Abstract

For $k$ a positive integer, we consider the problem of counting solutions $x$ to the equation $kx = 0$, where $x$ is to lie in a given subset $K$ of a torus group. This problem is considered for three classes of subsets $K$.

© 2005 Elsevier Inc. All rights reserved.

Keywords: Convex polytope; Ehrhart polynomial; Torus group; Characteristic polynomial

1. Introduction

Let $T^n$ denote the $n$-dimensional torus group, the $\mathbb{Z}$-module $T^n = \mathbb{R}^n / \mathbb{Z}^n$. It is a topological group. For $n = 1$ we have the circle group, $T^1 = T$. The canonical mapping $\pi : \mathbb{R}^n \to T^n$ is a local homeomorphism. Any closed connected subgroup of $T^n$ is isomorphic to $T^k$, for some $k$, and we refer to such groups as torus groups. Here we consider some counting problems involving certain subsets of $T^n$.

It is shown in [5] that the following three conditions on sets $K \subseteq T^n$ are equivalent:

(1) $K$ is a finite union of closed subgroups of $T^n$;
(2) $K$ is a topologically closed set which is a union of subgroups of $T^n$; and

This paper is based upon work supported by the US National Science Foundation under Grant no. DMS0101209.

E-mail address: lawrence@gmu.edu.

0022-314X/$ - see front matter © 2005 Elsevier Inc. All rights reserved.
doi:10.1016/j.jnt.2005.06.012
(3) $K$ is a topologically closed subset of $\mathcal{T}^n$ which is closed under the mapping $x \mapsto kx$, for each positive integer $k$.

We denote the collection of such subsets by $\hat{\mathcal{K}}^n$.

We will also consider elements of the larger collection $\hat{\mathcal{K}}^n$ of sets which are finite unions of cosets of closed subgroups of $\mathcal{T}^n$, as well as those of the smaller collection $\hat{\mathcal{K}}^n$ of finite unions of closed, $(n-1)$-dimensional subgroups of $\mathcal{T}^n$ (where the dimension is the topological dimension, which coincides with the dimension of the connected component containing 0, a torus group).

The counting problems considered involve counting solutions $x \in K$ to the equation $kx = 0$, where $k$ is a positive integer, for $K$ in the above collections.

2. Some background and three lemmas

The group $\mathbb{Z}^n$ acts on $\mathcal{R}^n$ by translation. A fundamental region for this group action is the “half-open $n$-cube” $[0, 1)^n$. The restriction of $\pi$ to $[0, 1)^n$ is a bijection of sets, $\pi|_{[0,1)^n} : [0, 1)^n \to \mathcal{T}^n$. If $\pi : \mathcal{R}^n \to \mathcal{T}^n$ is the canonical mapping, then the correspondence between the set of closed subgroups of $\mathcal{T}^n$ and the set of closed subgroups of $\mathcal{R}^n$ which contain $\mathbb{Z}^n$ given by $G \mapsto \pi^{-1}(G)$ is a bijection.

Closed subgroups of $\mathcal{T}^n$ are isomorphic to groups of the form $\mathcal{T}^a \oplus A$, where $A$ is a finite abelian group. The component containing 0 of such a group is therefore a torus group. Closed subgroups of $\mathcal{R}^n$ are isomorphic to groups of the form $\mathcal{R}^a \oplus \mathbb{Z}^b$, where $a + b \leq n$.

2.1. Smith normal form

Most of the facts about closed subgroups of $\mathcal{T}^n$ which are pertinent here can be ascertained from considerations involving the “Smith normal form” of a matrix of integers. We describe this relationship.

Let $M$ be an $m \times n$ matrix of integers. Define $\mathcal{R}_M = \{x \in \mathcal{R}^n : Mx \in \mathbb{Z}^m\}$ and $\mathcal{T}_M = \{x \in \mathcal{T}^n : Mx = 0\}$. (Since $\mathcal{T}^n$ is a $\mathbb{Z}$-module, $Mx$ makes sense.) Then the groups $\mathcal{R}_M$ and $\mathcal{T}_M$ are associated in the correspondence above, as $\mathcal{R}_M = \pi^{-1}(\mathcal{T}_M)$.

If $N_1$ and $N_2$ are nonsingular unimodular matrices of integers of sizes $m \times m$ and $n \times n$, respectively, then $\mathcal{T}_{N_1M\overrightarrow{N_2}}$ is isomorphic to $\mathcal{T}_M$ by the mapping $u \mapsto N_2u$ (and similarly for $\mathcal{R}_M$, $\mathcal{R}_{N_1M\overrightarrow{N_2}}$). Any matrix $M$ of integers can be reduced in a unique way by such a transformation to a matrix, the Smith normal form of $M$, $M = (\delta_{i,j})$, of the same size, such that if $\ell$ denotes the rank of $M$, $\delta_{i,j} = 0$ if $i \neq j$, or if $i = j > \ell$, and such that $\delta_{i,i}$ is a positive integer for $1 \leq i \leq \ell$, with $\delta_{i,i}$ dividing $\delta_{i+1,i+1}$ for $1 \leq i \leq \ell - 1$. The numbers $\delta_{i,i}$, henceforth denoted $\delta_i$, are called the elementary divisors of $M$. They are also determined by: $\delta_i = 0$ if all of the $i \times i$ subdeterminants of $M$ are 0; otherwise, the product $\prod_{j=1}^i \delta_j$ is the greatest common divisor of the $i \times i$ subdeterminants of $M$. For more details about Smith normal form, see [7].

Any closed subgroup of $\mathcal{R}^n$ containing $\mathbb{Z}^n$ is of the form $\mathcal{R}_M$, for some matrix $M$ of integers; and any closed subgroup of $\mathcal{T}^n$ is of the form $\mathcal{T}_M$. It is apparent that, for $M$ in
Smith normal form, the group $R_M$ is isomorphic to $R^{n-\ell} \oplus \mathbb{Z}^\ell$; and $T_M$ is isomorphic to $T^{n-\ell} \oplus A$, where the finite abelian group $A$ is the product of cyclic groups of orders $\delta_1, \ldots, \delta_\ell$. Therefore, any closed subgroup of $R^n (T^n)$ is of this form. If $K$ denotes a closed subgroup of $T^n$, we write $0_K$ to denote the connected component containing $0$. If $K$ is the group $T_M \cong T^{n-\ell} \oplus A$, then $0_K = T^{n-\ell}$ and $K/0_K \cong A$; and always, $K \cong 0_K \oplus (K/0_K)$.

Note that the elementary divisor $\delta_\ell$ is the smallest positive integer which annihilates the finite group $A$, or equivalently the largest order of an element of $A$; and the product of the nonzero elementary divisors is the order $|A|$ of $A$.

What is actually required to determine the subgroup $T_M \subseteq T^n$? It is clear that, if $\tilde{M} = NM$, where $N$ is unimodular, then $\tilde{T_M} = \tilde{T}_M$. The matrix $M$ can be reduced by such a transformation, $M \mapsto NM$, to a matrix $\tilde{M} = (\tilde{\beta}_{i,j})$ having $\tilde{\beta}_{i,j} = 0$ for $i > n$ and for $j < i$. (Indeed, $M$ can be reduced to a matrix which is in “Hermite normal form,” for which the above conditions certainly hold. See [7].) Therefore we may replace $M$ by the matrix consisting of the nonzero rows of $\tilde{M}$.

2.2. Quasi-polynomials

A function $c$ on the natural numbers $\mathcal{N}$ is called periodic if there is a number $p$, the period of $c$, such that, for each $k \in \mathcal{N}$, $c(k + p) = c(k)$. The periodic functions $c : \mathcal{N} \to \mathbb{Z}$ form a commutative ring with identity under pointwise operations. We denote this ring by $\mathcal{R}_{\text{per}}$.

A quasi-polynomial is a function $q : \mathcal{N} \to \mathbb{Z}$ of the form

$$q(k) = c_0(k) + c_1(k)k + c_2(k)k^2 + \cdots + c_d(k)k^d,$$

where the $c_i(k)$’s are in $\mathcal{R}_{\text{per}}$. The number $d$ (assuming $c_d(k)$ is not identically 0) is the degree of the quasi-polynomial. If the quasi-polynomial is identically zero, its degree is taken to be 0. The least common multiple of the periods of the $c_i(k)$’s is called the quasi-period of the quasi-polynomial (but of course the quasi-polynomial itself is not periodic unless its degree is 0). The restriction of a quasi-polynomial to any congruence class modulo its period is a polynomial function on that congruence class.

The quasi-polynomials form a ring under pointwise operations. It is not hard to show that this ring is isomorphic to the ring $\mathcal{R}_{\text{per}}[x]$ of polynomials in one variable over $\mathcal{R}_{\text{per}}$, and that the coefficient functions $c_j$ and degree $d$ are uniquely determined.

We shall also be interested in quasi-polynomials having coefficients in certain subrings of $\mathcal{R}_{\text{per}}$. The first of these subrings, denoted by $\mathcal{R}_{\text{gcd}}$, is the additive group of periodic functions generated by the functions of the form $f(k) = \gcd(k, m)$, where $m \in \mathcal{N}$. It is easily verified that this additive subgroup is also closed under multiplication in $\mathcal{R}_{\text{per}}$, and so forms a subring which is itself a commutative ring with identity. The second is $\mathcal{R}_{\text{mult}}$, which is the additive group of periodic functions generated by
functions of the form $f(k) = (b \mid k)$ for $b \in \mathcal{N}$, where
\[
(b \mid k) = \begin{cases} 
1 & \text{if } b|k, \\
0 & \text{otherwise.}
\end{cases}
\]

It is also closed under multiplication, and therefore forms a subring. We have $\mathcal{R}_{\gcd} \subseteq \mathcal{R}_{\text{mult}} \subseteq \mathcal{R}_{\text{per}}$.

It is not difficult to show that the quasi-polynomials having coefficients in either of the two smaller rings have the property that, if $p$ is the quasi-period, then each coefficient $c_i$ is constant when restricted to a set on which $\gcd(k, p)$ is constant; equivalently, the quasi-polynomial is a polynomial on each such set.

2.3. Three lemmas

The following lemmas provide solutions to the problem of counting solutions to the equation $kx = 0$ in special cases.

Recall that any finite abelian group is isomorphic to a direct sum of cyclic groups.

Lemma 1. Let

\[
A = \bigoplus_{i=1}^{m} C_i,
\]

where the $C_i$’s are finite cyclic groups. For $k \in \mathcal{N}$ let $f(k)$ denote the cardinality of the set $\{x \in A : kx = 0\}$. Then $f(k) = \prod_{i=1}^{m} \gcd(k, |C_i|)$. Therefore, $f(k)$ is an element of $\mathcal{R}_{\gcd}$ whose period equals the maximum order of elements of $A$, which is a divisor of the order $|A|$ of $A$.

Proof. Let $x = (x_1, \ldots, x_m)$ be an element of $A$. Then $kx = 0$ if and only if $kx_i = 0$ for each $i$; that is,

\[
\{x \in A : kx = 0\} = \bigcap_{i=1}^{m} \{x \in C_i : kx = 0\}.
\]

Then $f(k)$ is the product of the cardinalities of those of the sets on the right. For a finite cyclic group $C$, certainly

\[
|\{x \in C : kx = 0\}| = \gcd(k, |C|).
\]

The assertions of the last sentence are now easily verified. \Box

For a subset $K \subseteq \mathcal{T}^n$ and an integer $k \geq 1$, let $f(K, k) = |\{x \in K : kx = 0\}|$. For any such subset $K$ we have $0 \leq f(K, k) \leq f(\mathcal{T}^n, k) = k^n$. 
Lemma 2. Let K be a closed subgroup of $T^n$ having dimension d. Let $A = K/0K$ and let $f$ be as in Lemma 1. We have

$$f(K,k) = f(k)k^d.$$ 

It follows that $f(K,k)$ is a quasi-polynomial of degree d having coefficients in $\mathcal{R}_{\gcd}$, and its quasi-period divides the order of the group $K/0K$. Suppose further that $M$ is a matrix of integers, the rank of $M$ is $\ell$, the elementary divisors of $M$ are $\delta_1, \ldots, \delta_\ell$, and $K = \mathcal{T}_M$. Then $d = n - \ell$ and

$$f(K,k) = \left(\prod_{i=1}^\ell \gcd(k,\delta_i)\right)k^d.$$ 

Proof. We have $K \simeq 0K \oplus A$ and $\dim(0K) = \dim(K) = d$, from which the first assertions readily follow. For the rest, observe that $0K \simeq T^{n-\ell}$ and $A \simeq \oplus_{i=1}^\ell C_i$, where $C_i$ is cyclic of order $\delta_i$. □

Lemma 3. If $K$ is a d-dimensional closed subgroup of $T^n$ and $K'$ is a coset of $0K$ in $K$, then

$$f(K',k) = \langle b \mid k \rangle k^d,$$

where $b$ is the least positive integer such that $bK' = 0K$. (We call $b$ the order of $K'$.) It follows that $f(K',k)$ is a quasi-polynomial of degree d whose coefficients lie in $\mathcal{R}_{\text{mult}}$ and whose quasi-period is a divisor of $|K/0K|$.

Proof. There is an isomorphism $\tau: K \simeq 0K \oplus A$, where $A = K/0K$, and there is $u \in A$ such that $\tau(K') = \{(x,u) : x \in 0K\}$. Then $b$ is the least positive integer such that $bu = 0$. We have

$$f(K',k) = \begin{cases} f(0K,k) & \text{if } b|k, \\ 0 & \text{otherwise}. \end{cases} \quad \square$$

Notice that a coset $K'$ of a closed subgroup $K''$ is not necessarily contained in a closed subgroup $K$ having $K'' = 0K$. Lemma 3 does not apply; however it is clear that in this case $f(K',k) = 0$.

2.4. Möbius functions

Let $P = (P, \leq)$ be a finite poset. The Möbius function (see [6]) of $P$ is then the unique function $\mu: P \times P \rightarrow \mathbb{Z}$ satisfying:

1. $\mu(x, y) = 0$ unless $x \leq y$; and

2. $\mu(x, y) = \sum_{z \in P : x \leq z \leq y} \mu(x, z) \mu(z, y)$.
(2) For \( x, y \in P \) with \( x \leq y \),

\[
\sum_{z : x \leq z \leq y} \mu(x, z) = \begin{cases} 
1 & \text{if } x = y, \\
0 & \text{if } x \neq y.
\end{cases}
\]

(In view of (1), we usually view \( \mu \) as having domain of definition the set of pairs \( (x, y) \in P \times P \) such that \( x \leq y \).) The Möbius function of the poset of all subsets of a finite set \( X \) ordered by inclusion is given by

\[
\mu(I, J) = (-1)^{|J| - |I|}
\]

for \( I \subseteq J \subseteq X \).

The posets considered here will be finite lattices, and so will have greatest and least elements. Suppose therefore that \( P \) possesses a least element \( \bar{0} \) and a greatest element \( \bar{1} \). The Möbius invariant of \( P \) is then the value \( \mu(\bar{0}, \bar{1}) \). The Möbius invariant of \( P \) and its dual poset are equal.

Suppose that \( X \) is a finite set and let \( \gamma \) be a closure operator on \( X \), so that:

1. If \( I \subseteq X \) then \( I \subseteq \gamma(I) \subseteq X \);
2. If \( I \subseteq J \subseteq X \) then \( \gamma(I) \subseteq \gamma(J) \); and
3. For \( I \subseteq X \), \( \gamma(\gamma(I)) = \gamma(I) \).

Call a set \( I \subseteq X \gamma\)-closed provided that \( \gamma(I) = I \). The \( \gamma \)-closed sets include \( X \), and the intersection of any collection of \( \gamma \)-closed sets is another. Therefore the set \( \mathcal{L} \) of \( \gamma \)-closed sets partially ordered by inclusion is a lattice. For \( I, I' \in \mathcal{L} \) such that \( I \subseteq I' \), set

\[
\mu(I, I') = \sum_{J : I \subseteq J \subseteq I', \gamma(J) = I'} (-1)^{|J| - |I|}.
\]

Then we have

\[
\sum_{J \in \mathcal{L}, I \subseteq J \subseteq I'} \mu(I, J) = \sum_{J \subseteq I', J \geq I} (-1)^{|J| - |I|} = \begin{cases} 
1 & \text{if } I = I', \\
0 & \text{otherwise},
\end{cases}
\]

and it is clear that this is the Möbius function of \( \mathcal{L} \).

2.5. Ranked posets and characteristic polynomials

By a rank function on \( P \) we simply mean a function \( r \) mapping \( P \) to the nonnegative integers. Two primary examples of rank functions are (1) those determined by posets \( P \) which satisfy the Jordan–Dedekind chain condition, with \( r(p) \) giving the height in \( P \).
of the element \( p \), and (2) those determined by representations of posets \( P \) as partially ordered sets of arrangements of vector subspaces of a vector space, under inclusion, where now \( r(p) \) gives the dimension of the subspace corresponding to \( p \). In the second instance, the rank function cannot be ascertained from the poset alone. Therefore we refer to the \textit{ranked} poset, \( P \), to indicate that there is also specified a rank function. In this paper we are also interested in a third class, namely, that of posets \( P \) which arise as the partially ordered sets (under inclusion) of finite collections of closed subgroups of torus groups, closed under intersection, ranked by dimension.

Given a ranked poset \( P \) with \( \bar{0} \) and \( \bar{1} \), its \textit{characteristic polynomial} is

\[
\chi(t) = \sum_{p \in P} \mu(\bar{0}, p)t^{r(\bar{1}) - r(p)}.
\]

Let \( \mathcal{L} \) and \( X \) be as in the preceding subsection and suppose that \( \mathcal{L} \) is ranked, by a rank function \( r \); then the function \( r' \) given on subsets \( I \) of \( X \) by \( r'(I) = r(\gamma(I)) \) is certainly a rank function on the boolean lattice of subsets of \( X \). Furthermore, the characteristic polynomial of this ranked boolean lattice is given by

\[
\sum_{I \subseteq X} (-1)^{|I|}t^{r'(X) - r'(I)}.
\]

Breaking up this sum over the partition of the boolean lattice into the subsets on which \( \gamma \) is constant, and using the formula above for the Möbius function of \( \mathcal{L} \), we see that the characteristic function of the ranked boolean lattice coincides with the characteristic function of the ranked lattice \( \mathcal{L} \).

3. Counting solutions to \( kx = 0 \)

We consider the functions \( f(K, k) \) obtained when \( K \) is a finite union of subgroups of a torus group.

**Theorem 1.** Suppose

\[
K = \bigcup_{i=1}^{m} K_i \in \mathcal{K}^n,
\]

where the \( K_i \)'s are closed subgroups. Then

\[
f(K, k) = \sum_{\substack{I \subseteq [m] \setminus \{0\} \setminus \{i\} \not= \emptyset \atop i \in I}} (-1)^{|I| - 1} f(\bigcap_{i \in I} K_i, k).
\]
Furthermore, \( f(K, k) \) is a quasi-polynomial with coefficients in \( R_{\gcd} \) whose degree is the dimension of \( K \).

**Proof.** The expression for \( f(K, k) \) is the principle of inclusion–exclusion in the present context. We see from Lemma 2 applied to the summands that \( f(K, k) \) is a quasi-polynomial having coefficients in \( R_{\gcd} \) and that its degree is at most that of the maximum of the dimensions of the \( K_i \)'s, which is the dimension of \( K \). That the degree equals this maximum now follows from the observation that \( f(K, k) \geq f(K_i, k) \), for each \( i \). \( \square \)

Given a finite collection (arrangement) \( A = \{K_1, \ldots, K_m\} \) of closed subgroups of \( T^n \), the **characteristic polynomial** of \( A \) is defined to be

\[
\chi(A, t) = \sum_{I \subseteq [m], I \neq \emptyset} (-1)^{|I|} t^\dim(\bigcap_{i \in I} K_i).
\]

(Here the empty intersection is taken to be \( T^n \).) That is, it is the characteristic polynomial of the boolean lattice of subsets of \([n]\), ranked by the rank function

\[
r(I) = \dim\left(\bigcap_{i \in I} K_i\right).
\]

Then \( \chi(A, t) \) is a polynomial in \( t \) of degree \( n \). It coincides with the characteristic polynomial of the lattice \( L \) consisting of the subgroups of \( T^n \) which are intersections of the \( K_i \)'s ordered by inclusion and ranked by dimension.

**Theorem 2.** Suppose \( A \) is an arrangement of closed subgroups of \( T^n \) and let \( K \) denote the union of these subgroups. Let \( a \) be relatively prime to the quasi-period of the quasi-polynomial \( f(K, k) \). Then \( f(K, a) = a^n - \chi(A, a) \).

**Proof.** Again we have

\[
f(K, k) = \sum_{I \subseteq [m], I \neq \emptyset} (-1)^{|I|} t^\dim(\bigcap_{i \in I} K_i).
\]

Substituting \( a \) for \( k \) and using Lemma 1 we have that \( f(\bigcap_{i \in I} K_i, a) = a^\dim(\bigcap_{i \in I} K_i) \), and the sum clearly coincides with \( a^n - \chi(A, a) \). \( \square \)

A **coset arrangement** is a finite collection of cosets of closed connected subgroups of \( T^n \). Let \( A = \{\hat{K}_1, \ldots, \hat{K}_m\} \) be a coset arrangement; for \( 1 \leq i \leq m \), let \( K_i \) be the closed subgroup of which \( \hat{K}_i \) is a coset; and, for \( I \subseteq [m] \), let \( K_I \) denote \( \bigcap_{i \in I} K_i \) and similarly \( \hat{K}_I = \bigcap_{i \in I} \hat{K}_i \). Let \( P \) denote the collection of subsets \( C \) of \( T^n \) such
that, for some \( I \subseteq [m] \), \( C \) is a connected component of \( \hat{K}_I \). Note that such a set \( C \) is a coset of a closed connected subgroup of \( T^n \). Considering \( I = \emptyset \), we see that \( T^n \in \mathcal{P} \). We consider \( \mathcal{P} \) to be ordered by inclusion. This poset \( \mathcal{P} \) is called the coset poset of the arrangement \( A \). Note that, if \( C_1, C_2 \in \mathcal{P} \), then \( C_1 \cap C_2 \) need not be in \( \mathcal{P} \); however, any intersection of elements of \( \mathcal{P} \) has a partition into such elements. Let \( \mu \) denote the Möbius function of this partially ordered set. Finally, for each \( C \in \mathcal{P} \), let \( \omega(C) = -\mu(C, T^n) \).

**Lemma 4.** For \( x \in T^n \),

\[
\sum_{C \in \mathcal{P} : C \neq T^n \text{ and } x \in C} \omega(C) = \begin{cases} 1 & \text{if } x \in \bigcup Ki, \\ 0 & \text{otherwise.} \end{cases}
\]

**Proof.** Let \( x \) be an element of \( \bigcup_{i=1}^m \hat{K}_i \). Let \( D \) denote the minimal element of the coset poset which contains \( x \). It is unique, since the intersection of any two cosets in \( \mathcal{P} \) has a partition into elements of \( \mathcal{P} \). By the defining property of the Möbius function, \( \sum_{C \supseteq D} \omega(C) = 0 \) for each set \( D \in \mathcal{P} \) such that \( D \neq T^n \). Since \( \omega(T^n) = -1 \),

\[
\sum_{C \in \mathcal{P} : C \neq T^n \text{ and } x \in C} \omega(C) = 1.
\]

Clearly, for \( x \) not in the union, this sum is 0. \( \square \)

**Theorem 3.** Let \( A = \{\hat{K}_1, \ldots, \hat{K}_m\} \) be a coset arrangement, and let \( \hat{K} = \bigcup_{i=1}^m \hat{K}_i \in \hat{K}^n \). Let \( \mathcal{P} \) be the coset poset of \( A \), and let \( \omega \) be as above. Then

\[
f(\hat{K}, k) = \sum_{C \in \mathcal{P} : C \neq T^n} \omega(C) f(C, k).
\]

Furthermore, in this summation, \( \omega(C) \) is an integer and \( f(C, k) = \langle b \mid k \rangle k^{\dim(C)} \), where \( b \in N \) is as in Lemma 3 (for \( K' = C \)). It follows that, as a function of \( k \), \( f(\hat{K}, k) \) is a quasi-polynomial with coefficients in \( R_{\text{mult}} \) whose degree is at most the dimension of \( \hat{K} \) and whose quasi-period is the least common multiple of the orders of the cosets \( C \) for which \( \omega(C) \neq 0 \).

**Proof.** We have

\[
f(\hat{K}, k) = \sum_{x \in \hat{K} : kx = 0} 1
= \sum_{x \in \hat{K} : kx = 0} \sum_{C \in \mathcal{P} : C \neq T^n \text{ and } x \in C} \omega(C)
\]
\[\begin{align*}
\sum_{C \in \mathcal{P} : C \neq T^n} \omega(C) \sum_{x \in C : kx = 0} 1
\end{align*}\]

\[\begin{align*}
\sum_{C \in \mathcal{P} : C \neq T^n} \omega(C) f(C, k).
\end{align*}\]

The last two statements follow immediately. \(\square\)

The functions \(\langle b \mid k \rangle k^a\) form a basis for the \(\mathbb{Z}\)-module \(\mathcal{R}_{\text{mult}}\). For \(\hat{K}\) as in Theorem 3, the following corollary gives the coefficients of \(f(\hat{K}, k)\) in terms of this basis.

**Corollary 1.** For \(A\) and \(\hat{K}\) as in the theorem,

\[f(\hat{K}, k) = \sum_{a \geq 0, b \geq 1} \omega_{a,b} \langle b \mid k \rangle k^a,\]

where

\[\omega_{a,b} = \sum_{C} \omega(C),\]

the sum extending over all \(C \in \mathcal{P}\) having dimension \(a\) and order \(b\).

**Proof.** This follows immediately from the theorem. \(\square\)

Let \(K\) be in \(K^n\). We term \(K\) uni-parted if there exists an arrangement \(\mathcal{A} = \{K_1, \ldots, K_m\}\) of subgroups such that \(K = \bigcup K_i\) and, for each set \(I \subseteq [m]\), the set \(K_I\) is connected (or, equivalently, \(0K_I = K_I\)). Letting \(\mathcal{P}\) be the coset poset of \(\mathcal{A}\), the cosets in \(\mathcal{P}\) are torus groups. This will be the case, for example, if there exists a totally unimodular \(m \times n\) matrix \(A\) such that, for \(1 \leq i \leq n\), \(K_i = \{x \in \mathbb{T}^n : \sum_{j=1}^{n} A_{i,j} x_j = 0\}\). In this case, assuming \(A\) has no zero rows, the torus groups \(K_i\) have dimension \(n - 1\).

**Corollary 2.** If \(K\) is uni-parted and \(\mathcal{A}\) is an arrangement for which the defining condition above is satisfied, then the quasi-period of \(f(K, k)\) is \(1\); that is, \(f(K, k)\) is the polynomial \(f(K, k) = k^n - \chi(\mathcal{A}, k)\).

**Proof.** From Theorem 3 it is clear that the quasi-period of a uni-parted set \(K\) is \(1\). The rest then follows from Theorem 2. \(\square\)
Example. This example shows that $f(K, k)$ may be a polynomial even if $K$ is not uni-parted. Let $n = 4$ and $M_1$, $M_2$, and $M_3$ be the matrices

$$M_1 = \begin{pmatrix} 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix},$$

$$M_2 = \begin{pmatrix} 0 & 0 & 0 & 1 \\ 2 & 1 & 1 & 1 \end{pmatrix},$$

and

$$M_3 = \begin{pmatrix} 2 & 0 & 1 & 0 \\ 0 & 1 & 0 & 1 \end{pmatrix};$$

and let $A = \{K_1 = T_{M_1}, K_2 = T_{M_2}, K_3 = T_{M_3}\}$. Then from Lemma 2 we have

$$f(K_1, k) = f(K_2, k) = f(K_3, k) = k^2,$$

$$f(K_{\{1,2\}}) = f(K_{\{2,3\}}) = k,$$

and

$$f(K_{\{1,3\}}) = f(K_{\{1,2,3\}}) = \gcd(k, 2).$$

From Theorem 2, $f(K, k) = 3k^2 - 2k$. It is easily shown that any arrangement $A' = \{K'_1, \ldots, K'_m\}$ for which $K = \bigcup K'_i$ must include the groups $K_1$, $K_2$, and $K_3$, so $K$ is not uni-parted.

However, in the important special case in which $K$ is a union of subgroups of dimension $n - 1$, that $f(K, k)$ is a polynomial does imply $K$ is uni-parted. We obtain this as an immediate corollary of the next theorem.

For $x \in T^n$, let $\mathcal{P}_x$ be the poset of cosets $C \in \mathcal{P}$ such that $x \in C$.

**Theorem 4.** Suppose that each of the groups in $\mathcal{A}$ is of dimension $n - 1$. Then the coefficients $\alpha_{a, b}$ are weakly of the same sign as $(-1)^{n-a+1}$, and if there exists $C \in \mathcal{P}$ having dimension $a$ and order $b$, then $\alpha_{a, b} \neq 0$.

**Proof.** Let $C$ be such a coset and let $x$ be an element of $C$. Then $\mathcal{P}_x$ is isomorphic to the intersection lattice of the arrangement of hyperplanes in the tangent space to $T^n$ at $x$ consisting of the tangent hyperplanes to the groups $K_i$ at $x$. This intersection lattice is dual to a geometric (matroid) lattice having rank $n - a$. The Möbius invariant of
such a lattice is positive or negative, according as to whether the rank is even or odd. (See, for example [9].) Then \( \omega(C) = -\mu(C, T^n) \) has the same sign as \((-1)^{n-a+1} \). □

**Corollary 3.** Let \( K \) be as above, and suppose that \( f(K, k) \) is a polynomial. Then \( K \) is uni-parted.

**Proof.** In this case, by the theorem, there can be no coset \( C \) in \( P \) having order \( b > 1 \). □

### 4. Relation to Euclidean counting problems

There is a close relationship between the counting problems above and certain counting problems involving subsets of \( \mathcal{R}^n \). For \( \tilde{K} \subseteq \mathcal{R}^n \), define

\[
g(\tilde{K}, k) = |\{x \in [0, 1)^n : x \in \tilde{K} \text{ and } kx \in \mathbb{Z}^n\}|.
\]

Considering the canonical homomorphism \( \pi : \mathcal{R}^n \to \mathcal{T}^n \), it is clear that, for any set \( K \in \tilde{K}^n \) and for \( \tilde{K} = \pi^{-1}(K) \subseteq \mathcal{R}^n \), \( f(K, k) \) also gives the value of \( g(\tilde{K}, k) \). Here the fundamental region \([0, 1)^n\) can be replaced by any other fundamental region.

When attention is restricted to elements of \( \tilde{K}^n \), one gets the following theorem.

**Theorem 5.** Let \( \mathcal{A} \) be an arrangement of closed subgroups of \( \mathcal{R}^n \), each containing \( \mathbb{Z}^n \). Let \( \tilde{K} \subseteq \mathcal{R}^n \) be the union of the subgroups of \( \mathcal{A} \). Then \( g(\tilde{K}, k) \) is a quasi-polynomial having coefficients in \( \mathcal{R}_{\gcd} \). If \( a \) is a positive integer which is relatively prime to the quasi-period of the quasi-polynomial, then \( g(\tilde{K}, a) = a^n - \chi(\tilde{A}, a) \), where \( \tilde{A} \) is the arrangement of the linear subspaces which are connected components of the subgroups of \( \mathcal{A} \).

**Proof.** This follows immediately from Theorems 1, 2, and the comments preceding the statement of this theorem. □

Versions of the last sentence of Theorem 5 have been studied in many places. The genesis of these results seems to be in the work of Tutte, on chromatic polynomials, flow polynomials, and what we now call Tutte polynomials. See [8]. These results on graphs were generalized to regular matroids in [4]. These results are most closely related to Corollary 2 above. For a more recent version valid in the present generality, see Theorem 2.2 of Athanasiadis [1].

It has been noted by Blass and Sagan [3] that the subspaces of \( \mathcal{R}^n \) which are intersections of hyperplanes from the Weyl arrangement \( \mathcal{B}^n \) are well situated especially for integer lattice point counting problems involving the cubes \([-s, s]^n \) \((s = 1, 2, \ldots)\). We describe the relationship of their results to those of the preceding section.

Recall that \( \mathcal{B}^n \) consists of the following hyperplanes:

- (a) the \( n \) coordinate hyperplanes, \( \{(x_1, \ldots, x_n) : x_i = 0\} \), where \( 1 \leq i \leq n \);
- (b) the \( \binom{n}{2} \) hyperplanes \( \{(x_1, \ldots, x_n) : x_i = x_j\} \), where \( 1 \leq i < j \leq n \); and
- (c) the \( \binom{n}{2} \) hyperplanes \( \{(x_1, \ldots, x_n) : x_i = -x_j\} \), where \( 1 \leq i < j \leq n \).
These hyperplanes possess a certain property that will be used in the proof of the next theorem.

Given a closed subgroup \( \tilde{K} \) of \( \mathbb{R}^n \), let \( 0_{\tilde{K}} \) denote the connected component of \( \tilde{K} \) which contains the origin. Then \( 0_{\tilde{K}} \) is a vector space. Assume that \( \mathbb{Z}^n \subseteq \tilde{K} \), and consider the following property:

(*) For \( x = (x_1, \ldots, x_n) \in \tilde{K} \cap [-\frac{1}{2}, \frac{1}{2})^n \) letting \( y(x) = (y_1, \ldots, y_n) \) where

\[
y_i = \begin{cases} 
-\frac{1}{2} & \text{if } x_i = -\frac{1}{2}, \\
0 & \text{otherwise},
\end{cases}
\]

\( x - y(x) \in 0_{\tilde{K}} \).

(This implies that, for such \( x \), \( y(x) \) is also in \( \tilde{K} \).)

Suppose \( \tilde{K} \) satisfies (*). Let \( x \) be an element of \( \tilde{K} \). Then \( x \) is congruent to an element \( x' \in \tilde{K} \cap [-\frac{1}{2}, \frac{1}{2})^n \) modulo \( \mathbb{Z}^n \) and \( x' \) is congruent to \( y(x') \) modulo \( 0_{\tilde{K}} \). Thus each element in \( \tilde{K} \) is congruent modulo \( 0_{\tilde{K}} + \mathbb{Z}^n \subseteq \tilde{K} \) to a point in \( \frac{1}{2}\mathbb{Z}^n \). It follows if \( K = \pi(\tilde{K}) \subseteq \mathcal{T}^n \) then any coset of \( 0K \) in \( K \) has order 1 or 2.

Clearly the collection of subgroups \( \tilde{K} \) which have this property is closed under intersection. Also it is easy to verify that, for each \( H \in \mathcal{B}^n \), the group \( H + \mathbb{Z}^n \) has this property. (It can be shown that this collection consists of the subgroups of the form \( K = H + \mathbb{Z}^n \), where \( H \in \mathcal{B}^n \), of the form \( K = H + \frac{1}{2}\mathbb{Z}^n \), where \( H \in \mathcal{B}^n \) is of type (a), and intersections of these.)

**Theorem 6.** Let \( A \) be an arrangement of subspaces of \( \mathcal{R}^n \) each of which is an intersection of hyperplanes in \( \mathcal{B}^n \). Let \( \tilde{K} \) denote the union of the subspaces in the arrangement. Let

\[
h(k) = |\{x \in (-1/2, 1/2)^n \setminus \tilde{K} : (2k + 1)x \in \mathbb{Z}^n\}|.
\]

Then \( h(k) = \chi(A, 2k + 1) \).

**Proof.** We have

\[
h(k) = |\{x \in (-1/2, 1/2)^n \setminus \tilde{K} : (2k + 1)x \in \mathbb{Z}^n\}|
\]

\[
= k^n - |\{x \in \tilde{K} \cap (-1/2, 1/2)^n : (2k + 1)x \in \mathbb{Z}^n\}|.
\]

Using the property described above it is clear that

\[
\tilde{K} \cap (-1/2, 1/2)^n = (\tilde{K} + \mathbb{Z}^n) \cap (-1/2, 1/2)^n,
\]
so this coincides with
\[ k^n - \left| \{ x \in (\tilde{K} + \mathbb{Z}^n) \cap (-1/2, 1/2)^n : (2k + 1)x \in \mathbb{Z}^n \} \right| \]
which in turn coincides with
\[
k^n - \left| \{ x \in (\tilde{K} + \mathbb{Z}^n) \cap [-1/2, 1/2)^n : (2k + 1)x \in \mathbb{Z}^n \} \right| = k^n - g(\tilde{K}, 2k + 1).
\]

We must show that the quasi-period of \( g(\tilde{K}, k) \) is 1 or 2. Letting
\[ A = \{ \tilde{K}_i : 1 \leq i \leq m \}, \]
\[ K = \pi(\tilde{K}), \]
and \( K_i = \pi(\tilde{K}_i) \) for \( 1 \leq i \leq m \), we have that \( g(\tilde{K}, k) = f(K, k) \). Let \( K' \) be a coset in the coset poset of \( K \). Let \( \tilde{K} \) be the group it generates. By definition of the coset poset, \( \tilde{K} \) is an intersection of some of the groups \( K_i \); it follows that \( \tilde{K} = \pi^{-1}(\tilde{K}) \) is an intersection of some of the groups \( \tilde{K}_i \), and so possesses the property above. From the remark following (*), the coset \( K' \) is of order 1 or 2. By Theorem 3, \( f(K, k) \) has quasi-period 1 or 2.

The proof is completed by noting that \( 2k + 1 \) is relatively prime to the quasi-period, the coefficients being in \( \mathcal{R}_{gcd} \). \( \square \)

For additional related work, see [2,10].

5. Ehrhart quasi-polynomials

Given a bounded set \( P \subseteq \mathcal{R}^n \) we can consider the function on positive integers \( k \) given by
\[ \widehat{g}(k) = \left| \{ x \in P : kx \in \mathbb{Z}^n \} \right|. \]

If \( P \) is a convex polytope whose vertices have rational coordinates, or the relative interior of such a set, this function is a quasi-polynomial, called the Ehrhart quasi-polynomial of \( P \). If \( P \) is a convex polytope having vertices in \( \mathbb{Z}^n \), or the relative interior of such a set, then \( \widehat{g} \) is a polynomial of degree equal to the dimension of \( P \). We consider the Ehrhart quasi-polynomial of \( P \), where \( P \subseteq \mathcal{R}^n \) is the interior of a full-dimensional polytope having vertices with rational coordinates. Its Ehrhart quasi-polynomial has coefficients in \( \mathcal{R}_{per} \), but in general not in \( \mathcal{R}_{mult} \). Let \( S \) denote the semigroup generated by these functions under addition.

**Theorem 7.** Let \( K = \bigcup_{i=1}^{n} K_i \) be an element of \( \mathcal{K}^n \), where the \( K_i \)'s are \((n-1)\)-dimensional subgroups of \( \mathcal{T}^n \) whose intersection is finite. Then \( k^n - f(K, k) \in S \).

**Proof.** In this case, the complement of \( K \) is the disjoint union of open regions \( R \) having the property that \( R \) is the image \( \pi(P) \), where \( P \subseteq \mathcal{R}^n \) is the interior of an \( n \)-dimensional
polytope having vertices with rational coordinates. The projection \( \pi \), restricted to \( P \), is a bijection of \( P \) to \( R \). The cardinalities of \( \{x \in P : kx \in \mathbb{Z}^n\} \) and \( \{x \in R : kx = 0\} \) are equal, this function of \( k \) being the Ehrhart quasi-polynomial of \( P \). Summing over the regions \( R \), we get the desired conclusion. \( \Box \)

An interesting case arises when the regions \( R \) occurring in the proof are all equivalent by action of the unimodular group on \( T^n \). In this case, the Ehrhart quasi-polynomials which occur are equal, so \( k^n - f(K, k) \) is simply this Ehrhart quasi-polynomial multiplied by the number of regions \( R \). The analogue of this in Euclidean space is studied in [3], for the Weyl arrangements.

References