# Arithmetic inflection formulae for linear series on hyperelliptic curves

Joint with I. Darago (U. Chicago) and C. Han (U. Georgia)

31 August 2020

# Motivation: curve geometry over arbitrary fields

In classical AG, we study algebraic curves over $\mathbb{C}$ (i.e., compact Riemann surfaces) via their holomorphic maps to $\mathbb{P}^r$.

# Motivation: curve geometry over arbitrary fields

In classical AG, we study algebraic curves over $\mathbb{C}$ (i.e., compact Riemann surfaces) via their holomorphic maps to $\mathbb{P}^r$.

Degree-$d$ holomorphic maps $C \to \mathbb{P}^r$ are prescribed by *linear series*: pairs $(L, V)$ where $L$ is a degree-$d$ line bundle and $V \subset H^0(C, L)$ is an $(r+1)$-dimensional subspace of holomorphic sections.
**Notation**: $g^r_d$.

# Motivation: curve geometry over arbitrary fields

In classical AG, we study algebraic curves over $\mathbb{C}$ (i.e., compact Riemann surfaces) via their holomorphic maps to $\mathbb{P}^r$.

Degree-$d$ holomorphic maps $C \to \mathbb{P}^r$ are prescribed by *linear series*: pairs $(L, V)$ where $L$ is a degree-$d$ line bundle and $V \subset H^0(C, L)$ is an $(r+1)$-dimensional subspace of holomorphic sections.
**Notation**: $g^r_d$.

The fundamental *local* invariant of a $g^r_d$ is its *inflection* in a point $p \in C$, which is the total deviation of the $p$-vanishing orders of the $g^r_d$ from the generic sequence $(0, 1, \ldots, r)$.

# Motivation: curve geometry over arbitrary fields

In classical AG, we study algebraic curves over $\mathbb{C}$ (i.e., compact Riemann surfaces) via their holomorphic maps to $\mathbb{P}^r$.

Degree-$d$ holomorphic maps $C \to \mathbb{P}^r$ are prescribed by *linear series*: pairs $(L, V)$ where $L$ is a degree-$d$ line bundle and $V \subset H^0(C, L)$ is an $(r+1)$-dimensional subspace of holomorphic sections.
**Notation**: $g^r_d$.

The fundamental *local* invariant of a $g^r_d$ is its *inflection* in a point $p \in C$, which is the total deviation of the $p$-vanishing orders of the $g^r_d$ from the generic sequence $(0, 1, \ldots, r)$.

**Q**: What is the total inflection of a $g^r_d$ over an arbitrary field $F$?

# Inflection as an Euler class

When $F = \mathbb{C}$, we can compute inflection using jet bundles:

# Inflection as an Euler class

When $F = \mathbb{C}$, we can compute inflection using jet bundles:

The *inflection divisor* of $(L, V)$ is the non-surjectivity locus of

$$V \otimes \mathcal{O} \to J^{r+1}(L) \tag{1}$$

where $J^{r+1}(L)$ is the rank-$(r+1)$ bundle over $C$ with fibers $H^0(L/L(-(r+1)p))$.

# Inflection as an Euler class

When $F = \mathbb{C}$, we can compute inflection using jet bundles:

The *inflection divisor* of $(L, V)$ is the non-surjectivity locus of

$$V \otimes \mathcal{O} \to J^{r+1}(L) \tag{1}$$

where $J^{r+1}(L)$ is the rank-$(r+1)$ bundle over $C$ with fibers $H^0(L/L(-(r+1)p))$.

So the *class* of the inflection divisor is $c_1(\det J^{r+1}(L)) = c_1(L^{\otimes(r+1)} \otimes K_C^{\otimes\binom{r+1}{2}}) = (r+1)d + \binom{r+1}{2}(2g-2)$ (Plücker's formula).

# Inflection as an Euler class

When $F = \mathbb{C}$, we can compute inflection using jet bundles:

The *inflection divisor* of $(L, V)$ is the non-surjectivity locus of

$$V \otimes \mathcal{O} \to J^{r+1}(L) \tag{1}$$

where $J^{r+1}(L)$ is the rank-$(r+1)$ bundle over $C$ with fibers $H^0(L/L(-(r+1)p))$.

So the *class* of the inflection divisor is $c_1(\det J^{r+1}(L)) = c_1(L^{\otimes(r+1)} \otimes K_C^{\otimes\binom{r+1}{2}}) = (r+1)d + \binom{r+1}{2}(2g-2)$ (Plücker's formula).

**Upshot**: "inflection is an Euler class" of a line bundle over $C$.

# Inflection over arbitrary fields

**Q:** Can we write down analogues of Plücker's formula over non-algebraically closed fields $F$?

# Inflection over arbitrary fields

**Q:** Can we write down analogues of Plücker's formula over non-algebraically closed fields $F$?

**A:** Using $\mathbb{A}^1$-*homotopy theory*, we can, because inflection is an Euler class (caveat: $\mathrm{Hom}(T_C, \det J^{r+1}(L))$ should also be a tensor square).

# Inflection over arbitrary fields

**Q:** Can we write down analogues of Plücker's formula over non-algebraically closed fields $F$?

**A:** Using $\mathbb{A}^1$-*homotopy theory*, we can, because inflection is an Euler class (caveat: $\mathrm{Hom}(T_C, \det J^{r+1}(L))$ should also be a tensor square).

The formulas will be valued in the Grothendieck–Witt group $\mathrm{GW}(F)$, which is the (additive) groupification of the monoid of quadratic forms over $F$.

# Inflection over arbitrary fields

**Q:** Can we write down analogues of Plücker's formula over non-algebraically closed fields $F$?

**A:** Using $\mathbb{A}^1$-*homotopy theory*, we can, because inflection is an Euler class (caveat: $\mathrm{Hom}(T_C, \det J^{r+1}(L))$ should also be a tensor square).

The formulas will be valued in the Grothendieck–Witt group $\mathrm{GW}(F)$, which is the (additive) groupification of the monoid of quadratic forms over $F$.

$\mathrm{GW}(F)$ is generated by classes $\langle a \rangle$ associated to the bilinear form $(x, y) \to axy, a \in F$ modulo relations. The *hyperbolic class* $\mathbb{H} := \langle 1 \rangle + \langle -1 \rangle$ is distinguished.

# Inflection over arbitrary fields

**Q:** Can we write down analogues of Plücker's formula over non-algebraically closed fields $F$?

**A:** Using $\mathbb{A}^1$-*homotopy theory*, we can, because inflection is an Euler class (caveat: $\operatorname{Hom}(T_C, \det J^{r+1}(L))$ should also be a tensor square).

The formulas will be valued in the Grothendieck–Witt group $\mathrm{GW}(F)$, which is the (additive) groupification of the monoid of quadratic forms over $F$.

$\mathrm{GW}(F)$ is generated by classes $\langle a \rangle$ associated to the bilinear form $(x, y) \to axy, a \in F$ modulo relations. The *hyperbolic class* $\mathbb{H} := \langle 1 \rangle + \langle -1 \rangle$ is distinguished.

**Instructive examples:** $\mathrm{GW}(\mathbb{C}) = \mathbb{Z}$ (only invariant is the rank); $\mathrm{GW}(\mathbb{R}) = \mathbb{Z} \times \mathbb{Z}$ (rank and signature); $\mathrm{GW}(\mathbb{F}_q) = \mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$ (rank and discriminant, modulo squares).

# A test case for Grothendieck–Witt-valued inflection

In this talk, we will focus on GW-valued *arithmetic inflection* of arbitrary multiples of the $g^1_2$ on a hyperelliptic curve.

# A test case for Grothendieck–Witt-valued inflection

In this talk, we will focus on GW-valued *arithmetic inflection* of arbitrary multiples of the $g^1_2$ on a hyperelliptic curve.

Here $C$ is *hyperelliptic* if and only if $C$ admits a (ramified) 2-to-1 map $\pi : C \to \mathbb{P}^1$. If so, the cover is unique, and given by the $g^1_2$.

# A test case for Grothendieck–Witt-valued inflection

In this talk, we will focus on GW-valued *arithmetic inflection* of arbitrary multiples of the $g_2^1$ on a hyperelliptic curve.

Here $C$ is *hyperelliptic* if and only if $C$ admits a (ramified) 2-to-1 map $\pi : C \to \mathbb{P}^1$. If so, the cover is unique, and given by the $g_2^1$.

We can realize $C$ as a plane curve with equation $y^2 = f(x)$, where $\deg(f) = 2g + 1$ iff $\pi$ is ramified over $\infty \in \mathbb{P}^1$. Assume this.

# A test case for Grothendieck–Witt-valued inflection

In this talk, we will focus on GW-valued *arithmetic inflection* of arbitrary multiples of the $g^1_2$ on a hyperelliptic curve.

Here $C$ is *hyperelliptic* if and only if $C$ admits a (ramified) 2-to-1 map $\pi : C \to \mathbb{P}^1$. If so, the cover is unique, and given by the $g^1_2$.

We can realize $C$ as a plane curve with equation $y^2 = f(x)$, where $\deg(f) = 2g + 1$ iff $\pi$ is ramified over $\infty \in \mathbb{P}^1$. Assume this.

Let $\infty_C = \pi^{-1}(\infty)$. We will study the inflection of complete linear series on $C$ associated to even multiples $2\ell\infty_C$. These satisfy the technical caveat (*relative orientability*).

# A test case for Grothendieck–Witt-valued inflection

In this talk, we will focus on GW-valued *arithmetic inflection* of arbitrary multiples of the $g^1_2$ on a hyperelliptic curve.

Here $C$ is *hyperelliptic* if and only if $C$ admits a (ramified) 2-to-1 map $\pi : C \to \mathbb{P}^1$. If so, the cover is unique, and given by the $g^1_2$.

We can realize $C$ as a plane curve with equation $y^2 = f(x)$, where $\deg(f) = 2g + 1$ iff $\pi$ is ramified over $\infty \in \mathbb{P}^1$. Assume this.

Let $\infty_C = \pi^{-1}(\infty)$. We will study the inflection of complete linear series on $C$ associated to even multiples $2\ell\infty_C$. These satisfy the technical caveat (*relative orientability*).

**Goals:** 1) A global arithmetic Euler class; and 2) explicit formulas for local Euler indices, which codify subtle field-specific info.

# A global arithmetic Euler class

**Theorem 1 (C-Darago-Han)**: Let $F$ be a field with $\mathrm{char}(F) \neq 2$, let $L = \mathcal{O}(2\ell\infty_C)$, where $\ell \geq 1$ is a positive integer. Associated to the complete linear series $|L|$ on $C$ there is a well-defined arithmetic inflection class $[\mathrm{Inf}]_{\mathbb{A}^1}$ in $\mathrm{GW}(F)$ given by

$$[\mathrm{Inf}]_{\mathbb{A}^1} = \frac{\gamma_{\mathbb{C}}}{2}\mathbb{H}$$

where $\gamma_{\mathbb{C}} = g(2\ell - g + 1)^2$ is the $\mathbb{C}$-inflectionary Plücker degree.

# A global arithmetic Euler class

**Theorem 1 (C-Darago-Han)**: Let $F$ be a field with $\mathrm{char}(F) \neq 2$, let $L = \mathcal{O}(2\ell\infty_C)$, where $\ell \geq 1$ is a positive integer. Associated to the complete linear series $|L|$ on $C$ there is a well-defined arithmetic inflection class $[\mathrm{Inf}]_{\mathbb{A}^1}$ in $\mathrm{GW}(F)$ given by

$$[\mathrm{Inf}]_{\mathbb{A}^1} = \frac{\gamma_{\mathbb{C}}}{2}\mathbb{H}$$

where $\gamma_{\mathbb{C}} = g(2\ell - g + 1)^2$ is the $\mathbb{C}$-inflectionary Plücker degree.

**Remarks:** The proof is an easy application of a more general result for Euler classes of odd-rank bundles due to Fasel and Levine. The content is that the inflection class is a multiple of $\mathbb{H}$.

# A global arithmetic Euler class

**Theorem 1 (C-Darago-Han)**: Let $F$ be a field with $\mathrm{char}(F) \neq 2$, let $L = \mathcal{O}(2\ell\infty_C)$, where $\ell \geq 1$ is a positive integer. Associated to the complete linear series $|L|$ on $C$ there is a well-defined arithmetic inflection class $[\mathrm{Inf}]_{\mathbb{A}^1}$ in $\mathrm{GW}(F)$ given by

$$[\mathrm{Inf}]_{\mathbb{A}^1} = \frac{\gamma_{\mathbb{C}}}{2}\mathbb{H}$$

where $\gamma_{\mathbb{C}} = g(2\ell - g + 1)^2$ is the $\mathbb{C}$-inflectionary Plücker degree.

**Remarks:** The proof is an easy application of a more general result for Euler classes of odd-rank bundles due to Fasel and Levine. The content is that the inflection class is a multiple of $\mathbb{H}$.

**Example:** When $F = \mathbb{R}$, the sum of signs of (derivatives of) local Wronskians in inflection points is zero.

# Local arithmetic Euler indices via local Wronskians

The behavior of *local* arithmetic Euler indices $\mathrm{ind}_p(s)$ near inflection points $p \in C$ is more interesting.

# Local arithmetic Euler indices via local Wronskians

The behavior of *local* arithmetic Euler indices $\mathrm{ind}_p(s)$ near inflection points $p \in C$ is more interesting.

To calculate these, we first produce a *local Wronskian* determinant for (1) in a neighborhood of the inflection point $p$.

# Local arithmetic Euler indices via local Wronskians

The behavior of *local* arithmetic Euler indices $\mathrm{ind}_p(s)$ near inflection points $p \in C$ is more interesting.

To calculate these, we first produce a *local Wronskian* determinant for (1) in a neighborhood of the inflection point $p$.

For $\mathbb{A}^1$-homotopy theory, we use *Nisnevich* charts, i.e., open étale charts in which residue fields of fibers and targets are isomorphic. Concretely, étale charts arise from projections to the coordinate axes, while Nisnevich charts arise from generic projections.

# Local arithmetic Euler indices via local Wronskians

The behavior of *local* arithmetic Euler indices $\mathrm{ind}_p(s)$ near inflection points $p \in C$ is more interesting.

To calculate these, we first produce a *local Wronskian* determinant for (1) in a neighborhood of the inflection point $p$.

For $\mathbb{A}^1$-homotopy theory, we use *Nisnevich* charts, i.e., open étale charts in which residue fields of fibers and targets are isomorphic. Concretely, étale charts arise from projections to the coordinate axes, while Nisnevich charts arise from generic projections.

We then apply a linear algebraic result of Scheja and Storch to extract $\mathrm{ind}_p(s)$ from the Nisnevich local Wronskian.

# Local arithmetic Euler indices via local Wronskians

The behavior of *local* arithmetic Euler indices $\mathrm{ind}_p(s)$ near inflection points $p \in C$ is more interesting.

To calculate these, we first produce a *local Wronskian* determinant for (1) in a neighborhood of the inflection point $p$.

For $\mathbb{A}^1$-homotopy theory, we use *Nisnevich* charts, i.e., open étale charts in which residue fields of fibers and targets are isomorphic. Concretely, étale charts arise from projections to the coordinate axes, while Nisnevich charts arise from generic projections.

We then apply a linear algebraic result of Scheja and Storch to extract $\mathrm{ind}_p(s)$ from the Nisnevich local Wronskian.

The output of this procedure is a *trace* of a class in $\mathrm{GW}(k(p))$, where $k(p)$ is the splitting field of $p$ and the trace is induced by the field trace of $k(p)$ over $F$.

# Local Wronskians for the hyperelliptic ramification locus

For local calculations, we distinguish between cases according to whether or not $\ell \leq g$; and if $\ell > g$, whether or not the inflection point $p$ belongs to the ramification locus $R_\pi$ of $\pi : C \to \mathbb{P}^1$. For simplicity, assume hereafter that $p \neq \infty_C$.

# Local Wronskians for the hyperelliptic ramification locus

For local calculations, we distinguish between cases according to whether or not $\ell \leq g$; and if $\ell > g$, whether or not the inflection point $p$ belongs to the ramification locus $R_\pi$ of $\pi : C \to \mathbb{P}^1$. For simplicity, assume hereafter that $p \neq \infty_C$.

**Theorem 2 (C-Darago-Han):** Assume that $\ell \leq g$, in which case the complete linear series $|\mathcal{O}(2\ell\infty_X)|$ has basis $\lambda = (1, x, x^2, \ldots, x^\ell)$. The local Wronskian determinant $w(\lambda)$ in a point $p \in R_\pi$ is

$$w(\lambda) = \left(\frac{Dx}{dz}\right)^{\binom{\ell+1}{2}}$$

where $z$ is a Nisnevich coordinate.

# Local Wronskians for the hyperelliptic ramification locus

For local calculations, we distinguish between cases according to whether or not $\ell \leq g$; and if $\ell > g$, whether or not the inflection point $p$ belongs to the ramification locus $R_\pi$ of $\pi : C \to \mathbb{P}^1$. For simplicity, assume hereafter that $p \neq \infty_C$.

**Theorem 2 (C-Darago-Han):** Assume that $\ell \leq g$, in which case the complete linear series $|\mathcal{O}(2\ell\infty_X)|$ has basis $\lambda = (1, x, x^2, \ldots, x^\ell)$. The local Wronskian determinant $w(\lambda)$ in a point $p \in R_\pi$ is

$$w(\lambda) = \left(\frac{Dx}{dz}\right)^{\binom{\ell+1}{2}}$$

where $z$ is a Nisnevich coordinate.

**NB:** This refines the statement that the inflection multiplicity in a point $p \in R_\pi$ is $\binom{\ell+1}{2}$.

# Local Wronskians for the hyperelliptic ramification locus

**Theorem 3 (C-Darago-Han):** Assume $\ell > g$, in which case $|\mathcal{O}(2\ell\infty_X)|$ has basis $\lambda := (1, y, \ldots, x^{\ell-g-1}, x^{\ell-g-1}y; x^{\ell-g}, x^{\ell-g+1}, \ldots, x^{\ell})$. With respect to the local étale coordinate $y$, the lowest-order term of Wronskian $W(\lambda)$ is given by that of

$$\det M(\ell, g) \cdot \left(D_y^1 x\right)^{\binom{g+1}{2}} \left(D_y^2 x\right)^{\ell(\ell-g)}$$

whenever $\det M(\ell, g)$ is nonzero in $F$, where $D_y^i = \frac{D^i x}{dy^i}$ and $M(\ell, g)$ denotes the $(g+1) \times (g+1)$ matrix with entries $M_{ij} = \binom{\ell-g+j}{2j-i}$, $0 \leq i, j \leq g$.

# Local Wronskians for the hyperelliptic ramification locus

**Theorem 3 (C-Darago-Han):** Assume $\ell > g$, in which case $|\mathcal{O}(2\ell\infty_X)|$ has basis $\lambda := (1, y, \ldots, x^{\ell-g-1}, x^{\ell-g-1}y; x^{\ell-g}, x^{\ell-g+1}, \ldots, x^{\ell})$. With respect to the local étale coordinate $y$, the lowest-order term of Wronskian $W(\lambda)$ is given by that of

$$\det M(\ell, g) \cdot \left(D_y^1 x\right)^{\binom{g+1}{2}} \left(D_y^2 x\right)^{\ell(\ell-g)}$$

whenever $\det M(\ell, g)$ is nonzero in $F$, where $D_y^i = \frac{D^i x}{dy^i}$ and $M(\ell, g)$ denotes the $(g+1) \times (g+1)$ matrix with entries $M_{ij} = \binom{\ell-g+j}{2j-i}$, $0 \leq i, j \leq g$.

**NB:** Gessel–Viennot implies that (the integer underlying) $\det M(\ell, g)$ equals the number of non-intersecting lattice paths connecting a pair of $(g+1)$-tuples of points lying on the lines $x + y = 0$ and $2y + x = 2\ell - 2g$ in the $xy$-plane.

# Local Euler indices for the hyperelliptic ramification locus

**Theorem 4 (C-Darago-Han):** Let $C$ denote a hyperelliptic curve defined over a field $F$ of characteristic $\neq 2$. Whenever $\ell \leq g$, the local Euler index of the complete linear series $|2\ell\infty_C|$ in $\mathrm{GW}(F)$ associated to a ramification point of the hyperelliptic projection $\pi : C \to \mathbb{P}^1$ is given by

$$\operatorname{ind}_{(\gamma,0)} W(\lambda) = \operatorname{Tr}_{k(\gamma)/F}\left(\frac{\binom{l+1}{2} - 1}{2} \cdot \mathbb{H} + \left\langle \frac{(D^1 f)(\gamma)}{2} \right\rangle\right).$$

# Local Euler indices for the hyperelliptic ramification locus

Let $X$ denote a hyperelliptic curve defined over a field $F$ of characteristic $\neq 2$. When $\ell > g$ and $\det M(\ell, g)$ is nonzero in $F$, the local Euler index of the complete linear series $|2\ell\infty_C|$ in $\mathrm{GW}(F)$ associated to a ramification point of the hyperelliptic projection $\pi : X \to \mathbb{P}^1$ is given by

$$\mathrm{ind}_{(\gamma,0)} W(\lambda) = \begin{cases} \mathrm{Tr}_{k(\gamma)/F}\left(\frac{1}{2}\binom{g+1}{2} \cdot \mathbb{H}\right) \text{ if } \binom{g+1}{2} \text{ is even} \\ \mathrm{Tr}_{k(\gamma)/F}\left(\frac{\binom{g+1}{2} - 1}{2} \cdot \mathbb{H} + \left\langle (\det M(\ell, g)) 2^{\binom{g+1}{2}} (D^1 f)(\gamma)^{\binom{g+1}{2} + \ell(\ell - g)} \right\rangle\right) \text{ else} \end{cases}$$

# Local Euler indices away from $R_\pi$

Given positive integers $\ell > g$, we define the $(g, \ell)$*th inflection polynomial* $P_{g,\ell}(x) \in F[x]$ by

$$\det(D^{(j)} x^i y)_{0 \le i \le \ell - g - 1; \ell + 1 \le j \le 2\ell - g} = (f^{-(\ell+1)} y)^{\ell - g} P_{g,\ell}(x) \quad (2)$$

where $D^{(j)} = D_x^{(j)}$.

# Local Euler indices away from $R_\pi$

Given positive integers $\ell > g$, we define the $(g,\ell)$*th inflection polynomial* $P_{g,\ell}(x) \in F[x]$ by

$$\det(D^{(j)} x^i y)_{0\le i\le \ell-g-1;\ell+1\le j\le 2\ell-g} = (f^{-(\ell+1)}y)^{\ell-g} P_{g,\ell}(x) \quad (2)$$

where $D^{(j)} = D_x^{(j)}$.

Characteristic property of $P_{g,\ell}$: its roots parameterize the $x$-coordinates of $\overline{F}$-rational inflection points of the complete linear series $|2\ell\infty_X|$ on $X$ *supported on the complement of* $R_\pi$.

# Local Euler indices away from $R_\pi$

Given positive integers $\ell > g$, we define the $(g,\ell)$*th inflection polynomial* $P_{g,\ell}(x) \in F[x]$ by

$$\det(D^{(j)}x^i y)_{0\le i\le \ell-g-1;\ell+1\le j\le 2\ell-g} = (f^{-(\ell+1)}y)^{\ell-g}P_{g,\ell}(x) \quad (2)$$

where $D^{(j)} = D_x^{(j)}$.

Characteristic property of $P_{g,\ell}$: its roots parameterize the $x$-coordinates of $\overline{F}$-rational inflection points of the complete linear series $|2\ell\infty_X|$ on $X$ *supported on the complement of* $R_\pi$.

When $\ell = g+1$, the equation (2) reduces to the statement that

$$D^{(g+2)}y = f^{-(g+2)}y \cdot P_{g,g+1}(x).$$

# Local Euler indices away from $R_\pi$

Given positive integers $\ell > g$, we define the $(g, \ell)$*th inflection polynomial* $P_{g,\ell}(x) \in F[x]$ by

$$\det(D^{(j)} x^i y)_{0 \le i \le \ell - g - 1; \ell + 1 \le j \le 2\ell - g} = (f^{-(\ell+1)} y)^{\ell - g} P_{g,\ell}(x) \quad (2)$$

where $D^{(j)} = D_x^{(j)}$.

Characteristic property of $P_{g,\ell}$: its roots parameterize the $x$-coordinates of $\overline{F}$-rational inflection points of the complete linear series $|2\ell \infty_X|$ on $X$ *supported on the complement of* $R_\pi$.

When $\ell = g + 1$, the equation (2) reduces to the statement that

$$D^{(g+2)} y = f^{-(g+2)} y \cdot P_{g,g+1}(x).$$

In general, we can always realize inflection polynomials as determinants in the "atomic" polynomials $P_{g,g+1}(x)$.

# Atomic inflection polynomials...

Given a positive integer $g$, let $n = g + 2$; write $P_n$ in place of $P_{g,g+1}$.

# Atomic inflection polynomials. . .

Given a positive integer $g$, let $n = g + 2$; write $P_n$ in place of $P_{g,g+1}$.

**Theorem 5 (C-Darago-Han):** Suppose that $\mathrm{char}(F) \neq 2$. The atomic inflection polynomials of the hyperelliptic curve defined by the affine equation $y^2 = f(x)$ satisfies the recursion

$$P_{n+1} = \frac{1}{n+1}\left((D^1 P_n) \cdot f + \left(-n + \frac{1}{2}\right) P_n \cdot (D^1 f)\right)$$

for every $n \geq 1$, subject to the seed datum $P_1 = \frac{1}{2} D^1 f$.

# Atomic inflection polynomials...

Given a positive integer $g$, let $n = g + 2$; write $P_n$ in place of $P_{g,g+1}$.

**Theorem 5 (C-Darago-Han):** Suppose that $\mathrm{char}(F) \neq 2$. The atomic inflection polynomials of the hyperelliptic curve defined by the affine equation $y^2 = f(x)$ satisfies the recursion

$$P_{n+1} = \frac{1}{n+1}\left((D^1 P_n) \cdot f + \left(-n + \frac{1}{2}\right) P_n \cdot (D^1 f)\right)$$

for every $n \geq 1$, subject to the seed datum $P_1 = \frac{1}{2} D^1 f$.

**NB:** We use *Hasse* derivatives; the $k$th Hasse derivative is $\frac{1}{k!}$ times the usual derivative. Every $P_n$, multiplied by an appropriate power of 2, is an element of $\mathbb{Z}[x]$.

# …for elliptic curves

**Conjecture ($\mathbb{R}$-inflection for elliptic curves)**: Let $a \in \mathbb{R}$, and let $P_n(x)$, $n \geq 1$ denote the $n$th atomic inflection polynomial associated to the real Weierstrass elliptic curve $E_{(a,2)} : y^2 = x^3 + ax + 2$. The possible numbers of real zeroes of $P_n(x)$, as a function of the modular parameter $a$, are as follows.

| Value of $a$ | $n$ odd | $n$ even |
|---|---|---|
| $a < -3$ | 4, of which 2 satisfy $f > 0$ | 2, of which 1 satisfies $f > 0$ |
| $a > -3$ | $2i, i = 1, \ldots, \frac{n-1}{2}$, of which $(2i-1)$ satisfy $f > 0$ | $2i, i = 1, \ldots, \frac{n}{2}$, of which $(2i-1)$ satisfy $f > 0$ |

# . . . for elliptic curves

**Conjecture ($\mathbb{R}$-inflection for elliptic curves)**: Let $a \in \mathbb{R}$, and let $P_n(x)$, $n \geq 1$ denote the $n$th atomic inflection polynomial associated to the real Weierstrass elliptic curve $E_{(a,2)} : y^2 = x^3 + ax + 2$. The possible numbers of real zeroes of $P_n(x)$, as a function of the modular parameter $a$, are as follows.

| Value of $a$ | $n$ odd | $n$ even |
|---|---|---|
| $a < -3$ | 4, of which 2 satisfy $f > 0$ | 2, of which 1 satisfies $f > 0$ |
| $a > -3$ | $2i, i = 1, \ldots, \frac{n-1}{2}$, of which $(2i - 1)$ satisfy $f > 0$ | $2i, i = 1, \ldots, \frac{n}{2}$, of which $(2i - 1)$ satisfy $f > 0$ |

**NB:** When $a = -3$, the corresponding elliptic curve $y^2 = x^3 - 3x + 2$ has vanishing discriminant (and is singular).

# $\mathbb{R}$-inflection for elliptic curves, pictorially

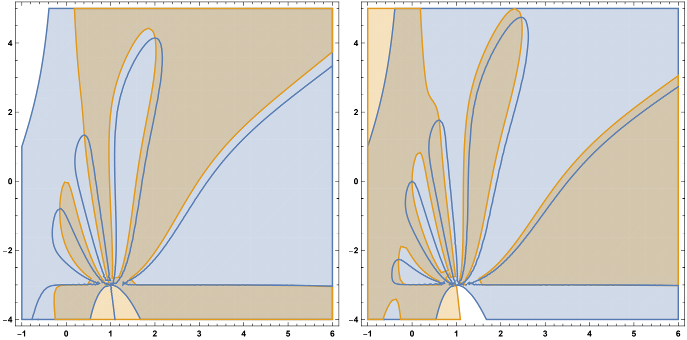


Figure: Dark blue curves trace out the real loci of $\mathcal{C}_n := (P_n = 0)$ for $n = 9, 10$ in the $(x, a)$-plane. Here $a$ parameterizes the punctured $j$-line, and the fiber over $a$ is the elliptic curve $E_{(a,2)} : z^2 = x^3 + ax + 2$ in the $(x, z)$-plane. Grey (resp., orange) shading indicates that the Weierstrass cubic $f(x) = x^3 + ax + 2$ (resp., $\frac{dP_n}{dx}$) is strictly positive.

# Elliptic curves over $\mathbb{F}_q$

Over $\mathbb{F}_q$, Hasse–Weil theory applies, and establishes that $\#\mathcal{C}_n(\mathbb{F}_q) = q + 1 + e_{n,q}$, where $|e_{n,q}| \leq 2g\sqrt{q}$. Here $g = \binom{2n-1}{2}$ is the arithmetic genus of $\mathcal{C}_n$ in the $xa$-plane.

# Elliptic curves over $\mathbb{F}_q$

Over $\mathbb{F}_q$, Hasse–Weil theory applies, and establishes that $\#\mathcal{C}_n(\mathbb{F}_q) = q + 1 + e_{n,q}$, where $|e_{n,q}| \leq 2g\sqrt{q}$. Here $g = \binom{2n-1}{2}$ is the arithmetic genus of $\mathcal{C}_n$ in the $xa$-plane.

**Conjecture 2 ($\mathbb{F}_q$-inflection for elliptic curves):** Let $n \geq 2$, and let $\widetilde{e}_{n,p} := \frac{e_{n,p}}{(2n-1)(2n-2)\sqrt{p}}$ denote the renormalized error associated with (the cardinality of) $\mathcal{C}_n(\mathbb{F}_p)$, where $\mathcal{C}_n := (P_n = 0)$ is the $n$th inflectionary curve derived from the Weierstrass family $E_{(a,2)}$ of elliptic curves. Then for every $n$, the values of $\widetilde{e}_{n,p}$ are equidistributed as $p$ varies over all odd primes.

# Elliptic curves over $\mathbb{F}_q$

Over $\mathbb{F}_q$, Hasse–Weil theory applies, and establishes that $\#\mathcal{C}_n(\mathbb{F}_q) = q + 1 + e_{n,q}$, where $|e_{n,q}| \leq 2g\sqrt{q}$. Here $g = \binom{2n-1}{2}$ is the arithmetic genus of $\mathcal{C}_n$ in the $xa$-plane.

**Conjecture 2 ($\mathbb{F}_q$-inflection for elliptic curves):** Let $n \geq 2$, and let $\widetilde{e}_{n,p} := \frac{e_{n,p}}{(2n-1)(2n-2)\sqrt{p}}$ denote the renormalized error associated with (the cardinality of) $\mathcal{C}_n(\mathbb{F}_p)$, where $\mathcal{C}_n := (P_n = 0)$ is the $n$th inflectionary curve derived from the Weierstrass family $E_{(a,2)}$ of elliptic curves. Then for every $n$, the values of $\widetilde{e}_{n,p}$ are equidistributed as $p$ varies over all odd primes.

**NB**: Conjecture 2 should be viewed as an analogue the Sato–Tate conjecture (now a theorem of Barnet-Lamb, Geraghty, Harris and Taylor), which establishes equidistribution for the error terms associated with an arbitrary elliptic curve (as opposed to an inflectionary curve) over $\mathbb{F}_q$.