BASES AND IDEAL GENERATORS FOR PROJECTIVE MONOMIAL CURVES

PING LI[1], D. P. PATIL[2], AND LESLIE G. ROBERTS[3]

Abstract. In this article we study bases for projective monomial curves and the relationship between the basis and the set of generators for the defining ideal of the curve. We understand this relationship best for curves in $\mathbb{P}^3$ and for curves defined by an arithmetic progression. We are able to prove that the latter are set theoretic complete intersections.

1. Introduction

Let $\mathscr{S} = \{a_1, \ldots, a_p\}$ with $a_i \in \mathbb{N}$, $0 < a_1 < \cdots < a_p = d$ and $\gcd(a_1, \ldots, a_p) = 1$. To $\mathscr{S}$ we associate two semigroups $\Gamma \subseteq \mathbb{N}$ and $S \subset \mathbb{N}^2$ (all our semigroups are finitely generated and contain 0). The numerical semigroup Γ is generated by $\mathscr{S}$, and S is generated by $\boldsymbol{\alpha}_0 = (d, 0), \boldsymbol{\alpha}_1 = (d - a_1, a_1), \cdots, \boldsymbol{\alpha}_{p-1} = (d - a_{p-1}, a_{p-1}), \boldsymbol{\alpha}_p = (0, d)$. Let K be a field and s, t indeterminates over K. We will identify the semigroup ring of S over K with the subalgebra $K[S] = K[s^d, s^{d-a_1}t^{a_1}, \ldots, s^{d-a_{p-1}}t^{a_{p-1}}, t^d] \subseteq K[s, t]$. The projective monomial curve associated to $\mathscr{S}$ is the scheme $\mathcal{C} = \operatorname{Proj}(K[S])$. Let $R = K[X_0, X_1, \ldots, X_p]$, a polynomial ring over K. The surjective K-algebra homomorphism $\varphi : R \to K[s, t]$ defined by $\varphi(X_i) = s^{d-a_i}t^{a_i}$ for $i = 0, \ldots, p$ (setting $a_0 = 0$) corresponds to an embedding $\mathcal{C} \hookrightarrow \mathbb{P}^p$ of $\mathcal{C}$ as a curve of degree d. The objects of study in this paper are the ideal $\operatorname{Ker}\varphi =: \mathfrak{p}$, the basis of S (defined below), and the relation between them. The ideal $\mathfrak{p}$ is a homogeneous prime ideal in R, called the defining ideal of $\mathcal{C}$, and $R/\mathfrak{p} \cong K[S]$ as K-algebra. To simplify terminology "curve" will always mean a projective monomial curve, and we may refer to the set $\mathscr{S}$, or the semigroup S, as the curve. Our methods work best if $\mathcal{C}$ is a curve in $\mathbb{P}^3$ (i.e. $p = 3$) or if $\mathcal{C}$ is an arithmetic progression curve, i.e. $\mathscr{S}$ is a finite set of consecutive elements in an arithmetic progression.

By the basis of S (or $\mathcal{C}$ or $\mathscr{S}$) we mean the following.

Definition 1.1. Let T be the subsemigroup of S generated by $\{\boldsymbol{\alpha}_0 = (d, 0), \boldsymbol{\alpha}_p = (0, d)\}$. The set $\mathcal{B} = \{\boldsymbol{\alpha} \in S \mid \boldsymbol{\alpha} - \boldsymbol{\alpha}_0 \notin S, \text{ and } \boldsymbol{\alpha} - \boldsymbol{\alpha}_p \notin S\}$ is called the basis of S over T (or simply the basis of S).

2000 *Mathematics Subject Classification.* Primary 14H50, 14M10, 20M25.

Key words and phrases. semigroup, projective monomial curve, ideal generators, arithmetic progression, set-theoretic complete intersection.

This work was done while the second author was visiting the Department of Mathematics and Statistics, Queens University, Kingston, Canada and was partially supported by the NSERC grant of the third author. The second author thanks Department of Mathematics and Statistics, Queens University, Kingston, Canada for its hospitality.

For $\boldsymbol{\alpha} = (\alpha_1, \alpha_2) \in S$, let $\mathbf{t}^{\boldsymbol{\alpha}} = s^{\alpha_1} t^{\alpha_2}$. Then $\mathbf{t}^{\mathcal{B}} = \{\mathbf{t}^{\boldsymbol{\alpha}} \mid \boldsymbol{\alpha} \in \mathcal{B}\}$ is a minimal spanning set of $K[S]$ as a module over $K[T] = K[s^d, t^d]$. Equivalently the canonical image of $\mathbf{t}^{\mathcal{B}}$ forms a K-basis of $K[S]/(s^d, t^d)K[S]$. Note that since $\{s^d, t^d\}$ is a system of parameters in $K[S]$, $K[S]/(s^d, t^d)K[S]$ is a finite dimensional K-vector space, so $\mathcal{B}$ is finite. Furthermore $K[S]$ is Cohen-Macaulay if and only if s^d, t^d (or equivalently t^d, s^d) is a regular sequence in $K[S]$. We now have

Theorem 1.2. [16, Theorem 1.1] *The following are equivalent:*

(i) *The semigroup ring $K[S]$ is Cohen-Macaulay.*
(ii) *$K[S]$ is a free $K[T]$-module with basis $\mathbf{t}^{\mathcal{B}}$.*
(iii) *$|\mathcal{B}| = d$.*

Bases can be computed with Macaulay 2 [5] (as the K-basis of $K[S]/(s^d, t^d)K[S]$) up to degree about 120, or up to degree about 1000 using a simple recursive algorithm based on Definition 1.1 ([8]). The lattice methods of Section 2 permit even more rapid calculation in $\mathbb{P}^3$, which we are still investigating. Our bases are a special case of the more general notion of "Apery set", which occurs in the literature in many places, for example in [4].

The rings R and $K[S]$ may be graded in several ways. The standard grading (denoted simply deg) is defined by setting $\deg(X_i) = \deg(\varphi(X_i)) = 1\,(0 \le i \le p)$. This is the grading used in the definition of $\mathrm{Proj}(S)$. The S (or $\mathbb{N}^2$) grading is defined by setting $\deg_S(X_i) = \deg_S(\varphi(X_i)) = \boldsymbol{\alpha}_i = (d - a_i, a_i) \in S \subset \mathbb{N}^2$. We will also need the s and t degrees, determined by $\deg_s(X_i) = \deg_s(\varphi(X_i)) = d - a_i$ and $\deg_t(X_i) = \deg_t(\varphi(X_i)) = a_i$. Trivially if $f \in K[S]$, $\deg(f) = (\deg_s(f) + \deg_t(f))/d$. The homomorphism φ (and hence also the ideal $\mathfrak{p}$) is homogeneous in all these gradings. For $\mu = (\mu_0, \mu_1, \ldots, \mu_p) \in \mathbb{N}^{p+1}$ define $X^\mu := X_0^{\mu_0} X_1^{\mu_1} \cdots X_p^{\mu_p}$. The ideal $\mathfrak{p}$ has a minimal set $\mathscr{G}$ of generators consisting of pure binomials (i.e. elements of the form $X^\mu - X^\nu$, for example see [9, Theorem[7.3]). These generators are homogeneous in all the above mentioned gradings. The cardinality r of $\mathscr{G}$ is uniquely determined, but the set $\mathscr{G}$ is not. We will say that $f \in \mathscr{G}$ is a type one generator of $\mathfrak{p}$ if f does not have X_0 in one term and X_p in the other, and a type two generator otherwise.

There are many papers on projective monomial curves, most notably [3] which gives an algorithm for finding a minimal set of binomial generators for $\mathfrak{p}$. In Section 2 we describe both the basis and the ideal generators of projective monomial curves in $\mathbb{P}^3$ in terms of lattices $\mathscr{L}$ and $\mathscr{L}'$. These sets can be visualized quite nicely by plotting diagrams in either $\boldsymbol{\alpha}_1$-$\boldsymbol{\alpha}_2$ or $\boldsymbol{\alpha}_0$-$\boldsymbol{\alpha}_2$ coordinates. We also give an easy way of recognizing the Cohen-Macaulay property in the first of these diagrams. These diagrams give a conceptual combinatorial description of the generators of $\mathfrak{p}$, in contrast with the algorithm of [3] (also expounded in [2, Section 3]). In Section 3, we use bases to determine explicitly the ideal generators for an arithmetic progression projective monomial curve. We know nowhere in the literature where ideal generators of a general projective arithmetic progression curve are found explicitly. Finally we show in Section 4 that a projective curve defined by an arithmetic progression is a set theoretic complete intersection.

The following summarizes some of the notation used throughout this article:

Notation 1.3. Let $\mathbb{N}$ (respectively, $\mathbb{N}^+$, $\mathbb{Z}$) denote the set of natural numbers $\{0,1,2,,\cdots\}$ (respectively, non-zero natural numbers $\{1,2,\cdots\}$, integers $\{0,\pm1,\pm2,\cdots\}$). For any two integers $a,b\in\mathbb{Z}$, we denote by $[a,b]$ the interval $\{i\in\mathbb{Z}\mid a\leq i\leq b\}$ of integers. The cardinality of a set X is denoted by $|X|$. On $\mathbb{N}^2$, $\leq$ will denote the coordinatewise partial order, i.e. $(a_1,b_1)\leq(a_2,b_2)$ if and only if $a_1\leq a_2$ and $b_1\leq b_2$.

2. Curves in $\mathbb{P}^3$

Curves $\mathscr{S}$ in $\mathbb{P}^3$ have a number of special features, which permit more detailed results than in higher dimension. First we introduce some notation that is more convenient than the general notation. Write $\mathscr{S}=\{a,b,d\}$ with $0<a<b<d$ and $\gcd(a,b,d)=1$ so that $\boldsymbol{\alpha}_0=(d,0),\boldsymbol{\alpha}_1=(d-a,a),\boldsymbol{\alpha}_2=(d-b,b)$, and $\boldsymbol{\alpha}_3=(0,d)$. Define $\gcd(a,b)=c\geq1$ and $a'=a/c$, $b'=b/c$, so that $\gcd(a',b')=1$.

Remark 2.1. First of all, any two of the $\boldsymbol{\alpha}_i$ are linearly independent over $\mathbb{Q}$, so that every element of S is a unique rational linear combination of two of the others. In particular we have

(1) $b'\boldsymbol{\alpha}_1-a'\boldsymbol{\alpha}_2=(b'-a')\boldsymbol{\alpha}_0$
(2) $-(d-b)\boldsymbol{\alpha}_1+(d-a)\boldsymbol{\alpha}_2=(b-a)\boldsymbol{\alpha}_3$
(3) $-(d-b)\boldsymbol{\alpha}_0+d\boldsymbol{\alpha}_2=b\boldsymbol{\alpha}_3$

In (1) the coefficients are relatively prime integers, but in (2) and (3) this may not be the case. Furthermore every basis element is a unique integer linear combination of $\boldsymbol{\alpha}_1$ and $\boldsymbol{\alpha}_2$. Secondly we have

Lemma 2.2. *In any minimal binomial generating set $\mathscr{G}$ of $\mathfrak{p}$, there is at most one generator in each S-degree.*

Proof. This follows from [9, Theorem 9.2]. Let $\mathbf{b}\in S$. In the language of this Theorem, $\Delta_{\mathbf{b}}$ is a simplicial complex on $\{0,1,2,3\}$ with i corresponding to $\boldsymbol{\alpha}_i$. The Theorem implies that the number of elements of $\mathscr{G}$ in degree $\mathbf{b}$ is $\dim\tilde{H}_0(\Delta_{\mathbf{b}},K)$, which is one less than the number of connected components of $\Delta_{\mathbf{b}}$. However if $\Delta_{\mathbf{b}}$ has more than two connected components then it must have two singleton components, say $\{i\}$ and $\{j\}$. But this would imply that $\mathbf{b}=m_i\boldsymbol{\alpha}_i=m_j\boldsymbol{\alpha}_j$ for positive integers m_i and m_j, which is impossible since the $\boldsymbol{\alpha}_i$ are linearly independent. □

There is an element of $\mathscr{G}$ in degree $\mathbf{b}$ if and only if $\Delta_{\mathbf{b}}$ is disconnected. If $\Delta_{\mathbf{b}}$ is disconnected it is easy to give a minimal binomial generator of $\mathfrak{p}$ in degree $\mathbf{b}$. Therefore a consequence of Lemma 2.2 is that in order to find a minimal set of binomial generators of $\mathfrak{p}$ it suffices to determine the S-degrees in which generators occur. (In a particular degree there may be a choice of generators, leading to different sets $\mathscr{G}$, as we will see in Example 2.5).

We can relate the degrees of the type one generators of $\mathfrak{p}$ to basis elements by factoring out by (X_0,X_3). Namely $K[S]/(s^d,t^d)K[S]\cong K[X_0,...,X_3]/(\mathfrak{p},X_0,X_3)\cong$

$K[X_1, X_2]/J_1$ for some ideal J_1 in $K[X_1, X_2]$. No binomial in $\mathfrak{p}$ can involve only X_1 and X_2 so J_1 is a monomial ideal. These isomorphisms identify the basis elements of S with the monomials of $K[X_1, X_2]$ not in J_1.

As above let $\mathscr{G}$ be a minimal set of pure binomial generators of $\mathfrak{p}$. Any type two generator in $\mathscr{G}$ (i.e. one that has X_0 in one term and X_3 in the other) maps to 0 in $K[X_1, X_2]$. The type one generators in $\mathscr{G}$ are mapped injectively into $K[X_1, X_2]$ by Lemma 2.2. Let $\overline{\mathscr{G}}$ be the images in $K[X_1, X_2]$ of the type one generators.

Lemma 2.3. *The ring homomorphism $K[X_0, \ldots, X_3] \to K[X_1, X_2]$ sending X_0 and X_3 to 0 and X_i to X_i ($i = 1, 2$) maps the type one generators in $\mathscr{G}$ bijectively onto $\overline{\mathscr{G}}$, which is a set of minimal generators of J_1.*

Proof. The bijection has already been noted. Clearly $\overline{\mathscr{G}}$ generates J_1, so it suffices to prove that one element of $\overline{\mathscr{G}}$ cannot be a multiple of another. Suppose on the contrary that $X_1^{a_1}X_2^{a_2}$ and $X_1^{b_1}X_2^{b_2}$ are two distinct elements of $\overline{\mathscr{G}}$, and that $a_1 \geq b_1, a_2 \geq b_2$ with at least one of these inequalities strict. We must have at least one of $b_1 > 0, b_2 > 0$, say $b_1 > 0$. Suppose that f and g are two pure binomials in $\mathscr{G}$ which map respectively to $X_1^{a_1}X_2^{a_2}$, $X_1^{b_1}X_2^{b_2}$. Since b_1 and a fortiori a_1 is greater than 0, the other term of both f and g must be divisible by X_0. We then conclude that $f - Mg$ is divisible by X_0, where $M = X_1^{a_1-b_1}X_2^{a_2-b_2}$. Since $\mathfrak{p}$ is prime and $X_0 \notin \mathfrak{p}$, $(f - Mg)/X_0 \in \mathfrak{p}$, from which it follows that f is in the ideal generated by $\mathscr{G}\backslash\{f\}$, contradicting the minimality of $\mathscr{G}$ as a set of generators of $\mathfrak{p}$. □

The type two generators in $\mathscr{G}$ (i.e. those that contain X_0 in one term and X_3 in the other) must be of the form $X_0^{a_0}X_2^{a_2} - X_1^{a_1}X_3^{a_3}$ with $a_0, a_1, a_2, a_3 > 0$ (in order for the two monomials to have the same S-degree). These can be detected by factoring out by (X_1, X_3), as follows. Namely $K[X_0, ..., X_3]/(\mathfrak{p}, X_1, X_3) \cong K[X_0, X_2]/J_2$ where J_2 is an ideal in $K[X_0, X_2]$. No binomial in $\mathfrak{p}$ can involve only X_0 and X_2 so J_2 is a monomial ideal.

Lemma 2.4. *For some minimal set $\mathscr{G}$ of pure binomial generators of $\mathfrak{p}$ there is a one-to-one correspondence between the elements of $\mathscr{G}$ not contained in $(X_1, X_3)K[X_0, X_1, X_2, X_3]$ and the minimal monomial generators of J_2.*

Proof. Start with some $\mathscr{G}$. The elements of $\mathscr{G}$ not in (X_1, X_3) must either be of type two or of the form $X_2^{a_2} - X_0^{a_0}X_1^{a_1}X_3^{a_3}$ with $a_3 > 0$ and $a_0 + a_1 > 0$. (This is the only other way to not be in (X_1, X_3) and have both monomials of the same S-degree.) If $X_0^{a_0}X_2^{a_2}$ and $X_0^{b_0}X_2^{b_2}$ are the images in $K[X_0, X_2]$ of two such generators it suffices to prove that neither divides the other. Suppose on the contrary that $X_0^{a_0}X_2^{a_2}$ is divisible by $X_0^{b_0}X_2^{b_2}$. That is, we have $a_0 \geq b_0, a_2 \geq b_2$ with at least one inequality strict. Furthermore $a_2 > 0$ and $b_2 > 0$. Let f and g be elements of $\mathscr{G}$ with one term respectively $X_0^{a_0}X_2^{a_2}, X_0^{b_0}X_2^{b_2}$. Then there is a monomial M involving only X_0 and X_2 so that the X_0-X_2 term of $f - Mg$ cancels. If $b_0 > 0$ (and hence also $a_0 > 0$) then both terms of $f - Mg$ are divisible by X_1 and, since $\mathfrak{p}$ is prime, we must have $(f - Mg)/X_1 \in \mathfrak{p}$. From this it follows that f is in the ideal generated by $\mathscr{G}\backslash\{f\}$ contradicting the minimality of $\mathscr{G}$. If $a_0 = 0$ and $b_0 = 0$ then both terms of $f - Mg$ are divisible by X_3, and since $\mathfrak{p}$ is prime, we must

have $(f - Mg)/X_3 \in \mathfrak{p}$. From this it follows again that f is in the ideal generated by $\mathscr{G}\backslash\{f\}$. We have not ruled out the possibility that $b_0 = 0$ and $a_0 > 0$. In this case we might have $f = X_0^{a_0}X_2^{a_2} - X_1^{a_1}$, $g = X_2^{b_2} - X_0^{b_0}X_3^{b_3}$ (other possibilities will have both terms of $f - Mg$ divisible by either X_1 or X_3 and the above argument goes through). But if this happens then $f - Mg = -X_1^{a_1} + X_0^{a_0+b_0}X_2^{a_2-b_2}X_3^{b_3}$. We have $a_1 > 0$ and $b_3 > 0$ so $f - Mg \in (X_1, X_3)$. Now replace the pair of minimal generators f, g by $g, f - Mg$, and we have a set $\mathscr{G}$ as stated in the Lemma. □

Example 2.5. The curve $\mathscr{S} = \{3, 4, 12\}$ has two sets of minimal generators $\{X_2^3 - X_0^2X_3, X_1^4 - X_0^3X_3\}$ and $\{X_2^3 - X_0^2X_3, X_0X_2^3 - X_1^4\}$, the second of which shows that Lemma 2.4 does not hold for arbitrary $\mathscr{G}$.

The minimal monomial generators of both J_1 and J_2 can both be described in terms of lattices as we now show. The reader should refer to the diagrams below, which illustrate the various definitions.

Definition 2.6. Let $\mathscr{L}_{ij}$ be the free abelian subgroup of $\mathbb{Z}^2$ generated by $\boldsymbol{\alpha}_i$ and $\boldsymbol{\alpha}_j$ $(0 \le i < j \le 3)$. Define $\mathscr{L} = \mathscr{L}_{12} \cap \mathscr{L}_{03}$ and $\mathscr{L}' = \mathscr{L}_{02} \cap \mathscr{L}_{13}$. Also for $i < j$ define $C_{ij} = \{r_i\boldsymbol{\alpha}_i + r_j\boldsymbol{\alpha}_j \mid r_i, r_j \in \mathbb{R}, r_i \ge 0, r_j \ge 0\}$, the real cone spanned by $\boldsymbol{\alpha}_i$ and $\boldsymbol{\alpha}_j$.

Since $\dim_K(K[X_1, X_2]/J_1)$ is finite, J_1 contains monomials $X_1^{c_1}$ and $X_2^{c_2}$ as minimal generators where, for example, c_2 is the smallest positive integer such that $c_2\boldsymbol{\alpha}_2 = a_0\boldsymbol{\alpha}_0 + a_1\boldsymbol{\alpha}_1 + a_3\boldsymbol{\alpha}_3$ with $a_i \ge 0$, $a_0 + a_1 > 0$ and $a_3 > 0$. So the element of $\mathscr{G}$ mapping to $X_2^{c_2}$ is of the form $X_2^{c_2} - X_0^{a_0}X_1^{a_1}X_3^{a_3}$. Similarly the element of $\mathscr{G}$ mapping to $X_1^{c_1}$ is of the form $X_1^{c_1} - X_0^{a_0}X_2^{a_2}X_3^{a_3}$. All remaining elements of $\mathscr{G}$ not vanishing in $K[X_1, X_2]$ are of the form $X_1^{a_1}X_2^{a_2} - X_0^{a_0}X_3^{a_3}$ with $a_i > 0$ for all i. Hence except for $X_1^{c_1}$ and $X_2^{c_2}$ the minimal generators of J_1 all have S-degree in $C_{12} \cap \mathscr{L}$.

It is convenient to represent elements of $\mathscr{L}_{12}$ in $\boldsymbol{\alpha}_1$-$\boldsymbol{\alpha}_2$ coordinates which will be written in pointy brackets to distinguish from the original coordinates, which we continue to write with ( )'s. Thus $\langle a_1, a_2\rangle = a_1\boldsymbol{\alpha}_1 + a_2\boldsymbol{\alpha}_2$. Given any element $\langle a_1, a_2\rangle \in \mathscr{L}\backslash\{\langle 0, 0\rangle\}$ with $a_1, a_2 \ge 0$, we can uniquely write $\langle a_1, a_2\rangle = a_0\boldsymbol{\alpha}_0 + a_3\boldsymbol{\alpha}_3$, necessarily with $a_0, a_3 > 0$. Then $f = X_1^{a_1}X_2^{a_2} - X_0^{a_0}X_3^{a_3}$ is the unique pure binomial element of $\mathfrak{p}$ mapping to $X_1^{a_1}X_2^{a_2} \in J_1$. This gives an order preserving map from $C_{12} \cap (\mathscr{L}\backslash\{\langle 0, 0\rangle\}) = \{\langle a_1, a_2\rangle \in \mathscr{L}\backslash\{\langle 0, 0\rangle\} \mid a_1, a_2 \ge 0\}$ to a subset of the monomials in J_1 sending $\langle a_1, a_2\rangle$ to $X_1^{a_1}X_2^{a_2}$ (where we order $C_{12} \cap \mathscr{L}$ by the coordinatewise partial order on $\boldsymbol{\alpha}_1$-$\boldsymbol{\alpha}_2$ coordinates and the monomials by divisibility). Let $M_{\mathscr{L}}(1, 2)$ be the minimal elements of $C_{12} \cap (\mathscr{L}\backslash\{\langle 0, 0\rangle\})$ (under the partial order). By Lemma 2.3 and the above discussion the minimal generators of J_1 are $\{X_1^{c_1}, X_2^{c_2}\} \cup \{X_1^{a_1}X_2^{a_2} \mid \langle a_1, a_2\rangle \in M_{\mathscr{L}}(1, 2),\ a_1 < c_1,\ a_2 < c_2\}$.

Define $B_{\mathscr{L}}(1, 2)$ to be the elements of $\mathscr{L}$ on the boundary of the convex hull of $C_{12} \cap (\mathscr{L}\backslash\{\langle 0, 0\rangle\})$.

Theorem 2.7. *Let $\mathscr{S} = \{a, b, d\}$ be a projective monomial curve in $\mathbb{P}^3$, with notation as above. Then the S-degrees of the type one generators of $\mathfrak{p}$ are $\{\langle c_1, 0\rangle, \langle 0, c_2\rangle\} \cup \{\langle a_1, a_2\rangle \in B_{\mathscr{L}}(1, 2) \mid a_1 < c_1, a_2 < c_2\}$ where c_2 is the smallest positive integer*

such that there exists a point $\langle -a_1', c_2\rangle \in C_{23} \cap \mathscr{L}$ *and* c_1 *is the smallest positive integer such that there is a point* $\langle c_1, -a_2'\rangle \in C_{01} \cap \mathscr{L}$.

Proof. In view of the above discussion, we need only show that $M_{\mathscr{L}}(1,2) = B_{\mathscr{L}}(1,2)$. The boundary of the convex hull of $C_{12} \cap (\mathscr{L}\backslash\{\langle 0,0\rangle\})$ forms a decreasing arc of line segments from a point $\langle 0, a_2\rangle$ with $a_2 \geq c_2$ to a point $\langle a_1, 0\rangle$ with $a_1 \geq c_1$. From this it follows that $B_{\mathscr{L}}(1,2) \subseteq M_{\mathscr{L}}(1,2)$.

If there is a point $\mathtt{P} = \langle a_1, a_2\rangle \in M_{\mathscr{L}}(1,2)\backslash B_{\mathscr{L}}(1,2)$, then $\mathtt{P}$ lies "between" two consecutive vertices $\mathtt{B} = \langle b_1, b_2\rangle$ and $\mathtt{B}' = \langle b_1', b_2'\rangle$, of the boundary of the convex hull of $C_{12} \cap (\mathscr{L}\backslash\{\langle 0,0\rangle\})$, i.e., $b_1 < a_1 < b_1'$ and $b_2' < a_2 < b_2$. Then $\mathtt{B} + \mathtt{B}' - \mathtt{P} = \langle b_1 + b_2 - a_1, b_2 + b_2' - a_2\rangle \in \mathscr{L}$ which lies in the interior of the first quadrant of $\boldsymbol{\alpha}_1$-$\boldsymbol{\alpha}_2$ plane, below the line segment $\mathtt{BB}'$. Contradiction. □

Definition 2.8. The points $\langle -a_1', c_2\rangle \in C_{23} \cap \mathscr{L}$ and $\langle c_1, -a_2'\rangle \in C_{01} \cap \mathscr{L}$ in the above Theorem will be referred to respectively as the left and right truncation points of (the basis diagram of) $\mathscr{S}$. (Necessarily $a_1' \geq 0, a_2' \geq 0$. There may be a choice of a_1' or a_2', in which case take the smallest.)

We represent elements of $\mathscr{L}_{02}$ in $\boldsymbol{\alpha}_0$-$\boldsymbol{\alpha}_2$ coordinates which will be written in double brackets. Thus $[\![a_0, a_2]\!] = a_0\boldsymbol{\alpha}_0 + a_2\boldsymbol{\alpha}_2$. Also $[\![a_0, a_2]\!]$ is the S-degree of the monomial $X_0^{a_0}X_2^{a_2}$.

Let $\mathscr{G}$ be a set of pure binomial generators of $\mathfrak{p}$ as in Lemma 2.4. Note that $\dim_K(K[X_0, X_2]/J_2)$ is infinite because J_2 contains no power of X_0. However J_2 contains a monomial $X_2^{c_2}$ as minimal generator, where c_2 is the same as occurred in J_1. The monomial $X_2^{c_2}$ is the image of a binomial of the form $X_2^{c_2} - X_0^{a_0}X_1^{a_1}X_3^{a_3} \in \mathscr{G}$, where $a_3 > 0$ and $a_0 + a_1 > 0$. All other elements of $\mathscr{G}$ not vanishing in $K[X_0, X_2]$ are of the form $X_0^{a_0}X_2^{a_2} - X_1^{a_1}X_3^{a_3}$ where $a_0, a_1, a_2 > 0$ and $a_3 \geq 0$. Hence (except for $X_2^{c_2}$) the minimal monomial generators of J_2 all have S-degree in $C_{12} \cap \mathscr{L}'$. Furthermore every element $[\![a_0, a_2]\!] \in C_{12} \cap (\mathscr{L}'\backslash\{\langle 0,0\rangle\})$ is the S-degree of a binomial of the form $X_0^{a_0}X_2^{a_2} - X_1^{a_1}X_3^{a_3}$ (uniquely except possibly for $[\![0, c_2]\!]$).

We now have an order preserving map from $C_{12} \cap (\mathscr{L}'\backslash\{[\![0,0]\!]\})$ to a subset of the monomials in J_2 sending $[\![a_0, a_2]\!]$ to $X_0^{a_0}X_2^{a_2}$ (where we order $C_{12} \cap \mathscr{L}'$ by the coordinatewise partial order on $\boldsymbol{\alpha}_0$-$\boldsymbol{\alpha}_2$ coordinates and the monomials by divisibility). Let $M_{\mathscr{L}'}(1,2)$ be the minimal elements of $C_{12} \cap (\mathscr{L}'\backslash\{[\![0,0]\!]\})$ (under the partial order). By Lemma 2.4 and the above discussion the minimal generators of J_2 are $\{X_2^{c_2}\} \cup \{X_0^{a_0}X_2^{a_2} \mid [\![a_0, a_2]\!] \in M_{\mathscr{L}'}(1,2), \quad a_2 < c_2\}$.

In the $\boldsymbol{\alpha}_0$-$\boldsymbol{\alpha}_2$ plane the boundary of the convex hull of $C_{12} \cap (\mathscr{L}'\backslash\{[\![0,0]\!]\})$ forms an arc of line segments from a point $\mathtt{A} = [\![0, a_2]\!]$ with $a_2 \geq c_2$ on the $\boldsymbol{\alpha}_2$ ray to a point $\mathtt{B}$ on the $\boldsymbol{\alpha}_1$ ray. (To better understand this construction, refer to Example 2.13 and Figure 1 below.) Since the $\boldsymbol{\alpha}_1$ ray has a positive slope, this arc will have a minimum point $\mathtt{M}$ which could be either $\mathtt{A}$ or $\mathtt{B}$, but in general the arc decreases strictly from $\mathtt{A}$ to $\mathtt{M}$, may stay at the same height for a while, then increases strictly to $\mathtt{B}$. Similarly to the type one case, define $B_{\mathscr{L}'}(1,2)$ to be the elements of $\mathscr{L}'$ on the boundary of the convex hull of $C_{12} \cap (\mathscr{L}'\backslash\{[\![0,0]\!]\})$. As in the type one case

we have $M_{\mathscr{L}'}(1,2) \subseteq B_{\mathscr{L}'}(1,2)$. However $M_{\mathscr{L}'}(1,2)$ is only the points of $B_{\mathscr{L}'}(1,2)$ to the left of M (including M). We now have

Theorem 2.9. *Let $\mathscr{S} = \{a, b, d\}$ be a projective monomial curve in $\mathbb{P}^3$, with notation as above. Then the S-degrees of the type two generators of* $\mathfrak{p}$ *are $\{[\![a_1, a_2]\!] \in M_{\mathscr{L}'}(1,2) \mid a_2 < c_2\} \backslash \{\mathtt{B}\}$ where c_2 is the smallest positive integer such that there exists a point $[\![-a_1', c_2]\!] \in C_{23} \cap \mathscr{L}'$.*

Definition 2.10. The point $[\![-a_1', c_2]\!]$ will be referred to as the left truncation point of (the 02-basis diagram of) $\mathscr{S}$.

We have that $[\![0, c_2]\!]$ is the degree of a minimal generator of J_2, but $[\![0, c_2]\!] = \langle 0, c_2\rangle$, which is the degree of a type one generator, hence is excluded in Theorem 2.9. The point B might not be in $M_{\mathscr{L}'}(1,2)$ (it can lie strictly to the right of M), but if it is, we exclude it in Theorem 2.9 because it is also the degree of a type one generator. There is no right truncation point in the sense of the previous definitions, but M serves the same function of preventing some elements of $B_{\mathscr{L}'}(1,2)$ from being the degrees of type two generators.

In order to give generators of the lattices $\mathscr{L}$ and $\mathscr{L}'$, we introduce the following notation. There exist integers $h > 0$ and $\ell \geq 0$ such that $d = hb' - \ell a'$. For sake of definiteness, we take h to be the smallest integer greater than or equal to $\lceil d/b' \rceil$ such that $hb' - d$ is divisible by a'.

Recall that $\mathscr{L} = \mathscr{L}_{12} \cap \mathscr{L}_{03}$. Elements of $\mathscr{L}_{03}$ are easily recognized in the original coordinates by having both coordinates divisible by d. In fact, since sum of the coordinates of an element of S is divisible by d, it suffices to check the second coordinate. Therefore, noting that $\gcd(d, c) = 1$, we have a surjection from $\mathscr{L}_{12}$ to $\mathbb{Z}/d\mathbb{Z}$ sending $\langle a_1, a_2\rangle = a_1\boldsymbol{\alpha}_1 + a_2\boldsymbol{\alpha}_2 = a_1(d-a, a) + a_2(d-b, b)$ to $a_1a' + a_2b'$ mod d with kernel L. Therefore $\mathscr{L}$ is of index d in $\mathscr{L}_{12}$.

Lemma 2.11. *The lattice $\mathscr{L}$ is generated by $\langle b', -a'\rangle$ and $\langle -\ell, h\rangle$.*

Proof. Clearly $\langle b', -a'\rangle$ and $\langle -\ell, h\rangle$ are in $\mathscr{L}$ and $\det \begin{pmatrix} b' & -\ell \\ -a' & h \end{pmatrix} = d$, so they generate $\mathscr{L}$. □

Generators of the lattice $\mathscr{L}'$ are given as follows.

Lemma 2.12. *The lattice $\mathscr{L}'$ (in $\boldsymbol{\alpha}_0$-$\boldsymbol{\alpha}_2$ coordinates) is generated by $[\![b' - a', a']\!]$ and $[\![\ell - h + c, h]\!]$. The index of $\mathscr{L}'$ in $\mathscr{L}_{02}$ is $d - a$.*

Proof. First of all $[\![b' - a', a']\!] = b'\boldsymbol{\alpha}_1$ by Remark 2.1-(1) and $[\![\ell - h + c, h]\!] = \ell\boldsymbol{\alpha}_1 + c\boldsymbol{\alpha}_3$ by a simple calculation, so $[\![b' - a', a']\!]$ and $[\![\ell - h + c, h]\!]$ are in $\mathscr{L}'$.

Suppose that $[\![\lambda_0, -\lambda_2]\!] \in \mathscr{L}'$. Then there exist integers λ_1 and λ_3 such that

$$\lambda_0\boldsymbol{\alpha}_0 - \lambda_2\boldsymbol{\alpha}_2 = \lambda_1\boldsymbol{\alpha}_1 + \lambda_3\boldsymbol{\alpha}_3 \tag{1}$$

Therefore $\lambda_1\boldsymbol{\alpha}_1 + \lambda_2\boldsymbol{\alpha}_2 \in \mathscr{L}_{12} \cap \mathscr{L}_{03} = \mathscr{L}$. By Lemma 2.11, there exist $e_1, e_2 \in \mathbb{Z}$ such that $\lambda_1\boldsymbol{\alpha}_1 + \lambda_2\boldsymbol{\alpha}_2 = e_1\langle b', -a'\rangle + e_2\langle -\ell, h\rangle = (e_1b' - e_2\ell)\boldsymbol{\alpha}_1 + (-e_1a' + e_2h)\boldsymbol{\alpha}_2$. Comparing $\boldsymbol{\alpha}_1$-$\boldsymbol{\alpha}_2$ coordinates we have $\lambda_1 = e_1b' - e_2\ell$ and $\lambda_2 = -e_1a' + e_2h$. Substituting that into Equation 1, we obtain $\lambda_0\boldsymbol{\alpha}_0 = (e_1b' - e_2\ell)\boldsymbol{\alpha}_1 + (-e_1a' +$

$e_2h)\boldsymbol{\alpha}_2+\lambda_3\boldsymbol{\alpha}_3$. Comparing the first coordinates (in the original coordinate system) and dividing by d, we have $\lambda_0 = e_1(b'-a') - e_2(\ell-h+c)$. Substituting into $[\![\lambda_0, -\lambda_2]\!]$ we get $[\![\lambda_0, -\lambda_2]\!] = [\![e_1(b'-a') - e_2(\ell-h+c), e_1a' - e_2h]\!] = e_1[\![b'-a', a']\!] - e_2[\![\ell-h+c, h]\!]$, so $[\![b'-a', a']\!]$ and $[\![\ell-h+c, h]\!]$ generate $\mathscr{L}'$. The matrix with first row $(b'-a', a')$ and second row $(\ell-h+c, h)$ has determinent $d-a$, from which the last assertion follows. □

Example 2.13. It is convenient to plot the basis and the lattice $\mathscr{L}$ in $\boldsymbol{\alpha}_1$-$\boldsymbol{\alpha}_2$ coordinates which we call the basis diagram, illustrated in the left graph of Figure 1 for the curve $\mathscr{S} = \{6, 11, 13\}$. Similarly we can plot S-degrees of monomials not in J_2 and the lattice $\mathscr{L}'$ in $\boldsymbol{\alpha}_0$-$\boldsymbol{\alpha}_2$ coordinates which we call 02-basis diagram. The right graph of Figure 1 illustrates the 02-basis diagram also for $\mathscr{S} = \{6, 11, 13\}$.

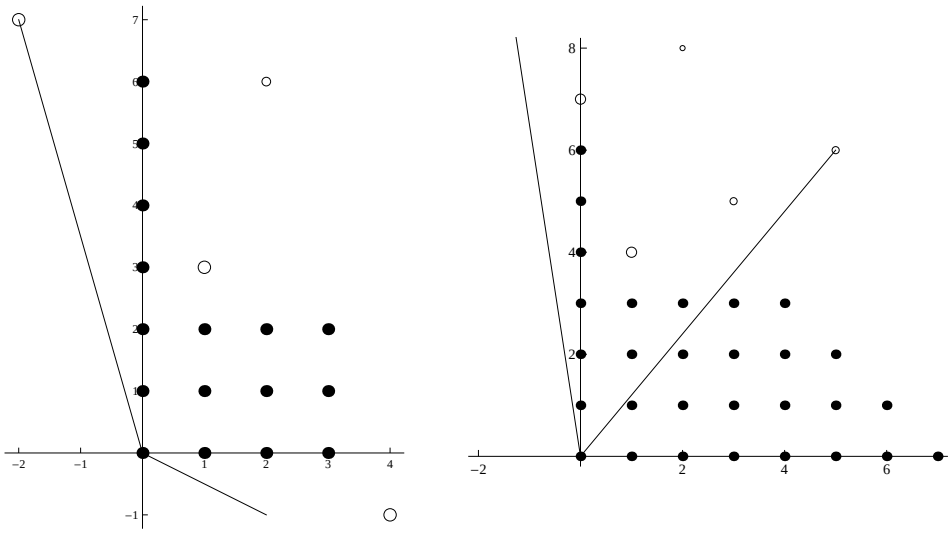

FIGURE 1

For $\mathscr{S} = \{6, 11, 13\}$, we have $a' = a = 6$, $b' = b = 11$, $c = 1$, $\ell = 7$ and $h = 5$. By Lemma 2.11, $\mathscr{L}$ is generated by $\langle b', -a'\rangle = \langle 11, -6\rangle$ and $\langle -\ell, h\rangle = \langle -7, 5\rangle$. By elementary operations on these generators, we obtain a set $\{\langle 1, 3\rangle, \langle 4, -1\rangle\}$ of more convenient generators. In the basis diagram, the diagonal lines indicate the directions of $\boldsymbol{\alpha}_0$ and $\boldsymbol{\alpha}_3$, given by Remark 2.1. These half lines we call the $\boldsymbol{\alpha}_0$ and $\boldsymbol{\alpha}_3$ rays respectively. For example, 2.1-(2) says that $(b-a)\boldsymbol{\alpha}_3 = \langle -(d-b), d-a\rangle = \langle -2, 7\rangle$ which is the first element of $\mathscr{L}$ on the $\boldsymbol{\alpha}_3$ ray, and is plotted in the diagram. In the basis diagram, C_{01} is the cone between the $\boldsymbol{\alpha}_0$ ray and the horizontal axis ($\boldsymbol{\alpha}_1$ ray) and C_{23} is the cone between the vertical axis ($\boldsymbol{\alpha}_2$ ray) and the $\boldsymbol{\alpha}_3$ ray. It is clear from the generators of $\mathscr{L}$ that the right truncation (Definition 2.8) point is $\langle 4, -1\rangle$ and the left truncation point is $\langle -2, 7\rangle$. The first non-zero elements of $\mathscr{L}$ on the axes are $\langle 13, 0\rangle$ and $\langle 0, 13\rangle$ (not plotted) so that $M_{\mathscr{L}}(1, 2) = \{\langle 13, 0\rangle, \langle 1, 3\rangle, \langle 0, 13\rangle\}$.

By Lemma 2.3 and Theorem 2.7 the minimal generators of J_1 and the type one generators of $\mathfrak{p}$ are in degrees $\langle 0, 7\rangle, \langle 1, 3\rangle, \langle 4, 0\rangle$, so that J_1 is minimally generated by $X_2^7, X_1X_2^3, X_1^4$. These lift easily to type one generators $\{X_2^7 - X_1^2X_3^5, X_1X_2^3 - X_0X_3^3, X_1^4 - X_2X_0^2X_3\}$ of $\mathfrak{p}$. The $\boldsymbol{\alpha}_1$-$\boldsymbol{\alpha}_2$ coordinates of monomials not in J_1 (the

basis elements) are plotted as solid dots. We observe that $|\mathcal{B}| = 16 > d = 13$ so that $\mathscr{S}$ is not Cohen-Macaulay by Theorem 1.2. In the basis diagram $\langle 1, 3\rangle$ and the truncation points $\langle -2, 7\rangle, \langle 4, -1\rangle$ are plotted as large open circles, and an additional lattice point $\langle 2, 6\rangle$ is plotted as a small open circle, so as to better illustrate the pattern of $\mathscr{L}$.

The 02-basis diagram is constructed in a similar manner. This time the $\boldsymbol{\alpha}_0$ ray is the horizontal axis and the $\boldsymbol{\alpha}_2$ ray is the vertical axis. Remark 2.1 gives points $[\![5, 6]\!]$ on $\boldsymbol{\alpha}_1$ ray and $[\![-2, 13]\!]$ on the $\boldsymbol{\alpha}_3$-ray. (The latter point is outside the diagram, but its direction is plotted.) Lemma 2.12 gives generators of $\mathscr{L}'$. Using these, some elements of $\mathscr{L}'$ are plotted as open circles. The left truncation point $[\![0, 7]\!]$ lies on the $\boldsymbol{\alpha}_2$ axis. In the 02-basis diagram the cone C_{12} is no longer the entire first quadrant because the $\boldsymbol{\alpha}_1$-ray now has positive slope. The arc referred to in the discussion before Theorem 2.9 consists of the line segment from $[\![0, 7]\!]$ on the $\boldsymbol{\alpha}_2$-ray to $\mathtt{M} = [\![1, 4]\!]$ followed by the line segment from $\mathtt{M}$ to $\mathtt{B} = [\![5, 6]\!]$ on the $\boldsymbol{\alpha}_1$-ray. There is an intermediate element $[\![3, 5]\!]$ of $\mathscr{L}'$ on the latter segment. From the diagram we see that $M_{\mathscr{L}'}(1, 2) = \{[\![0, 7]\!], [\![1, 4]\!]\}$ (plotted as large open circles) and that $B_{\mathscr{L}'}(1, 2) = \{[\![0, 7]\!], [\![1, 4]\!], [\![3, 5]\!], [\![5, 6]\!]\}$ (with $B_{\mathscr{L}'}(1, 2)\backslash M_{\mathscr{L}'}(1, 2)$ plotted as medium sized open circles). One additional element $[\![2, 8]\!]$ of $\mathscr{L}'$ is plotted as a small open circle. By Lemma 2.4 and Theorem 2.9 the ideal J_2 is minimally generated by X_2^7, $X_0X_2^4$, and there is one type two generator $X_0X_2^4 - X_1^3X_3^2$ of $\mathfrak{p}$ in degree $[\![1, 4]\!]$, giving a four element minimal set of generators for $\mathfrak{p}$. The solid dots in the diagram are the $\boldsymbol{\alpha}_0$-$\boldsymbol{\alpha}_2$ coordinates of monomials not in J_2 (with the bottom four rows extending indefinitely to the right).

The basis diagrams can be worked out explicitly for several infinite classes of examples. We describe two of these.

Example 2.14. Let d be even and $\gcd(a, d/2) = 1$. Let $\mathscr{S} = \{a, a+d/2, d\}$. Here $a' = a$, $b' = b = a + d/2$, $\ell = h = 2$. By Lemma 2.11 the lattice $\mathscr{L}$ is generated by $\langle b, -a\rangle$ and $\langle -\ell, h\rangle = \langle -2, 2\rangle$, and (in the basis diagram) looks like bands, the i-th band being $\{i\langle b, -a\rangle + j\langle -2, 2\rangle \mid j \in \mathbb{Z}\}$. If $i \leq 0$, by Remark 2.1, the intersection of the i-th band with C_{03} is at most $\langle 0, 0\rangle$. On the band $i = 1$ the first elements of $\mathscr{L}$ outside the interior of C_{12} are, on the right and left respectively, $\mathrm{A} = \langle b - 2\lfloor a/2\rfloor, -a + 2\lfloor a/2\rfloor\rangle$ and $\mathrm{B} = \langle b - 2\lceil b/2\rceil, 2\lceil b/2\rceil - a\rangle$. The points A and B are in C_{03} because $(b - a)\boldsymbol{\alpha}_0$ and $(b - a)\boldsymbol{\alpha}_3$ as given in Remark 2.1-(1) (2) are on the band $i = 1$. If $i > 1$ the corresponding points on the i-th band are further from the origin, so A and B are the truncation points. Now it follows from Theorem 2.7 that the S-degrees of type one generators consist of $\langle b - 2\lfloor a/2\rfloor, 0\rangle$, $\langle 0, 2\lceil b/2\rceil - a\rangle$, and the elements of $\mathscr{L}$ on the first band in the interior of the first quadrant. The first band consists of points on the line $\{\langle \lambda_1, \lambda_2\rangle \mid \lambda_1 + \lambda_2 = d/2\}$, and we are taking every second integer point on this line in the first quadrant. If $d/2$ is even then a and b are both odd and there are $d/4$ interior type one generators, and if $d/2$ is odd, then one of a, b is even and the other is odd, and there are $(d - 2)/4$. A simple calculation now shows that all these curves have $\lceil((d/2) + 1)^2/2\rceil$ basis elements. For these curves, a similar analysis of 02-basis diagram shows there is only one type two generator $[\![1, 2]\!]$.

The curves of Example 2.14 are of special interest because if d is even they appear to have the largest number of type one ideal generators and the largest number of basis elements among curves in $\mathbb{P}^3$ of degree d.

Example 2.15. Now we consider $\mathscr{S} = \{a, b, d\}$ where $b = d-a$, and $\gcd(a, d) = 1$ (equivalently $\gcd(a, b) = 1$). Since $b > a$ we have $d > 2a$. Here $\langle 1, 1\rangle = \boldsymbol{\alpha}_1 + \boldsymbol{\alpha}_2 = \boldsymbol{\alpha}_0 + \boldsymbol{\alpha}_3 \in \mathscr{L}$. Therefore there are three type one generators of $\mathfrak{p}$ with S-degrees $\langle 1, 1\rangle$ and the two points on the axes.

The lattice $\mathscr{L}'$ can be described as follows. Since $\boldsymbol{\alpha}_0 - \boldsymbol{\alpha}_2 = \boldsymbol{\alpha}_1 - \boldsymbol{\alpha}_3$, $[\![1, -1]\!] \in \mathscr{L}'$ and by Remark 2.1-(2) $[\![0, b]\!] \in \mathscr{L}'$. The subgroup of $\mathscr{L}_{02}$ generated by $[\![1, -1]\!]$ and $[\![0, b]\!]$ has index $b = d-a$ in $\mathscr{L}_{02}$, hence $\mathscr{L}'$ is generated by $[\![1, -1]\!]$ and $[\![0, b]\!]$ by Lemma 2.12. By Remark 2.1-(1) $[\![b - a, a]\!] = b\boldsymbol{\alpha}_1$. Thus $B_{\mathscr{L}'}(1, 2) = M_{\mathscr{L}'}(1, 2) = \{[\![0, b]\!] + i[\![1, -1]\!] = [\![i, b - i]\!] \mid 0 \le i \le b - a$. It follows that the ideal J_2 is generated by $X_0^i X_2^{b-i}$ for $i = 0, 1, \cdots, b - a$, which yields the type two generators $X_0^i X_2^{b-i} - X_1^{a+i} X_3^{b-a-i}, i = 1, \cdots, b - a - 1$ of $\mathfrak{p}$.

Remark 2.16. The curves $\{1, d - 1, d\}$ have the largest number of type two generators, namely $d - 3$, and appear to have the largest total number of ideal generators, namely d, among all monomial curves of degree d in $\mathbb{P}^3$. This is in contrast to the affine monomial curve case. For any projective monomial curve $\mathcal{C}$ given by $\mathscr{S} = \{a_1, \ldots a_p\}$, the intersection $\mathcal{C}_0 := \mathcal{C} \cap \mathbb{A}^p_K$ of $\mathcal{C}$ in the affine space $\mathbb{A}^p_K := \mathbb{P}^p_K \setminus \{(0 : c_1 : \cdots : c_p) \mid c_1, \ldots, c_p \in K\}$ is an affine monomial curve $\mathrm{Spec}(K[\Gamma])$ with defining ideal $\mathfrak{p}_0 = \ker \phi_0$, where $\phi_0 : K[X_1, \ldots, X_p] \to K[t]$ is defined by $\phi_0(X_i) = t^{a_i}$, $1 \le i \le p$. If $\mathfrak{p}$ is generated by $f_i(X_0, \ldots, X_p), 1 \le i \le s$ then $\mathfrak{p}_0$ is generated by $f_i(1, X_1, \cdots, X_p)$. However $\mathfrak{p}_0$, in general, has fewer generators than $\mathfrak{p}$. In particular, if $p = 3$, $\mathfrak{p}_0$ is always generated by at most three elements by a result of Herzog [7] or [19, Theorem 10.3.10].

Remark 2.17. We have proved, using Theorem 1.2, that $K[S]$ is Cohen-Macaulay if and only if the truncation points generate $\mathscr{L}$, equivalently, if and only if there exist $\mathtt{A} \in C_{01} \cap \mathscr{L}$ and $\mathtt{B} \in C_{23} \cap \mathscr{L}$ such that $\mathscr{L}$ is generated by $\mathtt{A}$ and $\mathtt{B}$. This permits easier visual recogonition of Cohen-Macaulay property than counting $|\mathcal{B}|$. For instance, $\mathscr{S} = \{6, 11, 13\}$ of Example 2.13 is not Cohen-Macaulay because $\langle 1, 4\rangle \in \mathscr{L}$ is clearly not in the lattice generated by the truncation points. Furthermore, we have $\langle -\ell, h\rangle = (h - \ell - c)\boldsymbol{\alpha}_0 + c\boldsymbol{\alpha}_3$, so that $\langle -\ell, h\rangle \in C_{23} \cap \mathscr{L}$ if and only if $h - \ell - c \ge 0$. If $h - \ell - c \ge 0$ then (taking $\mathtt{A} = \langle b', -a'\rangle$, $\mathtt{B} = \langle -\ell, h\rangle$) $K[S]$ is Cohen-Macaulay by Lemma 2.11. We may also choose a, b, ℓ, h and (so long as $hb' - \ell a' > b$ and $\gcd(a, b, hb' - \ell a') = 1$) define $\mathscr{S} = \{a, b, hb' - \ell a')$, thereby constructing curves with specified $\mathscr{L}$. Example 2.14 was found in this way.

3. Basis and ideal generators for an arithmetic progression

Throughout this section $\mathscr{S} = \{ a_1, \ldots, a_p\}$ will be an arithmetic progression with common difference δ, so that $a_i = a_1 + (i-1)\delta$, $1 \le i \le p$. We assume that $\delta > 0$ and $\gcd(a_1, \delta) = 1$. Let $S \subseteq \mathbb{N}^2$ be the semigroup generated by $\boldsymbol{\beta} = (a_p, 0)$ and $\boldsymbol{\alpha}_i = (a_p - a_i, a_i)$, $i = 1, \cdots, p$. In this section we will use $\boldsymbol{\beta}$ instead of $\boldsymbol{\alpha}_0$ because it plays a different role in our discussions than the other $\boldsymbol{\alpha}_i$, but we will continue

to use a_p and d interchangeably. Let T be the semigroup generated by $\boldsymbol{\beta}$ and $\boldsymbol{\alpha}_p$. In Theorem 3.4 below, we describe the basis $\mathcal{B}$ of S over T explicitly. To do this we first introduce a unique way of representing basis elements (for which $\mathscr{S}$ need not be an arithmetic progression).

Definition 3.1. Let $\tilde{S}$ be the semigroup generated by $\boldsymbol{\alpha}_1, \ldots, \boldsymbol{\alpha}_{p-1}$. Then clearly $\mathcal{B} \subseteq \tilde{S}$. For $\boldsymbol{\alpha} \in \tilde{S}$, let $\mathcal{E}(\boldsymbol{\alpha}) := \{(c_1, \ldots, c_{p-1}) \in \mathbb{N}^{p-1} \mid \boldsymbol{\alpha} = \sum_{i=1}^{p-1} c_i \boldsymbol{\alpha}_i\}$. Then $\mathcal{E}(\boldsymbol{\alpha})$ is a finite set for every $\boldsymbol{\alpha} \in \tilde{S}$. Let $\preceq$ denote the lexicographic (left to right) order on $\mathcal{E}(\boldsymbol{\alpha})$. Therefore for $\mathbf{c} = (c_1, \ldots, c_{p-1})$, $\mathbf{c}' = (c'_1, \ldots, c'_{p-1}) \in \mathcal{E}(\boldsymbol{\alpha})$, $\mathbf{c} \prec \mathbf{c}'$ if $c_1 = c'_1, \ldots, c_i = c'_i$ and $c_{i+1} < c'_{i+1}$ for some $i \in [0, p-2]$. Then $\preceq$ is a total order on $\mathcal{E}(\boldsymbol{\alpha})$ and, since $\mathcal{E}(\boldsymbol{\alpha})$ is a finite set, $\mathcal{E}(\boldsymbol{\alpha})$ has a maximum with respect to the order $\preceq$ which we denote by $\max \mathcal{E}(\boldsymbol{\alpha})$. Let $\mathcal{B}_{\max} := \{\max \mathcal{E}(\boldsymbol{\alpha}) \mid \boldsymbol{\alpha} \in \mathcal{B}\}$. Clearly the map $\mathcal{B} \to \mathcal{B}_{\max}$ defined by $\boldsymbol{\alpha} \mapsto \max \mathcal{E}(\boldsymbol{\alpha})$ is a bijection. The support Supp of a vector is the set of indices of its non-zero coordinates.

Since $\mathscr{S}$ is an arithmetic progression, $\mathscr{S}$ is Cohen-Macaulay by [10, Theorem 1.2 and Corollary 1.10], or [14, Theorem 2.2)]. Hence by Theorem 1.2

(**3.1.a**) $$|\mathcal{B}_{\max}| = |\mathcal{B}| = a_p\,.$$

The following easy observation is used in the proofs of Lemma 3.2 and Lemma 3.3:

(**3.1.b**) *If* $\mathbf{c} \in \mathbb{N}^{p-1}$ *and* $\mathbf{c} \notin \mathcal{B}_{\max}$ *then* $\mathbf{c} + \mathbf{c}' \notin \mathcal{B}_{\max}$ *for every* $\mathbf{c}' \in \mathbb{N}^{p-1}$.

Lemma 3.2. *Let* $\mathbf{e}_1, \ldots \mathbf{e}_{p-1}$ *denote the standard basis of* $\mathbb{N}^{p-1}$.

(1) $\max \mathcal{E}(\boldsymbol{\alpha}_i) = \mathbf{e}_i$ *for every* $i \in [1, p-1]$.
(2) $\mathbf{e}_i + \mathbf{e}_j \notin \mathcal{B}_{\max}$ *for every* $i, j \in [2, p-1]$.
(3) *If* $\boldsymbol{\alpha} \in \mathcal{B}$ *and* $\max \mathcal{E}(\boldsymbol{\alpha}) = \mathbf{c} = (c_1, \ldots, c_{p-1})$, *then* $|\mathrm{Supp}(\mathbf{c}) \cap [2, p-1]| \leq 1$ *and if* $i \in \mathrm{Supp}(\mathbf{c}) \cap [2, p-1]$, *then* $c_i = 1$.
(4) *If* $\boldsymbol{\alpha} \in S$ *and* $\boldsymbol{\alpha} = c_1\boldsymbol{\alpha}_1 + \boldsymbol{\alpha}_i + c_p\boldsymbol{\alpha}_p$, $1 \leq i \leq p-1$ *and* $c_1 \geq 0, c_p \geq 0$ *then* i, c_1 *and* c_p *are uniquely determined. Moreover, if* $\boldsymbol{\alpha} \in \mathcal{B}$ *then* $c_p = 0$ *and* $\max \mathcal{E}(\boldsymbol{\alpha}) = c_1\mathbf{e}_1 + \mathbf{e}_i$.
(5) *If* $\boldsymbol{\alpha} \in S$ *and* $\boldsymbol{\alpha} = c_0\boldsymbol{\beta} + \boldsymbol{\alpha}_i + c_p\boldsymbol{\alpha}_p$, $1 \leq i \leq p$ *and* $c_0 \geq 0, c_p \geq 0$ *then* i, c_0 *and* c_p *are uniquely determined.*

Proof. (1) Since $a_i < a_p$, we have $\boldsymbol{\alpha}_i \in \mathcal{B}$, $\mathcal{E}(\boldsymbol{\alpha}_i) = \{\mathbf{e}_i\}$ and hence $\max \mathcal{E}(\boldsymbol{\alpha}_i) = \mathbf{e}_i$ for every $i = 1, \ldots, p-1$.

(2) Since $a_1, \ldots, a_p$ is an arithmetic progression, we have

(3.2.a) $$\boldsymbol{\alpha}_i + \boldsymbol{\alpha}_j = \begin{cases} \boldsymbol{\alpha}_1 + \boldsymbol{\alpha}_{i+j-1}, & \text{if } i+j \leq p+1, \\ \boldsymbol{\alpha}_{i+j-p} + \boldsymbol{\alpha}_p, & \text{if } i+j \geq p+1. \end{cases}$$

Therefore, if $i+j > p$, then $\boldsymbol{\alpha}_i + \boldsymbol{\alpha}_j \notin \mathcal{B}$ and hence $\mathbf{e}_i + \mathbf{e}_j \notin \mathcal{B}_{\max}$. If $i+j \leq p$, then $\mathbf{e}_i + \mathbf{e}_j, \mathbf{e}_1 + \mathbf{e}_{i+j-1} \in \mathcal{E}(\boldsymbol{\alpha}_i + \boldsymbol{\alpha}_j)$ and $\mathbf{e}_i + \mathbf{e}_j \prec \mathbf{e}_1 + \mathbf{e}_{i+j-1}$. Therefore $\mathbf{e}_i + \mathbf{e}_j \neq \max \mathcal{E}(\boldsymbol{\alpha}_i + \boldsymbol{\alpha}_j)$, i .e. $\mathbf{e}_i + \mathbf{e}_j \notin \mathcal{B}_{\max}$.

(3) Immediate from (2) by using 3.1.b. (4) Suppose that $\boldsymbol{\alpha} = (\alpha_1, \alpha_2)$. The first coordinate of the equation $\boldsymbol{\alpha} = c_1\boldsymbol{\alpha}_1 + \boldsymbol{\alpha}_i + c_p\boldsymbol{\alpha}_p$ is $\alpha_1 = c_1(d - a_1) + (d - a_i)$

and $d - a_1 \geq d - a_i$ from which it follows that $d - a_i \equiv \alpha_1 \mod (d - a_1)$. This determines i. The uniqueness of c_1 and c_p now follows from the linear independence of $\boldsymbol{\alpha}_1$ and $\boldsymbol{\alpha}_p$. If $\boldsymbol{\alpha} \in \mathcal{B}$ then $c_p = 0$ by definition of $\mathcal{B}$ and the assertion about max $\mathcal{E}(\boldsymbol{\alpha})$ is clear. The proof of (5) is similar, taking congruence classes mod d. □

Lemma 3.3. *Let $q \in \mathbb{N}$ and $r \in [1, p-1]$ be defined by the (Euclidean algorithm) equation $a_1 = q(p-1) + r$ with $r \in [1, p-1]$. Then :*

(1) *$a_{r+1} + qa_p = (q + \delta + 1)a_1 \equiv 0 \pmod{a_1}$ and $(q + \delta)a_1 + a_i = qa_p + a_{r+i}$ for every $1 \leq i \leq p - r$. Moreover, $(q + \delta + 1)\boldsymbol{\alpha}_1 = \delta\boldsymbol{\beta} + \boldsymbol{\alpha}_{r+1} + q\boldsymbol{\alpha}_p$. In particular, $(q + \delta + 1)\boldsymbol{\alpha}_1 \notin \mathcal{B}$ and hence $(q + \delta + 1)\mathbf{e}_1 \notin \mathcal{B}_{\max}$.*

(2) *$(q + \delta)\boldsymbol{\alpha}_1 + \boldsymbol{\alpha}_i = \delta\boldsymbol{\beta} + \boldsymbol{\alpha}_{r+i} + q\boldsymbol{\alpha}_p$ for every $i = 2, \ldots p - r$. In particular, $(q + \delta)\boldsymbol{\alpha}_1 + \boldsymbol{\alpha}_i \notin \mathcal{B}$ for every $i \in [2, p - r]$ and hence $(q + \delta)\mathbf{e}_1 + \mathbf{e}_i \notin \mathcal{B}_{\max}$.*

(3) *Let $\mathcal{B}_1 = \{b\mathbf{e}_1 \mid b \in [0, q + \delta]\}$, $\mathcal{B}_2 = \{b\mathbf{e}_1 + \mathbf{e}_i \mid b \in [0, q + \delta - 1]$ and $i \in [2, p - r]\}$, and $\mathcal{B}_3 = \{b\mathbf{e}_1 + \mathbf{e}_j \mid b \in [0, q + \delta]$ and $j \in [p - r + 1, p - 1]\}$. Then $\mathcal{B}_{\max} \subseteq \mathcal{B}_1 \cup \mathcal{B}_2 \cup \mathcal{B}_3$.*

Proof. (1) By definitions of q and r, we have

$$a_{r+1} + qa_p = (q + 1)a_1 + (q(p - 1) + r)\delta = (q + \delta + 1)a_1 \tag{3.3.a}$$

and hence by adding a_i on both sides of (3.3.a), using the equality $a_{r+1} + a_i = a_1 + a_{r+i}$ and then cancelling a_1 on both sides we get $(q + \delta)a_1 + a_i = qa_p + a_{r+i}$ for every $1 \leq i \leq p - r$. Further, from (3.3.a) we have

$$\delta a_p + (a_p - a_{r+1}) = (q + \delta + 1)a_p - (a_{r+1} + qa_p) = (q + \delta + 1)(a_p - a_1) \tag{3.3.b}$$

Therefore using (3.3.a) for the second coordinate and (3.3.b) for the first coordinate we get the equality $\delta\boldsymbol{\beta} + \boldsymbol{\alpha}_{r+1} + q\boldsymbol{\alpha}_p = (q + \delta + 1)\boldsymbol{\alpha}_1$.

(2) For $i \in [2, p - r]$, we have $r + i \leq p$ and $\boldsymbol{\alpha}_{r+1} + \boldsymbol{\alpha}_i = \boldsymbol{\alpha}_1 + \boldsymbol{\alpha}_{r+i}$ by (3.2.a). Using this equality and by adding $\boldsymbol{\alpha}_i$ to the equation $\delta\boldsymbol{\beta} + \boldsymbol{\alpha}_{r+1} + q\boldsymbol{\alpha}_p = (q + \delta + 1)\boldsymbol{\alpha}_1$ and then canceling $\boldsymbol{\alpha}_1$, we get the required equality.

(3) Immediate from (1) and (2) by using (3.1.b). □

Theorem 3.4. *$\mathcal{B}_{\max} = \mathcal{B}_1 \cup \mathcal{B}_2 \cup \mathcal{B}_3$, where the sets $\mathcal{B}_1$, $\mathcal{B}_2$ and $\mathcal{B}_3$ are as in the* Lemma 3.3-(3).

Proof. The sets $\mathcal{B}_1$, $\mathcal{B}_2$ and $\mathcal{B}_3$ are mutually disjoint and $\mathcal{B}_{\max} \subseteq \mathcal{B}' := \mathcal{B}_1 \cup \mathcal{B}_2 \cup \mathcal{B}_3$ by Lemma 3.3-(3) and $|\mathcal{B}'| = (q + \delta + 1) + (p - r - 1)(q + \delta) + (r - 1)(q + \delta + 1) = q(p - 1) + r + (p - 1)\delta = a_1 + (p - 1)\delta = a_p = |\mathcal{B}_{\max}|$ by (3.1.a). Therefore we must have the equality $\mathcal{B}_{\max} = \mathcal{B}'$. □

The following examples may help the reader visualize Theorem 3.4.

Examples 3.5. (1) Let $\mathscr{S} = \{1, 4, 7, 10\}$. Here $a_1 = 1$, $p = 4$, $(d =)\ a_4 = 10$, $\delta = 3$, $q = 0$, $r = 1$. We have $\boldsymbol{\beta} = (10, 0), \boldsymbol{\alpha_1} = (9, 1), \boldsymbol{\alpha_2} = (6, 4), \boldsymbol{\alpha_3} = (3, 7)$ and $\boldsymbol{\alpha_4} = (0, 10)$.

(2) Let $\mathscr{S} = \{3, 5, 7, 9, 11\}$. Here $a_1 = 3,\ p = 5,\ (d =)\ a_5 = 11,\ \delta = 2,\ q = 0,\ r = 3$. We have $\boldsymbol{\beta} = (11, 0), \boldsymbol{\alpha_1} = (8, 3), \boldsymbol{\alpha_2} = (6, 5), \boldsymbol{\alpha_3} = (4, 7), \boldsymbol{\alpha_4} = (2, 9)$ and $\boldsymbol{\alpha_5} = (0, 11)$.

In Figure 2, we plot (in the original coordinates) the bases of Example 3.5, (1) on the left and (2) on the right. In each case the S-degrees of the basis elements are plotted as small dots, and the S-degrees of the ideal generators F_i (defined below) are large dots. (The degrees of the F_i are distinct from those of the basis elements.) The quadratic generators ξ_{ij} are omitted.

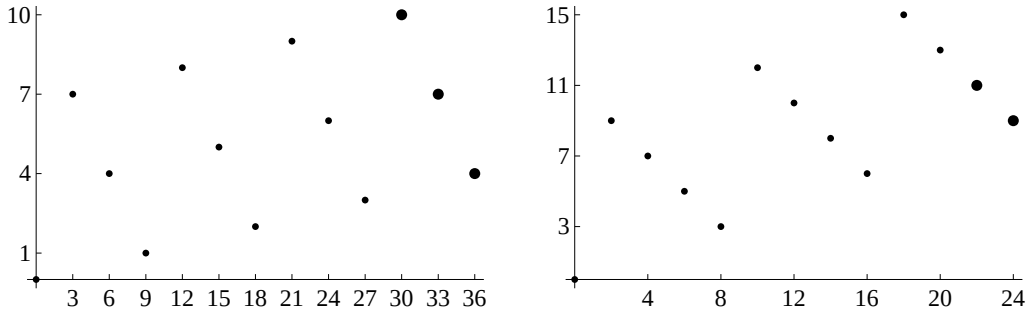

FIGURE 2

The basis $\mathcal{B}$ consists of points in $p-1$ diagonal lines, numbered $i = 1 \dots p-1$, each of slope $\boldsymbol{\alpha_1}$. In the bottom line, ($i = 1$, corresponding to $\mathcal{B}_1$), are the basis elements $\{i\boldsymbol{\alpha_1} \mid 0 \le i \le q + \delta\}$. Corresponding to $\mathcal{B}_2$ (possibly empty) are basis elements $\{i\boldsymbol{\alpha}_1 + (j-1)(-\delta, \delta)\}$, $1 \le i \le q + \delta$, in lines $j, 2 \le j \le p - r$. Corresponding to $\mathcal{B}_3$ (possibly empty) are basis elements $\{i\boldsymbol{\alpha}_1 + (j-1)(-\delta, \delta)\}$, $1 \le i \le q+\delta+1$, in lines $j, p-r+1 \le j \le p-1$. Basis elements corresponding to $\mathcal{B}_1$ and $\mathcal{B}_2$ end in degree $q + \delta$ and those corresponding to $\mathcal{B}_3$ extend one higher, to degree $q+\delta+1$. There are $p-r$ F_i's, $1 \le i \le p-r$, all of degree $q+\delta+1$. Their plots extend by one the basis elements in lines $i, 1 \le i \le p - r$ corresponding to $\mathcal{B}_1 \cup \mathcal{B}_2$. (If $\mathcal{B}_3 = \emptyset$ this will be every line, as in the left diagram.)

Notation 3.6. We continue using the notation introduced in Section 1, except we use the indeterminate W instead of X_0. This is to emphasize the fact that the second coordinate 0 of $\boldsymbol{\beta}$ is not part of the arithmetic progression (except for the case $\mathscr{S} = \{1, 2, \dots, p\}$). Therefore $R = K[W, X_1, \dots, X_p]$, and if $\mu = (\mu_0, \mu_1, \dots, \mu_p)$ then $X^\mu = W^{\mu_0} X_1^{\mu_1} \dots X_p^{\mu_p}$. We define $\deg(\mu) = \sum_i \mu_i$ (so that $\deg(\mu) = \deg(X^\mu)$) and similarly $\deg_t(\mu) = \sum_i \mu_i a_i$. Further, let $A = K[X_1, \dots, X_p]$ and let $\eta : A \to K[U, V]$ be the K-algebra homomorphism defined by $X_i \mapsto U^{p-i}V^{i-1}$, $i = 1, \dots, p$ and let $J := \operatorname{Ker} \eta$. Then J is a homogeneous prime ideal in A and the natural map $K[X_1, X_p] \longrightarrow A/J$ is injective.

Lemma 3.7. (1) *A homogeneous (in the standard grading) binomial $X^\mu - X^\nu$ (in A) belongs to J if and only if $\sum_{i=1}^p i\mu_i = \sum_{i=1}^p i\nu_i$. In particular, $X_i^{p-1} - X_1^{p-i} X_p^{i-1} \in J$ for every $i = 1, \dots, p$*

(2) *The ideal* J *is generated by* 2×2 *minors of the* $2 \times (p-1)$ *matrix*

$$\begin{pmatrix} X_1 & X_2 & \cdots & X_{p-1} \\ X_2 & X_3 & \cdots & X_p \end{pmatrix}. \tag{3.7.a}$$

Moreover, J *is generated minimally by the set* $\{\xi_{ij} \mid 2 \le i \le j \le p-1\}$, *where*

$$\xi_{ij} := \begin{cases} X_iX_j - X_1X_{i+j-1}, & \text{if} \quad i+j \le p, \\ X_iX_j - X_{i+j-p}X_p, & \text{if} \quad i+j > p. \end{cases}$$

(3) *Let* $x_2, \ldots, x_{p-1}$ *denote the images of* $X_2, \ldots, X_{p-1}$ *in* A/J. *Then* A/J *is a free* $K[X_1, X_p]$*-module with basis* $1, x_2, \ldots, x_{p-1}$.

(4) $JR \subseteq \mathfrak{p}$ *and* $A \cap \mathfrak{p} = J$. *In particular, the projective curve* $\mathcal{C}$ *is embedded in the projective surface* $\operatorname{Proj}(R/JR)$.

Proof. (1) is easy to check. For (2) note that the ξ_{ij} are sums of minors of the matrix, and the minors are in J. Therefore it is enough to prove that every binomial $X^\mu - X^\nu$ which belongs to J also belongs to the ideal generated by $\{\xi_{ij} \mid 1 \le i \le j \le p-1\}$. We work with the S-grading restricted to A. If $X^\mu - X^\nu \in J$ then, since $J \subseteq \mathfrak{p}$, X^μ and X^ν have the same S-degree $\boldsymbol{\alpha}$. Using the relations (3.2.a) we obtain either uniquely determined $c_1 \ge 0$, $c_p \ge 0$ such that $\boldsymbol{\alpha} = c_1\boldsymbol{\alpha}_1 + c_p\boldsymbol{\alpha}_p$ or uniquely determined $c_1 \ge 0$, $c_p \ge 0$ and i, $2 \le i \le p-1$ such that $\boldsymbol{\alpha} = c_1\boldsymbol{\alpha}_1 + \boldsymbol{\alpha}_i + c_p\boldsymbol{\alpha}_p$. In the first case we obtain that $X^\mu - X_1^{c_1}X_p^{c_p}$ and $X^\nu - X_1^{c_1}X_p^{c_p}$ belong to the ideal generated by $\{\xi_{ij} \mid 1 \le i \le j \le p-1\}$ and in the second case that $X^\mu - X_1^{c_1}X_iX_p^{c_p}$ and $X^\nu - X_1^{c_1}X_iX_p^{c_p}$ belong to the ideal generated by $\{\xi_{ij} \mid 1 \le i \le j \le p-1\}$. In both cases we obtain that $X^\mu - X^\nu$ also belongs to the the ideal generated by $\{\xi_{ij} \mid 1 \le i \le j \le p-1\}$, as required. The set $\{\xi_{ij} \mid 2 \le i \le j \le p-1\}$ generates J minimally because modulo the ideal generated by X_1 and X_p, the images of the ξ_{ij}, $2 \le i \le j \le p-1$ are K-linearly independent monomials in $X_2, \ldots, X_{p-1}$ of degree 2. We remark that it is well known that the minors of the matrix (3.7.a) generate J, for example see [6, (I) of § 2].

(3) The ring A/J is the homogeneous coordinate ring of the degree $p-1$ curve corresponding to $\mathscr{S} = \{1, 2, \ldots p-1\}$, which is an arithmetic progression. Therefore A/J is Cohen-Macaulay, hence a free module over $K[X_1, X_p]$.

(4) Note that if we identify $K[U, V]$ with the K-subalgebra $K[s^\delta, t^\delta]$ of $K[s, t]$ by putting $U = s^\delta$ and $V = t^\delta$, then for any homogeneous polynomial $F \in A$, we have $\varphi(F) = \eta(F) \cdot t^{a_1 \cdot \deg(F)}$. Now, since t is a non-zero divisor in $K[s, t]$, the assertions are immediate. □

Definition 3.8. Let $q \in \mathbb{N}$ and $r \in [1, p-1]$ be defined as in Lemma 3.3 by the equation $a_1 = q(p-1) + r$. We define $F_i := X_1^{q+\delta}X_i - W^\delta X_{r+i}X_p^q$, $i = 1, \ldots, p-r$.

It is straightforward to check, similarly to Lemma 3.3-(1), that $(q+\delta)\boldsymbol{\alpha}_1 + \boldsymbol{\alpha}_i = \delta\boldsymbol{\beta} + \boldsymbol{\alpha}_{r+i} + \boldsymbol{\alpha}_p$. Therefore $F_i \in \mathfrak{p}$ for every $i \in [1, p-r]$. Note that all F_i are

homogeneous of the same degree $q+\delta+1$, which is greater than or equal to 2 with equality if and only if $q=0$ and $\delta=1$.

Lemma 3.9. *For every $(p+1)$-tuple $\mu \in \mathbb{N}^{p+1}$, there exists a $(p+1)$-tuple $\tilde{\mu} \in \mathbb{N}^{p+1}$ with $|\mathrm{Supp}(\tilde{\mu}) \cap [2,p-1]| \leq 1$ and $\tilde{\mu}_i = 1$ if $i \in \mathrm{Supp}(\tilde{\mu}) \cap [2,p-1]$ such that $X^{\mu} - X^{\tilde{\mu}} \in JR$.*

Proof. Easily follows from Lemma 3.7-(3). □

Lemma 3.10. *Suppose that $\mathfrak{p}$ contains a binomial $X^{\mu} - X^{\nu}$ of degree 2. Then $X^{\mu} - X^{\nu} \in (J, F_1, \ldots, F_{p-r})$.*

Proof. If $0 \notin \mathrm{Supp}(\mu) \cup \mathrm{Supp}(\nu)$, then clearly $X^{\mu} - X^{\nu} \in J$ by Lemma 3.7-(4). We may therefore assume that $0 \in \mathrm{Supp}(\nu)$ and $0 \notin \mathrm{Supp}(\mu)$. We now have $X^{\nu} = WX_i$ and $X^{\mu} = X_jX_k$ for some $i,j,k \in [1,p]$ with $i \notin \{j,k\}$. Further, we have $a_i = \deg_t(\nu) = \deg_t(\mu) = a_j + a_k$ and so $(i-1)\delta = a_1 + (j+k-2)\delta$, i. e., $a_1 = (i+1-j-k)\delta$. Since $\gcd(a_1,\delta) = 1$, we must have $\delta = 1$ and hence $i = (j+k-1) + a_1$. Thus $p \geq i = (j+k-1) + a_1 \geq j+k$. Therefore $a_1 \leq p-1$ so $q = 0$ and $a_1 = r$ (remember that $q \in \mathbb{N}$ and $r \in [1,p]$ are defined by the equation $a_1 = q(p-1)+r$). Now, $p - r = p - a_1 \geq j+k-1$ and $F_{j+k-1} = X_1X_{j+k-1} - WX_i$. Therefore $X^{\mu} - X^{\nu} = F_{j+k-1} + (X_jX_k - X_1X_{j+k-1}) \in (J, F_1, \ldots, F_{p-r})$. □

Lemma 3.11. *Let $\mu, \nu \in \mathbb{N}^{p+1}$ be two $(p+1)$-tuples with the following properties*

(i) $\mathrm{Supp}(\mu) \cap \mathrm{Supp}(\nu) = \emptyset$.
(ii) $0 \in \mathrm{Supp}(\nu)$.
(iii) $|\mathrm{Supp}(\mu) \cap [2,p-1]| \leq 1$ *and* $\mu_i = 1$ *if* $i \in \mathrm{Supp}(\mu) \cap [2,p-1]$.
(iv) $|\mathrm{Supp}(\nu) \cap [2,p-1]| \leq 1$ *and* $\nu_i = 1$ *if* $i \in \mathrm{Supp}(\nu) \cap [2,p-1]$.
(v) $2 \leq \deg(\mu) = \deg(\nu)$ *and* $\deg_t(\mu) = \deg_t(\nu)$.

Then :

(1) $p \notin \mathrm{Supp}(\mu)$, $1 \in \mathrm{Supp}(\mu)$ *and* $1 \notin \mathrm{Supp}(\nu)$.
(2) $\sum_{k=1}^{p} \mu_k \mathbf{e}_k \notin \mathcal{B}_{\max}$ *and hence by* Theorem 3.4 *we have*

$$\mu_1 \geq \begin{cases} q+\delta+1, & \text{if } \mathrm{Supp}(\mu) = \{1\}, \\ q+\delta, & \text{if } \mathrm{Supp}(\mu) = \{1,i\} \text{ with } i \in [2,p-r], \\ q+\delta+1, & \text{if } \mathrm{Supp}(\mu) = \{1,i\} \text{ with } i \in [p-r+1,p-1]. \end{cases}$$

Proof. By assumptions (i) and (ii) $0 \notin \mathrm{Supp}(\mu)$. Further by assumptions (iii) and (iv) we have $\mathrm{Supp}(\mu) \subseteq \{1,i,p\}$ and $\{0\} \subseteq \mathrm{Supp}(\nu) \subseteq \{0,1,j,p\}$ with $i,j \in [2,p-1]$, $i \neq j$ and $\mu_i \leq 1$ and $\nu_j \leq 1$. Furthermore, by assumption (v) we have the following two equations :

$$\mu_1 + \mu_i + \mu_p = \deg(\mu) = \deg(\nu) = \nu_0 + \nu_1 + \nu_j + \nu_p \tag{3.11.a}$$

$$\mu_1a_1 + \mu_ia_i + \mu_pa_p = \deg_t(\mu) = \deg_t(\nu) = \nu_1a_1 + \nu_ja_j + \nu_pa_p \tag{3.11.b}$$

(1) Suppose on the contrary that $p \in \mathrm{Supp}(\mu)$, i. e. $\mu_p > 0$. Then by (i) $p \notin \mathrm{Supp}(\nu)$, i. e. $\nu_p = 0$. Substituting the expressions $a_i = a_1 + (i-1)\delta$ into equation (3.11.b), collecting the coefficients of a_1 and δ, and applying equation (3.11.a) we obtain the equation $\nu_0 a_1 + ((i-1)\mu_i + (p-1)\mu_p)\delta = (j-1)\nu_j\delta \leq (j-1)\delta$. We now have $(p-1)\delta < \nu_0 a_1 + ((i-1)\mu_i + (p-1)\mu_p)\delta = (j-1)\nu_j\delta \leq (j-1)\delta$ which is absurd, since $j < p$. Therefore $p \notin \mathrm{Supp}(\mu)$, i. e. $\mu_p = 0$. Now, since $\mu_1 + \mu_i = \deg(\mu) \geq 2$ and $\mu_i \leq 1$, $\mu_1 > 0$, i. e., $1 \in \mathrm{Supp}(\mu)$ and hence $1 \notin \mathrm{Supp}(\nu)$.

(2) By (v), we have $\sum_{k=1}^{p} \mu_k \boldsymbol{\alpha}_k = \nu_0 \boldsymbol{\beta} + \nu_j \boldsymbol{\alpha}_j + \nu_p \boldsymbol{\alpha}_p$. By (ii), $\nu_0 > 0$, hence $\sum_{k=1}^{p} \mu_k \mathbf{e}_k \notin \mathcal{B}_{\max}$. □

Theorem 3.12. *The ideal $\mathfrak{p}$ is generated by J and $F_1, \ldots, F_{p-r}$.*

Proof. Suppose not. Then there is a homogeneous pure binomial $F \in \mathfrak{p} \backslash \mathfrak{m}\mathfrak{p}$ which is not in the ideal generated by J and the F_i. Write $F = X^\mu - X^\nu$. Clearly $\deg(F) > 1$. If $\deg F = 2$ then $F \in (J, F_1, \ldots, F_{p-r})$ by Lemma 3.10. So we may assume that $\deg(F) \geq 3$. By Lemma 3.9 (and using that $\deg(F) \geq 3$) we may assume, after modifying F by an element of $\mathfrak{m}J$, that $|\mathrm{Supp}(\mu) \cap [2, p-1]| \leq 1$ and $\mu_i = 1$ if $i \in \mathrm{Supp}(\mu) \cap [2, p-1]$ and also that $|\mathrm{Supp}(\nu) \cap [2, p-1]| \leq 1$ and $\nu_j = 1$ if $j \in \mathrm{Supp}(\nu) \cap [2, p-1]$. Since $\mathfrak{p}$ is a prime ideal and F is a minimal generator, we have that $\mathrm{Supp}(\mu) \cap \mathrm{Supp}(\nu) = \emptyset$. Lemma 3.11 now applies, showing that we cannot have W as a factor of one of the monomials in F and X_p as a factor of the other. So suppose that X^μ contains neither W nor X_p as a factor. That is, $X^\mu = X_1^{\mu_1} X_i^{\mu_i}$ where $\mu_1 > 0$, $i \in [2, p-1]$ with $\mu_i \in \{0, 1\}$. We must now have X^ν of the form $W^{\nu_0} X_j^{\nu_j} X_p^{\nu_p}$ with $j \in [2, p-1], j \neq i, \nu_j \in \{0, 1\}$. On comparing the s-degrees of X^μ and X^ν we see that we must have $\nu_0 > 0$. Therefore $\mu_1\alpha_1 + \mu_i\alpha_i \notin \mathcal{B}$. By Lemma 3.11-(2) we must have one of the following cases, (i) $\mu_i = 0$ and $\mu_1 \geq q + \delta + 1$ (ii) $\mu_i = 1$, $i \in [2, p-r]$ and $\mu_1 \geq q + \delta$ or (iii) $\mu_1 = 1$, $i \in [p-r+1, p-1]$ and $\mu_1 \geq q + \delta + 1$. In case (i) or (iii) X^μ is a multiple of the first monomial $X_1^{q+\delta+1}$ in F_1. In case (ii) X^μ is a multiple of the first monomial $X_1^{q+\delta} X_i$ in F_i. Subtracting the corresponding multiple of F_i from F we obtain a non-zero binomial in $\mathfrak{p} \backslash \mathfrak{m}\mathfrak{p}$ with factor W, which is a contradiction. (Note that if the multiple is 1 we would have $F = F_i$ by Lemma 3.2-(5)). □

Remark 3.13. A minimal set of generators for J (e.g. $\xi_{ij}, 2 \leq i \leq j \leq p-1$ by Lemma 3.7-(2)) and $F_1, \ldots F_{p-r}$ form a minimal set of generators for $\mathfrak{p}$. To see this it suffices to observe that if we set $W = 0$ and apply η the images of the F_i are of the same degree and linearly independent over K. It follows that the minimal number of generators of $\mathfrak{p}$ is $\binom{p-1}{2} + p - r \leq \binom{p}{2}$.

Remark 3.14. As in Remark 2.16, the affine monomial curve $\mathcal{C}_0$ in the arithmetic progression case may have fewer generators than the projective curve $\mathcal{C}$. For example, consider $\mathscr{S} = \{1, 4, 7, 10\}$. By Theorem 3.12, $\mathfrak{p}$ is generated minimally by six elements $\xi_{22}, \xi_{23}, \xi_{33}, F_1, F_2$, and F_3, whereas $\mathfrak{p}_0$ is clearly generated by three elements $X_2 - X_1^4$, $X_3 - X_1^7$ and $X_4 - X_1^{10}$. If $\mathscr{S} = \{a_1, a_2, \cdots, a_p\}$ is an almost arithmetic progression (more general than arithmetic progression) then there is

some affine literature, for example, [15], [13], [17], [1], from which generators of $\mathfrak{p}_0$ may also be obtained, provided that $a_1, a_2, \ldots, a_p$ minimally generate Γ. Our Theorem 3.12 does not require that $a_1, a_2, \ldots, a_p$ generate Γ minimally. This is important in the projective case because extending the length of the arithmetic progression while leaving Γ the same always gives a different ring $K[S]$ and usually a different scheme $\mathrm{Proj}(K[S])$. Such an extension of the progression leaves the affine coordinate ring $K[\Gamma]$ the same but with a different embedding in affine space which will have different ideal generators which can be obtained from our projective results.

4. Set-theoretic Complete Intersection

In this section we shall prove that the projective monomial curve $\mathcal{C}$ in $\mathbb{P}^p$ defined parametrically by $W = X_0 = s^{a_p}, X_1 = s^{a_p - a_1}t^{a_1}, \ldots, X_p = t^{a_p}$ is a set-theoretic complete intersection if the positive integers $a_1, \ldots, a_p$ are in arithmetic progression. For $p \geq 4$, in general, it is unknown whether or not $\mathcal{C}$ is a set-theoretic complete intersection. More precisely, we prove the following :

Theorem 4.1. *There exists homogeneous polynomials $G_1, \ldots, G_{p-1} \in \mathfrak{p}$ such that $\mathfrak{p} = \sqrt{(G_1, \ldots, G_{p-1})}$.*

Proof. Follows from Lemma 4.3-(5) and Lemma 4.2-(2) below. □

Lemma 4.2. *With the same notation as in Notation* 3.6 *and Lemma* 3.7*, we have*

(1) *The ring R/JR is a free $K[X_1, X_p]$-module under the natural injection $K[X_1, X_p] \to A/J \to (A/J)[W] = R/JR$.*
(2) *There exists $p-2$ homogeneous polynomials $G_1, \ldots, G_{p-2} \in A$ such that $J = \sqrt{(G_1, \ldots, G_{p-2})}$.*

Proof. (1) The ring A/J is a free $K[X_1, X_p]$-module by Lemma 3.7-(3). Hence $R/J = (A/J)[W]$ is also a free $K[X_1, X_p]$-module.

(2) By Lemma 3.7-(2) the ideal J is generated by the two by two minors of the matrix in (3.7.a). The assertion now follows from [18, Corollary 1.2] because the matrix has the property that $a_{ij} = a_{kl}$ whenever $i + j = k + l$. □

Lemma 4.3. *With the same notation as in Notation* 3.6, Lemma 3.7 *and Definition* 3.8*, we have*

(1) $X_{p-i+1}F_i - X_pF_1 \in JR$ *for every* $i = 1, \ldots, p-r$.
(2) $\left(\prod_{i=r+2}^{p-1} X_i\right) \cdot \mathfrak{p} \subseteq (J, F_1, F_{p-r})$.
(3) *Let $\mathfrak{q}$ be a prime ideal in R with $(J, F_1, F_{p-r}) \subseteq \mathfrak{q}$ and $X_i \in \mathfrak{q}$ for some $2 \leq i \leq p-1$. Then $\mathfrak{p} \subseteq \mathfrak{q}$.*
(4) $\sqrt{(J, F_1, F_{p-r})} = \mathfrak{p}$.
(5) *There exists a polynomial $G \in \mathfrak{p}$ such that $\sqrt{(J, G)} = \mathfrak{p}$.*

Proof. (1) By the definition of the F_i we have $X_{p-i+1}F_i - X_pF_1 = X_1^{q+\delta}(X_{p-i+1}X_i - X_pX_1) - W^\delta X_p^q(X_{p-i+1}X_{r+i} - X_pX_{r+1}) \in JR$. (2) is immediate from (1).

(3) It follows from Lemma 3.7-(1) that $X_{i-1}^2 - X_iX_{i-2} \in J$ for $i \geq 3$ and $X_{i+1}^2 - X_iX_{i+2} \in J$ for $i \leq p-2$. Therefore, since $J \subseteq \mathfrak{q}$ and $\mathfrak{q}$ is a prime ideal, $X_{i-1} \in \mathfrak{q}$ for $i \geq 3$ and $X_{i+1} \in \mathfrak{q}$ for $i \leq p-2$. Continuing the above argument it follows that $X_2, \ldots, X_{p-1} \in \mathfrak{q}$ and hence $F_i = X_1^{q+\delta}X_i - W^\delta X_{r+i}X_p^q \in \mathfrak{q}$ for every $2 \leq i \leq p-r-1$. Therefore by Theorem 3.12 we have $\mathfrak{p} = (J, F_1, \ldots, F_{p-r}) \subseteq \mathfrak{q}$.

(4) If $r = p-1$, then $(J, F_1) = \mathfrak{p}$ and if $r = p-2$, then $(J, F_1, F_2) = \mathfrak{p}$. Therefore if $r \geq p-2$, then there is nothing to prove. We may therefore assume that $r \leq p-3$. It is enough to prove that $\mathfrak{p}$ is the only minimal prime ideal of (J, F_1, F_{p-r}). Let $\mathfrak{q}$ be a prime ideal in R with $(J, F_1, F_{p-r}) \subseteq \mathfrak{q}$. By (2) either $\mathfrak{p} \subseteq \mathfrak{q}$ or $X_i \in \mathfrak{q}$ for some $r+2 \leq i \leq p-1$ and hence $\mathfrak{p} \subseteq \mathfrak{q}$ by (3).

(5) For a polynomial $G \in R$, let g denote the image of G in R/JR. Further, let $x_1, \ldots, x_p$ denote the images of $X_1, \ldots, X_p$ in R/JR, respectively. Then, since $X_{r+1}F_{p-r} - X_pF_1 \in JR$ by (1), we have $x_{r+1}f_{p-r} = x_pf_1$. Moreover, by taking the $(p-1)$-th power on both sides and using $X_{r+1}^{p-1} - X_1^{p-r-1}X_p^r \in J$ (see Lemma 3.7-(1)), we get $x_1^{p-r-1}x_p^r f_{p-r}^{p-1} = x_p^{p-1}f_1^{p-1}$. Since R/JR is a free module over $K[X_1, X_p]$ by Lemma 4.2-(1), we can cancel x_p^r on both sides and get $x_1^{p-r-1}f_{p-r}^{p-1} = x_p^{p-r-1}f_1^{p-1}$. Now, since R/JR is a free module over a UFD $K[X_1, X_p]$ and $\gcd(X_1, X_p) = 1$, there exists $g \in R/JR$ such that $f_{p-r}^{p-1} = x_p^{p-r-1}g$ and $x_1^{p-r-1}g = f_1^{p-1}$. Let $G \in R$ be an arbitrary lift of g. Then $F_{p-r}^{p-1} - X_p^{p-r-1}G$ and $X_1^{p-r-1}G - F_1^{p-1} \in J \subseteq \mathfrak{p}$. Therefore $F_1, F_{p-r} \in \sqrt{(J,G)R}$ and $G \in \mathfrak{p}$, since $\mathfrak{p}$ is a prime ideal and $X_1, X_p \notin \mathfrak{p}$. This proves that $\sqrt{(J, F_1, F_{p-r})} \subseteq \sqrt{(J,G)R} \subseteq \mathfrak{p}$. But $\mathfrak{p} = \sqrt{(J, F_1, F_{p-r})}$ by (4) and hence $\sqrt{(J,G)R} = \mathfrak{p}$. □

Remark 4.4. As in the ideal generation case (Remarks 2.16 and 3.14) there is some affine literature on set-theoretic complete intersection curves (for example [12],[11]). If $\mathcal{C}$ is a set theoretic complete intersection it is easily seen that $\mathcal{C}_0$ is also. However we see no obvious reason for the converse to hold.

References

[1] I. Al-Ayyoub. Reduced Groebner Bases of Certain Toric Varieties: A New Short Proof. *Communications in Algebra*, 37(9):2945–2955, 2009.

[2] H. Bresinsky, F. Curtius, M. Fiorentini, and L.T. Hoa. On the structure of local cohomology modules for monomial curves in $\mathbb{P}_k^3$. *Nagoya Math. J.*, 136:81–114, 1994.

[3] H. Bresinsky and B. Renschuch. Basisbestimmung Veronesescher Projectionsideale mit allgemeiner Nullstelle $(t_0^m, t_0^{m-r}t_1^r, t_0^{m-s}t_1^s, t_1^m)$. *Math.Nachr.*, 96:257–269, 1980.

[4] A. Campillo and P. Giminez. Syzygies of affine toric varieties. *J.Alg*, 225:142–161, 2000.

[5] Daniel R. Grayson and Michael E. Stillman. Macaulay 2, a software system for research in algebraic geometry. Available at http://www.math.uiuc.edu/Macaulay2.

[6] W. Gröbner. Über Veronesesche varietäten und deren projektionen. *Arch. Math.*, XVI:257–264, 1965.

[7] J.Herzog. Generators and relations of abelian semigroups and semigroup rings. *Manuscripta Math*, 3:153–193, 1970.
[8] Ping Li. *Seminormality and the Cohen-Macaulay Property*. PhD thesis, Queen's University, 2005.
[9] E. Miller and B. Strumfels. *Computational Commutative Algebra*. Graduate Texts in Mathematics 227. Springer-Verlag, 2005.
[10] S. Molinelli and G. Tamone. On the Hilbert function of certain rings of monomial curves. *JPAA*, 101:191–206, 1995.
[11] D. P. Patil. Certain monomial curves are set-theoretic complete intersections. *Commutative Algebra (Trieste 1992)*, pages 195–203. World Sci. Publ., River Edge, NJ, 1994.
[12] D. P. Patil. Certain monomial curves are set-theoretic complete intersections. *Manuscripta Math.*, 68(4):399–404, 1990.
[13] D. P. Patil. Minimal sets of generators for the relation ideals of certain monomial curves. *Manuscripta Math.*, 80(3):239–248, 1993.
[14] D. P. Patil and L. G. Roberts. Hilbert functions of monomial curves. *Journal of Pure and Applied Algebra*, 183(1-3):275–292, 2003.
[15] D. P. Patil and Balwant Singh. Generators for the derivation modules and the relation ideals of certain curves. *Manuscripta Math.*, 90(3):327–335, 1990.
[16] Les Reid and Leslie G. Roberts. Non-Cohen-Macaulay projective monomial curves. *Journal of Algebra*, 291:171–186, 2005.
[17] I. Sengupta. A Gröbner basis for certain affine monomial curves. *Communications in Algebra*, 31(3):1113–1129, 2003.
[18] G. Valla. On determinantal ideals which are set-theoretic complete intersections. *Compositio Math.*, 42:3–11, 1981.
[19] R. Villarreal. *Monomial Algebras*. Marcel Dekker, 2001.

[2]Department of Mathematics, Indian Institute of Science, Bangalore 560 012, India.
[2]*E-mail address* : patil@math.iisc.ernet.in

[1,3]Department of Mathematics and Statistics, Queens University, Kingston K7L 3N6 , Ontario, Canada.
[1]*E-mail address* : pingli@mast.queensu.ca
[3]*E-mail address* : robertsl@mast.queensu.ca