ON LATTICE-FREE ORBIT POLYTOPES

KATRIN HERR, THOMAS REHN, AND ACHILL SCHÜRMANN

ABSTRACT. Given a permutation group acting on coordinates of $\mathbb{R}^n$, we consider lattice-free polytopes that are the convex hull of an orbit of one integral vector. The vertices of such polytopes are called core points and they play a key role in a recent approach to exploit symmetry in integer convex optimization problems. Here, naturally the question arises, for which groups the number of core points is finite up to translations by vectors fixed by the group. In this paper we consider transitive permutation groups and prove this finiteness for the 2-homogeneous ones. We provide tools for practical computations of core points and obtain a complete list of representatives for all 2-homogeneous groups up to degree twelve. For transitive groups that are not 2-homogeneous we conjecture that there exist infinitely many core points up to translations by the all-ones-vector. We prove our conjecture for two large classes of groups: For imprimitive groups and groups that have an irrational invariant subspace.

CONTENTS

1. Introduction 1
2. Basic definitions and core points 3
3. Core points are close to invariant subspaces 4
4. Precisely two invariant subspaces – finitely many core points! 6
5. More than two invariant subspaces – infinitely many core points? 16
   Acknowledgements 25
   References 26

1. Introduction

Let $\Gamma \leq S_n$ be a permutation group acting on $\mathbb{R}^n$ by permuting coordinates. We consider orbit polytopes that are convex hulls $\text{conv}(\Gamma z)$ of an orbit of an integral vector $z \in \mathbb{Z}^n$. Such an orbit polytope is called lattice-free, when its vertices are the only integral vectors in the polytope. We note that lattice-free polytopes (as used in [DO95, BK00]) are sometimes called empty lattice polytopes (see [Seb99, HZ00]). We call the integral vertices of lattice-free orbit polytopes core points with respect to $\Gamma$ (cf. [HRST13]). These core points play an important role in symmetric integer convex optimization as a $\Gamma$-symmetric convex set contains an integral point if and only if it contains a core point of $\Gamma$ (cf. [HRST13 Theorem 4]). Therefore, core points can be used to design algorithms that take advantage of available symmetries. This is in particular the case when the number of core points is finite up to translations by vectors in the fixed space of $\Gamma$.
(see [HRS13]). One of the main results in this paper is a sufficient criterion for groups to satisfy this finiteness requirement.

We focus on transitive permutation groups only, i.e., groups such that all coordinates lie in the same orbit. This is a first necessary step in a study of more general groups as every permutation group relates to a product of transitive groups. A detailed study of core points of intransitive groups in general is an open problem and requires further research (cf. [Her13, Reh13]).

In Section 2 we introduce some notation and recall elementary properties of core points. Using the John ellipsoid [Joh48] we prove in Section 3 that core points of a given group are always close to an invariant subspace of the group. It is a well known fact from representation theory that the space $\mathbb{R}^n$ can be decomposed into a direct sum of pairwise orthogonal invariant subspaces of the given group. A transitive group always fixes the one-dimensional linear subspace spanned by the all-ones vector $1$ and therefore also preserves its $(n-1)$-dimensional orthogonal complement $1^\perp$. Therefore, every transitive permutation group has at least these two invariant subspaces. In the following sections we distinguish two fundamentally different cases.

In Section 4 we study groups for which the $(n-1)$-dimensional invariant subspace $1^\perp$ cannot be decomposed into smaller invariant subspaces, that is, we consider groups acting irreducibly on $1^\perp$. By Cameron [Cam72, Lemma 2], these are precisely the 2-homogeneous groups. We show that in this case there exist only finitely many core points up to translation by the all-ones vector. This allows in principle to obtain a complete list of core points (up to translation). We provide mathematical tools for an exhaustive computer search, which we perform up to dimension twelve (see Table 3).

For the other case, that is, for groups having more than two invariant subspaces, we conjecture that there are infinitely many core points up to translation (see Conjecture 18). In Section 5 we prove our conjecture for two major cases: imprimitive groups and groups which have an irrational invariant subspace. Figure 1 depicts an overview of the groups whose core points we study in detail. Despite of convincing computational evidence (see Section 5) for the remaining cases, a complete proof for Conjecture 18 is still missing.

**Figure 1.** Finite vs. infinite core sets
2. Basic definitions and core points

2.1. Permutation groups and representations. We denote by $\langle \cdot , \cdot \rangle$ the standard inner product in $\mathbb{R}^n$. The orthogonal projection of a vector $x$ onto a linear subspace $V$ is denoted by $x|_V$.

By $S_n$ we denote the symmetric group on the set $[n] := \{1, \ldots, n\}$. Let $\Gamma \leq S_n$ be a permutation group. We say that $\Gamma$ is transitive if for every $x, y \in [n]$ there is a permutation $\gamma \in \Gamma$ with $\gamma x = y$. In other words, all elements of $[n]$ lie in the same $\Gamma$-orbit. More generally, we say that $\Gamma$ is $k$-transitive for a $k \in [n]$ if for every two $k$-tuples $(x_1, \ldots, x_k), (y_1, \ldots, y_k) \in [n]^k$, with $x_i \neq x_j$ and $y_i \neq y_j$ for $i \neq j$, there is a permutation $\gamma \in \Gamma$ with $\gamma x_i = y_i$ for all $i \in [k]$. The group $\Gamma$ is called $k$-homogeneous if for every two subsets $X, Y \subset [n]$ with $k$ elements there is a permutation $\gamma \in \Gamma$ with $\gamma X = Y$.

If there exists a non-trivial partition $[n] = \bigcup_{i=1}^{m} B_i$ with $2 \leq m \leq n - 1$ and a permutation $\sigma$ of $[m]$ such that $\Gamma B_i = B_{\sigma(i)}$ for all $i$, we call the $B_i$ blocks of imprimitivity. If no such partition exists, we say that $\Gamma$ is primitive.

Without distinction we also write $\Gamma$ for the canonical linear representation of the permutation group which acts on $\mathbb{R}^n$ by permuting coordinates. We call a subspace $V \subset \mathbb{R}^n$ an invariant subspace for $\Gamma$ if it is setwise fixed, i.e. $\Gamma V = V$. Note the difference to the fixed space $\text{Fix}(\Gamma)$, which is the subspace of all pointwise fixed elements of $\mathbb{R}^n$. We can always decompose $\mathbb{R}^n$ into a direct sum of orthogonal $\Gamma$-invariant subspaces because the linear representation of $\Gamma$ is an orthogonal group. For $\Gamma \leq S_n$ the space spanned by the all-ones vector $\mathbb{1}$ is always an invariant subspace, which is even fixed pointwise.

2.2. Core points and core sets. Core points were first studied in [BHJ13] with respect to full symmetric and alternating groups. The following definition is taken from [HRS13], which generalizes the definition of core points to arbitrary subgroups of $S_n$.

**Definition 1.** Given a group $\Gamma \leq S_n$, a core point with respect to $\Gamma$ is an integral point $z \in \mathbb{Z}^n$ such that the convex hull of its $\Gamma$-orbit does not contain any further integral points, that is, $\text{conv}(\Gamma z) \cap \mathbb{Z}^n = \Gamma z$. Phrased differently, the orbit polytope of $z$ with respect to $\Gamma$ is lattice-free.

**Remark 2.** Translation by $\mathbb{1}$ commutes with any element of $\Gamma$, therefore the polytope $\text{conv}(\Gamma (z + \mathbb{1}))$ is the translate $\mathbb{1} + \text{conv}(\Gamma z)$. Thus, it suffices to study core points up to translation by $\mathbb{1}$.

There are two canonical ways to choose representatives. The first is studying core points in the affine hyperplanes $H_{1,0}, \ldots, H_{1,n-1}$ where $H_{1,k} := \{x \in \mathbb{R}^n \mid \langle x, \mathbb{1} \rangle = k\}$. We refer to the set of integer points in these hyperplanes as layers $\mathbb{Z}(k) := \mathbb{Z}^n \cap H_{1,k}$ with index $k$. The second way is to select zero-based representatives according to the following definition.

**Definition 3.** A point $z \in \mathbb{Z}^n$ is called zero-based if all its coordinates are non-negative and at least one coordinate is zero.

At the end of this section we recall the only previously known result about core points of transitive groups. For the full symmetric and alternating group on $n$ variables the following characterization of core points was proven in [BHJ13]. Since any subgroup $\Gamma' \leq \Gamma$ inherits the core points of $\Gamma$, the core points with
respect to $\Gamma = S_n$ are core points with respect to any group $\Gamma' \leq S_n$. For this reason we call them universal core points.

**Example 4** (Universal core points). Let $\Gamma$ be the full symmetric or the alternating group on $n$ variables. For each $k \in [n]$, the core points in the affine hyperplane $H_{1,k}$ are precisely the vertices of the hypersimplex:

$$\text{core}_\Gamma(H_{1,k}) = \left\{ \sum_{i \in T} e_i : T \text{ a } k\text{-element subset of } [n] \right\}.$$ 

Thus, each core point with respect to $\Gamma$ is an integral point with coordinates in $\{t, t+1\}$ for some $t \in \mathbb{Z}$.

### 3. Core points are close to invariant subspaces

In this section we will show that core points are always close to an invariant subspace of the group. To prove this we use a well-known theorem from convex geometry ([Joh48], see also [Bar02]).

**Theorem 5** (John ellipsoid [Joh48]). Let $K \subset \mathbb{R}^n$ be a convex body, i.e., $K$ is compact and convex with non-empty interior. Among all ellipsoids containing $K$ there exists a unique ellipsoid $E$ of minimal volume. Further, a scaled version of $E$ is in turn contained in $K$:

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

where $t \in \mathbb{R}^n$ is a suitable translation vector that depends on the center of $E$. The scaling factor $\frac{1}{n}$ for $E$ is optimal as the case of a simplex shows.

This ellipsoid is called the minimal enclosing ellipsoid of $K$. For orbit polytopes this ellipsoid can be computed as follows. Let $\Gamma \leq S_n$ be a permutation group. Recall from Section 2.1 that we can decompose $\mathbb{R}^n$ into pairwise orthogonal $\Gamma$-invariant subspaces. We have

$$\mathbb{R}^n = \bigoplus_{i=1}^m V_i$$

where each $V_i \subset \mathbb{R}^n$ is setwise preserved by $\Gamma$ (i.e., $\gamma v \in V_i$ for all $\gamma \in \Gamma$ and $v \in V_i$) and is irreducible (i.e., $V_i$ does not contain a proper invariant subspace). Note that, depending on the group, this decomposition may not be unique, which is a well-known fact in representation theory (see, for instance, [Ser77]). The minimal enclosing ellipsoid of an orbit polytope is closely related to invariant subspaces as [BB05 Thm. 2.2] shows.

**Theorem 6** ([BB05]). Let $\Gamma \leq S_n$ be a transitive permutation group. Let $z \in \mathbb{Z}^n_{(k)}$ be such that the dimension of the orbit polytope of $z$ is maximal, i.e., $\dim \text{conv} \Gamma z = n-1$. Then there exists a decomposition $\mathbb{R}^n = \text{span} \mathbf{1} \oplus \bigoplus_{i=1}^m V_i$ of $\mathbb{R}^n$ into the fixed space $\text{span} \mathbf{1}$ and other $\Gamma$-invariant invariant subspaces $V_i$ such that the minimal enclosing ellipsoid of the orbit polytope $\text{conv}(\Gamma z)$ is given by

$$\frac{k}{n} \mathbf{1} + \left\{ x \in H_{1,0} : \sum_{i=1}^m (\dim V_i) \frac{\|x|_{V_i}\|^2}{\|z|_{V_i}\|^2} \leq n - 1 \right\}.$$
If the decomposition of \( \mathbb{R}^n \) into \( \Gamma \)-invariant subspaces is unique, then the minimal enclosing ellipsoid is also uniquely determined by the formula in the theorem. If there are multiple decompositions, only one of these leads to the minimal enclosing ellipsoid.

**Theorem 7.** Let \( \Gamma \leq S_n \) be a transitive permutation group. Then there exists a constant \( C(n) \) depending only on the dimension \( n \), such that for every core point \( z \) with respect to \( \Gamma \) there exists a \( \Gamma \)-invariant subspace \( V \) of \( \mathbb{R}^n \) different from \( \text{Fix}(\Gamma) = \text{span} \mathbb{1} \) such that \( \|z|_V\| \leq C(n) \).

**Proof.** We use the two preceding theorems in this section to find a necessary condition under which the orbit polytope \( P := \text{conv} \Gamma z \) contains integral points. We first consider \( z \in \mathbb{Z}_{(k)}^n \) with a fixed \( k \). By Theorem 6 there is a decomposition \( \mathbb{R}^n = \text{Fix}(\Gamma) \oplus \bigoplus_{i=1}^m V_i \) of \( \mathbb{R}^n \) into \( \Gamma \)-invariant subspaces related to the minimal enclosing ellipsoid of \( P \). If \( \|z|_{V_i}\| = 0 \) for one subspace \( V_i \), then nothing remains to be shown. So we assume that all projections \( z|_{V_i} \) have positive norm. Then the dimension of the polytope \( P \) is \( n - 1 \). By Theorem 6 we know that the minimal enclosing ellipsoid of the orbit polytope \( P \) is

\[
\frac{k}{n} \mathbb{1} + \left\{ x \in H_{1,0} : \sum_{i=1}^m (\dim V_i) \|x|_{V_i}\|^2 \|z|_{V_i}\|^2 \leq n - 1 \right\}.
\]

By John’s Theorem 5 the polytope \( P \) contains the following scaled ellipsoid:

\[
E' := \frac{k}{n} \mathbb{1} + \left\{ x \in H_{1,0} : \sum_{i=1}^m (\dim V_i) \|x|_{V_i}\|^2 \|z|_{V_i}\|^2 \leq \frac{1}{n - 1} \right\}.
\]

Since the dimension of \( P \) is \( n - 1 \), the scaling factor is \( \frac{1}{n - 1} \) 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 \( u \in \mathbb{Z}_{(k)}^n \subset H_{1,k} \) be an integer point with minimal norm. If for all subspaces \( V_i \) the length of the projection \( \|z|_{V_i}\| \) is large enough, then the following inequality is satisfied.

\[
\sum_{i=1}^m (\dim V_i) \|u|_{V_i}\|^2 \|z|_{V_i}\|^2 \leq \frac{1}{n - 1}.
\]

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 \( E' \) is fulfilled, let \( u' := u - \frac{k}{n} \mathbb{1} \) be the orthogonal projection of \( u \) onto \( H_{1,0} \). Because \( \|u|_{V_i}\| \leq \|u'\| \) and \( \dim V_i \leq n - 1 \), the inequality \( (2) \) is satisfied if for all \( i \) the projections satisfy

\[
\|z|_{V_i}\|^2 \geq m(n - 1)^2 \|u'\|^2.
\]

As \( u \) was chosen as an integer point in \( H_{1,k} \) with minimal norm, the bound in \( (3) \) depends only on the layer index \( k \) and the dimension \( n \). However, since \( u + \mathbb{1} \) has minimal norm in \( \mathbb{Z}_{(k+1,n)}^n \), for integers \( l \), the bound really depends only on the value \( k \mod n \). For each \( k \in [n] \) we get from \( (3) \) a constant \( C(n, k) \) such that: \( \|z|_{V_i}\| \geq C(n, k) \) for all \( i \) implies \( P \) contains an integer point. Since these are only finitely many layers, there exists a constant \( C(n) := \max_k C(n, k) \) as claimed in the theorem. \( \square \)
Theorem 7 remains valid under milder assumptions on $\Gamma$. It also holds when $\Gamma \leq \text{GL}_n(\mathbb{Z})$ is a finite group of unimodular matrices (see [Rah13]).

4. Precisely two invariant subspaces – finitely many core points!

In this section we consider groups for which the orthogonal complement of $\mathbb{1}$ is irreducible. Hence, these groups have precisely two invariant subspaces. Recall that it suffices to study core points up to translation by $\mathbb{1}$ (see Remark 2). It is an immediate consequence of Theorem 7 that the considered groups have only finitely many core points up to translation (see the following Section 4.1). Therefore all core points can be enumerated computationally. In Section 4.2 we give an overview of our exhaustive search. The necessary mathematical equipment is provided in Sections 4.3 and 4.4. In Section 4.5 we discuss the results of our computational search for core points.

4.1. Finiteness. From Theorem 7 it follows immediately that groups with precisely two invariant subspaces have only a finite number of core points up to translation. By Cameron [Cam72, Lemma 2], these are the 2-homogeneous groups.

Corollary 8. If $\Gamma \leq S_n$ is 2-homogeneous, then the number of core points up to translation by $\mathbb{1}$ is finite.

Proof. If $\Gamma$ has only two invariant subspaces, then $\mathbb{R}^n = \text{span } \mathbb{1} \oplus V$ for an irreducible invariant subspace $V$. Theorem 7 then shows that every core point must have a “small” projection onto $V$. Thus, every core point is contained in a cylinder with radius $C(n)$ around the fixed space $\text{span } \mathbb{1}$. This cylinder contains only finitely many integral points up to translation by $\mathbb{1}$. □

We conjecture (see Conjecture 18) that the converse statement is true, that is, every transitive group that is not 2-homogeneous has an infinite number of core points up to translation. In Section 5 we will look at this conjecture more closely.

In the following proposition we estimate the constant $C(n)$ from the proof of Corollary 8. To get a good estimate we also consider the dependency on the layer index $k$.

Proposition 9. Let $\Gamma \leq S_n$ be a 2-homogeneous group. For a core point $z \in \mathbb{Z}^n$ with $\langle z, \mathbb{1} \rangle = k$ for $k \in [n-1]$ we have:

$$\|z - z|_{\text{span } \mathbb{1}}\| < (n-1)\sqrt{\frac{k(n-k)}{n}}.$$ 

Proof. For the proof it is enough to obtain a value for the right hand side of (3) in the proof of Theorem 7. Let $V$ be the $(n-1)$-dimensional invariant subspace of $\Gamma$. Note that

$$\|z|_V\| = \|z - z|_{\text{span } \mathbb{1}}\| = \|z - \frac{k}{n}\mathbb{1}\|.$$ 

Since $V$ is the only invariant subspace besides the fixed space $\text{span } \mathbb{1}$, the value of $m$ in (3) equals one. Therefore we have

$$\left\|z - \frac{k}{n}\mathbb{1}\right\| = \|z|_V\| < (n-1)\|u|_V\|.$$
The points $u$ with minimal projected norm in this case are the universal core points from Example 4. For layer $k$ we can choose $u$ to be any point with $k$ ones and $n - k$ zeros as coordinates. We compute
\[\|u\|_V^2 = \|u\|^2 - \|u_{\text{span} 1}\|^2 = k - \left\| \frac{k}{n} \frac{1}{n} \right\|^2 = k - \frac{k^2}{n} = \frac{k(n - k)}{n}.\]

Using this value in (4) yields the inequality claimed in the proposition. \qed

### 4.2. On how to determine all core points.

We now present one way to practically compute all core points of a 2-homogeneous group up to translation. Our computational results with this approach will be discussed in Section 4.5 for 2-homogeneous groups of degree up to twelve.

For the core point enumeration two essential tasks are involved. First, we need to determine a set of candidates which is large enough to cover all core points, and enumerate its elements up to $\Gamma$-symmetry. The quality of the set strongly relies on the quality of the bounds used for the computation. The bound from Proposition 9 is not strong enough in general. Therefore we use improved bounds that we develop in Section 4.3. For our core point enumeration we look at the (zero-based) integral points in the cubes $[0, n - 3]^n$ for 2-transitive groups and $[0, \lfloor 1.09(n - 1) \rfloor]^n$ for the other 2-homogeneous groups. These numbers follow from Theorems 10 and 15, respectively. Note that, by Remark 2 and Definition 3, it is enough to consider only zero-based core points, which leads to the aforementioned cubes.

The second task is to check for each candidate whether it is a core point or not. There are two natural ways to tackle this task. One way is to set up a (mixed) integer program that is feasible if and only if an orbit polytope contains an integral point that is not a vertex (for details see [Reh13]). Another way is to count the number of integral points in the orbit polytope and compare it to the number of vertices. The candidate is a core point if and only if the two numbers coincide. For our examples we chose the second approach (see Section 4.5).

Dealing with problems that are NP-hard in general, the second task – checking whether a candidate is a core point – is the most time-consuming step in the computation. Hence, additional criteria are necessary to exclude points from the expensive core point check upfront. We use the following tweaks, which we will discuss in detail in the next sections.

- We can assume w.l.o.g. that each candidate $z$ is zero-based (see above) and that its first coordinate is minimal (by transitivity), i.e., $z_1 = 0$.
- We skip the check for all universal core points. Recall that they are core points with respect to every subgroup of $S_n$, compare Example 4.
- For $(k + 1)$-transitive groups, Proposition 17 allows for the exclusion of all integer points with layer index $l$ for $(l \mod n) \in \pm \{1, \ldots, k\}$ since they either are universal core points, or their orbit polytope contains one.
- All candidates $z$ whose nonzero coordinates have a greatest common divisor $\gcd > 1$ can be excluded by Lemma 13.
- Let $\Gamma'(z)$ be the stabilizer of the set of even coordinates of a candidate $z$. We skip all candidates which are not constant on the orbits of $\Gamma'(z)$. This is justified by Lemma 16.
• For 2-transitive groups we check whether
  \[
  \left( \sum_{i=1}^{n} z_i \right) \mod (n-1) \leq \max z_i,
  \]
  which follows from Proposition 14.

• Finally, we check whether the orbit polytope \( \text{conv} \, \Gamma z \) contains one of the universal core points (see Section 4.4.3).

We give statistics about the combined power of all these criteria in Table 3.

4.3. Box width bounds. Proposition 9 already provides a bound for the distance of a core point \( z \in H_{1,k} \) from its projection \( \frac{k}{n} \mathbb{1} \) onto the fixed space. This bound turns out to be weak, as shown by our results in Section 4.5. It also has the disadvantage that it is not straightforward to enumerate all integral points inside a ball of a given radius. In the following we show how to obtain stronger and more practical bounds, which are essential for the viability of our computations described in Section 4.5. These bounds will be in terms of the box width \( \text{bw}(z) \) which we define as

\[
\text{bw}(z) := \max_{i \in [n]} z_i - \min_{i \in [n]} z_i.
\]

We start with the special case of 2-transitive groups and come back to the more general case of 2-homogeneous groups at the end of this section.

Theorem 10. Let \( \Gamma \leq S_n \) be a 2-transitive group. For \( n \geq 4 \) the box width of any core point \( z \) with respect to \( \Gamma \) is bounded by \( \text{bw}(z) \leq n - 3 \).

For our proof of this theorem we use the following simple observation about intersection with and projection onto fixed spaces. Remember that the orthogonal projection of \( x \) onto \( \text{Fix}(\Gamma) \) is given by the barycenter of its orbit:

\[
(x|_{\text{Fix}(\Gamma)}) = \frac{1}{|\Gamma|} \sum_{\gamma \in \Gamma} \gamma x.
\]

Lemma 11. Let \( P \subset \mathbb{R}^n \) be a polytope and \( \Gamma \leq S_n \) be a symmetry group of \( P \), i.e., \( \Gamma P = P \). Then

\[
P \cap \text{Fix}(\Gamma) = P|_{\text{Fix}(\Gamma)}.
\]

Proof. For the \( \subseteq \)-part let \( x \in P \cap \text{Fix}(\Gamma) \). Since \( x \in \text{Fix}(\Gamma) \), we have \( x = x|_{\text{Fix}(\Gamma)} \in P|_{\text{Fix}(\Gamma)} \). For the reverse inclusion \( \supseteq \) let \( y \in P|_{\text{Fix}(\Gamma)} \). In particular, \( y = x|_{\text{Fix}(\Gamma)} \) is a convex combination of points \( \gamma x \) in \( \Gamma P \) by (5). Since \( \Gamma P = P \) is convex, this implies that the point \( y \) lies in \( P \). \( \square \)

In words, the lemma states that projection to the fixed space equals intersection with the fixed space for symmetric polytopes. 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 its vertices, so the projection is readily available. Lemma 11 allows us to find integral points in \( P \), which may be difficult, by finding projections of integral points, which may be a much easier problem. How easy it gets depends on the group we choose. Consider an orbit polytope \( \text{conv} \, \Gamma z \). If we intersect it with the fixed space \( \text{Fix}(\Gamma) \), this leaves us with the vertex barycenter of the orbit polytope, which does not provide new information. Thus, the goal is to find a subgroup \( \Gamma' \leq \Gamma \) with at least two but still a small number of orbits so that the projection
is not trivial. In particular, for 2-transitive groups, which we focus on in this section, we can obtain a one-dimensional projection, using a subgroup with two orbits. In such a line segment integral points are naturally easy to find. Theorem 10 follows from the fact that if the line segment is wide enough, it – and therefore also the original polytope – contain an integer point, which is not a vertex. To prove the main theorem, we start with an application of Lemma 11 to 2-transitive groups.

Proposition 12. Let $\Gamma \leq S_n$ be a 2-transitive group and let $P := \text{conv} \, \Gamma z$ be the orbit polytope of some zero-based $z \in \mathbb{Z}^n_+$. Then a point $p = (k, l, l, \ldots, l)^{\top} \in \mathbb{R}^n$ 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 $\Gamma' := \text{Stab}_\Gamma(p) = \text{Stab}_\Gamma(1)$ of $p$ acts transitively on $\{2, \ldots, n\}$ because $\Gamma$ is 2-transitive. Let $\{\gamma_1, \ldots, \gamma_n\} \subset \Gamma$ be a transversal for $\Gamma$ modulo $\Gamma'$, that is, $\gamma_i(i) = 1$ for each $i \in [n]$. Thus, for every $\gamma_i$ we have that

$$\gamma_i z)|_{\text{Fix}(\Gamma')} = (z_i, r_i, r_i, \ldots, r_i)^{\top} \text{ where } r_i = \frac{1}{n-1} \sum_{j \in [n] \setminus \{i\}} z_j.$$

Let $Q := P|_{\text{Fix}(\Gamma')}$ be the projection of $P$ onto the fixed space $\text{Fix} (\Gamma')$. It is the convex hull of vectors $q^{(i)} := (\gamma_i z)|_{\text{Fix}(\Gamma')}$ for $i \in [n]$. All these vectors lie in a one-dimensional affine subspace of $\mathbb{R}^n$, so $Q$ is a line segment. By Lemma 11 the point $p \in \text{Fix} (\Gamma')$ 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 $q^{(b)} = (b, r_b)^{\top}$. As inequality description we obtain

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

Hence, the polytope $Q'$ contains a point $u = (u_1, u_2)^{\top} \in \mathbb{R}^2$ if and only if $0 \leq u_1 \leq z_b$ 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.

A simple observation for which points cannot be core points is the following lemma.

Lemma 13. Let $z \in \mathbb{Z}^n$ be a core point for a group $\Gamma \leq S_n$. If $z \notin \text{Fix}(\Gamma)$, then $\gcd(z_1, \ldots, z_n) = 1$.

Proof. Let $z \in \mathbb{Z}^n$ have $c := \gcd(z_1, \ldots, z_n) > 1$. In order to prove the lemma we show that such a point $z$ is not a core point. Because $z \notin \text{Fix}(\Gamma)$ by assumption of the lemma, there is a permutation $\gamma \in \Gamma$ with $\gamma z \neq z$. Then $\frac{c-1}{c} z + \frac{1}{c} \gamma z$ is an integral, non-trivial convex combination of two vertices of $\text{conv} \, \Gamma z$. Hence, $\text{conv} \, \Gamma z$ is not lattice-free and $z$ is not a core point.
Theorem 10 will follow from the following proposition. The previous Proposition 12 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. It is also interesting in its own right because it states a necessary criterion for core points which is stronger than the box width alone.

**Proposition 14.** Let $\Gamma \leq S_n$ be a 2-transitive group with $n \geq 3$. Let $z \in \mathbb{Z}_{\geq 0}^n$ be zero-based with $\max z_i \geq 2$. If
\[
\left( \sum_{i=1}^n z_i \right) \mod (n - 1) \leq \max z_i,
\]
then $\conv \Gamma z$ is not lattice-free.

**Proof.** Let $k \in \{0, \ldots, n - 2\}$ be congruent $\sum_{i=1}^n z_i \mod (n - 1)$. Then $l := (\sum_{i=1}^n z_i)^{-(k)}$ is an integer. By Proposition 12 the integral point $p = (k, l, \ldots, l)^\top$ lies in $P := \conv \Gamma z$ because $0 \leq k \leq \max z_i$. 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, then $P$ is not lattice-free and we are done. So 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 $\gcd(p_1, \ldots, p_n) = \gcd(k, l) \geq 2$ because of our assumption $\max z_i \geq 2$. Thus, Lemma 13 implies that $\conv \Gamma p$ is not lattice-free and therefore $\conv \Gamma z \supset \conv \Gamma p$ is not lattice-free. \qed

With this proposition we are able to prove the maximal box width of core points for 2-transitive groups.

**Proof of Theorem 10** It suffices to prove the theorem for zero-based points because the box width is not affected by translation by 1. Let $z \in \mathbb{Z}_{\geq 0}^n$ be zero-based with $\max z_i \geq n - 2 \geq 2$. We have to show that $z$ is not a core point. It holds that $\sum_{i=1}^n z_i \mod (n - 1) \leq \max z_i$ because the remainder of $\sum_{i=1}^n z_i$ after division by $n - 1$ lies in $\{0, 1, \ldots, n - 2\}$. Thus, Proposition 14 ensures that the orbit polytope $\conv \Gamma z$ is not lattice-free. Hence, $z$ is not a core point and the claim of the theorem follows. \qed

For 2-homogeneous groups the situation is more complicated than for the 2-transitive groups. We can start similarly and study the projection of orbit polytopes onto the fixed space $\Fix(\Stab_\Gamma(1))$. Because this fixed space has dimension three (see [Cam72, Lemma 2]), the resulting projected polytope is in general not a line segment but a two-dimensional polygon. For two-dimensional polytopes, determining the vertices and integral points are non-trivial tasks. Using the classification of 2-homogeneous, not 2-transitive permutation groups (see [Kan72]) and the flatness theorem in dimension two (see [Hur90]), one can still obtain the following upper bound on the box width. Its proof is quite technical so we just state the result here and refer to [Reh13] for details.

**Theorem 15** ([Reh13]). Let $\Gamma \leq S_n$ be a 2-homogeneous group. The box width of any core point $z$ with respect to $\Gamma$ is bounded by $\bw(z) < 1.09 (n - 1)$. 

\[\text{ON LATTICE-FREE ORBIT POLYTOPES} \quad 10\]
4.4. Tweaks.

4.4.1. A parity tweak.

Lemma 16. Let $\Gamma \leq S_n$ be a transitive permutation group and $z \in \mathbb{Z}^n$. Let $E$ denote the sets of indices corresponding to the even coordinates of $z$ and let $\Gamma'(z) \leq \Gamma$ be the set-stabilizer of $E$. Further, let $I$ be the partition of $[n]$ into orbits under $\Gamma'(z)$. If any of the orbits in $I$ contains two indices $k, l$ such that $z_k$ is not equal to $z_l$, then the point $z$ is not a core point with respect to $\Gamma$.

Proof. Let $k$ and $l$ be two indices in the same orbit with $z_k \neq z_l$. Since $\Gamma'(z)$ acts transitively on its orbits, there exists a permutation $\gamma \in \Gamma'(z)$ such that the $l$-th coordinate of $\gamma z$ is equal to $z_k \neq z_l$. Since the coordinates corresponding to indices in one orbit are either all even or all odd, the point $z' := \frac{1}{2}z + \frac{1}{2}\gamma z$ is integral. Furthermore, it is a proper convex combination, as $z \neq \gamma z$. Hence, the integer point $z'$ is contained in the orbit polytope of $z$ without being a vertex, thus $z$ is not a core point.

Note that Lemma 16 also holds with respect to odd instead of even coordinates. In order to use the lemma in the candidate enumeration, it is necessary to compute the orbits of the set-stabilizers of all subsets of $[n]$ up to $\Gamma$-symmetry in a preprocessing step. However, using a software package like [GAP] the computation time for this task is negligibly small. The lemma is particularly effective if the set stabilizers have large orbits (so that many coordinates must have the same value). By a result of Seress [Ser97], many small 2-transitive groups are exceptional in the sense that no set stabilizer is trivial, i.e., has at least one orbit of size two (and usually many more).

4.4.2. Restriction on layer indices for $k$-transitive groups. We can generalize the argument behind Proposition 12 to groups of higher transitivity. The following proposition shows that transitivity enforces that core points with “small” layer index $k$ must be universal core points. For the enumeration in Section 4.5 we can thus skip these layers.

Proposition 17. Let $\Gamma \leq S_n$ be a $(k+1)$-transitive group with $k \geq 1$. Then the only core points with respect to $\Gamma$ in $\mathbb{Z}_{\geq 0}^n$, for $l \mod n$ congruent to an index in $\{-k, -k + 1, \ldots, k\}$, are universal core points.

Proof. Let $z \in \mathbb{Z}_{\geq 0}^n$ be zero-based and $\max z_i \geq 2$. We write $N$ for the layer index $N = N(z):= \{1, z\} = \sum_{i=1}^n z_i$. To prove the proposition, it is enough to show that every such $z$ with $N \equiv k \mod n$ is no core point because every $(k + 1)$-transitive group is $k$-transitive. In the following we prove that $P := \text{conv } \Gamma z$ is not lattice-free by using Lemma 11. More precisely, we show that $P$ contains

$$v = \left( c + 1, \ldots, c + 1, c, \ldots, c \right)$$

for $c = \lfloor \frac{N}{n} \rfloor$. Note that $v$ is contained in the fixed space $\text{Fix}(\Gamma')$ of the set stabilizer $\Gamma' := \text{Stab}_\Gamma(\{1, \ldots, k\})$. By Lemma 11 it suffices to prove that $v$ is contained in the projection $Q := P|_{\text{Fix}(\Gamma')}$ in order to ensure that $v$ lies in $P$.

Because the group $\Gamma$ is $(k + 1)$-transitive, the stabilizer $\Gamma'$ acts transitively on the sets $\{1, \ldots, k\}$ and $\{k + 1, \ldots, n\}$. Thus, the projection of an $x$ onto the fixed space is given by $x|_{\text{Fix}(\Gamma')} = (R(x), \ldots, R(x), S(x), \ldots, S(x))^\top$ with $R(x) :=$
by solving one linear program, see for instance [Fuk04]. For our enumeration we
prove that
\[ \gamma \in \Gamma \text{ is } k\text{-transitive} \]
therefore, the existence of such \( x \) and \( y \) implies that \( v \) lies on the line-segment \( Q \).

To keep the index notation simple we assume that \( z \) is sorted ascendingly. It will become clear that this is without loss of generality in the following argument because \( \Gamma \) is \( k\)-transitive. Our next step is to show that
\[
\sum_{i=1}^{k} z_i \leq k(c+1) \quad \text{and} \quad \sum_{i=n-k+1}^{n} z_i \geq k(c+1).
\]
If we have these inequalities, we immediately obtain the desired bounds \( x \) and \( y \) as follows. From the first equation (7) we get that \( R(z) \leq (c+1) = R(v) \). Because \( \Gamma \) is \( k\)-transitive, there is a permutation \( \gamma \in \Gamma \) that maps \( \{n-k+1, \ldots, n\} \) to \( \{1, \ldots, k\} \). Thus, we obtain \( R(v) = (c+1) = R(\gamma z) \) from (8).

It remains to show that inequalities (7) and (8) actually hold. For a contradiction assume that \( \sum_{i=1}^{k} z_i > k(c+1) \). Since \( z \) is sorted, this implies \( z_k \geq c+2 \) 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 \( z_{n-k+1} \leq c \) 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 (7) and (8) 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 \( c = 0 \). Otherwise, all coordinates of \( v \) are non-zero by choice of \( v \) in (6). So we can assume that \( c = 0 \). In this case we have \( \max z_i = c+1 = 1 \), which we have ruled out by our initial assumption. Hence, \( v \) is not a vertex of \( P \).

A simple corollary of this proposition is the following. If \( G \leq S_n \) is \( 2\)-transitive, then all core points in the layers with index 1 and \( n-1 \) are universal core points. A similar statement for general \( 2\)-homogeneous groups is false as the computer search in Section 4.5 shows.

4.4.3. Selective probing. If none of the other, easily testable criteria excluded a given candidate, we apply a last heuristic before we call the computationally expensive lattice point enumeration. For each point \( z \) which is not a core point the orbit polytope \( \text{conv } \Gamma z \) is likely to contain one of the core points already approved. The check whether a specific point is contained in \( \text{conv } \Gamma z \) can be done by solving one linear program, see for instance [Fuk04]. For our enumeration we
check whether the orbit polytope of a candidate contains a universal core point. These are a natural choice since they are the closest points to the vertex barycenter of the orbit polytope. Probing for these enabled us to eliminate a huge number of candidates (see Table 3).

4.5. Computational results. We now present the results of our exhaustive computer search based on the strategy described in the previous sections. To enumerate all core points of all 2-homogeneous groups with degree up to twelve we implemented the core point enumeration using the polymake framework \cite{pol}. An overview of these groups is shown in Table 1. The column “Id” is a composition of the group degree and the PrimitiveIdentification-id of the group in the library of primitive groups of \cite{GAP}.

| Id   | Order | Structure       | Transitivity | Homogeneity |
|------|-------|-----------------|--------------|-------------|
| 5-3  | 20    | AGL(1, 5)       | 2            | 5           |
| 6-1  | 60    | PSL(2, 5)       | 2            | 2           |
| 6-2  | 120   | PGL(2, 5)       | 3            | 6           |
| 7-3  | 21    | $C_7 \times C_3$ | 1            | 2           |
| 7-4  | 42    | AGL(1, 7)       | 2            | 2           |
| 7-5  | 168   | $L(3, 2)$       | 2            | 2           |
| 8-1  | 56    | AGL(1, 8)       | 2            | 3           |
| 8-2  | 168   | $A\Gamma L(1, 8)$ | 2            | 3           |
| 8-3  | 1344  | ASL(3, 2)       | 3            | 3           |
| 8-4  | 168   | PSL(2, 7)       | 2            | 3           |
| 8-5  | 336   | PGL(2, 7)       | 3            | 3           |
| 9-3  | 72    | $M_9$           | 2            | 2           |
| 9-4  | 72    | AGL(1, 9)       | 2            | 2           |
| 9-5  | 144   | $A\Gamma L(1, 9)$ | 2            | 2           |
| 9-6  | 216   | $3^2(2A(4))$    | 2            | 2           |
| 9-7  | 432   | AGL(2, 3)       | 2            | 2           |
| 9-8  | 504   | PSL(2, 8)       | 3            | 9           |
| 9-9  | 1512  | $P\Gamma L(2, 8)$ | 3            | 9           |
| 10-3 | 360   | PSL(2, 9)       | 2            | 2           |
| 10-4 | 720   | PGL(2, 9)       | 3            | 3           |
| 10-5 | 720   | $S_6$           | 2            | 2           |
| 10-6 | 720   | $M_{10}$        | 3            | 3           |
| 10-7 | 1440  | $P\Gamma L(2, 9)$ | 3            | 3           |
| 11-3 | 55    | $C_{11} \times C_5$ | 1            | 2           |
| 11-4 | 110   | AGL(1, 11)      | 2            | 2           |
| 11-5 | 660   | $L(2, 11)$      | 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   | PSL(2, 11)      | 2            | 3           |
| 12-4 | 1320  | PGL(2, 11)      | 3            | 3           |
Regarding the core point search, Table 2 shows that there is a vast number of core point candidates in the cube induced by our theoretical bound on the box width.

### Table 2. Theoretical maximal bounds for 2-transitive groups

| dim n | #points in $[0, \text{bw}]^n$ | bw | distance to span $\mathbb{I}$ |
|-------|-------------------------------|----|------------------------------|
| 5     | 243                           | 2  | 4.38                         |
| 6     | 4 096                         | 3  | 6.12                         |
| 7     | 78 125                        | 4  | 7.86                         |
| 8     | 823 543                       | 6  | 7.86                         |
| 9     | 1 679 616                     | 5  | 9.90                         |
| 10    | 40 353 607                    | 6  | 11.93                        |
| 11    | 1 073 741 824                 | 7  | 14.23                        |
| 12    | 31 381 059 609                | 8  | 16.51                        |
| a11   | 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 bw-bound applies

Table 3 illustrates the progress of our candidate elimination towards the actual set of core points. We introduce the table by columns. The first column shows the id of the group; this is the same as in Table 1. The second column “tweaks” gives the number of all actually enumerated candidates, using all necessary bounds and tweaks from Sections 4.3 and 4.4 but without selective probing. The number of candidates shown in this column is much smaller than the number of integral points in the cube $[0, n-3]^n$ for 2-transitive groups and $[0, \lfloor 1.09(n-1) \rfloor]^n$ for 2-homogeneous, not 2-transitive groups (cf. Table 2). This demonstrates the combined power of all the “small” necessary criteria displayed above. For the groups for which at least one set stabilizer is trivial (7-3, 9-3, 9-4, 11-3, 11-4, 12-3) the number of candidates is much higher than for the other groups (cf. [Ser97]).

Note that among the considered groups there are two that are 2-homogeneous but not 2-transitive. These occur in dimension seven and eleven only (groups 7-3 and 11-3). To these groups we cannot apply Proposition 14 to eliminate candidates. For the group with id 11-3, this leaves us with 1 331 476 291 candidates. This number is too large to proceed to the actual core point checks. To exclude candidates fast we implemented a test based on Lemma 11. We project each orbit polytope $P$ onto the three-dimensional fixed space $\text{Fix}(\text{Stab}_P(1))$. The corresponding projected polytope $Q$ is two-dimensional. We can find integral points in $Q$ quickly after a relatively cheap convex hull computation. As integer points in $Q$ correspond to integer points in $P$, this allows to eliminate core point candidates without constructing the complete orbit polytope. This reduced the number of candidates to under 300 000 without too much computational effort. More details can be found in [Reh13].

The third column of Table 3 “probing” shows the number of candidates that remain after 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 as confirmed by actually enumerating all integral points in the orbit polytopes. For this final check we use Normaliz \cite{Nor} via its interface to polymake. Comparing the third and fourth columns of Table \ref{table:candidate_elimination}, we see that the number of candidates after selective probing is already very close to the number of actual non-universal core points. This shows that a concise description of those who survive probing, i.e., of those points whose orbit polytopes do not contain universal core points, would probably make core point enumeration much easier.

The fifth column of Table \ref{table:candidate_elimination} “max bw” contains the maximal box width of a core point. The sixth column “max dist to span $1$” shows the maximal distance of a core point from the fixed space. Comparing these last two columns to the last two

\begin{table}[h]
\centering
\caption{Candidate elimination}
\begin{tabular}{rrrrrr}
\hline
\text{group id} & \text{tweaks} & \text{probing} & \text{core points} & \text{max bw} & \text{max dist to span $1$} \\
\hline
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 & 2546 & 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 \\
\hline
\end{tabular}
\footnote{a number after two-dimensional IPs; see text for an explanation}
\end{table}
columns of Table 2, we see that the bounds from Theorems 10 and 15 (for the box width) and Proposition 9 (for the cylinder radius) have room for improvement. The polytopes of all core points of the groups from Table 1 are available in the polymake-format at

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

5. More than two invariant subspaces – infinitely many core points?

In the previous section we showed that 2-homogeneous groups (those with precisely two invariant subspaces) have a finite number of core points (up to translation by 1). For other groups there may be an infinite number of core points. For instance, for all integers \( m \in \mathbb{Z} \) the point \((1 + m, -m, m, -m)^\top\) is a core point of the cyclic group \(C_4\) as we will see later (cf. Example 28). Figure 2 visualizes parts of this infinite series, showing orthogonal projections of the lattice-free orbit tetrahedra for \(0 \leq m \leq 4\). In this section we construct

![Figure 2. Impression of an infinite series of lattice-free orbit polytopes for \(C_4\)](image)

similar infinite series of core points (up to translation by 1) for two major classes of groups. These constructions, together with our computational experiments, suggest the following conjecture.

**Conjecture 18.** A transitive permutation group \(\Gamma\) has a finite number of core points up to translation by 1 if and only if \(\Gamma\) is 2-homogeneous.

For the aforementioned core point constructions we use the fact that all core points are close to an invariant subspace of the group by Theorem 7. In Section 5.1 we will look at an outline of a general core point construction based on proximity to invariant subspaces. We use this method to give constructions for all imprimitive groups (in Section Section 5.2) and for all groups with a non-rationally generated invariant subspace (in Section 5.3). For the remaining groups the construction can not be applied directly in general. However, we computationally verified Conjecture 18 for all transitive groups up to degree 127. Details about these special constructions can be found in [Her13, Reh13].
5.1. Constructing core points along invariant subspaces. Our main tool in this section is orthogonal projection to an arbitrary invariant subspace of a transitive group. If this projection of an integer point \( z \) has small norm, i.e., the point \( z \) seems to be a good candidate for a core point. Remember that we can always decompose \( \mathbb{R}^n \) into a direct sum of invariant subspaces \( \mathbb{R}^n = \text{span} 1 \oplus \bigoplus_i V_i \). 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 \( \mathbb{R} \)-irreducible invariant subspace is either rational or irrational. 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. A more detailed study of these groups can be found in [Dix05].

Our goal throughout this section is the construction of core points. Therefore we need a way to prove that an orbit polytope \( \text{conv} \, \Gamma z \) is lattice-free. The main tool that we use is projection onto an invariant subspace of \( \Gamma \). 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 21 will give a sufficient core point condition in quite general (and also quite technical) terms. The rest of this section makes the projection argument more precise.

An important property of the projection to an invariant subspace is that group action and projection operation commute:

**Lemma 19.** Let \( \Gamma \leq S_n \) be a permutation group and \( V \) an invariant subspace of \( \Gamma \). Group action and projection commute: \((\gamma x)|_V = \gamma(x|_V) \) for all \( \gamma \in \Gamma \) and \( x \in \mathbb{R}^n \).

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

We now turn to a method for proving lattice-freeness of orbit polytopes. Let \( \Gamma \leq S_n \) be a permutation group and \( V \) be an invariant subspace of \( \Gamma \). Furthermore, let \( z \in \mathbb{Z}^n_{(k)} \) be an integral point in the \( k \)-th layer. Since all integer points in the orbit polytope \( P := \text{conv} \, \Gamma z \) also lie in the \( k \)-th layer, we start with the following projection setup. We project both the orbit polytope \( P \) and all integer points \( \mathbb{Z}^n_{(k)} \) orthogonally onto \( V \). To ensure the lattice-freeness of \( P \) we have to control the pre-image of all points in the intersection \( Q := P|_V \cap \mathbb{Z}^n_{(k)}|_V \). If the pre-image of \( Q \) intersects \( P \) only at its vertices \( \text{vert}(P) \), 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 \( \text{vert}(P)|_V \). Second, we ensure that only vertices of \( P \) project onto \( \text{vert}(P)|_V \). These two steps together constitute Proposition 21. Before we get there, we start with an outline that introduces facts and notation.
For the first step we use arguments based on the Euclidean norm. We say that $z$ has globally minimal projection onto $V$ if

$$\|z|_V\| \leq \|z'|_V\| \quad \text{for all } z' \in \mathbb{Z}_n^{(k)}.$$  

(9)

If $z$ has globally minimal projection, then integer points in $P$ can project only onto $\text{vert}(P)|_V$, which completes the first step. The argument behind this will be made explicit in Proposition 21 below. However, we will see later that for irrational subspaces there is no point with global minimal projection (cf. Lemmas 32 and 33). In this case the following weaker condition suffices. We say that the point $z$ has locally minimal projection onto $V$ if

$$\|z|_V\| \leq \|z'|_V\| \quad \text{for all } z' \in \mathbb{Z}_n^{(k)} \text{ with } \|z'\| \leq \|z\|.$$  

(10)

Since only points with $\|z'\| \leq \|z\|$ can lie in the orbit polytope $P = \text{conv} \Gamma z$, it is enough to control the projection of these points.

For the second step of the outline above, proving lattice-freeness of $P$, we argue with the stabilizer group of the vertex $z$ and its projection $z|_V$. We will need the following lemma.

Lemma 20. Let $\Gamma \leq S_n$ and $V$ an invariant subspace of $\Gamma$. For any $z \in \mathbb{Z}^n$ we have $\text{Stab}_\Gamma(z) \leq \text{Stab}_\Gamma(z|_V)$.

Proof. Let $\gamma \in \text{Stab}_\Gamma(z)$, thus $\gamma z = z$. This implies $\gamma(z|_V + z|_W) = z|_V + z|_W$. Hence $\gamma z|_V - z|_V = z|_W - \gamma z|_W$. The only element in $V \cap W$ is the zero vector. Therefore $\gamma \in \text{Stab}_\Gamma(z|_V)$. \hfill $\square$

Proposition 21. Let $\Gamma \leq S_n$ be a permutation group and $V$ an invariant subspace of $\Gamma$. Let $z \in \mathbb{Z}^n$ have locally minimal projection for $V$. Then $z$ is a core point for $\Gamma$ if and only if $z$ is a core point for $\text{Stab}_\Gamma(z|_V)$.

Proof. Because $\text{Stab}_\Gamma(z|_V)$ is a subgroup of $\Gamma$, we only have to prove the “if”-part. For this let $y$ be an integer point in $\text{conv} \Gamma z$. We can write $y$ as convex combination

$$y = \sum_{\gamma \in \Gamma} \lambda_\gamma \gamma z$$

(11)

with $0 \leq \lambda_\gamma \leq 1$ and $\sum_{\gamma \in \Gamma} \lambda_\gamma = 1$. This yields:

$$\|z|_V\|^2 \leq \|y|_V\|^2 = \left\| \left( \sum_{\gamma \in \Gamma} \lambda_\gamma \gamma z \right) |_V \right\|^2$$

(12)

$$\leq \sum_{\gamma \in \Gamma} \lambda_\gamma \left( |(\gamma z)|_V \right)^2 = \|z|_V\|^2.$$
Since the squared norm is strictly convex on \( V \), equality in (12) holds if and only if there is a coset \( \gamma_0 \text{Stab}_\Gamma(z|_V) \) such that \( \sum_{\gamma \in \gamma_0 \text{Stab}_\Gamma(z|_V)} \lambda_\gamma = 1 \). Plugging this into (11) yields
\[
\gamma_0^{-1} y = \sum_{\gamma \in \text{Stab}_\Gamma(z|_V)} \lambda_\gamma \gamma z.
\]
Since \( z \) is a core point for \( \text{Stab}_\Gamma(z|_V) \), we must have \( \gamma_0^{-1} y \in \text{Stab}_\Gamma(z|_V)z \). Hence, the point \( y \) lies also in the orbit \( \Gamma z \). From this we conclude that \( z \) is a core point for \( \Gamma \).

5.2. **Imprimitive groups.** We start this section with a specialization of Proposition 21 and then prove that imprimitive groups have an infinite number of core points (up to translation).

**Corollary 22.** Let \( \Gamma \leq S_n \) be a permutation group and \( \mathbb{R}^n = \text{Fix}(\Gamma) \oplus V \oplus W \) a decomposition into \( \Gamma \)-invariant subspaces. Let \( z \in \mathbb{Z}^n_\Gamma \) be a core point for \( \text{Stab}_\Gamma(z|_V) \) with globally minimal projection. Let \( w \in W \cap \mathbb{Z}^n \) be such that \( \text{Stab}_\Gamma(z|_V) \leq \text{Stab}_\Gamma(w) \). Then for all \( m \in \mathbb{Z} \) the polytope \( P_m := \text{conv} \Gamma(z + mw) \) contains no integer points except its vertices.

**Proof.** To prove that \( P_m \) is lattice-free we apply Proposition 21. Since \( z \) has globally minimal projection onto \( V \), so has \( z + mw \). In particular, \( z + mw \) thus also has locally minimal projection. It remains to show that \( z + mw \) is a core point for \( \text{Stab}_\Gamma(z|_V) \). Because of the inclusion \( \text{Stab}_\Gamma(z|_V) \leq \text{Stab}_\Gamma(w) \), we have that
\[
P'_m := \text{conv}(\text{Stab}_\Gamma(z|_V)(z + mw)) = mw + \text{conv}(\text{Stab}_\Gamma(z|_V)z).
\]
Because \( z \) is a core point for \( \text{Stab}_\Gamma(z|_V) \) by assumption of the corollary, this shows that the polytope \( P'_m \) is lattice-free. Hence, \( z + mw \) is a core point for \( \text{Stab}_\Gamma(z|_V) \) and thus also for \( \Gamma \) by Proposition 21.

**Example 23.** As an example we consider the cyclic group \( C_4 = \langle (1234) \rangle \). The arguments here will be generalized in Section 5.2 to imprimitive groups. The vector \( w := (1, -1, 1, -1)^\top \) spans a one-dimensional invariant subspace. Its orthogonal complement, besides the fixed space, is spanned by \( v := (1, 0, -1, 0)^\top \) and \( v' := (0, 1, 0, -1)^\top \).

For applying Corollary 22 let \( V := \text{span}\{v, v'\} \) and \( W := \text{span}\{w\} \). We will see in Lemma 26 that \( e_1 := (1, 0, 0, 0)^\top \) is a core point for \( C_4 \) with globally minimal projection on \( V \). We compute \( e_1|_V = \frac{1}{2} v \), hence the stabilizer \( \text{Stab}_{C_4}(e_1|_V) \) is trivial. Therefore we may choose any integer direction from \( W \). 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 \( V \) and \( W \) in Corollary 22, we still have that \( e_1 \) has globally minimal projection on \( W \) (again cf. Lemma 26). Its projection is \( e_1|_W = \frac{1}{4} w \) with stabilizer \( \text{Stab}_{C_4}(e_1|_W) = \langle (13)(24) \rangle \). Since all non-zero elements from \( V \) have trivial stabilizer, we cannot find a suitable integer direction \( v \in V \) that is compatible with the stabilizer condition of Corollary 22.

However, we may also work with Proposition 21 directly. Let \( av + bv' \) with \( a, b \in \mathbb{Z} \) be an arbitrary integer direction in \( V \). By Proposition 21
\[
p(a, b) := e_1 + av + bv' = (1 + a, b, -a, -b)^\top
\]
is a core point for $C_4$ if and only if it is a core point for $\text{Stab}_{C_4}(e_1|_W) = \langle(1 \, 3)(2 \, 4)\rangle$.

The orbit polytope $\text{conv} \, \text{Stab}_{C_4}(e_1|_W)p(a, b)$ has only two vertices,

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

Consider a proper convex combination $\lambda u + (1 - \lambda)u'$ on the line segment between $u$ and $u'$ with $0 < \lambda < 1$. If $\lambda u + (1 - \lambda)u'$ is integral, then looking at the first coordinate shows that $\lambda(1 + a) + (1 - \lambda)(-a) = (2a + 1)\lambda$ must be an integer. Looking at the second coordinate, we similarly obtain that $2b\lambda$ must be an integer. If $\gcd(2a + 1, 2b) > 1$ this is possible for $\lambda = 1/\gcd(2a + 1, 2b)$. If $b = 0$, the second condition is automatically fulfilled and the first condition is satisfiable if $a \not\in \{-1, 0\}$. We have therefore proven: $p(a, b)$ is a core point for $C_4$ if and only if $\gcd(2a + 1, 2b) = 1$ (with our convention $\gcd(x, 0) = |x|$).

Figure 3 depicts instances of lattice-free orbit tetrahedra of $p(a, b)$ for $(a, b) \in \{(0, 0), (0, 1), (0, 2), (0, 3), (0, 4)\}$.

\[\text{Figure 3. Impression of an infinite series of lattice-free orbit polytopes for } C_4\]

We will show that the conditions of Corollary 22 are satisfied for imprimitive groups. However, it can also be applied to other groups with rational subspaces if a suitable direction is found, which may however be difficult.

Recall from Section 2.1 the definition of an imprimitive permutation group. For each imprimitive permutation group $G$ acting on $\Omega = [n]$, there is a partition of $\Omega = \bigsqcup_{i=1}^B \Omega_i$ such that $G$ acts on the $B$ sets $\Omega_i$. For every $\gamma \in \Gamma$ there exists an index $j$ such that $\gamma\Omega_i = \Omega_j$. Every such block $\Omega_i$ has size $S = \frac{n}{B}$. These blocks induce a rational invariant subspace of $G$ in the following way. Let

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

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

\[ \mathbb{R}^n = \text{span} \mathbf{1} \oplus W_\Omega \oplus V_\Omega. \]

**Example 24.** As an example we consider the cyclic group \( C_6 = \langle (1 2 3 4 5 6) \rangle \).

The group action of \( C_6 \) is imprimitive as it preserves the partition \( \Omega = \{\{1, 3, 5\}, \{2, 4, 6\}\} \).

The corresponding invariant subspace \( U_\Omega \) is \( \text{span}\{ (1, 0, 1, 0, 1, 0)^T, (0, 1, 0, 1, 0)^T \} \).

For its non-fixed summand we obtain \( W_\Omega = \text{span}(1, -1, 1, -1, 1, -1)^T \).

Note that the block system and the corresponding decomposition \((14)\) is not unique. For instance, the group \( C_6 \) has another block system \( \Omega' = \{\{1, 4\}, \{2, 5\}, \{3, 6\}\} \).

This corresponds to \( U_{\Omega'} = \text{span}\{ (1, 0, 0, 1, 0, 0)^T, (0, 1, 0, 0, 1, 0)^T, (0, 1, 0, 1, 0, 1)^T \} \) and \( W_{\Omega'} = \text{span}\{ (2, -1, -1, 2, -1, -1)^T, (-1, 2, -1, 2, -1, -1)^T \} \).

With these invariant subspaces \( V_\Omega \) and \( W_\Omega \) we show that the conditions of Corollary 22 are fulfilled for imprimitive groups.

**Theorem 25.** Let \( \Gamma \leq S_n \) act imprimitively, i.e. the permutation action of \( \Gamma \) preserves a block system with blocks of size \( 1 < S < n \). If \( k \) is not a multiple of \( S \), then the core set of \( \Gamma \) contains infinitely many core points in layer \( \mathbb{Z}^n_{(k)} \).

**Proof.** The proof of this theorem follows immediately from applying Corollary 22 to the following Lemma 26. By the latter, we find a core point \( z^{(k)} \) in the claimed layers with globally minimal projection onto \( V_\Omega \). Moreover, it produces a non-zero direction \( w \in W_\Omega \cap \mathbb{Z}^n \) such that \( \text{Stab}_\Gamma(z^{(k)}|V_\Omega) \leq \text{Stab}_\Gamma(w) \). Therefore, for every \( m \in \mathbb{Z} \), the point \( z^{(k)} + mw \) is a core point by Corollary 22. Since \( w \) is not the zero vector, these core points are different for varying \( m \).

**Lemma 26.** Let \( \Gamma \leq S_n \) act imprimitively, i.e. the permutation action of \( \Gamma \) preserves a block system with blocks of size \( 1 < S < n \). For the corresponding invariant subspaces \( U_\Omega, V_\Omega, W_\Omega \) from \((14)\) the following holds: If \( k \) is not a multiple of \( S \), then there exist a core point \( z^{(k)} \in \mathbb{Z}^n_{(k)} \) with globally minimal projection onto \( V_\Omega \) and a non-zero direction \( w \in W_\Omega \cap \mathbb{Z}^n \) such that \( \text{Stab}_\Gamma(z^{(k)}|V_\Omega) \leq \text{Stab}_\Gamma(w) \).

**Proof.** To keep notation as simple as possible, we assume w.l.o.g. that the first of the blocks \( \Omega_1, \ldots, \Omega_B \) of \( \Gamma \) is \( \Omega_1 = \{1, \ldots, S\} \). Consider an arbitrary \( z \in \mathbb{Z}^n \).

We compute the squared norm of the projection onto \( V_\Omega \) as

\[
\|z|V_\Omega\|^2 = \|z\|^2 - \|z|U_\Omega\|^2 = \left( \sum_{b=1}^{B} \sum_{j \in \Omega_b} z_j^2 \right) - \left( \frac{1}{S} \sum_{b=1}^{B} \left( \sum_{j \in \Omega_b} z_j \right)^2 \right).
\]

Looking at this sum of squares, we observe that the total expression is minimized if inside each block \( \Omega_b \), the coordinates differ in the least possible way and the total number of blocks with non-zero contribution is minimized. Let
\( l \in \{0, \ldots, S - 1\} \) be congruent to \( k \) mod \( S \). Then the point
\[
(16) \quad z^{(k)} = \sum_{i=1}^{\lfloor \frac{S}{2} \rfloor + 1} e_i + \sum_{j=2}^{\frac{S}{2}} u^{(j)}.
\]

with \( u^{(j)} \) as in \((13)\) satisfies this condition and hence has globally minimal projection. As a sum of squares, the projection in \((15)\) can be zero if and only if \( k \) is a multiple of \( S \). Thus, \( z^{(k)} \) has non-zero length if \( k \) is not a multiple of \( S \). The choice for the minimum in \((16)\) is not the most obvious, but it has the advantage that it is a universal core point because it has coordinates with only zeros and ones.

Now that we have found a core point \( z^{(k)} \) with globally minimal projection, it remains to find a suitable non-zero direction \( w \in W_\Omega \cap \mathbb{Z}^n \). For this we need the stabilizer \( \text{Stab}_U(z^{(k)}|_{V_\Omega}) \) to be contained in \( \text{Stab}_U(w) \). To compute the projection \( z^{(k)}|_{V_\Omega} \) we again use our explicit basis for \( U_\Omega \). Looking again at \((16)\) we see that \( z^{(k)}|_{V_\Omega} = z^{(k+S)}|_{V_\Omega} \) since the vectors differ only in summands from \( U_\Omega \), which is the orthogonal complement of \( V_\Omega \). For the projection we may thus assume w.l.o.g. that \( k < S \) and we compute
\[
(17) \quad z^{(k)}|_{V_\Omega} = z^{(k)} - z^{(k)}|_{U_\Omega} = \left( \sum_{i=1}^{k} e_i \right) - \frac{k}{S} u^{(1)} = \sum_{i=1}^{k} \left( 1 - \frac{k}{S} \right) e_i - \sum_{i=k+1}^{S} \frac{k}{S} e_i.
\]

For the direction \( w \) we look at the projection of \( u^{(1)} \) onto \( W_\Omega \), which is \( u^{(1)}|_{W_\Omega} = u^{(1)} - \frac{S}{n} \). After scaling this gives a non-zero integer vector \( w \) with stabilizer \( \text{Stab}_U(w) = \text{Stab}_U(\Omega_1) \). Looking again at \((17)\), we observe that \( z^{(k)}|_{V_\Omega} \) has a zero at coordinate \( i \) if and only if \( i \) is not in \( \Omega_1 \). Thus, the stabilizer of \( z^{(k)}|_{V_\Omega} \) must be a subgroup of \( \text{Stab}_U([n] \setminus \Omega_1) = \text{Stab}_U(\Omega_1) = \text{Stab}_U(w) \).

**Remark 27.** Note that many points minimize \((15)\). As long as they are core points, they are valid alternative choices for \( z^{(k)} \) in \((16)\). If used in the proof of Theorem \((25)\) they may also lead to infinite series of core points.

**Example 28.** We continue Example \((24)\) and construct core points for the cyclic group \( C_6 \). 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 \( k = 1, 2, 4, 5 \) because these are not multiples of \( S \). The layer minima \( z^{(k)} \) from Lemma \((26)\) are given by
\[
\begin{align*}
z^{(1)} &= (1, 0, 0, 0, 0, 0)^T, \\
z^{(2)} &= (1, 0, 1, 0, 0, 0)^T, \\
z^{(4)} &= (1, 1, 0, 1, 0, 1)^T, \\
z^{(5)} &= (1, 1, 1, 1, 0, 1)^T.
\end{align*}
\]

The corresponding direction is \( w = (1, -1, 1, -1, 1, -1)^T \) from Example \((24)\).

Corollary \((22)\) implies that for every \( m \in \mathbb{Z} \) the simplex \( \text{conv} \ C_6(z^{(k)} + mw) \) is lattice-free. In the case \( k = 1 \), for every \( m \in \mathbb{Z} \) the simplex given by the orbit of
\[
(18) \quad z^{(1)} + mw = (1 + m, -m, m, -m, m, -m)^T \in \mathbb{Z}_+(1)
\]
is lattice-free.
Note that for the layer with index $k = 3$ 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 $C_6$, 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 25. The corresponding layer minima are

$$z^{(1)} = (1, 0, 0, 0, 0, 0)^T,$$
$$z^{(3)} = (1, 1, 0, 0, 1, 0)^T,$$
$$z^{(5)} = (1, 1, 1, 0, 1, 1)^T.$$

As direction $w$ we choose a multiple of $u'(1)|_{\Omega'} = \frac{1}{3}(2, -1, -1, 2, -1, -1)^T$ such that the vector is integral. In the case $k = 3$, for instance, the simplex given by the orbit of

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

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 27), leading to the series of core points

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

for $m \in \mathbb{Z}$. The core points described by (20) and (19) are different. To see this we observe that in (20) two consecutive coordinates have the same value $-m$; this does happen in (19). Besides these constructions, there are entirely different ones that yield infinite series for $C_6$.

For instance, one can check that for every $a, b \in \mathbb{Z}$ the simplex given by the orbit of $(1, a, b, 0, -a, -b)^T \in \mathbb{Z}^n_{(1)}$ is lattice-free. We have already seen a proof of similar constructions for the special case $C_4$ in Example 23. More examples can be found in [Her13, Reh13].

### 5.3. Irrational subspaces.

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

**Theorem 29.** Let $\Gamma \leq S_n$ have an irrational invariant subspace. If $k$ is not a multiple of $n$, then the core set of $\Gamma$ contains infinitely many core points in layer $\mathbb{Z}^n_{(k)}$.

To prove this theorem, we begin this section with an adaption of Proposition 21.

**Corollary 30.** Let $\Gamma \leq S_n$ and let $V$ be an invariant subspace of $\Gamma$. Let $z \in \mathbb{Z}^n_{(k)}$ be an integer point with locally minimal projection. Moreover, let $\text{Stab}_\Gamma(z) = \text{Stab}_\Gamma(z|_V)$. Then $z$ is a core point for $\Gamma$.

**Proof.** The minimality condition is the same as in Proposition 21. If $\text{Stab}_\Gamma(z) = \text{Stab}_\Gamma(z|_V)$, then the orbit of $\text{Stab}_\Gamma(z|_V)z$ consists only of a single element, showing that $z$ is a core point for $\text{Stab}_\Gamma(z|_V)$. Thus by Proposition 21, $z$ is a core point for $\Gamma$.  

In order to apply Corollary 30 for the proof of Theorem 29 we show that its prerequisites are satisfied for an irrational invariant subspace. First we show in Lemma 31 that the stabilizer condition holds. Lemma 33 and Lemma 32 together show that the local minimality condition is fulfilled.
Lemma 31. Let $Γ \leq S_n$ and let $V$ be an irrational invariant subspace of $Γ$. Then $\text{Stab}_Γ(z) = \text{Stab}_Γ(z|_V)$ for any $z \in \mathbb{Z}^n$.

Proof. We have already proven $\text{Stab}_Γ(z) \leq \text{Stab}_Γ(z|_V)$ in Lemma 20. For the reverse direction let $\mathbb{R}^n = \text{span } 1 \oplus V \oplus W$. Then $W$ must be an irrational invariant subspace because $V$ is irrational. We consider a $γ ∈ Γ \setminus \text{Stab}_Γ(z)$ and show $γ ∉ \text{Stab}_Γ(z|_V)$. For $z = 0$ the statement is obviously true, so let $z ≠ 0$. Then

$$γz - z = (γz - z)|_V + (γz - z)|_W$$

is a non-zero integral vector. As $V$ and $W$ are irrational subspaces, both projections on the right must be non-zero, showing in particular $(γz - z)|_V = γz|_V - z|_V ≠ 0$. Hence $γ ∉ \text{Stab}_Γ(z|_V)$. □

Lemma 32. Let $Γ \leq S_n$ and let $V$ be an irrational invariant subspace of $Γ$. Then for all $k ∈ [n-1]$ and every $z ∈ Z^n_{(k)}$ it holds that $∥z|_V∥ > 0$.

Proof. Let $\mathbb{R}^n = \text{span } 1 \oplus V \oplus W$. Then $W$ is an irrational invariant subspace of $Γ$. We know that $z|_V$ is the zero vector if and only if $z ∈ \text{span } 1 \oplus W$. This is in turn equivalent to the rational vector $z - \frac{k}{n} 1$ 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 an integral multiple of $n$. □

Lemma 33. Let $Γ \leq S_n$ and let $V$ be an irrational invariant subspace of $Γ$. Then for every $ε > 0$ and $k ∈ [n-1]$ there exists a vector $z ∈ Z^n_{(k)}$ such that $∥z|_V∥ < ε$.

For the proof of Lemma 33 we use two auxiliary statements. We begin with the symmetry of the projection matrix $P_V = (e_i|_V)_{i ∈ [n]} ∈ \mathbb{R}^{n×n}$, which maps $\mathbb{R}^n$ onto an invariant subspace $V$.

Lemma 34. For the matrix $P_V$ of an orthogonal projection to a linear subspace $V$ holds:

(i) $\langle e_i|_V, e_j|_V \rangle = \langle e_i|_V, e_j|_V \rangle$

(ii) The projection matrix $P_V = (e_i|_V)_{i ∈ [n]} ∈ \mathbb{R}^{n×n}$ is symmetric.

Proof. Let $v_1, \ldots, v_d$ be an orthonormal basis for $V$.

$$\langle e_i|_V, e_j|_V \rangle = \left( \sum_{k=1}^d \langle e_i, v_k \rangle v_k, \sum_{l=1}^d \langle e_j, v_l \rangle v_l \right)$$

$$= \sum_{k=1}^d \langle e_i, v_k \rangle \langle e_j, v_k \rangle = \langle e_i|_V, e_j \rangle$$

The symmetry in the second part follows from the symmetry of the scalar product in $\langle e_i|_V, e_j \rangle = \langle e_i|_V, e_j|_V \rangle = \langle e_j|_V, e_i|_V \rangle = \langle e_j|_V, e_i \rangle$. □

The main ingredient to prove Lemma 33 is Kronecker’s Theorem, which is reproduced below as given in [Sch98 p. 80].

Theorem 35 (Kronecker’s Theorem). Let $A ∈ \mathbb{R}^{m×n}$ and let $b ∈ \mathbb{R}^n$. Then the following two statements are equivalent:

(i) for each $ε > 0$ there is an $x ∈ \mathbb{Z}^n$ with $∥Ax - b∥ < ε$;

(ii) for each $y ∈ \mathbb{R}^n$ the implication $A^Ty ∈ \mathbb{Z}^n ⇒ b^Ty ∈ \mathbb{Z}$ is true.
Proof of Lemma 33. 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 $\|P_V z\| < \varepsilon$.

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

$$\|kP_ve_1 + P_vBz'\| < \varepsilon.$$  (21)

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 34 we have to show that $B^\top y' \in \mathbb{Z}^n$ implies $(e_1)^\top y' \in \mathbb{Z}$ where $y' := PVy = y|_V$ 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 $(b^{(i)}, y') \in \mathbb{Z}$. Thus, we can write $y'$ as $y' = \zeta 1 + u$ for some $\zeta \in \mathbb{R}$ and an integral vector $u \in \mathbb{Z}^n$. Since $y'$ lies in $V$, we know that $0 = (1, y') = \zeta 1 + (1, u)$. This shows that $\zeta$ must be a rational number. Hence, $y'$ must be a rational vector. The only rational vector lying in the irrational invariant subspace $V$ is the zero vector.

Now we have all the ingredients for the proof of our main result of this section:

Proof of Theorem 29. Lemma 32 together with Lemma 33 show that for every $k \in [n-1]$ and every $\varepsilon > 0$ we find an integer point $z \in \mathbb{Z}_n^{(k)}$ such that $0 < \|z|_V\| < \varepsilon$ and, by choosing one with minimal norm, $\|z|_V\| \leq \|z'|_V\|$ for all $z' \in \mathbb{Z}_n^{(k)}$ with $\|z'\| \leq \|z\|$.

By letting $\varepsilon$ approach zero, we thus obtain a sequence of mutually distinct points $z^{(1)}, z^{(2)}, \ldots \in \mathbb{Z}_n^{(k)}$, which by construction each satisfy the minimality condition of Corollary 30. Lemma 31 shows that also the stabilizer condition of Corollary 30 is automatically fulfilled. Hence, each of these points $z^{(1)}, z^{(2)}, \ldots \in \mathbb{Z}_n^{(k)}$ is a core point.

We close the section with an example of an infinite series of core points that can be derived from Theorem 29. For a detailed discussion we refer to [Reh13 Section 5.2.2].

Example 36. Let $C_5 = \langle (1 \ 2 \ 3 \ 4 \ 5) \rangle$ be the cyclic group of order five. Moreover, let $f_j$ be the $j$-th Fibonacci number. For every $j$ the point $z^{(j)} = (0, f_j, f_j, 0, f_{j+1})^\top$ is a core point for $C_5$.

Acknowledgements

We thank Reinhard Knörr and Michael Joswig for valuable discussions and we thank Erik Friese and Frieder Ladisch for helpful comments on a previous version of the paper.
Bibliography.

[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.

[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](http://arxiv.org/abs/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.

[Cam72] Peter J. Cameron. Bounding the rank of certain permutation groups. *Math. Z.*, 124:343–352, 1972.

[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.

[Fuk04] Komei Fukuda. Polyhedral computation FAQ, 2004. [http://www.ifor.math.ethz.ch/fukuda/polyfaq/polyfaq.html](http://www.ifor.math.ethz.ch/fukuda/polyfaq/polyfaq.html).

[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.

[Her13] Katrin Herr. *Core Sets and Symmetric Convex Optimization*. PhD thesis, TU Darmstadt, 2013.

[HRS13] Katrin Herr, Thomas Rehn, and Achill Schürmann. Exploiting Symmetry in Integer Convex Optimization using Core Points. *Operations Research Letters*, 41:298–304, 2013.

[Hur90] C. 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.

[Job48] 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.

[Kan72] William M. Kantor. $k$-homogeneous groups. *Math. Z.*, 124:261–265, 1972.

[Kno11] Reinhard Knörr. personal communication, 2011.

[Reh13] Thomas Rehn. *Exploring core points for fun and profit – a study of lattice-free orbit polytopes*. PhD thesis, Universität Rostock, 2013.

[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.

Software.

[GAP] GAP – Groups, Algorithms, Programming – a System for Computational Discrete Algebra.

[Nor] Normaliz by W. Bruns, B. Ichim and C. Söger. [http://www.mathematik.uni-osnabrueck.de/normaliz/](http://www.mathematik.uni-osnabrueck.de/normaliz/)

[pol] polymake by E. Gawrilow, M. Joswig & al. [http://www.polymake.org/](http://www.polymake.org/)
Department of Mathematics, Technische Universität Darmstadt, Dolivostraße 15, 64293 Darmstadt, Germany
E-mail address: herr@mathematik.tu-darmstadt.de

initOS GmbH & Co. KG, Hegelstraße 28, 39104 Magdeburg, Germany
E-mail address: thomas.rehn@research.initos.com

Institute for Mathematics, University of Rostock, 18051 Rostock, Germany
E-mail address: achill.schuermann@uni-rostock.de