Contemporary Mathematics



# Ideals of curves given by points

E. Fortuna, P. Gianni, and B. Trager

Abstract. Let $C$ be an irreducible projective curve of degree $d$ in $\mathbb{P}^n(\mathbb{K})$, where $\mathbb{K}$ is an algebraically closed field, and let $I$ be the associated homogeneous prime ideal. We wish to compute generators for $I$, assuming we are given sufficiently many points on the curve $C$. In particular if $I$ can be generated by polynomials of degree at most $m$ and we are given $md+1$ points on $C$, then we can find a set of generators for $I$. We will show that a minimal set of generators of $I$ can be constructed in polynomial time. Our constructions are completely independent of any notion of term ordering; this allows us the maximal freedom in performing our constructions in order to improve the numerical stability. We also summarize some classical results on bounds for the degrees of the generators of our ideal in terms of the degree and genus of the curve.

## 1. Introduction

Let $C$ be an irreducible projective curve of degree $d$ in $\mathbb{P}^n(\mathbb{K})$, where $\mathbb{K}$ is an algebraically closed field, and let $I = \mathcal{I}(C)$ be the associated homogeneous prime ideal of $\mathcal{P} = \mathbb{K}[x_0, \ldots, x_n]$ consisting of all the polynomials vanishing on $C$. We wish to compute generators for $I$, assuming we are given sufficiently many points on the curve $C$. In particular if $I$ can be generated by polynomials of degree at most $m$ and we are given at least $md+1$ points on $C$, then we can find a set of generators for $I$. It is a simple consequence of Bezout's theorem that any polynomial of degree $k$ which vanishes on more than $kd$ points of $C$ must be contained in $I$. Although the number of monomials in $n+1$ variables of degree at most $m$ is not polynomial in both $n$ and $m$, we will present a process which constructs generators degree by degree and results in a polynomial time algorithm for computing generators for $I$. Polynomial time algorithms for computing Gröbner bases of ideals of affine points were presented in [**MB**], and then extended to minimal generators of ideals of projective points in [**MMM**]. These algorithms require exact arithmetic, and assume a term ordering is given. We present new algorithms which are completely independent of any notion of term ordering. We believe that this flexibility is necessary when working with approximate coefficients.

2010 *Mathematics Subject Classification.* Primary 14H50, Secondary 13P10.
*Key words and phrases.* Algebraic curves, border bases, interpolation.
This research was partially supported by M.I.U.R. and by G.N.S.A.G.A..

Given a homogeneous ideal $I$, there are many different choices for monomials representing cosets of $\mathcal{P}/I$, i.e. for a complement of $I$. It is well known that the natural coset representatives associated with Gröbner bases do not remain stable with respect to small coefficient perturbations of the ideal generators. Border bases were introduced to help overcome this problem ([**KR**]). Given a fixed choice of complement for a zero-dimensional ideal, its border basis is uniquely determined in contrast with Gröbner bases where the complement is uniquely determined by the given term ordering. Border bases are usually defined for zero-dimensional ideals, which guarantees a finite basis. We extend the definition to homogeneous ideals of any dimension, but bound the degree in order to preserve finiteness. In much of the literature on border bases, the complements are required to be closed under division by variables. This makes complements of border bases more similar to complements of Gröbner bases which also have this property. In particular this is done in [**HKPP**], therefore their algorithms need to explicitly decide whether or not candidate leading monomials have coefficients which are so small that they should be treated as zero. As suggested by Mourrain and Trébuchet ([**MT**]), we only require the complement to be connected to 1. This means we require that each complement monomial of degree $i$ is a multiple of some complement monomial of degree $i-1$. This extra flexibility in the choice of complement monomials means that we can use standard numerical software like the QR algorithm with column pivoting (QRP) ([**GVL**]) to choose our complement in each degree. One could define a complement to be any set of representatives for $\mathcal{P}/I$, but with this definition we would not be able to obtain algorithms which are polynomial in both the degree of the curve and the number of variables. In particular, requiring the complement to be connected to 1 implies a strong condition on the syzygy module. We show that the syzygy module for a vector space basis of a homogeneous ideal whose complement is connected to 1 is generated by vectors whose entries have degree at most one, generalizing the result of Mourrain and Trébuchet for border bases of zero-dimensional ideals. These special generators of the syzygy module can be used to obtain a polynomial time algorithm for constructing minimal generators for our ideals. The algorithms developed by Cioffi [**C**] have a similar complexity in the case of exact coefficients but her use of Gröbner bases requires a term ordering which determines a unique complement which may be numerically unstable when working with approximate points.

The motivation for this paper came from the desire to be able to compute the generators of space curves starting from numerical software which generates points on curves, in particular computing points on canonical or bicanonical models for Riemann surfaces presented as Fuchsian groups ([**GSST**]). Our intended applications differ from that of [**HKPP**] and [**AFT**] since we assume that the points defining our curve are generated by a numerical algorithm whose errors tend to be very small as opposed to empirical measurements whose errors could be much larger. Thus our goal is to present algorithms based on numerically stable constructions like SVD for computing ideal generators and QRP for deciding which monomials represent the complement of our ideal.

In section 2 of this paper we derive some general properties of border bases and complements for general homogeneous ideals. Using these properties we present a polynomial time algorithm for finding a minimal basis for a homogeneous ideal.

In section 3 we specialize to ideals of curves given by points, and use point evaluation matrices to complete the task of computing border bases for homogeneous ideals of curves. Assuming exact arithmetic of unit cost, we also provide an overall complexity analysis of the border basis algorithm and the minimal basis algorithm. In section 4 we consider the situation of approximate points and show how our algorithms can be adapted to use standard numerical software, where we allow numerical algorithms like the QRP to choose the complement monomials in order to help improve the numerical stability. In general the stability also strongly depends on how the points are distributed, and we feel this is an interesting problem for future research, along with the possibility of using other approaches such as interval arithmetic.

In order to use Bezout's theorem, we assume we have at least a bound on the degree of our curve. In the last section we summarize some classical results on bounds for the degrees of generators of our ideal in terms of the degree and genus of the curve. In particular, as shown by Petri ([**P**]), a non-hyperelliptic canonical curve of genus $g \geq 4$ can be generated in degrees 2 and 3. We also recall the completely general result of Gruson-Lazarsfeld-Peskine ([**GLP**]) which shows that any non-degenerate curve of degree $d$ in $\mathbb{P}^n(\mathbb{K})$ can be generated in degree $d-n+2$.

Sometimes we have additional information about the nature of the curve whose points we are given. For instance, if we know the Hilbert function, the rank of our point evaluation matrices is explicitly given instead of being determined by examining its singular value spectrum.

## 2. Border bases for homogeneous ideals

Let $\mathbb{K}$ be an algebraically closed field. For any $s \in \mathbb{N}$, let $\mathcal{T}_s$ be the set of all terms of degree $s$ in $\mathcal{P} = \mathbb{K}[x_0, \ldots, x_n]$ and let $\mathcal{P}_s$ be the vector subspace of $\mathcal{P}$ generated by $\mathcal{T}_s$. Recall that $\dim \mathcal{P}_s = \binom{n+s}{s}$. We will also set $\mathcal{P}_{\leq s} = \oplus_{i=0}^{s} \mathcal{P}_i$.

Notation 2.1. We will use the following notation:

(1) For any subset $Y \subset \mathbb{P}^n(\mathbb{K})$ denote by $\mathcal{I}(Y)$ the radical homogeneous ideal of $\mathcal{P}$ consisting of all the polynomials vanishing on $Y$.
(2) For any homogeneous ideal $I$ in $\mathcal{P}$, let $I_s = I \cap \mathcal{P}_s$ (so that $I = \oplus_{s \geq 0} I_s$) and let $I_{\leq s} = I \cap \mathcal{P}_{\leq s}$.
(3) For any $S \subset \mathcal{P}$, denote by $I(S)$ the ideal generated by $S$.
(4) For any $S \subset \mathcal{P}_s$, denote by $\langle S \rangle$ the vector subspace of $\mathcal{P}_s$ generated by $S$.
(5) For any $S \subset \mathcal{P}_s$, let $S^+ = \bigcup_{j=0}^{n} (x_j\, S) \subset \mathcal{P}_{s+1}$.
(6) If $\mathbf{a} = (a_1, \ldots, a_h) \in \mathbb{K}^h$ and $\mathcal{F} = [F_1, \ldots, F_h]$ is a list of polynomials, we set
$$\mathbf{a} \cdot \mathcal{F} = a_1 F_1 + \ldots + a_h F_h.$$
(7) For any finite set $A$, we denote by $|A|$ its cardinality.

Definition 2.2. Let $J$ be a proper homogeneous ideal in $\mathcal{P}$ and $s \in \mathbb{N}$. Let $\mathcal{N}_0 = \{1\}$ and, for each $k = 1, \ldots, s$, assume that $\mathcal{N}_k$ is a set of monomials in $\mathcal{T}_k$ such that
$$\mathcal{N}_k \subset \mathcal{N}_{k-1}^{+} \quad \text{and} \quad \mathcal{P}_k = J_k \oplus \langle \mathcal{N}_k \rangle.$$
We call $\mathcal{N} = \{\mathcal{N}_0, \ldots, \mathcal{N}_s\}$ a *complement* of the ideal $J$ up to degree $s$.

Remark 2.3. Let $\mathcal{N} = \{\mathcal{N}_0, \ldots, \mathcal{N}_s\}$ be a complement of a proper homogeneous ideal $J$ up to degree $s$. Then:

(1) the condition $\mathcal{N}_k \subset \mathcal{N}_{k-1}^+$ implies that $\mathcal{N}$ is connected to 1, i.e. for each $m \in \mathcal{N}$ there exist variables $x_{i_1}, \ldots, x_{i_k}$ such that $m = x_{i_1} \cdot \ldots \cdot x_{i_k}$ and $x_{i_1} \cdot \ldots \cdot x_{i_j} \in \mathcal{N}$ for each $j < k$,
(2) from the definition it follows that, for $k = 1, \ldots, s$,

$$\langle \mathcal{N}_{k-1}^+ \rangle = (J_k \cap \langle \mathcal{N}_{k-1}^+ \rangle) \oplus \langle \mathcal{N}_k \rangle.$$

□

LEMMA 2.4. *Let $J$ be a proper homogeneous ideal of $\mathcal{P}$. Assume that $\mathcal{N}_{k-1} \subseteq \mathcal{T}_{k-1}$ and $\mathcal{N}_k \subseteq \mathcal{T}_k$ are sets of monomials such that*

(a) $\mathcal{P}_{k-1} = J_{k-1} \oplus \langle \mathcal{N}_{k-1} \rangle$
(b) $\langle \mathcal{N}_{k-1}^+ \rangle = (J_k \cap \langle \mathcal{N}_{k-1}^+ \rangle) \oplus \langle \mathcal{N}_k \rangle$.

*Then*

(1) $J_k = \langle J_{k-1}^+ \rangle + (J_k \cap \langle \mathcal{N}_{k-1}^+ \rangle)$
(2) $\mathcal{P}_k = J_k \oplus \langle \mathcal{N}_k \rangle$.

PROOF. By hypothesis (a), we have

$$\mathcal{P}_k = \langle \mathcal{P}_{k-1}^+ \rangle = \langle J_{k-1}^+ \rangle + \langle \mathcal{N}_{k-1}^+ \rangle$$

and, since $J_k \supseteq \langle J_{k-1}^+ \rangle$, we have also

$$J_k = \mathcal{P}_k \cap J_k = \langle J_{k-1}^+ \rangle + (J_k \cap \langle \mathcal{N}_{k-1}^+ \rangle),$$

which proves (1). Hence, by the previous relations and hypothesis (b), we have

$$\mathcal{P}_k = \langle J_{k-1}^+ \rangle + \langle \mathcal{N}_{k-1}^+ \rangle = \langle J_{k-1}^+ \rangle + (J_k \cap \langle \mathcal{N}_{k-1}^+ \rangle) + \langle \mathcal{N}_k \rangle = J_k + \langle \mathcal{N}_k \rangle.$$

On the other hand, again by hypothesis (b) we have that $\langle \mathcal{N}_k \rangle \subseteq \langle \mathcal{N}_{k-1}^+ \rangle$ and hence

$$J_k \cap \langle \mathcal{N}_k \rangle \subseteq J_k \cap \langle \mathcal{N}_{k-1}^+ \rangle \cap \langle \mathcal{N}_k \rangle = \{0\},$$

which completes the proof of (2). □

REMARK 2.5. It is always possible to choose a complement up to any fixed degree for any proper homogeneous ideal $J$ of $\mathcal{P}$ incrementally. Namely, if $\mathcal{N} = \{\mathcal{N}_0, \ldots, \mathcal{N}_{k-1}\}$ is a complement of $J$ up to degree $k-1$, it is sufficient to choose a set $\mathcal{N}_k \subseteq \mathcal{T}_k$ such that $\langle \mathcal{N}_{k-1}^+ \rangle = (J_k \cap \langle \mathcal{N}_{k-1}^+ \rangle) \oplus \langle \mathcal{N}_k \rangle$: then Lemma 2.4 assures that $\mathcal{P}_k = J_k \oplus \langle \mathcal{N}_k \rangle$ and hence that $\mathcal{N} = \{\mathcal{N}_0, \ldots, \mathcal{N}_k\}$ is a complement of the ideal $J$ up to degree $k$.

Moreover, again by Lemma 2.4, once one has a complement $\mathcal{N}$ of $J$ up to any fixed degree $s$, one can get a set of generators of the ideal $I(J_1, \ldots, J_s)$ as the union of sets of generators of $J_k \cap \langle \mathcal{N}_{k-1}^+ \rangle$ for $k = 1, \ldots, s$.

DEFINITION 2.6. Let $J$ be a proper homogeneous ideal in $\mathcal{P}$ and assume that $\mathcal{N} = \{\mathcal{N}_0, \ldots, \mathcal{N}_s\}$ is a complement of $J$ up to degree $s$.

(1) For all $k = 1, \ldots, s$ let $(\partial\mathcal{N})_k = \mathcal{N}_{k-1}^+ \setminus \mathcal{N}_k$; the elements in $(\partial\mathcal{N})_k$ will be called *border monomials* in degree $k$.
(2) For each $m \in (\partial\mathcal{N})_k$ let $\psi(m)$ be the unique polynomial in $\langle \mathcal{N}_k \rangle$ such that $m + \psi(m) \in J_k$; we will call the homogeneous polynomial $m + \psi(m)$ the *border polynomial associated to $m$*.
(3) If $\mathcal{B}_k$ denotes the set of all border polynomials of degree $k$, the set $\mathcal{B} = \mathcal{B}_1 \cup \ldots \cup \mathcal{B}_s$ is called the *border basis of $J$ up to degree $s$ associated to $\mathcal{N}$*.

REMARK 2.7. This notion of bounded degree border basis applies to arbitrary homogeneous ideals and coincides with the classical notion of border basis ([**KR**]) in the case of homogeneous zero-dimensional ideals, provided we choose $s$ to be larger than the maximal degree of any monomial in the (finite) complement $\mathcal{N}$ of $J$. □

PROPOSITION 2.8. Assume that $\mathcal{N}$ is a complement of a proper homogeneous ideal $J$ up to degree $s$ and let $\mathcal{B} = \mathcal{B}_1 \cup \ldots \cup \mathcal{B}_s$ be the associated border basis. Then

(1) $\mathcal{B}_k$ is a basis of the vector space $J_k \cap \langle \mathcal{N}_{k-1}^+ \rangle$ for each $k = 1, \ldots, s$,
(2) $\mathcal{B}$ is a set of generators of the ideal $I(J_1, \ldots, J_s)$.

PROOF. (1) Let $b \in J_k \cap \langle \mathcal{N}_{k-1}^+ \rangle$. Since $\mathcal{N}_{k-1}^+ = (\partial\mathcal{N})_k \cup \mathcal{N}_k$, there exist $a_i, b_i \in \mathbb{K}$ such that

$$b = \sum_{m_i \in (\partial\mathcal{N})_k} a_i m_i + \sum_{m_i \in \mathcal{N}_k} b_i m_i.$$

For each $m_i \in (\partial\mathcal{N})_k$ let $\psi(m_i)$ be the unique polynomial in $\langle \mathcal{N}_k \rangle$ such that $m_i + \psi(m_i) \in J_k$. Then we can write $b = u + v$ with

$$u = \sum_{m_i \in (\partial\mathcal{N})_k} a_i(m_i + \psi(m_i)), \qquad v = \sum_{m_i \in \mathcal{N}_k} b_i m_i - \sum_{m_i \in (\partial\mathcal{N})_k} a_i \psi(m_i).$$

Note that $u \in J_k \cap \langle \mathcal{B}_k \rangle$ and $v \in \langle \mathcal{N}_k \rangle$. Since $b \in J_k$, then we have that $v = b - u \in J_k \cap \langle \mathcal{N}_k \rangle = \{0\}$. Thus $b = u$ and hence $b \in \langle \mathcal{B}_k \rangle$.

(2) follows immediately from (1) and Remark 2.5. □

We now suggest a simple method to construct recursively both a complement and a border basis of a homogeneous ideal $J$ up to any fixed degree. Even if the ideal may not have an explicit representation, if we assume the capability of computing a basis of its intersection with a vector subspace generated by a finite set $N$ of monomials of the same degree, we will be able to compute a border basis for $J$ up to any fixed degree. We will denote this condition by saying that the ideal is *represented* by the function $ComputeBasis_J$, which, for any such $N$, returns a basis for the intersection $J \cap \langle N \rangle$. In the next section we will see that such a function can be easily computed for ideals of points.

In the description of the algorithms we will use the following notations:

a. If $v$ is a polynomial and $S = \{n_1, \ldots, n_t\}$ is a set of monomials, then coeffs$(v, S)$ will denote the vector $(a_1, \ldots, a_t)$ of the coefficients of the monomials of $S$ in $v$.
b. Given a matrix $A$, we will denote $RRE(A) = (E, \Sigma)$ where
   - $E$ is the completely reduced row echelon form of $A$ (i.e. each pivot is equal to 1, and in each of the columns containing a pivot all the elements different from the pivot are zero)
   - $\Sigma$ is the set consisting of the indexes of the columns containing the pivots of $E$ .

Algorithm BorderBasisWithComplement

Input:

- a function $ComputeBasis_J$ representing a homogeneous ideal $J$
- $s \in \mathbb{N}$

Output:

- $\{\mathcal{N}_0, \ldots, \mathcal{N}_s\}$ a complement of $J$ up to degree $s$
- $\{\mathcal{B}_1, \ldots, \mathcal{B}_s\}$ the associated border basis.

Procedure:

- $\mathcal{N}_0 = \{1\}$
- for $k = 1..s$ repeat
  — construct the set of distinct monomials $\mathcal{N}_{k-1}^+ = \{m_1, \ldots, m_t\}$
  $\mathcal{N}_{k-1}^+ := \{x_i m \mid 1 \leq i \leq n, m \in \mathcal{N}_{k-1}\}$
  $\mathcal{V}_k := ComputeBasis_J(\mathcal{N}_{k-1}^+)$
  $q := |\mathcal{V}_k|$
  $t := |\mathcal{N}_{k-1}^+|$
  — compute the $q \times t$ matrix with rows coeffs$(v, \mathcal{N}_{k-1}^+)$ for $v \in \mathcal{V}_k$
  $A := matrix(\text{coeffs}(v, \mathcal{N}_{k-1}^+) \mid v \in \mathcal{V}_k)$
  $(E, \Sigma) := RRE(A)$
  — the monomial with index not in $\Sigma$ are put in $\mathcal{N}_k$
  $\mathcal{N}_k := \{m_j \mid j \notin \Sigma\}$
  — every row represents an element of $\mathcal{B}_k$
  $\mathcal{B}_k := \{\sum_j e_{i,j} m_j \mid i = 1, \ldots, q\}$

PROPOSITION 2.9. Given a proper homogeneous ideal $J$ in $\mathcal{P}$ represented by a function $ComputeBasis_J$ and $s \in \mathbb{N}$, the algorithm BorderBasisWithComplement constructs a complement and a border basis for $J$ up to degree $s$.

PROOF. At each step, the rows of $E$ correspond to polynomials of the form $m + \psi(m)$, with $m \notin \mathcal{N}_k$ and $\psi(m) \in \mathcal{N}_k$, which are a basis of $J_k \cap \langle \mathcal{N}_{k-1}^+ \rangle$. Moreover , since the monomials in $\mathcal{N}_k$ correspond to the non-pivot positions, by construction we have that $\langle \mathcal{N}_{k-1}^+ \rangle = (J_k \cap \langle \mathcal{N}_{k-1}^+ \rangle) \oplus \langle \mathcal{N}_k \rangle$.

Then by Lemma 2.4 we get that $\mathcal{P}_k = J_k \oplus \langle \mathcal{N}_k \rangle$; hence $\{\mathcal{N}_0, \ldots, \mathcal{N}_k\}$ is a complement of $J$ up to degree $k$ and $\mathcal{B}_1 \cup \ldots \cup \mathcal{B}_k$ is the associated border basis up to degree $k$. □

By Proposition 2.8 a border basis $\mathcal{B}$ of $J$ up to degree $s$ is a set of generators of the ideal $I(J_1, \ldots, J_s)$, but in general it is not minimal. We will see how one can eliminate redundant polynomials in $\mathcal{B}$ so as to obtain a minimal set of generators of that ideal.

PROPOSITION 2.10. Let $J$ be a proper homogeneous ideal in $\mathcal{P}$. Assume that $\mathcal{N} = \{\mathcal{N}_0, \ldots, \mathcal{N}_s\}$ is a complement of $J$ up to degree $s$ and let $\mathcal{B} = \mathcal{B}_1 \cup \ldots \cup \mathcal{B}_s$ be the associated border basis. Then:

(1) The ideal $L = I(\mathcal{B}, \mathcal{N}_s^+)$ is homogeneous and zero-dimensional, and $\mathcal{B} \cup \mathcal{N}_s^+$ is the border basis of $L$ associated to its complement $\mathcal{N}$.
(2) The module $Syz(\mathcal{B}, \mathcal{N}_s^+)$ is generated by vectors whose entries have degree at most 1.

PROOF. (1) Since $L_s = J_s$, we have that $\mathcal{P}_s = L_s \oplus \langle \mathcal{N}_s \rangle$. Moreover, since $\mathcal{N}_s^+ \subseteq L$, choosing $\mathcal{N}_{s+1} = \emptyset$ we see that the triple $L, \mathcal{N}_s, \mathcal{N}_{s+1}$ satisfies the hypotheses of Lemma 2.4 (we set $\langle \emptyset \rangle = \{0\}$). Thus we get that $\mathcal{P}_{s+1} = L_{s+1}$; so the ideal $L$ is zero-dimensional. If we set $\mathcal{N}_j = \emptyset$ for all $j \geq s+1$, then $\widetilde{\mathcal{N}} = \{\mathcal{N}_j\}_{j \in \mathbb{N}}$ is a complement of $L$. Moreover, since $(\partial \mathcal{N})_{s+1} = \mathcal{N}_s^+$, if we let $\mathcal{B}_{s+1} = \mathcal{N}_s^+$, then $\mathcal{B} \cup \mathcal{N}_s^+$ is a border basis of $L$.

(2) Since $\mathcal{N}_{k+1} \subseteq \mathcal{N}_k^+$ for each $k$ and $\mathcal{N}_0 = \{1\}$, we have that $\mathcal{N}$ is connected to 1 (see Remark 2.3). Thus it is possible to apply Theorem 4.3 in [**MT**], which implies that the syzygies among the elements of a border basis of a zero-dimensional ideal with a complement connected to 1 can be generated by syzygies whose coefficients have degree at most 1. □

By changing bases in each constant degree subspace we obtain the following more general result:

PROPOSITION 2.11. Let $J$ be a proper homogeneous ideal in $\mathcal{P}$. Assume that $\mathcal{N} = \{\mathcal{N}_0, \ldots, \mathcal{N}_s\}$ is a complement of $J$ up to degree $s$. Let $\mathcal{V} = \mathcal{V}_1 \cup \ldots \cup \mathcal{V}_s$ where $\mathcal{V}_k$ is a basis of $J_k \cap \langle \mathcal{N}_{k-1}^+ \rangle$ for each $k = 1, \ldots, s$. Then the module $Syz(\mathcal{V}, \mathcal{N}_s^+)$ is generated by vectors whose entries have degree at most 1.

The following corollary shows that the redundant elements in $\mathcal{V}_s$ can be expressed as a combination of elements in $\mathcal{V}_{s-1}$ and the other elements in $\mathcal{V}_s$:

COROLLARY 2.12. Under the hypotheses of Proposition 2.11, let $f \in \mathcal{V}_s$ and denote $\mathcal{W}_s = \mathcal{V}_s \setminus \{f\}$. If $f \in I(\mathcal{V}_1, \ldots, \mathcal{V}_{s-1}, \mathcal{W}_s)$, then $f \in \langle \mathcal{V}_{s-1}^+, \mathcal{W}_s \rangle$.

PROOF. By hypothesis there exists a syzygy among the elements of $\mathcal{V} = \mathcal{V}_1 \cup \ldots \cup \mathcal{V}_s$ such that the coefficient of $f$ is a non-zero constant. Hence by Proposition 2.11, there exists a homogeneous generator of $Syz(\mathcal{V}, \mathcal{N}_s^+)$ whose entries have degree at most 1 and where the coefficient of $f$ is a non-zero constant. Since $\deg f = k$ and the coefficient of $f$ is constant, in this generating syzygy only the elements of $\mathcal{V}_{k-1} \cup \mathcal{V}_k$ can have non-zero coefficients. □

We now describe two methods to construct a minimal set of generators of the ideal $I(J_1, \ldots, J_s)$ depending on whether we start with a set of generators which form a border basis or not.

PROPOSITION 2.13. Let $s \in \mathbb{N}$ and let $\mathcal{N} = \{\mathcal{N}_0, \ldots, \mathcal{N}_s\}$ be a complement up to degree $s$ of a proper homogeneous ideal $J$ in $\mathcal{P}$. Given $\{\mathcal{V}_1, \ldots, \mathcal{V}_s\}$ where $\mathcal{V}_k$ is a basis of $J \cap \langle \mathcal{N}_{k-1}^+ \rangle$, then for each $k = 1, \ldots, s$ it is possible to construct a set of polynomials $\mathcal{G}_k \subseteq \mathcal{V}_k$ such that $\mathcal{G}_1 \cup \ldots \cup \mathcal{G}_s$ is a minimal set of generators of the ideal $I(J_1, \ldots, J_s)$.

PROOF. Let $\mathcal{G}_1 = \mathcal{V}_1$ and assume that $\mathcal{G}_1 \cup \ldots \cup \mathcal{G}_{k-1}$ is a minimal set of generators of $I(J_1, \ldots, J_{k-1})$ with $\mathcal{G}_i \subseteq \mathcal{V}_i$ for $i = 1, \ldots, k-1$.

Note that a polynomial $f \in \mathcal{V}_k$ is redundant w.r.t. $\mathcal{G}_1 \cup \ldots \cup \mathcal{G}_{k-1} \cup \mathcal{V}_k$ if and only if it is redundant w.r.t. $\mathcal{V}_1 \cup \ldots \cup \mathcal{V}_k$. Thus, by Corollary 2.12 it suffices to look for linear relations among the elements of $\mathcal{V}_{k-1}^+ \cup \mathcal{V}_k$ and for a set $\mathcal{G}_k \subseteq \mathcal{V}_k$ such that $\langle \mathcal{V}_{k-1}^+ \rangle + \langle \mathcal{V}_k \rangle = \langle \mathcal{V}_{k-1}^+ \rangle \oplus \langle \mathcal{G}_k \rangle$. Hence it is sufficient to find a basis of $\langle \mathcal{V}_{k-1}^+ \rangle \cap \langle \mathcal{V}_k \rangle$, extend it with elements $w_1, \ldots, w_t$ to a basis of $\langle \mathcal{V}_k \rangle$ and define $\mathcal{G}_k = \{w_1, \ldots, w_t\}$.

In order to compute the intersection $\langle \mathcal{V}_{k-1}^+ \rangle \cap \langle \mathcal{V}_k \rangle$ consider the monomial basis $S = S_1 \cup S_2 \cup S_3$ of $\langle \mathcal{V}_{k-1}^+ \rangle + \langle \mathcal{V}_k \rangle$, where $S_1 = (\partial \mathcal{N})_{k-1}^+ \setminus \mathcal{N}_{k-1}^+$, $S_2 = (\partial \mathcal{N})_k$ and $S_3 = \mathcal{N}_k$. Observe that $\mathcal{N}_{k-1}^+ = (\partial \mathcal{N})_k \cup \mathcal{N}_k$ and $\mathcal{V}_{k-1}^+ \subset \langle (\partial \mathcal{N})_{k-1}^+ \rangle + \langle \mathcal{N}_{k-1}^+ \rangle$. Let $s_i = |S_i|$, for $i = 1, 2, 3$, and $l = |\mathcal{V}_{k-1}^+|$; with this notation $|\mathcal{V}_k| = |(\partial \mathcal{N})_k| = s_2$.

Let $U$ be the matrix whose columns contain the coefficients of the polynomials of $\mathcal{V}_{k-1}^+ \cup \mathcal{V}_k$ with respect to $S$. Thus $U$ is a $(s_1 + s_2 + s_3) \times (l + s_2)$ block matrix

of the form

$$U = \left(\begin{array}{c|c} U_1 & 0 \\ \hline U_2 & U_3 \\ \hline U_4 & U_5 \end{array}\right)$$

and, if we denote by $\pi_2 : \mathbb{K}^l \times \mathbb{K}^{s_2} \to \mathbb{K}^{s_2}$ the projection on the last $s_2$ coordinates, the vectors of $\pi_2(\operatorname{Ker} U)$ are the coordinates (w.r.t. $\mathcal{V}_k$) of the vectors of $\langle \mathcal{V}_{k-1}^+ \rangle \cap \langle \mathcal{V}_k \rangle$.

In order to compute $\operatorname{Ker} U$ we can reduce ourselves to consider the matrix

$$\widetilde{U} = \left(\begin{array}{c|c} U_1 & 0 \\ \hline U_2 & U_3 \end{array}\right).$$

Namely, since $S_3 = \mathcal{N}_k$, if $\widetilde{U}v = 0$, then $Uv \in J_k \cap \langle \mathcal{N}_k \rangle = \{0\}$, hence $\operatorname{Ker} U = \operatorname{Ker} \widetilde{U}$.

In order to finish the construction it is then sufficient to reduce to echelon form the matrix whose rows are generators of $\pi_2(\operatorname{Ker} \widetilde{U})$: the indexes of the columns without pivots correspond to the elements in $\mathcal{V}_k$ to select for constructing $\mathcal{G}_k$. □

The proof of the previous proposition guarantees the correctness of the following:

Algorithm MinimalBasis

Input:

- $s \in \mathbb{N}$
- $\{\mathcal{N}_0, \ldots, \mathcal{N}_s\}$ a complement of a homogeneous ideal $J$ up to degree $s$
- $\{\mathcal{V}_1, \ldots, \mathcal{V}_s\}$ where $\mathcal{V}_k$ is a basis for $J \cap \langle \mathcal{N}_{k-1}^+ \rangle$

Output: $\{\mathcal{G}_1, \ldots, \mathcal{G}_s\}$ where:

— $\mathcal{G}_k \subset \mathcal{V}_k$ for each $k \in \{1, \ldots, s\}$
— the polynomials in $\mathcal{G}_1 \cup \ldots \cup \mathcal{G}_s$ are a minimal set of generators of the ideal $I(J_1, .., J_s)$

Procedure:

- $\mathcal{G}_1 = \mathcal{V}_1$
- for $k = 2..s$ repeat
  $S_1 := (\partial \mathcal{N})_{k-1}^+ \setminus \mathcal{N}_{k-1}^+$
  $S_2 := (\partial \mathcal{N})_k$
  $l := |\mathcal{V}_{k-1}^+|$
  $s_1 := |S_1|$
  $s_2 := |S_2|$
  — construct the $(s_1 + s_2) \times (l + s_2)$ matrix with columns the $s_1 + s_2$
  — coefficients w.r.t. $S_1 \cup S_2$ of the polynomials $v \in \mathcal{V}_{k-1}^+ \cup \mathcal{V}_k$.
  $\widetilde{U} :=$ matrix $(\text{coeffs}(v, S_1 \cup S_2) \mid v \in \mathcal{V}_{k-1}^+ \cup \mathcal{V}_k)$
  — compute the intersection $\langle V_{k-1}^+ \rangle \cap \langle \mathcal{V}_k \rangle$
  $K := \operatorname{Ker}(\widetilde{U})$
  $dk := |K|$
  — construct the $dk \times s_2$ matrix with rows the last $s_2$ entries of the
  — vectors in $K$.
  $MK := matrix(\pi_2(v) \mid v \in K)$
  $(RMK, \Sigma) := RRE(MK)$
  — the polynomials in $\mathcal{V}_k$ with index not in $\Sigma$ are put in $\mathcal{G}_k$

$$\mathcal{G}_k := \{v_j \in \mathcal{V}_k \mid j \notin \Sigma\}$$

In the case when we start with a border basis, we can improve our previous construction. The computation of the generators of the intersection $\langle V_{k-1}^+ \rangle \cap \langle \mathcal{V}_k \rangle$ can then be accomplished with only some column subtractions, and the construction of each level of the minimal basis can be completed with one column echelon reduction of an $s_2 \times (l - s_1)$ matrix. The new algorithm is based on the following Proposition whose proof is an immediate consequence of the properties of a border basis.

PROPOSITION 2.14. Let $s \in \mathbb{N}$ and let $J$ be a proper homogeneous ideal in $\mathcal{P}$. Assume that $\mathcal{N} = \{\mathcal{N}_0, \ldots, \mathcal{N}_s\}$ is a complement of $J$ up to degree $s$ and let $\mathcal{B} = \mathcal{B}_1 \cup \ldots \cup \mathcal{B}_s$ be the associated border basis. With the notation of the previous proof, if $\widetilde{U} = \left(\begin{array}{c|c} U_1 & 0 \\ \hline U_2 & U_3 \end{array}\right)$ we have:

(i) after reordering the elements of $\mathcal{B}_k$ we can assume that the $s_2 \times s_2$ block $U_3$ is the identity matrix $I_{s_2}$
(ii) each element in $U_1$ is either 0 or 1; more precisely each row in $U_1$ contains at least one element equal to 1 and each column in $U_1$ contains at most one element equal to 1
(iii) by means of finitely many subtractions performed on the left $l$ columns of $\widetilde{U}$ we can reduce $\widetilde{U}$ to the form
$$\widehat{U} = \left(\begin{array}{c|c|c} I_{s_1} & 0 & 0 \\ \hline P_1 & P_2 & I_{s_2} \end{array}\right)$$
(iv) the set of the columns of the $s_2 \times (l - s_1)$ matrix $P_2$ is a basis of $\pi_2(\operatorname{Ker} \widetilde{U}) = \pi_2(\operatorname{Ker} \widehat{U})$
(v) $\widehat{U}$ has full row-rank and so $\dim \operatorname{Ker} \widetilde{U} = \dim \operatorname{Ker} \widehat{U} = l - s_1$
(vi) reducing $P_2$ to echelon form by column operations, the pivots indicate the redundant elements in $\mathcal{B}_k$.

## 3. Curves given by points

A natural application of the results of the previous section is the construction of the ideal of an irreducible projective curve starting from the knowledge of a finite set of points on it. Let us recall the following classic result:

PROPOSITION 3.1. Assume that $C$ is an irreducible projective curve in $\mathbb{P}^n(\mathbb{K})$ of degree $d$. Let $\mathcal{R} = \{R_1, \ldots, R_h\}$ be a set of points on $C$.

(1) For all $s \in \mathbb{N}$ such that $h > sd$, we have $\mathcal{I}(C)_{\leq s} = \mathcal{I}(\mathcal{R})_{\leq s}$.
(2) If $\mathcal{I}(C)$ can be generated by polynomials of degree at most $m$ and $h > md$, then $\mathcal{I}(C) = \mathcal{P} \cdot \mathcal{I}(\mathcal{R})_{\leq m}$

PROOF. (1) It suffices to prove that $\mathcal{I}(\mathcal{R})_k \subseteq \mathcal{I}(C)_k$ for all $k \leq s$. If $f \in \mathcal{I}(\mathcal{R})_k$, the polynomial $f$ vanishes on $h > sd \geq kd = \deg f \cdot \deg C$ points. Since $C$ is irreducible, by Bézout's Theorem the hypersurface $V(f)$ contains $C$, i.e. $f \in \mathcal{I}(C)_k$.

(2) By hypothesis $\mathcal{I}(C) = \mathcal{P} \cdot \mathcal{I}(C)_{\leq m}$, thus the result follows immediately from (1). □

The previous result allows us to reduce the construction of $\mathcal{I}(C)$ to the computation of a set of generators for the ideal $J = \mathcal{I}(\mathcal{R})$ where $\mathcal{R} = \{R_1, \ldots, R_h\}$ is a set

of $h$ points in $\mathbb{P}^n(\mathbb{K})$. By Proposition 2.8 this can be done by computing a border basis of $J$. In the case of an ideal of points, we are able to compute $J_k \cap \langle \mathcal{N}_{k-1}^+ \rangle$ using the point evaluation maps.

Assume that we have computed $\mathcal{N}_{k-1}$ and let $\mathcal{N}_{k-1}^+ = \{m_1, \ldots, m_t\} \subseteq \mathcal{P}_k$. Consider the $h \times t$ evaluation matrix

$$M_{\mathcal{R}} = \begin{pmatrix} m_1(R_1) & \ldots & m_t(R_1) \\ \vdots & & \vdots \\ m_1(R_h) & \ldots & m_t(R_h) \end{pmatrix}$$

where, if $R_i = [r_{i,0}, \ldots, r_{i,n}]$, by $m_j(R_i)$ we mean $m_j(r_{i,0}, \ldots, r_{i,n})$. Note that the rank of the matrix $M_{\mathcal{R}}$ and its null-space $\operatorname{Ker} M_{\mathcal{R}}$ does not depend on the chosen representation of the points in the projective space. Note also that each vector in $\operatorname{Ker} M_{\mathcal{R}}$ is the vector of the coordinates of a polynomial in $J_k \cap \langle \mathcal{N}_{k-1}^+ \rangle$ w.r.t. the basis $\{m_1, \ldots, m_t\}$. In particular $\dim \operatorname{Ker} M_{\mathcal{R}} = \dim(J_k \cap \langle \mathcal{N}_{k-1}^+ \rangle)$.

Performing Gaussian elimination by rows, followed if necessary by a permutation of the columns (which corresponds to a permutation of the basis $\{m_1, \ldots, m_t\}$), we can assume that $\mathcal{M}_{\mathcal{R}} = \left(\begin{array}{c|c} I_r & A \\ \hline 0 & 0 \end{array}\right)$. In this way the columns of $\left(\begin{array}{c} -A \\ \hline I_{t-r} \end{array}\right)$ are a basis of the null-space $\operatorname{Ker} M_{\mathcal{R}}$. If we choose as $\mathcal{N}_k$ the first $r$ monomials in the permuted basis, we have the null-space in border form, which gives us $\mathcal{B}_k$.

We now want to estimate the complexity of our procedure to compute a minimal set of generators up to degree $s$ of the ideal $J$ of $h$ distinct points.

Our algorithm first computes a border basis up to degree $s$, then minimizes this basis removing redundant elements. The basic tool is Gaussian elimination; recall that the complexity of Gaussian elimination performed on a $m \times p$ matrix is $O(mp \min(m, p))$.

As for the first phase to compute the border basis, the $k$-th step of the recursive procedure described above to compute $\mathcal{N}_k$ and $\mathcal{B}_k$ requires to perform Gaussian elimination on the $h \times t$ matrix $M_{\mathcal{R}}$. As already observed, $\dim \operatorname{Ker} M_{\mathcal{R}} = \dim(J_k \cap \langle \mathcal{N}_{k-1}^+ \rangle)$; hence, by Remark 2.3, $\dim \operatorname{Ker} M_{\mathcal{R}} = t - \dim\langle \mathcal{N}_k \rangle$. In particular $\dim\langle \mathcal{N}_k \rangle = |\mathcal{N}_k| = \operatorname{rk} M_{\mathcal{R}} \leq h$. Thus for each $i = 1, \ldots, s$ we have that $|\mathcal{N}_i| \leq h$ and hence $|\mathcal{N}_i^+| \leq (n+1)h$. Therefore the complexity of each step of the algorithm is $O(nh^3)$. As a consequence the complexity of the recursive algorithm in $s$ steps to compute a border basis of $I(J_1, \ldots, J_s)$ is $O(snh^3)$.

As for the minimizing phase outlined in Proposition 2.14, note that for each $k$ we have that $|\mathcal{B}_k| = |(\partial\mathcal{N})_k| \leq (n+1)h$, $|\mathcal{B}_{k-1}^+| \leq (n+1)^2 h$ and hence

$$|\widetilde{\mathcal{B}_k}| = |\mathcal{B}_{k-1}^+ \cup \mathcal{B}_k| \leq (n+1)(n+2)h.$$

Moreover the distinct monomials appearing in the polynomials of $\mathcal{B}_{k-1}^+ \cup \mathcal{B}_k$ form a subset of $\mathcal{N}_{k-2}^{++}$ and therefore they are at most $(n+1)^2 h$.

Since the number of the left columns in $U$ is $|\mathcal{B}_{k-1}^+| \leq (n+1)^2 h$, when we reduce the matrix $U$ to the form $\widehat{U}$ by means of subtractions among the left columns, we need at most $(n+1)^2 h$ column subtractions. The length of each of these columns is at most $(n+1)^2 h$, thus the complexity of the reduction of $U$ to $\widehat{U}$ is $O(n^4 h^2)$.

The last part of the minimizing phase requires to reduce the matrix $P_2$ to echelon form by column operations. The number of rows of $P_2$ is equal to $|(\partial\mathcal{N})_k| \leq$

$(n+1)h$, while the number of its columns is $\leq (n+1)^2 h$. Thus the complexity of the algorithm to reduce $P_2$ is $O(n^4h^3)$.

Hence the complexity of the algorithm outlined in Proposition 2.14 to compute a minimal set of generators for $J_{\leq s}$ is $O(sn^4h^3)$.

## 4. Curves in $\mathbb{P}^n(\mathbb{C})$ given by approximate points

In this section we consider the situation where the points $\mathcal{R} = \{R_1, \ldots, R_h\}$ on the irreducible projective curve $C$ in $\mathbb{P}^n(\mathbb{C})$ are given only approximately. In this case we can perform the computations needed for the described procedure by replacing Gaussian elimination by more suitable and numerically stable tools.

As observed in Section 2, if one is only interested in computing a set of generators of $I(J_1, \ldots, J_s)$ (not necessarily a border basis up to degree $s$), it is sufficient to compute a basis of $J_k \cap \langle \mathcal{N}_{k-1}^+ \rangle$ and compute a complement $\mathcal{N}_k$ for each $k$ (see Remark 2.5). The former task corresponds to computing a basis of the null-space of the $h \times t$ matrix

$$M_{\mathcal{R}} = \begin{pmatrix} m_1(R_1) & \ldots & m_t(R_1) \\ \vdots & & \vdots \\ m_1(R_h) & \ldots & m_t(R_h) \end{pmatrix}$$

where $\{m_1 \ldots, m_t\} = \mathcal{N}_{k-1}^+$.

A numerically stable way to compute both the rank and an orthogonal basis of $\operatorname{Ker} M_{\mathcal{R}}$ is the SVD-algorithm which assures that one can find a unitary $h \times h$ matrix $U$, a unitary $t \times t$ matrix $V$ and an $h \times t$ real matrix $\Sigma$ such that $M_{\mathcal{R}} = U\Sigma\overline{V}^t$; the elements $\sigma_{ij}$ of the matrix $\Sigma$ are zero whenever $i \neq j$ and for $i = 1, \ldots, l = \min\{h, t\}$ we have $\sigma_{1,1} \geq \ldots \geq \sigma_{l,l} \geq 0$.

Either we know the rank of $M_{\mathcal{R}}$ (see for instance Proposition 5.8) or we can examine the singular values $\sigma_i$ of $\Sigma$ in order to obtain a rank determination as in [**GVL**]. In any case if $\operatorname{rk} M_{\mathcal{R}} = r$, then by the properties of the SVD decomposition the last $t - r$ columns of $V$ are an orthogonal basis of $\operatorname{Ker} M_{\mathcal{R}}$.

In order to compute $\mathcal{N}_k$ and continue to the next step, we take advantage of the stability properties of the QRP-algorithm which, given a matrix $M$, constructs a unitary matrix $Q$, a permutation matrix $P$ and an upper-triangular matrix $R = \left(\begin{array}{c|c} R_1 & R_2 \end{array}\right)$ such that $S = QRP$. The permutation matrix $P$ exchanges columns in order to improve the condition number of the matrix $R_1$. If $M$ has full row-rank, then $R_1$ is invertible; otherwise it is possible to use the diagonal elements of $R_1$ to make a rank determination of $M$.

In our case we apply the QRP-algorithm to the $(t-r) \times t$ matrix $S$ whose rows are the last $t - r$ columns of $V$; recall that the columns of $S$ are indexed by $\mathcal{N}_{k-1}^+$. In the decomposition $S = QRP$ the columns of $R$ are a permutation of the columns of $S$ and the monomials corresponding to the columns of $R_1$ will be chosen to be border monomials, while the monomials corresponding to the columns of $R_2$ will be chosen as the complement $\mathcal{N}_k$. Observe that the rows of $R$ correspond to a new basis for $J_k \cap \langle \mathcal{N}_{k-1}^+ \rangle$.

If we want to compute a border basis of $I(J_1, \ldots, J_s)$, we can compute the matrix $R_1^{-1}R = \left(\begin{array}{c|c} I & R_1^{-1}R_2 \end{array}\right)$ whose rows correspond to a basis $\mathcal{B}_k$ of $\operatorname{Ker} M_{\mathcal{R}}$ consisting of border polynomials.

Otherwise, if we want to compute a minimal set of generators of $I(J_1, \ldots, J_s)$, we can proceed as described in the algorithm MinimalBasis using SVD to compute

kernels and QRP to select stable pivot columns. Using the notation of Proposition 2.13, the first step is to compute a basis of $\operatorname{Ker}\widetilde{U}$. In order to do this, we use an SVD construction taking into account that, by Proposition 2.14 (v) $\dim\operatorname{Ker}\widetilde{U} = \dim\operatorname{Ker}U = l - s_1$. We then apply the QRP-algorithm to the matrix $N$ whose rows contain the projection by $\pi_2$ of a set of generators of $\operatorname{Ker}\widetilde{U}$ and whose columns are indexed by the generators of $J_k \cap \langle\mathcal{N}_{k-1}^+\rangle$. We thus obtain $N = Q'R'P'$. Examining the diagonal elements of $R'$ we can determine its rank $r'$; the columns of $R'$ correspond to a permuted basis of $J_k \cap \langle\mathcal{N}_{k-1}^+\rangle$ and the generators corresponding to the first $r'$ columns are redundant and can be discarded.

Exact Gaussian elimination, SVD and QRP-algorithm applied to an $m \times n$ matrix all have the same complexity $O(mn\min(m,n))$. In the approximate algorithm the computation of the null-space using SVD has a complexity $O(nh^3)$ and is followed by a QRP-algorithm which has a complexity $O(n^3h^3)$. Thus the complexity to compute a set of generators or a border basis of $I(J_1,\dots,J_s)$ is $O(sn^3h^3)$, while the complexity to compute a minimal set of generators of $I(J_1,\dots,J_s)$ by the algorithm MinimalBasis is $O(sn^6h^3)$.

Alternatively, after computing a border basis, we can give a numerical algorithm based on Proposition 2.14, which would reduce the complexity to $O(sn^4h^3)$ with a slight loss of numerical precision.

Example 4.1. We implemented our algorithm in Octave. Here is the result we obtained when we tested it on the following parametric sextic space curve $C$ taken from [**JWG**]:

$$\begin{aligned} x &= 3s^4t^2 - 9s^3t^3 - 3s^2t^4 + 12st^5 + 6t^6\\ y &= -3s^6 + 18s^5t - 27s^4t^2 - 12s^3t^3 + 33s^2t^4 + 6st^5 - 6t^6\\ z &= s^6 - 6s^5t + 13s^4t^2 - 16s^3t^3 + 9s^2t^4 + 14st^5 - 6t^6\\ w &= -2s^4t^2 + 8s^3t^3 - 14s^2t^4 + 20st^5 - 6t^6. \end{aligned}$$

By Theorem 5.1 the ideal of this curve of degree 6 in $\mathbb{P}^3(\mathbb{C})$ can be generated by polynomials of degree at most 5.

We chose $31 > 6\cdot 5$ points using roots of unity of the following form:

$$s = 1; \quad t = exp(2\pi ik/31) \quad k \in \{1,\dots,31\}.$$

Running the algorithm BorderBasisWithComplement, we obtained no polynomials of degree 1 (showing that the ideal is not contained in any hyperplane), no polynomials of degree 2, 4 polynomials of degree 3, 11 of degree 4 and 22 of degree 5, yielding a set of generators for the ideal in .08 seconds. Among the 20 monomials of degree 3 the QRP-algorithm chose $z^2x, yxw, y^2w, z^2w$ as border monomials and the remaining 16 as generators of a complement.

We obtained a minimal basis consisting of only the 4 polynomials of degree 3 in an additional time of .02 seconds:

$$\begin{aligned} f_1 = {} & \mathbf{z^2x} + 0.06666666666\,z^2y + 0.06805555555\,zy^2 - 0.0361111111\,zyx\\ & -0.2833333333\,zyw - 0.55\,zx^2 - 1.066666667\,zxw + 0.01527777778\,y^3\\ & -0.09166666666\,y^2x + 0.3055555555\,yx^2 + 0.1833333334\,x^2w, \end{aligned}$$

$$\begin{aligned} f_2 = {} & \mathbf{yxw} + 0.2\,z^2y + 0.1416666667\,zy^2 - 0.4833333333\,zyx - 0.1\,zyw\\ & -0.9\,zx^2 - 0.2000000001\,zxw + 0.025\,y^3 - 0.15\,y^2x + 0.5\,yx^2\\ & +0.3000000001\,x^2w, \end{aligned}$$

$$\begin{aligned}
f_3 = \ & \mathbf{y^2w} - 0.8\,z^2y - 0.3166666667\,zy^2 - 0.5666666667\,zyx + 0.4\,zyw \\
& +0.6000000001\,zx^2 + 0.8000000002\,zxw - 0.01666666666\,y^3 \\
& +0.09999999999\,y^2x - 0.3333333333\,yx^2 - 0.2000000002\,x^2w, \\
f_4 = \ & \mathbf{z^2w} - 0.6666666667\,z^3 - 0.162962963\,z^2y + 0.06049382717\,zy^2 \\
& -0.03209876545\ zyx + 0.9703703704\,zyw - 0.4888888888\,zx^2 \\
& +0.3851851853\,zxw - 0.1666666667\,zw^2 + 0.01358024691\,y^3 \\
& -0.08148148149\,y^2x + 0.2716049383\,yx^2 - 0.9444444445\,yw^2 \\
& +0.1629629629\,x^2w - 0.2222222224\,xw^2
\end{aligned}$$

Using continued fractions, we then attempted to convert the coefficients from floating point numbers to rational numbers, obtaining the following polynomials:

$$\begin{aligned}
f_1 = \ & \mathbf{z^2x} + \tfrac{1}{15}\ z^2y + \tfrac{49}{720}\ zy^2 + \tfrac{11}{720}\ y^3 - \tfrac{13}{360}\ zyx - \tfrac{11}{120}\ y^2x - \tfrac{11}{20}\ zx^2 \\
& +\tfrac{11}{36}\ yx^2 - \tfrac{17}{60}\ zyw - \tfrac{16}{15}\ zxw + \tfrac{11}{60}\ x^2w, \\
f_2 = \ & \mathbf{yxw} + \tfrac{1}{5}\ z^2y + \tfrac{17}{120}\ zy^2 + \tfrac{1}{40}\ y^3 - \tfrac{29}{60}\ zyx - \tfrac{3}{20}\ y^2x - \tfrac{9}{10}\ zx^2 + \tfrac{1}{2}\ yx^2 \\
& -\tfrac{1}{10}\ zyw - \tfrac{1}{5}\ zxw + \tfrac{3}{10}\ x^2w, \\
f_3 = \ & \mathbf{y^2w} - \tfrac{4}{5}\ z^2y - \tfrac{19}{60}\ zy^2 - \tfrac{1}{60}\ y^3 - \tfrac{17}{30}\ zyx + \tfrac{1}{10}\ y^2x + \tfrac{3}{5}\ zx^2 - \tfrac{1}{3}\ yx^2 \\
& +\tfrac{2}{5}\ zyw + \tfrac{4}{5}\ zxw - \tfrac{1}{5}\ x^2w, \\
f_4 = \ & \mathbf{z^2w} - \tfrac{2}{3}\ z^3 - \tfrac{22}{135}\ z^2y + \tfrac{49}{810}\ zy^2 + \tfrac{11}{810}\ y^3 - \tfrac{13}{405}\ zyx - \tfrac{11}{135}\ y^2x \\
& -\tfrac{22}{45}\ zx^2 + \tfrac{22}{81}\ yx^2 + \tfrac{131}{135}\ zyw + \tfrac{52}{135}\ zxw + \tfrac{22}{135}\ x^2w - \tfrac{1}{6}\,zw^2 - \tfrac{17}{18}\ yw^2 \\
& -\tfrac{2}{9}\,xw^2.
\end{aligned}$$

The floating point coefficients were sufficiently accurate to recover the exact rational coefficients and the previous polynomials generate the exact ideal of the curve over $\mathbb{Q}$.

## 5. Degree bounds for ideal generators

Let $C$ be an irreducible projective curve (seen as a set of points in $\mathbb{P}^n(\mathbb{K})$) and let $I = \mathcal{I}(C) \subset \mathcal{P} = \mathbb{K}[x_0, \ldots, x_n]$ be the prime homogeneous ideal consisting of all the polynomials vanishing on $C$. In Section 3 we saw that the computation of $I$ can be reduced to the computation of the ideal of sufficiently many points on the curve (see Proposition 3.1). In order to be sure that one has enough points, it is necessary to bound the degrees of generators of the ideal $I$. Such a bound can be obtained from the *regularity* of the curve.

Recall that if $0 \to \ldots \to F_1 \to F_0 \to J \to 0$ is a graded free resolution of a polynomial ideal $J$ , we say that $J$ is $k$-regular if each $F_j$ can be generated by polynomials of degree $\leq k + j$. Then we call *regularity* of $J$ the integer $reg(J) = \min\{k \mid J \text{ is } k\text{-regular}\}$.

If $reg(C) = reg(\mathcal{I}(C)) = m$, then (see for instance [**E**]) $I$ can be generated by homogeneous polynomials of degree at most $m$; moreover the Hilbert function $HF_I(s)$ and the Hilbert polynomial $HP_I(s)$ of $\mathcal{P}/I$ take the same value for all integers $s \geq m$.

The next result gives information about the regularity of the curve as a function of the curve degree and of the dimension of the embedding projective space:

THEOREM 5.1 (Gruson-Lazarsfeld-Peskine [**GLP**]). *Let $\mathcal{D} \subset \mathbb{P}^n(\mathbb{K})$ be a reduced and irreducible curve of degree $d$ not contained in any hyperplane, with $\mathbb{K}$ algebraically closed and $n \geq 3$. Then $reg(\mathcal{D}) \leq d - n + 2$.*
*Moreover, if $\mathcal{D}$ has genus $g > 1$ then $reg(\mathcal{D}) \leq d - n + 1$.*

The previous result and many of the degree bounds apply to curves not contained in any hyperplane, i.e. non-degenerate, which happens if and only if $I_1 = \mathcal{I}(C)_1 = (0)$. On the other hand a degenerate curve in $\mathbb{P}^n(\mathbb{K})$ is a non-degenerate curve in the projective subspace $V(I_1)$ having dimension $n - \dim I_1$. So the bounds of this section apply to degenerate curves if we replace $n$ by $n - \dim I_1$.

REMARK 5.2. A parametrization of a curve $C \subset \mathbb{P}^n(\mathbb{K})$ can be regarded as a machine delivering as many points on the curve as needed. Moreover if $\psi\colon \mathbb{P}^1(\mathbb{K}) \to \mathbb{P}^n(\mathbb{K})$ is a rational map whose image is the curve $C$ and $\psi([t_0, t_1]) = [F_0(t_0, t_1), \ldots, F_n(t_0, t_1)]$ with $F_i(t_0, t_1)$ homogeneous polynomials of degree $s$, then $\deg C \leq s$. Using this upper bound for the curve degree, via Theorem 5.1 we obtain an upper bound for the degrees of generators of $C$. This allows us to use our procedure to compute generators of the ideal $I$ of the curve and in particular to compute an implicit representation of $C$ starting from a parametric one. □

Sharper bounds for the degrees of generators can be obtained for certain curves obtained as the image of the embedding given by a complete linear series. A first result in this direction concerns canonical curves (see for instance [**SD2**]):

THEOREM 5.3 (Petri [**P**]). *The ideal of a non-hyperelliptic canonical curve of genus $g \geq 4$ can be generated by polynomials of degree 2 and of degree 3.*

PROPOSITION 5.4. Let $C \subset \mathbb{P}^n(\mathbb{K})$ be a non-degenerate irreducible curve of geometric genus $g \geq 4$ and of degree $d = 2g - 2$, with $\mathbb{K}$ algebraically closed and $n = g - 1$. Then the ideal $I = \mathcal{I}(C)$ can be generated by polynomials of degree 2 and of degree 3.

PROOF. By Theorem VI.6.10 in [**W**] any non-degenerate curve of genus $g$ and degree $2g - 2$ embedded in $\mathbb{P}^{g-1}(\mathbb{K})$ is a smooth non-hyperelliptic canonical curve. Then the conclusion follows from Theorem 5.3. □

The following result of Saint-Donat gives bounds for the degrees of generators of curves of genus $g$ which are the image of an embedding given by a complete linear series of sufficiently high degree:

THEOREM 5.5. *([**SD1**]) Let $C \subset \mathbb{P}^n(\mathbb{K})$ be an irreducible nonsingular curve of genus $g$ embedded by a complete linear series of degree $d$.*

1. *If $d \geq 2g + 1$, then the ideal $I$ of $C$ can be generated by polynomials of degree 2 and of degree 3.*
2. *If $d \geq 2g + 2$, then $I$ can be generated by polynomials of degree 2.*

The following result shows that we can remove the condition of being embedded by a complete linear series:

PROPOSITION 5.6. Let $C \subset \mathbb{P}^n(\mathbb{K})$ be a non-degenerate irreducible curve of geometric genus $g$ and degree $d$, with $\mathbb{K}$ algebraically closed and $n = d - g$. Then

1. If $d \geq 2g + 1$, then the ideal $I = \mathcal{I}(C)$ can be generated by polynomials of degree 2 and of degree 3.
2. If $d \geq 2g + 2$, then $I = \mathcal{I}(C)$ can be generated by polynomials of degree 2.

PROOF. Recall that any curve $C$ of degree $d$ and genus $g$ in $\mathbb{P}^n(\mathbb{K})$ can be seen as the image of the map given by a linear series contained in $\mathcal{L}(D)$ for some divisor $D$ of degree $d$ on a non-singular model $\widetilde{C}$ of $C$.

For any divisor $D$ on $\widetilde{C}$, denote by $l(D)$ the dimension of the complete linear series $\mathcal{L}(D)$. We also denote by $K$ a canonical divisor.

If $d \geq 2g+1$, then $l(K-D) = 0$ and hence by Riemann-Roch Theorem $l(D) = d - g + 1$; moreover (see [**F**]) the map induced by $D$ is an embedding. Thus we can see $C$ as the image of an embedding of $\widetilde{C}$ in $\mathbb{P}^{d-g}(\mathbb{K})$. So, since $C$ is non-degenerate, $C$ is embedded by a complete linear series if and only if $n = d-g$.

Moreover, if $d \geq 2g+1$ and $n = d-g$, the curve $C$ is the image of a non-singular curve through a map which is an embedding, therefore $C$ is non-singular. Hence the hypotheses of Theorem 5.5 are fulfilled and it implies our result. □

**Example 1.** Assume that $C$ has genus $g \geq 3$ and is embedded by the bicanonical map. Since $\deg(2K) = 4g-4 \geq 2g+2$, by Theorem 5.5 $I$ can be generated by quadratic polynomials.

**Example 2.** If $C$ has genus $g = 2$ and is embedded by the tricanonical map (which gives an embedding because $\deg(3K) = 6g-6 = 6 \geq 2g+1$), since $\deg(3K) \geq 2g+2$ again by Theorem 5.5 $I$ can be generated by polynomials of degree 2.

Other results giving bounds for the degrees of generators of the curve ideal in different situations are available in the literature; the following one (see [**A**]) gives results in the hyperelliptic case:

PROPOSITION 5.7 (Akahori). Let $C \subset \mathbb{P}^n(\mathbb{K})$ be an irreducible non-degenerate and non-singular hyperelliptic curve of genus $g$ and degree $d$.

(1) If $d = 2g$, then the ideal $I$ of $C$ can be generated by polynomials of degrees 2, 3 and 4.
(2) If $d = 2g-1$, then $I$ can be generated by polynomials of degrees 2, 3, 4 and 5.

When we need to compute the null-space of the evaluation matrix $M_{\mathcal{R}}$ for approximate points (see Section 4), we can try to determine its rank by inspecting its singular value spectrum. Since this is not guaranteed to work, it is useful to predict what the rank should be. Since the rank of $M_{\mathcal{R}}$ equals $|\mathcal{N}_k| = \dim \mathcal{P}_k - \dim I_k$, the following proposition gives a situation where we can predict this value.

Recall that if $g_0, \ldots, g_n$ is a basis of the complete linear series $\mathcal{L}(D)$ of dimension $l(D) = n+1$, then $I_k = \operatorname{Ker} \varphi_k$ where $\varphi_k \colon \mathcal{P}_k \to \mathcal{L}(kD)$ defined by $\varphi_k(x_i) = g_i$.

PROPOSITION 5.8. If $\varphi_k$ is surjective and $k \cdot \deg(D) \geq 2g-1$, then

$$\dim \mathcal{P}_k - \dim I_k = k \cdot \deg(D) - g + 1.$$

PROOF. If $\varphi_k$ is surjective, then $\dim I_k = \dim \operatorname{Ker} \varphi_k = \dim \mathcal{P}_k - \dim \mathcal{L}(kD)$. Since $\deg(kD) = k \cdot \deg(D) \geq 2g-1$, then $i(kD) = 0$. Hence by Riemann-Roch Theorem we get $l(kD) = \deg(kD) - g + 1 = k \cdot \deg(D) - g + 1$ and the conclusion follows. □

**Examples.** 1. Assume that $C$ is non-hyperelliptic of genus $g \geq 4$ and take the canonical divisor $D = K$; in particular $\deg(D) = 2g-2$ and $l(D) = g$ (i.e. in this case $n = g-1$). By Theorem 5.3 we already know that $I$ can be generated by polynomials of degree 2 and of degree 3, and so it suffices to know $\dim I_2$ and $\dim I_3$.

Then by Noether's Theorem the map $\varphi_k \colon \mathcal{P}_k \to \mathcal{L}(kD)$ is surjective for all $k$. Furthermore for all $k \geq 2$ we have that $k \cdot \deg(D) \geq 2g-1$, hence by Proposition

5.8 we have $\dim \mathcal{P}_k - \dim I_k = k(2g-2) - g + 1$. In particular

$$|\mathcal{N}_2| = \dim \mathcal{P}_2 - \dim I_2 = 2(2g-2) - g + 1 = 3g - 3$$

$$|\mathcal{N}_3| = \dim \mathcal{P}_3 - \dim I_3 = 3(2g-2) - g + 1 = 5g - 5.$$

2. If we choose a divisor $D$ such that $\deg(D) \geq 2g+1$, then $\varphi_k \colon \mathcal{P}_k \to \mathcal{L}(kD)$ is surjective (see [**M**]); moreover for all $k \geq 1$ we have that $k \cdot \deg(D) \geq 2g - 1$. Then we can compute $\dim I_k$ by Proposition 5.8.

In particular if $D = 2K$ and $g \geq 3$, then we know that $I$ can be generated by quadratic polynomials. Since $i(2K) = 0$, by Riemann-Roch Theorem $l(2K) = 3g - 3$, i.e. $n = 3g - 4$. Then

$$|\mathcal{N}_2| = \dim \mathcal{P}_2 - \dim I_2 = 2(4g-4) - g + 1 = 7g - 7.$$

If $g = 2$ and we choose $D = 3K$, we know that $I$ can be generated by quadratic polynomials. Since $i(3K) = 0$, by Riemann-Roch Theorem $l(3K) = 5g - 5 = 5$, i.e. $n = 4$. Then

$$|\mathcal{N}_2| = \dim \mathcal{P}_2 - \dim I_2 = 2\deg(3K) - g + 1 = 11.$$

REMARK 5.9. When the ideal can be generated in degree 2 and we know $|\mathcal{N}_2|$ as above, then the algorithm to compute a minimal set of generators can be considerably simplified. If $M_{\mathcal{R}}$ is the point evaluation matrix for all monomials of degree 2, since we know that $\operatorname{rk} M_{\mathcal{R}} = |\mathcal{N}_2|$, a single application of the SVD-algorithm with this imposed rank computes a basis for the null-space of $M_{\mathcal{R}}$ which directly yields a minimal set of generators of the ideal.

## Acknowledgments

We wish to thank Mika Seppälä for proposing this problem to us and a referee for many helpful comments.

## References

[AFT] Abbott, J., Fassino, C., Torrente, M., *Stable border bases for ideals of points*, J. Symbolic Comput. **43** (2008), 883–894.

[A] Akahori, K., *The intersection of quadrics and defining equations of a projective curve*, Tsukuba J. Math. **20** n. 2 (1996), 413–424.

[ACOR] Albano, G., Cioffi, F., Orecchia, F., Ramella, I., *Minimally generating ideals of rational parametric curves in polynomial time*, J. Symbolic Comput. vol. **30** n. 2 (2000), 137–149.

[C] Cioffi, F., *Minimally generating ideals of points in polynomial time using linear algebra*, Ricerche Mat. vol. **48** n. 1 (1999), 55–63.

[E] Eisenbud, D., *The geometry of syzygies. A second course in commutative algebra and algebraic geometry*, Graduate Texts in Mathematics 229 Springer-Verlag, New York, 2005.

[F] Fulton, W., *Algebraic curves. An introduction to algebraic geometry*, W. A. Benjamin, Inc., New York-Amsterdam, 1969.

[GSST] Gianni, P., Seppälä, M., Silhol, R., Trager, B., *Riemann Surfaces, Plane Algebraic Curves and Their Period Matrices*, J. Symbolic Comput. **12** (1998), 789–803.

[GVL] Golub, G. H., Van Loan, C. F., *Matrix computations*, Johns Hopkins University Press, Baltimore, MD, 1996.

[GLP] Gruson, L., Lazarsfeld, R., Peskine, C., *On a theorem of Castelnuovo, and the equations defining space curves*, Invent. Math. **72** n. 3 (1983), 491–506.

[HKPP] Heldt, D., Kreuzer, M., Pokutta, S., Poulisse, H., *Approximate computation of zero-dimensional polynomial ideals*, J. Symbolic Comput. **44** (2009), 1566–1591.

[JWG] Jia, X., Wang, H., Goldman, R., *Set-theoretic generators of rational space curves*, J. Symbolic Comput. vol. **45** n. 4 (2010), 414–433.

[KR] Kreuzer, M., Robbiano, L., *Computational commutative algebra 2*, Springer-Verlag, Berlin, 2005.

[MMM] Marinari, M. G., Möller, H. M., Mora, T., *Gröbner Bases of Ideals Defined by Functionals with an Application to Ideals of Projective Points*, Appl. Algebra Eng. Commun. Comput. **4** (1993), 103–145.

[MB] Möller, H. M., Buchberger, B., *The Construction of Multivariate Polynomials with Preassigned Zeros*, Proc. EUROCAM 82, L.N.C.S **144** (1982), 24–31.

[MT] Mourrain, B., Trébuchet, P., *Stable normal forms for polynomial system solving*, Theoret. Comput. Sci. **409** n. 2 (2008), 229–240.

[M] Mumford, D., *Varieties defined by quadratic equations*, In: Questions on Algebraic Varieties (Corso C.I.M.E., III Ciclo, Varenna, 1969) Edizioni Cremonese, Roma, (1970) pp. 29–100.

[P] Petri, K., *Über die invariante Darstellung algebraischer Funktionen einer Veränderlichen*, Math. Ann. **88** n. 3-4 (1923), 242–289.

[SD1] Saint-Donat, B., *Sur les équations définissant une courbe algébrique*, C. R. Acad. Sci. Paris Sér. A-B **274** (1972), A324–A327.

[SD2] Saint-Donat, B., *On Petri's analysis of the linear system of quadrics through a canonical curve*, Math. Ann. **206** (1973), 157–175.

[W] Walker, R. J., *Algebraic curves*, Dover Publications Inc., New York, 1962.

Dipartimento di Matematica, Università di Pisa, Largo B. Pontecorvo 5, I-56127 Pisa, Italy

*E-mail address*: fortuna@dm.unipi.it

Dipartimento di Matematica, Università di Pisa, Largo B. Pontecorvo 5, I-56127 Pisa, Italy

*E-mail address*: gianni@dm.unipi.it

IBM T.J.Watson Research Center, 1101 Kitchawan Road, Yorktown Heights, NY 10598, USA

*E-mail address*: bmt@us.ibm.com