Universität Rostock

Traditio et Innovatio

Exploring core points for fun and profit — a study of lattice-free orbit polytopes

Dissertation
zur
Erlangung des akademischen Grades
doctor rerum naturalium (Dr. rer. nat.)
der Mathematisch-Naturwissenschaftlichen Fakultät
der Universität Rostock

vorgelegt von
Thomas Rehn

Rostock, 30. August 2013

urn:nbn:de:gbv:28-diss2014-0082-2

Gutachter:

Prof. Dr. Achill Schürmann, Universität Rostock
Prof. Dr. Marc Pfetsch, TU Darmstadt

Tag der öffentlichen Verteidigung:

9. Januar 2014

Contents

1. A Very Brief History of Core Points

This thesis is devoted to the study of lattice-free symmetric polytopes, whose vertices we will later get to know as core points. They first appeared in a geometrical examination of highly symmetric integer programming problems by Bödi, Herr & Joswig [BHJ13] and were then generalized by Herr, Rehn & Schürmann [HRS13]. Besides their applications in symmetric integer programming they are interesting geometric objects in their own right.

Lattice-free polyhedra and convex sets in general have been studied before, under different names and in various, slightly differing notions of lattice-freeness. The fact that lattice-free sets have a small width (are flat) in some sense was exploited by Lenstra [Len83] in his famous polynomial-time integer programming algorithm in fixed dimension.

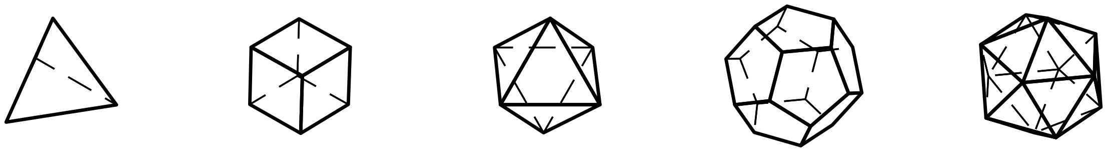


Figure 1.1.: Highly-symmetric: the five Platonic solids

Symmetric polyhedra have more appeal than their inherent beauty for the human eye. Symmetry adds structure to polytopes that can be used to make things easier which are difficult otherwise. For instance, the vertices of some polytopes can only be computed and some optimization problems only be solved if the underlying symmetry is taken into account (cf. [BDS09, Mar10]).

In this thesis we study properties of polytopes that are both symmetric and lattice-free, combining knowledge from these two worlds.

Outline

In Chapter 2 we settle necessary mathematical notation and remind ourselves of elementary theory that we will use in this thesis.

In Chapter 3 we first define core points as vertices of lattice-free orbit polytopes and study their elementary properties. As our orbit polytopes are the convex hulls of the orbit of one point each, they are a special class of symmetric polytopes. Throughout this thesis we study characteristics of core points and lattice-free orbit polytopes subject to some generating group. We show that core points cannot lie at arbitrary positions in space but must be close to an invariant subspace of the group. We then restrict our attention to groups which are permutation groups, i.e., groups which act on $\mathbb{R}^n$ by permuting coordinates. For these we introduce a notion of finiteness for the number of core points. In this sense we prove that the number of core points is finite for a special class of permutation groups (2-homogeneous permutation groups). We close with an analysis of core points of symmetric groups. The next three chapters discuss core points of different classes of permutation groups.

In Chapter 4 we treat the case of 2-homogeneous permutation groups, for which we know that the number of core points is finite. This enables us to perform an exhaustive computer search to find all core points for all pertinent groups in dimension twelve or less. To enumerate all core points we develop various necessary criteria for lattice-freeness, which limit the search space. Having computed a sample of core points, we prove some constructive sufficient criteria as well. We also study width-related properties of lattice-free orbit polytopes and prove a flatness theorem for orbit polytopes of 2-homogeneous groups.

In Chapter 5 we examine core points of transitive groups which are not 2-homogeneous. For these we cannot decide finiteness based on the previous results. The focus of this chapter is to prove that there are indeed infinitely many different core points. We see partial results in this direction, giving constructions based on minimal projections onto invariant subspaces, for instance, for imprimitive groups. We discuss solution strategies to close the remaining gap. At the end of the chapter we look at computational aspects of the core point constructions: computing invariant subspaces and minimal projections.

In Chapter 6 we briefly touch upon intransitive groups. As a case study we analyze the core points of subdirect products of two symmetric groups. This sample is already enough to highlight differences that occur between transitive and intransitive groups with respect to the finiteness of the number of core points.

In Chapter 7 we look at the original application for core points: integer programming. We analyze several core point based algorithms to solve symmetric integer programs and discuss results of computational experiments. Furthermore, we study examples of easy looking integer programming instances which are based on lattice-free symmetric simplices but are hard to solve for standard optimization software. We see that solving these problems can be simplified by using a variant of Lenstra's original integer programming algorithm [Len83]. The section closes with an analysis of the symmetry groups of real world integer programming problems. We survey the symmetries of the MIPLIB 2010 suite [KAA$^+$11] and discuss the applicability of the previously outlined core point based algorithms.

Parts of Chapters 4, 5 and 7 are a result of joint work with Katrin Herr & Achill Schürmann as published in [HRS13, Her13b]. The last chapter also includes parts of joint work with Marc Pfetsch [PR13]. All these collaborations will also be marked in the text.

2. Nota Bene

In this section we set up notation and we remind ourselves of some elementary definitions and facts from algebra and geometry.

2.1. Sets, vector spaces & lattices

We denote the set of all positive integers less or equal to some integer n by $[n] := \{1, \dots, n\}$. We write $\mathbb{Z}_{\geq 0}$ for the set of non-negative integers and $\mathbb{Z}_{>0}$ for the set of positive integers.

We will deal mostly with a real (Euclidean) vector space $\mathbb{R}^n$, which we endow with the standard inner product $\langle x, y \rangle := \sum_{i \in [n]} x_i y_i$ and the induced (Euclidean) norm $\|x\| := \sqrt{\langle x, x \rangle}$. We denote the canonical orthonormal basis vectors by $e^{(1)}, \dots, e^{(n)}$. We refer to the all-ones vector by $\mathbb{1} := (1, 1, \dots, 1)^\top$. Occasionally, we will also add a subscript, writing $\mathbb{1}_S := \sum_{i \in S} e^{(i)}$ for the characteristic vector of an index set S. We also set $\mathbb{1}_k := \mathbb{1}_{[k]} \in \mathbb{R}^k$ if we want to emphasize the ambient dimension. For a set $S \subset \mathbb{R}^n$ we denote by $\operatorname{span} S$, $\operatorname{conv} S$, $\operatorname{aff} S$, $\operatorname{cone} S$ its linear, convex, affine and conic (positive) hull, respectively. We write $\mathrm{GL}(V)$ for the group of all automorphisms of V. For a ring R we write $\mathrm{GL}_n(R)$ for the invertible $n \times n$-matrices. In particular, the group $\mathrm{GL}_n(\mathbb{Z})$ of unimodular matrices, i.e., integral matrices with determinant ± 1, will play an important role. This group consists of all matrices that map integral vectors on integral vectors and thus preserve the standard lattice $\mathbb{Z}^n$.

Let $\Lambda \subset \mathbb{R}^n$ be an arbitrary lattice, i.e., a discrete additive subgroup of $\mathbb{R}^n$. The **dual lattice** is given by $\Lambda^* = \{x \in \mathbb{R}^n : \langle u, x \rangle \in \mathbb{Z} \text{ for all } u \in \Lambda\}$. Important examples for lattices that we will work with are the lattices $\mathsf{A}_n = \{z \in \mathbb{Z}^{n+1} : \langle \mathbb{1}, z \rangle = 0\}$ of rank n in ambient dimension $n+1$ and their duals A_n^* (see also [CS99]). A basis for the lattice A_n is given by $b^{(j)} := e^{(j)} - e^{(j+1)} \in \mathbb{Z}^{n+1}$ for $j \in [n]$. The dual A_n^* has $b'^{(j)} := e^{(j)} - \frac{1}{n+1} \mathbb{1}_{n+1}$ for $j \in [n]$ as a basis. We call a translate $a + \Lambda := \{a + u : u \in \Lambda\}$ for $a \in \mathbb{R}^n$ an **affine lattice**.

2.2. Permutation groups

We stick to Knuth [Knu91] for his compact notation of group inverses, so g^- shall be the inverse group element of g. We denote by $\mathcal{S}_n$ the symmetric group of degree n, i.e., the group of all permutations of $[n]$; $\mathcal{A}_n$ denotes the alternating group of degree n. We say that a group $G \leq \mathcal{S}_n$ is **transitive**/acts transitively on $[n]$, if it has only one orbit on $[n]$. For every number $k \in [n]$ the permutation group G also acts naturally on the k-sets and k-tuples of $[n]$. We say that G is k-**homogeneous** if it acts transitively on all k-element subsets of $[n]$. Similarly, G is called k-**transitive** if it acts transitively on the set of k-tuples with pairwise distinct elements of $[n]$. More information about permutation groups can be found, for instance, in Cameron's book [Cam99].

A basic fact from permutation group theory is that every finite permutation group is a so called subdirect product of transitive groups (cf. [Cam99, Thm. 1.2]). Let $G := \bigtimes_{i=1}^{k} G_i$ be a direct product of groups G_i. For each factor there is a projection map $\pi_i : G \to G_i$ which maps $g_1 g_2 \cdots g_k \in G$ to g_i. A group H is a **subdirect product** of groups $G_1, \ldots, G_k$ if two things hold. First, H is a subgroup of the direct product $G_1 \times \cdots \times G_k$. Second, for each of these factors the restriction of the map π_i to H is surjective. We say that a subdirect product H is **proper** if H is not a direct product.

Example 2.1. Let $G_1 := \langle (1\,2), (3\,4) \rangle$ and $G_2 := \langle (1\,2)(3\,4) \rangle$ be two permutation groups on the set $\{1, 2, 3, 4\}$. The first group $G_1 \cong \mathcal{S}_2 \times \mathcal{S}_2$ is a direct product of two cyclic groups. The second group $G_2 \cong \mathcal{S}_2$ is a subdirect product of two cyclic groups. Restricted to each of the sets $\{1, 2\}$ and $\{3, 4\}$ individually, the group G_2 looks like a cyclic group, but these actions are not independent like in the case of G_1.

For some computations we will use the computer algebra system [GAP] and its library of permutation groups. In particular we refer to concrete primitive groups (a term which we will define later in Section 5.3.1) by their (primitive) id in GAP. A group with id n-k is the `PrimitiveGroup(`n`,`k`)` in GAP (and also in [`Sage`]).

2.3. Representations

In this section we remind ourselves of the very basics of representation theory. More information can be found, for instance, in [JL01] and [Ser77]. Let V be a vector space over a field K. Given a group G and a vector space V, a representation of G is a homomorphism $\rho : G \to \mathrm{GL}(V)$. A representation is called reducible if there exists a subspace W with $\{0\} \subsetneq W \subsetneq V$ which is invariant under $\rho(G)$. That is, for all $g \in G$ and $w \in W$ we must have $\rho(g)w \in W$. We call W an **invariant subspace** for ρ. For such a W we can restrict the action of ρ to W and obtain another representation $\rho|_W : G \to \mathrm{GL}(W)$ of G. We call this $\rho|_W$ a **subrepresentation** of ρ. A representation ρ is called completely reducible if ρ can be decomposed into a direct sum of irreducible subrepresentations. In terms of invariant subspaces, this means we find invariant subspaces $V_1, \ldots, V_k$ such that

$$V = V_1 \oplus \cdots \oplus V_k \tag{2.1}$$

and the induced subrepresentations $\rho|_{V_i}$ are irreducible. Maschke's Theorem states that every reducible representation of a finite group G over a field whose characteristic is prime to $|G|$ is completely reducible. This decomposition does not have to be unique (see, for instance, Example 6.5 on page 84).

Example 2.2. As a first example consider a cyclic group $\mathcal{C}_n$ of order n. A one-dimensional representation $\rho_1 : \mathcal{C}_n \to \mathbb{C}$ in complex numbers is given by $\rho_1(g) := \zeta$ where g is a generator of $\mathcal{C}_n$ and $\zeta := \exp(\frac{2\pi i}{n})$ is a primitive root of unity. Another representation of $\mathcal{C}_n$ in dimension n is given by $\rho_2 : \mathcal{C}_n \to \mathrm{GL}_n(\mathbb{C})$ with

$$\rho_2(g) := \left(\begin{array}{c|c} 0 & I_{n-1} \\ \hline 1 & 0 \end{array}\right)$$

where I_{n-1} is the identity matrix. Consider the vector $u^{(j)} := (1, \zeta^j, \zeta^{2j}, \ldots, \zeta^{(n-1)j})^\top$ for some $j \in [n]$. We then have $\rho_2(g)u^{(j)} = \zeta^j u^{(j)}$. Therefore, $\operatorname{span} u^{(j)}$ is an invariant subspace of $\mathbb{C}^n$. Hence, ρ_2 is reducible and thus completely reducible. We can decompose $\mathbb{C}^n = \bigoplus_{j=1}^n (\operatorname{span} u^{(j)})$ into a direct sum of one-dimensional invariant subspaces, which are pairwise orthogonal with respect to the Hermitian inner product $\langle x, y\rangle = \sum_{i=1}^n x_i \overline{y_i}$. Note that, if $u^{(j)}$ is not real, then $u'^{(j)} := u^{(j)} + u^{(n-j)}$ is a real vector and its orbit spans a two-dimensional invariant subspace of $\mathbb{R}^n$. We will see another example for the decomposition of representations and this “real” construction again later in Section 5.5.1. ■

Another example that is very important for this thesis is the following. Consider a permutation group $G \leq \mathcal{S}_n$. Then there is a canonical permutation representation $\rho : G \to \mathrm{GL}_n(K)$ by permutation matrices. For every group element $g \in G$ we define $\rho(g)$ to be the matrix which has a one at the $g(j)$-th row of each column j and zeros at all other places. For a field of characteristic zero the representation ρ is completely reducible. Regardless of G, we always have the linear hull of the all-ones vector $\operatorname{span} \mathbb{1}$ as invariant subspace. Since all permutation matrices are orthogonal matrices, all invariant subspaces are pairwise orthogonal with respect to the standard inner product. Depending on the group and the base field K, the orthogonal complement $(\operatorname{span} \mathbb{1})^\perp$ is reducible or irreducible.

Example 2.3. The representation ρ_2 from Example 2.2 provides an example for the canonical permutation representation of the cyclic group $\langle (1\,2\,\ldots\,n)^- \rangle$. The subspace $\operatorname{span} u^{(n)}$ is equal to $\operatorname{span} \mathbb{1}$. Its complement $(\operatorname{span} \mathbb{1})^\perp$ is irreducible if $K = \mathbb{Q}$ and n is a prime number, and it is reducible if $K = \mathbb{R}$ and $n \geq 4$. ■

Every linear group $G \leq \mathrm{GL}_n(K)$ preserves a set of vectors pointwise. We call this set

$$\mathrm{Fix}(G) := \{x \in K^n \ : \ gx = x \text{ for all } g \in G\}$$

the **fixed space**. This term is justified because $\mathrm{Fix}(G)$ can easily be seen to be a linear subspace of K^n. Every fixed space, which is a set that is preserved pointwise, is also an invariant subspace, which is a set that is preserved setwise.

Remark 2.4. For $G \leq \mathrm{GL}_n(\mathbb{Z})$ the intersection $\mathrm{Fix}(G) \cap \mathbb{Z}^n$ is a lattice. We denote it by $\mathrm{Fix}_{\mathbb{Z}}(G)$. Since the fixed space has a rational basis, the rank of $\mathrm{Fix}_{\mathbb{Z}}(G)$ and the dimension of $\mathrm{Fix}(G)$ coincide.

Example 2.5. Let $\rho(G) \leq \mathrm{GL}_n(\mathbb{Z})$ be the canonical representation of a permutation group $G \leq \mathcal{S}_n$. Let $O_1, \ldots, O_k \subseteq [n]$ be the orbits of G. Then $\dim \mathrm{Fix}(\rho(G)) = k$. The fixed space $\mathrm{Fix}(\rho(G))$ and also its lattice $\mathrm{Fix}_{\mathbb{Z}}(\rho(G))$ are spanned by the following pairwise orthogonal vectors $f^{(1)}, \ldots, f^{(k)}$:

$$f_j^{(i)} := \begin{cases} 1 & \text{if } j \in O_i, \\ 0 & \text{if } j \notin O_i. \end{cases}$$

In particular, if G has only one orbit, i.e., G is transitive, then $\mathrm{Fix}(\rho(G)) = \operatorname{span} \mathbb{1}$. ■

2.4. Polytopes

A polytope $P \subset \mathbb{R}^n$ can be described in two different ways. Either by a set of inequalities whose solution set is bounded or as a convex hull of a finite set:

$$P = \{x \in \mathbb{R}^n \ : \ Ax \leq b\} = \operatorname{conv} V$$

where $A \in \mathbb{R}^{m \times n}$, $b \in \mathbb{R}^m$, and $V \subset \mathbb{R}^n$ is a finite set. We refer to the first way as **facet** or **inequality description** and to the second way as **vertex description**. We write $\operatorname{vert} P$ for the set of vertices of P. More information about polytopes can be found in Ziegler's book [Zie95]. Computing one description from the other is an instance of the so called description conversion or representation conversion problem whose complexity is unknown (for a discussion see [KBB$^+$08]). We will perform all practical computations concerning polytopes with [`polymake`], which also integrates software packages for description conversion ([`cdd`, `lrs`]), description conversion up to symmetry ([`SymPol`]) and group actions ([`PermLib`]).

2.5. Convex geometry

For some proofs we will need a pinch of convex geometry. For a vector $v \in \mathbb{R}^n$ and a convex set $C \subset \mathbb{R}^n$ we define its **width** $\omega(C, v)$ **in direction** v as

$$\omega(C, v) := \max_{x \in C} \langle v, x \rangle - \min_{x \in C} \langle v, x \rangle \, .$$

The **width** $\omega(C)$ of C is the minimal width over all non-zero directions with normalized length: $\omega(C) := \min_{v \in \mathbb{R}^n, \|v\|=1} \omega(C, v)$. If we study the interplay with a lattice Λ, then the **lattice width** $\omega_\Lambda(C)$ is $\omega_\Lambda(C) := \min_{v \in \Lambda^* \setminus \{0\}} \omega(C, v)$ where Λ^* is the dual lattice of Λ. The following theorem is originally due to Khinchin [Khi48].

Theorem 2.6 (Flatness Theorem, [Khi48]). Let ω_Λ denote the lattice width with respect to the lattice $\Lambda \subset \mathbb{R}^n$. There exists a constant $c(n)$ depending only on n with the following property: If a convex set $C \subset \mathbb{R}^n$ does not contain a lattice point, then there exists a non-zero vector $v \in \Lambda^* \setminus \{0\}$ in the dual lattice with $\omega_\Lambda(C, v) \leq c(n)$. In other words, C is "flat" in direction of v.

In general the best choice for the flatness constant $c(n)$ is unknown and the best bounds are only asymptotic. One can choose $c(n) = n^{5/2}$ [Bar02] and asymptotically $c(n) = O\big(n^{3/2}\big)$ [BLPS99]. For the plane, however, the optimal solution is known and was proven by Hurkens [Hur90, p. 122].

Theorem 2.7 (Flatness Theorem in Dimension Two, [Hur90]). Let $P \subset \mathbb{R}^2$ be a convex polygon and $\omega_\Lambda(P)$ its lattice width for a lattice $\Lambda \subset \mathbb{R}^2$. If $\omega_\Lambda(P) \geq 1 + \frac{2}{\sqrt{3}}$, then P contains a lattice point that is not a vertex of P.

More information about convex geometry in general and the flatness theorem in particular can be found in Barvinok's book [Bar02].

3. Meet the Core Points

3.1. Lattice-free & orbit polytopes, core points

As outlined in the introduction, this thesis is about lattice-free and symmetric polytopes. In this section we look at definitions that clarify these two terms.

Definition 3.1. Let $P \subset \mathbb{R}^n$ be a polytope with integral vertices. We call P **lattice-free** if and only if $P \cap \mathbb{Z}^n = \operatorname{vert} P$ where $\operatorname{vert} P$ is the set of vertices of P.

Lattice-freeness has been used in the literature with slightly varying semantics. This Definition 3.1 is the same as in [BK00, Kan99, DO95]; in [Seb99, HZ00] lattice-free polytopes are called empty. These articles are mostly concerned with width-related properties of lattice-free polytopes. Other notions of lattice-freeness are used, for instance, in [AWW11] and [Lov89], where a convex set is lattice-free iff its interior does not contain integral points. These classification results are not applicable for lattice-freeness in the sense of Definition 3.1. Since we forbid non-vertex integral points on the boundary, we slightly abuse nomenclature and call x an **inner point** of a polytope P iff $x \in P \setminus \operatorname{vert}(P)$.

We use the following construction. Let $G \leq \mathrm{GL}_n(\mathbb{Z})$ be a finite group and let Gz be the orbit of some point $z \in \mathbb{Z}^n$. We call the convex hull of this orbit an **orbit polytope**. This name was introduced by Onn [Onn93] in the context of permutation polytopes. The same object also is called an orbitope by Sanyal, Sottile *&* Sturmfels [SSS11] who primarily study orbit polytopes of infinite linear groups.

Definition 3.2. Let $G \leq \mathrm{GL}_n(\mathbb{Z})$ be a finite group of unimodular matrices. A point $z \in \mathbb{Z}^n$ is called a **core point** for G if and only if the orbit polytope $\operatorname{conv}(Gz)$ is lattice-free, i.e., $(\operatorname{conv}(Gz)) \cap \mathbb{Z}^n = Gz$. We call the set of all core points of G its **core set** and denote it by $\operatorname{core}(G)$. If we refer to all core points in some set $S \subset \mathbb{R}^n$, we write denote these by $\operatorname{core}(G, S) := \operatorname{core}(G) \cap S$.

This definition of a core point slightly generalizes the permutation group definition by Herr, Rehn *&* Schürmann in [HRS13], which considers only permutation groups and which in turn is a natural augmentation of the original core point concept for symmetric groups by Bödi, Herr *&* Joswig [BHJ13]. In these articles core points were introduced as a tool to solve symmetric integer programs.

Example 3.3. As a first example we consider the matrix group $D_8 = \left\langle \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}, \begin{pmatrix} -1 & 0 \\ 0 & 1 \end{pmatrix} \right\rangle$. This group is a dihedral group of order eight and also the symmetry group of the square $[-1, 1]^2$. The orbit of $z = (z_1, z_2)^\top \in \mathbb{Z}^2$ contains the four points

$$a = z = \begin{pmatrix} z_1 \\ z_2 \end{pmatrix}, b = \begin{pmatrix} z_2 \\ z_1 \end{pmatrix}, c = \begin{pmatrix} -z_1 \\ z_2 \end{pmatrix}, d = \begin{pmatrix} -z_2 \\ z_1 \end{pmatrix}.$$

If z is not the zero vector, then $\frac{1}{2}(a+c)$ or $\frac{1}{2}(b+d)$ is an inner integral point of $\operatorname{conv} D_8 z$. Thus, $\operatorname{core}(D_8)$ consists only of the zero vector.

As a second example we look at the canonical matrix representation of the cyclic group $\mathcal{C}_3 = \langle(1\,2\,3)\rangle$. The orbit of $e^{(1)} = (1,0,0)^\top$ consists of the three standard basis vectors $e^{(1)}$, $e^{(2)}$ and $e^{(3)}$. Every point in the convex hull of these three points can be written as $(\lambda_1, \lambda_2, \lambda_3)^\top$ with $\lambda_i \in [0,1]$ and $\lambda_1 + \lambda_2 + \lambda_3 = 1$. This shows that the simplex $\operatorname{conv} \mathcal{C}_3 e^{(1)}$ is lattice-free. Hence, $e^{(1)}$, $e^{(2)}$ and $e^{(3)}$ are core points for $\mathcal{C}_3$. ■

Remark 3.4. We have the following elementary properties of core sets which are easy to prove.

(i) Core sets are G-symmetric:
$\operatorname{core}(G) = G \operatorname{core}(G)$.

(ii) Core sets are centrally symmetric:
$\operatorname{core}(G) = -\operatorname{core}(G)$.

(iii) Subgroup relation corresponds to core set inclusion:
$\operatorname{core}(G) \subseteq \operatorname{core}(H)$ for every $H \leq G$.

(iv) Core sets contain all integral points from the fixed space:
$\operatorname{core}(G) \supseteq \operatorname{Fix}_{\mathbb{Z}}(G)$.

(v) Core set structure is preserved by some translations:
$\operatorname{core}(G, S + z) = \operatorname{core}(G, S) + z$ for every set $S \subset \mathbb{R}^n$ and $z \in \operatorname{Fix}_{\mathbb{Z}}(G)$.

If we want to describe core sets for concrete groups, it is cumbersome to work with $\operatorname{core}(G)$ directly. If the dimension of the fixed space is positive, then $\operatorname{core}(G)$ contains the infinitely many integral points in the fixed space (cf. Remark 3.4 (iv)). Similarly, if a core set contains another point $z \notin \operatorname{Fix}(G)$ that is not in the fixed space, we also immediately obtain infinitely many core points. Translating z using Remark 3.4 (v) or applying group elements to z as in Remark 3.4 (i) yields infinitely many different points. We remove this computational redundancy by the following equivalence relation.

Definition 3.5. Two points $x, y \in \mathbb{Z}^n$ shall be called **isomorphic** if there exists a $g \in G$ such that $x - gy \in \operatorname{Fix}_{\mathbb{Z}}(G)$. This is an equivalence relation because $\operatorname{Fix}_{\mathbb{Z}}(G)$ is a lattice. We define a **fundamental core set** of G to be a set of equivalence class representatives of all core points. To denote an (arbitrary) fundamental core set of G we write $\operatorname{fcore}(G)$.

Note that fundamental core sets are well-defined since every point isomorphic to a core point is again a core point by Remark 3.4. As mentioned above, a fundamental core set often allows a concise description of a core set since we have

$$\operatorname{core}(G) = \{gx + z \ : \ x \in \operatorname{fcore}(G),\ g \in G,\ z \in \operatorname{Fix}_{\mathbb{Z}}(G)\}\,. \tag{3.1}$$

Remember that we can describe the lattice $\operatorname{Fix}_{\mathbb{Z}}(G)$ by its finite basis. If $\operatorname{fcore}(G)$ is finite, we thus obtain a finite description of the possibly infinite set $\operatorname{core}(G)$. We will see later that this finiteness is important for many applications. Also note that Definition 3.5 differs from Herr's definition of a fundamental core set in [Her13b, Def 4.10] by restricting it to orbit representatives and keeping the central symmetry (see Remark 3.4 (ii)). Both definitions thus induce the same notion of finiteness for transitive permutation groups (see also Remark 3.22).

Example 3.6. Consider the group $\mathcal{S}_2 = \langle g \rangle$ with $g = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$ of order two. For the lattice $\mathrm{Fix}_{\mathbb{Z}}(\mathcal{S}_2)$ of fixed integral points the vector $(1,1)^\top$ is a basis. Thus, the points $u = (1,0)^\top$, $v = (6,5)^\top$ and $w = (6,7)^\top$ all are isomorphic according to Definition 3.5 since $v - u = (5,5)^\top \in \mathrm{Fix}_{\mathbb{Z}}(\mathcal{S}_2)$ and $gw - u = (6,6)^\top \in \mathrm{Fix}_{\mathbb{Z}}(\mathcal{S}_2)$. In Section 3.4.3 we will see that in total there are only two equivalence classes with core points: $\mathrm{fcore}(\mathcal{S}_2) = \{(0,0)^\top, (1,0)^\top\}$. ■

3.2. The relationship of core points and invariant subspaces

In this section we prove that core points cannot lie at arbitrary positions. They must be close to an invariant subspace. For this we distinguish two cases, depending on the dimension of the fixed space. We start with the easy case that the group acts irreducibly on $\mathbb{R}^n$ and the fixed space is trivial, i.e., $\dim \mathrm{Fix}(G) = 0$. For the proof we use an important property of orbit polytopes.

Remark 3.7. Given a finite group $G \leq \mathrm{GL}_n(\mathbb{Z})$, consider the orbit polytope $\operatorname{conv} Gz$ for some $z \in \mathbb{Z}^n$. The vertex barycenter of the orbit polytope lies in the fixed space and is given by $\frac{1}{|G|} \sum_{g \in G} gz$.

We will often make use of the property that the vertex barycenter of an orbit polytope is easy to describe. One application is the following lemma, which generalizes the situation that we encountered in Example 3.3. For a finite subgroup of $\mathrm{GL}_n(\mathbb{Z})$ acting irreducibly on $\mathbb{R}^n$ the core set consists only of the zero vector.

Lemma 3.8. Let $G \leq \mathrm{GL}_n(\mathbb{Z})$ be a finite group. If the fixed space of G has dimension zero, then $\mathrm{core}(G)$ consists of only the zero vector.

Proof. Let $z \in \mathbb{Z}^n$ be an arbitrary integral point. As Remark 3.7 shows, the barycenter $\frac{1}{|G|} \sum_{g \in G} gz$ lies in the fixed space. Since the fixed space is a linear subspace of $\mathbb{R}^n$ of dimension zero, the barycenter thus equals zero. In particular, the barycenter is integral. It is a vertex if and only if $z = 0$. Thus, the orbit polytope $\operatorname{conv} Gz$ is lattice-free if and only if $z = 0$. Therefore this is the only core point of G. □

In the rest of the section we deal with the case that the fixed space is non-trivial, i.e., $\dim \mathrm{Fix}(G) \geq 1$. For the proof that core points lie close to an invariant subspace we use a well-known theorem from convex geometry ([Joh48], see also [Bar02, Chapter V]).

Theorem 3.9 (John ellipsoid [Joh48])**.** Let $K \subset \mathbb{R}^n$ be a convex body, i.e., K is compact and convex with non-empty interior. Then there is a unique ellipsoid $E \subset \mathbb{R}^n$ which contains K and which has minimal volume with this property. Further, a scaled version of E is in turn contained in K:

$$t + \frac{1}{n} E \subseteq K \subseteq E,$$

where $t \subseteq \mathbb{R}^n$ is a suitable translation vector that depends on the center of E. The scaling factor for E is optimal as the case of a simplex shows.

This ellipsoid is called the **minimal enclosing ellipsoid** of K. In order to describe the minimal enclosing ellipsoids of orbit polytopes, we have to take a closer look at invariant subspaces first. In the following let $G \leq \mathrm{GL}_n(\mathbb{Z})$ be a finite group. For the rest of this section let $\langle \cdot, \cdot \rangle_G : \mathbb{R}^n \times \mathbb{R}^n \to \mathbb{R}$ be a G-invariant inner product; for instance,

$$\langle x, y \rangle_G = \frac{1}{|G|} \sum_{g \in G} (gx)^\top (gy).$$

Moreover, all notions of orthogonality, for example, for projections and complements, shall be with respect to this invariant inner product. By $\|\cdot\|_G$ we denote the norm induced by the invariant inner product. As we saw in (2.1) before, we can decompose $\mathbb{R}^n$ into a direct sum of irreducible G-invariant subspaces:

$$\mathbb{R}^n = \mathrm{Fix}(G) \oplus V_1 \oplus \cdots \oplus V_m \tag{3.2}$$

With respect to the invariant inner product all these invariant subspaces are pairwise orthogonal.

Remark 3.10. We will frequently use that the orthogonal projection $\cdot|_{\mathrm{Fix}(G)} : \mathbb{R}^n \to \mathrm{Fix}(G)$ onto the fixed space of a finite group G which can be computed as

$$x|_{\mathrm{Fix}(G)} = \frac{1}{|G|} \sum_{g \in G} gx. \tag{3.3}$$

■

Let $z \in \mathbb{Z}^n$ and $P := \operatorname{conv} Gz$ be its orbit polytope. For the proof of the main theorem of this section – core points are close to an invariant subspace – we are interested only in those z for which the orbit polytope has maximal dimension, i.e., $\dim P = n - \dim \mathrm{Fix}(G)$. Looking at (3.2), we see that the affine hull $\operatorname{aff} P$ of the polytope P is given by

$$\operatorname{aff} P = z|_{\mathrm{Fix}(G)} + \mathrm{Fix}(G)^\perp$$

where $x|_V$ denotes the orthogonal projection of a point x onto a linear subspace V and $V^\perp$ denotes the orthogonal complement of V. For the proof of this section's main theorem we need the following observation. Consider the function $\mu : \mathbb{Z}^n \to \mathbb{R}_{\geq 0}$ defined as

$$\mu(z) := \min_{v \in (\operatorname{aff} Gz) \cap \mathbb{Z}^n} \left\| v|_{\mathrm{Fix}(G)^\perp} \right\|_G .$$

This is the minimal distance of an integral point in the affine hull of the orbit polytope of z to the fixed space (having minimal projection onto the complement of the fixed space). Note that $G \leq \mathrm{GL}_n(\mathbb{Z})$ implies that $\mathrm{Fix}(G)^\perp$ has a basis of integral vectors. Thus, the affine hull $\operatorname{aff} Gz$ contains infinitely many integral points and the definition of μ is sound.

Lemma 3.11. The function μ takes only finitely many distinct values.

Proof. Let $\Lambda := \mathbb{Z}^n|_{\mathrm{Fix}(G)}$ be the projection of all integral points to the fixed space. This set Λ is a lattice and contains the integral points $\mathrm{Fix}_{\mathbb{Z}}(G)$ of the fixed space as a sublattice. Since the orbit polytope $\operatorname{conv} Gz$ has maximal dimension, these lattices have the same rank. Moreover, the index $|\Lambda : \operatorname{Fix}_{\mathbb{Z}}(G)|$ of $\operatorname{Fix}_{\mathbb{Z}}(G)$ in Λ is finite. We show that μ takes at most $|\Lambda : \operatorname{Fix}_{\mathbb{Z}}(G)|$ distinct values. To see this we observe that, by definition, the function μ depends only on the affine hull as a whole set and not on the integer point z itself. Put differently,

$$\mu(z+f) = \mu(z) = \mu\left(z|_{\operatorname{Fix}(G)}\right) \quad \text{for every } f \in \operatorname{Fix}(G)^{\perp} \text{ and } z \in \mathbb{Z}^n. \tag{3.4}$$

We therefore consider the function $\mu' : \Lambda \to \mathbb{R}_{\geq 0}$ defined as

$$\mu'(u) := \min_{v \in (u+\operatorname{Fix}(G)^{\perp}) \cap \mathbb{Z}^n} \left\| v|_{\operatorname{Fix}(G)^{\perp}} \right\|_G .$$

Because of (3.4) it is enough to show that μ' takes only finitely many distinct values. Since $\mu'(u) = \mu'(u+f)$ for every $u \in \Lambda$ and $f \in \operatorname{Fix}_{\mathbb{Z}}(G)$, the function μ' depends only on the coset with respect to $\operatorname{Fix}_{\mathbb{Z}}(G)$. Hence, μ' and also μ take at most $|\Lambda : \operatorname{Fix}_{\mathbb{Z}}(G)|$ distinct values. □

After this observation we turn to the minimal ellipsoid of orbit polytopes. These ellipsoids are closely related to invariant subspaces as Barvinok & Blekherman [BB05, Thm 2.2] show.

Theorem 3.12 ([BB05])**.** Let $G \leq \mathrm{GL}_n(\mathbb{Z})$ be a finite group. Let $z \in \mathbb{Z}^n$ such that the dimension of the orbit polytope of z is maximal, i.e., $\dim \operatorname{conv} Gz = n - \dim \operatorname{Fix}(G)$. There exists a decomposition $\mathbb{R}^n = \operatorname{Fix}(G) \oplus \bigoplus_{i=1}^m V_i$ of $\mathbb{R}^n$ into the fixed space and other G-invariant invariant subspaces V_i such that the minimal enclosing ellipsoid of the orbit polytope $\operatorname{conv}(Gz)$ is given by

$$z|_{\operatorname{Fix}(G)} + \left\{ x \in \operatorname{Fix}(G)^{\perp} \;:\; \sum_{i=1}^{m} (\dim V_i) \frac{\left\|x|_{V_i}\right\|_G^2}{\left\|z|_{V_i}\right\|_G^2} \leq n - \dim \operatorname{Fix}(G) \right\}. \tag{3.5}$$

Note again that this decomposition into invariant subspaces does not have to be unique; see, for instance, Example 6.5 on page 84. Thus, the subspace decomposition for the minimal enclosing ellipsoid may depend on the point z.

Using this ellipsoid, we can prove one of the key results of this thesis. Core points have a small projection onto one invariant subspace, i.e., they always lie close to an invariant subspace of the group (cf. Figure 3.1).

Theorem 3.13. Let $G \leq \mathrm{GL}_n(\mathbb{Z})$ be a finite group and let z be a core point. Then there always exist a constant $C(G)$ depending on the group and a G-invariant subspace V of $\mathbb{R}^n$ different from $\operatorname{Fix}(G)$ such that $\left\|z|_V\right\|_G \leq C(G)$.

Proof. We use the other theorems in this section to find a necessary condition under which the orbit polytope $P := \operatorname{conv} Gz$ contains integral points. By Theorem 3.12 there is a decomposition $\mathbb{R}^n = \operatorname{Fix}(G) \oplus \bigoplus_{i=1}^m V_i$ of $\mathbb{R}^n$ into G-invariant subspaces related to the minimal enclosing ellipsoid of P. If $z|_{V_i} = 0$ for one subspace V_i, then nothing remains to show. So we assume that all projections have positive norm. Let $n' := n - \dim \operatorname{Fix}(G)$ be the dimension of the polytope P. The minimal enclosing ellipsoid of the orbit polytope P is given by

$$z|_{\operatorname{Fix}(G)} + \left\{ x \in \operatorname{Fix}(G)^{\perp} \;:\; \sum_{i=1}^{m} (\dim V_i) \frac{\left\|x|_{V_i}\right\|_G^2}{\left\|z|_{V_i}\right\|_G^2} \leq n' \right\}. \tag{3.6}$$

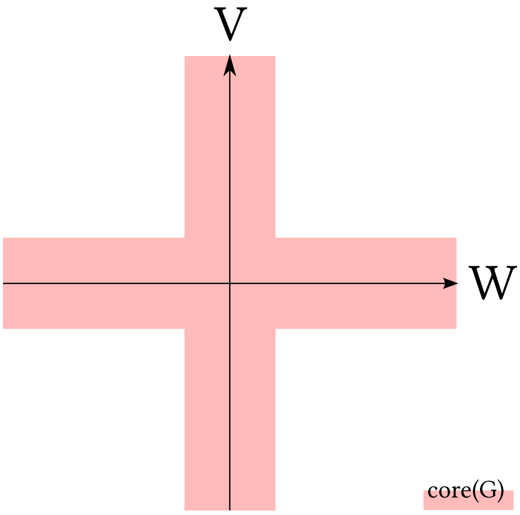


Figure 3.1.: Two orthogonal invariant subspaces V and W: Core points have a small projection onto one of them.

By John's Theorem 3.9, the polytope P contains the following ellipsoid, which is a scaled version of (3.6).

$$E' := z|_{\mathrm{Fix}(G)} + \left\{ x \in \mathrm{Fix}(G)^{\perp} \ : \ \sum_{i=1}^{m} (\dim V_i) \frac{\|x|_{V_i}\|_G^2}{\|z|_{V_i}\|_G^2} \leq \frac{1}{n'} \right\}.$$

Since the dimension of P is n', the scaling factor is $\frac{1}{n'}$ accordingly. Next we derive conditions under which E' and thus also P contain an interior integer point. In this case z cannot be a core point.

Let $u \in (\mathrm{aff}\, P) \cap \mathbb{Z}^n$ be an integral point in the affine hull of P with minimal norm. Such a point exists since the affine hull contains at least the vertices of P as integral points. If for all subspaces V_i the length of the projection $\|z|_{V_i}\|_G$ is large enough, then the following inequality is satisfied.

$$\sum_{i=1}^{m} (\dim V_i) \frac{\|u|_{V_i}\|_G^2}{\|z|_{V_i}\|_G^2} \leq \frac{1}{n'} \tag{3.7}$$

Hence, in this case the ellipsoid E' contains the integer point u. Then u must also lie in P by construction of E'. For an estimation of when (3.7) is fulfilled, let $u' := u|_{\mathrm{Fix}(G)^{\perp}}$ be the orthogonal projection of u on the orthogonal complement of $\mathrm{Fix}(G)$. Further, note that $\dim V_i \leq n'$ and $\|u|_{V_i}\|_G \leq \|u'\|_G$. Thus the inequality (3.7) is satisfied if for all i the projections are longer than

$$\|z|_{V_i}\|^2 \geq m \cdot (n')^2 \cdot \|u'\|_G^2 . \tag{3.8}$$

By Lemma 3.11 we know that $\mu(u') = \|u'\|_G$ takes only finitely many distinct values. Choosing the maximum of these values, we set $C(G) := m \cdot (n')^2 \cdot \max_{z \in \mathbb{Z}^n} \mu^2(z)$. By (3.8), this yields the bound claimed in the theorem. □

Remark 3.14. The proof of the theorem shows that the constant $C(G)$ depends really only on the fixed space $\mathrm{Fix}(G)$. For concrete groups and known invariant subspaces V_i we can obtain concrete bounds on core points by computing for each subspace the minima

$$\min_{u \in (\operatorname{aff} Gz) \cap \mathbb{Z}^n} \left\| u|_{V_i} \right\|_G .$$

Concrete bounds are an important step in classifying all core points of a group, which is what we will aim at in the next chapters.

Theorem 3.13 can also be interpreted as flatness theorem for orbit polytopes. Compared to the general flatness theorem (Theorem 2.6) it has the advantage that it adds some structure for the direction in which the polytope has to be flat. As we will see later, the constant is no improvement over the general case (see Remark 4.5).

3.3. Permutation groups

As Lemma 3.8 showed, all groups which act irreducibly on $\mathbb{R}^n$ have a very small core set (consisting only of the origin). To make things more interesting, we study in the remainder of this thesis a broad class of reducible matrix groups that are quite well understood: permutation groups in their canonical representation. Their core set and sometimes also their fundamental core set contain infinitely many points.

Remark 3.15. Since all infinitely many integral elements of the fixed space are core points, it follows that core sets of permutation groups are infinite by Example 2.5 and Remark 3.4 (iv).

Whenever it does not lead to ambiguities, we identify a permutation group $G \leq \mathcal{S}_n$ with its canonical representation in $\mathrm{GL}_n(\mathbb{Z})$. That is, we study the permutation group G and its action on $\mathbb{R}^n$ by permuting coordinates. We begin with an observation about core points that are universal in the sense that they are core points for every permutation group.

Definition 3.16. A point $z \in \mathbb{Z}^n$ is called a **universal core point** if $z \in \{0,1\}^n$. In the concrete context of a group we also call the point z a universal core point if z is isomorphic (in the sense of Definition 3.5) to a point in $\{0,1\}^n$.

To make sure that these points called universal core points are indeed core points and universal, we prove this in the following lemma.

Lemma 3.17. For every permutation group $G \leq \mathcal{S}_n$ all universal core points are core points.

Proof. Because $\mathrm{core}(\mathcal{S}_n) \subseteq \mathrm{core}(G)$ by Remark 3.4 (iii), it is enough to prove that every $z \in \{0,1\}^n$ is a core point for $\mathcal{S}_n$. Let k be the number of ones in z. The orbit $\mathcal{S}_n z$ is then the set of all $0/1$-vectors with exactly k ones. Let $y \in (\operatorname{conv} \mathcal{S}_n z) \cap \mathbb{Z}^n$ be an integral convex combination of these points. As a convex combination, the integral point y must also have k coordinates with value one. Thus, y lies in the vertex set $\mathcal{S}_n z$. We conclude that z is a core point for $\mathcal{S}_n$. □

This shows that the name universal core point is justified since they are core points for every permutation group. We now turn to a connection between the structure of a permutation group and the structure of its core set.

Remember from Section 2.2 that every permutation group is a subdirect product of transitive permutation groups. As subdirect products contain direct products as a special case, we can decompose an arbitrary permutation group G as follows. We write G as a direct product $G = \bigtimes_{i=1}^{k} G_i$ where each factor G_i cannot be written as a direct product. Then for every factor one of two cases applies: Either G_i is a transitive permutation group, or G_i is a proper subdirect product, i.e., an intransitive group that is not a direct product. The reason for this decomposition into direct products is that this structure carries over nicely to core sets. The following theorem originally appeared in [HRS13, Thm 8].

Theorem 3.18 ([HRS13]). Let $G = \bigtimes_{i=1}^{k} G_i \leq \mathcal{S}_n$. Then $\operatorname{core}(G) = \bigtimes_{i=1}^{k} \operatorname{core}(G_i)$.

Proof. The product structure of G induces a decomposition of $\mathbb{R}^n$ into a Cartesian product of pairwise orthogonal coordinate subspaces $\bigtimes_{i=1}^{k} X_i = \mathbb{R}^n$. Thus, we can write every point $z \in \mathbb{R}^n$ as $z = \bigoplus_{i=1}^{k} z_i$. The claim of the theorem follows immediately from $\operatorname{conv} Gz = \bigtimes_{i=1}^{k} \operatorname{conv} G_i z_i$. □

The theorem states that if a permutation group $G \leq \mathcal{S}_n$ is the direct product of other permutation groups, then the core set of G also is a Cartesian product. Thus, for understanding core sets of permutation groups it is enough to understand core sets of transitive groups and core sets of proper subdirect products. Furthermore, if we understand core sets of transitive groups, we can approximate the core set of proper subdirect products: Since every subdirect product H is the subgroup of a direct product of transitive groups $H_1, \ldots, H_k$, the core set of H contains the Cartesian product $\bigtimes_{i=1}^{k} \operatorname{core}(H_i)$ (cf. Remark 3.4 (iii)). Therefore, we focus in the next chapters on core sets of transitive groups. In the remainder of this section we start with some elementary results about core sets of transitive groups. We will discuss these core sets in depth in the following Chapters 4 and 5. Using these results, we will then explore the core set of (proper) subdirect products in Chapter 6.

3.4. Transitive permutation groups

In this section we start our study of the core set and in particular the fundamental core set of transitive groups. We begin with different ways of choosing a fundamental core set, which consists only of representatives, from a core set. We then address the question of when a fundamental core set is finite. Using a specialization of Theorem 3.13, we obtain a necessary criterion for a transitive group to have a finite fundamental core set.

3.4.1. Fundamental core sets

By Definition 3.5 the fundamental core set of a group is a set of core points which are representatives of an equivalence relation. This equivalence, which is meant to filter out group action and translation in the fixed space, leaves us some freedom for choosing representatives. In particular with respect to the translation part, one choice of representatives may be suited better for certain applications than another. In the following we look at two different ways to select a fundamental core set.

For a transitive group the fixed space is the linear span of the all-ones vector $\mathbb{1}$. Thus, all orbit polytopes lie in a hyperplane that is perpendicular to the all-ones vector. In order to work with all integral points that lie in an orbit polytope, we introduce the following object.

Definition 3.19. We define a **layer** to be the set

$$\mathbb{Z}^n_{(k)} := \{z \in \mathbb{Z}^n \ : \ \langle \mathbb{1}, z \rangle = k\}$$

for some integer k, which we call the **layer index**.

For some applications it is useful to use the lattice structure of these layers. The layer with index zero is the root lattice A_{n-1}, all other layers are translates $\mathbb{Z}^n_{(k)} = ke^{(1)} + \mathsf{A}_{n-1}$. Moreover, the lattice $\operatorname{Fix}_{\mathbb{Z}}(G)$ of a transitive group G consists of integral multiples of $\mathbb{1}$. Therefore, all core points in $\mathbb{Z}^n_{(k)}$ are isomorphic to the core points in $\mathbb{Z}^n_{(k+n)}$. A fundamental core set for G can thus be chosen as a set of orbit representatives from the core points in the layers with indices $1, \dots, n$. In a formula this means we choose orbit representatives from the core points in

$$\bigcup_{k=1}^{n} \mathbb{Z}^n_{(k)}. \tag{3.9}$$

An alternative, slightly less obvious choice is based on the following notion.

Definition 3.20. Let $z \in \mathbb{Z}^n$ be an integral point. We say that such a point z is **zero-based** if all coordinates of z are non-negative and at least one coordinate is zero.

We can select a fundamental core set from the set of all zero-based core points. That is, we may choose orbit representatives from the set

$$\left\{ z \in \mathbb{Z}^n \ : \ \min_{i \in [n]} z_i = 0 \right\}. \tag{3.10}$$

Because translating z by an element from $\operatorname{Fix}_{\mathbb{Z}}(G)$ affects the minimum $\min_i z_i$, it is clear that the core points in (3.10) are isomorphic if and only if they lie in the same orbit. Thus, picking a set of orbit representatives really yields a fundamental core set.

This shows that to understand fundamental core sets (and hence the whole core set) it is enough to study core points from either (3.9) or (3.10). Which setting to choose depends on the proof and computational techniques in use. We will see in the next chapters that for most proofs it will be more convenient to work with zero-based points.

Remark 3.21. From a practical point of view, the sets (3.9) and (3.10) still contain some redundancy that is not eliminated by a fundamental core set. For instance, instead of (3.9) it is enough to study core points in the layers

$$\mathbb{Z}^n_{(1)}, \dots, \mathbb{Z}^n_{(\lfloor \frac{n}{2} \rfloor)}. \tag{3.11}$$

This is because

$$\operatorname{core}(G, \mathbb{Z}^n_{(n-k)}) = \operatorname{core}(G, \mathbb{Z}^n_{(-k)} + \mathbb{1}) = -\operatorname{core}(G, \mathbb{Z}^n_{(k)}) + \mathbb{1},$$

so all core points in layer $n-k$ can easily be obtained from those in layer k. Moreover, the core set $\operatorname{core}(G, \mathbb{Z}^n_{(n)}) = \{\mathbb{1}\}$ is always rather boring.

Remark 3.22. Herr defines a fundamental core set to be the union of all core points in the layers (3.11). For transitive groups it suffices to study these core points but this layer restriction does not generalize easily to intransitive groups.

3.4.2. Finite fundamental core sets

Let $\mathbb{R}^n = \operatorname{Fix}(G) \oplus \bigoplus_{i=1}^m V_i$ be a decomposition into irreducible invariant subspaces. In this section we focus on the case $m = 1$, that is, the orthogonal complement of $\operatorname{Fix}(G) = \operatorname{span} \mathbb{1}$ is irreducible. This case can also be characterized in terms of permutations. A transitive permutation group has only one invariant subspaces besides the fixed space if and only if it is 2-homogeneous (see, for instance, [Cam72, Lemma 2]). In the following we use Theorem 3.13, which relates the core points of a group G to the invariant subspaces of G, to prove that 2-homogeneous groups have finite fundamental core sets. Before we can prove this fact, we need one more auxiliary calculation.

Lemma 3.23. Let $V := \{x \in \mathbb{R}^n : \langle \mathbb{1}, x\rangle = 0\}$ be the orthogonal complement of the fixed space $\operatorname{span} \mathbb{1}$. For $k \in [n]$ let $c^{(k)} := \sum_{i=1}^k e^{(i)}$. Then $\left\| c^{(k)}|_V \right\|^2 = \frac{k(n-k)}{n}$.

Proof. Let $W := \operatorname{span} \mathbb{1}$. Then we have $\left\|c^{(k)}|_V\right\|^2 = \left\|c^{(k)}\right\|^2 - \left\|c^{(k)}|_W\right\|^2$ by Pythagoras' theorem. Thus, using formula (3.3) for the projection onto the fixed space W, we obtain

$$\left\|c^{(k)}|_V\right\|^2 = k - \left\|\frac{k}{n}\mathbb{1}\right\|^2 = k - \frac{k^2}{n} = \frac{k(n-k)}{n}.$$

□

The following theorem states that for a core point z we have an explicit upper bound for the distance of z from the fixed space.

Theorem 3.24. Let $G \leq \mathcal{S}_n$ be 2-homogeneous. Let $z \in \mathbb{Z}^n_{(k)}$ be a core point with $k \in [n]$. The distance of z to the fixed space is bounded by

$$\left\| z - \frac{k}{n}\mathbb{1} \right\| < (n-1)\sqrt{\frac{k(n-k)}{n}}.$$

Proof. For a 2-homogeneous group G, there is exactly one invariant subspace V different from $\operatorname{Fix}(G)$. Moreover, since permutation matrices are orthogonal, the standard inner product already is G-invariant. Thus, equation (3.5) from Theorem 3.12 becomes:

$$\left\{ x \in \mathbb{R}^n : \langle \mathbb{1}, x\rangle = k \quad \text{and} \quad \frac{\|x|_V\|^2}{\|z|_V\|^2} \leq 1 \right\}. \tag{3.12}$$

To get this formula we use that $\operatorname{Fix}(G) = \operatorname{span} \mathbb{1}$ and $z|_{\operatorname{Fix}(G)} + \operatorname{Fix}(G)^\perp = \operatorname{aff} Gz = \{x \in \mathbb{R}^n : \langle \mathbb{1}, x\rangle = k\}$. We further follow the argument of the proof of Theorem 3.13. By using John's Theorem 3.9 we know that the orbit polytope $P := \operatorname{conv} Gz$ contains the following scaled version of the ellipsoid (3.12):

$$E' := \left\{ x \in \mathbb{R}^n \ : \ \langle \mathbb{1}, x\rangle = k \quad \text{and} \quad \frac{\|x|_V\|^2}{\|z|_V\|^2} \leq \frac{1}{(n-1)^2} \right\}. \tag{3.13}$$

This ellipsoid E' (and thus also P) contains the integral point $c^{(k)} := \sum_{i=1}^k e^{(i)}$ if $\|z|_V\|$ is big enough. Using the calculation from Lemma 3.23, we obtain that this is the case if:

$$\left\|z|_V\right\|^2 \geq \frac{k(n-k)}{n}(n-1)^2. \tag{3.14}$$

Note that E' does not contain any vertices of P, thus $c^{(k)}$ is always an inner point of P. This shows that P is not lattice-free whenever (3.14) holds. Since the length of the projection $\left\|z|_V\right\|^2 = \left\|z - z|_{\operatorname{Fix}(G)}\right\|^2 = \left\|z - \frac{k}{n}\mathbb{1}\right\|^2$ equals the distance of z from the fixed space, the proof is complete. □

The theorem is formulated only for $k \in [n]$ but generalizes to arbitrary k as already outlined in the proof of Theorem 3.13, using $k \bmod n$ instead. Lemma 3.28 and Figure 3.2 provide an illustrative example of the argument in the proof. A more graphic description of the theorem is that, if a group G is 2-homogeneous, then all core points lie in a cylinder with radius $O\big(n^{3/2}\big)$ and axis $\operatorname{span} \mathbb{1}$. Hence, we immediately obtain the following corollary.

Corollary 3.25. If G is 2-homogeneous, then its fundamental core set is finite.

Remark 3.26. The finiteness can also be proven by invoking the flatness theorem (for details see [Her13b, Thm 4.32]). Unfortunately, this approach does not seem to yield a concrete upper bound on the distance of core points from the fixed space.

It is not clear whether the converse statement holds, i.e., whether all transitive groups that are not 2-homogeneous have an infinite fundamental core set. In Chapter 5 we will see some evidence that the existence of more than one invariant subspace besides the fixed space could lead to an infinite fundamental core set. This motivates the following conjecture (see also [Her13b, Conj 4.45]).

Conjecture 3.27. The fundamental core set of a transitive group G is finite if and only if G is 2-homogeneous.

In the next Chapter 4 we will analyze (finite) fundamental core sets of some 2-homogeneous groups. Since we will compute fundamental core sets by exhaustive search, all bounds that restrict the search space for core points are important. At the end of this section we briefly discuss the tightness of the bound provided by Theorem 3.24.

For two reasons it is unlikely that the constant bound in Theorem 3.24 is tight. First, the proof uses an ellipsoid which often is only an approximation for the insphere. Second, the proof looks for integer points only in this insphere approximation instead of the whole orbit polytope. In general, the first issue cannot be improved since the approximation of the insphere is tight for the special case of simplices and there are orbit polytopes which are simplices. The second issue also is hard to resolve. We used the ball instead of the whole orbit polytope because finding integer points in the orbit polytope was a hard problem to begin with. We will see another strategy to find integer points in orbit polytopes that yields a different bound in Chapter 4. There we will also analyze real values for the distance from the vertex barycenter that come from computational experiments (cf. Table 4.3).

3.4.3. Core sets of the symmetric and alternating groups

In this section we analyze the core set of the symmetric and alternating groups. We show that the only core points of these groups are universal core points (cf. Proposition 3.32). Along the way to the proof we collect some auxiliary lemmas that provide necessary criteria for a point to be a core point. We will make use of these again for the computations in Chapter 4. We start with the core set proof of a special case.

Lemma 3.28. For $\mathcal{A}_3 \cong \mathcal{C}_3$, all core points are universal core points.

Proof. For $n = 3$ there are only two interesting layers $\mathbb{Z}^n_{(1)}$ and $\mathbb{Z}^n_{(2)}$ to look for core points. As shown in Remark 3.21, it suffices to look at core points in $\mathbb{Z}^n_{(1)}$. Let $b = \frac{1}{3}\mathbb{1}$ be the vertex barycenter of all orbit polytopes in this layer. By Theorem 3.24 we know that $\|z - b\| < 2\sqrt{\frac{2}{3}}$ for every core point z. The integral points closest to the barycenter in $\mathbb{Z}^n_{(1)}$ which are not universal core points all lie in the orbit of $p := (1, 1, -1)^\top$. We compute $\|p - b\| = 2\sqrt{\frac{2}{3}}$. Hence, the universal core points are the only core points in $\mathbb{Z}^n_{(1)}$. Figure 3.2 shows how the insphere of $\operatorname{conv}(\mathcal{A}_3 p)$ contains the universal core points since $\|p - b\|$ exceeds the bound given in Theorem 3.24. □

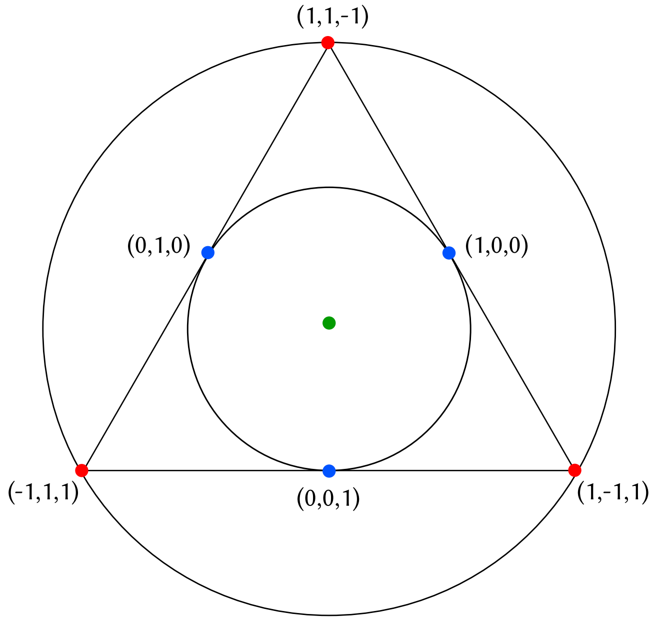


Figure 3.2.: Sketch for the proof of Lemma 3.28

The next two observations arose during the collaboration with Katrin Herr [Her13b, Sec 4.4]. The first of these lemmas is a generalization of parts of the proof idea of [BHJ13, Thm 33].

Lemma 3.29. Let $z \in \mathbb{Z}^n$ and denote by I the set of coordinates for which z is even. If z is a core point for $G \leq \mathcal{S}_n$, then z is constant on each orbit of $\mathrm{Stab}_G(I)$ on $[n]$.

Proof. Assume that there are an orbit $O \subseteq [n]$ of $\mathrm{Stab}_G(I)$ and two indices $i, j \in O$ such that $z_i \neq z_j$. Because i and j are in the same orbit, there exists a permutation $g \in \mathrm{Stab}_G(I)$ such that $g(i) = j$. We then have that $gz \neq z$. Moreover, the point $z' := \frac{1}{2}(z + gz)$ is integral, since g preserves parity by construction. Thus, the integral point z' lies in $\operatorname{conv} Gz$ and is not a vertex. □

The next lemma states another necessary condition for a point to be a core point. For this we define that $\gcd(a, 0) := |a|$, so that we can deal with zeros in the $\gcd$'s argument.

Lemma 3.30. Let $z \in \mathbb{Z}^n$ be a core point for a group $G \leq \mathcal{S}_n$. Let $g \in G$ be any permutation with $gz \neq z$ and let $x := gz - z$ be the non-zero difference. Then $\gcd(x_1, \ldots, x_n) = 1$. In particular, if z is zero-based and $z \notin \mathrm{Fix}(G)$, then $\gcd(z_1, \ldots, z_n) = 1$.

Proof. Let $z \in \mathbb{Z}^n$ be a point such that there exists a $g \in G$ with non-zero difference $x := gz - z \neq 0$ and $\gamma := \gcd(x_1, \ldots, x_n) > 1$. In order to prove the lemma we show that such a point z is not a core point. The point $z + \frac{1}{\gamma}x = \frac{\gamma-1}{\gamma}z + \frac{1}{\gamma}gz$ is an integral convex combination of two vertices of $\operatorname{conv} Gz$. Since $\gamma > 1$, this is not a vertex of $\operatorname{conv} Gz$. Hence, $\operatorname{conv} Gz$ is not lattice-free and z is not a core point. The claim of the lemma especially for zero-based core points follows immediately from the just proven more general statement. □

Lemma 3.31. Let $G \leq \mathcal{S}_n$ be a k-transitive group. If z is a non-universal zero-based core point, then z has at least k and at most $n - k$ even coordinates.

Proof. Suppose that z has at most $k - 1$ even coordinates with index set I. Because G is k-transitive, the stabilizer $\mathrm{Stab}_G(I)$ has only two orbits on $[n]$. Thus, by Lemma 3.29 the point z can only have two distinct coordinates. Since z is zero-based, these can only be 0 and 1 by Lemma 3.30. □

The following proposition was proven for almost all cases (except in dimension three and four) in [BHJ13, Thm 33] in a slightly different way. An alternative, more explicit proof for the special cases $\mathcal{A}_3$ and $\mathcal{A}_4$ is given by Herr in [Her13b, Sec 4.3.2].

Proposition 3.32 ([BHJ13])**.** If G is the symmetric group or the alternating group, then all core points are universal core points.

Proof. For $n = 2$ and $\mathcal{S}_2$ the claim follows immediately, for instance, from Lemma 3.30. It remains to discuss the case $n \geq 3$. For these it suffices to prove the proposition for alternating groups since this implies the claim for symmetric groups by Remark 3.4 (iii). Let z be a core point for $\mathcal{A}_n$ and w.l.o.g. we assume that z is zero-based. We then have to show that all coordinates of z are either 0 or 1 for z to be a universal core point. We denote by I the set of coordinates for which z is even and by $\bar{I} := [n] \setminus I$ its complement. W.l.o.g. we can further assume that $|I| \leq \left\lfloor \frac{n}{2} \right\rfloor$.

The alternating group $\mathcal{A}_n$ is $(n-2)$-transitive, so especially $(\lfloor \frac{n}{2} \rfloor + 1)$-transitive for $n \geq 5$. In this case the stabilizer $\mathrm{Stab}_G(I)$ acts transitively on $\bar{I}$. Hence, z must be constant on the sets I and $\bar{I}$ by Lemma 3.29. If z has the same value on all coordinates, we are done. In the other case that z has different values on I and $\bar{I}$, we apply Lemma 3.30. Because the greatest common divisor of the positive coordinates of z, which are all equal, must be 1, we conclude that all entries of z are either 0 or 1. Thus, z is a universal core point.

We still have to prove the cases $n \in \{3, 4\}$. For $\mathcal{A}_4$ the same argument can still be made: For all its set stabilizers, there are only two orbits. The case of $\mathcal{A}_3$ was treated in Lemma 3.28. □

Remark 3.33. Since both the symmetric group $\mathcal{S}_n$ and the alternating group $\mathcal{A}_n$ are n-homogeneous, all universal core points in one layer are in the same orbit. For these groups all fundamental core sets therefore have n elements, for instance,

$$\mathrm{fcore}(G) = \left\{ \sum_{i=1}^{k} e^{(i)} \;:\; k \in [n] \right\}.$$

Remark 3.34. Together with Theorem 3.18 this shows that every direct product of symmetric and alternating groups has a finite core set. Let $G = \bigtimes_{i=1}^{m} \mathcal{G}_{k_i}$ where $\mathcal{G}_k$ is either a symmetric or alternating group of degree k. Then

$$|\mathrm{fcore}(G)| = \prod_{i=1}^{m} k_i.$$

4. Finite Fundamental Core Sets of Transitive Groups

In this chapter we study finite fundamental core sets of transitive groups in dimensions less than or equal to twelve. The groups which these finite fundamental core sets come from are the 2-homogeneous groups. We obtain the fundamental core sets by an exhaustive computer-based search. In the previous chapter we have already seen some results that we can use to this end. Theorem 3.24 gives an explicit list of balls in which all core points are contained. Approximating the number of candidates to be checked by the volume of the balls suggests that the radius, which is roughly $\frac{1}{2}n^{3/2}$, is still too large for almost all relevant dimensions. In the following sections we obtain better bounds by combining knowledge of the group structure with convex geometry.

We start in Section 4.1 with a simple observation about symmetric projections. In the following Sections 4.2 and 4.3 we prove necessary criteria for core points for 2-transitive and 2-homogeneous groups, respectively. While the case of 2-transitive groups is quite elementary, similar results on 2-homogeneous groups require the classification of these groups. The necessary criteria are an important ingredient of the exhaustive search for core points, which is described in Section 4.4. In Section 4.5 we look at a construction that yields core points for almost every 2-homogeneous group. Moreover, we construct series of core points for affine groups.

4.1. A projection lemma

The major necessary criteria for core points in this chapter are based on the following simple observation. For a fixed space projection and intersection of symmetric sets are the same.

Lemma 4.1. Let $H \leq \mathcal{S}_n$ be a symmetry group of a polytope $P \subseteq \mathbb{R}^n$, i.e., $HP = P$. Then it holds that

$$P \cap \operatorname{Fix}(H) = P|_{\operatorname{Fix}(H)}.$$

Proof. For the "$\subseteq$"-part let $x \in P \cap \operatorname{Fix}(H)$. Since $x \in \operatorname{Fix}(H)$, we have $x = x|_{\operatorname{Fix}(H)} \in P|_{\operatorname{Fix}(H)}$. For the reverse inclusion "$\supseteq$" let $x \in P|_{\operatorname{Fix}(H)}$. In particular, x is a convex combination of points in HP by (3.3). Since P is invariant under H, this implies that the point x lies in P. □

In words, the lemma states that projection to some fixed space equals intersection with the fixed space for symmetric polytopes (see Figure 4.1). Depending on how a polytope is presented, either by facets or by vertices, one of these two operations is easier to handle. Since we are dealing with orbit polytopes, we naturally only have

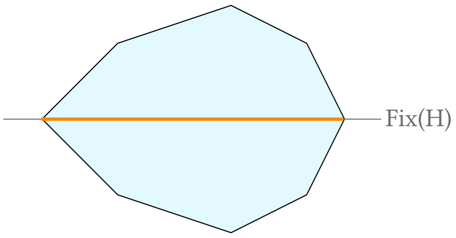


Figure 4.1.: Intersection of a symmetric polytope with a fixed space

its vertices, so the projection is readily available. Lemma 4.1 allows us to find integral points in P, which may be difficult, by finding integral points in the projection, which may be a much easier problem. How easy it gets depends on the group H we choose. Let $P := \operatorname{conv} Gz$ be an orbit polytope with respect to a transitive group G. Any subgroup $H \leq G$ is of course a symmetry group of P. Because P is contained in the orthogonal complement of $\operatorname{Fix}(G) = \operatorname{span} \mathbb{1}$ and $\operatorname{span} \mathbb{1}$ is contained in $\operatorname{Fix}(H)$, we know that $\dim(P \cap \operatorname{Fix}(H)) = \dim \operatorname{Fix}(H) - \dim \operatorname{Fix}(G) = \dim \operatorname{Fix}(H) - 1$. If the fixed spaces of G and H are the same, then the intersection consists only of the vertex barycenter of P, which does not provide new information (cf. Remark 3.7). The goal therefore is to find a non-transitive subgroup H with as few orbits as possible since this orbit number equals dimension of $\operatorname{Fix}(H)$. The smaller the dimension of $\operatorname{Fix}(H)$, the easier it is to find integral points.

In the following we apply Lemma 4.1 twice. For 2-transitive groups we will obtain a one-dimensional projection, for which interior integral points are naturally easy to find. In the case of 2-homogeneous groups that are not 2-transitive groups, we will reduce the problem to a two-dimensional projected polytope. From conditions that guarantee existence of integral points in the projections, we will obtain conditions for inner integral points in an orbit polytope $\operatorname{conv} Gz$. This will leads to better necessary criteria for z to be a core point.

4.2. 2-transitive groups

The following proposition is the key application of Lemma 4.1 for 2-transitive groups.

Proposition 4.2. Let $G \leq \mathcal{S}_n$ be a 2-transitive group and let $P := \operatorname{conv} Gz$ be the orbit polytope of some zero-based $z \in \mathbb{Z}^n_{\geq 0}$. Then a point $p = (k, l, l, \dots, l)^\top \in \mathbb{R}^n$ for some $k, l \in \mathbb{R}$ lies in P if and only if the following two conditions are met:

(i) $0 \leq k \leq \max z_i$,

(ii) $l = \frac{\sum_{j=1}^n z_j - k}{n-1}$.

Proof. The stabilizer $H := \operatorname{Stab}_G(p) = \operatorname{Stab}_G(1)$ of p acts transitively on $\{2, \dots, n\}$ because G is 2-transitive. Let $\{g_1, \dots, g_n\} \subset G$ be a transversal for G modulo H, that is, $g_i(i) = 1$ for each $i \in [n]$. Thus, for every g_i we have that

$$(g_i z)|_{\operatorname{Fix}(H)} = (z_i, r_i, r_i, \dots, r_i)^\top \qquad \text{where} \quad r_i = \frac{1}{n-1} \sum_{j \in [n] \setminus \{i\}} z_j.$$

Let $Q := P|_{\mathrm{Fix}(H)}$ be the projection of P onto the fixed space $\mathrm{Fix}(H)$. The vertices of P are projected onto $q^{(i)} := (g_i z)|_{\mathrm{Fix}(H)}$ for $i \in [n]$. All these points lie in a one-dimensional affine subspace of $\mathbb{R}^n$, so Q is a line segment. By Lemma 4.1 the point $p \in \mathrm{Fix}(H)$ lies in P if and only if it lies in the projection Q.

Let a be such that $z_a = \min_{i\in[n]} z_i = 0$ and let b be such that $z_b = \max_{i\in[n]} z_i$. With this setting we know that $q^{(a)}$ and $q^{(b)}$ are end points of Q because of the respective minimality and maximality of z_a and z_b. To simplify notation we project on the first two coordinates, which are the only relevant ones. We identify Q with the line segment $Q' \subset \mathbb{R}^2$, given as the convex hull of $q'^{(a)} = (0, r_a)^\top$ and $q'^{(b)} = (z_b, r_b)^\top$. As inequality description we obtain

$$Q' = \left\{ (x_1, x_2)^\top \in \mathbb{R}^2 \;:\; 0 \le x_1 \le z_b \quad \text{and} \quad x_1 + (n-1)x_2 = \sum_{j=1}^{n} z_j \right\}.$$

Hence, the polytope Q' contains a point $(u_1, u_2)^\top \in \mathbb{R}^2$ if and only if $0 \le u_1 \le z_b$ and $u_2 = \frac{1}{n-1}(\sum_{j=1}^n z_j) - \frac{u_1}{n-1}$. Because the point p of the proposition projects onto $(k, l) \in \mathbb{R}^2$, the claim of the proposition follows. □

Proposition 4.2 showed that we can find integral points in a polytope by finding integral points on a line segment in $\mathbb{R}^2$ with slope $(n-1) : 1$. The following proposition, due to Knörr [Knö11], quantifies the condition under which the induced line segment contains an integral point.

Proposition 4.3 ([Knö11])**.** Let $G \le \mathcal{S}_n$ be a 2-transitive group with $n \ge 3$. Let $z \in \mathbb{Z}^n_{\ge 0}$ be zero-based with $\max z_i \ge 2$. If

$$\left(\sum_{i=1}^{n} z_i \right) \bmod (n-1) \;\le\; \max z_i,$$

then z is not a core point.

Proof. Let $k = \sum_{i=1}^n z_i \bmod (n-1)$. Then $l := \frac{\sum_{i=1}^n z_i - k}{n-1}$ is an integer. By Proposition 4.2 the integral point $p = (k, l, \ldots, l)^\top$ lies in $P := \operatorname{conv} Gz$ because $0 \le k \le \max z_i$. The point p is a vertex of P if and only if p is in the orbit of z. If p is not a vertex, we know that p is an inner point of P, which then is not lattice-free.

Suppose that p is a vertex of P. Because z is zero-based, this can happen only if $l = 0$ or $k = 0$. In these two cases we still have to find an integer point in P which is not a vertex. Note that in both cases we must have $\gcd(p_1, \ldots, p_n) = \gcd(k, l) \ge 2$ because of our assumption $\max z_i \ge 2$. Thus, Lemma 3.30 implies that $\operatorname{conv} Gp$ is not lattice-free and therefore $\operatorname{conv} Gz = \operatorname{conv} Gp$ is not lattice-free. □

A simple corollary of this proposition yields the following bound on the infinity-norm of zero-based core points.

Corollary 4.4. Let $G \le \mathcal{S}_n$ be a 2-transitive group with $n \ge 4$. If $z \in \mathbb{Z}^n_{\ge 0}$ is a zero-based core point, then $\max z_i \le n - 3$.

Proof. Let $z \in \mathbb{Z}^n_{\geq 0}$ be zero-based with $\max z_i \geq n-2 \geq 2$. Then we must have that $\sum_{i=1}^n z_i \bmod (n-1) \leq \max z_i$ because the remainder of $\sum_{i=1}^n z_i$ after division by $n-1$ lies in $\{0, 1, \dots, n-2\}$. Thus, Proposition 4.3 ensures that the orbit polytope $\operatorname{conv} Gz$ is not lattice-free. Hence, z is not a core point. □

Remark 4.5. The bound in Corollary 4.4 partially improves the cylinder bound in Theorem 3.24. The latter yields only an $O\big(n^{3/2}\big)$ bound for $\max_{i,j\in[n]} |z_i - z_j|$ when we look at the layers with index near $\frac{n}{2}$. This is worse than the linear bound from Corollary 4.4.

In Lemma 3.31 we have seen that a non-universal core point of a k-transitive group must have at least k even and k odd coordinates. The following proposition gives a restriction on the layers in which non-universal core point can occur.

Proposition 4.6. Let $G \leq \mathcal{S}_n$ be a $(k+1)$-transitive group with $k \geq 1$. All core points in $\mathbb{Z}^n_{(l)}$ for $l \bmod n \in \{-k, -k+1, \dots, k\}$ are universal core points.

Proof. Let $z \in \mathbb{Z}^n_{\geq 0}$ be zero-based and $\max z_i \geq 2$. We write N for the layer index $N = N(z) := \langle \mathbb{1}, z\rangle = \sum_{i=1}^n z_i$. To prove the proposition, it is enough to show that every such z with $N \bmod n = k$ is not a core point because every $(k+1)$-transitive group is k-transitive. In the following we prove that $P := \operatorname{conv} Gz$ is not lattice-free by using Lemma 4.1. More precisely, we show that P contains

$$v = (\underbrace{c+1, \dots, c+1}_{k \text{ times}}, \underbrace{c, \dots, c}_{n-k \text{ times}})$$

for $c = \left\lfloor \frac{N}{n} \right\rfloor$. Note that v is contained in the fixed space $\operatorname{Fix}(H)$ of the set stabilizer $H := \operatorname{Stab}_G(\{1, \dots, k\})$. By Lemma 4.1 it suffices to prove that v is contained in the projection $Q := P|_{\operatorname{Fix}(H)}$ in order to ensure that v lies in P.

Because the group G is $(k+1)$-transitive, the stabilizer H acts transitively on the sets $\{1, \dots, k\}$ and $\{k+1, \dots, n\}$. Thus, the projection onto the fixed space is given by $x|_{\operatorname{Fix}(H)} = (R(x), \dots, R(x), S(x), \dots, S(x))^\top$ with $R(x) := \frac{1}{k}\sum_{i=1}^k x_i$ and $S(x) := \frac{1}{n-k}\sum_{i=k+1}^n x_i$. Therefore, Q is a line-segment that is contained in the hyperplane $\{x \in \mathbb{R}^n : \langle \mathbb{1}, x\rangle = N\}$. In the following we show the existence of two points $x, y \in Q$ such $R(x) \leq R(v) \leq R(y)$. By our initial assumption we have $N = cn + k = (n-k)c + k(c+1)$. Thus, v satisfies $\langle \mathbb{1}, v\rangle = N$ and lies in the right layer. Hence, the existence of these x and y implies that v lies on the line-segment Q.

To keep the index notation simple we assume that z is sorted non-decreasingly. It will become clear that this is without loss of generality in the following argument because G is k-transitive. Our next step is to show that

$$\sum_{i=1}^{k} z_i \leq k(c+1) \qquad \text{and} \tag{4.1}$$

$$\sum_{i=n-k+1}^{n} z_i \geq k(c+1). \tag{4.2}$$

If we establish these inequalities, we will immediately obtain the desired boundary points x and y as follows. From the first equation (4.1) we get that $R(z) \leq (c+1) = R(v)$.

Because G is k-transitive, there is a permutation g that maps $\{n-k+1,\dots,n\}$ to $\{1,\dots,k\}$. Thus, we obtain $R(v)=(c+1)\le R(gz)$ from (4.2).

It remains to show that inequalities (4.1) and (4.2) actually hold. For a contradiction assume that $\sum_{i=1}^{k} z_i > k(c+1)$. Since z is sorted, this implies $z_k \ge c+2$ and thus

$$N=\sum_{i=1}^{n} z_i=\sum_{i=1}^{k} z_i+\sum_{i=k+1}^{n} z_i > k(c+1)+(n-k)(c+2) > N.$$

We get a similar construction by assuming that $\sum_{i=n-k+1}^{n} z_i < k(c+1)$. This implies $z_{n-k+1}\le c$ and thus

$$N=\sum_{i=1}^{n} z_i=\sum_{i=1}^{n-k} z_i+\sum_{i=n-k+1}^{n} z_i < (n-k)c+k(c+1)=N.$$

Therefore the inequalities (4.1) and (4.2) must hold.

Thus, we have shown that $v\in Q$ and therefore also $v\in P$. We still have to prove that v is not a vertex of P, i.e., v is not in the orbit of z. Because z is zero-based, the point v can only be a vertex of P if $c=0$. In this case we would have $\max z_i = c+1 = 1$, which we have ruled out by our initial assumption. Hence, v is not a vertex of P. □

Corollary 4.7. If $G\le\mathcal{S}_n$ is 2-transitive, then all core points in the layers with index 1 and $n-1$ are universal core points.

As we will see in the next section, a similar statement for 2-homogeneous groups is false. For these, non-universal core points appear in all layers (except those whose index is a multiple of n).

4.3. 2-homogeneous groups

In this section we discuss the remaining groups which have a finite fundamental core set: groups which are 2-homogeneous but not 2-transitive. To these we cannot apply the improvements that we obtained in the previous section over the general cylinder bound in Theorem 3.24. As stated in Remark 4.5, this only yields a bound of $O(n^{3/2})$ for the maximal coordinate of a zero-based core point, compared with $O(n)$ for 2-transitive groups. In this section we deduce a bound of the same order for 2-homogeneous groups. We start with a description of all groups which are 2-homogeneous but not 2-transitive.

4.3.1. Structural description of 2-homogeneous groups

All groups which are 2-homogeneous but not 2-transitive were classified by Kantor ([Kan69, Prop. 3.1], see also [Kan72]). Let $\mathbb{F}_q$ be a finite field with q elements where q is a prime power with $q\equiv 3 \pmod 4$ and $q\ge 7$. Further, let A be any subgroup of the automorphism group of $\mathbb{F}_q$. Then every permutation group G which is 2-homogeneous but not 2-transitive is isomorphic to an affine semilinear group

$$G\cong\left\{x\to b^2x^\sigma+c \;:\; b\in\mathbb{F}_q^*, c\in\mathbb{F}_q, \sigma\in A\right\}\le \mathrm{A\Gamma L}(1,q) \tag{4.3}$$

over a finite field $\mathbb{F}_q$ with a group $A \leq \operatorname{Aut}(\mathbb{F}_q)$ of automorphisms. Here, $\mathbb{F}_q^*$ denotes the multiplicate group of $\mathbb{F}_q$ as usual. Viewed as a permutation group, G has degree q and order $\frac{q(q-1)|A|}{2}$. In contrast to all other group actions in this thesis we denote the action of an automorphism $\sigma \in A$ by x^σ from the (top) right to distinguish it from the usual field multiplication.

In the following we write briefly $\mathcal{S} := \{a^2 \ : \ a \in \mathbb{F}_q^*\}$ for the set of non-zero squares in $\mathbb{F}_q$. Because $q \equiv 3 \pmod 4$, we know that $-\mathcal{S}$ is the set of non-squares. Thus, we have a partition $\mathbb{F}_q = \{0\} \cup \mathcal{S} \cup -\mathcal{S}$. Because we study the action of G on $\mathbb{R}^q$, we identify the coordinates with field elements. That means, we fix some labeling $(e^{(i)})_{i \in \mathbb{F}_q}$ of the standard basis vectors in $\mathbb{R}^q$.

4.3.2. A width bound

In this section we derive a statement that is analogous to Corollary 4.4. More precisely, we prove the following proposition.

Proposition 4.8. Let $G \leq \mathcal{S}_n$ be a 2-homogeneous group. If $z \in \mathbb{Z}^n_{\geq 0}$ is a zero-based core point, then $\max z_i \leq \left(\frac{1}{2} + \frac{1}{\sqrt{3}}\right)(n-1) \leq 1.09\,(n-1)$.

The proof is split into several parts. The main goal is to show that every orbit polytope of a point that violates the given bound is not lattice-free. Like in the 2-transitive case we first use Lemma 4.1 to reduce the dimension of the problem. We answer the arising question of when some two-dimensional polytope contains an integer point with the planar flatness theorem (see Theorem 2.7).

Reduction to a two-dimensional problem

As in the proof of Proposition 4.3, we show that a wide enough orbit polytope contains an integer point of a special form. Because of the relationship to finite fields we denote the ambient dimension by q instead of n throughout this section. Let $P := \operatorname{conv} Gz$ be the orbit polytope of a zero-based integral point $z \in \mathbb{Z}^q$. We consider the subgroup $H := \operatorname{Stab}_G(\mathcal{S}) = \{g \in G \ : \ g(\mathcal{S}) = \mathcal{S}\}$ of G and search integral points in the intersection of P with $\operatorname{Fix}(H)$. By linearity it holds that $g(-\mathcal{S}) = -\mathcal{S}$ for every $g \in H$. Thus, every $g \in H$ has three orbits $\{0\}, \mathcal{S}, -\mathcal{S}$. This implies that

$$\operatorname{Fix}(H) = \operatorname{span}\left\{e^{(0)}, \mathbb{1}_{\mathcal{S}}, \mathbb{1}_{-\mathcal{S}}\right\}$$

where $\mathbb{1}_S \in \mathbb{R}^q$ denotes the characteristic vector of a set $S \subseteq \mathbb{F}_q$. By Lemma 4.1 the intersection $P' := P \cap \operatorname{Fix}(H)$ is the convex hull of $p'^{(1)}, \ldots, p'^{(q)}$ with

$$p'^{(i)} = z_i e^{(0)} + \left(\frac{1}{|\mathcal{S}|}\sum_{s \in \mathcal{S}} z_{i+s}\right)\mathbb{1}_{\mathcal{S}} + \left(\frac{1}{|\mathcal{S}|}\sum_{s \in \mathcal{S}} z_{i-s}\right)\mathbb{1}_{-\mathcal{S}},$$

which are the projections of the vertices of P. To simplify things further we look at the following polytope Q' with vertices

$$q'^{(i)} := \left(\frac{1}{|\mathcal{S}|}(z_i - N),\ \frac{1}{|\mathcal{S}|}\sum_{s \in \mathcal{S}} z_{i+s}\right)^{\top}. \tag{4.4}$$

where we denote the layer index by $N = \langle \mathbb{1}, z\rangle = \sum_{j\in\mathbb{F}_q} z_j$. The integral points in this polytope Q' are in one-to-one correspondence with the integral points in $P' = P \cap \operatorname{Fix}(H)$ as the following lemma shows.

Lemma 4.9. Integral points in P' and Q' are in one-to-one correspondence as

$$\left(\frac{k-N}{|\mathcal{S}|}, l\right)^\top \in Q' \cap \mathbb{Z}^2 \iff ke^{(0)} + l\mathbb{1}_{\mathcal{S}} + \left(\frac{N-k}{\mathcal{S}} - l\right)\mathbb{1}_{-\mathcal{S}} \in P' \cap \mathbb{Z}^q.$$

Moreover, the vertices of P' are in one-to-one correspondence to the vertices of Q'.

Proof. Let

$$u = \sum_{i\in\mathbb{F}_q} \lambda_i p'_i = ke^{(0)} + l\mathbb{1}_{\mathcal{S}} + \left(\frac{N-k}{\mathcal{S}} - l\right)\mathbb{1}_{-\mathcal{S}} \tag{4.5}$$

be an arbitrary (not necessarily integral) point in P' for some coordinates k and l and convex parameters $\lambda_i \in [0,1]$. Using these convex parameters λ_i also for the vertices $q'^{(i)}$, it follows that

$$v := \left(\frac{k-N}{|\mathcal{S}|}, l\right)^\top$$

lies in Q' if and only if u lies in P'. This argument also shows that there is a bijection between the vertices of P' and Q'. It is easy to see that the point u is integral if and only if v is integral: the only rational summand is $\frac{N-k}{|\mathcal{S}|}$ in both cases. □

By this lemma it suffices to find an integral point in the two-dimensional polytope Q' in order to find an integral point in $P' \subset P$. To ensure the existence of integer points in this polytope Q', we compute its width and use the flatness theorem in dimension two, which was stated in Theorem 2.7. In the following we always refer to the $\mathbb{Z}^2$-width simply as the width of a polygon. Because the width is invariant under translation, we may also look at the translated and scaled polygon R which is the convex hull of

$$r^{(i)} := \left(z_i, \sum_{s\in\mathcal{S}} z_{i+s}\right)^\top \qquad \text{for } i \in \mathbb{F}_q. \tag{4.6}$$

If we can show that

$$\omega_{\mathbb{Z}^2}(R) \geq \left(1 + \frac{2}{\sqrt{3}}\right)|\mathcal{S}|, \tag{4.7}$$

then we also have

$$\omega_{\mathbb{Z}^2}(Q') \geq \left(1 + \frac{2}{\sqrt{3}}\right)$$

and thus an integral point in the interior of Q'. The key part to prove the main proposition of this section is the following lemma.

Lemma 4.10. Let $z \in \mathbb{Z}^n_{\geq 0}$ be zero-based and let $R = R(z) \subset \mathbb{R}^2$ be the convex hull of the points from (4.6). Then it holds that

$$\omega_{\mathbb{Z}^2}(R) \geq \max z_i.$$

Before we prove this lemma, we first complete the proof of the main result, Proposition 4.8. This follows immediately from the two previous lemmas.

Proof of Proposition 4.8. If G is 2-transitive, then the result follows from Corollary 4.4. So let G be a 2-homogeneous group, which is not 2-transitive. Let $z \in \mathbb{Z}^q_{\geq 0}$ be zero-based with $\max z_i \geq \frac{1}{2}\left(1 + \frac{2}{\sqrt{3}}\right)(q-1)$. By Lemma 4.10 we therefore have

$$\omega_{\mathbb{Z}^2}(R) \geq \left(1 + \frac{2}{\sqrt{3}}\right)\frac{q-1}{2} = \left(1 + \frac{2}{\sqrt{3}}\right)|\mathcal{S}|\,.$$

By (4.7) this implies that Q' has an integral point v in its interior. Therefore also P' (by Lemma 4.9) and P (by Lemma 4.1) contain an integral point u. Since the point v is not a vertex of Q', the point u is not a vertex of P' by Lemma 4.9. Thus, $\operatorname{conv} Gz = P \supset P'$ is not lattice-free. □

Remark 4.11. It is unclear whether a statement like Proposition 4.3 exists, which is easy to check, depends on the concrete coordinate of z and is guaranteed to characterize all integral points in the projection Q'. Using the flatness-based arguments on Q', we lose information. For the computational application in the next section this loss of information will turn out to be too large. In order to fill in the gap computationally and increase the chance of finding an integral point in Q' (and P), we may also directly search for integral points in the concrete polygon Q' as follows. Since we do not know the vertices of Q', we use some convex hull algorithm to obtain the vertices or facets. Having these, we use general integer programming tools or two-dimensional integer programming specializations like [EL05] to look for an inner integral point in Q', which corresponds to an inner integral point in P and proves that P is not lattice-free.

Proof of Lemma 4.10

In order to prove Lemma 4.10, let $w = (w_1, w_2)^\top \in \mathbb{Z}^2 \setminus \{0\}$ be an arbitrary non-zero direction to measure the width. Because of transitivity we may assume w.l.o.g. that $z_0 = \min_{i\in\mathbb{F}_q} z_i = 0$. If z is the zero vector, then trivially the lemma holds, so we focus on the case $z \neq 0$. Let $m \in \mathbb{F}_q \setminus \{0\}$ be an index such that $z_m = \max_{i\in\mathbb{F}_q} z_i =: M \in \mathbb{Z}_{>0}$. We have to show that for every non-zero direction w there are two points $r^{(i)}$ and $r^{(j)}$ such that $\left\langle w, r^{(i)}\right\rangle - \left\langle w, r^{(j)}\right\rangle \geq \max z_i - \min z_i = M$. For the proof we frequently use the following observation:

Lemma 4.12 (Averaging)**.** Let $T_1, T_2 \subseteq \mathbb{F}_q$ be two sets such that $T_1 \setminus T_2$ and $T_2 \setminus T_1$ have the same size s. If

$$\sum_{t\in T_1}\left\langle w, r^{(t)}\right\rangle - \sum_{t\in T_2}\left\langle w, r^{(t)}\right\rangle \geq sM$$

for some value $M \in \mathbb{R}$, then $\omega(w, R) \geq M$.

Proof. Let $T_1 \setminus T_2 = \{c_1, \dots, c_s\}$ and $T_2 \setminus T_1 = \{d_1, \dots, d_s\}$. Then

$$\frac{1}{s}\sum_{i=1}^{s}\left\langle w, r^{(c_i)} - r^{(d_i)}\right\rangle = \frac{1}{s}\left(\sum_{t\in T_1}\left\langle w, r^{(t)}\right\rangle - \sum_{t\in T_2}\left\langle w, r^{(t)}\right\rangle\right) \geq M.$$

So there is an index j such that $\left\langle w, r^{(c_j)}\right\rangle - \left\langle w, r^{(d_j)}\right\rangle \geq M$, implying $\omega(w, R) \geq M$. □

We distinguish two cases regarding the index m of the maximal coordinate: either $m \in \mathcal{S}$ is a non-zero square or $m \in -\mathcal{S}$ is not a square. For this we introduce the following notation. We write $b + T = \{b + t \ : \ t \in T\}$ for any set $T \subseteq \mathbb{F}_q$ and $b \in \mathbb{F}_q$. Moreover, we denote the set of all squares including zero by $\mathcal{S}_0$, i.e., $\mathcal{S}_0 := \mathcal{S} \cup \{0\}$.

Case 1: $m \in \mathcal{S}$

Without loss of generality we can assume that $w_1 \geq 0$ because $\omega(w, C) = \omega(-w, C)$ for any direction w and every convex set C. Suppose that we want to measure the width in x-direction (or something close to the x-direction). Then we need two points with a large difference in their x-coordinate. Choosing $r^{(m)}$ and $r^{(0)}$, which have maximal and minimal x-coordinates, respectively, we obtain:

$$\begin{aligned} &\left\langle w, r^{(m)} \right\rangle - \left\langle w, r^{(0)} \right\rangle \\ &= w_1(z_m - z_0) + w_2 \left(\sum_{i \in \mathcal{S}} (z_{m+i} - z_i) \right) \\ &= (w_1 - w_2) z_m + w_2 \left(\sum_{i \in m + \mathcal{S}_0} z_i - \sum_{i \in \mathcal{S}_0} z_i \right). \end{aligned} \tag{4.8}$$

Under our assumption $w_1 \geq 0$, we see that (4.8) is at least M if

$$\boxed{w_1 > w_2 \quad \text{and} \quad \operatorname{sgn}(w_2) \left(\sum_{i \in m + \mathcal{S}_0} z_i - \sum_{i \in \mathcal{S}_0} z_i \right) \geq 0.} \tag{4.9}$$

Note that the first part of this condition is automatically satisfied if $w_2 < 0$. This completes the consideration for measuring width in x-direction. For the width in y-direction we use the following lemma, which seems to be elementary but hard to find in the literature in this form.

Lemma 4.13. Let q be a prime power with $q \equiv 3 \pmod 4$. For any $b, c \in \mathbb{F}_q$ the following equations hold:

(i) $\mathbb{F}_q = \{b\} \cup (b + \mathcal{S}) \cup (b - \mathcal{S})$, which is a partition.

(ii) $|(b + \mathcal{S}) \cap \mathcal{S}| = |(b + \mathcal{S}_0) \cap \mathcal{S}_0| - 1 = \begin{cases} \frac{q-1}{2} & \text{if } b = 0, \\ \frac{q-3}{4} & \text{otherwise.} \end{cases}$

(iii) $|(b - \mathcal{S}) \cap \mathcal{S}| = \begin{cases} 0 & \text{if } b = 0, \\ \frac{q-3}{4} & \text{if } b \in \mathcal{S}, \\ \frac{q+1}{4} & \text{if } b \in -\mathcal{S}. \end{cases}$

(iv) $|\{(x, y) \in (b - \mathcal{S}) \times \mathcal{S} \ : \ x + y = c\}| = \begin{cases} \frac{q-1}{2} & \text{if } b = c, \\ \frac{q-3}{4} & \text{otherwise.} \end{cases}$

Proof. Part (i) follows immediately from our observation $\mathbb{F}_q = \{0\} \cup \mathcal{S} \cup -\mathcal{S}$ above. Part (iv) is just a reformulation of (ii). Thus, it suffices to prove parts (ii) and (iii).

We begin with part (ii). The claim is trivial for $b = 0$. For $b \neq 0$ we need the quadratic character $\eta : \mathbb{F}_q \to \{-1, 0, 1\}$. This is defined by $\eta(0) = 0$, $\eta(x) = 1$ for $x \in \mathcal{S}$, and

$\eta(x) = -1$ for $x \in -\mathcal{S}$. By [LN08, Thm 5.48], it holds that $\sum_{x\in\mathbb{F}_q} \eta(b + x^2) = -1$ for $b \neq 0$. We can rewrite this as

$$-1 = \sum_{x\in\mathbb{F}_q} \eta(b + x^2) = \eta(b) + 2\sum_{x\in\mathcal{S}} \eta(b + x).$$

If b is a square, we thus have $\sum_{x\in\mathcal{S}} \eta(b+x) = -1$. Because $b \in \mathcal{S}$, each of the $|\mathcal{S}| = \frac{q-1}{2}$ summands is non-zero. Hence, $|(b + \mathcal{S}) \cap \mathcal{S}| = \frac{|\mathcal{S}|-1}{2} = \frac{q-3}{4}$. If b is not a square, it follows that $\sum_{x\in\mathcal{S}} \eta(b + x) = 0$. Because $b \in -\mathcal{S}$, there is exactly one summand that equals zero. Hence, $|(b + \mathcal{S}) \cap \mathcal{S}| = \frac{|\mathcal{S}|-1}{2} = \frac{q-3}{4}$. The equation with $\mathcal{S}$ replaced by $\mathcal{S}_0$ follows analogously.

This completes part (ii); we now turn to part (iii). This follows immediately from part (ii) because we can count as follows by part (i):

$$\frac{q-1}{2} = |\mathcal{S}| = |(b - \mathcal{S}) \cap \mathcal{S}| + |(b + \mathcal{S}) \cap \mathcal{S}| + |\{b\} \cap \mathcal{S}| .$$

We know the last two summands and thus also the sought size of $(b - \mathcal{S}) \cap \mathcal{S}$. □

Now our goal is to find points $r^{(i)}$ and $r^{(j)}$ with a big difference in their y-coordinate. Because their y-coordinates are sums of z_i, it is not as obvious as above which pair to choose. However, for every $i \in m - \mathcal{S}$ we know that z_m appears as a summand in the y-coordinate of $r^{(i)}$, which is $\sum_{s\in\mathcal{S}} z_{i+s}$. Similarly, for every $j \in -\mathcal{S}$ the term z_0 is a summand in the y-coordinate of $r^{(j)}$. Moreover, we observe that the disjoint sets $(m - \mathcal{S}) \setminus (-\mathcal{S})$ and $(-\mathcal{S}) \setminus (m - \mathcal{S})$ have the same size because $|m - \mathcal{S}| = |-\mathcal{S}|$. From Lemma 4.13 (ii) we deduce that their size is $|\mathcal{S}| - |(m - \mathcal{S}) \cap (-\mathcal{S})| = \frac{q-1}{2} - \frac{q-3}{4} = \frac{q+1}{4}$. In order to apply Lemma 4.12 with $T_1 = m - \mathcal{S}$ and $T_2 = -\mathcal{S}$, we compute:

$$\begin{aligned}
&\left\langle w, \sum_{i\in m-\mathcal{S}} r^{(i)} - \sum_{i\in -\mathcal{S}} r^{(i)} \right\rangle \\
&= w_1 \left(\sum_{i\in m-\mathcal{S}} z_i - \sum_{i\in -\mathcal{S}} z_i \right) + w_2 \left(\sum_{i\in m-\mathcal{S}} \sum_{j\in\mathcal{S}} z_{i+j} - \sum_{i\in -\mathcal{S}} \sum_{j\in\mathcal{S}} z_{i+j} \right) \\
&= w_1 \left(- \sum_{i\in m+\mathcal{S}_0} z_i + \sum_{i\in\mathcal{S}_0} z_i \right) + w_2 \frac{q+1}{4} (z_m - z_0) \\
&= - w_1 \left(\sum_{i\in m+\mathcal{S}_0} z_i - \sum_{i\in\mathcal{S}_0} z_i \right) + w_2 \frac{q+1}{4} M
\end{aligned} \tag{4.10}$$

To obtain the third line we apply Lemma 4.13 (iv) and compute the difference $\frac{q-1}{2} - \frac{q-3}{4} = \frac{q+1}{4}$. We also use Lemma 4.13 (i) to change the index set of the first two sums. For the fourth line we use $z_0 = 0$ and $z_m = M$. We see that (4.10) is at least $\frac{q+1}{4}M$ if

$$w_2 > 0 \text{ and } \left(w_1 = 0 \text{ or } \left(\sum_{i\in m+\mathcal{S}_0} z_i - \sum_{i\in\mathcal{S}_0} z_i \right) \leq 0 \right), \tag{4.11}$$

Thus by Lemma 4.12, we know that $\omega(w, R) \geq M$ under the condition (4.11). By swapping the roles of T_1 and T_2, we get a similar condition for $w_2 < 0$. Together with (4.11) this yields:

$$\boxed{w_2 \neq 0 \quad \text{and} \quad w_1 = 0 \text{ or } \operatorname{sgn}(w_2)\left(\sum_{i\in m+\mathcal{S}_0} z_i - \sum_{i\in\mathcal{S}_0} z_i\right) \leq 0.} \tag{4.12}$$

The two conditions (4.9) and (4.12) together do not cover all cases as there still is a gap for $w_2 \geq w_1 \geq 0$ and $\sum_{i\in m+\mathcal{S}_0} z_i - \sum_{i\in\mathcal{S}_0} z_i \geq 0$. To close this gap, we consider the disjoint sets $(m - \mathcal{S}_0) \setminus (-\mathcal{S}_0)$ and $(-\mathcal{S}_0) \setminus (m - \mathcal{S}_0)$, which have the same size $\frac{q+1}{4}$. To apply Lemma 4.12 with $T_1 = m - \mathcal{S}_0$ and $T_2 = -\mathcal{S}_0$, we compute:

$$\begin{aligned}
&\left\langle w, \sum_{i\in m-\mathcal{S}_0} r^{(i)} - \sum_{i\in -\mathcal{S}_0} r^{(i)} \right\rangle \\
&= \left\langle w, \sum_{i\in m-\mathcal{S}} r^{(i)} - \sum_{i\in -\mathcal{S}} r^{(i)} \right\rangle + \left\langle w, r^{(m)} - r^{(0)} \right\rangle \qquad (4.13)\\
&= \left(w_1 + \frac{q-3}{4} w_2\right) z_m + (w_2 - w_1)\left(\sum_{i\in m+\mathcal{S}_0} z_i - \sum_{i\in\mathcal{S}_0} z_i\right)
\end{aligned}$$

To obtain the last line we use (4.8) and (4.10). The term (4.13) is at least $\frac{q+1}{4}M$ if

$$\boxed{w_2 \geq w_1 \geq 1 \quad \text{and} \quad \left(\sum_{i\in m+\mathcal{S}_0} z_i - \sum_{i\in\mathcal{S}_0} z_i\right) \geq 0.} \tag{4.14}$$

Thus by Lemma 4.12, this is a sufficient condition for $\omega(w, R) \geq M$.

Table 4.1 shows that the presented conditions (4.9), (4.12), and (4.14) cover all relevant cases. Note again that we could assume without loss of generality that $w_1 \geq 0$ because of symmetry. Hence, R has width at least M.

$\operatorname{sgn}(w_1)$	$\operatorname{sgn}(w_2)$	$\operatorname{sgn}\left(\sum_{i\in m+\mathcal{S}_0} z_i - \sum_{i\in\mathcal{S}_0} z_i\right)$	case
0	$*$	$*$	(4.12)
1	1	1	(4.9) for $w_1 > w_2$, (4.14) for $w_1 \leq w_2$
1	1	-1	(4.12)
1	0	$*$	(4.9)
1	-1	1	(4.12)
1	-1	-1	(4.9)

Table 4.1.: Case coverage

Case 2: $m \in -\mathcal{S}$

This case can be treated in almost the same way and differs only in details. It will turn out to be easier to assume without loss of generality that $w_2 \geq 0$ due to symmetry (instead of $w_1 \geq 0$ as in the previous "$m \in \mathcal{S}$"-case). We apply Lemma 4.12 to the same pair of sets as above. The calculations are the same, the only difference is how we group the terms. Because m is not a square, it is necessary to isolate $\sum_{i \in m+\mathcal{S}} z_i - \sum_{i \in \mathcal{S}} z_i$ instead of $\sum_{i \in m+\mathcal{S}_0} z_i - \sum_{i \in \mathcal{S}_0} z_i$.

First, for $T_1 = \{m\}, T_2 = \{0\}$ we get the inequality

$$w_1 z_m + w_2 \left(\sum_{i \in m+\mathcal{S}} z_i - \sum_{i \in \mathcal{S}} z_i \right) \geq M.$$

Together with a similar inequality for $T_1 = \{0\}, T_2 = \{m\}$ this yields the condition

$$\boxed{w_1 \neq 0 \quad \text{and} \quad w_2 = 0 \text{ or } \operatorname{sgn}(w_1) \left(\sum_{i \in m+\mathcal{S}} z_i - \sum_{i \in \mathcal{S}} z_i \right) \geq 0.} \tag{4.15}$$

Second, from $T_1 = m - \mathcal{S}, T_2 = -\mathcal{S}$ we get the inequality

$$-w_1 \left(\sum_{i \in m+\mathcal{S}} a_i - \sum_{i \in \mathcal{S}} z_i \right) + \left(w_2 \frac{q+1}{4} - w_1 \right) z_m \geq \frac{q+1}{4} M.$$

This yields the condition

$$\boxed{w_2 > w_1 \quad \text{and} \quad \operatorname{sgn}(w_1) \left(\sum_{i \in m+\mathcal{S}} z_i - \sum_{i \in \mathcal{S}} z_i \right) \leq 0.} \tag{4.16}$$

Third, we use $T_1 = m - \mathcal{S}_0, T_2 = -\mathcal{S}_0$ to obtain

$$\frac{q+1}{4} w_2 z_m + (w_2 - w_1) \left(\sum_{i \in m+\mathcal{S}} z_i - \sum_{i \in \mathcal{S}} z_i \right) \geq \frac{q+1}{4} M.$$

Under our initial assumption $w_2 \geq 0$, this is satisfied if

$$\boxed{w_1 \geq w_2 \geq 1 \quad \text{and} \quad \left(\sum_{i \in m+\mathcal{S}} z_i - \sum_{i \in \mathcal{S}} z_i \right) \leq 0.} \tag{4.17}$$

Thus we have obtained three conditions (4.15), (4.16) and (4.17), under which we know that $\omega(w, R) \geq M$. Because these cover all cases under our assumption $w_2 \geq 0$, we know that R has width at least M.

This concludes the proof of Lemma 4.10. After a tedious calculation we have obtained an important width-like bound on core points of 2-homogeneous groups. This enables us to perform an exhaustive search for core points of these groups as described in the next section.

4.4. Exhaustive computational search for core points

In this section we discuss the computational means for enumerating the fundamental core set of a permutation group. This enumeration was a joint project with Katrin Herr (see also [Her13b, Sec 4.4.2]). We used the [polymake] framework for all polyhedral computations and the integrated [PermLib] (cf. [RS10]) for most permutation group operations. As we do not have a characterization of core points besides their definition, we perform an exhaustive computational search for core points. From the set of all integral points we filter core points by the various necessary criteria that we have seen in this and the previous chapter. If a candidate passes all these tests, then we have to check whether it is a core point by using the definition: testing whether the corresponding orbit polytope is lattice-free. In this section we first discuss ways to perform this test. Second, we examine the whole enumeration process. Last, we analyze the results of the enumeration, i.e., the (fundamental) core sets of the 2-homogeneous groups in dimension twelve or less.

All these groups, which can be found in the primitive group library of [GAP], are shown with some interesting properties in Table 4.2. The column id refers to the primitive id in the GAP library (cf. Section 2.2).

4.4.1. Deciding whether a point is a core point

To answer the question whether a polytope P is lattice-free we are aware of two strategies. First, we count all integral points in P and then check whether $|P \cap \mathbb{Z}^n|$ equals $|\mathrm{vert}(P)|$. Second, we solve an integer feasibility problem: Is there an integral point in $P \setminus \mathrm{vert}(P)$? Both ways have disadvantages.

In general, counting integral points in polytopes is a well investigated and hard problem (see, for instance, [De 05]). Two of the most commonly used tools are [LattE], which is based on Barvinok's algorithm (cf. [Bar02]), and [Normaliz] as explained in [BIS12]. LattE requires a facet description of the input polytope, its performance depends on the number of facets. Normaliz can work directly with a vertex description of the polytope. Since our orbit polytopes are given as convex hull and may have many facets (see below), we prefer Normaliz over LattE to count integral points in orbit polytopes.

The second way to decide whether a polytope is lattice-free, formulating the problem as an integer linear program (IP), has the advantage that there is highly sophisticated software for solving these programs (cf. [CPLEX, Gurobi, SCIP]). We have some degrees of freedom for the IP formulation. The most direct approach is based on the facets of the orbit polytope $P := \mathrm{conv}\, Gz$. If we have such a facet description, then we can add for each vertex v an inequality that cuts off v but no other integral point in P. This yields an inequality description which contains all integral points in $P \setminus \mathrm{vert}(P)$. The difficulty is that, as mentioned above, the facets of $\mathrm{conv}\, Gz$ may be many and thus expensive to obtain and to work with. This remains true even if the natural symmetry of the orbit polytope is taken into account, for example, by [SymPol]. For instance, for the group 11-3 the arithmetic mean of the number of facets of all lattice-free orbit polytopes is about 132 000. Another formulation, this time as mixed integer program, does not require facets. If we write integral points explicitly as convex combination

Table 4.2.: 2-homogeneous groups up to degree twelve

id	order	isomorphic description	transitivity	homogeneity
5-3	20	$\mathrm{AGL}(1,5)$	2	5
6-1	60	$\mathrm{PSL}(2,5)$	2	2
6-2	120	$\mathrm{PGL}(2,5)$	3	6
7-3	21	$\mathcal{C}_7 \rtimes \mathcal{C}_3$	1	2
7-4	42	$\mathrm{AGL}(1,7)$	2	2
7-5	168	$\mathrm{L}(3,2)$	2	2
8-1	56	$\mathrm{AGL}(1,8)$	2	3
8-2	168	$\mathrm{A\Gamma L}(1,8)$	2	3
8-3	1344	$\mathrm{ASL}(3,2)$	3	3
8-4	168	$\mathrm{PSL}(2,7)$	2	3
8-5	336	$\mathrm{PGL}(2,7)$	3	3
9-3	72	M_9	2	2
9-4	72	$\mathrm{AGL}(1,9)$	2	2
9-5	144	$\mathrm{A\Gamma L}(1,9)$	2	2
9-6	216	3^2:(2'$\mathcal{A}_4$)	2	2
9-7	432	$\mathrm{AGL}(2,3)$	2	2
9-8	504	$\mathrm{PSL}(2,8)$	3	9
9-9	1512	$\mathrm{P\Gamma L}(2,8)$	3	9
10-3	360	$\mathrm{PSL}(2,9)$	2	2
10-4	720	$\mathrm{PGL}(2,9)$	3	3
10-5	720	$\mathcal{S}_6$	2	2
10-6	720	M_{10}	3	3
10-7	1440	$\mathrm{P\Gamma L}(2,9)$	3	3
11-3	55	$\mathcal{C}_{11} \rtimes \mathcal{C}_5$	1	2
11-4	110	$\mathrm{AGL}(1,11)$	2	2
11-5	660	$\mathrm{L}(2,11)$	2	2
11-6	7920	M_{11}	4	4
12-1	7920	M_{11}	3	3
12-2	95040	M_{12}	5	5
12-3	660	$\mathrm{PSL}(2,11)$	2	3
12-4	1320	$\mathrm{PGL}(2,11)$	3	3

of the vertices, we see that every integral point in P corresponds to a solution of the following MIP:

$$A\lambda - x = 0, \quad \langle \mathbb{1}, \lambda \rangle = 1, \quad \lambda \geq 0, \tag{4.18}$$

where $\lambda \in \mathbb{R}^{|\mathrm{vert}(P)|}$ and $x \in \mathbb{Z}^n$ are variables and $A \in \mathbb{Z}^{n \times |\mathrm{vert}(P)|}$ is the matrix whose columns are the vertices Gz of P. The following lemma allows to restrict the problem to $P \setminus \mathrm{vert}(P)$.

Lemma 4.14. Let $z \in \mathbb{Z}^n_{\geq 0}$ be zero-based. Let $\sum_{g \in G} \lambda_g gz \in \mathbb{Z}^n$ with $\langle \mathbb{1}, \lambda \rangle = 1$ and $\lambda \geq 0$ be an inner integral point of $\operatorname{conv} Gz$. Then it holds that $\lambda_g \leq 1 - \frac{1}{\max_i z_i}$ for every $g \in G$.

Proof. Let $M := \max_i z_i$ be the maximal coordinate of z. For every $\varepsilon > 0$ and for every coordinate index i we have

$$\left(1 - \frac{1}{M} + \varepsilon\right) z_i > z_i - 1 \tag{4.19}$$

Assume that in a convex combination $y = \sum_{g \in G} \lambda_g gz$ there is one parameter $\lambda_g > 1 - \frac{1}{M}$. Because of (4.19) it holds component-wise that $\lceil \lambda_g gz \rceil \geq gz$. Moreover, we know that $y \geq \lambda_g gz$ because the right-hand side appears as a part of the convex combination of y. Thus, it follows that $y = \lceil y \rceil \geq \lceil \lambda_g gz \rceil \geq gz$. Because y and gz lie in the same layer, i.e., $\langle \mathbb{1}, y \rangle = \langle \mathbb{1}, gz \rangle$, we must have $y = gz$. □

Since the matrix A from (4.18) consists of the vertices of the orbit polytope, Lemma 4.14 implies that the solutions of the following MIP correspond to inner integral points of P:

$$A\lambda - x = 0, \quad \langle \mathbb{1}, \lambda \rangle = 1, \quad 0 \leq \lambda \leq 1 - \frac{1}{\max_i z_i}. \tag{4.20}$$

For our implementation we used lattice point counting with Normaliz as test for lattice-freeness. A test based on MIPs (4.20) did not result in a significant performance gain, at least for the groups with degree less than or equal to twelve.

4.4.2. Filtering core points

In this section we examine the exhaustive search for core points in detail. We have two rough approximations as bounding boxes for the fundamental core set to choose from: a cylinder by Theorem 3.24 and an axis-parallel cube by Corollary 4.4 and Proposition 4.8. Inside of such an approximation we test for each point whether it satisfies all the other known necessary criteria for a core point. We apply these tests in increasing order of running time. We start with those which can be integrated in the enumeration process itself and finish with those which have polynomial running time in the dimension. If all the necessary core point criteria are fulfilled, we use Normaliz to decide whether a point is a core point or not (cf. Section 4.4.1).

For the bounding box in which we enumerate all integral points we use the axis-parallel cube. The reason for this is that Lemma 3.29 can be easily integrated in the enumeration process. This lemma states that every core point is constant on the orbits of some stabilizer. For the groups in question these orbits can be computed very fast by [GAP]. If the orbits of every stabilizer are not too small, this reduces the search space significantly. For instance, if all orbits of all set stabilizers had at least size two, this would essentially halve the dimension of the cube. The results of Seress [Ser97] show that relatively many groups of small degree are special in the sense that no set stabilizer is trivial. This justifies the cube-based enumeration process as outlined in Algorithm 1. The algorithm is stated for 2-transitive groups and we will discuss adaptions for 2-homogeneous groups later.

The main part of this algorithm is the enumeration of all integer points in a cube in line 7. The additional conditions stated in this line can easily be integrated into the enumeration. Algorithm 1 is correct for 2-transitive groups for the following reasons:

Algorithm 1: Basic core point candidate enumeration for 2-transitive groups

```
  Input: $k$-transitive group $G \leq \mathcal{S}_n$ with $k \geq 2$
  Output: list $L$ that contains representatives for all fundamental core points of $G$
1 $L \leftarrow \emptyset$;
2 foreach $j \in \{k, \dots, n-k\}$ do
3     compute orbits $\mathcal{O}$ of all $j$-element subsets of $[n]$ under $G$;
4     foreach orbit $O \in \mathcal{O}$ do
5         choose one arbitrary element $S \in O$;
6         compute orbits $\mathcal{O}_S$ of $[n]$ under $\operatorname{Stab}_G(S)$;
7         enumerate list $L_S$ of all integer points in $[0, n-3]^n$ that are zero-based,
          constant on each orbit in $\mathcal{O}_S$, even on $S$, and whose first coordinate is zero;
8         $L \leftarrow L \cup L_S$;
```

- Every non-universal zero-based core point z has at least k even and at most $n-k$ odd coordinates where k is the transitivity of G (cf. Lemma 3.31).
- Every zero-based core point z lies in the cube $[0, n-3]^n$ by Corollary 4.4.
- For every zero-based core point z its orbit Gz contains a point whose even coordinates are indexed by S, the arbitrarily chosen orbit representative in line 5.
- Because the group is transitive, we can assume w.l.o.g. that the first coordinate is minimal, which is zero in this case.

Hence, the list L of the algorithm contains a list of representatives of every zero-based core point of G.

In the enumeration in line 7 of Algorithm 1 we can add further improvements. For all candidates we can check the $\gcd$-condition of Lemma 3.30, which eliminates a few points. Much more important is the necessary condition given by Proposition 4.3, which determines all integral points in a one-dimensional intersection of the polytope. This can be checked quickly and it turns out to be very helpful. Also note that the list L contains $(\max z_i)\mathbb{1} - z$ for every $z \in L$. For the fundamental core set it is enough to check only one of these two points since either both or none of them is a core point (cf. Remark 3.21). We may, for instance, ignore all z for which

$$2 \langle \mathbb{1}, z \rangle > n \max z_i. \tag{4.21}$$

For 2-homogeneous groups that are not 2-transitive, we have to change two things. First, the cube bound has to be adapted to $[0, \lfloor 1.09(n-1) \rfloor]^n$ according to Proposition 4.8. Second, we do not have a criterion like Proposition 4.3 that determines all integral points in the projected two-dimensional polytope (cf. Remark 4.11). We therefore solve this problem computationally. Since we potentially have to solve a huge number of these problems, it is essential to keep the overhead small that comes from calling external software libraries. All other convex hull software which is available in polymake like [`lrs`] or [`cdd`] is too generic to be fast. Instead, we implemented a simple and fast convex hull algorithm from [dBvKOS98, Sec 1.1] to compute a triangulation. For each triangle we then check whether it contains an inner integral point. We will see later in Table 4.3 that this two-dimensional search helped substantially to exclude many points which are not core points. As a side note, it is of course also possible to apply this projection method for other non-transitive subgroups. It is unclear if this would further speed up the enumeration.

All the described methods for filtering core points so far work without looking at the whole orbit polytope. We will see later in Table 4.3 that one more test based on the complete polytope helps significantly before we hand the problem over to Normaliz. This additional test is probing for inner integral points of the orbit polytope. Note that the question whether a point x is contained in a polytope P presented as convex hull can be answered efficiently by a linear program (cf. [Fuk04, Question 22]). It remains to decide which points are most likely to lie in an orbit polytope; these are natural choices for a linear programming-based probing. Remember that an orbit polytope $P := \operatorname{conv} Gz$ for $z \in \mathbb{Z}^n_{(k)}$ always contains its vertex barycenter $\frac{k}{n}\mathbb{1}$. Therefore it might be a good idea to check whether one of the integral points closest to $\frac{k}{n}\mathbb{1}$ is contained in P. These points are the universal core points in the layer $\mathbb{Z}^n_{(k)}$, of which there are $\binom{n}{k}$ many. We can test either all or a randomly selected sample of G-orbit representatives whether they lie in P. For our exhaustive search we tested all representatives of the universal core points. We call this test **selective probing**.

4.4.3. Computational results

In this section we look at the results from the exhaustive core point search. The computed fundamental core sets are available in polymake-format at

`http://www.polymake.org/polytopes/core-point-polytopes/.`

Table 4.3 contains statistics about the filtering process and the resulting fundamental core sets. The first column shows the id of the group; this is the same as in Table 4.2. Column "candidates" gives the number of candidates computed by Algorithm 1 as explained above. The third column "probing" shows the number of candidates that survive selective probing, that is, the number of orbit polytopes that do not contain a universal core point. The fourth column "core points" lists the number of actual non-universal core points in the initial candidate set, as confirmed by Normaliz. The remaining two columns will be introduced later. Note that the table does not show the real size $|\mathrm{fcore}(G)|$ but uses an aggregation. The actual size $|\mathrm{fcore}(G)|$ is about twice the value in the fourth column since not all universal core points are considered and the points z and $-z$ are not distinguished in the original candidate set (see Remark 3.21).

Looking at the second column, we see that for most groups the number of candidates coming out of Algorithm 1 is quite small, at least when compared to the number of points in the initial cube, which is shown in the second column of Table 4.4 below. The reason for this was already indicated above.

Remark 4.15. Many of these small and primitive groups are exceptional in the sense that for every set $S \subset [n]$ the stabilizer $\mathrm{Stab}_G(S)$ never is the trivial group. There are only finitely many with this property and all of them occur in dimension 32 or lower (cf. [Ser97]). For the groups in Table 4.3 that do not fall into this category (7-3, 9-3, 9-4, 11-3, 11-4, 12-3), the number of candidates is significantly larger.

The groups 7-3 and 11-3 differ further because they are 2-homogeneous but not 2-transitive. In this case we cannot prune using Proposition 4.3. For 7-3 this does not

Table 4.3.: Candidate elimination

group id	candidates	probing	core points	cube	cylinder
5-3	0	0	0	–	–
6-1	0	0	0	–	–
6-2	0	0	0	–	–
7-3	63 077	12	10	3	2.62
7-4	10	1	1	2	1.85
7-5	3	2	2	2	1.93
8-1	1 797	4	4	2	1.97
8-2	20	1	1	2	1.97
8-3	3	1	1	2	1.97
8-4	10	2	2	2	1.97
8-5	2	0	0	–	–
9-3	21 666	20	20	3	2.75
9-4	21 691	20	18	3	2.75
9-5	529	10	10	3	2.75
9-6	68	3	3	2	2.05
9-7	32	3	3	2	2.05
9-8	5	0	0	–	–
9-9	5	0	0	–	–
10-3	514	8	8	2	2.37
10-4	31	2	2	2	2.12
10-5	164	6	6	2	2.37
10-6	53	4	4	2	2.12
10-7	31	2	2	2	2.12
11-3	[a] 266 982	2 546	2 407	6	5.80
11-4	9 352 389	231	208	4	3.77
11-5	4 285	11	11	2	2.76
11-6	16	2	2	2	2.17
12-1	128	4	4	2	2.58
12-2	11	1	1	2	2.22
12-3	21 580 154	15	15	4	3.30
12-4	7 252	2	2	2	2.22

[a] number after two-dimensional IPs; see text for an explanation

matter much because the number of candidates is still quite small. However, for 11-3 without pruning we have to deal with 1 331 476 291 candidates. Instead of immediately starting with selective probing, we searched for integral points in a two-dimensional projection first (cf. Remark 4.11). This reduces the number of candidates to the tractable value shown in Table 4.3.

Comparing the third and fourth columns of Table 4.3, we see that the number of candidates after the probing step is already very close to the number of actual non-universal core points. This shows that a concise description of those points that survive selective probing, i.e., of those points whose orbit polytopes do not contain universal core points, would probably make core point enumeration much easier.

We now turn to the last two columns of Table 4.3. These fifth and sixth columns provide statistics about the non-universal core points found. The column "cube" contains

$$\max_{z \in \operatorname{core}(G)} (\max z_i - \min z_i), \tag{4.22}$$

the maximal side length of an axis-parallel cube that contains all non-universal core points. For this quantity we have the upper bound $n-3$ by Corollary 4.4 for 2-transitive groups and $\lfloor 1.09(n-1) \rfloor$ by Proposition 4.8 for 2-homogeneous groups. The computed values are often quite far away from these bounds (see Table 4.4 below). In the next section we will see lower bounds which come from core point constructions for this value (cf. Remarks 4.26 and 4.30). The column "cylinder" shows the maximal distance of a core point from the fixed space, i.e.,

$$\max_{z \in \operatorname{core}(G)} \left\| z - \frac{\langle \mathbb{1}, z \rangle}{n} \mathbb{1} \right\|. \tag{4.23}$$

By Theorem 3.24 this quantity is bounded from above by some number between

$$(n-1)\sqrt{\frac{n-1}{n}} \quad \text{and} \quad \frac{1}{2}(n-1)\sqrt{n};$$

the concrete value depends on the layer index k. As with the "cube" value, there is some gap between the computed values and the theoretical upper bound. Table 4.4 shows the maximal theoretical values of (4.22) and (4.23) in its third and fourth columns, respectively.

Table 4.4.: Theoretical maximal bounds for 2-transitive groups

dim n	#points in the cube $[0, n-3]^n$	max. "cube"	max. "cylinder"
5	243	2	4.38
6	4 096	3	6.12
7	78 125	4	7.86
[a]7	823 543	6	7.86
8	1 679 616	5	9.90
9	40 353 607	6	11.93
10	1 073 741 824	7	14.23
11	31 381 059 609	8	16.51
[a]11	285 311 670 611	10	16.51
12	1 000 000 000 000	9	19.05

[a] for the 2-homogeneous case, for which the larger cube $[0, \lfloor 1.09(n-1) \rfloor]^n$ applies

Interestingly, a more detailed analysis reveals that the maximal values in the "cylinder" column are often realized in layers with small index, for which the bound is the smallest. For instance, for the group 7-3 the maximal value is attained for layer $k = 1$, for the group 11-3 it is $k = 2$. In these two cases the computed values equal about half of the theoretical upper bound, 5.47 and 12.77, respectively.

At the end of this section we discuss the computational limits of an exhaustive search. For the groups with degree larger than twelve we have to distinguish two cases. If a group with degree n has at least one trivial set stabilizer, then we have to go through at least $\lfloor \frac{n-2}{2} \rfloor^{n-1}$ points in the cube. For $n = 11$ this number is of the order 10^6 and still manageable, but for $n = 13$ it reaches 10^9, which is very much at the limit of what the current implementation could handle. Thus, without tighter upper bounds on where to look for core points, going beyond $n = 12$ is quite hopeless. On the other hand, if no set stabilizer is trivial, the number of initial candidates can still be feasible. The next groups with this property are 13-7, 14-2, 15-4 (cf. Remark 4.15). The respective number of candidates, comparable to the second column of Table 4.3, are 1 940, 481 379, and 73 879, which are quite small. However, for these group sizes and dimensions, the exact rational arithmetic in both the LP-based selective probing and the core point test with Normaliz are an impediment for filtering core points. Using a commercial LP-solver like [Gurobi] together with an IP-model to prove lattice-freeness should push the practical limits to higher dimensions, so that fundamental core sets for a few more groups could be computed.

4.5. Core point constructions

In this section we look at various ways to provably or probably construct core points. All these constructions are inspired by the results of the core point enumeration as described in the previous section. For many of the computed core points, a quick analysis shows that it is rather obvious why the corresponding orbit polytope must be lattice-free. This is in particular true for all zero-based core points $z \in \mathbb{Z}^n_{\geq 0}$ with small layer index $0 < \langle \mathbb{1}, z \rangle < n$. Although there seems to be no common scheme, the following sections shed some light on reasons and proof techniques for lattice-freeness and core points of 2-homogeneous groups.

4.5.1. "Almost universal" core points

The first construction for core points is based on intersections within orbits. Let $S \subset [n]$ bet a set with $1 \leq |S| \leq n - 1$. For a transitive group $G \leq \mathcal{S}_n$ we define

$$I_G(S) := \max_{g \in G \setminus \mathrm{Stab}_G(S)} |S \cap g(S)|$$

to be the maximal non-trivial overlap of sets in an orbit GS. Note that the number $I_G(S)$ exists because G is transitive and S is neither the empty set nor $[n]$. The following is a sketch of the next proposition, illustrating the role of the intersection number $I_G(S)$.

Let $z \in \mathbb{Z}^n_{\geq 0}$ be a zero-based point with layer index $0 < \langle \mathbb{1}, z \rangle < n$ and denote by $S := \{i \in [n] \ : \ z_i = 0\}$ the set of indices of coordinates with value zero. Every integral point y in the orbit polytope $\operatorname{conv} Gz$ has at least $n - \langle \mathbb{1}, z \rangle$ zeros. Further, if $g \notin \mathrm{Stab}_G(S)$, then every non-trivial convex combination of z and gz has at most $I_G(S)$ zeros. Thus, if $I_G(S) < n - \langle \mathbb{1}, z \rangle$, we know that y has to be an integral point in

$\operatorname{conv}\operatorname{Stab}_G(S)z$. We can easily set up z in such a way that it is a core point for $\operatorname{Stab}_G(S)$ (see Corollary 4.17). Hence, we obtain core points for G if we manage to find a set S with $I_G(S) < n - \langle \mathbb{1}, z\rangle \leq |S|$. If $I_G(S) = |S| - 1$, the point z must be a universal core point. We obtain non-universal core points only if $I_G(S) \leq |S| - 2$.

Proposition 4.16. Let $G \leq \mathcal{S}_n$ be a transitive group. Let $S \subset [n]$ be a set with $1 \leq |S| \leq n-1$. Further, let $z \in \mathbb{Z}^n_{\geq 0}$ be zero-based with $z_i = 0$ for all $i \in S$ and $\langle \mathbb{1}, z\rangle = n - I_G(S) - 1$. Then z is a core point for G if and only if z is a core point for $\operatorname{Stab}_G(S)$.

Proof. Since the "only if" part is obvious, we only have to prove the "if" part. For this let $y \in \mathbb{Z}^n_{\geq 0}$ be an inner point of $\operatorname{conv} Gz$. The point y must have at least $n - \langle \mathbb{1}, z\rangle = I_G(S) + 1$ coordinates with value zero. We observe that for any $g \in G \setminus \operatorname{Stab}_G(S)$ every non-trivial convex combination $\lambda z + (1-\lambda) gz$ has at most $I_G(S)$ coordinates with value zero. Thus, y must lie in the polytope $\operatorname{conv}\operatorname{Stab}_G(S)z$. Hence, $\operatorname{conv} Gz$ is lattice-free if $\operatorname{conv}\operatorname{Stab}_G(S)z$ is lattice-free, which proves the claim of the proposition. □

Corollary 4.17. Let $G \leq \mathcal{S}_n$ be a transitive group. Let $S \subset [n]$ be a set with $1 \leq |S| \leq n-1$. Further, let $z \in \mathbb{Z}^n_{\geq 0}$ be zero-based with $z_i = 0$ for all $i \in S$ and $z_i \in \{1, 2\}$ for all $i \notin S$ such that $\langle \mathbb{1}, z\rangle = n - I_G(S) - 1$. Then z is a core point for G.

Proof. Since

$$\max_{i \in [n],\, g \in \operatorname{Stab}_G(S)} |(gz)_i - z_i| \leq 1,$$

the point z must be a core point for $\operatorname{Stab}_G(S)$ and thus also a core point for G by Proposition 4.16. □

Remark 4.18. Let $S \subset [n]$ and denote by $\bar{S}$ its complement in $[n]$. Since $|S| - |S \cap g(S)| = |\bar{S}| - |\bar{S} \cap g(\bar{S})|$, we also obtain a non-universal core point for $\bar{S}$ if there is one for S.

Example 4.19. As an example for this construction, consider the group G of degree nine with GAP-primitive id 9-3, generated by $G = \langle (2\,7\,3\,4)(5\,8\,9\,6), (1\,3\,4\,5)(2\,8\,6\,9)\rangle$. This group was part of the exhaustive enumeration of the previous section; statistics about its core points are shown later in Table 4.5. For the set $S := \{1, 2, 4, 5\}$ we compute (by enumerating the orbit of S with GAP, for instance) that $I_G(S) = 2$. By Corollary 4.17 we can distribute non-zero values on the coordinates of a point $z \in \mathbb{Z}^9_{\geq 0}$ so that $\langle \mathbb{1}, z\rangle = 9 - 2 - 1 = 6$. Since we have $9 - |S| = 5$ positions to fill, we have one coordinate with value 2 and four with value 1. The stabilizer $\operatorname{Stab}_G(S)$ has the orbits $\{1, 2, 4, 5\}$,$\{3, 6, 7, 8\}$, $\{9\}$. Thus, we obtain the following two non-isomorphic core points

$$(0, 0, 2, 0, 0, 1, 1, 1, 1)^\top,$$
$$(0, 0, 1, 0, 0, 1, 1, 1, 2)^\top.$$

Using the complement $\bar{S}$ of S yields another core point

$$(2, 1, 0, 1, 1, 0, 0, 0, 0)^\top.$$

In this manner 11 out of 20 non-universal core points can be constructed. ■

This example suggests that many core points from Table 4.3 can be obtained this way. Indeed, the only groups where this construction fails to produce non-universal core points are 7-4 and all groups for which all core points are universal core points. We will see statistics in Table 4.5. An obvious limitation of this construction method is transitivity on sets. If a group is k-homogeneous for some k, then the construction in Corollary 4.17 produces only universal core points in layer k. Thus, for permutation groups that are k-homogeneous for all $k \in [n]$ simultaneously, this method yields only universal core points since then $I_G(S) = |S| - 1$ for every set S. Besides $\mathcal{A}_n$ and $\mathcal{S}_n$, there are only four other groups that are homogeneous in this sense (cf. [HB82, Thm. 6.13]): these are 5-3, 6-2, 9-8, and 9-9. This together with computational experiments suggests the following conjecture.

Conjecture 4.20. For all 2-homogeneous groups $G \notin \{\mathcal{A}_n, \mathcal{S}_n\}$ of degree $n \geq 10$ there exists a set S such that $I_G(S) \leq |S| - 2$. That is, Corollary 4.17 produces non-universal core points.

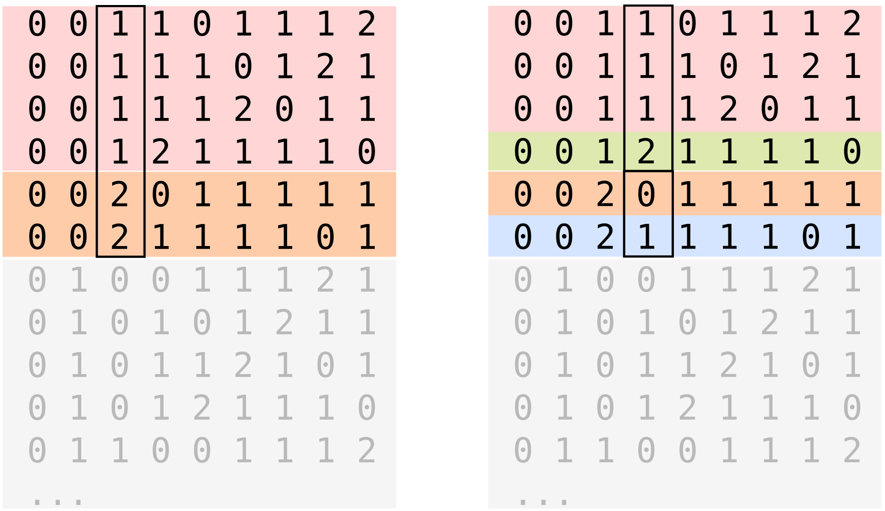
For the remaining core points that are not obtainable via Proposition 4.16 or its corollary there does not seem to be another construction recipe. However, core points $z \in \mathbb{Z}^n_{\geq 0}$ with $\langle \mathbb{1}, z \rangle < n$ can often be verified by the heuristic outlined in Algorithm 2. Its correctness is based on the following observation. Let $P := \operatorname{conv} V \subset \mathbb{R}^n$ be a polytope with vertex set V. Suppose that the projection of P onto the k-th coordinate takes only two distinct integer values a and $a + 1$. If P contains an integral point $u \in \mathbb{Z}^n$, then we must have either $u_k = a$ or $u_k = a + 1$. Thus, u lies either in the polytope $P_a := \operatorname{conv}\{v \in V \ : \ v_k = a\}$ or in the polytope $P_b := \operatorname{conv}\{v \in V \ : \ v_k = a + 1\}$. This splits the problem of checking lattice-freeness into two independent and smaller ones. Note that the only reason Algorithm 2 is described with fixed value $a = 0$ is to keep notation simple.

Algorithm 2: Heuristic to decide lattice-freeness of a polytope (branchLatticeFree)

```
Input: $V$ vertices of a polytope, a list $L$ of coordinates that was already branched
       on
Output: $1$ if a certificate was found that $\operatorname{conv} V$ is lattice-free; $0$ otherwise
if $|V| \leq 1$ then
    return $1$;          // A trivial polytope is lattice-free.
foreach $k \in [n] \setminus L$ do
    if for all $v \in V$ it holds that $v_k \in \{0, 1\}$ then
        $r_0 \leftarrow$ branchLatticeFree($\{v \in V \ : \ v_k = 0\}, L \cup \{k\}$);
        $r_1 \leftarrow$ branchLatticeFree($\{v \in V \ : \ v_k = 1\}, L \cup \{k\}$);
        if $r_0 + r_1 = 2$ then
            return $1$;
return $0$;
```

Example 4.21. Figure 4.2 shows how Algorithm 2 proves that the point $z := (0, 0, 1, 1, 0, 1, 1, 1, 2)^\top$ is a core point for the group $G = \langle (2\,5\,6\,7\,3\,9\,8\,4), (1\,2\,3)(4\,5\,6)(7\,8\,9) \rangle$ with id 9-4. Since $\langle \mathbb{1}, z \rangle = 7$, every integral point in $P := \operatorname{conv} Gz$ must have at least $2 = 9 - 7$ coordinates with value zero.

Because G is 2-transitive we can assume w.l.o.g. that these are the first two coordinates. Therefore, every integral point in P is a convex combination of the six vertices that are colored in Figure 4.2. All these vertices have at coordinate three only the values 1 or 2. Thus, every integral point in P must be a combination either of the first four (red) or the last two (orange) vertices in Figure 4.2a. In the next step, we can split these two sets further by looking at the fourth coordinate as shown in Figure 4.2b. Proceeding in this manner shows that all inner integral points must be vertices. Note that this core point is not constructible by Corollary 4.17 because $I\left(\{1,2,5\} = \{i \;:\; z_i = 0\}\right) = 2 > 1$. ■



```
0 0 1 1 0 1 1 1 2
0 0 1 1 1 0 1 2 1
0 0 1 1 1 2 0 1 1
0 0 1 2 1 1 1 1 0
0 0 2 0 1 1 1 1 1
0 0 2 1 1 1 1 0 1
0 1 0 0 1 1 1 2 1
0 1 0 1 0 1 2 1 1
0 1 0 1 1 2 1 0 1
0 1 0 1 2 1 1 1 0
0 1 1 0 0 1 1 1 2
...
```

(a) branching on third coordinate

```
0 0 1 1 0 1 1 1 2
0 0 1 1 1 0 1 2 1
0 0 1 1 1 2 0 1 1
0 0 1 2 1 1 1 1 0
0 0 2 0 1 1 1 1 1
0 0 2 1 1 1 1 0 1
0 1 0 0 1 1 1 2 1
0 1 0 1 0 1 2 1 1
0 1 0 1 1 2 1 0 1
0 1 0 1 2 1 1 1 0
0 1 1 0 0 1 1 1 2
...
```

(b) branching on fourth coordinate

Figure 4.2.: 11 of 72 vertices of a lattice-free orbit polytope, proof by Algorithm 2

Computational experiments show that many of the computed core points can be proven to be core points by recursive application of Algorithm 2 to their orbit polytopes (see Table 4.5). In some cases this heuristic does not suffice and there remain non-trivial sub-polytopes that are lattice-free and do not offer a coordinate to branch on. To make Algorithm 2 return 1 *if and only if* its input is lattice-free, some other check for lattice-freeness could be added in line 9 when no coordinate for branching was found.

Table 4.5 contains statistics about the core points that were found by the search described in the previous section. The table lists only groups which have non-universal core points. The columns of the table are as follows:

1. *(group id)* GAP primitive id
2. *(large layer)* number of core points $z \in \mathbb{Z}^n_{\geq 0}$ with $\langle \mathbb{1}, z\rangle > n$; for these, none of the techniques from this section applies
3. *(branch)* number of core points which can be verified by branching (cf. Algorithm 2)
4. *(intersection)* number of core points that can be obtained from Corollary 4.17
5. *(other)* number of core points $z \in \mathbb{Z}^n_{\geq 0}$ with $\langle \mathbb{1}, z\rangle < n$ that cannot be verified by branching and not be obtained from Corollary 4.17
6. *(total)* number of core points

In all these descriptions the expression “number of core points” refers to the number of non-universal non-isomorphic zero-based core points with $2\langle \mathbb{1}, z\rangle \leq n \max z_i$ because this part of a fundamental core set already contains all relevant constructions (cf. Remark 3.21 and (4.21)).

Table 4.5.: Core point types of 2-homogeneous groups up to degree twelve

group id	large layer	branch	intersection	other	total
7-3	0	8	8	0	10
7-4	0	1	0	0	1
7-5	0	1	2	0	2
8-1	0	0	1	3	4
8-2	0	0	1	0	1
8-3	0	0	1	0	1
8-4	0	0	2	0	2
9-3	0	10	11	3	20
9-4	0	8	5	7	18
9-5	0	6	5	1	10
9-6	0	1	2	1	3
9-7	0	1	2	1	3
10-3	0	0	6	2	8
10-4	0	0	2	0	2
10-5	0	0	4	2	6
10-6	0	0	4	0	4
10-7	0	0	2	0	2
11-3	1052	551	73	787	2407
11-4	29	38	9	133	208
11-5	0	2	7	2	11
11-6	0	0	2	0	2
12-1	0	0	3	1	4
12-2	0	0	1	0	1
12-3	2	0	7	6	15
12-4	0	0	1	1	2

4.5.2. Towards a better flatness theorem for orbit polytopes

In this section we reinterpret previous and following results in a different light. We have seen and we will see results concerning the quantity

$$\operatorname{bw}(z) := \max_{i\in[n]} z_i - \min_{i\in[n]} z_i \tag{4.24}$$

for a core point $z \in \mathbb{Z}^n$ (see Corollary 4.4, Proposition 4.8, Remarks 4.26 and 4.30). In this section we refer to $\operatorname{bw}(z)$ as the **box width** since it is the side length of an axis-parallel cube that encloses the orbit polytope. Moreover, we use the term “width” for the lattice width of a polytope. If $G \leq \mathcal{S}_n$ is a transitive group, we can interpret the box width (4.24) as a bound on the width of the corresponding orbit polytope because it holds that

$$\operatorname{bw}(z) = \omega(\operatorname{conv} Gz, e^{(1)}) \geq \min_{u \in \mathbb{Z}^n \setminus (\operatorname{span} \mathbb{1})} \omega(\operatorname{conv} Gz, u) = \omega_{\mathsf{A}_{n-1}}(\operatorname{conv} Gz). \tag{4.25}$$

Since all orbit polytopes live in an affine (translated) version of the lattice A_{n-1}, this enables us to compare results of this thesis with results from the literature about the (lattice) width of lattice-free polytopes. The following flatness result is an immediate consequence of (4.25) and Proposition 4.8

Theorem 4.22. Let $G \leq \mathcal{S}_n$ be a 2-homogeneous group. Then the width of a lattice-free orbit polytope $\operatorname{conv} Gz$ is bounded by

$$\omega_{\mathsf{A}_{n-1}}(\operatorname{conv} Gz) \leq 1.09\,(n-1).$$

If G is 2-transitive the right-hand side can be replaced by $n-3$.

This bound for symmetric polytopes is better than the $O(n^{3/2})$ best known bound for arbitrary lattice-free polytopes by Banaszczyk, Litvak, Pajor & Szarek [BLPS99] and also the best bound $O(n \log n)$ for centrally symmetric polytopes by Banaszczyk [Ban95]. As in the general case it is unknown whether the bound in Theorem 4.22 is optimal (cf. Table 4.3). In the following sections we will construct series of core points in many dimensions, which gives a lower bound on the upper bound in Theorem 4.22. Comparing again to the general case, the best constructions of lattice-free polytopes with large width are simplices by Sebö & Bárány [Seb99]. These n-dimensional simplices have width $n-2$ and $n-1$ for odd and even n, respectively. In our symmetric setting we will construct core points with the following box width bw. For 2-transitive groups we will obtain a core point $z \in \mathbb{Z}^n$ with $\operatorname{bw}(z) = \frac{n-1}{4}$ by Remark 4.26. For 2-homogeneous groups we will construct a core point $z \in \mathbb{Z}^n$ with $\operatorname{bw}(z) = \frac{n-1}{2}$ (see Remark 4.30) and look at a conjecture for another core point with $\operatorname{bw}(z) = \frac{3n-9}{4}$ (see Conjecture 4.33).

Another direction for assessing the tightness of Theorem 4.22 is the inequality in (4.25). Computational experiments with many thousands of randomly generated (not necessarily lattice-free) orbit polytopes of 2-homogeneous groups easily produced instances where the width is strictly smaller than $\operatorname{bw}(z)$. However, similar experiments with 2-transitive groups always satisfied the equation $\omega_{\mathsf{A}_{n-1}}(\operatorname{conv} Gz) = \operatorname{bw}(z)$. Note that the width of a simplex can be computed by an integer programming formulation suggested by Haase & Ziegler [HZ00]. This integer programming model can be adapted to compute the width of orbit polytopes of 2-homogeneous groups. The results of these experiments motivate the following question.

Question 4.23. Is there a difference between $\operatorname{bw}(z)$ and $\omega_{\mathsf{A}_{n-1}}(\operatorname{conv} Gz)$ for 2-transitive groups $G \leq \mathcal{S}_n$?

In the general setting, several authors studied the width-related properties of lattice-free simplices as a special case of lattice-free polytopes (see, for instance, [Seb99], [HZ00] and [BBBK11]). Without a complete classification, a prominent question has been what the maximal width of a lattice-free simplex is. We will come back to this topic for “orbit simplices” in Remark 4.31.

4.5.3. Affine groups over fields of odd order

In this section we use previous results to construct core points for a whole series of groups: affine semilinear groups over finite fields. Note that affine linear groups, which belong to this series, are **sharply** $\mathbf{2}$**-transitive**. That means, for every two pairs (a, b) and (c, d) there is exactly one permutation g with $g(a) = c$ and $g(b) = d$. Thus, these are the smallest 2-transitive groups for their degree. One could heuristically argue that this fact leads to a large variety of core points. Therefore, their core points might shed some light on the question how tight the various bounds from Section 4.2 are. All sharply 2-transitive groups arise as affine linear groups over near-fields ([Zas35], cf. [Cam99, Sec 1.12]), but for the sake of simplicity we work only with fields of odd order. For our study of these groups let q be an odd prime power with $q \geq 5$. We consider a one-dimensional affine semilinear group over $\mathbb{F}_q$. That is, we look at the group

$$G \cong \left\{x \to bx^\sigma + c \ : \ b \in \mathbb{F}_q^*, c \in \mathbb{F}_q, \sigma \in A\right\} \leq \mathrm{A\Gamma L}(1, q) \tag{4.26}$$

where $A \leq \mathrm{Aut}(\mathbb{F}_q)$ is a group of field automorphisms. Viewed as a permutation group, G acts 2-transitively on q points and has order $q(q-1)\,|A|$. For $q \equiv 3 \pmod 4$ these are supergroups of the 2-homogeneous groups, which we studied in Section 4.3. The only difference to (4.3) is that here b does not have to be a square. As before, we denote by $\mathcal{S}$ the set of non-zero squares in $\mathbb{F}_q$. Since we also allow for $q \equiv 1 \pmod 4$ in this section, we denote by $\mathcal{N}$ the set of non-squares in $\mathbb{F}_q$, which we could previously refer to simply as $-\mathcal{S}$.

Proposition 4.24. For an odd prime power q with $q \geq 5$ let $G \leq \mathrm{A\Gamma L}(1, q)$ be a 2-transitive group. If $q \equiv 3 \pmod 4$, let $M \in \{0, \ldots, \frac{q-3}{4}\}$. Otherwise, that is $q \equiv 1 \pmod 4$, let $M \in \{0, \ldots, \frac{q-1}{4}\}$. Let $z \in \mathbb{Z}^q$ be such that $z_0 = M$, $z_i = 0$ for $i \in \mathcal{S}$ and $z_i = 1$ for $i \in \mathcal{N}$. Then z is a core point.

Before we commence the proof, we remind ourselves of Lemma 4.13 from page 29, which deals with $q \equiv 3 \pmod 4$. Its parts (ii) and (iii) are the following:

$$|\mathcal{S} \cap (\mathcal{S} + c)| = \begin{cases} \frac{q-1}{2} & \text{if } c = 0, \\ \frac{q-3}{4} & \text{otherwise;} \end{cases} \quad \text{and} \quad |\mathcal{S} \cap (\mathcal{N} + c)| = \begin{cases} 0 & \text{if } c = 0, \\ \frac{q-3}{4} & \text{if } c \in \mathcal{S}, \\ \frac{q+1}{4} & \text{if } c \in \mathcal{N}. \end{cases} \tag{4.27}$$

For $q \equiv 1 \pmod 4$ one can prove by the very same technique as used for Lemma 4.13 that the following holds.

$$|\mathcal{S} \cap (\mathcal{S} + c)| = \begin{cases} \frac{q-1}{2} & \text{if } c = 0, \\ \frac{q-5}{4} & \text{if } c \in \mathcal{S}, \\ \frac{q-1}{4} & \text{if } c \in \mathcal{N}; \end{cases} \quad \text{and} \quad |\mathcal{S} \cap (\mathcal{N} + c)| = \begin{cases} 0 & \text{if } c = 0, \\ \frac{q-1}{4} & \text{otherwise.} \end{cases} \tag{4.28}$$

We will also use the following simple observation that we have used in the $q \equiv 3 \pmod 4$-case before.

Lemma 4.25. Let q be an odd prime power and $G \leq \mathrm{A\Gamma L}(1, q)$ be 2-homogeneous as in (4.3). Then

$$\mathrm{Stab}_G(\mathcal{S}) = \{x \to bx^\sigma \ : \ b \in \mathcal{S}, \sigma \in A\}$$

and this stabilizer has orbits $\{0\}, \mathcal{S}, \mathcal{N}$.

Proof. For every $\sigma \in \operatorname{Aut}(\mathbb{F}_q)$ the following holds: If $b \in \mathcal{S}$, we have that $b\mathcal{S}^\sigma = \mathcal{S}$ and $b\mathcal{N}^\sigma = \mathcal{N}$. If $b \in \mathcal{N}$, we have that $b\mathcal{S}^\sigma = \mathcal{N}$ and $b\mathcal{N}^\sigma = \mathcal{S}$. From (4.27) and (4.28) it follows that $\mathcal{S} + c = \mathcal{S}$ if and only if $c = 0$. Similarly, we deduce that $\mathcal{N} + c \neq \mathcal{S}$ for all $c \in \mathbb{F}_q$. Thus, all affine semilinear functions $x \to bx^\sigma + c$ that preserve the squares $\mathcal{S}$ must have translation part $c = 0$ and factor $b \in \mathcal{S}$. □

Now we have assembled all the ingredients to prove the main proposition of this section.

Proof of Proposition 4.24. We use the intersection construction from Proposition 4.16 with the set of non-zero squares $\mathcal{S} \subset \mathbb{F}_q$ playing the role of S. First, we compute the intersection number $I_G(\mathcal{S})$. From Lemma 4.25 and its proof we know that $I_G(\mathcal{S})$ is the maximum of the following two maxima:

$$M_1 := \max\left\{|\mathcal{S} \cap (\mathcal{S} + c)| \ : \ c \in \mathbb{F}_q^*\right\} \tag{4.29}$$

$$M_2 := \max\left\{|\mathcal{S} \cap (\mathcal{N} + c)| \ : \ c \in \mathbb{F}_q\right\} \tag{4.30}$$

In the case $q \equiv 3 \pmod 4$ we use (4.27) to compute $M_1 = \frac{q-3}{4}$ and $M_2 = \frac{q+1}{4}$. Hence,

$$I_G(\mathcal{S}) = \max\{M_1, M_2\} = \frac{q+1}{4}.$$

In the other case $q \equiv 1 \pmod 4$ we use (4.28) to compute $M_1 = M_2 = \frac{q-1}{4}$, yielding

$$I_G(\mathcal{S}) = \frac{q-1}{4}.$$

Knowing the value of $I_G(\mathcal{S})$, we apply Proposition 4.16. This allows a maximal coordinate M of at most

$$M \leq q - |\mathcal{S}| \cdot 1 - (I_G(\mathcal{S}) + 1) = \frac{q-1}{2} - I_G(\mathcal{S}).$$

The groups $\operatorname{Stab}_G(z)$ and $\operatorname{Stab}_G(\mathcal{S})$ are the same by Lemma 4.25 and construction of z. Hence, z is trivially a core point for $\operatorname{Stab}_G(\mathcal{S})$ and therefore also for G by Proposition 4.16. □

Remark 4.26. This shows that the best general upper bound on $\max z_i$ for a zero-based core point $z \in \mathbb{Z}^n_{\geq 0}$ of a 2-transitive group is at least $\frac{n-1}{4}$.

In the next section we will see a similar construction for 2-homogeneous groups, yielding a slightly larger minimal value for $\max z_i$.

4.5.4. 2-homogeneous groups

In this section we focus on the 2-homogeneous groups that are not 2-transitive. For these, we construct families of "large" core points. As in the previous section, knowledge of such series of core points helps us to estimate the quality of the various bounds derived before. Again, all core point constructions for these groups are closely related to properties of squares in finite fields. For the first family of core points we need the following lemma.

Lemma 4.27. Let $a, b \in -\mathcal{S}$ with $a \neq b$. Then $(a+\mathcal{S}) \cap (b-\mathcal{S})$ contains at least one square.

Proof. First, note that the condition $a \neq b$ implies $q \geq 7$ because we need two distinct non-squares. Assume, for a contradiction, that $(a+\mathcal{S}) \cap (b-\mathcal{S}) \cap \mathcal{S}$ is empty. By Lemma 4.13 (ii) the set $(a+\mathcal{S})$ contains $\frac{q-3}{4}$ squares. Similarly, we know from Lemma 4.13 (iii) that the set $(b-S)$ contains $\frac{q+1}{4}$ squares. Because there are only $\frac{q-1}{2}$ (non-zero) squares in total, our assumption implies that every square must lie either in $a+\mathcal{S}$ or $b-\mathcal{S}$, but not in both. Hence, for every square $s \in \mathcal{S}$ either $s-a \in \mathcal{S}$ or $s-b \in -\mathcal{S}$. Moreover, $s-a$ and $s-b$ are never zero since $a, b \in -\mathcal{S}$. This implies that the quadratic character η evaluates to the same non-zero value ± 1 for both $s-a$ and $s-b$. Therefore we obtain the following sum:

$$\sum_{s \in \mathcal{S}} \eta(s-a)\eta(s-b) = |\mathcal{S}| = \frac{q-1}{2}. \tag{4.31}$$

By Weil's Theorem [LN08, Thm 5.41] we know that for $a \neq b$ we have the bound

$$\left|1 + 2\sum_{s \in \mathcal{S}} \eta(s-a)\eta(s-b)\right| = \left|\sum_{x \in \mathbb{F}_q} \eta(x^2-a)\eta(x^2-b)\right| \leq 3\sqrt{q}.$$

Thus, $\left|\sum_{s \in \mathcal{S}} \eta(s-a)\eta(s-b)\right| \leq \frac{3\sqrt{q}+1}{2}$, which contradicts (4.31) for $q \geq 19$. For $q \in \{7, 11\}$ one can check by hand that the claim of the lemma holds. □

Remark 4.28. The previous lemma is very similar to Theorem A of [Iwa03], but this is not enough to prove Lemma 4.27 directly. Also, the quantity $|(a+\mathcal{S}) \cap (b-\mathcal{S}) \cap \mathcal{S}|$ varies considerably depending on a and b, which makes it hard to give an explicit formula.

Proposition 4.29. Let $G \leq \mathcal{S}_q$ be a 2-homogeneous group that is not 2-transitive. Let $M \in \{0, \ldots, \frac{q-1}{2}\}$. Let $z \in \mathbb{Z}^q$ be such that $z_0 = M$, $z_i = 0$ for $i \in \mathcal{S}$ and $z_i = 1$ for $i \in -\mathcal{S}$. Then z is a core point and the orbit polytope $\operatorname{conv} Gz$ is a lattice-free regular simplex.

Proof. Let $T := \operatorname{conv} Gz$. We will show that T is a regular simplex and that it is lattice-free. The group G has the same structure as in (4.3), that is,

$$G \cong \{x \to bx^\sigma + c \ : \ b \in \mathcal{S}, c \in \mathbb{F}_q, \sigma \in A\}$$

for an automorphism group $A \leq \operatorname{Aut}(\mathbb{F}_q)$. From Lemma 4.25 we know that the stabilizer of z in G is the group $\{x \to bx^\sigma \ : \ b \in S, \sigma \in A\}$ of semilinear transformations in G. Thus, the vertices of T are $g_e z$ where g_e corresponds to the translation $x \to x+e$ for an $e \in \mathbb{F}_q$. Since there are q such translations, the polytope T is a simplex. The simplex T is regular because its minimal enclosing ellipsoid is a ball by Theorem 3.12.

By construction $\langle \mathbb{1}, z\rangle$ is positive and is smaller than q. Hence, for each integer point $u \in T \cap \mathbb{Z}^q$ at least one coordinate must be zero. Because of transitivity we may assume without loss of generality that $u_0 = 0$. Thus, u must be a convex combination of the vertices from $T_0 := \{g_i z \ : \ i \in -\mathcal{S}\}$, for which the first coordinate is zero. Looking at T_0 again, we observe that the coordinates with value M are indexed by $-\mathcal{S}$. Hence, the points in T_0 have only 0 and 1 at their coordinates indexed by $\mathcal{S}$.

Let $g_i z$ and $g_j z$ be two vertices from T_0; this especially implies $i, j \in -\mathcal{S}$. The set $i+\mathcal{S}$ describes the indices of coordinates of $g_i z$ with value 0. Similarly, the set $j-\mathcal{S}$ describes coordinates with value 1 of $g_j z$. Lemma 4.27 tells us that for $i, j \in -\mathcal{S}$ the intersection $(i+\mathcal{S}) \cap (j-\mathcal{S}) \cap \mathcal{S}$ is never empty. Therefore, any two vertices $g_i z, g_j z \in T_0$ differ in at least one of their coordinates indexed by $\mathcal{S}$. By our considerations above, at these coordinates the values can only be 0 or 1. Thus, the only integral convex combinations of T_0 are the trivial ones. Hence, all integral points in $\operatorname{conv} T_0$ are vertices. So, T_0 and thus also T are lattice-free. □

Remark 4.30. This shows that the best upper bound on $\max z_i$ for a zero-based core point $z \in \mathbb{Z}^n_{\geq 0}$ of a 2-homogeneous group is at least $\frac{n-1}{2}$ (cf. Remark 4.26).

Remark 4.31. For ambient dimension $q = 11$ one can compute the lattice width of the simplex T as $\omega_{\mathsf{A}_{10}}(T) = 5$, using an integer optimization formulation based on [HZ00]. This width is realized by the direction $e^{(0)} - \frac{1}{10}\mathbb{1} \in \mathsf{A}^*_{10}$ (and all other elements from its orbit). This direction immediately provides the upper bound

$$\omega_{\mathsf{A}_{q-1}}(T) \leq \omega(T, e^{(0)}) = M - 0 \leq \frac{q-1}{2} \tag{4.32}$$

which probably already is the true value of the width. The simplices from Proposition 4.29 could have maximal width among all "orbit simplices" for the following reasons. An orbit polytope $\operatorname{conv} Gz$ of a transitive group G is a simplex if and only if the point z is constant on the orbits of a stabilizer $\operatorname{Stab}_G(j)$ for some $j \in [n]$. So, if G is 2-transitive, then the only lattice-free orbit simplices are translates of $\operatorname{conv}\{e^{(1)}, \ldots, e^{(n)}\}$, which obviously has lattice width one. For a 2-homogeneous, not 2-transitive group, orbit simplices follow the same pattern as in Proposition 4.29. Perhaps it can be shown using the projection technique from Section 4.3.2 that these contain an inner lattice point if the width is large. All lattice-free orbit polytopes of groups that are not 2-homogeneous have to be flat by the flatness theorem (see Theorem 3.13). These are likely to have smaller width than T so that T from Proposition 4.29 looks like a good candidate for an orbit simplex with large width.

After these general considerations we turn back to the construction of core points for 2-homogeneous groups.

Remark 4.32. Another way to look at the proof of Proposition 4.29 is with Algorithm 2 in mind. We first establish that it is enough to show that T_0 is lattice-free. We then show that we can branch on any coordinate indexed by $\mathcal{S}$. Since $|T_0| = |\mathcal{S}|$, we are certain that every recursion stops with a "polytope" consisting of a single point, which is lattice-free by definition.

This fact that we have many choices for a branching coordinate makes proving lattice-freeness quite easy. In the following we look at a generalization of this construction, which possibly leads to even larger core points. Computational experiments (cf. Remark 4.35) seem to support the following conjecture. However, a rigorous general proof is still missing since a more sophisticated branching strategy compared to the last proposition is required.

Conjecture 4.33. Let $G \cong \{x \to bx + c \ : \ b \in \mathcal{S},\ c \in \mathbb{F}_n\}$ be a 2-homogeneous group that is not 2-transitive. There is a zero-based core point z with $\max z_i = \frac{3n-9}{4}$.

Note that the pre-condition of this conjecture implies that the degree n of G is a prime power with $n \equiv 3 \bmod 4$ (see Section 4.3.1). The conjecture is based on the following construction. Let q be a prime power with $q \equiv 3 \bmod 4$. Let t be a primitive element of $\mathbb{F}_q$, i.e., $\mathbb{F}_q^* = \{1, t, t^2, \dots, t^{q-1}\}$. Let $\mathcal{S}' := \left\{t^{2i} \ : \ i \in \{0, \dots, \frac{q-3}{4}\}\right\}$ be a subset of squares. Let $z \in \mathbb{Z}^q$ be with coordinates as follows:

$$z_i := \begin{cases} M & \text{for } i = 0, \\ 1 & \text{for } i \in \mathcal{S}', \\ 0 & \text{otherwise,} \end{cases} \tag{4.33}$$

where $M \in \{2, \dots, \frac{3q-9}{4}\}$. In the computationally tested cases such a point z is a core point for almost all primitive t (cf. Remark 4.35). Note that M is chosen in such a way that $\langle \mathbb{1}, z\rangle \leq q - 2$. Hence, any integer point u in $P := \operatorname{conv} Gz$ must have at least two zeros. Without loss of generality we may assume that $u_0 = u_1 = 0$ because G is 2-homogeneous. As in the proof of Proposition 4.29, this imposes a condition on which vertices the point u can be a convex combination of.

Although it is unclear whether it leads to a proof, we can still proceed in the same way as before, outlined in Remark 4.32. It is enough to show that $P_0 := \operatorname{conv}\{gz \ : \ g \in G \text{ and } (gz)_0 = (gz)_1 = 0\}$ is lattice-free. We will prove that we always find a suitable first coordinate to branch on. The difficulty which makes the proof of the conjecture incomplete is showing that also for all subproblems a branching coordinate exists.

Lemma 4.34. There is a coordinate index $c_0 \in \{2, \dots, n\}$ such that for all vertices $v \in \operatorname{vert} P_0$ it holds that $v_{c_0} \in \{0, 1\}$.

Proof. Let $x \to bx + c$ be an affine transformation for some $b \in \mathcal{S}$ and $c \in \mathbb{F}_q$. We denote the induced permutation of $\mathbb{F}_q$ by $g(b, c)$. To characterize P_0 and its vertices more explicitly it is thus enough to determine a set $T_0 \subset \mathcal{S} \times \mathbb{F}_q$, such that $P_0 = \operatorname{conv}\{g(b, c)z \ : \ (b, c) \in T_0\}$. If we additionally know that there exists a $c_0 \in \mathbb{F}_q$ such that for all $b \in \mathcal{S}$ the pair (b, c_0) does not lie in T_0, then we know that all vertices of P_0 have only zeros and ones at the coordinate with index c_0. This is because the only coordinate of z that is neither zero nor one has index 0 and is therefore mapped by $g(b, c)$ onto index c. If a value of c_0 does not occur in T_0 at all, we thus have found a first coordinate to branch on. In the following we show that such a c_0 always exists.

For $c, d \in \mathbb{F}_q$ let $B(c, d) := \{\frac{d-c}{s} \ : \ s \in \mathcal{S}'\}$ the values of b such that $bs + c = d$ for an $s \in \mathcal{S}'$. In other words, $B(c, d)$ describes affine transformations that map the coordinate zero (and value M) onto c and one of the coordinates indexed by $\mathcal{S}'$ (each with value 1) onto d. For every $(b, c) \in T_0$ it holds that $b \notin B(c, 0) \cup B(c, 1)$ because we must not have value one at the coordinates with index 0 and 1. Similarly, we know that $c \notin \{0, 1\}$ because we exclude the value M. If we can show that there exists some $c_0 \notin \{0, 1\}$ so that the forbidden values for b cover all valid values for b, i.e.

$$\mathcal{S} \subseteq B(c_0, 0) \cup B(c_0, 1), \tag{4.34}$$

then we have found the sought index c_0. The idea to find such an index c_0 is that $B(c_0, 1)$ continues the series of squares started by $B(c_0, 0)$ or vice versa. Remember that

$$B(c,d) = \left\{ \frac{d-c}{t^{2j}} \ : \ j \in \left\{ 0, \dots, \frac{q-3}{4} \right\} \right\}.$$

Thus, if

$$\frac{-c_0}{t^{\frac{q+1}{2}}} = 1 - c_0 \quad \Longleftrightarrow \quad c_0 = 1 + \frac{1}{t^{\frac{q+1}{2}} - 1}, \tag{4.35}$$

then

$$B(c,0) \cup B(c,1) = \left\{ \frac{-c_0}{t^{2j}} \ : \ j \in \left\{ 0, \dots, \frac{q-3}{4} \right\} \cup \left\{ \frac{q+1}{4}, \dots, \frac{q-1}{2} \right\} \right\} = -c_0 \mathcal{S}. \tag{4.36}$$

This covers the set of squares $\mathcal{S}$ if and only if $-c_0 \in \mathcal{S}$. By (4.35) this depends on the primitive field element t. If this c_0 does not satisfy this condition, we can also join the B-sets the other way round. If

$$\frac{1-c_0}{t^{\frac{q+1}{2}}} = -c_0 \quad \Longleftrightarrow \quad c_0 = \frac{1}{1 - t^{\frac{q+1}{2}}}, \tag{4.37}$$

then

$$B(c,0) \cup B(c,1) = \left\{ \frac{1-c_0}{t^{2j}} \ : \ j \in \left\{ 0, \dots, \frac{q-3}{4}, \frac{q+1}{4}, \dots, \frac{q-1}{2} \right\} \right\} = (1-c_0)\mathcal{S}. \tag{4.38}$$

This covers the set of squares $\mathcal{S}$ if and only if

$$(1-c_0) \in \mathcal{S} \quad \Longleftrightarrow \quad 1 + \frac{1}{t^{\frac{q+1}{2}} - 1} \in \mathcal{S}. \tag{4.39}$$

As t is a primitive element, the power $t^{\frac{q+1}{2}}$ is never zero or one, implying that for both choices of c_0 the value of c_0 exists and never equals zero or one. Comparing the right-hand sides of (4.35) and (4.39), we conclude that either $-c_0 \in \mathcal{S}$ for c_0 from (4.35) or $1 - c_0 \in \mathcal{S}$ for c_0 from (4.37). Hence, there always exists a solution $c_0 \notin \{0, 1\}$ of (4.34). □

Remark 4.35. Conjecture 4.33 has been computationally verified for $n \leq 150$, using the aforementioned construction. Like in (4.36) and (4.38), one can give explicit formulas for possible branching variables in all the subproblems. In the tested range $n \in [7, 150]$ there are only two cases where for some subproblem no branching variable can be found; the corresponding orbit polytopes also are not lattice-free. This happens for all choices of t in dimension 7 and for $t \in \{2, 6\}$ in dimension 11. In dimension 11 the construction yields a core point for $t \in \{7, 8\}$. For all other tested dimensions and all choices of t the point z from (4.33) is a core point.

5. Infinite Fundamental Core Sets of Transitive Groups

In this chapter we construct core points for many transitive groups that are not covered by the previous Chapter 4. For transitive groups which are not 2-homogeneous we prove that the fundamental core set often is infinite. In fact, we see experiments that suggest this is always the case (cf. Conjecture 3.27). Theorem 5.6 in Section 5.2 and Theorem 5.18 in Section 5.3 prove parts of this conjecture. The remaining open case is discussed in Section 5.4.

For the core point constructions we proceed as follows. From Theorem 3.13 we know that core points are always close to an invariant subspace. In Section 5.1 we look at an outline of a core point construction that is based on proximity to invariant subspaces. Depending on the structure of the invariant subspace, different arguments apply. Section 5.2 constructs core points for non-rationally generated invariant subspaces. In Sections 5.3 and 5.4 we deal with rationally generated invariant subspaces, split in imprimitive and primitive groups.

5.1. Construction idea

The construction ideas in this section are a joint project with Katrin Herr [Her13b, Sec 4.5.1].

5.1.1. Invariant subspaces

As repeated above, Theorem 3.13 shows that core points are close to at least one invariant subspace. Our main tool will be orthogonal projection onto an arbitrary invariant subspace of a transitive group. If this projection of an integer point z has small norm, i.e., the point z is close to an invariant subspace, then z is a good candidate for a core point. Remember that we can always decompose $\mathbb{R}^n$ into a direct sum of invariant subspaces $\mathbb{R}^n = \operatorname{span} \mathbb{1} \oplus \bigoplus_i V_i$. If such an invariant subspace V_i contains no rational vectors, i.e., $V_i \cap \mathbb{Q}^n = \{0\}$, we call V_i an **irrational invariant subspace**. Similarly, we say that V_i is **rational** if it has a rational basis.

Every (non-trivial) irreducible invariant subspace of $\mathbb{R}^n$ is either rational or irrational because for every invariant subspace V_i the set $V_i \cap \mathbb{Q}^n \subseteq V_i$ is an invariant subspace as well. Thus, reducible subspaces may be neither rational nor irrational by this definition, but for our purposes it is enough to cover irreducible subspaces. For some groups, for instance, cyclic groups of prime order, all irreducible invariant subspaces except the fixed space are irrational (cf. Example 2.2). A detailed study of these groups was performed by Dixon [Dix05].

5.1.2. Core points by projection

Our goal throughout this section is to find core points. Therefore we need a way to prove that an orbit polytope $\operatorname{conv} Gz$ is lattice-free. The main tool that we use is projection onto an invariant subspace of G. If both the projection and the fibers are lattice-free in some sense, then we can prove lattice-freeness for the whole orbit polytope. Proposition 5.4 will give a sufficient core point condition in quite general (and also quite technical) terms. We start with an outline of the idea behind this proposition.

Let $G \leq \mathcal{S}_n$ be a permutation group and V be an invariant subspace of G. Furthermore, let $z \in \mathbb{Z}^n$ be an integral point. We will frequently use the following two easy observations. The first, important observation is that group action and projection to an invariant subspace commute. The second observation relates the stabilizer of a point to the stabilizer of its projection.

Lemma 5.1. Let $G \leq \mathcal{S}_n$ be a permutation group and V an invariant subspace of G. Group action and projection commute: $(gx)|_V = g(x|_V)$ for all $g \in G$ and $x \in \mathbb{R}^n$.

Proof. Let $W := V^\perp$ be the orthogonal complement of V. We can decompose $x = v \oplus w$ into a direct sum from distinct invariant subspaces $v \in V$ and $w \in W$. Since the action of G is linear, we have $gx = gv + gw$ for every permutation $g \in G$. Because V and W are invariant subspaces, we must have $gv \in V$ and $gw \in W$. Hence, this is a direct sum $gx = gv \oplus gw$. Thus, $(gx)|_V = gv = g(x|_V)$. □

Lemma 5.2. Let $G \leq \mathcal{S}_n$ be a permutation group and V an invariant subspace of G. For every $z \in \mathbb{Z}^n$ it holds that $\operatorname{Stab}_G(z) \leq \operatorname{Stab}_G(z|_V)$.

Proof. Let $g \in \operatorname{Stab}_G(z)$, that is $gz = z$. This implies $g(z|_V + z|_W) = z|_V + z|_W$, where $W := V^\perp$ is the orthogonal complement of V. Hence $gz|_V - z|_V = z|_W - gz|_W$. The only element in $V \cap W$ is the zero vector. Therefore $g \in \operatorname{Stab}_G(z|_V)$. □

We now turn to a method for proving lattice-freeness of orbit polytopes. Let $P := \operatorname{conv} Gz$ be an orbit polytope. Because P is not full-dimensional, it is enough to consider integral points in the affine hull of P. In the following we denote this set by $H := (\operatorname{aff} Gz) \cap \mathbb{Z}^n$. Note that for a transitive group the set H equals $\mathbb{Z}^n_{(k)}$ with $k = \langle \mathbb{1}, z \rangle$ as introduced before. Since we do not require transitivity for the results of this section, we proceed with the more general case and the set H. We use the following projection setup. We project both the orbit polytope P and all integral points H orthogonally onto V. To ensure the lattice-freeness of P we have to control the pre-image of all points in the intersection $Q := P|_V \cap H|_V$.

If the integral points in the pre-image of Q intersect P only at its vertices $\operatorname{vert}(P)$, then P is lattice-free. This condition is in general quite hard to test because it is an integer feasibility problem. Thus, we use relaxed conditions instead. The following two steps together allow us to control the pre-images of Q in some cases. First, we ensure that all integer points in P project only onto $\operatorname{vert}(P)|_V$. Second, we ensure that only vertices of P project onto $\operatorname{vert}(P)|_V$. These two steps together, controlling the projection and controlling the fibers, constitute Proposition 5.4. Before we get there, we need two more definitions.

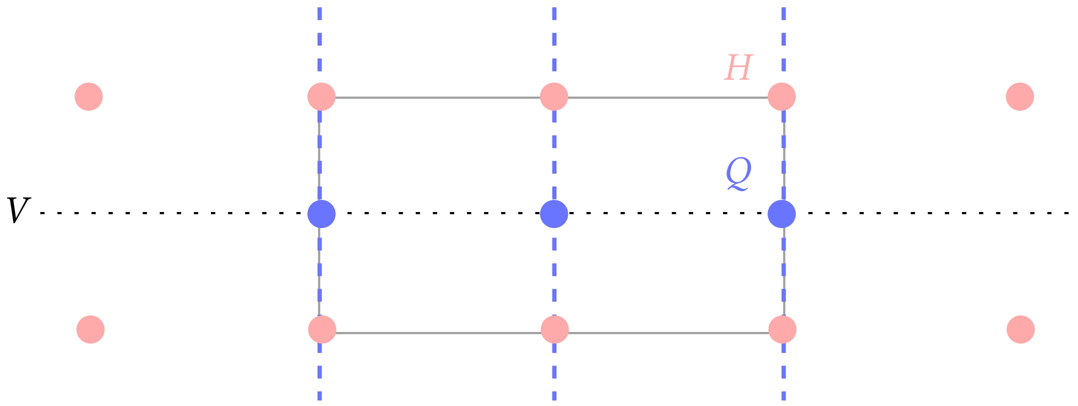


Figure 5.1.: Setup: subspace V, integral points H and their projection Q with fibers

For the first step we use arguments based on the Euclidean norm. We say that z has a **globally minimal** projection (with respect to some invariant subspace V) if

$$\|z|_V\| \leq \|z'|_V\| \quad \text{for all } z' \in (\operatorname{aff} Gz) \cap \mathbb{Z}^n, \tag{5.1}$$

If z has globally minimal projection, then integer points in P can project only onto $\operatorname{vert}(P)|_V$. The argument behind this will be made explicit in Proposition 5.4 below. This completes the first step. However, we will see later that for irrational subspaces there is no point with globally minimal projection (cf. Lemmas 5.8 and 5.9). In this case the following weaker condition suffices. We say that a point z has **locally minimal** projection (with respect to some invariant subspace V) if

$$\|z|_V\| \leq \|z'|_V\| \quad \text{for all } z' \in (\operatorname{conv} Gz) \cap \mathbb{Z}^n. \tag{5.2}$$

Remark 5.3. Verifying that a concrete z has locally minimal projection by using this definition directly may be hard because the integral points in the orbit polytope are unknown when we want to prove that z is a core point in the first place. For this purpose it suffices to prove a relaxed condition. It is enough to prove $\|z|_V\| \leq \|z'|_V\|$ either

- for all $z' \in (\operatorname{aff} Gz) \cap \mathbb{Z}^n$ with $\|z'\| \leq \|z\|$ (since all points in an orbit polytope of an orthogonal group cannot have a larger norm than the vertices), or,
- if G is transitive and $z \in \mathbb{Z}^n_{\geq 0}$ is zero-based, for all zero-based $z' \in \mathbb{Z}^n_{\geq 0}$ with $\langle \mathbb{1}, z' \rangle \leq \langle \mathbb{1}, z \rangle$ (since all inner integral points lie in the same layer as the vertex and are isomorphic to a zero-based point in a layer with the same or smaller index). ■

With this notion of minimality we can formulate our main tool to guarantee lattice-freeness of an orbit polytope. We use minimality to control the projection of integral points and then argue with the help of the stabilizer of the projected vertex to fully control the pre-images.

Proposition 5.4. Let $G \leq \mathcal{S}_n$ be a permutation group and V an invariant subspace of G. Let $z \in \mathbb{Z}^n$ have locally minimal projection for V. Then z is a core point for G if and only if z is a core point for $\operatorname{Stab}_G(z|_V)$.

Proof. Because $\operatorname{Stab}_G(z|_V)$ is a subgroup of G, we only have to prove the "if"-part. For this let y be an integral point in $\operatorname{conv} Gz$. We can write y as convex combination

$$y = \sum_{g \in G} \lambda_g g z \tag{5.3}$$

with $0 \leq \lambda_g \leq 1$ and $\sum_{g \in G} \lambda_g = 1$. This yields:

$$\begin{aligned} \|z|_V\|^2 \leq \|y|_V\|^2 &= \left\| \left(\sum_{g \in G} \lambda_g g z \right) |_V \right\|^2 \\ &\leq \sum_{g \in G} \lambda_g \|(gz)|_V\|^2 = \|z|_V\|^2 . \end{aligned} \tag{5.4}$$

The first inequality holds because we assumed that z has locally minimal projection. The second inequality holds because of convexity of a norm and Jensen's inequality. The last equation holds since $\|(gz)|_V\| = \|g(z|_V)\| = \|z|_V\|$. For this we use Lemma 5.1 and that the linear representation of g is an orthogonal matrix. Note that the left- and right-most terms of (5.4) are the same, so we must in fact have equality.

Since the squared norm is strictly convex on V, equality in (5.4) holds if and only if there is a coset $h \operatorname{Stab}_G(z|_V)$ such that $\sum_{g \in h \operatorname{Stab}_G(z|_V)} \lambda_g = 1$. Plugging this into (5.3) yields

$$h^{-} y = \sum_{g \in \operatorname{Stab}_G(z|_V)} \lambda_g g z.$$

with $\lambda_g \geq 0$ and $\sum_{g \in \operatorname{Stab}_G(z|_V)} \lambda_g = 1$. Since z is a core point for $\operatorname{Stab}_G(z|_V)$, we must have $h^{-} y \in \operatorname{Stab}_G(z|_V) z$. Hence, the point y lies also in the orbit Gz. From this we conclude that z is a core point for G. □

Remark 5.5. For the proof of Proposition 5.4 we did not require that the group G is transitive, so the result also is true for intransitive groups, which we will look at in Chapter 6.

5.2. Irrational subspaces

5.2.1. A general construction

In this section we construct core points using irrational invariant subspaces. The main result will be the following.

Theorem 5.6. Let $G \leq \mathcal{S}_n$ be a transitive group that has an irrational invariant subspace. If k is not a multiple of n, then the core set of G contains infinitely many non-isomorphic core points in layer $\mathbb{Z}^n_{(k)}$.

The proof of this theorem is based on Proposition 5.4. More precisely, we use the following refinement for irrational subspaces.

Lemma 5.7. Let $G \leq \mathcal{S}_n$ and V an irrational invariant subspace. Furthermore, let $z \in \mathbb{Z}^n$ be an arbitrary integral point. Then the two following statements hold:

(i) $\operatorname{Stab}_G(z) = \operatorname{Stab}_G(z|_V)$.

(ii) If z has locally minimal projection with respect to V, then z is a core point.

Proof. To prove part (i), note that we have already proven the inclusion $\operatorname{Stab}_G(z) \leq \operatorname{Stab}_G(z|_V)$ in Lemma 5.2. To show the reverse direction let $\mathbb{R}^n = \operatorname{span} \mathbb{1} \oplus V \oplus W$. Note that, since V is an irrational subspace, the subspace W must also be irrational. Further, let $g \notin \operatorname{Stab}_G(z)$. We will show that $g \notin \operatorname{Stab}_G(z|_V)$. For $z = 0$ the statement obviously holds, so let $z \neq 0$. Thus, $gz - z = (gz - z)|_V + (gz - z)|_W$ is a non-zero integral vector. Since V and W are irrational subspaces, both projections must be non-zero. Because

$$0 \neq (gz - z)|_V = gz|_V - z|_V,$$

the permutation g does not stabilize $z|_V$. This shows $\operatorname{Stab}_G(z|_V) \leq \operatorname{Stab}_G(z)$ and completes part (i).

For the proof of part (ii) we observe that the minimality condition is the same as in Proposition 5.4. Thus, it remains to prove that z is a core point for $\operatorname{Stab}_G(z|_V)$. By part (i) of this lemma we know that $\operatorname{Stab}_G(z|_V) = \operatorname{Stab}_G(z)$. Hence, the orbit $\operatorname{Stab}_G(z|_V)z$ consists only of a single element and the corresponding orbit polytope is trivially lattice-free. Thus all prerequisites of Proposition 5.4 are satisfied, which shows that z is a core point for G. □

The last part of the previous lemma shows that local minimality with respect to an irrational subspace suffices to prove that a point is a core point. The following two lemmas combined show that this local minimality condition can be fulfilled for infinitely many points.

Lemma 5.8. Let $G \leq \mathcal{S}_n$ be transitive and let V be an irrational invariant subspace. For all $k \in [n-1]$ and every $z \in \mathbb{Z}^n_{(k)}$ it holds that $\|z|_V\| > 0$.

Proof. Let $\mathbb{R}^n = \operatorname{span} \mathbb{1} \oplus V \oplus W$. Note that W must be an irrational invariant subspace because V is irrational. We know that $z|_V$ is the zero vector if and only if $z \in \operatorname{span} \mathbb{1} \oplus W$. This is equivalent to the rational vector $z - \frac{k}{n}\mathbb{1}$ lying in W. Because W is irrational, the only rational vector it contains is the zero vector. Thus, the projection $z|_V$ can be zero only if k is a multiple of n. □

Lemma 5.9. Let $G \leq \mathcal{S}_n$ be transitive and let V be an irrational invariant subspace. Then for every $\varepsilon > 0$ and $k \in [n-1]$ there exists a vector $z \in \mathbb{Z}^n_{(k)}$ such that $\|z|_V\| < \varepsilon$.

Before we start with the lengthy proof of Lemma 5.9, we quickly assemble the proof of Theorem 5.6.

Proof of Theorem 5.6. Lemma 5.8 together with Lemma 5.9 show that for every $k \in [n-1]$ and every $\varepsilon > 0$ we find an integer point $\hat{z} \in \mathbb{Z}^n_{(k)}$ such that $0 < \|\hat{z}|_V\| < \varepsilon$. Consider the finite set

$$Z_{\text{smallproj}} := \{z \in \mathbb{Z}^n_{(k)} \ : \ \|z|_V\| < \varepsilon \text{ and } \|z\| \leq \|\hat{z}\|\}.$$

In $Z_{\text{smallproj}}$ we choose a point with minimal projection as

$$z := \operatorname{argmin}_{u \in Z_{\text{smallproj}}} \|u|_V\| \,.$$

This ensures that z has locally minimal projection. By letting ε go to zero, we thus obtain a sequence of distinct points $z^{(1)}, z^{(2)}, \dots \in \mathbb{Z}^n_{(k)}$. By construction, each of these points satisfies the minimality condition of Lemma 5.7 (ii). Hence, each of these non-isomorphic points $z^{(1)}, z^{(2)}, \dots \in \mathbb{Z}^n_{(k)}$ is a core point. □

We proceed with the proof of Lemma 5.9, for which we need some auxiliary statements first. We begin with the symmetry of the projection matrix $P_V = (e^{(i)}|_V)_{i\in[n]} \in \mathbb{R}^{n\times n}$, which maps $\mathbb{R}^n$ onto an invariant subspace V. As the matrix of an orthogonal projection, it is easily seen to be symmetric.

Lemma 5.10. For the matrix P_V of an orthogonal projection to a linear subspace V it holds:

1. $\left\langle e^{(i)}|_V, e^{(j)} \right\rangle = \left\langle e^{(i)}|_V, e^{(j)}|_V \right\rangle$
2. The projection matrix $P_V = (e^{(i)}|_V)_{i\in[n]} \in \mathbb{R}^{n\times n}$ is symmetric.

Proof. Let $v^{(1)}, \dots, v^{(d)}$ be an orthonormal basis for V.

$$\begin{aligned}\left\langle e^{(i)}|_V, e^{(j)}|_V \right\rangle &= \left\langle \sum_{k=1}^{d} \left\langle e^{(i)}, v^{(k)} \right\rangle v^{(k)}, \sum_{l=1}^{d} \left\langle e^{(j)}, v^{(l)} \right\rangle v^{(l)} \right\rangle \\ &= \sum_{k=1}^{d} \left\langle e^{(i)}, v^{(k)} \right\rangle \left\langle e^{(j)}, v^{(k)} \right\rangle = \left\langle e^{(i)}|_V, e^{(j)} \right\rangle\end{aligned}$$

The symmetry in the second part follows from the symmetry of the scalar product in $\left\langle e^{(i)}|_V, e^{(j)} \right\rangle = \left\langle e^{(i)}|_V, e^{(j)}|_V \right\rangle = \left\langle e^{(j)}|_V, e^{(i)}|_V \right\rangle = \left\langle e^{(j)}|_V, e^{(i)} \right\rangle$. □

The main ingredient to prove Lemma 5.9 is Kronecker's Theorem, which is reproduced below as given in [Sch98, p. 80].

Theorem 5.11 (Kronecker's Theorem)**.** Let $A \in \mathbb{R}^{m\times n}$ and let $b \in \mathbb{R}^n$. Then the following two statements are equivalent:

1. for each $\varepsilon > 0$ there is an $x \in \mathbb{Z}^n$ with $\|Ax - b\| < \varepsilon$;
2. for each $y \in \mathbb{R}^m$ the implication $A^\top y \in \mathbb{Z}^n \;\Rightarrow\; b^\top y \in \mathbb{Z}$ is true.

Proof of Lemma 5.9. Using the projection matrix $P_V = (e^{(i)}|_V)_{i\in[n]} \in \mathbb{R}^{n\times n}$, our goal is to show that for every $\varepsilon > 0$ there exists a $z \in \mathbb{Z}^n_{(k)}$ with $\|z|_V\| = \|P_V z\| < \varepsilon$. Let $B \in \mathbb{R}^{n\times(n-1)}$ be the matrix whose columns consist of the vectors $b^{(i)} := e^{(i+1)} - e^{(i)}$ for $i \in [n-1]$. We can write every $z \in \mathbb{Z}^n_{(k)}$ as $z = ke^{(1)} + Bz'$ for a suitable $z' \in \mathbb{Z}^{n-1}$. Thus, we have to show that for every $\varepsilon > 0$ we find a $z' \in \mathbb{Z}^{n-1}$ such that

$$\|kP_V e^{(1)} + P_V B z'\| < \varepsilon. \tag{5.5}$$

Kronecker's Theorem states that this is equivalent to an implication concerning the integrality of $(P_V B)^\top y$ and $(P_V e^{(1)})^\top y$ for $y \in \mathbb{R}^n$. Using the symmetry of P_V from Lemma 5.10, we have to show that $B^\top y' \in \mathbb{Z}^n$ implies $(e^{(1)})^\top y' \in \mathbb{Z}$ where $y' := P_V y = y|_V$ is the projection of y onto V.

Let us assume that $B^\top y' \in \mathbb{Z}^n$ holds. We will show that this can only be the case for $y' = 0$, from which we immediately obtain that the implication required by Kronecker's

Theorem is satisfied. From $B^\top y' \in \mathbb{Z}^n$ we infer that for all $b^{(i)}$ we must have $\langle b^{(i)}, y' \rangle \in \mathbb{Z}$. Thus, we can write y' as $y' = \zeta\mathbb{1} + u$ for some $\zeta \in \mathbb{R}$ and an integral vector $u \in \mathbb{Z}^n$. Because as a projection y' lies in V, we know that $0 = \langle \mathbb{1}, y' \rangle = n\zeta + \langle \mathbb{1}, u \rangle$. This shows that ζ must be rational number. Hence, y' must be a rational vector. The only rational vector lying in the irrational invariant subspace V is the zero vector. Thus, Kronecker's Theorem shows that a solution of (5.5) exists, which is equivalent to the claim of Lemma 5.9. □

5.2.2. An example of core points for $\mathcal{C}_5$

Proposition 5.12. Let $f_1, f_2, f_3, \dots$ be the sequence of Fibonacci numbers. Then for every $j \in \mathbb{Z}_{>0}$ the point $z^{(j)} = (0, f_j, f_j, 0, f_{j+1})^\top \in \mathbb{Z}^5$ is a core point for the cyclic group $\mathcal{C}_5$ of order five.

In order to prove this proposition we will find an irrational invariant subspace $V \subset \mathbb{R}^n$ such that every $z^{(j)}$ has locally minimal projection. By Lemma 5.7 (ii) this proves that $z^{(j)}$ is a core point.

We start with the invariant subspace V. From Example 2.2 we know the invariant subspaces of the complex space $\mathbb{C}^n$. To get real invariant subspaces we combine a complex subspace and its complex conjugate, which must also be an invariant subspace because the permutation representation is real (cf. Section 5.5.1). The vector

$$u := (1, \zeta, \zeta^2, \overline{\zeta^2}, \overline{\zeta})^\top \tag{5.6}$$

with $\zeta := \exp(\frac{2\pi i}{5})$ is a basis for one complex invariant subspace of $\mathcal{C}_5$. The corresponding two-dimensional real invariant subspace V is spanned by the real vectors

$$v^{(1)} := \frac{u + \overline{u}}{2}, \quad v^{(2)} := \frac{u - \overline{u}}{2i}.$$

Their coordinates are given by $v^{(1)} = (1, c, c', c', c)^\top$ and $v^{(2)} = (0, s, s', -s', -s)^\top$ where

$$c := \cos\left(\frac{2\pi}{5}\right), \quad c' := \cos\left(\frac{4\pi}{5}\right), \quad s := \sin\left(\frac{2\pi}{5}\right), \quad s' := \sin\left(\frac{4\pi}{5}\right).$$

This implies that both $v^{(1)}$ and $v^{(2)}$ are orthogonal and have the same norm $\left\|v^{(1)}\right\|^2 = \left\|v^{(2)}\right\|^2 = \frac{5}{2}$. Next we show that $z^{(j)}$ has locally minimal projection with respect to V. It suffices to prove that $\left\|z^{(j)}|_V\right\|$ is minimal among all zero-based vectors $z \in \mathbb{Z}^5_{\geq 0}$ with $\langle \mathbb{1}, z \rangle \leq \langle \mathbb{1}, z^{(j)} \rangle = 2f_j + f_{j+1}$ (cf. Remark 5.3). Due to symmetry we may also assume w.l.o.g. that the first coordinate of z is zero. So let $z = (0, z_1, z_2, z_3, z_4) \in \mathbb{Z}^5_{\geq 0}$. Since $v^{(1)}$ and $v^{(2)}$ is an orthogonal basis, we obtain

$$\|z|_V\|^2 = \frac{2}{5}\left(\langle v^{(1)}, z \rangle^2 + \langle v^{(2)}, z \rangle^2\right).$$

Our goal is to minimize $\|z|_V\|$, so we may ignore the constant factor. It is enough to show that $z = z^{(j)}$ minimizes

$$\langle v^{(1)}, z \rangle^2 + \langle v^{(2)}, z \rangle^2 \tag{5.7}$$

under the constraints $\langle \mathbb{1}, z\rangle \leq 2f_j + f_{j+1}$ and $z = (0, z_1, z_2, z_3, z_4) \in \mathbb{Z}^5_{\geq 0}$. For this we need a little bit of theory about continued fractions. The following is taken from Sections 6 and 7 of Khinchin's book [Khi63]. Let $\alpha \in \mathbb{R}$ be a real number. We say that the fraction $\frac{p}{q} \in \mathbb{Q}$ is a **best approximation** of α if the following implication holds: If $\frac{a}{b} \neq \frac{p}{q}$ and $0 < b \leq q$, then

$$|b\alpha - a| > |q\alpha - p|.$$

This is sometimes also called a best approximation of the second kind. Regarding the quality of the approximation, we have the estimate

$$|q\alpha - p| < \frac{1}{q} \tag{5.8}$$

for a best approximation. Further, it can be shown that the ratio $\frac{f_{j+1}}{f_j}$ of consecutive Fibonacci numbers (as a so called convergent) is a best approximation for the golden ratio $\tau = \frac{1+\sqrt{5}}{2}$ if $j \geq 2$, meaning $f_{j+1} \geq 2$. We exploit this fact for the remaining proof of Proposition 5.12.

To simplify notation let $g_i(z) := \left\langle v^{(i)}, z\right\rangle^2$ for $i \in \{1, 2\}$. In order to expose the golden ratio in (5.7) we plug in the concrete coordinates and obtain

$$\begin{aligned} g_1(z) &= (c(z_2 + z_5) + c'(z_3 + z_4))^2, \\ g_2(z) &= (s(z_2 - z_5) + s'(z_3 - z_4))^2. \end{aligned}$$

Note that $\frac{c'}{c} = -(1 + \tau)$ and $\frac{s'}{s} = \tau - 1$. Thus,

$$g_1(z) = c^2(z_2 + z_5 - z_3 - z_4 - \tau(z_3 + z_4))^2 \tag{5.9}$$

$$g_2(z) = s^2(z_2 + z_4 - z_3 - z_5 + \tau(z_3 - z_4))^2. \tag{5.10}$$

We observe that the coordinates of $z^{(j)}$ are chosen in such a way that

$$\frac{1}{c^2} g_1(z^{(j)}) = \frac{1}{s^2} g_2(z^{(j)}) = (f_{j+1} - \tau f_j)^2.$$

Since the Fibonacci numbers are a best approximation for the golden ratio τ, we know by (5.8) that in particular

$$\frac{1}{c^2} g_1(z^{(j)}) < \frac{1}{f_j^2}. \tag{5.11}$$

If a point z has a smaller projection than $z^{(j)}$, then we must have $g_1(z) < g_1(z^{(j)})$ or $g_2(z) < g_2(z^{(j)})$.

For a contradiction, assume that $g_1(z) < g_1(z^{(j)})$. Then by the best approximation property we must have $z_3 + z_4 > f_j$; in particular $z_3 + z_4 \geq f_j + 1$. Since all coordinates of z are positive, this implies that $z_2 + z_5 \leq f_j + f_{j+1} - 1$. Thus,

$$z_2 + z_5 - z_3 - z_4 - \tau(z_3 + z_4) \leq f_{j+1} - \tau f_j - (2 + \tau) \leq \frac{1}{f_j} - (2 + \tau), \tag{5.12}$$

where we use (5.11) for the last estimate. Using this in (5.9) and again estimating via (5.11) shows that

$$\frac{1}{c^2} g_1(z) \geq \left(2 + \tau - \frac{1}{f_j}\right)^2 > 2 > \frac{1}{f_j^2} \geq \frac{1}{c^2} g_1(z^{(j)}). \tag{5.13}$$

This contradicts our initial assumption that $g_1(z)$ was better than $g_1(z^{(j)})$.

Now suppose that $g_2(z) < g_2(z^{(j)})$. Again by the best approximation property, we must have $|z_3 - z_4| > f_j$. Since all coordinates are non-negative, this implies $z_3 + z_4 > f_j$. As we have just seen, this leads to (5.13). Using this estimate, we obtain

$$g_1(z) + g_2(z) \geq g_1(z) > 2 = 2\left(c^2 + s^2\right) > \frac{c^2 + s^2}{f_j^2} > g_1(z^{(j)}) + g_2(z^{(j)}).$$

Thus, the projection of z cannot be smaller than the projection of $z^{(j)}$.

Altogether we have shown that for all zero-based z with $\langle \mathbb{1}, z\rangle \leq \left\langle \mathbb{1}, z^{(j)}\right\rangle$ it holds that $\|z|_V\| \geq \left\|z^{(j)}|_V\right\|$. This means $z^{(j)}$ has locally minimal projection with respect to V. Hence, $z^{(j)}$ is a core point, completing the proof of Proposition 5.12.

Remark 5.13. The core point $z^{(j)}$ lives in the layer with index $l_j := 2f_j + f_{j+1}$. The sequence $(l_j \bmod 5)_{j \in \mathbb{Z}_{>0}}$ traverses periodically all the non-zero residue classes 1,2,3 and 4. Thus, each layer $\mathbb{Z}^n_{(1)}, \mathbb{Z}^n_{(2)}, \mathbb{Z}^n_{(3)}, \mathbb{Z}^n_{(4)}$ contains infinitely many core points that are translates of a $z^{(j)}$.

Note that we have shown only that $z^{(j)}$ from Proposition 5.12 has locally minimal projection. There are also other points with locally minimal projection, for instance, $f_{j+1}\mathbb{1} - z^{(j)} = (f_{j+1}, f_{j-1}, f_{j-1}, f_{j+1}, 0)^\top$. Moreover, we find more non-isomorphic core points if we look at points with minimal projection onto the other two-dimensional real subspace W which is different from the V that we used. To easily find minima with respect to W we first go back to V. A point $z \in \mathbb{Z}^5$ has locally minimal projection onto V if and only if $\langle u, z\rangle^2$ is locally minimal with $u = (1, \zeta, \zeta^2, \overline{\zeta^2}, \overline{\zeta})^\top$ from (5.6). In other words, z induces a weighted sum of all roots of unity so that the total length is (locally) minimal (cf. Figure 5.2). Similarly, a point $z \in \mathbb{Z}^5$ has locally minimal projection onto W if and only if $\langle u', z\rangle^2$ is locally minimal with $u' := (1, \zeta^2, \overline{\zeta}, \zeta, \overline{\zeta^2})^\top$. Since the roots of unity are just arranged differently, we immediately conclude that

$$z'^{(j)} := (f_j, 0, 0, f_j, f_{j+1})^\top \in \mathbb{Z}^5$$

has locally minimal projection onto W and thus is a core point.

At the end of this section we look at the volume of the orbit polytopes. Since these live in a hyperplane, we consider the usual volume induced on the affine hull. We denote this volume by vol_d where d is the dimension of the affine hull. The following lemma shows that the volume of orbit polytopes of core points from this section is bounded. Although the diameter grows arbitrarily large, the volume does not. To formulate the statement we need the notion of a unimodular simplex. Let $\Lambda \in \mathbb{R}^n$ be an affine lattice and let $\{v^{(1)}, \ldots, v^{(m)}\} \subset \Lambda$ be the vertices of a simplex S. This lattice simplex S is called **unimodular** if $v^{(2)} - v^{(1)}, \ldots, v^{(m)} - v^{(1)}$ is a basis for the lattice $\Lambda - v^{(1)}$. In particular, a simplex is unimodular if it has the same volume as a unimodular simplex.

Lemma 5.14. Let $z^{(j)}$ as in Proposition 5.12. Its orbit polytope (for $\mathcal{C}_5$) is a unimodular simplex. For varying j these simplices have constant volume.

To prove this lemma we use so called circulant matrices. For a vector $z \in \mathbb{Z}^n$ let $\mathrm{circ}(z) \in \mathbb{Z}^{n\times n}$ be the matrix whose rows are $(1\,2\,\ldots\,n)^j z$ for $j \in \{0, \ldots, n-1\}$, cyclic shifts of z. This matrix is a **circulant matrix** and its eigenvalues (and eigenvectors) can be computed as follows.

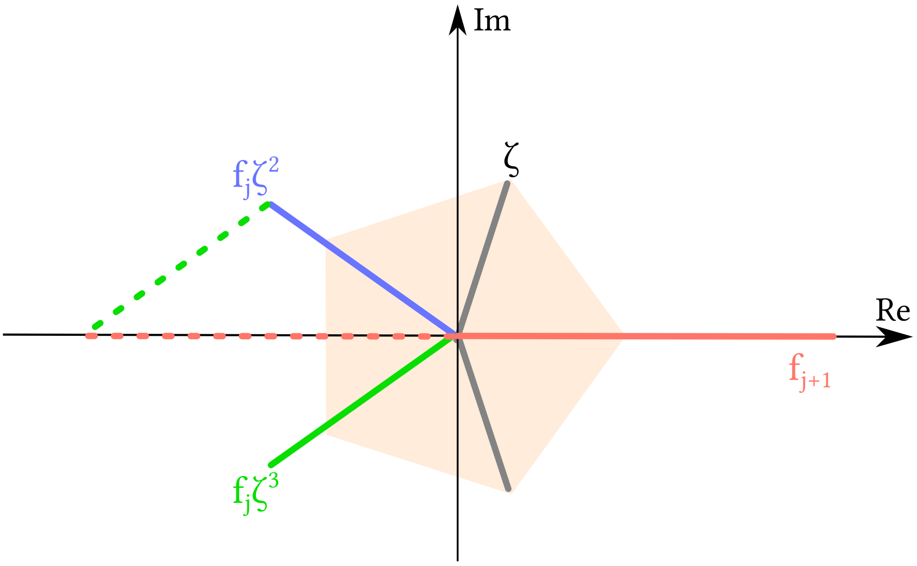


Figure 5.2.: Fibonacci numbers make a small weighted sum of fifth roots of unity

Theorem 5.15 (see [Dav79])**.** The eigenvalues of $\operatorname{circ}(z) \in \mathbb{R}^{n\times n}$ are

$$\mu_j = \mu_j(z) = \sum_{k=0}^{n-1} z_k \zeta^{kj}$$

for $j \in [n]$ where $\zeta := \exp(\frac{2\pi i}{n})$ is a root of unity. The corresponding eigenvectors are

$$v^{(j)} = v^{(j)}(z) = (1, \zeta^j, \zeta^{2j}, \dots, \zeta^{(n-1)j})^\top.$$

Proof of Lemma 5.14. To prove the lemma we show that the orbit simplex $T := \operatorname{conv} \mathcal{C}_5 z^{(j)}$, with vertices in the affine lattice $\left\langle \mathbb{1}, z^{(j)} \right\rangle e^{(1)} + \mathsf{A}_4$, has the same volume as the standard simplex $S := \operatorname{conv}\{e^{(1)}, \dots, e^{(5)}\}$, with vertices in $e^{(1)} + \mathsf{A}_4$. Since S clearly is unimodular and the vertices of S and T lie in the same lattice (up to translation), this implies that T is unimodular. To compute the volumes we observe that by the common volume formula for pyramids

$$\frac{1}{5!} \det \operatorname{circ}(z) = \operatorname{vol}_5 \operatorname{conv}\left(\{0\} \cup \mathcal{C}_5 z\right) = \frac{1}{5} \left\langle \frac{\mathbb{1}}{\|\mathbb{1}\|}, z \right\rangle \operatorname{vol}_4 \operatorname{conv}\left(\mathcal{C}_5 z\right). \tag{5.14}$$

Setting $z = e^{(1)}$ in (5.14) yields $\operatorname{vol}_4 S = \frac{\sqrt{5}}{24}$. To compute the volume of T we look at the determinant of $\operatorname{circ}(z)$. By Theorem 5.15 we have

$$\det \operatorname{circ}(z) = \prod_{j=1}^{5} \mu_j(z) = \langle \mathbb{1}, z \rangle \cdot \prod_{j=1}^{4} \mu_j(z). \tag{5.15}$$

Let $h(z) := \mu_1(z)\mu_2(z)\mu_3(z)\mu_4(z)$ be the product of eigenvalues without μ_5. Using this in (5.14), we obtain $\operatorname{vol}_4 \operatorname{conv}\left(\mathcal{C}_5 z\right) = \frac{\sqrt{5}}{24} h(z)$. As we are interested in the value of h for $z^{(j)} = (0, f_j, f_j, 0, f_{j+1})^\top$ from Proposition 5.12, we check (perhaps with a computer algebra system) that for $z = (0, a, a, 0, b)^\top$ it holds that

$$h\left((0, a, a, 0, b)^\top\right) = a^4 + 2a^3 b - a^2 b^2 - 2ab^3 + b^4 = (b^2 - ab - a^2)^2.$$

The term on the right equals 1 if (and only if for $a, b > 0$) we have $a = f_n$ and $b = f_{n+1}$ for some positive integer n (cf. [Ges72] and the proof by induction by [Jam09]). Thus,

$$\operatorname{vol}_4 T = \frac{\sqrt{5}}{24} h(z^{(j)}) = \frac{\sqrt{5}}{24} = \operatorname{vol}_4 S.$$

We conclude that T has the same volume as the unimodular simplex S and therefore also is unimodular. □

The proof is again quite ad-hoc but the statement is probably also true for other primitive cyclic groups and other orbit polytopes of core points with locally minimal projection. Remember that the eigenvectors $v^{(j)}$ are the (complex) invariant subspaces of the cyclic group $\mathcal{C}_n$. Thus, if $z^{(j)}$ has small projection onto a real subspace, then at least two of the eigenvalues $\sum_k z_k \zeta^{jk}$ in (5.15) have small length, which is getting smaller as j grows (cf. Figure 5.2). A few computational experiments suggest that this could be enough to compensate the growth in the orthogonal direction.

5.3. Rational subspaces: imprimitive groups

In this section we continue the construction of core points for transitive groups which are not 2-homogeneous, i.e., which have more than one invariant subspace besides $\operatorname{span} \mathbb{1}$. After the groups with irrational subspaces in the previous section, we now turn to a special case of groups with rational subspaces: the imprimitive groups.

5.3.1. Preliminaries

Let $G \leq \mathcal{S}_n$ be a transitive group. We call a subset $T \subseteq [n]$ a **block** for G if either $g(T) = T$ or $g(T) \cap T = \emptyset$ for all $g \in G$. A group is called **primitive** if every block has size 1 or n; it is **imprimitive** if there are blocks of other sizes. Given a block T, its orbit under G induces a partition of $[n]$. We call this partition a **block system** of size $|T|$. In the following we denote by S the size of the block system and by $B = \frac{n}{S}$ the number of blocks in a block system. Every such block system of an imprimitive group induces a rational invariant subspace of G in the following way. Let $[n] = \bigcup_{j=1}^{B} \Omega_j$ be a partition into blocks of size S each. Let

$$u^{(j)} := \sum_{i \in \Omega_j} e^{(i)} \in \mathbb{Z}^n \tag{5.16}$$

be the characteristic vector of Ω_j. Then the vectors $u^{(1)}, \ldots, u^{(B)}$ form an orthogonal basis of an G-invariant subspace of $\mathbb{R}^n$. We denote this B-dimensional subspace by $U_\Omega := \operatorname{span}\{u^{(1)}, \ldots, u^{(B)}\}$. Since $\mathbb{1} = \sum_{j=1}^{B} u^{(j)}$, we know that U_Ω contains $\operatorname{Fix}(G) = \operatorname{span} \mathbb{1}$. We can thus split U_Ω into a direct sum $U_\Omega = \operatorname{span} \mathbb{1} \oplus W_\Omega$ where W_Ω is another rational invariant subspace. Furthermore, there is an invariant subspace V_Ω which is the orthogonal complement of U_Ω in $\mathbb{R}^n$. In total we obtain for each block system Ω the following decomposition into invariant subspaces:

$$\mathbb{R}^n = \underbrace{\operatorname{span} \mathbb{1} \oplus W_\Omega}_{U_\Omega} \oplus V_\Omega. \tag{5.17}$$

Example 5.16. As an example we consider the cyclic group $\mathcal{C}_6 = \langle(1\,2\,3\,4\,5\,6)\rangle$. The group action of $\mathcal{C}_6$ is imprimitive as it preserves the partition $\Omega = \{\{1,3,5\},\{2,4,6\}\}$. The corresponding invariant subspace U_Ω is $\operatorname{span}\{(1,0,1,0,1,0)^\top,(0,1,0,1,0,1)^\top\}$. For its non-fixed summand we obtain $W_\Omega = \operatorname{span}(1,-1,1,-1,1,-1)^\top$.

The group $\mathcal{C}_6$ has another block system $\Omega' = \{\{1,4\},\{2,5\},\{3,6\}\}$. This corresponds to $U_{\Omega'} = \operatorname{span}\{(1,0,0,1,0,0)^\top,(0,1,0,0,1,0)^\top,(0,0,1,0,0,1)^\top\}$ and $W_{\Omega'} = \operatorname{span}\{(2,-1,-1,2,-1,-1)^\top,(-1,2,-1,-1,2,-1)^\top\}$. ■

Remark 5.17. It depends on the group whether the invariant subspaces V_Ω and W_Ω are irreducible. For instance, for cyclic groups of non prime order $n \geq 6$, the subspace W_Ω can be decomposed further since all irreducible invariant subspaces of cyclic groups have at most dimension two: Example 2.2 lists the complex invariant subspaces and Section 5.5.1 will show how these yield at most two-dimensional real invariant subspaces. On the other hand, for maximal imprimitive groups both invariant subspaces are irreducible (see Section 5.3.4).

5.3.2. A construction for infinite fundamental core sets

In this section we prove the following core point construction for imprimitive groups.

Theorem 5.18. Let $G \leq \mathcal{S}_n$ act imprimitively, i. e. the permutation action of G preserves a block system of size $1 < S < n$ each. If k is not a multiple of S, then the core set of G contains infinitely many non-isomorphic core points in layer $\mathbb{Z}^n_{(k)}$.

For the proof of this theorem we use the following specialization of Proposition 5.4. This specialization also is a result of the collaboration with Katrin Herr [Her13b, Cor 4.42]. Starting with a point with globally minimal projection onto some subspace, we grow a series of non-isomorphic core points in the direction of the complementary subspace. Figure 5.3 gives an idea how the corresponding orbit polytopes look like. It shows (an orthogonal projection of) the three-dimensional lattice-free orbit tetrahedra

$$\operatorname{conv}\mathcal{C}_4(1+m,-m,m,-m)^\top \subset \mathbb{Z}^4_{(1)}$$

for $m \in \{0,\ldots,5\}$ (see also Example 5.26).

Lemma 5.19. Let $G \leq \mathcal{S}_n$ be a permutation group and $\mathbb{R}^n = \operatorname{span}\mathbb{1} \oplus V \oplus W$ be a decomposition into invariant subspaces. Let $z^{(0)} \in \mathbb{Z}^n$ have globally minimal projection with respect to V. Moreover, let $z^{(0)}$ be a core point for $\operatorname{Stab}_G(z^{(0)}|_V)$. Let $w \in W \cap \mathbb{Z}^n$ such that $\operatorname{Stab}_G(z^{(0)}|_V) \leq \operatorname{Stab}_G(w)$. Then for all $m \in \mathbb{Z}$ the polytope $P_m := \operatorname{conv} G(z^{(0)} + mw)$ is lattice-free.

Proof. To prove that P_m is lattice-free we apply Proposition 5.4. Since $z^{(0)}$ has globally minimal projection onto V, so has $z^{(0)}+mw$. In particular, $z^{(0)}+mw$ thus also has locally minimal projection. It remains to show that $z^{(0)}+mw$ is a core point for $\operatorname{Stab}_G(z^{(0)}|_V)$. Because of the inclusion $\operatorname{Stab}_G(z^{(0)}|_V) \leq \operatorname{Stab}_G(w)$, we have that

$$P'_m := \operatorname{conv}\operatorname{Stab}_G(z^{(0)}|_V)(z^{(0)}+mw) = mw + \operatorname{conv}\operatorname{Stab}_G(z^{(0)}|_V)z^{(0)}.$$

Because $z^{(0)}$ is a core point for $\operatorname{Stab}_G(z^{(0)}|_V)$ by assumption of the corollary, this shows that the polytope P'_m is lattice-free. Hence, $z^{(0)}+mw$ is a core point for $\operatorname{Stab}_G(z^{(0)}|_V)$ and thus also for G by Proposition 5.4. □

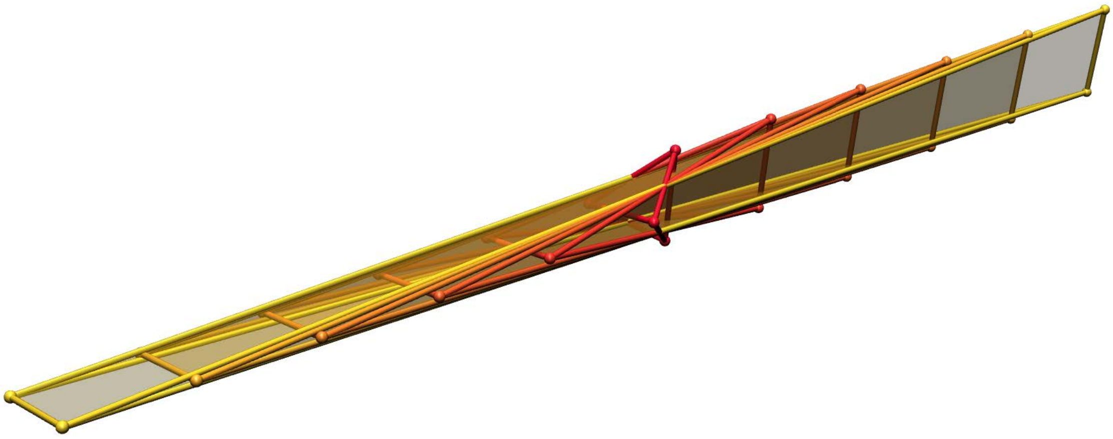


Figure 5.3.: Flat lattice-free orbit polytopes for $\mathcal{C}_4$, growing in one direction (inspired by [Her13b, Fig 4.8])

Note that, if the globally minimal projection $z^{(0)}|_V$ is zero, then the lemma becomes trivial since the stabilizer of the zero vector is the whole group. In order to prove Theorem 5.18 we show in two steps that the conditions of the previous lemma are satisfied for imprimitive groups. First, we find core points with globally minimal projection. Second, we find a non-zero direction in which the series of core points can grow. We begin with the minimal projections.

Lemma 5.20. Let $G \leq \mathcal{S}_n$ be an imprimitive group with a block system $\Omega = \{\Omega_1, \ldots, \Omega_B\}$ of size $1 < S < n$. Let $U_\Omega, V_\Omega, W_\Omega \subset \mathbb{R}^n$ be invariant subspaces as in (5.17). For $k \in [n]$, points with globally minimal projection are $z^{(k)} = \sum_{i \in I_k} e^{(i)}$

(i) with respect to W_Ω for every layer k with $B \nmid k$ and index set $I_k \subset [n]$ such that $|I_k \cap \Omega_b| \in \left\{\left\lfloor \frac{k}{B} \right\rfloor, \left\lceil \frac{k}{B} \right\rceil\right\}$ for all blocks $b \in [B]$;
in other words: the ones are distributed over all blocks as evenly as possible;

(ii) with respect to V_Ω for every layer k with $S \nmid k$ and index set $I_k \subset [n]$ such that $|I_k \cap \Omega_b| = S$ for $b \in J$ and $|I_k \cap \Omega_{b'}| \equiv k \pmod S$ for another block $b' \notin J$ where J is an arbitrary $\left\lfloor \frac{k}{S} \right\rfloor$-subset of $[B]$;
in other words: the ones are concentrated in as few blocks as possible.

For the subspace for which its projection is minimal, the projection of $z^{(k)}$ is not the zero vector.

Proof. These minima immediately follow from formulas for the respective projections. For this we use that U_Ω has a nice orthogonal basis with vectors $u^{(j)}$ of length $\left\|u^{(i)}\right\| = \sqrt{S}$ each. For a $z \in \mathbb{Z}^n$ we compute the projection onto W_Ω as

$$\|z|_{W_\Omega}\|^2 + \frac{1}{n}\langle \mathbb{1}, z\rangle^2 = \|z|_{U_\Omega}\|^2 = \frac{1}{S}\sum_{b=1}^{B}\left\langle z, u^{(i)}\right\rangle^2 = \frac{1}{S}\sum_{b=1}^{B}\left(\sum_{j\in\Omega_b} z_j\right)^2. \tag{5.18}$$

Remember that we want to minimize this expression for fixed layer index $\langle \mathbb{1}, z\rangle = \sum_{b=1}^{B}\sum_{j\in\Omega_b} z_j$. Under this condition the right-hand side expression in (5.18) is obviously minimized if the sums $\left(\sum_{j\in\Omega_b} z_j\right)^2$ have equal value. If $B \nmid k$, equality is not possible, but the minimum is still attained if the sums are as close to the arithmetic mean as possible. The point $z^{(k)}$ constructed in the lemma satisfies this condition and hence has globally minimal projection. It remains to show that the projection of $z^{(k)}$ onto W_Ω is non-zero if $B \nmid k$. Let $k = \alpha B + \beta$ with $\beta \in \{0, \dots, B-1\}$. Using (5.18), we compute

$$\begin{aligned} \left\| z^{(k)}|_{W_\Omega} \right\|^2 &= \frac{1}{S}\left(\beta(\alpha+1)^2 + (B-\beta)\alpha^2\right) - \frac{(\alpha B + \beta)^2}{n} \\ &= \frac{\beta(B-\beta)}{n} \end{aligned}$$

This shows that the projection is zero if and only if $\beta = 0$, i.e., k is a multiple of B. We now turn to the second part of the lemma and compute the projection onto V_Ω as

$$\begin{aligned} \|z|_{V_\Omega}\|^2 &= \|z\|^2 - \|z|_{U_\Omega}\|^2 \\ &= \left(\sum_{b=1}^{B}\sum_{j\in\Omega_b} z_j^2\right) - \left(\frac{1}{S}\sum_{b=1}^{B}\left(\sum_{j\in\Omega_b} z_j\right)^2\right) \\ &= \frac{1}{S}\sum_{b=1}^{B}\left(\sum_{\substack{i,j\in\Omega_b\\ i<j}} (z_i - z_j)^2\right). \end{aligned} \tag{5.19}$$

Looking at this sum of squares, we observe that the total expression is minimized if inside each block Ω_b the coordinates differ in the least possible way and the total number of blocks with non-zero contribution is minimized. The point $z^{(k)}$ constructed in the lemma satisfies this condition and hence has globally minimal projection. As a sum of squares, the projection can be zero if and only if k is a multiple of S. □

Remark 5.21. The minima $z^{(k)}$ constructed in the previous lemma are (universal) core points because they have only zeros and ones as coordinates.

Thus we have completed the first part on the way towards Theorem 5.18. It remains to find a direction in which to grow a series of core points.

Lemma 5.22. Let $G \leq \mathcal{S}_n$ be an imprimitive group with a block system $\Omega = \{\Omega_1, \dots, \Omega_B\}$ of size $1 < S < n$. Let $U_\Omega, V_\Omega, W_\Omega \subset \mathbb{R}^n$ be invariant subspaces as in (5.17). For the points $z^{(k)}$ from Lemma 5.20 (ii) with globally minimal projection onto V_Ω there is a non-zero direction $w \in W_\Omega \cap \mathbb{Z}^n$ such that $\mathrm{Stab}_G(z^{(k)}|_{V_\Omega}) \leq \mathrm{Stab}_G(w)$.

Proof. We first compute the projection $z^{(k)}|_{V_\Omega}$. For this we observe that all blocks indexed by $b \in J$ vanish under the projection since $\sum_{i\in\Omega_b} e^{(i)} = u^{(b)} \in U_\Omega = V_\Omega^\perp$. Let $I := I_k \cap \Omega_{b'}$ be the set of remaining indices. The sought projection is

$$\begin{aligned} z^{(k)}|_{V_\Omega} = z^{(k)} - z^{(k)}|_{U_\Omega} &= \left(\sum_{i\in I} e^{(i)}\right) - \frac{1}{S}\left\langle z^{(k)}, u^{(b')}\right\rangle u^{(b')} \\ &= \sum_{i\in I}\left(1 - \frac{k \bmod S}{S}\right) e^{(i)} - \sum_{i\in\Omega_{b'}\setminus I} \frac{k \bmod S}{S} e^{(i)}. \end{aligned} \tag{5.20}$$

As a direction w we choose the projection of $u^{(b')}$ onto W_Ω, which is $u^{(b')}|_{W_\Omega} = u^{(b')} - \frac{S}{n}\mathbb{1}$. After scaling, this is a non-zero integer vector w with stabilizer $\operatorname{Stab}_G(w) = \operatorname{Stab}_G(\Omega_{b'})$. Looking again at (5.20), we observe that $z^{(k)}|_{V_\Omega}$ has a zero at coordinate i if and only if i is not in $\Omega_{b'}$. Thus, the stabilizer of $z^{(k)}|_{V_\Omega}$ must be a subgroup of $\operatorname{Stab}_G([n] \setminus \Omega_{b'}) = \operatorname{Stab}_G(\Omega_{b'}) = \operatorname{Stab}_G(w)$. This shows that w is a non-zero direction satisfying the stabilizer condition. □

This enables us to proof the main theorem of this section by plugging all lemmas together.

Proof of Theorem 5.18. The proof of this theorem follows is based on the construction in Lemma 5.19. By Lemma 5.20 (ii) there exists a core point $z^{(k)}$ in the claimed layers with globally minimal projection onto V_Ω. Lemma 5.22 produces a non-zero direction $w \in W_\Omega \cap \mathbb{Z}^n$ such that $\operatorname{Stab}_G(z^{(k)}|_{V_\Omega}) \leq \operatorname{Stab}_G(w)$. Therefore, for every $m \in \mathbb{Z}$ the point $z^{(k)} + mw$ is a core point by Lemma 5.19. Since w is not the zero vector, these core points are non-isomorphic for different parameter value m. □

Remark 5.23. Note that many points minimize the projection (5.20). Using these points in Lemma 5.19 may lead to non-isomorphic series of core points which are different from those constructed in Theorem 5.18.

Example 5.24. We continue Example 5.16 and construct core points for the cyclic group $\mathcal{C}_6$. We begin with the block system $\Omega = \{\{1,3,5\},\{2,4,6\}\}$. We thus have $B = 2$ and size $S = 3$. Hence, we can expect infinite core sets in the layers with indices 1, 2, 4 and 5 because these are not multiples of S. The layer minima $z^{(k)}$ from Lemma 5.20 (ii) are given by

$$\begin{aligned} z^{(1)} &= (1,0,0,0,0,0)^\top, \\ z^{(2)} &= (1,0,1,0,0,0)^\top, \\ z^{(4)} &= (1,1,0,1,0,1)^\top, \\ z^{(5)} &= (1,1,1,1,0,1)^\top. \end{aligned}$$

The corresponding direction is $w = (1,-1,1,-1,1,-1)^\top$ from Example 5.16. Lemma 5.19 implies that for every $m \in \mathbb{Z}$ the simplex $\operatorname{conv} \mathcal{C}_6(z^{(k)} + mw)$ is lattice-free. In the case $k = 1$, for every $m \in \mathbb{Z}$ the simplex given by the orbit of

$$z^{(1)} + mw = (1+m, -m, m, -m, m, -m)^\top \in \mathbb{Z}^n_{(1)} \tag{5.21}$$

is lattice-free. Note that for the layer with index 3 this construction did not produce an infinite series of simplices. But we can find such a series by looking at the other invariant block system of $\mathcal{C}_6$, which is $\Omega' = \{\{1,4\},\{2,5\},\{3,6\}\}$ with size $S = 2$. Using this, we find infinite core sets in the layers 1, 3 and 5 by Theorem 5.18. The corresponding layer minima are

$$\begin{aligned} z^{(1)} &= (1,0,0,0,0,0)^\top, \\ z^{(3)} &= (1,1,0,0,1,0)^\top, \\ z^{(5)} &= (1,1,1,0,1,1)^\top. \end{aligned}$$

As direction w we choose a multiple of $u'^{(1)}|_{W_{\Omega'}} = \frac{1}{3}(2, -1, -1, 2, -1, -1)^\top$ such that the vector is integral. In the case $k = 3$, for instance, the simplex given by the orbit of

$$z^{(3)} + mw^{(1)} = (1 + 2m,\, 1 - m,\, -m,\, 2m,\, 1 - m,\, -m)^\top \in \mathbb{Z}^n_{(3)} \tag{5.22}$$

is lattice-free for every $m \in \mathbb{Z}$. An alternative choice for $z^{(3)}$ could be $(1, 0, 0, 1, 0, 1)$ (cf. Remark 5.23), leading to the series of core points

$$(1 + 2m,\, -m,\, -m,\, 1 + 2m,\, -m,\, 1 - m)^\top \in \mathbb{Z}^n_{(3)} \tag{5.23}$$

for $m \in \mathbb{Z}$. No core point in (5.23) is isomorphic to a core point from (5.22). To see this we observe that in (5.23) two consecutive coordinates have the same value $-m$; this does not happen in (5.22). Besides these constructions, there are entirely different ones that yield infinite series for $\mathcal{C}_6$. We will look at those in the next section (see, for instance, Example 5.29). ■

Remark 5.25. As for the "Fibonacci" simplices from Section 5.2.2 one can look at the volume of the symmetric simplices from the previous example. A computation similar to the proof of Lemma 5.14 – using eigenvalues of circulant matrices – shows that, for instance, the volume of the orbit polytope of (5.21) cannot be bounded for growing m because the eigenvalue μ_3 corresponding to the eigenvector $v^{(3)} = w$ tends to infinity whereas all other eigenvalues are one. Therefore, (at least some) orbit polytopes of imprimitive cyclic groups are symmetric siblings of Reeve's famous lattice-free simplices with unbounded volume [Ree57].

In the following two sections we discuss the limits of core point construction based on Proposition 5.4 and its specialization Lemma 5.19. In particular the latter has served its purpose well since it describes core point series for all imprimitive groups. Swapping the roles V and W, i.e., using $V = W_\Omega$ and $W = V_\Omega$ has some interesting consequences. We look at two different, in some sense extremal groups: cyclic groups, which are among the smallest imprimitive groups, and maximal imprimitive groups.

5.3.3. Small imprimitive groups: cyclic groups

In this section we construct core points which cannot be obtained by the previous construction based on Lemma 5.19. In particular for cyclic groups there are much more core points than those from Theorem 5.18.

Example 5.26. As an example we consider the cyclic group $\mathcal{C}_4 = \langle(1\,2\,3\,4)\rangle$. Given the block system $\Omega = \{\{1, 3\}, \{2, 4\}\}$, the corresponding invariant subspaces are $W_\Omega = \operatorname{span} w$ and $V_\Omega = \operatorname{span}\{v, v'\}$ with $w := (1, -1, 1, -1)^\top$, $v := (1, 0, -1, 0)^\top$ and $v' := (0, 1, 0, -1)^\top$. By Lemma 5.20 the point $e^{(1)} = (1, 0, 0, 0)^\top$ is a core point for $\mathcal{C}_4$ with globally minimal projection on V_Ω. We compute $e^{(1)}|_{V_\Omega} = \frac{1}{2}v$, hence the stabilizer $\operatorname{Stab}_{\mathcal{C}_4}(e^{(1)}|_{V_\Omega})$ is trivial. Therefore we may choose any integer direction from W_Ω. As these are all multiples of w, this yields only one series of core points, $e^{(1)} + mw = (1 + m, -m, m, -m)^\top$.

If we swap the roles of V_Ω and W_Ω for Lemma 5.19, we still know that $e^{(1)}$ has globally minimal projection on W_Ω (again by Lemma 5.20). Its projection is $e^{(1)}|_{W_\Omega} = \frac{1}{4}w$ and it has stabilizer $H := \mathrm{Stab}_{\mathcal{C}_4}(e^{(1)}|_{W_\Omega}) = \langle (1\,3)(2\,4) \rangle$. Since all non-zero elements from V_Ω have trivial stabilizer, we cannot find a suitable integer direction in V_Ω that is compatible with the stabilizer condition of Lemma 5.19.

However, we may also work with Proposition 5.4 directly. Let $av+bv'$ with $a, b \in \mathbb{Z}$ be an arbitrary integer direction in V. By Proposition 5.4, the point $p(a,b) := e^{(1)}+av+bv'$ is a core point for $\mathcal{C}_4$ if and only if it is a core point for $H = \langle (1\,3)(2\,4) \rangle$. The orbit polytope $\mathrm{conv}\, Hp(a,b)$ has only two vertices,

$$\begin{aligned} u &:= (1+a,\ b,\ -a,\ -b)^\top, \quad \text{and} \\ u' &:= (-a,\ -b,\ 1+a,\ b)^\top. \end{aligned}$$

We consider a proper convex combination $\lambda u + (1-\lambda)u'$ on the line segment between u and u' with $0 < \lambda < 1$. Looking at the first coordinate, we observe that $(2a+1)\lambda$ must be an integer. Looking at the second coordinate, we similarly obtain that $2b\lambda$ must be an integer. If $b = 0$, the second condition is automatically fulfilled and the first condition is satisfiable if $a \notin \{-1, 0\}$. We have therefore proven: $p(a,b)$ is a core point for $\mathcal{C}_4$ if and only if $\gcd(2a+1, 2b) = 1$ (with our convention $\gcd(x, 0) = |x|$). ■

Remark 5.27. It is unclear whether $\mathcal{C}_4$ has more core points than those described in Example 5.26. Perhaps one can use White's Theorem [Whi64] – every lattice-free tetrahedron has lattice width one – to show that the list is complete, at least regarding the "infinite" part. If a three-dimensional lattice-free $\mathcal{C}_4$-orbit simplex has lattice width one, then either the width is attained in the direction of an invariant subspace or the whole simplex must be flat in some sense. Another possible proof strategy is computing bounds as explained in Remark 3.14 and then performing an exhaustive search for points with minimal projections.

The previous example highlights two things. First, setting $V = W_\Omega$ and $W = V_\Omega$ in Lemma 5.19 may lead to an unsatisfiable stabilizer condition. Second, the more general construction Proposition 5.4 actually yields more core points, at least for $\mathcal{C}_4$. In general it is hard to find a characterization for when the combination of all possible basis vectors from V_Ω yields core points (referring to the condition $\gcd(2a+1, 2b) = 1$ above). The following proposition therefore aims rather at a generalization of a special case of this construction.

Proposition 5.28. Let $G \leq \mathcal{S}_n$ be an imprimitive group with block system $\Omega = \{\Omega_1, \dots, \Omega_B\}$. For an integer $k \in [B-1]$ let $i_1 \in \Omega_1, \dots, i_k \in \Omega_k$ be arbitrary elements from the first k blocks and let $I := \{i_1, \dots, i_k\}$ denote the set of those. Let $v \in V_\Omega \cap \mathbb{Z}^n$ such that

- $v_i = 0$ for all $i \in \bigcup_{i=1}^k \Omega_i$, i.e., for all indices from the first k blocks, and
- $\mathrm{Stab}_G(I) \leq \mathrm{Stab}_G(v)$, i.e., constant on the orbits of $\mathrm{Stab}_G(I)$.

Then $z := v + \sum_{i \in I} e^{(i)} \in \mathbb{Z}^n_{(k)}$ is a core point for G.

Proof. We first observe that $\sum_{i \in I} e^{(i)}$ has globally minimal projection onto W_Ω by Lemma 5.20 (i). Therefore also z has globally minimal projection onto W_Ω. By Proposition 5.4 it suffices to show that z is a core point for $\mathrm{Stab}_G(z|_{W_\Omega})$. Let $\Omega_I := \bigcup_{i=1}^k \Omega_i$ denote the union of the first k blocks. We compute that $z|_{W_\Omega}$ is some multiple of

$\left(\sum_{i=1}^{k} u^{(i)}\right) - \frac{k}{n}\mathbb{1}$. Hence, the stabilizer $H := \mathrm{Stab}_G(\Omega_I)$ also is the stabilizer of $z|_{W_\Omega}$. It is therefore enough to show that z is a core point for H.

We further observe that $\mathrm{Stab}_G(I)$ is a subgroup of H because a permutation $g \in G$ with $g(i_a) = i_b$ also maps the whole blocks $g(\Omega_a) = \Omega_b$. We can therefore decompose H into cosets modulo $\mathrm{Stab}_G(I)$. Let $T = \{g_1, \dots, g_l\}$ be a transversal, i.e., $H = \bigcup_{g \in T} g \,\mathrm{Stab}_G(I)$. By construction of z in the proposition, we know that $\mathrm{Stab}_G(I) \leq \mathrm{Stab}_G(z)$. Hence, the orbit $\mathrm{Stab}_G(I)z$ consists only of a single point. This implies for the whole orbit that $Hz = \bigcup_{g \in T} gz$. In order to see that z is a core point for H, we look at the coordinates indexed by Ω_I. For two distinct permutations $g, g' \in T$ we know that gz and $g'z$ differ in these coordinates. On the other hand, all these coordinates are either zero or one. Thus, all convex combinations in $Hz = \bigcup_{g \in T} gz$ which yield an integral point must be trivial convex combinations. This shows that z is a core point for H, thus also for G. □

A few remarks help to clarify the rather technical previous proposition. First, there is no need to restrict the construction to the first k blocks. This was done to simplify notation, and any k blocks would do as well. Second, the requirement that $v \in V_\Omega \cap \mathbb{Z}^n$ is zero on some blocks is easy to satisfy. Since V_Ω consists of all vectors x for which the sum $\sum_{j \in \Omega_b} x_j = 0$ is zero for all blocks $b \in [B]$, being all zero on one block is independent of all the other blocks. The requirement which may be a real obstacle for constructions is (again) the stabilizer condition. There are groups for which no vector v with suitable stabilizer can be found (cf. Section 5.3.4). However, for small groups this construction yields core points as the following example shows.

Example 5.29. Let $G = \mathcal{C}_{2m} = \langle (1\,2\,\dots\,2m) \rangle$ be a cyclic group of even order, $m \geq 2$. Then G has at least two block systems, $\Omega = \{\{1, 3, \dots, 2m-1\}, \{2, 4, \dots, 2m\}\}$ and $\Omega' = \{\{1, m+1\}, \{2, m+2\}, \dots, \{m, 2m\}\}$. For this example we use $k = 1$ and $i_1 = 1$ in Proposition 5.28. Since $\mathrm{Stab}_G(I) = \mathrm{Stab}_G(1)$ is the trivial group, the second condition of this proposition is automatically satisfied. Therefore any integral vector from V_Ω that is constant on Ω_1 can be used. For integer parameters $a_1, \dots, a_{m-1} \in \mathbb{Z}$ we obtain

$$\left(1, a_1, 0, a_2, 0, a_3, \dots, 0, a_{m-1}, 0, -\sum_{i=1}^{m-1} a_i\right)^\top, \tag{5.24}$$

$$(1, a_1, a_2, \dots, a_{m-1}, 0, -a_1, -a_2, \dots, -a_{m-1})^\top \tag{5.25}$$

as series of core points for G based on Ω and Ω', respectively. ■

Remark 5.30. The previous example shows that Proposition 5.28 contains [HRS13, Example 10] and [Her13b, Thm 4.51] as special cases. In addition, the section [Her13b, Sec 4.5.2] contains nice geometric interpretations of the corresponding orbit polytopes.

5.3.4. Maximal imprimitive groups: wreath products of symmetric groups

In this section we will see that Theorem 5.18 is fairly sharp in the sense that there are groups for which almost all core points come from this very construction (see Remark 5.32). In particular, all core points of these groups lie close to V_Ω. The groups that we look at are maximal imprimitive groups. For their characterization we need a bit more group theory.

The following definition is based on Wilson's book [Wil09, Sec 2.2.6] where a more abstract setting is used that we do not require here. Let $G \leq \mathcal{S}_l$ and $H \leq \mathcal{S}_m$ be two permutation groups. Moreover, let $G^m := \bigtimes_{i=1}^m G$ be the m-fold direct product of G. The **wreath product** $G \wr H$ of the groups G and H consists of all pairs (g, h) where $g = (g_1, \ldots, g_m) \in G^m$ and $h \in H$. The product of two group elements is defined as

$$(g', h')(g, h) = (\phi(h, g')g,\ h'h)$$

where $\phi : H \times G^m \to G^m$ defines an H-action on G^m via

$$\phi(h,\ (g_1, \ldots, g_m)) = (g_{h(1)}, \ldots, g_{h(m)}).$$

The wreath product acts on the Cartesian product $S := [l] \times [m]$ by

$$(g, h)(x, y) = (g_y(x), h(y)) \quad \text{for } (x, y) \in S.$$

If we canonically identify S with the set $[l \cdot m]$, the wreath product is a transitive group with degree lm and order $|G|^m\,|H|$. In this setting, $G \wr H$ is an imprimitive group whose $B = m$ blocks of size $S = l$ correspond to the "fibers" $\{(x, y) : x \in [l]\}$ (see [Cam99, Sec 1.10] for a figure of the fiber interpretation). It can be shown that the maximal imprimitive subgroups of $\mathcal{S}_n$ are the wreath products $\mathcal{S}_l \wr \mathcal{S}_m$ for $n = lm$ with $l, m \geq 2$ (see [Wil09, Sec 2.5.2]). That means, every imprimitive group is a subgroup of such a wreath product of symmetric groups. In fact, a more concise embedding theorem holds (see [Cam99, Thm 1.8]), which we do not require here.

From the definition of the wreath product it follows immediately that $G \wr H$ contains the direct product G^m as a subgroup (by choosing h in (g, h) to be the identity in H). By the elementary core set properties this yields the following bound on core sets (cf. Remark 3.4 (iii)).

Remark 5.31. The core set of the wreath product $G \wr H$ is contained in the core set of the direct product: $\operatorname{core}(G \wr H) \subseteq \operatorname{core}(G^m)$ where m is the degree of H.

In particular for symmetric groups, this shows that all core points of $\mathcal{S}_l \wr \mathcal{S}_m$ lie in $\bigtimes_{j=1}^m \operatorname{core}(\mathcal{S}_l)$, i.e., they are all of the form

$$\bigoplus_{j=1}^{m} \left(\beta_j \mathbb{1}_l + c^{(j)}\right) \tag{5.26}$$

for some integers $\beta_j \in \mathbb{Z}$ and universal core points $c^{(j)} \in \{0, 1\}^l$ (cf. Remark 3.33 and 3.34).

Remark 5.32. Note that the projection of (5.26) onto V_Ω is $\bigoplus_{j=1}^m c^{(j)}|_{V_\Omega}$. This shows that for all core points $z \in \operatorname{core}(\mathcal{S}_l \wr \mathcal{S}_m)$ the length of the projection $\|z|_{V_\Omega}\|$ is bounded by a global constant $C(l, m) \leq \|\mathbb{1}_n\|$ depending only on l and m. From Theorem 3.13 we only know that core points have a small projection onto at least one invariant subspace. For the product $\mathcal{S}_l \wr \mathcal{S}_m$ only finitely many elements of a fundamental core set have a small projection onto W_Ω. Therefore, almost all core points lie close to W_Ω (see Figure 5.4).

This also means that the construction behind Theorem 5.18 is sharp in the following sense. For the product $\mathcal{S}_l \wr \mathcal{S}_m$ all core points (except universal core points) are described by this construction based on Lemmas 5.19, 5.20 and 5.22. Swapping the roles of V_Ω and W_Ω in this construction is in general not possible as it depends on the group whether there are core points close to V_Ω (see Figure 5.4). ■

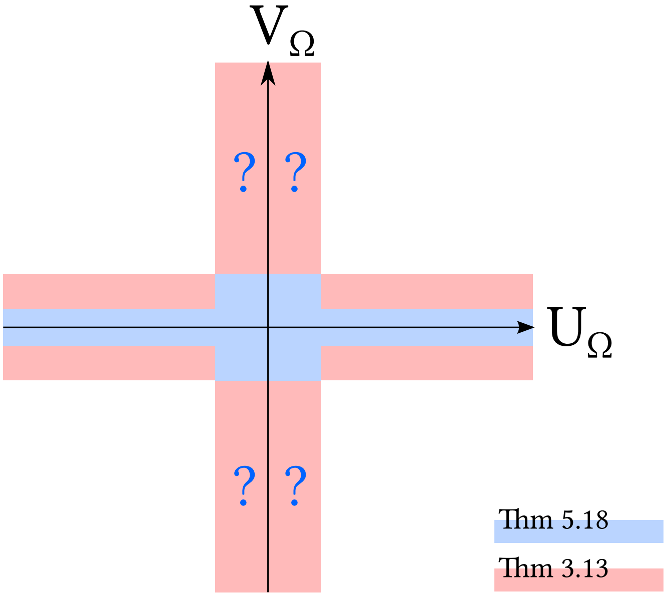


Figure 5.4.: For maximal imprimitive groups core points can only be found close to U_Ω

Besides this "upper bound" on the core set of $\mathcal{S}_l \wr \mathcal{S}_m$, we also have a "lower bound" because we constructed core points for imprimitive groups in Theorem 5.18. This construction yields core points which are also of the form (5.26). Because we need a minimal projection, for these at most one point $c^{(j)}$ is non-zero (cf. Lemma 5.20 (ii)). If we denote the set of core points from Theorem 5.18 (plus all universal core points, which are not mentioned in the theorem) by $C_{\text{imprimitive}}(G)$, then we have the relation

$$C_{\text{imprimitive}}(\mathcal{S}_l \wr \mathcal{S}_m) \subseteq \operatorname{core}(\mathcal{S}_l \wr \mathcal{S}_m) \subseteq \operatorname{core}\left((\mathcal{S}_l)^m\right) \tag{5.27}$$

It is not obvious how exactly the core set $\operatorname{core}(\mathcal{S}_l \wr \mathcal{S}_m)$ can be characterized. We close this section by showing that the right most inclusion in (5.27) is always strict, i.e., there are always core points of the direct product which are not core points for the wreath product. To see this we note that every core point of the form (5.26) can essentially be described by two tuples $\alpha \in \{0, 1, \ldots, l-1\}^m$ and $\beta \in \mathbb{Z}^m$ as

$$\bigoplus_{j=1}^{m} \left(\beta_j \mathbb{1}_l + \sum_{i=1}^{\alpha_j} e^{(i)} \right) . \tag{5.28}$$

Due to symmetry every point from (5.26) lies in an orbit of a point from (5.28); the value α_j equals the number of ones in $c^{(j)}$. With this parametrization we formulate a difference between the core sets of wreath and direct product.

Lemma 5.33. Let $z := \bigoplus_{j=1}^{m} \left(\beta_j \mathbb{1}_l + \sum_{i=1}^{\alpha_j} e^{(i)}\right)$ be a core point for $(\mathcal{S}_l)^m$. This point z is not a core point for the wreath product $\mathcal{S}_l \wr \mathcal{S}_m$ if there are two distinct indices i, j with $\alpha_i = \alpha_j$ and $|\beta_i - \beta_j| \geq 2$.

Proof. Let $(g, h) \in \mathcal{S}_l \wr \mathcal{S}_m$ be a permutation where g is the identity in $(\mathcal{S}_l)^m$ and $h = (i\, j) \in \mathcal{S}_m$ is a transposition. That means it swaps the blocks i and j and does not change anything else. Let $x := (g, h)z - z$ be the difference between two vertices of the orbit polytope. Then the i-th and j-th block of x are given by

$$(x)_i = (\beta_j - \beta_i)\mathbb{1}_l \quad \text{and} \quad (x)_j = (\beta_i - \beta_j)\mathbb{1}_l;$$

all other blocks of x are zero. Thus, the greatest common divisor of all coordinates is $\gcd(x_1, \ldots, x_{lm}) = |\beta_j - \beta_i|$. By Lemma 3.30 the point z is not a core point if $|\beta_j - \beta_i| > 1$. □

Example 5.34 (Fundamental core set of D_8)**.** As an example we consider the (dihedral) group $D_8 = \mathcal{S}_2 \wr \mathcal{S}_2 = \langle (1\,2), (3\,4), (1\,3)(2\,4) \rangle$ of order eight. We first look at the lower bound that comes from Theorem 5.18. Up to D_8-symmetry and using zero-based core points, this yields

$$\begin{aligned} \operatorname{fcore}(D_8) \supseteq &\left\{ (\alpha, 0, \alpha' + \beta, \beta)^\top \ : \ \alpha, \alpha' \in \{0,1\} \text{ with } \alpha + \alpha' = 1 \text{ and } \beta \in \mathbb{Z}_{\geq 0} \right\} \\ &\cup \left\{ (1,0,1,0)^\top, (0,0,1,1)^\top, (0,0,0,0)^\top \right\}. \end{aligned} \tag{5.29}$$

The first part comes immediately from the theorem, the second part adds three missing universal core point. Similarly eliminating D_8-symmetry and using zero-based points, the upper bound results in

$$\operatorname{fcore}(D_8) \subseteq \left\{ (\alpha, 0, \alpha' + \beta, \beta)^\top \ : \ \alpha, \alpha' \in \{0,1\} \text{ and } \beta \in \mathbb{Z}_{\geq 0} \right\}. \tag{5.30}$$

In order to get $\operatorname{fcore}(D_8)$ we thus have to decide whether $z^{(\beta)} := (1, 0, 1 + \beta, \beta)^\top$ is a core point for $\beta \geq 1$ and whether $z'^{(\beta)} := (0, 0, \beta, \beta)^\top$ is a core point for $\beta \geq 2$. By Lemma 3.29 the point $z^{(\beta)}$ is a core point if and only if $\beta = 0$. Lemma 5.33 implies that $z'^{(\beta)}$ is a core point if and only if $\beta \in \{0, 1\}$. Therefore we must in fact have equality in (5.29), which thus completely describes the core set of D_8.

Note that Lemma 5.33 also shows that $z^{(\beta)}$ cannot be a core point if $\beta \geq 2$, but does not claim anything in the case $\beta = 1$. ■

5.4. Rational subspaces: primitive groups

In this section we discuss core point constructions for rational subspaces of primitive groups. This is the only missing case towards a proof of Conjecture 3.27, which states that the existence of more than two invariant subspaces implies infinite fundamental core sets.

The constructions for imprimitive groups in the previous section were quite easy to prove because we had a nice description of invariant subspaces. With an orthogonal basis of 0/1-vectors, globally minimal projections are easy to characterize. However, primitivity of a group implies that such an orthogonal $0/1$-basis does not exist. This makes a general analysis for all groups difficult and we will not see a proof that works for every primitive group with rational subspaces. Instead, we discuss two complementary strategies to tackle this problem. The first strategy is applying Lemma 5.19 to a globally minimal point. The second strategy is proving that every group has a subspace for which $e^{(1)}$ has globally minimal projection.

For the rational subspaces of imprimitive groups our core point construction is based on Lemma 5.19. Let $V \subseteq \mathbb{R}^n$ be a rational invariant subspace of G and let W such that $\mathbb{R}^n = \operatorname{span} \mathbb{1} \oplus V \oplus W$. To apply the lemma we need two things: a point z with non-zero, globally minimal projection onto V and a non-zero direction $w \in W$ with $\operatorname{Stab}_G(z|_V) \leq \operatorname{Stab}_G(w)$. The first requirement is easy to satisfy because for a rational subspace there always exist points with globally minimal projection. Not all of them are non-zero but we prove that there always exist a layer and a subspace with non-zero globally minimal projection as follows. Suppose that $z \in \mathbb{Z}^n_{(k)}$ and $z' \in \mathbb{Z}^n_{(l)}$ which are orthogonal to V and W, respectively. That is,

$$z|_V = 0 \quad \text{and} \quad z'|_W = 0. \tag{5.31}$$

We compute the scalar product between z and z' as

$$\langle z, z' \rangle = \left\langle z|_V + z|_W + \frac{k}{n}\mathbb{1},\ z'|_V + z'|_W + \frac{l}{n}\mathbb{1} \right\rangle = \frac{kl}{n}.$$

This value must be integer because z and z' are integral vectors. Thus, a necessary condition for (5.31) to happen is that the product kl of layer indices is a multiple of n. In particular, this shows that for the layer with index one there is at least one subspace which has non-zero globally minimal projection. The remaining obstacle is to find a suitable direction $w \in W$ for a minimum z. Without control of the minimum z and its projection, it is hard to argue why a matching direction should exist. As we have seen before, for instance, in Example 5.26, such a direction may not exist.

The second strategy uses a special point whose projection we can control well to overcome this obstacle. The catch is that it is unclear when it has globally minimal projection. Consider the first standard basis vector $e^{(1)}$. If $e^{(1)}$ has globally minimal projection, then we can prove the existence of infinitely many non-isomorphic core points as follows, using a characterization of primitive groups.

Theorem 5.35 (cf. Thm 1.7 [Cam99]). Let G be a permutation group and $H \leq G$ be a point stabilizer. Then G is primitive if and only if H is a maximal subgroup.

Corollary 5.36. Let G be a primitive group and let V be a rational invariant subspace. It holds that $\operatorname{Stab}_G(e^{(1)}) = \operatorname{Stab}_G(e^{(1)}|_V)$.

Proof. First, note that G is transitive because it is primitive. Therefore, the projection $e^{(1)}|_V$ cannot be zero because its orbit spans V. This shows that the stabilizer $\operatorname{Stab}_G(e^{(1)}|_V) \lneq G$ is a proper subgroup of G. By Lemma 5.2 we know that the stabilizer of $e^{(1)}$ is contained in the stabilizer of its projection. Since $\operatorname{Stab}_G(e^{(1)}) = \operatorname{Stab}_G(1)$ is a maximal subgroup of G by Theorem 5.35, we must have equality. □

Proposition 5.37. Let $G \leq \mathcal{S}_n$ be primitive and let $V \subset \mathbb{R}^n$ be a rational invariant subspace. If $e^{(1)}$ has globally minimal projection onto V, then there are infinitely many core points in layer one. The corresponding orbit polytopes are simplices.

Proof. We prove the existence of core points using Lemma 5.19. Let W be the invariant subspace that satisfies $\mathbb{R}^n = \operatorname{span} \mathbb{1} \oplus V \oplus W$. If $e^{(1)}$ has globally minimal projection, then $e^{(1)}|_V \neq 0$ and $e^{(1)}|_W \neq 0$ (cf. the proof of Corollary 5.36). Thus, a suitable multiple w of $e^{(1)}|_W$ is a non-zero integral vector. By Corollary 5.36 it holds that $\operatorname{Stab}_G(e^{(1)}) = \operatorname{Stab}_G(e^{(1)}|_V) = \operatorname{Stab}_G(e^{(1)}|_W) = \operatorname{Stab}_G(w)$. Hence, for every $m \in \mathbb{Z}$ the orbit polytope of $e^{(1)} + mw$ is a lattice-free simplex. Since these are non-isomorphic for different values of m, the claim of the lemma follows. □

To complete the proof of Conjecture 3.27 it would suffice to prove that every primitive group with only rational invariant subspaces always has at least one subspace such that $e^{(1)}$ has globally minimal projection. As we have seen in Lemma 5.20, this is true at least for imprimitive groups. Computational experiments suggest that this also holds for primitive groups. For all primitive groups of non-prime degree $n \leq 127$ the rational invariant subspaces were computed; details can be found in Section 5.5.1. With respect to these subspaces the global minima in layer $\mathbb{Z}^n_{(1)}$ were computed as outlined in Section 5.5.2. The experiments show that for all groups the vector $e^{(1)}$ is minimal for at least one invariant subspace. For most groups it is even minimal for all invariant subspaces. Thus, for all primitive groups with $n \leq 127$ the fundamental core set is infinite by Proposition 5.37. However, it remains unclear what condition is necessary to make $e^{(1)}$ a global minimum.

5.5. Computational aspects

5.5.1. Invariant subspaces

Up to now we have worked with invariant subspaces of a group on an existential base. If we are interested in the core points of a specific group, bases for invariant subspaces help to locate core points. To actually compute some or all invariant subspaces of a group, we have to dive a bit deeper into representation and character theory. The following elementary results can be found, for instance, in [JL01, Ser77]. In this section we focus on statements that help in obtaining invariant subspaces. We start with complex invariant subspaces and discuss real invariant subspaces, which we are interested in for our geometric application, afterwards.

Given a representation $\rho : G \to \mathrm{GL}_n(\mathbb{C})$, its character is a function $\chi_\rho : G \to \mathbb{C}$ defined as $\chi_\rho(g) = \operatorname{tr}(\rho(g))$; here tr denotes the trace of a quadratic matrix. A character is called **irreducible** if it is the character of an irreducible representation. As every representation can be decomposed into a direct sum of irreducible representations, so can its characters. Every character χ of G can be written as

$$\chi = m_1\chi_1 + \cdots + m_k\chi_k \tag{5.32}$$

where m_i are non-negative integers and χ_i are distinct irreducible characters of G. The numbers m_i are called **multiplicities**. If all irreducible characters of G are known, then the decomposition (5.32) can easily be computed since the $m_i = \frac{1}{|G|}\sum_{g\in G}\chi_i(g)\chi(g^{-})$ are the value of an inner product between χ_i and χ.

The decomposition of a character χ in (5.32) corresponds to the decomposition of a related representation ρ. Remember from Section 2.3 that subrepresentations naturally correspond to invariant subspaces, which we are interested in. We start with the decomposition of ρ and look at the implications for invariant subspaces afterwards. We can decompose ρ as

$$\rho = \rho_1^{(m_1)} \oplus \cdots \oplus \rho_k^{(m_k)}, \tag{5.33}$$

where each summand $\rho_i^{(m_i)}$ is isomorphic to a direct sum

$$\underbrace{\rho_i \oplus \cdots \oplus \rho_i}_{m_i \text{ summands}}. \tag{5.34}$$

The reason for this two-leveled decomposition is that (5.33) is unique, whereas (5.34) may not be unique. If the multiplicity m_i is greater than one, there are many different choices for each summand in (5.34), depending on the chosen basis. Before we get to a first example for this, we look at a formula for computing $\rho_i^{(m_i)}$ and its invariant subspace. Let V_i be the invariant subspace of $\rho_i^{(m_i)}$. Then the orthogonal projection of $\mathbb{C}^n$ onto V_i is given by the following matrix P_i (cf. [JL01, Ch 14] and [Ser77, Sec 2.6]):

$$P_i = \frac{m_i\chi_i(1)}{|G|}\sum_{g\in G}\chi_i(g^{-})\rho(g). \tag{5.35}$$

This means that we obtain a basis for V_i by selecting linear independent columns from the matrix P_i. Equation (5.35) thus provides a method to split $\mathbb{C}^n$ into G-invariant subspaces (which are only irreducible if all multiplicities m_i equal 1). The value $m_i\chi_i(1)$ is interesting in its own right since it equals the dimension $\dim V_i$. The matrices for the complete representation $\rho_i^{(m_i)}$ are given by $\rho_i^{(m_i)}(g) = P_i\rho(g)$.

Example 5.38. As an example we consider the canonical representation ρ of the permutation group $G := \langle(1\,2),(3\,4)\rangle \cong \mathcal{S}_2 \times \mathcal{S}_2$. A quick calculation with GAP shows that the character χ_ρ of ρ can be written as $\chi_\rho = 2\chi_1 + \chi_2 + \chi_3$. In this decomposition χ_1 is the so called **trivial character** which has value 1 on all group elements. The remaining χ_2 and χ_3 are other irreducible characters which we ignore for the moment. Let V_1 be the invariant subspace of $\rho_1^{(2)}$, which is the subrepresentation of ρ with character $2\chi_1$. By formula (5.35) we obtain for the projection of $\mathbb{C}^4$ onto V_1:

$$P_1 = \frac{1}{2}\begin{pmatrix} 1 & 1 & 0 & 0 \\ 1 & 1 & 0 & 0 \\ 0 & 0 & 1 & 1 \\ 0 & 0 & 1 & 1 \end{pmatrix}.$$

Looking at the columns of P_1, we see that V_1 actually is the fixed space $\mathrm{Fix}(G)$. Since the multiplicity of χ_1 in χ is 2, this space is not irreducible and we have infinitely many choices for invariant subspaces of $V_1 = \mathrm{Fix}(G)$. Two examples for a decomposition are

$$\begin{aligned}\mathrm{Fix}(G) &= \mathrm{span}(1,1,0,0)^\top \oplus \mathrm{span}(0,0,1,1)^\top \\ &= \mathrm{span}(1,1,-1,-1)^\top \oplus \mathrm{span}(1,1,1,1)^\top.\end{aligned} \tag{5.36}$$

For the representation this looks as follows. We compute that $\rho_1^{(2)}(g)$ equals P_1 for every $g \in G$; the representation matrix is independent of the group element. We can decompose this representation into a direct sum

$$\rho_1^{(2)}(g) = \frac{1}{2}\begin{pmatrix}1&1&0&0\\1&1&0&0\\0&0&0&0\\0&0&0&0\end{pmatrix} \oplus \frac{1}{2}\begin{pmatrix}0&0&0&0\\0&0&0&0\\0&0&1&1\\0&0&1&1\end{pmatrix} \tag{5.37}$$

or

$$\rho_1^{(2)}(g) = \frac{1}{4}\begin{pmatrix}1&1&-1&-1\\1&1&-1&-1\\-1&-1&1&1\\-1&-1&1&1\end{pmatrix} \oplus \frac{1}{4}\begin{pmatrix}1&1&1&1\\1&1&1&1\\1&1&1&1\\1&1&1&1\end{pmatrix}, \tag{5.38}$$

these are again independent of the group element g. Equations (5.37) and (5.38) correspond to the two choices for the subspaces in (5.36). For the other projection matrices P_2 and P_3 we obtain by (5.35) and the character information about χ_2 and χ_3 stored in GAP:

$$P_2 = \frac{1}{2}\begin{pmatrix}1&-1&0&0\\-1&1&0&0\\0&0&0&0\\0&0&0&0\end{pmatrix} \quad \text{and} \quad P_3 = \frac{1}{2}\begin{pmatrix}0&0&0&0\\0&0&0&0\\0&0&1&-1\\0&0&-1&1\end{pmatrix}.$$

Thus, we have computed a (unique) decomposition of $\mathbb{C}^4$ into invariant subspaces as

$$\mathbb{C}^4 = \operatorname{Fix}(G) \oplus \operatorname{span}(1,-1,0,0)^\top \oplus \operatorname{span}(0,0,1,-1)^\top.$$

■

We will see another example for non-unique invariant subspaces in Example 6.5. In the context of this thesis it is not necessary to systematically compute decompositions of $\rho_i^{(m_i)}$. Methods for this are described in [Ser77, Sec 2.7].

So far we have seen how to compute generators for invariant subspaces of $\mathbb{C}^n$. For our geometric applications we need real invariant subspaces of a real representation. Since we have a real representation, the complex conjugate $\overline{V}$ of an invariant subspace $V \subset \mathbb{C}^n$ is also an invariant subspace of $\mathbb{C}^n$. Thus, $V' := V + \overline{V}$ is an invariant subspace of $\mathbb{R}^n$. By combining complex conjugate subspaces we obtain real invariant subspaces.

Now we have gathered all theoretical tools to compute real invariant subspaces of a permutation group. Irreducible characters are available for all groups of practical interest in GAP or similar systems. Based on these we use the projection formula (5.35) to compute a basis of the corresponding invariant subspace. Note that the straightforward implementation where each group element occurs as a summand may take too much time for large groups. A more sophisticated way to evaluate sums over conjugacy classes (for which the character-factor is constant) based on coherent configurations is implemented in the GAP package [PK10]. Its function `ProjComp` can be used to obtain the essential parts of the projection matrix P_i from a given permutation group and one of its irreducible characters.

For large groups the class sum computations can still take a long time. An alternative way to obtain invariant subspaces is by solving a polynomial equation system. Let $V \subseteq$

$\mathbb{R}^n$ be an arbitrary invariant subspace of a transitive group $G \leq \mathcal{S}_n$. Since the orbit of the projection $e^{(1)}|_V$ spans V, it is enough to characterize all vectors that arise as such a projection in order to characterize all invariant subspaces. We know a few things about the projection $e^{(1)}|_V$. First, it is constant on the orbits of $\mathrm{Stab}_G(1)$ by Lemma 5.2. Second, we have a relation among the coordinates by Lemma 5.10. Let $O_1, \ldots, O_k$ be the orbits of $\mathrm{Stab}_G(1)$. So,

$$e^{(1)}|_V = \sum_{i=1}^{k} \alpha_i \mathbb{1}_{O_i} \tag{5.39}$$

for some scalars $\alpha_i \in \mathbb{R}$. Here, $\mathbb{1}_O$ denotes the characteristic vector of an orbit O. Further, let $\{g_1, \ldots, g_n\} \subset G$ be a transversal for $\mathrm{Stab}_G(1)$, that is, $g_j(j) = 1$ for each $j \in [n]$. By Lemma 5.10, this yields the equation

$$\alpha_j = \left\langle e^{(1)}|_V, e^{(j)} \right\rangle = \left\langle e^{(1)}|_V, e^{(j)}|_V \right\rangle = \left\langle e^{(1)}|_V, g_j e^{(1)}|_V \right\rangle \tag{5.40}$$

for every orbit index i and every $j \in O_i$. Plugging (5.39) into (5.40), we obtain k quadratic equations in terms of the variables $\alpha_1, \ldots, \alpha_k$. The solutions of this polynomial equation system are candidates for projections of invariant subspaces of G. The solutions can be computed, for instance, with [Sage], which internally uses [Singular] for the actual solution process. Since there are only few (easy) stabilizer computations, this approach is not so much limited by the group size as by the number k of distinct orbits. If k gets too large, the polynomial equation system may be too big to be solved in reasonable time.

5.5.2. Minimal projections

All core point constructions that we have encountered in this chapter are based on vectors with minimal projection. If we are interested in core points for a specific group, we therefore need to find these minimal vectors. In this section we look at computational means for this task. We discuss rational and irrational invariant subspaces separately and start with the rational case.

To apply Lemma 5.19 we need an integral point with globally minimal projection for some rational invariant subspace $V \subset \mathbb{R}^n$. That is, given a layer index k, we are looking for $z \in \mathbb{Z}^n_{(k)}$ such that $\|z|_V\| \leq \|z'|_V\|$ for all $z' \in \mathbb{Z}^n_{(k)}$. Every $z \in \mathbb{Z}^n_{(k)}$ can be written as a sum $ke^{(1)} + z^{(0)}$ for a $z^{(0)} \in \mathbb{Z}^n_{(0)}$. Let $\Lambda_{(0)} := \mathbb{Z}^n_{(0)}|_V$ be the projection of all integral points in the layer with index zero. Since the subspace V has a rational basis, this set $\Lambda_{(0)}$ is a lattice and has rank $\dim V$. In this notation, finding a globally minimal projection is equivalent to finding a lattice point $u \in \Lambda_{(0)}$ which is closest to $ke^{(1)}|_V$, i.e., $\left\|u - ke^{(1)}|_V\right\|$ is minimal among all $u \in \Lambda_{(0)}$. Let u be such a closest lattice point and let $z^{(0)} \in \mathbb{Z}^n_{(0)}$ be a pre-image of the projection u. Then $z := -z^{(0)} + ke^{(1)}$ is a solution to the original problem, i.e., it has globally minimal projection. Computing such a closest lattice point is a standard problem in computational mathematics, albeit an NP-hard one, even for approximation (cf. [ABSS97]). Algorithms to solve the closest vector problem are implemented, for instance, in [fplll] and [Magma].

In the case of irrational subspaces the situation is different. The set $\Lambda_{(0)}$ is no longer a lattice and we are not able to store an exact representation of the irrational basis vectors anyway. We can set up a rational problem that approximates the irrational problem as follows (cf. [Han10, pp. 236]). Let $V \subset \mathbb{R}^n$ be an m-dimensional irrational invariant subspace and let $v^{(1)}, \dots, v^{(m)}$ be an orthogonal basis with vectors of the same length. Consider the matrix

$$M(C) := \begin{pmatrix} 1 & 0 & \dots & 0 \\ 0 & 1 & \dots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \dots & 1 \\ \left\lfloor Cv_2^{(1)} \right\rceil & \left\lfloor Cv_3^{(1)} \right\rceil & \dots & \left\lfloor Cv_n^{(1)} \right\rceil \\ \vdots & \vdots & \vdots & \vdots \\ \left\lfloor Cv_2^{(m)} \right\rceil & \left\lfloor Cv_3^{(m)} \right\rceil & \dots & \left\lfloor Cv_n^{(m)} \right\rceil \end{pmatrix} \in \mathbb{Z}^{(n+m-1)\times(n-1)} \tag{5.41}$$

where $C \in \mathbb{R}$ is some large number and $\lfloor \cdot \rceil$ denotes rounding to the nearest integer. The columns of the matrix $M(C)$ are a basis of a sublattice $\Lambda(C)$ of $\mathbb{Z}^{n+m-1}$. If $u \in \Lambda(C)$ is a shortest (non-zero) vector in this lattice, then the vector $(0, u_1, \dots, u_{n-1})^\top \in \mathbb{Z}^n$, formed by the first $n-1$ coordinates of u, has "small" projection onto V. Note that for the matrix $M(C)$ we discard the first coordinate of all vectors $v^{(i)}$. Otherwise the vector $\mathbb{1}$, which is orthogonal to V, would be a shortest vector of $\Lambda(C)$.

Example 5.39. For instance, for the cyclic group $\mathcal{C}_5$ of order five and the subspace V from Section 5.2.2 the matrix $M(C)$ could look like

$$M(C) = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \\ \left\lfloor C\cos\left(\frac{2\pi}{5}\right) \right\rceil & \left\lfloor C\cos\left(\frac{4\pi}{5}\right) \right\rceil & \left\lfloor C\cos\left(\frac{6\pi}{5}\right) \right\rceil & \left\lfloor C\cos\left(\frac{8\pi}{5}\right) \right\rceil \\ \left\lfloor C\sin\left(\frac{2\pi}{5}\right) \right\rceil & \left\lfloor C\sin\left(\frac{4\pi}{5}\right) \right\rceil & \left\lfloor C\sin\left(\frac{6\pi}{5}\right) \right\rceil & \left\lfloor C\sin\left(\frac{8\pi}{5}\right) \right\rceil \end{pmatrix}.$$

For $C \in \{10^2, 10^3, 10^4\}$ we obtain from the first four coordinates of shortest lattice vectors (computed by [fplll]) the points

$$\begin{aligned} u^{(100)} &= (0, 0, -5, 3, -5)^\top, \\ u^{(1000)} &= (0, 0, -13, 8, -13)^\top, \\ u^{(10000)} &= (0, 0, -55, 34, -55)^\top, \end{aligned}$$

which are core points by Proposition 5.12. ■

6. Core Sets of Proper Subdirect Products

The previous chapters gave a rough idea of how core sets of transitive groups look like. In this chapter we examine groups, which do not relate directly to the previous results. We study intransitive groups that cannot be written as a direct product of smaller permutation groups. These groups are subdirect products of transitive groups as noted in Section 2.2. We will study different classes of groups that arise in this manner and analyze how their core sets characteristics compare to the ones of transitive groups. As before, the main driver are questions about finiteness of fundamental core sets. In particular we focus on subdirect products of two symmetric groups since these products can all be characterized and yield interesting examples with respect to core sets. Some of these subdirect products are relevant for applications in optimization because they describe the action of a permutation group on the columns of a matrix, which frequently occurs in integer programming.

6.1. Permutation group theory

We start with a characterization of subdirect products. This is originally due to Remak [Rem30] and also explained in [Hal59, Ch. 5.5] and [Hul10, Ch. II.4]. The following clear formulation is taken from [HMPW12, Thm 2.4].

Theorem 6.1 (Subdirect product, [Rem30])**.** If G is a subdirect product of G_1 and G_2, then there exist a group K and surjective homomorphisms $\phi_i : G_i \to K$ for $i \in \{1, 2\}$ such that

$$G = \{(g_1, g_2) \in G_1 \times G_2 \ : \ \phi_1(g_1) = \phi_2(g_2)\}.$$

Every such construction yields a subdirect product.

Subdirect products of more than two groups are obtained naturally by iterating this construction. Two special cases are the following. If we take K as the trivial group and ϕ_1, ϕ_2 as trivial homomorphisms that map everything onto the identity, then we obtain the direct (Cartesian) product of G_1 and G_2 since the condition $\phi_1(g_1) = \phi_2(g_2)$ is fulfilled for all group elements. If at least one ϕ_i is not trivial, then the resulting group is a proper subdirect product. The other extremal case are the so called diagonals. If $G := G_1 = G_2$ and we choose $K = G$ and $\phi_1 = \phi_2 = \mathrm{id}$ to be the identity, then we obtain $H = \{(g, g) \ : \ g \in G\}$. This group H is called a **diagonal** of G (cf. [Cam99, Sec. 1.6]). For instance, the group $\langle(1\,2)(3\,4)\rangle$ from Example 2.1 is a diagonal of $\mathcal{S}_2$. If the degree of such a diagonal H is $\deg H = n \cdot k$ and $\deg G = n$, then we can interpret the action of H also as follows. We can think of the domain of H as a $k \times n$-matrix A;

then H acts on the columns of A. This kind of action often naturally occurs in some hard integer programming problems (see, for instance, [KP08]).

For relating core sets of subdirect products to our previous knowledge it helps to draw a connection to direct products. The core set of a direct product is the Cartesian product of core sets (cf. Theorem 3.18). The following observation follows straight from Theorem 6.1.

Remark 6.2. If G is a subdirect product of G_1 and G_2 with homomorphisms ϕ_1 and ϕ_2, then G contains the direct product $\ker\phi_1 \times \ker\phi_2$. In particular, $\mathrm{core}(G) \subseteq \mathrm{core}(\ker\phi_1) \times \mathrm{core}(\ker\phi_2)$.

If one of these kernels is not the trivial group, this yields a non-trivial bound on the core set of a subdirect product. This will help us to prove in Section 6.2.3 that also intransitive groups can have a finite fundamental core set.

6.2. Core points for subdirect products of $\mathcal{S}_n$

In this section we discuss the core sets of a special class of subdirect products: subdirect products of two symmetric groups. After a characterization of the possible combinations we analyze their core sets. As in the chapters before, the main question is whether the fundamental core set is finite or what other relations exist among core points.

6.2.1. Characterization

For the subdirect product of two symmetric groups we do not have much choice.

Lemma 6.3. If G is a subdirect product of two symmetric groups $\mathcal{S}_k$ and $\mathcal{S}_l$ with $k \leq l$, then one of the following cases holds:

(i) $G \cong \mathcal{S}_k \times \mathcal{S}_l$ is a direct product of two symmetric groups

(ii) $k \geq 3$ and $\mathcal{A}_k \times \mathcal{A}_l \lneq G \lneq \mathcal{S}_k \times \mathcal{S}_l$

(iii) $2 = k < l$ and $G \cong \mathcal{S}_l$

(iv) $k = l$ and G is a diagonal

(v) $k = l = 6$ and $G \cong \mathcal{S}_6$, but G is not a diagonal and $\mathcal{S}_6$ appears in two different permutation representations.

(vi) $k = 3, l = 4$ and $G \cong \mathcal{S}_4$

(vii) $k = 4, l = 4$ and $|G| = 96$

Proof. We can narrow the range of K by using the fact that, if $\phi : G \to K$ is a homomorphism, then $\ker\phi$ is a normal subgroup of G. In the following we write $\langle()\rangle$ for the trivial group. Since $\mathcal{A}_n$ is simple for $n \neq 4$, the only choices for K in this case are $\langle()\rangle$, $\mathcal{S}_2$, $\mathcal{S}_n$ (corresponding to the normal subgroups $\mathcal{S}_n, \mathcal{A}_n, \langle()\rangle$ of $\mathcal{S}_n$, respectively). For $n = 4$ the group K can also be $\mathcal{S}_3$ (by factoring out the Klein-four group, which is an exceptional fourth normal subgroup of $\mathcal{S}_4$). In the following we look at each choice of K separately.

Case $K = \mathcal{S}_2$. Either $k = 2$ and $\phi = \mathrm{id}$ is the identity or $k > 2$ and $\phi : \mathcal{S}_k \to \mathcal{S}_k/\mathcal{A}_k$ maps to the factor group mod $\mathcal{A}_n$. The same holds for l and ψ. This knowledge about ϕ and ψ lead to the following cases for k and l.

- For $k = l = 2$ we obtain the direct product $\mathcal{S}_2 \times \mathcal{S}_2$.
- For $2 = k < l$ we obtain a group isomorphic to $\mathcal{S}_l$ since the subdirect product contains $|\mathcal{S}_l|$ elements and the whole group $\mathcal{S}_l$ in its second component.
- For $2 < k \leq l$ we have $\ker \phi = \mathcal{A}_k$ and $\ker \psi = \mathcal{A}_l$. By Remark 6.2, the subdirect product G must contain $\mathcal{A}_k \times \mathcal{A}_l$. As the subdirect product contains $2 \cdot |\mathcal{A}_k| \cdot |\mathcal{A}_l|$ elements, it is neither the direct product of alternating nor of symmetric groups but lies in between. In fact, G is a so called semidirect product $\mathcal{S}_2 \rtimes (\mathcal{A}_k \times \mathcal{A}_l)$.

Case $K = \mathcal{S}_3$. If $k = l = 3$, the group G is a diagonal of $\mathcal{S}_3$. Since $\mathcal{S}_3$ is a normal subgroup of $\mathcal{S}_4$, we can also have $l = 4$. This leads to the two exceptional cases (vi) and (vii).

Case $K = \mathcal{S}_n$ and $n > 3$. In this case we must have $k = l$. For $k = l = 6$ there is an outer automorphism of $\mathcal{S}_6$ (see, for instance, [Wil09, Sec 2.4.2]), so both factors may appear in different permutation representations, which leads to the exceptional case (v) that is not a diagonal. For all other values of $k = l$, the outer automorphism group of $\mathcal{S}_k$ is trivial, so these are diagonals.

Case $K = \langle () \rangle$. The only remaining case is a trivial group K, which implies that G is a direct product. □

Next we study the core sets of the groups of these subdirect products of two symmetric groups. We already know by Remark 3.34 that the fundamental core set of the group (i) is finite. Group (ii) has the same (finite) fundamental core set as (i) since the group contains a direct product of alternating groups (cf. Remark 3.34). The remaining groups are the subject of the next sections: case (iv) in Section 6.2.2, case (iii) in Section 6.2.3, and the exceptional cases (v), (vi), (vii) in Section 6.2.4.

Many core points in this section are constructed according to the following simple observation. Let G be a subdirect product of G_1 and G_2 and let Ω_i be the domain of G_i. Acting on $\mathbb{R}^n$, this induces a decomposition into coordinate disjoint subspaces $\mathbb{R}^{|\Omega_1|} \oplus \mathbb{R}^{|\Omega_2|}$. Further, we denote by π_i the projection homomorphism $\pi_i : G_1 \times G_2 \to G_i$ that restricts the action to a factor. For a set $S \subset \Omega_1$ let $\mathbb{1}_S$ be its characteristic vector. That is, $\mathbb{1}_S$ is a vector of dimension $|\Omega_1|$ where the i-th coordinate $(\mathbb{1}_S)_i$ equals 1 if $i \in S$ and is 0 otherwise.

Lemma 6.4. Let $S \subset \Omega_1$ be an arbitrary set. For every core point $v \in \operatorname{core}(\pi_2(\operatorname{Stab}_G(S)))$ the direct sum $\mathbb{1}_S \oplus v$ is a core point for G.

Before we proceed with the proof we take a closer look at the statement. Our goal in this section is to find non-universal core points for certain subdirect products of symmetric groups. For a direct product the lemma is quite useless because the actions of G_1 and G_2 are independent and therefore $\pi_2(\operatorname{Stab}_G(S)) = G_2$ for every set S. However, in a proper subdirect product we might have a set S such that $\pi_2(\operatorname{Stab}_G(S))$ is a group for which we know that its fundamental core set is infinite. By the lemma we find an embedding of this infinite fundamental core set in the fundamental core set of G, showing that $\operatorname{fcore}(G)$ also is infinite. The following sections provide examples for this lemma.

Proof of Lemma 6.4. For $v \in \operatorname{core}(\pi_2(\operatorname{Stab}_G(S)))$ let $z := \mathbb{1}_S \oplus v$. We have to show that z is a core point for G. Let

$$y = \sum_{g \in G} \lambda_g g z = y' \oplus y''$$

be a convex combination of an integral point. Because $\mathbb{1}_S$ is a $0/1$-vector, the vector y' must also be $0/1$. In particular, it must be a permutation of $\mathbb{1}_S$. Hence, there is a coset $h\,\mathrm{Stab}_G(S)$ such that $\sum_{g \in h\,\mathrm{Stab}_G(S)} \lambda_g = 1$. Due to symmetry we can assume w.l.o.g. that h is the identity. Thus, y lies in the convex hull $\operatorname{conv} \mathrm{Stab}_G(S)z$. By choice of z,

$$\operatorname{conv}\left(\mathrm{Stab}_G(S)z\right) = \mathbb{1}_S \oplus \operatorname{conv}\left(\pi_2(\mathrm{Stab}_G(S))v\right).$$

By assumption of the lemma, the right-hand side is lattice-free. Hence, y is a vertex of $\operatorname{conv} \mathrm{Stab}_G(S)z$ and therefore also of $\operatorname{conv} Gz$. We conclude that z is a core point. □

6.2.2. Diagonals

In this section we show that fundamental core sets of diagonal groups are infinite. We start with the smallest possible example.

Example 6.5. Consider the group $G := \langle (1\,2)(3\,4) \rangle$, which is the diagonal of $\mathcal{S}_2$. The fixed space $\mathrm{Fix}(G)$ is the linear hull of $(1,1,0,0)^\top$ and $(0,0,1,1)^\top$. To study the fundamental core set of G it suffices to study zero-based core points. The notion of zero-based points was introduced in Definition 3.20 for transitive groups only, but it can easily be adapted to intransitive groups. With respect to the fixed space of G, "zero-based" for a point z means $z \in \mathbb{Z}^4_{\geq 0}$ and at least one of the coordinates $\{z_1, z_2\}$ and one of $\{z_3, z_4\}$ is zero. The symmetry allows us to assume w.l.o.g. that $z_1 = 0$. It is easy to see that for every two co-prime positive integers $p, q \in \mathbb{Z}_{>0}$ the two points $(0,p,0,q)^\top$ and $(0,p,q,0)^\top$ are core points. If p and q have a common divisor greater than one, the orbit polytopes of each of the two points are not lattice-free. Thus, a fundamental core set of G can be described as:

$$\begin{aligned} \mathrm{fcore}(G) = &\left\{(0,p,0,q)^\top \;:\; p,q \in \mathbb{Z}_{>0} \text{ and } \gcd(p,q) = 1\right\} \cup \\ &\left\{(0,p,q,0)^\top \;:\; p,q \in \mathbb{Z}_{>0} \text{ and } \gcd(p,q) = 1\right\} \cup \\ &\left\{(0,0,0,0)^\top, (0,1,0,0)^\top, (0,0,1,0)^\top\right\}. \end{aligned} \tag{6.1}$$

If we want to decompose $\mathbb{R}^4$ into invariant subspaces, an obvious choice is

$$\mathbb{R}^4 = \mathrm{Fix}(G) \oplus \mathrm{span}(1,-1,0,0)^\top \oplus \mathrm{span}(0,0,1,-1)^\top.$$

At the first glance this looks like the core points from (6.1) were arbitrarily far away from the invariant subspaces, in contrast to Theorem 3.13. This apparent contradiction can be resolved by using another decomposition of $\mathbb{R}^4$. It is also possible to decompose

$$\mathbb{R}^4 = \mathrm{Fix}(G) \oplus \mathrm{span}(a,-a,b,-b)^\top \oplus \mathrm{span}(b,-b,-a,a)^\top$$

for any non-zero a and b. For instance, the orbit polytope $\operatorname{conv} G(0,p,0,q)^\top$ is orthogonal to the invariant subspace $\mathrm{span}(q,-q,-p,p)^\top$. Thus it is contained in $U := \mathrm{Fix}(G) \oplus \mathrm{span}(p,-p,q,-q)^\top$. So in particular the orbit polytope is "close" to the invariant subspace U. This serves as an example for the case that Theorem 3.13 holds only for one of infinitely many possible decompositions into invariant subspaces. ■

The construction behind this example generalizes naturally to other diagonals. Let $G \cong \mathcal{S}_k$ be a diagonal in $\mathcal{S}_{2k}$. We identify $\mathbb{R}^{2k}$ with $\mathbb{R}^k \oplus \mathbb{R}^k$ so that G acts identically on both summands.

It is quite easy to see that the point $z := pe^{(1)} \oplus qe^{(1)}$ is a core point for all coprime integers p and q. For let $y := \sum_{i=1}^{k} \lambda_i (pe^{(i)} + qe^{(i)})$ with $\lambda_i \geq 0$ and $\sum \lambda_i = 1$ an inner integral point of the orbit polytope $\operatorname{conv} Gz$. Looking at the first component of y, we must have $p\lambda_i \in \mathbb{Z}$ for all i. Similarly, we deduce $q\lambda_i \in \mathbb{Z}$ for all i. For coprime p and q this is possible only if $\lambda_j = 1$ for one coordinate j. Thus, z is a core point. The orbit polytope $\operatorname{conv} Gz$ is a k-dimensional simplex in dimension $2k$. This is quite low-dimensional since the maximal dimension possible for an orbit polytope is $2k - \operatorname{Fix}(G) = 2k - 2$. We find a lattice-free orbit polytope with maximal dimension by changing the construction slightly.

Lemma 6.6. Let $I, J \subset \{1, \dots, k\}$ be two disjoint sets. For every positive integer q, the point $z(q, I, J) := \left(\sum_{i \in I} e^{(i)}\right) \oplus \left(q \sum_{i \in I} e^{(i)} + \sum_{j \in J} e^{(j)}\right)$ is a core point for G, the diagonal of $\mathcal{S}_k$ in $\mathcal{S}_{2k}$.

Proof. For the proof we use Lemma 6.4. This lemma states that $z(q, I, J)$ is a core point if $z' := q \sum_{i \in I} e^{(i)} + \sum_{j \in J} e^{(j)}$ is a core point for $\operatorname{Stab}_G(I)$. Since G acts identically on both components of $\mathbb{R}^k \oplus \mathbb{R}^k$, we know that $\pi_2(\operatorname{Stab}_G(I)) = \operatorname{Stab}_{\mathcal{S}_k}(I)$. We observe that $\max_{i,j \in S} \left|z'_i - z'_j\right| \leq 1$ for $S \in \{I, [k] \setminus I\}$, i.e., z' is a universal core point when restricted to I and $[k] \setminus I$. Hence, the point z' must be a core point for $\operatorname{Stab}_{\mathcal{S}_k}(I)$. This implies by Lemma 6.4 that $z(q, I, J)$ is a core point for G. □

For $I = \{1\}$ and $J = \emptyset$ we obtain a k-simplex like above. More generally, if $q > 1$, the orbit polytope of $z(q, I, J)$ has

$$\left|\mathcal{S}_k : (\mathcal{S}_{|I|} \times \mathcal{S}_{|J|} \times \mathcal{S}_{k-|I|-|J|})\right| = \binom{k}{|I|, |J|, k - |I| - |J|}$$

vertices, where the term on the right-hand side is a multinomial coefficient. Furthermore, if $|I|, |J| \geq 1$, then $\dim \operatorname{conv} Gz(q, I, J) = 2k - 2$.

Example 6.7. Let $G = \langle (1\,2\,3\,4)(5\,6\,7\,8), (1\,2)(5\,6) \rangle \cong \mathcal{S}_4$ be a diagonal in $\mathcal{S}_8$. Using $I = \{1, 2\}$ and $J = \{3\}$ we see that $(1, 1, 0, 0, q, q, 1, 0)^\top$ is a core point for every positive integer q. The corresponding lattice-free orbit polytopes are six-dimensional and have twelve vertices each. ■

This shows that there also are infinitely many non-isomorphic core points whose orbit polytopes have maximal dimension. More non-isomorphic core points can be found easily, for instance, by using the projection construction from Lemma 5.19. Since there are infinitely many invariant subspaces, a complete classification or useful bounds are probably hard to obtain. The results of this section also provide a lower bound on the core set of diagonals of other groups because the diagonal of any group $G \leq \mathcal{S}_k$ is a subgroup of the diagonal of $\mathcal{S}_k$. We will discuss the implications for integer programming later in Section 7.2.5.

6.2.3. A proper subdirect product of $\mathcal{S}_2$ and $\mathcal{S}_n$

In this section we discuss the core set in case (iii) of Lemma 6.3. There we build the subdirect product G of $\mathcal{S}_2$ and $\mathcal{S}_n$ with $n > 2$ which is not the direct product. In terms of Theorem 6.1, we have that $K = \mathcal{S}_2$ is the image of the two homomorphisms $\phi_1 = \mathrm{id}$, $\phi_2 : \mathcal{S}_n \to \mathcal{S}_n/\mathcal{A}_n$. We will show in Proposition 6.9 that this subdirect product G has a finite fundamental core set. Note that $\ker \phi_2 \cong \mathcal{A}_n$ and the kernel $\ker \phi_1$ is trivial. Thus, by Remark 6.2 we know that $\mathrm{core}(G) \subseteq \mathbb{Z}^2 \times \mathrm{core}(\mathcal{A}_n)$. This argument by itself is not strong enough to show that the fundamental core set of G is finite since we have no information about the first factor. So we need more results in order to prove the main proposition of this section. Our proof will use the following auxiliary lemma.

Lemma 6.8. Let $z \in \{0, 1\}^n$ with $n \geq 3$. There exists a permutation $h \in \mathcal{S}_n \setminus \mathcal{A}_n$ with $hz = z$.

Proof. The stabilizer $\mathrm{Stab}_{\mathcal{S}_n}(z)$ of z is isomorphic to $\mathcal{S}_k \times \mathcal{S}_{n-k}$ where k denotes the number of ones in z. Since $n \geq 3$ this stabilizer contains a transposition. This transposition is the sought permutation h. □

Proposition 6.9. Let $G \leq \mathcal{S}_{n+2}$ be the subdirect product of $\mathcal{S}_2$ and $\mathcal{S}_n$ for $n > 2$ which is not a direct product. The fundamental core set of this group is $\mathrm{fcore}(G) = \mathrm{fcore}(\mathcal{S}_2 \times \mathcal{S}_n)$.

Proof. We first show that $\mathrm{core}(G) = \mathrm{core}(\mathcal{S}_2 \times \mathcal{S}_n)$ and discuss the relation between the fundamental core sets fcore afterwards.

Let $z \in \mathrm{core}(G)$ be a core point of G. W.l.o.g. we can assume that z is zero-based, i.e., $z = z' \oplus z''$ with $z' \in \mathbb{Z}^2_{\geq 0}$ and $z'' \in \mathbb{Z}^n_{\geq 0}$ which each have at least one coordinate with value zero. Because of symmetry we can further assume that $z'_2 = 0$. It suffices to show that $z \in \{0, 1\}^{n+2}$ in order to ensure that $z \in \mathrm{core}(\mathcal{S}_2 \times \mathcal{S}_n)$. The reverse inclusion $\mathrm{core}(G) \supseteq \mathrm{core}(\mathcal{S}_2 \times \mathcal{S}_n)$ follows from the fact that, as a subdirect product, G is a subgroup of the direct product of $\mathcal{S}_2$ and $\mathcal{S}_n$.

We already know that $z'' \in \mathrm{core}(\mathcal{A}_n) = \mathrm{core}(\mathcal{S}_n)$ by our considerations before the proposition. By our assumption $z'_2 = 0$ it thus remains to show that $z'_1 \in \{0, 1\}$. Let $h \in \mathcal{S}_n \setminus \mathcal{A}_n$ be such that $hz'' = z''$. This permutation exists by Lemma 6.8 since $n \geq 3$. Consider the permutation $g := ((1\,2), h) \in \mathcal{S}_2 \times \mathcal{S}_n$. By choice of h, this permutation g lies in the group G. Applying g to z yields:

$$gz = ((1\,2)z') \oplus z''.$$

If $z'_1 > 1$, then $\frac{1}{z'_1} z + \frac{z'_1 - 1}{z'_1} gz$ is an inner integral point of $\mathrm{conv}\, Gz$. Hence, z is a core point if and only if $z'_1 \in \{0, 1\}$. This concludes the proof of $\mathrm{core}(G) = \mathrm{core}(\mathcal{S}_2 \times \mathcal{S}_n)$.

The reasoning above based on Lemma 6.8 also shows that G and $\mathcal{S}_2 \times \mathcal{S}_n$ have the same orbits on $0/1$-vectors. Thus, the fundamental core sets (where the action of G is factored out) must be the same: $\mathrm{fcore}(G) = \mathrm{fcore}(\mathcal{S}_2 \times \mathcal{S}_n)$. □

The proposition shows that there are intransitive groups which do not contain a direct product with finite fundamental core set as a subgroup but which still have a finite fundamental core set themselves.

6.2.4. Exceptional cases

$\mathcal{S}_3, \mathcal{S}_4$, case (vi)

A quick calculation with GAP shows that, up to conjugation, $G = \langle (1\,2\,3)(5\,7\,6), (2\,3)(4\,7\,5\,6) \rangle$. Choosing $S = \{1\}$, we compute $H := \mathrm{Stab}_G(S) = \langle (2\,3)(4\,7\,5\,6), (4\,6)(5\,7) \rangle$. For the projection onto the second G-orbit $\{4, 5, 6, 7\}$ we obtain $\pi_2(H) = \langle (4\,7\,5\,6), (4\,6)(5\,7) \rangle$. This is isomorphic to the dihedral group of order 8. In particular, it is an imprimitive group, for which we know the core set from Section 5.3, and for this group in particular from Example 5.34. We know that, for instance, for every integer $a \in \mathbb{Z}$ the point $(1 + a, a, -a, -a)^\top$ is a core point for $\pi_2(H)$. Thus, for every integer a the point $(1, 0, 0, 1 + a, a, -a, -a)^\top$ is a core point for G. For different values of a these are not isomorphic, so the fundamental core set of G is infinite.

We can also switch the roles of the groups G_1 and G_2. If we choose $S = \{4, 5\}$, we obtain $H := \mathrm{Stab}_G(S) = \langle (4\,5)(6\,7), (2\,3)(6\,7) \rangle$. Hence, $\pi_1(H) = \langle (2\,3) \rangle$. The core set of $\pi_1(H)$ contains $(0, a, 1 + a)^\top$ for every integer a. Thus, for every integer a the point $(0, a, 1 + a, 1, 1, 0, 0)^\top$ is a core point for G. Again, these are non isomorphic, providing another argument that the fundamental core set of G is infinite.

All fundamental core sets that we have seen before this section had the following interesting property. If a group had the same invariant subspaces as a direct product of symmetric groups, then its fundamental core set was finite. The group G from this section is different because it has the same invariant subspaces as $\mathcal{S}_3 \times \mathcal{S}_4$ but has infinite fundamental core set.

Question 6.10. Is there a necessary or sufficient criterion for the finiteness of fundamental core sets of intransitive groups?

$\mathcal{S}_4, \mathcal{S}_4$, case (vii)

We proceed as in the previous case. A calculation with GAP shows that $G = \langle (2\,3\,4)(6\,7\,8), (1\,4\,2\,3)(5\,7\,6\,8) \rangle$. Choosing $S = \{1, 2\}$, we obtain $\pi_2(\mathrm{Stab}_G(S)) = \langle (7\,8), (5\,7)(6\,8) \rangle$. Again, this is isomorphic to the dihedral group of order 8. Like in the previous section we see that for every integer a the point $(1, 0, 0, 0, 1 + a, a, -a, -a)^\top$ is a core point for G. For different values of a these are not isomorphic, so the fundamental core set of G is infinite.

$\mathcal{S}_6, \mathcal{S}_6$, case (v)

We proceed as in the previous case. A calculation with GAP shows that $G = \langle (1\,2\,3\,4\,5\,6)(7\,12\,8)(9\,11), (1\,2)(7\,8)(9\,10)(11\,12) \rangle$. Choosing $S = \{1, 3, 5\}$, we obtain $\pi_2(\mathrm{Stab}_G(S)) = \langle (7\,8)(9\,11), (7\,9\,8\,11\,12\,10) \rangle$. This is an imprimitive group of order 36. It has a block system consisting of $\{\{7, 8, 12\}, \{9, 10, 11\}\}$. By Theorem 5.18 we obtain core points for $\pi_2(\mathrm{Stab}_G(S))$ and lift them by Lemma 6.4 to G. For the group G we obtain the core points $(1, 0, 1, 0, 1, 0, 1 + a, a, -a, -a, -a, a)^\top$ for every integer a. These non-isomorphic core points show that the fundamental core set of G is infinite.

7. Applications in Integer Programming

In this chapter we discuss various applications of core points in symmetric convex optimization problems with integrality restrictions. We show that every convex optimization problem with integrality restrictions has a solution in the core set of the symmetry group. One of the main questions in this chapter is how this knowledge can be used to solve optimization problems faster. We start with the special case of a transitive symmetry group, for which we obtain an algorithm that is polynomial in the size of the input, provided the fundamental core set of the symmetry group is part of the input. If the symmetry group has multiple orbits, things get complicated. We look at several strategies to use core sets in this case and evaluate prototypical implementations. We pursue two side projects besides this main topic. First, we construct integer programming problems based on core points which look innocent but are hard to solve for standard optimization tools. Second, we survey the symmetries of the mixed integer programming problems in the MIPLIB 2010 collection and discuss the potential of core set based algorithms in this benchmark suite.

7.1. Warm up

7.1.1. Definition of symmetries in convex optimization

For a convex set $C \subseteq \mathbb{R}^n$ and a convex function $f : C \to \mathbb{R}$ consider the convex optimization problem

$$\min_{x \in C} f(x).$$

We say that a function $g : C \to C$ is a symmetry of this optimization problem if g is bijective and g does not change the objective function, i.e., $f(g(x)) = f(x)$ for all $x \in C$. This notion naturally generalizes to problems with integrality restrictions; we replace C by $C \cap \mathbb{Z}^n$ everywhere. We will be mostly concerned with a special case of this problem, integer linear programming (IP). That is, we look for a solution of

$$\min_{x \in P \cap \mathbb{Z}^n} \langle c, x \rangle$$

for an objective direction $c \in \mathbb{R}^n$ and a polyhedron $P = \{x \in \mathbb{R}^n \ : \ Ax \leq b\}$, where the constraints are given by a matrix $A \in \mathbb{R}^{m \times n}$ and a vector $b \in \mathbb{R}^m$. We only consider problems for which the LP relaxation is feasible, i.e., P is not empty and $\min_{x \in P} \langle c, x \rangle$ exists. A symmetry of such an optimization problem is a bijective linear map $g : P \to P$ such that $g(P \cap \mathbb{Z}^n) = P \cap \mathbb{Z}^n$ and $\langle c, g(z) \rangle = \langle c, z \rangle$ for all $z \in P \cap \mathbb{Z}^n$. Computing all symmetries usually is a hard problem because it depends on the feasibility of the integer programming instance, which is well-known to be NP-complete itself.

In practice we therefore rather look at the **formulation symmetries** of the problem, i.e., symmetries of the polytope with $g(P) = P$ that also preserve all integral points. That is, we are interested in $\mathrm{GL}_n(\mathbb{Z})$ matrices that preserve the polytope P and do not change the value of the objective function. Because systematically computing these $\mathrm{GL}_n(\mathbb{Z})$-symmetries of polyhedra again is a difficult problem (cf. [BDP+12]), we only look at permutation symmetries.

Definition 7.1. A **(formulation) symmetry** of an IP over a non-empty polyhedron $P \subset \mathbb{R}^n$ and objective $c \in \mathbb{R}^n$ is a permutation $g \in \mathcal{S}_n$ such that $gx \in P$ and $\langle c, x\rangle = \langle c, gx\rangle$ for all $x \in P$. We call the group of all these permutations the symmetry group $G \leq \mathcal{S}_n$ of the IP.

Note that the invariance of the objective function implies that c must lie in the fixed space $\mathrm{Fix}(G)$. In the remainder of this chapter we refer to formulation symmetries just as symmetries. We will look at the computational details of determining the symmetry group later in Section 7.4.

7.1.2. A fundamental theorem

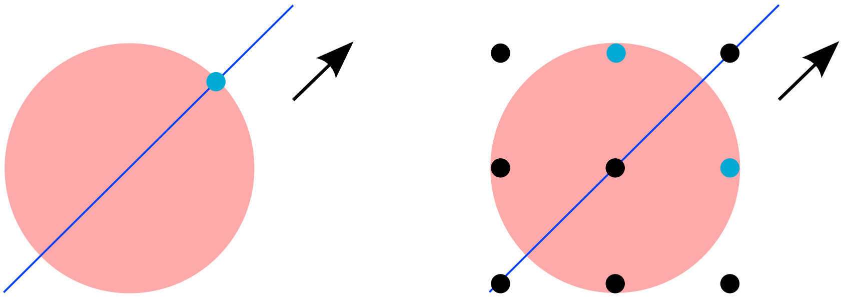
Over the last 15 years there has been substantial effort to develop techniques to exploit symmetries in integer programs. For the commonly used branch-and-bound (B&B) techniques to solve IPs, symmetry had always been regarded as a problem. Since isomorphic optimal solution occur at different places in the B&B-tree, pruning the tree efficiently may be difficult. Therefore, several methods have been developed to eliminate symmetry from the tree as far as possible. These methods, that aim at reducing the search space as much as possible while preserving at least one optimal solution, can be put into two categories (cf. [Mar10]). Static symmetry-breaking adds constraints to the problem before the solution process commences (for examples see [Lib08], [Fri07] and [KP08]). Dynamic symmetry-breaking techniques are embedded in the branch-and-bound process and are therefore able to adapt to the symmetry of subproblems. The two most prominent dynamic techniques are isomorphism pruning and orbital branching, which are explained in [Ost09] and [Mar10].

All these methods have in common that they treat IP symmetries as symmetries of the B&B-tree. Bödi, Herr *&* Joswig [BHJ13] demonstrated that there also is a rich geometric structure in IP symmetries beyond B&B. They give a polynomial-time algorithm for solving highly symmetric IPs. Their idea is based on the following well-known fact in convex optimization without integrality restrictions (see, for instance, [GP04]).

Theorem 7.2 (Folklore). Let $\min_{x\in C} f(x)$ be a convex optimization problem with convex function f and convex set C. Let G be a finite subgroup of the linear symmetry group of this instance. Then $\min_{x\in C} f(x) = \min_{x\in C\cap\mathrm{Fix}(G)} f(x)$.

Proof. Let $x \in C$ be an optimal solution of $\min_{x\in C} f(x)$. We define $\hat{x} := x|_{\mathrm{Fix}(G)} = \frac{1}{|G|}\sum_{g\in G} gx$ as the projection of x to the fixed space (cf. Remark 3.10). Because G consists of symmetries of C, all orbit elements gx lie in C. Thus, $\hat{x}$ as a convex combination is also in C. Moreover, we have $f(gx) = f(x)$ for all $x \in C$ since g is a symmetry of f. By convexity of f we therefore obtain $f(\hat{x}) \leq f(x)$. Hence, $\hat{x} \in \operatorname{Fix}(G)$ also is an optimal solution of $\min_{x \in C} f(x)$. □

This theorem implies that we only have to search for solutions in the fixed space of the symmetry group, which may lead to a huge reduction in problem dimension. Theorem 7.2 is also easily implementable in practice since we only have to add the constraint that the solution lies in a linear subspace. If we are interested only in optimal integral solutions, then the fixed space is not enough as the example in Figure 7.1 shows. Instead, we have to replace the fixed space of G by the core set of G (cf. [HRS13, Thm 4]).



(a) convex case: optimal solution lies in $\operatorname{Fix}(G)$

(b) integrality restrictions: optimal solution does not lie in $\operatorname{Fix}(G)$

Figure 7.1.: Optimal solutions and the fixed space

Theorem 7.3 ([HRS13])**.** Let $\min_{x \in C \cap \mathbb{Z}^n} f(x)$ be a convex integer optimization problem under integrality restrictions with a convex function f and a convex set $C \subseteq \mathbb{R}^n$. Let G be a finite subgroup of the linear symmetry group of this instance. Then $\min_{x \in C \cap \mathbb{Z}^n} f(x) = \min_{x \in C \cap \operatorname{core}(G)} f(x)$.

Proof. Let $x \in C \cap \mathbb{Z}^n$ be an optimal solution of $\min_{x \in C \cap \mathbb{Z}^n} f(x)$. If $x \in \operatorname{core}(G)$, the claim of the theorem is automatically satisfied. So consider the case that x is not a core point. Thus, $\operatorname{conv} Gx$ contains integer points that are not vertices. Let $\hat{x}$ be one of these points which has minimal norm among all integer points $\operatorname{conv} Gx \cap \mathbb{Z}^n$. By this choice the polytope $\operatorname{conv} G\hat{x}$ is lattice-free. Because f is convex, we have $f(\hat{x}) \leq f(x)$. Hence, $\hat{x} \in \operatorname{core}(G)$ also is an optimal solution of $\min_{x \in C \cap \mathbb{Z}^n} f(x)$. □

In other words, it suffices to search for a solution in the core set of the symmetry group. Since the core set is by definition a symmetric set, it suffices to search for solutions in a set of a-priori chosen orbit representatives. For almost all applications in this chapter it suffices to work with such a set of representatives. We therefore introduce a new symbol for notation.

Definition 7.4. For a group G we denote by $\operatorname{core}_{/}(G)$ a set of representatives from $\operatorname{core}(G)$ for the equivalence relation $x \sim y \quad :\Longleftrightarrow \quad x \in Gy$ (cf. Definition 3.5 of a fundamental core set).

The similarity in notation to core is intended to not confuse the reader since most statements remain true with $\operatorname{core}_{/}$ replaced by core. We have the following relations:

$$\operatorname{core}(G) = G \operatorname{core}_{/}(G) = G \operatorname{fcore}(G) + \operatorname{Fix}_{\mathbb{Z}}(G). \tag{7.1}$$

In particular, Theorem 7.3 remains correct if we replace $\operatorname{core}(G)$ by $\operatorname{core}_{/}(G)$. However, in contrast to the linear analogue above (Theorem 7.2), it is not obvious how to apply this theorem in practice.

For every permutation group G the core set $\operatorname{core}_{/}(G)$ consists of infinitely many points. Therefore we can not expect to check the feasibility of the integer hull $C \cap \mathbb{Z}^n$ by testing whether it contains each core point individually. In the next sections we will see algorithms that work if the symmetry group has a finite fundamental core set. In this case we can exploit the fact that $\operatorname{core}_{/}$ can be decomposed into a sum of $\operatorname{fcore}(G)$ and $\operatorname{Fix}_{\mathbb{Z}}(G)$ as seen in (7.1), both of which can then be described finitely. Before we discuss the general case in Section 7.2, we look at a special case.

7.1.3. A one-dimensional example

This section is based on the algorithm from [BHJ13] to solve integer programs with an $\mathcal{A}_n$ or $\mathcal{S}_n$ symmetry group. We slightly generalize it to all transitive groups with finite fundamental core set.

Consider an IP over an n-dimensional polyhedron $P \subset \mathbb{R}^n$ with a transitive symmetry group $G \leq \mathcal{S}_n$. Since the group is transitive, the objective function must be a multiple of $\mathbb{1}$. Remember from Definition 3.19 the definition of a layer $\mathbb{Z}^n_{(k)} := \{z \in \mathbb{Z}^n : \langle \mathbb{1}, z \rangle = k\}$ for some $k \in \mathbb{Z}$. The solution space $\mathbb{Z}^n$ of the integer program can be partitioned into layers. Note that all points in each layer have the same objective value. A possible strategy to solve the optimization problem could consist of the following two steps.

1. We enumerate all layers whose affine hull intersects P by ascending objective value. These affine hulls are hyperplanes, for which intersection with P is much easier to determine than the intersection of P with the discrete layer.
2. We check for each layer L found in the first step whether L itself intersects P.

The first step essentially amounts to solving a linear program $\min_{x \in P} \langle \mathbb{1}, x \rangle$. Remember that we only look at polyhedra P for which this minimum exists. Let c_{min} be the optimal value of this LP. Then we have to check the layers $\mathbb{Z}^n_{(k)}$ for $k \in \{\lceil c_{\text{min}} \rceil, \lceil c_{\text{min}} \rceil + 1, \lceil c_{\text{min}} \rceil + 2, \dots\}$. At first it seems as if we had to check infinitely many layers. We could of course solve a second linear program in the opposite direction to obtain an upper bound on k, at least if P is bounded in this direction. We will see in a minute that this second linear program is not necessary. Before we resolve this issue we look at the second part of the algorithm: checking whether a layer $\mathbb{Z}^n_{(k)}$ intersects P.

For this we assume that the symmetry group G has a finite fundamental core set. Because of the symmetry of P, a layer $\mathbb{Z}^n_{(k)}$ intersects P if and only if one of its core points $\operatorname{core}_{/}(G, \mathbb{Z}^n_{(k)})$ lies in P. Thus, for each layer index k that we computed in the first step, we enumerate all its core point representatives $\operatorname{core}_{/}(G, \mathbb{Z}^n_{(k)})$ and check whether one of them lies in P. Remember that core point representatives $\operatorname{core}_{/}(G, \mathbb{Z}^n_{(k)})$ in a layer $\mathbb{Z}^n_{(k)}$ can be chosen as translates of parts of the fundamental core set (cf. (3.9)). Thus, for every layer the set $\operatorname{core}_{/}(G, \mathbb{Z}^n_{(k)})$ is finite since the fundamental core set is finite. This ensures that we are able to actually test for all core points $z \in \operatorname{core}_{/}(G, \mathbb{Z}^n_{(k)})$ individually whether they lie in P. If none of these lies in P, we proceed with the next layer $k+1$. If one of the core points lies in P, then we have found an optimal solution since we process the layers by increasing k and hence increasing objective value.

For some layers the core set $\operatorname{core}_{/}(G, \mathbb{Z}^n_{(k)})$ is particularly easy to compute (cf. Remark 3.21). If $k := l \cdot n$ is an integer multiple of n, then $\operatorname{core}_{/}(G, \mathbb{Z}^n_{(k)}) = \{l\mathbb{1}\} \subset \operatorname{Fix}(G)$. By Theorem 7.2 the symmetry of P implies that P contains $l\mathbb{1}$ if and only if it intersects the affine hull of $\mathbb{Z}^n_{(ln)}$. Hence, these layers whose index is a multiple of n provide a stopping criterion as follows. One of the n consecutive layer indices $\{\lceil c_{\min} \rceil, \lceil c_{\min} \rceil + 1, \ldots, \lceil c_{\min} \rceil + n - 1\}$ must be a multiple of n. Let $\hat{c}$ be this index. If the core set $\operatorname{core}_{/}(G, \mathbb{Z}^n_{(\hat{c})})$ in this layer intersects P, we have found an optimal solution to the integer optimization problem. If $\operatorname{core}_{/}(G, \mathbb{Z}^n_{(\hat{c})})$ does not intersect P, then, as shown above, the affine hull of $\mathbb{Z}^n_{(\hat{c})}$ also cannot intersect P. Because P is convex, we can stop the search in this case. This shows that we can terminate the layer enumeration and checks after at most n layers. Combining all steps, we have proven the following result.

Theorem 7.5. Let G be the symmetry group of an integer program with n variables and m constraints. If G is transitive and the fundamental core set $\operatorname{fcore}(G)$ is finite, then the IP can be solved in $O(|\operatorname{fcore}(G)|\, nm)$ time if a fundamental core set is provided.

Proof. Suppose that we know the optimal LP relaxation $c_{\min} = \min_{x \in P} \langle \mathbb{1}, x \rangle$. Then our reasoning above shows that it suffices to test $\operatorname{core}_{/}(G, \mathbb{Z}^n_{(k)}) \cap P$ for $k \in \{\lceil c_{\min} \rceil, \lceil c_{\min} \rceil + 1, \ldots, \lceil c_{\min} \rceil + n - 1\}$. Note that $\operatorname{core}_{/}(G, \mathbb{Z}^n_{(k)})$ can be easily determined from $\operatorname{fcore}(G)$ by selecting the set

$$F_k := \{z \in \operatorname{fcore}(G) \ : \ \langle \mathbb{1}, z \rangle \equiv k \pmod{n}\}$$

and translating its elements by a suitable vector from $\operatorname{Fix}_{\mathbb{Z}}(G)$ so that $z \in \mathbb{Z}^n_{(k)}$. Thus, there are at most $|\operatorname{fcore}(G)|$ points to test and each test takes $O(nm)$ time. It remains to discuss how to obtain the LP relaxation $c_{\min}$.

Note that, like the IP, the LP also is symmetric. Therefore there exists an optimal solution in the fixed space $\operatorname{Fix}(G) = \operatorname{span} \mathbb{1}$ by Theorem 7.2. Let P be given as $P = \{x \in \mathbb{R}^n \ : \ Ax \leq b\}$. After intersecting P with the fixed space, we obtain $c_{\min}$ as minimum of the set

$$c_{\min} = n \cdot \min \{\lambda \in \mathbb{R} \ : \ \lambda A \mathbb{1} \leq b\},$$

which to determine also takes $O(nm)$ time. □

For the symmetric group $\mathcal{S}_n$ and the alternating group $\mathcal{A}_n$, every layer contains exactly one core point up to symmetry. For these groups we obtain as a special case the $O(n^2 m)$-polynomial time algorithm to solve highly symmetric integer programs which was introduced by [BHJ13]. This algorithm was improved to $O(nm)$-time by Herr & Rote [Her13b] by re-using results from previous computation steps. This improvement makes use of the special structure of the core sets of alternating groups and can probably not be easily generalized to arbitrary groups.

In [HRS13] Herr & Schürmann and the present author further generalized the approach which led to Theorem 7.5 to allow for arbitrary symmetry (permutation) groups. In the following section we discuss this and other core set-based algorithms to solve symmetric integer programs.

7.2. Core set-based IP algorithms

In this section we look at several ways to apply Theorem 7.3 to practical problems. Large parts of this section have been published in [HRS13]. This section also contains ideas that arose during the collaboration but did not make it into the mentioned article.

7.2.1. A naïve approach: enumeration

In this section we generalize the idea from Section 7.1.3 to work with arbitrary, not necessarily transitive symmetry groups that have a finite fundamental core set.

Let $G \leq \mathcal{S}_n$ be a symmetry group of an IP $\min_{x \in P \cap \mathbb{Z}^n} \langle c, x \rangle$. Our goal still is to decide whether an integer point lies in P and if so, determine the point with best objective value. To this end we consider a symmetric fibration of P. Let $\pi_G : \mathbb{R}^n \to \operatorname{Fix}(G)$ with $\pi_G(x) := x|_{\operatorname{Fix}(G)}$ be the orthogonal projection to the fixed space $\operatorname{Fix}(G)$. For $x \in \operatorname{Fix}(G)$ we call the set of pre-images $\pi_G^{-}(x)$ a **fiber**. Further, let $\Lambda := \pi_G(\mathbb{Z}^n)$ be the projection of integral points onto the fixed space. Note that the set Λ is a lattice and has $\operatorname{Fix}_{\mathbb{Z}}(G)$ as a sub-lattice. By construction, each integral point $z \in \mathbb{Z}^n$ lies in exactly one fiber through a lattice point $u \in \Lambda$. Since the objective direction c must lie in the fixed space, all points in a fiber have the same objective value. To find an optimal integral point in the polytope P, we proceed again in two steps.

1. Enumerate all fibers that intersect P and that go through a lattice point $u \in \Lambda$, sorted ascendingly by objective value.
2. For each of these fibers F check whether the intersection $P \cap F$ contains an integral point.

We start with the first part, the enumeration of fibers. To find all fibers that contain integral points and intersect P, we project P onto the fixed space. We then enumerate all points of Λ which lie in the projected polytope $\pi_G(P)$. An inequality description for $\pi_G(P)$ is readily available since projection to equals intersection with the fixed space by Lemma 4.1. Let $f^{(1)}, \dots, f^{(n_{\text{fix}})}$ be a basis of Λ (as a lattice) and thus also a basis for $\operatorname{Fix}(G)$ (as a vector space). Consider the polytope

$$P' := \left\{ \xi \in \mathbb{R}^{n_{\text{fix}}} \ : \ \sum_{i=1}^{n_{\text{fix}}} \xi_i A f^{(i)} \leq b \right\}.$$

Each integral point $\zeta \in P' \cap \mathbb{Z}^{n_{\text{fix}}}$ corresponds to a lattice point

$$\sum_{i=1}^{n_{\text{fix}}} \zeta_i f^{(i)} \in \pi_G(P) \cap \Lambda$$

and vice versa. Thus, the fiber enumeration step amounts to enumerating integral points in an n_{fix}-dimensional polytope P', whose inequalities are linear transformations of the inequalities of the original polytope P. We will discuss the practical aspects of this enumeration step later.

In the second step of the outline above we have to decide whether a fiber intersects the polytope P in an integral point. Like in the transitive case, we use core points for this test. Because fibers are symmetric sets, a fiber F intersects $P \cap \mathbb{Z}^n$ if and only if one of the core points $\operatorname{core}_{/}(G, F)$ in the fiber lies in P. We easily obtain $\operatorname{core}_{/}(G, F)$ from $\operatorname{fcore}(G)$ as follows. From $\operatorname{fcore}(G)$ we select all core points whose projection lies in the same coset as F with respect to the sub-lattice $\operatorname{Fix}_{\mathbb{Z}}(G) \subset \Lambda$. We then translate these selected core points by a suitable vector from $\operatorname{Fix}_{\mathbb{Z}}(G)$ so that they lie in F. This yields a set of core set representatives of F. In particular, the set $\operatorname{core}_{/}(G, F)$ is finite and it is possible to enumerate all core points in a fiber if a group has a finite fundamental core set. Thus, the performance of the second step only depends on the size of a fundamental core set and, of course, the dimension n.

We now return to the first step and discuss its implementation. Enumerating integral points in a polytope is a common problem and several software packages like [`Normaliz`, `LattE`] exist for the solution. However, there is a fundamental difference to the transitive case presented in the previous section. There we had to enumerate at most n points in Λ before we found a solution or determined infeasibility. As Example 7.6 shows, this is no longer true if the fixed space has dimension greater than one. In this case a polytope may be arbitrarily large without containing a point from $\operatorname{Fix}_{\mathbb{Z}}(G)$. For an unbounded polyhedron the lattice point enumeration thus may not terminate.

Example 7.6. Let $G := \langle (2\,3) \rangle \leq \mathcal{S}_3$. The fixed space $\operatorname{Fix}(G)$ has dimension two and is spanned by $(1, 0, 0)^\top$ and $(0, 1, 1)^\top$. For some number $m \geq 1$ consider the rectangle R with vertices

$$\left(0, \frac{1}{4}, \frac{1}{4}\right)^\top, \quad \left(0, \frac{3}{4}, \frac{3}{4}\right)^\top, \quad \left(m, \frac{1}{4}, \frac{1}{4}\right)^\top, \quad \left(m, \frac{3}{4}, \frac{3}{4}\right)^\top.$$

Clearly, this rectangle has symmetry group G and does not contain an integral point. Also note that R lies in $\operatorname{Fix}(G)$, thus R and its projection $\pi_G(R)$ coincide by Lemma 4.1.

Let $k \in [m]$ be some positive integer. If we adjoin to R a new pair of vertices $p = (k, 1, 0)^\top$ and $p' = (k, 0, 1)^\top$, then this new bipyramid $P_k := \operatorname{conv}(R \cup \{p, p'\})$ still has symmetry group G. However, it contains exactly two integral points p and p'. Since the projections $\pi_G(P_k)$ and $\pi_G(R)$ are the same for every k, we have to enumerate all lattice points in the projection and test its fibers to either find an optimal integral point or decide that the problem is infeasible. A similar example is presented in [Her13b, Ex 5.22]. ■

Another difficulty with enumerating integral points in polytopes is that the practically feasible dimensions are quite small. Despite these obstacles, the algorithm can be useful for some optimization instances. We will see results of computational experiments in Section 7.2.6.

7.2.2. Divide & impera

In this section we look at a different method to use core sets for solving integer programs. This method reduces a symmetric IP to several IPs in smaller dimension. As noted several times before, we can decompose a set of core set representatives $\operatorname{core}_{/}(G)$ into a disjoint union

$$\operatorname{core}_{/}(G) = \bigcup_{z \in \operatorname{fcore}(G)} \{z + u \ : \ u \in \operatorname{Fix}_{\mathbb{Z}}(G)\}. \tag{7.2}$$

For finding an optimal integral point in $\operatorname{core}_{/}(G) \cap P$ we split the problem into parts according to (7.2). Let $C(z) := \{z + u \ : \ u \in \operatorname{Fix}_{\mathbb{Z}}(G)\}$ be a set in this partition. For each $z \in \operatorname{fcore}(G)$ we solve an integer program $\min_{v \in C(z) \cap P} \langle c, v \rangle$. After these $|\operatorname{fcore}(G)|$-many IPs we either will have found a globally optimal integral point in P or determined that P does not contain an integral point. Note that $\min_{v \in C(z) \cap P} \langle c, v \rangle$ is an n_{fix}-dimensional problem. Each of these problems can be obtained from P by plugging a basis of $\operatorname{Fix}_{\mathbb{Z}}(G)$ into the constraints, which takes $O(n_{\text{fix}} nm)$ time. We thus have proven the following lemma.

Lemma 7.7. Let $G \leq \mathcal{S}_n$ be the symmetry group of an integer program $\min_{x \in P \cap \mathbb{Z}^n} \langle c, x \rangle$. If G has a finite fundamental core set, then this integer program can be solved by $|\operatorname{fcore}(G)|$ many integer programs in dimension $n_{\text{fix}} := \dim \operatorname{Fix}(G)$. The constraints of each of these subproblems can be computed from the original constraints in $O(n_{\text{fix}} nm)$ time.

This method is an improvement over the algorithm presented in the last section because it is guaranteed to terminate, regardless of the input. Its drawback is that there may be very many subproblems to solve. In general we also have to solve all of them. Instances like Example 7.6 show that we have no control about the best attainable objective value for each IP. However, the method is strong enough to yield the following asymptotic complexity result for a special class of groups. This result was also independently discovered by Herr [Her13b, Thm 5.30].

Proposition 7.8. Let n_{fix} be a fixed positive integer. Let $G = \bigtimes_{i=1}^{n_{\text{fix}}} \mathcal{S}_{k_i}$ be a direct product of symmetric groups. Every integer linear program with symmetry group G can be solved in polynomial time for fixed n_{fix}.

Proof. Consider an integer program with n variables, m constraints and symmetry group $G = \bigtimes_{i=1}^{n_{\text{fix}}} \mathcal{S}_{k_i}$; in particular, $n = \sum_{i=1}^{n_{\text{fix}}} k_i$. By Lemma 7.7 we can solve this IP by solving $|\operatorname{fcore}(G)|$ many IPs in dimension $n_{\text{fix}} := \dim \operatorname{Fix}(G)$. We obtain each of these subproblems by a polynomial algorithm from the original problem. Moreover, by Lenstra's result [Len83] (see also [Sch98, Sec 18.4]), there is a polynomial algorithm to solve integer programs in the fixed dimension n_{fix}. Using this polynomial algorithm for our subproblems, it remains to show two things to prove the proposition. First, the number of subproblems is polynomial in our input. Second, the (encoding) size of every subproblem is polynomial in our input.

To address the first part we compute the size of a fundamental core set. By Remark 3.34 we know that

$$\left| \operatorname{fcore}\left(\bigtimes_{i=1}^{n_{\text{fix}}} \mathcal{S}_{k_i} \right) \right| = \prod_{i=1}^{n_{\text{fix}}} k_i \leq \left(\frac{n}{n_{\text{fix}}} \right)^{n_{\text{fix}}} .$$

The bound on the right-hand side is polynomial in n because n_{fix} is fixed. Thus, the number of subproblems in Lemma 7.7 is polynomial in the input. For the second part, the (encoding) size of every subproblem, observe again that we obtain each subproblem by a polynomial algorithm from the original problem. Hence, every subproblem has polynomial size. This completes the proof of the proposition. □

Remark 7.9. Fischetti & Liberti [FL12] solve the problem $\min_{v \in \operatorname{Fix}_{\mathbb{Z}}(G) \cap P} \langle c, v \rangle$ for a symmetry group G in order to obtain an upper bound on the optimal solution. Especially, if the symmetry group is transitive (as it is the case for many classical problems by Margot [Mar03]), then it makes sense to use a subgroup of the whole group, which is what Fischetti *&* Liberti also propose under the name orbital shrinking.

7.2.3. Inequalities for core sets

We now look at a third way to find an optimal integral point in the intersection $\mathrm{core}_{/}(G) \cap P$. A natural way to model this problem in integer programming would be to find inequalities that describe the set $\mathrm{core}_{/}(G)$ and add these as constraints. Since $\mathrm{core}_{/}(G)$ is an infinite set, it is not clear whether such inequalities exist at all. We can reduce this question to the fundamental core set because we have the following decomposition into a Minkowski sum

$$\mathrm{conv}\,\mathrm{core}_{/}(G) = \mathrm{Fix}(G) + \mathrm{conv}\,\mathrm{fcore}(G).$$

If the fundamental core set is finite, there is a finite facet description for the convex hull of $\mathrm{fcore}(G)$ and thus also of $\mathrm{core}_{/}(G)$. However, if the fundamental core set is infinite, then meaningful inequalities do not necessarily exist. The core set may cling to invariant subspaces which together with the fixed space span the whole space $\mathbb{R}^n$. For instance, for the cyclic group $\mathcal{C}_4$, we know by Example 5.26 that

$$\begin{aligned}\mathrm{core}_{/}(\mathcal{C}_4) - e^{(1)} \supseteq{} & \left(\begin{pmatrix}0\\1\\0\\-1\end{pmatrix} + \mathrm{span}_{\mathbb{Z}}\begin{pmatrix}1\\0\\-1\\0\end{pmatrix}\right) \cup \mathrm{span}_{\mathbb{Z}}\begin{pmatrix}0\\1\\0\\-1\end{pmatrix}\\ & \cup \mathrm{span}_{\mathbb{Z}}\begin{pmatrix}1\\-1\\1\\-1\end{pmatrix} \cup \mathrm{span}_{\mathbb{Z}}\begin{pmatrix}1\\1\\1\\1\end{pmatrix}\end{aligned}$$

which shows that $\mathrm{conv}\,\mathrm{core}_{/}(\mathcal{C}_4) = \mathbb{R}^4$. Here $\mathrm{span}_{\mathbb{Z}}(v) = \{kv \ : \ k \in \mathbb{Z}\}$ denotes the integer span of a vector. Suppose for the remainder of this section that the fundamental core set is finite and we are thus theoretically guaranteed that an inequality description of $\mathrm{fcore}(G)$ exists. We also focus on transitive groups; the result can be generalized to direct products. Note that $\mathrm{fcore}(G)$ is by definition a set of representatives, so for practical computations we have to decide how to select representatives. For the alternating and symmetric groups this choice is easy.

Proposition 7.10. A set of core point representatives for the symmetric group $\mathcal{S}_n$ and the alternating group $\mathcal{A}_n$ is given by

$$\mathrm{core}_{/}(\mathcal{A}_n) = \mathrm{core}_{/}(\mathcal{S}_n) = \{x \in \mathbb{Z}^n \ : \ x_i \leq x_{i+1} \text{ for all } 1 \leq i \leq n-1, \text{ and } x_n \leq x_1 + 1\}.$$

Proof. The integral points that satisfy the inequalities on the right all lie in the set

$$\left\{ k\mathbb{1} + \sum_{i=m}^{n} e^{(i)} \ : \ k \in \mathbb{Z},\ m \in [n] \right\}.$$

All of these are core points for $\mathcal{A}_n$ and $\mathcal{S}_n$ and no two of these lie in the same orbit. □

Remark 7.11. For integer programs this tightens the folklore inequalities

$$x_1 \leq x_2 \leq \cdots \leq x_n,$$

which describe a fundamental domain for $\mathcal{S}_n$ and are often used to break symmetry.

In this case the inequality description is optimal in the sense that the contained integral points make up $\mathrm{core}_{/}(G)$. It is not clear if something similar can be achieved for other groups. Let $R := \mathrm{core}_{/}(G)$ be a fixed selection of core set representatives. In general it is not clear whether the optimal case $(\mathrm{conv}\, R) \cap \mathbb{Z}^n = R$ can be achieved or which choice of R minimizes the overhead. An idea could be to select R so that it is contained in a fundamental domain of the group (see also [Fri07]). This would at least ensure that all points in R lie close together.

Besides this issue regarding the approximation quality, there is also the problem of actually computing the facets. If there are many representatives, obtaining all facets may take a long time. This already happens for some of the groups for which we computed a fundamental core set in Chapter 4. For instance, for the group 11-4 with $|\mathrm{fcore}(G)| = 445$ neither [cdd] nor [lrs] are able to compute all facets in a reasonable amount of time. So it remains an open question whether there are more groups than the alternating and symmetric groups where $\mathrm{core}_{/}(G)$ can be efficiently described or approximated by inequalities.

7.2.4. Parametrization of core sets

If no inequality description of the core set is known, there is still another way to integrate core sets into problems to make them available to standard solvers. By a variable transformation and adding some inequalities, the core set can be encoded if the group has a finite fundamental core set. As we have seen before, the core set can be written as a sum

$$\mathrm{core}_{/}(G) = \{u + z \ : \ u \in \mathrm{Fix}_{\mathbb{Z}}(G), z \in \mathrm{fcore}(G)\} \tag{7.3}$$

Let $f^{(1)}, \dots, f^{(n_{\mathrm{fix}})}$ be a basis for the lattice $\mathrm{Fix}_{\mathbb{Z}}(G)$. If the fundamental core set is finite, we can write (7.3) as

$$\mathrm{core}_{/}(G) = \left\{ \sum_{i=1}^{n_{\mathrm{fix}}} l_i f^{(i)} + \sum_{b \in \mathrm{fcore}(G)} \lambda_b b \ : \ l_i \in \mathbb{Z}, \lambda_b \in \{0,1\}, \sum_{b \in \mathrm{fcore}(G)} \lambda_b = 1 \right\}. \tag{7.4}$$

This trivial reformulation can be slightly improved by removing the overlap between $\mathrm{fcore}(G)$ and $\mathrm{Fix}_{\mathbb{Z}}(G)$. First we look at the transitive case. If G is a transitive group, then $\mathrm{fcore}(G)$ contains exactly one multiple of $\mathbb{1}$. Excluding this representative from the sum, we obtain

$$\mathrm{core}_{/}(G) = \left\{ l\mathbb{1} + \sum_{b \in \mathrm{fcore}(G) \setminus \mathrm{Fix}_{\mathbb{Z}}(G)} \lambda_b b \ : \ l \in \mathbb{Z}, \lambda_b \in \{0,1\}, \sum_{b \in \mathrm{fcore}(G) \setminus \mathrm{Fix}_{\mathbb{Z}}(G)} \lambda_b \leq 1 \right\}. \tag{7.5}$$

If we optimize over a set $\{x \in \mathbb{Z}^n \ : \ Ax \leq b\}$, we can replace the x-variables by new variables $(l, \lambda_1, \dots, \lambda_F)$ with $F := |\mathrm{fcore}(G)| - 1$. The transformed problem has one general integer variable, $F-1$ binary variables and one more constraint (for the sum of the λ_b) than the original problem. This generalizes naturally to direct products of transitive groups. In particular, for a direct product of symmetric groups we obtain the following result.

Proposition 7.12 ([HRS13])**.** For a positive integer j let $c(j) := \sum_{i=1}^{j} e^{(i)}$ be a sum of standard basis vectors. An integer program with symmetry group $\bigtimes_{i=1}^{n_{\text{fix}}} \mathcal{S}_{k_i}$ is feasible with an optimal solution z if and only if there are integers $l_i \in \mathbb{Z}$ and $\lambda_{i,j} \in \{0,1\}$ for every $i \in [n_{\text{fix}}]$ and $j \in [k_i]$ such that

$$z = \bigoplus_{i=1}^{n_{\text{fix}}} \left(l_i \mathbb{1}_{k_i} + \sum_{j=1}^{k_i-1} \lambda_{i,j} c(j) \right)$$

under the constraints $\sum_{j=1}^{k_i-1} \lambda_{i,j} \leq 1$ for each $i \in [n_{\text{fix}}]$. The dimension of the vector $c(j)$ shall be k_i, depending on the summand in which it is used.

Proof. This proposition follows immediately from (7.5), using $\operatorname{fcore}(\mathcal{S}_{k_i}) = \{c(1),\dots,c(k_i)\} = \{c(1),\dots,c(k_i-1)\} \cup \{\mathbb{1}_{k_i}\}$ as seen in Remark 3.33. □

While performing a variable transformation according to Proposition 7.12, we easily spot redundant inequalities because we may assume that they are block-wise lexicographically maximal (see [HRS13] for details). As observed by Herr [Her13a], the number of variables can be lowered substantially by using a logarithmic encoding. For positive integers $j \leq \lfloor \log_2(n) \rfloor + 1$ let

$$d(j,n) := \sum_{i=2^{j-1}}^{\min(2^j-1,n)} e^{(i)} \in \mathbb{Z}^n.$$

Then we can parametrize the fundamental core set of a symmetric group as

$$\operatorname{fcore}(\mathcal{S}_n) = \left\{ \sum_{i=1}^{\lfloor \log_2(n) \rfloor + 1} \lambda_j d(j,n) \;:\; \lambda_j \in \{0,1\} \right\}. \tag{7.6}$$

Using this parametrization transforms a problem with n integer variables and symmetry group $\mathcal{S}_n$ into a problem with one integer and $\lfloor \log_2(n) \rfloor + 1$ binary variables and possibly one additional constraint on the sum of the λ_j to exclude $\mathbb{1}$. Again, this generalizes naturally to direct products of symmetric groups and improves Proposition 7.12.

For most groups the trivial parametrization in (7.5), which necessitates $|\operatorname{fcore}(G)|$ variables, is not very efficient. Moreover, it does not work for groups with an infinite fundamental core set. However, the case (7.6) shows that only some kind of encoding size matters. For instance, for the maximal imprimitive groups from Section 5.3.4 with infinite fundamental core set, the fundamental core set is very close to one invariant subspace, so it can be parametrized like a direct product of symmetric groups (cf. (5.26) and Example 5.34).

Question 7.13. Are there other "efficient" parametrizations for core sets? How can infinite fundamental core sets be parametrized?

7.2.5. Limitations

Before we look at results of computational experiments in the next section, we discuss two theoretical limitations of the presented ideas. First, for 0/1-problems none of the presented core-set based algorithms has a theoretical advantage over known techniques for symmetric integer programming. Since the relevant part of the core set is just the set of all solutions with symmetry removed, restricting to the core set amounts only to plain symmetry removal, which techniques like orbital branching, isomorphism pruning and symmetry-breaking inequalities do as well. We will see that there can nevertheless be positive side effects of the parametrization for binary problems in Section 7.4.3.

Second, there are – from an optimization perspective interesting – groups, for which the core set is hard to describe. As already mentioned in Section 6.2.2, diagonals of symmetric groups are important in optimization since they occur if columns of a matrix-type variable (e.g., colors in a graph coloring problem) can be permuted. Kaibel & Pfetsch [KP08] presented symmetry-breaking inequalities for these kind of symmetries. The core sets of these diagonals, however, do not seem to be exploitable for optimization. For instance, for diagonals of symmetric groups of order two, Example 6.5 shows that the core set differs from a fundamental domain only by some $\gcd$/divisibility-condition, which is hard to enforce in integer programming. This also shows that the core set of diagonals cannot be approximated like fundamental domains. A fundamental domain on one orbit already is a fundamental domain for the whole diagonal. However, the core set of a diagonal $G \cong \mathcal{S}_n$ is not related to the "restriction" $\operatorname{core}(\mathcal{S}_n) \times \mathbb{Z}^n$.

7.2.6. Computational experiments

This section is a slightly updated version of [HRS13, Sec 7.1].

To assess the practical feasibility of our proposed algorithms, we implemented prototypes of some of the ideas and algorithms from Section 7.2. We compared fiber enumeration (Section 7.2.1), symmetry breaking inequalities (Section 7.2.3) and a parametrization (Section 7.2.4).

To apply the enumeration algorithm the problem must not be too big. Since we enumerate lattice points in the dimension n_{fix} of the fixed space, the value of n_{fix} should not exceed about ten to remain tractable. At the same time we have explicit complete core set descriptions for symmetric and alternating groups. We therefore focus on problems with symmetry groups which are the product of ten or less symmetric groups. Since we are not aware of problem instances in the literature meeting these conditions, we constructed problems ourselves.

We created random instances by the following scheme, using [PermLib] and [polymake]. For different values n_{fix} less than ten and different values of $k_1, \dots, k_{n_{\text{fix}}} \in \mathbb{Z}_{>0}$ we constructed IPs in dimension $n = \sum_{i=1}^{n_{\text{fix}}} k_i$ and with symmetry group $G = \mathcal{S}_{k_1} \times \cdots \times \mathcal{S}_{k_{n_{\text{fix}}}}$. We generated $3n$ inequalities $\langle a, x \rangle \leq b$ where

$$a = \bigoplus_{i=1}^{n_{\text{fix}}} f_i \left(\sum_{j=1}^{k_i} a_{i,j} x_j \right) .$$

Here the f_i were chosen independently uniformly at random from the set $[20]$. The $a_{i,j}$ were zero with probability 0.1 and otherwise selected uniformly at random from the set

$\{5, \ldots, 15\}$. The right hand side b was set to $\lfloor 0.95 \cdot \langle a, \mathbb{1} \rangle \rfloor$. Finally, all inequalities in the orbit of G were added and the domain of all variables set to $\mathbb{Z}_{\geq 0}$. Additionally, to exclude the zero vector, we added the inequality $\sum_{i=1}^{n} x_i \geq 1$. The objective function c was chosen as $c_1 \mathbb{1}_{k_1} \oplus \cdots \oplus c_{n_{\text{fix}}} \mathbb{1}_{k_{n_{\text{fix}}}}$ where the c_i were chosen independently uniformly at random from the set $[10]$.

Since the constraint matrix is densely filled with many different coefficients, the number of inequalities grows in the same magnitude as the order of G, which in turn grows very quickly with n_{fix} and the k_i. Therefore, we conducted our experiments only for selected values of these parameters. For each $n \in \{10, 12, 15, 18\}$ we tried to find three different groups G each such that the number of constraints was comparable for different n. We selected the parameters n_{fix} and k_i so that we had one small instance and two large instances, the latter ones with different dimension n_{fix} of the fixed space. The average ratio of non-zeros in the instances was about 90%, as was to be expected from the choice of random variables.

After the description of the optimization problems we now turn to the algorithms and their implementation. For the fiber enumeration from Section 7.2.1 we use SCIP 2.0.1 [SCIP] to enumerate all lattice points of the projected polyhedron. Since we compare running times with commercial solvers which do not use exact arithmetic, this is a viable alternative to other lattice enumeration tools like [LattE] or [Normaliz]. Each enumerated point corresponds to a fiber. The integer feasibility of these fibers is tested by using core points. Currently, our knowledge of core sets of groups beyond the alternating and the symmetric group and their direct products is limited. Therefore we only implemented integer feasibility checks for these groups. This core point check is realized in a dedicated program written in C++, which reads a polyhedron and a list of fibers. It either returns an optimal fiber or reports that the input is infeasible.

For the parametrization from Section 7.2.4 we wrote a pre-processing script that applies a variable transformation as in Proposition 7.12. Note that while doing so we can eliminate all but one inequality from each orbit and thus obtain problems with n variables and $3n$ inequalities (cf. [HRS13, Sec 6]). As we will see later, this simplifies matters drastically.

Table 7.1 shows the average results for ten randomly generated instances for every set of dimension parameters. We performed the experiments on an Intel Core-i7 machine with eight logical CPUs at 2.8 GHz and 16 GB RAM. We ran our tests with Gurobi 5.5.0 [Gurobi] and our own fiber/core set-prototype. We used the commercial solvers with their default settings and allowed eight threads. The column “default” shows the running time of Gurobi for the original problem. The columns “FD” and “FDcore” contain the running time after adding inequalities according to Remark 7.11 and Proposition 7.10, respectively. The last column “FibEnum” shows the running time of our prototype.

The results show that our fiber enumeration prototype is faster than the commercial solvers on almost all of these instances. We can also observe that the running time of our prototype increases significantly with n_{fix} because we have to enumerate lattice points in this dimension. The input to our prototype included the symmetry group of the problem, so it did not have to be determined. The symmetry-breaking inequalities “FD” and “FDcore” often have some advantage over the default model. Whether the tighter inequalities “FDcore” are better seems to depend on the problem.

Table 7.1.: Running times in seconds on random symmetrized instances, averaged on 10 runs each

				Gurobi			
Groups	n	n_{fix}	#rows	default	FD	FDcore	FibEnum
$(\mathcal{S}_5)^2$	10	2	182151	30.71	21.11	24.02	0.25
$\mathcal{S}_5 \times \mathcal{S}_3 \times \mathcal{S}_2$	10	3	23204	3.22	2.58	2.65	0.05
$\mathcal{S}_8 \times (\mathrm{id})^2$	10	3	342289	67.83	45.03	46.55	0.47
$(\mathcal{S}_4)^3$	12	3	217273	40.31	36.96	36.64	0.36
$(\mathcal{S}_3)^4$	12	4	28353	4.08	4.01	4.02	0.07
$\mathcal{S}_6 \times \mathcal{S}_4 \times (\mathrm{id})^2$	12	4	236001	46.29	37.55	35.91	0.37
$(\mathcal{S}_3)^5$	15	5	182366	41.58	36.24	35.83	0.41
$\mathcal{S}_3 \times (\mathcal{S}_2)^6$	15	7	11751	2.55	2.08	1.94	0.35
$(\mathcal{S}_5)^2 \times (\mathrm{id})^5$	15	7	267434	59.94	53.76	54.27	0.63
$(\mathcal{S}_3)^4 \times (\mathcal{S}_2)^3$	18	7	286732	89.09	75.72	66.99	1.48
$(\mathcal{S}_2)^9$	18	9	18854	5.18	4.41	4.21	4.72
$\mathcal{S}_5 \times \mathcal{S}_3 \times (\mathcal{S}_2)^4 \times (\mathrm{id})^3$	18	9	315501	45.50	41.30	40.63	5.63

We also tested a variable transformation according to Proposition 7.12 on these instances. This reduced the problems to instances with 60 or less inequalities in dimensions $\{10, 12, 15, 18\}$. Since these are in general easy problems for IP solvers, we always have obtained the optimal solution in less than 0.1 seconds regardless of the original problem size and the solver used. Because the variable transformation only requires a symmetry group consisting of symmetric groups and has no obvious limits on the problem size which it can be applied to, we also tested it on a real world problem; details can be found in Section 7.4.3.

7.3. Show case for Lenstra-type algorithms

In this section we look at an interesting by-product of infinite fundamental core sets. As all techniques of the previous sections (except possibly parametrization) require a finite fundamental core set, there is no known way to exploit core sets to solve symmetric integer programs involving infinite core sets. However, infinite fundamental core sets allow to create integer programming instances that are hard to solve with standard solvers. We also see that a well-known alternative technique nevertheless solves these problems quickly. The ideas of this section are based on joint work with Katrin Herr.

Let $G \leq \mathcal{S}_n$ be a primitive group that is not 2-homogeneous. As explained in Section 5.4, it can be computationally verified that for $n \leq 127$ every such group has infinitely many non-isomorphic core points. The corresponding orbit polytopes are simplices $T_m = \operatorname{conv} Gz^{(m)}$ (see Proposition 5.37). For such a simplex we can easily compute its facet description as follows. Let $A \in \mathbb{Z}^{n \times n}$ be the matrix that has the vertices $Gz^{(m)}$ as columns. For all $\lambda \in [0,1]^n$ with $\langle \mathbb{1}, \lambda \rangle = 1$ the point $A\lambda$ lies in T_m because it is a convex combination of the vertices. In other terms, the simplex T_m arises as intersection of the cone $\operatorname{cone} Gz^{(m)} = \operatorname{cone} A$ with the hyperplane $\{x \in \mathbb{R}^n \ : \ \langle \mathbb{1}, x\rangle = \left\langle \mathbb{1}, z^{(m)}\right\rangle\}$. Thus,

$$T_m = \{x \in \mathbb{R}^n \ : \ A^{-}x \geq 0 \text{ and } \langle \mathbb{1}, x\rangle = \left\langle \mathbb{1}, z^{(m)}\right\rangle\}$$

is an inequality description for the simplex. Note that by construction the point $z^{(m)}$ has exactly one coordinate with maximal value $M := \max_i z_i^{(m)}$. We therefore obtain an inequality description for $T'_m := (T_m \cap \mathbb{Z}^n) \setminus \operatorname{vert} T_m$, which denotes all non-vertex integral points in T_m, by

$$T'_m = \{x \in \mathbb{Z}^n \ : \ A^{-}x \geq 0 \text{ and } \langle \mathbb{1}, x\rangle = \left\langle \mathbb{1}, z^{(m)}\right\rangle \text{ and } x \leq M-1\}. \qquad (7.7)$$

Since we started with a lattice-free T_m, this set T'_m must be empty. The corresponding IP feasibility problem – given the constraints of (7.7), finding an integral point which satisfies them – usually is hard for branch&bound-based standard solvers as the following experiments show.

Before we get to these, we look at a slightly different way to solve the feasibility problem (7.7). By construction, the lattice-free orbit polytope T_m is flat in the direction of one the invariant subspaces. This suggests to try the algorithm behind Lenstra's famous complexity result [Len83], branching on hyperplanes. The same idea also was successfully used to solve other IP-feasibility problems of simplices which are known to be hard for branch&bound (see [AL04] for some of these instances and [GZ02] for a general computational report). The algorithm roughly works as follows.

The goal is to find an integer point in a polyhedron P or decide that no such point exists. We first try to find a direction $u \in \mathbb{Z}^n$ in which the polyhedron is flat. If there is no such direction, then by the flatness theorem (cf. Theorem 2.6) the polyhedron must contain an integer point and we are done. Having such a "flat" direction u, we compute $h_{\text{max}} := \max_{x \in P} \langle u, x\rangle$ and $h_{\text{min}} := \min_{x\in P} \langle u, x\rangle$. Since P is flat in direction u, the width $\omega(P, u) = h_{\text{max}} - h_{\text{min}}$ is not too large. We partition the polytope into slices $P \cap \{x \in \mathbb{R}^n \ : \ \langle u, x\rangle = h\}$ for $h \in \mathbb{Z}$ and $\lceil h_{\text{min}}\rceil \leq h \leq \lfloor h_{\text{max}}\rfloor$. We then solve these lower-dimensional subproblems recursively. This idea is particularly easy to apply to problem (7.7) because we already know directions in which the simplex T_m is flat by construction. Thus, almost only the slicing has to be implemented.

For the following computational experiments, branching on hyperplanes was implemented in [polymake]. Let V, W be two non-trivial invariant subspaces of a permutation group $G \leq \mathcal{S}_n$ such that $\mathbb{R}^n = \operatorname{span} \mathbb{1} \oplus V \oplus W$. By construction, the original polytope T'_m is flat in the direction of one of these subspaces, say W. All elements from the orbit of $C := Ge^{(1)}|_W$ are considered as candidates for the "flatness" direction u. Among these the direction with the smallest width $\omega(P, u') = \min_{u\in C} \omega(P, u)$ is chosen and the corresponding subproblems are created. Note that for the original polytope T'_m the width is the same for all directions due to symmetry, so we may start with an arbitrary $u \in C$. However, for the subproblems differences occur since the set C is not an orthogonal basis for W. At recursion depth two, all feasibility problems are solved directly with Gurobi. The threshold of two levels to abort recursion seems to be a reasonable choice for the tested problems since most of these subproblems are solved by Gurobi instantly.

Table 7.2 shows the results for testing IP feasibility in (7.7) with Gurobi and the hybrid polymake/Gurobi-approach. The groups used for these experiments are the primitive groups with GAP-ids 15-2, 16-10, 21-1 (cf. Section 2.2), but any primitive, non 2-homogeneous group would do as well. For these groups integer feasibility problems with n variables and $n+1$ linear constraints with $n \in \{15, 16, 21\}$ are built using (7.7). The underlying polytopes T_m are the orbit polytopes of $z^{(m)} = e^{(1)} + me^{(1)}|_V$ where V is an invariant subspace of the group and $m \in \mathbb{Z}$ is a scalar that makes $z^{(m)}$ integral. For each group two different choices of m and both of the two invariant subspaces are tested. The main effect of the choice of m is the absolute size of the coefficients in the constraint matrix A^-. In the table the group id consists of the degree of the group followed by the dimension of the subspace which plays the role of V. For both methods the sum of nodes in the Gurobi B&B-tree over all subproblems and the total time is given; for the hybrid methods the number of calls to Gurobi is shown as well. All experiments were conducted on an Intel Core-i7 machine with eight logical CPUs at 2.8 GHz and 16 GB RAM. Gurobi was used in version 5.5.0 with four parallel threads, default settings and a time limit of three hours.

Table 7.2.: IP feasibility for orbit polytopes of primitive groups

		Gurobi		polymake & Gurobi		
Id	$\max \lvert A^-_{ij} \rvert$	#nodes (10^6)	time (s)	#nodes (10^6)	time (s)	#subp.
15(5)	2851	252.0	6017.5	0.0	10.7	29
15(5)	11101	387.6	>10800.0	0.3	16.9	29
15(9)	2053	0.0	0.7	0.0	54.3	456
15(9)	7993	0.3	23.8	0.0	63.4	456
16(6)	2749	102.1	1905.2	0.0	6.4	24
16(6)	10681	548.7	>10800.0	0.0	6.5	24
16(9)	2713	0.4	21.9	0.0	38.2	280
16(9)	6013	3.3	96.9	0.0	39.3	280
21(8)	9352	35.7	1609.1	3.3	120.6	22
21(8)	36847	216.4	>10800.0	200.2	6765.7	22
21(8)	36847	216.4	>10800.0	[a] 69.6	[a] 1944.0	[a] 27
21(12)	287	1.0	57.1	0.2	34.8	150
21(12)	2155	242.9	>10800.0	74.8	3368.5	150
21(12)	2155	242.9	>10800.0	[a] 29.5	[a] 828.9	[a] 349

[a] with one additional recursion level in polymake (depth three instead of two)

The numbers in Table 7.2 show that some of the problems are quite hard to solve for Gurobi before reaching the time limit. In the dimensions 15 and 16 branching on hyperplanes is able to detect infeasibility very fast. In dimension 21 a few of the subproblems are still difficult to solve which results in much longer running times. These can be reduced to some extent by increasing the recursion threshold before handing the problems over to Gurobi. Interestingly, the subspace V that is used in the projection seems to have a big influence. The problems where V has the larger dimension seem to be much easier for Gurobi. Conversely, if there are many branching hyperplanes, this leads to many subproblems which take quite long to be created in polymake. A possible explanation for this behavior is that the closer the problem is to a "full-dimensional" (meaning fewer dimensions in which it is flat), the easier it is to handle by Gurobi.

The experiments in this section show that there are integer feasibility problems which are hard to solve for standard solvers like Gurobi. These problems also may serve as a case study for the potential of methods that exploit geometric information as branching on hyperplanes does.

7.4. MIPLIB 2010 symmetries

This section is based on joint work with Marc Pfetsch and the resulting article [PR13]. We first study graph-based algorithms to compute the symmetry group of an integer program. Then we apply these to compute the symmetries of the MIPLIB 2010 collection [KAA$^+$11] and analyze the results with a focus on the applicability of core set-based algorithms.

7.4.1. Algorithms for computing symmetries of IPs

Computing the symmetry group is usually reduced to the determination of graph automorphisms, see, e.g., [Mar10]. Although the computational complexity of the latter problem is still unknown (it is neither known to be NP-hard, nor known to be solvable in polynomial time), there are many tools which compute graph automorphisms efficiently even for large graphs, e.g., [nauty], [saucy], and [bliss].

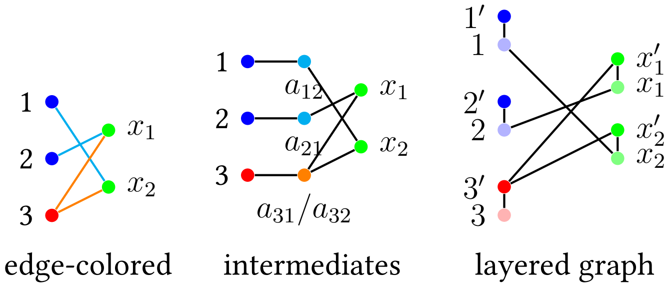
A natural way (folklore knowledge) to model MIP symmetries as graph automorphisms is via the following bipartite graph $G = (V \dot{\cup} V', E)$ with vertex and edge colors. The set $V = \{v_1, \dots, v_n\}$ contains a vertex v_j for each variable x_j of the problem; v_j is colored according to the objective coefficient c_j of variable x_j. The second set $V' = \{v'_1, \dots, v'_m\}$ contains a vertex for each linear inequality in $Ax \leq b$. Each vertex v'_i is colored with respect to the coefficient b_i of the right-hand side. There is an edge $\{v'_i, v_j\} \in E$ if $A_{ij} \neq 0$, and it is colored by the coefficient A_{ij} of variable x_j in the i-th constraint. Moreover, we use colors to distinguish vertices in V that belong to variables with and without integrality restrictions. Every color preserving automorphism of G which permutes variable-vertices corresponds to a MIP symmetry and vice versa. (The problem formulation may contain redundant rows, which results in automorphisms that fix all variable-vertices.)

Note that 0-coefficients play a special role in this construction. Of course, we can replace 0 by any other number. However, the matrices appearing in MIPs are often sparse. In this case, the choice of 0 as special coefficient reduces the number of edges in the graph and speeds up the symmetry computation.

The above mentioned graph automorphism software packages can only handle vertex colors. In fact, edge colors are not needed if A contains only one coefficient different from 0, e.g., if A is a $0/1$-matrix. In the other cases, one can reduce the problem to a purely vertex-colored instance by applying one of two techniques that we describe in the following.

Salvagnin [Sal05] discusses a transformation in which every edge $\{v', v\} \in E$ is replaced by two edges $\{v', w\}$, $\{w, v\}$, using an intermediate vertex w that is colored with the original edge color. The number of newly introduced vertices can often be substantially reduced by an idea of Puget [Pug05]. Instead of adding new intermediate vertices

$$A = \begin{pmatrix} 0 & 1 \\ 1 & 0 \\ 2 & 2 \end{pmatrix} \quad b = \begin{pmatrix} 1 \\ 1 \\ 2 \end{pmatrix} \quad c = \begin{pmatrix} 1 \\ 1 \end{pmatrix}$$



edge-colored intermediates layered graph

Figure 7.2.: Example for the reduction of symmetry computation with respect to (A, b, c) to graph automorphisms.

for all edges, vertices with the same color can be combined. For each $v_i' \in V'$ let $V_{i,c} \subseteq V$ be the set of vertices which are incident to v_i' with an edge of color c. Then it is enough to introduce one intermediate c-colored vertex w with edges to v_i' and to all elements of $V_{i,c}$. We call this construction **grouping by variables**. In many MIP-instances, each constraint contains only few distinct variable coefficients. In this case, the sets $V_{i,c}$ are large, and the number of vertices in the graph is significantly reduced. The resulting graph is similar to Liberti's expression DAG construction [Lib12]. Depending on the distribution of coefficients, it may be beneficial to swap the roles of constraints and variables to add as few intermediate vertices as possible. For instance, if there are much more constraints than variables, it may help to add one intermediate vertex between each v_i and the set $V_{i,c}' \subseteq V'$ of all constraint-vertices connected to v_i by an edge of color c. We call this construction **grouping by constraints**. Because our original graph is bipartite, both groupings are possible. In the following we refer to either of these constructions as **graph with intermediates**; see Figure 7.2 for an example. The underlying graph construction can also be generalized to signed permutations as described by Bödi, Herr & Joswig [BHJ13].

The second, fundamentally different transformation, is described in the manual of the software [nauty]. Since it does not depend on bipartiteness, we describe it for a general edge-colored graph $G = (V, E)$. Let C be the total number of distinct edge colors in G, and let $L = \lceil \log_2 C \rceil$ be the number of bits needed to represent C. We introduce new vertex colors $\{C_1, \dots, C_L\}$ and replace each vertex $v \in V$ with vertices $v_1, \dots, v_L$ that are colored with $\{C_1, \dots, C_L\}$, respectively. Additionally, we add edges $\{v_1, v_2\}$, $\{v_2, v_3\}$, …, $\{v_{L-1}, v_L\}$. For each edge $\{v, w\} \in E$ with color c of the original graph, we add edges between v_i and w_i for every i-th bit that is 1 in the binary representation of c. Thus we emulate the edge colors by vertex bit colors. We refer to this construction as **layered graph**; see Figure 7.2 for an example.

The graph with intermediates has $m + n + O(N)$ vertices, where N is the number of nonzeros in A. Depending on the distribution of different coefficients in the constraint matrix, the last part may be much smaller than N. The layered graph results in about $(n + m) \log_2(C)$ vertices, where C is the total number of distinct coefficients in the constraint matrix. Depending on the instance, either transformation might lead to a smaller graph. Thus, no construction dominates the other. We report on experience with graph sizes for practical instances in Section 7.4.2.

In every symmetry computation it is important to take numerical issues into account. For a very simple example, consider three matrix coefficients α, β, γ, such that α and β as well as β and γ are numerically equal (e.g., $|\alpha - \beta| \leq \varepsilon$, $|\beta - \gamma| \leq \varepsilon$ for some zero tolerance ε), but α and γ are not equal. Thus, the loss of transitivity has to be taken into account in order to avoid wrong symmetry computations. One method, also used by Salvagnin [Sal12], is to first sort all coefficients, say of A, non-decreasingly. Then passing through the sorted list, a new color for A_{ij} is used whenever $|A_{ij} - \delta| > \varepsilon$, where δ is the minimal coefficient belonging to the last used color. In this way, we have a stable behavior, but might consider two coefficients as different that are still numerically equal. Thus, we might compute a subgroup of the "real" symmetry group.

7.4.2. A brief survey of MIPLIB 2010 symmetries

In this section we survey the symmetries of MIPLIB 2010 problems [KAA$^+$11]. For the predecessor MIPLIB 2003 the symmetry groups were analyzed by Liberti [Lib12].

We implemented the two algorithms described in the previous section to construct the vertex-colored graphs whose automorphism group corresponds to the symmetry group of the MIPs. As a heuristic for the decision of whether to group by variables or by constraints in the graph with intermediates, we used the ratio of constraints to variables. We group by variables whenever there are more variables than constraints. For the experiments in this section we realized the graph constructions in a Python program. The output of this tool was a graph description that we fed into [bliss]. We then performed a rough analysis of the symmetry group we obtained from bliss.

Using [PermLib], we analyzed the structure of this symmetry group G. In a first pass we attempted to identify as many maximal symmetric subgroups as possible. This can efficiently be performed by looking only at those generators of G that are transpositions. In a second pass, we performed a more detailed analysis, checking for all symmetric groups and cyclic groups both in their natural action and as diagonals (cf. Section 6.1).

From the 361 problems in the complete MIPLIB 2010, we excluded the four largest hawaiiv10130, ivu06-big, zib01, and zib02 because the 16GB RAM on the test machine did not suffice. For the remaining 357 instances, we constructed the graphs and applied the group analysis as described above. Before presenting details about the groups, we compare the graph constructions.

For almost all instances, the graph with intermediates, using the simple grouping heuristic mentioned above, was smaller than the corresponding layered graph. In three of six other cases, the graph with intermediates could be made smaller than the layered graph by switching the grouping strategy. For the remaining three instances in, mik-250-1-100-1, and neos-916792, the layered graph was always the smaller one. It should be noted though that the number of edges also plays a role when computing graph automorphisms. For all tested instances the layered graph had at least as many edges as the graph with intermediates, in rare cases eight times more. Nevertheless, for the in problem bliss was 8 seconds (20%) faster on the layered construction. We also implemented the graph constructions in [SCIP] as C++ module for optimal speed, again

Table 7.3.: Times for MIPLIB 2010 (without unstable & xxl) symmetry detection; times geom. mean[s]

Parameters			w/ sym. (#201)			w/o sym. (#130)	
group	presol	graph	graph time	total time	fails	graph time	fails
full	init	layered	3.38	4.09	9	1.28	1
full	init	interm.	2.65	3.40	9	1.16	1
full	presol	layered	1.69	1.77	0	1.16	0
full	presol	interm.	1.49	1.59	0	1.07	0
heur	init	layered	2.26	2.26	7	1.24	1
heur	init	interm.	2.26	2.32	2	1.13	1
heur	presol	layered	1.42	1.42	0	1.17	0
heur	presol	interm.	1.32	1.32	0	1.07	0

using bliss for computing graph automorphisms. Table 7.3 shows the running times for symmetry detection in SCIP with different parameter settings. The column "group" states whether only symmetric groups were detected by a transposition heuristic (heur) or if the full group was computed (full). The column "presol" shows if symmetry was computed before (init) or after presolving (presol) The column "graph" lists the underlying graph construction. The "graph time" is the time required for graph construction and automorphism computation with bliss. The "total time" includes time needed by PermLib to process the bliss output and make it available for further computations. Overall, the graph with intermediates seems to be the fastest solution.

We now look at the analysis of the computed symmetry groups. At least 208 of the 361 MIPLIB instances have a non-trivial symmetry group. The complete list is included in Appendix A. The degree of symmetry ranges between a group of order 2 on 235 146 variables (sing245) and groups of order 10^{54600} on about 74 000 variables (t1717). We split the computed symmetry groups into components and analyzed their types. Almost all factors are $\mathcal{S}_n$ in their natural actions on coordinates, some factors are diagonals of symmetric groups. About 500 factors out of about 200 000 could not be determined. No cyclic groups (other than $\mathcal{S}_2$) were detected.

For 201 of the 357 examined MIPLIB 2010 instances, a complete symmetry group was found by the fast heuristic that only looks at transpositions to recognize symmetric groups. That is, the symmetry group of these instances is either trivial or is a direct product of $\mathcal{S}_k$'s in their natural permutation representation.

In order to analyze the amount of symmetry that has to be actually dealt with when solving a problem, we also analyzed the symmetries of presolved instances of SCIP and Gurobi. After presolving, 181 (SCIP) and 144 (Gurobi) instances still have a non-trivial symmetry group. In most cases, the order of the symmetry groups is significantly reduced by presolving. To put this reduction into numbers we can look at the geometric mean of $\log_{10}|G|$ over all non-trivial groups. This value is about 64, 16, and 8.6 for the original, SCIP-presolved, and Gurobi-presolved problems, respectively. Thus, in many cases symmetries in MIPs occur in such a way that they can be eliminated by presolving. On the other hand, for some problems presolving added symmetry to the problem (cf. n[349]-3).

7.4.3. Toll!

This section is based on joint work published in [HRS13, Sec 7.2], which we have already seen parts of in Section 7.2.6.

Since the variable transformation from Section 7.2.4 has no obvious limits on the problem sizes it can be applied to, we looked for a real world problem to test it on. We searched the MIPLIB 2010 collection for a small problem whose symmetry group is large and consists to a large extent of a product of symmetric groups. One of the candidates that came up in the analysis (cf. Section 7.4.2) was toll-like, a then open $0/1$-problem with 4408 constraints in dimension 2883. Its symmetry group has $(\mathcal{S}_2)^{230}$ as a subgroup. After our transformation it had 4638 constraints, still in dimension 2883. However, the presolvers of CPLEX, Gurobi and SCIP were able to eliminate 230 variables, one for each $\mathcal{S}_2$ factor in the original problem. Moreover, the number of constraints could be reduced to 3948, which is 460 less than in the original problem. These reductions allowed us to solve this previously open problem with Gurobi 4.5.1 after about 4.5 days on our workstation from Section 7.2.6. Under the same conditions, solving the original, untransformed problem was not possible because both CPLEX and Gurobi ran into memory problems.

The following analysis of the toll-like symmetry is based on a hint of the anonymous referee of [HRS13]. The instance contains 230 pairs of variables x, y that appear in the following way:

$$\begin{aligned} x + R &\geq 0, \qquad & y + R &\geq 0, \\ x - R &\geq 0, \qquad & y - R &\geq 0, \end{aligned} \tag{7.8}$$

where R is some term in other variables. In this case we can aggregate x and y into a single variable. It is unclear why none of the tested solvers did perform this variable elimination that seems to be easily detectable without knowledge of core sets. The transformation described in Section 7.2.4 rewrites the constraints in such a way that solvers notice the redundancy in the model.

Since the problem contains only binary variables, the core set parametrization does not reduce the search space more than previously known techniques like symmetry-breaking inequalities (cf. Section 7.2.5). Therefore it is an interesting question whether MIPLIB instances contain $\mathcal{S}_k$-symmetries on general integer variables that are not eliminated by current presolvers. From the collaboration with Marc Pfetsch, parts of which are outlined at the beginning of this section, we had access to the symmetry groups of most MIPLIB 2010 instances before and after presolving of SCIP and Gurobi. There are only nine instances with symmetries on general integer (non-binary) variables: ds-big, eilB101, neos-1224597, ns1631475, ns1952667, ns2118727, ns2122603, rococoC10-001000, and rvb-sub. All these symmetries in the original formulation are removed by the presolver of Gurobi. However, presolving introduces new $\mathcal{S}_k$-symmetries on integer variables with non-binary bounds on five instances (atlanta-ip, biella1, dc1c, msc98-ip, nsr8k). Subsequently, only parts of these symmetries are eliminated by a manually enforced presolving step, although all of them seem to be of a similar type as (7.8), which allows aggregation.

A. Symmetry Groups of MIPLIB 2010 Instances

The following table lists details about the symmetry groups of MIPLIB 2010 instances. The second column shows the order of magnitude of the symmetry groups. The third column contains the percentage of variables that lie in an orbit of at least size two, i.e., variables on which the symmetry group acts non-trivially. The fourth column shows the groups which the symmetry group is a direct product of. The following notation is used.

- $\mathcal{S}_k$ denotes a symmetric group of degree k in its natural representation;
- $\hat{\mathcal{S}}_k$ denotes a diagonal of a symmetric group which is isomorphic to $\mathcal{S}_k$;
- ? stands for a group whose type could not be determined by [`PermLib`], i.e. the group is neither a cyclic or symmetric group in the natural representation nor a diagonal thereof.

For some optimization instances, only a subgroup of the full symmetry group could be analyzed. Numbers and factors are given for this subgroup.

Also note that the table lists only permutation symmetries. Some instances may have a bigger linear symmetry group in $\mathrm{GL}_n(\mathbb{Z})$ (see [BDP⁺12]).

name	$\log_{10} \lvert G \rvert$	vars	factors
30_70_45_095_100	1	0.0%	$\mathcal{S}_2$
acc-tight4	5	97.8%	?
ash608gpia-3col	1	100.0%	$\hat{\mathcal{S}}_3$
atlanta-ip	4450	40.5%	$(\mathcal{S}_2)^{5898}$, $(\mathcal{S}_3)^{1441}$, $(\mathcal{S}_4)^{284}$, $(\mathcal{S}_5)^{175}$, $(\mathcal{S}_6)^{165}$, $(\mathcal{S}_7)^{88}$
bab3	71	9.5%	$(\hat{\mathcal{S}}_2)^3$, $(\mathcal{S}_2)^{10}$, $(\mathcal{S}_5)^{16}$, $(\mathcal{S}_6)^4$, $(\mathcal{S}_{10})^2$, ?
bab5	2	17.9%	$(\hat{\mathcal{S}}_2)^4$
beasleyC3	1	0.6%	$(\hat{\mathcal{S}}_2)^2$
biella1	218	11.7%	$(\mathcal{S}_2)^{261}$, $(\mathcal{S}_3)^{30}$, $(\mathcal{S}_4)^{20}$, $(\mathcal{S}_5)^{13}$, $(\mathcal{S}_6)^2$, $(\mathcal{S}_7)^5$, $\mathcal{S}_8$, $(\mathcal{S}_9)^2$, $(\mathcal{S}_{10})^2$, $\mathcal{S}_{11}$
blp-ar98	1	0.0%	$(\mathcal{S}_2)^2$
blp-ic97	1	0.0%	$(\mathcal{S}_2)^2$
bnatt350	504	43.3%	$(\mathcal{S}_2)^{42}$, $(\mathcal{S}_3)^{81}$, $(\mathcal{S}_4)^{88}$, $(\mathcal{S}_5)^{76}$, $(\mathcal{S}_6)^{39}$, $(\mathcal{S}_7)^{10}$
bnatt400	588	43.6%	$(\mathcal{S}_2)^{50}$, $(\mathcal{S}_3)^{83}$, $(\mathcal{S}_4)^{98}$, $(\mathcal{S}_5)^{91}$, $(\mathcal{S}_6)^{42}$, $(\mathcal{S}_7)^{16}$, $\mathcal{S}_8$
cdma	912	91.2%	$\hat{\mathcal{S}}_{12}$, $(\mathcal{S}_{12})^{104}$
circ10-3	2	100.0%	?
co-100	736	6.3%	$(\mathcal{S}_2)^{837}$, $(\mathcal{S}_3)^{399}$, $(\mathcal{S}_4)^3$, $(\mathcal{S}_5)^3$, $\mathcal{S}_6$, $(\mathcal{S}_7)^2$, $\mathcal{S}_{12}$, $\mathcal{S}_{17}$, $\mathcal{S}_{19}$, $\mathcal{S}_{21}$, $\mathcal{S}_{28}$, $\mathcal{S}_{29}$, $\mathcal{S}_{30}$
core2536-691	4	0.1%	$(\mathcal{S}_2)^5$, $\mathcal{S}_5$
core4872-1529	69	2.0%	$(\mathcal{S}_2)^{211}$, $(\hat{\mathcal{S}}_2)^3$, $(\mathcal{S}_3)^2$, $\mathcal{S}_6$
cov1075	7	100.0%	?
datt256	4	0.0%	$(\mathcal{S}_2)^{12}$
dc1c	357	19.8%	$(\mathcal{S}_2)^{819}$, $(\mathcal{S}_3)^{64}$, $(\mathcal{S}_4)^{24}$, $(\mathcal{S}_5)^2$, $(\mathcal{S}_6)^8$
dc1l	795	11.4%	$(\mathcal{S}_2)^{1640}$, $(\mathcal{S}_3)^{174}$, $(\mathcal{S}_4)^{69}$, $(\mathcal{S}_5)^{18}$, $(\mathcal{S}_6)^9$, $(\mathcal{S}_7)^2$
dg012142	90	3.1%	$\mathcal{S}_{64}$

dolom1	469	19.4%	$(\mathcal{S}_2)^{907}$, $(\mathcal{S}_3)^{71}$, $(\mathcal{S}_4)^{25}$, $(\mathcal{S}_5)^{5}$, $(\mathcal{S}_7)^{2}$, $\mathcal{S}_{15}$, $\mathcal{S}_{33}$, $\mathcal{S}_{34}$
ds-big	469	1.8%	$(\mathcal{S}_2)^{1516}$, $(\mathcal{S}_3)^{15}$
eilB101	1	0.1%	$\mathcal{S}_3$
enlight13	1	92.3%	$\hat{\mathcal{S}}_2$
enlight14	1	92.9%	$\hat{\mathcal{S}}_2$
enlight15	1	93.3%	$\hat{\mathcal{S}}_2$
enlight16	1	93.8%	$\hat{\mathcal{S}}_2$
enlight9	1	88.9%	$\hat{\mathcal{S}}_2$
ex10	1	100.0%	?
ex1010-pi	1482	21.7%	$(\mathcal{S}_2)^{1324}$, $(\mathcal{S}_3)^{366}$, $(\mathcal{S}_4)^{148}$, $(\mathcal{S}_5)^{70}$, $(\mathcal{S}_6)^{32}$, $(\mathcal{S}_7)^{27}$, $(\mathcal{S}_8)^{20}$, $(\mathcal{S}_9)^{13}$, $(\mathcal{S}_{10})^{3}$, $(\mathcal{S}_{11})^{5}$, $\mathcal{S}_{12}$, $(\mathcal{S}_{16})^{2}$
ex9	31	100.0%	?
glass4	1	0.6%	$\mathcal{S}_2$
gmu-35-40	802	39.3%	$(\mathcal{S}_2)^{18}$, $(\mathcal{S}_3)^{16}$, $(\mathcal{S}_4)^{3}$, $(\mathcal{S}_5)^{3}$, $\mathcal{S}_{363}$
gmu-35-50	1838	44.5%	$(\mathcal{S}_2)^{18}$, $(\mathcal{S}_3)^{16}$, $(\mathcal{S}_4)^{3}$, $(\mathcal{S}_5)^{3}$, $\mathcal{S}_{742}$
gmut-75-50	**?**	?	?
gmut-77-40	40583	47.2%	$(\mathcal{S}_2)^{12}$, $(\mathcal{S}_3)^{7}$, $(\mathcal{S}_4)^{20}$, $(\mathcal{S}_5)^{31}$, $\mathcal{S}_{11198}$
go19	4	99.8%	$\mathcal{S}_4$, ?
iis-bupa-cov	3	2.0%	$\mathcal{S}_3$, $\mathcal{S}_4$
iis-pima-cov	36	4.2%	$\mathcal{S}_{32}$
in	610	0.0%	$\mathcal{S}_{298}$
lectsched-1-obj	625	12.4%	$(\hat{\mathcal{S}}_2)^{797}$, $(\mathcal{S}_2)^{3}$, $(\mathcal{S}_3)^{3}$, $(\hat{\mathcal{S}}_3)^{18}$, $(\hat{\mathcal{S}}_4)^{6}$, $\mathcal{S}_{193}$
lectsched-1	625	12.4%	$(\hat{\mathcal{S}}_2)^{797}$, $(\mathcal{S}_2)^{3}$, $(\mathcal{S}_3)^{3}$, $(\hat{\mathcal{S}}_3)^{18}$, $(\hat{\mathcal{S}}_4)^{6}$, $\mathcal{S}_{193}$
lectsched-2	409	11.7%	$(\mathcal{S}_2)^{3}$, $(\hat{\mathcal{S}}_2)^{462}$, $(\hat{\mathcal{S}}_3)^{6}$, $(\hat{\mathcal{S}}_4)^{4}$, $\mathcal{S}_{148}$
lectsched-3	544	10.9%	$(\hat{\mathcal{S}}_2)^{633}$, $(\mathcal{S}_2)^{3}$, $(\mathcal{S}_3)^{3}$, $(\hat{\mathcal{S}}_3)^{15}$, $\mathcal{S}_{184}$
lectsched-4-obj	218	13.2%	$(\hat{\mathcal{S}}_2)^{230}$, $(\hat{\mathcal{S}}_3)^{3}$, $\hat{\mathcal{S}}_4$, $\mathcal{S}_{93}$
liu	1	0.2%	$\mathcal{S}_2$
macrophage	62	25.0%	$(\mathcal{S}_2)^{146}$, $(\hat{\mathcal{S}}_2)^{27}$, $\hat{\mathcal{S}}_4$, $\hat{\mathcal{S}}_6$, ?
map06	≥ 320577	$\geq 71.9\%$	$(\mathcal{S}_2)^{58}$, $(\mathcal{S}_3)^{5}$, $(\mathcal{S}_4)^{2}$, $\mathcal{S}_7$, $(\mathcal{S}_8)^{2}$, $\mathcal{S}_{136}$, $\mathcal{S}_{163}$, $\mathcal{S}_{178}$, $\mathcal{S}_{185}$, $\mathcal{S}_{186}$, $\mathcal{S}_{198}$, $\mathcal{S}_{199}$, $\mathcal{S}_{201}$, $\mathcal{S}_{202}$, $\mathcal{S}_{203}$, $\mathcal{S}_{204}$, $\mathcal{S}_{214}$, $\mathcal{S}_{221}$, $\mathcal{S}_{222}$, $\mathcal{S}_{225}$, $\mathcal{S}_{226}$, $\mathcal{S}_{234}$, $\mathcal{S}_{239}$, $\mathcal{S}_{241}$, $\mathcal{S}_{243}$, $\mathcal{S}_{254}$, $\mathcal{S}_{257}$, $\mathcal{S}_{263}$, $\mathcal{S}_{266}$, $\mathcal{S}_{268}$, $(\mathcal{S}_{269})^{2}$, $\mathcal{S}_{275}$, $\mathcal{S}_{280}$, $\mathcal{S}_{281}$, $\mathcal{S}_{282}$, $\mathcal{S}_{285}$, $\mathcal{S}_{287}$, $(\mathcal{S}_{289})^{2}$, $\mathcal{S}_{294}$, $\mathcal{S}_{298}$, $\mathcal{S}_{305}$, $\mathcal{S}_{311}$, $\mathcal{S}_{315}$, $\mathcal{S}_{322}$, $\mathcal{S}_{325}$, $\mathcal{S}_{329}$, $\mathcal{S}_{334}$, $\mathcal{S}_{335}$, $\mathcal{S}_{336}$, $\mathcal{S}_{337}$, $\mathcal{S}_{339}$, $\mathcal{S}_{341}$, $(\mathcal{S}_{343})^{2}$, $\mathcal{S}_{345}$, $(\mathcal{S}_{346})^{2}$, $\mathcal{S}_{349}$, $(\mathcal{S}_{350})^{2}$, $\mathcal{S}_{352}$, $\mathcal{S}_{356}$, $\mathcal{S}_{357}$, $\mathcal{S}_{358}$, $\mathcal{S}_{360}$, $\mathcal{S}_{361}$, $\mathcal{S}_{364}$, $\mathcal{S}_{366}$, $\mathcal{S}_{367}$, $(\mathcal{S}_{368})^{3}$, $\mathcal{S}_{370}$, $\mathcal{S}_{372}$, $\mathcal{S}_{373}$, $\mathcal{S}_{374}$, $\mathcal{S}_{383}$, $\mathcal{S}_{384}$, $(\mathcal{S}_{393})^{2}$, $\mathcal{S}_{398}$, $(\mathcal{S}_{400})^{7}$, $\mathcal{S}_{413}$, $\mathcal{S}_{443}$, $\mathcal{S}_{452}$, $\mathcal{S}_{457}$, $\mathcal{S}_{458}$, $\mathcal{S}_{466}$, $\mathcal{S}_{479}$, $\mathcal{S}_{501}$, $\mathcal{S}_{505}$, $\mathcal{S}_{511}$, $\mathcal{S}_{582}$, $\mathcal{S}_{592}$, $\mathcal{S}_{601}$, $\mathcal{S}_{610}$, $\mathcal{S}_{613}$, $\mathcal{S}_{618}$, $\mathcal{S}_{676}$, $\mathcal{S}_{704}$, $\mathcal{S}_{713}$, $\mathcal{S}_{717}$, $\mathcal{S}_{735}$, $\mathcal{S}_{743}$, $\mathcal{S}_{744}$, $\mathcal{S}_{751}$, $\mathcal{S}_{769}$, $\mathcal{S}_{788}$, $\mathcal{S}_{791}$, $(\mathcal{S}_{800})^{3}$, $\mathcal{S}_{808}$, $\mathcal{S}_{813}$, $\mathcal{S}_{824}$, $\mathcal{S}_{856}$, $\mathcal{S}_{898}$, $\mathcal{S}_{1146}$, $\mathcal{S}_{1150}$, $\mathcal{S}_{1226}$, $\mathcal{S}_{1280}$, $\mathcal{S}_{1332}$, $\mathcal{S}_{1376}$, $\mathcal{S}_{1624}$, $\mathcal{S}_{1764}$, $\mathcal{S}_{1819}$, $\mathcal{S}_{1945}$, $\mathcal{S}_{1953}$, $\mathcal{S}_{1989}$, $\mathcal{S}_{2241}$, $\mathcal{S}_{2391}$, $\mathcal{S}_{2422}$, $\mathcal{S}_{2506}$, $\mathcal{S}_{2507}$, $\mathcal{S}_{2550}$, $\mathcal{S}_{2728}$, $\mathcal{S}_{2895}$, $\mathcal{S}_{3337}$, $\mathcal{S}_{3512}$, $\mathcal{S}_{3694}$, $\mathcal{S}_{4776}$, $\mathcal{S}_{6466}$, $\mathcal{S}_{8454}$

map10	≥ 320577	$\geq 71.9\%$	$(\mathcal{S}_2)^{58}$, $(\mathcal{S}_3)^5$, $(\mathcal{S}_4)^2$, $\mathcal{S}_7$, $(\mathcal{S}_8)^2$, $\mathcal{S}_{136}$, $\mathcal{S}_{163}$, $\mathcal{S}_{178}$, $\mathcal{S}_{185}$, $\mathcal{S}_{186}$, $\mathcal{S}_{198}$, $\mathcal{S}_{199}$, $\mathcal{S}_{201}$, $\mathcal{S}_{202}$, $\mathcal{S}_{203}$, $\mathcal{S}_{204}$, $\mathcal{S}_{214}$, $\mathcal{S}_{221}$, $\mathcal{S}_{222}$, $\mathcal{S}_{225}$, $\mathcal{S}_{226}$, $\mathcal{S}_{234}$, $\mathcal{S}_{239}$, $\mathcal{S}_{241}$, $\mathcal{S}_{243}$, $\mathcal{S}_{254}$, $\mathcal{S}_{257}$, $\mathcal{S}_{263}$, $\mathcal{S}_{266}$, $\mathcal{S}_{268}$, $(\mathcal{S}_{269})^2$, $\mathcal{S}_{275}$, $\mathcal{S}_{280}$, $\mathcal{S}_{281}$, $\mathcal{S}_{282}$, $\mathcal{S}_{285}$, $\mathcal{S}_{287}$, $(\mathcal{S}_{289})^2$, $\mathcal{S}_{294}$, $\mathcal{S}_{298}$, $\mathcal{S}_{305}$, $\mathcal{S}_{311}$, $\mathcal{S}_{315}$, $\mathcal{S}_{322}$, $\mathcal{S}_{325}$, $\mathcal{S}_{329}$, $\mathcal{S}_{334}$, $\mathcal{S}_{335}$, $\mathcal{S}_{336}$, $\mathcal{S}_{337}$, $\mathcal{S}_{339}$, $\mathcal{S}_{341}$, $(\mathcal{S}_{343})^2$, $\mathcal{S}_{345}$, $(\mathcal{S}_{346})^2$, $\mathcal{S}_{349}$, $(\mathcal{S}_{350})^2$, $\mathcal{S}_{352}$, $\mathcal{S}_{356}$, $\mathcal{S}_{357}$, $\mathcal{S}_{358}$, $\mathcal{S}_{360}$, $\mathcal{S}_{361}$, $\mathcal{S}_{364}$, $\mathcal{S}_{366}$, $\mathcal{S}_{367}$, $(\mathcal{S}_{368})^3$, $\mathcal{S}_{370}$, $\mathcal{S}_{372}$, $\mathcal{S}_{373}$, $\mathcal{S}_{374}$, $\mathcal{S}_{383}$, $\mathcal{S}_{384}$, $(\mathcal{S}_{393})^2$, $\mathcal{S}_{398}$, $(\mathcal{S}_{400})^7$, $\mathcal{S}_{413}$, $\mathcal{S}_{443}$, $\mathcal{S}_{452}$, $\mathcal{S}_{457}$, $\mathcal{S}_{458}$, $\mathcal{S}_{466}$, $\mathcal{S}_{479}$, $\mathcal{S}_{501}$, $\mathcal{S}_{505}$, $\mathcal{S}_{511}$, $\mathcal{S}_{582}$, $\mathcal{S}_{592}$, $\mathcal{S}_{601}$, $\mathcal{S}_{610}$, $\mathcal{S}_{613}$, $\mathcal{S}_{618}$, $\mathcal{S}_{676}$, $\mathcal{S}_{704}$, $\mathcal{S}_{713}$, $\mathcal{S}_{717}$, $\mathcal{S}_{735}$, $\mathcal{S}_{743}$, $\mathcal{S}_{744}$, $\mathcal{S}_{751}$, $\mathcal{S}_{769}$, $\mathcal{S}_{788}$, $\mathcal{S}_{791}$, $(\mathcal{S}_{800})^3$, $\mathcal{S}_{808}$, $\mathcal{S}_{813}$, $\mathcal{S}_{824}$, $\mathcal{S}_{856}$, $\mathcal{S}_{898}$, $\mathcal{S}_{1146}$, $\mathcal{S}_{1150}$, $\mathcal{S}_{1226}$, $\mathcal{S}_{1280}$, $\mathcal{S}_{1332}$, $\mathcal{S}_{1376}$, $\mathcal{S}_{1624}$, $\mathcal{S}_{1764}$, $\mathcal{S}_{1819}$, $\mathcal{S}_{1945}$, $\mathcal{S}_{1953}$, $\mathcal{S}_{1989}$, $\mathcal{S}_{2241}$, $\mathcal{S}_{2391}$, $\mathcal{S}_{2422}$, $\mathcal{S}_{2506}$, $\mathcal{S}_{2507}$, $\mathcal{S}_{2550}$, $\mathcal{S}_{2728}$, $\mathcal{S}_{2895}$, $\mathcal{S}_{3337}$, $\mathcal{S}_{3512}$, $\mathcal{S}_{3694}$, $\mathcal{S}_{4776}$, $\mathcal{S}_{6466}$, $\mathcal{S}_{8454}$
map14	≥ 320577	$\geq 71.9\%$	$(\mathcal{S}_2)^{58}$, $(\mathcal{S}_3)^5$, $(\mathcal{S}_4)^2$, $\mathcal{S}_7$, $(\mathcal{S}_8)^2$, $\mathcal{S}_{136}$, $\mathcal{S}_{163}$, $\mathcal{S}_{178}$, $\mathcal{S}_{185}$, $\mathcal{S}_{186}$, $\mathcal{S}_{198}$, $\mathcal{S}_{199}$, $\mathcal{S}_{201}$, $\mathcal{S}_{202}$, $\mathcal{S}_{203}$, $\mathcal{S}_{204}$, $\mathcal{S}_{214}$, $\mathcal{S}_{221}$, $\mathcal{S}_{222}$, $\mathcal{S}_{225}$, $\mathcal{S}_{226}$, $\mathcal{S}_{234}$, $\mathcal{S}_{239}$, $\mathcal{S}_{241}$, $\mathcal{S}_{243}$, $\mathcal{S}_{254}$, $\mathcal{S}_{257}$, $\mathcal{S}_{263}$, $\mathcal{S}_{266}$, $\mathcal{S}_{268}$, $(\mathcal{S}_{269})^2$, $\mathcal{S}_{275}$, $\mathcal{S}_{280}$, $\mathcal{S}_{281}$, $\mathcal{S}_{282}$, $\mathcal{S}_{285}$, $\mathcal{S}_{287}$, $(\mathcal{S}_{289})^2$, $\mathcal{S}_{294}$, $\mathcal{S}_{298}$, $\mathcal{S}_{305}$, $\mathcal{S}_{311}$, $\mathcal{S}_{315}$, $\mathcal{S}_{322}$, $\mathcal{S}_{325}$, $\mathcal{S}_{329}$, $\mathcal{S}_{334}$, $\mathcal{S}_{335}$, $\mathcal{S}_{336}$, $\mathcal{S}_{337}$, $\mathcal{S}_{339}$, $\mathcal{S}_{341}$, $(\mathcal{S}_{343})^2$, $\mathcal{S}_{345}$, $(\mathcal{S}_{346})^2$, $\mathcal{S}_{349}$, $(\mathcal{S}_{350})^2$, $\mathcal{S}_{352}$, $\mathcal{S}_{356}$, $\mathcal{S}_{357}$, $\mathcal{S}_{358}$, $\mathcal{S}_{360}$, $\mathcal{S}_{361}$, $\mathcal{S}_{364}$, $\mathcal{S}_{366}$, $\mathcal{S}_{367}$, $(\mathcal{S}_{368})^3$, $\mathcal{S}_{370}$, $\mathcal{S}_{372}$, $\mathcal{S}_{373}$, $\mathcal{S}_{374}$, $\mathcal{S}_{383}$, $\mathcal{S}_{384}$, $(\mathcal{S}_{393})^2$, $\mathcal{S}_{398}$, $(\mathcal{S}_{400})^7$, $\mathcal{S}_{413}$, $\mathcal{S}_{443}$, $\mathcal{S}_{452}$, $\mathcal{S}_{457}$, $\mathcal{S}_{458}$, $\mathcal{S}_{466}$, $\mathcal{S}_{479}$, $\mathcal{S}_{501}$, $\mathcal{S}_{505}$, $\mathcal{S}_{511}$, $\mathcal{S}_{582}$, $\mathcal{S}_{592}$, $\mathcal{S}_{601}$, $\mathcal{S}_{610}$, $\mathcal{S}_{613}$, $\mathcal{S}_{618}$, $\mathcal{S}_{676}$, $\mathcal{S}_{704}$, $\mathcal{S}_{713}$, $\mathcal{S}_{717}$, $\mathcal{S}_{735}$, $\mathcal{S}_{743}$, $\mathcal{S}_{744}$, $\mathcal{S}_{751}$, $\mathcal{S}_{769}$, $\mathcal{S}_{788}$, $\mathcal{S}_{791}$, $(\mathcal{S}_{800})^3$, $\mathcal{S}_{808}$, $\mathcal{S}_{813}$, $\mathcal{S}_{824}$, $\mathcal{S}_{856}$, $\mathcal{S}_{898}$, $\mathcal{S}_{1146}$, $\mathcal{S}_{1150}$, $\mathcal{S}_{1226}$, $\mathcal{S}_{1280}$, $\mathcal{S}_{1332}$, $\mathcal{S}_{1376}$, $\mathcal{S}_{1624}$, $\mathcal{S}_{1764}$, $\mathcal{S}_{1819}$, $\mathcal{S}_{1945}$, $\mathcal{S}_{1953}$, $\mathcal{S}_{1989}$, $\mathcal{S}_{2241}$, $\mathcal{S}_{2391}$, $\mathcal{S}_{2422}$, $\mathcal{S}_{2506}$, $\mathcal{S}_{2507}$, $\mathcal{S}_{2550}$, $\mathcal{S}_{2728}$, $\mathcal{S}_{2895}$, $\mathcal{S}_{3337}$, $\mathcal{S}_{3512}$, $\mathcal{S}_{3694}$, $\mathcal{S}_{4776}$, $\mathcal{S}_{6466}$, $\mathcal{S}_{8454}$
map18	≥ 320577	$\geq 71.9\%$	$(\mathcal{S}_2)^{58}$, $(\mathcal{S}_3)^5$, $(\mathcal{S}_4)^2$, $\mathcal{S}_7$, $(\mathcal{S}_8)^2$, $\mathcal{S}_{136}$, $\mathcal{S}_{163}$, $\mathcal{S}_{178}$, $\mathcal{S}_{185}$, $\mathcal{S}_{186}$, $\mathcal{S}_{198}$, $\mathcal{S}_{199}$, $\mathcal{S}_{201}$, $\mathcal{S}_{202}$, $\mathcal{S}_{203}$, $\mathcal{S}_{204}$, $\mathcal{S}_{214}$, $\mathcal{S}_{221}$, $\mathcal{S}_{222}$, $\mathcal{S}_{225}$, $\mathcal{S}_{226}$, $\mathcal{S}_{234}$, $\mathcal{S}_{239}$, $\mathcal{S}_{241}$, $\mathcal{S}_{243}$, $\mathcal{S}_{254}$, $\mathcal{S}_{257}$, $\mathcal{S}_{263}$, $\mathcal{S}_{266}$, $\mathcal{S}_{268}$, $(\mathcal{S}_{269})^2$, $\mathcal{S}_{275}$, $\mathcal{S}_{280}$, $\mathcal{S}_{281}$, $\mathcal{S}_{282}$, $\mathcal{S}_{285}$, $\mathcal{S}_{287}$, $(\mathcal{S}_{289})^2$, $\mathcal{S}_{294}$, $\mathcal{S}_{298}$, $\mathcal{S}_{305}$, $\mathcal{S}_{311}$, $\mathcal{S}_{315}$, $\mathcal{S}_{322}$, $\mathcal{S}_{325}$, $\mathcal{S}_{329}$, $\mathcal{S}_{334}$, $\mathcal{S}_{335}$, $\mathcal{S}_{336}$, $\mathcal{S}_{337}$, $\mathcal{S}_{339}$, $\mathcal{S}_{341}$, $(\mathcal{S}_{343})^2$, $\mathcal{S}_{345}$, $(\mathcal{S}_{346})^2$, $\mathcal{S}_{349}$, $(\mathcal{S}_{350})^2$, $\mathcal{S}_{352}$, $\mathcal{S}_{356}$, $\mathcal{S}_{357}$, $\mathcal{S}_{358}$, $\mathcal{S}_{360}$, $\mathcal{S}_{361}$, $\mathcal{S}_{364}$, $\mathcal{S}_{366}$, $\mathcal{S}_{367}$, $(\mathcal{S}_{368})^3$, $\mathcal{S}_{370}$, $\mathcal{S}_{372}$, $\mathcal{S}_{373}$, $\mathcal{S}_{374}$, $\mathcal{S}_{383}$, $\mathcal{S}_{384}$, $(\mathcal{S}_{393})^2$, $\mathcal{S}_{398}$, $(\mathcal{S}_{400})^7$, $\mathcal{S}_{413}$, $\mathcal{S}_{443}$, $\mathcal{S}_{452}$, $\mathcal{S}_{457}$, $\mathcal{S}_{458}$, $\mathcal{S}_{466}$, $\mathcal{S}_{479}$, $\mathcal{S}_{501}$, $\mathcal{S}_{505}$, $\mathcal{S}_{511}$, $\mathcal{S}_{582}$, $\mathcal{S}_{592}$, $\mathcal{S}_{601}$, $\mathcal{S}_{610}$, $\mathcal{S}_{613}$, $\mathcal{S}_{618}$, $\mathcal{S}_{676}$, $\mathcal{S}_{704}$, $\mathcal{S}_{713}$, $\mathcal{S}_{717}$, $\mathcal{S}_{735}$, $\mathcal{S}_{743}$, $\mathcal{S}_{744}$, $\mathcal{S}_{751}$, $\mathcal{S}_{769}$, $\mathcal{S}_{788}$, $\mathcal{S}_{791}$, $(\mathcal{S}_{800})^3$, $\mathcal{S}_{808}$, $\mathcal{S}_{813}$, $\mathcal{S}_{824}$, $\mathcal{S}_{856}$, $\mathcal{S}_{898}$, $\mathcal{S}_{1146}$, $\mathcal{S}_{1150}$, $\mathcal{S}_{1226}$, $\mathcal{S}_{1280}$, $\mathcal{S}_{1332}$, $\mathcal{S}_{1376}$, $\mathcal{S}_{1624}$, $\mathcal{S}_{1764}$, $\mathcal{S}_{1819}$, $\mathcal{S}_{1945}$, $\mathcal{S}_{1953}$, $\mathcal{S}_{1989}$, $\mathcal{S}_{2241}$, $\mathcal{S}_{2391}$, $\mathcal{S}_{2422}$, $\mathcal{S}_{2506}$, $\mathcal{S}_{2507}$, $\mathcal{S}_{2550}$, $\mathcal{S}_{2728}$, $\mathcal{S}_{2895}$, $\mathcal{S}_{3337}$, $\mathcal{S}_{3512}$, $\mathcal{S}_{3694}$, $\mathcal{S}_{4776}$, $\mathcal{S}_{6466}$, $\mathcal{S}_{8454}$

map20	≥ 320577	$\geq 71.9\%$	$(\mathcal{S}_2)^{58}, (\mathcal{S}_3)^5, (\mathcal{S}_4)^2, \mathcal{S}_7, (\mathcal{S}_8)^2, \mathcal{S}_{136}, \mathcal{S}_{163}, \mathcal{S}_{178}, \mathcal{S}_{185}, \mathcal{S}_{186}, \mathcal{S}_{198}, \mathcal{S}_{199}, \mathcal{S}_{201}, \mathcal{S}_{202}, \mathcal{S}_{203}, \mathcal{S}_{204}, \mathcal{S}_{214}, \mathcal{S}_{221}, \mathcal{S}_{222}, \mathcal{S}_{225}, \mathcal{S}_{226}, \mathcal{S}_{234}, \mathcal{S}_{239}, \mathcal{S}_{241}, \mathcal{S}_{243}, \mathcal{S}_{254}, \mathcal{S}_{257}, \mathcal{S}_{263}, \mathcal{S}_{266}, \mathcal{S}_{268}, (\mathcal{S}_{269})^2, \mathcal{S}_{275}, \mathcal{S}_{280}, \mathcal{S}_{281}, \mathcal{S}_{282}, \mathcal{S}_{285}, \mathcal{S}_{287}, (\mathcal{S}_{289})^2, \mathcal{S}_{294}, \mathcal{S}_{298}, \mathcal{S}_{305}, \mathcal{S}_{311}, \mathcal{S}_{315}, \mathcal{S}_{322}, \mathcal{S}_{325}, \mathcal{S}_{329}, \mathcal{S}_{334}, \mathcal{S}_{335}, \mathcal{S}_{336}, \mathcal{S}_{337}, \mathcal{S}_{339}, \mathcal{S}_{341}, (\mathcal{S}_{343})^2, \mathcal{S}_{345}, (\mathcal{S}_{346})^2, \mathcal{S}_{349}, (\mathcal{S}_{350})^2, \mathcal{S}_{352}, \mathcal{S}_{356}, \mathcal{S}_{357}, \mathcal{S}_{358}, \mathcal{S}_{360}, \mathcal{S}_{361}, \mathcal{S}_{364}, \mathcal{S}_{366}, \mathcal{S}_{367}, (\mathcal{S}_{368})^3, \mathcal{S}_{370}, \mathcal{S}_{372}, \mathcal{S}_{373}, \mathcal{S}_{374}, \mathcal{S}_{383}, \mathcal{S}_{384}, (\mathcal{S}_{393})^2, \mathcal{S}_{398}, (\mathcal{S}_{400})^7, \mathcal{S}_{413}, \mathcal{S}_{443}, \mathcal{S}_{452}, \mathcal{S}_{457}, \mathcal{S}_{458}, \mathcal{S}_{466}, \mathcal{S}_{479}, \mathcal{S}_{501}, \mathcal{S}_{505}, \mathcal{S}_{511}, \mathcal{S}_{582}, \mathcal{S}_{592}, \mathcal{S}_{601}, \mathcal{S}_{610}, \mathcal{S}_{613}, \mathcal{S}_{618}, \mathcal{S}_{676}, \mathcal{S}_{704}, \mathcal{S}_{713}, \mathcal{S}_{717}, \mathcal{S}_{735}, \mathcal{S}_{743}, \mathcal{S}_{744}, \mathcal{S}_{751}, \mathcal{S}_{769}, \mathcal{S}_{788}, \mathcal{S}_{791}, (\mathcal{S}_{800})^3, \mathcal{S}_{808}, \mathcal{S}_{813}, \mathcal{S}_{824}, \mathcal{S}_{856}, \mathcal{S}_{898}, \mathcal{S}_{1146}, \mathcal{S}_{1150}, \mathcal{S}_{1226}, \mathcal{S}_{1280}, \mathcal{S}_{1332}, \mathcal{S}_{1376}, \mathcal{S}_{1624}, \mathcal{S}_{1764}, \mathcal{S}_{1819}, \mathcal{S}_{1945}, \mathcal{S}_{1953}, \mathcal{S}_{1989}, \mathcal{S}_{2241}, \mathcal{S}_{2391}, \mathcal{S}_{2422}, \mathcal{S}_{2506}, \mathcal{S}_{2507}, \mathcal{S}_{2550}, \mathcal{S}_{2728}, \mathcal{S}_{2895}, \mathcal{S}_{3337}, \mathcal{S}_{3512}, \mathcal{S}_{3694}, \mathcal{S}_{4776}, \mathcal{S}_{6466}, \mathcal{S}_{8454}$
maxgasflow	6	1.8%	$(\hat{\mathcal{S}}_2)^{13}, (\hat{\mathcal{S}}_3)^2$
mcsched	5	5.2%	$(\hat{\mathcal{S}}_2)^{15}$
methanosarcina	763	64.7%	$(\mathcal{S}_2)^{2505}, ?$
mkc	78	61.3%	$(\hat{\mathcal{S}}_2)^{25}, (\mathcal{S}_2)^9, (\hat{\mathcal{S}}_3)^{13}, (\mathcal{S}_3)^4, (\hat{\mathcal{S}}_4)^5, (\hat{\mathcal{S}}_5)^2, \hat{\mathcal{S}}_6, \hat{\mathcal{S}}_7, \hat{\mathcal{S}}_8, (?)^3$
momentum3	37	0.9%	$(\hat{\mathcal{S}}_3)^2, \hat{\mathcal{S}}_5, \hat{\mathcal{S}}_6, \hat{\mathcal{S}}_7, (\hat{\mathcal{S}}_9)^3, \hat{\mathcal{S}}_{13}$
msc98-ip	2674	33.2%	$(\hat{\mathcal{S}}_2)^6, (\mathcal{S}_2)^{609}, (\mathcal{S}_3)^{266}, (\mathcal{S}_4)^{219}, (\mathcal{S}_5)^{198}, (\mathcal{S}_6)^{210}, (\mathcal{S}_7)^{108}, (\mathcal{S}_8)^{112}, (\mathcal{S}_9)^2, (\mathcal{S}_{10})^6, (?)^2$
mspp16	≥ 19551	$\geq 85.2\%$	$(\mathcal{S}_2)^{420}, (\mathcal{S}_{14})^{420}, (\mathcal{S}_{15})^{960}, (\mathcal{S}_{16})^{240}$
mzzv11	47	3.0%	$(\mathcal{S}_2)^{155}$
n3seq24	10	11.4%	$(\hat{\mathcal{S}}_2)^{28}, \hat{\mathcal{S}}_4$
nag	1	0.1%	$\mathcal{S}_2$
nb10tb	1127	45.5%	$(\hat{\mathcal{S}}_2)^{25}, (\mathcal{S}_2)^{44}, (\hat{\mathcal{S}}_3)^4, (\mathcal{S}_3)^{33}, (\hat{\mathcal{S}}_4)^2, (\hat{\mathcal{S}}_5)^3, \hat{\mathcal{S}}_6, (\hat{\mathcal{S}}_7)^2, (\hat{\mathcal{S}}_8)^2, \hat{\mathcal{S}}_{10}, \hat{\mathcal{S}}_{11}, \hat{\mathcal{S}}_{12}, (?)^3$
neos-1109824	2	100.0%	?
neos-1112782	57	2.2%	$\hat{\mathcal{S}}_{45}$
neos-1112787	48	2.4%	$\hat{\mathcal{S}}_{40}$
neos-1171692	20	100.0%	$\hat{\mathcal{S}}_{21}$
neos-1171737	33	100.0%	$\hat{\mathcal{S}}_{30}$
neos-1224597	505	100.0%	$(\mathcal{S}_5)^{17}, (\mathcal{S}_{10})^3, \mathcal{S}_{35}, ?$
neos-1225589	26	3.8%	$\hat{\mathcal{S}}_{25}$
neos-1311124	79	100.0%	$(\hat{\mathcal{S}}_{21})^4$
neos-1337307	4	87.5%	$\hat{\mathcal{S}}_7$
neos-1396125	1	78.3%	$\hat{\mathcal{S}}_3$
neos-1426635	27	100.0%	$(\hat{\mathcal{S}}_{10})^4$
neos-1426662	54	100.0%	$(\hat{\mathcal{S}}_{16})^4$
neos-1429212	?	?	?
neos-1436709	40	100.0%	$(\hat{\mathcal{S}}_{13})^4$
neos-1440460	23	100.0%	$(\hat{\mathcal{S}}_9)^4$
neos-1442119	44	100.0%	$(\hat{\mathcal{S}}_{14})^4$
neos-1442657	35	100.0%	$(\hat{\mathcal{S}}_{12})^4$
neos-1601936	433	9.2%	$\mathcal{S}_{72}, ?$
neos-1605061	104	1.8%	$\mathcal{S}_{72}$
neos-1605075	104	1.7%	$\mathcal{S}_{72}$
neos-1620770	4	97.2%	?
neos-476283	40	1.1%	$(\hat{\mathcal{S}}_2)^{12}, \mathcal{S}_7, \mathcal{S}_{27}, ?$
neos-520729	≥ 1	?	?
neos-555424	147	99.9%	$(\hat{\mathcal{S}}_{10})^3, \hat{\mathcal{S}}_{20}, \hat{\mathcal{S}}_{30}, ?$
neos-631710	314	99.7%	$\hat{\mathcal{S}}_{11}, (\hat{\mathcal{S}}_{15})^2, \hat{\mathcal{S}}_{16}, \hat{\mathcal{S}}_{18}, \hat{\mathcal{S}}_{19}, \hat{\mathcal{S}}_{24}, \hat{\mathcal{S}}_{28}, \hat{\mathcal{S}}_{33}, \hat{\mathcal{S}}_{39}, \hat{\mathcal{S}}_{40}, \hat{\mathcal{S}}_{42}$
neos-738098	21	93.5%	?

neos-777800	1	100.0%	?
neos-785912	10	91.3%	?
neos-820146	107	100.0%	?
neos-820157	558	100.0%	?
neos-824661	937	100.0%	?
neos-824695	937	100.0%	?
neos-826650	476	98.6%	?
neos-826694	973	99.3%	?
neos-826812	142	99.3%	?
neos-826841	42	98.5%	?
neos-849702	4	100.0%	?
neos-859770	770	98.9%	$(\mathcal{S}_2)^{11}, \mathcal{S}_6, \mathcal{S}_{12}, \mathcal{S}_{20}, \mathcal{S}_{25}, \mathcal{S}_{32}, ?$
neos-885086	57	100.0%	$\hat{\mathcal{S}}_{45}$
neos-885524	≥ 3778	$\geq 24.6\%$	$(\mathcal{S}_2)^{9850}, (\mathcal{S}_3)^{760}, (\mathcal{S}_4)^{70}, (\mathcal{S}_5)^{60}$
neos-911880	8	100.0%	$(\hat{\mathcal{S}}_3)^6, \hat{\mathcal{S}}_6$
neos-932816	599	85.3%	$\hat{\mathcal{S}}_4, \mathcal{S}_{293}$
neos-933638	1185	93.9%	$\mathcal{S}_{42}, \mathcal{S}_{495}, ?$
neos-933966	1184	95.7%	$\hat{\mathcal{S}}_2, \hat{\mathcal{S}}_3, \mathcal{S}_{42}, \mathcal{S}_{495}, ?$
neos-934278	1710	81.4%	$\hat{\mathcal{S}}_2, \mathcal{S}_{389}, \mathcal{S}_{396}, ?$
neos-935627	5818	75.9%	$\hat{\mathcal{S}}_2, \mathcal{S}_{2022}, ?$
neos-935769	5818	80.9%	$(\hat{\mathcal{S}}_3)^4, \mathcal{S}_{2022}, ?$
neos-937511	5262	79.7%	$(\hat{\mathcal{S}}_3)^4, \mathcal{S}_{1853}, ?$
neos-937815	5336	72.6%	$(\hat{\mathcal{S}}_2)^3, \mathcal{S}_{1876}, ?$
neos-941262	5571	76.3%	$(\hat{\mathcal{S}}_2)^9, \mathcal{S}_{1948}, ?$
neos-941313	≥ 6475	$\geq 9.9\%$	$(\mathcal{S}_2)^{1920}, (\mathcal{S}_3)^{1020}, (\mathcal{S}_4)^{450}, (\mathcal{S}_5)^{540}, (\mathcal{S}_6)^{150}, (\mathcal{S}_7)^{120}, (\mathcal{S}_8)^{60}, (\mathcal{S}_9)^{60}, (\mathcal{S}_{11})^{30}, (\mathcal{S}_{12})^{30}, (\mathcal{S}_{13})^{60}, (\mathcal{S}_{15})^{30}, (\mathcal{S}_{17})^{30}$
neos-948126	4970	78.9%	$(\hat{\mathcal{S}}_2)^6, \mathcal{S}_{1764}, ?$
neos-952987	17	0.3%	$(\mathcal{S}_2)^{36}, \mathcal{S}_9$
neos-957389	34	75.1%	$\hat{\mathcal{S}}_2, (\hat{\mathcal{S}}_4)^2, (\hat{\mathcal{S}}_{10})^2, ?$
neos-984165	4281	75.8%	$(\mathcal{S}_2)^{11}, (\hat{\mathcal{S}}_2)^8, \mathcal{S}_{1549}, ?$
neos13	1	0.1%	$\mathcal{S}_2$
neos18	248	36.1%	$(\hat{\mathcal{S}}_2)^{31}, (\mathcal{S}_2)^6, (\mathcal{S}_3)^2, (\hat{\mathcal{S}}_3)^5, (\hat{\mathcal{S}}_4)^{22}, (\mathcal{S}_4)^2, \hat{\mathcal{S}}_6, \hat{\mathcal{S}}_8, (?)^2$
neos6	7	94.9%	$\hat{\mathcal{S}}_{10}$
neos788725	1	100.0%	?
neos808444	1	11.5%	$\hat{\mathcal{S}}_2$
noswot	1	40.6%	$\hat{\mathcal{S}}_2$
npmv07	≥ 398	$\geq 0.8\%$	$(\mathcal{S}_2)^{532}, (\mathcal{S}_3)^{56}, (\mathcal{S}_4)^{56}, (\mathcal{S}_5)^{56}$
ns1111636	≥ 396403	$\geq 78.7\%$	$(\mathcal{S}_{61})^{1200}, (\mathcal{S}_{64})^{1920}, (\mathcal{S}_{66})^{480}, (\mathcal{S}_{69})^{480}, (\mathcal{S}_{72})^{320}$
ns1116954	554	99.9%	?
ns1158817	**?**	?	?
ns1208400	3	97.8%	?
ns1456591	37	99.8%	$\hat{\mathcal{S}}_{20}, \mathcal{S}_{20}$
ns1606230	104	1.7%	$\mathcal{S}_{72}$
ns1631475	32	0.9%	$(\mathcal{S}_2)^{105}$
ns1663818	393	0.2%	$(\mathcal{S}_{50})^3, (\mathcal{S}_{51})^3$
ns1702808	3	100.0%	$\hat{\mathcal{S}}_6$
ns1758913	1	3.0%	$\hat{\mathcal{S}}_2$
ns1830653	16	1.1%	$\mathcal{S}_{18}$
ns1853823	1	56.1%	?
ns1854840	2	88.0%	?
ns1856153	1	92.5%	$\hat{\mathcal{S}}_2$
ns1905797	2	100.0%	$\hat{\mathcal{S}}_4$
ns1905800	2	100.0%	?
ns1952667	70	3.4%	$(\mathcal{S}_2)^{222}, \mathcal{S}_3, \mathcal{S}_5$

ns2017839	156	1.9%	$(\mathcal{S}_2)^{516}$
ns2081729	1	90.8%	$(\hat{\mathcal{S}}_2)^3$
ns2118727	1162	0.5%	$(\hat{\mathcal{S}}_2)^{36}$, $(\mathcal{S}_2)^{40}$, $(\mathcal{S}_3)^{90}$, $(\mathcal{S}_4)^4$, $(\mathcal{S}_5)^{20}$, $\mathcal{S}_{90}$, $\mathcal{S}_{218}$, $(\mathcal{S}_{235})^2$, $\mathcal{S}_{308}$
ns2122603	1162	4.4%	$(\hat{\mathcal{S}}_2)^{36}$, $(\mathcal{S}_2)^{40}$, $(\mathcal{S}_3)^{90}$, $(\mathcal{S}_4)^4$, $(\mathcal{S}_5)^{20}$, $\mathcal{S}_{90}$, $\mathcal{S}_{218}$, $(\mathcal{S}_{235})^2$, $\mathcal{S}_{308}$
ns2124243	≥ 7	$\geq$ 0.0%	$\mathcal{S}_3$, $\mathcal{S}_9$
ns2137859	756	96.0%	$\mathcal{S}_{321}$, ?
ns894236	9	2.4%	$\hat{\mathcal{S}}_{12}$
ns903616	18	2.3%	$\hat{\mathcal{S}}_4$, $\hat{\mathcal{S}}_{18}$
nsr8k	101	1.2%	$(\mathcal{S}_2)^{198}$, $(\mathcal{S}_3)^7$, $\mathcal{S}_{32}$
ofi	≥ 1565	$\geq$ 2.5%	$(\mathcal{S}_2)^{5197}$
p2m2p1m1p0n100	33	92.0%	$(\mathcal{S}_2)^6$, $(\mathcal{S}_3)^8$, $(\mathcal{S}_4)^4$, $(\mathcal{S}_5)^3$, $(\mathcal{S}_6)^3$, $\mathcal{S}_7$
p6b	2	100.0%	?
pb-simp-nonunif	1	1.9%	$\hat{\mathcal{S}}_2$
pigeon-10	119	93.5%	$\mathcal{S}_{30}$, $\mathcal{S}_{60}$, ?
pigeon-11	136	94.4%	$\mathcal{S}_{33}$, $\mathcal{S}_{66}$, ?
pigeon-12	152	95.2%	$\mathcal{S}_{36}$, $\mathcal{S}_{72}$, ?
pigeon-13	169	95.8%	$\mathcal{S}_{39}$, $\mathcal{S}_{78}$, ?
pigeon-19	278	97.8%	$\mathcal{S}_{57}$, $\mathcal{S}_{114}$, ?
protfold	1	98.1%	?
pw-myciel4	2	86.9%	?
qiu	2	100.0%	?
queens-30	1	100.0%	?
rail01	2171	5.6%	$(\mathcal{S}_2)^{931}$, $(\mathcal{S}_3)^{579}$, $(\mathcal{S}_4)^{204}$, $(\mathcal{S}_5)^{170}$, $(\mathcal{S}_6)^{28}$, $(\mathcal{S}_7)^{77}$, $(\mathcal{S}_8)^4$, $(\mathcal{S}_{11})^3$, $(\mathcal{S}_{12})^6$, $(\mathcal{S}_{13})^6$, $(\mathcal{S}_{14})^9$, $(\mathcal{S}_{15})^9$, $(\mathcal{S}_{16})^6$
rail02	35984	13.4%	$(\mathcal{S}_2)^{1533}$, $(\mathcal{S}_3)^{188}$, $(\mathcal{S}_4)^{400}$, $(\mathcal{S}_5)^{149}$, $(\mathcal{S}_6)^{42}$, $(\mathcal{S}_7)^{43}$, $(\mathcal{S}_8)^{69}$, $(\mathcal{S}_9)^9$, $(\mathcal{S}_{10})^8$, $(\mathcal{S}_{11})^3$, $(\mathcal{S}_{12})^{11}$, $(\mathcal{S}_{13})^{22}$, $(\mathcal{S}_{14})^{22}$, $(\mathcal{S}_{15})^{15}$, $(\mathcal{S}_{16})^{16}$, $(\mathcal{S}_{17})^9$, $(\mathcal{S}_{18})^{15}$, $(\mathcal{S}_{19})^{14}$, $(\mathcal{S}_{20})^{28}$, $(\mathcal{S}_{21})^{11}$, $(\mathcal{S}_{22})^{20}$, $(\mathcal{S}_{23})^7$, $(\mathcal{S}_{24})^{17}$, $(\mathcal{S}_{25})^{15}$, $(\mathcal{S}_{26})^{12}$, $(\mathcal{S}_{27})^{11}$, $(\mathcal{S}_{28})^{21}$, $(\mathcal{S}_{29})^6$, $(\mathcal{S}_{30})^{18}$, $(\mathcal{S}_{31})^{11}$, $(\mathcal{S}_{32})^{19}$, $(\mathcal{S}_{33})^8$, $(\mathcal{S}_{34})^{18}$, $(\mathcal{S}_{35})^9$, $(\mathcal{S}_{36})^{21}$, $(\mathcal{S}_{37})^{20}$, $(\mathcal{S}_{38})^{39}$, $(\mathcal{S}_{39})^{26}$, $(\mathcal{S}_{40})^{30}$, $(\mathcal{S}_{41})^{21}$, $(\mathcal{S}_{42})^{44}$, $(\mathcal{S}_{43})^{43}$, $(\mathcal{S}_{44})^{34}$, $(\mathcal{S}_{45})^{23}$, $(\mathcal{S}_{46})^{54}$, $(\mathcal{S}_{47})^2$, $(\mathcal{S}_{48})^{65}$, $(\mathcal{S}_{49})^{10}$, $(\mathcal{S}_{50})^{32}$, $(\mathcal{S}_{51})^8$, $(\mathcal{S}_{52})^4$, $\mathcal{S}_{53}$, $\mathcal{S}_{54}$, $\mathcal{S}_{55}$
rail03	69014	8.6%	$(\mathcal{S}_2)^{1431}$, $(\mathcal{S}_3)^{364}$, $(\mathcal{S}_4)^{342}$, $(\mathcal{S}_5)^{129}$, $(\mathcal{S}_6)^{159}$, $(\mathcal{S}_7)^{16}$, $(\mathcal{S}_8)^{68}$, $(\mathcal{S}_9)^{22}$, $(\mathcal{S}_{11})^{12}$, $(\mathcal{S}_{12})^{38}$, $(\mathcal{S}_{13})^6$, $(\mathcal{S}_{14})^{34}$, $(\mathcal{S}_{15})^9$, $(\mathcal{S}_{16})^3$, $(\mathcal{S}_{17})^{15}$, $(\mathcal{S}_{18})^{27}$, $(\mathcal{S}_{19})^{18}$, $(\mathcal{S}_{20})^7$, $(\mathcal{S}_{21})^{17}$, $(\mathcal{S}_{22})^{30}$, $(\mathcal{S}_{23})^7$, $(\mathcal{S}_{24})^{17}$, $(\mathcal{S}_{25})^{78}$, $(\mathcal{S}_{26})^7$, $(\mathcal{S}_{27})^{19}$, $(\mathcal{S}_{28})^{76}$, $(\mathcal{S}_{29})^{28}$, $(\mathcal{S}_{30})^{42}$, $(\mathcal{S}_{31})^{74}$, $(\mathcal{S}_{32})^{34}$, $(\mathcal{S}_{33})^{72}$, $(\mathcal{S}_{34})^{77}$, $(\mathcal{S}_{35})^{75}$, $(\mathcal{S}_{36})^{77}$, $(\mathcal{S}_{37})^{66}$, $(\mathcal{S}_{38})^{43}$, $(\mathcal{S}_{39})^{44}$, $(\mathcal{S}_{40})^{18}$, $(\mathcal{S}_{41})^{131}$, $(\mathcal{S}_{42})^{164}$, $(\mathcal{S}_{43})^{93}$, $(\mathcal{S}_{44})^{36}$, $(\mathcal{S}_{45})^{36}$, $(\mathcal{S}_{46})^{51}$, $(\mathcal{S}_{47})^{45}$, $(\mathcal{S}_{48})^{21}$, $(\mathcal{S}_{49})^9$, $(\mathcal{S}_{50})^6$, $(\mathcal{S}_{51})^6$, $(\mathcal{S}_{52})^3$, $(\mathcal{S}_{53})^3$, $(\mathcal{S}_{54})^3$
rail507	257	2.6%	$(\mathcal{S}_2)^{788}$, $(\mathcal{S}_3)^{21}$, $\mathcal{S}_6$
ramos3	10	100.0%	?
rococoB10-011000	57	1.0%	$\mathcal{S}_{45}$
rococoC10-001000	63	4.1%	$(\mathcal{S}_2)^{44}$, $\mathcal{S}_{41}$
rococoC11-011100	74	0.8%	$\mathcal{S}_{55}$
rococoC12-111000	412	8.5%	$(\mathcal{S}_5)^{34}$, $(\mathcal{S}_6)^{62}$, $(\mathcal{S}_9)^{14}$, $\mathcal{S}_{62}$
rvb-sub	32	0.6%	$(\mathcal{S}_2)^{103}$
satellites1-25	61	4.4%	$(\mathcal{S}_2)^{200}$
satellites2-60-fs	607	5.1%	$(\mathcal{S}_2)^6$, $(?)^8$
satellites2-60	181	3.4%	$(\mathcal{S}_2)^{600}$
satellites3-40-fs	1180	4.2%	$(?)^{78}$
satellites3-40	341	2.8%	$(\mathcal{S}_2)^{1131}$

sct1	3337	64.1%	$(\hat{\mathcal{S}}_2)^{327}, (\mathcal{S}_2)^{4}, (\mathcal{S}_3)^{211}, (\hat{\mathcal{S}}_4)^{23}, (\mathcal{S}_4)^{594}, (\mathcal{S}_5)^{17}, (\mathcal{S}_6)^{121}, (\mathcal{S}_7)^{5}, \mathcal{S}_{471}, ?$
sct32	397	49.1%	$(\hat{\mathcal{S}}_2)^{11}, (\mathcal{S}_2)^{150}, (\mathcal{S}_3)^{15}, (\hat{\mathcal{S}}_3)^{110}, (\hat{\mathcal{S}}_4)^{12}, \mathcal{S}_4, (\hat{\mathcal{S}}_5)^{4}, (\hat{\mathcal{S}}_6)^{15}, (\hat{\mathcal{S}}_7)^{4}, \hat{\mathcal{S}}_{24}, (?)^{3}$
sct5	3063	76.5%	$(\hat{\mathcal{S}}_2)^{4}, (\mathcal{S}_2)^{314}, (\hat{\mathcal{S}}_3)^{3}, (\hat{\mathcal{S}}_4)^{161}, \mathcal{S}_4, (\mathcal{S}_5)^{65}, (\hat{\mathcal{S}}_5)^{7}, (\hat{\mathcal{S}}_6)^{3}, (\mathcal{S}_6)^{64}, (\mathcal{S}_7)^{9}, (\hat{\mathcal{S}}_7)^{3}, (\mathcal{S}_8)^{6}, (\hat{\mathcal{S}}_8)^{5}, (\mathcal{S}_9)^{10}, (\hat{\mathcal{S}}_9)^{3}, (\mathcal{S}_{10})^{13}, ?$
seymour-disj-10	19	8.8%	$(\mathcal{S}_2)^{41}, \hat{\mathcal{S}}_2, (\mathcal{S}_3)^{4}, (\mathcal{S}_4)^{2}$
seymour	235	19.9%	$\hat{\mathcal{S}}_2, (\mathcal{S}_2)^{43}, (\mathcal{S}_3)^{4}, (\mathcal{S}_4)^{3}, \mathcal{S}_6, \mathcal{S}_{117}, ?$
shipsched	1	0.5%	$\hat{\mathcal{S}}_2$
shs1023	1	13.5%	$\hat{\mathcal{S}}_2$
siena1	147	4.7%	$(\mathcal{S}_2)^{271}, (\mathcal{S}_3)^{14}, (\mathcal{S}_5)^{2}, \mathcal{S}_7, \mathcal{S}_{11}, \mathcal{S}_{34}$
sing161	1	10.8%	$(\hat{\mathcal{S}}_2)^{2}$
sing2	1	13.7%	$\hat{\mathcal{S}}_2$
sing245	1	5.3%	$\hat{\mathcal{S}}_2$
splan1	≥ 1166	$\geq 0.3\%$	$(\mathcal{S}_2)^{94}, (\mathcal{S}_3)^{449}, (\mathcal{S}_4)^{571}$
stp3d	179	1.6%	$(\hat{\mathcal{S}}_2)^{594}$
sts405	8	100.0%	?
sts729	20	100.0%	?
swath	817	7.1%	$(\mathcal{S}_4)^{20}, \mathcal{S}_{83}, \mathcal{S}_{320}$
t1717	54604	90.2%	$(\mathcal{S}_2)^{3015}, (\mathcal{S}_3)^{1607}, (\mathcal{S}_4)^{1045}, (\mathcal{S}_5)^{680}, (\mathcal{S}_6)^{550}, (\mathcal{S}_7)^{346}, (\mathcal{S}_8)^{302}, (\mathcal{S}_9)^{237}, (\mathcal{S}_{10})^{181}, (\mathcal{S}_{11})^{149}, (\mathcal{S}_{12})^{111}, (\mathcal{S}_{13})^{95}, (\mathcal{S}_{14})^{97}, (\mathcal{S}_{15})^{71}, (\mathcal{S}_{16})^{55}, (\mathcal{S}_{17})^{55}, (\mathcal{S}_{18})^{41}, (\mathcal{S}_{19})^{31}, (\mathcal{S}_{20})^{39}, (\mathcal{S}_{21})^{33}, (\mathcal{S}_{22})^{31}, (\mathcal{S}_{23})^{30}, (\mathcal{S}_{24})^{23}, (\mathcal{S}_{25})^{18}, (\mathcal{S}_{26})^{16}, (\mathcal{S}_{27})^{13}, (\mathcal{S}_{28})^{17}, (\mathcal{S}_{29})^{17}, (\mathcal{S}_{30})^{19}, (\mathcal{S}_{31})^{15}, (\mathcal{S}_{32})^{11}, (\mathcal{S}_{33})^{17}, (\mathcal{S}_{34})^{19}, (\mathcal{S}_{35})^{14}, (\mathcal{S}_{36})^{14}, (\mathcal{S}_{37})^{8}, (\mathcal{S}_{38})^{14}, (\mathcal{S}_{39})^{7}, (\mathcal{S}_{40})^{11}, (\mathcal{S}_{41})^{11}, (\mathcal{S}_{42})^{6}, (\mathcal{S}_{43})^{8}, (\mathcal{S}_{44})^{6}, (\mathcal{S}_{45})^{6}, (\mathcal{S}_{46})^{5}, (\mathcal{S}_{47})^{6}, (\mathcal{S}_{48})^{5}, (\mathcal{S}_{49})^{7}, (\mathcal{S}_{50})^{3}, (\mathcal{S}_{51})^{5}, (\mathcal{S}_{52})^{4}, (\mathcal{S}_{53})^{2}, (\mathcal{S}_{54})^{4}, (\mathcal{S}_{55})^{5}, \mathcal{S}_{56}, (\mathcal{S}_{57})^{4}, (\mathcal{S}_{58})^{4}, (\mathcal{S}_{59})^{5}, (\mathcal{S}_{60})^{4}, (\mathcal{S}_{61})^{3}, (\mathcal{S}_{62})^{4}, (\mathcal{S}_{63})^{3}, (\mathcal{S}_{64})^{4}, (\mathcal{S}_{65})^{4}, (\mathcal{S}_{66})^{3}, (\mathcal{S}_{67})^{3}, (\mathcal{S}_{68})^{6}, \mathcal{S}_{69}, (\mathcal{S}_{70})^{4}, (\mathcal{S}_{72})^{2}, (\mathcal{S}_{73})^{3}, (\mathcal{S}_{74})^{2}, \mathcal{S}_{75}, (\mathcal{S}_{76})^{2}, (\mathcal{S}_{77})^{2}, \mathcal{S}_{78}, (\mathcal{S}_{79})^{2}, (\mathcal{S}_{80})^{2}, (\mathcal{S}_{82})^{2}, \mathcal{S}_{84}, (\mathcal{S}_{85})^{3}, (\mathcal{S}_{86})^{2}, \mathcal{S}_{87}, \mathcal{S}_{90}, (\mathcal{S}_{91})^{2}, (\mathcal{S}_{93})^{3}, \mathcal{S}_{94}, (\mathcal{S}_{97})^{2}, (\mathcal{S}_{100})^{3}, \mathcal{S}_{101}, \mathcal{S}_{102}, (\mathcal{S}_{106})^{2}, \mathcal{S}_{108}, (\mathcal{S}_{109})^{2}, (\mathcal{S}_{112})^{2}, \mathcal{S}_{113}, \mathcal{S}_{119}, (\mathcal{S}_{121})^{2}, \mathcal{S}_{129}, (\mathcal{S}_{131})^{2}, \mathcal{S}_{132}, \mathcal{S}_{137}, \mathcal{S}_{138}, \mathcal{S}_{141}, \mathcal{S}_{146}, \mathcal{S}_{154}, (\mathcal{S}_{156})^{2}, \mathcal{S}_{157}, \mathcal{S}_{158}, \mathcal{S}_{160}, \mathcal{S}_{184}, \mathcal{S}_{243}, \mathcal{S}_{262}, \mathcal{S}_{356}, \mathcal{S}_{358}, \mathcal{S}_{360}$
t1722	24390	89.5%	$(\mathcal{S}_2)^{1822}, (\mathcal{S}_3)^{977}, (\mathcal{S}_4)^{583}, (\mathcal{S}_5)^{393}, (\mathcal{S}_6)^{314}, (\mathcal{S}_7)^{187}, (\mathcal{S}_8)^{153}, (\mathcal{S}_9)^{102}, (\mathcal{S}_{10})^{93}, (\mathcal{S}_{11})^{75}, (\mathcal{S}_{12})^{65}, (\mathcal{S}_{13})^{47}, (\mathcal{S}_{14})^{37}, (\mathcal{S}_{15})^{35}, (\mathcal{S}_{16})^{31}, (\mathcal{S}_{17})^{33}, (\mathcal{S}_{18})^{21}, (\mathcal{S}_{19})^{24}, (\mathcal{S}_{20})^{15}, (\mathcal{S}_{21})^{13}, (\mathcal{S}_{22})^{22}, (\mathcal{S}_{23})^{14}, (\mathcal{S}_{24})^{10}, (\mathcal{S}_{25})^{6}, (\mathcal{S}_{26})^{11}, (\mathcal{S}_{27})^{5}, (\mathcal{S}_{28})^{9}, (\mathcal{S}_{29})^{6}, (\mathcal{S}_{30})^{5}, (\mathcal{S}_{31})^{4}, (\mathcal{S}_{32})^{6}, (\mathcal{S}_{33})^{3}, (\mathcal{S}_{34})^{7}, (\mathcal{S}_{35})^{7}, (\mathcal{S}_{36})^{5}, (\mathcal{S}_{37})^{8}, (\mathcal{S}_{38})^{3}, (\mathcal{S}_{39})^{6}, (\mathcal{S}_{40})^{4}, (\mathcal{S}_{41})^{4}, (\mathcal{S}_{42})^{2}, (\mathcal{S}_{43})^{2}, \mathcal{S}_{44}, (\mathcal{S}_{45})^{2}, (\mathcal{S}_{46})^{4}, (\mathcal{S}_{47})^{2}, (\mathcal{S}_{48})^{3}, (\mathcal{S}_{49})^{2}, \mathcal{S}_{50}, \mathcal{S}_{51}, (\mathcal{S}_{52})^{3}, \mathcal{S}_{53}, \mathcal{S}_{54}, \mathcal{S}_{55}, \mathcal{S}_{56}, (\mathcal{S}_{57})^{4}, (\mathcal{S}_{58})^{2}, \mathcal{S}_{59}, \mathcal{S}_{63}, (\mathcal{S}_{65})^{2}, \mathcal{S}_{66}, \mathcal{S}_{67}, \mathcal{S}_{68}, \mathcal{S}_{69}, \mathcal{S}_{73}, \mathcal{S}_{74}, \mathcal{S}_{76}, \mathcal{S}_{79}, (\mathcal{S}_{80})^{3}, \mathcal{S}_{82}, \mathcal{S}_{83}, \mathcal{S}_{84}, (\mathcal{S}_{86})^{2}, \mathcal{S}_{87}, \mathcal{S}_{89}, (\mathcal{S}_{97})^{2}, \mathcal{S}_{98}, \mathcal{S}_{100}, \mathcal{S}_{123}, \mathcal{S}_{133}, \mathcal{S}_{148}, \mathcal{S}_{158}, (\mathcal{S}_{159})^{2}, \mathcal{S}_{178}, \mathcal{S}_{185}, \mathcal{S}_{221}, \mathcal{S}_{226}, \mathcal{S}_{292}$

tanglegram1	≥ 68331	$\geq 97.6\%$	$(\mathcal{S}_2)^{95}$, $(\mathcal{S}_3)^{70}$, $(\mathcal{S}_4)^{47}$, $(\mathcal{S}_5)^{31}$, $(\mathcal{S}_6)^{22}$, $(\mathcal{S}_7)^{21}$, $(\mathcal{S}_8)^{28}$, $(\mathcal{S}_9)^{32}$, $(\mathcal{S}_{10})^{15}$, $(\mathcal{S}_{11})^{6}$, $(\mathcal{S}_{12})^{16}$, $(\mathcal{S}_{13})^{11}$, $(\mathcal{S}_{14})^{6}$, $(\mathcal{S}_{15})^{6}$, $(\mathcal{S}_{16})^{11}$, $(\mathcal{S}_{18})^{6}$, $\mathcal{S}_{19}$, $(\mathcal{S}_{20})^{6}$, $(\mathcal{S}_{21})^{4}$, $\mathcal{S}_{22}$, $(\mathcal{S}_{23})^{2}$, $(\mathcal{S}_{24})^{8}$, $(\mathcal{S}_{25})^{2}$, $(\mathcal{S}_{26})^{3}$, $(\mathcal{S}_{27})^{4}$, $(\mathcal{S}_{28})^{2}$, $\mathcal{S}_{29}$, $(\mathcal{S}_{30})^{6}$, $\mathcal{S}_{31}$, $(\mathcal{S}_{32})^{10}$, $(\mathcal{S}_{34})^{2}$, $(\mathcal{S}_{35})^{4}$, $\mathcal{S}_{36}$, $(\mathcal{S}_{38})^{2}$, $(\mathcal{S}_{39})^{3}$, $(\mathcal{S}_{40})^{2}$, $(\mathcal{S}_{42})^{3}$, $\mathcal{S}_{44}$, $\mathcal{S}_{45}$, $(\mathcal{S}_{48})^{2}$, $(\mathcal{S}_{49})^{2}$, $\mathcal{S}_{52}$, $\mathcal{S}_{53}$, $(\mathcal{S}_{54})^{3}$, $(\mathcal{S}_{55})^{2}$, $(\mathcal{S}_{56})^{3}$, $\mathcal{S}_{57}$, $(\mathcal{S}_{58})^{4}$, $\mathcal{S}_{59}$, $\mathcal{S}_{60}$, $(\mathcal{S}_{62})^{2}$, $(\mathcal{S}_{64})^{3}$, $\mathcal{S}_{65}$, $\mathcal{S}_{67}$, $\mathcal{S}_{68}$, $(\mathcal{S}_{70})^{4}$, $(\mathcal{S}_{72})^{4}$, $\mathcal{S}_{73}$, $\mathcal{S}_{76}$, $(\mathcal{S}_{77})^{2}$, $\mathcal{S}_{78}$, $\mathcal{S}_{81}$, $\mathcal{S}_{84}$, $\mathcal{S}_{85}$, $\mathcal{S}_{87}$, $\mathcal{S}_{88}$, $(\mathcal{S}_{91})^{2}$, $\mathcal{S}_{96}$, $\mathcal{S}_{105}$, $\mathcal{S}_{108}$, $\mathcal{S}_{110}$, $\mathcal{S}_{111}$, $(\mathcal{S}_{112})^{2}$, $\mathcal{S}_{117}$, $\mathcal{S}_{120}$, $\mathcal{S}_{124}$, $\mathcal{S}_{126}$, $(\mathcal{S}_{128})^{4}$, $\mathcal{S}_{130}$, $\mathcal{S}_{138}$, $\mathcal{S}_{140}$, $(\mathcal{S}_{144})^{2}$, $\mathcal{S}_{149}$, $(\mathcal{S}_{160})^{2}$, $\mathcal{S}_{161}$, $\mathcal{S}_{162}$, $\mathcal{S}_{168}$, $\mathcal{S}_{174}$, $\mathcal{S}_{185}$, $\mathcal{S}_{186}$, $\mathcal{S}_{196}$, $\mathcal{S}_{202}$, $(\mathcal{S}_{204})^{2}$, $\mathcal{S}_{214}$, $\mathcal{S}_{216}$, $\mathcal{S}_{229}$, $\mathcal{S}_{234}$, $\mathcal{S}_{240}$, $\mathcal{S}_{250}$, $\mathcal{S}_{273}$, $\mathcal{S}_{285}$, $\mathcal{S}_{290}$, $\mathcal{S}_{292}$, $\mathcal{S}_{309}$, $\mathcal{S}_{385}$, $\mathcal{S}_{386}$, $\mathcal{S}_{410}$, $\mathcal{S}_{432}$, $\mathcal{S}_{441}$, $\mathcal{S}_{444}$, $\mathcal{S}_{446}$, $\mathcal{S}_{464}$, $\mathcal{S}_{474}$, $\mathcal{S}_{515}$, $\mathcal{S}_{537}$, $\mathcal{S}_{581}$, $\mathcal{S}_{584}$, $(\mathcal{S}_{609})^{2}$, $\mathcal{S}_{640}$, $\mathcal{S}_{665}$, $\mathcal{S}_{791}$, $\mathcal{S}_{845}$, $\mathcal{S}_{1008}$, $\mathcal{S}_{1020}$, $\mathcal{S}_{1307}$, $\mathcal{S}_{1320}$, $\mathcal{S}_{1722}$, $\mathcal{S}_{1886}$
tanglegram2	6074	95.5%	$(\hat{\mathcal{S}}_2)^{3}$, $(\mathcal{S}_2)^{45}$, $(\mathcal{S}_3)^{26}$, $(\hat{\mathcal{S}}_3)^{2}$, $(\mathcal{S}_4)^{25}$, $\hat{\mathcal{S}}_5$, $(\mathcal{S}_5)^{11}$, $(\mathcal{S}_6)^{10}$, $(\mathcal{S}_7)^{3}$, $(\mathcal{S}_8)^{9}$, $(\mathcal{S}_9)^{9}$, $(\mathcal{S}_{10})^{8}$, $(\mathcal{S}_{11})^{6}$, $(\mathcal{S}_{12})^{7}$, $(\mathcal{S}_{14})^{4}$, $(\mathcal{S}_{15})^{10}$, $(\mathcal{S}_{16})^{3}$, $\mathcal{S}_{19}$, $(\mathcal{S}_{20})^{6}$, $(\mathcal{S}_{22})^{7}$, $\mathcal{S}_{25}$, $(\mathcal{S}_{27})^{2}$, $\mathcal{S}_{28}$, $\mathcal{S}_{30}$, $(\mathcal{S}_{31})^{2}$, $(\mathcal{S}_{36})^{2}$, $\mathcal{S}_{40}$, $\mathcal{S}_{41}$, $\mathcal{S}_{44}$, $(\mathcal{S}_{48})^{3}$, $\mathcal{S}_{49}$, $\mathcal{S}_{50}$, $\mathcal{S}_{55}$, $\mathcal{S}_{59}$, $(\mathcal{S}_{60})^{2}$, $\mathcal{S}_{89}$, $\mathcal{S}_{98}$, $\mathcal{S}_{108}$, $\mathcal{S}_{112}$, $\mathcal{S}_{130}$, $\mathcal{S}_{154}$, $\mathcal{S}_{193}$, $\mathcal{S}_{236}$, $\mathcal{S}_{287}$, $\mathcal{S}_{297}$, $\mathcal{S}_{425}$, ?
timtab1	1	0.5%	$\mathcal{S}_2$
toll-like	141	37.8%	$(\hat{\mathcal{S}}_2)^{18}$, $(\mathcal{S}_2)^{230}$, $\hat{\mathcal{S}}_5$, ?
transportmoment	6	1.7%	$(\hat{\mathcal{S}}_2)^{13}$, $(\hat{\mathcal{S}}_3)^{2}$
uc-case11	1	5.9%	$\hat{\mathcal{S}}_3$
uc-case3	1	14.2%	$(\hat{\mathcal{S}}_2)^{2}$
uct-subprob	30	14.0%	$(\hat{\mathcal{S}}_2)^{59}$, $(\hat{\mathcal{S}}_3)^{8}$, $\hat{\mathcal{S}}_4$, $\hat{\mathcal{S}}_7$
unitcal_7	305	52.3%	$(\mathcal{S}_2)^{672}$, $(\hat{\mathcal{S}}_2)^{3}$, ?
van	16060	39.5%	$\mathcal{S}_{4928}$
vpphard	≥ 39973	$\geq 86.7\%$	$(\mathcal{S}_2)^{3771}$, $(\mathcal{S}_3)^{3343}$, $(\mathcal{S}_4)^{1602}$, $(\mathcal{S}_5)^{354}$, $(\mathcal{S}_6)^{140}$, $(\mathcal{S}_7)^{96}$, $(\mathcal{S}_8)^{79}$, $(\mathcal{S}_9)^{58}$, $(\mathcal{S}_{10})^{47}$, $(\mathcal{S}_{11})^{25}$, $(\mathcal{S}_{12})^{42}$, $(\mathcal{S}_{13})^{16}$, $(\mathcal{S}_{14})^{24}$, $(\mathcal{S}_{15})^{26}$, $(\mathcal{S}_{16})^{15}$, $(\mathcal{S}_{17})^{8}$, $(\mathcal{S}_{18})^{10}$, $(\mathcal{S}_{19})^{13}$, $(\mathcal{S}_{23})^{5}$, $(\mathcal{S}_{26})^{3}$, $(\mathcal{S}_{30})^{3}$, $(\mathcal{S}_{42})^{5}$, $(\mathcal{S}_{45})^{3}$, $(\mathcal{S}_{49})^{10}$, $(\mathcal{S}_{50})^{5}$, $(\mathcal{S}_{51})^{10}$, $(\mathcal{S}_{53})^{10}$, $(\mathcal{S}_{56})^{10}$, $(\mathcal{S}_{57})^{25}$, $(\mathcal{S}_{59})^{10}$, $(\mathcal{S}_{60})^{5}$, $(\mathcal{S}_{62})^{5}$, $(\mathcal{S}_{63})^{5}$, $(\mathcal{S}_{67})^{10}$, $(\mathcal{S}_{69})^{5}$, $(\mathcal{S}_{83})^{5}$, $\mathcal{S}_{5912}$
vpphard2	**?**	?	?
wachplan	2	96.6%	?
zib54-UUE	1	2.4%	$\hat{\mathcal{S}}_2$

Nomenclature

$\cdot^{-}$	inverse of a group element, page 3
$\langle \cdot, \cdot \rangle$	Euclidean inner product in $\mathbb{R}^n$, page 3
$\cdot\vert_V$	orthogonal projection onto linear subspace V, page 10
$[n]$	set of numbers $1, \dots, n$, page 3
$\mathbb{1}$	all-ones vector, page 3
$\operatorname{aff} S$	affine hull of a set S, page 3
$\mathcal{A}_n$	alternating group of degree n, page 19
A_n	root lattice, page 3
A_n^*	dual lattice of A_n, page 3
$\mathrm{bw}(z)$	box width of an integral point z, page 44
$\mathcal{C}_n$	cyclic group of order n, page 4
$\operatorname{cone} S$	conic (positive) hull of a set S, page 3
$\operatorname{conv} S$	convex hull of a set S, page 3
$\mathrm{core}(G)$	set of all core points of a group G, page 7
$\mathrm{core}(G, S)$	set of core points of a group G that are contained in a set S, page 7
$\mathrm{core}_{/}(G)$	G-orbit representatives of the core set of a group G, page 91
$e^{(i)}$	i-th standard basis vector, page 3
η	quadratic character of a finite field, page 29
$\mathrm{fcore}(G)$	fundamental core set of a group G, page 8
$\mathrm{Fix}(G)$	fixed space of a group G, page 5
$\mathrm{Fix}_{\mathbb{Z}}(G)$	integral points in the fixes space of G, page 5
$\mathbb{F}_q^*$	multiplicative group of field $\mathbb{F}_q$, page 26
$\mathrm{GL}_n(R)$	group of invertible $n \times n$ matrices over a ring R, page 3
$I_G(S)$	intersection number of a set S in a permutation group G, page 40
Λ^*	dual lattice of a lattice Λ, page 3
$\operatorname{span} S$	linear hull of a set S, page 3

$\omega(C)$	width of a convex set C, page 6
$\omega(C, v)$	width of a convex set C in direction v, page 6
$\omega_\Lambda(C)$	Λ-lattice width of a convex set C, page 6
$\mathcal{S}$	set of squares in a finite field, page 26
$\mathcal{S}_n$	symmetric group; all permutations of n elements, page 5
$\hat{\mathcal{S}}_n$	diagonal of a symmetric group of degree n, page 111
$\operatorname{span}_{\mathbb{Z}}(B)$	lattice with basis B, page 97
$\operatorname{Stab}_G(S)$	stabilizer of a set S in a permutation group G, page 19
$\operatorname{vert} P$	vertices of a polytope P, page 7
$\mathbb{Z}^n_{(k)}$	layer with index k, page 15

References

Bibliography

[ABSS97] Sanjeev Arora, László Babai, Jacques Stern, and Z. Sweedyk. The hardness of approximate optima in lattices, codes, and systems of linear equations. *J. Comput. System Sci.*, 54(2, part 2):317–331, 1997. 34th Annual Symposium on Foundations of Computer Science (Palo Alto, CA, 1993).

[AL04] Karen Aardal and Arjen K. Lenstra. Hard equality constrained integer knapsacks. *Math. Oper. Res.*, 29(3):724–738, 2004.

[AWW11] Gennadiy Averkov, Christian Wagner, and Robert Weismantel. Maximal lattice-free polyhedra: finiteness and an explicit description in dimension three. *Math. Oper. Res.*, 36(4):721–742, 2011.

[Ban95] Wojciech Banaszczyk. Inequalities for convex bodies and polar reciprocal lattices in $\mathbf{R}^n$. *Discrete Comput. Geom.*, 13(2):217–231, 1995.

[Bar02] Alexander Barvinok. *A course in convexity.* Graduate Studies in Mathematics. 54. Providence, RI: American Mathematical Society (AMS), 2002.

[BB05] Alexander Barvinok and Grigoriy Blekherman. Convex geometry of orbits. In *Combinatorial and computational geometry*, volume 52 of *Math. Sci. Res. Inst. Publ.*, pages 51–77. Cambridge Univ. Press, Cambridge, 2005.

[BBBK11] Margherita Barile, Dominique Bernardi, Alexander Borisov, and Jean-Michel Kantor. On empty lattice simplices in dimension 4. *Proc. Amer. Math. Soc.*, 139(12):4247–4253, 2011.

[BDP$^+$12] David Bremner, Mathieu Dutour Sikirić, Dmitrii V. Pasechnik, Thomas Rehn, and Achill Schürmann. Computing symmetry groups of polyhedra, 2012. submitted.

[BDS09] David Bremner, Mathieu Dutour Sikiric, and Achill Schürmann. Polyhedral representation conversion up to symmetries. In David Avis, David Bremner, and Antoine Deza, editors, *Polyhedral computation*, CRM Proceedings & Lecture Notes, pages 45–72. American Mathematical Society, 2009.

[BHJ13] Richard Bödi, Katrin Herr, and Michael Joswig. Algorithms for highly symmetric linear and integer programs. *Math. Program., Ser. A*, 137:65–90, 2013. 10.1007/s10107-011-0487-6.

[BIS12] Winfried Bruns, Bogdan Ichim, and Christof Söger. The Power of Pyramid Decomposition in normaliz, 2012. preprint at `arXiv:1206.1916`.

[BK00] Imre Bárány and Jean-Michel Kantor. On the number of lattice free polytopes. *European J. Combin.*, 21(1):103–110, 2000. Combinatorics of polytopes.

[BLPS99] Wojciech Banaszczyk, Alexander E. Litvak, Alain Pajor, and Stanislaw J. Szarek. The flatness theorem for nonsymmetric convex bodies via the local theory of Banach spaces. *Math. Oper. Res.*, 24(3):728–750, 1999.

[Cam72] Peter J. Cameron. Bounding the rank of certain permutation groups. *Math. Z.*, 124:343–352, 1972.

[Cam99] Peter J. Cameron. *Permutation groups*, volume 45 of *London Mathematical Society Student Texts.* Cambridge University Press, Cambridge, 1999.

[CS99] J. H. Conway and N. J. A. Sloane. *Sphere packings, lattices and groups*, volume 290 of *Grundlehren der Mathematischen Wissenschaften [Fundamental Principles of Mathematical Sciences].* Springer-Verlag, New York, third edition, 1999. With additional contributions by E. Bannai, R. E. Borcherds, J. Leech, S. P. Norton, A. M. Odlyzko, R. A. Parker, L. Queen and B. B. Venkov.

[Dav79] Philip J. Davis. *Circulant Matrices.* John Wiley & Sons, New York-Chichester-Brisbane, 1979. A Wiley-Interscience Publication, Pure and Applied Mathematics.

[dBvKOS98] Mark de Berg, Marc van Kreveld, Mark Overmars, and Otfried Schwarzkopf. *Computational Geometry: Algorithms and Applications.* Springer, 3rd edition, 1998.

[De 05] Jesús A. De Loera. The many aspects of counting lattice points in polytopes. *Math. Semesterber.*, 52(2):175–195, 2005.

[Dix05] John D. Dixon. Permutation representations and rational irreducibility. *Bull. Austral. Math. Soc.*, 71(3):493–503, 2005.

[DO95] Michel Deza and Shmuel Onn. Lattice-free polytopes and their diameter. *Discrete Comput. Geom.*, 13(1):59–75, 1995.

[EL05] Friedrich Eisenbrand and Sören Laue. A linear algorithm for integer programming in the plane. *Math. Program., Ser. A*, 102(2):249–259, 2005.

[FL12] Matteo Fischetti and Leo Liberti. Orbital Shrinking. In A.Ridha Mahjoub, Vangelis Markakis, Ioannis Milis, and Vangelis Th. Paschos, editors, *Combinatorial Optimization*, volume 7422 of *Lecture Notes in Computer Science*, pages 48–58. Springer Berlin Heidelberg, 2012.

[Fri07] Eric J. Friedman. Fundamental domains for integer programs with symmetries. In *Combinatorial optimization and applications*, volume 4616 of *Lecture Notes in Comput. Sci.*, pages 146–153. Springer, Berlin, 2007.

[Fuk04] Komei Fukuda. Polyhedral computation FAQ, 2004. `http://www.ifor.math.ethz.ch/~fukuda/polyfaq/polyfaq.html`.

[Ges72] Ira Gessel. Fibonacci is a square. *Fibonacci Quarterly*, 10(4):417–419, October 1972.

[GJ00] Ewgenij Gawrilow and Michael Joswig. polymake: a framework for analyzing convex polytopes. In *Polytopes—combinatorics and computation (Oberwolfach, 1997)*, volume 29 of *DMV Sem.*, pages 43–73. Birkhäuser, Basel, 2000.

[GP04] Karin Gatermann and Pablo A. Parrilo. Symmetry groups, semidefinite programs, and sums of squares. *Journal of Pure and Appl. Algebra*, 192(1–3):95–128, 2004.

[GZ02] Liyan Gao and Yin Zhang. Computational Experience with Lenstra's Algorithm. Technical Report TR02-12, Department of Computational and Applied Mathematics, Rice University, 2002.

[Hal59] Marshall Hall Jr. *The Theory of Groups.* The Macmillan Co., New York, N.Y., 1959.

[Han10] Guillaume Hanrot. LLL: A Tool for Effective Diophantine Approximation. In P. Q. Nguyen and B. Vallée, editors, *The LLL Algorithm: Survey and Applications*, Information Security and Cryptography, pages 215–264. Springer Berlin Heidelberg, 2010.

[HB82] Bertram Huppert and Norman Blackburn. *Finite groups. III*, volume 243 of *Grundlehren der Mathematischen Wissenschaften [Fundamental Principles of Mathematical Sciences].* Springer-Verlag, Berlin, 1982.

[Her13a] Katrin Herr. Private communication, 2013.

[Her13b] Katrin Herr. *Core Sets and Symmetric Convex Optimization.* PhD thesis, TU Darmstadt, 2013.

[HMPW12] Eszter K. Horváth, Géza Makay, Reinhard Pöschel, and Tamás Waldhauser. Invariance groups of finite functions and orbit equivalence of permutation groups, 2012. preprint at `http://arxiv.org/abs/1210.1015`.

[HRS13] Katrin Herr, Thomas Rehn, and Achill Schürmann. Exploiting Symmetry in Integer Convex Optimization using Core Points. *Operations Research Letters*, 41:298–304, 2013.

[Hul10] Alexander Hulpke. Notes on Computational Group Theory, 2010. Lecture Notes.

[Hur90] Cor A. J. Hurkens. Blowing up convex sets in the plane. *Linear Algebra Appl.*, 134:121–128, 1990.

[HZ00] Christian Haase and Günter M. Ziegler. On the maximal width of empty lattice simplices. *European J. Combin.*, 21(1):111–119, 2000. Combinatorics of polytopes.

[Iwa03] Shiro Iwasaki. Translations of the squares in a finite field and an infinite family of 3-designs. *European J. Combin.*, 24(3):253–266, 2003.

[Jam09] Phillip James. When is a number Fibonacci? Technical report, Department of Computer Science, Swansea University, January 2009.

[JL01] Gordon James and Martin Liebeck. *Representations and Characters of Groups.* Cambridge Univ. Press, 2nd edition, 2001.

[Joh48] Fritz John. Extremum problems with inequalities as subsidiary conditions. In *Studies and Essays Presented to R. Courant on his 60th Birthday, January 8, 1948*, pages 187–204. Interscience Publishers, Inc., New York, N. Y., 1948.

[KAA$^+$11] Thorsten Koch, Tobias Achterberg, Erling Andersen, Oliver Bastert, Timo Berthold, Robert E. Bixby, Emilie Danna, Gerald Gamrath, Ambros M. Gleixner, Stefan Heinz, Andrea Lodi, Hans Mittelmann, Ted Ralphs, Domenico Salvagnin, Daniel E. Steffy, and Kati Wolter. MIPLIB 2010: mixed integer programming library version 5. *Math. Program. Comput.*, 3(2):103–163, 2011.

[Kan69] William M. Kantor. Automorphism groups of designs. *Math. Z.*, 109:246–252, 1969.

[Kan72] William M. Kantor. k-homogeneous groups. *Math. Z.*, 124:261–265, 1972.

[Kan99] Jean-Michel Kantor. On the width of lattice-free simplices. *Compositio Math.*, 118(3):235–241, 1999.

[KBB$^+$08] Leonid Khachiyan, Endre Boros, Konrad Borys, Khaled Elbassioni, and Vladimir Gurvich. Generating all vertices of a polyhedron is hard. *Discrete Comput. Geom.*, 39(1-3):174–190, 2008.

[Khi48] Aleksandr Ya. Khinchin. A quantitative formulation of the approximation theory of Kronecker. *Izvestiya Akad. Nauk SSSR. Ser. Mat.*, 12:113–122, 1948.

[Khi63] Aleksandr Ya. Khinchin. *Continued fractions.* Translated by Peter Wynn. P. Noordhoff Ltd., Groningen, 1963.

[Knö11] Reinhard Knörr. Private communication, 2011.

[Knu91] Donald E. Knuth. Efficient representation of perm groups. *Combinatorica*, 11(1):33–43, 1991.

[KP08] Volker Kaibel and Marc E. Pfetsch. Packing and Partitioning Orbitopes. *Math. Program., Ser.A*, 114:1–36, 2008.

[Len83] Hendrik W. Lenstra. Integer programming with a fixed number of variables. *Math. Oper. Res.*, 8(4):538–548, 1983.

[Lib08] Leo Liberti. Automatic generation of symmetry-breaking constraints. In *Combinatorial optimization and applications*, volume 5165 of *Lecture Notes in Comput. Sci.*, pages 328–338. Springer, Berlin, 2008.

[Lib12] Leo Liberti. Reformulations in mathematical programming: automatic symmetry detection and exploitation. *Math. Program.*, 131(1-2):273–304, 2012.

[LN08] Rudolf Lidl and Harald Niederreiter. *Finite Fields.* Encyclopedia of Mathematics and its Applications. Cambridge University Press, 2008.

[Lov89] László Lovász. Geometry of numbers and integer programming. In *Mathematical programming (Tokyo, 1988)*, volume 6 of *Math. Appl. (Japanese Ser.)*, pages 177–201. SCIPRESS, Tokyo, 1989.

[Mar03] François Margot. Exploiting orbits in symmetric ILP. *Math. Program.*, 98(1-3):3–21, 2003.

[Mar10] François Margot. Symmetry in Integer Linear Programming. In *50 Years of Integer Programming 1958-2008*, chapter 17, pages 647–686. Springer, 2010.

[Onn93] Shmuel Onn. Geometry, complexity, and combinatorics of permutation polytopes. *J. Combin. Theory Ser. A*, 64(1):31–49, 1993.

[Ost09] James Ostrowski. *Symmetry in Integer Programming.* PhD thesis, Lehigh University, 2009.

[PK10] Dmitrii V. Pasechnik and Keshav Kini. A GAP package for computation with coherent configurations. In *Proceedings of the Third international congress conference on Mathematical software*, ICMS'10, pages 69–72, Berlin, Heidelberg, 2010. Springer-Verlag.

[PR13] Marc E. Pfetch and Thomas Rehn. Symmetry handling in integer programs revisited, 2013. in preparation.

[Pug05] Jean-François Puget. Automatic Detection of Variable and Value Symmetries. In *Principles and Practice of Constraint Programming - CP 2005*, pages 475–489, 2005.

[Ree57] John E. Reeve. On the volume of lattice polyhedra. *Proc. London Math. Soc. (3)*, 7:378–395, 1957.

[Rem30] Robert Remak. Über die Darstellung der endlichen Gruppen als Untergruppen direkter Produkte. *J. Reine Angew. Mathematik*, 163:1–44, 1930.

[RS10] Thomas Rehn and Achill Schürmann. C++ tools for exploiting polyhedral symmetries. In *Proceedings of the Third international congress conference on Mathematical software*, ICMS'10, pages 295–298, Berlin, Heidelberg, 2010. Springer-Verlag.

[S$^+$13] W. A. Stein et al. *Sage Mathematics Software (Version 5.9).* The Sage Development Team, 2013.

[Sal05] Domenico Salvagnin. A dominance procedure for integer programming, 2005. Master's Thesis, University of Padova.

[Sal12] Domenico Salvagnin, 2012. Private communication.

[Sch98] Alexander Schrijver. *Theory of linear and integer programming.* Wiley, 1998.

[Seb99] András Sebő. An introduction to empty lattice simplices. In *Integer programming and combinatorial optimization (Graz, 1999)*, volume 1610 of *Lecture Notes in Comput. Sci.*, pages 400–414. Springer, Berlin, 1999.

[Ser77] Jean-Pierre Serre. *Linear representations of finite groups.* Springer-Verlag, New York, 1977. Translated from the second French edition by Leonard L. Scott, Graduate Texts in Mathematics, Vol. 42.

[Ser97] Ákos Seress. Primitive groups with no regular orbits on the set of subsets. *Bull. London Math. Soc.*, 29(6):697–704, 1997.

[SSS11] Raman Sanyal, Frank Sottile, and Bernd Sturmfels. Orbitopes. *Mathematika*, 57(2):275–314, 2011.

[Whi64] G. K. White. Lattice tetrahedra. *Canadian J. Math*, 16:389–396, 1964.

[Wil09] Robert A. Wilson. *The finite simple groups*, volume 251 of *Graduate Texts in Mathematics.* Springer-Verlag London Ltd., London, 2009.

[Zas35] Hans Zassenhaus. Kennzeichnung endlicher linearer Gruppen als Permutationsgruppen. *Abh. Math. Semin. Hamb. Univ.*, 11:17–40, 1935.

[Zie95] Günter M. Ziegler. *Lectures on Polytopes.* Graduate Texts in Mathematics. Springer, 1995.

Software

[bliss] bliss: A Tool for Computing Automorphism Groups and Canonical Labelings of Graphs by T. Junttila and P. Kaski. http://www.tcs.hut.fi/Software/bliss/.

[cdd] cdd, cddplus and cddlib by K. Fukuda. http://www.ifor.math.ethz.ch/~fukuda/cdd_home/cdd.html.

[CPLEX] CPLEX by IBM ILOG.

[fplll] fplll by D. Cadé, X. Pujol and D. Stehlé. http://perso.ens-lyon.fr/damien.stehle/fplll/.

[GAP] GAP – Groups, Algorithms, Programming – a System for Computational Discrete Algebra. http://www.gap-system.org/.

[Gurobi] Gurobi by Gurobi Inc.

[LattE] LattE by J. De Loera, M. Köppe et. al. http://www.math.ucdavis.edu/~latte/.

[lrs] lrs by D. Avis. http://cgm.cs.mcgill.ca/~avis/C/lrs.html.

[Magma] Magma Computational Algebra System. http://magma.maths.usyd.edu.au/magma/.

[nauty] The nauty program by B. D. McKay. http://cs.anu.edu.au/people/bdm/nauty/.

[Normaliz] normaliz by W. Bruns, B. Ichim and C. Söger. http://www.mathematik.uni-osnabrueck.de/normaliz/.

[PermLib] PermLib by T. Rehn. http://www.math.uni-rostock.de/~rehn/software/permlib.html.

[polymake] polymake by E. Gawrilow, M. Joswig & al. http://www.polymake.org/.

[Sage] Sage Mathematics Software. http://www.sagemath.org/.

[saucy] Saucy by P. T. Darga and H. Katebi and M. Liffiton and I, Markov and K. Sakallah. http://vlsicad.eecs.umich.edu/BK/SAUCY/.

[SCIP] SCIP. http://scip.zib.de.

[Singular] Singular — A computer algebra system for polynomial computations. http://www.singular.uni-kl.de/.

[SymPol] sympol by T. Rehn and A. Schürmann. http://www.math.uni-rostock.de/~rehn/software/sympol.html.

Zusammenfassung

Deutsch

Diese Arbeit behandelt gitterpunkt-freie symmetrische Polytope. Gitterpunkt-frei heißt, dass die Ecken des Polytops die einzigen enthaltenen ganzzahligen Punkte sind. Symmetrisch im Kontext dieser Arbeit meint, dass alle Ecken in einem einzigen Orbit einer Gruppenwirkung liegen. Diese Arbeit beschäftigt sich besonders mit Gruppen, die als Permutationsgruppen auf $\mathbb{R}^n$ wirken, indem sie Koordinaten permutieren. Die Ecken eines gitterpunkt-freien symmetrischen Polytops werden *core points* genannt. Alle core points von 2-homogenen Permutationsgruppen bis Grad zwölf werden mittels computergestützter Suche bestimmt. Für andere Gruppen werden Konstruktionsmethoden für core points entwickelt. Darüber hinaus diskutiert diese Arbeit Anwendungen von core points in ganzzahliger Optimierung und gibt einen Überblick über die Symmetriegruppen der Sammlung MIPLIB 2010 von ganzzahligen Optimierungsproblemen.

Englisch

This thesis studies minimal lattice-free symmetric polytopes. Lattice-free means that the only integral points in the polytope are its vertices. Symmetric in context of the thesis means that all vertices lie in one single orbit under a group action. The thesis focuses on groups that are permutation groups acting on $\mathbb{R}^n$ by permuting coordinates. If a symmetric polytope is lattice-free, its vertices are called core points. All core points are enumerated by an exhaustive computer search for 2-homogeneous permutation groups with degree up to twelve. For other groups, methods to construct core points are explored. Moreover, this thesis discusses the application of core points in symmetric integer linear programming and gives a survey of the symmetry groups in the MIPLIB 2010 collection of integer programming problems.

Erklärung gemäß §4 Absatz 1 der Promotionsordnung

Ich versichere hiermit an Eides statt, dass ich die vorliegende Arbeit selbstständig angefertigt und ohne fremde Hilfe verfasst habe. Dazu habe ich keine außer den von mir angegebenen Hilfsmitteln und Quellen verwendet und die den benutzten Werken inhaltlich und wörtlich entnommenen Stellen habe ich als solche kenntlich gemacht.

Rostock, den 30.08.2013

Thomas Rehn