NON-COHEN-MACAULAY PROJECTIVE MONOMIAL CURVES

LES REID AND LESLIE G. ROBERTS

Abstract. We compare several ways of describing how far the homogeneous coordinate ring of a projective monomial curve is from being Cohen-Macaulay. We give a number of examples and then use these ideas to show that the fraction of projective monomial curves of a given degree that are Cohen-Macaulay approaches zero as the degree goes to infinity.

1. Introduction

Let $\mathscr{S} = \{a_1, \ldots, a_k\}$ be a sequence of integers with $0 < a_1 < \cdots < a_k = d$ and $\gcd(a_1, \ldots, a_k) = 1$. Let $\Gamma_{\mathscr{S}}$ (or simply Γ if there is no ambiguity) be the numerical semigroup generated by $\mathscr{S}$. To $\mathscr{S}$ we associate the semigroup $S_{\mathscr{S}}$ (or simply S) generated by $\{(d, 0), (d-a_1, a_1), (d-a_2, a_2) \cdots (d-a_{k-1}, a_{k-1}), (0, d)\}$, and the rings $R_{\mathscr{S}} = K[s^d, s^{d-a_1}t^{a_1}, s^{d-a_2}t^{a_2}, \ldots, t^d]$ (or simply R) and $\mathrm{gr}(\mathscr{S})$ (defined below). Here K can be any field. Note that $R_{\mathscr{S}} \cong K[S]$, the semigroup ring of S. The quotient group of $S_{\mathscr{S}}$ will be denoted $G_{\mathscr{S}}$ (or simply G, or G_d if we wish to indicate what d is) and (because of our assumption that $\gcd(a_1, \ldots, a_k) = 1$) is equal to $\{(x, y) \in \mathbb{Z}^2 | x + y \equiv 0 \mod d\}$. We assume that $\gcd(a_1, \ldots, a_k) = 1$, because if not, one could divide all the a_i by their gcd and obtain an isomorphic semigroup. Furthermore, assuming that $\gcd(a_1, \ldots, a_k) = 1$ ensures that there are elements of Γ in each congruence class mod d. The generating set $\{(d, 0), (d-a_1, a_1), (d-a_2, a_2) \cdots (d-a_{k-1}, a_{k-1}), (0, d)\}$ is the Hilbert basis $\mathrm{Hilb}(S)$ of S in the language of [1]. The scheme $\mathrm{Proj}(R_{\mathscr{S}})$ is a projective monomial curve of degree d whose homogeneous coordinate ring is $R_{\mathscr{S}}$. We will informally identify $\mathscr{S}$ with the curve.

In this paper we first compare several ways of describing how far R is from being Cohen-Macaulay. In Section 3 we illustrate our theory with an easy example. Then in Section 4 we we apply our results to the more

---

2000 *Mathematics Subject Classification.* Primary 14M05.

This work was partially supported by the NSERC grant of the second author. The first author thanks the Department of Mathematics and Statistics, Queen's University, Kingston, Canada for its hospitality.

complicated examples of [6], gaining new insight into what is special about these examples. Then in Section 5 we prove that as d goes to infinity the fraction of the rings $R_{\mathscr{S}}$ that are Cohen-Macaulay goes to 0 (as $\mathscr{S}$ ranges over all sequences $\{a_1, \ldots, a_k\}$ with $0 < a_1 < \cdots < a_k = d$ as above). In Section 6 we present some numerical results illustrating the previous work. Note that if $k = 1$ then we have only $\mathscr{S} = \{1\}$ (corresponding to $S = \mathbb{N}^2$) and if $k = 2$ then R is always Cohen-Macaulay.

Throughout, $\mathbb{N}$ denotes the natural numbers $\{0, 1, 2, 3, \cdots\}$. All our semigroups are contained in $\mathbb{N}^n$ for some integer $n > 0$, and contain 0. A numerical semigroup is a subsemigroup of $\mathbb{N}$. The cardinality of a set X is denoted by $|X|$.

For $x \in \Gamma$, $\mathrm{ord}_{\mathscr{S}}(x)$ was defined in [7] to be the smallest integer n such that x can be written as the sum of n elements of $\mathscr{S}$ (repetition allowed). The ring $R_{\mathscr{S}}$ is graded by assigning degree 1 to its algebra generators. That is, if $s^i t^j \in R_{\mathscr{S}}$ then $s^i t^j$ is assigned degree $(i + j)/d$ as an element of R. (Note that $i + j$ is a multiple of d). Similarly if $(x, y) \in G_{\mathscr{S}}$ define $\deg(x, y) = (x + y)/d$. It is easily seen that if $x \in \Gamma$ then $\mathrm{ord}_{\mathscr{S}}(x)$ is the smallest integer n such that $s^{nd-x}t^x \in R$. In [7] the ring $\mathrm{gr}(\mathscr{S})$ is defined to be the K-vector space with basis $\{t^n \mid n \in \Gamma\}$ and multiplication defined by

$$t^a \cdot t^b := \begin{cases} t^{a+b}, & \text{if } \mathrm{ord}_{\mathscr{S}}(a+b) = \mathrm{ord}_{\mathscr{S}}(a) + \mathrm{ord}_{\mathscr{S}}(b). \\ 0, & \text{otherwise.} \end{cases} \tag{1}$$

The ring $\mathrm{gr}(\mathscr{S})$ is graded by $\deg(t^a) = \mathrm{ord}_{\mathscr{S}}(a)$. Then it is easily checked that $R/s^dR \cong \mathrm{gr}(\mathscr{S})$ (as graded rings) with the class of $s^{nd-x}t^x$ in R/s^dR corresponding to t^x (where $\mathrm{ord}_{\mathscr{S}}(x) = n$). Since $\{s^d, t^d\}$ is a homogeneous system of parameters of $R_{\mathscr{S}}$, $R_{\mathscr{S}}$ is Cohen-Macaulay if and only if t^d is a non-zero-divisor in $\mathrm{gr}(\mathscr{S})$. Integers $x \in \Gamma$ were defined in [6] to be unstable if t^x is killed by some power of t^d in $\mathrm{gr}(\mathscr{S})$, equivalently there exists a positive integer i such that $\mathrm{ord}_{\mathscr{S}}(x + id) < \mathrm{ord}_{\mathscr{S}}(x) + i$. Let T be the subsemigroup of S generated by $(d, 0)$ and $(0, d)$. The spanning set of S over T is defined in [5] to be $\mathcal{B} = \{\sigma \in S | \sigma \text{ cannot be written in the form } \sigma = \sigma' + \tau \text{ with } \tau \in T,\ \sigma' \in S\}$. It is shown in [5] that a minimal generating set of R as a module over $K[s^d, t^d] \cong K[T]$ is $\{(s^a t^b | (a, b) \in \mathcal{B}\}$, and that R is a free T-module if and only if $\mathcal{B}$ contains d elements. Furthermore it is well known (or true by definition in some developments of the theory) that R is Cohen-Macaulay if and only if R is a free T-module (see for example [3, Proposition 2.5.3]).

In [4] and [8] the semigroup S' is defined to be $\{\sigma \in G_{\mathscr{S}} | \sigma + a(0,d) \in S$ and $\sigma + b(d,0) \in S$ for some $a, b \geq 0\}$. By [4], $R_{\mathscr{S}}$ is Cohen-Macaulay if and only if $S' = S$. We will also define $\tilde{S}$ to be $\{\sigma \in G_{\mathscr{S}} | \sigma + (0,d) \in S$ and $\sigma + (d,0) \in S\}$. It is immediate that $S \subseteq \tilde{S} \subseteq S' \subseteq G_{\mathscr{S}} \cap \mathbb{N}^2$. These observations and some minor variants can be summarized in

Theorem 1.1. *Let $\mathscr{S} = \{a_1, \ldots, a_k\}$ be a sequence of integers with $0 < a_1 < \cdots < a_k = d$ and $\gcd(a_1, \ldots, a_k) = 1$, and let $S = S_{\mathscr{S}}$, Γ, T, $R = R_{\mathscr{S}}$, $\tilde{S}$, S', $\mathcal{B}$ and $\mathrm{gr}(\mathscr{S})$ be as defined in the above discussion. Then the following are equivalent.*

1. *R is Cohen-Macaulay.*
2. *R is a free $K[T]$-module.*
3. *The spanning set $\mathcal{B}$ of S over T contains d elements.*
4. $S' \backslash S = \emptyset$
5. $\tilde{S} \backslash S = \emptyset$
6. *Γ contains no unstable elements (which is the same as saying that no non-zero element of $\mathrm{gr}(\mathscr{S})$ is killed by a power of t^d).*
7. *No non-zero element of $\mathrm{gr}(\mathscr{S})$ is killed by t^d .*

Example 1.2. Let $\mathscr{S} = \{1, 5, 6, 7, 8, 9, 11, 13, 15\}$. Then $\tilde{S} \backslash S = \{(13, 2), (27, 3), (41, 4)\}$. We have $(13, 2) + (13, 2) = (26, 4) \notin \tilde{S}$ (because $(26, 4) + (15, 0) = (41, 4) \in \tilde{S} \backslash S$). So $\tilde{S}$ need not be a semigroup.

2. A generalization of Theorem 1.1.

In this section we compare several ways of describing how far R is from being Cohen-Macaulay. The case $a = 0$ of Theorem 2.1 below, together with the observations from [5], give a new proof of Theorem 1.1.

Theorem 2.1. *Let the notation be as in Theorem 1.1. Then the following are equivalent.*

1. *The spanning set $\mathcal{B}$ of S over T contains $d+a$ elements ($a \geq 0$).*
2. $|\tilde{S} \backslash S| = a$.
3. $a = |\{x \in \Gamma | t^x t^d = 0 \text{ in } \mathrm{gr}(\mathscr{S})\}|$

Proof. First consider the equivalence of parts 1 and 2. Choose one particular congruence class mod d of $\mathbb{N}^2 \cap G_{\mathscr{S}}$ and let (α_1, α_2) be the representative of this congruence class with $0 \leq \alpha_i < d$. The points $(\alpha_1 + id, \alpha_2 + jd)$ can be identified with the lattice points $(i, j) \in \mathbb{N}^2$. Let I be the set of all (i, j) that correspond to an element of S. Then I is nonempty and is an "ideal", i.e. if $(i, j) \in I$ then so is (i', j') whenever $i' \geq i$, $j' \geq j$. The minimal elements of I in the product partial ordering on $\mathbb{N}^2$ given by $\leq$ are the elements of $\mathcal{B}$ in the congruence class mod d of (α_1, α_2), and can be visualized as the "corners" of I. Similarly the maximal elements of $\mathbb{N}^2 \backslash I$ correspond to the elements of $\tilde{S} \backslash S$ in this congruence class, and can be visualized as the corners of $\mathbb{N}^2 \backslash I$. Clearly I has one more corner than $\mathbb{N}^2 \backslash I$. Repeating this argument over all d congruence classes we obtain the equivalence of parts 1 and 2.

Now we establish a one-to-one correspondence between $\tilde{S} \backslash S$ and $\{x \in \Gamma | t^x t^d = 0 \text{ in } \mathrm{gr}(\mathscr{S})\}$. Suppose that $(id - x, x) \in \tilde{S} \backslash S$. Then, by definition of $\tilde{S}$, $((i+1)d - x, x) \in S$ and $((id - x, x + d) \in S$, so that $\mathrm{ord}_{\mathscr{S}}(x) = i + 1$ and $\mathrm{ord}_{\mathscr{S}}(x + d) \leq i + 1$. From this it follows that $t^x t^d = 0$ in $\mathrm{gr}(\mathscr{S})$. Conversely suppose that $t^x t^d = 0$ in $\mathrm{gr}(\mathscr{S})$. Clearly $x > d$ so that $\mathrm{ord}_{\mathscr{S}}(x) \geq 2$. Let $i + 1 = \mathrm{ord}_{\mathscr{S}}(x)$. Since $t^x t^d = 0$ in $\mathrm{gr}(\mathscr{S})$ we have that $\mathrm{ord}_{\mathscr{S}}(x+d) \leq i+1$. Then $(id-x, x) \notin S$ but $((i+1)d-x, x) \in S$ and $((id-x, x+d) \in S$, so that $(id-x, x) \in \tilde{S}$. This establishes the equivalence of parts 2 and 3. $\square$

Definition 2.2. Let $\mathscr{S} = \{a_1, \cdots, a_k\}$ with $0 < a_1 < \cdots < a_k = d$ as in the Introduction. Then define the dual of $\mathscr{S}$ to be $\hat{\mathscr{S}} = \{d - a_{k-1}, d - a_{k-2}, \cdots d - a_1, d\}$. The semigroup generated by the elements of $\hat{\mathscr{S}}$ will be denoted by $\hat{\Gamma}$.

It is easily seen that $S_{\hat{\mathscr{S}}} \cong S_{\mathscr{S}}$, by interchanging coordinates. Furthermore Γ is the projection of $S_{\mathscr{S}}$ onto the second coordinate and $\hat{\Gamma}$ is the projection of $S_{\mathscr{S}}$ onto the first coordinate. In the same way as with $\mathscr{S}$, one defines $\mathrm{ord}_{\hat{\mathscr{S}}}(x)$ for any $x \in \hat{\Gamma}$ and uses this to define $\mathrm{gr}(\hat{\mathscr{S}})$, with the result that $R/t^d R \cong \mathrm{gr}(\hat{\mathscr{S}})$. If $x \in \hat{\Gamma}$ with $\mathrm{ord}_{\hat{\mathscr{S}}}(x) = n$, then the class of $s^x t^{nd-x}$ in $R/t^d R$ corresponds to $s^x \in \mathrm{gr}(\hat{\mathscr{S}})$.

We can give more precise information about the correspondences in Theorem 2.1.

Theorem 2.3. *Let the notation be as in Theorem 1.1 and Definition 2.2.*

(1) *The elements x of Γ such that $t^x t^d = 0$ in $\mathrm{gr}(\mathscr{S})$, equivalently $\mathrm{ord}_{\mathscr{S}}(x + d) \leq \mathrm{ord}_{\mathscr{S}}(x)$, are the second coordinates of the elements of $\tilde{S} \backslash S$.*
(2) *The unstable elements of Γ are the second coordinates of the elements of $S' \backslash S$.*
(3) *The corresponding elements of $\hat{\Gamma}$ are the first coordinates of $\tilde{S} \backslash S$, respectively $S' \backslash S$.*

Proof. Part 1 is proved in the proof of Theorem 2.1. Now consider part 2. Suppose that x is the second coordinate of an element of $S' \backslash S$, with $(id - x, x) \in S' \backslash S$. Clearly x is not a multiple of d so $id > x$, and hence $i > 0$. By the definition of S' there exist $a, b > 0$ such that $((i+a)d - x, x)$, $(id - x, x + bd) \in S$. Pick the smallest such a, b. Then $\mathrm{ord}_{\mathscr{S}}(x) = i + a$, and $\mathrm{ord}_{\mathscr{S}}(x + bd) \leq i + b$. Since $b + \mathrm{ord}_{\mathscr{S}}(x) = b + a + i$ we have $\mathrm{ord}_{\mathscr{S}}(x + bd) < b + \mathrm{ord}_{\mathscr{S}}(x)$ so x is unstable. Conversely suppose $x \in \Gamma$ is unstable. Then $\alpha = \mathrm{ord}_{\mathscr{S}}(x + bd) < b + \mathrm{ord}_{\mathscr{S}}(x)$ for some $b \geq 1$. Again we can assume that x is not a multiple of d. Let $\beta = \mathrm{ord}_{\mathscr{S}}(x)$, so $(\beta d - x, x) \in S$ but $((\beta - 1)d - x, x) \notin S$. Since $\alpha = \mathrm{ord}_{\mathscr{S}}(x + bd)$ we have $((\alpha - b)d - x, x + bd) \in S$. But $\alpha < b + \beta$ so also $((\beta - 1)d - x, x + bd) \in S$. Hence $((\beta - 1)d - x, x)$ is an element of $S' \backslash S$ with second coordinate x, as desired, proving part 2. Part 3 follows by interchanging coordinates. $\square$

Remark 2.4. It follows from the equivalence of parts 2 and 3 in Theorem 2.1 that $|\{x \in \Gamma | t^x t^d = 0 \text{ in } \mathrm{gr}(\mathscr{S})\}| = |\{x \in \hat{\Gamma} | s^x s^d = 0 \text{ in } \mathrm{gr}(\hat{\mathscr{S}})\}|$. An independent ring-theoretic proof of this is as follows. For any integral domain A, and $f, g \in A$, let $(f), (g)$ be the ideals of A generated by f and g respectively, and $(f) : (g) = \{x \in A | x(g) \subseteq (f)\}$. We have $(f) : (g) \cong (g) : (f)$ as A-modules. For if $a \in (f) : (g)$ then $ag = bf$ for $b \in A$. Since A is a domain, b is unique. Mapping a to $b \in (g) : (f)$ gives the desired isomorphism. Applying this to $K[S]$ with $f = t^d, g = s^d$ and noting that in this particular case $(f) : (g)$ and $(g) : (f)$ are finite dimensional K-vector spaces with the indicated bases yields the desired result. However Γ and $\hat{\Gamma}$ need not have the same number of unstable elements, as we see in Example 3.1 and in Section 4. Thus the number of unstable elements is not an invariant of R. We might remark that, even though a is an invariant of S, we do not have an interpretation of a in terms of (for example, the cohomology of) R. This is in contrast to the socle of $\mathrm{gr}(\mathscr{S})$ respectively $\mathrm{gr}(\hat{\mathscr{S}})$ (the elements killed by the entire maximal ideal of the respective ring) which does have a cohomological interpretation in terms of R [2, 1.2.15 and 1.2.19].

Now we discuss the "missing elements", i.e. the elements of $(G_{\mathscr{S}} \backslash S) \cap \mathbb{N}^2$.

Definition 2.5. An element (α, β) of $(G_{\mathscr{S}} \backslash S) \cap \mathbb{N}^2$ is stably missing if either $(\alpha, \beta) + a(d, 0) \notin S$ for all $a \geq 0$ or $(\alpha, \beta) + a(0, d) \notin S$ for all $a \geq 0$.

The "stably missing" elements are just the elements of $(G_{\mathscr{S}} \cap \mathbb{N}^2) \backslash S'$, however the terminology is very suggestive. If $(\alpha, \beta) + a(d, 0) \notin S$ for all $a \geq 0$ we say that (α, β) is stably missing horizontally, and if

$(\alpha, \beta)+a(0, d) \notin S$ for all $a \geq 0$ we will say that (α, β) is stably missing vertically.

Lemma 2.6. *An element (α, β) of $(G_{\mathscr{S}} \backslash S) \cap \mathbb{N}^2$ is stably missing if and only if either $\beta \notin \Gamma$ or $\alpha \notin \hat{\Gamma}$. Equivalently $S' = \{(\alpha, \beta\} \in G_{\mathscr{S}} \cap \mathbb{N}^2 | \alpha \in \hat{\Gamma}, \beta \in \Gamma\}$.*

Proof. It follows from the description of the relation between $\mathscr{S}$ and $S_{\mathscr{S}}$ in the Introduction that $(\alpha, \beta)+a(d, 0) \notin S$ for all $a \geq 0$ if and only if $\beta \notin \Gamma$. Similarly by interchanging coordinates $(\alpha, \beta)+a(0, d) \notin S$ for all $a \geq 0$ if and only if $\alpha \notin \hat{\Gamma}$. □

3. An easy example

The above theory is illustrated by the following example.

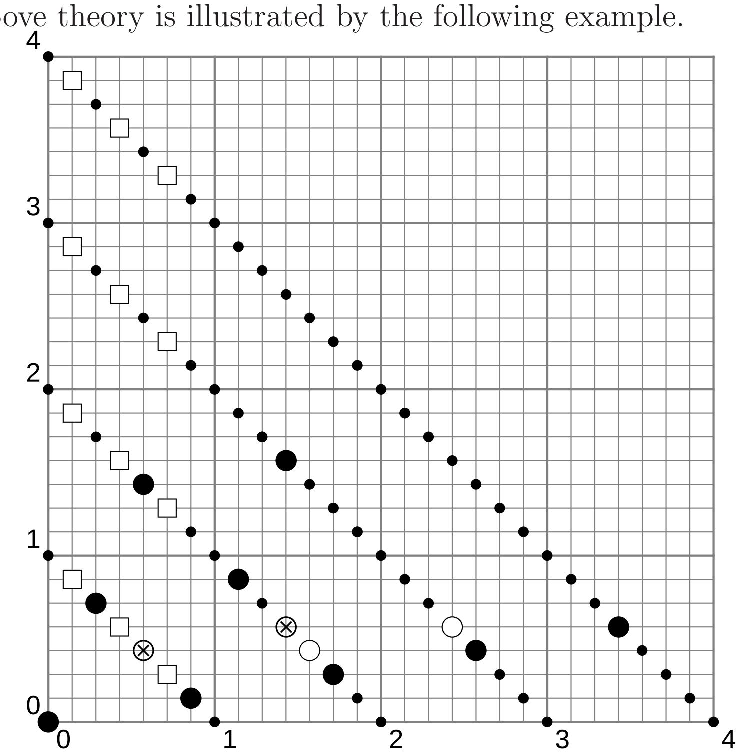

Fig. 1

Example 3.1. Let $\mathscr{S} = \{1, 5, 7\}$. Then $\Gamma = \mathbb{N}$, $\hat{\mathscr{S}} = \{2, 6, 7\}$, $\hat{\Gamma} = \mathbb{N} \backslash \{1, 3, 5\}$. The elements of $S_{\mathscr{S}}$ up to degree 4 are illustrated by solid dots in Figure 1. The origin is at the lower left, with s-axis horizontal and t-axis vertical. The numbers indicate the degree of the elements in the diagonal between them. The large solid dots are the elements of the spanning set $\mathcal{B}$ of S over the subsemigroup generated by $(7, 0)$ and $(0, 7)$. These are identified graphically by the observation that one does not remain in S if one moves either 7 units left or 7 units down. The small solid dots are the remaining elements of S. The open squares are the stably missing elements, namely $(1,6),(3,4),(5,2)$ and all vertical translations of these. These correspond to the complement of $\hat{\Gamma}$ as explained in the proof of Lemma 2.6. Since $\Gamma = \mathbb{N}$, no elements are stably missing horizontally. The open circles $(11,3),(17,4)$ are the elements of $\tilde{S}\backslash S$ and are identified graphically by the observation that one moves into S if one moves 7 units to the right and also if one moves 7 units up. The open circles $(4,3),(10,4)$ with the $\times$ in them are the remaining elements of $S'\backslash S$. They are identified graphically by the observation that one gets into S by moving both in the horizontal and vertical directions, but one of these directions (here horizontal) requires movement by more that one multiple of d. The unstable elements of $\hat{\mathscr{S}}$ are 4,10,11,17. For example $\text{ord}_{\hat{\mathscr{S}}}(4) = 2$ but $\text{ord}_{\hat{\mathscr{S}}}(4+2\cdot 7) = \text{ord}_{\hat{\mathscr{S}}}(18) = 3$ (instead of 4). These are the projections of $S'\backslash S$ onto the first coordinate, as indicated in Theorem 2.3. The unstable elements of $\mathscr{S}$ are 3 and 4, which are the projections of $S'\backslash S$ onto the second coordinate by Theorem 2.3. The two sets of unstable elements have different cardinalities because the four elements of $S'\backslash S$ have distinct first coordinates, but not distinct second coordinates. But two distinct elements of $\tilde{S}\backslash S$ cannot have a coordinate in common so their projections have the same cardinality in both directions, which is a graphical explanation of Remark 2.4. (In fact, if $S'\backslash\tilde{S}$ is non-empty, some distinct elements of $S'\backslash S$ must have a coordinate in common.) Here $a = |\tilde{S}\backslash S| = 2$ and $\{x \in \Gamma | t^x t^d = 0 \text{ in } \text{gr}\mathscr{S}\} = \{3,4\}$, in agreement with Theorem 2.1 (2) $\Leftrightarrow$ (3).

As an illustation of the proof of Theorem 2.1 (1) $\Leftrightarrow$ (2) consider the congruence class of (3,4) mod 7. With (3,4) in the lower left hand corner the elements in this class looks like

$$\begin{array}{cccc}
\square & \bullet & \bullet & \bullet \\
\square & \bullet & \bullet & \bullet \\
\square & {\Large\bullet} & \bullet & \bullet \\
\square & \otimes & \circ & {\Large\bullet}
\end{array}$$

The corner of the elements not in S (represented by the open circle) is the element $(17,4)$ of $\tilde{S}\backslash S$ and the corners of S in this congruence class are the elements $(24,4)$ and $(10,11)$ of $\mathcal{B}$ (represented by the large solid dots). This illustrates graphically how one element of $\tilde{S}\backslash S$ leads to two elements of $\mathcal{B}$ in the same congruence class. Similarly the congruence class of $(4,3)$ contains one element of $\tilde{S}\backslash S$ and two elements of $\mathcal{B}$, leading to the two surplus elements of $\mathcal{B}$ in this example.

We have found examples where a congruence class mod d contains more than one element of $\tilde{S}\backslash S$. For example $\mathscr{S} = \{4, 10, 11, 13, 14, 20, 24\}$ where the congruence class of $(12,12)$ mod 24 contains 2 elements of $\tilde{S}\backslash S$, namely $(12,36)$ and $(36,12)$ and 3 elements of $\mathcal{B}$, namely $(12,60)$, $(36,36)$, $(60,12)$.

4. The examples of Patil-Roberts.

In this section let $\mathscr{S} = \{\delta, m_0, m_1, \ldots, m_p, m_{p+1}\}$ where $\delta, m = m_0$ are relatively prime, and $m_i = m + i\delta$, $0 \leq i \leq p+1$. This case was studied in [6], where the authors found explicitly the degrees of all elements of Γ, and hence the unstable elements, and Hilbert function for curves arising from $\mathscr{S}$. (Here we use δ in place of d, which was used in [6] for this quantity, to avoid conflict with our use of d for degree. Of course $d = m_{p+1}$ and $k = p+3$, but we will use m and p in this section to facilitate use of results from [6].) As in previous sections of this paper $S_{\mathscr{S}}$ (or simply S) will denote the semigroup in $\mathbb{N}^2$ constructed from $\mathscr{S}$ in the Introduction, Γ will denote the projection of S onto the second coordinate and $\hat{\Gamma}$ be the projection onto the first coordinate. Our goal in this section is to study the elements of $S'\backslash S$, starting from the unstable elements of Γ.

If $\delta < m$ the unstable elements of Γ (together with their $\mathrm{ord}_{\mathscr{S}}$) are given by [6, (4.5)], which we will now recall. Put the unstable elements in the form of a table with first row $\ell\delta$, $\delta < \ell \leq m-1$ and each successive row obtained from the preceding row by adding m_{p+1} in each coordinate, and dropping the last $p+1$ entries. Altogether this yields $\sigma = \lceil (m-\delta-1)/(p+1) \rceil$ rows. As an illustration we use [6, Example (4.7)], where $\mathscr{S} = \{4, 11, 15, 19\}$ (i.e. $\delta = 4, m = 11, p = 1$). Then the table of unstable elements is

20	24	28	32	36	40
39	43	47	51		
58	62				

The element $\delta(\delta+1)$ in the top left corner is of order $\delta+1$ with the order increasing by 1 in each subsequent upward diagonal, so that here 20 is of $\mathscr{S}$-order 5, 39 and 24 are of order 6, etc.

Definition 4.1. Let U_j denote column j of this table, $1 \leq j \leq m-\delta-1$, starting with $j=1$ at the left. Explicitly $U_j = \{\delta(j+\delta) + \ell m_{p+1}, 0 \leq \ell < \lceil (m-\delta-j)/(p+1) \rceil\}$.

The next definition will be explained by the proof of Theorem 4.3.

Definition 4.2. Let $\hat{U}_j = \{(j+\delta)m_p - \ell m_{p+1},\ 1 \leq \ell \leq j\}$, $1 \leq j \leq m-\delta-1$.

Theorem 4.3. *Let $\mathscr{S} = \{\delta, m_0, m_1, \ldots, m_p, m_{p+1}\}$ with $\delta < m = m_0$ and $m_i = m+i\delta$, $0 \leq i \leq p+1$. Let $S = S_{\mathscr{S}}$ and S' be constructed from this data as in the Introduction and let U_j and $\hat{U}_j$ be as in Definitions 4.1 and 4.2. Let $x \in U_j$. Then*

(1) $\{(a,x)|a \in \hat{U}_j\}$ *is the set of elements of $S'\backslash S$ projecting onto x,*
(2) *the set of all unstable elements of $\hat{\Gamma}$ is $\cup_{1\leq j\leq m-\delta-1}\hat{U}_j$,*
(3) $S'\backslash S = \cup_{1\leq j \leq m-\delta-1}\{(a,b)|a \in \hat{U}_j \text{ and } b \in U_j\}$, *and*
(4) *there is one element of $\tilde{S}\backslash S$ for each j, namely (a_j, b_j) where a_j is the largest element of $\hat{U}_j$ and b_j is the largest element of U_j.*

Proof. First recall from the proofs of Theorem 2.1 and 2.3 how the number of elements of $S'\backslash S$ projecting onto $x \in \Gamma$ can be found. If $\mathrm{ord}_{\mathscr{S}}(x) = e$ then to x we have associated the element $(em_{p+1}-x, x) \in S$. The elements of $S'\backslash S$ projecting onto $x \in \Gamma$ are then all the pairs $((e-u)m_{p+1}-x, x)$, $u \geq 1$ such that $(e-u)m_{p+1} - x \in \hat{\Gamma}$. (Since $(em_{p+1}-x, x) \in S$, $((e-1)m_{p+1}-x, x) \notin S$, and $m_{p+1} \in \hat{\Gamma}$ the set of such u is an interval $1 \leq u \leq r$ for some integer $r \geq 1$). The element in column j of the first row of our table of unstable elements is $(j+\delta)\delta$ and this is of order $j+\delta$. The element of S corresponding to this is $((j+\delta)m_{p+1} - (j+\delta)\delta, (j+\delta)\delta) = ((j+\delta)m_p, (j+\delta)\delta)$. Any other element of column j corresponds to an element of S with the same first coordinate. Our claim is that $(j+\delta)m_p - jm_{p+1} \in \hat{\Gamma}$ but $(j+\delta)m_p - (j+1)m_{p+1} \notin \hat{\Gamma}$. For the first claim we have $(j+\delta)m_p - jm_{p+1} = (j+\delta)m_p - j(m_p+\delta) = \delta(m_p - j) \in \hat{\Gamma}$ (remembering that $j \leq m-1 < m_p$ so that $m_p - j > 0$). For the second we have $(j+\delta)m_p - (j+1)m_{p+1} = (j+\delta)m_p - (j+1)(m_p+\delta) = (\delta-1)m_p - (j+1)\delta$. Usually it will be difficult to decide if a general integer is an element of $\hat{\Gamma}$, but in this particular case $\hat{\Gamma}$ is the numerical semigroup generated by δ and m_p, which are relatively prime. From this it is clear that $(\delta-1)m_p - (j+1)\delta \notin \hat{\Gamma}$. This proves our first claim. The remaining assertions follow from this and Theorem 2.3. □

Note that there is at most one element of $\tilde{S}\backslash S$ in each congruence class mod m_{p+1}, making the example at the end of the previous section more interesting. The unstable elements of $\hat{\Gamma}$ can be arranged in a table whose j^{th} column (decreasing downwards, say) is $\hat{U}_j$, $(1 \leq j \leq m - \delta - 1)$. In the example $\mathscr{S} = \{4, 11, 15, 19\}$ the table of unstable elements of $\hat{\Gamma}$ is

56	71	86	101	116	131
	52	67	82	97	112
		48	63	78	93
			44	59	74
				40	55
					36

the elements of $S'\backslash S$ are (56,20), (56,39), (56,58), (71,24), (52,24), (71,43), (52,43), (71,62), (52,62), (86,28), (67,28), (48,28), (86,47), (67,47), (48,47), (101,32), (82,32), (63,32), (44,32), (101,51), (82,51), (63,51), (44,51), (116,36), (97,36), (78,36), (59,36), (40,36), (131,40), (112,40), (93,40), (74,40), (55,40), (36,40) and the elements of $\tilde{S}\backslash S$ are (56,58), (71,62), (86,47), (101,51), (116,36), (131,40).

In general (still in the case $\delta < m$) the table of unstable elements of $\hat{\Gamma}$ is of a similar triangular form with $\delta m_p - \delta$ (here $4 \cdot 15 - 4 = 56$) at the upper left hand corner, the integers $\delta m_p - j\delta$, $1 \leq j \leq m - \delta - 1$ down the diagonal, and with addition of m_p (here 15) as one moves one step right in the table and subtraction of m_{p+1} (here 19) as one goes one step down in the table.

If $\delta > m$ then the unstable elements of Γ are described by [6, (4.4)]. They are of the form $n = \ell\delta + cm_{p+1}$ with $c < 0$ and $m-(p+1)c \leq \ell < \delta$, with $\operatorname{ord}_{\mathscr{S}}(n) = c + \delta$. (In order for there to be any unstable elements we must thus have $m+p+1 < \delta$.) For convenience we will write $C = -c$ so that $C > 0$. The unstable elements can be arranged in a table with rows $C = 1, C = 2, \ldots$ justified at the right. As an illustration consider [6, Example (4.8)], where $\mathscr{S} = \{8, 3, 11, 19\}$ (i.e. $\delta = 8, m = 3, p = 1$), and the table of unstable elements is

21	29	37
		18

The first row of our table ($C = 1$) contains the most elements, namely $\delta - (m + p + 1)$, so there are $\delta - m - p - 1$ columns in our table.

Definition 4.4. Let U_j denote the j^{th} column of the above table, $1 \leq j \leq \delta - m - p - 1$ counting from the right beginning with with $j = 1$ (corresponding to $\ell = \delta - j$ in the above expression $n = \ell\delta + cm_{p+1}$). Explicitly $U_j = \{\delta(\delta - j) - Cm_{p+1}, 1 \leq C \leq \lfloor(\delta - j - m)/(p + 1)\rfloor\}$.

The next definition is explained by the proof of Theorem 4.6.

Definition 4.5. For $1 \leq j \leq \delta - m - p - 1$ let $\hat{U}_j = \{(\delta - \ell)m_p - (\ell - j)\delta,\ 1 \leq \ell \leq j\}$.

Then we have

Theorem 4.6. *Let $\mathscr{S} = \{\delta, m_0, m_1, \ldots, m_p, m_{p+1}\}$ with $\delta > m = m_0$ and $m_i = m + i\delta,\ 0 \leq i \leq p+1$. Let $S = S_{\mathscr{S}}$ and S' be constructed from this data as in the Introduction and U_j and $\hat{U}_j$ be as in Definitions 4.4 and 4.5. Let $x \in U_j$. Then*

1. *$\{(a, x) | a \in \hat{U}_j\}$ is the set of elements of $S' \backslash S$ projecting onto x,*
2. *the set of all unstable elements of $\hat{\Gamma}$ is $\cup_{1 \leq j \leq \delta - m - p - 1} \hat{U}_j$,*
3. *$S' \backslash S = \cup_{1 \leq j \leq \delta - m - p - 1}\{(a, b) | a \in \hat{U}_j$ and $b \in U_j\}$,*
4. *there is one element of $\tilde{S} \backslash S$ for each j, namely (a_j, b_j) where a_j is the largest element of $\hat{U}_j$ and b_j is the largest element of U_j.*

Proof. If x is in row C and column j of the above table then $x = (\delta - j)\delta - Cm_{p+1}$. Since x is of degree $\delta - C$ the element of S corresponding to x is $((\delta - C)m_{p+1} - (\delta - j)\delta + Cm_{p+1}, (\delta - j)\delta - Cm_{p+1})$. Subtracting ℓm_{p+1} from the first coordinate we get $(\delta - C)m_{p+1} - (\delta - j)\delta + Cm_{p+1} - \ell m_{p+1}$, which simplifies to $(\delta - \ell)m_p - (\ell - j)\delta$. As in the proof of Theorem 4.3 it suffices to prove that this is in $\hat{\Gamma}$ if $\ell = j$ but not if $\ell = j+1$. In the first case we have $(\delta - j)m_p$ which is clearly in $\hat{\Gamma}$. In the second case we have $(\delta - j - 1)m_p - \delta$. Since $\delta - j - 1 < \delta$ and m_p, δ are relatively prime (generating $\hat{\Gamma}$) we must have $(\delta - j - 1)m_p - \delta \notin \hat{\Gamma}$. Our claims now follow as in the proof of Theorem 4.3. $\square$

Again note that there is at most one element of $\tilde{S} \backslash S$ in each congruence class mod m_{p+1}. The unstable elements of $\hat{\Gamma}$ can be arranged in a table whose j^{th} column (counting from the right, decreasing downwards) is $\hat{U}_j$, $(1 \leq j \leq \delta - m - p - 1)$. In the example $\mathscr{S} = \{8, 3, 11, 19\}$ this table is

93	85	77
74	66	
55		

the elements of $S' \backslash S$ are (93,21), (74,21), (55,21), (85,29), (66,29), (77,37), (77,18) and the elements of $\tilde{S} \backslash S$ are (93,21), (85,29), (77,37).

In general (still in the case $\delta > m$) the table of unstable elements of $\hat{\Gamma}$ is of a similar triangular form with $(\delta - 1)m_p$ (here $7 \cdot 11 = 77$) at the upper right corner, the integers $(\delta - j)m_p,\ 1 \leq j \leq \delta - m - p - 1$ down the diagonal, with addition of δ (here 8) as one goes one step left in the table, and subtraction of m_{p+1} as one goes one step down.

The degrees of the unstable elements of $\hat{\Gamma}$ follow from the above results. If $x \in \hat{U}_j$ and y is the largest element of U_j then $(x, y) \in S' \backslash S$ but $(x, y + m_{p+1}) \in S$ so $\mathrm{ord}_{\hat{\mathscr{S}}}(x) = (x + y + m_{p+1})/m_{p+1}$.

If $\delta < m$ then $x = (j + \delta)m_p - \ell m_{p+1}$ for some $\ell, 1 \leq \ell \leq j$ and $y = \delta(j+\delta) + (\lceil (m - \delta - j)/(p+1) \rceil - 1)m_{p+1}$ which yields $\mathrm{ord}_{\hat{\mathscr{S}}}(x) = j + \delta - \ell + \lceil (m - \delta - j)/(p+1) \rceil$. In the example $\mathscr{S} = \{4, 11, 15, 19\}$ the degrees of unstable elements of $\hat{\Gamma}$ (arranged in the same manner as the table of unstable elements itself, ℓ being the row of our table starting with $\ell = 1$) are thus

$$\begin{array}{cccccc}
7 & 8 & 8 & 9 & 9 & 10 \\
 & 7 & 7 & 8 & 8 & 9 \\
 & & 6 & 7 & 7 & 8 \\
 & & & 6 & 6 & 7 \\
 & & & & 5 & 6 \\
 & & & & & 5
\end{array}$$

If $\delta > m$ then $x = (\delta - \ell)m_p - (\ell - j)\delta$ for an integer $\ell, 1 \leq \ell \leq j$ and $y = \delta(\delta - j) - m_{p+1}$ so $\mathrm{ord}_{\hat{\mathscr{S}}}(x) = \delta - \ell$, where again ℓ is the row in our table, starting with 1. In the example $\mathscr{S} = \{8, 3, 11, 19\}$ the unstable elements 93 85 77 thus have $\hat{\mathscr{S}}$-order $\delta - 1 = 7$, 74 66 have order 6 and 55 has order 5.

Remark 4.7. In both Theorem 4.3 and Theorem 4.6, for each j there are two elements of $\mathcal{B}$ in the corresponding congruence class $\mod m_{p+1}$, namely (α_1, β_1) and (α_2, β_2) where α_1 is the smallest element in $\hat{U}_j$, β_1 is m_{p+1} plus the largest element in U_j, α_2 is m_{p+1} plus the largest element in $\hat{U}_j$, and β_2 is the smallest element in U_j. In the congruence classes $\mod m_{p+1}$ where there is only one element of $\mathcal{B}$, this element (as is the case for any curve) is (a, b) where b is the smallest element of Γ in its congrucence class $\mod m_{p+1}$ and a is the smallest element of $\hat{\Gamma}$ congruent to $m_{p+1} - a$.

Remark 4.8. In the non-Cohen-Macaulay examples of this section, the smallest degree of an element of $\tilde{S} \backslash S$ is $\delta + \sigma - 1$ if $\delta < m$ and all elements of $\tilde{S} \backslash S$ have degree $\delta - 2$ if $\delta > m$. This is in contrast to the results of the next section where we prove that "most" of the time there is an element of degree 1 in $\tilde{S} \backslash S$.

In the examples $\mathscr{S} = \{\delta, m_0, m_1, \ldots, m_p, m_{p+1}\}$ of [6] we have seen that if a is an unstable element of $\hat{\Gamma}$ and b is an unstable element of Γ (such that $a + b \equiv 0$ mod the degree m_{p+1} of the curve) then $(a, b) \in S' \backslash S$. This is not true for arbitrary $\mathscr{S}$, as shown by the following example.

Example 4.9. Let $\mathscr{S} = \{1, 3, 7, 8\}$. Then the unstable elements of $\hat{\Gamma}$ are 2,3,4,6,11 and the unstable elements of Γ are 2,4,5,6,12,13,20, but $(11, 13) = (5, 3) + (5, 3) + (1, 7) \in S$.

5. The fraction of curves that are Cohen-Macaulay is asymptotically 0

In this section we prove in Theorem 5.3 that as $d \to \infty$ the fraction of all curves of degree d that contain an element of $\tilde{S}\backslash S$ of degree one approaches 1. By Theorem 1.1 it follows that the fraction of all curves of degree d that are Cohen-Macaulay approaches 0. We use the notation of the Introduction, namely $\mathscr{S} = \{a_1, a_2, \ldots, a_k\}$ with $a_1 < a_2 < \cdots < a_k = d$ and $\gcd(a_1, \ldots, a_k) = 1$. An element of $\tilde{S}\backslash S$ of degree 1 is of the form $(d - x, x)$ where $x \in \Gamma$, with $(d - x, x) \notin S, (2d - x, x) \in S$, and $(d - x, x + d) \in S$. These three assertions mean that $\mathrm{ord}_{\mathscr{S}}(x) = 2$ and $\mathrm{ord}_{\mathscr{S}}(x + d) \leq 2$ or equivalently that $x \notin \mathscr{S}$, $x = a_i + a_j$ and $x + d = a_\ell + a_m$ with $a_i, a_j, a_\ell, a_m \in \mathscr{S}$. We wish to show that as d becomes large there will be such an x for "most" $\mathscr{S}$. In the course of the proof we will find it convenient to consider sets $\mathscr{S} = \{a_1, a_2, \ldots, a_k\}$ with $a_1 < a_2 < \cdots < a_k = d$ and $\gcd(a_1, \ldots, a_k) = g > 1$. Setting $\overline{a_i} = a_i/g,\ 1 \leq i \leq k$ yields $\overline{\mathscr{S}} = \{\overline{a_1}, \overline{a_2}, \ldots, \overline{a_k}\}$ satisfying our usual hypotheses, along with corresponding semigroup ring $\overline{S} = S_{\overline{S}}$, and accompanying sets $\overline{S}'$ and $\tilde{\overline{S}}$. It is clear that $\tilde{\overline{S}}\backslash\overline{S}$ contains an element of degree one in the grading of $\overline{S}$ if and only if there exists x satisfying the same conditions $x \notin \mathscr{S}$, $x = a_i + a_j$ and $x + d = a_\ell + a_m$ with $a_i, a_j, a_\ell, a_m \in \mathscr{S}$. We first prove a proposition on sets which will be applied in the proof of Theorem 5.3 to subsets A_i of the set of all projective monomial curves of a given degree.

Proposition 5.1. *Suppose we have a collection of nonempty finite sets $A_i,\ 1 \leq i \leq n$, and a subset $X_i \subseteq A_i$ for each i, such that $|X_i|/|A_i| = \alpha_i > 0$. Then*
$$\frac{|\cup X_i|}{|\cup A_i|} \geq \frac{1}{(\sum_{i=1}^n 1/\alpha_i) - (n-1)}.$$

Proof. Let $\gamma_i = 1/\alpha_i = |A_i|/|X_i|$. Clearly we have
$$|\cup A_i| \leq |\cup X_i| + \sum_{i=1}^n |A_i\backslash X_i| = |\cup X_i| + \sum_{i=1}^n (\gamma_i - 1)|X_i|.$$
Dividing by $|\cup X_i|$ we obtain
$$\frac{|\cup A_i|}{|\cup X_i|} \leq 1 + \sum_{i=1}^n (\gamma_i - 1)\frac{|X_i|}{|\cup X_i|} \leq 1 + \sum_{i=1}^n (\gamma_i - 1) = (\sum_{i=1}^n \gamma_i) - (n-1).$$

Taking the reciprocal of the above expression and replacing γ_i by $1/\alpha_i$ yields the result. $\square$

Corollary 5.2. *Suppose that $|X_i|/|A_i| \geq \alpha$ for all i. Then*

$$\frac{|\cup X_i|}{|\cup A_i|} \geq \frac{\alpha}{(1-\alpha)n+\alpha}.$$

Proof. Since the function of $\alpha_1, \ldots, \alpha_n$ in the previous proposition is increasing in each variable, the result follows by replacing each α_i with α and regrouping. $\square$

Theorem 5.3. *Let $C_d = \{\{a_1, a_2, \ldots, a_k\} | a_i \in \mathbb{N}, 0 < a_1 < a_2 < \ldots < a_k = d,\ \gcd(a_1, \ldots, a_k) = 1\}$ and $CM_d = \{\mathscr{S} \in C_d | R_{\mathscr{S}}$ is Cohen-Macaulay$\}$. Then $\lim_{d\to\infty} |CM_d|/|C_d| = 0$.*

Proof. We will temporarily drop the condition that $\gcd(a_1, \ldots, a_k) = 1$. Let $C'_d = \{\{a_1, a_2, \ldots, a_k\} | a_i \in \mathbb{N}, 0 < a_1 < a_2 < \ldots < a_k = d\}$, $CM'_d = \{\mathscr{S} \in C'_d | R_{\mathscr{S}}$ is Cohen-Macaulay$\}$, and $NCM'_d = C'_d \setminus CM'_d$. We will first show that $\lim_{d\to\infty} |NCM'_d|/|C'_d| = 1$. As explained at the beginning of this section, for a given $\mathscr{S} \in C'_d$, we seek an element $x \notin \mathscr{S}$ such that $x = a_i + a_j$ and $x + d = a_\ell + a_m$ with $a_i, a_j, a_\ell, a_m \in \mathscr{S}$.

Let $C'_{d,x} = \{\mathscr{S} \in C'_d | x \notin \mathscr{S}\}$, $CM'_{d,x} = CM'_d \cap C'_{d,x}$, and $NCM'_{d,x} = C'_{d,x} \setminus CM'_{d,x}$. Now $NCM'_d = \cup_{0<x<d} NCM'_{d,x}$, so we would like to have a uniform lower bound for $|NCM'_{d,x}|$ in order to apply our corollary. We wish to determine the number of ways of choosing subsets $B_1 \subseteq \{1, 2, \ldots, x-1\}$ and $B_2 \subseteq \{x+1, x+2, \ldots, d-1\}$ such that $x = a_i + a_j$ has a solution with $a_i, a_j \in B_1$ and $x + d = a_\ell + a_m$ has a solution with $a_\ell, a_m \in B_2$ for then $\mathscr{S} = B_1 \cup B_2$ will yield a non-Cohen-Macaulay $R_{\mathscr{S}}$. For a fixed $x, 0 < x < d$, there are $\lfloor (x-1)/2 \rfloor$ pairs $\{a_i, a_j\} = \{1, x-1\}, \{2, x-2\}, \ldots, \{\lfloor (x-1)/2 \rfloor, \lceil (x+1)/2 \rceil\}$ such that $x = a_i + a_j$ with $a_i < a_j$. If x is even, there is also the possibility of a singleton with $a_i = a_j = x/2$. There are $3^{\lfloor (x-1)/2 \rfloor}$ ways of choosing a subset of $\{1, 2, \ldots, x-1\}$ such that none of these pairs (or singleton) occur (we cannot choose the singleton (if x is even) and for each of the $\lfloor (x-1)/2 \rfloor$ pairs, there are three subsets of the pair which do not include both elements). There are a total of 2^{x-1} subsets of $\{1, 2, \ldots, x-1\}$, so the number of subsets where there is at least one solution to $x = a_i + a_j$ is $2^{x-1} - 3^{\lfloor (x-1)/2 \rfloor}$. Similarly, the number of subsets of $\{x+1, x+2, \ldots, d-1\}$ where there is at least one solution to $x + d = a_\ell + a_m$ is $2^{d-x-1} - 3^{\lfloor (d-x-1)/2 \rfloor}$. There are 2^{d-2} elements in

$C'_{d,x}$, so we have

$$\begin{aligned}\frac{|NCM'_{d,x}|}{|C'_{d,x}|} &\geq \frac{(2^{x-1}-3^{\lfloor (x-1)/2\rfloor})(2^{d-x-1}-3^{\lfloor (d-x-1)/2\rfloor})}{2^{d-2}} \\ &= \left(1-\frac{3^{\lfloor (x-1)/2\rfloor}}{2^{x-1}}\right)\left(1-\frac{3^{\lfloor (d-x-1)/2\rfloor}}{2^{d-x-1}}\right) \\ &= f(x).\end{aligned}$$

We would like to apply Corollary 5.2 with $\alpha = \min(f(x))$, but there are two problems with this. First $f(x)$ is small for x close to 1 or d, so we will bound x away from 1 and d for the time being. The second problem is that $f(x)$ is highly nonmonotonic. We will therefore bound it below by the unimodal function $g(x) = (1-3^{(x-1)/2}/2^{x-1})(1-3^{(d-x-1)/2}/2^{d-x-1})$. (In what follows $d/4$ could be replaced by λd for any λ such that $0<\lambda<1/2$.) Consider $\cup_{x=\lfloor d/4\rfloor}^{d-\lfloor d/4\rfloor} NCM'_{d,x}$. Since $g(x)$ is symmetric about $x=\lfloor d/2\rfloor$ and is increasing on $[0,\lfloor d/2\rfloor]$, we have $|NCM'_{d,x}|/|C'_{d,x}| \geq g(x) \geq g(\lfloor d/4\rfloor)$, for $\lfloor d/4\rfloor \leq x \leq d-\lfloor d/4\rfloor$. Taking $\alpha(d) = g(\lfloor d/4\rfloor)$, noting that there are $n(d) = d-2\lfloor d/4\rfloor + 1$ subsets in our union, and applying the corollary above we obtain

$$\frac{|\cup_{x=\lfloor d/4\rfloor}^{d-\lfloor d/4\rfloor} NCM'_{d,x}|}{|\cup_{x=\lfloor d/4\rfloor}^{d-\lfloor d/4\rfloor} C'_{d,x}|} \geq \frac{\alpha(d)}{(1-\alpha(d))n(d)+\alpha(d)}.$$

Now $\cup_{x=\lfloor d/4\rfloor}^{d-\lfloor d/4\rfloor} C'_{d,x} = \{\mathscr{S} \in C'_d \mid$ there is an x, $\lfloor d/4\rfloor \leq x \leq d-\lfloor d/4\rfloor$ such that $x \notin \mathscr{S}\}$, so its complement in C'_d consists of all $\mathscr{S}$ containing $\{\lfloor d/4\rfloor, \ldots, d-\lfloor d/4\rfloor\}$. Since each such $\mathscr{S}$ is determined by a subset of the $2\lfloor d/4\rfloor-2$ element set $\{1,2,\ldots,\lfloor d/4\rfloor-1, d-\lfloor d/4\rfloor+1,\ldots,d-1\}$, there are $2^{2\lfloor d/4\rfloor-2}$ elements in the complement. As $|C'_d| = 2^{d-1}$, we have $|\cup_{x=\lfloor d/4\rfloor}^{d-\lfloor d/4\rfloor} C'_{d,x}| = 2^{d-1}-2^{2\lfloor d/4\rfloor-2}$ and therefore

$$\begin{aligned}\frac{|NCM'_d|}{|C'_d|} &\geq \frac{|\cup_{x=\lfloor d/4\rfloor}^{d-\lfloor d/4\rfloor} NCM'_{d,x}|}{|C'_{d,x}|}\frac{|C'_{d,x}|}{|C'_d|} \\ &\geq \frac{\alpha(d)}{(1-\alpha(d))n(d)+\alpha(d)}\frac{2^{d-1}-2^{2\lfloor d/4\rfloor-2}}{2^{d-1}} \\ &= \frac{\alpha(d)}{(1-\alpha(d))n(d)+\alpha(d)}\left(1-2^{2\lfloor d/4\rfloor-d-1}\right)\end{aligned}$$

Asymptotically $1-\alpha(d)$ decays exponentially and $n(d)$ grows linearly, so $\lim_{d\to\infty}(1-\alpha(d))n(d) = 0$. Combining this with the fact that $\lim_{d\to\infty}\alpha(d) = 1$ and $\lim_{d\to\infty} 1-2^{2\lfloor d/4\rfloor-d-1} = 0$, we have $\lim_{d\to\infty}|NCM'_d|/|C'_d| = 1$.

Letting $NCM_d = C_d \backslash CM_d$, the last step is to show that, in fact, $\lim_{d\to\infty} |NCM_d|/|C_d| = 1$. Since $|C'_d| = \sum_{i|d} |C_i|$, by the Möbius Inversion Formula, $|C_d| = \sum_{i|d} \mu(i)|C'_{d/i}| = \sum_{i|d} \mu(i)2^{d/i-1}$, where $\mu(x)$ is the Möbius function. More concretely, if $d = p_1^{\beta_1} p_2^{\beta_1} \ldots p_r^{\beta_r}$ with the p_i being distinct primes, then $|C_d| = 2^{d-1} - \sum_{1\leq i\leq r} 2^{d/p_i-1} + \sum_{1\leq i<j\leq r} 2^{d/(p_ip_j)-1} \ldots$. Letting $h(d) = \sum_{1\leq i\leq r} 2^{d/p_i-1} - \sum_{1\leq i<j\leq r} 2^{d/(p_ip_j)-1} \ldots$, we have $|C_d| = |C'_d| - h(d)$ and

$$\begin{aligned} \frac{|NCM_d|}{|C_d|} &\geq \frac{|NCM'_d| - h(d)}{|C'_d| - h(d)} \\ &= \frac{|NCM'_d|/|C'_d| - h(d)/|C'_d|}{1 - h(d)/|C'_d|} \end{aligned}$$

Therefore if we can show that $\lim_{d\to\infty} h(d)/|C'_d| = \lim_{d\to\infty} h(d)/2^{d-1} = 0$, we will be done. But

$$\begin{aligned} h(d) &\leq \sum_{1\leq i\leq r} 2^{d/p_i-1} \\ &\leq \sum_{1\leq i\leq r} 2^{d/2-1} \\ &= r2^{d/2-1} \\ &\leq d2^{d/2-1} \end{aligned}$$

and since $\lim_{d\to\infty} d2^{d/2-1}/2^{d-1} = 0$, the result follows. □

6. Numerical results

In this section we describe computational results illustrating the previous section. Notation is as in the Introduction. In particular we identify $\mathscr{S}$ with the curve, and will refer to k as the length of the curve. In the table below c $(= |C_d|)$ is the number of curves of degree d, cm $(= |CM_d|)$ is the number of our curves that are Cohen-Macaulay, and ncm $(= |NCM_d|)$ is the number that are not. The number of curves of degree d that contain an element of degree 1 in $\tilde{S}\backslash S$ is denoted by d_1. The table is computed using the algorithm described in [7] or [6].

Clearly, for a given d we have $c \geq ncm \geq d_1$. In (the proof of) Theorem 5.3 we proved as $d \to \infty$ the ratio $d_1/c \to 1$ (hence a fortiori the ratio $ncm/c \to 1$). This is clearly illustrated by the values in the table. From our discussion it is clear that c, ncm and d_1 all grow approximately as 2^{d-1}. As $d \to \infty$, $cm \to \infty$ because as d becomes large the number of possible sets $\mathscr{S}$ that are arithmetic progressions grows at least in proportion to d (for example $\mathscr{S} = \{d-1, d\}, \{d-2, d-1, d\}, \ldots$) and these curves are all Cohen-Macaulay. It would be interesting to have a better estimate of the growth of cm. The differences $ncm - d_1 = 1$ for $d = 5, 6$ are accounted for by $\{1, 4, 5\}$ and $\{1, 5, 6\}$.

d	c	cm	ncm	d_1
1	1	1	0	0
2	1	1	0	0
3	3	3	0	0
4	6	5	1	1
5	15	12	3	2
6	27	16	11	10
7	63	37	26	20
8	120	51	69	62
9	252	97	155	123
10	495	142	353	333
11	1023	257	766	663
12	2010	359	1651	1555
13	4095	647	3448	3132
14	8127	920	7207	6966
15	16365	1605	14760	13886
16	32640	2266	30374	29631
17	65535	3795	61740	59431
18	130788	5410	125378	123555

References

[1] W. Bruns, J. Gubeladze, and N. Trung. Problems and algorithms for affine semigroups. *Semigroup Forum*, 64:180–212, 2002.

[2] W. Bruns and J. Herzog. *Cohen-Macaulay Rings*. Cambrige University Press, 1993.

[3] H Derksen and G. Kemper. *Computational Invariant Theory*. Encyclopedia of Mathematical Sciences. Springer-Verlag, 2002.

[4] S. Goto, N. Suzuku, and K. Watanabe. On affine semigroup rings. *Japan J. Math*, 2:1–12, 1976.

[5] Ping Li. PhD thesis, Queen's University, 2005.

[6] D. P. Patil and L. G. Roberts. Hilbert functions of monomial curves. *Journal of Pure and Applied Algebra*, 183:275–292, 2002.

[7] L. G. Roberts. Certain projective curves with unusual Hilbert function. *JPAA*, 104:303–311, 1995.

[8] L. Trung and L. Hoa. Affine semigroups and Cohen-Macaulay rings generated by monomials. *Transactions of the American Math. Society*, 298:145–167, 1986.

Department of Mathematics, Southwest Missouri State University, Springfield, MO 65804
E-mail address: `les@math.smsu.edu`

Department of Mathematics and Statistics, Queen's University, Kingston, Ontario, CANADA K7L 3N6
E-mail address: `robertsl@mast.queensu.ca`