

## PERMUTATION POLYTOPES OF CYCLIC GROUPS

BARBARA BAUMEISTER, CHRISTIAN HAASE, BENJAMIN NILL,  
AND ANDREAS PAFFENHOLZ

ABSTRACT. We investigate the combinatorics and geometry of permutation polytopes associated to cyclic permutation groups, i.e., the convex hulls of cyclic groups of permutation matrices. We give formulas for their dimension and vertex degree. In the situation that the generator of the group consists of at most two orbits, we can give a complete combinatorial description of the associated permutation polytope. In the case of three orbits the facet structure is already quite complex. For a large class of examples we show that there exist exponentially many facets.

### INTRODUCTION

A *Permutation polytope* is the convex hull of a group of permutation matrices. We refer to the preceding article [2] for some historical and motivational remarks. The most famous permutation polytope is the *Birkhoff polytope*, whose vertex set is the entire set of  $n \times n$ -permutation matrices. In [2] we proposed the systematic study of permutation polytopes in their own right. We introduced suitable notion of equivalences, studied the vertex-edge graph, products and free sums, and classified all permutation polytopes up to dimension four.

In this article, we investigate permutation polytopes associated to cyclic permutation groups. In order to learn more about general permutation polytopes it seems to be crucial to enhance our understanding of the convex hulls of subgroups generated by only one element. This boils down to the study of the elementary number theory of the cycle structure of the generator permutation. Already a relatively small input can generate fairly complicated polytopes: take the group generated by a permutation which is the product of three disjoint cycles of lengths 10, 18, 45. This leads to a 57-dimensional polytope with 90 vertices and 15373 facets whose vertex-edge graph is complete. This example is about as complex as we can handle computationally. Still, using the structure of a permutation polytope it is possible to determine important invariants of the polytope like the dimension and the vertex degree in terms of the cycle lengths (see Section 2). For groups generated by a permutation which is a product of at most two cycles we can characterize the polytopes completely (Proposition 3.3). However, the previous example indicates that in the situation of three cycles the complexity of the facet structure of these polytopes becomes enormous. We show in Theorem 3.6 that the number of facets in such a specific situation grows indeed exponentially in the dimension.

In many respects, our experience has turned out to be similar to the challenges faced by Hood and Perkinson [11] when investigating the facets of the permutation polytope associated to the group of even permutations. They also constructed

---

<sup>1</sup>52B12, 20B35, 05E10, 52B05

<sup>2</sup>Permutation polytope, permutation matrices, combinatorial description, facet structure, marginal polytope

exponentially many facets with respect to the dimension of the polytope. However, in their situation the number of vertices grows exponentially as well, while in our case the number of vertices remains polynomially bounded.

The features of many of these objects such as a large number of facets and a complete vertex-edge graph are reminiscent of the properties of cyclic polytopes [19, pp.10-16]. While the latter ones are simplicial, in many of the cases considered here, each facet contains far more than half of the total number of vertices of the polytope. Permutation polytopes of cyclic permutation groups might be considered as highly symmetric analogues of cyclic polytopes. It was recently shown by Rehn [15] that if the order of a cyclic permutation group is  $n = k_1 \cdots k_r$ , where  $k_1, \dots, k_r$  are coprime prime powers, then the associated permutation polytope has at least  $k_1! \cdots k_r!$  many affine automorphisms. On the other hand, Kaibel and Waßmer [14] show that the order of the combinatorial automorphism group of a cyclic polytope is at most twice its number of vertices.

Cyclic permutation polytopes – and more generally abelian permutation polytopes – are instances of so-called marginal polytopes. Their inequality description is important in statistics and optimization. This will be explored in an upcoming paper [3] (cf. Remark 3.11).

**Note.** One should not confuse ‘permutation polytopes’ with ‘orbitopes’, the convex hull of an orbit of a compact group acting linearly on a vector space. Recently, Sanyal, Sottile and Sturmfels [16] gave a systematic approach to orbitopes. They also studied the permutation polytopes associated to the groups  $O(n)$  and  $SO(n)$ . In this setting permutation polytopes are called *tautological orbitopes*. Since for each orbitope there is a permutation polytope mapping linearly onto it, permutation polytopes serve as *initial objects* in this context.

**Organization of the paper.** In Section 1 we introduce notation and basic properties. In Section 2 we give formulas for the dimension and the vertex degree, and we describe a criterion when a vertex forms an edge with the unit of the group. In Section 3 we study closely the situation when the group generator is decomposed in at most three cycles. While we can completely describe the case of the one or two cycles, the first difficult situation occurs for three cycles, where we construct a large family of facets for one infinite class of examples.

**Acknowledgments.** Many of these results are based on extensive calculations using the software packages GAP [7] and polymake [12]. The first author likes to thank the support by the DFG through the SFB 701 “Spektral Structures and Topological Methods in Mathematics”. The last three authors were supported by Emmy Noether fellowship HA 4383/1 of the German Research Foundation (DFG). The third author is supported by the US National Science Foundation (DMS 1102424). The last author is supported by the DFG Priority Program 1489.

## 1. NOTATION AND BASIC PROPERTIES

1.1. **Notation.** For a positive integer  $n \in \mathbb{N}$  we denote

$$[n] := \{1, \dots, n\}.$$

Since it will be more suitable later on, we also define

$$[[n]] := \{0, \dots, n-1\}.$$

For a finite set  $I \subset \mathbb{N}$  we denote by  $\gcd(I)$  and  $\text{lcm}(I)$  the greatest common divisor and the least common multiple of all elements in  $I$ , respectively. By convention  $\gcd(\emptyset) := 0$  and  $\text{lcm}(\emptyset) := 1$ . For integers  $k, l \in \mathbb{Z}$  we write  $k | l$  if  $k$  divides  $l$ .

The convex and the affine hull of a set  $S$  in a real vector space will be denoted by  $\text{conv}(S)$  and by  $\text{aff}(S)$ , respectively.

**1.2. Representation polytopes.** Let  $V$  be a real  $n$ -dimensional vector space. Then  $\text{GL}(V)$  denotes the set of automorphisms. By choosing a basis we can identify  $\text{GL}(V)$  with the set  $\text{GL}_n(\mathbb{R})$  of invertible  $n \times n$ -matrices. In the same way, we identify  $\text{End}(V)$  with the vector space  $\text{Mat}_n(\mathbb{R})$  of  $n \times n$ -matrices.

Let  $G$  be a group. A homomorphism  $\rho: G \rightarrow \text{GL}(V)$  is called a *real representation*. In this case

$$(\rho) := \text{conv}(\rho(g) : g \in G) \subseteq \text{Mat}_n(\mathbb{R}) \cong \mathbb{R}^{n^2}$$

is called the associated *representation polytope*.

**1.3. Permutation polytopes.** The symmetric group  $S_n$  acts on the set  $[n]$ . By identifying  $[n]$  with the basis vectors  $\{e_1, \dots, e_n\}$  of  $\mathbb{R}^n$ , we get a representation  $S_n \rightarrow \text{GL}(\mathbb{R}^n)$ . This map identifies the symmetric group  $S_n$  with the set of  $n \times n$  *permutation matrices*, i.e., the set of matrices with entries 0 or 1 such that in any column and any row there is precisely one 1. For a subset  $G \subseteq S_n$  we let  $\text{M}(G)$  be the corresponding set of permutation matrices. For  $S \subseteq G$  we let  $\langle S \rangle$  be the smallest subgroup of  $G$  containing  $S$ .

An injective homomorphism  $G \rightarrow S_n$  is called *permutation representation*. Subgroups  $G \leq S_n$  are called *permutation groups*. In this case, the representation polytope

$$P(G) := \text{conv}(\text{M}(G))$$

is called the *permutation polytope* associated to  $G$ .

The special case  $G = S_n$  yields the well-known *n*th *Birkhoff polytope*  $B_n := P(\text{M}(S_n))$  (see e.g. [4]). It has dimension  $(n - 1)^2$ .

**1.4. Equivalences.** When working with permutation polytopes, one would like to identify permutation groups that clearly define affinely equivalent permutation polytopes. Therefore, we introduced in [2] the notion of stable equivalence. Here,  $\mathbb{R}[G]$  denotes the group algebra of  $G$  with real coefficients.

**Definition 1.1.** For a representation  $\rho: G \rightarrow \text{GL}(V)$  define the affine kernel  $\ker^\circ \rho$  as

$$\ker^\circ \rho := \left\{ \sum_{g \in G} \lambda_g g \in \mathbb{R}[G] : \sum_{g \in G} \lambda_g \rho(g) = 0 \text{ and } \sum_{g \in G} \lambda_g = 0 \right\}$$

Say that a real representation  $\rho': G \rightarrow \text{GL}(V')$  is an *affine quotient* of  $\rho$  if  $\ker^\circ \rho \subseteq \ker^\circ \rho'$ . Then real representations  $\rho_1$  and  $\rho_2$  of  $G$  are *stably equivalent*, if there are affine quotients  $\rho'_1$  of  $\rho_1$  and  $\rho'_2$  of  $\rho_2$  such that  $\rho_1 \oplus \rho'_1 \cong \rho_2 \oplus \rho'_2$  as  $G$ -representations.

**Example 1.2.** The following representations of the group  $\mathbb{Z}_4$  are stably equivalent:

$$\begin{aligned} \langle (1234) \rangle &\leq S_4, & \langle (1234)(5) \rangle &\leq S_5, \\ \langle (1234)(56) \rangle &\leq S_6, & \langle (1234)(56)(78) \rangle &\leq S_8, \\ \langle (1234)(5678) \rangle &\leq S_8. \end{aligned}$$

For the following, let us denote by  $\text{Irr}(G)$  the set of pairwise non-isomorphic irreducible  $\mathbb{C}$ -representations, i.e., homomorphisms  $G \rightarrow \text{GL}(W)$  where  $W$  is a  $\mathbb{C}$ -vector space which does not contain a proper  $G$ -invariant subspace. For instance, there is the *trivial representation*,  $1_G: G \rightarrow \text{GL}(\mathbb{C})$ ,  $g \mapsto 1$ . As a  $G$ -representation over  $\mathbb{C}$  any real representation  $\rho: G \rightarrow \text{GL}(V)$  splits into irreducible representations. We denote these *irreducible factors* of  $\rho$  by  $\text{Irr}(\rho) \subseteq \text{Irr}(G)$ .

In [2] we proved an explicit criterion for the polytopes of two representations to be stably equivalent.

**Theorem 1.3** (Baumeister et al. [2, 2.3]). *Suppose  $\rho$  and  $\bar{\rho}$  are stably equivalent real representations of a finite group  $G$ . Then  $P(\rho)$  and  $P(\bar{\rho})$  are affinely equivalent.*

*Two real representations are stably equivalent if and only if they contain the same non-trivial irreducible factors.*

**Definition 1.4.** Two real representations  $\rho_i: G_i \rightarrow \text{GL}(V_i)$  (for  $i = 1, 2$ ) of finite groups are *effectively equivalent*, if there exists an isomorphism  $\phi: G_1 \rightarrow G_2$  such that  $\rho_1$  and  $\rho_2 \circ \phi$  are stably equivalent  $G_1$ -representations.

Moreover, we say  $G_1 \leq S_{n_1}$  and  $G_2 \leq S_{n_2}$  are *effectively equivalent* permutation groups, if  $G_1 \hookrightarrow S_{n_1}$  and  $G_2 \hookrightarrow S_{n_2}$  are effectively equivalent permutation representations.

By Theorem 1.3 two permutation groups are effectively equivalent if they are isomorphic as abstract groups such that via this isomorphism the permutation representations contain the same non-trivial irreducible factors. In particular, the associated permutation polytopes are affinely equivalent.

The vector space  $\text{Mat}_n(\mathbb{R})$  in which permutation polytopes live comes with a natural lattice  $\text{Mat}_n(\mathbb{Z})$  of integral matrices. For polytopes with vertices in a lattice – such as permutation polytopes – we can ask whether an affine equivalence preserves the lattice. In that case we call the polytopes lattice equivalent. Lattice equivalence of permutation polytopes is a subtle issue – cf. [2, Example 2.9].

**1.5. Dimension formula.** Let us recall that the degree of a representation is the dimension of the vector space the group is acting on. Guralnick and Perkinson [9] determined the dimension of the polytope associated to a representation of a group.

**Theorem 1.5** (Guralnick and Perkinson [9, Thm. 3.2]). *Let  $G \leq S_n$  be a permutation group and  $\rho$  a representation of  $G$ . Then*

$$\dim P(\rho) = \sum_{1_G \neq \sigma \in \text{Irr}(\rho)} (\deg \sigma)^2.$$

**1.6. Indecomposable elements.** Every vertex of  $P(G)$  corresponds bijectively to a group element of  $G$ . For the edges of  $P(G)$  there is an explicit description. It was used by Guralnick and Perkinson [9] to determine the diameter of a permutation polytope.

**Definition 1.6.** Let  $e \neq g \in G$ .

- We denote by  $F_g$  the smallest face of  $P(G)$  containing the identity  $e$  and  $g$ .
- We denote by  $g = z_1 \circ \cdots \circ z_r$  the unique *disjoint cycle decomposition* of  $g$  in  $S_n$ , i.e.,  $z_1, \dots, z_r$  are cycles with pairwise disjoint support, and  $g = z_1 \cdots z_r$ .
- Let  $g = z_1 \circ \cdots \circ z_r$ . For  $h \in S_n$  we say  $h$  is a *subelement* of  $g$  (we write  $h \preceq g$ ), if there is a set  $I \subseteq [r]$  such that  $h = \prod_{i \in I} z_i$ .

- $g$  is called *indecomposable* in  $G$ , if  $e$  and  $g$  are the only subelements of  $g$  in  $G$ .

With this definition one can characterize the faces  $F_g$ .

**Theorem 1.7** (Guralnick and Perkinson [9, Thm. 3.5]). *Let  $g \in G$ . The vertices of  $F_g$  are precisely the subelements of  $g$  in  $G$ . In particular,  $e$  and  $g$  form an edge of  $P(G)$  if and only if  $g$  is indecomposable in  $G$ .*

The *degree* of a vertex of a polytope is the number of edges it is contained in. Since  $G$  acts transitively on the vertices of  $P(G)$  each vertex has the same degree.

**Corollary 1.8.** *The number of indecomposable elements (different from  $e$ ) in  $G$  equals the degree of any vertex of  $P(G)$ .*

**1.7. Products.** For the purpose of reference, let us cite the following result concerning products of permutation polytopes. Here, the support  $\text{supp}(H)$  of a permutation group  $H \leq S_n$  is the complement in  $[n]$  of the set of fixed points of  $H$ .

**Theorem 1.9** (Baumeister et al. [2, 3.5]).  *$P(G)$  is a combinatorial product of two polytopes  $P_1$  and  $P_2$  if and only if there are subgroups  $H_1$  and  $H_2$  in  $G$  such that*

- (1)  $P(H_i)$  is combinatorially equivalent to  $P_i$  for  $i = 1, 2$ .
- (2)  $\text{supp}(H_1) \cap \text{supp}(H_2) = \emptyset$
- (3)  $G = H_1 \times H_2$ .

## 2. DIMENSION AND VERTEX DEGREE

**2.1. Our setting.** In this section, we give formulas for the dimension and the vertex degree of cyclic permutation polytopes in terms of the cycle type of the generator permutation. Let  $G = \langle g \rangle$ , where  $g$  has a disjoint cycle decomposition into  $t$  cycles of lengths  $\ell_1, \dots, \ell_t$ . In this case, we set

$$d := |G| = o(g) = \text{lcm}(\ell_1, \dots, \ell_t),$$

so  $G = \{e, g, \dots, g^{d-1}\}$ .

**2.2. Dimension formula.** In our setting, we can explicitly determine the dimension of  $P(G)$ .

**Proposition 2.1.** *Let  $G = \langle g \rangle$  be a cyclic permutation group of order  $d$ , where  $g$  has  $t$  disjoint cycles of lengths  $\ell_1, \dots, \ell_t$ . We have two ways to compute the dimension of  $P(G)$ :*

- (1)  $\dim(P(G))$  equals the number of  $\ell_i^{\text{th}}$ -roots of unity,  $i \in [t]$ , which are different from 1, i.e.

$$\dim(P(G)) = \left| \{x \in \mathbb{C} : x \neq 1 \text{ and } x^{\ell_i} = 1 \text{ for some } i \in [t]\} \right|.$$

- (2)  $\dim(P(G))$  equals the number of elements in  $[d-1]$  which are divisible by  $\frac{d}{\ell_i}$  for some  $i \in [t]$ .

In particular,

$$\max(\ell_i - 1 : i \in [t]) \leq \dim(P(G)) \leq d - 1.$$

*Proof.* We consider the permutation representation of  $G$  over  $\mathbb{C}$ . As  $G$  is cyclic, it splits over  $\mathbb{C}$  in 1-dimensional representations. The eigenvalues of  $G$  are then the  $\ell_i$ -th roots of unity. In order to determine the number of non-isomorphic non-trivial irreducible representations it suffices to count the different non-trivial  $\ell_i$ -th roots of unity, which shows (1). Part (2) follows from Theorem 1.5 and by observing that the subgroup  $\{x \in \mathbb{C} : x^d = 1\}$  is generated by a primitive  $d$ 'th root of unity.  $\square$

For instance, for  $\ell_1 = 2, \ell_2 = 4, \ell_3 = 8$  we get  $\dim(P(G)) = 7$ , cf. Corollary 2.3. Note that the first criterion is more conceptual, while the second one is easier to implement. Using the inclusion-exclusion-formula we obtain a closed formula for the dimension:

**Corollary 2.2.** *Under the assumptions of the proposition we have:*

$$\dim(P(G)) = -1 + \sum_{\emptyset \neq I \subseteq [t]} (-1)^{|I|+1} \gcd(\ell_i : i \in I).$$

*Proof.* Let  $\emptyset \neq I \subseteq [t]$ . Applying the inclusion-exclusion formula to Proposition 2.1(2) we only have to observe that the set

$$\{k \in [d-1] : \text{lcm}(\frac{d}{\ell_i} : i \in I) \mid k\}$$

has cardinality  $\gcd(\ell_i : i \in I) - 1$ . Note that

$$\sum_{\emptyset \neq I \subseteq [t]} (-1)^{|I|+1} (-1) = \sum_{a=1}^t \binom{t}{a} (-1)^a = -1. \quad \square$$

Since a polytope is a simplex if and only if  $\dim(P(G)) + 1$  equals the number of vertices (here,  $|G| = d$ ) we get from Proposition 2.1 the following criterion (cf. [9]). Let us define the *unimodular  $m$ -simplex*  $\Delta_m$  as the convex hull of the standard basis vectors in  $\mathbb{R}^{m+1}$ .

**Corollary 2.3.** *Let  $G$  be cyclic with  $|G| = d$ . Then  $P(G)$  is a simplex if and only if  $G$  has a cycle of order  $d$ . In this case, there is an isomorphism  $\mathbb{Z}^{n^2} \cap \text{aff}(P(G)) \rightarrow \mathbb{Z}^d \cap \text{aff}(\Delta_{d-1})$  mapping the vertices of  $P(G)$  onto the vertices of  $\Delta_{d-1}$ . In other words,  $P(G)$  is a unimodular simplex up to lattice isomorphisms. In particular this holds, if  $|G|$  is a prime power.*

*Proof.* We observe that  $\dim(P(G)) = d - 1$  if and only if 1 is in the set given in the Proposition 2.1(2), or, equivalently, if and only if there is an  $i \in [t]$  such that  $d/\ell_i = 1$ .

For the additional statement, we may assume that the first cycle in the cycle decomposition of  $g$  is of the form  $(1 \cdots d)$ . Let  $e_1, \dots, e_d$  be the canonical basis of  $\mathbb{Z}^d$ . Then by projecting onto the first  $d$  coordinates of the first row the permutation matrix  $M(g^{i-1})$  gets mapped to  $e_i$  (for  $i \in [d]$ ). Since the inverse map given by mapping  $e_i$  to  $M(g^{i-1})$  for  $i = 1, \dots, d$  is affine and integral, this yields a lattice isomorphism  $P(G) \cap \mathbb{Z}^{n^2} \rightarrow \text{aff}(e_1, \dots, e_d) \cap \mathbb{Z}^d$ . In particular,  $P(G)$  is isomorphic to the convex hull of the  $d$  canonical basis vectors of  $\mathbb{R}^d$ , a unimodular simplex.  $\square$

In particular, since Ehrhart polynomials and volume of unimodular simplices are well-known, this gives an immediate proof of Theorem 1.2(1) and Lemma 3.1 in [5].

Notice that Corollary 2.3 also follows directly from Corollary 2.8 of [BHNP]: According to that corollary  $P(G)$  is a simplex if and only if the permutation representation of  $G$  contains every irreducible complex representation of  $G$ . Hence, if  $P(G)$  is a simplex, then all the  $d$ 'th roots of unity are eigenvalues of this representation. This implies that  $G$  has a cycle of order  $d$ .

Here is another special situation, which is a generalization of 2.3.

**Proposition 2.4.** *Let  $G = \langle g \rangle \leq S_n$  be a cyclic permutation group where the orders  $\ell_1, \dots, \ell_t$  of the disjoint cycles of  $g$  are pairwise coprime. Then  $P(G)$  is a product of unimodular simplices of dimensions  $\ell_1 - 1, \dots, \ell_t - 1$ .*

*Proof.* The Chinese remainder theorem implies that  $G$  is isomorphic to the product of cyclic permutation groups (with disjoint support) of orders  $\ell_1, \dots, \ell_t$ . From the previous corollary and Theorem 1.9 the statement follows.  $\square$

**2.3. The number of indecomposable elements.** We will give a criterion to determine whether  $z \in G = \langle g \rangle = \{e, g, \dots, g^{d-1}\}$  is decomposable or not. Let  $g = z_1 \circ \dots \circ z_t$  be the cycle decomposition into  $t$  cycles of lengths  $\ell_1, \dots, \ell_t$ . For  $I \subset [t]$  we set

$$I^c := [t] \setminus I, \text{ and } d_I := \text{lcm}(\ell_i \mid i \in I).$$

**Proposition 2.5.** *Let  $g^k$  ( $k \in \{0, \dots, d-1\}$ ) be an element in the cyclic group  $G = \langle g \rangle \leq S_n$ . Then  $g^k$  is decomposable if and only if there is a proper non-empty subset  $I$  of  $[t]$  such that*

- (1)  $\text{gcd}(d_I, d_{I^c})$  divides  $k$
- (2) neither  $d_I$  nor  $d_{I^c}$  divides  $k$

*Proof.* Suppose that  $z = g^k$  is not indecomposable. Then there exist  $0 < r, s < d$  such that  $z = g^r g^s$  where  $g^r$  and  $g^s$  have disjoint support. Therefore, for all  $i \in [t]$  we get that in the group  $\langle z_i \rangle$  the element  $z_i^k$  is decomposable in  $z_i^r$  and  $z_i^s$ . Since in  $\langle z_i \rangle$  all elements are indecomposable due to Corollary 2.3 and Theorem 1.7, we have either  $z_i^r = 1$  or  $z_i^s = 1$ . Therefore, we can find a proper non-empty subset  $I$  of  $[t]$  such that  $z_i^r = 1$  for all  $i \in I$ , and  $z_i^s = 1$  for all  $i \in I^c$ . This implies  $d_I \mid r$  and  $d_{I^c} \mid s$ . Since  $k \equiv r + s \pmod{d}$  and  $\text{lcm}(d_I, d_{I^c}) = d$ , we easily see that (1) and (2) hold.

Now, let us assume that there is a proper non-empty subset  $I$  of  $[t]$  such that (1) and (2) hold. Let  $a'$  and  $b'$  be integers such that  $\text{gcd}(d_I, d_{I^c}) = a'd_I + b'd_{I^c}$ . Due to (1) we have  $k = ad_I + bd_{I^c}$  with  $a := a'k/\text{gcd}(d_I, d_{I^c}) \in \mathbb{Z}$  and  $b := b'k/\text{gcd}(d_I, d_{I^c}) \in \mathbb{Z}$ . Let  $a = q_1(d/d_I) + r_1$  with  $q_1 \in \mathbb{Z}$  and  $r_1 \in [[d/d_I]]$  and  $b = q_2(d/d_{I^c}) + r_2$  with  $q_2 \in \mathbb{Z}$  and  $r_2 \in [[d/d_{I^c}]]$ . Then  $k = (q_1 + q_2)d + r_1d_I + r_2d_{I^c}$ . We set  $0 \leq s := r_1d_I < d$  and  $0 \leq t := r_2d_{I^c} < t$ . Hence,  $g^k = g^s g^t$ . If  $s = 0$ , then  $r_1 = 0$  and therefore  $d_{I^c}$  divides  $k$  in contradiction to (2). In the same way we obtain  $t \neq 0$ . This shows that  $g^k$  is decomposable.  $\square$

As the following result shows, it is possible to determine whether a given element  $z \in G$  is indecomposable without having to know the cycle decomposition of a generator  $g$  of the cyclic group  $G$ .

**Corollary 2.6.** *Let  $z$  be an element in the cyclic group  $G \leq S_n$  having cycle decomposition into  $r$  non-trivial cycles of lengths  $\ell_1, \dots, \ell_r$ .*

*Then  $z$  is decomposable if and only if there is a proper non-empty subset  $K$  of  $[r]$  such that  $\text{gcd}(\ell_i, \ell_j) = 1$  for all  $i \in K$  and  $j \in K^c$ .*

*Proof.* Let us observe that for a cycle  $w$  of length  $\ell$ , the multiple  $w^k$  has a cycle decomposition into disjoint cycles of the same length  $\ell/\gcd(\ell, k)$ . Therefore, for  $z = g^k$  with  $0 \leq k < d$  the second condition translates into the following statement: there is a proper non-empty subset  $I$  of  $[t]$  such that  $\ell_i/\gcd(\ell_i, k) \neq 1$  for some  $i \in I$ ,  $\ell_j/\gcd(\ell_j, k) \neq 1$  for some  $j \in I^c$ , and  $\gcd(\ell_i/\gcd(\ell_i, k), \ell_j/\gcd(\ell_j, k)) = 1$  for all  $i \in I$  and  $j \in I^c$ . Now, the proof follows by applying Proposition 2.5.  $\square$

Given the lengths of cycles in the generating element we can immediately determine the number of indecomposable elements of the group by using an obvious sieve method. By Corollary 1.8 this allows to deduce an explicit formula for the constant vertex degree of the associated permutation polytope. We leave the proof to the reader.

**Corollary 2.7.** *Let us set up the following notation:*

- For  $s = (2^t - 2)/2$ , let  $I_1, \dots, I_s$  denote the pairwise different partitions of  $[t]$ , i.e.,  $\emptyset \neq I_m \subsetneq [t]$  and  $I_m \uplus I_m^c = [t]$  for  $m \in [s]$ ;
- for  $M \subseteq [s]$ , let  $y_M$  be the least common multiple of  $\gcd(d_{I_m}, d_{I_m^c})$  for all  $m \in M$ ;
- for  $T \subseteq N \subseteq [s]$ , let  $z_{N,T}$  be the least common multiple of  $d_{I_n^c}$  (for all  $n \in N \setminus T$ ) and of  $d_{I_n}$  (for all  $n \in T$ ).

Then the degree of a vertex in a permutation polytope associated to the cyclic group  $G = \langle g \rangle$  is given by

$$\sum_{M \subseteq [s]} \sum_{N \subseteq M} \sum_{T \subseteq N} (-1)^{|M|+|N|} \left( \frac{d}{\text{lcm}(y_M, z_{N,T})} - 1 \right).$$

As another application of Proposition 2.5 we can characterize permutation polytopes with complete vertex-edge graph.

**Corollary 2.8.** *The vertex-edge graph of  $P(G)$  is complete if and only if for all  $I \subseteq [t]$ :  $d_I = d$  or  $d_{I^c} = d$ .*

*Proof.* The vertex-edge graph is not complete if and only if there is a decomposable element in  $G$ .

If  $g^k$  is decomposable, then the subset  $I \subseteq [t]$  from Proposition 2.5 has obviously the property  $d_I < d$  and  $d_{I^c} < d$ . On the other hand, if there is some  $I \subseteq [t]$  with  $d_I < d$  and  $d_{I^c} < d$ , then  $d_I$  and  $d_{I^c}$  do not divide  $d_I + d_{I^c}$ , since  $\text{lcm}(d_I, d_{I^c}) = d$ . Hence  $g^{d_I+d_{I^c}}$  is decomposable due to Proposition 2.5.  $\square$

This criterion may be used to give many interesting high-dimensional examples of such polytopes, cf. Section 3. We finish the section with the following conjecture, which holds for  $l = 1$  by the previous corollary and has been experimentally checked in many cases.

**Conjecture 2.9.** *Let  $l \geq 1$ . If  $d_I = d$  for all  $I \subseteq [t]$  with  $|I| \geq \lceil \frac{t}{l+1} \rceil$ , then  $P(G)$  is  $(l+1)$ -neighborly, i.e., every subset of at most  $l+1$  vertices of  $P(G)$  forms the vertex set of a face.*

### 3. CYCLIC PERMUTATION GROUPS WITH FEW ORBITS

Cyclic permutation groups with one orbit are completely described in Corollary 2.3. In this section we study those with two or more orbits.



**3.1. Projection map and joins.** Let  $G \leq S_n$  be a permutation group with orbits  $O_1, \dots, O_t$ . Let  $g \in G$ . The permutation matrix  $M(g)$  has a blockdiagonal-structure corresponding to the  $t$  orbits:

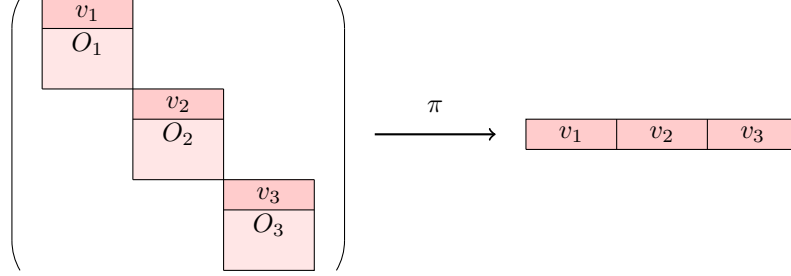


Figure 1. A permutation matrix with three orbits and the relevant first rows of each block

For any such matrix let  $v_i(M) \in \mathbb{R}^{|O_i|}$  be the first row in the  $i$ th block. Since any element in  $\text{aff}(P(G))$  has such a block-diagonal-structure, we define the linear projection map

$$\pi : \text{aff}(P(G)) \rightarrow \{x \in \mathbb{R}^n : \sum_{i=1}^n x_i = t\}$$

by projecting any matrix  $M$  onto  $(v_1(M), \dots, v_t(M))$ .

Let us assume that  $G$  acts cyclic on every orbit, i.e., for each  $i \in [t]$  the quotient group  $G/K_i$  is cyclic, where  $K_i$  is the kernel of the action of  $G$  on  $O_i$  (the set of group elements which leave each element in  $O_i$  fixed). Under this assumption,  $\pi$  is a lattice isomorphism of  $P(G)$  onto its image in  $\mathbb{R}^n$ .

In some cases one can say more. For this let us give the following definition.

**Definition 3.1.** Let us assume that the polytope  $P$  lies in an affine hyperplane of  $\mathbb{R}^n$ . Then  $P$  is a *join* of polytopes  $P_1, \dots, P_s$ , if  $P$  is the convex hull of  $P_1, \dots, P_s$ , and  $\text{lin}(P) = \oplus_{i=1}^s \text{lin}(P_i)$ . We say,  $P$  a  $\mathbb{Z}$ -*join*, if  $\text{lin}(P) \cap \mathbb{Z}^n = \oplus_{i=1}^s \text{lin}(P_i) \cap \mathbb{Z}^n$ .

A typical example is a tetrahedron: it is the join of two disjoint edges.

**Lemma 3.2.** Let  $G \leq S_n$  be a permutation group with orbits  $O_1, \dots, O_t$ . For each  $i \in [t]$  let  $G_i$  be the stabilizer of an element  $k_i \in O_i$ .

If  $G$  acts cyclic on every orbit, then the permutation polytope  $P(G)$  is the  $[G : H]$ -fold  $\mathbb{Z}$ -join of permutation polytopes  $P(H)$ , for  $H := G_1 \cdots G_t \leq G$ .

*Proof.* Let  $K_i$  be the kernel of the action of  $G$  on  $O_i$ ,  $i \in [t]$ . Then, as  $G/K_i$  is cyclic,  $[G, G] \leq K_i$  for  $i \in [t]$ . Thus  $[G, G] \leq \bigcap_{i=1}^t K_i = \{e\}$ . So  $G$  is abelian. This implies that  $K_i = G_i$  for  $i \in [t]$  and that  $H := G_1 \cdots G_t$  is a subgroup of  $G$ .

Now let  $s := [G : H]$ , and let  $Hg_1, \dots, Hg_s$  be the right cosets of  $G/H$ . For  $j \in [s]$  we define  $P_j := \pi(P(Hg_j)) \cong P(Hg_j) \cong P(H)$ , where these are lattice isomorphisms. It remains to show that  $\pi(P(G))$  is the  $\mathbb{Z}$ -join of  $P_1, \dots, P_s$ . It is clear that  $\pi(P(G))$  is the convex hull of  $P_1, \dots, P_s$ .

Let  $i, j \in [t]$ . We set  $k_i^{Hg_j} := \{k_i^{hg_j} : h \in H\}$ . Then it is straightforward to prove that the orbit  $O_i$  is partitioned into the sets  $k_i^{Hg_1}, \dots, k_i^{Hg_s}$ . This implies

that for  $j_1, j_2 \in [s]$  with  $j_1 \neq j_2$ , the vertices of  $P_{j_1}$  and  $P_{j_2}$  have disjoint support. Therefore,  $\text{lin}(\pi(P(G))) \cap \mathbb{Z}^n = \bigoplus_{i=1}^s \text{lin}(P_i) \cap \mathbb{Z}^n$ .  $\square$

Let us apply this lemma to the cyclic case. Let  $g \in S_n$  have cycle decomposition into cycles of lengths  $\ell_1, \dots, \ell_t$ . Then  $G_i$  is generated by  $g^{\ell_i}$  for  $i \in [t]$ . Let  $q := \text{gcd}(\ell_1, \dots, \ell_t)$ . Hence,  $H$  is generated by  $g^q$ . Therefore,  $[G : H] = q$ . Moreover, since  $g^q$  has a cycle decomposition into cycles of the lengths  $\ell_1/q, \dots, \ell_t/q$  (with possible repetitions), we see that  $H$  is effectively equivalent to a permutation group  $H'$  generated by a product of  $t$  disjoint cycles of lengths  $\ell_1/q, \dots, \ell_t/q$ . By Theorem 1.3 we have  $P(H) \cong P(H')$ , and this projection map is even a lattice isomorphism. Lemma 3.2 implies that it suffices to consider the case  $\text{gcd}(\ell_1, \dots, \ell_t) = 1$  in order to understand the complete face structure of  $P(G)$ . Together with Proposition 2.4 we obtain the following result.

**Proposition 3.3.** *Let  $G = \langle g \rangle \leq S_n$  where  $g$  has a cycle decomposition into two cycles of lengths  $\ell_1, \ell_2$ . We set  $q := \text{gcd}(\ell_1, \ell_2)$ . Then  $P(G)$  is the  $q$ -fold  $\mathbb{Z}$ -join of*

$$\Delta_{\frac{\ell_1}{q}-1} \times \Delta_{\frac{\ell_2}{q}-1},$$

where  $\Delta_l$  is the  $l$ -dimensional unimodular simplex.

The dimension of this polytope is  $\ell_1 + \ell_2 - \text{gcd}(\ell_1, \ell_2) - 1$  in accordance with the dimension formula given in Corollary 2.2. It has  $\text{lcm}(\ell_1, \ell_2)$  vertices and  $\ell_1 + \ell_2$  facets.

Ehrhart polynomials count lattice points in multiples of a lattice polytope [18, 6]. In [5] Ehrhart polynomials of certain permutation polytopes are computed, including the case of a cyclic permutation group with one orbit. In Corollary 3.5 below, we will provide an explicit formula for the generating function of the Ehrhart polynomial of a permutation polytope associated to a cyclic permutation group with two orbits. For this purpose, we need a folklore result for which we couldn't find a suitable reference.

**Lemma 3.4.** *Let  $\Delta_a, \Delta_b$  be two unimodular simplices in lattices  $N_1, N_2$  respectively. Then*

$$\sum_{k=0}^{\infty} |(k(\Delta_a \times \Delta_b)) \cap (N_1 \oplus N_2)| t^k = \frac{\sum_{i=0}^{\min(a,b)} \binom{a}{i} \binom{b}{i} t^i}{(1-t)^{a+b+1}}.$$

*Proof.* By definition, we have

$$|(k(\Delta_a \times \Delta_b)) \cap (N_1 \oplus N_2)| = \binom{k+a}{a} \binom{k+b}{b}.$$

Since  $t^i/(1-t)^{a+b+1} = \sum_{k=0}^{\infty} \binom{k+a+b-i}{a+b} t^k$  (e.g., [18]), it remains to show that

$$\binom{k+a}{a} \binom{k+b}{b} = \sum_{i=0}^{\min(a,b)} \binom{a}{i} \binom{b}{i} \binom{k+a+b-i}{a+b}.$$

This is a well-known binomial identity. For instance, it can be deduced from (5.28) in [8].  $\square$

It is also possible to prove the previous result by computing the  $h$ -vector from a shelling of the staircase triangulation of the product of two simplices, cf. [1].

**Corollary 3.5.** *Let  $G = \langle g \rangle \leq S_n$  where  $g$  has a cycle decomposition into two cycles of lengths  $\ell_1, \ell_2$ . We set  $q := \gcd(\ell_1, \ell_2)$ . Then*

$$\sum_{k=0}^{\infty} |(kP(G)) \cap \mathbb{Z}^{n^2}| t^k = \frac{\left( \sum_{i=0}^{\min(\frac{\ell_1}{q}-1, \frac{\ell_2}{q}-1)} \binom{\frac{\ell_1}{q}-1}{i} \binom{\frac{\ell_2}{q}-1}{i} t^i \right)^q}{(1-t)^{\ell_1+\ell_2-\gcd(\ell_1, \ell_2)}}.$$

*Proof.* By Lemma 1.3 in [10] the enumerator polynomials of the Ehrhart generating series of  $\mathbb{Z}$ -joins are multiplicative. Hence, the result follows from Lemma 3.4 and Proposition 3.3.  $\square$

**3.2. Permutation polytopes of cyclic groups with three orbits.** Let  $G = \langle g \rangle \leq S_n$  be a cyclic permutation group of order  $d$ . In Corollary 2.3 and Proposition 3.3 we completely described the combinatorial type of  $P(G)$  when  $G$  has at most two orbits. In the case of three orbits, we cannot present a corresponding result. Here the situation is much more complicated. In the following we will focus on one crucial case. For three pairwise coprime numbers  $a, b, c \in \mathbb{N}_{\geq 2}$  let  $z_{ab}, z_{ac}$  and  $z_{bc}$  be three disjoint cycles of lengths  $ab, ac$ , and  $bc$ , respectively. We define

$$P(a, b, c) := P(\langle z_{ab}z_{ac}z_{bc} \rangle).$$

By Corollary 2.2,  $P(a, b, c)$  has dimension  $ab + ac + bc - a - b - c$ . The number of vertices is  $abc$ . By Corollary 2.8 all of these polytopes have a complete vertex-edge graph. In Table 1 we present the number of facets which we were able to compute using `polymake` [12]. Note that one very quickly reaches the limits of computational power.

$(a, b, c)$	(2, 3, 5)	(2, 3, 7)	(2, 5, 7)	(2, 5, 9)	(3, 4, 5)
# dimension	21	29	45	57	35
# vertices	30	42	70	90	60
# facets	211	797	3839	15373	29387

Table 1. Dimension, vertices and facets of  $P(a, b, c)$

The following result shows that the number of facets grows indeed exponentially.

**Theorem 3.6.** *Let  $a, b, c \geq 2$  be pairwise coprime integers.*

*Then  $P(a, b, c)$  has at least  $\frac{1}{2}(2^a - 2)(2^b - 2)(2^c - 2) + ab + ac + bc$  facets.*

For  $a = 2$  this result seems to be optimal, see Table 1. This motivates the following conjecture. Note that the bound in the theorem is not sharp for  $a = 3$ .

**Conjecture 3.7.** *Let  $b, c \geq 3$  be odd and coprime. Then the number of facets of  $P(2, b, c)$  equals  $(2^b - 2)(2^c - 2) + 2b + 2c + bc$ .*

The proof of Theorem 3.6 will be given in the remainder of this paper. We are going to describe explicitly a set of facets for  $P(a, b, c)$ .

k divisible by			coefficient of $g^k$ times $abc$	no. vertices of this type
$a$	$b$	$c$		
yes	no	no	$a$	$(b-1)(c-1)$
no	yes	no	$b$	$(a-1)(c-1)$
no	no	yes	$c$	$(a-1)(b-1)$
yes	yes	no	$a+b-ab$	$c-1$
yes	no	yes	$a+c-ac$	$b-1$
no	yes	yes	$b+c-bc$	$a-1$
yes	yes	yes	$abc-ab-ac-bc+a+b+c$	1

Table 2. Coefficients of the vertex barycenter

3.2.1. *Setting and outline of the proof of Theorem 3.6.* From now on let  $a, b, c$  be pairwise coprime positive integers. Let  $n = ab + ac + bc$ , and  $G \leq S_n$  be generated by the product  $g$  of three disjoint cycles of lengths  $ab$ ,  $ac$  and  $bc$ . In the following we will always identify  $P(a, b, c)$  with  $\pi(P(a, b, c))$ , as described in 3.1. In particular, any element of  $G$  will be considered as a vector in  $\mathbb{R}^{ab+ac+bc}$  having coordinates  $x_0, \dots, x_{ab-1}$ ,  $y_0, \dots, y_{ac-1}$ , and  $z_0, \dots, z_{bc-1}$ . For  $u \in \mathbb{R}^{ab+ac+bc}$ , we let  $\pi_x(u)$ ,  $\pi_y(u)$ , and  $\pi_z(u)$  be the projections onto the  $x$ -,  $y$ -, and  $z$ -coordinates, respectively.

**Proposition 3.8.** *The inequalities*

$$x_i \geq 0 \qquad y_j \geq 0 \qquad z_k \geq 0$$

define facets of  $P(a, b, c)$ .

*Proof.* It suffices to prove that these faces are facets. For this, we will show that for any vertex  $g^m$  outside of such a face  $F$  we can write

$$\hat{G} := \frac{1}{abc} \sum_{g \in G} g$$

as an affine combination of vertices of the face together with the given vertex.

Up to symmetry, we may assume that the face  $F$  of concern is given by  $x_1 \geq 0$ . In particular, it contains all vertices  $g^k$  such that  $k$  is divisible by  $a$  or  $b$ . The vertices outside of  $F$  are of the form  $g^m$  for  $m \equiv 1 \pmod{ab}$ . Again, up to symmetry, we can choose  $m$  such that  $m \equiv 0 \pmod{c}$ . Now, Table 2 gives the coefficients of  $\hat{G}$  as an affine combination of all vertices  $g^k$  such that  $k$  is divisible by  $a$ ,  $b$  or  $c$ .

Here is how the reader can check its validity: For instance, the projection on the  $x$ -coordinates of  $abc \hat{G}$  equals  $(c \cdots c) \in \mathbb{R}^{ab}$ . Let's consider the  $x$ -coordinate corresponding to  $0 \pmod{a}$  and  $1 \pmod{b}$ . There are  $c$  vertices  $g^k$  in this equivalence class,  $c-1$  not divisible by  $c$  and one divisible by  $c$ . By the first and fifth rows of Table 2, this coordinate of the affine combination equals

$$(c-1)a + (a+c-ac) = c.$$

In the same manner, the statement can be verified for any coordinate.  $\square$

We say that a facet is *essential*, if it is not of the type  $x_i \geq 0$ ,  $y_j \geq 0$ , or  $z_k \geq 0$ . There are  $n = ab + ac + bc$  non-essential facets. We want to define a large family of essential facets of  $P(a, b, c)$ . The next subsection defines a certain class of subsets of  $[[abc]]$  via projections onto the  $x$ -,  $y$ -, and  $z$ -coordinates. In Lemma 3.9 we give a general criterion when such a set defines a face of  $P(a, b, c)$ . The final subsection

gives an explicit construction of sets that satisfy the conditions of the lemma. We prove that our vertex sets define facets and count their number.

**3.2.2. Faces as unions of preimages of projection maps.** Throughout, we will identify  $[[abc]]$  and  $G$  via the natural bijection  $i \mapsto g^i$ . The Chinese remainder theorem yields a bijection between  $[[abc]]$  and  $[[a]] \times [[b]] \times [[c]]$  by mapping  $k$  to  $(k \pmod{a}, k \pmod{b}, k \pmod{c})$ . In the same way, we identify  $[[ab]]$  and  $[[a]] \times [[b]]$ ,  $[[ac]]$  and  $[[a]] \times [[c]]$ , and  $[[bc]]$  and  $[[b]] \times [[c]]$ .

To any proper subset  $S_x \subsetneq [[ab]]$  we associate a subset of  $[[abc]]$  via

$$F_x(S_x) := \pi_x^{-1}(\{e_i : i \in S_x\}) = \bigcup_{x \in S_x} x \times [[c]] \subsetneq [[abc]],$$

where  $e_0, \dots, e_{ab-1}$  is the standard basis of  $\mathbb{R}^{ab}$ . This is (the vertex set of) a face of  $P(a, b, c)$ , given by setting  $x_i = 0$  for  $i \notin S_x$ . Similarly, we define  $F_y(S_y)$  and  $F_z(S_z)$  for subsets  $S_y \subsetneq [[ac]]$  and  $S_z \subsetneq [[bc]]$ .

In the following we want to consider unions of the form  $F_x(S_x) \cup F_y(S_y) \cup F_z(S_z)$  for  $S_x \subsetneq [[ab]]$ ,  $S_y \subsetneq [[ac]]$ ,  $S_z \subsetneq [[bc]]$ . In general, this is not the vertex set of a face. However, the following lemma gives a sufficient criterion.

**Lemma 3.9.** *Let  $S_x \subsetneq [[ab]]$ ,  $S_y \subsetneq [[ac]]$  and  $S_z \subsetneq [[bc]]$ . If*

$$(1) \quad F_x(S_x) \cap F_y(S_y) \cap F_z(S_z) = \emptyset,$$

*and if for all permutations  $(i, j, k)$  of  $(x, y, z)$*

$$(2) \quad F_i(S_i) \cap \pi_k^{-1}(\pi_k(F_i(S_i) \cap F_j(S_j))) \subseteq F_j(S_j),$$

*then  $F_x(S_x) \cup F_y(S_y) \cup F_z(S_z)$  is the vertex set of a (not necessarily proper) face of  $P(a, b, c)$ .*

*Proof.* The first assumption implies that

$$\begin{aligned} S_x \cap \pi_x(F_y(S_y) \cap F_z(S_z)) &= \emptyset, \\ S_y \cap \pi_y(F_x(S_x) \cap F_z(S_z)) &= \emptyset, \\ \text{and } S_z \cap \pi_z(F_x(S_x) \cap F_y(S_y)) &= \emptyset. \end{aligned}$$

We define a functional  $\lambda = (\lambda^{(x)}, \lambda^{(y)}, \lambda^{(z)}) \in \mathbb{R}^n$  in the following way. Let  $I_x := [[ab]]$ ,  $I_y := [[ac]]$  and  $I_z := [[bc]]$ . For all permutations  $(i, j, k)$  of  $(x, y, z)$  we define

$$\lambda_m^{(i)} := \begin{cases} -1 & m \in S_i \\ 1 & m \in \pi_i(F_j(S_j) \cap F_k(S_k)) \\ 0 & \text{else.} \end{cases}$$

Let  $\langle \cdot, \cdot \rangle$  by the standard scalar product on  $\mathbb{R}^n$  and  $v \in G$ . Using assumptions (1) and (2) it is straightforward to check that  $\langle \lambda, v \rangle \geq -1$ , with equality if and only if  $v \in F_x(S_x) \cup F_y(S_y) \cup F_z(S_z)$ .  $\square$

**3.2.3. Explicit constructions of facets.**

**Proposition 3.10.** *Given three non-trivial subsets  $\emptyset \neq I \subsetneq [[a]]$ ,  $\emptyset \neq J \subsetneq [[b]]$ , and  $\emptyset \neq K \subsetneq [[c]]$ , the set*

$$([[a]] \times [[b]] \times [[c]]) \setminus (I \times J \times K) \setminus (I^c \times J^c \times K^c)$$

*is the set of vertices of a facet of  $P(a, b, c)$ .*

*Proof.* We set

$$\begin{aligned} S_x &:= I \times J^c \cup I^c \times J \subset [[a]] \times [[b]] \cong [[ab]], \\ S_y &:= I \times K^c \cup I^c \times K \subset [[a]] \times [[c]] \cong [[ac]], \\ S_z &:= J \times K^c \cup J^c \times K \subset [[b]] \times [[c]] \cong [[bc]]. \end{aligned}$$

Then  $S_x, S_y, S_z$  satisfy the conditions of Lemma 3.9. The resulting face  $F_x(S_x) \cup F_y(S_y) \cup F_z(S_z)$  has the vertex set  $V$  as given in the statement. We claim that this face is, in fact, a facet. To prove this claim, let  $v_0 \notin V$  be an additional vertex of  $P(a, b, c)$ . We show that any other vertex  $v_1$  of  $P(a, b, c)$  can be written as an affine combination of elements of  $V$  together with  $v_0$ .

As before, we identify the elements of  $G$  with triples  $(i, j, k) \in [[a]] \times [[b]] \times [[c]]$ . We can assume that  $v_0 = (i_0, j_0, k_0) \in I \times J \times K$ . Then either  $v_1 = (i_1, j_1, k_1) \in I \times J \times K$  as well, or  $v_1 \in I^c \times J^c \times K^c$ .

In the latter case, we see that we have  $v_1 = v_0 - (i_0, j_0, k_1) - (i_0, j_1, k_0) - (i_1, j_0, k_0) + (i_1, j_1, k_0) + (i_1, j_0, k_1) + (i_0, j_1, k_1)$ , where the last six vertices all belong to  $V$ . When verifying this statement, the reader should beware that this is actually a sum of elements in  $\mathbb{R}^{ab+ac+bc}$ .

In the former case, we choose  $v_2 \in I^c \times J^c \times K^c$ , and construct combinations  $v_0 = v_2 + w_0, v_1 = v_2 + w_1$ , where  $w_0$  and  $w_1$  are combinations of elements of  $V$  with vanishing coefficient sum. But then  $v_1 = v_0 - w_0 + w_1$  yields the desired affine representation.  $\square$

Finally, let us count the number of different facets we obtain in this way. We have  $(2^a - 2)(2^b - 2)(2^c - 2)$  different choices for  $I, J, K$ . Simultaneously exchanging all three sets by their complements yields the same facet, so the facet depends only on the pairs  $(I, I^c), (J, J^c)$  and  $(K, K^c)$ . On the other hand, the set  $S := (I \times J \times K) \cup (I^c \times J^c \times K^c)$  already determines these pairs: If  $(i, j, k) \in S$ , then either  $I = \{i' \in [[a]] \mid (i', j, k) \in S\}$  or  $I^c = \{i' \in [[a]] \mid (i', j, k) \in S\}$ , and similarly for  $(J, J^c)$  and  $(K, K^c)$ . Hence, we get  $(2^a - 2)(2^b - 2)(2^c - 2)/2$  different facets of this type, and all of these facets are essential by construction. This finishes the proof of Theorem 3.6.

**Remark 3.11.** It is possible to trace the inequalities described in Lemma 3.9 back to the ‘cycle inequalities’ in [17]: face inequalities of so-called *marginal polytopes*. In particular, the ‘checkerboard inequalities’ in Proposition 3.10 may be found in that paper. However, it is not shown in [17] that they actually define facets. The precise relation of permutation polytopes to marginal polytopes [13, 17] will be investigated in an upcoming paper [3].

## REFERENCES

- [1] Federico Ardila, Matthias Beck, Serkan Hosten, Julian Pfeifle, and Kim Seashore, *Root polytopes and growth series of root lattices*, (2008), arXiv:0809.5123.
- [2] Barbara Baumeister, Christian Haase, Benjamin Nill, and Andreas Paffenholz, *On permutation polytopes.*, Adv. Math. **222** (2009), no. 2, 431–452.
- [3] ———, *Face inequalities of marginal polytopes*, 2011, in preparation.
- [4] Louis J. Billera and A. Sarangarajan, *The combinatorics of permutation polytopes.*, Billera, Louis J. (ed.) et al., Formal power series and algebraic combinatorics. DIMACS, Ser. Discrete Math. Theor. Comput. Sci. 24, 1-23 (1996)., 1996.

- [5] Katherine Burggraf, Jesus A. De Loera, and Mohammed Omar, *On Volumes of Permutation Polytopes*, February 2011, arXiv:1103.0039.
- [6] Eugène Ehrhart, *Sur les polyèdres rationnels homothétiques à  $n$  dimensions*, C. R. Acad. Sci., Paris **254** (1962), 616–618.
- [7] The GAP Group, *GAP – Groups, Algorithms, and Programming, Version 4.4.12*, 2008, (<http://www.gap-system.org>).
- [8] Ronald L. Graham, Donald E. Knuth, and Oren Patashnik, *Concrete mathematics*, second ed., Addison-Wesley Publishing Company, Reading, MA, 1994.
- [9] Robert M. Guralnick and David Perkinson, *Permutation polytopes and indecomposable elements in permutation groups.*, J. Comb. Theory, Ser. A **113** (2006), no. 7, 1243–1256.
- [10] Martin Henk and Makoto Tagami, *Lower bounds on the coefficients of Ehrhart polynomials*, European J. Combin. **30** (2009), no. 1, 70–83.
- [11] Jeffrey Hood and David Perkinson, *Some facets of the polytope of even permutation matrices.*, Linear Algebra Appl. **381** (2004), 237–244.
- [12] Michael Joswig and Evgenij Gawrilow, *polymake: A framework for analyzing convex polytopes*, October 1999.
- [13] Thomas Kahle, Walter Wenzel, and Nihat Ay, *Hierarchical models, marginal polytopes, and linear codes*, Kybernetika (Prague) **45** (2009), no. 2, 189–207.
- [14] Volker Kaibel and Arnold Waßmer, *Automorphism groups of cyclic polytopes*, To appear as Chapter 8 of: Frank H. Lutz, *Triangulated Manifolds with Few Vertices, Algorithms and Combinatorics*, Springer, 2011.
- [15] Thomas Rehn, *Polyhedral description conversion up to symmetries*, Diploma thesis, Otto von Guericke University Magdeburg, 2010.
- [16] Raman Sanyal, Frank Sottile, and Bernd Sturmfels, *Orbitopes*, (2009), arXiv:0911.5436.
- [17] David Sontag and Tommi Jaakkola, *New outer bounds on the marginal polytope*, Advances in Neural Information Processing Systems 20 (Cambridge, MA) (J.C. Platt, D. Koller, Y. Singer, and S. Roweis, eds.), MIT Press, 2008, pp. 1393–1400.
- [18] Richard P. Stanley, *Enumerative combinatorics. Vol. I*, The Wadsworth & Brooks/Cole Mathematics Series, Wadsworth & Brooks/Cole Advanced Books & Software, Monterey, CA, 1986, With a foreword by Gian-Carlo Rota.
- [19] Günter M. Ziegler, *Lectures on polytopes*, Graduate Texts in Mathematics, vol. 152, Springer-Verlag, New York, 1995.

BARBARA BAUMEISTER, UNIVERSITÄT BIELEFELD, GERMANY  
*E-mail address:* [b.baumeister@math.uni-bielefeld.de](mailto:b.baumeister@math.uni-bielefeld.de)

CHRISTIAN HAASE, GOETHE-UNIVERSITÄT FRANKFURT, GERMANY  
*E-mail address:* [haase@mathematik.uni-frankfurt.de](mailto:haase@mathematik.uni-frankfurt.de)

BENJAMIN NILL, CASE WESTERN RESERVE UNIVERSITY, CLEVELAND, OH, USA  
*E-mail address:* [benjamin.nill@case.edu](mailto:benjamin.nill@case.edu)

ANDREAS PAFFENHOLZ, TECHNISCHE UNIVERSITÄT DARMSTADT, GERMANY  
*E-mail address:* [paffenholz@mathematik.tu-darmstadt.de](mailto:paffenholz@mathematik.tu-darmstadt.de)