Matemática Contemporânea, Vol. 47, 73–81
http://doi.org/10.21711/231766362020/rmc473

Inflection divisors of linear series on an elliptic curve

Ethan Cotterill, Cristhian Garay

Abstract

In this largely-expository note, we describe a class of divisors on elliptic curves that index the inflection points of linear series arising (as subspaces of holomorphic sections) from line bundles on $\mathbb{P}^1$ via pullback along the canonical 2-to-1 projection. Associated to each inflection divisor on an elliptic curve $E_\lambda : y^2 = x(x-1)(x-\lambda)$, there is an associated *inflectionary curve* in (the projective compactification of) the affine plane in coordinates x and λ. These inflectionary curves have remarkable features; among other things, they lead directly to an explicit conjecture for the number of *real* inflection points of linear series on E_λ whenever the Legendre parameter λ is real.

1 Introduction

1.1 Motivation

The *torsion points* of an elliptic curve E defined over a field K are classical objects of study, and they are parametrized by the *division polynomials* defined in [6]. Given integers $k > g > 0$, set $\mu := k - g$. Below

2000 AMS Subject Classification: 14C20, 14N10, 14P25, 14H99, 11G99, 11C08.
Key Words and Phrases: linear series; real algebraic curves; Wronskians.

we introduce an effective divisor $I(\mu, k)$ on E of degree $4\mu(k+1)$ that generalizes the divisor $E[2k]$ of order-$2k$ torsion points, in that

$$I(k-1,k) = \sum_{p \in E[2k]} p - R_\pi$$

where R_π is the ramification divisor of the double cover $\pi : E \longrightarrow \mathbb{P}^1$. This *inflection divisor* is the zero locus of a Wronskian of partial derivatives of a space of regular sections of a line bundle L. When $\mu = k-1$ this *linear series* is complete, and it is well-known that inflection points of a complete series on an elliptic curve are in bijection with torsion points of order $\deg(L)$; see, e.g., [2].

1.2 Formal definition

Suppose that $E = (E, O)$ is given by the affine equation $y^2 = f(x)$ and $O = \infty$, so that $R_\pi = E[2]$. Over the open set $E_y = E \setminus R_\pi$, the Wronskian whose zeroes describe the inflection locus of the linear series with basis

$$\mathcal{F} = \{1, x, \ldots, x^k, y, yx, \ldots, yx^{\mu-1}\}$$

is precisely the determinant of the matrix

$$M(\mu,k) := \left(D^j(x^i y)\right)_{\substack{0 \le i \le \mu-1 \\ k+1 \le j \le k+\mu}}$$

where $D = \frac{d}{dx}$. Accordingly, we set

$$I(\mu,k) := \operatorname{div}(\det M(\mu,k)).$$

2 Properties of inflection divisors

2.1 Basic structure

Each divisor $I(\mu,k)$ is determined by an *inflection polynomial* $P_{\mu,k}(x) \in K[x]$ defined by

$$\det M(\mu,k) = (f^{-(k+1)}y)^\mu P_{\mu,k}(x).$$

The zeroes of $P_{\mu,k}$ give the *x-coordinates* of points belonging to the inflection divisor $I(\mu,k)$. Clearly $I(\mu,k)$ is invariant under the involution $(x,y)\mapsto(x,-y)$ on E_y, and it follows that $\deg_x(P_{\mu,k})=2\mu(k+1)$. More to the point, if we write $f=x(x-1)(x-\lambda)$ in Legendre form with $\lambda\in\mathbb{C}$, we may view $P_{\mu,k}$ as a function of both x and λ, and $\deg_\lambda(P_{\mu,k})=\mu(k+1)$.

The case $\mu=1$ is distinguished: in that case the matrix $M=M(\mu,k)$ is a 1×1 matrix, and the corresponding family of inflection polynomials $P_{1,k}$ is described inductively by the rule

$$P_{1,k+1}=D(P_{1,k})f+(-k+1/2)P_{1,k}D(f) \tag{1}$$

for all $k\geq 0$, subject to the seed datum $P_{1,0}=\frac{1}{2}D(f)$.

Inflection polynomials associated with higher values of μ may be realized as polynomials in the "basic" inflection polynomials $P_{1,k}$, as follows.

Lemma 2.1. *Given positive integers $\mu\geq 2$ and $k\geq 3$, set $n=k+1$. There exists a homogeneous polynomial $Q_{\mu,n}\in\mathbb{Z}[t_{1-\mu},\dots t_0,\dots,t_{\mu-1}]$ of degree μ for which*

$$P_{\mu,k}=Q_{\mu,n}|_{t_\ell=P_{1,n+\ell-1}} \tag{2}$$

where

$$Q_{\mu,n}(t_{1-\mu},\dots t_0,\dots,t_{\mu-1}):=\det\left((n+j)_{(i)}t_{j-i}\right)_{0\leq i,j\leq\mu-1}$$

and where, for any non-negative integers a and i, $a_{(i)}=\frac{a!}{(a-i)!}$ denotes the i-th falling factorial of a.

Proof. We make use of the following expression from [2]:

$$\det\,(M(\mu,k))\;=\;\det\left(\frac{(k+1+j)!}{(k+1+j-i)!}D^{k+1+j-i}y\right)_{0\leq i,j\leq\mu-1}. \tag{3}$$

Substituting $t_{j-i}=D^{k+1+j-i}y$ and $n=k+1$ in (3) yields

$$\det\,(M(\mu,k))\;=\;\det\left(\frac{(n+j)!}{(n+j-i)!}t_{j-i}\right)_{0\leq i,j\leq\mu-1}=Q_{\mu,n}|_{t_\ell=D^{n+\ell}y},$$

The desired result now follows from the fact that $D^{n+\ell}y=f^{n+\ell}yP_{1,n+\ell-1}$, since $Q_{\mu,n}|_{t_\ell=D^{n+\ell}y}=(f^{-n}y)^\mu Q_{\mu,n}|_{t_\ell=P_{1,n+\ell-1}}$. □

The upshot of Lemma 2.1 is that the projective geometry of the inflection divisor $I(\mu, k)$ is controlled by the inductive prescription (1) for basic inflection polynomials, and also (in a more obscure way) by the hypersurfaces of degree μ defined by the $Q_{\mu,n}$ in $\mathbb{P}^{2(\mu-1)}$. Note that the division polynomials are essentially the inflection polynomials $P_{k-1,k}$.

Remarks.

i. When $m \geq 3$, a basis for the complete linear series on E induced by the divisor $m \cdot \infty$ is $\mathcal{F} = \{x^i, x^j y\}_{i,j}$, where

$$\begin{cases} 0 \leq i \leq m/2,\ 0 \leq j \leq (m-4)/2 & \text{if } m \text{ is even,} \\ 0 \leq i \leq (m-1)/2,\ 0 \leq j \leq (m-3)/2 & \text{if } m \text{ is odd.} \end{cases}$$

It should be straightforward to adapt our degeneration-based analysis of inflection points to account for the odd case as well.

ii. Whenever the curve E is defined over a field of positive characteristic $p \neq 2, 3$, it has a Weierstrass equation and the associated Wronskian $\det M(\mu, k)$ may still be defined by using Hasse derivatives in place of the differential operators $D^i = \frac{d^i}{dx^i}$. Stöhr and Voloch have used these Wronskians to carry out (refinements of) rational point counts for algebraic curves defined over finite fields [8].

iii. The Wronskian of a rank-r linear series (L, V) on an arbitrary algebraic curve C naturally defines an *Euler class*, associated to (the determinant of) the jet bundle $J^{r+1}(L)$ on C whose fiber in a point p is $H^0(L/L(-(r+1)p))$. Moreover, when C is (hyper)elliptic and L arises via pullback from $\mathbb{P}^1$, the jet bundle in question is *(relatively) orientable*, which ensures that the Wronskian defines an *arithmetic* Euler class in the sense of $\mathbb{A}^1$-homotopy theory [4, 5]. In [3] we calculate a global arithmetic inflection formula over an arbitrary field of characteristic $p \neq 2, 3$, and we analyze the geometric meaning of its constituent local arithmetic inflection indices over $\mathbb{F}_q$.

2.2 Symmetries of inflection polynomials

The inductive formula (1) has a number of interesting consequences.

Lemma 2.2. *For every positive integer $k \geq 1$, we have*

$$P_{1,k}(x,\lambda) = P_{1,k}(x,z) \text{ and } P_{1,k}(x+1,\lambda+1) = P_{1,k}(-x,-\lambda). \quad (4)$$

Here by $P_{1,k}(x,z)$ we mean the polynomial obtained by homogenizing with respect to z to obtain a degree-$2(k+1)$ polynomial in $\mathbb{Q}[x,\lambda,z]$; and then dehomogenizing with respect to λ to obtain a degree-$2(k+1)$ polynomial in $\mathbb{Q}[x,z]$.

Proof. See [1, Lemma 4.2]. □

Lemma 2.2 implies that the monodromy group associated to the projection from the point $[0:0:1]$ of the projective closure $\overline{\mathcal{C}(1,k)}$ of the *inflectionary curve* $\mathcal{C}(1,k)$ defined by $P_{1,k} = 0$ inside $\mathbb{P}^2_{x,\lambda,z}$ contains transpositions that freely permute the points p_1, p_2, and p_3 with coordinates $[0:0:1]$, $[0:1:0]$, and $[1:1:1]$. In particular, the singularities of $\overline{\mathcal{C}(1,k)}$ in these three points are analytically isomorphic.

Conjecture 2.3. *For every positive integer $k \geq 1$, the plane curve $\overline{\mathcal{C}(1,k)}$ is nonsingular along $\mathbb{P}^2 \setminus \{p_1,p_2,p_3\}$.*

Remarks.

iv. The second symmetry in (4) suggests that modular properties of E and λ are at play in Conjecture 2.3.

v. The canonical (i.e. Néron–Tate) height of a torsion point on E is zero. In [7], Silverman obtains bounds on the canonical heights of inflection points for pluricanonical series on hyperelliptic curves. It would be interesting to extend his analysis to our incomplete series on the elliptic curve E, as doing so would quantify the extent to which inflection points "stray" from the torsion lattice on the universal cover of E.

2.3 Genera of inflectionary curves

The inductive prescription (1) for the inflection polynomials $P_{1,k}$ strongly suggests the following is true.

Conjecture 2.4. *For $k \geq 1$, let $\Delta_1(k) = Conv\{(0, k+1), (k-1, k+1), (k-1, 2), (2k-2, 2)\}$ and $\Delta_2(k) = Conv\{(2k, 1), (2k+1, 1), (2k+1, 0), (2k+2, 0)\}$. Then*

1. *$P_{1,k}$ has support:*

$$Supp(P_{1,k}) = (\Delta_1(k) \cap \mathbb{Z}^2) \cup (\Delta_2(k) \cap \mathbb{Z}^2)$$

2. *Let $\sigma_k : Supp(P_{1,k}) \to Supp(P_{1,k})$ be the reflection along the diagonal $Conv\{(0, k+1), (2k+2, 0)\}$, this is $\sigma_k(i, j) = (i, 2k+2-i-j)$. If $a^{(k)}_{(i,j)} x^i \lambda^j$ is a monomial of $P_{1,k}$, then $a^{(k)}_{(i,j)} = a^{(k)}_{\sigma_k(i,j)}$.*

Conjecture 2.4 predicts that whenever $k \geq 2$, the lower faces of the Newton polygon of $P_{1,k}$ that contribute to the singularity of the inflectionary curve $\overline{\mathcal{C}(1,k)}$ in $(0,0)$ are $\Gamma_1(k) := \mathrm{Conv}\{(0, k+1), (k-1, 2)\}$ and $\Gamma_2(k) = \mathrm{Conv}\{(k-1, 2), (2k+1, 0)\}$. In particular, we have

$$P_{1,k}|_{\Gamma_1(k)} = y^2 Q_{k-1}(x, y), \quad P_{1,k}|_{\Gamma_2(k)} = x^{k-1}(a_k y^2 + b_k x^{k+2})$$

where $Q_{k-1}(x, y) = \prod_{j=1}^{k-1}(a_j x + b_j y)$. Geometrically, this means that the singularity in $(0,0)$ is the union of $k-1$ smooth branches corresponding to the linear factors of Q_{k-1}, together with an additional singularity of analytic type $y^2 + x^{k+2} = 0$. Assuming all of these intersect transversely, we would expect the following to hold.

Conjecture 2.5. *The delta-invariant of the singularity of the inflectionary curve $P_{1,k} = 0$ in $(0,0)$ is $\delta = \lfloor \frac{k^2}{2} \rfloor + k$.*

Indeed, one arrives at Conjecture 2.5 by viewing δ as a "local number of nodes". The $(k-1)$-fold point defined by Q_{k-1} generically will have delta-invariant $\binom{k-1}{2}$, while $y^2 + x^{k+2} = 0$ has delta-invariant $\lfloor \frac{k}{2} \rfloor + 1$.

Finally, their union will generically have delta-invariant equal to $2(k-1)$ plus their sum.

Conjectures 2.3 and 2.5, in tandem with the degree-arithmetic genus formula for plane curves, predict that the geometric genus of $\overline{\mathcal{C}(1,k)}$ is $p_g = \binom{2k+1}{2} - 3\lfloor \frac{k^2}{2} \rfloor - 3k$.

3 Reality phenomena

3.1 Separability

In the papers [2] and [1], our primary objective was constructing real linear series with many real inflection points on (hyper)elliptic curves X. The situation when $X = E$ is elliptic and the real locus $E(\mathbb{R})$ has two connected components is distinguished.

Conjecture 3.1. *When the polynomial $f = x(x-1)(x-\lambda)$ has three distinct real roots (i.e., when $\lambda \in \mathbb{R}$), each corresponding inflection polynomial $P_{\mu,k}$ has only simple roots in x away from $\{0,1\}$ for every fixed value of λ.*

In particular, Conjecture 3.1 predicts that each real zero $x = \gamma$ of $P_{\mu,k}$ lifts to either 2 or 0 real points of $I(\mu,k)$, depending upon whether the number $P_{\mu,k}(\gamma,\lambda)$ is positive or not.

3.2 Real loci of inflectionary curves in the maximally-real case

Conjecture 3.2. *Let $\mu \geq 1$ and $k \geq \mu + 1$ be nonnegative integers. Assume that f is associated with a real Legendre parameter λ. For every fixed value of $\lambda \neq 0, 1$, the corresponding inflection polynomial $P_{\mu,k}$ has precisely either μ or 2μ real roots $x = \gamma$ such that $f(\gamma,\lambda) > 0$, depending upon whether $k - \mu$ is even or odd.*

The most striking evidence in favor of Conjecture 3.2 is graphical in nature; see [1] and Figure 1 above. The topology of the real locus of the

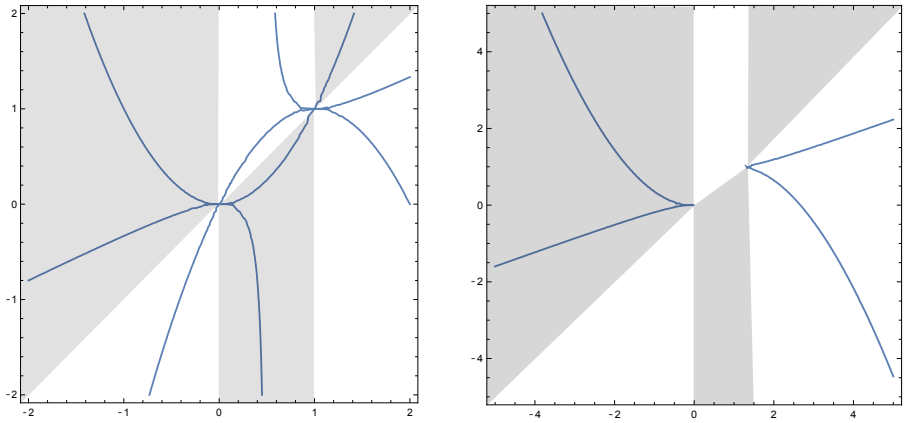

Figure 1: Real loci of the inflectionary curves $\mathcal{C}(1,2)$ and $\mathcal{C}(1,3)$, respectively. The regions where $f > 0$ are shaded.

inflectionary curve $\overline{\mathcal{C}(\mu,k)}$ defined by $P_{\mu,k} = 0$ seemingly is controlled by the singularities in the distinguished points $[0:0:1]$, $[0:1:0]$, and $[1:1:1]$.

References

[1] E. Cotterill and C. Garay, *Real inflection points of real linear series on an elliptic curve*, Experiment. Math. (2019), doi:10.1080/10586458.2019.1655815.

[2] I. Biswas, E. Cotterill, and C. Garay, *Real inflection points of real hyperelliptic curves*, Trans. AMS **372** (2019), no. 7, 4805–4827.

[3] E. Cotterill, I. Darago, and C. Han, *Arithmetic inflection formulas for linear series on hyperelliptic curves*, in progress.

[4] J. Kass and K. Wickelgren, *The class of Eisenbud–Khimshiashvili–Levine is the local $\mathbb{A}^1$-Brouwer degree*, Duke Math J. **168** (2019), no. 3, 429–469.

[5] J. Kass and K. Wickelgren, *An arithmetic count of the lines on a smooth cubic surface*, arXiv:1708.01175, to appear in Compositio Math.

[6] J. Silverman, "The arithmetic of elliptic curves", second edition, Springer, 2009.

[7] J. Silverman, *Some arithmetic properties of Weierstrass points: hyperelliptic curves*, Bull. Brazilian Math. Soc. **21** (1990), no. 1, 11–50.

[8] K.-O. Stöhr and J. F. Voloch, *Weierstrass points and curves over finite fields*, Proc. London Math. Soc. **52** (1986), no. 3, 1–19.

Ethan Cotterill
Instituto de Matemática, UFF
Rua Prof Waldemar de Freitas, S/N,
24.210-201 Niterói RJ, Brazil
Email: cotterill.ethan@gmail.com

Cristhian Garay López
Departamento de Matemáticas, Centro de Investigación y de Estudios Avanzados del IPN
Apartado Postal 14-740, 07000. Ciudad de México, México.
Email: cgaray@math.cinvestav.mx