DIVISORIAL LINEAR ALGEBRA OF NORMAL SEMIGROUP RINGS

WINFRIED BRUNS AND JOSEPH GUBELADZE

ABSTRACT. We investigate the minimal number of generators μ and the depth of divisorial ideals over normal semigroup rings. Such ideals are defined by the inhomogeneous systems of linear inequalities associated with the support hyperplanes of the semigroup. The main result is that for every bound C there exist, up to isomorphism, only finitely divisorial ideals I such that $\mu(I) \leq C$. It follows that there exist only finitely many Cohen–Macaulay divisor classes. Moreover we determine the minimal depth of all divisorial ideals and the behaviour of μ and depth in "arithmetic progressions" in the divisor class group.

The results are generalized to more general systems of linear inequalities whose homogeneous versions define the semigroup in a not necessarily irredundant way. The ideals arising this way can also be considered as defined by the non-negative solutions of an inhomogeneous system of linear diophantine equations.

We also give a more ring-theoretic approach to the theorem on minimal number of generators of divisorial ideals: it turns out to be a special instance of a theorem on the growth of multigraded Hilbert functions.

1. INTRODUCTION

A normal semigroup $S \subset \mathbb{Z}^n$ can be described as the set of lattice points in a finitely generated rational cone. Equivalently, it is the set

$$(*) \qquad S = \{x \in \mathbb{Z}^n \colon \sigma_i(x) \geq 0, \ i = 1, \dots, s\}$$

of lattice points satisfying a system of homogeneous inequalities given by linear forms σ_i with integral (or rational) coefficients. For a field K the K-algebra $K[S]$ is a normal semigroup ring. In the introduction we always assume that S is positive, i.e. 0 is the only invertible element in S.

Let $a_1, \dots, a_s$ be integers. Then the set

$$T = \{x \in \mathbb{Z}^n \colon \sigma_i(x) \geq a_i, \ i = 1, \dots, s\}$$

satisfies the condition $S + T \subset T$, and therefore the K-vector space $KT \subset K[\mathbb{Z}^n]$ is an R-module in a natural way.

It is not hard to show that such an R-module is a (fractional) ideal of R if the group $\mathrm{gp}(S)$ generated by S equals $\mathbb{Z}^n$. Moreover, if the presentation $(*)$ of S is irredundant, then the R-modules KT are even divisorial ideals. These divisorial ideals represent the full divisor class group $\mathrm{Cl}(R)$. Therefore an irredundant system

---

1991 *Mathematics Subject Classification.* Primary 13C14, 13C20, 14M25, 20M25, 52B20, Secondary 11D75, 20G15.

The second author was partially supported by the Max-Planck-Institut für Mathematik at Bonn.

of homogeneous linear inequalities is the most interesting from the ring-theoretic point of view, but we will also treat the general case.

We are mainly interested in two invariants of divisorial ideals D, namely their number of generators $\mu(D)$ and their depth as R-modules, and in particular in the Cohen–Macaulay property. Our main result, based on combinatorial arguments, is that for each $C \in \mathbb{Z}_+$ there exist, up to isomorphism, only finitely many divisorial ideals D such that $\mu(D) \le C$. It then follows by Serre's numerical Cohen–Macaulay criterion that only finitely many divisor classes represent Cohen–Macaulay modules.

The second main result concerns the growth of Hilbert functions of certain multigraded modules and algebras. Roughly speaking, it says that the Hilbert function takes values $\le C$ only at finitely many graded components, provided this holds along each arithmetic progression in the grading semigroup. The theorem on Hilbert functions can be applied to the minimal number of generators of divisorial ideals since R can be embedded into a polynomial ring P over K such that P is a $\mathrm{Cl}(R)$-graded R-algebra in a natural way. This leads to a second proof of the result on number of generators mentioned above.

In Section 2 we study this "standard" embedding of R into a polynomial ring P over K. It has been used many times already, for example by Hochster [Ho] and Stanley [St1]. The standard embedding into a polynomial ring graded by the divisor class group, as described in Theorem 2.1(a), are exactly the homogeneous coordinate rings in the sense of [Cox] of the affine toric varieties $\mathrm{Spec}(k[S])$. Moreover, Theorem 2.1(b) corresponds to the results in [Cox, Section 2] on representing (not necessarily affine) toric varieties as quotients of affine spaces by diagonalizable linear groups. We include the details because they are essential for the subsequent sections.

More generally we discuss so-called pure embeddings of normal affine semigroups into polynomial rings $Q = K[X_1 \dots, X_n]$, and the natural splitting of Q into the coset modules of R , i.e. those submodules of Q whose monomial basis is defined by a single residue class modulo $\mathrm{gp}(S) \subset \mathbb{Z}^n$. Such pure embeddings arise from linear actions of diagonalizable linear algebraic groups on polynomial rings over K, and, more generally, from systems of linear diophantine equations and congruences. In the setting of invariant theory the coset modules appear as modules of covariants, and in the context of diophantine equations they correspond to the sets of non-negative solutions of the associated inhomogeneous systems. We describe all pure embeddings of a normal affine semigroup into finitely generated free semigroups, and characterize those embeddings for which all coset modules are divisorial ideals.

Section 3 contains results on the depth of divisorial ideals. We first show that a divisorial ideal whose class is a torsion element in $\mathrm{Cl}(R)$ is Cohen–Macaulay. This follows easily from Hochster's theorem that normal semigroup rings are Cohen–Macaulay. Then we give a combinatorial description of the minimal depth of all divisorial ideals of R: it coincides with the minimal number of facets $F_1, \dots, F_u$ of the cone generated by S such that $F_1 \cap \dots \cap F_u = \{0\}$.

Section 4 contains our main result on number of generators. The crucial point in its proof is that the convex polyhedron $C(D)$ naturally associated with a divisorial ideal D has a compact face of positive dimension if (and only if) the class of D

is non-torsion. One can show that $\mu(D) \geq M\lambda$ where M is a positive constant only depending on the semigroup S and λ is the maximal length of a compact 1-dimensional face of $C(D)$. Moreover, since the compact 1-dimensional faces are in discrete positions and uniquely determine the divisor class, it follows that λ has to go to infinity in each infinite family of divisor classes.

The observation on compact faces of positive dimension is also crucial for our second approach to the number of generators via Hilbert functions. Their well-established theory allows us to prove quite precise results about the asymptotic behaviour of μ and depth along an arithmetic progression in the divisor class group.

From the viewpoint of applications it is quite unnatural to study only the sets of solutions $T(a)$ of inhomogeneous systems of linear inequalities $\xi_i(x) \geq a_i$, $i = 1, \dots, n$, whose associated homogeneous system defines its set of solutions $S = T(0)$ irredundantly. Therefore we turn to the general case (but still under the assumption $\mathrm{gp}(S) = \mathbb{Z}^n$) in Section 5, replacing divisorial ideals by the *ξ-convex ideals* $I = KT(a)$. The result on numbers of generators has a fully satisfactory generalization: up to isomorphism over R, there exist only finitely many ξ-convex ideals I such that $\mu(I) \leq C$ for every constant C.

Section 6 finally contains the theorem on the growth of Hilbert functions outlined above. It is proved by an analysis of homomorphisms of affine semigroups and their "modules".

The Cohen–Macaulay property of coset modules has been characterized by Stanley [St1, St3] in terms of local cohomology. Brion [Bri] has shown that the number of isomorphism classes of Cohen–Macaulay modules of covariants is finite for certain actions of linear algebraic groups; however, the hypotheses of his theorem exclude groups with infinitely many characters. Therefore our result is to some extent complementary to Brion's.

For unexplained terminology we refer the reader to Bruns and Herzog [BH], Eisenbud [Ei] or Stanley [St3]. A standard reference for the theory of divisor class groups and divisorial ideals is Fossum [Fo]. Divisor class groups of normal semigroup rings are discussed in detail by Gubeladze [Gu2]. The theory of linear algebraic groups used in Section 2 can be found in Humphreys [Hu].

There also exists a considerable literature on the divisor theory of not necessarily finitely generated Krull monoids. See Halter-Koch [HK] for a comprehensive overview and further references.

2. Coset modules

Usually we write the operation in a semigroup additively, and in our terminology a semigroup is always commutative and contains a neutral element 0. Let $S \subset T$ be semigroups. Then the *integral closure* (or *saturation*) of S in T is the subsemigroup

$$\widehat{S} = \{x \in T \colon mx \in S \text{ for some } m \in \mathbb{Z}_+,\ m > 0\}$$

of T; if $S = \widehat{S}$, then S is *integrally closed* in T. By definition, an *affine semigroup* S is a finitely generated subsemigroup of $\mathbb{Z}^n$. The *normalization* $\overline{S}$ of an affine semigroup S is its integral closure in its group of differences $\mathrm{gp}(S)$. We call an affine semigroup *normal* if $S = \overline{S}$. All this terminology is consistent with (and derived from) its use in commutative algebra: for a field K the semigroup algebra $K[\widehat{S}]$ is the integral closure of $K[S]$ in $K[T]$ etc., at least if T can be linearly ordered and every element in $K[T]$ has a leading monomial.

Let $S \subset \mathbb{Z}^n$ be an affine semigroup. One sees easily that its integral closure in $\mathbb{Z}^n$ is

$$\widehat{S} = C(S) \cap \mathbb{Z}^n$$

where $C(S) \subset \mathbb{R}^r$, the *cone generated by* S, is the set of all linear combinations of elements of S with non-negative real coefficients. The normalization $\overline{S}$ of S is given by $\bar{S} = C(S) \cap \operatorname{gp}(S)$. It follows from results of commutative algebra or Gordan's lemma that $\widehat{S}$ and $\overline{S}$ are again affine semigroups.

Since S, and therefore the cone $C(S)$, are finitely generated, $C(S)$ is the intersection of finitely many rational halfspaces,

$$C(S) = \bigcap_{i=1}^{s} \{x \in \mathbb{R}^r : \sigma_i(x) \geq 0\}.$$

That the halfspaces are rational means that we can define them by linear forms $\sigma_i \in (\mathbb{R}^r)^*$ with coprime integer coefficients, and if we require in addition that the representation is minimal, then the σ_i are uniquely determined (up to order). We call them as well as their restrictions to $\mathbb{Z}^r$ the *support forms* of S, and we set

$$\operatorname{supp}(S) = \{\sigma_1, \dots, \sigma_s\}.$$

We will often assume that S is *positive*, i.e. 0 is the only invertible element in S.

Let K be a field and $R = K[S]$. By choosing a basis in $\operatorname{gp}(S)$, we identify it with $\mathbb{Z}^r$ for some $r \geq 0$. From the ring-theoretic point of view, S can then be considered as a semigroup of monomials of the Laurent polynomial ring $K[X_1^{\pm 1}, \dots, X_r^{\pm 1}] \cong K[\mathbb{Z}^r]$. The support forms, so far defined on $\operatorname{gp}(S) \subset K[X_1^{\pm 1}, \dots, X_r^{\pm 1}]$, can be extended to discrete valuations on the quotient field of $K[S]$, which we also denote by σ_i. The prime ideals

$$\mathfrak{p}_i = \{x \in K[S] \colon \sigma_i(x) \geq 1\}$$

are exactly the divisorial prime ideals generated by monomials. By a theorem of Chouinard [Ch], the divisor class group $\operatorname{Cl}(R)$ is isomorphic to the quotient of the free abelian group generated by $\mathfrak{p}_1, \dots, \mathfrak{p}_s$ modulo the subgroup generated by the principal divisors of the monomials $x \in S$. We define the linear map $\sigma \colon \mathbb{Z}^r \to \mathbb{Z}^s$ by

$$\sigma(x) = (\sigma_1(x), \dots, \sigma_s(x)).$$

Note that σ is injective if S is *positive*; in fact $x \in S$ and $-x \in S$ for any element $x \in \operatorname{Ker}\sigma$. One has $\sigma(S) \subset \mathbb{Z}_+^s$, and we can extend σ to an embedding

$$\sigma \colon K[S] \to K[\mathbb{Z}_+^s] \cong K[Y_1, \dots, Y_s].$$

We call these embeddings the *standard embeddings* of S and $K[S]$ respectively. Note that $\sigma(S)$ (up to an automorphism of $\mathbb{Z}_+^s$) only depends on the isomorphism class of S; in fact, according to Gubeladze [Gu3], it only depends on the isomorphism class of the K-algebra $K[S]$.

Let K be an algebraically closed field, and S a positive normal affine semigroup. It is well-known that $K[S]$ can be represented as the ring of invariants of a diagonal action of a suitable algebraic torus $T_n(K) = (K^\times)^n$ on a polynomial ring $K[X_1, \dots, X_n]$ for some $n \in \mathbb{N}$. Conversely, the ring of invariants of a linear action of a diagonalizable group D over K on such a polynomial ring has the structure of a normal affine semigroup ring $K[S]$. The diagonalizable groups are exactly those isomorphic to a direct product $T_n(K) \times A$ where A is a finite abelian group whose order is not divisible by $\operatorname{char} K$. In the following theorem we will discuss the problem how D and $K[S]$ are related. As we shall see, the connection is given through the divisor class group of $K[S]$.

Theorem 2.1. *Let K be a field, S a positive normal affine semigroup, $R = K[S]$, and $\sigma\colon R \to P = K[Y_1, \dots, Y_s]$ the standard embedding.*

(a) *Then P decomposes as an R-module into a direct sum of rank 1 $K[S]$-modules M_c, $c \in \operatorname{Cl}(R)$, such that M_c is isomorphic to a divisorial ideal of class c.*
(b) *Suppose that K is algebraically closed and that $\operatorname{Cl}(R)$ does not contain an element of order $\operatorname{char} K$. Then $R = P^D$ where $D = \operatorname{Hom}_{\mathbb{Z}}(\operatorname{Cl}(R), K^\times) \subset T_s(K)$ acts naturally on P.*

Proof. To each divisorial ideal $\mathfrak{p}_1^{(a_1)} \cap \dots \cap \mathfrak{p}_s^{(a_s)}$, $a_i \in \mathbb{Z}$, we associate $(a_1, \dots, a_s) \in \mathbb{Z}^s$. Under this assignment, the principal divisorial ideal generated by $s \in \operatorname{gp}(S)$ is mapped to $\sigma(s)$. By Chouinard's theorem this yields the isomorphism

$$\operatorname{Cl}(R) \cong \mathbb{Z}^s / \sigma(\mathbb{Z}^r).$$

For each $c \in \mathbb{Z}^s/\sigma(\mathbb{Z}^r)$ we let M_c be the K-vector subspace of P generated by all monomials whose exponent vector in $\mathbb{Z}^s/\sigma(\mathbb{Z}^r)$ has residue class $-c$. Then M_c is clearly an R-submodule of P. Moreover, by construction, P is the direct sum of these R-modules.

It remains to show for (a) that M_c, $c \in \operatorname{Cl}(R)$, is a divisorial ideal of class c (relative to the isomorphism above). We choose a representative $a = (a_1, \dots, a_s)$ of c. Then a monomial $s \in \sigma(\mathbb{Z}^r)$ belongs to $\mathfrak{p}_1^{(a_1)} \cap \dots \cap \mathfrak{p}_s^{(a_s)}$ if and only if $s_i \geq a_i$ for all i, and this is equivalent to $s_i - a_i \in \mathbb{Z}_+$ for all i. Hence the assignment $s \mapsto s - a$, in ring-theoretic terms: multiplication by the monomial Y^{-a}, induces an R-isomorphism $\mathfrak{p}_1^{(a_1)} \cap \dots \cap \mathfrak{p}_s^{(a_s)} \cong M_c$.

For (b) we consider the exact sequence

$$0 \to \sigma(\mathbb{Z}^r) \to \mathbb{Z}^s \to \operatorname{Cl}(R) \to 0.$$

If K is algebraically closed, then this sequence induces an exact sequence

$$1 \to \operatorname{Hom}_{\mathbb{Z}}(\operatorname{Cl}(R), K^\times) \to \operatorname{Hom}_{\mathbb{Z}}(\mathbb{Z}^s, K^\times) \to \operatorname{Hom}_{\mathbb{Z}}(\sigma(\mathbb{Z}^r), K^\times) \to 1$$

since $K^\times$ is an injective $\mathbb{Z}$-module.

The torus $T_s(K) \cong \operatorname{Hom}_{\mathbb{Z}}(\mathbb{Z}^s, K^\times)$ operates naturally on the Laurent polynomial ring $L = K[Y_1^{\pm 1}, \dots, Y_s^{\pm 1}]$ through the substitution $Y^t \mapsto \tau(t) Y^t$ for each $\tau \in T_s(K)$ and each monomial Y^t of P, $t \in \mathbb{Z}_+^s$. In the following we identify t and Y^t.

The homomorphism

$$\delta\colon \mathbb{Z}^s \to \operatorname{Hom}_{\mathrm{alg}}(T_s(K), K^\times), \qquad \delta(t)(\tau) = \tau(t),$$

is an isomorphism, and it induces an isomorphism

$$\operatorname{Hom}_{\mathrm{alg}}\bigl(\operatorname{Hom}_{\mathbb{Z}}(\sigma(\mathbb{Z}^r), K^\times), K^\times\bigr) \cong U$$

where U is the subgroup of all $t \in \mathbb{Z}^s$ such that $\delta(\tau)(t) = 1$ for all $\tau \in D$. Thus the ring of invariants L^D is the K-vector space spanned by all monomials $t \in U$. There is a commutative diagram

$$\begin{tikzcd}
0 \arrow[r] & \sigma(\mathbb{Z}^r) \arrow[r] \arrow[d] & \mathbb{Z}^s \arrow[r] \arrow[d, equal] & \mathrm{Cl}(R) \arrow[r] \arrow[d] & 0 \\
0 \arrow[r] & U \arrow[r] & \mathbb{Z}^s \arrow[r] & \operatorname{Hom}_{\mathrm{alg}}(D, K^\times) \arrow[r] & 0
\end{tikzcd}$$

with exact rows and in which the vertical maps are the natural ones. The right hand vertical map is an isomorphism if and only if the characteristic of K does not divide the order of any element of $\mathrm{Cl}(R)$, and therefore $U = \sigma(\mathbb{Z}^r)$ in this case. Then the set of monomials generating P^D is exactly $\sigma(\mathbb{Z}^r) \cap \mathbb{Z}^s_+$. □

Let S and T be affine semigroups, $S \subset T$. Then S is called a *pure subsemigroup* if $S = T \cap \mathrm{gp}(S)$ in $\mathrm{gp}(T)$ (in Hochster's terminology [Ho] S is a *full* subsemigroup). It is not hard to check that S is a pure subsemigroup if and only if $K[S] \subset K[T]$ is a pure extension of rings. More generally, we say that an injective homomorphism $\xi\colon S \to T$ is *pure* if $\xi(S)$ is a pure subsemigroup of T. If T is normal, then every pure subsemigroup of T is also normal. Examples of pure embeddings are given by the standard embedding $S \to \mathbb{Z}^s_+$, $s = \#\operatorname{supp}(S)$, and the embedding $S \to \mathbb{Z}^n$ resulting from a representation of $K[S]$ as a ring of invariants of a subgroup of the torus $T_n(K)$ acting diagonally on $K[Y_1, \dots, Y_n]$.

The most basic source of pure subsemigroups are systems composed of homogeneous linear diophantine equations

$$a_{i1}x_1 + \cdots + a_{in}x_n = 0, \qquad i = 1, \dots, u,$$

and homogeneous congruences

$$b_{j1}x_1 + \cdots + b_{jn}x_n \equiv 0 \mod c_j \qquad j = 1, \dots, v.$$

The set of nonnegative solutions $x \in \mathbb{Z}^n_+$ of such a system evidently forms a pure subsemigroup of $\mathbb{Z}^n_+$.

In module-theoretic terms the equation $S = T \cap \mathrm{gp}(S)$ says that the monomial K-vector space complement of $K[S]$ in $K[T]$ is a $K[S]$-submodule of $K[T]$, and this condition is actually equivalent to the requirement that $K[S]$ is a direct summand of $K[T]$ as a $K[S]$-module.

The next proposition describes all pure embeddings of S into a free affine semigroup:

Proposition 2.2. *Let S be a positive normal affine semigroup, and $\xi\colon \mathrm{gp}(S) \to \mathbb{Z}^n_+$ an embedding. Then ξ is a pure embedding if and only if $n \geq s = \#\operatorname{supp}(S)$ and, up to renumbering, there exist $e_i \in \mathbb{Z}$, $e_i > 0$, such that $\xi_i = e_i\sigma_i$, $i = 1, \dots, s$.*

Moreover, each of $\xi_{s+1},\dots,\xi_n$ is a rational linear combination of $\sigma_1,\dots,\sigma_s$ with non-negative coefficients.

Proof. Write $\operatorname{gp}(S)=\mathbb{Z}^r$. The embedding ξ can be extended to an $\mathbb{R}$-linear embedding $\xi\colon \mathbb{R}^r\to\mathbb{R}^n$. Then $\xi(C(S))=C(\xi(S))$. Suppose that $\xi(S)$ is a pure subsemigroup of $\mathbb{Z}_+^n$. Then the restrictions of the coordinate linear forms of $\mathbb{R}^n$ to $\xi(\mathbb{R}^r)$ cut out the cone $\xi(C(S))$ from $\xi(\mathbb{R}^r)$. In other words, the inequalities $\xi_i(s)\geq 0$, $i=1,\dots,n$, define the cone $C(S)$. Thus the ξ_i belong to the dual cone

$$C(S)^*=\{\alpha\in\operatorname{Hom}_{\mathbb{R}}(\mathbb{R}^r,\mathbb{R})\colon \alpha(x)\geq 0 \text{ for all } x\in C(S)\},$$

and they in fact generate it since $C(S)=C(S)^{**}$. However, then we must have at least one linear form from each extreme ray of $C(S^*)$ among the ξ_i. The extreme rays of $C(S)^*$ correspond bijectively to the support forms σ_i, and each non-zero linear form α in the extreme ray through σ_i is of the form $\alpha=e\sigma_i$ with $e\in\mathbb{Z}_+$. The rest is clear, as well as the converse implication. $\square$

Corollary 2.3. $\operatorname{Cl}(K[S])$ *is isomorphic to a subquotient of* $\mathbb{Z}^n/\xi(\operatorname{gp}(S))$ *if* ξ *is pure.*

Proof. By the proposition we can assume that $\xi_i=e_i s_i$, $e_i\in\mathbb{Z}_+$, $e_i>0$, $i=1,\dots,s$. We define $\zeta\colon\mathbb{Z}^n\to\mathbb{Z}^s$ as the restriction to the first s coordinates. Then $\vartheta=\zeta\circ\xi$ is injective, and we have a chain of subgroups

$$\vartheta(\operatorname{gp}(S))\subset\mathbb{Z}e_1\oplus\dots\oplus\mathbb{Z}e_s\subset\mathbb{Z}^s.$$

The corollary follows since $\mathbb{Z}^s/\vartheta(\operatorname{gp}(S))$ is a quotient of $\mathbb{Z}^n/\xi(\operatorname{gp}(S)))$, and $(\mathbb{Z}e_1\oplus\dots\oplus\mathbb{Z}e_s)/\vartheta(\operatorname{gp}(S))$ is isomorphic to $\operatorname{Cl}(K[S])$. $\square$

Theorem 2.1 and Corollary 2.3 show that the divisor class group sets the lower limit to all diagonalizable groups D having $K[S]$ as their ring of invariants. In fact, if $D\subset T_n(K)$ acts on $Q=K[X_1,\dots,X_n]$, then Q^D is generated by a pure (normal) subsemigroup of the semigroup $\mathbb{Z}_+^n$ of monomials of Q, and as in the proof of Theorem 2.1 one sees that $\mathbb{Z}^n/\operatorname{gp}(S)\cong\operatorname{Hom}_{\mathbb{Z}}(D,K^\times)$.

If S is a pure subsemigroup of $\mathbb{Z}_+^n$, then (as in the special case of the standard embedding)

$$Q=K[X_1,\dots,X_n]=\bigoplus_{z\in\mathbb{Z}^n/\operatorname{gp}(S)}Q_z$$

where Q_z is the K-vector space generated by all monomials that have residue class $-z$. Clearly Q_z is an $K[S]$-submodule, and Q is a $\mathbb{Z}^n/\operatorname{gp}(S)$-graded $K[S]$-algebra.

Evidently $Q_z\neq 0$ for all $z\in\mathbb{Z}^n/\operatorname{gp}(S)$ if and only if S contains an element of $\mathbb{Z}_+^n$ all of whose components are positive. Every non-zero $K[S]$-module Q_z is finitely generated and of rank 1. In fact, multiplication by the monomial X^z maps Q_z into $K[\operatorname{gp}(S)]$ and if the image contains a monomial with a negative exponent, then S contains an element whose corresponding component is positive. Since the exponents of the monomials in Q_z are bounded below by z we can embed Q_z into $K[S]$. The modules Q_z are called the *coset modules* of S.

In the invariant-theoretic context discussed above, the Q_z are simply the modules of covariants associated with the character $z\in\mathbb{Z}^n/\operatorname{gp}(S)\cong\operatorname{Hom}_{\mathrm{alg}}(D,K^\times)$. In fact, an element $x \in Q = K[X_1, \dots, x_n]$ belongs to Q_z if and only if $\delta(x) = \delta(z)x$ for all $\delta \in D$.

In the context of systems of linear equations and congruences the coset modules correspond to inhomogeneous such systems. In fact, the monomials forming the K-basis of Q_z are the set of non-negative solutions of an inhomogeneous system of linear diophantine equations and inequalities whose associated homogeneous system defines S.

Proposition 2.4. *Suppose that S is a positive normal affine semigroup and $\xi\colon S \to \mathbb{Z}_+^n$ a pure embedding. Let $R = K[S]$, $s = \#\operatorname{supp}(S)$, and $Q = K[X_1, \dots, X_n]$. With the notation as in Proposition 2.2, the following are equivalent:*

(a) *every non-zero coset module Q_z of $\xi(S)$ is divisorial;*
(b) *for each $i = 1, \dots, n$ there exists $j_i \in \{1, \dots, s\}$ and $e_i \in \mathbb{Z}_+$ with $\xi_i = e_i\sigma_{j_i}$.*

Proof. The implication (b) $\implies$ (a) is proved in the same way as Theorem 2.1. In fact,

$$Q_z \cong \bigcap_{i=1}^{n} \mathfrak{p}_{j_i}^{(z_i')}, \qquad z_i' = \lceil z_i/e_i \rceil.$$

For the converse implication we may assume that ξ_n is not a multiple of any σ_j. Then we write ξ_n as a non-negative linear combination of $\sigma_1, \dots, \sigma_s$ with as few non-zero coefficients as possible. By Carathédory's theorem on convex cones and after reordering the σ_j we can assume that $\xi_n = a_1\sigma_1 + \dots + a_p\sigma_p$ where $p \geq 2$, $\sigma_1, \dots, \sigma_p$ are linearly independent, and $a_1, \dots, a_p > 0$ are rational numbers.

It is not hard to check that $\operatorname{gp}(S)$ contains elements t_j with $\sigma_j(t_j) < 0$ and $\sigma_k(t_j) \geq 0$ for all $k = 1, \dots, s$, $j \neq k$. Furthermore S contains elements $u_1, \dots, u_s$ with $\sigma_j(u_j) = 0$ and $\sigma_k(u_j) > 0$ for $j \neq k$. Given $q \in \mathbb{Z}_+$ and $j \in \{1, \dots, s\}$, we can therefore find an element $v_{jq} \in \operatorname{gp}(S)$ such that $\sigma_j(v_{jq}) \leq -q$, but $\xi_n(v_{jq}) \geq 0$.

Set

$$z_m = (-m, \dots, -m, 0) \mod \xi(\operatorname{gp}(S)).$$

Then Q_{z_m} is isomorphic to the fractional ideal $I(m)$ spanned by all the monomials $x \in S$ with $\xi_j(x) \geq -m$ for $j = 1, \dots, n-1$ and $\xi_n(x) \geq 0$. Let

$$J(m) = \mathfrak{p}_1^{(b_1(m))} \cap \dots \cap \mathfrak{p}_s^{(b_s(m))}$$

be the smallest divisorial ideal containing $I(m)$. Then the existence of the elements v_{jq} implies $b_i(m) \to -\infty$ with $m \to \infty$ for all $i = 1, \dots, s$.

On the other hand we can find an element $w \in \operatorname{gp}(S)$ with $\sigma_1(w) < 0$ and $\sigma_j(w) = 0$ for $j = 2, \dots, p$. In particular $w \in J(m)$ for $m \gg 0$. However $\xi_n(w) < 0$. Therefore $I(m) \neq J(m)$ for $m \gg 0$, and $Q_{z_m} \cong I(m)$ is not divisorial. $\square$

Condition (b) of Proposition 2.4 can easily be checked algorithmically. For example, if a system of generators $E = \{x_1, \dots, x_m\}$ of S is known, then one forms the sets $E_i = \{x_j : \xi_i(x_j) = 0\}$ for each coordinate $i = 1, \dots, n$. Condition (b) is satisfied if and only if none of the E_i contains some E_k properly, and one has $n = \#\operatorname{supp}(S)$ if and only if none of the E_i contains some E_k, $k \neq i$.

3. Depth of divisor classes

Divisorial ideals of normal semigroup rings whose class is a torsion element are Cohen–Macaulay. More generally, the following holds:

Theorem 3.1. *Let $S \subset \mathbb{Z}_+^n$ be a pure subsemigroup and set $R = K[S]$, $Q = K[\mathbb{Z}_+^n]$. Furthermore let $\widehat{S} = \{z \in \mathbb{Z}_+^n \colon mz \in S$ for some $m \in \mathbb{N}\}$ be the integral closure of S in $\mathbb{Z}_+^n$.*

(a) *For all $z \in \operatorname{gp}(\widehat{S})/\operatorname{gp}(S)$ the coset module Q_z is a Cohen–Macaulay R-module, provided $Q_z \neq 0$.*
(b) *In particular every divisorial ideal I of R whose class in $\operatorname{Cl}(R)$ is a torsion element is a Cohen–Macaulay R-module.*

Proof. (a) Since $K[\widehat{S}]$ is a normal affine semigroup, the ring $K[\widehat{S}]$ is Cohen–Macaulay by Hochster's theorem [Ho]. It decomposes into the direct sum of the finitely many and finitely generated R-modules Q_z considered in (a). Therefore it is a Cohen–Macaulay ring if and only if all the Q_z are Cohen–Macaulay R-modules.

(b) This follows from (a) if one chooses $S \subset \mathbb{Z}_+^s$ as the standard embedding of R. ☐

In general a normal semigroup ring R may very well have Cohen–Macaulay divisorial ideals whose classes are not torsion. This fact and several other aspects of our discussion are illustrated by the following

Example 3.2. Consider the Segre product

$$R_{mn} = K[X_iY_j \colon 1 \le i \le m,\ 1 \le j \le n]$$

of the polynomial rings $K[X_1, \dots, X_m]$ and $K[Y_1, \dots, Y_n]$. It has divisor class group isomorphic to $\mathbb{Z}$, and the two generators of $\operatorname{Cl}(R)$ correspond to the prime ideals $\mathfrak{p} = (X_1Y_1, \dots, X_1Y_n)$ and $\mathfrak{q} = (X_1Y_1, \dots, X_mY_1)$. Their symbolic powers coincide with the ordinary ones: $\mathfrak{p}^{(i)} = \mathfrak{p}^i$ and $\mathfrak{q}^{(i)} = \mathfrak{q}^i$ for all $i \ge 0$ (see [BV, (9.18)]). Therefore

$$\mu(\mathfrak{p}^{(i)}) = \mu(\mathfrak{p}^i) = \binom{n+i-1}{n-1}, \qquad \mu(\mathfrak{q}^{(i)}) = \mu(\mathfrak{q}^i) = \binom{m+i-1}{m-1}.$$

The Cohen–Macaulay divisorial ideals are represented by

$$\mathfrak{q}^{(n-1)}, \dots, \mathfrak{q}, R_{mn}, \mathfrak{p}, \dots, \mathfrak{p}^{(m-1)}$$

(see Bruns and Guerrieri [BGu]), and in particular, their number is finite. However, the finiteness of the number of Cohen–Macaulay classes is not a peculiar property of R_{mn}: it holds for all normal semigroup rings, as we will see in Corollary 4.2.

Moreover, one has

$$\inf_i \operatorname{depth} \mathfrak{p}^{(i)} = m, \qquad \inf_i \operatorname{depth} \mathfrak{q}^{(i)} = n,$$

and for $i \gg 0$ the minimal values are attained (see [BV, (9.27)]). Set $p(i) = \mu(\mathfrak{p}^{(i)})$.It follows that the degree of the polynomial p and $\inf_i \operatorname{depth} \mathfrak{p}^{(i)}$ add up to $m+n-1 = \dim R$. This is another instance of a general fact (see Theorem 4.5).

That divisorial ideals I of non-torsion class are in general not Cohen-Macaulay, follows already from the asymptotic behaviour of $\operatorname{depth} I$ described in the next theorem. (See the proof of Theorem 2.1 for the definition of the modules M_c representing the divisor classes.) By $\operatorname{depth}_R M$ or simply $\operatorname{depth} M$ we denote the length of a maximal M-sequence for a finitely generated R-module M. If S is positive, $R = K[S]$ and M is $\operatorname{gp}(S)$-graded, then $\operatorname{depth}_R M = \operatorname{depth}_{R_\mathfrak{m}} M_\mathfrak{m}$ where $\mathfrak{m}$ is the maximal ideal generated by all the non-unit monomials of R. (See [BH, 1.5.15] for the proof of an analogous statement about $\mathbb{Z}$-graded rings and modules.) For an ideal I in a noetherian ring R we let $\operatorname{grade} I$ denote the length of a maximal R-sequence in I; one always has $\operatorname{grade} I \le \operatorname{height} I$. But if R is Cohen–Macaulay, then $\operatorname{grade} I = \operatorname{height} I$.

Theorem 3.3. *Let K be a field, S a positive normal affine semigroup, $R = K[S]$, and $\sigma\colon R \to P = K[X_1, \dots, X_s]$ the standard embedding. Furthermore let $\mathfrak{m}$ be the irrelevant maximal ideal of R generated by all non-unit monomials, and λ the maximal length of a monomial R-sequence. Then*

$$\lambda \le \operatorname{grade} \mathfrak{m}P = \min\{\operatorname{depth} M_c\colon c \in \operatorname{Cl}(R)\}.$$

Proof. For the inequality it is enough to show that a monomial R-sequence is also a P-sequence. (It is irrelevant whether we consider P as an R-module or a P-module if elements from R are concerned.) Let $\mu_1, \dots, \mu_u$ be monomials in R forming an R-sequence. Then the subsets $A_i = \operatorname{Ass}_R(R/(\mu_i))$ are certainly pairwise disjoint. On the other hand, A_i consists only of monomial prime ideals of height 1 in R, since R is normal. So $A_i = \{\mathfrak{p}_j\colon \sigma_j(\mu_i) > 0\}$, and the sets of indeterminates of P that divide $\sigma(\mu_i)$ in P, $i = 1, \dots, u$, are pairwise disjoint. It follows that $\mu_1, \dots, \mu_u$ form a P-sequence.

In order to prove the equality we first extend the field K to an uncountable one. This is harmless, since all data are preserved by base field extension. Then we can form a maximal P-sequence in $\mathfrak{m}P$ by elements from the K-vector subspace $\mathfrak{m}$. Such a P-sequence of elements in R then has length equal to $\operatorname{grade} \mathfrak{m}P$ and is clearly an M-sequence for every R-direct summand M of P, and in particular for each of the modules M_c representing the divisor classes. Thus $\operatorname{depth} M_c \ge \operatorname{grade} \mathfrak{m}P$.

Whereas this argument needs only finite prime avoidance, we have to use countable prime avoidance for the converse inequality. Suppose that $u < \min\{\operatorname{depth} M_c\colon c \in \operatorname{Cl}(R)\}$ and that $x_1, \dots, x_u$ is a P-sequence in $\mathfrak{m}$. Then the set

$$A = \bigcup_{c \in \operatorname{Cl}(R)} \operatorname{Ass}\bigl(M_c/(x_1, \dots, x_u)M_c\bigr)$$

is a countable set of K-vector subspaces of $\mathfrak{m}$. Each prime ideal associated to $M_c/(x_1, \dots, x_u)M_c$ is a proper subspace of $\mathfrak{m}$ because of $u < \operatorname{depth} M_c$. Hence A cannot exhaust $\mathfrak{m}$, as follows from elementary arguments. So we can choose an element x_{u+1} in $\mathfrak{m}$ not contained in a prime ideal associated to any of the $M_c/(x_1, \dots, x_u)M_c$. So x_{u+1} extends $x_1, \dots, x_u$ to an M_c-sequence simultaneously for all $c \in \operatorname{Cl}(R)$. $\square$

Both the numbers λ and $\operatorname{grade} \mathfrak{m}P$ can be characterized combinatorially:

Proposition 3.4. *With the notation of the previous theorem, the following hold:*

(a) grade $\mathfrak{m}P$ *is the minimal number* u *of facets* $F_{i_1},\dots,F_{i_u}$ *of* $C(S)$ *such that* $F_{i_1}\cap\dots\cap F_{i_u}=\{0\}$.
(b) λ *is the maximal number* ℓ *of subsets* $\mathcal{F}_1,\dots,\mathcal{F}_\ell$ *of* $\mathcal{F}=\{F_1,\dots,F_s\}$ *with the following properties:*

$$\text{(i)}\quad \mathcal{F}_i\cap\mathcal{F}_j=\emptyset,\qquad \text{(ii)}\ \bigcap_{F\in\mathcal{F}\setminus\mathcal{F}_i} F\neq\{0\}$$

for all i,j *such that* $i\neq j$.

Proof. (a) The ideal $\mathfrak{m}P$ of P is generated by monomials. Therefore all its minimal prime ideals are generated by indeterminates of P. The ideal generated by $X_{i_1},\dots,X_{i_u}$ contains $\mathfrak{m}P$ if and only if for each monomial $\mu\in\mathfrak{m}$ there exists a σ_{i_j} such that $\sigma_{i_j}(\mu)>0$. The monomials for which none such inequality holds are precisely those in $F_{i_1}\cap\dots\cap F_{i_u}$.

(b) Let $\mu_1,\dots,\mu_\ell$ be a monomial R-sequence. Then the sets $\mathcal{F}_i=\{F\colon \mathfrak{p}_F\in \operatorname{Ass}(R/(\mu_i))\}$ are pairwise disjoint, and moreover $\mu_i\in\bigcap_{F\in\mathcal{F}\setminus\mathcal{F}_i}F$. Thus conditions (i) and (ii) are both satisfied.

For the converse one chooses monomials $\mu_i\in\bigcap_{F\in\mathcal{F}\setminus\mathcal{F}_i}F$. Then $\{F\colon \mathfrak{p}_F\in \operatorname{Ass}(R/(\mu_i))\}\subset\mathcal{F}_i$, and since the $\mathcal{F}_i$ are pairwise disjoint, the μ_i form even a P-sequence as observed above. □

Remark 3.5. The following are equivalent:
(a) S is simplicial;
(b) every divisorial ideal of R is a Cohen–Macaulay module.

If S is simplicial, then $\operatorname{Cl}(R)$ is finite, and so every divisorial ideal is Cohen–Macaulay by Theorem 3.1. Conversely, if every divisorial ideal is Cohen–Macaulay, then it is impossible that facets $F_1,\dots,F_u$, $u<\operatorname{rank}S$, of $C(S)$ intersect only in 0, and this property characterizes simplicial cones. However, the implication (b) $\Longrightarrow$ (a) follows also from Theorem 4.1 below.

It is an amusing consequence that a rank 2 affine semigroup is simplicial – an evident geometric fact. In fact, if $\dim R\geq 2$, then $\operatorname{depth} I\geq 2$ for every divisorial ideal.

The results of this section can be partially generalized to arbitrary pure embeddings; we leave the details to the reader.

4. The number of generators

In this section we first prove our main result on the number of generators of divisorial ideals of normal semigroup rings $R=K[S]$. In its second part we then show that it can also be understood and proved as an assertion about the growth of the Hilbert function of a certain multigraded K-algebra.

Theorem 4.1. *Let* R *be a positive normal semigroup ring over the field* K, *and* $m\in\mathbb{Z}_+$. *Then there exist only finitely many* $c\in\operatorname{Cl}(R)$ *such that a divisorial ideal* D *of class* c *has* $\mu(D)\leq m$.

As a consequence of Theorem 4.1, the number of Cohen–Macaulay classes is also finite:

Corollary 4.2. *There exist only finitely many $c \in \operatorname{Cl}(R)$ for which a divisorial ideal of class c is a Cohen–Macaulay module.*

Remark 4.3. (a) One should note that $\mu(D)$ is a purely combinatorial invariant. If S is the underlying semigroup and T is a monomial basis of a monomial representative of D, then $\mu(D)$ is the smallest number g such that there exists $x_1, \dots, x_g \in T$ with $T = (S + x_1) \cup \dots \cup (S + x_g)$. Therefore Theorem 4.1 can very well be interpreted as a result on the generation of the sets of solutions to inhomogeneous linear diophantine equations and congruences (with fixed associated homogeneous system).

(b) Both the theorem and the corollary hold for all normal affine semigroups S, and not only for positive ones. It is easily seen that a normal semigroup S splits into a direct summand of its largest subgroup S_0 and a positive normal semigroup S' Thus one can write $R = K[S]$ as a Laurent polynomial extension of the K-algebra $R' = K[S']$. Each divisor class of R has a representative $D' \otimes_{R'} R$. Furthermore $\mu_{R'}(D') = \mu_R(D' \otimes_{R'} R)$ and the Cohen–Macaulay property is invariant under Laurent polynomial extensions.

We first derive the corollary from the theorem. Let $\mathfrak{m}$ be the irrelevant maximal ideal of R. If M_c is a Cohen–Macaulay module, then $(M_c)_\mathfrak{m}$ is a Cohen–Macaulay module (and conversely). Furthermore

$$e((M_c)_\mathfrak{m}) \geq \mu((M_c)_\mathfrak{m}) = \mu(M_c).$$

By Serre's numerical Cohen–Macaulay criterion (for example, see [BH, 4.7.11]), the rank 1 $R_\mathfrak{m}$-module $(M_c)_\mathfrak{m}$ is Cohen–Macaulay if and only if its multiplicity $e((M_c)_\mathfrak{m})$ coincides with $e(R_\mathfrak{m})$.

Proof of Theorem 4.1. Let D be a monomial divisorial ideal of R. As pointed out already, there exist integers $a_1, \dots, a_s$ such that the lattice points in the set

$$C(D) = \{x \in S \colon \sigma_i(x) \geq a_i,\ i = 1, \dots, s\}$$

give a K-basis of D (again $s = \#\operatorname{supp}(S)$, and the σ_i are the suppoprt forms). The polyhedron $C(D)$ is uniquely determined by its extreme points since each of its facets is parallel to one of the facets of $C(S)$ and passes through such an extreme point. (Otherwise $C(D)$ would contain a full line, and this is impossible if S is positive.)

Moreover, D is of torsion class if and only if $C(D)$ has a single extreme point. This has been proved in [Gu2], but since it is the crucial point (sic!) we include the argument.

Suppose first that D is of torsion class. Then there exists $m \in \mathbb{Z}_+$, $m > 0$, such that $D^{(m)}$ is a principal ideal, $D^{(m)} = xR$ with a monomial x. It follows that $C(D^{(m)}) = mC(D)$ has a single extreme point in (the lattice point corresponding to) x, and therefore $C(D)$ has a single extreme point.

Conversely, suppose that $C(D)$ has a single extreme point. The extreme point has rational coordinates. After multiplication with a suitable $m \in \mathbb{Z}_+$, $m > 0$, we obtain that $C(D^{(m)}) = mC(D)$ has a single extreme point x which is even a lattice point. All the facets of $C(D^{(m)})$ are parallel to those of S and must pass through the single extreme point. Therefore $C(D^{(m)})$ has the same facets as $C(S) + x$. Hence $C(D^{(m)}) = C(S) + x$. This implies $D^{(m)} = Rx$ (in multiplicative notation), and so m annihilates the divisor class of D.

Suppose that D is not of torsion class. We form the line complex $\overline{\mathcal{L}}$ consisting of all 1-dimensional faces of the polyhedron $C(D)$. Then $\overline{\mathcal{L}}$ is connected, and each extreme point is an endpoint of a 1-dimensional face. Since there are more than one extreme points, all extreme points are endpoints of compact 1-dimensional faces, and the line complex $\mathcal{L}(D)$ formed by the *compact* 1-dimensional faces is also connected. Since each facet passes through an extreme point, D is uniquely determined by $\mathcal{L}(D)$ (as a subset of $\mathbb{R}^s$).

Let $\mathcal{C}$ be an infinite family of divisor classes and choose a divisorial ideal D_c of class c for each $c \in \mathcal{C}$. Assume that the minimal number of generators $\mu(D_c)$, $c \in \mathcal{C}$, is bounded above by a constant C. By Lemma 4.4 below the Euclidean length of all the line segments $\ell \in \mathcal{L}(D_c)$, $c \in \mathcal{C}$, is then bounded by a constant C'.

It is now crucial to observe that the endpoints of all the line segments under consideration lie in an overlattice $L = \mathbb{Z}^n[1/d]$ of $\mathbb{Z}^n$. In fact each such point is the unique solution of a certain system of linear equations composed of equations $\sigma_i(x) = a_i$, and therefore can be solved over $\mathbb{Z}[1/d]$ where $d \in \mathbb{Z}$ is a suitable common denominator. (Again we have denoted the support forms of S by σ_i.)

Let us consider two line segments ℓ and ℓ' in $\mathbb{R}^n$ as equivalent if there exists $z \in \mathbb{Z}^n$ such that $\ell' = \ell + z$. Since the length of all the line segments under consideration is bounded and their endpoints lie in $\mathbb{Z}^n[1/d]$, there are only finitely many equivalence classes of line segments $\ell \in \mathcal{L}(D_c)$, $c \in \mathcal{C}$.

Similarly we consider two line complexes $\mathcal{L}(D)$ and $\mathcal{L}(D')$ as equivalent if $\mathcal{L}(D') = \mathcal{L}(D) + z$, $z \in \mathbb{Z}^n$. However, this equation holds if and only if $C(D') = C(D) + z$, or, in other words, the divisor classes of D and D' coincide.

Since there are only finitely many equivalence classes of line segments and the number of lines that can appear in a complex $\mathcal{L}(D)$ is globally bounded (for example, by 2^s), one can only construct finitely many connected line complexes that appear as $\mathcal{L}(D)$, up to equivalence of line complexes. This contradicts the infinity of the family $\mathcal{C}$. $\square$

Lemma 4.4. *Let S be a positive normal semigroup, K a field, D a monomial divisorial ideal whose class is not torsion. Then there exists a constant $M > 0$, which is independent of K, such that $\mu(D) \geq M\lambda$ where λ is the maximal Euclidean length of a compact 1-dimensional face of $C(D)$.*

Proof. We assume that $\mathbb{Z}^n = \operatorname{gp}(S)$ so that the cone $C(S)$ and the polyhedron $C(D)$ are subsets of $\mathbb{R}^n$. Let ℓ be a 1-dimensional compact face of $C(D)$. Suppose D is given by the inequalities

$$\sigma_i(x) \geq a_i, \qquad i = 1, \dots, s \qquad \bigl(s = \#\operatorname{supp}(C(S))\bigr).$$

There exists $\varepsilon > 0$ such that $U_\varepsilon(x) \cap C(D)$ contains a lattice point for each $x \in C(D)$. (In fact, $C(S)$ contains a unit cube, and $x + C(S) \subset C(D)$ for $x \in C(D)$.) Let $x \in \ell$.

We can assume that
$$\sigma_i(x) \begin{cases} = a_i, & i = 1, \dots, m, \\ > a_i, & i > m. \end{cases}$$
Let $\tau = \sigma_1 + \cdots + \sigma_m$. There exists $C > 0$ such that $\tau(y) < C$ for all $y \in \mathbb{R}^n$ with $|y| < \varepsilon$.

Furthermore we have $\tau(z) > 0$ for all $z \in C(S)$, $z \neq 0$. Otherwise the facets $F_1, \dots, F_m$ would meet in a line contained in $C(S)$, and this is impossible if ℓ is compact. In particular there are only finitely many lattice points z in S such that $\tau(z) < C$, and so there exists $\delta > 0$ such that $\tau(z) < C$ for $z \in S$ is only possible with $|z| < \delta$.

Now suppose that D is generated by $x_1, \dots, x_q$. For $x \in \ell$ we choose a lattice point $p \in U_\varepsilon(x) \cap C(D)$. By assumption there exists $z \in C(S)$ such that $p = x_i + z$. Then
$$\tau(z) = \tau(p) - \tau(x_i) \le \tau(p) - \tau(x) = \tau(p - x) < C.$$
Thus $|z| < \delta$, and therefore $|x - x_i| < \delta + \varepsilon$.

It follows that the Euclidean length of ℓ is bounded by $2q(\delta + \varepsilon)$. Of course δ depends on τ, but there exist only finitely many choices for τ if one varies ℓ. $\square$

As pointed out, the polyhedron $C(D)$ contains a 1-dimensional compact face if D is not of torsion class, but in general one cannot expect anything stronger. On the other hand, there exist examples for which $C(D)$ for every non-torsion D has a compact face of arbitrarily high dimension; see Example 3.2.

If $C(D)$ has a d-dimensional face F, then the argument in the proof of Lemma 4.4 immediately yields that $\mu(D^{(j)}) \ge Mj^d$ for a constant $M > 0$: one has only to replace the length of the line segment by the d-dimensional volume of F. We now give another proof of a slightly more general statement. As we will see, it leads to a quite different proof of Theorem 4.1.

Let S be a positive normal affine semigroup. Recall that the polynomial ring P of the standard embedding $\sigma\colon R \to P$ decomposes into the direct sum of modules M_c, $c \in \operatorname{Cl}(R)$. In the following $C(M_c)$ stands for any of the congruent polyhedra $C(D)$ where D is a divisorial ideal of class c.

Theorem 4.5. *Let $c, d \in \operatorname{Cl}(R)$ and suppose that c is not a torsion element.*

(a) *Then $\lim_{c\to\infty} \mu(M_{jc+d}) = \infty$.*

(b) *More precisely, let d be the maximal dimension of the compact faces of $C(M_c)$. Then there exists $e \in \mathbb{N}$ such that*
$$\lim_{c\to\infty} \frac{\mu(M_{(ej+k)c+d})}{c^d}$$
is a positive real number for each $k = 0, \dots, e-1$.

(c) *One has $\inf_j \operatorname{depth} M_{jc} = \dim R - d$ and $\inf_j \operatorname{depth} M_{cj+d} \le \dim R - d$.*

Proof. Let
$$\mathcal{D} = \bigoplus_{j=0}^{\infty} M_{jc} \qquad \text{and} \qquad \mathcal{M} = \bigoplus_{j=0}^{\infty} M_{jc+d}.$$

Then $\mathcal{D}$ is a finitely generated K-algebra. This follows for general reasons from Theorem 6.1 below: $\mathcal{D}$ is the direct sum of graded components of the $\mathrm{Cl}(R)$-graded R-algebra P, taken over a finitely generated subsemigroup of $\mathrm{Cl}(R)$. Theorem 6.1 also shows that $\mathcal{M}$ is a finitely generated $\mathcal{D}$-module. However, these assertions will be proved directly in the following. In particular we will see that $\mathcal{D}$ is a normal semigroup ring over K.

By definition $\mathcal{D}$ is a $\mathbb{Z}_+$-graded R-algebra with $\mathcal{D}_0 = M_0 = R$, and $\mathcal{M}$ is a graded $\mathcal{D}$-module if we assign degree j to the elements of M_{jc+d}. There exists $e > 0$ such that $\mathcal{D}$ is a finitely generated module over its R-subalgebra generated by elements of degree e; for example, we can take e to be the least common multiple of the degrees of the generators of $\mathcal{D}$ as an R-algebra. Let $\mathcal{E}$ be the eth Veronese subalgebra of $\mathcal{D}$. We decompose $\mathcal{M}$ into the direct sum of its $\mathcal{E}$-submodules

$$\mathcal{M}_k = \bigoplus_{j=0}^{\infty} M_{(ej+k)c+d}, \qquad k = 0, \dots, e-1.$$

In view of what has to be proved, we can replace $\mathcal{D}$ by $\mathcal{E}$ and $\mathcal{M}$ by $\mathcal{M}_k$. Then we have reached a situation in which $\mathcal{D}$ is a finitely generated module over the subalgebra generated by its degree 1 elements.

Note that $\mathcal{M}$ is isomorphic to an ideal of $\mathcal{D}$: multiplication by a monomial X^a such that a has residue class $-(d+k)$ in $\mathrm{Cl}(R) \cong \mathbb{Z}^s/\sigma(\mathrm{gp}(S))$ maps $\mathcal{M}$ into $\mathcal{D}$. Since $\mathcal{M}$ is not zero (and $\mathcal{D}$ is an integral domain), we see that $\operatorname{Supp}\mathcal{M} = \operatorname{Spec}\mathcal{D}$.

Let $\mathfrak{m}$ be the irrelevant maximal ideal of R; it is generated by all elements $x \in S$, $x \neq 1$ (in multiplicative notation). Then clearly $\overline{\mathcal{M}} = \mathcal{M}/\mathfrak{m}\mathcal{M}$ is a finitely generated $D = \mathcal{D}/\mathfrak{m}\mathcal{D}$-module with $\operatorname{Supp}\overline{\mathcal{M}} = \operatorname{Spec} D$. Note that D is a K-algebra with $D_0 = K$ in a natural way. Furthermore it is a finitely generated module over its subalgebra D' generated by its degree 1 elements. In particular $\overline{\mathcal{M}}$ is a finitely generated D'-module. By construction (and Nakayama's lemma) we have

$$\mu(M_{(ej+k)c+d}) = \dim_K M_{(ej+k)c+d}/\mathfrak{m}M_{(ej+k)c+d} = H(\overline{\mathcal{M}}, j)$$

where H denotes the Hilbert function of $\overline{\mathcal{M}}$ as a $\mathbb{Z}_+$-graded D- or D'-module. For $j \gg 0$ the Hilbert function is given by the Hilbert polynomial. It is a polynomial of degree $\delta - 1$ where δ is the Krull dimension of $\overline{\mathcal{M}}$. Note that $\operatorname{Supp}\overline{\mathcal{M}} = \operatorname{Spec} D$, since $\operatorname{Supp}\mathcal{M} = \operatorname{Spec}\mathcal{D}$; in particular one has $\dim\overline{\mathcal{M}} = \dim D$. Moreover the leading coefficient of the Hilbert polynomial is $e(\overline{\mathcal{M}})/(\delta-1)!$ and so all the claims for $\mathcal{M}$ follow if $d + 1 = \delta > 1$.

At this point we have to clarify the structure of $\mathcal{D}$ as a normal semigroup ring over K. For convenience we choose a divisorial ideal $I \subset R$ of class c generated by monomials. Then there exists an R-module isomorphism $M_c \to I$ mapping monomials to monomials, and such an isomorphism induces a K-algebra isomorphism from $\mathcal{D}$ to

$$\mathcal{R} = \bigoplus_{j=0}^{\infty} I^{(j)}T^j \subset R[T] = K[S \oplus \mathbb{Z}_+].$$

There exist $a_1,\dots,a_s \ge 0$ such that $I = \mathfrak{p}_1^{(a_1)} \cap \dots \cap \mathfrak{p}_s^{(a_s)}$. The monomial corresponding to $(s,z) \in \operatorname{gp}(S) \oplus \mathbb{Z}$ belongs to $\mathcal{R}$ if and only if

$$z \ge 0, \qquad \sigma_i(s) \ge 0, \qquad \sigma_i(s) - za_i \ge 0, \qquad i = 1,\dots,s.$$

It follows immediately that $\mathcal{R}$ is a normal semigroup ring over K. Let $\mathcal{S}$ be its semigroup of monomials. One has $\operatorname{gp}(\mathcal{S}) = \operatorname{gp}(S) \oplus \mathbb{Z}$, and the elements with last component j give the monomials of $I^{(j)}$.

It is not hard to show that the faces $\not\subset C(S)$ of $C(\mathcal{S})$ are the closed envelopes of the $\mathbb{R}_+$-envelopes of the faces of $C(I)' = \{(x,1) \colon x \in C(I)\}$, and that exactly those faces that do not contain an element from $\mathfrak{m}$ intersect $C(I)'$ in a compact face. Since the dimension of $\mathcal{R}/\mathfrak{m}\mathcal{R}$ is just the maximal dimension of a face F of $C(\mathcal{S})$ not containing an element of $\mathfrak{m}$, we see that $\dim \mathcal{R}/\mathfrak{m}\mathcal{R} = d+1$. In fact, the largest dimension of a compact face of $C(I)'$ is d, and it extends to a $d+1$-dimensional face of $C(\mathcal{S})$.

Thus $\delta = d+1$ and $\delta > 1$, since $C(I)$ has at least a 1-dimensional compact face: by hypothesis I is not of torsion class.

For part (c) we note that height $\mathfrak{m}R = \operatorname{grade} \mathfrak{m}\mathcal{R} = \dim \mathcal{R} - \dim \mathcal{R}/\mathfrak{m}\mathcal{R} = \dim R - d$ since $\mathcal{R}$ is Cohen–Macaulay by Hochster's theorem (and all the invariants involved are stable under localization with respect to the maximal ideal of $\mathcal{R}$ generated by monomials). Moreover $\operatorname{grade} \mathfrak{m}\mathcal{R} = \inf_j \operatorname{depth} M_{cj}$, as follows by arguments analogous to those in the proof of Theorem 3.3.

By similar arguments the inequality for $\inf_j \operatorname{depth} M_{cj+d}$ results from height $\mathfrak{m}\mathcal{R} = \dim R - d$. □

Remark 4.6. The limits in Theorem 4.5(b) coincide if and only if the D'-modules $\mathcal{M}_k/\mathfrak{m}\mathcal{M}_k$ all have the same multiplicity. However, in general this is not the case. As an example one can take the semigroup ring $R = K[U^2, UV, V^2, XW, YW, XZ, YZ]$. It has divisor class group $\operatorname{Cl}(R) = \mathbb{Z}/(2) \oplus \mathbb{Z}$; the class of $\mathfrak{p} = (U^2, UV)$ is non-zero, but a 2-torsion element, and the class of $\mathfrak{q} = (XW, YW)$ generates the free direct summand. Let $c \in \operatorname{Cl}(R)$ be the class of $\mathfrak{p}\mathfrak{q}$. It is not hard to show that jc is represented by the divisorial ideal $\mathfrak{q}\mathfrak{p}^j$ for j odd, and by $\mathfrak{p}^j$ for j even. The limits for $k = 0$ and $k = 1$ therefore differ by a factor of 2 ($d = 0$, $e = 2$).

Second proof of Theorem 4.1. Let P be the polynomial ring of the standard embedding of R. Then P is a $\operatorname{Cl}(R)$-graded R-algebra whose graded component P_c, $c \in \operatorname{Cl}(R)$ is the module M_c. Passing to residue classes modulo $\mathfrak{m}$ converts the assertion of the theorem into a statement about the Hilbert function (with respect to K) of the $\operatorname{Cl}(R)$-graded K-algebra $P/\mathfrak{m}P$; note that $(P/\mathfrak{m}P)_0 = R/\mathfrak{m} = K$. By Theorem 4.5 the Hilbert function goes to infinity along each arithmetic progression in $\operatorname{Cl}(R)$. Therefore we are in a position to apply Theorem 6.3 below. It says that there are only finitely many $c \in \operatorname{Cl}(R)$ where $\mu(M_c) = H(P/\mathfrak{m}P, c)$ does not exceed a given bound m. □

This deduction of Theorem 4.1 uses the combinatorial hypotheses on R only at a single point in the proof of Theorem 4.5, namely where we show that $\dim \mathcal{D}/\mathfrak{m}\mathcal{D} \ge 2$. Thus the whole argument can be transferred into a more general setting, provided an analogous condition on dimension holds.

5. Convex ideals

Let $\xi_1, \dots, \xi_n$ be $\mathbb{Z}$-linear forms on $\mathbb{Z}^r$. Then

$$(*) \qquad S = \{x \in \mathbb{Z}^r \colon \xi_i(x) \geq 0,\ i = 1, \dots, n\}$$

is a normal semigroup. For $a \in \mathbb{Z}^n$ we set

$$T(a;\xi) = \{x \in \mathbb{Z}^r \colon \xi_i(x) \geq a_i,\ i = 1, \dots, n\}.$$

Let K be a field. Then $I(a;\xi) = KT(a;\xi)$ is an $R = K[S]$-module in a natural way.

In the following we will always assume that S is positive and that $\operatorname{gp}(S) = \mathbb{Z}^r$; furthermore we will assume that ξ is non-degenerate, i.e. $\xi_i \neq 0$ for all i; this assumption is certainly no restriction of generality. Then it follows easily that $I(a;\xi)$ is a non-zero fractional ideal of R for every a. These ideals are called *ξ-convex*.

If $\sigma = (\sigma_1, \dots, \sigma_s)$ consists of the support forms of S, then the σ-convex ideals are just the monomial divisorial ideals of R studied in the previous sections.

The linear map $\xi \colon \operatorname{gp}(S) \to \mathbb{Z}^n$ evidently restricts to a pure embedding of S into $\mathbb{Z}^n$ (if S is positive), and, conversely, a pure embedding induces a presentation $(*)$ of S. As in the proof of Theorem 2.1 one sees that each coset modules of $\xi(S)$ is isomorphic to a ξ-convex ideal, and vice versa. Proposition 2.4 therefore describes the condition under which all ξ-convex ideals are divisorial (and in its proof we have actually switched from a coset module to the corresponding ξ-convex ideal).

However, in contrast to the standard embedding, different coset modules can now be isomorphic. Proposition 5.1 below clarifies this fact. For $T \subset \operatorname{gp}(S)$ we define the "effective ξ-bounds" $\operatorname{eff}(T;\xi) \in \mathbb{Z}^n$ component wise by

$$\operatorname{eff}(T;\xi)_i = \inf\{\xi_i(t) \colon t \in T\};$$

for a fractional monomial ideal I we set $\operatorname{eff}(I;\xi) = \operatorname{eff}(T;\xi)$ where T is the monomial basis of I; and for $a \in \mathbb{Z}^n$ we set $\operatorname{eff}(a;\xi) = \operatorname{eff}(I(a;\xi);\xi)$. The convex polyhedron $C(I;\xi) \subset \mathbb{R}^r$ associated with I is given by

$$C(I;\xi) = \{x \in \mathbb{R}^r \colon \xi_i(x) \geq \operatorname{eff}(I;\xi)_i,\ i = 1, \dots, n\}.$$

Proposition 5.1. (a) *The assignment $I \mapsto C(I;\xi)$ is injective on the set of ξ-convex ideals I.*

(b) *The following are equivalent for ξ-convex ideals I and J:*
  (i) *I and J are isomorphic R-modules.*
  (ii) *There exists $y \in \operatorname{gp}(S)$ such that $\operatorname{eff}(J;\xi) = \operatorname{eff}(I,\xi) + \xi(y)$.*
  (iii) *There exists $y \in \operatorname{gp}(S)$ such that $C(I;\xi) = C(J;\xi) + \xi(y)$.*

(c) *If $C(I;\xi)$ has a single extreme point for a ξ-convex ideal, then I is a divisorial ideal of torsion class.*

(d) *The coset modules Q_a, Q_b of $\xi(S)$ associated with the residue classes of $a, b \in \mathbb{Z}^n$ are isomorphic if and only if* $\operatorname{eff}(a;\xi) \equiv \operatorname{eff}(b;\xi) \mod \xi(\operatorname{gp}(S))$.

Proof. (a) One can recover I from $C(I;\xi)$.

(b) Fractional monomial ideals I and J of $K[S]$ are isomorphic if and only if there exists a monomial $x \in K[\operatorname{gp}(S)]$ such that $J = Ix$. If one converts this into additive notation, one immediately obtains the equivalence of (i), (ii), and (iii).

(c) Set $a_i = \operatorname{eff}(I;\xi_i)$, $i = 1,\dots,n$. Each of the hyperplanes given by the equations $\xi_i(x) = a_i$ passes through an extreme point of $C(I;\xi)$. Since there is a single extreme point z, all the parallels to the support hyperplanes pass through this point. Thus $C(I;\xi) = C(S) + z$, and $C(I;\xi)$ is cut out by parallels of the support hyperplanes of S. Then I is a divisorial ideal. Divisorial ideals I for which $C(I)$ has a single extreme point are of torsion class as observed in the proof of Theorem 4.1.

(d) Since $Q_a \cong I(\operatorname{eff}(a;\xi);\xi)$ and $Q_b \cong I(\operatorname{eff}(b;\xi);\xi)$, this follows from (b). $\square$

It is now clear that Lemma 4.4 generalizes to the case of ξ-convex ideals, and since the isomorphism classes of ξ-convex ideals are again parameterized by the equivalence classes of the polyhedra $C(I;\xi)$ modulo translations by vectors from $\operatorname{gp}(S)$, we obtain a complete generalization of Theorem 4.1:

Theorem 5.2. *For every $m \in \mathbb{Z}_+$ there exist only finitely many isomorphism classes of ξ-convex ideals such that a representative I has $\mu(I) \le m$.*

There is no need for a corollary regarding the Cohen–Macaulay property, since Cohen–Macaulay fractional ideals are automatically divisorial. As outlined in Remark 4.3, Theorem 5.2 has a purely combinatorial statement (and, by the way, has been proved by purely combinatorial arguments).

Remark 5.3. (a) Let us set $\operatorname{Eff}(\mathbb{Z}^n;\xi) = \{\operatorname{eff}(a;\xi)\colon a \in \mathbb{Z}^n\}$. Then it is not hard to show that $\operatorname{Eff}(\mathbb{Z}^n;\xi)$ is a subsemigroup of $\mathbb{Z}^n$ containing $\xi(\operatorname{gp}(S))$, and it follows immediately from Proposition 5.1 that the semigroup $\operatorname{Cl}(R;\xi) = \operatorname{Eff}(\mathbb{Z}^n;\xi)/\xi(\operatorname{gp}(S))$ parametrizes the isomorphism classes of ξ-convex ideals.

For the converse of Proposition 5.1(c) one has to replace "torsion class" (in $\operatorname{Cl}(R)$) by "torsion class in $\operatorname{Cl}(R;\xi)$".

Theorem 4.5 generalizes to arithmetic progressions in $\operatorname{Cl}(R;\xi)$. We leave the details to the reader. If $\operatorname{Cl}(R;\xi)$ is always finitely generated, then the second proof of Theorem 4.1 can also be generalized.

(b) Theorem 5.2 can be generalized to arbitrary normal affine semigroups in the same way as Theorem 4.1 was generalized in Remark 4.3.

(c) It is necessary to fix ξ in Theorem 5.2. Already for $S = \mathbb{Z}_+^2$ one can easily find infinitely many pairwise non-isomorphic ideals generated by 2 elements such that each of them is ξ-convex for a suitable ξ.

6. On the growth of Hilbert functions

We introduce some terminology: if S is a subsemigroup of an abelian group G, then $T \subset G$ is an S-module if $S + T \subset T$ (the case $T = \emptyset$ is not excluded). If S is finitely generated and T is a finitely generated S-module, then every S-module $T' \subset T$ is also finitely generated. For example, this follows by "linearization" with coefficients in a field K: $M = KT \subset K[G]$ is a finitely generated module over the noetherian ring $R = K[S]$, and so all its submodules are finitely generated over R. For KT' this implies the finite generation of T' over S.

First we note a result on the finite generation of certain subalgebras of graded algebras and submodules of graded modules. We do not know of a reference covering it in the generality of Theorem 6.1.

Gordan's lemma says that a subsemigroup $S \subset \mathbb{Z}^n$ is finitely generated if and only if the cone $C(S) \subset \mathbb{R}^n$ is finitely generated. It implies that the integral closure $\widehat{S}$ of an affine subsemigroup S in $\mathbb{Z}^n$ is finitely generated, since $C(S) = C(\widehat{S})$. The reader may check that we do not use Gordan's lemma in the proof of Theorem 6.1. We will however use that a finitely generated cone has only finitely many support hyperplanes and that $\widehat{S} = C(S) \cap \mathbb{Z}^n$.

Theorem 6.1. *Let G be a finitely generated abelian group, S a finitely generated subsemigroup of G, and $T \subset G$ a finitely generated S-module. Furthermore let R be a noetherian G-graded ring and M a G-graded finitely generated R-module. Then the following hold:*

(a) *R_0 is noetherian ring, and each graded component M_g, $g \in G$, of M is a finitely generated R_0–module.*
(b) *$A = \bigoplus_{s\in S} R_s$ is a finitely generated R_0-algebra.*
(c) *$N = \bigoplus_{t\in T} M_t$ is a finitely generated A-module.*

Proof. (a) One easily checks that $M'R \cap M_g = M'$ for each R_0-submodule M' of M_g. Therefore ascending chains of such submodules M' of M_g are stationery.

(b) First we do the case in which G is torsionfree, $G = \mathbb{Z}^m$, and S is an integrally closed subsemigroup of $\mathbb{Z}^m$.

Let $\varphi\colon \mathbb{Z}^m \to \mathbb{Z}$ be a non-zero linear form. It induces a $\mathbb{Z}$-grading on R with $\deg_{\mathbb{Z}}(a) = \varphi(\deg_{\mathbb{Z}^M}(a))$ for each non-zero $\mathbb{Z}^m$-homogeneous element of R. Let R' denote R with this $\mathbb{Z}$-grading. Set $R'_- = \bigoplus_{k\le 0} R'_k$ and define R'_+ is analogously. By [BH, 1.5.5] the R'_0-algebras R'_+ and R'_- are finitely generated R'_0-algebras, and R'_0 is a noetherian ring (by (a)). On the other hand, R'_0 is a $(\operatorname{Ker}\varphi)$-graded ring in a natural way, and by induction we can conclude that R'_0 is a finitely generated R_0-algebra.

If $S = \mathbb{Z}^m$, then it follows immediately that R, the sum of R_- and R_+ as an R_0-algebra, is again a finitely generated R_0-algebra.

Otherwise $S = \mathbb{Z}^m \cap C(S)$, and $C(S)$ has at least one support hyperplane:

$$S = \{s \in \mathbb{Z}^m\colon \alpha_i(s) \ge 0,\ i = 1,\dots,v\}$$

with $v \ge 1$. We use induction on v, and the induction hypothesis applies to $R' = \bigoplus_{s\in S'} R_s$,

$$S' = \{s \in \mathbb{Z}^m\colon \alpha_i(s) \ge 0,\ i = 1,\dots,v-1\}.$$

Applying the argument above with $\varphi = \alpha_v$, one concludes that $A = R'_+$ is a finitely generated R_0-algebra.

In the general case for G and S we set $G' = G/H$ where H is the torsion subgroup of G, and denote the natural surjection by $\pi\colon G \to G'$. Let R' be R with the G'-grading induced by π (its homogeneous components are the direct sums of the components R_g where g is in a fixed fiber of π). Let S' be the integral closure of $\pi(S)$ in G'. Then $A' = \bigoplus_{s'\in S'} R'_{s'}$ is a finitely generated algebra over the noetherian ring R'_0, as we have already shown. But R'_0 is a finitely generated module over R_0 by (a), and so A' is a finitely generated R_0-algebra. In particular, R itself is finitely generated over R_0.

It is not hard to check that A' is integral over A; in fact, each element $s \in \pi^{-1}(S')$ has a power $s^n \in S$ for suitable $n \in \mathbb{N}$. Furthermore it is a finitely generated A-algebra, and so a finitely generated A-module. But then a lemma of Artin and Tate (see Eisenbud [Ei, p. 143]) implies that A is noetherian. As shown above, noetherian G-graded rings are finitely generated R_0-algebras.

(c) By hypothesis, T is the union of finitely many translates $S + t$. Therefore we can assume that $T = S + t$. Passing to the shifted module $M(-t)$ (given by $M(-t)_g = M_{g-t}$), we can even assume that $S = T$. Now the proof follows the same pattern as that of (b). In order to deal with an integrally closed subsemigroup of a free abelian group $G = \mathbb{Z}^m$, one notes that M_+ is a finitely generated module over R_+ where M_+ is the positive part of M with respect to a $\mathbb{Z}$-grading (induced by a linear form $\varphi\colon \mathbb{Z}^m \to \mathbb{Z}$). This is shown as follows: the extended module RM_+ is finitely generated over R , and every of its generating systems $E \subset M_+$ together with finitely many components M_i, $i \geq 0$, generate M_+ over R_+; furthermore the M_i are finitely generated over R_0 by (a).

For the general situation we consider N' defined analogously as A'. It is a finitely generated A'-module by the previous argument. Since A' is a finitely generated A-module, N' is finitely generated over A, and so is its submodule N. □

We note a purely combinatorial consequence.

Corollary 6.2. *Let S and S' be affine subsemigroups of $\mathbb{Z}^m$, $T \subset \mathbb{Z}^m$ a finitely generated S-module, and $T' \subset \mathbb{Z}^m$ a finitely generated T-module. Then $S \cap S'$ is an affine semigroup, and $T \cap T'$ is a finitely generated $S \cap S'$-module.*

Proof. We choose a field K of coefficients and set $R = K[S']$, $M = KT'$. Then the hypotheses of the theorem are satisfied, and it therefore implies the finite generation of

$$A = \bigoplus_{s \in S} R_s = K[S \cap S'], \qquad \text{and} \qquad N = \bigoplus_{t \in T} M_t = K(T \cap T').$$

as a $K = R_0$-algebra and an A-module respectively. However, finite generation of the "linearized" objects is equivalent to that of the combinatorial ones. □

The next theorem is our main result on the growth of Hilbert functions. Note that we do not assume that $R_0 = K$; the graded components of R and M may even have infinite K-dimension.

Theorem 6.3. *Let K be a field, G a finitely generated abelian group, R a noetherian G-graded K-algebra, and M a finitely generated G-graded R-module. Define S to be the subsemigroup of G generated by the elements $\deg r$, $r \in R \setminus \{0\}$ homogeneous, and define T to be the S-submodule of G generated by the elements $\deg x$, $x \in M \setminus \{0\}$ homogeneous. Furthermore let H be the G-graded Hilbert function, $H(M,t) = \dim_K M_t$ for all $t \in G$.*

Suppose $\lim_{k\to\infty} H(M, kc + d) = \infty$ for all choices of $c \in T$, c not a torsion element of G, and $d \in T$. Then

$$\#\{t \in T : H(M,t) \leq C\} < \infty$$

for all $C \in \mathbb{Z}_+$.

Proof. Note that S is a finitely generated subsemigroup of G, and T is a finitely generated S-module, generated by the degrees of the elements in a finite generating system of homogeneous elements of R as an R_0-algebra and M as an R-module respectively. (The finite generation follows from Theorem 6.1.)

We split G as a direct sum of a torsionfree subgroup L and its torsion subgroup G_{tor}. Let $R' = \bigoplus_{\ell \in L} R_\ell$, and split M into the direct sum

$$M = \bigoplus_{h \in G_{\mathrm{tor}}} M'_h, \qquad M'_h = \bigoplus_{\ell \in L} M_{(\ell,h)}.$$

By Theorem 6.1 R' is a finitely generated R_0-algebra and M'_h is a finitely generated L-graded R'-module for all $h \in G_{\mathrm{tor}}$, and since the hypothesis on the Hilbert function is inherited by M'_h, it is enough to do the case $G = L = \mathbb{Z}^m$.

We use induction on m. In the case $m = 1$ the hypothesis contains the conclusion.

As a first step we want to improve the hypothesis on the Hilbert function from a "1-dimensional " condition to a "1-codimensional" condition by an application of the induction hypothesis.

Let U be a proper subgroup of L and $u \in L$. Then U is finitely generated as a subsemigroup. We set

$$R' = \bigoplus_{s \in U} R_s \quad \text{and} \quad M' = \bigoplus_{t \in U+u} M_t.$$

Theorem 6.1 implies that R' is a finitely generated K-algebra, and M' is a finitely generated R'-module.

After fixing an origin in $U + u$ we can identify it with U. Therefore we can apply the induction hypothesis to R' and M'. It follows that

$$(*) \qquad \#\{t \in T \cap (U + u) : H(t, M) \le C\} < \infty.$$

Now we represent R as the residue class ring of an L-graded polynomial ring P over K in a natural way (in particular the monomials in P are homogeneous in the L-grading). Thus we may assume that R itself is generated by algebraically independent elements as a K-algebra.

Obviously M has a filtration

$$0 = M_0 \subset M_1 \subset \cdots \subset M_n = M$$

where each successive quotient M_{i+1}/M_i is a cyclic L-graded R-module, that is

$$M_{i+1}/M_i \cong (R/I_{i+1})(-s_i)$$

with an L-graded ideal I_{i+1} in R and a shift $s_i \in L$. As far as the Hilbert function is concerned, we can replace M by the direct sum of these cyclic modules. After the introduction of a term order we can replace $R/(I_{i+1})(-s_i)$ by $R/(\mathrm{in}(I_{i+1}))(-s_i)$ where $\mathrm{in}(I_{i+1})$ is the initial ideal. It is well known that $R/\mathrm{in}(I_{i+1})$ has a filtration whose successive quotients are of the form $R/\mathfrak{p}$ with a prime ideal $\mathfrak{p}$ generated by monomials, and therefore by indeterminates of R. (For example, see the proof of [BH, 4.1.3], and use that associated prime ideals of multigraded modules are generated by indeterminates if the multigrading is that induced by the semigroup of all monomials in R.)

Altogether this reduces the problem to the case in which the K-vector space M is isomorphic to the direct sum of vector spaces $P_i(-s_i)$ where P_i a polynomial ring generated by indeterminates with degrees in L, and $s_i \in L$. Furthermore we can use that the Hilbert function of M satisfies condition $(*)$. The Hilbert function now counts the total number of monomials in each degree. Replacing the monomials by their exponent vectors, we can deduce the theorem from the next one. $\square$

Theorem 6.4. *Let G be a finitely generated abelian group, S a finitely generated subsemigroup of G, and T a finitely generated S-submodule of G. Consider maps*

$$\psi_i\colon A_i \to T, \qquad \psi_i(x) = \varphi_i(x) + t_i \text{ for all } x \in A_i$$

where A_i is an affine semigroup, $\varphi_i : A_i \to S$ is a homomorphism of semigroups, and $t_i \in T$, $i = 1, \dots, v$. Furthermore let

$$\Psi\colon A_1 \cup \dots \cup A_v \to T, \qquad \Psi|_{A_i} = \psi_i,$$

be the map defined on the disjoint union of the A_i by all the ψ_i. For $t \in G$ set

$$H(t) = \#\{x \in A_1 \cup \dots \cup A_v : \Psi(x) = t\}.$$

Suppose that $\lim_{k\to\infty} H(kc + d) = \infty$ for all $c \in S$, c not a torsion element of G, and all $d \in T$. Then

$$\#\{t \in T : H(t) \le C\} < \infty$$

for all $C \in \mathbb{Z}_+$.

Proof. In step (a) we prove the theorem under the assumption that $G = L = \mathbb{Z}^m$ for some m and that

$$\#\{t \in T \cap (U + u) : H(t) \le C\} < \infty.$$

for all proper subgroups U of L. This is enough to complete the proof of Theorem 6.3. In step (b) we can then use Theorem 6.3.

(a) The first observation is that we can omit all the maps ψ_i that are injective. This reduces the function H in each degree by at most v, and has therefore no influence on the hypothesis or the desired conclusion.

The difficult case is $C = 0$, and we postpone it. So suppose that we have already shown that the number of "gaps" (elements in T with no preimage at all) is finite. Then we can restrict ourselves to $\operatorname{Im}\Psi$ if we want to show that there are only finitely many elements with at most $C > 0$ preimages.

It is enough to show that the elements in $\operatorname{Im}\psi_i$ with at most C preimages are contained in the union of finitely many sets of the form $U + u$ where U is a proper direct summand of L. Then we can use the hypothesis on the sets $\{x \in T \cap (U + u) : H(x) \le C\}$. We can certainly assume that $v = 1$ and $t_1 = 0$, and have only to consider a *non-injective, surjective* homomorphism $\varphi : A \to S$.

For an ideal (i. e. S-submodule) $I \neq \emptyset$ of S we have that $S \setminus I$ is contained in finitely many sets $U + u$. In fact, I contains an ideal $J \neq \emptyset$ of the normalization $\bar{S}$ of S, namely the conductor ideal $\{s \in S\colon \bar{S} + s \subset S\}$. (This follows from the corresponding theorem of commutative algebra; see [Gu2, Lemma 5.3] where the assertion has been proved under the superfluous condition that S is positive.) Therefore S contains a set $\bar{S} + s$ with $s \in S$. It follows that $\bigl(S \setminus I\bigr) \subset \bigl(\bar{S} \setminus (\bar{S} + s)\bigr)$.

The latter set is contained in finitely many parallels to the facets of S through points of S (in $\operatorname{gp}(S)$). Each of these parallels is itself contained in a set of type $U+u$. To sum up, it is enough to find an ideal I in S such that each element of I has at least $C+1$ preimages.

Now we go to A and choose $a \in A$ such that $\bar{A}+a \subset A$ where $\bar{A}$ is again the normalization. The homomorphism φ has a unique extension to a group homomorphism $\operatorname{gp}(A) \to L$, also denoted by φ. By assumption $\operatorname{Ker}\varphi \neq 0$. A sufficiently large ball B in $\operatorname{gp}(A) \otimes \mathbb{R}$ with center 0 therefore contains $C+1$ elements of $\operatorname{Ker}\varphi$, and there exists $b \in \bar{A}$ for which $B+b$ is contained in the cone $\mathbb{R}_+ A$. Thus $(B \cap \operatorname{Ker}\varphi)+b \subset \bar{A}$. It follows that each element in $I = \varphi(\bar{A}+a+b)$ has at least $C+1$ preimages. Since $\bar{A}+a+b$ is an ideal in A and φ is surjective, I is an ideal in S.

(b) By linearization we now derive Theorem 6.4 from Theorem 6.3. Let K be a field. Then we set $R_i = K[A_i]$, and the homomorphism φ_i allows us to consider R_i as a G-graded K-algebra. Next we choose a polynomial ring P_i whose indeterminates are mapped to a finite monomial system of generators of A_i, and so P_i is also G-graded. Set

$$R = P_1 \otimes_K \cdots \otimes_K P_v \qquad \text{and} \qquad M = R_1(-s_1) \oplus \cdots \oplus R_v(-s_v)$$

Evidently R is a finitely generated G-graded K-algebra; in particular it is noetherian. Moreover R_i is residue class ring of R in a natural way, and therefore $R_i(-s_i)$ can be considered a G-graded R-module. Therefore M is a G-graded R-module whose Hilbert function is the function H of the theorem. $\square$

It remains to do the case $C = 0$. For simplicity we only formulate it under the special assumptions of step (a) in the proof of Theorem 6.4. We leave the general as well as the commutative algebra version to the reader. The semigroups A_i of Theorem 6.4 can now be replaced by their images.

Proposition 6.5. *Let $L = \mathbb{Z}^m$, S an affine subsemigroup of L, T a finitely generated S-submodule of L. Consider subsemigroups $A_1, \dots, A_v$ of L and elements $t_1, \dots, t_v \in T$ such that the set*

$$\mathcal{G} = T \setminus ((A_1+t_1) \cup \cdots \cup (A_v+t_v))$$

of "gaps" satisfies the following condition: for each proper subgroup U of L and each $u \in L$ the intersection $(U+u) \cap \mathcal{G}$ is finite. Then $\mathcal{G}$ is finite.

Proof. Note that T is contained in finitely many residue classes modulo $\operatorname{gp}(S)$. Therefore we can replace each A_i by $A_i \cap \operatorname{gp}(S)$: the intersection of A_i+t_i with a residue class modulo $\operatorname{gp}(S)$ is a finitely generated $A_i \cap \operatorname{gp}(S)$-module by Corollary 6.2.

We order the A_i in such a way that $A_1, \dots, A_w$ have the same rank as S, and $A_{w+1}, \dots, A_v$ have lower rank. Let W be the intersection of $\operatorname{gp}(A_i)$, $i = 1, \dots, w$. Since $\operatorname{gp}(S)/W$ is a finite group, we can replace all the semigroups involved by their intersections with W, and split the modules into their intersection with the residue classes modulo W. We have now reached a situation where $A_i \subset \operatorname{gp}(S)$ for all i, and $\operatorname{gp}(A_i) = \operatorname{gp}(S)$, unless $\operatorname{rank} A_i < \operatorname{rank} S$.

Next one can replace the $A_1, \dots, A_w$ by their normalizations. In this way we fill the gaps in only finitely many $U+u$ (compare the argument in the proof of Theorem 6.4), and therefore we fill only finitely many gaps.

At this point we can assume that $A_1, \dots, A_w$ are integrally closed in L. Furthermore we must have $C(S) \subset C(A_1) \cup \dots \cup C(A_w)$ – otherwise an open subcone of $C(S)$ would remain uncovered, and this would remain so in T: the lower rank semigroups cannot fill it, and neither can it be filled by finitely many translates $U + u$ where U is a proper subsemigroup of S. In fact, $(A_i + t_i) \setminus A_i$ is contained in the union of finitely many such translates, and the same holds for $(C(S) \cap L) \setminus S$. Since $A_1, \dots, A_w$ are integrally closed, we have $S \subset A_1 \cup \dots \cup A_w$.

Now we choose a system of generators $u_1, \dots, u_q$ of T over S. We have

$$T \subset \bigcup_{i,j} A_i + u_j.$$

But $A_i + u_j$ and $A_i + t_i$ only differ in finitely many translates of proper direct subgroups of L parallel to the support hyperplanes of A_i. So in the last step we have filled only finitely many gaps. Since no gaps remain, their number must have been finite from the beginning. □

References

[Bri] M. Brion, *Sur les modules de covariants*, Ann. scient. Éc. Norm. Sup., 4e série, **26** (1993), 1–21.

[BGu] W. Bruns and A. Guerrieri, *The Dedekind–Mertens lemma and determinantal rings*, Proc. Amer. Math. Soc. **127**, (1999), 657–663.

[BH] W. Bruns and J. Herzog. *Cohen–Macaulay rings* (Rev. Ed.). Cambridge University Press, 1998.

[BV] W. Bruns and U. Vetter, *Determinantal rings*, Springer Lecture Notes **1327** (1988).

[Ch] L. Chouinard, *Krull semigroups and divisor class groups*, Canad. J. Math. **33** (1981), 1459–1468.

[Cox] D. A. Cox, *The homogeneous coordinate ring of a toric variety*, J. Algebr. Geom. **4** (1995), 17–50.

[Ei] D. Eisenbud, *Commutative algebra with a view towards algebraic geometry*, Springer 1995.

[Fo] R. M. Fossum, *The divisor class group of a Krull domain*, Springer 1973.

[Gu1] J. Gubeladze, *The elementary action on unimodular rows over a monoid ring*, J. Algebra **148** (1992), 135–161.

[Gu2] J. Gubeladze, *Geometric and algebraic representations of commutative cancellative monoids*, Proc. A. Razmadze Math. Inst., Georg. Acad. Sci. **113** (1995), 31-81.

[Gu3] J. Gubeladze, *The isomorphism problem for commutative monoid rings*, J. Pure Appl. Algebra **129** (1998), 35–65.

[HK] F. Halter-Koch, *Finitely generated monoids, finitely primary monoids and factorization properties of integral domains*, pp. 31–72 in: D. D. Anderson (Ed.), *Factorization in integral domains*, M. Dekker 1997.

[Ho] M. Hochster, *Rings of invariants of tori, Cohen–Macaulay rings generated by monomials, and polytopes*, Ann. Math. **96** (1972), 318–337.

[Hu] J. E. Humphreys, *Linear algebraic groups*, Springer 1975.

[St1] R. P. Stanley, *Hilbert functions of graded algebras*, Adv. in Math. **28** (1978), 57–83.

[St2] R. P. Stanley, *Linear diophantine equations and local cohomology*, Invent. math. **68** (1982), 175–193.

[St3] R. P. Stanley, *Combinatorics and commutative algebra* (2nd ed.), Birkhäuser 1996.

Universität Osnabrück, FB Mathematik/Informatik, 49069 Osnabrück, Germany
E-mail address: Winfried.Bruns@mathematik.uni-osnabrueck.de

A. Razmadze Mathematical Institute, Alexidze St. 1, 380093 Tbilisi, Georgia
E-mail address: gubel@rmi.acnet.ge