DISJOINT ELLIPTIC CURVES IN A PROJECTIVE SPACE

L. CHIANTINI, F. CIOFFI, F. ORECCHIA

ABSTRACT. In this paper results about the Hilbert function and about the number of minimal generators stated in [21] for disjoint unions of rational smooth curves are generalized to disjoint unions of distinct smooth non special curves. Hence, the maximal rank and the minimal generation of such curves are studied. In particular, we consider elliptic curves and we describe a method to compute their Hilbert functions in any dimension and for every choice of the degree. Applications to the study of elliptic curves on threefolds are shown.

1. Introduction

In this paper we study the maximal rank and the minimal generation of disjoint unions of distinct non special curves, with applications to elliptic curves. We construct elliptic curves in projective spaces $\mathbb{P}^n$ of any dimension $n \geq 3$ and for every choice of the degree via their rational points.

Remind that a curve $C \subset \mathbb{P}^n$ is said to have maximal rank if for every integer $t > 0$ the restriction map $\rho_C(t) : H^0(\mathbb{P}^n, \mathcal{O}_{\mathbb{P}^n}(t)) \to H^0(C, \mathcal{O}_C(t))$ has maximal rank as a map of vector spaces, i.e., if it is injective or surjective. Standard semicontinuity arguments show that the maximal rank property is open in the Hilbert scheme ([11], p.2); hence if it holds for one curve, then it holds also for the general curve in the same irreducible component. The maximal rank for general curves has been deeply studied by E. Ballico and P. Ellia who proved that a general non degenerate and non special curve of genus $g \geq 0$ and degree $d \geq g + n$ in $\mathbb{P}^n$ has maximal rank, where $n \geq 3$ (see [3] and the references therein). In [21] disjoint unions of rational curves with maximal rank are characterized by means of the Hilbert function; moreover results about the number of minimal generators for such unions of rational curves are described. In section 2 we generalize these results to disjoint unions of non special curves, i.e. of curves C whose index of speciality $e_C := max\{t | H^1(\mathcal{O}_C(t)) \neq 0\}$ is null.

In section 3 we describe how to construct an elliptic curve of any degree $d \geq 3$ via its rational points (Remark 3.1). So, recall that a point $[y_0 : \ldots : y_n]$ of $\mathbb{P}^n_{\bar{K}}$ is a "rational point" over K if there exist $y'_0, \ldots, y'_r$ of K such that $[y_0 : \ldots : y_r] = [y'_0 : \ldots : y'_r]$. The Mordell-Weil group of rational points of an elliptic curve has been studied in many different contests (for example, see [6], [8]). We have implemented our construction of elliptic curves of given degree in the object-oriented language C++ by using the NTL library of V. Shoup [22] in a software called "Points" that is available at `http://cds.unina.it/~orecchia/Edownload.html` or by anonymous `ftp` on `matna3.dma.unina.it`, directory `pub/Points2`.

In section 4, by our method we check the maximal rank and the minimal generation for disjoint unions of degree $d \leq 30$ of $s \leq 6$ distinct elliptic curves in $\mathbb{P}^n$, where $3 \leq n \leq 30$, and we show the existence of smooth elliptic quintic curves on a general threefold in $\mathbb{P}^4$.

We also show an application to the study of elliptic curves and threefolds in $\mathbb{P}^4$. The question about which curves lie in a smooth general threefold recently grew in interest because of its connections with hyperbolic geometry (see e.g. [13], [7], [14]); the problem is also related with the study of Hilbert schemes of curves (see [15]). We show in section 4 how one can use the equations of an elliptic curve, generated by our algorithm, to obtain the existence of elliptic normal curves on a general quartic threefold in $\mathbb{P}^4$. The method was used in [16], where a complete classification of rank 2 bundles without intermediate cohomology on general quartic threefolds is achieved. We also hope to apply it for the study of rank 22 bundles over the general (Calabi-Yau) quintic threefold

In the following $S = K[x_0, \dots, x_n]$ is a ring of polynomials over a field K, $\bar{K}$ is the algebraic closure of K and the characteristic of K is not 2. By projective algebraic variety we mean the set of points of $\mathbb{P}^n_{\bar{K}}$ that are the zeros of the polynomials of a homogeneous ideal of S. In particular, by a (projective) curve in $\mathbb{P}^n_{\bar{K}}$ we mean a projective variety of pure dimension 1.

2. Maximal rank and minimal generation of disjoint unions of non special curves

We will use freely the common notations of sheaf cohomology in $\mathbb{P}^n$. We say that a variety is generated in degree t if its ideal I can be generated by forms of degree $\le t$.

Remark 2.1. We recall briefly some well-known fact about the generators of a homogeneous ideal and its Castelnuovo - Mumford regularity.

Let m be an integer. A coherent sheaf $\mathcal{F}$ is m-regular if $H^q(\mathcal{F}(m-q)) = 0$ for all $q > 0$ [19].

If I is a saturated homogeneous ideal, then we say that I is m-regular when its sheafification $\mathcal{I}$ is. It turns out that I is m-regular if its j^{th} module of syzygies is generated in degree $\le m-j$, for each $j > 0$ (see, for example, [9, Prop. 2.6]). This last definition can be extended to any homogeneous ideal I.

Let $Y \subset \mathbb{P}^n$ be a projective variety. We say that Y is m-regular when its associated homogeneous ideal I is.

It can be proved that if I is m-regular, then it is also $(m+t)$-regular, for every $t \ge 0$ [19]. The regularity $reg(I)$ of I is defined as the smallest integer m for which I is m-regular. Regularity provides a stop for an algorithm that finds generators of a saturated ideal. In fact if I is m-regular, then it is generated in degree m [19, Lecture 14].

Let $I = I(Y) = \bigoplus_{t \ge 0} I(Y)_t$ be the ideal of a closed subvariety Y and $A = S/I$ be the coordinate ring of Y. Set

$$H_Y(t) = dim_K A_t = dim_K S_t - dim_K I_t = \left(\begin{array}{c} t+n \\ n \end{array} \right) - dim_K I_t$$

for the Hilbert function of Y and call $P_Y(t)$ the Hilbert polynomial of Y. Let

$$\Delta H_Y(t) := H_Y(t) - H_Y(t-1), \quad \Delta^i H_Y(t) := \Delta^{i-1} H_Y(t) - \Delta^{i-1} H_Y(t-1)$$

be the difference functions.

The Poincaré series of Y

$$HP_Y(z) = \sum_{t \ge 0} H_Y(t) z^t$$

can be expressed as a rational function $h(z)/(1-z)^{d+1}$; let δ be the degree of $h(z)$.

Definition 2.1. *Let Y be a closed (possibly reducible) subvariety of $\mathbb{P}^n$; define $\rho_Y(t)$ as the natural restriction map*

$$\rho_Y(t) : H^0(\mathbb{P}^n, \mathcal{O}_{\mathbb{P}^n}(t)) \to H^0(Y, \mathcal{O}_Y(t)).$$

We say that Y has maximal rank if, for every integer $t > 0$, $\rho_Y(t)$ has maximal rank as a map of vector spaces, i.e., it is injective or surjective.

Definition 2.2. *The index of speciality of a curve C is*

$$e_C := max\{t | H^1(\mathcal{O}_C(t)) \neq 0\}$$

and the sheaf $\mathcal{O}_C(t)$ is called non special if $H^1(\mathcal{O}_C(t)) = 0$.

Using the previous notation, we can restate the notion of regularity in the case of homogeneous ideals associated to curves:

Lemma 2.1. *Let C be a curve. For all $t \geq 0$, C is t-regular if and only if $\mathcal{O}_C(t-2)$ is non special and $\rho_C(t-1) : H^0(\mathbb{P}^n, \mathcal{O}_{\mathbb{P}^n}(t-1)) \to H^0(C, \mathcal{O}_C(t-1))$ is surjective.*

Furthermore, if $m \geq reg(C)$, then

(1) $H_C(t) = P_C(t)$, *for* $t \geq m-1$;
(2) $P_C(t) = \Delta H_C(m)t + H_C(m-1) - \Delta H_C(m)(m-1)$;
(3) $HP_C(z) = \sum_{i=1}^m h_i z^i/(1-z)^2$, *with* $h_i = \Delta^2 H_C(i)$.

Proof. The first assertion is obvious. For (1) see, for example, [20, Lemma 4(i)]. (2) Since the Hilbert polynomial $P_C(t)$ has degree 1, it is sufficient to determine the unique polynomial of degree 1 in a variable t which assumes the values $H_C(m)$ and $H_C(m-1)$ respectively for $t = m$ and $t = m-1$. (3) See, for example, [18, section 1.4]. ■

The following results extend to non-special curves properties that have been already proved in [21] for rational smooth curves.

Theorem 2.1. *Let $C \subset \mathbb{P}^n$ $(n \geq 3)$ be a non degenerate disjoint union of s distinct irreducible smooth curves C_i of genus g and of degrees d_i. Assume that $\mathcal{O}_{C_i}(t)$ is non special for every $t > 0$ and for every $i = 1, \ldots, s$, and let I be the ideal of C.*

Then $H_C(t) \leq P_C(t) = dt + s(1-g)$, for every $t > 0$. Furthermore:

(1) *for every $t > 0$ one has* $H_C(t) \leq min\left\{\binom{t+n}{n}, dt + s(1-g)\right\}$;
(2) *in (1) the equality holds for all $t > 0$ if and only if $\rho_C(t)$ has maximal rank;*
(3) $reg(I) = \min\{t \geq 3 | H_C(t-1) = P_C(t-1)\}$

Proof. Since $\mathcal{O}_C(t) = \oplus \mathcal{O}_{C_i}(t)$ and the cohomology commutes with direct sums, then $H^1(\mathcal{O}_C(t))$ $= 0$ for all $t > 0$. By applying sheafification to the short exact sequence $0 \to I \to S \to S/I \to 0$, we determine the exact sequence

$$0 \to \mathcal{I}_C(t) \to \mathcal{O}_{\mathbb{P}^r}(t) \to \mathcal{O}_C(t) \to 0 \qquad (*)$$

to which we apply cohomology, getting

$$0 \to H^0(\mathcal{I}_C(t)) \to H^0(\mathcal{O}_{\mathbb{P}^r}(t)) \xrightarrow{\rho_C(t)} H^0(\mathcal{O}_C(t)) \to H^1(\mathcal{I}_C(t)) \to 0$$

Since $H^1(\mathcal{O}_C(t)) = 0$, for every $t > 0$,

$$H_C(t) = dim_K(Im(\rho_C(t))) \leq h^0(\mathcal{O}_C(t)) = h^0(\mathcal{O}_C(t)) - h^1(\mathcal{O}_C(t)) = P_C(t).$$

The first assertion follows since clearly $H_C(t) \leq \dim H^0(\mathcal{O}_{\mathbb{P}^r}(t)) = \binom{t+n}{n}$, for any t. Also equality means that $\rho_C(t)$ has maximal rank.

To see (3), observe that sequence $(*)$ and our assumptions imply $H^2(\mathcal{I}_C(t-2)) = H^1(\mathcal{O}_C(t-2)) = 0$ for all $t \geq 3$. If $H_C(\bar{t}-1) = P_C(\bar{t}-1)$ for some $\bar{t} \geq 3$, then the map $\rho_C(\bar{t}-1)$ surjects, so $H^1(\mathcal{I}_C(\bar{t}-1))=0$. Moreover, by Grothendieck, it is $H^i(\mathcal{O}_C(t))=0$, for every $i>1$ and for every t. Since $H^q(\mathcal{O}_{\mathbb{P}^n}(t))=0$ for every $q>0$ ($q\neq n$) and every t, then from the same exact long sequence in cohomology one sees that $0=H^{q-1}(\mathcal{O}_C(t))=H^q(\mathcal{I}_C(t))$, for every $q>2$ ($q\neq n$) and t. If $q=n$, then $H^q(\mathcal{O}_{\mathbb{P}^n})=0$ for every $t>-(n+1)$. Since $\bar{t}\geq 3$, thus $H^q(\mathcal{I}_C(t-q))=0$ for every $q>2$ and $t\geq\bar{t}$. It follows that I is $\bar{t}$-regular. Then, by Lemma 2.1(1) we are done. ■

Next proposition provides our main tool for determining when we get an embedding of disjoint union of smooth non-special curves.

Proposition 2.1. *Let $\bar{C}$ be a disjoint union of smooth curves $\bar{C}_1,\dots,\bar{C}_s$ of geometric genus g. Let $\phi:\bar{C}\to\mathbb{P}^n$ be a map of $\bar{C}$ to some projective space and call $C=\cup_{i=1}^s C_i$ the image. Assume that the pull-back H_i of $\mathcal{O}_{\mathbb{P}^n}(1)$ to any $\bar{C}_i$ is a very ample and non special divisor of degree d_i. Put $d=\sum_{i=1}^s d_i$.*

If $H_C(\bar{t})=d\bar{t}+s(1-g)$ for some $\bar{t}>0$, then ϕ is an embedding, i.e. C is a disjoint union of smooth curves of degrees $d_1,\dots,d_s$.

Proof. By Riemann-Roch, on each $\bar{C}_i$ one has $h^0(\mathcal{O}_{\bar{C}_i}(tH_i))=d_it-g+1$ for all $t>0$. Now we have $H^0(\mathcal{O}_{\bar{C}})=\oplus_{i=1}^s H^0(\mathcal{O}_{\bar{C}_i})$ so that $\dim H^0(\mathcal{O}_{\bar{C}}(tH))=dt-sg+s$ for all $t>0$, where H is the pull-back to $\bar{C}$ of $\mathcal{O}_{\mathbb{P}^n}(1)$.

Assume now $H_C(\bar{t})=d\bar{t}+s(1-g)$. The map ϕ induces a map $\mathcal{O}_{C_i}\to\mathcal{O}_{\bar{C}_i}$ which is injective, for the kernel cannot have torsion and $\phi_{|\bar{C}_i}$ is not trivial. It follows that the composition $H^0(\mathcal{O}_{\mathbb{P}^r}(\bar{t}))\to H^0(\mathcal{O}_{\bar{C}}(\bar{t}H))$ is surjective; so it induces on each $\bar{C}_i$ the complete linear series associated to H_i; by assumptions it follows that ϕ restricts to an embedding of any $\bar{C}_i$. Furthermore, by assumptions since the restriction map surjects onto $H^0(\mathcal{O}_C(t))$, then there are surfaces of degree $\bar{t}$ which separate the points of two different pieces $\bar{C}_i$, $\bar{C}_j$ of $\bar{C}$. The claim follows. ■

Proposition 2.2. *Let $C=\cup_{i=1}^s C_i$ be a non degenerate curve such that $C_1,\dots,C_s$ are irreducible curves of geometric genus g and of degrees $d_1,\dots,d_s$, where $d_i\geq 2g+1$ for every $i=1,\dots,s$. Let $d=\sum_{i=1}^s d_i$ and $\alpha=min\{t\in N|\begin{pmatrix} t+n\\ n\end{pmatrix}>dt+s(1-g)\}$. Then the curves C_i are smooth and disjoint and C has maximal rank if, and only if, $H_C(\alpha-1)=\begin{pmatrix}\alpha-1+n\\ n\end{pmatrix}$ and $H_C(\alpha)=d\alpha+s(1-g)$. Moreover, in this situation $I(C)$ is generated by forms of degrees α and $\alpha+1$ because $reg(I(C))=\alpha+1$.*

Proof. It is sufficient to apply Theorem 2.1 and Proposition 2.1. Indeed, in the hypotheses that $H_C(\alpha-1)=\begin{pmatrix}\alpha-1+n\\ n\end{pmatrix}$ and $H_C(\alpha)=d\alpha+s(1-g)$, let $\Phi_i:\tilde{C}_i\to C_i$ be the normalization of C_i. Hence $\tilde{C}_i$ is a smooth curve of degree d_i and genus g and $H_{C_i}(t)\leq H_{\tilde{C}_i}(t)$. Since $d_i\geq 2g+1$, $\mathcal{O}_{\tilde{C}_i}(1)$ is a very ample and non special divisor of degree d_i. By Theorem 2.1 it is $H_{\tilde{C}_i}(t)\leq d_it+1-g$, for every $t\geq 0$, and hence

$$d\alpha+s(1-g)=H_C(\alpha)\leq\sum H_{C_i}(\alpha)\leq\sum H_{\tilde{C}_i}(\alpha)\leq d\alpha+s(1-g).$$

If $\cup\tilde{C}_i$ were not a disjoint union, it would be $\sum H_{\tilde{C}_i}(\alpha)<d\alpha+s(1-g)$, a contradiction. Hence we can apply Proposition 2.1 and so C is a disjoint union of smooth curves. The maximal rank follows by Theorem 2.1(2). Viceversa, apply Theorem 2.1 (1) and (2). The result about the regularity follows from Theorem 2.1(3) and Lemma 2.1(1). ■

Notice that since the index of speciality of an elliptic curve E is null and, so, $H^1(\mathcal{O}_E(t)) = 0$ for every $t > 0$, then Theorem 2.1 and Propositions 2.1 and 2.2 can be applied for every elliptic curve and for non degenerate unions of distinct elliptic curves.

Let C be a non degenerate disjoint union of s distinct irreducible smooth curves C_i of degrees d_i and of the same genus g, with $\mathcal{O}_{C_i}(t)$ non special, for every $t > 0$. Moreover, assume that C has maximal rank. By Proposition 2.2 we know that these properties of C are characterized by the behaviour of the Hilbert function of C.

In this situation, the ideal $I(C)$ is generated by forms of degrees α and $\alpha + 1$, where $\alpha = min\{t| \left(\begin{array}{c} t+n \\ n \end{array} \right) > dt + s(1-g)\Big\}$, since $reg(I) = \alpha + 1$. So it is interesting to study the expected number for the minimal generators of $I(C)$ (see [21], for rational curves).

Definition 2.3. *The curve C is minimally generated if a minimal set of homogeneous generators of $I(C)$ has cardinality*

$$dim_K(I_\alpha) + dim_K(I_{\alpha+1}) - min\{(n+1)dim_K(I_\alpha), dim_K(I_{\alpha+1})\}$$

that is

$$\sigma(\alpha) : H^0(I_C(\alpha)) \otimes H^0(\mathcal{O}_{\mathbb{P}^n}(1)) \to H^0(I_C(\alpha+1))$$

is of maximal rank.

Since the kernel of $\sigma(\alpha)$ is $H^0(I_C(\alpha) \otimes \Omega(1))$ (see [12]), then for curves of maximal rank, by semicontinuity, minimal generation is an open property hence if it holds for one curve, then it holds also for the general curve in the same irreducible component.

It turns out that the maximal rank and the minimal generation can be checked by computing the generators of a suitable number of points on C.

Lemma 2.2. *Let C be a curve, I its ideal and $C_1, \ldots, C_h$ its irreducible components of degrees $d_1, \ldots, d_h$ respectively, so that $d = \sum_{i=1}^h d_i$ is the degree of C. Let $m \geq reg(I)$. Suppose that every curve C_i, $i = 1, \ldots, h$, contains $d_i \cdot m + 1$ distinct rational points and let J be the ideal of these $d \cdot m + h$ points of C. Then, the polynomials of degree $\leq m$ of a minimal set of generators for J form a minimal set of generators for I. Hence $H(I, t) = H(J, t)$, for $t \leq m$.*

Proof. [1, Lemma 2.1] Clearly $I \subset J$ and it is well known that a hypersurface of degree $t \leq m$ containing $d_i m+1$ points of C_i must contain C_i. Hence, $I_t = J_t$ for each degree $t \leq m$. It remains to observe that, since I is generated in degree m, then I is generated by $\bigoplus_{t \leq m} I_t = \bigoplus_{t \leq m} J_t$. ■

Hence we may use suitable sets of points on C to control that C has maximal rank and is minimally generated.

Theorem 2.2. *Let C be a non degenerate disjoint union of s distinct irreducible smooth curves C_i of the same genus g, of degree d_i, respectively, and with $\mathcal{O}_{C_i}(t)$ non special, for every $t > 0$. Let $d = \sum_{i=1}^s d_i$ and $\alpha = min\{t \in N| \left(\begin{array}{c} t+n \\ n \end{array} \right) > dt + s(1-g)\Big\}$. Let V_t^i a set of $d_i t + 1$ distinct points of C_i and $V_t = \cup V_t^i$. Let G_t be the matrix whose columns are the vectors of the evaluations of the terms of degree t over the points of V_t. Then the curves $C_1, \ldots, C_s$ are smooth and disjoint and C has maximal rank if, and only if, $H_V(\alpha-1) = rank(G_{\alpha-1}) = \left(\begin{array}{c} \alpha-1+n \\ n \end{array} \right)$ and $H_V(\alpha) = rank(G_\alpha) = d\alpha + s(1-g)$. Moreover, if $g_1, \ldots, g_e$ is a basis for $I(C)_\alpha$ and $H_{\alpha+1}$ is the matrix whose columns are the vectors of the coefficients of $x_i g_j$ (for every $i = 0, \ldots, n$*

and $j = 1, \ldots, e$*), then* C *is minimally generated if, and only if,* $rank(H_{\alpha+1}) = min\{(n+1)dim_K I(C)_\alpha, dim_K I(C)_{\alpha+1}\} = min\{(n+1)\left(\binom{\alpha+n}{n} - d\alpha - s\right), \binom{\alpha+1+n}{n} - d(\alpha+1) - s\}$.

Note that Theorem 2.2 can be applied to elliptic curves.

3. **How to construct an elliptic curve in** $\mathbb{P}^n$

In this section we show an effective method to compute elliptic curves by exploiting the availability of algorithms that construct minimal generators of ideals of points in polynomial time (for example, see [4] and the references therein). This construction allows to check the minimal rank and the minimally generation of elliptic curves. The described algorithm has been implemented in the object oriented language C++ by using the NTL library of Shoup [22] in a software called "Points" that is available at `http://cds.unina.it/~orecchia/Edownload.html` or by anonymous `ftp` on `matna3.dma.unina.it`, directory `pub/Points2`.

Recall that a point $[y_0 : \ldots : y_n]$ of $\mathbb{P}^n_{\bar{K}}$ is a "rational point" over K if there exist $y'_0, \ldots, y'_r$ of K such that $[y_0 : \ldots : y_r] = [y'_0 : \ldots : y'_r]$. Over a field K of characteristic different from 2 every elliptic curve E can be trasformed by an isomorphism over $\bar{K}$ into a plane curve with an equation of the following form

$$y^2 = x(x-1)(x-\lambda) \tag{1}$$

where $\lambda \neq 0, 1$ [23, III, Prop. 1.7]. The equation (1) is a Weierstrass representation of an elliptic plane curve in the Legendre form. The condition $\lambda \neq 0, 1$ is equivalent to the fact that E is smooth (for example, see [24, IV, section 3]). We suppose that $\lambda \in K$.

Every field K contains a copy of $\mathbb{Q}$ or of $\mathbb{Z}_p$ for some prime p and so we can assume that $K = \mathbb{Q}$ or $\mathbb{Z}_p$. To study an algebraic object over $\mathbb{Q}$ it is useful to study the reduction of the object modulo primes. Hence, let K be the field $\mathbb{F}_q$ with q elements, where q is a power of a prime $p \geq 3$. Moreover, let $E(\mathbb{F}_q)$ be the Mordell-Weil group of the rational points over $\mathbb{F}_q$ of an elliptic curve E.

Lemma 3.1. *Let* E *be an elliptic curve defined over the field* $\mathbb{F}_q$ *with* q *elements, where* q *is a power of* p*. Then* $|\#E(\mathbb{F}_q) - q - 1| \leq 2\sqrt{q}$.

Proof. This result was conjectured by Artin and was proved by Hasse in 1930. See, for example, [23, V, Theorem 1.1]. ∎

Remark 3.1. Now we can describe how from any equation of type (1) it is possible to construct a non degenerate elliptic curve E of degree $d \geq 3$ in $\mathbb{P}^n$ over a field K of characteristic $p \geq 3$ such that $p+1-2\sqrt{p} > d(d+2-n)+1$. The regularity of an irreducible non degenerate curve of degree d in $\mathbb{P}^n$ is lower than or equal to $d+2-n$ [10]. Hence, by Lemma 2.2 and by the availability of algorithms that compute generators of ideals of points, it is possible to determine the ideal of the curve from a set of $d(d+2-n)+1$ distinct points of the curve. So, it is enough to construct $d(d+2-n)+1$ distinct points of E. Note that by Lemma 3.1 it is $\#E(K) \geq p+1-2\sqrt{p}$. Hence over a field K of characteristic p such that $p+1-2\sqrt{p} > d(d+2-n)+1$, an elliptic curve represented by (1) has at least $d(d+2-n)+1$ distinct rational points. So, if we evaluate the polynomial $x(x-1)(x-\lambda)$ on every $\bar{x}$ of F_p and then we compare the result with the evaluation of y^2 on every $\bar{y}$ of F_p, we must find at least $d(d+2-n)+1$ points $(\bar{x},\bar{y})$ of $\mathbb{A}^2$ that belong to E. Let $f_0(y_0,y_1,y_2),\ldots,f_n(y_0,y_1,y_2)$ be $n+1$ polynomials of degree $\bar{d}$ with no common zeros in $\mathbb{P}^2$; they define a birational map $\phi:\mathbb{P}^2\to X\subset\mathbb{P}^n$ into a surface X of $\mathbb{P}^n$. The image of the projective closure of a curve (1) by ϕ is a curve of geometric genus 1. We put $\bar{d}=d/3$ if $d\equiv 0 \pmod 3$, otherwise $\bar{d}=d/3+1$. Moreover, if $d\equiv 2 \pmod 3$, we make all the polynomials f_i to have a null coefficient of $y_2^{\bar{d}}$ (the unique point at infinity of the curve (1) becomes a base point of the map), and if $d\equiv 1 \pmod 3$ also the coefficient of $y_0^{\bar{d}}$ are null (the origin becomes a base point of the map). In this way, when it is necessary we put enough base points in the rational map so that the curve through the images of the computed points of the curve (1) is an elliptic curve of degree d.

Hence, if we want to determine elliptic curves of any degree d in $\mathbb{P}^n$ we need to compute enough rational points on a curve of type (1) and to take a suitable rational map. About the computation of the points, it is enough to choose the characteristic p of the field as it is suggested in Lemma 3.1. About the rational map, we take random coefficients for the polynomials f_i and then we impose the conditions on base points described in Remark 3.1. So now we can formulate the following algorithm, where E_i is an elliptic curve, n_i is the minimum degree of a linear variety that contains the curve E_i and m_i is an upper bound for the regularity of E_i, as it is proved in [10].

ALGORITHM

Input: number s of the irreducible components $E_1,\ldots,E_s$ of a curve E and their degrees $d_1,\ldots,d_s$; characteristic $p\geq 3$ of the field K.

Output: if the variable q is false, then the characteristic of the field is too low for a successful computation. Otherwise, the output consists of a minimal set of homogeneous generators of the ideal of the curve $I(E)$, the Hilbert function $H_E(t)$, the Hilbert polynomial and the Poincaré series of $I(E)$. If the Hilbert polynomial is the expected one, then the properties of maximal rank and of minimally generation of E are checked.

begin

1. set $d=\sum_{j=1}^{s} d_i$, $q=true$ and $i=0$;

2. **while** $i<s$ and $q=true$ **do**

2.1. set $i=i+1$ and $\bar{d}=d_i/3$

2.2. random choise of an equation of type (1)

2.3. **if** $d_i\not\equiv 0 \pmod 3$ **then** $\bar{d}=\bar{d}+1$ **endif**

2.4. random choise of a rational map $x_0=f_0(y_0,y_1,y_2),\ldots,x_n=f_n(y_0,y_1,y_2)$ where every f_j is a homogeneous polynomial of degree $\bar{d}$

2.5. **if** $d_i\equiv 2 \pmod 3$ **then**
set the coefficient of $y_2^{\bar{d}}$ equal to zero in all the polynomials f_i
endif

2.6. **if** $d_i\equiv 1 \pmod 3$ **then**
set the coefficients of $y_2^{\bar{d}}$ and of $y_2^{\bar{d}}$ equal to zero in all the polynomials f_i
endif

2.7. computation of a set of d_i+1 points that satisfy the equation (1) (as it is described in Remark 3.1) and of their images by the rational map; hence, determination of n_i (as it is described in Remark 3.2) and of $m_i=d_i+2-n_i$

2.8. **if** $p+1-2\sqrt{p} > d_i m_i + 1$ **then**
computation of $d_i m_i + 1$ points that satisfy the equation of type (1) that was determined in step 2.2 (see Remark 3.1) and of the set X_i of their images by the rational map
else
set $q = false$
endif
endwhile
3. **if** $q = true$ **then**
3.1. set $X = \cup_{i=1}^{h} X_t^i$ and $m = \sum_{i=1}^{h} m_i$
3.2. construction of the minimal generators of the ideal $I(X)$ and computation of the Hilbert function, the Hilbert polynomial and the Poincaré series of $I(E)$ by applying the algorithm of [4] up to degree $\alpha + 1$, if the curve has maximal rank, or with the same termination criterion as algorithm of [1]
3.3. if the Hilbert polynomial is $dt + s$, then check of the properties of maximal rank and of minimally generation by Theorem 2.2
else
3.4. print: "the chosen characteristic is too low for a successful computation"
endif

end

4. Some applications

Example 4.1. Disjoint union of elliptic curves.
By running the implementation of the above algorithm over $\mathbb{F}_p$ with $p = 32003$ we have observed the behaviour of disjoint union of space elliptic curves (see [2], expecially the introduction). It turns out that if at least one of the irreducible components is degenerate, then there are many examples of union of elliptic curves that are not minimally generated.

If we consider only non degenerate irreducible components, for every $d \leq 30$ and every n such that $3 \leq n \leq 10$ there exists always a union of $s \leq 6$ distinct non degenerate elliptic curves with maximal rank and minimally generated, except for $s = 2$ and $d_1 = d_2 = 4$ or $d_1 = d_2 = 5$ in $\mathbb{P}^3$.

It is easy to explain the first exception. In fact, if $d_1 = d_2 = 4$, each curve E_1, E_2 has maximal rank for every $t \geq 2$ by the results of [10] (each curve is complete intersection, hence projectively normal). Then $\alpha_{E_i} = 2$ and $I(E_i)$, $i = 1, 2$ has 2 minimal generators of degree 2. Hence $I(E_1 \cup E_2)$ has 4 minimal generators of degree 4. But if the maximal rank holds, then there are no more than 3 generators of degree 4.

The second exception can be proved directly by observing that any elliptic quintic curve E_i sits in 5 independent cubic surfaces, so the union E is contained in 25 sestics (1 more than the expected): if the 25 sestics are independent, the exception is proved; in fact the independence of the 25 sestics can be checked directly by computer.

One would like to get an easy geometrical description of the reason why a general union E of 2 disjoint elliptic curves in $\mathbb{P}^3$ has necessarily one minimal generator of degree 6. Observe that E has no 6-secant lines, for 3-secants to any of its components describe a surface.

Example 4.2. Existence of elliptic curves on quartic threefolds.

As an application, we show how one can use the previous algorithm to prove the existence of smooth elliptic quintic curves on a general quartic threefold in $\mathbb{P}^4$. This algorithm was used in [16], where curves over a general quartic threefold are studied extensively.

Start with a plane elliptic curve Γ as in the beginning of the algorithm and take 5 general polynomials of degree 2 with one base point on Γ; these polynomial define a map $\Gamma \to \mathbb{P}^4$; call C the image. One uses the algorithm to compute the Hilbert function of C and the generators of its ideal in $\mathbb{P}^4$. As in Proposition 2.1 one can deduce from the Hilbert function that the map is in fact an embedding of Γ as an elliptic quintic curve of maximal rank in $\mathbb{P}^4$.

The ideal of C contains some quartic element F, corresponding to a smooth quartic threefold X (see [10]). Next one considers the component $\mathcal{H}$ of the Hilbert scheme in $\mathbb{P}^4$, containing C, whose elements are quintic elliptic curves of maximal rank; then one looks at the subvariety $J \subset \mathcal{H} \times H^0(\mathcal{O}_{\mathbb{P}^4}(4))$ of all pairs (C', F') such that C' lies in the threefold defined by F'. The goal is to prove that J dominates $H^0(\mathcal{O}_{\mathbb{P}^4}(4))$. J dominates $\mathcal{H}$, with fibers of dimension 42, so one computes $\dim J = 75$. It is enough to prove that a general fiber of the map $J \to H^0(\mathcal{O}_{\mathbb{P}^4}(4))$ has dimension 5, for $\dim H^0(\mathcal{O}_{\mathbb{P}^4}(4)) = 70$. So one needs to extimate the dimension of H^0 of the normal bundle N of C on X. By Riemann-Roch one gets $\dim H^0(N) = 5$ if and only if $\dim H^1(N) = 0$.

In order to see the vanishing of $H^1(N)$, it is enough to prove the vanishing of $H^1(T_{X|C})$, where $T_{X|C}$ is the restriction to C of the tangent bundle of X. Consider the exact sequence of bundles on C

$$0 \to T_{X|C} \to T_{\mathbb{P}^4|C} \to \mathcal{O}_C(4) \to 0;$$

the image of the induced map $\alpha : H^0(T_{\mathbb{P}^4|C}) \to H^0(\mathcal{O}_C(4))$ is generated by the 5 derivatives of the equation F, modulo the ideal of C (the Jacobian ideal of F mod C). Since $H^1(T_{\mathbb{P}^4|C}) = 0$, it is enough to show that α surjects. Since $\dim(H^0(\mathcal{O}_C(4)) = 20$, one just needs to prove that the ideal of C intersects the ideal generated by the derivatives of F, in degree 4, in a vector space of dimension 5.

Once the algorithm provides the equations of C, this last computation is a straightforward application of Groebner bases calculus that can be made by many softwares dedicated to symbolic computation. All the computations were performed over the finite field $\mathbb{F}_p$ with $p = 32003$ and the output was as expected.

Observe that all the previous computations can be performed in positive characteristic and the output is valid over the complex field. Indeed the curve Γ exists in any characteristic, so does C. We only compute the generators for the ideal of C in some positive characteristic p, but they correspond, mod p, to the equations of C in characteristic 0.

Remark 4.1. Problems arise in attempting to apply directly the procedure that we described in section 3 to obtain results also over the rational field $\mathbb{Q}$.

Indeed we need to check that the elliptic curve E has "enough" rational points over $\mathbb{Q}$. Recall that the set $E(K)$ of the rational points of an elliptic curve over $K = \mathbb{Q}$ can be structured as an abelian algebraic group that is always finitely generated by a theorem of Mordell (for example, see [23]). In fact, it is $E(\mathbb{Q}) = E(\mathbb{Q})_{tors} \oplus \mathbb{Z}^r$, where r is called rank of the curve. Since the number of points with finite order is at most 16 [17], the curve has infinite rational points if, and only if, its rank is at least 1. The question of deciding whether the curve has positive rank is still open. However, there are many results about the rank of an elliptic curve and there are many examples of curves with infinitely many rational points. So, to study elliptic curves over $\mathbb{Q}$ it is enough to apply the described algorithm to a plane elliptic curve that is known to have positive rank (for some example of such a curve see [23] and for a very recent result see [25]).

References

1. G. Albano, F. Cioffi, F. Orecchia, I. Ramella (2000). Minimally generating ideals of rational parametric curves in polynomial time. *J. Symbolic Computation* **30**, n. 2, 137-149.
2. E. Ballico (1986). On the postulation of disjoint rational curves in a projective space, *Rend. Sem. Mat. Univers. Politecn. Torino* **44**, 207-249.
3. E. Ballico, Ph. Ellia (1987). The Maximal Rank Conjecture for Non-Special Curves in $\mathbb{P}^n$, *Math. Z.* **196**, 355-367.
4. F. Cioffi (1999). Minimally generating ideals of points in polynomial time using linear algebra, *Ricerche di Matematica* **XLVIII**, Fasc. 1, 55-63.
5. H. Cohen (1995). *A Course in Computational Algebraic Number Theory.* GTM 138, Springer Verlag.
6. J. Cremona (1992). *Algorithms for Modular Elliptics Curves*, Cambridge University Press.
7. H. Clemens (1986). Curves in generic hypersurfaces, *Ann. Sup. Sc. Ecole Norm. Sup.* **19**, 629-636.
8. H. Darmon (1999). A Proof of the Full Shimura-Taniyama-Weil Conjecture is Announced. Research News in *Notices of AMS*, Vol. 46, N. 11, 1397-1401.
9. M. Green (1996). Generic Initial Ideals. In: *Six Lectures on Commutative Algebra*, Progress in Mathematics 166, Birkhäuser Verlag.
10. L. Gruson, R. Lazarsfeld, C. Peskine (1983). On a Theorem of Castelnuovo and the Equations Defining Space Curves, *Invent. math.* **72**, 491-506.
11. R. Hartshorne, A. Hirschowitz (1982). Droites en position générale dans l'espace projectif, *Lect.Notes Math.* **961**, 169-189.
12. M. Idá,(1990). On the homogeneous ideal of the generic union of s-lines in $\mathbb{P}^3$ *J. Reine Angew. Math.* **403**, 67-153.
13. T. Johnsen T., S. Kleiman (1996) Rational curves of degree at most 9 on a general quintic threefold, *Comm. Alg.* **24**, 2721-2753.
14. H.P. Kley (2000) Rigid curves in complete intersection Calabi-Yau threefolds, *Comm. Alg.* to appear.
15. J.O. Kleppe, R.M. Miró-Roig (1998) The dimension of the Hilbert scheme of Gorenstein codimension 3 subschemes, *J. Pure Appl. Alg.* **127**, 73-82.
16. C. Madonna (2000). Rank 2 vector bundles on general quartic hypersurfaces in $\mathbb{P}^4$, *preprint.*
17. B. Mazur (1978). Rational isogenies of prime degree, *Invent. Math.* **44**, 129-162.
18. J. Migliore (1998). *Introduction to Liaison Theory and Deficiency Modules.* Progress in Mathematics 165, Birkhäuser.
19. D. Mumford (1966). *Lectures on curves on an algebraic surface.* Ann. of Math. Studies **59**.
20. U. Nagel (1990). On Castelnuovo's regularity and Hilbert functions. *Compositio Mathematica* **76**, 265-275.
21. F. Orecchia (2001). The ideal generation conjecture for s general rational curves in $\mathbb{P}^r$. *Journal of Pure and Applied Algebra* **155**, 77-89.
22. V. Shoup (1999). NTL: a Library for doing Number Theory, version 3.9b, available at `http://www.shoup.net/ntl`.
23. J. Silverman (1986). *The Arithmetic of Elliptic Curves.* GTM 106, Springer Verlag.
24. J. Silverman, J. Tate (1992). *Rational Points on Elliptic Curves.* UTM 56, Springer Verlag.
25. H. Yamagishi (1999). A unified method of construction of elliptic curves with high Mordell-Weil rank, *Pacific J. Math.* **191**, No. 1, 189-200.