Hessian graphs

Joint work with F. Pintore and D. Taufer

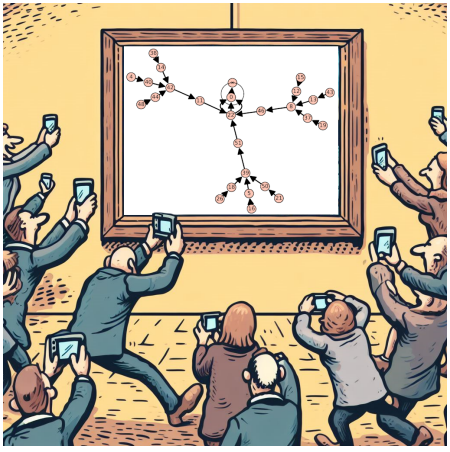
Marzio Mula

Leuven Isogeny days 4 • October 13, 2023



Goals of this talk

- Draw some beautiful graphs of elliptic curves (not isogeny graphs, for once!)
- Partially explain why they look nice
- Fantasize on exploiting their beauty



Hessian of a cubic curve

Main ingredients

$$K = \text{(perfect) field of characteristic} \neq 2, 3$$
$$G(X, Y, Z) = \text{homogeneous cubic polynomial in } K[X, Y, Z]$$
$$\mathrm{Hess}(G) = \text{Hessian matrix of } G = \begin{pmatrix} \frac{\partial^2 G}{\partial X^2} & \frac{\partial^2 G}{\partial X \partial Y} & \frac{\partial^2 G}{\partial X \partial Z} \\ \frac{\partial^2 G}{\partial Y \partial X} & \frac{\partial^2 G}{\partial Y^2} & \frac{\partial^2 G}{\partial Y \partial Z} \\ \frac{\partial^2 G}{\partial Z \partial X} & \frac{\partial^2 G}{\partial Z \partial Y} & \frac{\partial^2 G}{\partial Z^2} \end{pmatrix}$$

Consider the (possibly singular) cubic

$$E\colon\ G(X, Y, Z) = 0.$$

The *Hessian of E* is the (possibly singular) cubic

$$\mathrm{Hess}(E)\colon\ \det(\mathrm{Hess}(G)) = 0.$$

Geometric interpretation

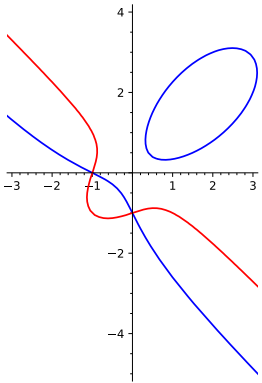
$$\begin{aligned} E \cap \mathrm{Hess}(E) &= \textit{inflection points of } E \\ &= E[3] && \text{(when } E \text{ is an elliptic curve)} \\ &= \mathrm{Hess}(E)[3] && \text{(when } \mathrm{Hess}(E) \text{ is an elliptic curve)} \end{aligned}$$

Example (over $\mathbb{Q}$):

$$E : x^3 + y^3 + 1 = 6xy$$

$$\mathrm{Hess}(E) : x^3 + y^3 + 1 = -xy$$

$$E \cap \mathrm{Hess}(E) = \left\{ \left(\frac{1 \pm \sqrt{-3}}{2} : 0 : 1 \right), \left(\frac{1 \pm \sqrt{-3}}{2} : 1 : 0 \right), \left(0 : \frac{1 \pm \sqrt{-3}}{2} : 1 \right), (-1 : 0 : 1), (0 : -1 : 1) (-1 : 1 : 0) \right\}$$



Singular or nonsingular?

$E\colon x^3 + Ax + B - y^2 = 0$

Homogenize

$X^3 + AXZ^2 + BZ^3 - Y^2Z = 0$

Hessian of E

$-8(3XY^2 + 3AX^2Z + 9BXZ^2 - A^2Z^3) = 0$ — if $A = 0 \ldots$ → the point $[1 : 0 : 0]$ is singular

Dehomogenize ($X \neq 0$)

$-6A^2\left(\left(\frac{2y}{A}\right)^2 + \frac{4}{A}x + \frac{12B}{A^2}x^2 - \frac{4}{3}x^3\right) = 0$

Short Weierstrass form

$x^3 + \frac{-A^3/3 - 3B^2}{A^4}x + \frac{-A^3B/3 - 2B^3}{A^6} - y^2 = 0$

$\mathrm{Hess}(E)$ is nonsingular if and only if E is nonsingular and $A \neq 0$.

$$j\big(\mathrm{Hess}(E)\big) \;=\; \frac{(6912 - j(E))^3}{27(j(E))^2}$$

Functional graphs

Functional graphs

$\mathbb{F}_q$ = finite field of characteristic ≥ 5

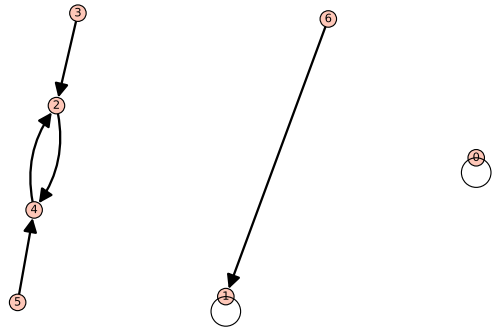
$g(x)$ = rational function in $\mathbb{F}_q(x)$

Example: $g(x) = x^2$ on $\mathbb{F}_7$

The *functional graph* of g is the directed graph s.t.

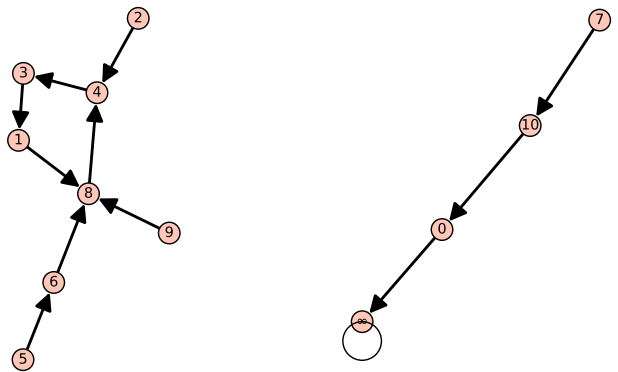
- the vertices are the elements of $\mathbb{F}_q$;
- there is an edge $\alpha \to \beta$ iff $\beta = g(\alpha)$ (counted with multiplicity).

When $g(\alpha)$ is not defined, we set $g(\alpha) = \infty$. Moreover, $g(\infty) = \infty$.



Some general (obvious) remarks

Example: $g(x) = \frac{(x+1)^3}{x^2}$ on $\mathbb{F}_{11}$



- Each connected component of the graph has exactly one loop.
- The indegree of each vertex is at most the the maximum between the degree of the numerator and the degree of the denominator of $g(x)$.
- The outdegree of each vertex is (usually) 1.

Hessian graphs (and their brothers)

The *Hessian graph* is the functional graph of the map

$$\mathrm{Hess}(j) = \frac{(6912 - j(E))^3}{27(j(E))^2}.$$

More generally, we can consider, for each $k, \ell \in \mathbb{F}_q^*$, the functional graphs of

$$g_{k,\ell}(x) = \frac{(x+k)^3}{\ell \cdot x^2},$$

so that $\mathrm{Hess} = g_{-4\cdot 1728,-27}$.

Proposition 1

The functional graphs corresponding to $g_{1,\ell}, g_{2,\ell}, \ldots$ are isomorphic.

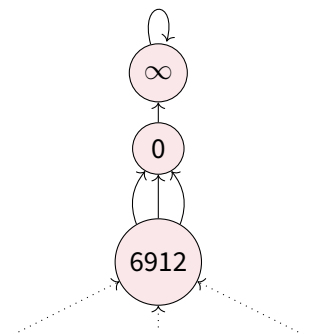
Regularity of Hessian graphs

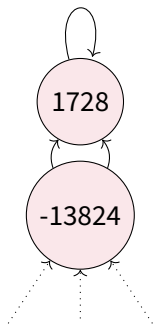
A LIMITED NUMBER OF MULTIPLE EDGES

PROPOSITION 2

In the Hessian graph over $\mathbb{F}_q$*...*

- *...the only triple edge is from* $4 \cdot 1728$ *to* 0*;*
- *... the only double edge is from* $-8 \cdot 1728$ *to* 1728*.*





Loops

n	1	2	3	4	5	6	7	8	9	10	...
#loops in $\overline{\mathbb{F}_q}$	4	3	8	18	48	116	312	810	2184	5880	...

Proposition 3

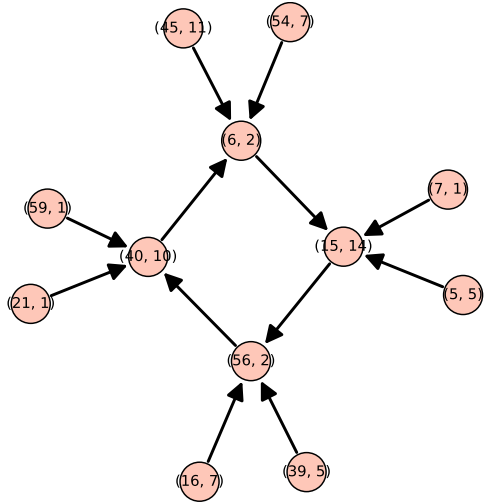
The only loops of length 1 *in the Hessian graph start from the vertices* $\infty, 1728$ *and, if* -3 *is a square in* $\mathbb{F}_q$*, the roots of* $7j^2 + 6912j + 47775744$.

More generally, let $n = \prod_{i=1}^{k} p_i^{f_i}$ *be an integer* > 1 *and define* $P = \prod_{i=1}^{k} p_i^{f_i - 1}$*. The number of loops of length n in* $\overline{\mathbb{F}_q}$ *is*

$$\frac{1}{n} \cdot \left(\sum_{(e_1,\ldots,e_k) \in \{0,1\}^k} (-1)^{k+e_1+\cdots+e_k} 3^{p_1^{e_1} \cdots p_k^{e_k} P} \right).$$

Leaves and traces

Example: Connected component of Hessian graph over $\mathbb{F}_{61}$, vertices labelled as $(j, |\mathrm{tr}(E_j)|)$.



Proposition 4

The leaves (i.e. the vertices of indegree 0) of the Hessian graph are exactly those corresponding to curves with odd trace.

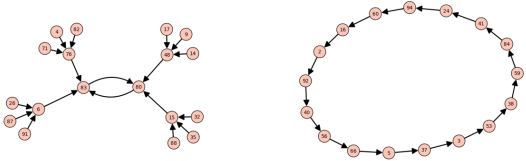
Regularity – as far as we can explain

Theorem

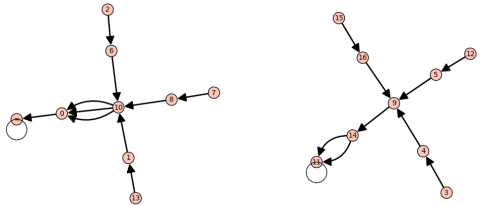
Let G be the Hessian graph $\mathbb{F}_q$. Then

- *if -3 is a square in $\mathbb{F}_q$, the connected components of G are either pure loops or "totally ramified" trees (in the sense that every vertex, apart from the leaves, has indegree 3).*
- *if -3 is not a square in $\mathbb{F}_q$, a vertex of indegree 1 in G is followed by a vertex with indegree 3, and every vertex with indegree 0 or 3 is followed by a vertex of indegree 1.*

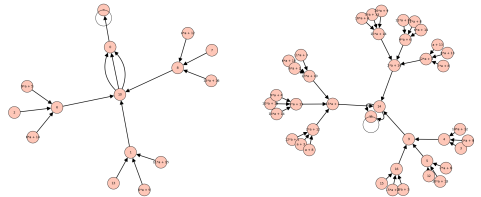
Example: Two connected components of Hessian graph over $\mathbb{F}_{97}$.



Example: Hessian graph over $\mathbb{F}_{17}$.



Example: Two connected components of Hessian graph over $\mathbb{F}_{17^2}$.



Regularity – as far as we can ~~explain~~ conjecture

Define the *depth* of a vertex to be its distance from the loop of its connected component.

Conjecture

Any two branches starting from vertices of depth $N > 0$ in the same connected component are isomorphic.

We also define the *depth of a connected component* to be the maximum of the depths of its vertices.

Conjecture

If $q \equiv 2 \bmod 3$, each connected component has the same depth.

Chasing supersingular ECs

SECUERS: AN OPEN PROBLEM

Some cryptosystems require Supersingular Elliptic Curves of Unknown Endomorphism Ring (SECUERS).
Problem: The only known way to get a SECUER is by means of a trusted setup.

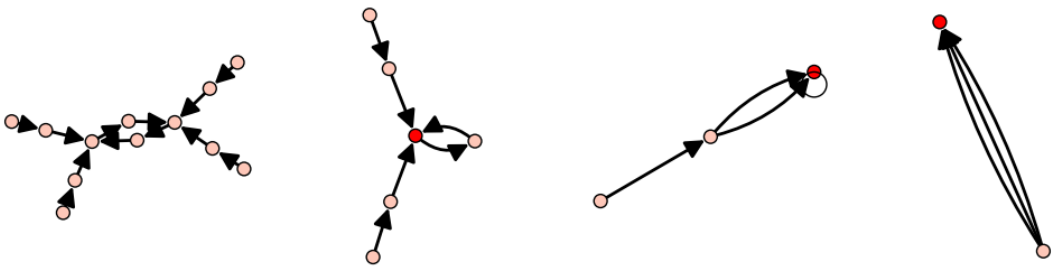
Dream: exploiting Hessian graphs by...

- ...finding which connected components contain supersingular elliptic curves,
- ...finding sufficient conditions on a (possibly ordinary) elliptic curve E to enforce that $\mathrm{Hess}^n(E)$ is supersingular for some $n \geq 1$.

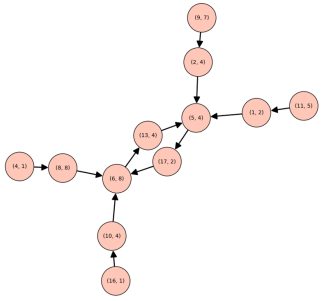
Supersingular components

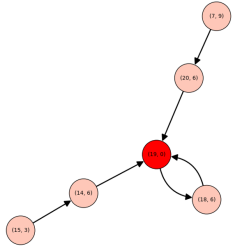
We say that a component of the Hessian graph is *supersingular* if it contains at least one supersingular vertex.

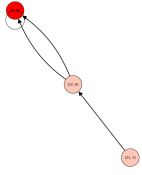
Example: Supersingular vertices on Hessian graph over $\mathbb{F}_{23}$.

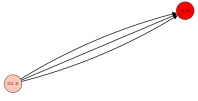


A necessary condition for supersingular components









Theorem

In the Hessian graph over $\mathbb{F}_p$, the trace of each elliptic curve (defined over $\mathbb{F}_p$) in a supersingular component is a multiple of 3.


Thank you for your attention!