Trisecció de divisors sobre corbes hiperel·líptiques de gènere 2

Autor: Ricard Garra Oronich

Director: Josep M. Miret Biosca

Universitat de Lleida
Escola Politècnica Superior
Enginyeria Tècnica en Informàtica de Sistemes

Treball de final de carrera

Setembre 2012

Índex

Pàgina

Índex d'algorismes

Capítol 1

Introducció

La criptografia amb corbes el·líptiques i hiperel·líptiques ha adquirit un gran interès en els últims anys, ja que ofereix alternatives als criptosistemes clàssics que s'acostumen a utilitzar en criptografia [1, 6, 8]. El problema del logaritme discret sobre corbes el·líptiques i hiperel·líptiques no és vulnerable als mateixos atacs que sobre cossos finits, la qual cosa permet implementar el criptosistema de ElGamal [4, 7] i utilitzar mides de claus més petites, però garantint el mateix nivell de seguretat.

Això és útil sobretot en entorns limitats, on la memòria o capacitat de càlcul són reduïdes, ja que al treballar amb claus de menor mida, les operacions es poden fer més ràpid. Un exemple són les targetes intel·ligents, les quals tenen fortes limitacions de còmput i memòria, però necessiten que les dades estiguin xifrades per donar seguretat als usuaris.

És necessari treballar amb corbes que siguin segures criptogràficament, de manera que no sigui possible realitzar-hi un atac amb èxit en un temps acceptable. Per a determinar si una corba és bona criptogràficament, és necessari, en el cas d'una corba el·líptica, trobar el cardinal del grup de punts sobre el cos on està definida i, en el cas d'una corba hiperel·lítptica, cal trobar el cardinal de la seva varietat Jacobiana.

En aquest treball de final de carrera, donem mètodes per trobar els trisecats d'un divisor de la jacobiana d'una corba de gènere 2, particularment els trisecats de divisors d'ordre potència de 3. Per aquesta raó ha set necessari també poder trobar inicialment els divisors d'ordre 3 d'una corba donada, per a partir d'ells trobar els seus trisecats. Aquestes tècniques ens permetran determinar el subgrup de 3-Sylow de la corba i, en particular, trobar la major potència de 3 que divideix al cardinal de la seva Jacobiana, obtenint

així informació parcial sobre aquest cardinal, ja que ens pot ser útil saber si hi ha algun factor petit que el divideix, per a descartar corbes que no són bones criptogràficament.

Capítol 2

Corbes hiperel·líptiques

Les corbes hiperel·líptiques són una classe especial de corbes que són una generalització de les corbes el·líptiques. Les corbes hiperel·líptiques poden tenir qualsevol gènere $g \geq 1$, i en particular les de gènere $g = 1$ són les anomenades corbes el·líptiques.

Les corbes hiperel·líptiques són molt interessants en el camp de la criptografia de clau pública, ja que permeten obtenir un mateix nivell de seguretat amb mides de clau més petites, la qual cosa redueix els temps de càlcul en dispositius mòbils amb poca capacitat, com ara en targetes intel·ligents.

En particular, les corbes definides sobre cossos finits de característica dos de la forma F_{2^m}, són interessants a l'hora d'implementar codis i criptosistemes, i són les que utilitzarem en aquest treball.

2.1 Definicions bàsiques

En aquesta secció donarem un conjunt de definicions referents a les corbes hiperel·líptiques que seran necessàries per a comprendre la seva teoria.

2.1.1 Corba hiperel·líptica

Sigui $\mathbb{F}$ un cos. Una corba hiperel·líptica C de gènere g sobre $\mathbb{F}$, amb $g > 1$ és una corba algebraica plana no singular definida per l'equació següent:

$$C : y^2 + h(x)y = f(x) \in \mathbb{F}[x, y], \tag{2.1}$$

on $h(x) \in \mathbb{F}[x]$ és un polinomi tal que $deg(h) \leq g$ i $f(x)$ és un polinomi mònic amb $deg(f) = 2g+1$. Aquesta equació és l'anomenada de Weierstrass.

Un *punt singular* de C és un punt $(x, y) \in \mathbb{F} \times \mathbb{F}$, el qual satisfà simultàniament l'equació $y^2 + h(x)y = f(x)$ i les seves derivades parcials $2y + h(x) = 0$ i $h'(x)y - f'(x) = 0$.

En el nostre cas, treballarem amb corbes de característica 2, les quals han de complir que $h(x) \neq 0$ per a que les corbes no tinguin punts singulars.

Definim el *punt de l'infinit* P_∞ de C com el punt que es troba en la intersecció de C amb la recta de l'infinit r_∞, és a dir:

$$P_\infty = C \cap r_\infty = C \cap \{z = 0\} = [0, 1, 0].$$

Podem verificar que el punt P_∞ és un punt singular de C si la corba és de gènere > 1.

El conjunt de punts de la corba definits sobre el cos junt amb el punt de l'infinit el denotem per $C(\mathbb{F})$, és a dir:

$$C(\mathbb{F}) = \{(x, y) \in \mathbb{F} \times \mathbb{F} \mid y^2 + h(x)y = f(x)\} \quad \cup P_\infty.$$

Sigui $P = (x, y)$ un punt d'una corba hiperel·líptica. S'anomena el conjugat de P per la *involució hiperel·líptica* al punt $\tilde{P} = (x, -y - h(x))$. Definim també el conjugat del punt de l'infinit com ell mateix.

Si un punt $P \neq P_\infty$ satisfà que $P = \tilde{P}$, llavors diem que es un punt *especial* o *ramificat*.

2.2 Divisors

En aquest apartat veurem les propietats bàsiques dels divisors i introduirem la varietat Jacobiana d'una corba hiperel·líptica.

Un *divisor* D és una suma formal de punts en C de la forma

$$D = \sum_{P \in C(\mathbb{F})} n_P P, \quad n_P \in \mathbb{Z}$$

on únicament un número finit dels enters n_P són diferents de 0.

El *grau* de D, anomenat $deg(D)$, és la suma dels valors de n_P, és a dir:

$$deg(D) = \sum_{P \in C(\mathbb{F})} n_P.$$

El conjunt de tots els divisors de la corba hiperel·líptica C denotada per $\mathbb{D}(C)$, junt amb l'operació suma $(\mathbb{D}(C), +)$ formen una estructura de grup abelià.

El conjunt de tots els divisors de grau 0, és un subgrup de $\mathbb{D}(C)$, i el denotem així:

$$\mathbb{D}^0(C) = \{D \in \mathbb{D}(C) \mid deg(D) = 0\}$$

2.2.1 Divisors principals

Considerem una funció polinòmica ω sobre C. És a dir, una classe de polinomis en les variables x i y equivalents mòdul $y^2 + h(x)y - f(x)$. Una funció racional R sobre C és un quocient $\frac{\omega_1}{\omega_2}$ de dos funcions polinòmiques sobre C.

Donada una funció racional R sobre C s'anomena *divisor* de R i es denota $div(R)$ al divisor format pels zeros i pols de C comptats amb les seves multiplicitats.

Un divisor $D \in \mathbb{D}^0(C)$ és un *divisor principal* si $D = div(R)$ per alguna funció racional R sobre C.

El conjunt de tots els divisors principals es denota $\mathbb{P}(C)$, és a dir:

$$\mathbb{P}(C) = \{div(R) \mid R \in \bar{\mathbb{F}}(C)\}.$$

Aquest conjunt $\mathbb{P}(C)$ és un subgrup de $\mathbb{D}^0(C)$

El grup quocient $Jac(C)(\mathbb{F}) = \frac{\mathbb{D}^0(C)}{\mathbb{P}(C)}$ és el que anomenem *varietat Jacobiana* de la corba C. En el cas de treballar sobre un cos finit $\mathbb{F}_q$, el grup $Jac(C)(\mathbb{F}_q)$ és un grup abelià finit.

Siguin $D_1, D_2 \in \mathbb{D}^0(C)$ dos divisors, diem que són *equivalents* si:

$$D_1 \equiv D_2 \iff D_1 - D_2 \in \mathbb{P}(C).$$

D'aquesta manera, amb la varietat Jacobiana, hem aconseguit agrupar el conjunt dels infinits divisors de grau 0 en una corba hiperel·líptica en classes d'equivalència, construint així un grup finit.

Definim el *neutre* de l'operació suma en aquest grup com 0.

Anomenem *ordre d'un divisor* a l'enter n més petit tal que $nD = 0$, és a dir, $ord(D) = n$ si $nD = 0$ i $\nexists m < n$ tal que $mD = 0$.

Un cop definit el grup solament ens queda donar una representació als seus elements per a poder treballar amb ells de forma còmoda.

2.2.2 Divisors semireduïts i reduïts

Sigui $u(x), v(x) \in \bar{\mathbb{F}}[x]$ dos polinomis tals que $deg_x v < deg_x u$.

Si $u \mid (v^2 + vh - f)$, llavors $div(u, v)$ és un divisor semireduït.

Si a més a més, $deg_x u \leq g$, llavors $div(u, v)$ és un divisor reduït.

A partir del teorema de Riemann-Roch es pot provar el següent:

Per a cada divisor $D \in \mathbb{D}^0(C)$ existeix un únic divisor reduït D_1 tal que $D \sim D_1$. Aquests elements ens serviran per a identificar cada element de la Jacobiana $Jac(C)(\mathbb{F}_q)$.

2.3 Operacions amb divisors

En aquesta secció explicarem algorismes per a fer diferents operacions amb divisors de la varietat Jacobiana d'una corba hiperel·líptica de gènere 2 definida sobre un cos finit binari $\mathbb{F}_{2^n}$. Vegis [1, 5].

2.3.1 Suma de divisors

Per a la suma, utilitzem l'*algorisme de Cantor* (1), el qual ens serveix per a corbes de qualsevol gènere.

Algorithm 1 Suma de divisors

Input: $D_1 = (U_1, V_1), D_2 = (U_2, V_2)$
Output: $D_3 = (U_3, V_3) = D_1 + D_2$
  $d = gcd(U_1, U_2, V_1 + v_2 + h) = s_1 U1 + s_2 U_2 + s_3(V_1 + V_2 + h)$
  $U = \frac{U_1 U_2}{d^2}$
  $V = \frac{s_1 U_1 V_2 + s_2 U_2 V_1 + s3(V_1 V_2 + f)}{d} \bmod U$
  while $degree(U) > g$ **do**
    $k = \frac{f + Vh + V^2}{U}$
    $V = h + V \bmod U$
  end while
  $U_3 = MakeMonic(U)$
  $V_3 = V$
  return (U_3, V_3)

Cal fer notar que per a calcular $gcd(f_1, f_2, f_3)$, podem fer les següents

operacions:

$$gcd(f_1, f_2) = c = a_1 f_1 + a_2 f_2$$

$$gcd(c, f_3) = d = b_1 c + b_2 f_3$$

Llavors substituïm c en la segona equació i ens quedaria així:

$$d = (a_1 b_1) f_1 + (a_2 b_1) f_2 + b_2 f_3$$

D'aquesta manera identifiquem $s_1 = (a_1 b_1)$, $s_2 = (a_2 b_1)$ i $s_3 = b_2$, obtenint així les s_i que utilitzarem en l'algorisme de Cantor dels passos següents de l'algorisme.

2.3.2 Doblat d'un divisor

Tot seguit definim l'algorisme de doblat d'un divisor de la Jacobiana.

Algorithm 2 Doblat d'un divisor

Input: $D_1 = (U_1, V_1)$
Output: $D_2 = (U_2, V_2) = 2D_1$

$U_1' = U_1^2$
$S = \frac{f + hV_1 + V_1^2}{U_1}$
$S = Sh^{-1} \bmod U_1$
$V_1' = SU_1 + v_1$
$U_2' = \frac{f + hV_1' + V_1'^2}{U_1'}$
$U_2 = MakeMonic(U_2')$
$V_2 = V_1' + h \bmod U_2$
return (U_2, V_2)

2.4 Segona component d'un divisor

Hem trobat que ens seria molt útil i necessari disposar d'una funció per poder obtenir tots els divisors amb una primera component donada. En el programa utilitzat, Magma [2], trobem aquesta funció però només per a corbes el·líptiques, no per a hiperel·líptiques. Per tant, l'hem hagut d'implementar ja que ens era necessària per a altres funcions.

A continuació explicarem el mètode seguit per a trobar les segones components d'un divisor, així com l'algorisme en pseudocodi.

En general, un divisor serà de la forma $D = (x^2 + u_1x + u_0, v_1x + v_0)$. Un divisor ens representa normalment a 2 punts de la corba $P_1 = (\alpha_1, \beta_1)$ i $P_2 = (\alpha_2, \beta_2)$.

La primera component també es pot escriure com $(x+\alpha_1)(x+\alpha_2)$, on α_1 i α_2 són les arrels del polinomi (recordem que estem treballant en cossos de característica 2, i que per tant restar és el mateix que sumar).

Un cop trobades aquestes arrels, les podem substituir a la segona component per obtenir les abscisses dels punts amb el següent sistema d'equacions:

$$\begin{aligned} v_1\alpha_1 + v_0 &= \beta_1, \\ v_1\alpha_2 + v_0 &= \beta_2. \end{aligned}$$

Operant podem aïllar:

$$\begin{aligned} v_1 &= \frac{\beta_1 + \beta_2}{u_1}, \\ v_0 &= \beta_1 + v_1\alpha_1. \end{aligned}$$

Els valors de β_1 i β_2 són els que compleixen l'equació de la corba (2.1) per a cadascun dels valors de α_1 i α_2. Per tant, trobarem els valors que volem buscant les arrels de l'equació de la corba avaluada en cadascuna de les ordenades:

$$\begin{aligned} \beta_1 &= Roots(y^2 + h(\alpha_1)y + f(\alpha_1)), \\ \beta_2 &= Roots(y^2 + h(\alpha_2)y + f(\alpha_2)). \end{aligned}$$

Hem de considerar, però, alguns casos especials en que haurem de seguir un mètode una mica diferent, segons si:

- Les arrels de l'equació de la primera component no estan al cos base, sinó a una extensió. Haurem de fer el mateix procés però en l'extensió, i després tornar al cos base.

- Només hi ha una arrel amb multiplicitat 2, la qual cosa indica que els dos punts dels quals s'ha obtingut el divisor, tenen la mateixa ordenada, i per tant es tracta d'un punt i del seu oposat. En aquest cas només hi ha una α, i les dos abscisses seran les 2 arrels de l'equació $y^2 + h(\alpha)y + f(\alpha)$. El que fem és trobar els 2 punts $P = (\alpha, \beta_1)$ i $Q = (\alpha, \beta_2)$, i calcular els 2 divisors que es poden aconseguir combinant-los.

- El divisor és de pes 1, és a dir, un divisor de la forma $D = (x + u_0, v_0)$. En aquest cas el divisor només representa a un sol punt $P = (\alpha, \beta)$, on $u_0 = \alpha$ i $v_0 = \beta$.

Seguidament hi ha l'algorisme en pseudocodi, tenint em compte tots els possibles casos:

Algorithm 3 Segona component d'un divisor

Input: $C : y^2 + h(x)y = f(x) \in \mathbb{F}_{2^m}$, $u(x) \mid D = (u(x), v(x)) \in Jac(C)$
Output: List of all $v(x) \mid D = (u(x), v(x)) \in Jac(C)$

```
Component_list = EmptyList()
if Deg(u(x)) = 1 then
    /* u(x) = (x + u_0) */
    β = Roots(y^2 + h(u_0)y + f(u_0))
    for all β_i ∈ β do
        v_0 = β_i
        Append(Component_list,v_0)
    end for
    return Component_list
end if
/* u(x) = (x^2 + u_1 x + u_0) */
alphas = Roots(u(x))
if #alphas ≠ 0 then
    if #alphas = 2 then
        α_1 = alphas[1]
        α_2 = alphas[2]
        β_1 = Roots(y^2 + h(α_1)y + f(α_1))
        β_2 = Roots(y^2 + h(α_2)y + f(α_2))
        for all β_i ∈ β_1 do
            for all β_j ∈ β_2 do
                v_1 = (β_i + β_j) / u_1
                v_0 = β_i + v_1 α_1
                Append(Component_list,(v_1 x + v_0))
            end for
        end for
    else
        /* #alphas = 1 */
        α = alphas[1]
        β = Roots(y^2 + h(α)y + f(α))
        β_1 = β[1]
        β_2 = β[2]
        P = (α_1, β_1) ∈ C
        Q = (α_2, β_2) ∈ C
```

$D_1 = ConstructDivisor(P-Q) = (x^2+u_1x+u_0, v_{11}x+v_{10}) \in Jac(C)$

$D_2 = ConstructDivisor(Q-P) = (x^2+u_1x+u_0, v_{21}x+v_{20}) \in Jac(C)$
Append(Component_list,$(v_{11}x + v_{10})$)
Append(Component_list,$(v_{21}x + v_{20})$)
end if
else
/* $\#alphas = 0$ */
$alphas = Roots(u(x)) \in \mathbb{F}_{2^{2m}}$
$\alpha_1 = alphas[1]$
$\alpha_2 = alphas[2]$
$\beta_1 = Roots(y^2 + h(\alpha_1)y + f(\alpha_1)) \in \mathbb{F}_{2^{2m}}$
$\beta_2 = Roots(y^2 + h(\alpha_2)y + f(\alpha_2)) \in \mathbb{F}_{2^{2m}}$
for all $\beta_i \in \beta_1$ **do**
for all $\beta_j \in \beta_2$ **do**
if $(\beta_i + \beta_j)$ is in $\mathbb{F}_{2^m}$ **then**
$v_1 = \dfrac{\beta_i + \beta_j}{u_1}$
$v_0 = \beta_i + v_1\alpha_1$
if v_0 is in $\mathbb{F}_{2^m}$ **then**
$v(x) = v_1x + v_0 \in \mathbb{F}_{2^m}$
Append(Component_list,$(v(x))$)
end if
end if
end for
end for
end if
return Component_list

Capítol 3

Divisors d'ordre 3

Una part interessant d'aquest treball és poder trobar el 3-Sylow d'una corba donada, i per a això és necessari trobar els divisors d'ordre 3, ja que seran la base a partir dels quals podrem aplicar la resta d'algorismes. Un cop tinguem els divisors d'ordre 3, podrem anar fent les diferents *triseccions*.

Tot seguit expliquem el mètode utilitzat per a aconseguir-los.

Tenim la corba hiperel·líptica C definida per l'equació $y^2+h(x)y = f(x)$, on $f(x) = x^5 + f_4x^4 + f_3x^3 + f_2x^2 + f_1x + f_0$ i $h(x) = h_2x^2 + h_1x + h_0$. Volem buscar divisors $D = (u(x), v(x))$ de tal forma que $3D = 0$, on aquí el 0 representa l'element neutre del grup. Una altra manera d'escriure-ho seria: $2D + D = 0$, és a dir, $2D = -D$ Per tant, igualarem les equacions que resulten de duplicar un divisor al fer $2D$, amb les de la desreducció de $-D$.

Siguin $u(x)$ i $v(x)$ components del divisor D, i $k(x)$ un polinomi auxiliar:

$$\begin{aligned} k(x) &= k_1x + k_0, \\ u(x) &= x^2 + u_1x + u_0, \\ v(x) &= v_1x + v_0. \end{aligned}$$

La desreducció $D' = (u'(x), v'(x))$ del divisor $-D = (u(x), v(x) + h(x))$, ve donada per

$$u'(x) = \frac{f(x) + v(x)h(x) + v(x)^2}{u(x)} + k(x)^2u(x) + h(x)k(x),$$

és a dir,

$$\begin{aligned} u'(x) \quad &= k_1^2x^4 + (k_1^2u_1 + h_2k_1 + 1)x^3 + (k_1^2u_0 + h_1k_1 + h_2k_0 + k_0^2 + f_4 + u_1)x^2 \\ &+(k_0^2u_1 + h_0k_1 + h_1k_0 + f_4u_1 + u_1^2 + h_2v_1 + f_3 + u_0)x \\ &+(f_4u_1^2 + u_1^3 + k_0^2u_0 + h_2u_1v_1 + h_0k_0 + f_3u_1 + f_4u_0 + h_1v_1 + v_1^2 + h_2v_0 \\ &+f_2). \end{aligned}$$

Necessitem que l'expressió sigui mònica, per tant dividim tota l'expressió pel coeficient del terme amb major exponent, k_1^2.

Ara ens falta igualar amb $2D$, que equival a elevar al quadrat la primera component de D, per trobar la primera component de $2D$, és a dir:

$$u(x)^2 = x^4 + u_1^2 x^2 + u_0^2.$$

Igualant cada terme obtenim el sistema:

$$\begin{array}{ll} 0 & = k_1^2 u_1 + 1 + h_2 k_1 \\ u_1^2 & = k_1^2 u_0 + h_1 k_1 + h_2 k_0 + k_0^2 + f_4 + u_1 \\ 0 & = k_0^2 u_1 + h_0 k_1 + h_1 k_0 + f_4 u_1 + u_1^2 + h_2 v_1 + f_3 + u_0 \\ k_1^2 u_0^2 & = f_4 u_1^2 + u_1^3 + k_0^2 u_0 + h_2 u_1 v_1 + h_0 k_0 + f_3 u_1 + f_4 u_0 + h_1 v_1 + v_1^2 + h_2 v_0 \\ & + f_2 \end{array}$$

De les 2 primeres equacions, podem aïllar u_1 i u_0:

$$\begin{aligned} u_1 &= \frac{1}{k_1^2} + \frac{h_2}{k_1} \\ u_0 &= \frac{h_1}{k_1} + \frac{h_2^2 + h_2 k_0 + k_0^2 + f_4}{k_1^2} + \frac{h_2}{k_1^3} \end{aligned}$$

Tot seguit, substituïm a les altres:

$$0 = h_0 k_1^5 + h_1 k_1^4 k_0 + h_2 k_1^3 k_0^2 + h_2 k_1^4 v_1 + f_4 h_2 k_1^3 + f_3 k_1^4 + h_1 k_1^3 + h_2 k_1^2 k_0 + h_2 k_1 + 1 \tag{3.1}$$

$$\begin{array}{ll} 0 & = h_0 k_1^6 k_0 + h_2^2 k_1^4 k_0^2 + h_1 k_1^5 k_0^2 + h_2 k_1^4 k_0^3 + k_1^4 k_0^4 + h_2^2 k_1^5 v_1 + h_1 k_1^6 v_1 + k_1^6 v_1^2 \\ & + h_2 k_1^6 v_0 + f_3 h_2 k_1^5 + f_4 h_1 k_1^5 + f_2 k_1^6 + f_4 h_2 k_1^4 k_0 + h_2^3 k_1^3 + f_4^2 k_1^4 + h_2 k_1^3 k_0^2 \\ & + h_2 k_1^4 v_1 + f_4 h_2 k_1^3 + f_3 k_1^4 + h_2^2 k_1^2 + f_4 k_1^2 + h_2 k_1 + 1 + u_0^2 k_1^6 \end{array} \tag{3.2}$$

Finalment, igualarem a 0 el residu de la divisió que hem fet a l'hora de trobar la desreducció. Per separat, del terme lineal i del terme independent obtenim:

$$\begin{array}{ll} 0 & = h_0 k_1^8 v_1 + h_2^2 k_1^6 k_0 v_1 + h_2 k_1^6 k_0^2 v_1 + h_2 k_1^7 v_1^2 + h_2^2 k_1^7 v_0 + h_1 k_1^8 v_0 + f_4 h_2^3 k_1^5 + f_2 h_2 k_1^7 \\ & + f_3 h_1 k_1^7 + f_1 k_1^8 + f_3 h_2 k_1^6 k_0 + f_3 k_1^6 k_0^2 + f_4 h_2 k_1^6 v_1 + h_2^4 k_1^4 + h_2^2 h_1 k_1^5 + f_4 f_3 k_1^6 \\ & + h_1^2 k_1^6 + h_2^3 k_1^4 k_0 + k_1^4 k_0^4 + h_2^2 k_1^5 v_1 + h_1 k_1^6 v_1 + k_1^6 v_1^2 + h_2 k_1^6 v_0 + f_3 h_2 k_1^5 + f_2 k_1^6 \\ & + h_2^3 k_1^3 + f_4^2 k_1^4 + h_2 k_1^4 v_1 + f_4 h_2 k_1^3 + f_3 k_1^4 + h_1 k_1^3 + h_2 k_1^2 k_0 + k_1^2 k_0^2 + h_2 k_1 + 1 \end{array} \tag{3.3}$$

$$\begin{aligned}0 &= h_2^4k_1^6v_1 + h_1^2k_1^8v_1 + h_2^3k_1^6k_0v_1 + h_2h_1k_1^7k_0v_1 + h_2^2k_1^6k_0^2v_1 + h_1k_1^7k_0^2v_1 + h_2^2k_1^7v_1^2\\ &+h_1k_1^8v_1^2 + h_2k_1^7k_0v_1^2 + k_1^7k_0^2v_1^2 + h_2^3k_1^7v_0 + h_2h_1k_1^8v_0 + h_0k_1^9v_0 + h_2^2k_1^7k_0v_0\\ &+h_2k_1^7k_0^2v_0 + k_1^9v_0^2 + f_3h_2^3k_1^6 + f_4h_2^2h_1k_1^6f_2h_2^2k_1^7 + f_3h_2h_1k_1^7 + f_4h_1^2k_1^7 + f_2h_1k_1^8\\ &+f_0k_1^9 + f_4h_2^3k_1^5k_0 + f_3h_2^2k_1^6k_0 + f_2h_2k_1^7k_0 + f_3h_2k_1^6k_0^2 + f_2k_1^7k_0^2 + f_4k_1^5k_0^4\\ &+f_4h_2^2k_1^6v_1 + f_4h_1k_1^7v_1 + f_4k_1^7v_1^2 + f_4h_2k_1^7v_0h_2^5k_1^4 + f_4^2h_2^2k_1^5 + h_2^3h_1k_1^5 + f_4f_3h_2k_1^6\\ &+f_4f_2k_1^7 + h_2^4k_1^4k_0 + h_2^3k_1^4k_0^2 + h_2^2k_1^5k_0v_1 + h_2k_1^5k_0^2v_1 + h_2k_1^6v_1^2 + h_2^2k_1^6v_0 + f_4^3k_1^5\\ &+f_2h_2k_1^6 + f_3h_1k_1^6 + f_3h_2k_1^5k_0 + f_3k_1^5k_0^2 + f_4h_2k_1^5v_1 + h_2^2h_1k_1^4 + f_4f_3k_1^5 + h_2^3k_1^3k_0\\ &+h_2^2k_1^3k_0^2 + h_2^2k_1^4v_1 + f_4h_2^2k_1^3 + f_3h_2k_1^4 + f_4h_1k_1^4 + f_4h_2k_1^3k_0 + f_4k_1^3k_0^2 + f_4^2k_1^3\\ &+h_2h_1k_1^3 + h_2^2k_1^2k_0 + h_2k_1^2k_0^2 + h_1k_1^2 + h_2k_1k_0 + k_1k_0^2 + f_4k_1 + h_2\end{aligned} \tag{3.4}$$

Aquí haurem de diferenciar 3 casos: quan $h_2 \neq 0$; $h_2 = 0$ i $h_1 \neq 0$; i quant $h_2 = h_1 = 0$.

3.1 Cas $h_2 = h_1 = 0$

Si fem que $h(x)$ sigui constant, el sistema ens queda així amb les equacions (3.1), (3.2) i (3.3). En aquest cas, no ens fa falta l'equació de la part del terme independent del residu:

$$\begin{aligned}0 &= h_0k_1^5 + f_3k_1^4 + 1,\\ 0 &= h_0k_1^6k_0 + k_1^6v_1^2 + f_2k_1^6 + f_3k_1^4 + f_4k_1^2 + 1,\\ 0 &= h_0k_1^8v_1 + f_1k_1^8 + f_3k_1^6k_0^2 + f_4f_3k_1^6 + k_1^4k_0^4 + k_1^6v_1^2 + f_2k_1^6 + f_4^2k_1^4 + f_3k_1^4\\ &+k_1^2k_0^2 + 1.\end{aligned}$$

Trobant les arrels de la primera equació, podem trobar els possibles valors de k_1 directament. Si fem la resultant de les 2 últimes equacions, aconseguim un polinomi sense v_1 i amb només k_1 i k_0 com a incògnites. Ja que els valors de l'equació de la corba són coneguts i tenim les possibles solucions de k_1, només ens cal trobar les arrels de la resultant per obtenir els valors de k_0 per cada k_1. La resultant ens queda de la següent forma:

$$\begin{aligned}0 &= h_0^3k_1^{12}k_0 + f_2h_0^2k_1^{12} + f_1^2k_1^{12} + f_3^2k_1^8k_0^4 + f_3h_0^2k_1^{10} + f_4^2f_3^2k_1^8 + h_0^2k_1^8k_0^2\\ &+k_1^4k_0^8 + f_4h_0^2k_1^8 + f_4^4k_1^4 + h_0^2k_1^6 + k_0^4 + f_4^2.\end{aligned}$$

Un cop tenim k_1 i k_0, fem servir les equacions d'abans per trobar u_1 i u_0:

$$u_1 = \frac{1}{k_1^2}, \quad u_0 = \frac{f_4 + k_0^2}{k_1^2}.$$

Un cop tenim la primera component, només ens cal trobar la segona component mitjançant la funció que hem explicat en la secció 2.4 i comprovar que realment és un divisor d'ordre 3.

3.2 Cas $h_2 = 0$ i $h_1 \neq 0$

Aquí partim de les equacions (3.1), (3.2), (3.3), (3.4) originals. De la primera equació aïllem k_0:

$$k_0 = \frac{h_0 k_1^5 + f_3 k_1^4 + h_1 k_1^3 + 1}{h_1 k_1^4}$$

Substituint aquest valor, el sistema ens queda així:

$$\begin{aligned}
0 &= h_1^3 k_1^9 + h_1^2 k_1^9 v_1 + h_1 k_1^9 v_1^2 + f_4 h_1^2 k_1^8 + f_2 h_1 k_1^9 + f_3 h_0 k_1^9 + f_3^2 k_1^8 + h_1 h_0 k_1^8 \\
&\quad + f_3 h_1 k_1^7 + h_1^2 k_1^6 + f_4 h_1 k_1^5 + h_0 k_1^5 + h_1 k_1^3 + 1 \\
0 &= h_1^4 h_0 k_1^{20} v_1 + h_1^5 k_1^{20} v_0 + f_3 h_1^5 k_1^{19} + f_1 h_1^4 k_1^{20} + f_3 h_1^2 h_0^2 k_1^{20} + f_4 f_3 h_1^4 k_1^{18} \\
&\quad + h_1^6 k_1^{18} + h_0^4 k_1^{20} + h_1^5 k_1^{18} v_1 + h_1^4 k_1^{18} v_1^2 + f_3^3 h_1^2 k_1^{18} + f_2 h_1^4 k_1^{18} + f_4^2 h_1^4 k_1^{16} \\
&\quad + h_1^5 k_1^{15} + f_3^4 k_1^{16} + h_1^2 h_0^2 k_1^{16} + f_3^2 h_1^2 k_1^{14} + h_1^4 k_1^{12} + f_3 h_1^2 k_1^{10} + h_1^2 k_1^6 + 1 \\
0 &= h_1^6 k_1^{19} v_1 + h_1^3 h_0^2 k_1^{20} v_1 + h_1^5 k_1^{19} v_1^2 + h_1^2 h_0^2 k_1^{20} v_1^2 + h_1^4 h_0 k_1^{20} v_0 + h_1^4 k_1^{20} v_0^2 \\
&\quad + f_4 h_1^6 k_1^{18} + f_2 h_1^5 k_1^{19} + f_0 h_1^4 k_1^{20} + f_2 h_1^2 h_0^2 k_1^{20} + f_4 h_0^4 k_1^{20} + f_4 h_1^5 k_1^{18} v_1 \\
&\quad + f_4 h_1^4 k_1^{18} v_1^2 + f_4 f_2 h_1^4 k_1^{18} + f_3^2 h_1^3 k_1^{18} v_1 + f_3^2 h_1^2 k_1^{18} v_1^2 + f_4^3 h_1^4 k_1^{16} + f_3 h_1^5 k_1^{17} \\
&\quad + f_3^2 f_2 h_1^2 k_1^{18} + f_3 h_1^2 h_0^2 k_1^{18} + f_4 f_3 h_1^4 k_1^{16} + h_1^5 k_1^{16} v_1 + h_1^4 k_1^{16} v_1^2 + f_4 h_1^5 k_1^{15} \\
&\quad + f_4 f_3^4 k_1^{16} + f_3^3 h_1^2 k_1^{16} + f_2 h_1^4 k_1^{16} + f_4 h_1^2 h_0^2 k_1^{16} + f_4^2 h_1^4 k_1^{14} + f_4 f_3^2 h_1^2 k_1^{14} \\
&\quad + f_3 h_1^4 k_1^{14} + h_1^5 k_1^{13} + h_1^2 h_0^2 k_1^{14} + f_4 h_1^4 k_1^{12} + f_3^2 h_1^2 k_1^{12} + h_1^4 k_1^{10} + h_1^3 k_1^{10} v_1 \\
&\quad + h_1^2 k_1^{10} v_1^2 + f_2 h_1^2 k_1^{10} + f_3 h_1^2 k_1^8 + f_4 h_1^2 k_1^6 + h_1^2 k_1^4 + f_4
\end{aligned}$$

De la segona equació aïllem v_0:

$$\begin{aligned}
v_0 &= (h_1^4 h_0 k_1^{20} v_1 + f_3 h_1^5 k_1^{19} + f_1 h_1^4 k_1^{20} + f_3 h_1^2 h_0^2 k_1^{20} + f_4 f_3 h_1^4 k_1^{18} + h_1^6 k_1^{18} \\
&\quad + h_0^4 k_1^{20} + h_1^5 k_1^{18} v_1 + h_1^4 k_1^{18} v_1^2 + f_3^3 h_1^2 k_1^{18} + f_2 h_1^4 k_1^{18} + f_4^2 h_1^4 k_1^{16} + h_1^5 k_1^{15} \\
&\quad + f_3^4 k_1^{16} + h_1^2 h_0^2 k_1^{16} + f_3^2 h_1^2 k_1^{14} + h_1^4 k_1^{12} f_3 h_1^2 k_1^{10} + h_1^2 k_1^6 + 1) \cdot \frac{1}{h_1^5 k_1^{20}}
\end{aligned}$$

Substituint a les altres 2 equacions i fent la resultant entre elles eliminant v_1, obtenim una equació amb només k_1 d'incògnita, amb grau 40:

$$\begin{aligned}
0 &= h_1^{13} k_1^{39} + f_4 h_1^{12} k_1^{38} + f_0 h_1^{10} k_1^{40} + f_1 h_1^9 h_0 k_1^{40} + f_2 h_1^8 h_0^2 k_1^{40} + f_3 h_1^7 h_0^3 k_1^{40} \\
&\quad + f_4 h_1^6 h_0^4 k_1^{40} + f_4^2 h_1^{11} k_1^{37} + f_3^2 h_1^{10} k_1^{38} + h_1^{11} h_0 k_1^{38} + f_1^2 h_1^8 k_1^{40} + f_3^2 h_1^4 h_0^4 k_1^{40} \\
&\quad + h_1^5 h_0^5 k_1^{40} + f_4^3 h_1^{10} k_1^{36} + f_4^2 f_3^2 h_1^8 k_1^{36} + f_4^2 h_1^9 h_0 k_1^{36} + f_3^4 h_1^7 k_1^{37} + h_1^9 h_0^2 k_1^{37} \\
&\quad + h_0^8 k_1^{40} + f_4 f_3^4 h_1^6 k_1^{36} + f_4 h_1^8 h_0^2 k_1^{36} + f_4^2 h_1^{10} k_1^{34} + f_3^6 h_1^4 k_1^{36} + f_3^4 h_1^5 h_0 k_1^{36} \\
&\quad + f_3^2 h_1^6 h_0^2 k_1^{36} + h_1^7 h_0^3 k_1^{36} + f_4^4 h_1^8 k_1^{32} + h_1^{11} k_1^{33} + f_3^4 h_1^6 k_1^{34} + h_1^8 h_0^2 k_1^{34} \\
&\quad + f_4 h_1^{10} k_1^{32} + f_3^2 h_1^8 k_1^{32} + h_1^9 h_0 k_1^{32} + f_3^8 k_1^{32} + h_1^4 h_0^4 k_1^{32} + f_4^2 h_1^8 k_1^{28} + f_3^4 h_1^4 k_1^{28} \\
&\quad + h_1^6 h_0^2 k_1^{28} + h_1^7 k_1^{21} + f_4 h_1^6 k_1^{20} + f_3^2 h_1^4 k_1^{20} + h_1^5 h_0 k_1^{20} + h_1^6 k_1^{18} + h_1^4 k_1^{12} + 1
\end{aligned}$$

D'aquí trobem les solucions de k_1, amb les quals es poden trobar les k_0 per cada una. Amb això podem obtenir tots els coeficients de les components del divisor.

3.3 Cas $h_2 \neq 0$

A partir de (3.1) aïllem v_1 i substituïm a (3.2), d'on podem aïllar v_0:

$$\begin{aligned} v_1 &= \frac{h_0k_1^5 + h_1k_1^4k_0 + h_2k_1^3k_0^2 + f_4h_2k_1^3 + f_3k_1^4 + h_1k_1^3 + h_2k_1^2k_0 + h_2k_1 + 1}{h_2k_1^4} \\ v_0 &= (h_2^6k_1^6 + h_2^2h_1^2k_1^8 + h_2^3h_0k_1^8 + h_2h_1h_0k_1^9 + h_0^2k_1^{10} + h_2^3h_1k_1^7k_0 + h_2h_1^2k_1^8k_0 \\ &\quad + h_2^2h_0k_1^8k_0 + h_2^4k_1^6k_0^2 + h_1^2k_1^8k_0^2 + h_2^3k_1^6k_0^3 + h_2^2k_1^6k_0^4 + f_4h_2^4k_1^6 + f_2h_2^2k_1^8 \\ &\quad + f_3h_2h_1k_1^8 + f_4h_2^3k_1^6k_0 + h_2^5k_1^5 + f_4^2h_2^2k_1^6 + h_2^3h_1k_1^6 + h_2h_1^2k_1^7 + h_2^2h_0k_1^7 \\ &\quad + f_3^2k_1^8 + h_2^4k_1^5k_0 + h_2^4k_1^4 + h_1^2k_1^6 + h_2^3k_1^4k_0 + h_2^2k_1^4k_0^2 + f_4h_2^2k_1^4 + h_2^3k_1^3 \\ &\quad + h_2h_1k_1^4 + h_2^2k_1^2 + 1) \cdot \frac{1}{h_2^3k_1^8} \end{aligned}$$

Com hem fet abans, substituïm a les altres i fem la resultant, eliminant en aquest cas k_0, d'aquesta manera ens quedarà una única equació amb k_1, que si factoritzem i ens quedem amb el factor bo, aquest és de grau 40. Aquest és el valor esperat, ja que hi pot haver fins a 40 primeres components diferents de divisors d'ordre 3.

Per cada una hi haurà 2 segones components diferents, que farien un total de 80 divisors d'ordre 3, que és el màxim. No ficarem aquí la resultant ja que és especialment llarga.

3.4 Divisors independents

Amb els mètodes explicats anteriorment, podem trobar 2, 8, 26 o 80 divisors d'ordre 3 diferents. Ens interessa que, donada una llista dels divisors d'ordre 3 d'una corba, puguem trobar els divisors independents, és a dir, quedar-nos únicament amb aquells que no són combinació de cap altre.

Això ens permetrà trobar el 3-Rang de la corba, que serà igual al número de divisors d'ordre 3 independents.

Per a cadascun dels casos, tindrem 1, 2, 3 o 4 divisors independents segons si hi ha 2, 8, 26 o 80 divisors d'ordre 3 respectivament.

Per a aconseguir-ho, hem d'anar eliminant tots els divisors que siguin combinació d'altres:

- Primer, eliminem la meitat dels divisors, traient els seus inversos.
- Després d'això, com a mínim 1 dels divisors ja es independent. Si fos rang 1, ja hauríem acabat.

- Si el rang és més gran, haurem de treure també totes les combinacions possibles entre divisors. Triarem un segon divisor com a bo, i eliminarem els divisors que es puguin aconseguir amb els dos bons: si tenim D_1 i D_2, eliminarem $D_1 + D_2$, $D_1 - D_2$, $-D_1 + D_2$ i $-D_1 - D_2$. Si la corba és de rang 2, amb això és suficient.

- Procedirem de la mateixa forma per corbes de rang 3 i 4: anirem fixant un divisor més, i eliminant els que es puguin trobar com a una combinació d'aquests.

Cal fer notar que per a que una corba pugui tenir rang 3, és necessari que $h_2 \neq 0$, sinó només podrà tenir rang 1, 2 o 4.

Capítol 4

Trisecció de divisors

Una part important d'aquest treball consisteix en aconseguir trobar el *trisecat*, o divisor tercera part, d'un divisor donat. Volem trobar doncs, divisors D_1, tals que $3D_1 = D_3$, sent D_3 conegut. Llavors direm que D_1 és el *trisecat* de D_3.

Tindrem doncs 2 divisors de la següent forma:

$D_3 = (u_3(x), v_3(x)) = (x^2 + u_{31}x + u_{30}, v_{31}x + v_{30})$

$D_1 = (u_1(x), v_1(x)) = (x^2 + u_{11}x + u_{10}, -)$

Només ens interessa trobar la primera component de D_1, ja que la segona la podem trobar coneixent la primera.

Procedirem de manera semblant a com ho hem fet per a trobar els divisors d'ordre 3: per trobar la primera component de $3D_1$, només ens cal elevar al cub la primera component de D_1:

$u_3(x)^3 = x^6 + u_{11}x^5 + (u_{11}^2 + u_{10})x^4 + u_{11}^3x^3 + (u_{10}^2 + u_{11}^2u_{10})x^2 + u_{11}u_{10}^2x + u_{10}^3$

Tot seguit buscarem la desreducció $\overline{D}_3$ de D_3:

$$\overline{D}_3 = (\overline{u}_3, \overline{v}_3) = \frac{f(x) + h(x)v_3(x) + v_3^2(x)}{u_3(x)} + h(x)k(x) + k(x)u(x)),$$

on $k(x) = k_2x^2 + k_1x + k_0$. Això ens donarà la primera component del divisor desreduït. Desenvolupant l'expressió, ens queda el següent:

$$\begin{aligned}\overline{u}_3(x) &= k_2^2x^6 + u_{31}k_2^2x^5 + (k_2^2u_{30} + k_1^2 + k_2h_2)x^4 + (u_{31}k_1^2 + k_1h_2 + k_2h_1 \\ &+1)x^3 + (k_1^2u_{30} + k_0^2 + k_0h_2 + k_1h_1 + k_2h_0 + u_{31} + f_4)x^2 + (u_{31}k_0^2 \\ &+u_{31}^2 + u_{31}f_4 + v_{31}h_2 + k_0h_1 + k_1h_0 + u_{30} + f_3)x + u_{31}^3 + k_0^2u_{30} \\ &+u_{31}^2f_4 + u_{31}v_{31}h_2 + v_{31}^2 + u_{30}f_4 + u_{31}f_3 + v_{30}h_2 + v_{31}h_1 + k_0h_0 \\ &+f_2\end{aligned}$$

En aquest treball, ens centrarem en el cas que la $h(x)$ és constant, és a dir, $h_2 = h_1 = 0$, $h_0 \neq 0$. A més, en aquests casos, farem que $f_4 = 0$, ja que sempre es pot trobar una corba equivalent amb $f_4 = 0$.

Podem observar que, amb aquest mètode d'una desreducció, trobarem els trisecats que tinguin $u_{11} = u_{31}$, i per tant hem de diferenciar 2 casos, segons si són iguals o no aquests coeficients. A més, en el cas que siguin iguals, no poden ser 0.

4.1 Cas $u_{11} = u_{31}$

La primera component de la desreducció ha de ser un polinomi mònic, per tant dividim tot per k_2^2, i després igualem terme a terme amb l'expressió de $3D_1$. De moment, passem multiplicant a l'altre costat de l'equació el k_2^2. En aquest cas, del terme de grau 5 obtenim que:

$$u_{11} = u_{31}.$$

Per tant, substituïm directament a les altres equacions, i el sistema que queda és el següent:

$$\begin{aligned}k_2^2(u_{31}^2 + u_{10}) &= k_2^2u_{30} + k_1^2 + k_2h_2 \\ k_2^2u_{31}^3 &= k_1^2u_{31} + 1 \\ k_2^2(u_{10}^2 + u_{31}^2u_{10}) &= k_1^2u_{30} + k_0^2 + h_0k_2 + u_{31} \\ k_2^2u_{31}u_{10}^2 &= u_{31}k_0^2 + h_0k_1 + u_{31}^2 + f_3 + u_{30} \\ k_2^2u_{10}^3 &= k_0^2u_{30} + h_0k_0 + f_2 + u_{31}f_3 + u_{31}^3 + v_{31}^2\end{aligned}$$

Tot seguit, passarem dividint el k_2^2 de les 4 últimes equacions, i farem els següents canvis de variables:

$$z = \frac{k_1}{k_2}, \quad t = \frac{1}{k_2}, \quad w = \frac{k_0}{k_2}.$$

Així, la segona equació podem aïllar z^2 i substituir a les altres. També substituïm el valor de u_{10} que podem aïllar de la primera equació:

$$u_{10} = u_{30} + \frac{t^2}{u_{31}}.$$

Aquesta equació ens servirà després per trobar els valors de u_{10}. Podem observar aquí, que la u_{31} no pot ser 0, ja que no podem dividir per 0.

Només ens faran falta 2 de les altres 3 equacions. Ens quedem la tercera i la cinquena, quedant-nos així 2 equacions amb 2 incògnites, w i t.

$$\begin{aligned} 0 &= u_{31}^2 f_4 t^2 + u_{31}^2 u_{30}^2 + u_{31}^2 h_0 t + u_{31} u_{30} t^2 + t^4 + u_{31}^2 w^2 \\ 0 &= u_{31}^6 t^2 + u_{31}^5 f_4 t^2 + u_{31}^3 v_{31}^2 t^2 + u_{31}^3 u_{30} f_4 t^2 + u_{31}^4 f_3 t^2 + u_{31}^3 u_{30}^3 + u_{31}^2 u_{30}^2 t^2 \\ &\quad + u_{31}^3 f_2 t^2 + u_{31} u_{30} t^4 + t^6 + u_{31}^3 h_0 t w + u_{31}^3 u_{30} w^2. \end{aligned}$$

Finalment, fem la resultant entre aquestes dos equacions eliminant w, de manera que ens quedarà una equació amb nomes t d'incògnita, on tots els altres valors seran coneguts. Un cop factoritzada, la resultant queda de la següent forma:

$$\begin{aligned} 0 &= t^9 + (u_{31}^4 h_0^2) t^3 + (u_{31}^5 u_{30} h_0^2 + u_{31}^{10} f_4^2 + u_{31}^6 v_{31}^4 + u_{31}^8 f_3^2 + u_{31}^6 f_4 h_0^2 + u_{31}^6 f_2^2 \\ &\quad + u_{31}^{12}) t + u_{31}^6 h_0^3. \end{aligned}$$

Trobant les arrels d'aquesta equació, tenim els valors de t que podrem substituir a l'expressió trobada abans, per obtenir directament tots els valors de u_{10} dels trisecats.

D'aquesta forma doncs, trobem els u_{10} per als trisecats tals que $u_{11} = u_{31}$, aconseguint així la primera component del divisor trisecat. Com es pot veure pel grau de l'equació en t, podem trobar fins a 9 trisecats. Sol quedaria trobar la segona component mitjançant interpolació. En la secció 2.4 s'explica l'algorisme implementat que utilitzem per a trobar la segona component d'un divisor donada la primera.

4.2 Cas $u_{11} \neq u_{31}$

Per a poder trobar els trisecats tals que $u_{11} \neq u_{31}$, necessitarem tornar a aplicar la fórmula de la desreducció, és a dir, desreduir 2 cops. Per a simplificar la resolució del sistema, hem agafat $h_0 = 1$, per tant només ens servirà amb corbes que tinguin aquest valor.

Farem la desreducció en 2 passos, primer passarem de grau 2 a grau 4 la primera component del divisor, i després fins a grau 6.

Amb la primera desreducció de D_3 obtenim:

$$\begin{aligned} \overline{D}_3 = (\overline{u}_3, \overline{v}_3) = \; & \left(\frac{(v_3 + h + \overline{k} u_3)^2 + (v_3 + h + \overline{k} u_3) h + f}{u_3}, v_3 + h + \overline{k} u_3\right) \\ & \left(\frac{v_3^2 + v_3 h + f}{u_3} + \overline{k}^2 u_3 + \overline{k} h, v_3 + h + \overline{k} u_3\right), \end{aligned}$$

on $\overline{k} = k_1 x + k_0$ amb $k_1 \neq 0$. Abans de fer la segona desreducció, la primera component de $\overline{D}_3$ ha de ser mònica, per tant:

$$\overline{D}_3 = (\frac{v_3^2 + v_3 h + f}{k_1^2 u_3} + \frac{\overline{k}^2 u_3 + \overline{k} h}{k_1^2}, v_3 + h + \overline{k} u_3).$$

La desreducció de $\overline{D}_3$ ens dóna:

$$\begin{aligned} \overline{\overline{D}} = (\overline{\overline{u}}_3, \overline{\overline{v}}_3) = & \ (\frac{\overline{v}_3^2 + \overline{v}_3 h + f}{\overline{u}_3} + \overline{\overline{k}}^2 \overline{u}_3 + \overline{\overline{k}} h, \overline{v}_3 + h + \overline{\overline{k}} \overline{u}_3) \\ & = (k_1^2 u_3 + \overline{\overline{k}}^2 \overline{u}_3 + \overline{\overline{k}} h, v_3 + \overline{k} u_3 + \overline{\overline{k}} \overline{u}_3), \end{aligned}$$

on $\overline{\overline{k}} = k_3 x + k_2$ amb $k_3 \neq 0$. Igualant la primera component de $\overline{\overline{D}}_3$, la qual ha de ser mònica, amb la primera component de $3D_1$, és a dir:

$$(x^2 + u_{11} x + u_{10})^3 = \frac{k_1^2 u_3 + \overline{\overline{k}}^2 \overline{u}_3 + \overline{\overline{k}} h}{k_3^2}.$$

Fent els següents canvis de variables:

$$t_3 = \frac{1}{k_3}, \quad t_1 = \frac{1}{k_1}, \quad A = k_0^2, \quad B = t_3 k_2$$

Aconseguim el següent sistema d'equacions:

$$\begin{aligned}
u_{11} &= u_{31} + t_1^2 \\
u_{10} &= k_0^2 t_1^2 + t_1^4 + B^2 + u_{31} t_1^2 + u_{31}^2 + u_{30} \\
0 &= t_1^6 + u_{31} t_1^4 + B^2 t_1^2 + A u_{31} t_1^2 + B^2 u_{31} + u_{31}^3 + u_{30} t_1^2 + f_3 t_1^2 + t_1 \\
0 &= A t_1^8 + u_{31} t_1^8 + A^2 t_1^6 + B^2 t_1^6 + u_{31}^2 t_1^6 + A B^2 t_1^4 + B^2 u_{31} t_1^4 + A u_{31}^2 t_1^4 \\
&\quad + u_{30} t_1^6 + B^4 t_1^2 + B^2 u_{31}^2 t_1^2 + v_{31}^2 t_1^4 + A u_{30} t_1^4 + u_{31} f_3 t_1^4 + B^2 u_{30} t_1^2 \\
&\quad + u_{31}^2 u_{30} t_1^2 + k_0 t_1^4 + f_2 t_1^4 + u_{30}^2 t_1^2 + t_3^2 \\
0 &= t_1^{12} + u_{31} t_1^{10} + A^2 t_1^8 + u_{31}^2 t_1^8 + A^2 u_{31} t_1^6 + u_{31}^3 t_1^6 + B^4 t_1^4 + A B^2 u_{31} t_1^4 \\
&\quad + B^2 u_{31}^2 t_1^4 + u_{31}^4 t_1^4 + B^4 u_{31} t_1^2 + u_{31}^5 t_1^2 + B^2 u_{30} t_1^4 + B^2 f_3 t_1^4 + u_{30}^2 t_1^4 \\
&\quad + u_{31} u_{30}^2 t_1^2 + B^2 t_1^3 + t_1^2 t_3 + u_{31} t_3^2 \\
0 &= t_1^{14} + A t_1^{12} + u_{31} t_1^{12} + A^2 t_1^{10} + B^2 t_1^{10} + A^3 t_1^8 + A^2 u_{31} t_1^8 + A u_{31}^2 t_1^8 \\
&\quad + u_{31}^3 t_1^8 + u_{30} t_1^{10} + A^2 B^2 t_1^6 + B^4 t_1^6 + A^2 u_{31}^2 t_1^6 + B^2 u_{31}^2 t_1^6 + A B^4 t_1^4 \\
&\quad + B^4 u_{31} t_1^4 + B^2 u_{31}^3 t_1^4 + A u_{31}^4 t_1^4 + u_{31}^5 t_1^4 + A^2 u_{30} t_1^6 + u_{31}^2 u_{30} t_1^6 + B^6 t_1^2 \\
&\quad + B^4 u_{31}^2 t_1^2 + B^2 u_{31}^4 t_1^2 + u_{31}^6 t_1^2 + B^2 v_{31}^2 t_1^4 + A B^2 u_{30} t_1^4 + B^2 u_{31} f_3 t_1^4 + u_{30}^2 t_1^6 \\
&\quad + B^4 u_{30} t_1^2 + u_{31}^4 u_{30} t_1^2 + B^2 k_0 t_1^4 + A u_{30}^2 t_1^4 + u_{31} u_{30}^2 t_1^4 + B^2 f_2 t_1^4 + B^2 u_{30}^2 t_1^2 \\
&\quad + u_{31}^2 u_{30}^2 t_1^2 + u_{30}^3 t_1^2 + B t_1^2 t_3 + u_{30} t_3^2
\end{aligned}$$

De la tercera equació aïllem el valor de A, després el substituïm a la quarta, i podem aïllar k_0:

$$A = \frac{t_1^6 + u_{31}t_1^4 + B^2t_1^2 + B^2u_{31} + u_{31}^3 + u_{30}t_1^2 + f_3t_1^2 + t_1}{u_{31}t_1^2}$$

$$\begin{aligned} k_0 &= (t_1^{14} + u_{31}t_1^{12} + B^4t_1^6 + B^2u_{31}^2t_1^6 + u_{31}^4t_1^6 + u_{31}f_3t_1^8 + B^4u_{31}t_1^4 + B^4u_{31}^2t_1^2 \\ &+B^2u_{31}^4t_1^2 + u_{31}^2v_{31}^2t_1^4 + u_{31}^3u_{30}t_1^4 + B^2u_{31}f_3t_1^4 + u_{30}^2t_1^6 + f_3^2t_1^6 + u_{31}t_1^7 \\ &+u_{31}u_{30}^2t_1^4 + u_{31}u_{30}f_3t_1^4 + u_{31}^2f_2t_1^4 + u_{31}^2u_{30}^2t_1^2 + B^2u_{31}t_1^3 + u_{31}^3t_1^3 + u_{31}u_{30}t_1^3 \\ &+t_1^4 + u_{31}^2t_3^2) \cdot \frac{1}{u_{31}^2t_1^4} \end{aligned}$$

Ara, podem agafar el valor de k_0, elevar-lo al quadrat, i substituir-lo per les A de la tercera equació. Agafarem també les dos últimes i hi substituïm els valors de A i k_0 trobats respectivament, i fent combinacions entre elles, podem aïllar per separat els valors de t_3 i t_3^2. El valor de t_3 és el següent:

$$\begin{aligned} t_3 &= (t_1^{18} + u_{31}^2t_1^{14} + f_3t_1^{14} + B^4t_1^{10} + B^2u_{31}^2t_1^{10} + u_{31}^4t_1^{10} + t_1^{13} + u_{31}^6t_1^6 + u_{30}^2t_1^{10} \\ &+f_3^2t_1^{10} + B^4f_3t_1^6 + B^2u_{31}^2f_3t_1^6 + u_{31}^4f_3t_1^6 + B^4u_{31}^4t_1^2 + B^2u_{31}^6t_1^2 + u_{31}^2f_3^2t_1^6 \\ &+B^4u_{31}^2f_3t_1^2 + B^2u_{31}^4f_3t_1^2 + B^4t_1^5 + B^2u_{31}^2t_1^5 + u_{31}^4t_1^5 + u_{30}^2f_3t_1^6 + f_3^3t_1^6 \\ &+u_{31}^4u_{30}^2t_1^2 + t_1^8 + B^4u_{31}^2t_1 + B^2u_{31}^4t_1 + u_{31}^2u_{30}^2f_3t_1^2 + u_{30}^2t_1^5 + f_3^2t_1^5 + u_{31}^2t_1^4 \\ &+u_{31}^2u_{30}^2t_1 + f_3t_1^4 + t_1^3) \cdot \frac{1}{B^2u_{31}^2 + Bu_{31}^3 + u_{31}^2u_{30}} \end{aligned}$$

Ara podem expressar el valor de t_3^4 que ens apareixerà a la tercera equació com a $(t_3^2)^2$, i substituir a qualsevol de les altres 2 el valor de t_3. Un cop fet això, i factoritzat, tindrem 2 equacions amb només B i t_1 com a incògnites:

Finalment, fem la resultant entre les 2 equacions, eliminant B i quedant-nos només t_1. D'entrada ens queda de grau molt alt, així que l'hem simplificat de la següent manera.

Traiem el factor $u_{31}^{12}t_1^9$ de la resultant, llavors fem el màxim comú divisor de la resultant amb la seva derivada respecte t_1, i d'aquesta manera trobem un altre factor de la resultant, que podem treure també. Així, ens queda una equació amb grau 81 de t_1, que és el número màxim de trisecats que podem tenir.

D'aquesta manera, donat un divisor, trobem les solucions de t_1, llavors amb aquestes, mirem quines són bones, mirant que donin la mateixa solució per a B les 2 equacions de les quals ha sortit la resultant. Amb els valors de B i t_1, podem calcular k_0, i així ja tindrem tot el necessari per a calcular u_{11} i u_{10}. Com en el cas anterior, la segona component del divisor la calcularem amb el nostre propi algorisme.

Les 2 equacions a partir de les quals aconseguim la resultant final són les següents:

$$
\begin{aligned}
0 \;&= t_1^{33} + B^4 t_1^{25} + B^2 u_{31}^2 t_1^{25} + u_{31}^4 t_1^{25} + u_{30}^2 t_1^{25} + f_3^2 t_1^{25} + B^8 t_1^{17} + B^2 u_{31}^6 t_1^{17} \\
&+ u_{31}^8 t_1^{17} + u_{31}^4 u_{30}^2 t_1^{17} + t_1^{23} + B^{12} t_1^9 + B^{10} u_{31}^2 t_1^9 + B^8 u_{31}^4 t_1^9 + B^6 u_{31}^6 t_1^9 \\
&+ B^4 u_{31}^8 t_1^9 + B^2 u_{31}^{10} t_1^9 + u_{31}^{12} t_1^9 + u_{30}^4 t_1^{17} + f_3^4 t_1^{17} + B^8 u_{30}^2 t_1^9 + B^4 u_{31}^4 u_{30}^2 t_1^9 \\
&+ u_{31}^8 u_{30}^2 t_1^9 + B^8 f_3^2 t_1^9 + B^2 u_{31}^6 f_3^2 t_1^9 + u_{31}^8 f_3^2 t_1^9 + B^6 u_{31}^{10} t_1 + B^4 u_{31}^{12} t_1 \\
&+ B^4 u_{30}^4 t_1^9 + B^2 u_{31}^2 u_{30}^4 t_1^9 + u_{31}^4 u_{30}^2 f_3^2 t_1^9 + B^4 f_3^4 t_1^9 + B^2 u_{31}^2 f_3^4 t_1^9 + u_{31}^4 f_3^4 t_1^9 \\
&+ B^4 u_{31}^6 v_{31}^4 t_1 + B^2 u_{31}^8 v_{31}^4 t_1 + B^2 u_{31}^{10} u_{30}^2 t_1 + B^6 u_{31}^6 f_3^2 t_1 + B^4 u_{31}^8 f_3^2 t_1 \\
&+ B^8 t_1^7 + B^2 u_{31}^6 t_1^7 + u_{31}^8 t_1^7 + u_{30}^6 t_1^9 + u_{30}^4 f_3^2 t_1^9 + u_{30}^2 f_3^4 t_1^9 + f_3^6 t_1^9 + B^4 u_{31}^5 t_1^5 \\
&+ B^2 u_{31}^7 t_1^5 + u_{31}^6 v_{31}^4 u_{30}^2 t_1 + B^2 u_{31}^6 u_{30}^2 f_3^2 t_1 + B^4 u_{31}^6 f_2^2 t_1 + B^2 u_{31}^8 f_2^2 t_1 \\
&+ B^4 u_{31}^6 t_1^3 + B^2 u_{31}^8 t_1^3 + u_{31}^4 u_{30}^2 t_1^7 + t_1^{13} + B^6 u_{31}^5 t_1 + B^4 u_{31}^7 t_1 + u_{31}^5 u_{30}^2 t_1^5 \\
&+ B^4 u_{31}^5 u_{30} t_1 + B^2 u_{31}^7 u_{30} t_1 + B^4 u_{31}^5 f_3 t_1 + B^2 u_{31}^7 f_3 t_1 + u_{31}^6 u_{30}^2 f_2^2 t_1 \\
&+ u_{31}^6 u_{30}^2 t_1^3 + u_{30}^4 t_1^7 + f_3^4 t_1^7 + B^2 u_{31}^5 u_{30}^2 t_1 + B^4 u_{31}^5 + B^2 u_{31}^7 + u_{31}^5 u_{30}^3 t_1 \\
&+ u_{31}^5 u_{30}^2 f_3 t_1 + B^4 t_1^5 + B^2 u_{31}^2 t_1^5 + u_{31}^4 t_1^5 + u_{31}^5 u_{30}^2 + u_{30}^2 t_1^5 + f_3^2 t_1^5 + t_1^3
\end{aligned}
$$

$$
\begin{aligned}
0 \;&= t_1^{15} + B^2 t_1^{11} + B u_{31} t_1^{11} + u_{31}^2 t_1^{11} + B^2 u_{31} t_1^9 + B u_{31}^2 t_1^9 + u_{30} t_1^{11} + f_3 t_1^{11} \\
&+ u_{31}^4 t_1^7 + u_{31} u_{30} t_1^9 + t_1^{10} + B^2 u_{31}^4 t_1^3 + B u_{31}^5 t_1^3 + u_{31}^6 t_1^3 + f_3^2 t_1^7 + B^2 u_{31}^5 t_1 \\
&+ B u_{31}^6 t_1 + u_{31}^4 u_{30} t_1^3 + u_{31}^4 f_3 t_1^3 + u_{31}^5 u_{30} t_1 + B^2 f_3^2 t_1^3 + B u_{31} f_3^2 t_1^3 + u_{31}^2 f_3^2 t_1^3 \\
&+ B^2 u_{31} f_3^2 t_1 + B u_{31}^2 f_3^2 t_1 + u_{31}^4 t_1^2 + u_{30} f_3^2 t_1^3 + f_3^3 t_1^3 + u_{31} u_{30} f_3^2 t_1 + t_1^5 + f_3^2 t_1^2 \\
&+ B^2 t_1 + B u_{31} t_1 + u_{31}^2 t_1 + u_{30} t_1 + f_3 t_1 + 1
\end{aligned}
$$

Capítol 5

Subgrup de 3-Sylow

En anteriors treballs s'ha estudiat la 2-torsió en corbes hiperel·líptiques [9], els subgrups de Sylow en corbes el·líptiques [10] o la 3^n-torsió sobre corbes el·líptiques [11]. Nosaltres en aquest treball explicarem com trobar la 3^n-torsió i el 3-Sylow sobre corbes hiperel·líptiques.

Un cop tenim els mètodes per trobar els divisors d'ordre 3 d'una corba i els seus trisecats, podem passar a definir els subgrups de 3-torsió i de 3-Sylow.

5.1 Subgrups de 3-torsió i de 3-Sylow d'una corba hiperel·líptica

Donades una corba C definida sobre un cos $\mathbb{F}_{2^m}$ i la seva Jacobiana $Jac_C(\mathbb{F}_{2^m})$, definim el subgrup de *3-torsió* $Jac_C(\mathbb{F}_{2^m})[3]$ com el conjunt de divisors d'ordre 3 més el divisor de zero. És a dir:

$$Jac_C(\mathbb{F}_{2^m})[3] = \{D \in Jac_C(\mathbb{F}_{2^m}) : 3D = 0\}.$$

De manera similar, per a tot natural $k > 1$ podem definir el subgrup de *3^k-torsió* $Jac_C(\mathbb{F}_{2^m})[3^k]$ com:

$$Jac_C(\mathbb{F}_{2^m})[3^k] = \{D \in Jac_C(\mathbb{F}_{2^m}) : 3^k D = 0\}$$

Aquests conjunts tenen estructura de grup, i cal notar que

$$Jac_C(\mathbb{F}_{2^m})[3^k] \subseteq Jac_C(\mathbb{F}_{2^m})[3^{k+1}].$$

A partir d'un cert valor de k, trobarem $Jac_C(\mathbb{F}_{2^m})[3^k] = Jac_C(\mathbb{F}_{2^m})[3^{k+1}]$. Això voldrà dir, que tindrem divisors de com a molt ordre 3^k, i podem definir

el subgrup *3-Sylow* d'una corba com:

$$S_3(Jac_C(\mathbb{F}_{2^m})) = Jac_C(\mathbb{F}_{2^m})[3^k].$$

Aquest serà un subgrup format per tots els divisors amb ordre 3^n de la corba, on $0 \leq n \leq k$.

Aquest subgrup és isomorf a:

$$S_3(Jac_C(\mathbb{F}_{2^m})) \cong \mathbb{Z}_{3^{n_1}} \times \mathbb{Z}_{3^{n_2}} \times \mathbb{Z}_{3^{n_3}} \times \mathbb{Z}_{3^{n_4}},$$

on $n_1 \geq n_2 \geq n_3 \geq n_4 \geq 0$. El número de n_i diferents de 0 s'anomena el 3-rang de la corba, sent 4 el màxim. Coneixent aquests valors, podem dir que el cardinal de la Jacobiana satisfà que:

$$\#Jac_C(\mathbb{F}_{2^m}) = 3^{n_1+n_2+n_3+n_4} \cdot t, \quad 3 \nmid t.$$

Així doncs, tenim un mètode per a poder trobar el major factor de 3 del cardinal de la Jacobiana, obtenint-ne així una informació parcial.

5.2 Determinació del subgrup de 3-Sylow

Per a trobar el subgrup de 3-Sylow volem una funció que, donada una corba, ens retorni els valors dels diferents n_i, així com un número de divisors generadors igual al 3-rang de la corba, on cada divisor serà d'ordre 3^{n_i}.

El primer pas serà calcular els divisors d'ordre 3 de la Jacobiana, la qual cosa podem fer tal com està explicat al capítol 3. Tot seguit, ens quedarem només amb divisors independents seguint el mètode de la secció 3.4. El número de divisors que ens quedin serà el 3-rang de la corba.

Podem representar el subgrup de 3-Sylow amb tants arbres com divisors independents d'ordre 3 té la corba, on aquests en són l'arrel (veure figura 5.1). Al primer nivell, només hi haurà les arrels, que són divisors d'ordre 3. Al segon nivell, trobarem els trisecats de cada una, que són d'ordre 3^2. Així, podem anar baixant per cada arbre fent trisecats, fins arribar al nivell màxim k que tindrà divisors d'ordre 3^k. El nivell al que arribi cada un dels arbres determinarà els valors dels diferents n_i.

Haurem d'anar baixant per aquests arbres per a arribar al nivell màxim. En alguns casos, quan el 3-rang és més gran que 1, com que només provem de baixar per 1 dels trisecats cada cop, pot ser que aquell no baixi més, però sí alguna altre branca de l'arbre. Per tant, diferenciarem segons el cas.

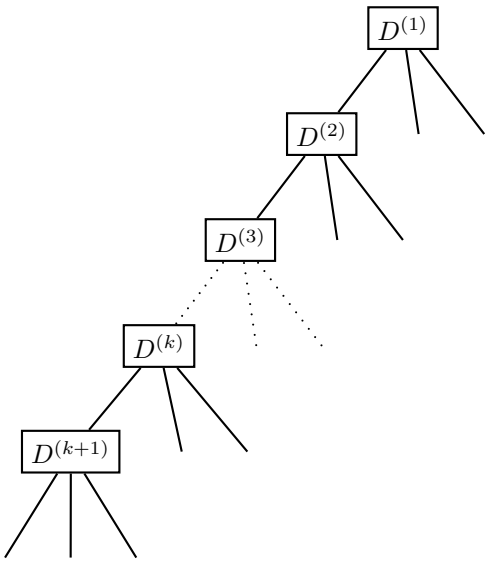

Figura 5.1: Representació del Sylow en forma d'arbre

5.2.1 Cas 3-Rang 1 (cas cíclic)

En el cas que només hi hagi 1 divisor independent, voldrà dir que el subgrup del 3-Sylow serà isomorf a $\mathbb{Z}_{3^n}$, on n serà l'exponent més gran tal que existeixin divisors d'ordre 3^n. Aquest és el cas més fàcil, ja que no ens cal canviar de branca.

L'únic que hem de fer en aquest cas és agafar un dels divisors d'ordre 3, i buscar si té trisecats. Si en trobem, buscarem un trisecat del trisecat, fins que no en trobem cap. Llavors haurem acabat, i retornaríem l'enter n i un divisor d'ordre 3^n.

5.2.2 Casos 3-Rangs 2, 3 i 4

En els casos en que tinguem més d'un divisor independent, haurem de començar seguint el mateix sistema explicat en el cas anterior. Per cadascun dels divisors independents, anirem trisecant i baixant per l'arbre fins a no poder més. Arribats a aquest punt, tindrem per cada arbre el nivell al que hem arribat, segons el nombre de vegades que hem pogut trisecar.

Si els ordenem, el nivell n_1 més petit que haguem trobat, ja serà correcte. Però els altres, podria ser que per aquesta branca no hi hagi més trisecats, però sí en alguna altra. Per a poder saltar per les diferents branques, haurem

d'anar fent combinacions de sumes i restes amb els divisors que ja sabem que són bons, per obtenir nous divisors, i intentar trisecar a partir d'ells.

Primer fem sumes i restes del divisor de nivell n_1 amb tots els altres i busquem trisecats a partir d'ells. Ara els dos nivells més petits ja seran correctes. En el cas que hi hagi més divisors independents, continuarem amb el mateix sistema, sumant i restant totes les possibles combinacions amb els divisors correctes ja trobats.

Finalment, obtindrem tots els nivells n_i dels arbres que ens permetran trobar el subgrup de 3-Sylow de la corba.

Capítol 6

Implementació

En aquest capítol descriurem breument el software utilitzat i donarem la definició de les funcions que hem programat. Explicarem solament les funcions principals, les quals n'utilitzen d'altres auxiliars.

6.1 Software i hardware utilitzats

Per a la primera part del treball, que ha consistit en resoldre els sistemes d'equacions, fent derivades, resultants etc, s'ha utilitat Sage versió 4.6.2 [12]. Però vam veure que no funcionava gaire bé amb corbes hiperel·líptiques, ja que tenia molt poques funcions per a treballar-hi.

Per tant, per a la implementació de les funcions i totes les proves, s'ha utilitzat Magma versió 2.10-8 [2], excepte en alguns casos que ha estat necessari utilitzar la versió online de Magma [3]. La implementació ha estat realitzada sobre el sistema operatiu Linux Ubuntu 64 bits 10.04 *Lucid Lynx*.

Respecte al hardware, disposava d'un processador Intel core i5 de doble nucli a 3.33 GHz i 8 Gb de memòria RAM.

6.2 Funcions implementades

A continuació donarem la capçalera de les funcions que hem implementat, explicant cadascun dels paràmetres d'entrada de la funció, quins requisits han de complir, i què ens retornarà la funció.

- **SegonaComponentDivisor(f4,f3,f2,f1,f0,h2,h1,h0,u1,u0,m : pes := 2)**

  En aquesta funció i en totes les altres, els diferents paràmetres f_i i h_i fan referencia als coeficients de la corba hiperel·líptica corresponents, i els u_i i v_i als coeficients del divisor. El paràmetre m és l'extensió del cos, és a dir, voldrà dir que estem treballant en un cos de $\mathbb{F}_{2^m}$.

  Els paràmetres que apareixen després dels dos punts, són opcionals, i si no són definits al cridar la funció, prenen per defecte el valor indicat. En aquest cas, *pes* representa el pes del divisor, que normalment serà 2.

  Donada una corba definida pels paràmetres f_i i h_i, i la primera component $u(x) = x^2 + u_1x + u_0$ d'un divisor D (o $u(x) = x + u_0$ en el cas de divisors de pes 1), ens retorna una llista de totes les segones components $v(x) = v_1x + v_0$ tals que $D = (u(x), v(x))$ és un divisor de la Jacobiana.

  Aquesta funció no té cap restricció en quant als paràmetres d'entrada i funciona amb qualsevol corba amb qualsevol $h(x)$. El pseudocodi de la funció l'hem explicat a 3.

- **Divisors3(f4,f3,f2,f1,f0,h2,h1,h0,m)**

  Donats els paràmetres d'una corba i l'extensió del cos, retorna una llista amb tots els divisors d'ordre 3 de la corba.

  Funciona amb qualsevol corba.

- **Trisecats(f4,f3,f2,f1,f0,h2,h1,h0,u31,u30,v31,v30,m :all:=true, pes := 2)**

  Donada una corba i un divisor de la Jacobiana, retorna tots els trisecats del divisor donat.

  El paràmetre opcional *all* es pot posar a *false* al cridar la funció per a que, un cop trobat un únic trisecat, ens el retorni, i la funció no continuï. Això ens serà útil a l'hora de fer el 3-Sylow, per a que sigui més eficient. El paràmetre *pes* fa referencia al pes del divisor entrat.

  Aquesta funció està implementada completament només per als casos en que $f_4 = 0, h_2 = 0, h_1 = 0$, i està pensada per trobar trisecats de pes 2.

  Per a corbes amb $f_4 \neq 0$ o $h_1 \neq 0$ només trobarà trisecats amb $u_{11} = u_{31}$. Pot trobar algun trisecat de pes 1, però no s'assegura.

- **Divisors3Independents(llista)**

  Donada una llista de divisors d'ordre 3, retorna una altra llista amb només divisors independents. Això ens permetrà saber el 3-rang de la corba, i seran els divisors que farem servir per al 3-Sylow.

- **Sylow3(f4,f3,f2,f1,f0,h0,m)**

  Donada una corba amb només h_0, retorna una llista on el nombre d'elements equivaldrà al seu 3-rang.

  Cada un dels elements, serà una llista de 2 posicions: en la primera, hi haurà un divisor que servirà de generador per al subgrup de 3-Sylow; en la segona, hi anirà un número natural n, que indicarà el nivell de l'arbre del 3-Sylow al que s'ha arribat, i que per tant indicarà que l'ordre del divisor és 3^n.

  Si sumem tots els n retornats, obtindrem l'exponent de la màxima potència de 3 que divideix al cardinal de la Jacobiana de la corba d'entrada.

Capítol 7

Resultats i conclusions

En aquest capítol mostrarem alguns exemples en els que hem utilitzat les nostres pròpies funcions, les quals fan servir les equacions i resultats anteriorment trobats. S'ha utilitzat l'entorn de programació de Magma, ja que s'ha trobat que és útil per treballar amb corbes hiperel·líptiques i disposa de vàries funcions per a treballar-hi i d'un bon manual online [2].

7.1 Trisecció de divisors

En aquesta secció mostrarem exemples de trisecats de divisors, ja sigui de divisors de potències de 3 o no.

7.1.1 Exemple 3-rang 2

Considerem la corba sobre el cos $\mathbb{F}_{2^3}$ definida per l'equació

$$C : y^2 + y = x^5 + x^3 + a^3x$$

on a és el generador del cos. La Jacobiana d'aquesta corba té cardinal $81 = 3^4$, i té 8 divisors d'ordre 3, el que significa que és de rang 2. Agafarem 2 d'aquests divisors d'ordre 3 i buscarem tots els seus trisecats.

Els divisors que agafarem són els següents, on l'exponent $^{(i)}$ indica l'exponent de 3 de l'ordre del divisor, per tant és d'ordre 3^i:

$$\begin{aligned} D_1^{(1)} &= (x^2 + a^5x, a^3x) \\ D_2^{(1)} &= (x^2 + a^5x + 1, a^6x + a^6) \end{aligned}$$

Amb els mètodes explicats en el capítol 4, podem trobar els trisecats $D_1^{(2)}$ per exemple de $D_1^{(1)}$, tals que $3D_1^{(2)} = D_1^{(1)}$, tant els que tenen $u_{11} = u_{31}$ com els que $u_{11} \neq u_{31}$. Els $D_1^{(2)}$ són:

$$(x^2 + a^5x + a^2, a^6)$$
$$(x^2 + a^5x + a^3, a^6x + a^3)$$
$$(x^2 + a^5x + 1, x + a^5)$$
$$(x + a^6, a^3)$$
$$(x^2 + x + a^6, a^5x + a^5)$$
$$(x^2 + x + 1, a^2x + a^3)$$
$$(x^2 + a^5, a^5x + a)2$$
$$(x^2 + a^2, x + a^5)$$

I els $D_2^{(2)}$ són:

$$(x^2 + a^5x + a^6, a^4x + a^3)$$
$$(x^2 + a^5x + a, a^3x)$$
$$(x^2 + a^5x, a^5x)$$
$$(x + a^5, a, 1)$$
$$(x^2 + x + a^5, 1)$$
$$(x^2 + x + a^3, a^3x + a^4)$$
$$(x^2 + a^3, a^6x + a^6)$$
$$(x, 1, 1)$$
$$(x^2, a^3x, 2)$$

7.1.2 Exemple 3-rang 0

En les corbes en que no hi ha divisors d'ordre 3, hi ha exactament 1 trisecat per cada divisor, que serà del mateix ordre. Anem-ho a veure amb el següent exemple.

Considerem la corba

$$y^2 + y = x^5 + a^{55}x^3 + a^{30}x^2 + a^{46}x + a^{27},$$

definida sobre $\mathbb{F}_{2^6}$. El cardinal de la Jacobiana és $= 17 \cdot 241 = 4097$. Agafem un divisor aleatori D_1:

$$D_1 = (x^2 + a^{34}x + a^{39}, a^{62}x + a^{19}).$$

L'ordre del divisor és de 4097. Amb les nostres funcions aconseguim trobar el seu trisecat D_1' tal que $3D_1' = D_1$. L'ordre de D_1' també és 4097.

$$D_1' = (x^2 + a^4x + a^{51}, a^5 2x + a^{23}).$$

Ho provem ara amb un altre divisor D_2, d'ordre 241, i trobem el seu trisecat D_2', amb el mateix ordre:

$$\begin{aligned} D_2 &= (x^2 + a^{14}x + a^{56}, a^{43}x + a^{47}), \\ D_2' &= (x^2 + a^{40}x + a^{19}, a^{18}x). \end{aligned}$$

7.2 Determinació de subgrups de 3-Sylow

Per a aquests exemples, agafarem una corba i trobarem els seus divisors d'ordre 3, per a després quedar-nos només amb els independents. Llavors buscarem el 3-Sylow de la manera explicada, fent trisecats.

7.2.1 Exemple 3-rang 4

En aquest altre exemple, treballarem sobre un cos més gran, $\mathbb{F}_{2^{18}}$. També farem servir a com a generador del cos. La corba que tenim és

$$C : y^2 + y = x^5 + a^{100432}x^3 + a^{243085}x^2 + a^{29702}x + a^{49028}$$

i tenim que $\#Jac_C(\mathbb{F}_{2^{18}}) = 3^{12} \cdot 19^4$.

Amb les nostres funcions, trobem que hi ha un total de 80 divisors d'ordre 3, així que aquesta corba té 3-rang de 4. Els 4 divisors d'ordre 3 independents que agafem són els següents:

$$\begin{aligned} &(x^2 + a^{233781}x + a^{31862}, a^{157859}x + a^{224369}) \\ &(x^2 + a^{233781}x + a^{115742}, a^{55607}x + a^{210062}) \\ &(x^2 + a^{164229}x + a^{236163}, a^{52380}x + a^{76855}) \\ &(x^2 + a^{164229}x + a^{37386}, a^{254128}x + a^{68267}) \end{aligned}$$

Per cadascun d'aquests, seguirem els mateixos processos, i anirem trisecant fins a aconseguir un generador de màxim nivell, de manera que si anem multiplicant per 3, arribem a l'arrel. En aquest cas, cada divisor té 81 trisecats, 9 amb $u_{11} = u_{31}$ i 72 amb $u_{11} \neq u_{31}$. Tot seguit, mostrem els generadors del subgrup de 3-Sylow:

$$\begin{aligned} &(x^2 + a^{233781}x + a^{208972}, a^{90357}x + a^{92266}) \\ &(x^2 + a^{233781}x + a^{70474}, a^{166951}x + a^{68661}) \\ &(x^2 + a^{164229}x + a^{1459}, a^{102311}x + a^{57483}) \\ &(x^2 + a^{164229}x + a^{76389}, a^{138336}x + a^{49670}) \end{aligned}$$

Tots aquests divisors són d'ordre $27 = 3^3$. Com podem veure, tenim que la suma dels nivells és 12, que és l'exponent màxim de la potència de 3 que divideix a l'ordre de la Jacobiana, que és 69257922561.

7.2.2 Exemple 3-rang 1

Per a poder trobar divisors d'odres més grans, augmentarem de cos també. Ara el nostre cos és $\mathbb{F}_{2^{27}}$, i seguim denotant amb a al seu generador. La corba C que tenim és:

$$y^2 + y = x^5 + f_3x^3 + f_2x^2 + f_1x + f_0$$

On:

$$\begin{aligned}
f_3 = {} & (a^{25} + a^{24} + a^{23} + a^{22} + a^{20} + a^{17} + a^{16} + a^{15} + a^{11} + a^{10} + a^9 + a^5 + \\
& a^4 + a^3 + a^2 + 1) \\
f_2 = {} & (a^{25} + a^{24} + a^{21} + a^{20} + a^{19} + a^{13} + a^{10} + a^9 + a^6 + a^3 + a^2 + a) \\
f_1 = {} & (a^{26} + a^{25} + a^{20} + a^{18} + a^{16} + a^{14} + a^{11} + a^{10} + a^8 + a^5 + a^4) \\
f_0 = {} & a^{25} + a^{24} + a^{23} + a^{20} + a^{19} + a^{18} + a^{16} + a^{15} + a^{14} + a^{10} + a^9 + a^5 + \\
& a^3 + 1
\end{aligned}$$

El cardinal de la Jacobiana és :

$$18016597801189377 = 3^4 \cdot 13 \cdot 19 \cdot 37 \cdot 87211 \cdot 279073.$$

Com que només té 2 divisors d'ordre 3, significa que només 1 és independent. Per tant, l'anirem trisecant fins a no poder més, ja que ens trobem en el cas cíclic 5.2.1. Com podem veure per la factorització del cardinal de la Jacobiana, esperem trobar divisors d'ordre $3^4 = 81$.

El divisor d'ordre 3 és de la forma $(x^2 + u_1x + u_o, v_1x + v_0)$ on:

$$\begin{aligned}
u_1 = {} & a^{25} + a^{24} + a^{22} + a^{20} + a^{19} + a^{13} + a^{12} + a^{11} + a^8 + a^7 + a^5 + a^3 + a \\
u_0 = {} & a^{25} + a^{24} + a^{23} + a^{22} + a^{18} + a^{16} + a^{14} + a^{11} + a^{10} + a^7 + a^6 + a^5 + \\
& a^4 + a^3 + a^2 + a + 1 \\
v_1 = {} & a^{26} + a^{23} + a^{22} + a^{19} + a^{17} + a^{16} + a^{15} + a^{12} + a^{11} + a^{10} + a^8 + a^3 + a \\
v_0 = {} & a^{24} + a^{23} + a^{22} + a^{20} + a^{19} + a^{18} + a^{14} + a^{12} + a^9 + a^7 + a^6 + a^3 + \\
& a^2 + a
\end{aligned}$$

I veiem que efectivament, arribem a trobar un divisor d'ordre 81 de la forma $(x^2 + u_1'x + u_o', v_1'x + v_0')$ on:

$$\begin{aligned}
u_1' = {} & a^{25} + a^{24} + a^{22} + a^{20} + a^{19} + a^{13} + a^{12} + a^{11} + a^8 + a^7 + a^5 + a^3 + a \\
u_0' = {} & a^{26} + a^{25} + a^{23} + a^{22} + a^{17} + a^{15} + a^{13} + a^{11} + a^9 + a^8 + a^7 + a^6 + \\
& a^5 + a^2 \\
v_1' = {} & a^{24} + a^{23} + a^{22} + a^{21} + a^{17} + a^{16} + a^{14} + a^{10} + a^7 + a^6 + a^5 + a^2 \\
v_0' = {} & a^{26} + a^{22} + a^{21} + a^{18} + a^{16} + a^{15} + a^{12} + a^9 + a^8 + a^7 + a^5 + a^4 + a^2
\end{aligned}$$

Així doncs, veiem es compleix l'explicat a 5.1, i que aquest mètode ens funciona per a trobar informació parcial del cardinal de la Jacobiana d'una corba.

7.2.3 Exemple sobre un cos gran

Per acabar, mostrarem un exemple sobre un cos mes gran, $\mathbb{F}_{2^{180}}$, en el qual és difícil calcular el cardinal de la Jacobiana, però ens és fàcil trobar el 3-Sylow, el qual ens en donarà informació en un temps molt menor. Per a donar una idea dels temps, per a calcular el cardinal de la Jacobiana d'una corba, hem utilitzat la versió online que ofereix el Magma [3], que utilitza la versió 2.18-8, ja que la versió de la que disposem nosaltres (2.10-8), no calcula gaire bé aquests cardinals i tarda molt més.

Amb un exemple d'una corba sobre un cos de $\mathbb{F}_{2^{150}}$, tarda aproximadament un minut i mig a trobar el seu cardinal. Si augmentem a un cos de $\mathbb{F}_{2^{180}}$, ens passem dels 2 minuts màxims de còmput que ens ofereix la versió online.

Considerem la corba $C : y^2+y = x^5+x^3+a^{28}x^2+a^{12}x+a^8$ definida sobre $\mathbb{F}_{2^{180}}$. Amb les nostres funcions podem arribar a trobar els divisors d'ordre 3, de manera que sabem que el seu 3-rang és 2. Busquem doncs el 3-Sylow, i en trobem els 2 generadors D_1 i D_2.

El divisor té la forma $D_1 = (x^2 + u_{11}x + u_{10}, v_{11}x + v_{10})$, on:

$$\begin{aligned} u_{11} = \; & a^{174} + a^{171} + a^{168} + a^{162} + a^{153} + a^{150} + a^{141} + a^{135} + a^{132} + a^{129} + \\ & a^{123} + a^{117} + a^{114} + a^{111} + a^{108} + a^{105} + a^{93} + a^{90} + a^{66} + a^{63} + a^{57} + \\ & a^{48} + a^{45} + a^{42} + a^{39} + a^{30} + a^{27} + a^{18} + a^{15} + a^{12} + a^3 + 1 \end{aligned}$$

$$\begin{aligned} u_{10} = \; & a^{178} + a^{175} + a^{174} + a^{172} + a^{171} + a^{170} + a^{166} + a^{164} + a^{161} + a^{157} + \\ & a^{155} + a^{153} + a^{151} + a^{146} + a^{144} + a^{140} + a^{138} + a^{137} + a^{135} + a^{134} + \\ & a^{133} + a^{130} + a^{129} + a^{127} + a^{125} + a^{124} + a^{123} + a^{118} + a^{114} + a^{111} + \\ & a^{110} + a^{109} + a^{106} + a^{105} + a^{104} + a^{103} + a^{101} + a^{100} + a^{99} + a^{96} + \\ & a^{94} + a^{93} + a^{91} + a^{84} + a^{80} + a^{77} + a^{76} + a^{72} + a^{70} + a^{69} + a^{68} + \\ & a^{67} + a^{66} + a^{65} + a^{62} + a^{58} + a^{57} + a^{56} + a^{55} + a^{53} + a^{50} + a^{47} + \\ & a^{46} + a^{39} + a^{35} + a^{31} + a^{28} + a^{26} + a^{22} + a^{21} + a^{20} + a^{18} + a^{17} + \\ & a^{14} + a^{12} + a^{11} + a^{10} + a^9 + a^8 + a + 1 \end{aligned}$$

$$\begin{aligned} v_{11} = \; & a^{176} + a^{175} + a^{172} + a^{171} + a^{168} + a^{167} + a^{166} + a^{165} + a^{164} + a^{163} + \\ & a^{160} + a^{157} + a^{156} + a^{154} + a^{148} + a^{146} + a^{144} + a^{143} + a^{141} + a^{139} + \\ & a^{138} + a^{137} + a^{134} + a^{132} + a^{131} + a^{129} + a^{128} + a^{127} + a^{126} + a^{123} + \\ & a^{121} + a^{120} + a^{119} + a^{118} + a^{114} + a^{113} + a^{112} + a^{111} + a^{110} + a^{108} + \\ & a^{102} + a^{101} + a^{99} + a^{98} + a^{92} + a^{88} + a^{87} + a^{85} + a^{82} + a^{81} + a^{78} + \\ & a^{71} + a^{67} + a^{66} + a^{64} + a^{63} + a^{62} + a^{60} + a^{57} + a^{55} + a^{54} + a^{51} + \\ & a^{50} + a^{45} + a^{42} + a^{40} + a^{38} + a^{37} + a^{35} + a^{30} + a^{27} + a^{26} + a^{24} + \\ & a^{23} + a^{19} + a^{18} + a^{15} + a^{13} + a^{12} + a^8 + a^5 + a^2 \end{aligned}$$

$$\begin{aligned} v_{10} = \; & a^{179} + a^{178} + a^{176} + a^{174} + a^{172} + a^{167} + a^{162} + a^{160} + a^{159} + a^{157} + \\ & a^{155} + a^{151} + a^{150} + a^{149} + a^{148} + a^{147} + a^{144} + a^{143} + a^{142} + a^{141} + \\ & a^{137} + a^{136} + a^{134} + a^{133} + a^{132} + a^{130} + a^{127} + a^{126} + a^{125} + a^{124} + \\ & a^{120} + a^{117} + a^{114} + a^{113} + a^{112} + a^{111} + a^{110} + a^{107} + a^{105} + a^{103} + \\ & a^{102} + a^{100} + a^{98} + a^{97} + a^{96} + a^{95} + a^{91} + a^{90} + a^{88} + a^{84} + a^{83} + \\ & a^{82} + a^{81} + a^{78} + a^{76} + a^{75} + a^{74} + a^{72} + a^{68} + a^{67} + a^{65} + a^{64} + \\ & a^{62} + a^{58} + a^{54} + a^{53} + a^{52} + a^{51} + a^{50} + a^{48} + a^{45} + a^{44} + a^{43} + \\ & a^{42} + a^{40} + a^{37} + a^{36} + a^{35} + a^{33} + a^{32} + a^{30} + a^{28} + a^{22} + a^{20} + \\ & a^{18} + a^{16} + a^{11} + a^{10} + a^9 + a^8 + a^7 + a^5 + a^4 + a^2 \end{aligned}$$

I de manera similar tenim $D_2 = (x^2 + u_{21}x + u_{20}, v_{21}x + v_{20})$ on:

$$\begin{aligned} u_{21} = \; & a^{174} + a^{171} + a^{168} + a^{162} + a^{153} + a^{150} + a^{141} + a^{135} + a^{132} + a^{129} + \\ & a^{123} + a^{117} + a^{114} + a^{111} + a^{108} + a^{105} + a^{93} + a^{90} + a^{66} + a^{63} + \\ & a^{57} + a^{48} + a^{45} + a^{42} + a^{39} + a^{30} + a^{27} + a^{18} + a^{15} + a^{12} + a^3 + 1 \end{aligned}$$

$$\begin{aligned} u_{20} = \; & a^{178} + a^{175} + a^{172} + a^{170} + a^{168} + a^{166} + a^{164} + a^{162} + a^{161} + a^{157} + \\ & a^{155} + a^{151} + a^{150} + a^{146} + a^{144} + a^{141} + a^{140} + a^{138} + a^{137} + a^{134} + \\ & a^{133} + a^{132} + a^{130} + a^{127} + a^{125} + a^{124} + a^{118} + a^{117} + a^{110} + a^{109} + \\ & a^{108} + a^{106} + a^{104} + a^{103} + a^{101} + a^{100} + a^{99} + a^{96} + a^{94} + a^{91} + \\ & a^{90} + a^{84} + a^{80} + a^{77} + a^{76} + a^{72} + a^{70} + a^{69} + a^{68} + a^{67} + a^{65} + \\ & a^{63} + a^{62} + a^{58} + a^{56} + a^{55} + a^{53} + a^{50} + a^{48} + a^{47} + a^{46} + a^{45} + \\ & a^{42} + a^{35} + a^{31} + a^{30} + a^{28} + a^{27} + a^{26} + a^{22} + a^{21} + a^{20} + a^{17} + a^{15} + \\ & a^{14} + a^{11} + a^{10} + a^9 + a^8 + a^3 + a + 1 \end{aligned}$$

$$\begin{aligned} v_{21} = \; & a^{176} + a^{175} + a^{174} + a^{172} + a^{167} + a^{166} + a^{165} + a^{164} + a^{163} + a^{162} + \\ & a^{160} + a^{157} + a^{156} + a^{154} + a^{153} + a^{150} + a^{148} + a^{146} + a^{144} + a^{143} + \\ & a^{139} + a^{138} + a^{137} + a^{135} + a^{134} + a^{131} + a^{128} + a^{127} + a^{126} + a^{121} + \\ & a^{120} + a^{119} + a^{118} + a^{117} + a^{113} + a^{112} + a^{110} + a^{105} + a^{102} + a^{101} + \\ & a^{99} + a^{98} + a^{93} + a^{92} + a^{90} + a^{88} + a^{87} + a^{85} + a^{82} + a^{81} + a^{78} + a^{71} + \\ & a^{67} + a^{64} + a^{62} + a^{60} + a^{55} + a^{54} + a^{51} + a^{50} + a^{48} + a^{40} + a^{39} + a^{38} + \\ & a^{37} + a^{35} + a^{26} + a^{24} + a^{23} + a^{19} + a^{13} + a^8 + a^5 + a^3 + a^2 + 1 \end{aligned}$$

$$\begin{aligned} v_{20} = \; & a^{179} + a^{177} + a^{174} + a^{172} + a^{171} + a^{170} + a^{165} + a^{163} + a^{161} + a^{159} + \\ & a^{157} + a^{156} + a^{154} + a^{150} + a^{149} + a^{147} + a^{144} + a^{142} + a^{141} + a^{140} + \\ & a^{139} + a^{138} + a^{137} + a^{136} + a^{134} + a^{131} + a^{129} + a^{128} + a^{127} + a^{126} + \\ & a^{121} + a^{120} + a^{119} + a^{118} + a^{110} + a^{109} + a^{107} + a^{106} + a^{105} + a^{104} + \\ & a^{99} + a^{97} + a^{96} + a^{95} + a^{94} + a^{92} + a^{85} + a^{83} + a^{80} + a^{77} + a^{74} + \\ & a^{71} + a^{70} + a^{67} + a^{63} + a^{62} + a^{60} + a^{59} + a^{57} + a^{56} + a^{52} + a^{50} + \\ & a^{47} + a^{46} + a^{45} + a^{44} + a^{43} + a^{38} + a^{35} + a^{33} + a^{32} + a^{31} + a^{28} + \\ & a^{24} + a^{23} + a^{19} + a^{18} + a^{17} + a^{16} + a^{15} + a^{14} + a^{13} + a^{12} + a^8 + a^7 + \\ & a^4 + a^3 + a + 1 \end{aligned}$$

En aquest exemple, els dos generadors han arribat fins al nivell 3 de l'arbre, és a dir, són divisors d'ordre $3^3 = 27$. Per tant, podem afirmar que el major factor de 3 que hi ha al cardinal de la Jacobiana és 3^6, ja que tenim 2 generadors de nivell 3 cada un.

El temps per a trobar aquests 2 divisors amb les nostres funcions, executant el codi també al Calculator de Magma [3] ha estat de 0.16 segons. Això és més de 750 vegades més ràpid que el que podria tardar a calcular el cardinal de la Jacobiana, de manera que ens proporciona un mètode ràpid per a poder descartar corbes que no siguin bones criptogràficament sense haver de calcular tot el cardinal abans.

7.3 Conclusions

Anteriorment ja s'havien realitzat altres treballs sobre els subgrups de 2-Sylow, 3-Sylow i més en general de l-Sylow en corbes el·líptiques [10, 11]. En el cas de corbes hiperel·líptiques sobre cossos binaris s'han realitzat treballs per a determinar el 2-Sylow [9]. Nosaltres hem aconseguit implementar un algorisme eficient i ràpid per a calcular el 3-Sylow en corbes hiperel·líptiques sobre cossos binaris.

A mesura que anàvem fent proves amb diferents corbes, ens hem adonat d'algunes particularitats. Vam implementar l'algorisme del 3-Sylow tenint en compte que per a cada arbre (segons el número de divisors d'ordre 3 independents), podríem arribar a un nivell diferent, de manera que podria haver fins a 4 arbres amb 4 nivells diferents.

Però vam veure que tots els arbres arribaven sempre el mateix nivell. Vam descartar que fos algun error del nostre algorisme, comparant els valors obtinguts amb el valor real del cardinal de la Jacobiana que ens dóna Magma amb les seves funcions. Després de milers de milions de proves amb diferents corbes aleatòries sobre diferents cossos, vam arribar a la conclusió que, amb les corbes que nosaltres treballem, tots els nivells seran sempre iguals.

Una altra situació particular, era que no vam trobar tampoc mai cap corba amb 3-rang igual a 3. Finalment, ens vam adonar que el requisit que ha de complir una corba hiperel·líptica per a poder tenir 3-rang igual a 3 i/o nivells diferents als arbres del 3-Sylow, era que $h_2 \neq 0$.

Tot i que encara no hem acabat una demostració formal, podem afirmar amb bastanta seguretat que és així. És interessant tenir-ho en compte ja que podem aprofitar aquesta informació per a modificar el nostre algorisme

de manera que sigui considerablement més ràpid, ja que no seria necessari provar les combinacions de divisors per saltar de branca. N'hi hauria prou d'aplicar el cas cíclic a cada divisor independent.

O si només volem saber el màxim exponent de la potència de 3 que divideix al cardinal de la Jacobiana, trobant el 3-rang de la corba i aplicant el cas cíclic a un únic divisor, i després multiplicant el nivell de l'arbre al que ha arribat pel 3-rang, en seria suficient.

Hem aplicat aquesta optimització al nostre algorisme, i hem pogut observar una millora considerable en els temps d'execució, sobretot quan el 3-rang és 4. A mesura que augmentem la mida dels cossos, la diferència és major. Aproximadament podem dir que, després de la millora, calcular el 3-Sylow d'una corba de 3-rang 4, sobre un cos de $\mathbb{F}_{2^{180}}$, el temps passa d'uns 17 segons a 1.2 segons. Ja en cossos petits la diferència és de 10 vegades menys temps com a mínim, per tant és una millora important, sempre tenint en compte que només és vàlida per a corbes amb $h_2 = 0$.

Per a futurs treballs, seria interessant poder trobar els trisecats de qualsevol corba, sense importar-ne els seus paràmetres. Caldria completar la funció explicada en aquest treball per a trobar els trisecats d'un divisor, ja que per ara només està implementat en corbes amb $h(x)$ constant, i aquesta és la que utilitzem per a trobar el 3-Sylow.

Però si disposéssim d'una funció més general per a trisecar, donat que el nostre codi del 3-Sylow està programat pensant en el cas més general, només seria necessari actualitzar l'algorisme del 3-Sylow amb aquesta nova funció.

Bibliografia

[1] H. Cohen, G. Frey. *Handbook of elliptic and hyperelliptic curve cryptography*, Discrete mathematics and its aplications, Chapman Hall/CxRC, 2006

[2] Computational Algebra Group. *Handbook of Magma*, http://magma.maths.usyd.edu.au/magma/handbook/, School of Mathematics and Statistics, University of Sydney, 1993

[3] Computational Algebra Group. *Magma Calculator*, http://magma.maths.usyd.edu.au/calc/, School of Mathematics and Statistics, University of Sydney, 1993

[4] T. ElGammal. *A publick-key cryptosystem and a signtaure scheme based on discrete logarithms*, Advances in Cryptology: Proceedings of CRYPTO'84, Springer, 1985

[5] N. Koblitz. *Algebraic aspects of cryptography, with an Appendix on Hyperelliptic Curves*, Algorithms and Computation in Mathematics Volume 3, Springer, 1998

[6] N. Koblitz. *Elliptic curve cryptosystems*, Math. Comp. 48, 1987

[7] F.J. Marías. *Criptosistema ElGamal mediante curvas hiperelípticas*, Treball fi de carrera, Universitat de Lleida, 2007

[8] V. Miller. *Use of elliptic curves in cryptography*, Advances in Cryptology-CRYPTO'85, Springer-Verlag, 1986

[9] J.M. Miret, J. Pujolàs, A. Rio. *Explicit 2-power torsion of genus 2 curves over finite fields*, Advances in mathematics of comunications, 2010

[10] R. Moreno. *Subgrupos de Sylow de las curvas elípticas definidas sobre cuerpos finitos*, PhD thesis, Universitat Politècnica de Catalunya, 2005

[11] E. Porta. *Algorisme per determinar la 3^n-torsió d'una corba el·líptica*, Treball fi de carrera, Universitat de Lleida, 2003

[12] W. Stein et al. *Sage's Reference Manual*, http://www.sagemath.org, Sagemath.org, 2005