity of the optimization problem over a sequence of orbit polytopes when changing the orbit in a continuous and uniform way. For example, taking $h_n, m_n \in \{0,1\}^{\binom{n}{2}}$ to be a Hamiltonian cycle and a maximum matching in the complete n-graph K_n, we have for every $\alpha \in [0,1]$ the decision problem related to linear optimization over the sequence $P((n-2,2), \alpha h_n + (1-\alpha)m_n)$. This problem is polynomial time solvable for $\alpha = 0$ but NP-complete for $\alpha = 1$, and the question is what is the complexity for other values of α.

The generic matroid we associate with each group representation is an interesting object of study. As in Section 1.1, let $\mathcal{K}$ be a field, $\mathcal{F} = \mathcal{K}(x_1, \cdots, x_d)$, and $x = (x_1, \cdots, x_d) \in \mathcal{F}^d$. The generic matroid of the representation $\pi : G \longrightarrow GL(\mathcal{K}^d)$ is then the matroid of $\mathcal{F}$-linear relations on the orbit $Gx \subset \mathcal{F}^d$. The

problem here, which is currently being studied by the author, is to characterize those d-subsets which form bases of this matroid. We believe that the key to the solution lies in the decomposition of π into irreducible representations. With this in mind, one of the directions currently taken by the author in trying to resolve this problem is the use of the $\mathcal{A}$-module structure of Gx regarded as lying in $\mathcal{A}^d$, where $\mathcal{A} = \mathcal{K}[x_1, \cdots, x_d]$. As mentioned before, a d-subset of the orbit is a basis if and only if the $\mathcal{A}^d$-submodule it generates is free of rank d. While the module generated by the entire orbit was studied in Chapter 3, understanding the submodules generated by d-subsets is still on the way. A more general question than the matroidal one is the determination of the rank and minimal number of generators of all submodules generated by d-subsets.

Turning to the Radon invariant of the integer lattice, the main question remains of finding tighter lower and upper bounds - or better yet - an exact expression for the lattice Radon function $r(d)$ studied in Chapter 4. More generally, it is desirable to determine the lattice Tverberg function $t(k, d)$ which is the smallest n such that any n-subset of $\mathbb{Z}^d$ is k-partitionable so that the convex hulls of the parts intersect in an integer point. The determination of these numbers, as well as our study of the Radon numbers, is motivated in part by a conjecture of Eckhoff stating that, for an arbitrary convexity space, the kth Tverberg number is of order k times the 2nd Tverberg number. The lattice $\mathbb{Z}^d$ provides a nontrivial testing case for that conjecture.

We anticipate that finding an exact expression for $r(d)$, not to mention $t(k, d)$, may be very hard, perhaps impossible: it is not clear whether the function $r(d)$ is *computable* [HU79], or equivalently, whether the set $\{(d, r(d)) : d \in \mathbb{N}\}$ is *decidable*. It is easy to see that the set $\{(d, n) \in \mathbb{N}^2 : n < r(d)\}$ is *recursively enumerable*. Indeed, it is accepted by an algorithm that searches a grid $\{0, \cdots, g\}^d \subset \mathbb{Z}^d$ for a configuration of n points admitting no integral Radon partition. If such a configuration is found, then the pair (d, n) is correctly declared to satisfy $n < r(d)$,

whereas if none is found, the grid is increased by incrementing g and the search is resumed. Yet, to show that $r(d)$ is computable, one would need to prove that the complementary set $\{(d,n) \in \mathbb{N}^2 : \ n \geq r(d)\}$ is recursively enumerable as well, which is not clear.

Finally, we mention again the following question raised in Chapter 5. Is it possible to construct, for every k, approximations $Q_k(S)$ for all sets S of $\{0,1\}$-vectors, and an oracle Turing machine M_k such that M_k^S optimizes linear functionals over $Q_k(S)$ in polynomial time, and in addition, for every $S \subseteq \{0,1\}^n$, $Q_n(S)$ is the smallest polytope with facet normals in $\{-1,0,1\}^n$ containing S?

Bibliography

[AM69] M.F. Atiyah and I.G. Macdonald. *Introduction to Commutative Algebra.* Addison Wesley, Reading, Mass, 1969.

[Bar92] A.I. Barvinok. Combinatorial complexity of orbits in representations of the symmetric group. In A.M. Vershik, editor, *Representation Theory and Dynamical Systems*, pages 188–215. Adva. Soviet Math., 1992.

[BCS88] L.J. Billera, R. Cushman, and J.A. Sanders. The Stanley decomposition of the harmonic oscillator. *Proc. Kininklijke Nederlandse Akademie von Wetenschappen*, A91:375–393, 1988.

[BE75] D.A. Buchsbaum and D. Eisenbud. Generic free resolutions and a family of generically perfect ideals. *Advances in Math.*, 18:245–301, 1975.

[Bel77] D.E. Bell. A theorem concerning the integer lattice. *Stud. in Appl. Math.*, 56:187–188, 1977.

[Ber73] C. Berge. *Graphs and Hypergraphs.* North Holland, Amsterdam, 1973.

[BG77] R.A. Brualdi and P.M. Gibson. Convex polyhedra of doubly stochastic matrices: II. graph of ω_n. *J. Combin. Theory Ser. B*, 22:175–198, 1977.

[Bir46] G. Birkhoff. Très observaciones sobre el algebra linear. *Rev. Univ. Nac. Tucuman. Revista.*, A5, 1946.

[BLVS+92] A. Björner, M. Las Vergnas, B. Sturmfels, N. White, and G.M. Ziegler. *Oriented Matroids.* Cambridge University Press, Cambridge, 1992. In press.

[BR74] M.L. Balinski and A. Russakoff. On the assignment polytope. *SIAM Rev.*, 16:516–525, 1974.

[Brø83] A. Brøndsted. *An Introduction to Convex Polytopes.* Springer-Verlag, Berlin, 1983.

[BS92] L.J. Billera and B. Sturmfels. Fiber polytopes. *Ann. Math.*, 135:527–549, 1992.

[Buc85] B. Buchberger. Gröbner bases - an algorithmic method in polynomial ideal theory. In N.K. Bose, editor, *Multidimensional Systems Theory*, chapter 6. D. Reidel, 1985.

[BV88] A.I. Barvinok and A.M. Vershik. Convex hulls of representation orbits of finite groups and combinatorial optimization. *Funkts. Anal.*, 22:66–67, 1988.

[BZ92] D. Bernstein and A. Zelevinsky. Combinatorics of maximal minors. 1992. To appear.

[CFS86] W. Cook, J. Fonlupt, and A. Schrijver. An integer analogue of Carathéodory's theorem. *J. Combin. Theory Ser. B*, 40:63–70, 1986.

[CR62] C.W. Curtis and I. Reiner. *Representation Theory of Finite Groups and Associative Algebras.* Interscience, New York, 1962.

[DGK63] L. Danzer, B. Grünbaum, and V. Klee. Helly's theorem and its relatives. *Proc. Sympos. Pure Math.*, 7:101–180, 1963.

[Doi73] J.P. Doignon. Convexity in crystallographical lattices. *J. Geom.*, 3:71–85, 1973.

[Eck68] J. Eckhoff. Der satz von Radon in konvexen produktstrukturen i. *Monatsh. Math.*, 72:303–314, 1968.

[Eis89] D. Eisenbud. Commutative algebra with a view toward algebraic geometry. Lecture Notes 4, Brandeis University, Waltham, Mass., Spring 1989.

[Fed69] H. Federer. *Geometric Measure Theory.* Springer-Verlag, Berlin, 1969.

[GJ79] M.R. Garey and D.S. Johnson. *Computers and Intractability.* W.H. Freeman, San Francisco, Cal., 1979.

[GL87] P.M. Gruber and C.G. Lekkerkerker. *Geometry of Numbers.* North Holland, Amsterdam, 1987.

[GLS81] M. Grötschel, L. Lovász, and A. Schrijver. The ellipsoid method and its consequences in combinatorial optimization. *Combinatorica*, 1:169–197, 1981.

[Grü67] B. Grünbaum. *Convex Polytopes.* John Wiley, New York, 1967.

[Ham65] P.C. Hammer. Extended topology: Carathéodory's theorem on convex hulls. *Rend. Circ. Math. Palermo*, 14:34–42, 1965.

[Hir75] H. Hironaka. Triangulations of algebraic sets. *AMS Symp. in Pure Math.*, 29:165–185, 1975.

[HLP29] G.H. Hardy, J.E. Littlewood, and G. Pólya. Some simple inequalities satisfied by convex functions. *Messenger of Math*, 58:145–152, 1929.

[HU79] J.E. Hopcroft and J.D. Ullman. *Introduction to Automata Theory, Languages, and Computation.* Addison Wesley, Reading, Mass., 1979.

[Jam78] G.D. James. *The Representation Theory of the Symmetric Group.* Lecture Notes in Math. 682, Springer-Verlag, Berlin, 1978.

[Kal90] G. Kalai. Symmetric matroids. *J. Combin. Theory Ser. B*, 50:54–64, 1990.

[KO92] P. Kleinschmidt and S. Onn. On the diameter of convex polytopes. *Discr. Math.*, 1992. In print.

[Kun86] J.P.S. Kung. *A Source Book in Matroid Theory.* Birkhauser, Boston, Mass., 1986.

[Len83] H.W. Lenstra, Jr. Integer programming with a fixed number of variables. *Math. Oper. Res.*, 8:538–548, 1983.

[Lev51] F.W. Levi. On Helly's theorem and the axioms of convexity. *J. Indian Math. Society*, 15:65–76, 1951.

[Lov86] L. Lovász. *An Algorithmic Theory of Numbers, Graphs and Convexity.* CBMS-NSF Regional Conference Series on Applied Mathematics, Philadelphia, Penn., 1986.

[LS91] L. Lovász and A. Schrijver. Cones of matrices and set-functions and $0-1$ optimization. *SIAM J. Optim.*, 1:166–190, 1991.

[LV80] M. Las Vergnas. Convexity in oriented matroids. *J. Combin. Theory Ser. B*, 29:231–243, 1980.

[Mir63] L. Mirsky. Results and problems in the theory of doubly-stochastic matrices. *Z. Wahrscheinlichkeitstheorie und Verw. Gebiete*, 1:319–334, 1963.

[Nad89] D.J. Naddef. The Hirsch conjecture is true for $\{0,1\}$-polytopes. *Math. Prog.*, 45:109–111, 1989.

[NP84] D.J. Naddef and W.R. Pulleyblank. Hamiltonicity in (0−1)-polyhedra. *J. Combin. Theory Ser. B*, 37:41–52, 1984.

[Onn91] S. Onn. On the geometry and computational complexity of Radon partitions in the integer lattice. *SIAM J. Discr. Math.*, 4:436–447, 1991.

[Onn92] S. Onn. Geometry, complexity, and combinatorics of permutation polytopes. *J. Combin. Theory Ser. A*, 1992. To appear.

[Pap78] C.H. Papadimitriou. The adjacency relation on the traveling salesman polytope is NP-complete. *Math. Prog.*, 14:312–324, 1978.

[PR74] M.W. Padberg and M.R. Rao. The traveling salesman problem and a class of polyhedra of diameter two. *Math. Prog.*, 7:32–45, 1974.

[Rad52] R. Rado. An inequality. *J. London Math. Society*, 27:1–6, 1952.

[Sca77] H.E. Scarf. An observation on the structure of production sets with indivisibilities. *Proc. Nat. Acad. Sci. U.S.A.*, 74:3637–3641, 1977.

[Sch86] A. Schrijver. *Theory of Linear and Integer Programming.* John Wiley, New York, 1986.

[Sie77] G. Sierksma. Relationships between Carathéodory, Helly, Radon and exchange numbers of convexity spaces. *Nieuw Arch. Wisk.*, 3:115–132, 1977.

[Sta78] R.P. Stanley. Hilbert functions of graded algebras. *Advances in Math.*, 28:57–83, 1978.

[Sta83] R.P. Stanley. *Combinatorics and Commutative Algebra.* Birkhäuser, Boston, 1983.

[Stu90] B. Sturmfels. Gröbner bases and Stanley decompositions of determinantal rings. *Math. Z.*, 205:137–144, 1990.

[SZ92] B. Sturmfels and A. Zelevinsky. Maximal minors and their leading terms. *Advances in Math.*, 1992. To appear.

[Tar86] E. Tardos. A strongly polynomial algorithm to solve combinatorial linear programs. *Oper. Res.*, 34:250–256, 1986.

[Tve66] H. Tverberg. A generalization of Radon's theorem. *J. London Math. Society*, 41:123–128, 1966.

[Vin89] E.B. Vinberg. *Linear Representations of Groups.* Birkhäuser, Boston, 1989.