Ehrhart's theorem on numbers of lattice points in polytopes and the reciprocity relation

Martin Klazar

May 20, 2015

A *polytope* $P \subset \mathbb{R}^d$ is a convex hull of a finite set $A \subset \mathbb{R}^d$,

$$P = P(A) = \mathrm{conv}(A) = \{\textstyle\sum_{a\in A} \lambda_a a \mid \lambda_a \in \mathbb{R}_{\ge 0}, \sum_{a\in A} \lambda_a = 1\}\ .$$

For $M \subset \mathbb{R}^d$ and $n \in \mathbb{N}_0 = \{0, 1, 2, \dots\}$,

$$nM = \{nx = (nx_1, nx_2, \dots, nx_d) \in \mathbb{R}^d \mid x \in M\}\ .$$

By $\dim M$ we denote the minimum dimension of an affine subspace of $\mathbb{R}^d$ containing M and write $S = S(M)$ for the corresponding unique subspace. We prove the following theorem and proposition.

Theorem 0.1 (Ehrhart, 1962). *Let $A \subset \mathbb{Q}^d$ be finite and $m \in \mathbb{N} = \{1, 2, \dots\}$ satisfy $mA \subset \mathbb{Z}^d$. Then there is a quasi-polynomial $q(x) \in \mathbb{Q}[x]^m$ with rational coefficients and period m such that for every $n \in \mathbb{N}_0$,*

$$|\mathbb{Z}^d \cap nP(A)| = q(n)\ .$$

Moreover, the maximum degree of a component of $q(x)$ equals $\dim A$.

Proposition 0.2 (reciprocity relation). *If $q(x)$ is the quasi-polynomial of the previous theorem then for every $n \in \mathbb{N}_0$,*

$$q(-n) = (-1)^{\dim A} |\mathbb{Z}^d \cap nP(A)^o|$$

where $P(A)^o$ is the relative interior of $P(A)$ in $S(A)$.

Recall that a quasi-polynomial $q:\ \mathbb{Z} \to \mathbb{C}$ with period m is given by an m-tuple of polynomials $p_i(x)$, $i = 1, 2, \dots, m$, so that $q(n) = p_i(n)$ for every $n \in \mathbb{Z}$ congruent to i modulo m.

The proofs are based on the three propositions below. A *cone* $K \subset \mathbb{R}^d$ is determined by a finite set $A \subset \mathbb{R}^d_{\ge 0}$ by

$$K = K(A) = \{\textstyle\sum_{a\in A} \lambda_a a \mid \lambda_a \in \mathbb{R}_{\ge 0}\}\ .$$

It is *elementary* if A consists of linearly independent vectors; the set

$$T = T_K = \{\sum_{a\in A} \lambda_a a \mid \lambda_a \in [0,1)\}$$

is then the *fundamental parallelepiped of* K. For $M \subset \mathbb{R}^d$ we define the generating function of (the lattice points lying in) M as the formal series

$$F_M(\overline{x}) = F_M(x_1, x_2, \ldots, x_d) = \sum_{a\in\mathbb{Z}^d\cap M} \overline{x}^a = \sum_{(a_1,\ldots,a_d)\in\mathbb{Z}^d\cap M} x_1^{a_1} x_2^{a_2} \ldots x_d^{a_d} \ .$$

For every cone, $F_K \in \mathbb{Z}[[x_1, \ldots, x_d]]$ is a formal power series in d variables.

Proposition 0.3. *If $K = K(A) \subset \mathbb{R}^d$ is an elementary cone with $A \subset \mathbb{N}_0^d$ and fundamental parallelepiped T, then*

$$F_K(\overline{x}) = \frac{p(\overline{x})}{\prod_{a\in A}(1-\overline{x}^a)},\ p(\overline{x}) = F_T(\overline{x}) \in \mathbb{Z}[\overline{x}] \ .$$

Proof. K is partitioned into the shifts $c+T$ of T by all nonnegative integral linear combinations $c = \sum_{a\in A} c_a a$, $c_a \in \mathbb{N}_0$, so (disjoint union)

$$K = \bigcup_c (c+T) \ .$$

It follows from the fact that the elements of K one-to-one correspond to the expressions $\sum_{a\in A} \lambda_a a$ with $\lambda_a \geq 0$ (the elements of A are linearly independent), and $\lambda_a = \lfloor\lambda_a\rfloor + \{\lambda_a\} = c_a + \{\lambda_a\}$, $c_a \in \mathbb{N}_0$ and $\{\lambda_a\} \in [0,1)$. Since

$$F_{c+T}(\overline{x}) = \prod_{a\in A} \overline{x}^{c_a a} \cdot F_T(\overline{x}) = F_T(\overline{x}) \prod_{a\in A} (\overline{x}^a)^{c_a} \ ,$$

formal geometric series yields the stated formula:

$$F_K(\overline{x}) = \sum_c F_{c+T}(\overline{x}) = F_T(\overline{x}) \prod_{a\in A} \sum_{c_a=0}^{\infty} (\overline{x}^a)^{c_a} = F_T(\overline{x}) \prod_{a\in A} \frac{1}{1-\overline{x}^a} \ .$$

□

A *simplicial complex* $\mathcal{S}$ on a set X is a hereditary system of subsets of X, that is, $\mathcal{S} \subset \exp(X)$ and $A \subset B \in \mathcal{S} \Rightarrow A \in \mathcal{S}$. Clearly, $\mathcal{S}$ is determined by its maximal elements $A_1, A_2, \ldots, A_t$, and we write $\mathcal{S} = \mathcal{S}(A_1, A_2, \ldots, A_t)$.

Proposition 0.4 (triangulation of K). *For every finite set $A \subset \mathbb{R}^d_{\geq 0}$ there is a simplicial complex $\mathcal{S} = \mathcal{S}(A_1, A_2, \ldots, A_t)$ on A such that always $|A_i| =$* $\dim K(A)$*, all cones $K(A_i)$ (and hence all cones $K(B)$, $B \in \mathcal{S}$) are elementary,*

$$K(A) = \bigcup_{i=1}^{t} K(A_i) \quad \textit{and} \quad B, C \in \mathcal{S} \Rightarrow K(B) \cap K(C) = K(B\cap C) \ .$$

Proof. Let $K = K(A)$. We proceed by induction on $|A|$ and assume (as we may) that A is minimal with respect to generating K. The claim holds if $|A| = \dim K$: then K is elementary and $\mathcal{S} = \mathcal{S}(A)$ works. Let $|A| > \dim K$. We take any $a \in A$ and set $A' = A\backslash\{a\}$. Then $K(A')$ is a strict subset of K but $\dim K(A') = \dim K$ and by induction A' has the required simplicial complex $\mathcal{S}(A_1, \dots, A_s)$. We claim that there is a set B such that $a \in B \subset A$, $|B| = \dim K$, $K(B)$ is elementary, $K = K(A') \cup K(B)$, and $K(A') \cap K(B) = K(B\backslash\{a\})$. Then $\mathcal{S}(A_1, \dots, A_s, B)$ is the required simplicial complex on A.
[to be continued] □

Proof of Ehrhart's theorem. We move $P = P(A)$ by an integral shift in the nonnegative orthant of $\mathbb{R}^d$, thus we may assume that A is a finite nonempty subset of $\mathbb{Q}^d_{\geq 0}$ and $mA \subset \mathbb{N}_0^d$. We denote $e = \dim A = \dim P$, so $0 \leq e \leq d$. We consider the cone

$$K = K(B) \subset \mathbb{R}^{d+1}_{\geq 0},\ B = \{m(a, 1) = (ma_1, \dots, ma_d, m) \mid a \in A\} \subset \mathbb{N}_0^{d+1} .$$

Clearly, $\dim K = e + 1$. Also, $c \in \mathbb{Z}^d \cap nP$ iff $(c, n) \in \mathbb{Z}^{d+1} \cap K$, and $|\mathbb{Z}^d \cap nP|$ equals to the number of the lattice points lying in the section of K by the hyperplane $x_{d+1} = n$. In terms of generating functions,

$$f_P(x) := \sum_{n\geq 0} |\mathbb{Z}^d \cap nP| x^n = F_K(x_1, \dots, x_{d+1})\,|_{x_1=\cdots=x_d=1, x_{d+1}=x} .$$

Using Proposition 0.4, we take the triangulation $K_i = K(B_i)$, $i = 1, 2, \dots, t$, of K into $(e + 1)$-dimensional elementary cones. The inclusion-exclusion principle and Propositions 0.4 and 0.3 give ($[t] = \{1, 2, \dots, t\}$ and for $I \subset [t]$ we denote $K_I = K(B_I)$, $B_I = \bigcap_{i\in I} B_i$, so $K_{\{i\}} = K_i$ and $K(\emptyset) = \{\overline{0}\}$)

$$F_K(\overline{x}) = \sum_{\emptyset\neq I\subset[t]} (-1)^{|I|+1} F_{K_I}(\overline{x}) = \sum_{\emptyset\neq I\subset[t]} (-1)^{|I|+1} \frac{p_I(\overline{x})}{\prod_{b\in B_I}(1 - \overline{x}^b)} .$$

Since $|B_I| \leq e + 1$ and $\overline{x}^b = \dots x_{d+1}^m$,

$$f_P(x) = F_K(1, 1, \dots, 1, x) = \sum_{\emptyset\neq I\subset[t]} \frac{(-1)^{|I|+1} q_I(x)}{(1 - x^m)^{e+1}} = \frac{q(x)}{(1 - x^m)^{e+1}}$$

with $q_I(x), q(x) \in \mathbb{Z}[x]$. Since $p_I(\overline{x}) = F_{T_I}(\overline{x})$, where T_I is the fundamental parallelepiped of K_I, and $c = (\dots, c_{d+1}) \in \mathbb{Z}^{d+1} \cap T_I \Rightarrow c_{d+1} \leq \sum_{b\in B_I} \lambda_b m < m|B_I|$ (because $\lambda_b \in [0, 1)$), each $q_I(x)$ has degree at most $m(e + 1) - 1 = me + m - 1$ and so has $q(x)$. Expressing $q(x)$ as an integral linear combination of $x^s(1-x^m)^t$, $0 \leq s \leq m-1$ and $0 \leq t \leq e$, and using the generalized geometric series $1/(1-x)^j = \sum_{n\ge 0}\binom{n+j-1}{j-1}x^n$, $j\in\mathbb{N}$, we get the expression

$$\begin{aligned} f_P(x) &= \frac{q(x)}{(1-x^m)^{e+1}} = \sum_{j=1}^{e+1}\frac{\beta_{j,0}+\beta_{j,1}x+\cdots+\beta_{j,m-1}x^{m-1}}{(1-x^m)^j} \\ &= \sum_{s=0}^{m-1}\sum_{n\ge 0}\left(\sum_{j=1}^{e+1}\beta_{j,s}\binom{n+j-1}{j-1}\right)x^{mn+s} \\ &= \sum_{s=0}^{m-1}\sum_{n\ge 0}\left(\sum_{j=1}^{e+1}\frac{\beta_{j,s}}{(j-1)!}\prod_{i=0}^{j-2}(n+j-1-i)\right)x^{mn+s} \end{aligned}$$

for some $\beta_{j,s}\in\mathbb{Z}$. Thus for each fixed $s\in\mathbb{N}_0$, $s\le m-1$, the coefficient of x^{mn+s} in $f_P(x)$ is a rational polynomial in n, hence in $mn+s$, of degree at most e. Thus $n\mapsto|\mathbb{Z}^d\cap nP|$, $n\in\mathbb{N}_0$, is a rational quasi-polynomial in n with period m, each component of which has degree $\le e$. The maximum degree is e because P contains a relative open ball $C=\{x\in S(P)\mid \|x-a\|<r\}$, $a\in S(P)$ and $r>0$, which implies that $|\mathbb{Z}^d\cap mnP|\ge|\mathbb{Z}^d\cap mnC|\gg n^e$.

[But there is a problem with the inclusion-exclusion formula with the terms with $B_I=\emptyset$ for which in fact $\deg q_I =$ deg of the denominator.] □

Proposition 0.5 (perturbation trick). *Suppose that $K=K(A)\subset\mathbb{R}^d$ is a cone with $A\subset\mathbb{Q}^d_{\ge 0}$ and $K_i=K(A_i)$, $i=1,2,\ldots,t$, is its triangulation into $\dim K$-dimensional elementary cones. Then there is a vector $v\in -K$ such that*

$$\mathbb{Z}^d\cap K=\mathbb{Z}^d\cap(v+K) \ \text{ and } \ i\ne j\Rightarrow \mathbb{Z}^d\cap(v+K_i)\cap(v+K_j)=\emptyset\,.$$

Proof. The relative boundary of K and all intersections $K_i\cap K_j$, $i\ne j$, are contained in the union U of the linear subspaces $S_B=S(K(\overline{0},B))\subset S(K)$, where $B\subset A$ runs through all $(\dim K-1)$-element linearly independent subsets. One can show that every $c\in\mathbb{Z}^d\backslash S_B$ has from S_B distance at least $b_B>0$. We put

$$\beta=\min_B b_B>0\,.$$

We claim that every vector $v\in(-K)\backslash U$ with $0<\|v\|<\beta$ has the required property; since U is a finite union of subspaces with dimensions $\dim K-1$, $(-K)\backslash U$ contains relative open balls arbitrarily close to the origin and many such v exist. Since $v\in(-K)$, we have $v+K\supset K$ and $\mathbb{Z}^d\cap(v+K)\supset\mathbb{Z}^d\cap K$. The last inclusion is an equality, as every $c\in(\mathbb{Z}^d\cap S(K))\backslash K$ has from K distance larger than $\|v\|$. Since $v\notin U$ and is nonzero, the shift by v shakes off lattice points from every $K_i\cap K_j$, $i\ne j$. The distance argument again shows that the shifted $K_i\cap K_j$ does not acquire any new lattice point. □

Proof of the reciprocity relation.

[to be continued] □

References

[1]

[2] M. Beck and F. Sottile, Irrational proofs of three theorems of Stanley, Europ. J. Combin. 28 (2007) 403–409.

[3] E. Ehrhart, Sur les polyèdres rationnels homothétiques à n dimensions, C. R. Acad. Sci. Paris 254 (1962) 616–618.

[4] R. Stanley, Enumerative Combinatorics, vol. I, Cambridge University Press, Cambridge, 1997 (corrected reprint of the 1986 original).