Distancia entre vértices en multigrafos de isogenias de curvas elípticas

D. Sadornil[1] F. Sebé[2] J. Tena[3] M. Valls[2]

[1]UC, [2]UdL, [3]UVa

VIII JMDA
Julio 2012

Definicion

Una curva elíptica sobre $\mathbb{F}_q$ es un par $(E, \mathcal{O})$, donde E es una curva proyectiva no singular de género 1 definida sobre $\mathbb{F}_q$ y $\mathcal{O}$ es un punto sobre E.

$$y^2 = x^3 + Ax + B, \qquad 4A^3 + 27B^2 \neq 0 \qquad char(\mathbb{F}_q) \neq 2, 3$$

Sobre el grupo de puntos de una curva elíptica se puede definir una ley de grupo (aditiva).

Isogenias

- Una **isogenia** entre dos curvas elípticas E_1 y E_2 sobre un cuerpo k es un morfismo $\mathcal{I} : E_1 \to E_2$ tal que $\mathcal{I}(O_{E_1}) = O_{E_2}$
- $\mathcal{I}$ es un morfismo de grupos.
- El grado de una isogenia es el orden del núcleo de $\mathcal{I}$ (si $\mathcal{I}$ es separable).
- El grado de la composición es el producto de grados.

Teorema (Tate)

Dadas dos **curvas elípticas** E_1 *y* E_2 *definidas sobre un* **cuerpo finito** k*, las siguientes afirmaciones son equivalentes:*

- $\#E_1(k) = \#E_2(k)$
- *Existe una isogenia* $\mathcal{I}$ *entre* E_1 *y* E_2*.*

Preguntas

¿cuáles?, ¿de qué grado?, ¿cómo?

Primera aproximación

JMDA 2010 Castro-Urdiales.

Presentamos un algoritmo para hallar la isogenia de **grado mínimo *smooth*** entre dos curvas elípticas E_1 y E_2 definidas sobre un cuerpo $\mathbb{F}_q$

No necesariamente es la de grado más pequeño.

Objetivo

Construir la isogenia de grado mínimo entre dos curvas.

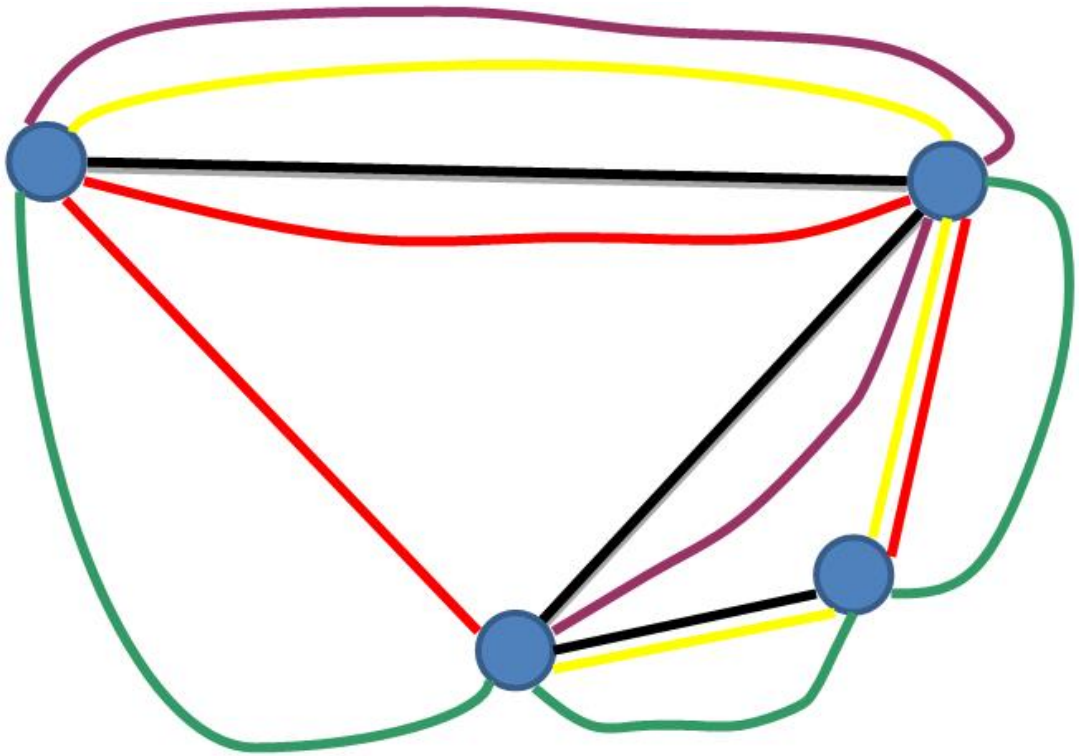
Nos permitirá obtener el grado de TODAS las isogenias existentes entre dos curvas.

Multigrafo de isogenias

Definición

Nodos: Clases de isomorfía de curvas elípticas.
Aristas: Isogenias de grado (primo) entre dos clases.

- Entre dos clases existen diversas isogenias.
- Tate implica que el grafo es conexo.
- Podemos suponer grado acotado y sigue siendo conexo.
- Isogenia dual nos permite dar el grafo no dirigido.
- Para cada vértice y fijado un primo ℓ pueden existir $0, 1, 2$ ó $\ell + 1$ aristas adyacentes a este vértice de dicho grado.

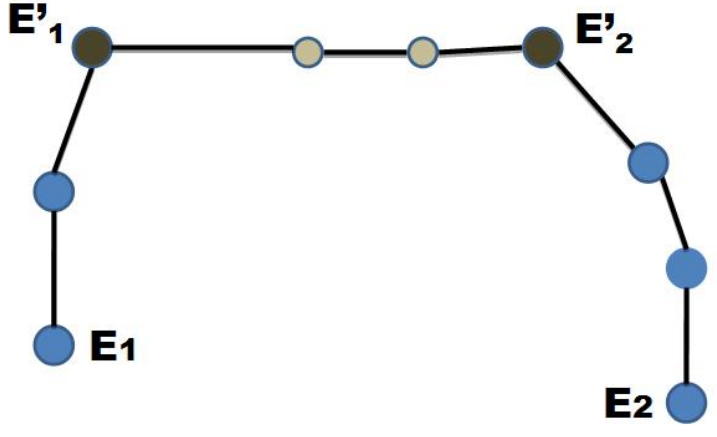


Objetivo

Calcular la distancia mínima entre dos vértices del multigrafo (completo).

Algunos conceptos

- El conjunto de isogenias de una curva E sobre $\mathbb{F}_q$ consigo misma, junto con la aplicación cero, tiene estructura de anillo, $\mathcal{O}$
- $\mathcal{O}$ es un orden en el anillo de enteros $\mathbb{Z}(\sqrt{t^2-4q})$ (con E de cardinal $q+1-t$ sobre $\mathbb{F}_q$). $t^2-4q=f^2D_K$. Dicho orden viene determinado por su conductor g, $g \mid f$.
- Toda isogenia $\mathcal{I}$ entre dos curvas E_1, E_2 puede descomponerse como composición de tres isogenias:



Isogenias - Formas cuadráticas

Dadas E_1, E_2 curvas elípticas isógenas, $Hom(E_1, E_2)$ es un $\mathbb{Z}$-módulo libre de rango 2.

Sea $\{\mathcal{I}_1, \mathcal{I}_2\}$ base de Hom(E_1, E_2).

$$\mathfrak{q} = \text{gr}(\mathcal{I}_1)x^2 + (\text{gr}(\mathcal{I}_1 + \mathcal{I}_2) - \text{gr}(\mathcal{I}_1) - \text{gr}(\mathcal{I}_2))y + \text{gr}(\mathcal{I}_2)y^2$$

- Igual anillo de endomorfismos $\Leftrightarrow$ $\mathfrak{q}$ Primitiva .
- $End(E_1) = End(E_2)$ e $\mathcal{I} : E_1 \to E_2$ de grado ℓ, $\mathfrak{q}$ queda determinada por ℓ (salvo el signo del coeficiente de xy).

Teorema

$End(E_1) = End(E_2) = \mathcal{O}$, $Disc(\mathcal{O}) = D$, $Hom(E_1, E_2) = \langle \mathcal{I}_1, \mathcal{I}_2 \rangle$

$$\mathfrak{q} = gr(\mathcal{I}_1)x^2 + bxy + gr(\mathcal{I}_1)y^2$$

$b^2 = D + 4gr(\mathcal{I}_1)gr(\mathcal{I}_2)$.

$\mathfrak{q} = ax^2 + bxy + cy^2$ y $\mathfrak{q}' = ax^2 - bxy + cy^2$ representan los mismos elementos.

$$\mathrm{Hom}(E_1, E_2) \leftrightarrow \mathfrak{q} \qquad \mathrm{Hom}(E_2, E_1) \leftrightarrow \mathfrak{q}'$$

Algoritmo de distancia mínima

Fundamento

La distancia mínima entre dos vértices del multigrafo corresponde a la isogenia de grado mínimo entre las dos curvas.

Viene dado por el menor entero representado por la forma cuadrática asociada.

Se obtiene a partir de la forma cuadrática reducida (en la misma clase de equivalencia).

$\mathfrak{q} = ax^2 + bxy + cy^2$ reducida si

$$|b| \leq a \leq c, \text{ con } b \geq 0 \text{ si } c = a \text{ ó } |b| = a.$$

Isogenia mínima

- El cálculo de la forma reducida equivalente a una forma cuadrática dada se hace mediante un algoritmo (Gauss) que realiza un cambio lineal en la base de isogenias.
- Uno de los elementos de la nueva base (expresado como cl de la base inicial) es precisamente la isogenia de grado mínimo.

Algoritmo

Input: E_1, E_2 curvas elípticas $|E_1| = |E_2|$, $End(E_1) = End(E_2)$.

1. Encontrar dos caminos $\mathcal{I}_1$ e $\mathcal{I}_2$ entre los vértices E_1 y E_2. (VIIJmda-Castro).
2. Construir la forma cuadrática

$$\mathfrak{q}(x, y) = \deg(\mathcal{I}_1)x^2 + bxy + \deg(\mathcal{I}_2)y^2$$
$$b = \sqrt{D + 4\deg(\mathcal{I}_1)\deg(\mathcal{I}_2)}.$$

3. Determinar la forma cuadrática reducida en la clase de equivalencia de$\mathfrak{q}$. Nueva base $\mathcal{I}'_1, \mathcal{I}'_2$.

$$\mathfrak{q}'(x, y) = \deg(\mathcal{I}'_1)x^2 + bxy + \deg(\mathcal{I}'_2)y^2$$
$$b = \sqrt{D + 4\deg(\mathcal{I}'_1)\deg(\mathcal{I}'_2)}.$$

Notas

- En el paso 1 se construyen (de forma recursiva) dos árboles tomando E_1 y E_2 como nodos raíz, hasta encontrarse en un vértice común. Tras encontrar el primer camino, el algoritmo continuará hasta encontrarse un segundo camino tal que ambas isogenias formen base.
- El signo de b no es relevante para el cálculo de la distancia.
- $\mathcal{I}_1' = d_1\mathcal{I}_1 + d_2\mathcal{I}_2$.
- $\mathcal{I}_1'$ es la isogenia de grado mínimo.
- $\mathfrak{q}'$ representa todas las distancias entre E_1 y E_2.
- Número de vértices en el multigrafo $O(ulog(u)loglog(u)))$, $u = \sqrt{t^2 - 4q}$.
- Sólo se consideran aristas de peso menor o igual a 109.

Ejemplo

- Determinar la isogenia de grado mínimo entre las curvas E_1 y E_2 sobre $\mathbb{F}_p$, $p = 143843287801$.

  $j(E_1) = 114206442741$ y $j(E_2)16004433667$.

- $\#E_1(\mathbb{F}_p) = \#E_2(\mathbb{F}_p) = 143842644900$.
- $\mathbb{Q}(\sqrt{t^2 - 4p}) = \mathbb{Q}(\sqrt{(-1) \cdot 2^8 \cdot 3^2 \cdot 5^2 \cdot 11^2 \cdot 23251})$.
- $\mathrm{End}(E_i) = \mathbb{Z}(\sqrt{(2^3 \cdot 11)^2 \cdot (-23251)})$.
- Número de curvas con este anillo de endomorfismos es 3480 y el número total de curvas con este cardinal es 366850.

Ejemplo (II)

Pasos

1. Dos caminos $(\mathcal{I}_1, \mathcal{I}_2)$ de E_1 a E_2 de longitud $17545 = 5 \cdot 11^2 \cdot 29$ y $69184 = 2^6 \cdot 23 \cdot 47$, respectivamente.
2. $\mathfrak{q}(x, y) = 17545x^2 + 68376xy + 69184y^2$.
3. $\mathfrak{q}_{red}(x, y) = 2612x^2 + 1804xy + 17545y^2$.
   $\mathcal{I}'_1 = -2\mathcal{I}_1 + \mathcal{I}_2$
4. El grado de $\mathcal{I}'_1$ es $2612 = 2^2 \cdot 653$.

Notas:

- El camino mínimo no se podría encontrar con una búsqueda aleatoria (sólo aristas de grado primo menor que 109).
- Se han visitado un total de 273 curvas (0,07 % del total).

Algunos ejemplos más

Conductor	$\mathrm{gr}(\mathcal{I}_1)$	$\mathrm{gr}(\mathcal{I}_2)$	grado mínimo	Curvas visitadas
1	95	209	67 (p)	24
1	95	319	73 (p)	36
2^3	2500	22781	149 (p)	181
$2^2 \cdot 11$	2204	17545	$2204(2^2 \cdot 19 \cdot 29)$	141
$2^2 \cdot 11$	2117	7705	$2117(29 \cdot 73)$	119
$5 \cdot 11$	38525	49039	1039 (p)	333
$3 \cdot 5 \cdot 11$	600039	7108375	9181 (p)	1075
$3 \cdot 5 \cdot 11$	109989	111725	1439 (p)	377
$2^4 \cdot 3 \cdot 5$	725	702144	$725(5^2 \cdot 29)$	533
$2^4 \cdot 3 \cdot 5 \cdot 11$	1940912	2586375	$64367(191 \cdot 337)$	865
$2^4 \cdot 3 \cdot 5 \cdot 11$	733248	40925467	214363 (p)	2657

Distancia entre vértices en multigrafos de isogenias de curvas elípticas

D. Sadornil[1] F. Sebé[2] J. Tena[3] M. Valls[2]

[1]UC, [2]UdL, [3]UVa

VIII JMDA
Julio 2012