Short generating functions for some semigroup algebras

Graham Denham*

Department of Mathematics

University of Western Ontario

London, Ontario, Canada

gdenham@uwo.ca

Submitted: Aug 26, 2003; Accepted: Sep 7, 2003; Published: Sep 17, 2003

MR Subject Classifications: 05A15, 13P10

Abstract

Let $a_1, a_2, \ldots, a_n$ be distinct, positive integers with $(a_1, a_2, \ldots, a_n) = 1$, and let k be an arbitrary field. Let $H(a_1, \ldots, a_n; z)$ denote the Hilbert series of the graded algebra $\mathrm{k}[t^{a_1}, t^{a_2}, \ldots, t^{a_n}]$. We show that, when $n = 3$, this rational function has a simple expression in terms of a_1, a_2, a_3; in particular, the numerator has at most six terms. By way of contrast, it is known that no such expression exists for any $n \geq 4$.

1 Introduction

The algebra $\mathrm{k}[t^{a_1}, \ldots, t^{a_n}]$ is, variously, the semigroup algebra of a subsemigroup of $\mathbf{Z}_+$, and the coordinate ring of a monomial curve. Our point of view will be combinatorial: let $S \subseteq \mathbf{Z}$ be the set of all nonnegative integer linear combinations of $\{a_1, a_2, \ldots, a_n\}$. Then, by definition,

$$H(a_1, \ldots, a_n; z) = \sum_{k \in S} z^k.$$

By assuming the a_i's have no common factor, it is apparent that the coefficient of z^k is 1 for sufficiently large k. Finding the the largest k for which the coefficient is zero or, equivalently, the largest integer k that is not a $\mathbf{Z}_+$-linear combination of elements of S, is known as Frobenius' problem: references are found in the paper of Székely and Wormald, [12].

For $n = 2$, it happens that $H(a_1, a_2; z) = (1 - z^{a_1 a_2})(1 - z^{a_1})^{-1}(1 - z^{a_2})^{-1}$. This appears in [12, Theorem 1] but apparently was also known to Sylvester, reported in [8].

*partially supported by a grant from NSERC of Canada

When $n = 3$, a similar formula holds: this is stated here as Theorem 1, the main point of this note.

Let $R = \mathrm{k}[x_1, x_2, \ldots, x_n]$ be the polynomial ring graded by $\deg x_i = a_i$, for $1 \le i \le n$. Let π be the map induced by $\pi(x_i) = t^{a_i}$, and let I be the kernel of π, so that $\mathrm{k}[t^{a_1}, \ldots, t^{a_n}] \cong R/I$. If $n = 2$, then I is principal. If $n = 3$, Herzog [6] shows that I has either two or three generators. By contrast, for any fixed integers $n \ge 4$ and $m \ge 1$, Bresinsky shows in [4] that there exist choices of $a_1, \ldots, a_n$ for which I requires at least m generators. It follows that, for any $n \ge 4$, there is no way to write

$$H(a_1, \ldots, a_n; z) = \frac{f(a_1, \ldots, a_n; z)}{(1 - z^{a_1}) \cdots (1 - z^{a_n})}$$

so that the polynomial f has a bounded number of nonzero terms for all choices of $a_1, \ldots, a_n$. This is also made explicit in [12, Theorem 3]. That is, the generating function $H(a_1, \ldots, a_n; z)$ changes qualitatively once n exceeds 3.

Nevertheless, Barvinok and Woods show in [3] that, for any fixed n, an expression for $H(a_1, \ldots, a_n; z)$ can be computed in polynomial time. This is a special case of a more general algorithmic theory, for which one should also read the survey [2].

Theorem 1 is a refinement of [12, Theorem 2], which shows that one can write the Hilbert series when $n = 3$ using at most twelve terms in the numerator. Our proof makes use of a free resolution of R/I, which we note could be deduced in particular as a special case of a general method due to Peeva and Sturmfels, [10]. The commutative algebra here is by no means new, then, and our objective is only to draw attention to its combinatorial consequences, in a way that is semi-expository and self-contained, given a reference such as [5].

2 Proof of Theorem 1

For all that follows, fix $n = 3$. We shall regard $R/I \cong \mathrm{k}[t^{a_1}, t^{a_2}, t^{a_3}]$ as a R-module. Since $\mathrm{pd}_R R/I = 2$, there is a free resolution of the form

$$0 \longrightarrow F_2 \xrightarrow{\phi} F_1 \longrightarrow R \xrightarrow{\pi} \mathrm{k}[t^{a_1}, t^{a_2}, t^{a_3}] \longrightarrow 0, \tag{2.1}$$

where $F_1 = R^k$ and $F_2 = R^{k-1}$, and k is the number of generators of I. By [6], k may be taken to be 2 or 3, depending on (a_1, a_2, a_3): for the reader's convenience, we make this explicit in the following pair of lemmas.

Definition 2.1 Choose binomials p_1, p_2 and p_3 as follows. Let

$$p_1 = x_1^{r_1} - x_2^{s_{12}} x_3^{s_{13}}, \quad p_2 = x_2^{r_2} - x_1^{s_{21}} x_3^{s_{23}}, \quad p_3 = x_3^{r_3} - x_1^{s_{31}} x_2^{s_{32}},$$

where each r_i is the minimum positive integer for which the equation $r_i a_i = \sum_{j \ne i} s_{ij} a_j$ admits a solution in nonnegative integers. Equivalently, r_i is the minimum positive integer for which there exists a p_i as above satisfying $\pi(p_i) = 0$.

Lemma 2.2 *Given a triple* (a_1, a_2, a_3)*, either:*

(N) $s_{ij} \neq 0$ *for all* $i \neq j$*, or*

(C) *Two of the binomials above are the same up to sign:* $p_i = -p_j$ *for some* i, j*, and the third binomial* $p_k = x_k^{r_k} - x_i^{s_{ki}} x_j^{s_{kj}}$ *has both* s_{ki} *and* s_{kj} *strictly positive.*

Proof: Either all s_{ij} are nonzero or, without loss of generality, $s_{13} = 0$. Then we show that $p_2 = -p_1$ as follows. First, s_{23} must also be zero: to prove it, suppose not. By the minimality of the r_i's, $r_2 \leq s_{12}$. It is not hard to see that $s_{21} > 0$, by our assumption that $\gcd(a_1, a_2, a_3) = 1$. Then one replaces $x_2^{r_2}$ in p_1 with $x_1^{s_{21}} x_3^{s_{23}}$ to obtain $x_1^{r_1} - x_1^{s_{21}} x_2^{s_{12}-r_2} x_3^{s_{23}}$; then dividing through by the common, nonzero power of x_1 gives a binomial p_1' for which $\pi(p_1') = 0$, contradicting the minimality of r_1. This means that the first two equations have the form

$$p_1 = x_1^{r_1} - x_2^{s_{12}} \text{ and } p_2 = x_2^{r_2} - x_1^{s_{21}}.$$

By the minimality of r_1, we have $\gcd(r_1, s_{12}) = 1$. Then (s_{21}, r_2) is a multiple of (r_1, s_{12}); by minimality again, these pairs must be equal. This completes the proof. $\square$

Remark 2.3 We will say that a triple is either type (**C**) or (**N**) according to the cases in Lemma 2.2. It is shown in [6] that I is a complete intersection iff (a_1, a_2, a_3) is type (**C**).

Lemma 2.4 ([6]) *Let* $I = \ker \pi$ *as above. Then* I *is generated by* $\{p_1, p_2, p_3\}$*.*

Proof: First observe that I is generated over k by all homogeneous binomials $x_1^{\alpha_1} x_2^{\alpha_2} x_3^{\alpha_3} - x_1^{\beta_1} x_2^{\beta_2} x_3^{\beta_3}$. (Recall $\deg x_i = a_i$.) Using multiplication by each x_i, one can see that I is generated as an ideal by homogeneous binomials of the form $x_i^{\alpha} - \prod_{j \neq i} x_j^{\beta_j}$. Now use induction on the degree of such binomials.

Let $J = \langle p_1, p_2, p_3 \rangle$. If $J \neq I$, then choose $b = x_i^{\alpha} - \prod_{j \neq i} x_j^{\beta_j}$ of smallest degree in $I \backslash J$. By the minimality of r_i, we must have $\alpha \geq r_i$. Without loss of generality assume $i = 1$, and use p_1 to form the binomial

$$b' = x_1^{\alpha - r_1} x_2^{s_{12}} x_3^{s_{13}} - x_2^{\beta_2} x_3^{\beta_3}.$$

Now $b = b' \mod J$, so we find $b' \in I \backslash J$ also. Now a contradiction arises if both s_{12} and s_{13} are nonzero: then either $b' = x_i b''$ for some binomial b'' and $i = 2$ or 3. The degree of b'' is less than that of b, so $b'' \in J$; therefore b' would be too.

Consequently, either $s_{12} = \beta_3 = 0$ or $s_{13} = \beta_2 = 0$. Again, without loss of generality, assume the latter. This means (a_1, a_2, a_3) is type (**C**), so $b' = x_1^{\alpha - r_1} x_2^{r_2} - x_3^{\beta_3}$ and $\alpha - r_1 > 0$. By the minimality of r_3, we see that $\beta_3 \geq r_3$, so we can use p_3 to form a new binomial $b'' = x_1^{\alpha - r_1} x_2^{r_2} - x_3^{\beta_3 - r_3} x_1^{s_{31}} x_2^{s_{32}}$ in $I \backslash J$. Now both s_{31} and s_{32} are strictly positive (Lemma 2.2, case (**C**)). Thus one can divide b'' by one of x_1 or x_2, again contradicting the minimality of $\deg b$. $\square$

In type (**C**), then, I is generated by two of $\{p_1, p_2, p_3\}$. We will now state our main result, proving at first only the first half.

Theorem 1 *If* (a_1, a_2, a_3) *is type* $(\mathbf{C})$*, then*

$$H(a_1, a_2, a_3; z) \quad = \quad \frac{(1 - z^{a_i r_i})(1 - z^{a_j r_j})}{(1 - z^{a_1})(1 - z^{a_2})(1 - z^{a_3})}, \tag{2.2}$$

where i*,* j *are the indices of the generators given by Lemmas 2.2, 2.4. Otherwise,*

$$H(a_1, a_2, a_3; z) = \frac{1 - z^{a_1 r_1} - z^{a_2 r_2} - z^{a_3 r_3} + z^m + z^n}{(1 - z^{a_1})(1 - z^{a_2})(1 - z^{a_3})}, \tag{2.3}$$

for triples of type $(\mathbf{N})$*, where*

$$\begin{aligned} m &= a_3 s_{23} + a_1 r_1 = a_1 s_{31} + a_2 r_2 = a_2 s_{12} + a_3 r_3, \quad \textit{and} \\ n &= a_2 s_{32} + a_1 r_1 = a_3 s_{13} + a_2 r_2 = a_1 s_{21} + a_3 r_3. \end{aligned}$$

Proof: [Proof of case $(\mathbf{C})$] Reorder the indices so that $i = 1$ and $j = 2$. Let $F_1 = R\langle u_1, u_2 \rangle$, a free R-module. By the work above, the complex

$$F_1 \xrightarrow{\psi} R \longrightarrow R/I \longrightarrow 0 \tag{2.4}$$

is exact, where $u_i \mapsto p_i$, the generators of I. It remains to extend (2.4) to the left by $F_2 = \ker \psi$. Let v be a generator of F_2. The Euler characteristic shows

$$H(F_2, z) - H(F_1, z) + H(R, z) - H(R/I, z) = 0.$$

Then $H(R, z) = (1 - z^{a_1})(1 - z^{a_2})(1 - z^{a_3})$, and since F_1 and F_2 are free,

$$\begin{aligned} H(F_1, z) &= (z^{\deg p_1} + z^{\deg p_2}) H(R, z), \quad \text{and} \\ H(F_2, z) &= z^{\deg v} H(R, z). \end{aligned}$$

Since $\deg p_i = a_i r_i$, formula (2.2) follows from checking $\deg v = \deg p_1 + \deg p_2$.

To do so, suppose for some $r, s \in R$ that $ru_1 + su_2 \in \ker \phi$. That is, $rp_1 + sp_2 = 0$. By minimality, p_1 and p_2 have no common factor, so $(s, -r)$ must be a multiple of (p_1, p_2). That is, $(-u_2, u_1)$ generates $\ker \phi$, and it has degree $\deg u_1 + \deg u_2$. $\square$

For triples (a_1, a_2, a_3) of type $(\mathbf{N})$, the resolution is more interesting, and it will help to describe the map ϕ as follows.

Lemma 2.5 *If* (a_1, a_2, a_3) *is type* $(\mathbf{N})$*, then* $\phi : F_2 \to F_1$ *can be written as a matrix*

$$M = \begin{pmatrix} x_3^{s_{23}} & x_1^{s_{31}} & x_2^{s_{12}} \\ x_2^{s_{32}} & x_3^{s_{13}} & x_1^{s_{21}} \end{pmatrix}.$$

Proof: The idea is to verify that the 2×2 minors of M are p_1, p_2, and p_3. Then, by the Hilbert-Burch Theorem, the image of a 2×3 matrix is generated by its 2×2 minors, which shows (2.1) is exact.

The minor obtained by deleting column i above is, up to sign, $x_i^{s_{i-1,i}+s_{i+1,i}} - \prod_{j\neq i} x_j^{s_{ij}}$, writing the indices cyclically. Since $p_i = x_i^{r_i} - \prod_{j\neq i} x_j^{s_{ij}}$, we need only check that $r_i = s_{ji} + s_{ki}$, whenever i, j, and k are distinct. Let

$$N = \begin{pmatrix} -r_1 & s_{12} & s_{13} \\ s_{21} & -r_2 & s_{23} \\ s_{31} & s_{32} & -r_3 \end{pmatrix}.$$

Then $N(a_1, a_2, a_3)^t = 0$, and the trace of N is maximal with respect to this property, by construction. By an exercise of linear algebra, the kernel of right-multiplication by N is generated by $(1, 1, 1)$.

□

We may now complete the proof of Theorem 1.

Proof: [Proof of case (**N**)] Now let (a_1, a_2, a_3) be of type (**N**). Write $F_1 = R\langle u_1, u_2, u_3\rangle$ and $F_2 = R\langle v_1, v_2\rangle$, where these bases are chosen so that $\phi : F_2 \to F_1$ is given by right-multiplication by the matrix M from the lemma above. As before, set $\psi(u_i) = p_i$. We find that $\deg u_i = \deg p_i = a_i r_i$, and $\deg v_1 = m$, $\deg v_2 = n$. Then $H(F_2, z) = (z^m + z^n)H(R, z)$, and

$$H(F_1, z) = (z^{\deg p_1} + z^{\deg p_2} + z^{\deg p_3})H(R, z).$$

The Euler characteristic argument, as before, gives (2.3). □

3 Examples

Example 3.1 Consider the triple $(6, 7, 8)$. We find:

$$p_1 = x_1^4 - x_3^3, \quad p_2 = x_2^2 - x_1x_3, \text{ and } p_3 = -p_1.$$

This triple is type (**C**), so p_1 and p_2 generate $\ker\pi : R \to \mathrm{k}[t^6, t^7, t^8]$. Since $\deg p_1 = 24$ and $\deg p_2 = 14$, we see F_1 is generated in degrees 14 and 24, while F_2 is generated in degree 38, giving by (2.2)

$$H(6, 7, 8; z) = \frac{(1 - z^{14})(1 - z^{24})}{(1 - z^6)(1 - z^7)(1 - z^8)}.$$

Example 3.2 On the other hand, the triple $(5, 7, 9)$ is type (**N**):

$$p_1 = x_1^5 - x_2x_3^2, \quad p_2 = x_2^2 - x_1x_3, \text{ and } p_3 = x_3^3 - x_1^4x_2,$$

with degrees 25, 14, and 27, respectively. Then

$$M = \begin{pmatrix} x_3 & x_1^4 & x_2 \\ x_2 & x_3^2 & x_1 \end{pmatrix}.$$

We find that $m = 9 \cdot 1 + 25$ and $n = 7 \cdot 1 + 25$, so by (2.3),

$$H(5, 7, 9; z) = \frac{1 - z^{25} - z^{14} - z^{27} + z^{34} + z^{32}}{(1 - z^5)(1 - z^7)(1 - z^9)}.$$

4 Another Generating Function

Various authors have considered the associated graded ring of $k[t^{a_1}, \ldots, t^{a_n}]$ with respect to filtration by powers of its maximal ideal $\mathfrak{m} = (t^{a_1}, \ldots, t^{a_n})$; for references, see [1, 9]. Denote this ring by $\mathrm{gr}_{\mathfrak{m}} R/I$.

Its Hilbert series is the following generating function: let

$$S_r = \left\{ k \in \mathbf{Z}_+ : k = \sum_{i=1}^{n} \lambda_i a_i, \text{ where } r = \sum_{i=1}^{n} \lambda_i, \text{ and each } \lambda_i \in \mathbf{Z}_+. \right\},$$

for $r \geq 0$, and let $T_r = S_r \setminus \bigcup_{i<r} S_i$. Then $S = \bigcup_{r \geq 0} T_r$, and the Hilbert series is

$$H(\mathrm{gr}_m R/I, z) = \sum_{r \geq 0} |T_r| \, z^r. \tag{4.1}$$

When $n = 3$ and the generators of the ideal I given by Lemma 2.2 form a Gröbner basis, then standard arguments show that the resolution (2.1) passes to $\mathrm{gr}_{\mathfrak{m}} R/I$. In this case, a formula analogous to that of Theorem 1 holds, (4.2) below.

However, $\{p_1, p_2, p_3\}$ need not form a Gröbner basis. In [7, Theorem 3.8] Kamoi gives the following characterization. If (a_1, a_2, a_3) is type ($\mathbf{N}$) and $a_1 < a_2 < a_3$, then clearly $r_1 > s_{12} + s_{13}$ and $r_3 < s_{31} + s_{32}$. However, $\{p_1, p_2, p_3\}$ is a Gröbner basis if and only if $r_2 \geq s_{21} + s_{23}$. It follows from the Gröbner basis criteria given in Sengupta [11] that, in contrast to our previous Hilbert series, (4.1) cannot be written as a quotient with a bounded number of terms in all cases, even for $n = 3$.

In summary, if $a_1 < a_2 < a_3$, then $H(\mathrm{gr}_{\mathfrak{m}} R/I, z) = f(z)/(1-z)^3$, where

$$f(z) = \begin{cases} (1 - z^{\deg p_i})(1 - z^{\deg p_j}) & \text{in case } (\mathbf{C}); \\ (1 - z^{\deg p_1} - z^{\deg p_2} - z^{\deg p_3} + z^m + z^n) & \begin{array}{l}\text{in case } (\mathbf{N}), \\ \text{if } r_2 \geq s_{21} + s_{23};\end{array} \\ ? & \text{otherwise.} \end{cases} \tag{4.2}$$

where i and j are the indices of generators of I in the first case, $m = r_1 + \max\{s_{32}, s_{21}\}$, and $n = r_2 + \max\{s_{31}, s_{12}\}$. Note that, unlike before, degrees are taken with respect to the standard $\mathbf{Z}$-grading of R, so $\deg p_i = \max\{r_i, s_{ij} + s_{ik}\}$, where i, j, and k are distinct.

References

[1] Feza Arslan, *Cohen-Macaulayness of tangent cones*, Proc. Amer. Math. Soc. **128** (2000), no. 8, 2243–2251. MR 2000k:13021

[2] Alexander Barvinok and James E. Pommersheim, *An algorithmic theory of lattice points in polyhedra*, New perspectives in algebraic combinatorics (Berkeley, CA, 1996–97), Math. Sci. Res. Inst. Publ., vol. 38, Cambridge Univ. Press, Cambridge, 1999, pp. 91–147. MR 2000k:52014

[3] Alexander Barvinok and Kevin Woods, *Short rational generating functions for lattice point problems*, J. Amer. Math. Soc. **16** (2003), 957–979.

[4] H. Bresinsky, *On prime ideals with generic zero $x_i = t^{n_i}$*, Proc. Amer. Math. Soc. **47** (1975), 329–332. MR 52 #10741

[5] David Eisenbud, *Commutative algebra*, Graduate Texts in Mathematics, vol. 150, Springer-Verlag, New York, 1995, With a view toward algebraic geometry. MR 97a:13001

[6] Jürgen Herzog, *Generators and relations of abelian semigroups and semigroup rings.*, Manuscripta Math. **3** (1970), 175–193. MR 42 #4657

[7] Yuuji Kamoi, *Defining ideals of Cohen-Macaulay semigroup rings*, Comm. Algebra **20** (1992), no. 11, 3163–3189. MR 94a:13023

[8] Jürgen Kraft, *Singularity of monomial curves in $\mathbf{A}^3$ and Gorenstein monomial curves in $\mathbf{A}^4$*, Canad. J. Math. **37** (1985), no. 5, 872–892. MR 86m:14020

[9] S. Molinelli and G. Tamone, *On the Hilbert function of certain rings of monomial curves*, J. Pure Appl. Algebra **101** (1995), no. 2, 191–206. MR 96g:13020

[10] Irena Peeva and Bernd Sturmfels, *Syzygies of codimension 2 lattice ideals*, Math. Z. **229** (1998), no. 1, 163–194. MR 99g:13020

[11] Indranath Sengupta, *A Gröbner basis for certain affine monomial curves*, Comm. Algebra **31** (2003), no. 3, 1113–1129. MR 1 971 052

[12] L. A. Székely and N. C. Wormald, *Generating functions for the Frobenius problem with 2 and 3 generators*, Math. Chronicle **15** (1986), 49–57. MR 88i:05013