Biseccions y raíces cuadradas

para curvas hiperelípticas

Josep Miret[1], Jordi Pujolàs[1] y **Nicolas Thériault**[2]

[1]Departament de Matemàtica, Universitat de Lleida, Spain.

[2]Departamento de Matemática y Ciencia de la Computación,
Universidad de Santiago de Chile.

Curvas hiperelípticas

Una curva hiperelíptica no-singular sobre un cuerpo de característica impar $\mathbb{F}_q$ se puede dar por una ecuación de la forma

$$y^2 = f(x) = f_{d_f} \prod_{i=1}^{d_f} (x - \theta_i)$$

donde los θ_i son todos distintos elementos de $\mathbb{F}_{q^s}$ tales que $f(x)$ está definido en $\mathbb{F}_q[x]$. Si $d_f = 5$ o 6, la curva tiene genero dos.

Cuando d_f es impar, tenemos un modelo imaginario y podemos tomar $f_{d_f} = 1$.

Cuando d_f es par, tenemos un modelo real (puramente real si nigún θ_i está en $\mathbb{F}_q$).

Si $d_f = 2g + 1$ (resp. $d_f = 2g + 1$) la curva es imaginaria (resp. real) de genero g.

A partir de una curva hiperelíptica, podemos definir la Jacobiana: el grupo de clases de divisores: los divisores de grado 0 módulo por los divisores principales.

Curvas hiperelípticas

Definición

Una ℓ-sección es una pre-imagen de la multiplicación (escalar) por ℓ en el grupo de la curva.

En general (si ℓ es coprimo con q), un divisor definido sobre $\mathbb{F}_q$ tiene ℓ^{2g} posibles ℓ-secciones en $\overline{\mathbb{F}_q}$. Un problema natural es de determinar si un divisor admite bisecciones y en el caso que sí, encontrarlas.

Las ℓ-secciones tienen aplicaciones en criptografía:

- En curvas elípticas de orden impar sobre cuerpos de característica 2, los "halvings" (las bisecciones) permiten reemplazar la multiplicación escalar "double-and-add" por una multiplicación escalar "halve-and-add", que puede ser más eficiente.
- Las ℓ-secciones pueden servir a construir puntos de orden ℓ^k en algoritmos de tipo Schoof, lo que permite calcular el orden de grupo más rápidamente.

Representación de Mumford

Para modelos imaginarios, hay un único punto al infinito, P_∞.

Cada divisor reducido $D \in Jac(C)(\mathbb{F}_q)$, $D = \sum_{i=1}^{k} (P_i - P_\infty)$ con $P_i = (x_i, y_i) \in C\left(\overline{\mathbb{F}_q}\right)$ puede representarse de manera única por un par de polinomios $[u(x), v(x)]$, tales que:

1. $u, v \in \mathbb{F}_q[x]$,
2. $\deg(u) \leq g$,
3. u es mónico,
4. $\deg(v) < \deg(u)$,
5. $u(x)$ divide a $v(x)^2 - f(x)$.

Desde los P_i, los polinomios $u(x)$ y $v(x)$ se definen por:

$$u(x) = \prod_{i=1}^{k} (x - x_i) \quad \text{y} \quad v(x_i) = y_i \ \ \forall\ i$$

Cuando el punto P_i es repetido r veces, las $r-1$ primeras derivadas de $y - v(x)$ deben coincidir con las $r-1$ primeras derivadas de la ecuación de la curva en P_i.

Representación de Mumford

Para modelos reales, hay dos puntos al infinito, P_{∞_1} y P_{∞_2}.

P_{∞_1} y P_{∞_2} son $\mathbb{F}_q$-racinales si y solo si f_{2g+2} es un cuadrado en $\mathbb{F}_q$.

La definición de *divisor reducido* es más complicada (no hay una unicidad tan clara).

En algunos casos, se puede adaptar la representación de Mumford, si el divisor tiene $k/2$ copias de ambos P_{∞_1} y P_{∞_2} (divisores balanceados).

En genero par, da un representante único en la mayor parte de las clases de divisores, y los divisores balanceados permiten obtener una operación de grupo un poco más sencilla.

En genero impar es un poco más complicado (especialmente para las bisecciones).

Algoritmo de Cantor (versión sencilla)

Dado $[u_1, v_1]$ y $[u_2, v_2]$, obtener $[u_3, v_3]$ reducido tal que $[u_3, v_3] \equiv [u_1, v_1] + [u_2, v_2]$

- Composición:
  - $d \longleftarrow gcd(u_1, u_2, v_1 + v_2) = s_1 u_1 + s_2 u_2 + s_3(v_1 + v_2)$
  - $u \longleftarrow u_1 u_2 / d^2$
  - $v \longleftarrow \frac{s_1 u_1 v_2 + s_2 u_2 v_1 + s_3(v_1 v_2 + f)}{d} \bmod u$
- Reducción (iterativa):
  - Mientrás $\deg(u) > g$, repetir:
    - $u \longleftarrow (f - v^2)/u$
    - $u \longleftarrow Monico(u)$
    - $v \longleftarrow -v \bmod u$
  - $[u_3, v_3] \longleftarrow [u, v]$

Para genero 2, la reducción requiere a lo más un paso.
Para genero > 2, casi siempre son más de un paso de reducción.

Algoritmo de Cantor

Para genero 2:

Dado $[u_1, v_1]$ con $\gcd(u_1, f) = 1$, obtener $[u_2, v_2]$ reducido tal que $[u_2, v_2] \equiv 2[u_1, v_1]$

- Composición:
  - $u \longleftarrow u_1^2$
  - $v \longleftarrow v_1 + \ell \cdot u_1$ con $\ell \equiv \cdots \bmod u_1 = \ell_1 x + \ell_0$
- Reducción (iterativa):
  - $u_2 \longleftarrow Monico((f - v^2)/u) = (v^2 - f)/(c \cdot u_1^2)$ con $c = \ell_1^2 - f_6$
  - $v_2 \longleftarrow -v \bmod u_2 = -v + k \cdot u_2$ con $k(x) = k_1 x + k_0 = \ell_1 x + k_0$

Para calcular la bisección, hacemos una *de-reducción* que intenta retroceder esos pasos.

Bisecciones en genero 1

En curvas elípticas $y^2 = f(x)$ (con $f(x) = x^3 + ax + b = (x - \theta_1)(x - \theta_2)(x - \theta_3)$), las bisecciones y los cuadrados están relacionados en el contexto del teorema (débil) de Mordell-Weil.

Para ilustrar la idea básica de nuestra técnica, consideramos resolver $2P = Q$ para un Q dado.
Buscamos una recta $y = k_0(x - x_Q) - y_Q$ (que pasa por Q) tal que

$$(k_0(x - x_Q) - y_Q)^2 - f(x) = (x - x_P)^2(x - x_Q),$$

es decir una recta tales que los dos otros puntos de intersección son repetidos.

Biseccions en genero 1

La evaluación de la ecuación en una raíces θ_i de $f(x)$ da

$$(k_0(\theta_i - x_Q) - y_Q)^2 = (\theta_i - x_P)^2(\theta_i - x_Q),$$

lo que implica que $(x_Q - \theta_i)$ debe ser un cuadrado en $\mathbb{F}_q$.

La reciproca también es valida: si todos los $\omega_i = \sqrt{(x_Q - \theta_i)}$ existen en $\mathbb{F}_q$, entonces las variables k_0, x_P satisfacen un sistema de ecuaciones lineales de la forma

$$k_0(\theta_i - x_Q) - y_Q = \omega_i(\theta_i - x_P)$$
$$k_0(\theta_j - x_Q) - y_Q = \omega_j(\theta_j - x_P),$$

es decir

$$\begin{pmatrix} \theta_i - x_Q & \omega_i \\ \theta_j - x_Q & \omega_j \end{pmatrix} \begin{pmatrix} k_0 \\ x_P \end{pmatrix} = \begin{pmatrix} \omega_i\theta_i + y_Q \\ \omega_j\theta_j + y_Q \end{pmatrix}$$

lo que siempre tiene solución dado que los ω_i son distintos (dado que $\omega_i^2 = \theta_i - x_Q$).

Bisecciones en genero 2

Sea un divisor reducido $D_2 = [u_2(x), v_2(x)]$, queremos encontrar todos los divisores reducidos $D_1 = [u_1(x), v_1(x)]$ tales que

$$D_2 = 2D_1,$$

las bisecciones de D_2.

En el caso más general, calcular una bisección corresponde a obtener polinomios $u_1(x) = x^2 + u_{11}x + u_{10}$ y $k(x) = k_1x + k_0$ $(k_1 \neq 0)$ tales que

$$\Big((k_1x + k_0)u_2(x) - v_2(x)\Big)^2 - f(x) = c \cdot u_1^2(x) \cdot u_2(x)$$

con $c = k_1^2$ en el caso imaginario, y $k_1^2 - f_6$ en el caso real.

Eso determine todo el divisor porque $v_1 \equiv k(x)u_2(x) - v_2(x) \bmod u_1(x)$.

Observación: $u_2(x)$ divide a $v_2(x)^2 - f(x)$ para todo divisor D_2.

Biseccions en genero 2

Por la estructura de grupo, sabemos que

$$Jac(C)[2] \cong (\mathbb{Z}/2\mathbb{Z})^4 .$$

Como la diferencia entre dos biseccions es un divisor de orden 2, el problema consiste en encontrar las 16 biseccions de D_2, o sea 16 tuples

$$(u_{11}, u_{10}, k_1, k_0).$$

Primero estudiamos como calcular las pre-imagenes de la duplicación cuando todos los θ_i están definidos sobre $\mathbb{F}_q$, y después miraremos el caso cuando $f(x)$ tiene factores (no-lineales) irreducibles.

Caso general

El caso más común de divisores es de la forma

$$D = [u(x), v(x)] = [(x - \alpha)(x - \beta), v_1 x + v_0]$$

donde $\alpha \neq \beta$ y $f(\alpha)f(\beta) \neq 0$.

Queda una proporción $O(1/q)$ de divisores que tiene formas especiales:

- $u(x) = x + u_0$ (divisor de peso 1)
- $\gcd(u(x), f(x)) \neq 1$ (contiene puntos de Weierstrass)
- $u(x) = (x + \alpha)^2$ (doble de un divisor obtenido directamente)

Esos casos se pueden manejar con métodos parecidos, pero se pueden trabajar desde el caso general con la idea:

$$[2]D_1 = D_2 \qquad \Longleftrightarrow \qquad [2]\Big(D_1 + (P_0 - P_\infty)\Big) = \Big(D_2 + (2P_0 - 2P_\infty)\Big).$$

donde P_0 es un punto (no de Weierstrass) elegido al azar.

Modelo imaginario

En realidad, la ecuación

$$\Big((k_1x + k_0)u_2(x) - v_2(x)\Big)^2 - f(x) = k_1^2 \cdot u_1^2(x) \cdot u_2(x)$$

es

$$(k_1x + k_0)^2 u_2(x) - 2(k_1x + k_0)v_2(x) + \frac{v_2(x)^2 - f(x)}{u_2(x)} = k_1^2 \cdot u_1^2(x)$$

una igualdad de dos polinomios de grado 4 con el mismo coeficiente en x^4.

Solo necesitamos verificar la igualdad en 4 valores de x (distintos de las raíces de $u_2(x)$). La idea es de considerar cuatro de los θ_i (raíces de $f(x)$).

En estos valores, la primera igualdad se convierte en

$$\Big((k_1\theta_i + k_0)u_2(\theta_i) - v_2(\theta_i)\Big)^2 = k_1^2 \cdot u_1^2(\theta_i) \cdot u_2(\theta_i).$$

Si D_1 es bisección de D_2, la igualdad se verifica, y los $u_2(\theta_i)$ deben ser cuadrados en $\mathbb{F}_q$.

Sistema de ecuaciones

Podemos definir el *bisector* $\omega_i = \sqrt{u_2(\theta_i)}$ (una de las dos raíces cuadradas de $u_2(\theta_i)$).

Con esta definición, la ecuación da:

$$(k_1\theta_i + k_0)\omega_i^2 - (v_{21}\theta_i + v_{20}) = k_1\omega_i(\theta_i^2 + u_{11}\theta_i + u_{10}).$$

Obtenemos un sistema lineal de ecuaciones,

$$\begin{pmatrix} \theta_1(\omega_1^2 - \omega_1\theta_1) & \omega_1^2 & -\theta_1\omega_1 & -\omega_1 \\ \theta_2(\omega_2^2 - \omega_2\theta_2) & \omega_2^2 & -\theta_2\omega_2 & -\omega_2 \\ \theta_3(\omega_3^2 - \omega_3\theta_3) & \omega_3^2 & -\theta_3\omega_3 & -\omega_3 \\ \theta_4(\omega_4^2 - \omega_4\theta_4) & \omega_4^2 & -\theta_4\omega_4 & -\omega_4 \end{pmatrix} \begin{pmatrix} k_1 \\ k_0 \\ k_1 u_{11} \\ k_1 u_{10} \end{pmatrix} = \begin{pmatrix} v_{21}\theta_1 + v_{20} \\ v_{21}\theta_2 + v_{20} \\ v_{21}\theta_3 + v_{20} \\ v_{21}\theta_4 + v_{20} \end{pmatrix}$$

Existencia y unicidad

Teorema

Si $d_f = 5$ y $f(x)$ se descompose en factores lineales de $\mathbb{F}_q[x]$, entonces un divisor D_2 de orden más grande que 2 tiene biseciones si y solo si $u_2(\theta_i)$ es un cuadrado en $\mathbb{F}_q$ para todo θ_i.

Ya vimos que tener una bisección es suficiente para que los $u_2(\theta_i)$ sean cuadrados.

Para ver que es necesario, primero observamos que

$$\begin{vmatrix} \theta_1(\omega_1^2 - \omega_1\theta_1) & \omega_1^2 & -\theta_1\omega_1 & -\omega_1 \\ \theta_2(\omega_2^2 - \omega_2\theta_2) & \omega_2^2 & -\theta_2\omega_2 & -\omega_2 \\ \theta_3(\omega_3^2 - \omega_3\theta_3) & \omega_3^2 & -\theta_3\omega_3 & -\omega_3 \\ \theta_4(\omega_4^2 - \omega_4\theta_4) & \omega_4^2 & -\theta_4\omega_4 & -\omega_4 \end{vmatrix} = \omega_1\omega_2\omega_3\omega_4 \cdot \begin{vmatrix} \theta_1^2 - \theta_1\omega_1 & \omega_1 & \theta_1 & 1 \\ \theta_2^2 - \theta_2\omega_2 & \omega_2 & \theta_2 & 1 \\ \theta_3^2 - \theta_3\omega_3 & \omega_3 & \theta_3 & 1 \\ \theta_4^2 - \theta_4\omega_4 & \omega_4 & \theta_4 & 1 \end{vmatrix}$$

donde $\omega_1\omega_2\omega_3\omega_4 \neq 0$.
Si el determinante es cero, existen $\alpha, \beta, \gamma, \delta \in \mathbb{F}_q$ no todos cero tales que

$$\delta\theta_i^2 + \beta\theta_i + \gamma = \omega_i(\delta\theta_i - \alpha), \ \forall i = 1, 2, 3, 4.$$

Tomando el cuadrado de ambos lados, obtenemos un polinomio (en x en vez de θ_i) de grado a lo más 3 con 4 raíces $(\theta_1, \theta_2, \theta_3, \theta_4)$ en $\mathbb{F}_q$.
Existe $(\alpha, \beta, \gamma, \delta) \neq \vec{0} \iff u_{20} - \frac{1}{4}u_{21}^2 = 0 \iff u_2(x)$ es un cuadrado.

Observación: si $u_2(x)$ es un cuadrado, $D_2 = 2(P - P_\infty)$ y el resultado es trivial.

Modelo real

Cuando $d_f = 6$, tenemos $c = k_1^2 - f_6$, lo que puede ser un cuadrado o no (y determina si los $u_2(\theta_i)$ son cuadrados o no).

Como k_1 es uno de los valores que queremos encontrar, tenerlo dentro de una raíz cuadrada complica el "sistema".

Para evitar el problema, trabajamos con cuocientes $u_2(\theta_i)/u_2(\theta_j)$:

$$\left(\frac{k(\theta_i)u_2(\theta_i) - v_2(\theta_i)}{k(\theta_j)u_2(\theta_j) - v_2(\theta_j)} \cdot \frac{u_1(\theta_j)}{u_1(\theta_i)}\right)^2 = \frac{u_2(\theta_i)}{u_2(\theta_j)}.$$

Si D_1 es bisección de D_2, los $u_2(\theta_i)$ son todos cuadrados o todos no-cuadrados según que $k_1^2 - f_6$ es cuadrado o no.

En ambos casos, todos los cocientes $u_2(\theta_i)/u_2(\theta_j)$ son cuadrados.

Sistema de ecuaciones

Podemos definir el *bisector* $\omega_{ij} = \sqrt{u_2(\theta_i)/u_2(\theta_j)}$ (una de las dos raíces cuadradas).

Para llegar a un sistema, fijamos el indice $j = 6$.

Utilizamos una raíz cuadrada extra: $\ell = \sqrt{(k_1^2 - f_6)u_2(\theta_6)}$.

Con estas definiciones, la ecuación da:

$$k(\theta_i)u_2(\theta_i) - v_2(\theta_i) - \omega_{i6}\ell u_1(\theta_i) = 0.$$

Obtenemos un sistema lineal de ecuaciones,

$$\begin{pmatrix} \theta_1 u_2(\theta_1) & u_2(\theta_1) & -\theta_1^2\omega_{16} & -\theta_1\omega_{16} & -\omega_{16} \\ \theta_2 u_2(\theta_2) & u_2(\theta_2) & -\theta_2^2\omega_{26} & -\theta_2\omega_{26} & -\omega_{26} \\ \theta_3 u_2(\theta_3) & u_2(\theta_3) & -\theta_3^2\omega_{36} & -\theta_3\omega_{36} & -\omega_{36} \\ \theta_4 u_2(\theta_4) & u_2(\theta_4) & -\theta_4^2\omega_{46} & -\theta_4\omega_{46} & -\omega_{46} \\ \theta_5 u_2(\theta_5) & u_2(\theta_5) & -\theta_5^2\omega_{56} & -\theta_5\omega_{56} & -\omega_{56} \end{pmatrix} \begin{pmatrix} k_1 \\ k_0 \\ \ell \\ \ell u_{11} \\ \ell u_{10} \end{pmatrix} = \begin{pmatrix} v_2(\theta_1) \\ v_2(\theta_2) \\ v_2(\theta_3) \\ v_2(\theta_4) \\ v_2(\theta_5) \end{pmatrix}$$

Existencia y unicidad

Teorema

Si $d_f = 6$ y $f(x)$ se descompose en factores lineales de $\mathbb{F}_q[x]$, entonces un divisor D_2 de orden más grande que 2 tiene bisecciones si y solo si $u_2(\theta_i)/u_2(\theta_j)$ es un cuadrado en $\mathbb{F}_q$ para todos pares θ_i, θ_j con $u_2(\theta_j) \neq 0$.

De nuevo, vimos que la existencia de una bisección es suficiente para tener cuadrados.

Para ver que es necesario, primero observamos que

$$\left|sistema\right| = \omega_{16}\omega_{26}\omega_{36}\omega_{46}\omega_{56} \cdot \begin{vmatrix} \theta_1 u_2(\theta_6)\omega_{16} & u_2(\theta_6)\omega_{16} & \theta_1^2 & \theta_1 & 1 \\ \theta_2 u_2(\theta_6)\omega_{26} & u_2(\theta_6)\omega_{26} & \theta_2^2 & \theta_2 & 1 \\ \theta_3 u_2(\theta_6)\omega_{36} & u_2(\theta_6)\omega_{36} & \theta_3^2 & \theta_3 & 1 \\ \theta_4 u_2(\theta_6)\omega_{46} & u_2(\theta_6)\omega_{46} & \theta_4^2 & \theta_4 & 1 \\ \theta_5 u_2(\theta_6)\omega_{56} & u_2(\theta_6)\omega_{56} & \theta_5^2 & \theta_5 & 1 \end{vmatrix}$$

Si el determinante es cero, existen $\alpha, \beta, \gamma, \delta, \epsilon \in \mathbb{F}_q$ no todos cero tales que

$$\omega_{i6} u_2(\theta_6)(\alpha\theta_i - \beta) = \gamma\theta_i^2 + \delta\theta_i + \epsilon, \ \forall i = 1, 2, 3, 4, 5.$$

El cuadrado da un polinomio de grado a lo más 4 con 5 raíces en $\mathbb{F}_q$.
Existe $(\alpha, \beta, \gamma, \delta, \epsilon) \neq \vec{0} \iff u_{20} - \frac{1}{4}u_{21}^2 = 0 \iff u_2(x)$ es un cuadrado.

Observación: si $u_2(x) = (x - \alpha)^2$, entonces existe un $u_1 = (x - \alpha)(x - \theta_i)$ con $f(\theta_i) = 0$.

Modelos imaginarios en generos más altos

Ahora la estructura de grupo nos da

$$Jac(C)[2] \cong (\mathbb{Z}/2\mathbb{Z})^{2g},$$

y la mayor parte de los divisores (con probabilidad $1 + O(1/q)$) tienen $u(x)$ de la forma

$$u(x) = x^g + u_{g-1}x^{g-1} + \ldots + u_1 x + u_0,$$

De nuevo la diferencia entre dos bisecciones es un divisor de orden 2, y debemos encontrar 2^{2g} bisecciones de D_2, o sea 2^{2g} tuples de la forma

$$(u_{1(g-1)}, \ldots, u_{10}, ?, \ldots, ?).$$

Reducción directa (Cantor "avanzado")

Dado $[u, v]$ el resultado de una composición de Cantor tal que $\deg(u) > g$, siempre se puede hacer una reducción en un paso:
Encontrar polinomios $\alpha(x)$, $\beta(x)$ y $\gamma(x)$ tales que:

- $\beta = \gamma \cdot u + \alpha \cdot v$;
- u divide a $\beta^2 - \alpha^2 f$;
- $v \equiv -\beta/\alpha \bmod u$;
- $(\beta^2 - \alpha^2 f)/u$ tiene grado $\leq g$.

Los polinomios $\alpha(x)$ y $\gamma(x)$ se pueden obtener de un algoritmo Euclidiano parcial.

Si agregamos que $\beta^2 - \alpha^2 f$ es mónico, entonces el par α, γ es único.

Reducción directa (Cantor "avanzado")

En el caso más común, $\deg(u) = 2g$ y $\gcd(\beta, \alpha) = 1$. Aquí tenemos

- $\deg(\alpha) \leq (g-1)/2$ y es igual, con α mónico si g es impar;
- $\deg(\gamma) \leq g/2$ y es igual, con γ mónico si g es par;
- $u_2 = (-1)^g(\beta^2 - \alpha^2 f)/u$;
- $v_2 \equiv -\beta/\alpha \bmod u_2$.

Quedan $2g$ coeficientes "variables" en α y γ.

Si empezamos con u_2 y v_2, y calculamos α y β (de alguna forma), entonces podemos reconstruir los polinomios u y v como:

- $u = (-1)^g(\beta^2 - \alpha^2 f)/u_2$
- $v \equiv -\beta/\alpha \bmod u$

Por lo tanto, la bisección (con $u = u_1^2$ y $v_1 \equiv v \bmod u_1$) buscará los $2g$-tuples asociados a los coeficientes de α y γ.

De-reducción general

Para bisectar (en el caso más común), buscamos polinomios $u_1(x)$, $\alpha(x)$ y $\gamma(x)$ tales que

1. u_1 tiene grado g y es mónico
2. $\beta = \alpha \cdot v_2 + \gamma \cdot u_2$
3. $(-1)^g(\beta^2 - \alpha^2 \cdot f)$ tiene grado $3g$ y es mónico
4. $u_1^2 \cdot u_2 = (-1)^g(\beta^2 - \alpha^2 \cdot f)$

Las condiciones 1-3 determinan los grados de α y γ, y cual de los dos debe ser monico.

La dificultad principal consiste en satisfacer la condición 4.

Para tener un sistema lineal que depende de raíces cuadradas, el desarrollo es parecido al caso de genero 2 (con θ_i raíz de $f(x)$), con la forma general de los bisectores:

$$\omega_i^2 = (-1)^g u_2(\theta_i)$$

De-reducción general

Teorema

Si $f(x) = \prod_{i=1}^{2g+1} (x - \theta_i)$ *donde los* θ_i *son elementos distintos en* $\mathbb{F}_q$*, entonces un divisor* $D_2 = [u_2, v_2]$ *tal que* $\gcd(u_2, f) = 1$ *tiene biseccciones si y solo si* $u_2(\theta_i)$ *es un cuadrado en* $\mathbb{F}_q$ *para todo* θ_i*.*

El nuevo sistema (para todo genero) viene de las ecuaciones:

$$\omega_i \cdot u_1(\theta_i) = \alpha(\theta_i) \cdot v_2(\theta_i) + \gamma(\theta_i) \cdot u_2(\theta_i)$$

Detalle:

- Al hacer γ monico cuando g es par, cambiamos el sistema para genero 2:
  - ahora tenemos $\gamma = x + k_0/k_1$ y $\alpha = 1/k_1$.
  - Es sencillo demostrar que para genero 2, los dos sistemas son equivalentes.

Modelos imaginarios en generos más altos

Teorema

Si $f(x) = \prod_{i=1}^{2g+1} (x - \theta_i)$ *donde los* θ_i *son elementos distintos en* $\mathbb{F}_q$*, entonces un divisor* $D_2 = [u_2, v_2]$ *tal que* $\gcd(u_2, f) = 1$*, entonces el sistema*

$$\omega_i \cdot u_1(\theta_i) = \alpha(\theta_i) \cdot v_2(\theta_i) + \gamma(\theta_i) \cdot u_2(\theta_i)$$

en los coeficientes de u_1*,* α *y* γ *(excepto los coeficientes fijados a* 1*) tiene solución única si y solo si* $u_2(x)$ *no es un cuadrado perfecto.*

En genero 2, para la unicidad teníamos que factorizar ω_i en el determinante, pero ahora los $v_2(\theta_i)$ pasaron del vector solución a la matriz...

- Podemos escribir $(-1)^g(v_2^2 - f) = u_2 \cdot z_2$ (z_2 es un polinomio de grado $g + 1$)
- Como $f(\theta_i) = 0$, $z_2(\theta_i)$ es un cuadrado $\iff$ $(-1)^g u_2(\theta_i)$ es un cuadrado $(= \omega_i^2)$.
- Si hay biseccciones, $z_2(\theta_i) = \sigma_i^2$ y $v_2(\theta_i) = (\sigma_i \cdot \omega_i)^2$, lo que permite factorizar el determinante (solamente para la demostración).

Número de bisecciones

En el caso imaginario, utilizamos 4 raíces cuadradas w_i, por lo tanto las 4 elecciones de signo, dando $2^4 = 16$ bisecciones.

A primera vista, todo va bien.

A segunda vista, elegimos 4 de los 5 raíces θ_i de $f(x)$, y no nos preocupemos del signo del último ω_i, entonces tendríamos más bisecciones posibles...

El teorema siguiente confirma que es suficiente definir 4 de los ω_i:

Teorema

Si $u_2(x)$ no es un cuadrado, entonces el producto de los bisectores es

i) $\prod_{i=1}^{2g+1} \omega_i = \prod_{j=1}^{g} \beta_j$ *si el modelo es imaginario,*

donde los β_j son los valores de $v_2(x)$ en las raíces de $u_2(x)$.

En consecuencia, la quinta raíz está completamente por las otras cuatro.

Número de biseccions

En el caso real, hay 5 raíces cuadradas w_{i6}, lo que daría $2^5 = 32$ biseccions.

Pero por la forma de la matriz, cambiar el signo de los cinco ω_{i6} al mismo tiempo corresponde a cambiar el signo de $\ell = \sqrt{(k_1^2 - f_6)u_2(\theta_6)}$.

Entonces, llegamos bien a $2^4 = 16$ biseccions.

De nuevo queda un ω_{ij}: $\omega_{66} = \pm 1$.

Observación: La demostración del teorema de bisección se queda igual si intercambiamos la i-esima fila (en ω_{i6}) con la "sexta" fila (en ω_{66}).

De nuevo, el teorema siguiente confirma que el último ω_{ik} está definido por los anteriores:

Teorema

Si $u_2(x)$ no es un cuadrado, para cualquier k fijo, el producto de los bisectores es

ii) $\prod_{i=1}^{6} \omega_{ik} = \frac{-1}{f_6} \prod_{j=1}^{2} \beta_j$ *si* $d = 6$ *(modelo real de genero 2),*

donde los β_j son los valores de $v_2(x)$ en las raíces de $u_2(x)$.

Modelos con 2-torsiones incompletas

Sea $\phi(x)$ un factor irreducible de $f(x)$, por lo que los θ_i asociados son conjugados.

Una consecuencia directa es que algunos elementos del grupo de 2-torsión de la curva están definidos en una extensión (de grado $\deg(\phi)$) de $\mathbb{F}_q$. La cantidad de bisecciones corresponderá al orden del subgrupo de 2-torsiones definidas sobre $\mathbb{F}_q$.

Los ω_i o ω_{ij} correspondientes a esos θ_i también serán conjugados, por lo tanto tendremos $\deg(\phi)$ de los ω_i o ω_{ij} fijados por una elección de signo de raíz cuadrada.

Se puede trabajar con (coeficientes de) polinomios modulo $\phi(x)$ en vez de los θ_i para obtener un nuevo sistema lineal definido sobre $\mathbb{F}_q$.

Pero, ¿Qué hay del teorema diciendo que el sistema tiene una solución única?

En el caso imaginario, se puede transformar el sistema original (en una extensión de $\mathbb{F}_q$) en un sistema definido sobre $\mathbb{F}_q$ utilizando bloques de Vandermonde asociados a $Norm(\theta_i)/\theta_i$, y mostrar que esa matriz es equivalente a la matriz que proviene de los coeficientes de polinomios modulo $\phi(x)$.

En el caso real, también podemos pasar por las normas para llegar a sistemas sobre $\mathbb{F}_q$.

Generalizaciones (trabajos en curso)

- Si hacemos un $2g$-tuple con los carácteres cuadraticos de los $(-1)^g u_2(\theta_i)$, obtenemos un carácter para la existencia de biseccciones;
- Este carácter permite mejorar algoritmos para encontrar generadores del 2-Sylow;
- En curvas elípticas donde el grupo de 3-torsión es $\mathbb{F}_q$-racional, se pueden definir dos trisectores provenientes de raíces cúbicas tales que cada elección de las raíces cúbicas da exactamente un pre-imagen;
- Para cualquier curva plana, se puede definir un $2g$-tuple de carácteres ℓ-adicos para obtener un carácter sobre la existencia de ℓ-secciones;
- Las ℓ-secciones son asociadas a $2g$ raíces ℓ-ésimas (los ℓ-sectores);
- Parece posible construir un sistema lineal con solución única asociado a un conjunto de $2g$ ℓ-sectores (independientes).