TORSION POINTS AND MATRICES DEFINING ELLIPTIC CURVES

G. V. RAVINDRA AND AMIT TRIPATHI

Abstract. Let k be an algebraically closed field, $\operatorname{char} \mathrm{k} \neq 2, 3$, and let $X \subset \mathbb{P}^2$ be an elliptic curve with defining polynomial f. We show that any non-trivial torsion point of order r, determines up to equivalence, a unique minimal matrix Φ_r of size $3r \times 3r$ with linear polynomial entries such that $\det \Phi_r = f^r$. We also show that the identity, thought of as the trivial torsion point of order r, determines up to equivalence, a unique minimal matrix Ψ_r of size $(3r-2) \times (3r-2)$ with linear and quadratic polynomial entries such that $\det \Psi_r = f^r$.

1. Introduction

In this note, we investigate matrix representations of homogeneous polynomials. The precise question, which dates back to at least the work of Dickson (see [6]) is the following: given a homogeneous polynomial of degree d in n variables, is it possible to obtain it as the determinant of a matrix whose entries are linear homogeneous polynomials in the same variables.

More recently, questions which are slightly different and more general have been a subject of investigation. These include investigating if a positive integral power of the polynomial has a determinantal representation, removing the restriction that the entries of the matrices are linear so that they are now allowed to be homogeneous polynomials of degree less than d, or demanding that the matrix satisfy additional conditions such as being symmetric or skew-symmetric. Of course, every polynomial f is the determinant of a 1×1 matrix with entry f, and has a trivial Pfaffian (= square root of the determinant) representation via the matrix $\begin{pmatrix} 0 & f \\ -f & 0 \end{pmatrix}$, and so on. To avoid any kind of degeneracy, we will assume that the matrix is *minimal*: i.e., no non-zero scalar entries are allowed in the matrix.

Notice that given an $m \times m$ matrix Φ with linear entries and $M,\ N \in \mathrm{GL}(m, k)$, the determinant of the product $M\Phi N$ is a scalar multiple of the determinant of Φ; hence we shall only be interested in "suitable" equivalence classes of representations rather than all representations.

Questions about matrix representations of polynomials arise in diverse contexts. One such instance is in complexity theory, and is exemplified by the "Permanent vs Determinant conjecture" due to Valiant (see [11]) and its strengthening due to Mulmuley and Sohoni (see [9]). Our interest though stems from classical questions in algebraic geometry, which is a natural setting for the study of homogeneous polynomials and their zero sets, which we briefly describe.

2. Statement of results

In this note, we take up the study of matrix representations of positive integral powers of smooth, cubic homogeneous polynomials in three variables and give explicit descriptions of these representations using methods from algebraic geometry. This is done by first rephrasing the question in terms of vector bundles on an elliptic curve. Here is a brief sketch of how this is done.

Given a vector bundle E on a smooth hypersurface $X \subset \mathbb{P}^n$, $n > 1$, we consider $\mathrm{H}^0_*(X, E) := \bigoplus_{\nu \in \mathbb{Z}} \mathrm{H}^0(X, E(\nu))$ as a graded S-module where $S := \mathrm{H}^0_*(\mathbb{P}^n, \mathcal{O}_{\mathbb{P}^n})$ is the polynomial ring in $(n+$

1) variables. By Serre's theorems, this is a finitely generated S-module. Let $s_i \in \mathrm{H}^0(X, E(a_i))$ for $1 \leq i \leq l$ be a set of minimal generators. Then we have a surjection of $\mathcal{O}_{\mathbb{P}^n}$-sheaves, $L_0 := \bigoplus_{i=1}^{l} \mathcal{O}_{\mathbb{P}^n}(-a_i) \twoheadrightarrow E$, which induces a surjection $\mathrm{H}^0_*(\mathbb{P}^n, L_0) \twoheadrightarrow \mathrm{H}^0_*(X, E)$. The sheafification of the associated minimal graded resolution yields an exact sequence

$$0 \to L_1 \xrightarrow{\Phi} L_0 \to E \to 0,$$

where L_1 is the sheaf corresponding to the first syzygy module. Since X is smooth, and E is a vector bundle on X, it is Cohen-Macaulay. By the Auslander-Buchsbaum formula (see [7], Chapter 19), we see that L_1 is a vector bundle on $\mathbb{P}^n$. Furthermore, $\mathrm{H}^1_*(\mathbb{P}^n, L_1) = 0$ and hence when $n = 2$, it follows by Horrocks' theorem that L_1 is a sum of line bundles on $\mathbb{P}^n$. Consequently, Φ is a minimal square matrix whose entries are homogeneous polynomials in 3 variables whose determinant is the defining polynomial of X. Furthermore, if for example, E is a line bundle, then the size of the matrix Φ is of size atmost $d \times d$. In case E is rank 2 with $\det E = \mathcal{O}_X(\alpha)$ for some $\alpha \in \mathbb{Z}$, then using the alternate bilinear pairing $E \times E \to \det E$, one sees that Φ can be taken to be skew-symmetric (see [2]) of size atmost $2d \times 2d$ and that the Pfaffian of Φ is the defining polynomial of X. Conversely, any such matrix defines a rank 2 bundle E. This establishes a dictionary between equivalence classes of matrices representing the defining polynomial of X, and vector bundles supported on X.

Here is the statement of the main theorem of this note.

Theorem 1. *Let X be an elliptic curve in the plane given by a homogeneous cubic polynomial $f \in k[x_0, x_1, x_2]$. Then up to a constant factor,*

1. *There are 3 (inequivalent) representations of f by symmetric linear determinants and these are in one-to-one correspondence with the non-trivial 2-torsion points of X.*
2. *Every point of the elliptic curve determines, up to equivalence, a linear Pfaffian representation of f which corresponds to a decomposable rank 2 bundle; in addition to these, there are 3 other linear Pfaffian representations of f; each of which correspond to indecomposable rank 2 bundles. Furthermore, these are completely determined by the non-trivial 2-torsion points of X.*
3. *There are 2 (inequivalent) representations of f as Pfaffians of skew-symmetric minimal matrices of size 4×4, each of which correspond to indecomposable rank 2 bundles.*
4. *For any r, there is a bijective correspondence between torsion points of order r and (equivalence classes of) indecomposable $3r \times 3r$ matrices with linear entries whose determinant is f^r.*
5. *For any $r \geq 2$, the identity, thought of as a torsion point of order r, yields a unique (up to equivalence) $(3r-2) \times (3r-2)$ matrix with linear and quadratic entries whose determinant is f^r.*

Remark 1. In Theorem 1.3 and 1.4, we cannot describe the equivalence completely for $r \geq 3$.

As mentioned before, the first part of the above theorem is well-known and a proof can be found for instance in [2].

3. Preliminaries

Let V be the 3-dimensional vector space of linear forms on $\mathbb{P}^2$. Let $\mathbb{M}_{3\times 3}(V)$ denote the space of all 3×3 matrices with entries in V. Let $\mathcal{M}_0 \subset \mathbb{M}_{3\times 3}(V)$ be the open set consisting of matrices whose determinants have smooth zero loci. Let $G_0 := \mathrm{GL}(3, k) \times \mathrm{GL}(3, k)$. Then G_0 acts freely and properly on $\mathcal{M}_0$ via $\Phi \mapsto M\Phi N^t$. This action in turn factors via the group $G_0' := G_0/\mathbb{G}_m$ where $\mathbb{G}_m$ embeds in G_0 diagonally as $\lambda \mapsto (\lambda, \lambda^{-1})$. The determinant map,

$$\det : \mathcal{M}_0 \to \mathbb{P}(\mathrm{Sym}^3 V)$$

which associates to a matrix Φ, its determinant $\det\Phi$, factors via

$$\widetilde{\det} : \mathcal{M}_0/G_0' \to \mathbb{P}(\operatorname{Sym}^3 V).$$

One checks that $\dim \mathcal{M}_0/G_0' = 10$ and $\dim \mathbb{P}(\operatorname{Sym}^3 V) = 9$.

Let $\mathbb{M}^{\mathrm{sym}}_{3\times 3}(V)$ denote the space of all 3×3 symmetric matrices with entries in V. Let $\mathcal{M} \subset \mathbb{M}^{\mathrm{sym}}_{3\times 3}(V)$ be the open set consisting of matrices whose determinants have smooth zero loci. Let $G_1 := \mathrm{GL}(3, k)$. It is clear that the determinant map factors as

$$\widetilde{\det} : \mathcal{M}/G_1 \to \mathbb{P}(\operatorname{Sym}^3 V)$$

where $\mathcal{M}/G_1$ is the quotient for the G_1 action on $\mathcal{M}$ given by $\Phi \mapsto M\Phi M^t$. One checks that $\dim \mathcal{M}/G_1 = \dim \mathbb{P}(\operatorname{Sym}^3 V) = 9$.

Finally, let $\mathbb{M}^{\mathrm{ss}}_{6\times 6}(V)$ denote the space of all 6×6 skew-symmetric matrices with entries in V. There is an embedding

$$\mathbb{M}_{3\times 3}(V) \hookrightarrow \mathbb{M}^{\mathrm{ss}}_{6\times 6}(V)$$

defined by

$$\phi \mapsto \begin{pmatrix} 0 & \phi \\ -\phi^t & 0 \end{pmatrix}.$$

We shall, by abuse of notation, refer to the image of the above embedding by $\mathbb{M}_{3\times 3}(V)$. Let $\mathcal{N}$ denote the open set in $\mathbb{M}^{\mathrm{ss}}_{6\times 6}(V)$ of those matrices whose Pfaffians have smooth zero loci. Let $G_2 := \mathrm{GL}(6, k)$. It is clear that the *Pfaffian* map

$$\mathrm{Pf} : \mathcal{N} \to \mathbb{P}(\operatorname{Sym}^3 V)$$

which associates to a matrix Φ, its *Pfaffian* $\mathrm{Pf}(\Phi)$, which has the property that $(\mathrm{Pf}(\Phi))^2 = \det\Phi$, factors via

$$\widetilde{\mathrm{Pf}} : \mathcal{N}/G_2 \to \mathbb{P}(\operatorname{Sym}^3 V)$$

where $\mathcal{N}/G_2$ is the quotient for the G_2 action on $\mathcal{N}$ is given by $\Phi \mapsto M\Phi M^t$.

For the case of non-degenerate Pfaffian representations, we let

$$\mathcal{X} := \{[\Phi] \in \mathcal{N}/G_2 \mid \Phi \not\sim_{G_2} \begin{pmatrix} 0 & \phi \\ -\phi^t & 0 \end{pmatrix}, \phi \in \mathbb{M}^{\mathrm{ss}}_{3\times 3}(V)\},$$

and this gives a map

$$\widetilde{\mathrm{Pf}}_{\mathrm{indec}} : \mathcal{X} \to \mathbb{P}(\operatorname{Sym}^3 V).$$

4. Linear Matrix representations: Proofs of Theorem 1.1 and 1.2

Proof of Theorem 1.1. Every elliptic curve in the plane has three distinct non-trivial theta characteristics, each of which corresponds to a non-trivial 2-torsion point on the elliptic curve. The required statement is a direct consequence of Proposition 4.2, [2]. □

The following important theorem due to Atiyah (see [1], Theorem 5 and Corollary 1) will play an important role for us.

Theorem 2. *Let X be an elliptic curve.*

(1) *Then for any $r > 0$, there exists an indecomposable vector bundle F_r, unique up to isomorphism, with $h^0(F_r) = 1$. Moreover, $F_0 = \mathcal{O}_X$ and F_r is defined inductively by the exact sequence,*

$$0 \to \mathcal{O}_X \to F_r \to F_{r-1} \to 0.$$

(2) *Let E be any indecomposable rank r bundle of degree 0. Then there exists a line bundle A such that $E \cong F_r \otimes A$ and such that $A^{\otimes r} = \det E$.*

(3) *$F_r \cong F_r^\vee$ (i.e., F_r is self-dual).*

Theorem 3. *With notation as above,*

1. *The general fibre of the morphism* $\widetilde{\mathrm{Pf}}$ *has dimension* 1.
2. *The morphism* $\widetilde{\mathrm{Pf}}_{\mathrm{indec}}$ *is generically finite of degree* 3.

Proof. We will first need to show that the map $\widetilde{\mathrm{Pf}}$ is dominant. By Proposition 5.1 of [2], this is equivalent to the fact that any smooth elliptic curve X supports a rank two vector bundle E with $\det E = \mathcal{O}_X$ and $h^0(E) = 0$ and has a minimal resolution of the form

$$0 \to \mathcal{O}_{\mathbb{P}^2}(-2)^{\oplus 6} \xrightarrow{\Phi} \mathcal{O}_{\mathbb{P}^2}(-1)^{\oplus 6} \to E \to 0. \tag{1}$$

Take any $L \in \mathrm{Pic}^0(X)$, $L \ncong \mathcal{O}_X$, and let ϕ be the matrix in the minimal resolution of L (see Prop 3.1, [2]). Then the bundle $L \oplus L^{-1}$ (which has determinant $\mathcal{O}_X$ and $h^0 = 0$) has a minimal resolution with matrix $\Phi = \begin{pmatrix} 0 & \phi \\ -\phi^t & 0 \end{pmatrix}$. Thus the map $\widetilde{\mathrm{Pf}}$ is dominant. Since $\mathrm{Pic}^0(X) \cong X$, we see that the fibre is indeed at least 1- dimensional.

To understand the fibres, we will consider two cases: namely when $E \cong A \oplus A'$ is a sum of line bundles and the other case when E is indecomposable. So let $E \cong A \oplus A'$. Since $\det E = \mathcal{O}_X$, $A' \cong A^{-1}$ and so $E \cong A \oplus A^{-1}$. Since $h^0(E) = 0$, this implies that $h^0(A) = 0 = h^0(A^{-1})$ and so $\deg A = 0$, $A \ncong \mathcal{O}_X$. Thus the decomposable Pfaffian representations are precisely the ones in the previous paragraph.

Now suppose that E is indecomposable. Then by Theorem 2, there exists a line bundle A of degree 0 such that $E \cong F_2 \otimes A$. Thus E can be written as a non-trivial extension

$$0 \to A \to E \to A \to 0.$$

Taking determinants, we get $A^{\otimes 2} \cong \mathcal{O}_X$. The indecomposable bundle E which is described by the non-trivial extension

$$0 \to \mathcal{O}_X \to E \to \mathcal{O}_X \to 0$$

has $h^0(E) = 1$ and hence is not the desired element. Thus E has to be isomorphic to one of the three non-trivial extensions

$$0 \to \kappa_i \to E \to \kappa_i \to 0, \quad i = 1,\ 2,\ 3,$$

where κ_i's are non-trivial 2-torsion elements in $\mathrm{Pic}^0(X)$. Thus the total number of equivalence classes of indecomposable Pfaffian representations of a smooth cubic is 3. □

We refer the reader to [3, 4] for more general results on Pfaffian representations of plane curves of all degrees.

5. Non-linear matrix representations

As mentioned in the introduction, one might ask whether the defining polynomial of any elliptic curve in the plane can be written as the determinant of say, a minimal (symmetric) 2×2 matrix or as a Pfaffian of a minimal 4×4 skew-symmetric matrix.

5.1. Non-linear determinants.

Proposition 1. *Let* $X \subset \mathbb{P}^2$ *be an elliptic curve.*

1. X *cannot be defined as the zero set of the determinant of a minimal, symmetric* 2×2 *matrix with homogeneous polynomial entries.*
2. *There are two families of* 1*-dimensional minimal, non-symmetric* 2×2 *matrices, transpose to each other, which represent* X *in the above sense.*

Proof. Any such matrix $\begin{pmatrix} a & b \\ b & c \end{pmatrix}$ has determinant of the form $ac - b^2$ where a, b, c are homogeneous polynomials. If $b = 0$, then the determinant is not irreducible, hence the resulting zero locus is not smooth. If $b \neq 0$, the determinant has even degree. Since the elliptic curve is given by a cubic polynomial, the statement of (1) is obvious. For (2), it is easy to see that in the 2×2 matrix $\begin{pmatrix} a & b \\ c & d \end{pmatrix}$, either (a, b) are linear forms and (c, d) are quadratic forms, or (a, c) are linear forms and (b, d) are quadratic forms. The two possibilities (up to a twist) are

$$0 \to \mathcal{O}_{\mathbb{P}^2}(-2)^{\oplus 2} \xrightarrow{\phi} \mathcal{O}_{\mathbb{P}^2}(-1) \oplus \mathcal{O}_{\mathbb{P}^2} \to L \to 0 \quad \text{and,} \tag{2}$$

$$0 \to \mathcal{O}_{\mathbb{P}^2}(-1) \oplus \mathcal{O}_{\mathbb{P}^2}(-2) \xrightarrow{\psi} \mathcal{O}_{\mathbb{P}^2}^{\oplus 2} \to M \to 0. \tag{3}$$

It is straightforward to check (i) (using Riemann-Roch for instance) that $\deg L = 1$ and $\deg M = 2$ and, (ii) ϕ and ψ are transpose to each other.

□

5.2. **Non-linear Pfaffians.** Any skew-symmetric matrix Φ whose Pfaffian, denoted by $\mathrm{Pf}(\Phi)$, is the defining equation of the elliptic curve X has to be of even size since the Pfaffian of any odd sized skew-symmetric matrix is zero. This leaves us with two choices viz. 6×6 which yields a linear Pfaffian representation and 4×4 which yields a non-linear Pfaffian representation of X. Any 4×4 skew-symmetric matrix has the form

$$\Phi = \begin{pmatrix} 0 & a & b & c \\ -a & 0 & d & e \\ -b & -d & 0 & g \\ -c & -e & -g & 0 \end{pmatrix} \quad \text{with } \mathrm{Pf}(\Phi) = \mathrm{ag} - \mathrm{be} + \mathrm{cd}. \tag{4}$$

In particular, we have

$$\deg a + \deg g = \deg b + \deg e = \deg c + \deg d = 3,$$

and so each non-zero entry is either a linear or quadratic polynomial. To determine the possible $\Phi's$ (see [5, 8] for similar computations), we look at the possible minimum resolutions

$$0 \to L_1 \xrightarrow{\Phi} L_0 \to E \to 0.$$

It is easy to check that $L_1 \cong L_0^\vee \otimes \mathcal{O}_{\mathbb{P}^2}(\alpha - 3)$ where $\det E = \mathcal{O}_X(\alpha)$. By twisting with a suitable $\mathcal{O}_X(m)$, we may assume that

$$L_0 = \mathcal{O}_{\mathbb{P}^2}^{\oplus \ell} \oplus \bigoplus_{i=1}^{4-\ell} \mathcal{O}_{\mathbb{P}^2}(-m_i), \quad l \geq 0, \quad 0 < m_1 \leq \cdots \leq m_{4-\ell}.$$

Lemma 1. *The only possible minimum resolutions are of the form*

$$0 \to L_1 \xrightarrow{\Phi} L_0 \to E \to 0,$$

where

(a) $L_0 = \mathcal{O}_{\mathbb{P}^2}^{\oplus 3} \oplus \mathcal{O}_{\mathbb{P}^2}(-1)$, or
(b) $L_0 = \mathcal{O}_{\mathbb{P}^2} \oplus \mathcal{O}_{\mathbb{P}^2}(-1)^{\oplus 3}$.

Proof. We first need to rule out the possibilities $L_0 = \mathcal{O}_{\mathbb{P}^2}^{\oplus 4}$ and $L_0 = \mathcal{O}_{\mathbb{P}^2}^{\oplus 2} \oplus \mathcal{O}_{\mathbb{P}^2}(-m_1) \oplus \mathcal{O}_{\mathbb{P}^2}(-m_2)$ with $0 < m_1 \leq m_2$.

If $L_0 = \mathcal{O}_{\mathbb{P}^2}^{\oplus 4}$, then this implies that $L_1 = \mathcal{O}_{\mathbb{P}^2}(-m)^{\oplus 4}$ for some m. Hence the degrees of all the non-zero terms in the matrix Φ are equal. This is not possible since $\mathrm{Pf}(\Phi)$ has odd degree.

Now suppose that $L_0 = \mathcal{O}_{\mathbb{P}^2}^{\oplus 2} \oplus \mathcal{O}_{\mathbb{P}^2}(-m_1) \oplus \mathcal{O}_{\mathbb{P}^2}(-m_2)$. Since $L_1 = L_0^\vee \otimes \mathcal{O}_{\mathbb{P}^2}(\alpha - 3)$, we see that

$$\begin{gathered} \deg a = 3-\alpha, \qquad \deg b = 3-\alpha-m_1, \qquad \deg c = 3-\alpha-m_2, \\ \deg d = 3-\alpha-m_1, \quad \deg e = 3-\alpha-m_2 \quad \deg g = 3-\alpha-m_1-m_2. \end{gathered}$$

Since $\deg a + \deg g = \deg b + \deg e = \deg c + \deg d = 3$, we see on solving for α, m_1 and m_2, that that this is impossible.

Next let $L_0 = \mathcal{O}_{\mathbb{P}^2}^{\oplus 3} \oplus \mathcal{O}_{\mathbb{P}^2}(-m)$ with $m > 0$. Then $L_1 = \mathcal{O}_{\mathbb{P}^2}(\alpha-3)^{\oplus 3} \oplus \mathcal{O}_{\mathbb{P}^2}(m+\alpha-3)$. We see that, using the fact that $\deg a + \deg g = 3$, this implies that $\deg a = 3-\alpha$ and $\deg g = -m+3-\alpha$. We see that the only possible solution is $m = 1$ and $\alpha = 1$.

Finally suppose that $L_0 = \mathcal{O}_{\mathbb{P}^2} \oplus \bigoplus_{i=1}^{3} \mathcal{O}_{\mathbb{P}^2}(-m_i)$ with $m_3 \geq m_2 \geq m_1 > 0$. Plugging in for $\deg a + \deg g = \deg b + \deg e = \deg c + \deg d = 3$, we get

$$\begin{gathered} \deg a = 3-\alpha-m_1, \qquad \deg b = 3-\alpha-m_2, \qquad \deg c = 3-\alpha-m_3, \\ \deg d = 3-\alpha-m_1-m_2, \quad \deg e = 3-\alpha-m_1-m_3, \quad \deg g = 3-\alpha-m_2-m_3. \end{gathered}$$

Solving these, we get $m_1 = m_2 = m_3 = 1$ and $\alpha = 0$. □

Let

$$0 \to \mathcal{O}_{\mathbb{P}^2}(-2)^{\oplus 3} \oplus \mathcal{O}_{\mathbb{P}^2}(-1) \xrightarrow{\Phi} \mathcal{O}_{\mathbb{P}^2}^{\oplus 3} \oplus \mathcal{O}_{\mathbb{P}^2}(-1) \to E \to 0 \quad \text{and,} \tag{5}$$

$$0 \to \mathcal{O}_{\mathbb{P}^2}(-2)^{\oplus 3} \oplus \mathcal{O}_{\mathbb{P}^2}(-3) \xrightarrow{\Psi} \mathcal{O}_{\mathbb{P}^2}(-1)^{\oplus 3} \oplus \mathcal{O}_{\mathbb{P}^2} \to G \to 0 \tag{6}$$

be the two possibilities from the above lemma. We shall refer to E above (resp. a resolution of E) as being of the *first kind*. Similarly, we shall refer to G above (resp. a resolution of G) as being of the *second kind*.

Lemma 2. *Let E be a rank 2 vector bundle of the first kind on X. Then there is a rank 2 bundle G which fits into an exact sequence*

$$0 \to G \otimes \mathcal{O}_X(-1) \to \mathcal{O}_X^{\oplus 3} \oplus \mathcal{O}_X(-1) \to E \to 0,$$

such that G has a minimal resolution of the second kind. Similarly if G is a rank 2 bundle of the second kind on X, then there is a rank 2 bundle E which fits into an exact sequence

$$0 \to E \otimes \mathcal{O}_X(-2) \to \mathcal{O}_X(-1)^{\oplus 3} \oplus \mathcal{O}_X \to G \to 0,$$

such that E has a minimal resolution of the first kind.

Equivalently, the matrices Φ and Ψ always occur in pairs and satisfy $\Phi.\Psi = f.I_4 = \Psi.\Phi$ where I_4 is the 4×4 identity matrix and $f = \mathrm{Pf}(\Phi) = \mathrm{Pf}(\Psi)$.

Proof. Let $0 \to L_1 \xrightarrow{\Phi} L_0 \to E \to 0$ be a minimal resolution as above. Consider the map $L_0(-3) \xrightarrow{f.I_4} L_0$ given by multiplication by the diagonal matrix $f.I_4$, where f is the polynomial defining X. Since the composite map $L_0(-3) \xrightarrow{f.I_4} L_0 \to E$ is zero, we get a map $L_0(-3) \xrightarrow{\Psi} L_1$ satisfying $\Phi.\Psi = fI_4$. We will now show that Ψ is skew-symmetric. This will in particular prove that $\mathrm{Pf}(\Psi) = f$. To do this, we repeat the same process for the map Ψ, to get a map Φ_0 such that $\Psi.\Phi_0 = fI_4$. Multiplying on the right of both sides by the matrix Φ, we get $f\Phi_0 = f\Phi$. This implies that $\Phi_0 = \Phi$. Thus we have $\Psi.\Phi = fI_4 = \Phi.\Psi$. Taking transposes for the first equality, we get $\Phi^t.\Psi^t = fI_4 = \Phi.\Psi$. Since $\Phi^t = -\Phi$, we get $\Psi^t = -\Psi$. □

Remark 2. There is a constructive proof to show that that if Φ is a skew-symmetric matrix of size $2d \times 2d$, then there exists a companion skew- symmetric matrix Ψ of size $2d \times 2d$ such that $\Psi \circ \Phi = fI_{2d}$ where $f := \mathrm{Pf}(\Phi) = \mathrm{Pf}(\Psi)$ and I_{2d} is the identity matrix of size $2d \times 2d$. The matrix Ψ is obtained from Φ in the following way: the (i,j)-th entry of Ψ is the Pfaffian of the skew-symmetric matrix obtained by deleting the i-th and j-th rows and columns of Φ. We refer the reader to [10] for details.

Corollary 1. *In Lemma 2, E is indecomposable if and only if G is so.*

Proof. Assume that E is decomposable. Then $E \cong A \oplus A^{-1}(\alpha)$ for some degree 0 line bundle A. Here as usual $\det E = \mathcal{O}_X(\alpha)$. This implies that the matrix Φ is degenerate i.e., of the form

$$\Phi = \begin{pmatrix} 0 & 0 & q_2 & l_3 \\ 0 & 0 & q_3 & -l_2 \\ -q_2 & -q_3 & 0 & 0 \\ -l_3 & l_2 & 0 & 0 \end{pmatrix}$$

Then by remark 2, we have

$$\Psi = \begin{pmatrix} 0 & 0 & -l_2 & q_3 \\ 0 & 0 & l_3 & q_2 \\ l_2 & -l_3 & 0 & 0 \\ -q_3 & -q_2 & 0 & 0 \end{pmatrix}$$

and so G is also decomposable. The converse follows by interchanging E and G. □

The following result gives a concrete example of a bundle of the first kind.

Lemma 3. *The bundle $E := T_{\mathbb{P}^2}(-1)_{|X}$ is indecomposable and has a minimal resolution of the first kind.*

Proof. Restricting the Euler sequence on $\mathbb{P}^2$ to X yields the sequence

$$0 \to \mathcal{O}_X(-1) \to \mathcal{O}_X^{\oplus 3} \to E \to 0. \tag{7}$$

Standard cohomology computations will show that E is globally generated with $h^0(E) = 3$ and $h^0(E(-1)) = h^0(E^\vee) = 0$. By Serre duality, $h^1(E) = 0$ and hence E is 1-regular. Let $s \in \mathrm{H}^0(E)$ be a general section. Since E is globally generated, the zero locus is pure of codimension 2 and hence nowhere vanishing. Thus we have an exact sequence of bundles

$$0 \to \mathcal{O}_X \xrightarrow{s} E \to L \to 0.$$

Determinant considerations imply that $L \cong \mathcal{O}_X(1)$. Tensoring this sequence by $\mathcal{O}_X(-1)$ and taking cohomology, we get a cohomology sequence

$$\cdots \to \mathrm{H}^0(X, E(-1)) \to \mathrm{H}^0(X, \mathcal{O}_X) \xrightarrow{\partial} \mathrm{H}^1(X, \mathcal{O}_X(-1)) \to \cdots .$$

Since the first term is zero, this means that the boundary map ∂ is non-zero. In particular, the above extension is non-split. To prove indecomposability, let us suppose that $E = A \oplus B$. Since E is globally generated, this means that both A and B are globally generated too. Hence $\deg(A) \geq 0$ and $\deg(B) \geq 0$. Suppose $\deg(A) = 1$. Then by Riemann-Roch, $h^0(A) = 1$. Global generation implies that there is a surjection $\mathrm{H}^0(A) \otimes \mathcal{O}_X = \mathcal{O}_X \to A$. This implies that $A \cong \mathcal{O}_X$, hence a contradiction. Similarly $\deg(A) \neq 2$ (for then $\deg(B) = 1$ and then we arrive at a contradiction). Thus $\deg(A) = 0$ or $\deg(B) = 0$. Global generation implies that $A \cong \mathcal{O}_X$ or $B \cong \mathcal{O}_X$. Thus we have $E = \mathcal{O}_X \oplus \mathcal{O}_X(1)$, again a contradiction.

Since E is 1-regular and $h^0(E(-\nu)) = 0$ for $\nu > 0$, the minimal generators of E lie in degrees 0 and 1. From the cohomology long exact sequence associated to sequence (7), one first checks that not all its generators are in degree 0 i.e.,

$$\bigoplus_{\nu \in \mathbb{Z}} \mathrm{H}^0(\mathcal{O}_X(\nu)^{\oplus 3}) \to \bigoplus_{\nu \in \mathbb{Z}} \mathrm{H}^0(E(\nu))$$

is not a surjection. This fails for $\nu = 1$ and can be seen as follows. We have the long exact sequence of cohomology for the sequence (7) after tensoring with $\mathcal{O}_X(1)$:

$$\cdots \to \mathrm{H}^0(\mathcal{O}_X(1)^{\oplus 3}) \to \mathrm{H}^0(E(1)) \to \mathrm{H}^1(\mathcal{O}_X) \to \mathrm{H}^1(\mathcal{O}_X(1)) \to \mathrm{H}^1(E(1)) \to 0.$$

Since $\mathrm{H}^1(\mathcal{O}_X(1)) = 0$, this implies that E has one generator in degree 1 which is not generated by the sections in degree 0. The same argument as above shows that these are all the generators and so we have an induced surjection $\mathcal{O}_X^{\oplus 3} \oplus \mathcal{O}_X(-1) \twoheadrightarrow E$. This surjection in turn can be lifted to a minimal resolution of E on $\mathbb{P}^2$:

$$0 \to \mathcal{O}_{\mathbb{P}^2}(-2)^{\oplus 3} \oplus \mathcal{O}_{\mathbb{P}^2}(-1) \xrightarrow{\Phi} \mathcal{O}_{\mathbb{P}^2}^{\oplus 3} \oplus \mathcal{O}_{\mathbb{P}^2}(-1) \twoheadrightarrow E \to 0,$$

such that $\mathrm{Pf}(\Phi)$ is the defining polynomial of X. □

Proof of Theorem 1.3. By Lemma 3, the existence of a 4×4 skew-symmetric matrix whose Pfaffian is the defining polynomial of X is guaranteed. By theorem 2, the bundle E above is unique up to unique isomorphism. By Lemma 2 and Corollary 1, there is an indecomposable bundle G of the second kind, unique up to unique isomorphism. The Pfaffian of the skew-symmetric matrix which occurs in the minimal resolution of G is the defining polynomial of X. This finishes of the proof. □

6. Higher order torsion points on an elliptic curve

Theorem 4. *Let $X \subset \mathbb{P}^2$ be a smooth elliptic curve with defining polynomial f. Let Φ_r be a minimal $3r \times 3r$ linear matrix such that*

$$\mathrm{Coker}[\mathcal{O}_{\mathbb{P}^2}(-2)^{\oplus 3\mathrm{r}} \xrightarrow{\Phi_\mathrm{r}} \mathcal{O}_{\mathbb{P}^2}(-1)^{\oplus 3\mathrm{r}}]$$

is an indecomposable rank r bundle E with $\det E = \mathcal{O}_X$. Then $\det \Phi_r = f^r$. Furthermore, such E and Φ_r exist and there is a bijective correspondence between the set of such bundles and the non-trivial r-torsion points of X.

Proof. Consider the exact sequence

$$0 \to \mathcal{O}_{\mathbb{P}^2}(-2)^{\oplus 3r} \xrightarrow{\Phi_r} \mathcal{O}_{\mathbb{P}^2}(-1)^{\oplus 3r} \to E \to 0,$$

thought about as a minimal resolution of the bundle E. Then locally since $E \cong \mathcal{O}_X^{\oplus r}$, Φ_r is the diagonal matrix

$$\Phi_r = (f, f, \cdots, f, 1, \cdots, 1)$$

with f occuring r times, and so $\det E = f^r$. Since E is indecomposable of degree 0, by Theorem 2, $E \cong F_r \otimes A$ for some line bundle A with $A^{\otimes r} = \mathcal{O}_X$. Finally $h^0(E) = 0$ implies that $A \not\cong \mathcal{O}_X$.

To prove the converse, we first check (the details of which we omit) that any rank r bundle E obtained as a repeated extension of an r-torsion line bundle with itself has the following properties:

(i) E is 1-regular (in the sense of Castelnuovo-Mumford),
(ii) $h^0(E(-\nu)) = 0$ for $\nu \geq 0$, and
(iii) $\det(E) = \mathcal{O}_X$.

Conditions (i) and (ii) imply that E has all its minimal generators in degree 1 and Riemann-Roch implies that there are $3r$ of them. So E has a minimal resolution of the form

$$0 \to L_1 \to L_0 \cong \mathcal{O}_{\mathbb{P}^2}(-1)^{\oplus 3r} \to E \to 0,$$

where L_1 is a sum of line bundles on $\mathbb{P}^2$. Dualising as before, we get

$$0 \to L_0^\vee \to L_1^\vee \to E^\vee(3) \to 0. \qquad (8)$$

Now

$$E^\vee \cong (F_r \otimes A)^\vee \cong F_r^\vee \otimes A^\vee \cong F_r \otimes A'$$

where $A' = A^\vee \cong A^{r-1}$, and the surjection

$$L_1^\vee(-3) \to E^\vee$$

from (8) induces a surjection

$$\mathrm{H}^0_*(\mathbb{P}^2, L_1^\vee) \twoheadrightarrow \mathrm{H}^0_*(X, E^\vee).$$

This together with the fact that $\mathrm{rank}(\mathrm{L}_1) = \mathrm{rank}(\mathrm{L}_0)$, implies that $L_1^\vee \to E^\vee$ is induced by a set of minimal generators. Since $E^\vee$ also satisfies properties (i)-(iii) above and $h^0(E^\vee(1)) = 3r$ by Riemann-Roch, this implies $L_1^\vee(-3) \cong \mathcal{O}_{\mathbb{P}^2}(-1)^{\oplus 3r}$. Thus $L_1 \cong \mathcal{O}_{\mathbb{P}^2}(-2)^{\oplus 3r}$. □

Theorem 5. *Let $X \subset \mathbb{P}^2$ be an elliptic curve and F_r denote the unique indecomposable rank r bundle with $h^0(F_r) = 1$ and $\det F_r = \mathcal{O}_X$. Then F_r has a minimal resolution of the form*

$$0 \to \mathcal{O}_{\mathbb{P}^2}(-2)^{\oplus 3(r-1)} \oplus \mathcal{O}_{\mathbb{P}^2}(-3) \xrightarrow{\Psi_r} \mathcal{O}_{\mathbb{P}^2}(-1)^{\oplus 3(r-1)} \oplus \mathcal{O}_{\mathbb{P}^2} \to F_r \to 0. \tag{9}$$

In particular, Ψ_r is a minimal $(3r-2) \times (3r-2)$ matrix with linear and quadratic polynomial entries such that $\det \Psi_r = f^r$.

Proof. The proof is by induction. For the base case of $r = 2$, F_r is the bundle G above. Now suppose that the theorem holds for F_{r-1}. Consider the exact sequence

$$0 \to \mathcal{O}_X \to F_r \to F_{r-1} \to 0.$$

Since $F_r^\vee \cong F_r$ for all r, we can consider the dual exact sequence

$$0 \to F_{r-1} \to F_r \to \mathcal{O}_X \to 0.$$

Since this is a non-trivial extension, we see that the coboundary map in the long exact sequence of cohomology, $\mathrm{H}^0(X, \mathcal{O}_X) \to \mathrm{H}^1(X, F_{r-1})$ is non-zero. However, $\forall s > 0$, $\mathrm{H}^1(X, F_s(a)) = 0$ for $a > 0$, and so we have a short exact sequence

$$0 \to \mathrm{H}^0(X, F_{r-1}(a)) \to \mathrm{H}^0(X, F_r(a)) \to \mathrm{H}^0(X, \mathcal{O}_X(a)) \to 0 \quad \forall\ a > 0.$$

The graded module $N := \oplus_{a>0} \mathrm{H}^0(X, \mathcal{O}_X(a))$ is generated by its degree 1 elements (and there are three of them). This implies that the minimal generators of F_{r-1} and N together generate F_r and that this set is minimal. Thus we have a surjection

$$\Theta : \left(\mathcal{O}_{\mathbb{P}^2}(-1)^{\oplus 3(r-2)} \oplus \mathcal{O}_{\mathbb{P}^2}\right) \oplus \mathcal{O}_{\mathbb{P}^2}(-1)^{\oplus 3} \twoheadrightarrow F_r.$$

This yields an exact sequence

$$0 \to L_1 \to L_0 := \mathcal{O}_{\mathbb{P}^2}(-2)^{\oplus 3(r-1)} \oplus \mathcal{O}_{\mathbb{P}^2} \to F_r \to 0,$$

where L_1 is the kernel of the the map Θ. Dualising the exact sequence, we get

$$0 \to L_0^\vee \to L_1^\vee \to F_r^\vee(3) \to 0.$$

Now $F_r^\vee \cong F_r$ and since L_0 is a sum of line bundles, the map of graded modules $\mathrm{H}^0_*(L_1^\vee(-3)) \to \mathrm{H}^0_*(F_r)$ is a surjection. This implies, by the same reasoning as in the proof of the above theorem, that $L_1^\vee(-3) \cong L_0$ and thus we are done. □

References

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

[2] Beauville, Arnaud., *Determinantal hypersurfaces*, Dedicated to William Fulton on the occasion of his 60th birthday. Michigan Math. J. 48 (2000), 39–64.

[3] Buckley, Anita, *Elementary transformations of Pfaffian representations of plane curves*, Linear Algebra Appl. 433 (2010), no. 4, 758–780.

[4] Buckley, Anita, Košir, Tomaž, *Plane curves as Pfaffians,* Ann. Sc. Norm. Super. Pisa Cl. Sci. (5) 10 (2011), no. 2, 363–388.

[5] Biswas, I; Biswas, J; Ravindra, G. V., *On some moduli spaces of stable vector bundles on cubic and quartic threefolds,* Journal of Pure and Applied Algebra 212 (2008), No. 10, 2298–2306.

[6] Dickson, Leonard Eugene, *Determination of all general homogeneous polynomials expressible as determinants with linear elements,* Trans. Amer. Math. Soc. 22 (1921), no. 2, 167–179.

[7] Eisenbud, David, *Commutative algebra. With a view toward algebraic geometry,* Graduate Texts in Mathematics, 150. Springer-Verlag, New York, 1995.

[8] Faenzi, Daniele, *Rank 2 ACM bundles on a non-singular cubic surface*, J. Algebra 319 (2008), no. 1, 143-186.

[9] Mulmuley, Ketan D. and Sohoni, Milind, *Geometric complexity theory I: an approach to the P vs. NP and related problems*, SIAM J. Comput. 31 (2001), no. 2, 496526.

[10] Northcott, D. G., *Multilinear algebra*, Cambridge University Press, Cambridge, 1984. x+198 pp.

[11] Valiant, L; *Completeness classes in algebra*, STOC 79: 11th Annual ACM Symposium on Theory of Computing, ACM, 1979, pp. 249–261.

Department of Mathematics and Computer Science, 1 University Boulevard, University of Missouri, St. Louis, MO 63121, USA.

E-mail address: girivarur@umsl.edu

Theoretical Statistics and Mathematics Unit, Indian Statistical Institute, Bangalore 560 059, INDIA.

E-mail address: amittr@gmail.com