GENUS ONE CURVES DEFINED BY PFAFFIANS

TOM FISHER

ABSTRACT. We show that genus one normal curves of odd degree can be presented by alternating matrices of linear forms, and give an algorithm for computing these matrices.

1. Introduction

Let C be a smooth projective curve of genus one defined over an arbitrary field k. If D is a k-rational divisor on C of degree $n \geq 3$ then we may embed $C \subset \mathbb{P}^{n-1}$ via the complete linear system $|D|$. The image is called a genus one normal curve. Equivalently, a genus one normal curve is a smooth curve of genus one and degree n that spans $\mathbb{P}^{n-1}$. The genus one normal curves of degrees 3 and 4 are plane cubics and intersections of two quadrics respectively.

It is well known that the homogeneous ideal of a genus one normal curve of degree $n \geq 4$ is generated by a vector space of quadrics of dimension $n(n-3)/2$. It follows that for $n \geq 5$ the homogeneous ideal is not a complete intersection. Moreover a generic choice of $n(n-3)/2$ quadrics will not define a curve, let alone a genus one normal curve.

In the case $n = 5$ the homogeneous ideal is generated by the 4×4 Pfaffians of a 5×5 alternating matrix of linear forms. This is a classical fact: see [2, Lemma 4.4(i)] and the references given there to works of Bianchi and Klein. It is also a special case of the structure theorem for Gorenstein ideals of codimension 3, due to Buchsbaum and Eisenbud [5], [6].

We generalise this observation to curves of higher odd degree. Specifically for $n \geq 5$ an odd integer we show that the homogeneous ideal of a genus one normal curve of degree n is generated by the 4×4 Pfaffians of an $n \times n$ alternating matrix of linear forms. The proof over an algebraically closed field has already appeared in [12]. Here we concentrate on arithmetic and algorithmic aspects. The key definition is

Date: 1st June 2006.

Definition 1.1. Let $n \geq 3$ be an odd integer. Let C be a genus one normal curve of degree n. A Klein matrix Φ for C is an $n \times n$ alternating matrix of linear forms defined over k such that
(i) Φ has rank at most 2 on C, and
(ii) the n submaximal Pfaffians of Φ are linearly independent.

This definition is well suited to computation. Indeed condition (i) holds if and only if the 4×4 Pfaffians of Φ belong to the homogeneous ideal of C. Condition (ii) may be checked directly. In §§3,5 we recall some alternative characterisations of Klein matrices.

If $n \geq 5$ then C is precisely the rank 2 locus of Φ. In fact a much stronger result is true. Let $\mathrm{Sec}^r C$ be the rth higher secant variety of C, *i.e.* the Zariski closure of the locus of all $(r-1)$-planes spanned by r points on C. As special cases we have $\mathrm{Sec}^0 C = \emptyset$, $\mathrm{Sec}^1 C = C$ and $\mathrm{Sec}^2 C = \mathrm{Sec}\, C$. We write $I(X)$ for the homogeneous ideal of a projective variety X. By convention $I(\emptyset)$ is the irrelevant ideal.

Theorem 1.2. *Let $n \geq 3$ be an odd integer. Let C be a genus one normal curve of degree n with Klein matrix Φ. If $n \geq 2r+3$ then*
(i) $\mathrm{Sec}^r C$ is the locus where Φ has rank at most $2r$, and
(ii) $I(\mathrm{Sec}^r C)$ is generated by the $(2r+2) \times (2r+2)$ Pfaffians of Φ.

PROOF: It suffices to prove the theorem over an algebraically closed field, and for this we refer to [12, Corollary 1.8]. □

We show that Klein matrices exist and are unique.

Theorem 1.3. *Let $n \geq 3$ be an odd integer.*
(a) Every genus one normal curve of degree n has a Klein matrix.
(b) If Φ_1 and Φ_2 are Klein matrices for C then
(i) There exist $B \in \mathrm{GL}_n(k)$ and $c \in k^\times$ such that $\Phi_1 = cB^T \Phi_2 B$.
(ii) The matrix B is uniquely determined up to scalars.

If k is algebraically closed then we may extract a square root and so dispense with the constant c in Theorem 1.3(b). With this convention the matrix B is uniquely determined up to sign.

We give two different proofs of Theorem 1.3. The first proof (see §3) uses rank 2 vector bundles and Galois descent. The second proof (see §§4,5) replaces C by a higher secant variety of codimension 3 and applies the Buchsbaum-Eisenbud structure theorem. In both approaches the assumption that n is odd is essential. In §§6,7 we turn the seond proof into an algorithm for computing Klein matrices. We then use our algorithm to give some examples in §8.

In the case $n = 5$ the existence of Klein matrices has the following converse, pointed out to me by Nick Shepherd-Barron.

Proposition 1.4. *A generic* 5×5 *alternating matrix of linear forms on* $\mathbb{P}^4$ *is a Klein matrix for a genus one normal quintic.*

Proof: For the proof we may assume that k is algebraically closed. Let $\mathrm{Gr}(2,5)$ be the Grassmannian of 2-dimensional vector subspaces of a 5-dimensional vector space V. The image of the Plücker embedding $\mathrm{Gr}(2,5) \hookrightarrow \mathbb{P}(\wedge^2 V) = \mathbb{P}^9$ is defined by the 4×4 Pfaffians of a generic 5×5 alternating matrix. Let H be hyperplane section for this embedding. It is known that $\mathrm{Gr}(2,5)$ has dimension 6, degree 5 and canonical divisor $K = -5H$. We apply Bertini's theorem [15, II, 8.18] to show that a generic $\mathbb{P}^4$-section is a smooth irreducible curve C. Since $K = -5H$ the adjunction formula [15, II, 8.20] gives $K_C \sim 0$. Thus C is a genus one curve of degree 5 defined by quadrics. Since there are no such curves in $\mathbb{P}^3$ it follows that C spans $\mathbb{P}^4$. To fit our definition of a Klein matrix, it only remains to show that the 4×4 Pfaffians of Φ are linearly independent. One possible proof of this is given in [12, Corollary 5.5]. □

Proposition 1.4 makes it possible to develop an invariant theory for genus one curves of degree $n = 5$ analogous to that classically known in the cases $n = 2, 3, 4$. We give details in a sequel to this paper. In particular we have found an algorithm for computing the Jacobian of a genus one normal quintic. The first step is to compute a Klein matrix using the algorithm described in this paper.

The analogue of Proposition 1.4 for $n \geq 7$ is false, as is already apparent by counting dimensions. Nonetheless it is hoped that Klein matrices will find applications to the study of genus one curves of higher odd degree. We hint at these in §9 where we explore the relationship between Klein matrices and the index of a genus one curve.

Remark 1.5. In the geometric literature the term used is "elliptic normal curve" rather than "genus one normal curve". We have changed the name since we are interested in curves that do not have or are not known to have a k-rational point. The word "normal" means that the curve is embedded by a complete linear system, equivalently that the homogeneous co-ordinate ring is integrally closed.

2. Pfaffians

We recall some basic facts about Pfaffians.

Definition 2.1. A square matrix over a ring R is *alternating* if it is skew-symmetric and all its diagonal entries are zero.

We temporarily work over a field k of characteristic 0. Let $A = (a_{ij})$ be an $n \times n$ alternating matrix with entries in k. If $n = 2r$ is even then the Pfaffian of A is

$$\mathrm{pf}(A) = \frac{1}{2^r r!} \sum_{\sigma \in S_{2r}} \mathrm{sign}(\sigma) \prod_{i=1}^{r} a_{\sigma(2i-1)\sigma(2i)}. \tag{1}$$

Standard calculations, cf. [3, Ch. IX, §5], show that

$$\begin{aligned} \mathrm{pf}(P^T A P) &= \det(P)\,\mathrm{pf}(A), & (2)\\ \mathrm{pf}\begin{pmatrix} 0 & A \\ -A^T & 0 \end{pmatrix} &= \pm\det(A). & (3) \end{aligned}$$

It is well known that any alternating matrix over a field is congruent to a matrix of the form

$$\begin{pmatrix} 0 & I_t & 0 \\ -I_t & 0 & 0 \\ 0 & 0 & 0 \end{pmatrix}.$$

In particular alternating matrices have even rank. It also follows, with the help of (2) and (3), that $\det(A) = \mathrm{pf}(A)^2$.

The denominator in (1) may be avoided by restricting the summation to an appropriate subset of S_{2r}. Alternatively, let k be the field of fractions of the polynomial ring

$$R_0 = \mathbb{Z}[a_{12}, a_{13}, \ldots, a_{n-1\,n}].$$

Since $\mathrm{pf}(A)^2 = \det(A) \in R_0$ it follows by unique factorisation that $\mathrm{pf}(A) \in R_0$. We use this polynomial to define the Pfaffian of an alternating matrix over an arbitrary ring.

Pfaffians, just like determinants, may be expanded along a row. We write $A^{\{i,j\}}$ for the matrix obtained from A by deleting the ith and jth rows and columns. Using (1) we find

$$\mathrm{pf}(A) = \sum_{j=2}^{n} (-1)^j a_{1j}\,\mathrm{pf}(A^{\{1,j\}}). \tag{4}$$

For example in the 4×4 case we have

$$\mathrm{pf}\begin{pmatrix} 0 & a_{12} & a_{13} & a_{14} \\ & 0 & a_{23} & a_{24} \\ & & 0 & a_{34} \\ & & & 0 \end{pmatrix} = a_{12}a_{34} - a_{13}a_{24} + a_{14}a_{23}.$$

Let A be a matrix over a ring R. We write $I_m(A)$ for the ideal generated by the $m \times m$ minors of A. Likewise if A is alternating and m is even then we write $\mathrm{Pf}_m(A)$ for the ideal generated by the $m \times m$

Pfaffians of A, where it is understood that these are the Pfaffians of the $m \times m$ submatrices obtained by deleting the same rows and columns. The proof of (2) gives $\mathrm{Pf}_m(P^T AP) \subset \mathrm{Pf}_m(A)$. So if P is invertible then $\mathrm{Pf}_m(P^T AP) = \mathrm{Pf}_m(A)$.

For any fixed value of m the following lemma is equivalent to some identities in R_0.

Lemma 2.2. *Let A be an $n \times n$ alternating matrix over a ring R. Then*

$$I_m(A) \subset \begin{cases} \mathrm{Pf}_m(A)^2 & \text{if } m \text{ is even,} \\ \mathrm{Pf}_{m-1}(A)\,\mathrm{Pf}_{m+1}(A) & \text{if } m \text{ is odd.} \end{cases}$$

If $2 \in R^\times$ or $m = n-1$ then the reverse inclusions hold.

Proof: We refer to [16, §3, §4] for the inclusions "$\subset$" and "$\supset$", the latter being conditional on $2 \in R^\times$. The case $m = n-1$ is covered by the identities of Cayley cited in [16, §2.2]. Let us note that the inclusion "$\supset$" does not hold in general. Indeed if A is the generic 4×4 alternating matrix over $R_0 = \mathbb{Z}[a_{12}, \ldots, a_{34}]$ then $I_2(A) \neq \mathrm{Pf}_2(A)^2$. □

The next lemma is recalled from [6, Corollary 2.6]. If $2 \in R^\times$ then it is an immediate corollary of Lemma 2.2.

Lemma 2.3. *Let A be an alternating matrix over a ring R. If m is even then the ideals $I_m(A)$ and $\mathrm{Pf}_m(A)$ have the same radical.*

Proof: By Lemma 2.2 we have $I_m(A) \subset \mathrm{Pf}_m(A)$. We recall that $\mathrm{Pf}_m(A)$ is generated by finitely many Pfaffians, say $p_1, \ldots, p_N$. Since each p_i^2 is a $m \times m$ minor of A we have:

$$f \in \mathrm{Pf}_m(A) \implies f^{N+1} \in I_m(A).$$

Thus $I_m(A) \subset \mathrm{Pf}_m(A) \subset \sqrt{I_m(A)}$. □

Definition 2.4. Let A be an $n \times n$ alternating matrix with n odd. The vector of submaximal Pfaffians of A is $P = (p_1, \ldots, p_n)$ where $p_i = (-1)^i \operatorname{pf}(A^{\{i\}})$ and $A^{\{i\}}$ is the matrix obtained by deleting the ith row and column of A.

We recall from [4, §3.4]:

Lemma 2.5. *Let n be an odd integer. Let A be an $n \times n$ alternating matrix with vector of submaximal Pfaffians P. Then $PA = 0$.*

Proof: Let A' be the $(n+1) \times (n+1)$ matrix obtained from A by repeating the first row and column. We apply (4) to A'. □

Lemma 2.6. *Let n be an odd integer. Let A_1, A_2 and B be $n \times n$ matrices over a ring R. Suppose that A_1 and A_2 are alternating with vectors of submaximal Pfaffians P_1 and P_2. If $A_1 = B^T A_2 B$ then $P_1 B^T = \det(B) P_2$.*

Proof: It suffices to give a proof in the case $R = k$ is an algebraically closed field. We may further suppose that A_2 has rank $n-1$. If B is invertible then from $P_1 B^T A_2 = P_1 A_1 B^{-1} = 0$ and $P_2 A_2 = 0$ we deduce that $P_1 B^T = c P_2$ for some $c \in k$. Then fixing A_2 and varying B we get $P_1 B^T = f(B) P_2$ where f is a polynomial in the entries of B and $f(B) \neq 0$ whenever B is invertible. Hence $f(B) = c(\det B)^r$ for some $c \in k^\times$ and $r \geq 0$. By considering the case B is a scalar matrix it follows that $c = 1$ and $r = 1$. □

3. Vector bundles

Let $n \geq 3$ be an odd integer and let C be a genus one normal curve of degree n. Let $\mathcal{O}(1)$ be the line bundle of degree n on C associated to the hyperplane section. For $\mathcal{E}$ a rank 2 vector bundle on C with $\det \mathcal{E} \simeq \mathcal{O}(1)$ we write $\Phi(\mathcal{E})$ for the alternating matrix of linear forms representing the determinant map

$$\wedge^2 H^0(C, \mathcal{E}) \to H^0(C, \mathcal{O}(1)).$$

Notice that to make $\Phi(\mathcal{E})$ explicit it is necessary both to choose a basis for $H^0(C, \mathcal{E})$ and to fix an isomorphism $\det \mathcal{E} \simeq \mathcal{O}(1)$. We recall the characterisation of Klein matrices in terms of vector bundles.

Proposition 3.1. *Let Φ be an $n \times n$ alternating matrix of linear forms defined over k. Then Φ is a Klein matrix for C if and only if it is of the form $\Phi(\mathcal{E})$ for $\mathcal{E}$ an indecomposable rank 2 vector bundle on C with $\det \mathcal{E} \simeq \mathcal{O}(1)$.*

Proof: See [12, Proposition 5.3]. □

We recall a special case of a theorem of Atiyah.

Proposition 3.2. *Let k be an algebraically closed field.*
(i) There is a unique indecomposable rank 2 vector bundle $\mathcal{E}$ on C with $\det \mathcal{E} \simeq \mathcal{O}(1)$.
(ii) If $\operatorname{char}(k) \neq 2$ then $\operatorname{End}(\mathcal{E}) \simeq k$.

Proof. (i) See [1, Corollary to Theorem 7].
(ii) We take global sections in [1, Lemma 22]. □

Proposition 3.1 tells us that to prove the existence of Klein matrices over a non-algebraically closed field it suffices to remove the restriction on k in Proposition 3.2(i). If k is perfect and char $(k) \neq 2$ this may be achieved by Galois descent, as we now explain. These restrictions on k will remain in force for the rest of this section.

Lemma 3.3. *Let $\mathcal{E}_1$ and $\mathcal{E}_2$ be indecomposable k-rational rank 2 vector bundles on C with $\det \mathcal{E}_1 \simeq \det \mathcal{E}_2 \simeq \mathcal{O}(1)$. Then $\mathcal{E}_1 \simeq \mathcal{E}_2$ over k.*

Proof: By Proposition 3.2(i) there is an isomorphism $\phi : \mathcal{E}_1 \to \mathcal{E}_2$ defined over $\overline{k}$. By Proposition 3.2(ii) the cocycle $\sigma \mapsto \phi^\sigma \phi^{-1}$ takes values in $\overline{k}^\times$. We are done by Hilbert's theorem 90. □

Proposition 3.4. *There exists an indecomposable k-rational rank 2 vector bundle $\mathcal{E}$ on C with $\det \mathcal{E} \simeq \mathcal{O}(1)$.*

Proof: Since n is odd there is a field extension k_0/k of odd degree with $C(k_0) \neq \emptyset$. Let $P, Q \in C(k_0)$ with $(n-1)P + Q \sim H$, where H is the hyperplane section. Let $\mathcal{E}_1$ be the non-trivial extension of $\mathcal{O}(Q)$ by $\mathcal{O}$ and let $\mathcal{E} = \mathcal{E}_1 \otimes \mathcal{O}(((n-1)/2)P)$. Then $\mathcal{E}$ is an indecomposable k_0-rational rank 2 vector bundle on C with $\det \mathcal{E} \simeq \mathcal{O}(1)$.

We must show that $\mathcal{E}$ descends to k. Let k_1/k be the Galois closure of k_0/k. We write $G = \mathrm{Gal}(k_1/k)$ and $H = \mathrm{Gal}(k_1/k_0)$. For each $\sigma \in G$, Lemma 3.3 gives an isomorphism $h_\sigma : \mathcal{E} \to \mathcal{E}^\sigma$ defined over k_1. By Proposition 3.2(ii) the cocycle $(\sigma, \tau) \mapsto h_{\sigma\tau}^{-1} (h_\sigma)^\tau h_\tau$ takes values in $k_1^\times$ and so defines an element $\xi \in H^2(G, k_1^\times)$. We write the elements of this group additively. Since $\det \mathcal{E} \simeq \mathcal{O}(1)$ is k-rational, we have $2\xi = 0$. Since $\mathcal{E}$ is defined over k_0, we have $\mathrm{res}_H^G \xi = 0$. But $[k_0 : k]$ is odd, so

$$\xi = [k_0 : k]\xi = \mathrm{cor}_H^G \, \mathrm{res}_H^G \, \xi = 0.$$

We may therefore scale the h_σ so that $h_{\sigma\tau} = (h_\sigma)^\tau h_\tau$ for all $\sigma, \tau \in G$. As explained in [20, Chapter V, §4] this is precisely the descent data required to descend $\mathcal{E}$ from k_1 to k. □

We give our first proof of Theorem 1.3 under the assumptions on k specified above, namely that k is perfect and char $(k) \neq 2$.

Proof of Theorem 1.3: (a) The existence of Klein matrices follows immediately from Propositions 3.1 and 3.4.

(b) Let Φ_1 and Φ_2 be Klein matrices for C. By Proposition 3.1 we have $\Phi_1 = \Phi(\mathcal{E}_1)$ and $\Phi_2 = \Phi(\mathcal{E}_2)$ where $\mathcal{E}_1$ and $\mathcal{E}_2$ are indecomposable rank 2 vector bundles on C with $\det \mathcal{E}_1 \simeq \det \mathcal{E}_2 \simeq \mathcal{O}(1)$. By Lemma 3.3 there is an isomorphism $\mathcal{E}_1 \simeq \mathcal{E}_2$. Let $B \in \mathrm{GL}_n(k)$ represent the corresponding map on global sections. The isomorphisms $\det \mathcal{E}_1 \simeq \mathcal{O}(1)$ and $\det \mathcal{E}_2 \simeq \mathcal{O}(1)$ used in the construction of $\Phi(\mathcal{E}_1)$ and $\Phi(\mathcal{E}_2)$ now give rise to an automorphism of $\mathcal{O}(1)$. Since $\mathrm{End}(\mathcal{O}(1)) \simeq H^0(C, \mathcal{O}) \simeq k$ it follows that $\Phi_1 = cB^T \Phi_2 B$ for some $c \in k^\times$.

Finally we must show that if $\Phi(\mathcal{E}) = cB^T\Phi(\mathcal{E})B$ then B is a scalar matrix. Such a matrix B describes an endomorphism of $H^0(C,\mathcal{E})$. We saw in [12, §4] that $\mathcal{E}$ may be recovered from $\Phi(\mathcal{E})$. So B extends to an endomorphism of $\mathcal{E}$. Then Proposition 3.2(ii) tells us that B is a scalar matrix. □

The approach via vector bundles was crucial to the proof of Theorem 1.2. We have now seen that it leads rapidly to a proof of the existence and uniqueness of Klein matrices. Unfortunately it does not appear to give any practical method for computing Klein matrices. In §5 we give an alternative proof of Theorem 1.3 that is both constructive and applies over an arbitrary field.

4. Gorenstein Ideals

We prepare for our second proof of the existence and uniqueness of Klein matrices by recalling some basic commutative algebra. Our main references are [4] and [8]. We work over an arbitrary field k.

Let $R = k[x_1, \ldots, x_n]$ be the homogeneous co-ordinate ring of $\mathbb{P}^{n-1}$, with its usual grading $R = \oplus_{d \geq 0} R_d$. Let $R_+ = \oplus_{d\geq 1} R_d$ be the irrelevant ideal and let M be any finitely generated graded R-module.

Definition 4.1. 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 *minimal* if $\phi_i(F_i) \subset R_+ F_{i-1}$ for all i.

Lemma 4.2. *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 [8, §20.1]. □

The common length of all minimal resolutions is called the projective dimension of M and denoted proj dim M. Hilbert's syzygy theorem asserts that proj dim $M \leq n$. We write codim I for the codimension, or height, of an ideal $I \subset R$. It follows by the Auslander-Buchsbaum formula that codim $I \leq$ proj dim R/I. A homogeneous ideal $I \subset R$ is *perfect* if codim $I =$ proj dim R/I.

The dual of M is $M^* = \mathrm{Hom}_R(M, R)$. The dual of a complex of graded free R-modules is again a complex of graded free R-modules.

Definition 4.3. A perfect ideal $I \subset R$ is a *Gorenstein ideal* if the minimal graded free resolution of R/I is isomorphic to its dual (up to a shift in degree).

We recall a theorem of Buchsbaum and Eisenbud [5], [6].

Proposition 4.4. *Let $I \subset R$ be a Gorenstein ideal of codimension 3. Let R/I have minimal graded free resolution $F_\bullet$. Then there is an isomorphism of complexes*

$$\begin{tikzcd}
0 \arrow[r] & F_3 \arrow[r, "\phi_3"] \arrow[d, "s_3"] & F_2 \arrow[r, "\phi_2"] \arrow[d, "s_2"] & F_1 \arrow[r, "\phi_1"] \arrow[d, "s_1"] & F_0 \arrow[r] \arrow[d, "s_0"] & 0 \\
0 \arrow[r] & F_0^* \arrow[r, "\phi_1^*"] & F_1^* \arrow[r, "\phi_2^*"] & F_2^* \arrow[r, "\phi_3^*"] & F_3^* \arrow[r] & 0
\end{tikzcd}$$

with $s_1\phi_2$ $(= \phi_2^* s_2)$ represented by an alternating matrix.

Proof: We know by Definition 4.3 that there is an isomorphism of complexes. The proof works by putting an algebra structure on $\oplus_{i=0}^3 F_i$ and then using this algebra structure to choose an isomorphism with the required additional property. We refer to [4, §3.4] for details. □

From now on we label all maps of graded free R-modules by the matrices that represent them.

Definition 4.5. Let $m \geq 3$ be an odd integer. Let $r_1, \ldots, r_m$ be integers that are either all odd or all even. A *Buchsbaum-Eisenbud matrix* Φ is an $m \times m$ alternating matrix with each entry Φ_{ij} either 0 or a non-constant homogeneous polynomial of degree $(r_i + r_j)/2$.

Let Φ be a Buchsbaum-Eisenbud matrix, and let $P = (p_1, \ldots, p_m)$ be the vector of submaximal Pfaffians of Φ as defined in §2. Then each p_i is either 0 or a non-constant homogeneous polynomial of degree $t_i = (s - r_i)/2$ where $s = \sum_{j=1}^m r_j$. We write $R(d)$ for the graded free R-module of rank 1 with $R(d)_e = R_{d+e}$.

Lemma 4.6. *Let Φ be a Buchsbaum-Eisenbud matrix, and let P be the vector of submaximal Pfaffians of Φ. Then there is a complex of graded free R-modules*

$$F_\bullet(\Phi): \quad 0 \to R(-s) \xrightarrow{P^T} \oplus_{i=1}^m R(-s + t_i) \xrightarrow{\Phi} \oplus_{i=1}^m R(-t_i) \xrightarrow{P} R \to 0.$$

Proof: This is immediate from Lemma 2.5. □

We recall the structure theorem of Buchsbaum and Eisenbud [5], [6] for Gorenstein ideal of codimension 3.

Theorem 4.7 (Buchsbaum-Eisenbud). *(a) Let $I \subset R$ be a homogeneous ideal of codimension at least 3 generated by the submaximal Pfaffians of a Buchsbaum-Eisenbud matrix Φ. Then $F_\bullet(\Phi)$ is a minimal graded free resolution of R/I. In particular I is a Gorenstein ideal of codimension 3.*

(b) Let $I \subset R$ be a Gorenstein ideal of codimension 3*. Then there exists a Buchsbaum-Eisenbud matrix Φ such that $F_\bullet(\Phi)$ is a minimal graded free resolution of R/I. In particular I is generated by the submaximal Pfaffians of Φ.*

Proof: (a) Since the submaximal Pfaffians of Φ are not all zero, $\operatorname{rank}(\Phi) = m-1$ and $\operatorname{rank}(P) = 1$. By Lemma 2.3 the ideals $I = \operatorname{Pf}_{m-1}(\Phi)$ and $I_{m-1}(\Phi)$ have the same radical. So $I_{m-1}(\Phi)$ has codimension at least 3. Then $F_\bullet(\Phi)$ is exact by the Buchsbaum-Eisenbud acyclicity criterion: see [4, Theorem 1.4.13] or [8, Theorem 20.9]. It follows from Definition 4.5 that $F_\bullet(\Phi)$ is minimal. So $F_\bullet(\Phi)$ is a minimal graded free resolution of R/I and $\text{proj dim}\, R/I = 3$. But in general we have $\operatorname{codim} I \le \text{proj dim}\, R/I$. So I is a Gorenstein ideal of codimension 3.

(b) Granted Proposition 4.4 it suffices to prove

Proposition 4.8. *Let $I \subset R$ be a Gorenstein ideal of codimension 3. Suppose that R/I has minimal graded free resolution*

$$G_\bullet : \quad 0 \to R(-s) \xrightarrow{Q^T} \oplus_{i=1}^m R(-s+t_i) \xrightarrow{\Phi} \oplus_{i=1}^m R(-t_i) \xrightarrow{Q} R \to 0$$

where Φ is an alternating matrix. Then Φ is a Buchsbaum-Eisenbud matrix and Q is a scalar multiple of the vector of submaximal Pfaffians of Φ. In particular $F_\bullet(\Phi)$ is a minimal graded free resolution of R/I.

Proof: Let $Q = (q_1, \ldots, q_m)$ where q_i is a homogeneous polynomial of degree t_i. Then Φ is an $m \times m$ alternating matrix with each entry Φ_{ij} either 0 or a non-constant homogeneous polynomial of degree $s - t_i - t_j = (r_i + r_j)/2$ where $r_i = s - 2t_i$. Since $G_\bullet$ is exact it is clear that Φ has rank $m-1$, and so m is odd. Hence Φ satisfies our definition of a Buchsbaum-Eisenbud matrix.

Let $J = \operatorname{Pf}_{m-1}(\Phi)$. By Lemma 2.3 it has the same radical as $I_{m-1}(\Phi)$. Then [8, Corollary 20.12] applied to $G_\bullet$ gives $\sqrt{I} \subset \sqrt{J}$. So J has codimension at least 3. By Theorem 4.7(a), R/J has minimal graded free resolution $F_\bullet(\Phi)$. Let P be the vector of submaximal Pfaffians of Φ. Since both $F_\bullet(\Phi)$ and $G_\bullet$ are exact we have that $\operatorname{im}(P^T) = \ker(\Phi) = \operatorname{im}(Q^T)$. Hence Q is a scalar multiple of P and $I = J$. □

This completes the proof of Theorem 4.7. □

The following uniqueness result is sufficient for our purposes. It is indicated on page 471 of [6] that a stronger result is true.

Proposition 4.9. *Let $I \subset R$ be a Gorenstein ideal of codimension 3. Suppose that R/I has minimal graded free resolutions*

$$0 \longrightarrow R(-s) \xrightarrow{Q_1^T} R(-s+t)^m \xrightarrow{\Phi_1} R(-t)^m \xrightarrow{Q_1} R \longrightarrow 0$$

and

$$0 \longrightarrow R(-s) \xrightarrow{Q_2^T} R(-s+t)^m \xrightarrow{\Phi_2} R(-t)^m \xrightarrow{Q_2} R \longrightarrow 0$$

where Φ_1 and Φ_2 are alternating matrices. Then $\Phi_1 = cB^T\Phi_2 B$ for some $B \in \mathrm{GL}_m(k)$ and $c \in k^\times$. Moreover B is uniquely determined up to scalars.

Proof: By Lemma 4.2 there is an isomorphism of complexes

$$\begin{tikzcd}
0 \arrow[r] & R(-s) \arrow[r, "Q_1^T"] \arrow[d, "c^{-1}"] & R(-s+t)^m \arrow[r, "\Phi_1"] \arrow[d, "B"] & R(-t)^m \arrow[r, "Q_1"] \arrow[d, "A^{-T}"] & R \arrow[r] \arrow[d, equal] & 0 \\
0 \arrow[r] & R(-s) \arrow[r, "Q_2^T"] & R(-s+t)^m \arrow[r, "\Phi_2"] & R(-t)^m \arrow[r, "Q_2"] & R \arrow[r] & 0
\end{tikzcd}$$

for some $A, B \in \mathrm{GL}_m(k)$ and $c \in k^\times$. By [8, Lemma 20.3] this isomorphism is unique up to homotopy. Since we have restricted to the case of pure resolutions, there are in fact no homotopies. Hence A and B are uniquely determined. Comparing the above diagram with its dual we find that $A = cB$, and so $\Phi_1 = cB^T\Phi_2 B$.

For the final statement we suppose $\Phi_1 = cB^T\Phi_2 B$. Let P_1 and P_2 be the vectors of submaximal Pfaffians of Φ_1 and Φ_2. Then Lemma 2.6 shows that $P_1 B^T$ is a scalar multiple of P_2. According to Proposition 4.8 the entries of P_1 and P_2 are bases for the vector space of t-ics generating I. Hence B is uniquely determined up to scalars. □

5. Klein matrices

Let $C \subset \mathbb{P}^{n-1}$ be a genus one normal curve of degree n. The rth higher secant variety $\mathrm{Sec}^r C \subset \mathbb{P}^{n-1}$ was defined in §1. It has codimension $\max(n-2r, 0)$. So if n is odd then there is a higher secant variety of codimension 3. This leads to a characterisation of Klein matrices in terms of higher secant varieties.

Proposition 5.1. *Let $n \geq 3$ be an odd integer. Let C be a genus one normal curve of degree n. Let Φ be an $n \times n$ alternating matrix of linear forms. Then Φ is a Klein matrix for C if and only if the submaximal Pfaffians of Φ generate $I(\mathrm{Sec}^r C)$ where $r = (n-3)/2$.*

Proof: See [12, Proposition 3.1]. □

It is well known that genus one normal curves are projectively Gorenstein. We recall the generalisation of this result to higher secant varieties. Let $\beta(r, n)$ be the number of ways of choosing r elements of

$\mathbb{Z}/n\mathbb{Z}$ such that no two elements are adjacent. By considering the subsets that do or do not contain a given element, one finds

$$\beta(r,n) = \binom{n-r}{r} + \binom{n-r-1}{r-1} = \frac{n(n-r-1)!}{r!(n-2r)!}. \tag{5}$$

We call a homogeneous polynomial of degree r an r-ic.

Proposition 5.2. *Let C be a genus one normal curve of degree n. If $m = n-2r \geq 2$ then $I = I(\mathrm{Sec}^r C)$ is a Gorenstein ideal and R/I has a minimal graded free resolution of the form*

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

where $b_1 = \beta(r+1,n)$. In particular I is generated by a vector space of $(r+1)$-ics of dimension $\beta(r+1,n)$.

Proof: It suffices to prove the proposition over an algebraically closed field, and for this we refer to [11] or [22]. □

We put everything together to prove the existence and uniqueness of Klein matrices over an arbitrary field.

Proof of Theorem 1.3: (a) Let C be a genus one normal curve of degree $n = 2r+3$ and let $I = I(\mathrm{Sec}^r C)$. Proposition 5.2 tells us that I is a Gorenstein ideal of codimension 3, and that R/I has a minimal graded free resolution of the form

$$0 \to R(-n) \to R(-r-2)^n \to R(-r-1)^n \to R \to 0.$$

We apply Theorem 4.7(b) to show that I is generated by the submaximal Pfaffians of an $n \times n$ alternating matrix of linear forms Φ. Then Φ is a Klein matrix by Proposition 5.1.

(b) Let $n = 2r+3$ and let $I = I(\mathrm{Sec}^r C)$. By Proposition 5.1 and Theorem 4.7(a) the complexes $F_\bullet(\Phi_1)$ and $F_\bullet(\Phi_2)$ are minimal graded free resolutions of R/I. We are done by Proposition 4.9. □

In the next two sections we turn the above proof into an algorithm for computing Klein matrices.

6. Computing the higher secant varieties

Let $X \subset \mathbb{P}^{n-1}$ be a projective variety. If $I(X)$ has generators $f_1, \ldots, f_m$ then $I(\mathrm{Sec}\, X)$ may be computed by eliminating $y_1, \ldots, y_n$ from the ideal

$$(f_1(x+y), \ldots, f_m(x+y), f_1(y), \ldots, f_m(y))$$

in $k[x_1, \ldots, x_n, y_1, \ldots, y_n]$. This is extremely inefficient. The purpose of this section is to explain a better method. The following definition is not the usual one (see [8, §3.9]) but is convenient for our purposes.

Definition 6.1. The rth symbolic power of $I(X)$ is the set of polynomials in R that vanish to order at least r at every point of X.

In the case of a genus one normal curve the symbolic powers and higher secant varieties are closely related.

Lemma 6.2. *Let C be a genus one normal curve of degree $n \geq 2r+2$. Then $I(\mathrm{Sec}^r C)$ is generated by the vector space of $(r+1)$-ics belonging to the rth symbolic power of $I(C)$.*

Proof: Granted Proposition 5.2 this is [11, Lemma 4.5]. □

The following variant of Definition 6.1 is more convenient for computations. We employ the multi-index notation $x^\alpha = x_1^{\alpha_1} \ldots x_n^{\alpha_n}$ where $\alpha = (\alpha_1, \ldots, \alpha_n)$ and $|\alpha| = \alpha_1 + \ldots + \alpha_n$.

Definition 6.3. The rth infinitesimal power of $I(X)$ is the set of polynomials $f \in R$ with $\frac{\partial^{|\alpha|} f}{\partial x^\alpha} \in I(X)$ for all multi-indices α with $|\alpha| < r$.

If char $(k) = 0$ then the infinitesimal and symbolic powers agree. An efficient method for computing infinitesimal powers is given in [21, §2]. In our situation we know in advance the degrees of the polynomials we are looking for. This allows us to reduce the computation to linear algebra. As in §4 we write R_d for the vector space of homogeneous polynomials of degree d.

Proposition 6.4. *Assume* char $(k) = 0$. *Let C be a genus one normal curve of degree $n \geq 2r+2$. Let $f_1, \ldots, f_m$ be a basis for the vector space of r-ics generating $I(\mathrm{Sec}^{r-1} C)$. Then $I(\mathrm{Sec}^r C)$ is generated by*

$$\begin{aligned} V &= \{g \in R_{r+1} | \tfrac{\partial g}{\partial x_j} \in \langle f_1, \ldots, f_m \rangle \textit{ for all } 1 \leq j \leq n\} \\ &= \{\textstyle\sum \ell_i f_i \mid \sum \ell_i \frac{\partial f_i}{\partial x_j} \in \langle f_1, \ldots, f_m \rangle \textit{ for all } 1 \leq j \leq n\} \end{aligned}$$

where the ℓ_i are linear forms.

Proof: Granted Proposition 5.2 it suffices to show that V is the vector space of $(r+1)$-ics in $I(\mathrm{Sec}^r C)$. If g belongs to V then by Lemma 6.2 its partial derivatives belong to the $(r-1)$st symbolic power of $I(C)$. Since char $(k) = 0$ the infinitesimal and symbolic powers agree. So g belongs to the rth symbolic power of $I(C)$. Applying Lemma 6.2 again shows that g belongs to $I(\mathrm{Sec}^r C)$. Conversely, we saw in [11, Remark 4.6] that if g belongs to $I(\mathrm{Sec}^r C)$ then its partial derivatives belong to $I(\mathrm{Sec}^{r-1} C)$. Since $I(\mathrm{Sec}^r C) \subset I(\mathrm{Sec}^{r-1} C)$ the alternative description of V is clear. □

Remark 6.5. In practice we minimise the number of unknowns by using the first expression to calculate V if $\binom{n+r}{r+1} < n\beta(r,n)$, and the second expression otherwise.

We recall from [11, Proposition 7.3(i)] that if $n = 2r+1$ then $\mathrm{Sec}^r C$ is a hypersurface of degree n. Proposition 6.4 leaves open the problem of computing an equation for this hypersurface. Fortunately this is not required for the computation of Klein matrices. The following discussion is included for completeness.

Lemma 6.6. *Let C be a genus one normal curve of degree $n = 2r+3$. Let $p_1, \ldots, p_n$ be a basis for the vector space of $(r+1)$-ics generating $I(\mathrm{Sec}^r C)$. If $r \geq 1$ then $\det(\partial p_i / \partial x_j)$ belongs to $I(\mathrm{Sec}^{r+1} C)$.*

PROOF: Let P belong to the linear span Π of a set of $r+1$ distinct points on C, but not to the linear span of any proper subset. Then any $(r+1)$-ic vanishing on $\mathrm{Sec}^r C$ and at P must also vanish on Π. It follows that the space of $(r+1)$-ics vanishing on $\mathrm{Sec}^r C$ and singular at P has dimension at least r. In particular $\det(\partial p_i / \partial x_j)$ vanishes at P. We are done since the points P of the above form are Zariski dense in $\mathrm{Sec}^{r+1} C$. □

If $n = 5$ then it turns out that $\det(\partial p_i / \partial x_j)$ is a non-zero quintic, and so a generator for $I(\mathrm{Sec}\, C)$. See [14, Theorem 5.3] or [17, VIII.2.5] for further discussion of this result. We give the following version.

Lemma 6.7. *Let C be a genus one normal quintic. Let $p_1, \ldots, p_5$ be a basis for the vector space of quadrics generating $I(C)$. Then the rank of the Jacobian matrix $J = (\partial p_i / \partial x_j)$ evaluated at $P \in \mathbb{P}^4$ is*

$$\operatorname{rank} J(P) = \begin{cases} 3 & \text{if } P \in C, \\ 4 & \text{if } P \in \mathrm{Sec}\, C \setminus C, \\ 5 & \text{if } P \notin \mathrm{Sec}\, C. \end{cases}$$

In particular $\mathrm{Sec}\, C$ *has equation* $\det(J) = 0$.

Proof. Let $C_P \subset \mathbb{P}^3$ be the projection of C away from P. Then

$$\operatorname{rank} J(P) \leq 5 - r \iff C_P \text{ lies on } r \text{ linearly independent quadrics.}$$

If $P \notin \mathrm{Sec}\, C$ then C_P is a smooth curve of degree 5. As explained in the proof of [17, IV.3.4], it cannot lie on any quadric. Thus $\operatorname{rank} J(P) = 5$.

If $P \in \mathrm{Sec}\, C$ then Lemma 6.6 gives $\operatorname{rank} J(P) \leq 4$. If $P \notin C$ then $C_P \subset \mathbb{P}^3$ is a curve of degree 5. It therefore lies on at most one quadric and so $\operatorname{rank} J(P) = 4$. If $P \in C$ then the Jacobian criterion for smoothness gives $\operatorname{rank} J(P) = 3$. □

If $n = 7$ then we find in numerical examples that $\det(\partial p_i/\partial x_j)$ factorises as a scalar times the square of a 7-ic. It follows by Lemma 6.6 that this 7-ic is an equation for $\mathrm{Sec}^3 C$. We suggest the following generalisation of Lemma 6.7.

Conjecture 6.8. *Assume* $\mathrm{char}\,(k) = 0$. *Let C be a genus one normal curve of degree $n = 2r+3$. Let $p_1, \ldots, p_n$ be a basis for the vector space of $(r+1)$-ics generating $I(\mathrm{Sec}^r C)$. Then* $\det(\partial p_i/\partial x_j)$ *is a generator for $I(\mathrm{Sec}^{r+1} C)^r$.*

7. Computing Klein matrices

Let C be a genus one normal curve of degree $n = 2r + 3$. We turn the methods of §§4,5 into a practical algorithm for computing Klein matrices. The first step, already discussed in §6, is to compute generators for $I = I(\mathrm{Sec}^r C)$.

Our next tasks are to compute the graded minimal free resolution of R/I, and to compute an isomorphism between this complex and its dual. Since we are dealing with pure resolutions such an isomorphism is unique. Proposition 4.4 tells us that, for a suitable choice of bases, the map in the middle of our complex is represented by an alternating matrix Φ. This matrix Φ is a Klein matrix for C.

In practice it is extremely wasteful to call a general procedure for computing minimal resolutions. Roughly speaking, we already know that the minimal resolution is self-dual, so we only need to compute half of it. We also know in advance the degrees of all polynomials that appear. This allows us to reduce the computation to linear algebra.

Proposition 7.1. *Let $I \subset R$ be a Gorenstein ideal of codimension* 3. *Suppose that R/I has minimal graded free resolution*

$$0 \longrightarrow R(-s) \xrightarrow{Q_2^T} R(-s+t)^m \xrightarrow{\Psi} R(-t)^m \xrightarrow{Q_1} R \longrightarrow 0.$$

(i) There exists $B \in \mathrm{GL}_m(k)$ such that ΨB is alternating.
(ii) The matrices B for which ΨB is alternating form a 1*-dimensional vector subspace of* $\mathrm{Mat}_m(k)$.
(iii) If $\Phi = \Psi B$ is alternating and P is the vector of submaximal Pfaffians of Φ then $P = cQ_1$ for some $c \in k$. Moreover if B is non-zero then c is non-zero.

Proof: (i) This is immediate from Proposition 4.4.
(ii) Let $B \in \mathrm{Mat}_m(k)$ be a non-zero matrix such that $\Phi = \Psi B$ is

alternating. We construct a commutative diagram

$$\begin{tikzcd}
0 \arrow[r] & R(-s) \arrow[r, "Q_1^T"] \arrow[d, dashed] & R(-s+t)^m \arrow[r, "\Phi"] \arrow[d, "B"] & R(-t)^m \arrow[r, "Q_1"] \arrow[d, equal] & R \arrow[r] \arrow[d, equal] & 0 \\
0 \arrow[r] & R(-s) \arrow[r, "Q_2^T"] & R(-s+t)^m \arrow[r, "\Psi"] & R(-t)^m \arrow[r, "Q_1"] & R \arrow[r] & 0
\end{tikzcd}$$

The top row is a complex since $\Phi Q_1^T = -(Q_1 \Phi)^T = 0$. The dotted arrow is constructed by a diagram chase. It is multiplication by a constant $c \in k$. The commutativity of the lefthand square gives $BQ_1^T = cQ_2^T$. But the entries of Q_1 are linearly independent and, recalling that the minimal resolution for R/I is self-dual, the same is true for Q_2. So this relation determines B uniquely up to scalars.
(iii) If $B = 0$ then there is nothing to prove. Otherwise it follows by (i) and (ii) that B is invertible. In this case the above diagram is an isomorphism of complexes. The proof is completed by applying Proposition 4.8 to the top row. □

Our algorithm for computing Klein matrices is as follows. We assume char $(k) = 0$ and write R_1 for the space of linear forms on $\mathbb{P}^{n-1}$.

Algorithm 7.2. *Let $n \geq 5$ be an odd integer. Let $C \subset \mathbb{P}^{n-1}$ be a genus one normal curve of degree n and let $r = (n-3)/2$.*
INPUT: A set of polynomials $f_1, \ldots, f_m$ defining C.
OUTPUT: A Klein matrix Φ for C.

(1) *Compute a minimal basis for the radical of $(f_1, \ldots, f_m)$. This reduces us to the case where $f_1, \ldots, f_m$ is a basis for the vector space of quadrics generating $I(C) = I(\mathrm{Sec}^1 C)$.*
(2) *Use Proposition 6.4 to compute a basis $p_1, \ldots, p_n$ for the vector space of $(r+1)$-ics generating $I(\mathrm{Sec}^r C)$.*
(3) *Compute an $n \times n$ matrix of linear forms Ψ whose columns generate the vector space $\{(\ell_1, \ldots, \ell_n) \in R_1^n | \sum \ell_i p_i = 0\}$.*
(4) *Compute any non-zero solution $B \in \mathrm{Mat}_n(k)$ to $\Psi B = -B^T \Psi^T$.*
(5) *Let $\Phi = \Psi B$. Check that the vector of submaximal Pfaffians of Φ is a non-zero scalar multiple of $(p_1, \ldots, p_n)$.*

Step 1 may be accomplished using standard Gröbner basis algorithms, as implemented in MAGMA for example. Steps 2, 3 and 4 use only linear algebra. If $n = 5$ then there is nothing to do in Step 2. Step 5 checks that we have not made a mistake. Since the submaximal Pfaffians are homogeneous polynomials of degree $(n-1)/2$, it is not always possible to get rid of the scalar in Step 5 by rescaling Φ.

The proof that Algorithm 7.2 computes a Klein matrix is as follows. Let $Q_1 = (p_1, \ldots, p_n)$ and Ψ be the quantities computed in Steps 2 and 3. Then by Proposition 5.2 the hypotheses of Proposition 7.1 are satisfied for $I = I(\mathrm{Sec}^r C)$ and some (unknown) Q_2. The condition of Step 5 is satisfied by Proposition 7.1(iii). Finally Proposition 5.1 shows that Φ is a Klein matrix.

The proof of the uniqueness of Klein matrices given in §5 provides us with the following simple algorithm.

Algorithm 7.3. *Let $n \geq 5$ be an odd integer. Let C be a genus one normal curve of degree n.*
INPUT: Klein matrices Φ_1 and Φ_2 for C.
OUTPUT: Elements $B \in \mathrm{GL}_m(k)$ and $c \in k^\times$ such that $\Phi_1 = cB^T\Phi_2 B$.

1. *Let P_1, P_2 be the vectors of submaximal Pfaffians for Φ_1, Φ_2.*
2. *Compute $B \in \mathrm{GL}_m(k)$ such that $BP_1^T = P_2^T$.*
3. *Compute $c \in k^\times$ such that $\Phi_1 = cB^T\Phi_2 B$.*

Implementations of Algorithms 7.2 and 7.3 in MAGMA [19] are available from the author's website [13].

8. Examples

8.1. **Elliptic curves.** Let E have Weierstrass equation

$$y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6.$$

We embed E in $\mathbb{P}^{n-1}$ via $|n.0|$ to give a genus one normal curve of degree n. If $n = 5$ then the embedding is given by

$$(x_1 : \ldots : x_5) = (1 : x : y : x^2 : xy)$$

and the image has Klein matrix

$$\Phi_5 = \begin{pmatrix} 0 & a_2x_4 + a_6x_1 & x_5 & x_4 - a_1x_3 + a_4x_1 & -x_3 \\ & 0 & -x_4 & -x_3 - a_3x_1 & x_2 \\ & & 0 & -x_2 & 0 \\ & - & & 0 & -x_1 \\ & & & & 0 \end{pmatrix}.$$

If $n = 7$ then the embedding is given by

$$(x_1 : \ldots : x_7) = (1 : x : y : x^2 : xy : x^3 : x^2y).$$

and the image has Klein matrix

$$\Phi_7 = \begin{pmatrix} 0 & x_7 & 0 & -p & x_3 & x_5 & 0 \\ & 0 & x_6 & -q & -x_5 & 0 & x_4 \\ & & 0 & x_5 & -x_2 & -x_4 & 0 \\ & & & 0 & r & s & -x_3 \\ & & - & & 0 & x_3 & x_1 \\ & & & & & 0 & x_2 \\ & & & & & & 0 \end{pmatrix},$$

where

$$\begin{aligned} p &= x_6 - a_1x_5 + a_2x_4 - a_3x_3 + a_4x_2 + a_6x_1, \\ q &= a_3x_5 - a_4x_4 - a_6x_2, \\ r &= x_4 - a_1x_3 + a_2x_2, \\ s &= a_3x_3 - a_4x_2 - a_6x_1. \end{aligned}$$

It may be checked directly from Definition 1.1 that Φ_5 and Φ_7 are Klein matrices. The above expressions are far from canonical. Different choices are related as described in Theorem 1.3(b).

8.2. **Plane cubics.** Let C be a smooth curve of genus one, realised as a plane cubic $C_3 \subset \mathbb{P}^2$ with hyperplane section H. We embed C in $\mathbb{P}^8$ via $|3H|$ to give a genus one normal curve C_9. We explain how to construct a Klein matrix for C_9 from the ternary cubic $U(x, y, z)$ defining C_3.

Let $\mathcal{O}(1) = \mathcal{O}(H)$ be the line bundle associated to the embedding $C_3 \subset \mathbb{P}^2$. It is tautological that C_3 has Klein matrix

$$\Phi_3 = \begin{pmatrix} 0 & z & -y \\ -z & 0 & x \\ y & -x & 0 \end{pmatrix}.$$

By Proposition 3.1, $\Phi_3 = \Phi(\mathcal{E})$ where $\mathcal{E}$ is an indecomposable rank 2 vector bundle on C with $\det \mathcal{E} \simeq \mathcal{O}(1)$. Since $\det(\mathcal{E} \otimes \mathcal{O}(1)) \simeq \mathcal{O}(3)$ it is natural to consider the matrix of cubic forms

$$\begin{pmatrix} xI_3 \\ yI_3 \\ zI_3 \end{pmatrix} \begin{pmatrix} 0 & z & -y \\ -z & 0 & x \\ y & -x & 0 \end{pmatrix} \begin{pmatrix} xI_3 & yI_3 & zI_3 \end{pmatrix}.$$

Let Φ' be the 9×9 alternating matrix of linear forms on $\mathbb{P}^8$ obtained by
(i) substituting $x_1, \ldots, x_{10}$ for $x^3, y^3, z^3 \ldots, xyz$, and
(ii) using the equation $U = 0$ to eliminate one of the x_i.

By [12, Lemma 4.2] we have

$$\Phi' = B^T \Phi(\mathcal{E} \otimes \mathcal{O}(1))B$$

where B represents the linear map

$$H^0(C,\mathcal{E}) \otimes H^0(C,\mathcal{O}(1)) \to H^0(C,\mathcal{E}\otimes\mathcal{O}(1)).$$

It is clear that Φ' has rank 2 on C_9. But since rows 1, 5 and 9 sum to zero, it is not a Klein matrix. However, after step (i), one of the 8×8 Pfaffians is a non-zero irreducible quartic. So $\operatorname{rank}(B) = 8$ and Φ' can be modified to give a Klein matrix by changing the entries in just one row and column.

The following recipe was found by studying numerical examples using Algorithm 7.2. We write our ternary cubic in the form $U = x\alpha + y\beta + z\gamma$ where α, β, γ are quadrics in x, y, z. We then consider the matrix of cubic forms $P^T M P$ where

$$M = \begin{pmatrix} 0 & z & -y & \alpha \\ -z & 0 & x & \beta \\ y & -x & 0 & \gamma \\ -\alpha & -\beta & -\gamma & 0 \end{pmatrix} \text{ and } P = \begin{pmatrix} xI_3 & yI_3 & zI_3 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix}.$$

Let Φ be the 10×10 alternating matrix of linear forms on $\mathbb{P}^8$ obtained by following steps (i) and (ii) above. Since $\operatorname{pf}(M) = x\alpha + y\beta + z\gamma$ it is clear that Φ has rank 2 on C_9. Deleting the last row and column gives the matrix Φ' considered above. We claim that deleting the first row and column instead gives a Klein matrix for C_9.

To prove our claim it suffices to show that the last row of Φ cannot be written as a linear combination of the other rows. We suppose for a contradiction that this is possible. Reading off from the first 3 columns we find that there are linear forms p, q, r in x, y, z such that

$$\begin{pmatrix} 0 & z & -y \\ -z & 0 & x \\ y & -x & 0 \end{pmatrix} \begin{pmatrix} p \\ q \\ r \end{pmatrix} = \begin{pmatrix} \alpha \\ \beta \\ \gamma \end{pmatrix}.$$

This argument survives step (ii) since U is not divisible by x. Premultiplying by $\begin{pmatrix} x & y & z \end{pmatrix}$ it follows that $U = x\alpha + y\beta + z\gamma$ is identically zero. This is the required contradiction.

8.3. **Curves with a diagonal action of μ_n.** In this subsection we assume that $\operatorname{char}(k) \nmid n$. We take co-ordinates $x_0, \ldots, x_{n-1}$ on $\mathbb{P}^{n-1}$ and agree to read all subscripts mod n. There is a diagonal action of μ_n on $\mathbb{P}^{n-1}$ given by $\zeta : x_i \mapsto \zeta^i x_i$, and an action of $\mathbb{Z}/n\mathbb{Z}$ given by $x_i \mapsto x_{i+1}$.

Let $n \geq 5$ be an odd integer, and let C be a genus one normal curve of degree n, invariant under the actions of μ_n and $\mathbb{Z}/n\mathbb{Z}$. It is shown in [12, Proposition 2.7] that C has a rational point of the form

$$P_0 = (0 : a_1 : a_2 : \ldots : -a_2 : -a_1)$$

and that C has Klein matrix $\Phi = (a_{i-j}x_{i+j})$. The 4×4 Pfaffians of this matrix appear in the works of Klein [18, §11] as relations between theta functions. This is our reason for calling Φ a Klein matrix.

Next we abandon the action of $\mathbb{Z}/n\mathbb{Z}$.

Lemma 8.1. *Let $n = 5$ or $n = 7$. Let C be a genus normal curve of degree n invariant under the diagonal action of μ_n. Then $I(C)$ is generated by the quadrics*

$$\begin{array}{lcl} n = 5 & \tau_0 x_0^2 + x_1 x_4 - \tau_2\tau_3 x_2 x_3 & \text{\& cyclic permutes} \\ n = 7 & \left\{ \begin{array}{r} \tau_0 x_0^2 + x_1 x_6 - (1/\lambda^2)\tau_2\tau_3\tau_4\tau_5 x_2 x_5 \\ \tau_0 x_0^2 + \lambda x_1 x_6 - (1/\lambda^3)\tau_2\tau_3^2\tau_4^2\tau_5 x_3 x_4 \end{array} \right. & \text{\& cyclic permutes} \end{array}$$

for some non-zero $\lambda, \tau_0, \ldots, \tau_{n-1} \in k$ satisfying

$$\prod_{i=0}^{n-1} \tau_i = \left\{ \begin{array}{ll} \lambda & \text{if } n = 5, \\ \lambda^4(\lambda - 1) & \text{if } n = 7. \end{array} \right.$$

Proof: See [10, Proposition 2.8]. □

The variable λ in Lemma 8.1 should be viewed as a co-ordinate on $X_1(n) \simeq \mathbb{P}^1$. Away from a cusp the above equations define a genus one normal curve. The μ_5-invariant curves have Klein matrix

$$\begin{pmatrix} 0 & \tau_1 x_1 & x_2 & -x_3 & -\tau_4 x_4 \\ & 0 & \tau_3 x_3 & x_4 & -x_0 \\ & & 0 & \tau_0 x_0 & x_1 \\ & - & & 0 & \tau_2 x_2 \\ & & & & 0 \end{pmatrix}.$$

The μ_7-invariant curves have Klein matrix

$$\begin{pmatrix} 0 & \tau_0\tau_1\tau_2 x_1 & -\lambda\tau_2 x_2 & -\lambda^2 x_3 & \lambda^2 x_4 & \lambda\tau_5 x_5 & -\tau_5\tau_6\tau_0 x_6 \\ & 0 & \tau_2\tau_3\tau_4 x_3 & -\lambda\tau_4 x_4 & -\lambda^2 x_5 & \lambda^2 x_6 & \lambda\tau_0 x_0 \\ & & 0 & \tau_4\tau_5\tau_6 x_5 & -\lambda\tau_6 x_6 & -\lambda^2 x_0 & \lambda^2 x_1 \\ & & & 0 & \tau_6\tau_0\tau_1 x_0 & -\lambda\tau_1 x_1 & -\lambda^2 x_2 \\ & & - & & 0 & \tau_1\tau_2\tau_3 x_2 & -\lambda\tau_3 x_3 \\ & & & & & 0 & \tau_3\tau_4\tau_5 x_4 \\ & & & & & & 0 \end{pmatrix}.$$

In [10] we took $k = \mathbb{Q}$ and exhibited some counterexamples to the Hasse principle. For example

$$\begin{array}{llcl} n = 5 & (\lambda; \tau_0, \ldots, \tau_4) & = & (30; 1, 1, 2, 3, 5), \\ n = 7 & (\lambda; \tau_0, \ldots, \tau_6) & = & (6; 1, 1, 1, 1, 2^4, 3^4, 5). \end{array}$$

8.4. **Numerical examples.** Let $k=\mathbb{Q}$. In Cremona's tables [7] the first elliptic curve with non-trivial 5-torsion in its Tate-Shafarevich group is labelled 275B3. We saw in [9, Appendix B] that its Tate-Shafarevich group contains a non-zero element with equations

$$\begin{array}{rcl}
0 & = & 11x_1^2 - x_2^2 + 5x_3^2 + x_4^2 - 5x_5^2 \\
0 & = & x_2^2 + 10x_2x_3 + 5x_3^2 + 2x_1x_4 - x_2x_4 - 5x_3x_4 - 5x_2x_5 - 5x_3x_5 \\
0 & = & x_2^2 + 2x_2x_3 + 5x_3^2 + x_2x_4 + x_3x_4 + 2x_1x_5 + x_2x_5 + 5x_3x_5 \\
0 & = & 11x_1x_2 + 55x_1x_3 + 2x_2x_4 + 2x_4^2 - 10x_3x_5 + 10x_5^2 \\
0 & = & 11x_1x_2 + 11x_1x_3 - 2x_3x_4 + 2x_2x_5 - 4x_4x_5.
\end{array}$$

Algorithm 7.2 computes the Klein matrix

$$\left(\begin{array}{ccccc}
0 & -2x_5 & 2x_4 & -x_2-x_3 & x_2+5x_3 \\
 & 0 & -11x_1 & x_3+x_5 & x_2+x_4 \\
 & & 0 & -x_2+x_4 & -5x_3+5x_5 \\
 & - & & 0 & -x_1 \\
 & & & & 0
\end{array}\right).$$

In the case $n=7$ the only known explicit counterexamples to the Hasse principle have a diagonal action of μ_7, so have already been treated in §8.3. To give another numerical example we embed the elliptic curve $y^2+y=x^3-x$ in $\mathbb{P}^6$ via $|6.0+P|$ where $P=(0,0)$. The embedding is given by

$$(x_1:\ldots:x_7) = (1:x:y:x^2:xy:x^3:(y+1)/x)$$

and the image has Klein matrix

$$\left(\begin{array}{ccccccc}
0 & x_1 & -x_2 & 0 & x_2 & x_4 & -x_1+x_3 \\
 & 0 & x_7 & x_2 & -2x_7 & x_1-x_3 & -x_2 \\
 & & 0 & -x_4 & x_1+x_3 & -2x_2 & x_1+x_7 \\
 & & & 0 & -x_4 & -x_6 & x_2-x_5 \\
 & & - & & 0 & 3x_2+x_5 & -2x_1+x_4-2x_7 \\
 & & & & & 0 & x_1-x_2-3x_3 \\
 & & & & & & 0
\end{array}\right).$$

See [13] for further numerical examples, up to degree $n=11$.

9. Relationship with the index

In this section we work over a perfect field k.

Definition 9.1. Let C be a smooth projective curve defined over k. The *index* of C is the least positive degree of a k-rational divisor on C.

It is clear that the index of a genus one normal curve divides its degree. We give a criterion for these numbers to be equal.

Proposition 9.2. *Let $n \geq 5$ be an odd integer. Let C be a genus one normal curve of degree n with Klein matrix Φ. Then C has index n if and only if* $\operatorname{rank} \Phi(P) = n - 1$ *for every $P \in \mathbb{P}^{n-1}(k)$.*

Before giving the proof we need a little more notation. Let H be the divisor of a hyperplane section. For D an effective divisor on C we write $\overline{D}$ for the linear subspace cut out by the Riemann-Roch space $\mathcal{L}(H-D) \subset \mathcal{L}(H)$. So if D is a sum of distinct points then $\overline{D}$ is simply the linear span of these points. In this notation

$$\operatorname{Sec}^r C = \bigcup_{\deg D = r} \overline{D}. \tag{6}$$

Lemma 9.3. *Let C be a genus one normal curve of degree n, and let D, D_1, D_2 be effective divisors on C.*
(i) If $\deg D < n$ *then* $\dim \overline{D} = \deg D - 1$.
(ii) The linear span of $\overline{D_1}$ and $\overline{D_2}$ is $\overline{\operatorname{lcm}(D_1, D_2)}$.
(iii) If $\deg \operatorname{lcm}(D_1, D_2) < n$ *then* $\overline{D_1} \cap \overline{D_2} = \overline{\gcd(D_1, D_2)}$.

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). □

Proof of Proposition 9.2: Let $P \in \mathbb{P}^{n-1}$ with $\operatorname{rank} \Phi(P) < n - 1$. Theorem 1.2 tells us that $P \in \operatorname{Sec}^r C$ for some $r \leq (n-3)/2$. We take r minimal so that $P \notin \operatorname{Sec}^{r-1} C$. Then (6) gives $P \in \overline{D}$ where D is an effective divisor on C of degree r. If P is k-rational then $P^\sigma = P$ for all $\sigma \in \operatorname{Gal}(\overline{k}/k)$. So by Lemma 9.3(iii),

$$P \in \overline{D} \cap \overline{D^\sigma} = \overline{\gcd(D, D^\sigma)}.$$

Since $P \notin \operatorname{Sec}^{r-1} C$ it follows that $D^\sigma = D$. So D is a k-rational divisor of degree r and this shows that the index of C is less than n.

Conversely, suppose that C has index r with $r < n$. Since $r \,|\, n$ and $n \geq 5$ is odd, it follows that $r \leq (n-3)/2$. Let D be a k-rational divisor on C of degree r. By Riemann-Roch we may assume that D is effective. Then $\overline{D}$ is a k-rational linear subspace of $\mathbb{P}^{n-1}$. Let $P \in \overline{D}$ be any k-rational point. Since Φ has rank at most 2 on C it follows that $\operatorname{rank} \Phi(P) \leq 2r < n - 1$. □

Remark 9.4. Let E be an elliptic curve curve defined over a number field k. It is conjectured that the Tate-Shafarevich group of E is finite, equivalently there is a bound on the index of an everywhere locally soluble genus one curve with Jacobian E. It is hoped that Proposition 9.2 might be used to show that genus one curves of large index are "arithmetically complicated" in some precise sense (perhaps in terms of a discriminant or a height).

A related result is the following.

Corollary 9.5. *Let $n \geq 5$ be an odd prime power. Let C be a genus one normal curve of degree n with Klein matrix Φ. If C has index n then every entry of Φ, not on the diagonal, is non-zero.*

Proof: We suppose for a contradiction that $\Phi_{12} = 0$. Then the linear forms in the first row of Φ vanish on a line $\ell \subset \mathbb{P}^{n-1}$. Restricting the submaximal Pfaffians of Φ to ℓ we are left with a single homogeneous polynomial of degree $d = (n-1)/2$. Since $(d, n) = 1$ and n is a prime power, this polynomial has a root over a field k_1 with $[k_1 : k]$ prime to n. So given that C has index n over k, it still has index n over k_1. This is a contradiction to Proposition 9.2. □

References

[1] M.F. Atiyah, Vector bundles over an elliptic curve, *Proc. London Math. Soc.* (3), **7** (1957) 414–452.

[2] A. Aure, W. Decker, K. Hulek, S. Popescu, K. Ranestad, Syzygies of abelian and bielliptic surfaces in $\mathbb{P}^4$, *Internat. J. Math.* **8** (1997), no. 7, 849–919.

[3] N. Bourbaki, Algèbre, Chap. I-X. Hermann, Masson, 1970-1980.

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

[5] 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.

[6] 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.

[7] J.E. Cremona, *Algorithms for modular elliptic curves*, Cambridge University Press, Cambridge, 1997.

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

[9] T.A. Fisher, *On 5 and 7 descents for elliptic curves*, PhD thesis, University of Cambridge, 2000.

[10] T.A. Fisher, Some examples of 5 and 7 descent for elliptic curves over $\mathbb{Q}$, *J. Eur. Math. Soc.* **3** (2001), 169–201.

[11] T.A. Fisher, *The higher secant varieties of an elliptic normal curve*, preprint.

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

[13] T. A. Fisher, website: `http://www.dpmms.cam.ac.uk/~taf1000`

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

[15] R. Hartshorne, *Algebraic geometry*, GTM **52**, Springer-Verlag, 1977.

[16] P. Heymans, Pfaffians and skew-symmetric matrices, *Proc. London Math. Soc.* (3) **19** (1969) 730–768.

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

[18] F. Klein, Über die elliptischen Normalkurven der n-ten Ordnung (1885), in *Gesammelte Mathematische Abhandlungen, 3: Elliptische Funktionen etc.*, R. Fricke et al (eds.) Springer (1923).

[19] MAGMA is described in W. Bosma, J. Cannon and C. Playoust, The Magma algebra system I: The user language, *J. Symb. Comb.* **24**, 235-265 (1997). (See also the Magma home page at `http://magma.maths.usyd.edu.au/magma/`.)

[20] J.-P. Serre, *Algebraic groups and class fields*, GTM **117**, Springer-Verlag, 1988.

[21] A. Simis, Effective computation of symbolic powers by Jacobian matrices, *Comm. Algebra* **24** (1996), no. 11, 3561–3565.

[22] 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`