Three Rings of Polyhedral Simple Functions

Jim Lawrence

Department of Mathematical Sciences,
George Mason University,
Fairfax, VA 22030
and
National Institute of Standards and Technology,
Gaithersburg, MD 20899-8910

james.lawrence@nist.gov

We survey three ways to multiply elements of the additive subgroup of the group of real-valued functions on R^d which is generated by the indicator functions of polyhedra. In the resulting commutative rings, identities often correspond to useful techniques of decomposition of polyhedra. We are led immediately to various interesting topics, including Ehrhart polynomials, mixed volumes, Gram's relation, and transversal characteristics.

1. Introduction

Let S^d denote the group of *polyhedral simple functions on R^d*, the additive subgroup of the group of Z-valued functions on R^d which is generated by the indicator functions of polyhedra. Here we study three ways to introduce multiplication on S^d, each giving it the structure of a commutative ring. The purpose of this paper is to note parallels among these three constructions, involving identities in the rings and resulting methods of decomposition of convex polyhedra. These considerations lead immediately to the principle of inclusion-exclusion, the combinatorial form of Gram's relation, Ehrhart polynomials of polytopes, and other useful notions.

Each of the multiplications we consider arises from a binary operation on closed convex polyhedra; the three binary operations are intersection, convex hull of the union, and Minkowski addition.

For background on convex sets and polyhedra, consult the book by Stoer and Witzgall, [10].

2. The Principle of Inclusion-Exclusion

As the first example, illustrating the basic ideas, we describe a ring in which multiplication is related to intersection, and we use the ring structure to derive the principle of inclusion-exclusion.

If $P \subseteq R^d$ we let $[P]$ denote its indicator function, $[P] : R^d \to Z$:

$$[P](x) = \begin{cases} 1 & \text{if } x \in P, \\ 0 & \text{if } x \in P. \end{cases}$$

The (additive) group of *simple functions* consists of the functions $F : R^d \to Z$ of the form

$$F(x) = \sum_{i=1}^{n} \alpha_i [P_i](x),$$

where the α_i's are integers and the P_i's are sets in R^d. These are the Z-valued functions having finitely many values. In later sections, we will be interested in the subgroup of the group of simple functions consisting of the *polyhedral* simple functions, the functions having such a representation, in which the P_i's are polyhedra.

Here, a polyhedron is a finite union of sets which are relative interiors of convex polyhedra. Equivalently, it is an element of the Boolean lattice generated under intersection, union, and complementation by the closed halfspaces. The polyhedral simple functions are those functions $F : R^d \to Z$ having finitely many values and such that, for each $k \in Z$, the inverse image of k, the set $F^{-1}(k) = \{x \in R^d : F(x) = k\}$, is a polyhedron. The group of polyhedral simple functions on R^d is denoted by S^d.

In this section, the multiplication we describe is defined on the collection consisting of all the Z-valued simple functions on R^d; S^d forms a subring.

The operation under consideration in this section is intersection, $\cap$. Is there a multiplication, to be denoted by $\cdot$, on the group of simple functions which gives it the structure of a commutative ring, such that, whenever P and Q are sets in R^d, we have

$$[P] \cdot [Q] = [P \cap Q]?$$

Of course, the answer is "Yes"; for simple functions F, G, we take

$$(F \cdot G)(x) = F(x)G(x),$$

pointwise multiplication. For $F = [P]$ and $G = [Q]$, we have $F \cdot G = [P \cap Q]$.

Furthermore, this multiplication is unique. If

$$F = \sum_i \alpha_i [P_i] \text{ and } G = \sum_j \beta_j [Q_j],$$

then we must have

$$F \cdot G = \sum_{i,j} \alpha_i \beta_j [P_i \cap Q_j];$$

then $F \cdot G$ must be the function which, for $x \in R^d$, maps

$$x \mapsto \sum_{i,j} \alpha_i \beta_j [P_i \cap Q_j](x)$$
$$= \sum_{i,j} \alpha_i \beta_j [P_i](x)[Q_j](x)$$
$$= (\sum_i \alpha_i [P_i](x))(\sum_j \beta_j [Q_j](x))$$
$$= F(x)G(x).$$

Now suppose A_1, A_2, and B are sets in R^d, with $B = A_1 \cup A_2$. Then

$$([B] - [A_1]) \cdot ([B] - [A_2]) = 0,$$

as is clear, since, for any $x \in R^d$, evaluating the left-hand side yields $([B](x) - [A_1](x))([B](x) - [A_2](x))$, and

since $B = A_1 \cup A_2$, at least one of the integers $[B](x) - [A_1](x)$ and $[B](x) - [A_2](x)$ must be zero. (Here we use that the function on simple functions which takes F to $F(x)$—evaluation at x—is a homomorphism of the ring, and that the simple function F is zero if and only if, for each $x \in R^d$, $F(x) = 0$.) Expanding, we get

$$0 = [B] \cdot [B] - [B] \cdot [A_1] - [A_2] \cdot [B] + [A_1] \cdot [A_2]$$
$$= [B] - [A_1] - [A_2] + [A_1 \cap A_2],$$

or, for each $x \in R^d$,

$$[B](x) = [A_1](x) + [A_2](x) - [A_1 \cap A_2](x).$$

This yields the simple counting principle called the "principle of inclusion-exclusion" in the case of two sets, A_1, A_2: If B is finite then summing both sides of the last equation over all $x \in R^d$ (essentially a finite sum, since finiteness of B ensures that there are only finitely many $x \in R^d$ for which the values are nonzero), we obtain the cardinality of B in the equation

$$|B| = |A_1| + |A_2| - |A_1 \cap A_2|.$$

Similar consequences hold when summing or integrating other functions over a set B.

More generally, for an arbitrary number n of sets A_i, letting $B = A_1 \cup \cdots \cup A_n \subseteq R^d$, we have

$$([B] - [A_1]) \cdot ([B] - [A_2]) \cdot \ldots \cdot ([B] - [A_n]) = 0.$$

Expanding as before we get an expression for $[B]$ in terms of the indicator functions of the intersections of the A_i's:

$$[B] = \sum_{\substack{\Lambda \subseteq [n], \\ \Lambda \neq \varnothing}} (-1)^{|\Lambda|-1} [\bigcap_{i \in \Lambda} A_i].$$

3. Convex Hull and Gram's Relation

In this section, we consider what happens when we substitute the binary operation of taking the convex hull of the union for that of intersection (of the preceding section). Does there exist a multiplication $\vee$ on the additive group of polyhedral simple functions, S^d, such that, for the indicator functions of any nonempty closed convex polyhedra P and Q, the product is given by the indicator of their convex hull,

$$[P] \vee [Q] = [\mathrm{conv}(P \cup Q)]?$$

Indeed there is such a product.

In the preceding section it was not necessary to restrict the simple functions which were considered, to be in the group S^d of polyhedral simple functions. In this section and the next, this restrictive assumption will be made. We note, however, that we could equally well make one of two somewhat less restrictive assumptions; we could assume that the sets $F^{-1}(k)$ lie either in the Boolean lattice generated by the collection of open convex sets, or in that generated by the collection of closed convex sets. The group of polyhedral simple functions is a subgroup of each of these larger groups. See [6].

There is a very useful homomorphism $\bar{\chi} : S^d \to Z$. We briefly describe how to obtain it, using the Euler characteristic.

The (topological) Euler characteristic χ is defined on polyhedra by the following properties:

1. $\chi(\emptyset) = 0$;
2. If P is the relative interior of a nonempty convex polyhedron of dimension k then $\chi(P) = (-1)^k$;
3. If P is partitioned into polyhedra P_i ($1 \leq i \leq m$), so that $P = \cup_i P_i$, and, for $i \neq j$, $P_i \cap P_j = \emptyset$, then $\chi(P) = \Sigma_i \chi(P_i)$.

Any polyhedron has an Euler characteristic, and if $P,Q \in R^d$ are homeomorphic polyhedra, then $\chi(P) = \chi(Q)$.

If $P \subseteq R^d$ is a nonempty open convex polyhedron then $\chi(P) = (-1)^d$, while $\chi(\emptyset) = 0$. These and the fact that χ has the additivity property, $\chi(P \cup Q) + \chi(P \cap Q) = \chi(P) + \chi(Q)$ for any polyhedra P,Q, determine it uniquely.

See [7] for an easy proof of the existence of the function χ on polyhedra and its use in establishing Euler's relation for the f-vector of a convex polytope. In this paper we have restricted the discussion to polyhedral simple functions; however, most of the results hold more generally for either the group of simple functions generated by the indicator functions of open convex sets, or that generated by indicator functions of closed convex sets. Two useful tools for accomplishing these extensions may be found in [4]; they are additive functions on the Boolean lattices, namely, the Euler characteristic for the family of open convex sets, which has value 1 on all nonempty open convex sets, and the Euler characteristic for the family of closed convex sets, which has value 1 on all nonempty closed convex sets (both functions having value 0 on the empty set). The first of these Euler characteristics, when restricted to polyhedra, yields the function χ above multiplied by

a factor of $(-1)^d$, while the second yields the function χ' described below. These functions differ only by a multiplicative factor of $(-1)^d$ when applied to bounded polyhedra. See also [6], where the relationship between the two functions is made clear by making use of the "Sallee-Shephard mapping" which is introduced in that paper.

If P is a nonempty compact convex polyhedron—a nonempty convex polytope—then $\chi(P) = 1$, while if P is a pointed unbounded closed convex polyhedron then $\chi(P) = 0$. There is a second "Euler characteristic" χ' characterized by the additivity property, $\chi'(\emptyset) = 0$, and $\chi'(P) = 1$ for any nonempty closed convex polyhedron P. For any polyhedron P, $\chi'(P)$ may be obtained by taking $\chi'(P) = \chi(P) + \chi(P \cap \partial(\lambda C^d))$, for sufficiently large $\lambda \in R$, where C^d denotes the cube, $C^d = \{x = (x_1, ..., x_d) \in R^d : -1 \leq x_i \leq 1 \text{ for } 1 \leq i \leq d\}$ and $\partial(\lambda C^d)$ represents the boundary of the dilation by a factor of λ of the cube. Here we dispense with χ in favor of χ', as being better suited to the current needs. It has value 1 on every nonempty closed convex polyhedron, while $\chi'(\emptyset) = 0$; and these properties together with additivity characterize it. However it is not invariant under homeomorphism.

Given $F \in S^d$ and $k \in Z$, the inverse image $F^{-1}(k)$ is a polyhedron, since $F \in S^d$; and it is empty for all but finitely many integers k. Therefore, we may define

$$\bar{\chi}(F) = \sum_{k \in Z} k \chi'(F^{-1}(k)),$$

essentially a finite sum. Note that since the nonempty sets of the form $F^{-1}(k)$ partition R^d,

$$\sum_{k \in Z} \chi'(F^{-1}(k)) = \chi'(R^d) = 1.$$

Lemma 1 *The function $\bar{\chi} : S^d \to Z$ is a group homomorphism. If P is a nonempty closed convex polyhedron then $\bar{\chi}([P]) = 1$.*

Proof. That $\bar{\chi} : S^d \to Z$ is a group homomorphism is easily verified:

$$\bar{\chi}(F + G) = \sum_{k} k \chi'(\{x \in R^d : F(x) + G(x) = k\})$$

$$= \sum_{a,b} (a+b) \chi'(F^{-1}(a) \cap G^{-1}(b))$$

$$= \sum_{a} \sum_{b} a \chi'(F^{-1}(a) \cap G^{-1}(b))$$

$$+ \sum_{b} \sum_{a} b \chi'(F^{-1}(a) \cap G^{-1}(b)),$$

which, since the sets $F^{-1}(a) \cap G^{-1}(b)$, for fixed a, form a partition of $G^{-1}(b)$, and for fixed b, form a partition of

$F^{-1}(a)$, may be continued,

$$= \sum_a a\chi'(F^{-1}(a)) + \sum_b b\chi'(G^{-1}(b))$$

$$= \bar{\chi}(F) + \bar{\chi}(G).$$

If P is a closed convex polyhedron then, letting F denote $[P]$, $\bar{\chi}(F) = \chi'(P) = 1$, by definition.   •

The collection of evaluation mappings, used in the preceding section (but perhaps "transparently, to the user") have simple properties which made them useful there. For $x \in R^d$, denote by ε_x the mapping $\varepsilon_x : S^d \to Z$ which maps $F \mapsto F(x)$, for $F \in S^d$. These functions are group homomorphisms; they are ring homomorphisms, when S^d is considered as a ring under intersection multiplication. Also, if $F \in S^d$ is not the zero function, then there exists an evaluation homomorphism ε_x such that $\varepsilon_x(F) \neq 0$. Equivalently, if $F, G \in S^d$ then $F = G$ if and only if, for each $x \in R^d$, $\varepsilon_x(F) = \varepsilon_x(G)$. We say that the evaluation homomorphisms *distinguish elements* of S^d. (Some authors would say that the set of evaluation homomorphisms constitutes a *separating set of functions*.) Using $\bar{\chi}$, we construct another collection of homomorphisms which distinguish elements of S^d.

Given an open halfspace $H \subseteq R^d$, define

$$\varphi_H(F) = \bar{\chi}([H] \cdot F) \text{ for } F \in S^d.$$

If P is a nonempty closed convex polyhedron we have

$$\varphi_H([P]) = \begin{cases} 1 & \text{if } P \subseteq H \\ 0 & \text{otherwise,} \end{cases}$$

using

$$\varphi_H[P] = \bar{\chi}([H \cap P]) = \bar{\chi}([(H \cup \partial H) \cap P]) - \bar{\chi}([(\partial H) \cap P]),$$

which is easy to compute, since the arguments of $\bar{\chi}$ in the last expression are indicator functions of closed convex polyhedra (possibly empty).

Lemma 2 *The mappings φ_H are group homomorphisms. The collection of such mappings, together with $\bar{\chi}$, distinguish elements in S^d. If P, Q are nonempty closed convex polyhedra and H is an open halfspace, then*

$$\varphi_H([\text{conv}(P \cup Q)]) = \varphi_H([P])\varphi_H([Q]).$$

Proof. The first and last sentences of the lemma are immediate from what has just been stated and the prop-

erties of $\bar{\chi}$. For the middle sentence, we refer the reader to Theorem 12 of [6], from which it can be easily derived.   •

In Theorem 1 we see that convex hull of the union yields a multiplicative structure on S^d.

Theorem 1 *There is a unique multiplication $\vee$ on S^d, making S^d into a (commutative) ring, such that, whenever P and Q are nonempty closed convex polyhedra, $[P] \vee [Q] = [\text{conv}(P \cup Q)]$. The mappings $\varphi_H : S^d \to Z$ and $\bar{\chi} : S^d \to Z$ are ring homomorphisms.*

Proof. As in the case of intersection, if such a multiplication exists, it is unique; for if

$$F = \sum_i \alpha_i[P_i] \text{ and } G = \sum_j \beta_j[Q_j],$$

where the P_i's and Q_j's are nonempty closed convex polyhedra, then

$$F \vee G = \sum_{i,j} \alpha_i \beta_j [P_i] \vee [Q_j]$$

$$= \sum_{i,j} \alpha_i \beta_j [\text{conv}(P_i \cup Q_j)].$$

We use this as the definition for arbitrary $F, G \in S^d$ and show that it is well-defined. Denote the right-hand side in this equation by J. We have:

$$\varphi_H(J) = \sum_{i,j} \alpha_i \beta_j \chi'(H \cap \text{conv}(P_i \cup Q_j))$$

$$= \sum_{i,j} \alpha_i \beta_j \chi'(H \cap P_i)\chi'(H \cap Q_i)$$

$$= \sum_i \alpha_i \chi'(H \cap P_i) \sum_j \beta_j \chi'(H \cap Q_i)$$

This depends only on F and G, not on their representations, so, given different representations, resulting in J' rather than J in the above, the value of $\varphi_H(J')$ would be unchanged: $\varphi_H(J') = \varphi_H(F)\varphi_H(G) = \varphi_H(J)$. Replacing φ_H by $\bar{\chi}$ in the above, we similarly get $\bar{\chi}(J') = \bar{\chi}(J)$. From this and the fact that the homomorphisms φ_H, $\bar{\chi}$ distinguish elements of S^d it follows that $J' = J$, so that $F \vee G$ is well-defined by the above expression.

We have seen that $\varphi_H(F \vee G) = \varphi_H(F)\varphi_H(G)$, so φ_H is a ring homomorphism. That $\bar{\chi}$ is also a ring homomorphism can be verified similarly without difficulty.   •

We use arithmetic in this ring to verify the combinatorial form of Gram's relation, in Theorem 2, below.

Lemma 3 *Let $P \subseteq R^d$ be a nonempty convex polytope and let $C_1, ..., C_n$ be the cones emanating from its vertices generated by P. Then*

$$([C_1] - [P]) \vee ([C_2] - [P]) \vee \cdots \vee ([C_n] - [P]) = 0.$$

Proof. Suppose H is an open halfspace. We consider the effect of applying φ_H to the left-hand side. $P \subseteq H$ if and only if there is a vertex of P for which the corresponding cone C_j is contained in H. Therefore, if $P \not\subset H$ then $\varphi_H([C_i]) = \varphi_H(P) = 0$ for each i; and, otherwise, for this j we have $\varphi_H([P]) - \varphi_H([C_j]) = 0$. In each case we have

$$\varphi_H \big(([C_1] - [P]) \vee ([C_2] - [P]) \vee \cdots \vee ([C_n] - [P]) \big) = 0.$$

This holds for each open halfspace H. Also, it is clear that $\bar{\chi}$, when applied to the left-hand side, yields 0. Since the mappings φ_H, $\bar{\chi}$ distinguish elements of S^d, the stated equality follows. •

Let P be as in the lemma, and suppose that the vertices of P are $v_1, ..., v_n$ and the cones at the vertices are, as before, $C_1, ..., C_n$. For each nonempty face F of P, let C_F denote the cone generated by P from F. It is easily verified that for $\Lambda \subseteq [n]$, $\Lambda \neq \emptyset$, $\mathrm{conv}(\cup_{i \in \Lambda} C_i) = C_F$, where F is the smallest face of P containing $\{v_i : i \in \Lambda\}$.

Theorem 2 *(Gram's relation, combinatorial form.)*

$$[P] = \sum_{\substack{F, \text{ a face} \\ \text{of } P, F \neq \emptyset}} (-1)^{\dim(F)-1} [C_F].$$

Proof. Expanding the expression in the lemma leads immediately to the equation

$$[P] = \sum_{\substack{\Lambda \subseteq [n], \\ \Lambda \neq \emptyset}} (-1)^{|\Lambda|-1} [\mathrm{conv}(\bigcup_{i \in \Lambda} C_i)].$$

For a nonempty face F of P, let Λ_F denote the collection of subsets $\Lambda \subseteq [n]$ such that the smallest face containing $\{v_i : i \in \Lambda\}$ is F. The sets Λ_F, for F a nonempty face, form a partition of the set of nonempty subsets of $[n]$. We then have

$$[P] = \sum_{\substack{F, \text{ a face} \\ \text{of } P, F \neq \emptyset}} \sum_{\Lambda \in \Lambda_F} (-1)^{|\Lambda|-1} [C_F].$$

The result now follows from the fact that

$$\sum_{\Lambda \in \Lambda_F} (-1)^{|\Lambda|-1} = (-1)^{\dim(F)-1},$$

which can be derived as a consequence of Euler's relation for the *f*-vectors of convex polytopes. •

This theorem can be generalized in a way, by making use of the notion of the "transversal characteristic" of [6]. Given a nonempty finite collection $C = \{P_1, ..., P_n\}$ of closed convex polyhedra, the *transversal characteristic* of C is the element of S^d given by

$$\tau(C) = \sum_{\substack{\Lambda \subseteq [n], \\ \Lambda \neq \emptyset}} (-1)^{|\Lambda|-1} [\mathrm{conv}(\bigcup_{i \in \Lambda} P_i)].$$

A convex set C is a *transversal* of C if, for each $i \in [n]$, $C \cap P_i \neq \emptyset$.

Theorem 3 *Two finite collections of closed convex polyhedra have the same convex transversals if and only if their transversal characteristics are equal.*

Proof. Let $C = \{P_1, ..., P_n\}$, as above. If, for some i, $P_i = \emptyset$, then C has no convex transversals; and in this case it is easy to see that $\tau(C) = 0$. If no P_i is empty then certainly convex transversals of C exist; also, in this case, $\bar{\chi}(\tau(C)) = 1$. Therefore the theorem holds whenever one of the two collections has $\emptyset$ as an element. We may assume that this is not the case.

It is not difficult to verify that two collections have the same convex transversals if and only if the set of closed halfspaces which are transversals are the same for each.

Let H be an open halfspace. It is clear that

$$\varphi_H(\tau(C)) = \sum_{\substack{\Lambda \subseteq [n], \\ \Lambda \neq \emptyset}} (-1)^{|\Lambda|-1} \varphi_H([\mathrm{conv}(\bigcup_{i \in \Lambda} P_i)]).$$

Suppose then that H is an open halfspace whose complement is a transversal of C. In this case H contains none of the P_i's, so $\varphi_H(\tau(C)) = 0$. If, however, the complement of H is not a transversal of C, letting $\Gamma = \{i \in [n] : P_i \subseteq H\}$, we have

$$\varphi_H([\mathrm{conv}(\bigcup_{i \in \Lambda} P_i)]) = \begin{cases} 1 & \text{if } \Lambda \subseteq \Gamma \\ 0 & \text{otherwise.} \end{cases}$$

Then the summation reduces to

$$\varphi_H(\tau(C)) = \sum_{\substack{\Lambda \subseteq \Gamma, \\ \Lambda \neq \emptyset}} (-1)^{|\Lambda|-1},$$

which has value 1, Γ being nonempty. Summarizing,

$$\varphi_H(\tau(C)) = \begin{cases} 0 & \text{if the complement of H is a transversal} \\ 1 & \text{if it is not.} \end{cases}$$

It follows immediately that collections C and $\mathcal{D}$ of nonempty polytopes have the same transversals if and only if, for each open halfspace H, the values of φ_H on their transversal characteristics are equal. Since also $\bar{\chi}(C) = \bar{\chi}(\mathcal{D}) = 1$, and the homomorphisms φ_H, $\bar{\chi}$ distinguish elements of S^d, this happens if and only if their transversal characteristics are equal. •

Gram's relation is obtained from Theorem 3 by applying this theorem to the collection $\{C_1, ..., C_n\}$ of cones emanating from the vertices of P. This collection has the same convex transversals as $\{P\}$.

We call a family of convex sets *clustered* if each transversal is a transversal of the intersection of the family. In this case, as in Gram's relation, the transversal characteristic is the indicator function of the intersection.

4. Minkowski Addition as the Product

Finally, we consider the existence of and a use for the multiplication *, for which, if P and Q are nonempty closed convex polyhedra in R^d, $[P] * [Q] = [P + Q]$. This ring, studied by Groemer in [3], is called a "Minkowski ring" in [2] and [5]. The "polytope algebra" studied by McMullen in [8] and used by him to study the "g-theorem" for simplicial polytopes is a homomorphic image of a Minkowski ring.

It is necessary to introduce yet another collection of homomorphisms distinguishing elements of S^d. This time, the range will also be different. We denote by T the additive group of expressions which are finite sums of the form $\Sigma_i \alpha_i t^{\rho_i}$, where the ρ_i's are real numbers and the α_i's are integers. Elements of T may be viewed as functions on the nonnegative real numbers, and then T forms a ring, with pointwise multiplication as the product.

For each linear function $\lambda : R^d \to R$, we describe a homomorphism $\mu_\lambda : S^d \to T$. We define μ_λ to be the (unique) homomorphism such that, for each nonempty closed convex polyhedron P,

$$\mu_\lambda([P]) = \begin{cases} t^m & \text{if } m = \max\{\lambda(x) : x \in P\} \\ 0 & \text{otherwise.} \end{cases}$$

Lemma 4 *The homomorphism μ_λ is well-defined by the above. The homomorphisms of this form distinguish elements of S^d.*

Proof. Note that $Z \subseteq T$ and if the linear functional λ is identically zero then μ_λ is $\bar{\chi} : S^d \to Z \subseteq T$.

Suppose $\lambda \neq 0$. Let m be a real number. For any real number r, let $H(r)$ be the open halfspace $H(r) = \{x \in R^d : \lambda(x) < r\}$. For $F \in S^d$, consider

$$\alpha_m(F) = \lim_{\varepsilon \to 0^+} \varphi_{H(m+\varepsilon)}(F) - \varphi_{H(m)}(F).$$

It is easy to see that the limit exists, the function $\varphi_{H(m+\varepsilon)}(F)$ being constant for $\varepsilon > 0$ sufficiently small. Clearly $\alpha_m : S^d \to Z$ is a group homomorphism. Furthermore, if P is a closed convex polyhedron, then

$$\alpha_m([P]) = \begin{cases} 1 & \text{if } m = \max\{\lambda(x) : x \in P\} \\ 0 & \text{otherwise.} \end{cases}$$

It follows that $\mu_\lambda(F) = \Sigma_m \alpha_m(F) t^m$ for $F \in S^d$, a group homomorphism.

If $H = \{x \in R^d : \lambda(x) < m\}$, we can retrieve $\varphi_H(F)$ from $\mu_\lambda(F)$: Letting $\mu_\lambda(F) = \Sigma_{m'} \alpha_{m'} t^{m'}$, we have $\varphi_H(F) = \Sigma\{\alpha_{m'} : m' > m\}$. From this and the fact that the φ_H's and $\bar{\chi}$ distinguish elements, it follows that the μ_λ's do so, as well.

In Theorem 4 we see that Minkowski addition yields a multiplicative structure on S^d.

Theorem 4 *There is a unique multiplication * on S^d such that, for closed convex polyhedra P and Q, $[P] * [Q] = [P + Q]$, making S^d into a commutative ring. The mappings $\mu_\lambda : S^d \to T$ and $\bar{\chi} : S^d \to Z$ are ring homomorphisms.*

Proof. The proof proceeds in a manner similar to that of Theorem 1. We skip the details, except to note that for nonempty closed convex polyhedra P and Q and a linear functional λ, $\mu_\lambda([P + Q]) = \mu_\lambda([P])\mu_\lambda([Q])$: λ is bounded above on $P + Q$ if and only if it is bounded above on P and on Q, in which case, if m_{P+Q}, m_P, and m_Q represent the three maximum values, we certainly have $m_{P+Q} = m_P + m_Q$. •

Using the arithmetic of this ring will lead us quickly to the Ehrhart polynomials.

Lemma 5 *Let $P \subseteq R^d$ be a convex polytope having vertices $v_1, ..., v_n$. Then, in the Minkowski ring,*

$$([P] - [\{v_1\}]) * ([P] - [\{v_2\}]) * \cdots * ([P] - [\{v_n\}]) = 0.$$

Proof. The proof proceeds in a manner similar to that of Lemma 3. This time we apply μ_λ and note that the maximum of λ on a convex polytope occurs at a vertex. •

In the following theorem it will be proven that a certain sequence of complex numbers, $s_0, s_1, s_2, ...$, is the sequence of values at the nonnegative integers of a polynomial. We briefly review the technique to be used to establish this. Suppose $s_0, s_1, s_2, ...$, is a sequence of complex numbers. We denote the sequence by the symbol s_*. We form a new sequence Δs_*, by taking differences of consecutive values: $s_1 - s_0, s_2 - s_1, s_3 - s_2, ... $ It is true that s_* is the sequence of values of a polynomial if and only if Δs_* is the sequence of values of a polynomial; and, if s_* is not already the sequence of zeroes, then the degree of the polynomial representing Δs_* is one less than that representing s_* (taking the degree of the zero polynomial to be –1). Using this "difference" operator Δ multiple times, we see that s_* is the sequence of values of a polynomial of degree at most $n - 1$ if and only if $\Delta^n s_*$ is the sequence of 0's. We shall also make use of the fact that $\Delta^n s_*$ is $t_0, t_1, t_2, ...$, where

$$t_j = \sum_{k=0}^{n} (-1)^k \binom{n}{k} s_{n-k+j} \quad \text{for } j = 0,1,2,....$$

Theorem 5 *Let $P \subseteq R^d$ be a convex polytope and let $\mathcal{P}$ denote the subring of S^d generated by $[P]$ and the elements $[\{x\}]$, for $x \in R^d$. Suppose γ is a homomorphism of the abelian groups which maps $\mathcal{P}$ to the additive group of complex numbers. Suppose that, for each vertex v of P and each $F \in \mathcal{P}$, $\gamma(F * [v]) = \gamma(F)$. Then the sequence s_*, where $s_k = \gamma([P]^k)$, is a polynomial of degree at most d.*

Proof. Note that $F * [\{v\}]$ is the function taking $x \mapsto F(x - v)$.

Expanding the left-hand side in the equation of Lemma 5 and multiplying by $[P]^j$, we obtain

$$\sum_{\Lambda \subseteq [n]} (-1)^{|\Lambda|} (\prod_{i \in \Lambda} [\{v_i\}])[P]^{n-|\Lambda|+j} = 0.$$

Here the products are of course multiplications in the Minkowski ring. Applying γ and using the fact that $\gamma(F) = \gamma(F * [\{v_i\}])$ for any $F \in S^d$ and any i, we get

$$\sum_{\Lambda \subseteq [n]} (-1)^{|\Lambda|} \gamma([P]^{n-|\Lambda|+j}) = 0,$$

which, upon counting sets, reduces to

$$\sum_{k=0}^{n} (-1)^k \binom{n}{k} \gamma([P]^{n-k+j}) = 0;$$

then

$$\sum_{k=0}^{n} (-1)^k \binom{n}{k} s_{n-k+j} = 0.$$

Comparing this with the expression preceding the statement of the theorem, we see that s_* is the sequence of values of a polynomial of degree at most $n - 1$.

We observe that the degree is actually no more than d. From a triangulation of P using simplexes having only vertices among those of P, $[P]$ can be written as a sum-and-difference of indicator functions of simplexes. The sequence s_* of the theorem is then the sum-and-difference of those of the simplexes. Each of these is the sequence of values of a polynomial of degree at most d, so the same is true of s_*. •

Note that the group homomorphism γ need not be a ring homomorphism. It is easy to produce homomorphisms γ having the property required by the theorem. Here are two examples.

1. Let Q be a second convex polytope. For $F \in \mathcal{P}$, let

$$\gamma(F) = \int_{R^d} [Q] * F d\mu$$

where μ is ordinary Lebesgue measure.

2. Assume that the polytope P has only vertices in Z^d. For $F \in \mathcal{P}$, let

$$\gamma(F) = \sum_{z \in Z^d} F(z).$$

This is essentially a finite sum, since any element of $\mathcal{P}$ has bounded support.

In the first case, the terms of the sequence s_* are the volumes of the polytopes $Q + kP$, and the coefficients of the polynomial of the theorem, properly normalized, are the mixed volumes of P and Q ([3]); in the second, the terms are the cardinalities of the sets $Z^d \cap kP$, and the polynomial is the Ehrhart polynomial of P.

The Minkowski ring S^d has a multiplicative identity element, $[\{0\}]$, the function having value 1 at the origin and 0 elsewhere. The indicator functions of nonempty polytopes are invertible: $[P]^{-1} = (-1)^{\dim(P)}[-P^o]$, where $-P^o$ is the reflection through the origin of the relative interior P^o of P. It is a simple extension of the theorem to show that the doubly infinite sequence s_* having $s_k = \gamma([P]^k)$ for all $k \in Z$ is a polynomial. Applied to Ehrhart polynomials, so that P and γ are as in the second case, we have that $s^k = |Z^d \cap kP|$ for $k \geq 0$, and $s_k = (-1)^{\dim(P)}|Z^d \cap (-k)P^o|$, when $k < 0$. That the one polynomial serves both sequences is the reciprocity theorem studied by Ehrhart in [1], albeit in somewhat greater generality than is here described, and again by Stanley in [9].

Acknowledgment

5. References

[1] E. Ehrhart, Sur un problèm e de géométrie diophantienne linéaire. I. Polyèdres et réseaux, J. Reine Angew. Math. **226** 1-29 (1967).

[2] K. G. Fischer and J. Shapiro, The prime ideal structure of the Minkowski ring of polytopes, J. Pure Appl. Algebra **78**, 239-251 (1992).

[3] H. Groemer, Minkowski addition and mixed volumes, Geom. Dedicata **6**, 141-163 (1977).

[4] V. Klee, The Euler characteristic in combinatorial geometry, Amer. Math. Monthly **70**, 119-127 (1963).

[5] J. Lawrence, Minkowski rings. (Unpublished manuscript, 1986.)

[6] J. Lawrence, Valuations and polarity, Discrete Comput. Geom. **3**, 307-324 (1988).

[7] J. Lawrence, A short proof of Euler's relation for convex polytopes, Can. Math. Bull. **40**, 471-474 (1997).

[8] P. McMullen, Separation in the polytope algebra, Beiträge Algebra Geom. **34**, 15-30 (1993).

[9] R. Stanley, Combinatorial reciprocity theorems, Advan. Math. **14**, 194-253 (1974).

[10] J. Stoer and C. Witzgall, Convexity and Optimization in Finite Dimensions, Springer-Verlag (1970).

About the author: Jim Lawrence is a professor in the Department of Mathematical Sciences at George Mason University, where he has taught since 1983. Since 1986, he has been a Faculty Appointee at NIST. His first affiliation with NIST (1977-79, then the National Bureau of Standards) was as an NBS/NRC Postdoctoral Research Associate, with co-advisers Alan Goldman and Christoph Witzgall. The National Institute of Standards and Technology is an agency of the Technology Administration, U.S. Department of Commerce.