View metadata, citation and similar papers at core.ac.uk
brought to you by CORE
provided by Elsevier - Publisher Connector

Available online at www.sciencedirect.com
ScienceDirect
ELSEVIER
Journal of Combinatorial Theory, Series A 114 (2007) 619–630
Journal of Combinatorial Theory Series A
www.elsevier.com/locate/jcta

# Combinatorial families enumerated by quasi-polynomials ☆

Petr Lisoněk

*Department of Mathematics, Simon Fraser University, Burnaby, BC, Canada V5A 1S6*

Received 12 November 2005
Available online 15 September 2006

**Abstract**

We say that the sequence $(a_n)$ is *quasi-polynomial* in $n$ if there exist polynomials $P_0, \dots, P_{s-1}$ and an integer $n_0$ such that, for all $n \geqslant n_0$, $a_n = P_i(n)$ where $i \equiv n \pmod{s}$. We present several families of combinatorial objects with the following properties: Each family of objects depends on two or more parameters, and the number of isomorphism types of objects is quasi-polynomial in one of the parameters whenever the values of the remaining parameters are fixed to arbitrary constants. For each family we are able to translate the problem of counting isomorphism types of objects into the problem of counting integer points in a union of parametrized rational polytopes. The families of objects to which this approach is applicable include combinatorial designs, linear and unrestricted codes, and dissections of regular polygons.
© 2006 Elsevier Inc. All rights reserved.

*Keywords:* Quasi-polynomial; Group action; Rational polytope; Isomorphism; Block design; Polygon dissection; Linear code; Unrestricted code

## 1. Introduction

The goal of this paper is to provide a unifying theoretical framework for a class of combinatorial enumeration problems. We consider families of combinatorial objects which depend on two or more parameters, and we study the number of isomorphism types of objects as a function of one of the parameters (when the values of the remaining parameters are fixed to arbitrary integer constants).

A theorem due to Ehrhart asserts that the number of integer points in the $n$th dilate of a fixed rational polytope is quasi-polynomial in $n$. A precise statement including all necessary

☆ Research partially supported by the Natural Sciences and Engineering Research Council of Canada (NSERC).
*E-mail address:* lisonek@math.sfu.ca.

0097-3165/$ – see front matter © 2006 Elsevier Inc. All rights reserved.
doi:10.1016/j.jcta.2006.06.013

definitions is given at the beginning of Section 2. We show that Ehrhart's theorem remains valid when we relax it to a semi-dilation case. We state this result (which is a special case of a more general theorem due to Beck [1]) in a form that suits the needs of this paper. The main objective of Section 2 is to prove that also the number of *orbits* of integer points in the $n$th semi-dilate of a convex rational polytope is quasi-polynomial in $n$, assuming a suitable group action on the integer lattice.

In the remaining sections we apply the main theorem of Section 2 to proving quasi-polynomiality of various counting sequences. We present applications to combinatorial designs and dissections of regular polygons, as well as linear and unrestricted codes. These applications are not exhaustive. They have been chosen to demonstrate that the theory is applicable to diverse areas of combinatorics.

The article provides a common background for some previously known but isolated results. We focus on qualitative results, and we defer explicit calculations to a later publication that will require extending the proof methods presented here. As a consequence, in this paper we keep numerical examples very small or we point to references.

Since all counting sequences that we study have polynomial growth, the corresponding task of exhaustive generation of representatives of isomorphism classes may be feasible, and explicit calculation of the counting sequences would then determine the sizes of lists produced in the isomorph-free generation.

## 2. Counting integer points in polytopes

Throughout the article let $\mathbb{N}$ denote the set of all non-negative integers.

**Definition 2.1.** We say that the sequence $(a_n)_{n\in\mathbb{N}}$ is *quasi-polynomial* in $n$ if there exist $n_0 \in \mathbb{N}$ and polynomials $P_0, \ldots, P_{s-1}$ such that, for all $n \geqslant n_0$, $a_n = P_i(n)$ where $i \equiv n \pmod{s}$.

**Remarks.** 1. Our definition of quasi-polynomial is broader than the standard definition [15, Section 4.4] since we require that the values $a_n$ are determined by polynomials $P_i$ only for $n \geqslant n_0$. This relaxation makes the class of quasi-polynomial sequences closed under the shift operator. Examples 3.2 and 4.2 below show that our broader definition of quasi-polynomial is needed if one wants to work with some naturally defined enumeration sequences introduced elsewhere in the literature, because in these two examples the degree of the numerator of the ordinary generating function (o.g.f.) is greater than or equal to the degree of the denominator.

2. Proposition 4.4.1 in [15] implies that $(a_n)$ is quasi-polynomial (in our sense) if and only if its o.g.f. $f(z) = \sum_{n\geqslant 0} a_n z^n$ can be written in the form

$$f(z) = \frac{Q(z)}{\prod_{i=1}^{k}(1 - z^{m_i})}$$

for some polynomial $Q \in \mathbb{Q}[z]$ and some positive integers $m_1, \ldots, m_k$.

For a ring $R$ we will denote by $R^{s\times t}$ the set of all $s \times t$ matrices over $R$.

A *rational convex polyhedron* is the set of those points $u \in \mathbb{R}^d$ that satisfy $Au \geqslant b$ for some $A \in \mathbb{Z}^{k\times d}$ and $b \in \mathbb{Z}^k$. If a rational convex polyhedron is bounded, then we call it a *rational convex polytope.*

If $P$ is a rational convex polytope or a union of rational convex polytopes, then by $i(P)$ we denote the number of integer points in $P$, i.e., $i(P) := |P \cap \mathbb{Z}^d|$.

If $P$ is the rational convex polytope determined by $Au \geqslant b$, then for $n \in \mathbb{N}$ the $n$th *dilate of* $P$, denoted by $nP$, is defined as the polytope determined by $Au \geqslant nb$.

The following theorem is due to Ehrhart:

**Theorem 2.2.** [3] *For each rational convex polytope $P$ the sequence $(i(nP))$ is quasi-polynomial in $n$.*

Ehrhart's theorem was proved also for non-convex rational polytopes. However, for the purpose of this article the statement of Theorem 2.2 (the convex case) is sufficient. Another reference where a complete proof for the convex case can be found is Theorem 4.6.25 in [15]. One reason for emphasizing the convex case is that the software packages for computing the Ehrhart quasi-polynomial, such as LattE [2], require the polytopes to be convex.

We will now generalize the concept of polytope dilation to polytope semi-dilation, which is specifically tailored to the theory and applications pursued in this article. Then we will prove a generalization of Theorem 2.2 for the case when we assume a group action on the integer lattice, and we count the number of *orbits* of integer points in the sequence of polytope semi-dilates.

Throughout the article we will use $[k]$ to denote the set $\{1, \ldots, k\}$, where $k$ is a positive integer.

**Definition 2.3.** Let $P = \{u \in \mathbb{R}^d\colon\ Au \geqslant b\}$ be a rational convex polytope, where $A \in \mathbb{Z}^{k\times d}$ and $b \in \mathbb{Z}^k$. Let $D \subseteq [k]$ and let us define for each $n \in \mathbb{N}$ the polytope $P^{n,D} = \{u \in \mathbb{R}^d\colon\ Au \geqslant b^{n,D}\}$, where $b_i^{n,D} = nb_i$ if $i \in D$, and $b_i^{n,D} = 1$ if $i \notin D$. We say that $P^{n,D}$ is the $n$th *semi-dilate of $P$ with respect to $D$.*

Let $A_i$ denote the $i$th row of $A$. For $P$, $A$, $b$ and $D$ as in Definition 2.3 we will denote

$$P^D := \bigcap_{i\in D} \{u \in \mathbb{R}^d\colon\ A_i u \geqslant b_i\}.$$

The following theorem is a special case of [1, Theorem 4]. For the sake of completeness we include a self-contained proof.

**Theorem 2.4.** *Let $P = \{u \in \mathbb{R}^d\colon\ Au \geqslant b\}$ be a rational convex polytope, where $A \in \mathbb{Z}^{k\times d}$ and $b \in \mathbb{Z}^k$. Let $D \subseteq [k]$ such that $P^D$ is bounded. Then the sequence $(i(P^{n,D}))$ is quasi-polynomial in $n$.*

**Proof.** Let $\hat{P} := P^D \cap \{u \in \mathbb{R}^d\colon\ A_i u \geqslant 0 \text{ for } i \notin D\}$. For each $z \in [k] \setminus D$ let $P^z := \hat{P} \cap \{u \in \mathbb{R}^d\colon\ A_z u = 0\}$. Clearly,

$$P^{n,D} \cap \mathbb{Z}^d = \left(n\hat{P} \cap \mathbb{Z}^d\right) \Big\backslash \bigcup_{z\in[k]\setminus D} \left(nP^z \cap \mathbb{Z}^d\right). \tag{1}$$

For each $z \in [k] \setminus D$ we have $P^z \subseteq \hat{P} \subseteq P^D$. Consequently, $\hat{P}$ and $P^z$ (for each $z$) are rational convex polytopes, because $P^D$ is bounded by the assumption. Since the class of quasi-polynomial sequences is closed with respect to addition and scalar multiplication, it follows from the Principle of Inclusion–Exclusion and from Theorem 2.2 that $i(\bigcup_{z\in[k]\setminus D}(nP^z))$ is quasi-polynomial in $n$. Thus it follows from (1) that $i(P^{n,D})$ is the difference of two quasi-polynomials in $n$, which finishes the proof. □

Throughout the article we assume familiarity with the basic concepts and properties of group actions. These can be found, for example, in [7]. For a positive integer $d$, by $S_d$ we mean the symmetric group of degree $d$ (as an abstract group). If we want to emphasize that we deal with the symmetric group on some specific set $X$, we will write $S_X$. However, if there is no risk of confusion we will not formally distinguish between $S_d$ and $S_X$ where $|X| = d$.

We will assume that $S_d$ acts on sequences of cardinality $d$ by $\pi(x_1, \dots, x_d) = (x_{\pi^{-1}(1)}, \dots, x_{\pi^{-1}(d)})$. (This definition includes the action of $S_d$ on $\mathbb{R}^d$.) Further we will assume that $S_X$ acts on subsets of $X$ by $\pi S = \{\pi(s)\colon s \in S\}$.

**Theorem 2.5.** *Let $P = \{u \in \mathbb{R}^d\colon Au \geqslant b\}$ be a rational convex polytope, where $A \in \mathbb{Z}^{k\times d}$ and $b \in \mathbb{Z}^k$. Let $D \subseteq [k]$ such that $P^D$ is bounded. Let $G$ be a subgroup of $S_d$ acting on $\mathbb{R}^d$ such that for each $n \in \mathbb{N}$, $P^{n,D} \cap \mathbb{Z}^d$ is a union of $G$-orbits on $\mathbb{Z}^d$. Then the number of $G$-orbits on $P^{n,D} \cap \mathbb{Z}^d$ is quasi-polynomial in $n$.*

**Proof.** For each $G$-orbit on $P^{n,D} \cap \mathbb{Z}^d$ let the lexicographically largest vector in that orbit be designated as the unique representative of that orbit. We will prove the theorem by showing that the total number of representatives is quasi-polynomial in $n$.

The proposition that the representative $u$ is the lexicographically largest vector in its $G$-orbit is the conjunction of $|G| - 1$ propositions $u \geqslant_{\mathrm{lex}} \pi(u)$, $\pi \in G \setminus \{\mathrm{id}_G\}$. By the definition of the lexicographic ordering, each of these $|G| - 1$ propositions is a disjunction of conjunctions of atomic propositions of the form $u_i = u_j$ or $u_i > u_j$ (equivalently, $u_i - u_j \geqslant 1$) or $u_i \geqslant u_j$. Thus, by elementary logical operations we can transform the proposition "*$u$ is the lexicographically largest vector in its $G$-orbit*" into the disjunctive normal form, say $C_1 \vee \dots \vee C_t$, in which each $C_l$ is a conjunction of atomic propositions of the form $u_i - u_j = 0$ or $u_i - u_j \geqslant 1$ or $u_i - u_j \geqslant 0$.

For each $l \in [t]$ let $P_l := P \cap Q_l$ where $Q_l$ is the convex rational polytope determined by $C_l$. It now follows that the set of lexicographically largest representatives of $G$-orbits on $P^{n,D} \cap \mathbb{Z}^d$ is precisely the set of integer points in $\bigcup_{l=1}^t P_l^{n,D_l}$ where, for each $l$, the set $D_l$ is determined by $D$ and $C_l$. Since $P^D$ is bounded by assumption and $D \subseteq D_l$ for each $l$ (in the sense that all constraints being dilated in $P$ are also being dilated in $P_l$), it follows that $P_l^{D_l} \subseteq P^D$ for each $l$. Thus $P_l^{D_l}$ is a convex rational polytope for each $l$. As in the previous proof, by an Inclusion–Exclusion argument and by the closure of quasi-polynomials with respect to addition and scalar multiplication we conclude that $i(\bigcup_{l=1}^t P_l^{n,D_l})$ is quasi-polynomial in $n$, which finishes the proof. □

In the rest of the paper we will show applications of Theorem 2.5 to various types of combinatorial objects.

## 3. Combinatorial designs

In this section, by an $m$-set (or an $m$-subset) we mean a set of cardinality $m$. For a set $A$, let $\binom{A}{m}$ denote the set of all $m$-subsets of $A$.

Let $t, k, v$ be fixed positive integers such that $0 < t < k < v$. A $t$-$(v, k, \lambda)$ design $\mathcal{D} = (X, \mathcal{B})$ consists of a $v$-set $X$ and a multiset $\mathcal{B}$ of $k$-subsets of $X$ (called blocks) such that each $t$-subset of $X$ is contained in exactly $\lambda$ blocks of $\mathcal{B}$. Two designs $\mathcal{D}_1 = (X, \mathcal{B}_1)$ and $\mathcal{D}_2 = (X, \mathcal{B}_2)$ are *isomorphic* if there exists a permutation $\pi$ of $X$ such that $\mathcal{B}_2 = \{\pi(b)\colon b \in \mathcal{B}_1\}$ (as multisets), where $\pi(b) := \{\pi(x)\colon x \in b\}$ for any $b \in \binom{X}{k}$.

**Theorem 3.1.** *For fixed positive integers $t, k, v$, the number of isomorphism types of $t$-$(v, k, \lambda)$ designs is quasi-polynomial in $\lambda$.*

**Proof.** Let us assume that we have fixed an ordering on $\binom{X}{t}$ as well as an ordering on $\binom{X}{k}$. Let $A = (a_{ij})$ be the $\binom{v}{t} \times \binom{v}{k}$ matrix whose rows and columns are indexed by $t$-subsets of $X$ and $k$-subsets of $X$, respectively, such that $a_{ij} = 1$ if the $i$th $t$-subset is contained in the $j$th $k$-subset, and $a_{ij} = 0$ otherwise. For any multiset $\mathcal{B}$ of $k$-subsets of $X$, let $\chi^{\mathcal{B}} \in \mathbb{N}^{\binom{v}{k}}$ be the characteristic vector of $\mathcal{B}$, i.e., $\chi_j^{\mathcal{B}}$ is equal to the number of times the $j$th $k$-subset of $X$ occurs in $\mathcal{B}$. Then $(X, \mathcal{B})$ is a $t$-$(v, k, \lambda)$ design if and only if $A\chi^{\mathcal{B}} = \lambda\mathbf{1}$ where $\mathbf{1}$ is the all-one vector. Moreover, two designs $\mathcal{D}_1 = (X, \mathcal{B}_1)$ and $\mathcal{D}_2 = (X, \mathcal{B}_2)$ are isomorphic if and only if the characteristic vectors of $\mathcal{B}_1, \mathcal{B}_2$ satisfy $\chi^{\mathcal{B}_2} = \pi'(\chi^{\mathcal{B}_1})$ where $\pi'$ is a permutation of $\binom{X}{k}$ induced by a permutation of $X$.

Let $d = \binom{v}{k}$ and let $G \simeq S_v$ be the subgroup of $S_d$ consisting of all permutations of $\binom{X}{k}$ that are induced by permutations of $X$. It follows from the discussion above that the number of isomorphism types of $t$-$(v, k, \lambda)$ designs is equal to the number of $G$-orbits on the set of integer points in the polytope $\lambda P$, where $P = \{u \in \mathbb{R}^d\colon\ Au = \mathbf{1},\ u \geqslant \mathbf{0}\}$ and $A$ is as above. Since $P$ is bounded, the result now follows from Theorem 2.5. □

**Example 3.2.** The quasi-polynomial function $N(q)$ counting the isomorphism classes of 2-$(6, 3, 2q)$ designs ($q$ a positive integer) was computed in [11]. The period of the quasi-polynomial is 12, and the degree is 5. Table 2 on page 109 of [11] displays all $12 \cdot 6 = 72$ coefficients of $N(q)$ on the residue classes of $q$ modulo 12. This data can be converted into the o.g.f.

$$\sum_{q \geqslant 0} N(q)z^q = \frac{z + z^2 - 4z^3 + 4z^4 - 5z^5 + 7z^6 - 5z^7 + 4z^8 - 3z^9 - z^{10} + 3z^{11} - z^{12}}{(1-z)^3(1-z^2)(1-z^3)(1-z^4)}$$
$$= z + 4z^2 + 6z^3 + 13z^4 + 19z^5 + 34z^6 + 48z^7 + 76z^8 + \cdots,$$

cf. table of designs with small parameters in [12, pp. 14–35].

## 4. Dissections of regular polygons

By a *polygon dissection* we mean a subdivision of the interior of a convex $s$-gon into smaller polygons (which we call *cells*) by means of non-intersecting, but possibly touching diagonals. In this article we only deal with dissections of *regular* $s$-gons. We say that two dissections of the same regular $s$-gon are *isomorphic* if one can be obtained from the other by the action of an element of $C_s$ (the cyclic group of degree $s$) or by the action of an element of $D_s$ (the dihedral group of degree $s$), where we consider $C_s$ and $D_s$ as groups of symmetries of the regular $s$-gon that is being subdivided. We thus have two definitions of dissection isomorphism. Let $H_{r,s}$ denote the number of $C_s$-orbits of dissections into $r$ cells and let $h_{r,s}$ denote the number of $D_s$-orbits of dissections into $r$ cells. For example, $H_{3,6} = 4$ and $h_{3,6} = 3$.

**Theorem 4.1.** *For any fixed positive integer $r$, the sequences $(H_{r,s})$ and $(h_{r,s})$ are quasi-polynomial in $s$.*

**Proof.** A proof using generating functions and Pólya theory can be found in [9]. We now give a proof in the spirit of the present article.

Let $\mathbb{Z}_n$ denote the integers modulo $n$. We say that $(l_i)_{i\in\mathbb{Z}_{2(r-1)}}$ is a *circular non-crossing sequence* (*CNCS*) *of length* $2(r-1)$ if it satisfies the following two properties: (i) Each element of $[r-1]=\{1,\dots,r-1\}$ occurs exactly twice in $l$. (ii) $l$ does not contain a subsequence of the form $(a,b,a,b)$, that is, there do not exist integers $0\leqslant w<x<y<z<2(r-1)$ such that $l_w=l_y$ and $l_x=l_z$.

Consider a dissection $D$ of a regular $s$-gon into $r$ cells, and let us label each diagonal of the dissection with a number in $[r-1]$ so that each number is used for exactly one diagonal. Then let us form the sequence $l$ as follows: During one full clockwise traversal of the circumference of the $s$-gon (starting from an arbitrary vertex), record the labels of diagonals in the order in which the diagonals are encountered at their endpoints (vertices of the $s$-gon). If more than one diagonal is incident with the same vertex $v$ of the $s$-gon, then in order to record the labels of all diagonals incident with $v$, traverse the internal angle of the $s$-gon at $v$ in the counterclockwise ordering. The sequence $l$ formed this way is a CNCS of length $2(r-1)$; let us call it a *label sequence* for the dissection $D$.

For a dissection of a regular $s$-gon into $r$ cells and for one of its label sequences $l$ we define the *distance sequence* $(d_i)$ as follows: For $i\in\mathbb{Z}_{2(r-1)}$ let $d_i$ denote the length (number of edges) of the directed path which runs in the clockwise direction on the circumference of the $s$-gon from the vertex at which the label $l_i$ was recorded to the vertex at which the label $l_{i+1}$ was recorded.

Let $l,l'$ be two label sequences indexed by $\mathbb{Z}_{2(r-1)}$ and let $d,d'$ be two distance sequences indexed by $\mathbb{Z}_{2(r-1)}$. We say that the pairs $(l,d)$ and $(l',d')$ are *isomorphic* if there exists $s\in\mathbb{Z}_{2(r-1)}$ such that: (a) for each $i,j\in\mathbb{Z}_{2(r-1)}$, $l_i=l_j$ if and only if $l'_{i+s}=l'_{j+s}$, and (b) for each $i\in\mathbb{Z}_{2(r-1)}$, $d_i=d'_{i+s}$.

We also introduce an isomorphism definition which is restricted to label sequences only: We say that two label sequences $l$ and $l'$ both indexed by $\mathbb{Z}_{2(r-1)}$ are *isomorphic* if there exists $s\in\mathbb{Z}_{2(r-1)}$ such that, for each $i,j\in\mathbb{Z}_{2(r-1)}$, $l_i=l_j$ if and only if $l'_{i+s}=l'_{j+s}$.

Let $D$ and $D'$ be two dissections of a regular $s$-gon into $r$ cells. Suppose that the dissection $D$ can produce a pair of sequences $(l,d)$ as described above, and suppose that the dissection $D'$ can produce a pair of sequences $(l',d')$. The crucial observation now is that $D$ and $D'$ belong to the same $C_s$-orbit if and only if the sequence pairs $(l,d)$ and $(l',d')$ are isomorphic.

We will now translate the problem of counting $C_s$-orbits of dissections into the problem of counting orbits of integer points in semi-dilated polytopes. It can be easily proved by induction that each CNCS indexed by $\mathbb{Z}_{2(r-1)}$ is a label sequence for some dissection into $r$ cells. Since two dissections belonging to the same $C_s$-orbit produce isomorphic label sequences, for the counting purposes it is sufficient to consider one label sequence from each isomorphism class of label sequences.

Let us now fix a label sequence $(l_i)_{i\in\mathbb{Z}_{2(r-1)}}$. The following linear constraints are necessary and sufficient for a sequence $(d_i)$ to be a distance sequence with the underlying label sequence $l$:

(i) $\sum_{i\in\mathbb{Z}_{2(r-1)}} d_i=s$,
(ii) $d_i\geqslant 2$ whenever $l_i=l_{i+1}$,
(iii) $d_i+d_j\geqslant 1$ whenever $l_i=l_{j+1}\wedge l_{i+1}=l_j\wedge i\neq j$,
(iv) $d_i\geqslant 0$ for all $i\in\mathbb{Z}_{2(r-1)}$.

The constraints of type (ii) and (iii) ensure that no cell of the dissection collapses into a line segment.

It remains to investigate under which conditions two distance sequences $d,d'$ (corresponding to the same label sequence $l$) encode $C_s$-isomorphic dissections. (For example, if $r=2$ then

$(d_0, d_1) = (a, b)$ and $(d_0, d_1) = (b, a)$ always encode $C_{a+b}$-isomorphic dissections.) As before let $l$ be fixed. An $s \in \mathbb{Z}_{2(r-1)}$ is called an *automorphism* of $l$ if, for each $i, j \in \mathbb{Z}_{2(r-1)}$, $l_i = l_j$ if and only if $l_{i+s} = l_{j+s}$. The set $G$ of all automorphisms of $l$ is a subgroup of $(\mathbb{Z}_{2(r-1)}, +)$; let us call it the *automorphism group* of $l$. The only way in which two distance sequences $d, d'$ with the *same* underlying label sequence $l$ arise from two $C_s$-equivalent dissections is if there is an automorphism $s$ of $l$ such that, for each $i \in \mathbb{Z}_{2(r-1)}$, $d_i = d'_{i+s}$.

In order to reconcile the notation for label and distance sequences with the definition of polytopes as subsets of $\mathbb{R}^n$, let us now consider these sequences as indexed by $[2(r-1)]$ rather than by $\mathbb{Z}_{2(r-1)}$, where now indices are taken modulo $2(r-1)$ if necessary. If $G \leqslant \mathbb{Z}_{2(r-1)}$ denotes the automorphism group of $l$ as defined above, then let $\bar{G} \leqslant S_{2(r-1)}$ be the corresponding group acting on sequences indexed by $[2(r-1)]$. We conclude that the value $H_{r,s,l}$, defined as *the number of $C_s$-orbits of dissections into $r$ cells with label sequence $l$,* is equal to the number of $\bar{G}$-orbits of integer points in the polytope determined by the constraints (i)–(iv) listed above.

Let $I \subseteq [2(r-1)]$ be the set of those indices $i$ which appear in the constraints of type (ii). Since the right-hand sides of these constraints are equal to 2, we need the following change of variables in order to be able to apply Theorem 2.5. Let $\bar{d}_i := d_i - 1$ if $i \in I$, and $\bar{d}_i := d_i$ otherwise. Let $\bar{s} := s - |I|$. Then $H_{r,s,l}$ is equal to the number of $\bar{G}$-orbits of integer points $\bar{d}$ in the polytope determined by the constraints

(i′) $\sum_{i \in \mathbb{Z}_{2(r-1)}} \bar{d}_i = \bar{s}$,
(ii′) $\bar{d}_i \geqslant 1$ whenever $l_i = l_{i+1}$ (i.e., $i \in I$),
(iii′) $\bar{d}_i + \bar{d}_j \geqslant 1$ whenever $l_i = l_{j+1} \wedge l_{i+1} = l_j \wedge i \neq j$,
(iv′) $\bar{d}_i \geqslant 0$ for all $i \in [2(r-1)]$.

Theorem 2.5 now implies that, for any fixed label sequence $l$, $H_{r,s,l}$ is quasi-polynomial in $\bar{s}$. Since $s = \bar{s} + |I|$, we see that $H_{r,s,l}$ is quasi-polynomial in $s$; see Remark 1 after Definition 2.1.

Summing over all non-isomorphic label sequences in $[r-1]^{2(r-1)}$, the statement of Theorem 4.1 follows for $H_{r,s}$ (i.e., the cyclic case).

In the dihedral case the proof is very similar, with the exception that the isomorphism relation for the label and distance sequences is appropriately extended to also allow for reflection. □

**Example 4.2.** Let us calculate the o.g.f. for the quasi-polynomial sequence $(h_{3,s})$ counting the number of isomorphism types of dissections of the regular $s$-gon into three cells under the dihedral symmetry.

We have $2(r-1) = 4$. After some simplifications one can see that $h_{3,s} = i(P_s)$ where

$$P_s = \big\{(d_1, d_2, d_3, d_4) \in \mathbb{R}^4\colon\ d_1 + d_2 + d_3 + d_4 = s \wedge d_1 \geqslant d_3 \wedge d_3 \geqslant 2 \\ \wedge d_2 + d_4 \geqslant 1 \wedge d_2 \geqslant d_4 \wedge d_4 \geqslant 0\big\}$$

where $d_2, d_4$ are the numbers of edges of the regular $s$-gon incident with the central cell of the dissection, and $d_1$ and $d_3$ are the numbers of edges of the regular $s$-gon incident with the two remaining cells of the dissection. The inequalities encode the geometric properties of a dissection and they ensure that each isomorphism type is accounted for exactly once. It is easy to see that in the formal power series

$$\frac{z_1^2 z_3^2}{1 - z_1 z_3} \cdot \frac{1}{1 - z_1} \cdot \left(\frac{1}{1 - z_2} \cdot \frac{1}{1 - z_2 z_4} - 1\right)$$

each term $z_1^{d_1} z_2^{d_2} z_3^{d_3} z_4^{d_4}$ corresponds to an integer point $(d_1, d_2, d_3, d_4) \in P_s$ (where $s = \sum_{i=1}^{4} d_i$), and vice versa. Consequently,

$$\sum_{s=0}^{\infty} h_{3,s} z^s = \frac{z^5 + z^6 - z^7}{(1-z)^2(1-z^2)^2}$$
$$= z^5 + 3z^6 + 6z^7 + 11z^8 + 17z^9 + 26z^{10} + 36z^{11} + 50z^{12} + \cdots,$$

cf. the third row of Table 5 on page 388 of [13].

## 5. Linear codes

For a prime power $q$, let $\mathbb{F}_q$ denote the field with $q$ elements. An $[n,k]_q$ linear code $C$ is a $k$-dimensional subspace of $\mathbb{F}_q^n$. (We will say just "code" for short.) To exclude unnecessary trivialities we will assume that no coordinate of $C$ is identically zero. A matrix $M \in \mathbb{F}_q^{k \times n}$ whose rows span $C$ is called a generator matrix for $C$. It is quite natural to study codes by considering the columns of a generator matrix as points in $\mathrm{PG}(k-1,q)$, the $(k-1)$-dimensional projective space over $\mathbb{F}_q$. A nice presentation of this approach to codes is available, for example, in [8]. Thus, let us denote by $\mathrm{Col}(M)$ the multiset of columns (considered as points in $\mathrm{PG}(k-1,q)$) of a generator matrix $M$. Two $[n,k]_q$ codes with generator matrices $M_1$ and $M_2$ are equivalent if there exists a collineation $\Pi \in \mathrm{PGL}(k,q)$ such that $\mathrm{Col}(M_2) = \{\Pi(x)\colon x \in \mathrm{Col}(M_1)\}$ (as multisets). It is easily seen that this definition of code equivalence coincides with the usual definition of monomial equivalence; see [8, Section 2.3]. Equivalent codes are isometric as metric spaces endowed with the Hamming distance function. Since it is the metric aspect which is typically most interesting in the study and application of codes, we often study codes up to equivalence.

**Theorem 5.1.** *Let $k$ be a fixed positive integer and let $q$ be a fixed prime power. The number of equivalence classes of $[n,k]_q$ linear codes is quasi-polynomial in $n$.*

**Proof.** Let $\theta(k,q) := (q^k - 1)/(q-1)$ and let us fix a numbering $P_1, \ldots, P_{\theta(k,q)}$ of points of $\mathrm{PG}(k-1,q)$. Let $G_{k,q} \leqslant S_{\theta(k,q)}$ denote the permutation representation of $\mathrm{PGL}(k,q)$'s action on the point set of $\mathrm{PG}(k-1,q)$. For a multiset $S$ of points of $\mathrm{PG}(k-1,q)$, let $u_i^S$ be the number of occurrences of $P_i$ in $S$. It follows from the previous discussion that the codes represented by the multisets $S_1, S_2$ are equivalent if and only if $u^{S_1}$ and $u^{S_2}$ belong to the same $G_{k,q}$-orbit. Let $l_{n,k,q}$ denote the number of equivalence classes of $[n,k]_q$ codes, where $q$ is a fixed prime power, and let $L_{n,k,q} = \sum_{m=1}^{k} l_{n,m,q}$. Then $L_{n,k,q}$ is the number of $G_{k,q}$-orbits on the set of integer points in the polytope $\{u \in \mathbb{R}^{\theta(k,q)}\colon \sum_{i=1}^{\theta(k,q)} u_i = n,\ u \geqslant \mathbf{0}\}$, which is quasi-polynomial in $n$ by Theorem 2.5. Finally, $l_{n,k,q} = 1$ if $k = 1$, and $l_{n,k,q} = L_{n,k,q} - L_{n,k-1,q}$ if $k > 1$. Thus $l_{n,k,q}$ is quasi-polynomial in $n$ for each fixed $k$ and $q$. $\square$

The following definitions and facts are useful for facilitating computations related to the previous theorem. Recall that we denote $[n] = \{1, \ldots, n\}$. For $f \in \mathbb{N}^{[n]}$ let $c_f := \sum_{x \in [n]} f(x)$. Let $G$ be a subgroup of $S_{[n]}$ and for $f \in \mathbb{N}^{[n]}$ let $G(f)$ denote the $G$-orbit of $f$. We say that $G(f)$ is a *$G$-partition of the number $c_f$*. For any $c \in \mathbb{N}$, let $P_G(c)$ denote the number of $G$-partitions of $c$. The following lemma is immediate and well known.

**Lemma 5.2.** *The o.g.f.* $\sum_{c\geqslant 0} P_G(c)t^c$ *is obtained by Pólya-substitution of the formal power series* $1/(1-t) = 1+t+t^2+\cdots$ *in the cycle index of* $G$*'s action on* $[n]$*, that is, for each* $1 \leqslant i \leqslant n$*, the variable* $z_i$ *of the cycle index is substituted by* $1/(1-t^i)$*.*

Because the cycle index is a multivariate polynomial, we see that $P_G(c)$ is quasi-polynomial in $c$ for each $G \leqslant S_{[n]}$. In fact, Lemma 5.2 provides an alternative proof of Theorem 5.1.

**Example 5.3.** The paper [4] contains all that is needed to work out numerical examples for Theorem 5.1. That paper also remotely hints at Theorem 5.1 via Lemma 5.2.

Since the value $L_{n,k,q}$ defined above is the number of $G_{k,q}$-partitions of $n$, it follows from Lemma 5.2 that in order to compute the generating functions explicitly we only need the cycle index of $G_{k,q}$'s natural action on $[\theta(k,q)]$, which is the cycle index of $\mathrm{PGL}(k,q)$'s natural action on $\mathrm{PG}(k,q)$. Formulas for the cycle indices of linear groups were indeed computed in [4] and they are implemented in the software system SYMMETRICA developed at the University of Bayreuth. It is thus a routine matter to find, for example, that the o.g.f. for the number of isomorphism types of binary 3-dimensional linear codes with block length $n$ is

$$\sum_{n=0}^{\infty} l_{n,3,2}z^n = \frac{z^3+z^4-z^7+z^9+z^{12}-z^{13}+2z^{14}-z^{15}}{(1-z)^2(1-z^2)(1-z^3)^2(1-z^4)(1-z^7)}$$
$$= z^3+3z^4+6z^5+12z^6+21z^7+34z^8+54z^9+\cdots.$$

The sequence $(l_{n,3,2})$ is the entry A034344 in [14]. The existence of the closed form for its o.g.f. is not noted in [14].

## 6. Unrestricted codes

Let $q$ and $n$ be positive integers, $q \geqslant 2$. Notice that we no longer assume that $q$ is a prime power. Let $A$ be an alphabet of $q$ symbols. A subset $C \subseteq A^n$ is called an *unrestricted $q$-ary code of block length $n$*. Again we will say just "code" for short. Let $r$ denote the cardinality of the code: $|C| = r$. Elements of $C$ are called *codewords*. Throughout this section we will reserve the symbols $n, q, r$ to denote the parameters of a code introduced in this paragraph. As before let $[u]$ denote the set $\{1, \ldots, u\}$.

Two codes are *isomorphic* if one can be obtained from the other by permuting the $n$ coordinates and then in each coordinate independently permuting the alphabet symbols by some permutation from $S_A$. This isomorphism relation is induced by the group action of the wreath product $S_A \wr S_n$ on $A^n$. As in Section 5, the motivation for defining this isomorphism relation is the fact that it preserves the Hamming distance.

Let $c_{q,r,n}$ denote the number of isomorphism classes of $q$-ary codes with block length $n$ and $r$ codewords. We note that $c_{q,r,n}$ is the coefficient of $x^r$ in the expansion of the Pólya substitution $z_i := 1 + x^i$ into the cycle index of the exponentiation $S_q \wr S_n$; see Theorem 1 in [5]. Trivially $c_{q,0,n} = c_{q,1,n} = 1$ and $c_{q,2,n} = n$. The values $c_{q,r,n}$ for $q \leqslant 4$ and some small values of $n, r$ are tabulated in [5]. More extended tables can be found on the WWW [6]. It appears that the behavior of $(c_{q,r,n})$ as a function of $n$ for fixed values of $q, r$ has not been studied previously.

While codes are naturally defined as sets, for technical reasons it will be easier for us to work with *ordered codes,* which we define as $r$-tuples $(w_1, \ldots, w_r) \in (A^n)^r$. We say that two ordered codes $(w_1, \ldots, w_r)$ and $(w'_1, \ldots, w'_r)$ are *isomorphic* if and only if there exists $g \in S_A \wr S_n$ such that $g(w_i) = w'_i$ for all $i \in [r]$. Let $(w_i)_j$ denote the $j$th coordinate of the codeword $w_i$. We say that the *$j$th coordinate of the ordered code $C = (w_1, \dots, w_r)$ induces the partition $\Pi$* of $[r]$ if

$$\bigl\{\bigl\{i \in [r]\colon\ (w_i)_j = a\bigr\}\colon\ a \in A\bigr\} = \Pi,$$

where on the left-hand side we omit the empty sets corresponding to those symbols of $A$ that never occur in the $j$th coordinate of $C$.

Let $S(t, u)$ denote the Stirling numbers of the second kind. Then

$$N(q, r) := \sum_{i=1}^{q} S(r, i)$$

denotes the number of partitions of $[r]$ into at most $q$ non-empty subsets. Let us fix an ordering $(\Pi_1, \dots, \Pi_{N(q,r)})$ of these partitions. For an ordered code $C$ and $i \in [N(q, r)]$ let $a_i(C)$ denote the number of those coordinates of $C$ that induce the partition $\Pi_i$. Naturally, $\sum_{i=1}^{N(q,r)} a_i(C) = n$. Clearly, for two ordered codes $C, C'$ we have $a_i(C) = a_i(C')$ for all $i \in [N(q, r)]$ if and only if $C$ and $C'$ are isomorphic as ordered codes.

The natural action of $S_{[r]}$ on subsets of $[r]$ induces the action of $S_{[r]}$ on $\{\Pi_1, \dots, \Pi_{N(q,r)}\}$. This action then induces the action of $S_{[r]}$ on vectors $(a_i(C))$ defined above, which we can formally view as the action

$$S_{[r]} \times \mathbb{N}^{N(q,r)} \to \mathbb{N}^{N(q,r)} \tag{2}$$

defined by $\pi a = a'$ such that, for each $i \in [N(q, r)]$, $a'_i := a_j$ with $j$ uniquely determined by $\pi\Pi_j = \Pi_i$. The codes $\{w_1, \dots, w_r\}$ and $\{w'_1, \dots, w'_r\}$ are isomorphic if and only if there exists $\pi \in S_{[r]}$ such that the ordered codes $(w_1, \dots, w_r)$ and $(w'_{\pi(1)}, \dots, w'_{\pi(r)})$ are isomorphic. (Notice that the definition of ordered codes allows repeated codewords.) Thus we can summarize the last two paragraphs in the following statement:

**Lemma 6.1.** *The isomorphism classes of $q$-ary unrestricted codes with block length $n$ and $r$ codewords* (*with repeated codewords allowed*) *correspond to the $S_{[r]}$-orbits of functions $a : [N(q, r)] \to \mathbb{N}$ satisfying $\sum_{i=1}^{N(q,r)} a(i) = n$.*

We are now ready for the main result of this section:

**Theorem 6.2.** *Let $c_{q,r,n}$ denote the number of isomorphism classes of $q$-ary unrestricted codes with block length $n$ and $r$ codewords. For any fixed values of $q$ and $r$, the sequence $(c_{q,r,n})$ is quasi-polynomial in $n$.*

**Proof.** Let $q$ and $r$ be fixed. It follows from Lemma 6.1 that, for each $n \in \mathbb{N}$, the value $c_{q,r,n}$ is equal to the number of $S_{[r]}$-orbits on the set of integer points $(a_1, \dots, a_{N(q,r)})$ in the polytope which is defined by the following three types of constraints:

(i) $a_i \geqslant 0$ for $i = 1, \dots, N(q, r)$,
(ii) $\sum_{i=1}^{N(q,r)} a_i = n$,
(iii) for each $i, j \in [r]$, $i \neq j$, we have $\sum_k a_k \geqslant 1$ where the sum extends over precisely those $k$ for which $i$ and $j$ belong to different parts of the partition $\Pi_k$.

Constraints of the type (iii) assure that the code consists of precisely $r$ distinct codewords by asserting that for $i \neq j$ there exists at least one coordinate $l$ such that $(w_i)_l \neq (w_j)_l$. Once again, the result now follows from Theorem 2.5. □

**Example 6.3.** Let us find the o.g.f. for the sequence $(c_{2,3,n})$ counting the number of isomorphism types of binary unrestricted codes with block length $n$ and exactly three codewords.

We have $c_{2,3,n} = i(P_n)$, where

$$P_n = \big\{(a_1, a_2, a_3, a_4) \in \mathbb{R}^4\colon\ a_1 + a_2 + a_3 + a_4 = n \wedge a_2 \geqslant a_3 \wedge a_3 \geqslant a_4 \\ \wedge a_3 + a_4 \geqslant 1 \wedge a_4 \geqslant 0\big\}.$$

This can be seen by bringing any binary unrestricted code with block length $n$ and exactly three codewords into the canonical form

$$\begin{array}{cccc} 0\dots0 & 1\dots1 & 0\dots0 & 0\dots0 \\ 0\dots0 & 0\dots0 & 1\dots1 & 0\dots0 \\ \underbrace{0\dots0}_{a_1} & \underbrace{0\dots0}_{a_2} & \underbrace{0\dots0}_{a_3} & \underbrace{1\dots1}_{a_4} \end{array}$$

where the constraints defining the polytope $P_n$ ensure that each isomorphism type is counted exactly once, and that there are exactly three codewords (no two codewords are identical).

It is easy to see that in the formal power series

$$\frac{1}{1-z_1} \cdot \left(\frac{1}{1-z_2} \cdot \frac{1}{1-z_2z_3} \cdot \frac{1}{1-z_2z_3z_4} - \frac{1}{1-z_3}\right)$$

each term $z_1^{a_1} z_2^{a_2} z_3^{a_3} z_4^{a_4}$ corresponds to the integer point $(a_1, a_2, a_3, a_4) \in P_n$ (where $n = \sum_{i=1}^4 a_i$), and vice versa. Therefore

$$\sum_{n=0}^{\infty} c_{2,3,n} z^n = \frac{z^2 + z^3 - z^5}{(1-z)^2(1-z^2)(1-z^3)} \\ = z^2 + 3z^3 + 6z^4 + 10z^5 + 16z^6 + 23z^7 + \cdots,$$

in accordance with the third row of Table 1 on page 215 of [5].

## 7. Conclusion

We have introduced a general method for proving that certain enumerating sequences naturally arising in combinatorics are quasi-polynomial. We have presented a variety of examples that demonstrate that the method is widely applicable.

We have not been concerned with actually *computing* the closed form of the quasi-polynomial functions whose existence we have proved. For this goal, which we consider an interesting research topic of its own, we can envision two approaches:

Firstly, one may seek further geometric insight into the set of polytopes arising in our proof of Theorem 2.5. The high number of polytopes arising in our proof is not a problem when one wants to prove theoretical results as we do in this article, but it becomes a limiting factor when one wants to perform explicit numerical computations with polytopes such as those facilitated by the LattE package [2].

Secondly, one may use the Pólya Theory as the main tool. In the case of polygon dissections this approach was successfully used in [9]. For unrestricted codes, an example combining Pólya

Theory and polytope methods was given in [10]. However, this approach requires a deeper understanding of the isomorphism relation that one works with, and it is usually specifically tailored for the application at hand. In a situation when one is faced with a new type of combinatorial objects and proving a quasi-polynomiality result is the first task to be attempted, the approach outlined in the present article seems to be more likely to succeed.

## References

[1] M. Beck, Multidimensional Ehrhart reciprocity, J. Combin. Theory Ser. A 97 (1) (2002) 187–194.
[2] J.A. De Loera, D. Haws, R. Hemmecke, P. Huggins, J. Tauzer, R. Yoshida, A User's Guide for LattE v1.1, Univ. of California, Davis, 2003, http://www.math.ucdavis.edu/~latte/.
[3] E. Ehrhart, Sur les polyèdres rationnels homothétiques à $n$ dimensions, C. R. Acad. Sci. Paris 254 (1962) 616–618.
[4] H. Fripertinger, Cycle indices of linear, affine, and projective groups, Linear Algebra Appl. 263 (1997) 133–156.
[5] H. Fripertinger, Enumeration, construction and random generation of block codes, Des. Codes Cryptogr. 14 (3) (1998) 213–219.
[6] H. Fripertinger, Isometry classes of codes, http://www.mathe2.uni-bayreuth.de/frib/codes/tables.html.
[7] A. Kerber, Applied Finite Group Actions, second ed., Algorithms Combin., vol. 19, Springer-Verlag, Berlin, 1999.
[8] I.N. Landjev, Linear codes over finite fields and finite projective geometries, Discrete Math. 213 (1–3) (2000) 211–244.
[9] P. Lisoněk, Closed forms for the number of polygon dissections, J. Symbolic Comput. 20 (5–6) (1995) 595–601.
[10] P. Lisoněk, Enumeration of codes of fixed cardinality up to isomorphism, in: Proceedings of Algebraic Combinatorics and Applications (ALCOMA05), Thurnau, April 2005, Bayreuth. Math. Schr. 74 (2005) 256–265.
[11] R. Mathon, Computational methods in design theory, in: Surveys in Combinatorics, Guildford, 1991, in: London Math. Soc. Lecture Note Ser., vol. 166, Cambridge Univ. Press, Cambridge, 1991, pp. 101–117.
[12] R. Mathon, A. Rosa, 2-$(v, k, \lambda)$ designs of small order, in: C.J. Colbourn, J.H. Dinitz (Eds.), The CRC Handbook of Combinatorial Designs, CRC Press, 1996.
[13] R.C. Read, On general dissections of a polygon, Aequationes Math. 18 (3) (1978) 370–388.
[14] N.J.A. Sloane, The on-line encyclopedia of integer sequences, http://www.research.att.com/~njas/sequences/.
[15] R.P. Stanley, Enumerative Combinatorics, vol. I, Wadsworth & Brooks, 1986.