THE HIGHER SECANT VARIETIES OF AN ELLIPTIC NORMAL CURVE

TOM FISHER

Abstract. We study the higher secant varieties of an elliptic normal curve, determining the form of their minimal free resolutions and classifying their determinantal presentations.

1. Introduction

We work over an algebraically closed field k of arbitrary characteristic. An elliptic normal curve $C \subset \mathbb{P}^{n-1}$ is a smooth curve of genus one and degree n that is contained in no hyperplane. The rth higher secant variety $\mathrm{Sec}^r C$ is the Zariski closure of the locus of all $(r-1)$-planes spanned by r points of C. It is shown in [L] that $\mathrm{Sec}^r C$ is an irreducible variety of codimension $\max(n-2r, 0)$.

Let $R = k[x_1, \ldots, x_n]$ be the homogeneous co-ordinate ring of $\mathbb{P}^{n-1}$. For $M = \oplus M_d$ a graded R-module we write $M(c)$ for the graded R-module with $M(c)_d = M_{c+d}$. We give a new proof of the following theorem that was recently proved independently by Graf v. Bothmer and Hulek [vBH].

Theorem 1.1. *Let $C \subset \mathbb{P}^{n-1}$ be an elliptic normal curve of degree n. Let $m = n - 2r$. If $m \geq 1$ then the homogeneous co-ordinate ring of $\mathrm{Sec}^r C$ has a minimal graded free resolution of the form*

$$0 \to R(-n) \to R(-n+r+1)^{b_{m-1}} \to R(-n+r+2)^{b_{m-2}} \to \ldots$$
$$\ldots \to R(-r-2)^{b_2} \to R(-r-1)^{b_1} \to R \to 0.$$

In particular $\mathrm{Sec}^r C$ is projectively Gorenstein of codimension m.

Our proof is different from that given in [vBH, §8] in that we build the minimal free resolutions by induction on r and n. The induction step is closely related to a technique of Kustin and Miller [KM, Theorem 1.5] for constructing new Gorenstein ideals from old. This approach provides additional information that is essential to our subsequent work on Pfaffian presentations of elliptic normal curves [F2]. It also serves as a prototype for our forthcoming work on the the minimisation of

Date: 30th May 2006.

genus one curves. In this application we use the main results of [CS] and [F1] to start the induction.

A great deal of information may be read off from Theorem 1.1. If $m \geq 2$ then the theorem is equivalent to the statement that the homogeneous co-ordinate ring of $\mathrm{Sec}^r C$ is an extremal Gorenstein ring (in the sense of Schenzel [S]) with a-invariant 0. As we recall in §2, the Betti numbers, Hilbert series and Hilbert polynomial of an extremal Gorenstein ring are explicitly known. For instance we deduce that if $n - 2r \geq 1$ then $\mathrm{Sec}^r C$ has degree

$$\beta(r,n) = \binom{n-r}{r} + \binom{n-r-1}{r-1} = \frac{n(n-r-1)!}{r!(n-2r)!}. \tag{1}$$

Alternative proofs are given in [Ro, §9.3] and [vBH, Proposition 8.5]. The numbers $\beta(r,n)$ are most conveniently thought of as the number of ways of choosing r elements from $\mathbb{Z}/n\mathbb{Z}$ such that no two elements are adjacent. The expression as a sum of binomial coefficients is found by considering the subsets that do or do not contain a given element.

We call a homogeneous polynomial of degree r an r-ic. Theorem 1.1 has the following consequence.

Theorem 1.2. *Let $C \subset \mathbb{P}^{n-1}$ be an elliptic normal curve of degree n. The space of $(r+1)$-ics containing $\mathrm{Sec}^r C$ has dimension $\beta(r+1,n)$. If $n-2r \geq 2$ then these $(r+1)$-ics generate the homogeneous ideal of $\mathrm{Sec}^r C$.*

In fact we prove Theorem 1.2 first, and then use it in the proof of Theorem 1.1. Both proofs are by induction on r and n, and are guided by the recurrence relation

$$\beta(r+1,n) = \beta(r+1,n-1) + \beta(r,n-2).$$

We adapt the proof of Theorem 1.2 to give the following result on determinantal presentations. First we fix some notation. We write $\mathcal{L}(D) = H^0(C, \mathcal{O}(D))$ for the Riemann-Roch space associated to a divisor D on C. Let H be the divisor of a hyperplane section, and let D_1, D_2 be divisors on C with $D_1 + D_2 = H$. We write $\Phi(D_1, D_2)$ for the matrix of linear forms representing the multiplication map

$$\mathcal{L}(D_1) \times \mathcal{L}(D_2) \to \mathcal{L}(H).$$

It is clear that $\Phi(D_1, D_2)$ has rank at most 1 on C, and so has rank at most r on $\mathrm{Sec}^r C$. We write $I(X)$ for the homogeneous ideal of a projective variety X.

Definition 1.3. A matrix of linear forms is a *determinantal presentation* of $\mathrm{Sec}^r C$ if its $(r+1) \times (r+1)$ minors generate $I(\mathrm{Sec}^r C)$.

Determinantal presentations for curves of arbitrary genus have been studied in [EKS]. A set-theoretic generalisation to higher secant varieties is given in [Ra]. In §10 we establish the following analogue of the main result of [EKS].

Theorem 1.4. *Let $n \geq 2r+1$. Then $\Phi(D_1, D_2)$ is a determinantal presentation of $\mathrm{Sec}^r C$ if and only if*
(i) $\deg D_1, \deg D_2 \geq r+2$, *and*
(ii) if $\deg D_1 = \deg D_2 = r+2$ *then* $D_1 \not\sim D_2$.

An easy corollary of Theorem 1.4 is that if $n \geq 2r+1$ then $\mathrm{Sec}^r C$ has singular locus $\mathrm{Sec}^{r-1} C$. It follows that an elliptic normal curve is uniquely determined by any one of its higher secant varieties that is not the whole of projective space. Since the method is closely related to that given in [vBH, Proposition 8.15] we omit the details. The case $r = 2$ was previously treated in [GP, Proposition 5.1].

If $r = 1$ then $\mathrm{Sec}^r C = C$. Theorems 1.1 and 1.2 are well known in this case. Theorem 1.1 is stated in [GP, Theorem 5.5] and supported by a reference to [E, Exercise A2.22]. It can also be deduced from the fact C has trivial canonical sheaf. Theorem 1.2 asserts that the space of quadrics vanishing on an elliptic normal curve of degree $n \geq 3$ has dimension $n(n-3)/2$, and that if $n \geq 4$ then these quadrics generate the homogeneous ideal. Generalisations are known both for curves of genus g [M, Corollary to Theorem 8], and for abelian varieties [LB, Chapter 7, Section 4]. The statement that an elliptic normal curve of degree $n \geq 4$ is defined by quadrics is proved in [H, IV.1.3].

If $r = 2$ then $\mathrm{Sec}^2 C = \mathrm{Sec}\, C$ is the ordinary secant variety. In this case, it is shown in [GP, Theorem 5.5] that Theorem 1.1 holds for all but finitely many j-invariants. They compute the degree of the secant variety by the following method, of which [vBH, Proposition 8.5] is a generalisation. Projecting C away from a general $(n-4)$-plane we obtain a plane curve C' with d nodes. Then computing the arithmetic genus of C' in two different ways gives $d + 1 = (n-1)(n-2)/2$. So $\mathrm{Sec}\, C$ has degree $d = n(n-3)/2 = \beta(2, n)$ as claimed.

The special cases where $\mathrm{Sec}^r C \subset \mathbb{P}^{n-1}$ has small codimension are also of interest.

If $m = 1$ then Theorem 1.1 asserts that $\mathrm{Sec}^r C$ is a hypersurface of degree n. This was previously known when the characteristic of k does not divide n. (The proof for $n = 7$ given in [GP, Example 2.10] generalises immediately.) We remove this restriction on the characteristic.

If $m = 2$ then Theorem 1.1 asserts that $\mathrm{Sec}^r C$ is the complete intersection of two $(r+1)$-ics. This is a result of Room (see §7).

If $m = 3$ then Theorem 1.1 asserts that the homogeneous ideal $I = I(\mathrm{Sec}^r C)$ is Gorenstein of codimension 3, and that I is generated by a space of $(r+1)$-ics of dimension n. By the Buchsbaum-Eisenbud structure theorem [BE1], [BE2] we can write these $(r+1)$-ics as the submaximal Pfaffians of an $n \times n$ alternating matrix of linear forms on $\mathbb{P}^{n-1}$. This application, explained further in [F2], was the motivation for the present work.

Let us also note that our practical algorithm for computing the Jacobian of an elliptic normal curve of degree 5 (see [F3]) relies on a geometric "accident" that we initially checked by a generic calculation over the modular curve $X(5)$, but is explained here in Corollary 7.5. This application is of course an arithmetic one, since over an algebraically closed field a smooth curve of genus one is its own Jacobian.

The plan of the paper is as follows. In §2 we give the necessary background on extremal Gorenstein ideals. (This will only be needed in §§3,9.) The results of Gross and Popescu [GP] in the case $r = 2$ were obtained by letting an elliptic normal curve degenerate to a Néron polygon. We give details in §3. In §4 we make some general remarks on higher secant varieties. Then in §§5,6 we restrict to the case of an elliptic normal curve and prove the first part of Theorem 1.2. The second part of Theorem 1.2 is proved in §§7,8. Finally in §9 and §10 we present our proofs of Theorem 1.1 and Theorem 1.4.

2. Extremal Gorenstein ideals

Let $R = k[x_1, \ldots, x_n]$ be the homogeneous co-ordinate ring of $\mathbb{P}^{n-1}$. Let $R_+ = \oplus_{d \geq 1} R_d$ be the irrelevant ideal and let M be a finitely generated graded R-module.

Definition 2.1. A graded free resolution of M is a complex of graded free R-modules

$$F_\bullet : \qquad \ldots \longrightarrow F_2 \xrightarrow{\phi_2} F_1 \xrightarrow{\phi_1} F_0 \longrightarrow 0$$

that is exact except at F_0 where the homology is M. The resolution $F_\bullet$ is called minimal if $\phi_i(F_i) \subset R_+ F_{i-1}$ for all i.

Lemma 2.2. *Let $F_\bullet$ be a minimal graded free resolution of M. Then any graded free resolution of M is a direct sum of $F_\bullet$ and a trivial complex. In particular minimal resolutions are unique up to isomorphism.*

Proof: See [E, §20.1]. □

The common length of all minimal resolutions is called the projective dimension of M and denoted $\operatorname{proj\,dim} M$. Hilbert's syzygy theorem asserts that $\text{proj dim}\, M \leq n$. We write $\operatorname{codim} I$ for the codimension, or height, of an ideal $I \subset R$. It is equal to $n - \dim R/I$.

Proposition 2.3. *Let $I \subset R$ be a homogeneous ideal. The following are equivalent.*
(i) The quotient ring R/I is a Cohen-Macaulay ring.
(ii) $\text{proj dim}\, R/I = \operatorname{codim} I$.

PROOF: This follows from [BH, Corollary 2.2.15] or the graded analogue of [E, Corollary 19.5]. □

Definition 2.4. If the conditions of Proposition 2.3 are satisfied then we say that I is a perfect ideal.

Proposition 2.5. *Let $I \subset R$ be a perfect ideal with minimal graded free resolution*

$$F_\bullet : \qquad 0 \to F_m \to F_{m-1} \to \ldots \to F_1 \to F_0 \to 0.$$

The following are equivalent.
(i) The quotient ring R/I is a Gorenstein ring.
(ii) The graded free R-module F_m has rank 1.
(iii) The complex of free R-modules $F_\bullet$ is self-dual.

PROOF: This is the graded analogue of [E, Corollary 21.16]. □

Definition 2.6. If the conditions of Proposition 2.5 are satisfied then we say that I is a Gorenstein ideal.

We recall from [BH, Definition 4.4.4]:

Definition 2.7. Let $I \subset R$ be a homogeneous ideal. The a-invariant $a(R/I)$ is the degree of the Hilbert series of R/I viewed as a rational function.

Lemma 2.8. *Let $I \subset R$ be a Gorenstein ideal of codimension $m \geq 2$ with $I_d = 0$ for all $d \leq r$. Then*

$$a(R/I) \geq m + 2r - n.$$

In the case of equality I is generated in degree $r + 1$.

PROOF: Let R/I have minimal graded free resolution

$$F_\bullet : \qquad 0 \to F_m \to F_{m-1} \to \ldots \to F_1 \to F_0 \to 0.$$

Let d_i be the smallest integer such that $R(-d_i)$ appears as a direct summand of F_i. Since $F_\bullet$ is a minimal resolution the sequence $d_1, d_2, \ldots, d_m$ is strictly increasing. We are given that $d_1 \geq r+1$. Since $F_\bullet$ is self-dual it follows that $d_m \geq d_{m-1} + (r + 1)$. Thus $d_m \geq m + 2r$. Using this resolution to compute the Hilbert series we find

$$a(R/I) = d_m - n \geq m + 2r - n.$$

In the case of equality we have $d_i + d_{m-i} = m + 2r$ for all $0 \le i \le m$. Then since $F_\bullet$ is self-dual it must also be pure, i.e. each F_i is a direct sum of copies of $R(-d_i)$. In particular I is generated in degree $d_1 = r + 1$. □

Definition 2.9. If equality holds in Lemma 2.8 then we say that I is an extremal Gorenstein ideal, and that R/I is an extremal Gorenstein ring.

It is shown in [BH, Proposition 4.1.12] that the a-invariant is the largest integer for which the Hilbert function and Hilbert polynomial differ. So our definition of an extremal Gorenstein ring is equivalent to that originally made by Schenzel. The numerical properties of an extremal Gorenstein ring were determined by Schenzel [S, Theorem B]. We rewrite some of his expressions using the numbers $\beta(r, n)$ defined in the introduction.

Proposition 2.10. *Let $I \subset R$ be an extremal Gorenstein ideal of codimension m, generated in degree $r + 1$. Let $a = a(R/I) = m + 2r - n$.*
(i) The minimal graded free resolution of R/I takes the form

$$0 \to R(-m-2r) \to R(-m-r+1)^{b_{m-1}} \to R(-m-r+2)^{b_{m-2}} \to \dots$$
$$\dots \to R(-r-2)^{b_2} \to R(-r-1)^{b_1} \to R \to 0.$$

(ii) The Betti numbers $b_i = b_i(r, m)$ are given by

$$b_i(r,m) = \frac{1}{r!} . \frac{m+2r}{(i+r)(m-i+r)} . \frac{(m+r-1)!}{(i-1)!(m-i-1)!}.$$

In particular I_{r+1} has dimension $b_1(r, m) = \beta(r + 1, n + a)$.
(iii) The Hilbert series of R/I is

$$h(t) = (1-t)^a \sum_{\rho=0}^{r} \beta(\rho, n+a) t^\rho / (1-t)^{2\rho}.$$

(iv) The Hilbert polynomial of R/I is

$$H(d) = \sum_{\rho=0}^{r} \beta(\rho, n+a) \binom{d+\rho-a-1}{2\rho-a-1}.$$

In particular R/I has multiplicity $\beta(r, n + a)$.

Proof: (i) This is a consequence of equality in Lemma 2.8.
(ii) By [BH, Theorem 4.1.15(a)] we have

$$b_i(r,m) = \frac{m+2r}{m+r-i} \prod_{j=r+1, j \neq r+i}^{m+r-1} \frac{j}{|r+i-j|}.$$

(iii) The Hilbert series of R/I is

$$h(t) = \big(1 + \sum_{i=1}^{m-1} (-1)^i b_i t^{r+i} + (-1)^m t^{m+2r}\big)/(1-t)^n.$$

Since $b_i(0,m) = \binom{m}{i}$, this reduces in the case $r = 0$ to

$$h(t) = (1-t)^{m-n} = (1-t)^a.$$

The general case follows by induction on r using the identity

$$b_i(r,m) + b_{i+1}(r-1, m+2) = \beta(r, m+2r)\binom{m}{i}.$$

(iv) This follows from (iii) and the binomial theorem. □

Remark 2.11. Schenzel [S] takes the proof in a different order, leading to different (but of course equivalent) expressions. By reducing to the zero-dimensional case he computes the Hilbert series as

$$h(t) = \sum_{\rho=-r}^{r} \binom{m-1-r+|\rho|}{m-1} t^{r+\rho}/(1-t)^{n-m}.$$

He then computes the Betti numbers from the Hilbert series, and leaves the answer in terms of binomial coefficients.

If $n - 2r \geq 2$ then Theorem 1.1 is equivalent to the statement that the homogeneous co-ordinate ring of $\mathrm{Sec}^r C$ is an extremal Gorenstein ring with a-invariant 0. The Hilbert series, Hilbert function and degree of $\mathrm{Sec}^r C$ are found by setting $a = 0$ in the above formulae. In particular Theorem 1.2 may be deduced from Theorem 1.1.

3. Néron polygons and cyclic polytopes

Definition 3.1. Let $n \geq 3$ be an integer. A *Néron polygon* $C \subset \mathbb{P}^{n-1}$ of degree n is the union of n lines $\ell_1, \ldots, \ell_n$ spanning $\mathbb{P}^{n-1}$ and arranged such that ℓ_i meets ℓ_j if and only if $i - j \equiv \pm 1 \pmod{n}$.

It is well known that Néron polygons arise as degenerations of elliptic normal curves. In this section we show, following [GP], that Theorems 1.1 and 1.2 hold when C is replaced by a Néron polygon. This provides a valuable heuristic and explains the appearance of the numbers $\beta(r,n)$. However our proofs of Theorems 1.1 and 1.2 are independent of the results in this section.

Let $\mathbb{P}^{n-1}$ have co-ordinates $(x_1 : \ldots : x_n)$, where the subscripts are read modulo n. Let Γ_n be the standard Néron polygon, that is to say, with vertices $P_1 = (1 : 0 : 0 : \ldots : 0), P_2 = (0 : 1 : 0 : \ldots : 0), \ldots, P_n =$

$(0 : 0 : \ldots : 0 : 1)$ and edges $\ell_i = P_i P_{i+1}$ for $i \in \mathbb{Z}/n\mathbb{Z}$. The following definitions are recalled from [BH, §5.1].

Definition 3.2. A simplicial complex Δ on vertex set $V = \{v_1, \ldots, v_n\}$ is a collection of subsets of V, called faces, such that
(i) If $F \in \Delta$ and $G \subset F$ then $G \in \Delta$.
(ii) All singleton sets $\{v_i\}$ belong to Δ.

Definition 3.3. Let Δ be a simplicial complex on vertex set $\{1, \ldots, n\}$. The Stanley-Reisner ring of Δ is $k[\Delta] = k[x_1, \ldots, x_n]/I_\Delta$ where I_Δ is the ideal generated by all monomials $\prod_{i \in F} x_i$ with $F \notin \Delta$.

For $r \geq 1$ and $n \geq 2r + 1$ we put

$$\Delta_{r,n} = \{A \subset \mathbb{Z}/n\mathbb{Z} : A \subset B \cup (1 + B) \text{ for some } |B| \leq r\}.$$

Then $\Delta_{r,n}$ is a simplicial complex on vertex set $\mathbb{Z}/n\mathbb{Z}$ and $k[\Delta_{r,n}]$ is the homogeneous co-ordinate ring of $\text{Sec}^r \Gamma_n$.

Lemma 3.4. *Let $A \subset \mathbb{Z}/n\mathbb{Z}$ be a proper subset.*
(i) There is a unique subset $A^* \subset \mathbb{Z}/n\mathbb{Z}$ satisfying

$$A^* \subset A \subset A^* \cup (1 + A^*) \quad \textit{and} \quad A^* \cap (1 + A^*) = \emptyset.$$

(ii) $|A^*| = \min\{|B| : A \subset B \cup (1 + B)\}$.
(iii) $|A^*| = \max\{|B| : B \subset A, B \cap (1 + B) = \emptyset\}$.

Proof: (i) We may assume that $0 \notin A$. Initially we take $A^* = \emptyset$. Then for $i = 1, 2, \ldots, n-1$ we add i to A^* if $i \in A$ and $i - 1 \notin A^*$. This construction yields the unique subset A^* with the stated properties.
(ii) and (iii). It is clear that the righthand side of (iii) is at most the righthand side of (ii). The existence of A^* establishes equality. □

Lemma 3.5. *The maximal faces (facets) of $\Delta_{r,n}$ are*

$$\{B \cup (1 + B) : B \subset \mathbb{Z}/n\mathbb{Z}, |B| = r, B \cap (1 + B) = \emptyset\}.$$

In particular $\text{Sec}^r \Gamma_n$ is the union of $\beta(r, n)$ $(2r - 1)$-planes.

Proof: Since $\mathbb{Z}/n\mathbb{Z}$ is not a face we have

$$\Delta_{r,n} = \{A \subset \mathbb{Z}/n\mathbb{Z} : |A^*| \leq r\}.$$

By Lemma 3.4(ii) every maximal face A satisfies $|A^*| = r$. Since $A \subset A^* \cup (1 + A^*)$ the maximality of A then gives $A = A^* \cup (1 + A^*)$. □

If $n = 2r + 1$ then $\Delta_{r,n}$ consists of all proper subsets of $\mathbb{Z}/n\mathbb{Z}$ and $I(\text{Sec}^r \Gamma_n)$ is generated by $\prod_{i=1}^n x_i$.

Lemma 3.6. *If $n \geq 2r+2$ then the minimal non-faces of $\Delta_{r,n}$ are*

$$\{B : B \subset \mathbb{Z}/n\mathbb{Z}, |B| = r+1, B \cap (1+B) = \emptyset\}.$$

In particular $I(\mathrm{Sec}^r \Gamma_n)$ is generated by a space of $(r+1)$-ics of dimension $\beta(r+1, n)$.

PROOF: The non-faces of $\Delta_{r,n}$ are

$$\{A \subset \mathbb{Z}/n\mathbb{Z} : A = \mathbb{Z}/n\mathbb{Z} \text{ or } |A^*| \geq r+1\}.$$

Since $n \geq 2r+2$ the non-face $\mathbb{Z}/n\mathbb{Z}$ is not minimal. By Lemma 3.4(iii) every minimal non-face A satisfies $|A^*| = r+1$. Since $A \supset A^*$ the minimality of A then gives $A = A^*$. □

Lemma 3.7. *(i) The Hilbert series of $k[\Delta_{r,n}]$ is*

$$h(t) = \sum_{\rho=0}^{r} \beta(\rho, n) t^\rho / (1-t)^{2\rho}.$$

(ii) The Hilbert function of $k[\Delta_{r,n}]$ is

$$H(d) = \begin{cases} 1 & \text{if } d = 0 \\ \sum_{\rho=1}^{r} \beta(\rho, n) \binom{d+\rho-1}{2\rho-1} & \text{if } d > 0. \end{cases}$$

PROOF: The support of a monomial $m = x_1^{a_1} \dots x_n^{a_n}$ is

$$\mathrm{supp}(m) = \{i \in \mathbb{Z}/n\mathbb{Z} : a_i \neq 0\}.$$

We must count the monomials of degree d with $\mathrm{supp}(m) \in \Delta_{r,n}$. Notice that $\mathrm{supp}(m)^* = B$ if and only if m is the product of $\prod_{i \in B} x_i$ and a monomial m' with $\mathrm{supp}(m') \subset B \cup (1+B)$. So for $d \geq 1$,

$$\begin{aligned} H(d) &= \sum_{|B| \leq r, B \cap (1+B) = \emptyset} \# \left\{ m : \begin{array}{l} \deg(m) = d, \\ \mathrm{supp}(m)^* = B \end{array} \right\} \\ &= \sum_{\rho=1}^{r} \sum_{|B| = \rho, B \cap (1+B) = \emptyset} \# \left\{ m' : \begin{array}{l} \deg(m') = d - \rho, \\ \mathrm{supp}(m') \subset B \cup (1+B) \end{array} \right\} \\ &= \sum_{\rho=1}^{r} \beta(\rho, n) \binom{d+\rho-1}{2\rho-1}. \end{aligned}$$

The expression for the Hilbert series $h(t) = \sum_{d \geq 0} H(d) t^d$ follows. □

To show that $k[\Delta_{r,n}]$ is Gorenstein, we quote

Proposition 3.8. *If Δ is a simplicial complex whose geometric realisation is homeomorphic to a sphere, then $k[\Delta]$ is a Gorenstein ring.*

Proof: See [BH, Corollary 5.6.5]. □

The moment curve M_d is the image of

$$\phi_d : \mathbb{R} \to \mathbb{R}^d; t \mapsto (t, t^2, \ldots, t^d).$$

Definition 3.9. Let $2 \le d \le n-1$. The cyclic polytope $C(n,d)$ is the convex hull of any n distinct points on the moment curve M_d.

Lemma 3.10. *The vertex scheme of $C(n,2r)$ is isomorphic (as a simplicial complex) to $\Delta_{r,n}$.*

Proof: Let $C(n,2r)$ be the convex hull of the points $\phi_d(\tau_i)$ with $\tau_1 < \tau_2 < \ldots < \tau_n$. By [BH, 5.2.7, 5.2.10] the vertex scheme of $C(n,2r)$ is a simplicial complex on $V = \{\phi_d(\tau_i) : 1 \le i \le n\}$. We identify the vertex sets V and $\mathbb{Z}/n\mathbb{Z}$ via $\phi_d(\tau_i) \leftrightarrow i$. The lemma now follows from the descriptions of the maximal faces (facets) given in Lemma 3.5 and [BH, Theorem 5.2.11]. □

It follows by Proposition 3.8 and Lemma 3.10 that $k[\Delta_{r,n}]$ is a Gorenstein ring. Let $m = n - 2r$ and suppose that $m \ge 2$. We saw in Lemmas 3.5 and 3.6 that $I(\mathrm{Sec}^r \Gamma_n)$ has codimension m and is generated in degree $r+1$. It is clear from the Hilbert series, computed in Lemma 3.7, that $k[\Delta_{r,n}]$ has a-invariant 0. This gives equality in Lemma 2.8, so $k[\Delta_{r,n}]$ is an extremal Gorenstein ring. The analogue of Theorem 1.1 for Néron polygons now follows from Proposition 2.10(i).

4. Higher secant varieties

Let $C \subset \mathbb{P}^{n-1}$ be any variety. The rth higher secant variety $\mathrm{Sec}^r C$ is the Zariski closure of the locus of all $(r-1)$-planes spanned by r points of C.

Proposition 4.1 (Lange). *Let $C \subset \mathbb{P}^{n-1}$ be an irreducible curve contained in no hyperplane. Then $\mathrm{Sec}^r C$ is an irreducible variety of dimension $\min(2r-1, n-1)$.*

Proof: See [L]. □

For future reference, we outline a proof of Proposition 4.1 in the case C is an elliptic normal curve. Let H be the divisor of a hyperplane section. For D an effective divisor on C we write $\overline{D}$ for the linear subspace of $\mathbb{P}^{n-1}$ cut out by $\mathcal{L}(H - D) \subset \mathcal{L}(H)$. If D is a sum of distinct points then $\overline{D}$ is simply the linear span of these points.

Lemma 4.2. *Let $C \subset \mathbb{P}^{n-1}$ be an elliptic normal curve of degree n, and let D, D_1, D_2 be effective divisors on C. Then* *(i)* $\dim \overline{D} = \begin{cases} \deg D - 1 & \text{if } \deg D < n \\ n-2 & \text{if } D \sim H \\ n-1 & \text{otherwise.} \end{cases}$

(ii) The linear span of $\overline{D_1}$ *and* $\overline{D_2}$ *is* $\overline{\operatorname{lcm}(D_1, D_2)}$.

(iii) $\overline{D_1} \cap \overline{D_2} = \overline{\gcd(D_1, D_2)}$ *if* $\operatorname{lcm}(D_1, D_2)$ *has degree at most* n *and is not linearly equivalent to* H.

Proof: (i) This is immediate from Riemann-Roch.

(ii) We have $\mathcal{L}(H - D_1) \cap \mathcal{L}(H - D_2) = \mathcal{L}(H - \operatorname{lcm}(D_1, D_2))$.

(iii) The inclusion "$\supset$" is clear. Equality follows by counting dimensions using (i) and (ii). □

We identify the set of effective divisors on C of degree r with the rth symmetric power $S^r C$. Let

$$Z = \{(D, P) \in S^r C \times \mathbb{P}^{n-1} | P \in \overline{D}\}$$

and write p_1, p_2 for the first and second projections. If $r < n$ then each fibre of p_1 is an $(r-1)$-plane. So $\dim Z = 2r - 1$, and $\operatorname{Sec}^r C = p_2(Z)$ is an irreducible variety of dimension at most $2r - 1$.

Let $D^\circ = \overline{D} \setminus \bigcup_{D' < D} \overline{D'}$. If $n \geq 2r + 1$ then we claim that the restriction of p_2 to the open subset

$$U = \{(D, P) \in S^r C \times \mathbb{P}^{n-1} | P \in D^\circ\}$$

is injective. Indeed if $P \in D_1^\circ \cap D_2^\circ$ for some $D_1, D_2 \in S^r C$ then Lemma 4.2(iii) gives $P \in \overline{\gcd(D_1, D_2)}$ since $\deg \operatorname{lcm}(D_1, D_2) \leq 2r < n$. It follows that $D_1 = D_2$ and this proves our claim. Hence $\operatorname{Sec}^r C$ has dimension $2r - 1$. For the case $n \leq 2r$ we still refer to [L].

We make some elementary observations concerning the homogeneous ideal of a higher secant variety.

Definition 4.3. A hypersurface $\{f = 0\} \subset \mathbb{P}^{n-1}$ contains a variety $C \subset \mathbb{P}^{n-1}$ with multiplicity r if (passing to affine co-ordinates) the Taylor expansion of f at each point $P \in C$ begins with terms of order greater than or equal to r.

Lemma 4.4. *Let* $P_1, \ldots, P_r$ *span* $\mathbb{P}^{r-1}$. *Then there are no hypersurfaces of degree* $r+1$ *containing* $\{P_1, \ldots, P_r\}$ *with multiplicity* r.

Proof: We choose co-ordinates $(x_1 : \ldots : x_r)$ on $\mathbb{P}^{r-1}$ such that $P_1 = (1 : 0 : \ldots : 0), \ldots, P_r = (0 : 0 : \ldots : 1)$. The lemma reduces to the statement that a monomial in $x_1, \ldots, x_r$ of degree $r+1$ cannot be square-free. □

Lemma 4.5. *Let $C \subset \mathbb{P}^{n-1}$ be a variety contained in no hyperplane.*
(i) There are no r-ics containing $\mathrm{Sec}^r C$.
(ii) An $(r+1)$-ic contains $\mathrm{Sec}^r C$ *if and only if it contains C with multiplicity r.*

PROOF: Let $f \in I(\mathrm{Sec}^r C)$ be a homogeneous polynomial. We choose $P_1, \ldots, P_n \in C$ spanning $\mathbb{P}^{n-1}$ and then choose co-ordinates $(x_1 : \ldots : x_n)$ on $\mathbb{P}^{n-1}$ with $P_1 = (1 : 0 : \ldots : 0), \ldots, P_n = (0 : 0 : \ldots : 1)$. Then every monomial appearing in f involves at least $r+1$ of the x_i. This proves (i). If $\deg(f) = r+1$ then f contains P_1 with multiplicity r. The first implication of (ii) follows since $P_1 \in C$ is arbitrary. Conversely if f is an $(r+1)$-ic containing C with multiplicity r, and $\Pi \simeq \mathbb{P}^{r-1}$ is spanned by r points of C, then f vanishes on Π by Lemma 4.4. By definition $\mathrm{Sec}^r C$ is the Zariski closure of the union of all such $(r-1)$-planes Π. Thus $f \in I(\mathrm{Sec}^r C)$ as required. □

Remark 4.6. If $f \in I(\mathrm{Sec}^r C)$ and $P = (a_1 : \ldots : a_n) \in C$ then it is easy to show that $\sum a_i \frac{\partial f}{\partial x_i} \in I(\mathrm{Sec}^{r-1} C)$. Since C is contained in no hyperplane we have:

$$f \in I(\mathrm{Sec}^r C) \implies \frac{\partial f}{\partial x_i} \in I(\mathrm{Sec}^{r-1} C).$$

This leads to an alternative proof of Lemma 4.5 in the case $\mathrm{char}\,(k) = 0$. See [CJ] for recent work in this area.

Corollary 4.7. *Let $C \subset \mathbb{P}^{n-1}$ be an irreducible curve contained in no hyperplane. Then any $(r+1)$-ic containing* $\mathrm{Sec}^r C$ *is irreducible.*

PROOF: We know by Proposition 4.1 that $I(\mathrm{Sec}^r C)$ is a prime ideal, and by Lemma 4.5 that it contains no r-ics. □

5. The upper bound

In this section we prove the following upper bound.

Proposition 5.1. *Let $C \subset \mathbb{P}^{n-1}$ be an elliptic normal curve of degree n. Then the space of $(r+1)$-ics containing* $\mathrm{Sec}^r C$ *has dimension at most $\beta(r+1, n)$.*

We state an elementary lemma to fix our notation.

Lemma 5.2. *Let $C_n \subset \mathbb{P}^{n-1}$ be an elliptic normal curve of degree n. Let $P \in C_n$ be any point, and choose co-ordinates $(x_1 : \ldots : x_n)$ on $\mathbb{P}^{n-1}$ such that $P = (0 : 0 : \ldots : 0 : 1)$ and $T_P C_n = \{(0 : \ldots : 0 : s : t)\}$. Let*

$$\pi_1 : \mathbb{P}^{n-1} \dashrightarrow \mathbb{P}^{n-2}; (x_1 : \ldots : x_n) \mapsto (x_1 : \ldots : x_{n-1})$$

and

$$\pi_2 : \mathbb{P}^{n-1} - \rightarrow \mathbb{P}^{n-3}; (x_1 : \ldots : x_n) \mapsto (x_1 : \ldots : x_{n-2})$$

be the projection maps away from P and $T_P C_n$. We continue to write π_1, π_2 for the morphisms obtained by restricting to C_n.
(i) If $n \geq 4$ then $C_{n-1} = \pi_1(C_n) \subset \mathbb{P}^{n-2}$ is an elliptic normal curve of degree $n-1$. Moreover $\pi_1(P) = (0 : \ldots : 0 : 1) \in \mathbb{P}^{n-2}$.
(ii) If $n \geq 5$ then $C_{n-2} = \pi_2(C_n) \subset \mathbb{P}^{n-3}$ is an elliptic normal curve of degree $n-2$.

We first prove Proposition 5.1 in the case $r = 1$.

Lemma 5.3. *Let $C \subset \mathbb{P}^{n-1}$ be an elliptic normal curve of degree n. Then the space of quadrics containing C has dimension at most $\beta(2, n) = n(n-3)/2$.*

Proof: The proof is by induction on n, the case $n = 3$ being clear. We may therefore suppose that $n \geq 4$. Let C_n and C_{n-1} be as in Lemma 5.2. Then every quadric vanishing on C_n can be written as

$$x_n g(x_1, \ldots, x_{n-2}) + h(x_1, \ldots, x_{n-1}) \tag{2}$$

where g is a linear form and h is a quadric. But it is evident that

$$I(C_n) \cap k[x_1, \ldots, x_{n-1}] = I(C_{n-1}). \tag{3}$$

These observations, combined with the induction hypothesis, show that the space of quadrics containing C_n has dimension at most

$$\beta(2, n-1) + (n-2) = \beta(2, n).$$

□

We generalise (3) and (2) to higher secant varieties.

Lemma 5.4. *Let C_n and C_{n-1} be as in Lemma 5.2.*
(i) $\mathrm{Sec}^r C_{n-1}$ is the Zariski closure of $\pi_1(\mathrm{Sec}^r C_n)$.
(ii) $I(\mathrm{Sec}^r C_n) \cap k[x_1, \ldots, x_{n-1}] = I(\mathrm{Sec}^r C_{n-1})$.

Proof: This is clear. □

Lemma 5.5. *Let C_n and C_{n-2} be as in Lemma 5.2. Let $f \in I(\mathrm{Sec}^r C_n)$ be a homogeneous polynomial and write*

$$f(x_1, \ldots, x_n) = \sum_{(i,j) \leq (p,q)} x_{n-1}^i x_n^j g_{ij}(x_1, \ldots, x_{n-2}) \tag{4}$$

where $(i, j) \leq (p, q)$ means that either $j < q$ or $j = q$ and $i \leq p$.
(i) If $r = 1$ then g_{pq} belongs to the irrelevant ideal.
(ii) If $r \geq 2$ then $g_{pq} \in I(\mathrm{Sec}^{r-1} C_{n-2})$.

PROOF: Let H be the divisor of a hyperplane section on C_n. By a standard abuse of notation we identify $x_1, \ldots, x_n$ as a basis for $\mathcal{L}(H)$. Then $\mathcal{L}(H - iP)$ has basis $x_1, \ldots, x_{n-i}$ for $i = 0, 1, 2$. In particular we have $\text{ord}_P(x_n) < \text{ord}_P(x_{n-1}) < \text{ord}_P(x_i)$ for all $1 \leq i \leq n-2$.

(i) We must show that if $\deg(f) = p + q$ then $g_{pq} = 0$. Suppose that $x^I = x_1^{i_1} \ldots x_n^{i_n}$ is a monomial appearing in f with

$$\text{ord}_P(x^I) \leq \text{ord}_P(x_{n-1}^p x_n^q). \tag{5}$$

We see from (4) that $i_n \leq q$, and from (5) that $i_n \geq q$. So $i_n = q$, and repeating the same arguments gives $i_{n-1} = p$. Thus $x_{n-1}^p x_n^q$ is the only such monomial. Since $f \in I(C_n)$ the coefficient of $x_{n-1}^p x_n^q$ must therefore be zero, *i.e.* $g_{pq} = 0$ as was to be shown.

(ii) We continue to employ the multi-index notation $x^I = x_1^{i_1} \ldots x_n^{i_n}$ and write $|I| = i_1 + \ldots + i_n$. We define homogeneous polynomials f_I via

$$f(x_1 + y_1, \ldots, x_n + y_n) \;=\; \textstyle\sum_I f_I(y_1, \ldots, y_n) x^I.$$

Fixing $(a_1 : \ldots : a_n) \in \text{Sec}^{r-1} C_n$ we put

$$\widetilde{f}(x_1, \ldots, x_n) \;=\; \textstyle\sum_{|I|=p+q} f_I(a_1, \ldots, a_n) x^I.$$

Then $\widetilde{f} \in I(C_n)$ and it follows by (i) that $g_{pq}(a_1, \ldots, a_n) = 0$. But $(a_1 : \ldots : a_n) \in \text{Sec}^{r-1} C_n$ was arbitrary. Thus

$$g_{pq} \in I(\text{Sec}^{r-1} C_n) \cap k[x_1, \ldots, x_{n-2}]$$

and we are done by a double application of Lemma 5.4(ii). □

PROOF OF PROPOSITION 5.1: The proof is by induction on r and n. The case $r = 1$ was treated in Lemma 5.3. If $n \leq 2r$ then Proposition 4.1 gives $\text{Sec}^r C = \mathbb{P}^{n-1}$ in which case the result is trivial. We may therefore suppose that $r \geq 2$ and $n \geq 2r + 1$, and that the proposition is known for all smaller values of r and n.

Let C_n, C_{n-1} and C_{n-2} as in Lemma 5.2. Let $f \in I(\text{Sec}^r C_n)$ be an $(r+1)$-ic. By Lemma 5.5(ii), and then Lemma 4.5(i) applied to $\text{Sec}^{r-1} C_{n-2}$, we have

$$f(x_1, \ldots, x_n) = x_n g(x_1, \ldots, x_{n-2}) + h(x_1, \ldots, x_{n-1})$$

where $g \in I(\text{Sec}^{r-1} C_{n-2})$ is an r-ic and $h \in k[x_1, \ldots, x_{n-1}]$ is an $(r+1)$-ic. By this observation, Lemma 5.4(ii) and the induction hypothesis, we deduce that the space of $(r+1)$-ics containing $\text{Sec}^r C_n$ has dimension at most

$$\beta(r+1, n-1) + \beta(r, n-2) = \beta(r+1, n).$$

□

6. The lower bound

We present a simplified proof of the following theorem of Knight [K].

Proposition 6.1 (Knight)**.** *Let $C \subset \mathbb{P}^{n-1}$ be an elliptic normal curve of degree n. Then the space of $(r+1)$-ics containing $\mathrm{Sec}^r C$ has dimension $\beta(r+1, n)$.*

Remark 6.2. Knight states his theorem in terms of the $(r+1)$-ics containing C with multiplicity r. By Lemma 4.5(ii) this is equivalent to our version.

Let C be any smooth projective curve, and let H be a divisor on C such that $\mathcal{L}(H)$ has basis $x_1, \ldots, x_n$. If D_1 and D_2 are divisors on C with $D_1 + D_2 = H$ then the multiplication map

$$\mathcal{L}(D_1) \times \mathcal{L}(D_2) \to \mathcal{L}(H)$$

is represented by a matrix of linear forms in $k[x_1, \ldots, x_n]$. As in the introduction, we call this matrix $\Phi(D_1, D_2)$. By the multilinearity of determinants, the linear span of the $(r+1)\times(r+1)$ minors of $\Phi(D_1, D_2)$ is independent of our choice of bases for $\mathcal{L}(D_1)$ and $\mathcal{L}(D_2)$. The following elementary observation is made in [K], [EKS]:

Lemma 6.3. *Let $C \subset \mathbb{P}^{n-1}$ be a smooth curve embedded by a complete linear system. Let D_1 and D_2 be divisors on C with $D_1 + D_2 = H$ where H is the hyperplane section. Then the $(r+1) \times (r+1)$ minors of $\Phi(D_1, D_2)$ vanish on $\mathrm{Sec}^r C$.*

Proof: The matrix $\Phi(D_1, D_2)$ has rank at most 1 on C, and so has rank at most r on $\mathrm{Sec}^r C$. $\square$

Lemma 6.4. *Let C be a smooth curve of genus one. Let H be a divisor on C of degree $n \geq 2$. Let $\mathcal{L}(H)$ have basis $x_1, \ldots, x_n$. Let V be the vector space of r-ics in $k[x_1, \ldots, x_n]$ spanned by the $r \times r$ minors of all matrices $\Phi(D_1, D_2)$ as D_1, D_2 run over all divisors on C with $D_1 + D_2 = H$ and $\deg D_1$, $\deg D_2 \geq 1$. Then $\dim V \geq \beta(r, n)$.*

Proof: We begin by treating the case $r = 1$. Let P_1 and P_2 be distinct points on C with $P_1 + P_2 \not\sim H$. Then $\mathcal{L}(H) = \mathcal{L}(H - P_1) + \mathcal{L}(H - P_2)$ is spanned by the entries of $\Phi(P_1, H - P_1)$ and $\Phi(P_2, H - P_2)$. So $\dim V = n = \beta(1, n)$ as required.

The proof is now by induction on r and n. The case $n < 2r$ is trivial since $\beta(r, n) = 0$. We may therefore suppose that $r \geq 2$ and $n \geq 2r$, and that the result is known for all smaller values of r and n.

Let $P \in C$ be any point. We may arrange that $x_1, \ldots, x_{n-i}$ is a basis for $\mathcal{L}(H - iP)$ for $i = 0, 1, 2$. Let $g(x_1, \ldots, x_{n-2})$ be an $(r-1) \times (r-1)$

minor of $\Phi(D_1, D_2)$ where $D_1+D_2 = H-2P$ and $\deg D_1, \deg D_2 \geq 1$. It is determined by $(r-1)$-dimensional subspaces $W_1 \subset \mathcal{L}(D_1)$ and $W_2 \subset \mathcal{L}(D_2)$. Since $\deg D_1, \deg D_2 \geq 1$ we may pick $w_1 \in \mathcal{L}(D_1+P) \setminus \mathcal{L}(D_1)$ and $w_2 \in \mathcal{L}(D_2+P) \setminus \mathcal{L}(D_2)$. Then $w_1 w_2 \in \mathcal{L}(H) \setminus \mathcal{L}(H-P)$. Rescaling w_1 if necessary we may assume that

$$w_1 w_2 = x_n + \ell(x_1, \ldots, x_{n-1})$$

where ℓ is a linear form. Let f be the $r \times r$ minor of $\Phi(D_1+P, D_2+P)$ determined by $W_1 \oplus \langle w_1 \rangle$ and $W_2 \oplus \langle w_2 \rangle$. Then

$$f(x_1, \ldots, x_n) = x_n g(x_1, \ldots, x_{n-2}) + h(x_1, \ldots, x_{n-1})$$

for some $h \in k[x_1, \ldots, x_{n-1}]$. This construction of f from g, combined with the induction hypothesis shows that $V \cap k[x_1, \ldots, x_{n-1}]$ is a subspace of V of codimension at least $\beta(r-1, n-2)$. But trivially, if $f(x_1, \ldots, x_{n-1})$ is an $r \times r$ minor of $\Phi(D_1, D_2)$ with $D_1 + D_2 = H - P$, then it is also an $r \times r$ minor of $\Phi(D_1, D_2 + P)$. Thus

$$\dim V \geq \beta(r, n-1) + \beta(r-1, n-2) = \beta(r, n).$$

□

Lemmas 6.3 and 6.4 show that the inequality established in Proposition 5.1 is in fact an equality. This completes our proof of Proposition 6.1.

Remark 6.5. In Knight's analogue of Lemma 6.4 he takes $H = nP$ and only considers divisors D_1 and D_2 that are multiples of P. It turns out that not all $(r+1)$-ics vanishing on $\mathrm{Sec}^r C$ arise in this way. This makes his proof of Proposition 6.1 more complicated than the one presented here.

We record two immediate corollaries of our proof.

Corollary 6.6. *Let $C \subset \mathbb{P}^{n-1}$ be an elliptic normal curve of degree n. Then the space of $(r+1)$-ics containing $\mathrm{Sec}^r C$ is generated by the $(r+1) \times (r+1)$ minors of the matrices $\Phi(D_1, D_2)$ as D_1, D_2 run over all divisors on C with $D_1 + D_2 = H$.*

Corollary 6.7. *Let C_n and C_{n-2} as in Lemma 5.2. Then for every r-ic $g \in I(\mathrm{Sec}^{r-1} C_{n-2})$ there exists an $(r+1)$-ic $h \in k[x_1, \ldots, x_{n-1}]$ such that $x_n g + h \in I(\mathrm{Sec}^r C_n)$.*

7. Complete Intersections

In this section we prove Theorem 1.1 in the cases $m = 1$ and $m = 2$. Notice that we have not yet determined the degree of $\mathrm{Sec}^r C$. Our proof for $m = 2$ follows [Ro, §§9.22-9.26].

Let $C \subset \mathbb{P}^{n-1}$ be an elliptic normal curve of degree n, with hyperplane section H. As in §4 we write $\overline{D}$ for the linear span of an effective divisor D. The following lemma is [Ro, 9.26.1].

Lemma 7.1 (Room)**.** *Let D_1, D_2 be divisors on C with $D_1 + D_2 = H$ and $\deg D_1 \le \deg D_2$. Then*

$$\{\operatorname{rank} \Phi(D_1, D_2) < \deg D_1\} \;=\; \bigcup_{D \in |D_1|} \overline{D}.$$

Proof: A point $P \in \mathbb{P}^{n-1}$ corresponds to a codimension 1 subspace $V_P \subset \mathcal{L}(H)$. If $\Phi(D_1, D_2)$ evaluated at P has rank less than $\deg D_1$ then there exists $f \in \mathcal{L}(D_1)$ such that $fg \in V_P$ for all $g \in \mathcal{L}(D_2)$. Say $(f) = D - D_1$. Then $\mathcal{L}(H - D) \subset V_P$, so $P \in \overline{D}$. The converse is obtained by reversing these steps. □

The next proposition is our version of [Ro, 9.22.1]. If $n = 2r + 2$ then we already know by Proposition 6.1 that the space of $(r + 1)$-ics vanishing on $\operatorname{Sec}^r C$ has dimension $\beta(r + 1, n) = 2$.

Proposition 7.2 (Room)**.** *Let $r \ge 1$ and $n = 2r + 2$.*
(i) If D_1, D_2 are divisors on C of degree $r + 1$ with $D_1 + D_2 = H$ then

$$\{\det \Phi(D_1, D_2) = 0\} \;=\; \bigcup_{D \in |D_1|} \overline{D} \;=\; \bigcup_{D \in |D_2|} \overline{D}.$$

(ii) If D_1, D_2 and D_1', D_2' as in (i) with $D_1 \not\sim D_1'$ and $D_1 \not\sim D_2'$ then

$$\{\det \Phi(D_1, D_2) = \det \Phi(D_1', D_2') = 0\} \;=\; \operatorname{Sec}^r C.$$

Proof: (i) This is a special case of Lemma 7.1.
(ii) By Lemma 6.3 each of these $(r+1)$-ics contains $\operatorname{Sec}^r C$. Conversely, if P belongs to the lefthand side, we know by (i) that $P \in \overline{D} \cap \overline{D'}$ for some $D \in |D_1|$ and $D' \in |D_1'|$. Then $D + D' \not\sim H$ and Lemma 4.2(iii) gives $P \in \overline{\gcd(D, D')}$. Since $D \ne D'$ it follows that $P \in \operatorname{Sec}^r C$. □

Proposition 7.2 tells us that if $\operatorname{Sec}^r C$ has codimension $m = 2$ then it is set-theoretically the intersection of two $(r + 1)$-ics, say f_1, f_2. It follows by the Nullstellensatz that

$$I(\operatorname{Sec}^r C) = \sqrt{(f_1, f_2)}. \tag{6}$$

To prove Theorem 1.1 in the case $m = 2$ we must show that $I(\operatorname{Sec}^r C) = (f_1, f_2)$. In fact we treat the case $m = 1$ at the same time. The notation C_n, C_{n-1}, C_{n-2} is recalled from Lemma 5.2.

Proposition 7.3. *Let $r \ge 1$ and $n = 2r + 2$. Then*
(i) $\operatorname{Sec}^r C_{n-1}$ is a hypersurface of degree $n - 1$.
(ii) $\operatorname{Sec}^r C_n$ is the complete intersection of two $(r + 1)$-ics.

Proof: The proof is by induction on r, the case $r = 1$ being well known. We have already seen that $I(\mathrm{Sec}^r C_n)$ contains linearly independent $(r+1)$-ics f_1, f_2. As in §5 we write

$$f_i(x_1, \ldots, x_n) = x_n g_i(x_1, \ldots, x_{n-2}) + h_i(x_1, \ldots, x_{n-1})$$

for $i = 1, 2$ where $g_1, g_2 \in I(\mathrm{Sec}^{r-1} C_{n-2})$. Lemma 5.4(ii) asserts that

$$I(\mathrm{Sec}^r C_n) \cap k[x_1, \ldots, x_{n-1}] = I(\mathrm{Sec}^r C_{n-1}). \tag{7}$$

By Proposition 6.1 this ideal contains no $(r+1)$-ics. It follows that g_1, g_2 are linearly independent. By induction hypothesis they generate $I(\mathrm{Sec}^{r-1} C_{n-2})$. Moreover g_1, g_2 are irreducible by Corollary 4.7. Thus

$$(f_1, f_2) \cap k[x_1, \ldots, x_{n-1}] = (g_1 h_2 - g_2 h_1). \tag{8}$$

From (6), (7) and (8) we deduce

$$I(\mathrm{Sec}^r C_{n-1}) = \sqrt{(g_1 h_2 - g_2 h_1)}.$$

Proposition 4.1 tells us that $\mathrm{Sec}^r C_{n-1}$ is an irreducible hypersurface, say with equation $s(x_1, \ldots, x_{n-1}) = 0$. Since s is irreducible, $g_1 h_2 - g_2 h_1$ is a power of s. But $\deg(g_1 h_2 - g_2 h_1) = 2r + 1 = n - 1$ and we know by Lemma 4.5(i) that $\deg(s) \geq r + 1$. Thus

$$I(\mathrm{Sec}^r C_{n-1}) = (g_1 h_2 - g_2 h_1) \tag{9}$$

and this completes the proof of (i).

To prove (ii) we must show that $I(\mathrm{Sec}^r C_n) = (f_1, f_2)$. We suppose, for a contradiction, that $f \in I(\mathrm{Sec}^r C_n)$ is a homogeneous polynomial with $f \notin (f_1, f_2)$. By Lemma 5.5 we have

$$f(x_1, \ldots, x_n) = \sum_{(i,j) \leq (p,q)} x_{n-1}^i x_n^j g_{ij}(x_1, \ldots, x_{n-2})$$

with $g_{pq} \in I(\mathrm{Sec}^{r-1} C_{n-2})$. We may suppose that f is chosen with (p, q) minimal. Since $I(\mathrm{Sec}^{r-1} C_{n-2})$ is generated by g_1, g_2, we can write $g_{pq} = \xi_1 g_1 + \xi_2 g_2$. If $q \geq 1$ then $f - x_{n-1}^p x_n^{q-1}(\xi_1 f_1 + \xi_2 f_2)$ contradicts our minimal choice of f. Therefore $q = 0$. So $f \in k[x_1, \ldots, x_{n-1}]$ and it follows by (7), (8), (9) that $f \in (f_1, f_2)$. This is the required contradiction. □

Remark 7.4. An alternative proof of Proposition 7.3 uses properties of the Heisenberg group in place of Proposition 7.2. It is necessary to split into cases $\mathrm{char}\,(k) \nmid (n-1)$ and $\mathrm{char}\,(k) \nmid n$. We omit the details.

We obtain a strengthening of Remark 4.6 that is of independent interest. For instance it explains why, as found in the proof of [H, VI.3.2], the quintic defining $\mathrm{Sec}\, C_5$ belongs to $I(C_5)^2$.

Corollary 7.5. *Let $r \geq 2$ and $n = 2r+2$. Let $\operatorname{Sec}^r C_{n-1}$ have equation $s(x_1, \ldots, x_{n-1}) = 0$. Then $\frac{\partial s}{\partial x_i} \in I(\operatorname{Sec}^{r-1} C_{n-1})^2$ for all i.*

Proof: Keeping the notation of the previous proof we may assume that $s = g_1 h_2 - g_2 h_1$. Then

$$\frac{\partial s}{\partial x_{n-1}} = g_1 \frac{\partial f_2}{\partial x_{n-1}} - g_2 \frac{\partial f_1}{\partial x_{n-1}}.$$

Since $f_1, f_2 \in I(\operatorname{Sec}^r C_n)$ and $g_1, g_2 \in I(\operatorname{Sec}^{r-1} C_{n-2})$, it follows by Remark 4.6 and Lemma 5.4 that $\frac{\partial s}{\partial x_{n-1}} \in I(\operatorname{Sec}^{r-1} C_{n-1})^2$. But we can make our choice of co-ordinates in Lemma 5.2 so that $\pi_1(P)$ is any point on C_{n-1}. Since C_{n-1} is contained in no hyperplane, it follows that $\frac{\partial s}{\partial x_i} \in I(\operatorname{Sec}^{r-1} C_{n-1})^2$ for all i. □

8. Proof of Theorem 1.2

Let $C \subset \mathbb{P}^{n-1}$ be an elliptic normal curve of degree n. When we write $\operatorname{Sec}^r C$ it has so far been implicit that $r \geq 1$. To avoid unnecessary repetition of our arguments we adopt the convention that if $r = 0$ then $\operatorname{Sec}^r C$ is the empty set and $I(\operatorname{Sec}^r C)$ is the irrelevant ideal. To complete the proof of Theorem 1.2 we prove

Proposition 8.1. *Let $C \subset \mathbb{P}^{n-1}$ be an elliptic normal curve of degree n, and let $r \geq 0$. If $n - 2r \geq 2$ then $I(\operatorname{Sec}^r C)$ is generated by $(r+1)$-ics.*

Proof: In view of the above convention, the case $r = 0$ is clear. The case $n = 2r+2$ was proved in Proposition 7.3(ii). We may therefore suppose that $r \geq 1$ and $n \geq 2r+3$, and that the proposition is known for all smaller values of r and n.

Let C_n, C_{n-1} and C_{n-2} as in Lemma 5.2. By induction hypothesis $I(\operatorname{Sec}^r C_{n-1})$ is generated by $(r+1)$-ics, say $f_1, \ldots, f_s$, and $I(\operatorname{Sec}^{r-1} C_{n-2})$ is generated by r-ics, say $g_1, \ldots, g_t$. By Corollary 6.7 there exist $(r+1)$-ics $h_1, \ldots, h_t \in k[x_1, \ldots, x_{n-1}]$ with $x_n g_i + h_i \in I(\operatorname{Sec}^r C_n)$. We must show that $I(\operatorname{Sec}^r C_n)$ is equal to

$$I' = (f_1, \ldots, f_s, x_n g_1 + h_1, \ldots, x_n g_t + h_t).$$

Suppose for a contradiction that $f \in I(\operatorname{Sec}^r C_n)$ is a homogeneous polynomial with $f \notin I'$. By Lemma 5.5 we have

$$f(x_1, \ldots, x_n) = \sum_{(i,j) \leq (p,q)} x_{n-1}^i x_n^j g_{ij}(x_1, \ldots, x_{n-2})$$

with $g_{pq} = \sum \xi_i g_i$. We suppose that f is chosen with (p,q) minimal. If $q \geq 1$ then $f - x_{n-1}^p x_n^{q-1} \sum \xi_i (x_n g_i + h_i)$ contradicts our minimal choice of f. Therefore $q = 0$ and

$$f \in I(\operatorname{Sec}^r C_n) \cap k[x_1, \ldots, x_{n-1}] = I(\operatorname{Sec}^r C_{n-1}) \subset I'.$$

This is the required contradiction. □

Theorem 1.2 is obtained by combining Propositions 6.1 and 8.1.

Definition 8.2. Let $\mathcal{I}$ be an ideal in a polynomial ring $\mathcal{R} = R[x]$. The leading coefficient ideal of $\mathcal{I}$ is the set of leading coefficients of elements of $\mathcal{I}$. It is an ideal in R.

Corollary 8.3. *Let $n - 2r \geq 1$ and C_n, C_{n-2} as in Lemma 5.2. If $R = k[x_1, \ldots, x_{n-1}]$ and $\mathcal{R} = R[x_n]$ then $I(\mathrm{Sec}^{r-1} C_{n-2})R$ is the leading coefficient ideal of $I(\mathrm{Sec}^r C_n)$.*

Proof: We have shown that $I(\mathrm{Sec}^{r-1} C_{n-2})$ is generated by r-ics, so by Corollary 6.7 it is contained in the leading coefficient ideal of $I(\mathrm{Sec}^r C_n)$. The inclusion of the leading coefficient ideal in $I(\mathrm{Sec}^{r-1} C_{n-2})R$ then follows by Lemma 5.5. □

9. Minimal free resoutions

The induction step in the proof of Theorem 1.1 is given by:

Proposition 9.1. *Let $r \geq 1$ and $m \geq 3$. Let I and J be extremal Gorenstein ideals in $R = k[x_1, \ldots, x_{n-1}]$. Let $\mathcal{I}$ be a prime ideal in $\mathcal{R} = R[x_n]$. Suppose that*
(i) I, J and $\mathcal{I}$ are generated in degrees $r+1$, r and $r+1$,
(ii) I, J and $\mathcal{I}$ have codimensions $m-1$, m and m,
(iii) $\mathcal{I} \cap R = I$,
(iv) J is the leading coefficient ideal of $\mathcal{I}$.
Then $\mathcal{I}$ is an extremal Gorenstein ideal.

Proof: Let R/I have minimal graded free resolution

$$F_\bullet : \qquad 0 \longrightarrow F_{m-1} \xrightarrow{\phi_{m-1}} F_{m-2} \longrightarrow \ldots \longrightarrow F_1 \xrightarrow{\phi_1} F_0 \longrightarrow 0.$$

We identify $F_0 = R$, and fix a basis $a_1, \ldots, a_s$ for F_1. Then I is generated by the $(r+1)$-ics $f_1, \ldots, f_s$ where $f_i = \phi_1(a_i)$.

Let R/J have minimal graded free resolution

$$G_\bullet : \qquad 0 \longrightarrow G_m \xrightarrow{\psi_m} G_{m-1} \longrightarrow \ldots \longrightarrow G_1 \xrightarrow{\psi_1} G_0 \longrightarrow 0.$$

We identify $G_0 = R$, and fix a basis $b_1, \ldots, b_t$ for G_1. Then J is generated by the r-ics $g_1, \ldots, g_t$ where $g_i = \psi_1(b_i)$.

By (i), (iii) and (iv) there exist $(r+1)$-ics $h_1, \ldots, h_t$ such that

$$\mathcal{I} = (f_1, \ldots, f_s, x_n g_1 + h_1, \ldots, x_n g_t + h_t). \tag{10}$$

The proof works by constructing a minimal graded free resolution of $\mathcal{R}/\mathcal{I}$. First we must define certain graded R-module maps α_i, β_i and

γ_i. Let $\alpha_1 : G_1(-1) \to F_0$ be given by $\alpha_1(b_i) = h_i$. We extend α_1 to a map of complexes

$$\begin{array}{ccccccccc} \cdots \longrightarrow & G_3(-1) & \xrightarrow{\psi_3} & G_2(-1) & \xrightarrow{\psi_2} & G_1(-1) & \xrightarrow{\psi_1} & G_0(-1) \\ & \downarrow{\scriptstyle \alpha_3} & & \downarrow{\scriptstyle \alpha_2} & & \downarrow{\scriptstyle \alpha_1} & & \\ \cdots \longrightarrow & F_2 & \xrightarrow{\phi_2} & F_1 & \xrightarrow{\phi_1} & F_0 & \longrightarrow & 0 \end{array} \tag{11}$$

The construction of α_2 is as follows. Let $e_1, \dots, e_p$ be a basis for G_2. Then $\psi_2(e_j) = \sum \xi_{ij} b_i$ for some $\xi_{ij} \in R$. Since $\psi_1\psi_2 = 0$ it follows that $\sum \xi_{ij} g_i = 0$. Then

$$\alpha_1\psi_2(e_j) = \sum \xi_{ij} h_i = \sum \xi_{ij}(x_n g_i + h_i) \in \mathcal{I} \cap R = I.$$

Since $I = \operatorname{im} \phi_1$ we can choose α_2 with $\alpha_1\psi_2 = \phi_1\alpha_2$. The remaining α_i are constructed by standard diagram chasing. (These maps are not unique.)

Lemma 9.2. *The map $\alpha_m : G_m(-1) \to F_{m-1}$ is an isomorphism.*

Proof: The graded R-modules $G_m(-1)$ and F_{m-1} are both copies of $R(-m-2r+1)$. So it suffices to show that α_m is non-zero. We suppose for a contradiction that $\alpha_m = 0$. Since I and J are Gorenstein ideals the following diagram, dual to (11), has exact rows.

$$\begin{array}{ccccccccccc} & & 0 & \longrightarrow & F_0^* & \xrightarrow{\phi_1^*} & F_1^* & \longrightarrow \cdots \longrightarrow & F_{m-2}^* & \xrightarrow{\phi_{m-1}^*} & F_{m-1}^* \\ & & & & \downarrow{\scriptstyle \alpha_1^*} & & \downarrow{\scriptstyle \alpha_2^*} & & \downarrow{\scriptstyle \alpha_{m-1}^*} & & \downarrow{\scriptstyle \alpha_m^*} \\ G_0^*(1) & \xrightarrow{\psi_1^*} & & & G_1^*(1) & \xrightarrow{\psi_2^*} & G_2^*(1) & \longrightarrow \cdots \longrightarrow & G_{m-1}^*(1) & \xrightarrow{\psi_m^*} & G_m^*(1) \end{array}$$

Since $\alpha_m^* = 0$, this map of complexes is homotopic to zero. Specifically, we construct maps $\rho_i : F_i^* \to G_i^*(1)$ with $\rho_{m-1} = 0$ and

$$\alpha_i^* = \rho_i\phi_i^* + \psi_i^*\rho_{i-1}$$

for all $i \leq m-1$. Then $\alpha_1 = \phi_1\rho_1^* + \rho_0^*\psi_1$. Since we have identified $F_0 = G_0 = R$, the map $\rho_0^* : G_0(-1) \to F_0$ is multiplication by some linear form $\ell \in R$. Then

$$\ell g_i - h_i = \rho_0^*\psi_1(b_i) - \alpha_1(b_i) = -\phi_1\rho_1^*(b_i) \in I \subset \mathcal{I}.$$

Since $x_n g_i + h_i \in \mathcal{I}$ it follows that $(\ell + x_n)g_i \in \mathcal{I}$. But $\mathcal{I}$ is a prime ideal generated by $(r+1)$-ics, so $\ell = -x_n \notin R$ and this is the required contradiction. $\square$

It follows from (iii) and (iv) that $I \subset J$. The natural map $R/I \to R/J$ extends to a map of complexes

$$\begin{array}{ccccccccc} \cdots & \longrightarrow & F_2 & \xrightarrow{\phi_2} & F_1 & \xrightarrow{\phi_1} & F_0 & \longrightarrow & 0 \\ & & \downarrow{\scriptstyle \beta_3} & & \downarrow{\scriptstyle \beta_2} & & \downarrow{\scriptstyle \beta_1} & & \\ \cdots & \longrightarrow & G_2 & \xrightarrow{\psi_2} & G_1 & \xrightarrow{\psi_1} & G_0 & \longrightarrow & 0 \end{array} \tag{12}$$

where β_1 is the identity map on $F_0 = G_0 = R$.

Composing the α_i and the β_i gives a map of complexes that we claim is homotopic to zero.

$$\begin{array}{ccccccccc} \cdots & \longrightarrow & F_3(-1) & \xrightarrow{\phi_3} & F_2(-1) & \xrightarrow{\phi_2} & F_1(-1) & \xrightarrow{\phi_1} & F_0(-1) \\ & & \downarrow{\scriptstyle \alpha_3\beta_4} & & \downarrow{\scriptstyle \alpha_2\beta_3} & & \downarrow{\scriptstyle \alpha_1\beta_2} & & \\ \cdots & \longrightarrow & F_2 & \xrightarrow[\phi_2]{} & F_1 & \xrightarrow[\phi_1]{} & F_0 & \longrightarrow & 0 \end{array}$$

Specifically, we construct $\gamma_i : F_{i-1}(-1) \to F_{i-1}$ with $\gamma_1 = 0$ and

$$\alpha_i\beta_{i+1} = \phi_i\gamma_{i+1} + \gamma_i\phi_i \tag{13}$$

for all $i \geq 1$. The construction of γ_2 is as follows. We have $\beta_2(a_j) = \sum \xi_{ij}b_i$ for some $\xi_{ij} \in R$. Then

$$f_j = \beta_1\phi_1(a_j) = \psi_1\beta_2(a_j) = \sum \xi_{ij}g_i$$

and

$$\alpha_1\beta_2(a_j) = \sum \xi_{ij}h_i = \sum \xi_{ij}(x_n g_i + h_i) - x_n f_j \in \mathcal{I} \cap R = I.$$

Since $I = \operatorname{im}\phi_1$ we can choose γ_2 with $\alpha_1\beta_2 = \phi_1\gamma_2$. The remaining γ_i are constructed by standard diagram chasing.

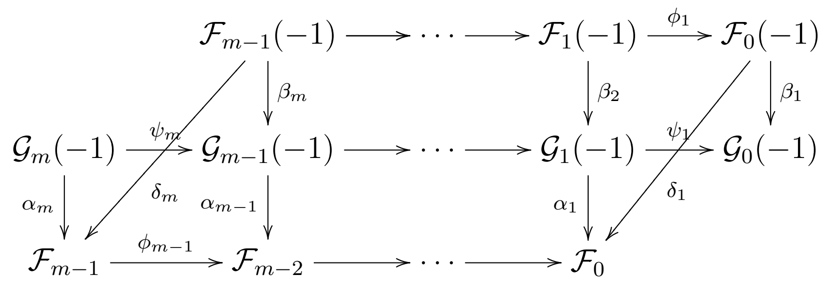
We have constructed graded R-module maps α_i, β_i and γ_i. We now pass from working over R to working over $\mathcal{R} = R[x_n]$. Let $\mathcal{F}_i = F_i \otimes_R \mathcal{R}$ and $\mathcal{G}_i = G_i \otimes_R \mathcal{R}$. We continue to write ϕ_i, ψ_i, α_i, β_i, γ_i for the extensions of these maps to the category of $\mathcal{R}$-modules. We put

$$\delta_i = \gamma_i + (-1)^i x_n : \mathcal{F}_{i-1}(-1) \to \mathcal{F}_{i-1}$$

so that (13) becomes

$$\alpha_i\beta_{i+1} = \phi_i\delta_{i+1} + \delta_i\phi_i. \tag{14}$$

We consider the diagram



and form the total complex

$$\ldots \longrightarrow \mathcal{F}_i \oplus \mathcal{G}_i(-1) \oplus \mathcal{F}_{i-1}(-1) \xrightarrow{d_i} \mathcal{F}_{i-1} \oplus \mathcal{G}_{i-1}(-1) \oplus \mathcal{F}_{i-2}(-1) \longrightarrow \ldots$$

with differential

$$d_i = \begin{pmatrix} \phi_i & \alpha_i & -\delta_i \\ 0 & -\psi_i & \beta_i \\ 0 & 0 & \phi_{i-1} \end{pmatrix}.$$

Since $\mathcal{F}_\bullet$ and $\mathcal{G}_\bullet$ are complexes, it follows from (14), and the commutativity of the diagrams (11) and (12), that $d_i d_{i+1} = 0$, *i.e.* this total complex really is a complex.

Lemma 9.3. *The total complex is a graded free resolution of $\mathcal{R}/\mathcal{I}$.*

Proof: The exactness of $\mathcal{F}_\bullet$ and $\mathcal{G}_\bullet$ gives exactness of the total complex at all terms up to and including $\mathcal{F}_2 \oplus \mathcal{G}_2(-1) \oplus \mathcal{F}_1(-1)$. It remains to consider

$$\mathcal{F}_2 \oplus \mathcal{G}_2(-1) \oplus \mathcal{F}_1(-1) \xrightarrow{d_2} \mathcal{F}_1 \oplus \mathcal{G}_1(-1) \oplus \mathcal{F}_0(-1) \xrightarrow{d_1} \mathcal{F}_0 \oplus \mathcal{G}_0(-1)$$

where $d_1(u,v,w) = (\phi_1(u) + \alpha_1(v) + x_n w, -\psi_1(v) + w)$. We must show that (i) $\operatorname{im} d_2 = \ker d_1$ and (ii) $\operatorname{coker} d_1 \simeq \mathcal{R}/\mathcal{I}$.

(i) Let $(u,v,w) \in \ker d_1$. Then

$$w = \psi_1(v) \quad \text{and} \quad \phi_1(u) + \alpha_1(v) + \psi_1(v) x_n = 0. \tag{15}$$

We must show that $(u,v,w) \in \operatorname{im} d_2$. We write

$$u = u_p x_n^p + \ldots + u_1 x_n + u_0$$

and

$$v = v_q x_n^q + \ldots + v_1 x_n + v_0$$

with $u_0, \ldots, u_p \in F_1$ and $v_0, \ldots, v_q \in G_1$. The proof is by induction on $\Delta(u,v) := \max(2p, 2q+1)$. We start the induction by noting that if $p = q = 0$ then $u \in F_1$, $v \in G_1$. So (15) gives $w = 0$, whence $(u,v,0) \in \operatorname{im} d_2$ by the exactness of $\mathcal{F}_\bullet$ and $\mathcal{G}_\bullet$.

We split the induction step into two cases. If $p > q$ we put $(u', v', w') = (u, v, w) + d_2(0, 0, u_p x_n^{p-1})$. Then $\Delta(u', v') < \Delta(u, v)$ since

$$d_2(0, 0, u_p x_n^{p-1}) = (-u_p x_n^p - \gamma_2(u_p) x_n^{p-1}, \beta_2(u_p) x_n^{p-1}, \phi_1(u_p) x_n^{p-1}).$$

If $p \leq q$ then (15) gives $\psi_1(v_q) = 0$. So $v_q = \psi_2(e)$ for some $e \in G_2$. We put $(u', v', w') = (u, v, w) + d_2(0, e x_n^q, 0)$. Then $\Delta(u', v') < \Delta(u, v)$ since

$$d_2(0, e x_n^q, 0) = (\alpha_2(e) x_n^q, -v_q x_n^q, 0).$$

(ii) We identify $\mathcal{F}_0 \oplus \mathcal{G}_0(-1) = \mathcal{R} \oplus \mathcal{R}(-1)$. Then $\operatorname{im} d_1$ is generated by the pairs $(f_i, 0)$, $(h_i, -g_i)$ and $(x_n, 1)$. It follows by (10) that

$$\operatorname{coker} d_1 = \frac{\mathcal{R} \oplus \mathcal{R}(-1)}{\operatorname{im} d_1} \simeq \mathcal{R}/\mathcal{I}.$$

□

The total complex is not minimal. This is rectified by eliminating the isomorphisms α_m and β_1. If $m \geq 4$ we put

$$d'_m = \begin{pmatrix} \beta_m - \psi_m \alpha_m^{-1} \delta_m \\ \phi_{m-1} \end{pmatrix}, \quad d'_{m-1} = \begin{pmatrix} \alpha_{m-1} & -\delta_{m-1} \\ -\psi_{m-1} & \beta_{m-1} \\ 0 & \phi_{m-2} \end{pmatrix},$$

$$d'_2 = \begin{pmatrix} \phi_2 & \alpha_2 & -\delta_2 \\ 0 & -\psi_2 & \beta_2 \end{pmatrix}, \qquad d'_1 = \begin{pmatrix} \phi_1 & \alpha_1 - \delta_1 \beta_1^{-1} \psi_1 \end{pmatrix},$$

and $d'_i = d_i$ for $3 \leq i \leq m-2$. Then $\mathcal{R}/\mathcal{I}$ has minimal graded free resolution

$$0 \longrightarrow \mathcal{F}_{m-1}(-1) \xrightarrow{d'_m} \mathcal{G}_{m-1}(-1) \oplus \mathcal{F}_{m-2}(-1) \xrightarrow{d'_{m-1}} \ldots$$
$$\ldots \longrightarrow \mathcal{F}_2 \oplus \mathcal{G}_2(-1) \oplus \mathcal{F}_1(-1) \xrightarrow{d'_2} \mathcal{F}_1 \oplus \mathcal{G}_1(-1) \xrightarrow{d'_1} \mathcal{F}_0 \longrightarrow 0.$$

The modifications for $m = 3$ are similar.

Since $\mathcal{F}_{m-1}(-1) \simeq \mathcal{R}(-m-2r)$ it follows that $\mathcal{I}$ is an extremal Gorenstein ideal. This completes the proof of Proposition 9.1. □

Proposition 9.4. *Let $C \subset \mathbb{P}^{n-1}$ be an elliptic normal curve of degree n, and let $r \geq 0$. If $n - 2r \geq 2$ then $I(\operatorname{Sec}^r C)$ is an extremal Gorenstein ideal.*

PROOF: The proof is by induction on r and n. When $r = 0$ it is understood (see §8) that $I(\operatorname{Sec}^r C)$ is the irrelevant ideal. By inspection of the Koszul complex, this is an extremal Gorenstein ideal. When $n = 2r + 2$ we saw in Proposition 7.3(ii) that $\operatorname{Sec}^r C$ is the complete intersection of two $(r+1)$-ics. So again $I(\operatorname{Sec}^r C)$ is an extremal Gorenstein ideal. We may therefore suppose that $r \geq 1$ and $n \geq 2r + 3$, and that the proposition is known for all smaller values of r and n.

Let C_n, C_{n-1} and C_{n-2} as in Lemma 5.2. Let $R = k[x_1, \ldots, x_{n-1}]$ and $\mathcal{R} = R[x_n]$. We put

$$I = I(\mathrm{Sec}^r C_{n-1}), \quad J = I(\mathrm{Sec}^{r-1} C_{n-2})R, \quad \mathcal{I} = I(\mathrm{Sec}^r C_n).$$

By induction hypothesis, I and J are extremal Gorenstein ideals. By Proposition 4.1, $\mathcal{I}$ is a prime ideal. Let $m = n-2r$. Hypotheses (i)-(iv) of Proposition 9.1 follow from Theorem 1.2, Proposition 4.1, Lemma 5.4 and Corollary 8.3. Hence $\mathcal{I}$ is an extremal Gorenstein ideal. $\square$

Theorem 1.1 follows from Proposition 7.3(i) in the case $m = 1$, and from Propositions 9.4 and 2.10 in the case $m \geq 2$.

10. Determinantal presentations

Let $C \subset \mathbb{P}^{n-1}$ be an elliptic normal curve of degree n. In the light of Theorem 1.2 we may restate Corollary 6.6 as

Lemma 10.1. *If $n \geq 2r+2$ then $I(\mathrm{Sec}^r C)$ is generated by the $(r+1) \times (r+1)$ minors of the matrices $\Phi(D_1, D_2)$ as D_1, D_2 run over all divisors on C with $D_1 + D_2 = H$.*

The aim of this section is to prove Theorem 1.4. This theorem is a variant of Lemma 10.1 giving necessary and sufficient conditions for $I(\mathrm{Sec}^r C)$ to be generated by the $(r+1) \times (r+1)$ minors of a *single* matrix $\Phi(D_1, D_2)$.

Let $C_P \subset \mathbb{P}^{n-2}$ be the elliptic normal curve of degree $n-1$ obtained by projecting away from a point $P \in C$. There is a natural inclusion $I(\mathrm{Sec}^r C_P) \subset I(\mathrm{Sec}^r C)$ where these ideals belong to different rings.

Lemma 10.2. *If $n \geq 2r+3$ then $I(\mathrm{Sec}^r C)$ is generated by the ideals $I(\mathrm{Sec}^r C_P)$ as P runs over any n distinct points on C.*

Proof: Let X be a subset of C with $|X| \geq n$. Let I be the ideal in $k[x_1, \ldots, x_n]$ generated by the $I(\mathrm{Sec}^r C_P)$ for $P \in X$. By Lemma 10.1 it suffices to show that if $D_1 + D_2 = H$ then all $(r+1) \times (r+1)$ minors of $\Phi(D_1, D_2)$ belong to I. Swapping D_1 and D_2 if necessary we may assume that $\deg D_1 \geq r+2$. Let $d = \deg D_1$. We pick distinct points $P_1, \ldots, P_d \in X$ with $D_1 \not\sim P_1 + \ldots + P_d$. Then

$$\bigcap_{i=1}^{d} \mathcal{L}(D_1 - P_i) = \mathcal{L}(D_1 - (P_1 + \ldots + P_d)) = 0.$$

So there exists a basis $v_1, \ldots, v_d$ for $\mathcal{L}(D_1)$ such that $\mathcal{L}(D_1 - P_i)$ has basis $v_1, \ldots, \widehat{v_i}, \ldots, v_d$. Then each $(r+1) \times (r+1)$ minor of $\Phi(D_1, D_2)$ is an $(r+1) \times (r+1)$ minor of $\Phi(D_1 - P_i, D_2)$ for some $1 \leq i \leq d$. We are done since the latter belong to $I(\mathrm{Sec}^r C_{P_i})$. $\square$

Remark 10.3. The proof of Lemma 10.2 shows that it would be sufficient for P to run over any $n-r$ distinct points. This improvement is irrelevant for our applications.

We obtain an alternative proof of [H, IV.1.3].

Corollary 10.4. *If* $\mathrm{char}\,(k) \neq 2$ *then the homogeneous ideal of an elliptic normal curve of degree* $n \geq 4$ *is generated by rank* 3 *quadrics.*

PROOF: By Lemma 10.2 it suffices to prove the case $n = 4$. It is well known (cf. Lemma 10.6 in the case $r = 1$) that there is a bijection between the singular fibres of the pencil of quadrics containing an elliptic normal quartic, and the 2-torsion of its Jacobian. So provided $\mathrm{char}\,(k) \neq 2$ the pencil is spanned by rank 3 quadrics. □

We make a temporary definition.

Definition 10.5. A *divisor pair* (D_1, D_2) consists of divisors D_1, D_2 on C with $D_1 + D_2 = H$ and $\deg D_1$, $\deg D_2 \geq r+1$. We say that divisor pairs (D_1, D_2) and (D_1', D_2') are equivalent if $D_1 \sim D_1'$ or $D_1 \sim D_2'$.

If $n = 2r+2$ then Theorem 1.2 asserts that $\mathrm{Sec}^r C$ is the complete intersection of two $(r+1)$-ics. We make some further observations.

Lemma 10.6. *Let* $n = 2r+2$. *Let* V *be the* 2*-dimensional vector space of* $(r+1)$*-ics generating* $I(\mathrm{Sec}^r C)$. *Then there is a bijection between the set of equivalence classes of divisor pairs and* $\mathbb{P}(V)$ *given by* $(D_1, D_2) \mapsto \det \Phi(D_1, D_2)$.

PROOF: The injectivity was shown in Proposition 7.2. For the surjectivity we may assume that C is the image of an elliptic curve $(E, 0)$ embedded by $|n.0|$. We put $D_1 = r.(0) + (P)$ and $D_2 = r.(0) + (-P)$. Then $P \mapsto \det \Phi(D_1, D_2)$ is a non-constant morphism $E \to \mathbb{P}(V) = \mathbb{P}^1$ and is therefore surjective. □

We strengthen Lemma 10.1.

Lemma 10.7. *If* $n \geq 2r+2$ *then* $I(\mathrm{Sec}^r C)$ *is generated by the* $(r+1) \times (r+1)$ *minors of* $\Phi(D_1, D_2)$ *and* $\Phi(D_1', D_2')$ *where* (D_1, D_2) *and* (D_1', D_2') *are any two inequivalent divisor pairs.*

PROOF: The proof is by induction on n. The case $n = 2r+2$ was treated in Lemma 10.6. We may therefore suppose that $n \geq 2r+3$ and $\deg D_1$, $\deg D_1' \geq r+2$. Let P run over any n distinct points on C with $D_1 - D_2' \not\sim P$. Then $(D_1 - P, D_2)$ and $(D_1' - P, D_2')$ are inequivalent divisor pairs on $C_P \subset \mathbb{P}^{n-2}$. By induction hypothesis the $(r+1) \times (r+1)$ minors of $\Phi(D_1 - P, D_2)$ and $\Phi(D_1' - P, D_2')$ generate

$I(\mathrm{Sec}^r C_P)$. Since these are submatrices of $\Phi(D_1, D_2)$ and $\Phi(D_1', D_2')$ we are done by Lemma 10.2. □

PROOF OF THEOREM 1.4: We assume that $\deg D_1$, $\deg D_2 \geq r+1$ since otherwise there are no $(r+1) \times (r+1)$ minors to consider. The proof is divided into 4 cases.

(i) Suppose that $\deg D_1, \deg D_2 \geq r+2$ and $D_1 \not\sim D_2$. Let P run over any n distinct points on C. Then $(D_1 - P, D_2)$ and $(D_1, D_2 - P)$ are inequivalent divisor pairs on $C_P \subset \mathbb{P}^{n-2}$. We know by Lemma 10.7 that $I(\mathrm{Sec}^r C_P)$ is generated by the $(r+1) \times (r+1)$ minors of $\Phi(D_1 - P, D_2)$ and $\Phi(D_1, D_2 - P)$. Since these are submatrices of $\Phi(D_1, D_2)$ we are done by Lemma 10.2.

(ii) Suppose that $\deg D_1$, $\deg D_2 \geq r+3$ and $D_1 \sim D_2$. Let P run over any n distinct points on C. We know by case (i) that $I(\mathrm{Sec}^r C_P)$ is generated by the $(r+1) \times (r+1)$ minors of $\Phi(D_1, D_2 - P)$. Since this is a submatrix of $\Phi(D_1, D_2)$ we are done by Lemma 10.2.

(iii) Suppose that $\deg D_1 = r+1$ and $\deg D_2 \geq r+1$. Then $\Phi(D_1, D_2)$ has at most $\binom{r+t+1}{t}$ linearly independent minors where

$$t = \deg D_2 - \deg D_1 = n - 2r - 2.$$

By Theorem 1.2 the vector space of $(r+1)$-ics generating $I(\mathrm{Sec}^r C)$ has dimension

$$\beta(r+1, n) = \binom{r+t+1}{t} + \binom{r+t}{t} > \binom{r+t+1}{t}.$$

Hence $\Phi(D_1, D_2)$ is not a determinantal presentation of $\mathrm{Sec}^r C$.

(iv) Suppose that $\deg D_1 = \deg D_2 = r+2$ and $D_1 \sim D_2$. Choosing suitable bases for $\mathcal{L}(D_1)$ and $\mathcal{L}(D_2)$ we may arrange that $\Phi(D_1, D_2)$ is symmetric. Then $\Phi(D_1, D_2)$ has at most $(r+2)(r+3)/2$ linearly independent minors. By Theorem 1.2 the vector space of $(r+1)$-ics generating $I(\mathrm{Sec}^r C)$ has dimension

$$\beta(r+1, n) = (r+2)^2 > (r+2)(r+3)/2.$$

Hence $\Phi(D_1, D_2)$ is not a determinantal presentation of $\mathrm{Sec}^r C$.

This completes the proof of Theorem 1.4. □

REFERENCES

[BH] W. Bruns, J. Herzog, *Cohen-Macaulay rings*, Cambridge Studies in Advanced Mathematics **39**, Cambridge University Press, 1993.

[BE1] D.A. Buchsbaum and D. Eisenbud, Gorenstein ideals of height 3, *Seminar D. Eisenbud/B. Singh/W. Vogel*, Vol. 2, pp. 30–48, Teubner-Texte zur Math., **48**, Teubner, Leipzig, 1982.

[BE2] D.A. Buchsbaum and D. Eisenbud, Algebra structures for finite free resolutions, and some structure theorems for ideals of codimension 3, *Amer. J. Math.* **99** (1977) 447-485.

[CJ] M.L. Catalano-Johnson, The homogeneous ideals of higher secant varieties, *J. Pure Appl. Algebra* **158** (2001), no. 2-3, 123–129.

[CS] J.E. Cremona and M. Stoll, *Minimisation and reduction for* 3- *and* 4-*coverings of elliptic curves*, in preparation.

[E] D. Eisenbud, Commutative algebra with a view toward algebraic geometry, GTM **150**, Springer-Verlag, 1995.

[EKS] D. Eisenbud, J. Koh, M. Stillman, Determinantal equations for curves of high degree, *Amer. J. Math.* **110** (1988), no. 3, 513–539.

[F1] T.A. Fisher, *A new approach to minimising binary quartics and ternary cubics*, submitted.

[F2] T.A. Fisher, *Pfaffian presentations of elliptic normal curves*, preprint.

[F3] T.A. Fisher, *The invariants of a genus one curve*, in preparation.

[GP] M. Gross, S. Popescu, Equations of $(1, d)$-polarized abelian surfaces, *Math. Ann.* **310** (1998), no. 2, 333–377.

[H] K. Hulek, *Projective geometry of elliptic curves*, Soc. Math. de France, Astérisque **137** (1986).

[K] A.J. Knight, Primals passing multiply through elliptic normal curves, *Proc. London Math. Soc.* (3) **23** (1971), 445–458.

[KM] A.R. Kustin, M. Miller, Constructing big Gorenstein ideals from small ones, *J. Algebra* **85** (1983), no. 2, 303–322.

[L] H. Lange, Higher secant varieties of curves and the theorem of Nagata on ruled surfaces, *Manuscripta Math.* **47** (1984), no. 1-3, 263–269.

[LB] H. Lange, C. Birkenhake, *Complex abelian varieties*, Springer-Verlag, Berlin, 1992.

[M] D. Mumford, Varieties defined by quadratic equations, *Questions on algebraic varieties*, C.I.M.E., III Ciclo, Varenna, 1969, (1970), 29–100.

[Ra] M.S. Ravi, Determinantal equations for secant varieties of curves, *Comm. Algebra* 22 (1994), no. 8, 3103–3106.

[Ro] T.G. Room, *The geometry of determinantal loci*, Cambridge University Press, 1938.

[S] P. Schenzel, Über die freien Auflösungen extremaler Cohen-Macaulay-Ringe, *J. Algebra* **64** (1980), no. 1, 93–101.

[vBH] H.-Chr. Graf v. Bothmer, K. Hulek, Geometric syzygies of elliptic normal curves and their secant varieties, *Manuscripta Math.* **113** (2004), no. 1, 35–68.

University of Cambridge, DPMMS, Centre for Mathematical Sciences, Wilberforce Road, Cambridge CB3 0WB, UK

E-mail address: `T.A.Fisher@dpmms.cam.ac.uk`