Curvas Frobenius não clássicas e cotas superiores para pontos racionais em curvas sobre corpos finitos

Nazar Arakelian

Tese apresentada
ao
Instituto de Matemática e Estatística
da
Universidade de São Paulo
para
obtenção do título
de
Doutor em Ciências

Programa: Matemática

Orientador: Prof. Dr. Herivelto Martins Borges Filho

Durante o desenvolvimento deste trabalho o autor recebeu auxílio financeiro do CNPq

São Paulo, maio de 2013

Curvas Frobenius não clássicas e cotas superiores para pontos racionais em curvas sobre corpos finitos

Esta versão da tese contém as correções e alterações sugeridas pela Comissão Julgadora durante a defesa da versão original do trabalho, realizada em 24/05/2013. Uma cópia da versão original está disponível no Instituto de Matemática e Estatística da Universidade de São Paulo.

Comissão Julgadora:

- Prof. Dr. Herivelto Martins Borges Filho (orientador) - IME-USP
- Prof. Dr. Orlando Stanley Juriaans - IME-USP
- Prof. Dr. Daniel Levcovitz - ICMC-USP
- Prof. Dr. Fernando Eduardo Torres Orihuela - IMECC-UNICAMP
- Prof. Dr. Cícero Fernandes de Carvalho - UFU

Agradecimentos

Ao meu orientador e amigo, professor Herivelto Martins Borges Filho, por toda dedicação e incentivo durante os últimos anos. Aos professores da banca examinadora, pela cuidadosa leitura deste trabalho. Ao professor Eduardo Tengan, pela amizade e por toda a ajuda durante os dias que passei em São Carlos. Ao professor Orlando Stanley Juriaans, pela motivação e pelos valiosos conselhos. À Paula Lucas Mari, pelo carinho e companherismo. À todos os meus amigos e à minha família. Finalmente, à minha mãe Khatoun, à minha irmã Maria Lucia, pelo apoio e pela paciência.

Resumo

ARAKELIAN, N. **Curvas Frobenius não clássicas e cotas superiores para pontos racionais em curvas sobre corpos finitos.** 2013. 120 f. Tese (Doutorado) - Instituto de Matemática e Estatística, Universidade de São Paulo, São Paulo, 2013.

Este trabalho se divide em duas partes distintas. Na primeira parte, para cada inteiro $s \geq 1$, apresentamos uma família de curvas definidas sobre um corpo finito $\mathbb{F}_q$ que, sob certas hipóteses, são $\mathbb{F}_q$-Frobenius não clássicas com relação ao sistema linear de curvas planas de grau s. Para o caso $s = 2$, sob certas hipóteses, apresentamos um critério necessário e suficiente para que tais curvas sejam $\mathbb{F}_q$-Frobenius não clássicas com relação ao sistema linear de cônicas, obtendo assim exemplos de curvas diferentes das curvas de Fermat que atendem tal propriedade.

Na segunda parte, dada uma curva $\mathcal{X}$ definida sobre um corpo finito $\mathbb{F}_q$, através de um morfismo birracional definido sobre $\mathbb{F}_q$ de $\mathcal{X}$ em um espaço projetivo $\mathbb{P}^n$, obtemos uma cota superior para o número de seus pontos $\mathbb{F}_{q^r}$-racionais , onde $\mathbb{F}_{q^r}$ é uma extensão finita de $\mathbb{F}_q$. Tal cota fornece uma melhora para as cotas de Stöhr-Voloch e Hasse-Weil em vários tipos de curvas; dentre elas, as curvas Frobenius não clássicas com relação ao morfismo em questão, que em geral, são curvas que tendem a possuir muitos pontos racionais.

Palavras-chave: Curvas algébricas, Corpos finitos, Pontos racionais.

Abstract

ARAKELIAN, n. **Frobenius non-classical curves and upper bounds for rational points on curves over finite fields**. 2013. 120 f. Tese (Doutorado) - Instituto de Matemática e Estatística, Universidade de São Paulo, São Paulo, 2013.

This work is composed of two different parts. In the first one, for each integer $s \geq 1$, we present a family of curves defined over a finite field $\mathbb{F}_q$ that, under certain hypotheses, are $\mathbb{F}_q$-Frobenius non-classical with respect to the linear system of plane curves of degree s. For the case $s = 2$, we give, under certain hypotheses, a necessary and sufficient condition for such curves be $\mathbb{F}_q$-Frobenius non-classical with respect to the linear system of conics, which give examples of curves with such property, different of the Fermat curves.

In the secound part, given a curve $\mathcal{X}$ defined over a finite field $\mathbb{F}_q$, by a birrational morphism defined over $\mathbb{F}_q$ from $\mathcal{X}$ into a projective space $\mathbb{P}^n$, we obtain an upper bound for the number of its $\mathbb{F}_{q^r}$-rational points, were $\mathbb{F}_{q^r}$ is a finite extension of $\mathbb{F}_q$. Such bound provides an inprovement of the Stöhr-Voloch and Hasse-Weil bounds in several types of curves; among these, the Frobenius non-classical curves with respect to the referred morphism, that in general, are curves that tend to have many rational points.

Keywords: Algebraic curves, Finite fields, Rational points.

Sumário

1 Introdução e resultados preliminares 1

1.1 Morfismos e séries lineares 2

1.2 Pontos de Weierstrass e o divisor de ramificação 3

1.3 O divisor de Frobenius e o Teorema de Stöhr-Voloch 6

2 Curvas Frobenius não clássicas com relação a curvas de grau $s \geq 1$ 11

2.1 Curvas $\mathbb{F}_q$-Frobenius não clássicas 13

2.2 O caso $s = 2$ 17

2.2.1 O caso $p|2n-1$ 22

2.3 Curvas não clássicas 24

3 Pontos racionais em curvas sobre corpos finitos 27

3.1 Introdução 27

3.2 O divisor (q^u, q^m)-Frobenius 27

3.3 Exemplos 46

3.4 Curvas $\mathbb{F}_{q^r}$-Frobenius não clássicas, para $r = u, m$ 48

3.5 Aplicação a uma curva de Fermat 55

Capítulo 1

Introdução e resultados preliminares

A contagem/estimativa de pontos racionais em uma curva algébrica definida sobre um corpo finito é de extrema importância na teoria de curvas algébricas, pois possui diversas aplicações, como por exemplo em teoria de códigos, geometria finita, teoria dos números e problemas de Waring (ver [15] e [23, Capítulo 6]). Seja $\mathcal{X}$ curva algébrica arbitrária de gênero g definida sobre um corpo finito $\mathbb{F}_q$ com $q = p^h$ elementos, e defina N como sendo o número de pontos $\mathbb{F}_q$-racionais de $\mathcal{X}$. Calcular o valor preciso de N não costuma ser uma tarefa fácil; fórmulas práticas para a obtenção deste número só são conhecidas para certas classes de curvas (por exemplo, ver [14, Teorema 1]).

O resultado mais conhecido à esse respeito é o Teorema de Hasse-Weil (hipótese de Riemann para curvas algébricas sobre corpos finitos), através do qual se estabelece a seguinte cota para N (chamada cota de Hasse-Weil)

$$|N - (q+1)| \leq 2g\sqrt{q}. \tag{1.0.1}$$

Em particular, temos

$$N \leq q + 1 + 2g\sqrt{q}. \tag{1.0.2}$$

Existem curvas que atingem a cota (1.0.2), conhecidas como curvas maximais, cujo exemplo mais conhecido é a curva Hermitiana sobre $\mathbb{F}_{q^2}$, que é dada pela equação $X^{q+1}+Y^{q+1}+Z^{q+1} = 0$. Por conta disto, a cota superior de Hasse-Weil não pode ser melhorada de maneira geral; mas existem várias situações em que um aprimoramento desta cota pode ser obtido. Por exemplo, em [27], Serre prova que

$$|N - (q+1)| \leq g[2\sqrt{q}],$$

onde $[a]$ denota a parte inteira do número real a.

Em [29], Stöhr e Voloch introduziram uma técnica para obter novas cotas para pontos racionais de uma curva algébrica sobre um corpo finito. Através desta técnica, obtém-se em particular a cota de Hasse-Weil, e esta pode ser ser melhorada em vários casos. Neste capítulo, relembraremos alguns resultados básicos da teoria de Stöhr-Voloch. Durante todo o texto, a menos de

menção contrária, estabelecemos o seguinte:

- $\mathbb{F}_q$ é um corpo finito com $q = p^h$ elementos;
- $\mathcal{X}$ é uma curva algébrica projetiva não singular de gênero g irredutível definida sobre $\mathbb{F}_q$;
- $\mathbb{K}$ é o fecho algébrico de $\mathbb{F}_q$;
- N_r é o número de pontos $\mathbb{F}_{q^r}$-racionais da curva $\mathcal{X}$, onde $\mathbb{F}_{q^r}$ é uma extensão finita de $\mathbb{F}_q$;
- $\mathbb{P}^n(\mathbb{K})$ e $\mathbb{P}^n(\mathbb{F}_{q^r})$ são os espaços projetivos de dimensão n respectivamente sobre $\mathbb{K}$ e $\mathbb{F}_{q^r}$;
- $\mathbb{K}(\mathcal{X})$ e $\mathbb{F}_{q^r}(\mathcal{X})$ são os corpos de funções de $\mathcal{X}$ respectivamente sobre $\mathbb{K}$ e $\mathbb{F}_{q^r}$;
- $\mathcal{X}(F)$ é o conjunto de pontos F-racionais de $\mathcal{X}$, onde $F \subseteq \mathbb{K}$ é um subcorpo de $\mathbb{K}$;
- Se $\mathcal{X} \subseteq \mathbb{P}^n(\mathbb{K})$, o mapa $\mathbb{F}_q$-Frobenius Φ_q é definido em $\mathcal{X}$ por

$$\begin{array}{rccc} \Phi_q : & \mathcal{X} & \longrightarrow & \mathcal{X} \\ & (a_0 : \ldots : a_n) & \longmapsto & (a_0^q : \ldots : a_n^q); \end{array}$$

- Sejam $\mathcal{X}, \mathcal{Y} \subseteq \mathbb{P}^n(\mathbb{K})$ duas curvas algébricas e $P \in \mathbb{P}^n(\mathbb{K})$. Denotaremos por $I(P, \mathcal{X} \cap \mathcal{Y})$ a multiplicidade de interseção de $\mathcal{X}$ e $\mathcal{Y}$ no ponto P;
- Para um ponto não singular $P \in \mathcal{X}$, a valorização discreta em P será denotada por v_P;
- Dados dois inteiros $n \geq m \geq 1$ e uma matriz quadrada M de ordem n, o desenvolvimento de Laplace utilizando as m primeiras linhas(colunas) de M nos fornece que $det(M)$ é igual à soma alternada dos produtos que se obtêm multiplicando todos os menores de ordem m contidos nas m primeiras linhas(colunas) de M pelos correspondentes menores complementares de ordem $n - m$.

Daqui por diante, sempre que mencionarmos a palavra curva, estaremos nos referindo a uma curva algébrica projetiva. Para detalhes e provas dos resultados exibidos neste capítulo, recomendamos [29], [31] e [18].

1.1 Morfismos e séries lineares

Seja $\phi = (f_0 : \ldots : f_n) : \mathcal{X} \longrightarrow \mathbb{P}^n(\mathbb{K})$ um morfismo não degenerado (ou seja, $f_0, \ldots, f_n$ são linearmente independentes sobre $\mathbb{K}$), onde $f_0, \ldots, f_n \in \mathbb{K}(\mathcal{X})$, com $f_i \neq 0$ para algum i, são as funções coordenadas de ϕ. O morfismo ϕ define unicamente suas funções coordenadas a menos de um fator não nulo em $\mathbb{K}(\mathcal{X})$, ou seja, podemos enxergar ϕ como um ponto de $\mathbb{P}^n(\mathbb{K}(\mathcal{X}))$. Dado um ponto $P \in \mathcal{X}$, temos que

$$\phi(P) = ((t^{e_P} f_0)(P) : \ldots : (t^{e_P} f_n)(P)),$$

onde $e_P = -min\{v_P(f_0), ..., v_P(f_n)\}$ e $t \in \mathbb{K}(\mathcal{X})$ é um parâmetro local em P. A imagem $\phi(\mathcal{X})$ é uma curva (possivelmente singular) em $\mathbb{P}^n(\mathbb{K})$, cujo corpo de funções é $\mathbb{K}(\phi(\mathcal{X})) = \mathbb{K}(\frac{f_0}{f_i}, ..., \frac{f_n}{f_i})$, onde $f_i \neq 0$. O grau de ϕ é definido por $\deg(\phi) = [\mathbb{K}(\mathcal{X}) : \mathbb{K}(\phi(\mathcal{X}))]$. O morfismo ϕ é dito birracional quando $\mathbb{K}(\phi(\mathcal{X})) = \mathbb{K}(\mathcal{X})$, ou seja, quando $\deg(\phi) = 1$. Caso ϕ seja birracional, curva $\mathcal{X}$ pode ser pensada como uma curva parametrizada em $\mathbb{P}^n(\mathbb{K})$, ou $\phi(\mathcal{X})$ como uma manifestação de $\mathcal{X}$ em $\mathbb{P}^n(\mathbb{K})$. Neste caso, para $Q \in \phi(\mathcal{X})$, os pontos da fibra $\phi^{-1}(Q)$ são ramos (de $\mathcal{X}$) de $\phi(\mathcal{X})$ centrados em Q (ver [18, Capítulo 4, seção 4.3]).

Seja $Div(\mathbb{K}(\mathcal{X}))$ o grupo dos divisores de $\mathbb{K}(\mathcal{X})$, e seja $E \in Div(\mathbb{K}(\mathcal{X}))$ definido por

$$E := \sum_{P \in \mathcal{X}} e_P P.$$

Pela definição de E, temos que todas as fuções coordenadas de ϕ pertencem ao espaço de Riemann-Roch $\mathcal{L}(E) = \{f \in \mathbb{K}(\mathcal{X})^* \mid div(f) + E \geq 0\} \cup \{0\}$; estas geram um subespaço V_ϕ de $\mathcal{L}(E)$ de dimensão n (uma vez que ϕ é não degenerado).

Portanto, associado a ϕ temos, a menos de mudança de coordenadas projetivas em $\mathbb{P}^n(\mathbb{K}(\mathcal{X}))$, uma única série linear de dimensão n livre de ponto base

$$\mathcal{D}_\phi = \left\{ div\left(\sum_{i=0}^{n} a_i f_i\right) + E \mid a_0, ..., a_n \in \mathbb{K} \right\} \subseteq |E| := \{D \in Div(\mathbb{K}(\mathcal{X})) \mid D \geq 0,\ D \sim E\}.$$

O grau da série $\mathcal{D}_\phi$ é o grau do divisor E. Reciprocamente, pode-se provar que a cada série linear livre de ponto base $\mathcal{D}$ de dimensão n está associado, a menos de mudança de coordenadas projetivas em $\mathbb{P}^n(\mathbb{K})$, um único morfismo não degenerado $\phi : \mathcal{X} \longrightarrow \mathbb{P}^n(\mathbb{K})$. Dizemos que uma série linear é simples quando o morfismo associado a ela é birracional. No que segue, a menos de menção contrária, sempre que usarmos a palavra morfismo, estaremos nos referindo a um morfismo birracional não degenerado.

Outra interpretação para a relação entre séries lineares e morfismos é a seguinte: A interseção de um hiperplano de $\mathbb{P}^n(\mathbb{K})$ com os ramos da curva $\mathcal{X}$ da origem a um divisor $D \in \mathcal{D}_\phi$; por outro lado, todo divisor $D \in \mathcal{D}_\phi$ também é obtido pela interseção de um hiperplano de $\mathbb{P}^n(\mathbb{K})$ com os ramos da curva $\mathcal{X}$.

1.2 Pontos de Weierstrass e o divisor de ramificação

Seja $\phi : \mathcal{X} \longrightarrow \mathbb{P}^n(\mathbb{K})$ um morfismo (birracional não degenerado) e $\mathcal{D}$ a série linear correspondente. Dado um ponto $P \in \mathcal{X}$, a idéia é considerar todas as possíveis multiplicidades de interseção dos hiperplanos de $\mathbb{P}^n(\mathbb{K})$ e o ponto P (centrado em $\phi(P)$) da curva $\mathcal{X}$. Os divisores obtidos pela interseção dos hiperplanos de $\mathbb{P}^n(\mathbb{K})$ com os pontos de $\mathcal{X}$ também dão origem à série linear $\mathcal{D}$. Uma maneira de observar que $\mathcal{D}$ é, de fato, livre de ponto base, é através do fato de que dado um ponto $\phi(P) \in \phi(\mathcal{X})$, existe um hiperplano de $\mathbb{P}^n(\mathbb{K})$ que não passa por $\phi(P)$.

Definição 1.2.1. *Seja $P \in \mathcal{X}$. Um inteiro positivo j é um P-invariante Hermitiano de $\mathcal{D}$ ou*

uma $(\mathcal{D}, P)$-ordem se existir um divisor $D \in \mathcal{D}$ tal que $v_P(D) = j$; isto significa que existe um hiperplano $H \subset \mathbb{P}^n(\mathbb{K})$ intersectando o ponto P com multiplicidade j.

Para cada inteiro i, temos que

$$\mathcal{D}_i = \{D \in \mathcal{D} \mid D \geq iP\}$$

é uma subsérie de $\mathcal{D}$. Para todo i, temos que $\mathcal{D}_i$ corresponde ao subespaço de $\mathbb{P}^n(\mathbb{K})$ formado por todos os hiperplanos que intersectam o ponto P com multiplicidade maior ou igual a i. Pela própria definição, temos

$$\mathcal{D} = \mathcal{D}_0 \supseteq \mathcal{D}_1 \supseteq \mathcal{D}_2 \supseteq ... \supseteq \mathcal{D}_n \supseteq ....$$

Além disto, a codimensão de $\mathcal{D}_{i+1}$ em $\mathcal{D}_i$ é 0 ou 1. Portanto, um inteiro j é uma $(\mathcal{D}, P)$-ordem se, e somente se, $\mathcal{D}_j \neq \mathcal{D}_{j+1}$, e neste caso, $\mathcal{D}_{j+1}$ tem codimensão 1 em $\mathcal{D}_j$. Observe que $\mathcal{D}_i = \emptyset$ se $i > d = \deg \mathcal{D}$. Desta maneira, existem exatamente $n+1$ $(\mathcal{D}, P)$-ordens, digamos

$$j_0(P) < j_1(P) < j_2(P) < ... < j_n(P),$$

$j_n(P) \leq d$. Como $\mathcal{D}$ é livre de ponto base, temos $j_0(P) = 0$. Quando não houver dúvida quanto ao ponto P ao qual estamos nos referindo, escreveremos j_i ao invés de $j_i(P)$.

Seja L_i a interseção de todos os hiperplanos em $\mathbb{P}^n(\mathbb{K})$ que intersectam o ponto P com multiplicidade maior ou igual a $j_{i+1}(P)$. O subespaço L_i é o i-ésimo plano osculador em P, e L_{n-1} o hiperplano osculador em P. Repare que $L_0 = \phi(P)$ e L_1 é a reta tangente a $\phi(\mathcal{X})$ em P.

Definição 1.2.2. *Seja t um elemento transcendente sobre $\mathbb{K}$. Definimos a i-ésima derivada de Hasse em $\mathbb{K}[t]$ da seguinte maneira:*

$$D_t^{(i)}\left(\sum c_j t^j\right) := \sum \binom{j}{i} c_j t^{j-i},$$

onde $i, j \geq 0$. Convencionaremos que $\binom{j}{i} = 0$ se $i > j$. Note que esta derivada pode ser naturalmente estendida a $\mathbb{K}(t)$, ao corpo das séries de Laurent $\mathbb{K}((t))$ e a qualquer extensão finita separável de $\mathbb{K}(t)$. Em particular, a i-ésima derivada de Hasse $D_t^{(i)}$ está definida em $\mathbb{K}(\mathcal{X})$, onde t é uma variável separante (Para mais detalhes, referimos [31, Seção 2.1] e [18, Seções 5.7 e 5.10]).

Teorema 1.2.3. *Sejam $P \in \mathcal{X}$ e t um parâmetro local em P, e suponha (multiplicando f_i por t^{e_P}) que $e_P = 0$. Assuma que as primeiras i $(\mathcal{D}, P)$-ordens $j_0, ..., j_{i-1}$ são conhecidas. Então j_i é o menor inteiro tal que os pontos $((D_t^{(j_s)} f_0)(P) : ... : (D_t^{(j_s)} f_n)(P))$ com $s = 0, ..., i$ são linearmente independentes sobre $\mathbb{K}$, e o i-ésimo plano osculador em P é gerado por esses pontos.*

Corolário 1.2.4. *O hiperplano osculador em $P \in \mathcal{X}$ é dado pela equação*

$$\det \begin{pmatrix} X_0 & \dots & X_n \\ (D_t^{(j_0)} f_0)(P) & \dots & (D_t^{(j_0)} f_n)(P) \\ \vdots & \ddots & \vdots \\ (D_t^{(j_{n-1})} f_0)(P) & \dots & (D_t^{(j_{n-1})} f_n)(P) \end{pmatrix} = 0.$$

Seja agora t uma variável separante de $\mathbb{K}(\mathcal{X})$ e considere o conjunto

$$H_\phi := \{(m_0, ..., m_n) \mid m_i \in \mathbb{Z},\ 0 \leq m_0 < ... < m_n,\ \det(D_t^{(m_i)} f_j)_{0 \leq i,j \leq n} \neq 0\}$$

munido da ordem lexicográfica. Pelo Teorema 1.2.3, temos $H_\phi \neq \emptyset$. O elemento mínimo $(0 = \epsilon_0, ..., \epsilon_n)$ de H_ϕ é chamado sequência de $\mathcal{D}$-ordens de $\mathcal{X}$, e esta depende apenas da série linear $\mathcal{D}$ (do morfismo ϕ). Os inteiros ϵ_i são chamados $\mathcal{D}$-ordens de $\mathcal{X}$. Dado $P \in \mathcal{X}$ com $(\mathcal{D}, P)$-ordens $j_0, ..., j_n$, pela minimalidade de $(\epsilon_0, ..., \epsilon_n)$ temos que $\epsilon_i \leq j_i$ para todo $i = 0, ..., n$.

Definição 1.2.5. *O divisor de ramificação de $\mathcal{D}$ é definido por*

$$R := div(\det(D_t^{(\epsilon_i)} f_j)) + (\epsilon_1 + ... + \epsilon_n) div(dt) + (n+1)E,$$

onde t é uma variável separante e $E = \sum e_P P$, com $e_P = -min\{v_P(f_0), ..., v_P(f_n)\}$.

Assim como a sequência de $\mathcal{D}$-ordens de $\mathcal{X}$, o divisor de ramificação depende apenas da série linear $\mathcal{D}$ (do morfismo ϕ). Além disso, o divisor R é efetivo (ou seja, $R \geq 0$) e seu grau é $\deg(R) = (\epsilon_1 + ... + \epsilon_n)(2g-2) + (n+1)d$.

Teorema 1.2.6. *Seja $P \in \mathcal{X}$ e $j_0, ..., j_n$ suas $(\mathcal{D}, P)$-ordens. Então*

$$v_P(R) \geq \sum_{i=0}^{n} (j_i - \epsilon_i),$$

e a igualdade vale se, e somente se,

$$\det\left(\binom{j_i}{\epsilon_s}\right) \not\equiv 0 \mod p.$$

Os pontos $P \in \mathcal{X}$ que pertencem ao suporte de R são chamados de pontos $\mathcal{D}$-Weierstrass, e para estes pontos, temos que $(j_0(P), ..., j_n(P)) \neq (\epsilon_0, ..., \epsilon_n)$. O restante dos pontos $P \in \mathcal{X}$ são chamados $\mathcal{D}$-ordinários, e para estes temos $(j_0(P), ..., j_n(P)) = (\epsilon_0, ..., \epsilon_n)$. Em particular, temos que a menos de um subconjunto finito de pontos de $\mathcal{X}$, a sequência de $(\mathcal{D}, P)$-ordens e a sequência de $\mathcal{D}$-ordens coincidem.

Dizemos que a curva $\mathcal{X}$ é clássica com relação a $\mathcal{D}$ se $(\epsilon_0, ..., \epsilon_n) = (0, 1, ..., n)$. Caso $\epsilon_i \neq i$ para algum i, dizemos que $\mathcal{X}$ é não clássica com relação a $\mathcal{D}$.

Proposição 1.2.7. *Sejam $P \in \mathcal{X}$ e $j_0, ..., j_n$ as $(\mathcal{D}, P)$-ordens. Se o inteiro $\prod_{i>s}(j_i - j_s)/(i-s)$ não é divisível por p então $\mathcal{X}$ é clássica com relação a $\mathcal{D}$ e o peso de P no divisor R é igual a $\sum(j_i - i)$.*

Como consequência da Proposição 1.2.7, temos que se $p > d = \deg(\mathcal{D})$, a curva $\mathcal{X}$ é clássica com relação a $\mathcal{D}$. Também, toda curva definida sobre um corpo de característica 0 é clássica com relação a qualquer série linear.

Proposição 1.2.8. *Seja ϵ uma $\mathcal{D}$-ordem e μ um inteiro tal que $\binom{\epsilon}{\mu} \not\equiv 0 \mod p$. Então μ também é uma $\mathcal{D}$-ordem. Em particular, se ϵ é uma $\mathcal{D}$-ordem menor que p então os inteiros $0, 1, ..., \epsilon - 1$ também são $\mathcal{D}$-ordens.*

Corolário 1.2.9. *Suponha que $p \geq n = \dim(\mathcal{D})$, e que para $0, 1, ..., n-1$ as $\mathcal{D}$-ordens são $\epsilon_i = i$. Se $\mathcal{D}$ é não clássica, então ϵ_n é uma potência de p.*

Seja $(\mathbb{K}(\mathcal{X}))_m = \{u^{p^m} \mid u \in \mathbb{K}(\mathcal{X})\}$, que é um subcorpo de $\mathbb{K}(\mathcal{X})$. O seguinte resultado de Garcia e Voloch [11] é muito útil para decidir-se se dada curva é ou não clássica para certo morfismo.

Teorema 1.2.10 (Garcia-Voloch). *Seja $\phi = (f_0 : ... : f_n) : \mathcal{X} \longrightarrow \mathbb{P}^n(\mathbb{K})$ um morfismo com $f_0, ..., f_n \in \mathbb{K}(\mathcal{X})$. Então $f_0, ..., f_n$ são linearmente independentes sobre $(\mathbb{K}(\mathcal{X}))_m$ se, e somente se, existirem inteiros $\epsilon_0, ..., \epsilon_n < p^m$ tais que $\det(D^{(\epsilon_i)}x_j) \neq 0$.*

1.3 O divisor de Frobenius e o Teorema de Stöhr-Voloch

Nesta seção, vamos supor que o morfismo $\phi = (f_0 : ... : f_n)$ está definido sobre $\mathbb{F}_q$, ou seja, $f_0, ..., f_n \in \mathbb{F}_q(\mathcal{X})$. Neste caso, dizemos também que ϕ é um $\mathbb{F}_q$-morfismo. Como a curva $\mathcal{X}$ está definida sobre $\mathbb{F}_q$, temos que está definido o mapa $\mathbb{F}_q$-Frobenius $\Phi_q : \mathcal{X} \longrightarrow \mathcal{X}$, de maneira que um ponto $P \in \mathcal{X}$ é $\mathbb{F}_q$-racional se, e somente se, $\Phi_q(P) = P$. O mapa Φ_q induz uma ação no grupo $Div(\mathbb{K}(\mathcal{X}))$, e dizemos que um divisor D é $\mathbb{F}_q$-racional se $\Phi_q(D) = D$. Da mesma forma, dizemos que uma série linear $\mathcal{D}$ está definida sobre $\mathbb{F}_q$ se $\Phi_q(D) = D$ para todo $D \in \mathcal{D}$. Prova-se que o morfismo ϕ é um $\mathbb{F}_q$-morfismo se, e somente se, o divisor $E = \sum_{P \in \mathcal{X}} e_P P$ e a série linear $\mathcal{D} = \mathcal{D}_\phi$ estão definidos sobre $\mathbb{F}_q$ (para detalhes, recomendamos [18, Capítulo 8]).

A idéia de Stöhr e Voloch em [29] para obter cotas superiores para N_1 é coletar os pontos $P \in \mathcal{X}$ tais que a imagem de $\phi(P)$ pelo mapa de Frobenius Φ_q em $\mathbb{P}^n(\mathbb{K})$ pertença ao hiperplano osculador em P. Um ponto $P \in \mathcal{X}$ atende a essa propriedade se, e somente se,

$$\det \begin{pmatrix} f_0(P)^q & ... & f_n(P)^q \\ (D_t^{(j_0)} f_0)(P) & ... & (D_t^{(j_0)} f_n)(P) \\ \vdots & \ddots & \vdots \\ (D_t^{(j_{n-1})} f_0)(P) & ... & (D_t^{(j_{n-1})} f_n)(P) \end{pmatrix} = 0,$$

onde t é um parâmetro local em P e j_i são as $(\mathcal{D}, P)$-ordens, com $i = 0, ..., n$. Isso motiva o estudo das funções

$$W_t^{m_0,...,m_{n-1}}(f_0, ..., f_n) := \det \begin{pmatrix} f_0^q & \cdots & f_n^q \\ D_t^{(m_0)} f_0 & \cdots & D_t^{(m_0)} f_n \\ \vdots & \ddots & \vdots \\ D_t^{(m_{n-1})} f_0 & \cdots & D_t^{(m_{n-1})} f_n \end{pmatrix}, \tag{1.3.1}$$

onde t é uma variável separante de $\mathbb{F}_q(\mathcal{X})$ e $m_0 \leq ... \leq m_{n-1}$ são inteiros não negativos. Como fizemos antes, fixado t, consideramos o conjunto

$$K_\phi := \{(m_0, ..., m_{n-1}) \mid m_i \in \mathbb{Z},\ 0 \leq m_0 < ... < m_{n-1},\ W_t^{m_0,...,m_{n-1}}(f_0, ..., f_n) \neq 0\}$$

munido da ordem lexicográfica. Pode-se provar que o conjunto K_ϕ é não vazio e portanto admite um elemento mínimo $(0 = \nu_0, ..., \nu_{n-1})$. A sequência $(\nu_0, ..., \nu_{n-1})$ é denotada sequêcia de ordens $\mathbb{F}_q$-Frobenius de $\mathcal{X}$ com relação a $\mathcal{D}$, e os inteiros ν_i são chamados ordens $\mathbb{F}_q$-Frobenius de $\mathcal{X}$. Prova-se também que esta sequência depende apenas da série linear $\mathcal{D}$, e que existe um inteiro $I \in \{1, ..., n\}$ (denotado índice $\mathbb{F}_q$-Frobenius) tal que $\{\nu_0, ..., \nu_{n-1}\} = \{\epsilon_0, ..., \epsilon_n\} \backslash \{\epsilon_I\}$.

Definição 1.3.1. *O divisor de Frobenius de $\mathcal{D}$ é definido por*

$$S := div(W_t^{\nu_0,...,\nu_{n-1}}(f_0, ..., f_n)) + (\nu_1 + ... + \nu_{n-1}) div(dt) + (q + n)E,$$

onde t é uma variável separante e $E = \sum e_P P$, com $e_P = -min\{v_P(f_0), ..., v_P(f_n)\}$.

O divisor de Frobenius, assim como o divisor de ramificação, depende apenas da série linear $\mathcal{D}$. Ele é um divisor efetivo e seu grau é $\deg(S) = (\nu_1 + ... + \nu_{n-1})(2g - 2) + (q + n)d$. A curva $\mathcal{X}$ é dita $\mathbb{F}_q$-Frobenius clássica com relação a $\mathcal{D}$ se $(\nu_0, ..., \nu_{n-1}) = (0, ..., n - 1)$; caso contrário, a curva $\mathcal{X}$ é $\mathbb{F}_q$-Frobenius não clássica com relação a $\mathcal{D}$. Sempre que não houver dúvida sobre qual série linear estamos tratando e sobre qual corpo finito a curva $\mathcal{X}$ é definida, diremos simplesmente que a curva $\mathcal{X}$ é Frobenius (não) clássica se $\mathcal{X}$ for $\mathbb{F}_q$-Frobenius (não) clássica com relação a $\mathcal{D}$.

O próximo resultado, provado por Hefez e Voloch [14], relaciona $\mathcal{D}$-ordens de $\mathcal{X}$ com suas ordens de $\mathbb{F}_q$-Frobenius.

Teorema 1.3.2. *Seja $\mathcal{X}$ uma curva irredutível não singular definida sobre $\mathbb{F}_q$, onde $q = p^h$ com $p > 2$. Seja $\phi = (f_0 : ... : f_n) : \mathcal{X} \longrightarrow \mathbb{P}^n(\mathbb{K})$ um $\mathbb{F}_q$-morfismo, e sejam $(\epsilon_0, ..., \epsilon_n)$ e $(\nu_0, ..., \nu_{n-1})$ respectivamente suas sequência de $\mathcal{D}$-ordens e sequência de ordens $\mathbb{F}_q$-Frobenius. Se $\nu_1 > 1$ então $\epsilon_2 > 2$.*

Temos um resultado análogo à Proposição 1.2.8 para ordens $\mathbb{F}_q$-Frobenius.

Proposição 1.3.3. *Se ν é uma ordem de Frobenius de $\mathcal{D}$ menor que q, então todo μ tal que $\binom{\nu}{\mu} \not\equiv 0 \mod p$ também é uma ordem de Frobenius de $\mathcal{D}$. Em particular, se $\nu_i < p$, então $(\nu_0, ..., \nu_i) = (0, ..., i)$.*

Corolário 1.3.4. *Suponha que $p \geq n-1$, onde $n = \dim(\mathcal{D})$, e que para $0, 1, ..., n-2$ as ordens $\mathbb{F}_q$-Frobenius em relação a $\mathcal{D}$ são $\nu_i = i$. Se $\mathcal{D}$ é $\mathbb{F}_q$-Frobenius não clássica, então ν_{n-1} é uma potência de p.*

Os dois seguintes resultados avaliam os pesos dos pontos $P \in \mathcal{X}$ no divisor S, especialmente os pontos $\mathbb{F}_q$-racionais. O Teorema de Stöhr-Voloch é provado a partir destes resultados.

Proposição 1.3.5. *(a) Se $P \in \mathcal{X}$ é um ponto $\mathbb{F}_q$-racional com $(\mathcal{D}, P)$-ordens $j_0, ..., j_n$, então*

$$v_P(S) \geq \sum_{i=1}^{n} (j_i - \nu_{i-1}),$$

e a igualdade vale se, e somente se,

$$\det\left(\binom{j_i}{\nu_s}\right)_{0 \leq s \leq n-1,\ 1 \leq i \leq n} \not\equiv 0 \mod p.$$

(b) Se $P \in \mathcal{X}$ é um ponto arbitrário com $(\mathcal{D}, P)$-ordens $j_0, ..., j_n$, então

$$v_P(S) \geq \sum_{i=1}^{n-1} (j_i - \nu_i),$$

e se

$$\det\left(\binom{j_i}{\nu_s}\right)_{0 \leq s, i \leq n-1} \equiv 0 \mod p,$$

vale a desigualdade estrita.

Proposição 1.3.6. *Sejam $P \in \mathcal{X}$ um ponto $\mathbb{F}_q$-racional e $j_0, ..., j_n$ as $(\mathcal{D}, P)$-ordens, Então $\nu_i \leq j_{i+1} - j_1$ para cada $i = 0, ..., n-1$, e $v_P(S) \geq n j_1$.*

Teorema 1.3.7 (Stöhr-Voloch). *Seja $\mathcal{X}$ uma curva irredutível não singular de gênero g definida sobre $\mathbb{F}_q$, e seja N_1 o número de pontos $\mathbb{F}_q$-racionais de $\mathcal{X}$. Se existir em $\mathcal{X}$ uma série linear livre de ponto base definida sobre $\mathbb{F}_q$ de grau d, dimensão n, e com sequência de ordens de $\mathbb{F}_q$-Frobenius $\nu_0, ..., \nu_{n-1}$, então*

$$N_1 \leq \frac{(\nu_1 + ... + \nu_{n-1})(2g-2) + (q+n)d}{n}.$$

Seja $(\epsilon_0, ..., \epsilon_n)$ a sequência de $\mathcal{D}$-ordens de $\mathcal{X}$. Tendo em vista a Proposição 1.3.5(a), temos que a cota de Stöhr-Voloch admite a seguinte versão:

$$\sum_{i=1}^{n} (\epsilon_i - \nu_{i-1}) N_1 \leq (\nu_1 + ... + \nu_{n-1})(2g-2) + (q+n)d. \tag{1.3.2}$$

Ao longo deste texto, a desigualdade (1.3.2) também será denomindada cota de Stöhr-Voloch.

Fazendo uso do método de Stöhr-Voloch, em [14] Hefez e Voloch determinam o valor exato de N_1 para certas curvas Frobenius não clássicas.

Teorema 1.3.8 (Hefez-Voloch). *Seja $\mathcal{X}$ uma curva irredutível não singular de gênero g definida sobre $\mathbb{F}_q$ obtida através de uma série linear $\mathcal{D}$ de dimensão n e grau d com ordens $\mathbb{F}_q$-Frobenius $\nu_0, ..., \nu_{n-1}$ tal que $\nu_1 > 1$. Então*

$$N_1 = d(q-1) - (2g-2).$$

Encerraremos este capítulo introdutório com outro resultado que relaciona classicalidade e Frobenius classicalidade de uma curva, que nos será útil ao longo deste texto.

Proposição 1.3.9. *Seja $\mathcal{D}$ uma série linear de dimensão n da curva $\mathcal{X}$, definida sobre $\mathbb{F}_q$, tal que $p > n$. Se $\mathcal{X}$ é $\mathbb{F}_q$-Frobenius não clássica com relação a $\mathcal{D}$, então $\mathcal{X}$ é não clássica com relação a $\mathcal{D}$.*

Demonstração. Sejam $(\nu_0, ..., \nu_{n-1})$ e $(\epsilon_0, ..., \epsilon_n)$ respectivamente a sequência de ordens $\mathbb{F}_q$-Frobenius com relação a $\mathcal{D}$ e a sequência de $\mathcal{D}$-ordens de $\mathcal{X}$. Se $(\nu_0, ..., \nu_{n-1}) = (\epsilon_0, ..., \epsilon_{n-1})$, temos o resultado trivialmente. Caso contrário, temos que $\{\nu_0, ..., \nu_{n-1}\} = \{\epsilon_0, ..., \epsilon_n\} \backslash \{\epsilon_I\}$ para algum $I \in \{1, ..., n-1\}$. Logo, por [10, Corolário 3], temos que $\epsilon_{I+1} \equiv 0 \mod p$. Como $p > n$, segue o resultado. □

Capítulo 2

Curvas Frobenius não clássicas com relação a curvas de grau $s \geq 1$

Considere um polinômio homogêneo $F(x,y,z) \in \mathbb{F}_q[x,y,z]$ tal que $\mathcal{X} : F(x,y,z) = 0$ é uma curva plana projetiva irredutível de grau d. O corpo de funções de $\mathcal{X}$ é dado por $\mathbb{K}(\mathcal{X}) = \mathbb{K}(x,y)$, com $f(x,y) = 0$, onde $f(x,y) := F(x,y,1)$. Para cada inteiro s tal que $1 \leq s \leq d-3$, definimos o morfismo

$$\phi_s = (1 : x : y : x^2 : ... : x^i y^j : ... : y^s) : \mathcal{X} \longrightarrow \mathbb{P}^M(\mathbb{K}) \tag{2.0.1}$$

onde $i + j \leq s$ e $M = \binom{s+2}{2} - 1 = (s^2 + 3s)/2$. Este morfismo é chamado morfismo de Veronese. Associada a ele, temos a série linear $\mathcal{D}_s$, que é simples, livre de ponto base e tem grau sd (ver [18, Seção 7.7]).

Agora, para toda curva $\mathcal{C} \subset \mathbb{P}^2(\mathbb{K})$, a interseção de $\mathcal{C}$ com um ramo da curva $\mathcal{X}$ da origem a um divisor $D \in Div(\mathbb{K}(\mathcal{X}))$, e dado um sistema linear de curvas planas Γ, as interseções de todas as curvas de Γ com os ramos da curva $\mathcal{X}$ dão origem a uma série linear (dizemos que tal série é obtida pelo corte de $\mathcal{X}$ pelo sistema linear Γ).

Considere Γ_s o sistema linear formado por todas as curvas planas de grau s. A série linear $\mathcal{D}_s$ é obtida também pelo corte de $\mathcal{X}$ pelo sistema linear Γ_s (ver [18, capítulo 6]). Desta maneira, dado um ponto não singular $P \in \mathcal{X}$, a multiplicidade de interseção de $\mathcal{X}$ com uma curva plana $\mathcal{C}$ de grau s em P corresponde à multiplicidade de interseção do ramo P da curva $\phi_s(\mathcal{X})$ com algum hiperplano $H \subset \mathbb{P}^M(\mathbb{K})$. Assim, as $(\mathcal{D}_s, P)$-ordens $j_0(P), ..., j_M(P)$ correspondem a todas as possíveis multiplicidades de interseção de $\mathcal{X}$ com alguma curva plana de grau s em P. Em particular, existe uma única curva plana $\mathcal{H}_P^s$, chamada curva s-osculadora a $\mathcal{X}$ em P, tal que a muiltiplicidade de interseção de $\mathcal{X}$ e $\mathcal{H}_P^s$ no ponto P é $I(P, \mathcal{X} \cap \mathcal{H}_P^s) = j_M(P)$.

Pelo Teorema de Stöhr-Voloch 1.3.7, segue que

$$N_1 \leq \frac{d(d-3)(\nu_0 + ... + \nu_{M-1}) + sd(q+M)}{M}, \tag{2.0.2}$$

onde $\nu_0, ..., \nu_M$ é a sequência de ordens $\mathbb{F}_q$-Frobenius de $\mathcal{X}$ com relação a $\mathcal{D}_s$. Se a curva $\mathcal{X}$ for

$\mathbb{F}_q$-Fobenius clássica, temos que (2.0.2) nos fornece a seguinte cota:

$$N_1 \leq \frac{d(d-3)(M-1)}{2} + \frac{sn(q+M)}{M}. \tag{2.0.3}$$

A cota (2.0.3) melhora a cota de Hasse-Weil em diversos casos (por exemplo, ver [29, Seção 3] e [12]).

Em contrapartida, se a curva $\mathcal{X}$ é $\mathbb{F}_q$-Frobenius não clássica, obtemos um valor maior no lado direito da desigualdade (2.0.2), isto é, a cota obtida não é tão boa quanto (2.0.3). Em particular, para p suficientemente grande em comparação a s, temos pela Proposição 1.3.3 que $p|\nu_i$ para algum $i \in \{1, ..., M-1\}$. Assim, conclue-se facilmente que o método de Stöhr-Voloch é mais eficiente quando aplicado a curvas $\mathbb{F}_q$-Frobenius clássicas. Contrastando com este fato, temos que o valor maior no lado direito da desigualdade (2.0.2) nos casos $\mathbb{F}_q$-Frobenius não clássicos indica que tais curvas tendem a possuir muitos pontos $\mathbb{F}_q$-racionais.

Portanto, caracterizar as curvas $\mathbb{F}_q$-Frobenius não clássicas com relação a um sistema linear de curvas pode ser visto como um problema de duas vertentes. Por um lado, excluindo as curvas $\mathbb{F}_q$-Frobenius não clássicas, ficamos com uma classe de curvas para as quais uma boa cota (2.0.3) pode ser aplicada. Por outro lado, com as curvas $\mathbb{F}_q$-Frobenius não clássicas em mãos, temos uma potencial fonte de curvas com muitos pontos $\mathbb{F}_q$-racionais, como ilustraremos a seguir.

Curvas com muitos pontos $\mathbb{F}_q$-racionais são muito úteis, pois possuem diversas aplicações; dentre elas, a teoria de códigos (ver, por exemplo, [28, Capítulos 2 e 8]). A cota (2.0.3) para $s = r+1$ é melhor do que para $s = r$ se, aproximadamente,

$$d < \left(\frac{4(r+1)}{r^4 + 10r^3 + 35r^2 + 50r + 24}\right) q,$$

onde $r \geq 1$. Para $s = 1$ (ou seja, para a série obtida pelo corte de $\mathcal{X}$ por retas em $\mathbb{P}^2(\mathbb{K})$), a cota (2.0.3) é

$$N_1 \leq \frac{d(d+q-1)}{2}. \tag{2.0.4}$$

Portanto, a cota (2.0.4) não pode ser atingida por uma curva $\mathcal{X}$ tal que $d < q/15$, a menos que esta seja $\mathbb{F}_q$-Frobenius não clássica com relação a $\mathcal{D}_2$. Da mesma maneira, a cota (2.0.3) para $s = 2$ não pode ser atingida por uma curva $\mathcal{X}$ tal que $d < q/30$, a menos que $\mathcal{X}$ seja $\mathbb{F}_q$-Frobenius não clássica com relação a $\mathcal{D}_3$, e assim por diante. Logo, apesar de raras, tais curvas são muito importantes.

O caso $s = 1$ foi investigado por vários autores. Por exemplo em [4],[9],[12] e [14], alguns exemplos de classes de curvas $\mathbb{F}_q$-Frobenius não clássicas são apresentados. No entanto, mesmo para o caso $s = 1$, não existe uma caracterização completa de uma curva $\mathbb{F}_q$-Frobenius não clássica.

Em [12], Garcia e Voloch estabeleceram critérios nescessários e suficientes para que uma curva de Fermat (ou seja, as curvas dadas por $ax^d + by^d = z^d$, com $ab \neq 0$ e $d > 1$ não divisível por p) seja $\mathbb{F}_q$-Frobenius não clássicas para $\mathcal{D}_1$ e $\mathcal{D}_2$. Aparentemente, além das curvas de Fermat,

não são conhecidos muitos exemplos de curvas $\mathbb{F}_q$-Frobenius não clássicas com relação ao sistema linear de cônicas.

Neste capítulo apresentaremos uma família de curvas $\mathbb{F}_q$-Frobenius não clássicas com relação a $\mathcal{D}_s$ para $s \geq 1$ diferentes das curvas de Fermat. Para o caso $s = 2$ estabeleceremos, sob certas hipóteses, condições necessárias e suficientes para que tais curvas sejam $\mathbb{F}_q$-Frobenius não clássicas.

2.1 Curvas $\mathbb{F}_q$-Frobenius não clássicas

Seja $\mathcal{X}$ uma curva plana projetiva, não singular, de grau sn definida sobre $\mathbb{F}_q$ ($q = p^h$, com $h \geq 1$), dada pela equação $F(x, y, z) = 0$, com $s(n-1) \geq 3$, $p|n-1$, $p > s^2$ e

$$F(x, y, z) = \sum_{i+j+t=s} c_{ij} x^{in} y^{jn} z^{tn}. \tag{2.1.1}$$

Nesta seção, estudaremos a $\mathbb{F}_q$-Frobenius classicalidade de $\mathcal{X}$ com relação à série linear $\mathcal{D}_s$. Note que a curva $\mathcal{X}$ pode ser vista como uma generalização da curva de Fermat, isto é, a curva dada por $ax^n + by^n = z^n$ com $ab \neq 0$. Para investigarmos a Frobenius classicalidade de $\mathcal{X}$, precisaremos dos dois resultados seguintes.

Lema 2.1.1. *Sejam $\mathcal{F}$, $\mathcal{G}$, $\mathcal{H}$ três curvas planas, $b > 0$ um inteiro e $P \in \mathcal{F}$ um ponto não singular. Se $I(P, \mathcal{F} \cap \mathcal{G}) \geq b$ e $I(P, \mathcal{F} \cap \mathcal{H}) \geq b$, então $I(P, \mathcal{H} \cap \mathcal{G}) \geq b$.*

Demonstração. Segue de [25, Lema 1.3.8] (embora o resultado referido seja para curvas sobre o corpo $\mathbb{C}$ dos números complexos, a prova continua válida para curvas sobre corpos de característica positiva). □

Lema 2.1.2. *Seja $\mathcal{X}$ a curva dada por (2.1.1). Então para todos os pontos $P = (a : b : c) \in \mathcal{X}$ tais que $abc \neq 0$, a curva $\mathcal{H}_P^s$ s-osculadora a $\mathcal{X}$ em P é uma curva irredutível dada por $H(x, y, z) = 0$, onde*

$$H(x, y, z) = \sum_{i+j+t=s} c_{ij} (a^{id} b^{jd} c^{td})^{p^v} x^i y^j z^t, \tag{2.1.2}$$

$n = dp^v + 1$ e $mdc(p, d) = 1$. Além disto, se $s > 1$, temos que $\mathcal{X}$ é não clássica com relação a $\mathcal{D}_s$, mas é clássica com relação a $\mathcal{D}_i$, para $i \in \{1, ..., s-1\}$.

Demonstração. Seja $f(x, y) = F(x, y, 1)$. Note que $f(x, y) = 0$ pode ser escrito como

$$\sum_{0 \leq i+j \leq s} c_{ij} (x^{id} y^{jd})^{p^v} x^i y^j = 0 \tag{2.1.3}$$

no corpo de funções $\mathbb{K}(\mathcal{X})$, e o Teorema 1.2.10 implica que $\mathcal{X}$ é não clássica com relação a $\mathcal{D}_s$. Além disto, se $(\epsilon_0, \epsilon_1, ..., \epsilon_M)$ é a sequência de $\mathcal{D}_s$-ordens de $\mathcal{X}$, temos que $\epsilon_M \geq p^v$. Tome $P = (a : b : c) \in \mathcal{X}$ com $abc \neq 0$; podemos assumir, sem perda de generalidade, que $c = 1$. Seja

$h(x,y) = H(x,y,1)$ e considere a curva $\mathcal{C} : H(x,y,z) = 0$ de grau s. Afirmamos que a curva $\mathcal{C}$ é irredutível. De fato, seja $\mathcal{G}$ o fecho projetivo da curva dada por $g(x,y) = 0$, onde

$$g(x,y) = \sum_{0 \leq i+j \leq s} c_{ij} x^i y^j.$$

Como $h(x,y) = g(a^{dp^v}x, b^{dp^v}y)$, temos que $\mathcal{G}$ e $\mathcal{C}$ são isomorfas. Além disto, como $\mathcal{X}$ é irredutível e $f(x,y) = g(x^n, y^n)$, temos que $\mathcal{G}$ é irredutível, e portanto, $\mathcal{C}$ também o é.

Agora, $f(x,y) = 0$ fornece

$$h(x,y) = h(x,y) - f(x,y) = \sum_{0 \leq i+j \leq s} c_{ij}(a^{id}b^{jd} - x^{id}y^{jd})^{p^v} x^i y^j. \tag{2.1.4}$$

Logo $v_P(\mathcal{C}) \geq p^v$, ou seja, $I(P, \mathcal{X} \cap \mathcal{C}) \geq p^v$. Seja $\mathcal{H}_P^s$ a curva s-osculadora a $\mathcal{X}$ em P. Como $\epsilon_M \geq p^v$, temos $I(P, \mathcal{X} \cap \mathcal{H}_P^s) \geq p^v$. Como $\mathcal{X}$ é não singular, pelo Lema 2.1.1 temos que $I(P, \mathcal{H}_P^s \cap \mathcal{C}) \geq p^v$. Mas $p > s^2$ e portanto $I(P, \mathcal{H}_P^s \cap \mathcal{C}) > s^2 = \deg(\mathcal{H}_P^s) \cdot \deg(\mathcal{C})$. Logo, pelo Teorema de Bézout temos que $\mathcal{C}$ e $\mathcal{H}_P^s$ têm uma componente em comum. Entretanto, $\mathcal{C}$ é irredutível e $\deg(\mathcal{H}_P^s) = \deg(\mathcal{C})$. Portanto, temos que $\mathcal{C} = \mathcal{H}_P^s$; em particular, $\mathcal{H}_P^s$ é irredutível.

Para a última afirmação, é suficiente mostrarmos que $\mathcal{X}$ é clássica com relação a $\mathcal{D}_{s-1}$. Suponha que $\mathcal{X}$ é não clássica com relação a $\mathcal{D}_{s-1}$; daí por [29, Corolário 1.9] teríamos que a multiplicidade de interseção da curva $(s-1)$-osculadora $\mathcal{H}_P^{s-1}$ a $\mathcal{X}$ em um ponto genérico P seria $I(P, \mathcal{X} \cap \mathcal{H}_P^{s-1}) \geq p$. Vimos que $I(P, \mathcal{X} \cap \mathcal{H}_P^s) \geq p^v$. Novamente, como $\mathcal{X}$ é não singular, pelo Lema 2.1.1 temos que $I(P, \mathcal{H}_P^s \cap \mathcal{H}_P^{s-1}) \geq p > s^2 > s(s-1) = \deg(\mathcal{H}_P^s) \cdot \deg(\mathcal{H}_P^{s-1})$. Logo, pelo Teorema de Bézout $\mathcal{H}_P^{s-1}$ é uma componente de $\mathcal{H}_P^s$, um absurdo, uma vez que $\mathcal{H}_P^s$ é irredutível. □

Segue agora o principal resultado desta seção.

Teorema 2.1.3. *Seja $\mathcal{X}$ a curva dada por (2.1.1). Então $\Phi_q(P) \in \mathcal{H}_p^s$ para infinitos pontos $P \in \mathcal{X}$ se e somente se $n = (p^h - 1)/(p^v - 1)$ e $c_{i,j} \in \mathbb{F}_{p^v}$ para todo i, j, onde $q = p^h$, $h > v$, $v|h$, e $\mathcal{H}_p^s$ é a curva s-osculadora a P em $\mathcal{X}$.*

Demonstração. Como $p|n-1$, temos que $n = dp^v + 1$ para certos inteiros positivos v, d, com $\mathrm{mdc}(p,d) = 1$. Suponhamos que $\Phi_q(P) \in \mathcal{H}_P^s$ para infinitos pontos $P \in \mathcal{X}$. Tendo em vista o Lema 2.1.2, temos que isto é equivalente a dizermos que para infinitos pontos $P = (a : b : 1) \in \mathcal{X}$ com $ab \neq 0$, temos

$$\sum_{0 \leq i+j \leq s} c_{ij}(a^{id}b^{jd})^{p^v} a^{iq} b^{jq} = 0.$$

Sendo assim, a função $g(x,y)$ é identicamente nula no corpo de funções de $\mathcal{X}$, onde

$$g(x,y) = \sum_{0 \leq i+j \leq s} c_{ij}(x^{id}y^{jd})^{p^v} x^{iq} y^{jq}.$$

Em outras palavras, $f(x,y)|g(x,y)$, onde $f(x,y) = F(x,y,1)$. Como $dp^v + q = n + q - 1$, temos que

$$g(x,y) = \sum_{0 \le i+j \le s} c_{ij} x^{i(n+q-1)} y^{j(n+q-1)}.$$

Note que $v < h$, pois caso contrário teríamos $n + q - 1 = dp^v + p^h = p^h(dp^{v-h} + 1)$, e $g(x,y) = l(x,y)^{p^h}$, onde

$$l(x,y) = \sum_{0 \le i+j \le s} \eta_{ij} x^{i(dp^{v-h}+1)} y^{j(dp^{v-h}+1)},$$

com $\eta_{ij} = c_{ij}^{1/p^h}$ para todo i,j. Mas $f(x,y)$ é irredutível, e portanto teríamos $f(x,y)|l(x,y)$, que é uma contradição, uma vez que $h > 1$ e portanto $\deg(l(x,y)) < \deg(f(x,y))$ Assim, temos que $n + q - 1 = dp^v + p^h = p^v(d + p^{h-v})$, e $g(x,y) = r(x,y)^{p^v}$, onde

$$r(x,y) = \sum_{0 \le i+j \le s} \eta_{ij} x^{i(d+p^{h-v})} y^{j(d+p^{h-v})},$$

com $\eta_{ij} = c_{ij}^{1/p^v}$ para todo i,j. Pela irredutibilidade de $f(x,y)$, temos que $f(x,y)|r(x,y)$.

Afirmação: O fecho projetivo $\mathcal{R}$ da curva dada por $r(x,y) = 0$ é não singular.

Assumindo a afirmação, temos que $r(x,y)$ é irredutível, e portanto $f(x,y) = r(x,y)$. Assim $d + p^{h-v} = n$ e logo $n + q - 1 = p^v n \Longrightarrow n(p^v - 1) = p^h - 1$. Além disso, $c_{ij} = \eta_{ij}$ para todo i,j, ou seja, $c_{ij} \in \mathbb{F}_{p^v}$.

Prova da afirmação: Suponha que $\mathcal{R}$ possui um ponto singular $P = (a : b : c)$. Primeiro, suponha que $abc \neq 0$. Podemos assumir que $c = 1$. Seja $k = d + p^{h-v}$. Daí temos $r(a,b) = r_x(a,b) = r_y(a,b) = 0$, isto é

$$\begin{aligned}
\sum_{0 \le i+j \le s} \eta_{ij} a^{ik} b^{jk} &= 0 \\
s\eta_{s0} a^{(s-1)k} + (s-1)\eta_{(s-1)1} a^{(s-2)k} b^k + \ldots + 2\eta_{20} a^k + \eta_{11} b^k + \eta_{10} &= 0 \\
\eta_{(s-1)1} a^{(s-1)k} + \ldots + s\eta_{0s} b^{(s-1)k} + \ldots + \eta_{11} a^k + 2\eta_{02} b^k + \eta_{01} &= 0,
\end{aligned}$$

onde $r_x(x,y)$ e $r_y(x,y)$ são as derivadas parciais do polinômio $r(x,y)$ com relação a x e a y, respectivamente. Elevando os dois lados de cada igualdade acima a p^v obtemos

$$\begin{aligned}
\sum_{0 \le i+j \le s} c_{ij} a^{ikp^v} b^{jkp^v} &= 0 \\
sc_{s0} a^{(s-1)kp^v} + (s-1)c_{(s-1)1} a^{(s-2)kp^v} b^{kp^v} + \ldots + 2c_{20} a^{kp^v} + c_{11} b^{kp^v} + c_{10} = &= 0 \\
c_{(s-1)1} a^{(s-1)kp^v} + \ldots + sc_{0s} b^{(s-1)kp^v} + \ldots + c_{11} a^{kp^v} + 2c_{02} b^{kp^v} + c_{01} &= 0,
\end{aligned}$$

e logo $(a^{\frac{kp^v}{n}} : b^{\frac{kp^v}{n}} : 1)$ é um ponto singular de $\mathcal{X}$, uma contradição.

Agora, sem perda de generalidade, suponhamos que $a = 0$. Assim temos $bc \neq 0$ e portanto

podemos supor $P = (0 : b : 1)$. De $r(0, b) = r_x(0, b) = r_y(0, b)$ obtemos

$$\begin{aligned} \eta_{0s}b^{sk} + \eta_{0(s-1)}b^{(s-1)k} + ... + \eta_{02}b^{2k} + \eta_{01}b^k + \eta_{00} &= 0 \\ s\eta_{0s}b^{(s-1)k} + (s-1)\eta_{0(s-1)}b^{(s-2)k} + ... + 2\eta_{02}b^k + \eta_{01} &= 0. \end{aligned}$$

Elevando os dois lados de cada igualdade acima a p^v obtemos

$$\begin{aligned} c_{0s}(b^{kp^v})^s + c_{0(s-1)}(b^{kp^v})^{s-1} + ... + c_{02}(b^{kp^v})^2 + c_{01}(b^{kp^v}) + c_{00} &= 0 \\ sc_{0s}(b^{kp^v})^{s-1} + (s-1)c_{0(s-1)}(b^{kp^v})^{s-2} + ... + 2c_{02}(b^{kp^v}) + c_{01} &= 0, \end{aligned}$$

e neste caso também temos que $(0 : b^{\frac{kp^v}{n}} : 1)$ é um ponto singular de $\mathcal{X}$, contradizendo a não singularidade da mesma. Portanto a afirmação está provada.

Reciprocamente, se $n = (p^h - 1)/(p^v - 1)$ e $c_{i,j} \in \mathbb{F}_{p^v}$ para todo i, j, com $h > v$, $v|h$, temos que $n + q - 1 = np^v$. Logo $g(x, y) = f(x, y)^{p^v} = 0$, e portanto o resultado segue do Lema 2.1.2. □

Corolário 2.1.4. *Suponha que $\mathcal{X}$ é dada por (2.1.1), com $n = (p^h - 1)/(p^v - 1)$ e $c_{i,j} \in \mathbb{F}_{p^v}$ para todo i, j, onde $h > v$, $v|h$. Então $\mathcal{X}$ é $\mathbb{F}_q$-Frobenius não clássica com relação a $\mathcal{D}_s$.*

Demonstração. Pelo Teorema 2.1.3, temos que $\Phi_q(P) \in \mathcal{H}_P^s$ para infinitos pontos $P \in \mathcal{X}$. Isto significa que para infinitos pontos $P \in \mathcal{X}$, o ponto $\Phi_q(\phi_s(P))$ pertence ao hiperplano osculador a $\phi_s(\mathcal{X})$ em P. Como para um ponto ordinário $P \in \mathcal{X}$ as $(\mathcal{D}_s, P)$-ordens são $\epsilon_0, ..., \epsilon_M$, temos pelo Teorema 1.2.4 que isto é equivalente a

$$\det \begin{pmatrix} f_0^q & \cdots & f_M^q \\ f_0 & \cdots & f_M \\ D_\tau^{(\epsilon_1)} f_0 & \cdots & D_\tau^{(\epsilon_1)} f_M \\ \vdots & \ddots & \vdots \\ D_\tau^{(\epsilon_{M-1})} f_0 & \cdots & D_\tau^{(\epsilon_{M-1})} f_M \end{pmatrix} = 0,$$

onde τ é uma variável separante de $\mathbb{F}_q(\mathcal{X})$. Assim, temos que $\nu_i > \epsilon_i$ para algum $i = 1, ..., M-1$. Portanto $\mathcal{X}$ é $\mathbb{F}_q$-Frobenius não clássica para $\mathcal{D}_s$. □

Observação 2.1.5. *No corolário anterior, vimos que caso $\mathcal{X}$ seja tal que $\Phi_q(P) \in \mathcal{H}_P^s$ para infinitos $P \in \mathcal{X}$, temos que $\mathcal{X}$ é $\mathbb{F}_q$-Frobenius não clássica com relação a $\mathcal{D}_s$. A recíproca nem sempre é verdadeira; podemos ter que $\mathcal{X}$ é $\mathbb{F}_q$-Frobenius não clássica com relação a $\mathcal{D}_s$ com sequência de ordens $\mathbb{F}_q$-Frobenius $(\nu_0, ..., \nu_{M-1}) = (\epsilon_0, ..., \epsilon_{M-1})$. Neste caso, teremos $\Phi_q(P) \in \mathcal{H}_P^s$ apenas para um número finito de pontos de $\mathcal{X}$ (os pontos do suporte do divisor de Frobenius S).*

Como mencionamos na introdução deste capítulo, se uma curva de grau $d < q/15$ atingir a cota (2.0.4), então tal curva é $\mathbb{F}_q$-Frobenius não clássicas com relação a $\mathcal{D}_2$. O próximo teorema ilustra como algumas destas curvas podem ser explicitamente construidas.

Teorema 2.1.6. *Seja $\mathcal{C}$ uma curva não singular de grau s, definida sobre $\mathbb{F}_{p^v}$, com $p \nmid s-1$, dada por $G(x,y,z) = 0$, onde*

$$G(x,y,y) = \sum_{i+j+t=s} c_{ij} x^i y^j z^t, \tag{2.1.5}$$

tal que $\mathcal{C}$ atinge a cota (2.0.4) e não possui nenhum ponto $\mathbb{F}_{p^v}$-racional tal que $xyz = 0$. Seja $\mathcal{X}$ a curva de grau $d = sn$ dada por $F(x,y,z) := G(x^n, y^n, z^n) = 0$, onde $n = \frac{p^h-1}{p^v-1}$, com $h > v$ e $v|h$. Então $\mathcal{X}$ possui $d(d+q-1)/2$ pontos $\mathbb{F}_q$-racionais, onde $q = p^h$. Em outras palavras, a curva $\mathcal{X}$ atinge a cota (2.0.4).

Demonstração. Seja $N : \mathbb{F}_q \longrightarrow \mathbb{F}_{p^v}$ a aplicação norma definida por $\alpha \longmapsto \alpha^n$. Sabemos que para todo $\beta \in \mathbb{F}_{p^v}^*$, existem n elementos distintos $\beta' \in \mathbb{F}_q^*$ tais que $N(\beta') = \beta$. Seja $Q = (a : b : c) \in \mathcal{C}$ um ponto $\mathbb{F}_{p^v}$-racional. Como $\mathcal{C}$ não possui pontos $\mathbb{F}_{p^v}$-racionais com $xyz = 0$, podemos supor sem perda de generalidade que $c = 1$. Assim, se $\alpha, \beta \in \mathbb{F}_q$ são tais que $\alpha^n = a$ e $\beta^n = b$, temos que $P = (\alpha : \beta : 1)$ é um ponto $\mathbb{F}_q$-racional de $\mathcal{X}$. Portanto, temos que a todo ponto $\mathbb{F}_{p^v}$-racional de $\mathcal{C}$ estão associados n^2 pontos $\mathbb{F}_q$-racionais de $\mathcal{X}$. Como $\mathcal{C}$ atinge a cota (2.0.4), temos que $\mathcal{C}$ possui $s(s+p^v-1)/2$ pontos $\mathbb{F}_{p^v}$-racionais. Portanto, existem pelo menos $n^2 s(s+p^v-1)/2$ pontos $\mathbb{F}_q$-racionais em $\mathcal{X}$.

Agora, afirmamos que $\mathcal{X}$ é $\mathbb{F}_q$-Frobenius classica com relação $\mathcal{D}_1$. De fato, suponha que $\mathcal{X}$ é $\mathbb{F}_q$-Frobenius não clássica; em particular, pela Proposição 1.3.2, temos que $\mathcal{X}$ é não classica e assim, por um resultado de Pardini [26, Corolário 2.2], temos que $p|(sn-1)$. Como $p|n-1$, concluímos que $p|(s-1)n$, uma contradição. Portanto, por (2.0.4) temos

$$N_q \leq \frac{sn(sn+q-1)}{2} = \frac{s}{2}\cdot\left(\frac{(q-1)^2}{(p^v-1)^2}s + \frac{(q-1)^2}{(p^v-1)}\right) = \frac{s}{2}\cdot\frac{(q-1)^2}{(p^v-1)^2}\cdot(s+p^v-1) = \frac{sn^2(s+p^v-1)}{2}.$$

Logo, $\mathcal{X}$ atinge a cota (2.0.4). □

Podemos usar o Teorema 2.1.6 para construirmos curvas de grau $d < q/15$ definidas sobre $\mathbb{F}_q$ que atingem a cota (2.0.4)(e tais curvas serão $\mathbb{F}_q$-Frobenius não clássicas com relação a $\mathcal{D}_2$).

Por exemplo, vejamos o caso $s = 2$: é fácil contruir uma cônica irredutível $\mathcal{C}$ definida sobre $\mathbb{F}_{p^v}$ tal que $\mathcal{C}$ não possui pontos $\mathbb{F}_{p^v}$-racionais com $xyz = 0$. Como $\mathcal{C}$ é irredutível, temos que $\mathcal{C}$ possui $p^v + 1$ pontos $\mathbb{F}_{p^v}$-racionas, ou seja, $\mathcal{C}$ atinge a cota (2.0.4). Portanto, existem vários exemplos de cônicas que podem fazer o papel da curva $\mathcal{C}$ do Teorema 2.1.6. Logo, pelo mesmo teorema, obtemos diversos exemplos de curvas ($\mathbb{F}_q$-Frobenius não clássicas com relação a $\mathcal{D}_2$) de grau $2n < q/15$ que atingem a cota (2.0.4). Na próxima seção, iremos mais adiante na investigação do caso $s = 2$.

2.2 O caso $s = 2$

Se $s = 1$, a curva $\mathcal{X}$ dada por uma equação do tipo (2.1.1) é a curva de Fermat dada por $ax^n + by^n = z^n$, e suas classicalidade e $\mathbb{F}_q$-Frobenius classicalidade com relação à série linear $\mathcal{D}_1$

foram estudadas em [11] e [12]. Nesta seção, estudaremos o caso $s = 2$, ou seja, estudaremos a classicalidade e a $\mathbb{F}_q$-Frobenius classicalidade da curva $\mathcal{X}$ de grau $2n$ dada por $F(x, y, z) = 0$, onde

$$F(x, y, z) = a_1x^{2n} + a_2x^ny^n + a_3y^{2n} + a_4x^nz^n + a_5y^nz^n + a_6z^{2n},$$

$a_i \in \mathbb{F}_q$, $i = 1, 2, 3, 4, 5, 6$, sob as hipóteses de que $\mathcal{X}$ é não singular (em particular, temos $a_1a_3a_6 \neq 0$) e $\mathcal{X}$ não é uma curva de Fermat. Ao longo desta seção, denotaremos $f(x, y) = F(x, y, 1)$. Começaremos com o seguinte resultado

Proposição 2.2.1. *Existe um ponto $P \in \mathcal{X}$ cuja sequência de $(\mathcal{D}_1, P)$-ordens é $(0, 1, n)$.*

Demonstração. Como $\mathcal{X}$ não é uma curva de Fermat, temos que a_2, a_4 e a_5 não são todos nulos. Então, sem perda de generalidade, podemos supor que $a_2 \neq 0$. Tome um ponto $P = (u : 0 : 1) \in \mathcal{X}$. Daí, temos que $f(u, 0) = 0$, ou seja,

$$a_1u^{2n} + a_4u^n + a_6 = 0$$

e a reta tangente a $\mathcal{X}$ em P é dada por $l_P : x - uz = 0$. Agora, $f(u, y) = y^nt(y)$, onde $t(y) = a_2u^n + a_5 + a_3y^n$.

Note que como $\mathcal{X}$ é irredutível, $t(y) \neq 0$. Logo, se $a_2u^n + a_5 = 0$, temos que $a_3, a_5 \neq 0$ e $I(P, l_P \cap \mathcal{X}) = 2n$ e se $a_2u^n + a_5 \neq 0$, temos que $I(P, l_P \cap \mathcal{X}) = n$, pois neste caso, $t(0) \neq 0$. Sendo assim, o problema se resume a encontrarmos um ponto $P = (u : 0 : 1) \in \mathcal{X}$ com $a_2u^n + a_5 \neq 0$.

Suponha que não existem tais pontos. Daí, se u é uma raiz do polinômio $g(\lambda) = a_1\lambda^{2n} + a_4\lambda^n + a_6 = 0$, temos que $a_2u^n + a_5 = 0$. Logo, a equação $a_1x^2 + a_4x + a_6 = 0$ tem uma raiz dupla $\alpha = -a_5/a_2$, o que significa que

$$a_4^2 - 4a_1a_6 = 0, \qquad a_1a_5^2 - a_2a_4a_5 + a_2^2a_6 = 0. \tag{2.2.1}$$

Das equações (2.2.1), obtemos

$$\det \begin{pmatrix} a_1 & a_2/2 & a_4/2 \\ a_2/2 & a_3 & a_5/2 \\ a_4/2 & a_5/2 & a_6 \end{pmatrix} = 0,$$

que é uma contradição, uma vez que a cônica definida por $a_1x^2 + a_2xy + a_3y^2 + a_4x + a_5y + 1 = 0$ é irredutível (tal fato segue da irredutibilidade de $\mathcal{X}$). □

Proposição 2.2.2. *Suponha que $p > 2$. Então $\mathcal{X}$ é clássica com relação a $\mathcal{D}_1$; consequentemente, $\mathcal{X}$ é $\mathbb{F}_q$-Frobenius clássica com relação a $\mathcal{D}_1$.*

Demonstração. Suponha que $\mathcal{X}$ é não clássica com relação a $\mathcal{D}_1$. Como $\mathcal{X}$ é não singular, por [26, Corolário 2.2], temos que $p|(2n - 1)$. Por outro lado, pela Proposição 2.2.1, existe $P \in \mathcal{X}$ tal que sua sequência de $(\mathcal{D}_1, P)$-ordens é $(0, 1, n)$. Assim, pela Proposição 1.2.7, $p|n(n - 1)$;

portanto, temos que $p|n$, contradizendo a irredutibilidade de $\mathcal{X}$. Logo, $\mathcal{X}$ é clássica com relação a $\mathcal{D}_1$. Por [14, Proposição 1], temos também que $\mathcal{X}$ é $\mathbb{F}_q$-Frobenius clássica para $\mathcal{D}_1$. □

No restante desta seção, vamos supor que $p > 7$ e $n > 2$. Vamos agora estudar a classicalidade da curva $\mathcal{X}$ com relação ao sistema linear $\mathcal{D}_2$. Mais precisamente, provaremos o seguinte teorema.

Teorema 2.2.3. *Se $\mathcal{X}$ for não clássica com relação a $\mathcal{D}_2$, então $p|(n-1)(2n-1)$. Além disto, se $p|n-1$, a recíproca é verdadeira.*

O caso $p|2n-1$ mais sutil, e será discutido na subseção 2.2.1. Agora, para provarmos o Teorema 2.2.3, precisaremos dos seguintes lemas.

Lema 2.2.4. *Se $\mathcal{X}$ é não clássica com relação a $\mathcal{D}_2$, então $p|(n-1)(n+1)(n-2)(2n-1)$.*

Demonstração. Pela Proposição 2.2.1, existe $P \in \mathcal{X}$ com sequência de $(\mathcal{D}_1, P)$-ordens $(0, 1, n)$, ou seja, $0, 1$ e n são todas as possíveis multiplicidades de interseção de $\mathcal{X}$ com uma reta de $\mathbb{P}^2(\mathbb{K})$. Logo, como a dimensão (projetiva) de $\mathcal{D}_2$ é 5, temos que existem 6 possíveis multiplicidades de interseção de $\mathcal{X}$ com uma cônica em $\mathbb{P}^2(\mathbb{K})$. Portanto estas possibilidades são $0, 1, 2, n, n+1$ e $2n$. Em outras palavras, a sequência de $(\mathcal{D}_2, P)$-ordens é $(0, 1, 2, n, n+1, 2n)$. Assim, o resultado segue pela Proposição 1.2.7. □

Lema 2.2.5. *Se $p|(n+1)(n-2)$, então $\mathcal{X}$ é clássica com relação a $\mathcal{D}_2$.*

Demonstração. Como $\mathcal{X}$ é clássica com relação a $\mathcal{D}_1$, temos que a sequência de $\mathcal{D}_2$-ordens de $\mathcal{X}$ é dada por $(0, 1, 2, 3, 4, \epsilon)$, onde $\epsilon \geq 5$. Se $\epsilon > 5$, por [11, Proposição 2], temos que $\epsilon = p^d$, para algum $d > 0$. Suponhamos que $\epsilon > 5$.

Primeiro, assuma que $p|n-2$. Daí $n = mp^v + 2$, para certos $m, v > 0$, com mdc(m, p)=1. Assim, como $f(x, y) = 0$ em $\mathbb{K}(\mathcal{X})$, temos

$$\begin{aligned} 0 &= f(x,y) = a_1x^{2n} + a_2x^ny^n + a_3y^{2n} + a_4x^n + a_5y^n + a_6 \Longrightarrow \\ 0 &= a_1(x^{2m})^{p^v}x^4 + a_2(x^my^m)^{p^v}x^2y^2 + a_3(y^{2m})^{p^v}y^4 + a_4(x^m)^{p^v}x^2 + a_5(y^m)^{p^v}y^2 + a_6. \end{aligned}$$

Seja $P = (u : w : 1) \in \mathcal{X}$ com $uw \neq 0$ e considere o fecho projetivo $\mathcal{Q}_P \subset \mathbb{P}^2(\mathbb{K})$ da curva dada por

$$r(x,y) = a_1(u^{2m})^{p^v}x^4 + a_2(u^mw^m)^{p^v}x^2y^2 + a_3(w^{2m})^{p^v}y^4 + a_4(u^m)^{p^v}x^2 + a_5(w^m)^{p^v}y^2 + a_6 = 0$$

A curva $\mathcal{Q}_P$ é uma quártica, pois caso contrário $\mathcal{X}$ seria uma curva de Fermat. Afirmamos que $\mathcal{Q}_P$ é irredutível. De fato, para todo $P = (u : w : 1)$ com $uw \neq 0$, a curva $\mathcal{Q}_P$ é isomorfa à curva $\mathcal{C}$ dada por

$$a_1x^4 + a_2x^2y^2 + a_3y^4 + a_4x^2z^2 + a_5y^2z^2 + a_6z^4 = 0,$$

onde o isomorfismo é dado por $(x : y : z) \mapsto (u^{mp^v}x : w^{mp^v}y : z)$, e a curva $\mathcal{C}$ é não singular. Com efeito, suponha que $\mathcal{C}$ possui um ponto singular $P = (a : b : c)$. Podemos supor sem perda

de generalidade que $c \neq 0$ e assim, podemos assumir que $P = (a : b : 1)$. Daí temos

$$\begin{aligned} a_1a^4 + a_2a^2b^2 + a_3b^4 + a_4a^2 + a_5b^2 + a_6 &= 0 \\ 2a(2a_1a^2 + a_2b^2 + a_4) &= 0 \\ 2b(a_2a^2 + 2a_3b^2 + a_5) &= 0. \end{aligned}$$

Logo, o ponto $Q = (a^{2/n} : b^{2/n} : 1)$ satisfaz o sistema de equações

$$\begin{aligned} f(x,y) = a_1x^{2n} + a_2x^ny^n + a_3y^{2n} + a_4x^n + a_5y^n + a_6 &= 0 \\ nx^{n-1}(2a_1x^n + a_2y^n + a_4) &= 0 \\ ny^{n-1}(a_2x^n + 2a_3y^n + a_5) &= 0, \end{aligned}$$

e portanto Q é um ponto singular de $\mathcal{X}$, o que contradiz a hipótese de a curva $\mathcal{X}$ ser não singular. Logo, para todo $P = (u : w : 1) \in \mathcal{X}$ com $uw \neq 0$, no corpo de funções da curva $\mathcal{X}$ temos

$$\begin{aligned} r(x,y) &= r(x,y) - f(x,y) \\ &= a_1(u^{2m} - x^{2m})^{p^v}x^4 + a_2(u^mw^m - x^my^m)^{p^v}x^2y^2 + a_3(w^{2m} - y^{2m})^{p^v}y^4 \\ &+ a_4(u^m - x^m)^{p^v}x^2 + a_5(w^m - y^m)^{p^v}y^2. \end{aligned}$$

Assim, $v_P(r(x,y)) \geq p^v$, e portanto $I(P, \mathcal{Q}_P \cap \mathcal{X}) \geq p^v$. Seja $\mathcal{H}_P^2$ a cônica osculadora a $\mathcal{X}$ em P. Como estamos supondo $\epsilon = p^d$, temos que $I(P, \mathcal{H}_P^2 \cap \mathcal{X}) \geq p^d$. Logo, como $\mathcal{X}$ é não singular, pelo Lema 2.1.1, temos que $I(P, \mathcal{H}_P^2 \cap \mathcal{Q}_P) \geq p \geq 11 > 8 = \deg(\mathcal{H}_P^2) \cdot \deg(\mathcal{Q}_P)$. Logo pelo Teorema de Bézout, a cônica $\mathcal{H}_P^2$ é uma componente de $\mathcal{Q}_P$, uma contradição, visto que $\mathcal{Q}_P$ é irredutível. Portando $\mathcal{X}$ é clássica com relação a $\mathcal{D}_2$ quando $p|n-2$.

Suponhamos agora $p|n+1$. Existem $m, v > 0$ tais que $n = mp^v - 1$, com mdc(m,p)=1. De $f(x,y) = 0$ obtemos

$$\begin{aligned} 0 &= f(x,y)x^2y^2 \Longrightarrow \\ 0 &= a_1(x^{2m})^{p^v}y^2 + a_2(x^my^m)^{p^v}xy + a_3(y^{2m})^{p^v}x^2 + a_4(x^m)^{p^v}xy^2 + a_5(y^m)^{p^v}x^2y + a_6x^2y^2. \end{aligned}$$

Mais uma vez aqui, consideremos um ponto $P = (u : w : 1) \in \mathcal{X}$ com $uw \neq 0$ e o fecho projetivo $\mathcal{Q}_P' \subset \mathbb{P}^2(\mathbb{K})$ da curva dada por $s(x,y) = 0$, onde

$$s(x,y) = a_6x^2y^2 + a_5(w^m)^{p^v}x^2y + a_4(u^m)^{p^v}xy^2 + a_3(w^{2m})^{p^v}x^2 + a_2(u^mw^m)^{p^v}xy + a_1(u^{2m})^{p^v}y^2.$$

Note que $\mathcal{Q}_P'$ é uma quártica, uma vez que $a_6 \neq 0$. Sejam $\alpha = u^{mp^v}$ e $\beta = w^{mp^v}$. Multiplicando $s(x,y)$ por $1/\alpha^2\beta^2$, temos que $\mathcal{Q}_P'$ é o fecho projetivo da curva dada pela equação

$$a_6\frac{x^2y^2}{\alpha^2\beta^2} + a_5\frac{x^2y}{\alpha^2\beta} + a_4\frac{xy^2}{\alpha\beta^2} + a_3\frac{x^2}{\alpha^2} + a_2\frac{xy}{\alpha\beta} + a_1\frac{y^2}{\beta^2} = 0.$$

Logo $\mathcal{Q}'_P$ é isomorfa à curva $\mathcal{Y}$ dada por

$$H(x, y, z) = a_6x^2y^2 + a_5x^2yz + a_4xy^2z + a_3x^2z^2 + a_2xyz^2 + a_1y^2z^2 = 0,$$

via $(x : y : z) \mapsto (x/\alpha : y/\beta : z)$.

Assim, temos que $\mathcal{Q}'_P$ é birracionalmente equivalente à curva $\mathcal{E}$ dada por

$$a_1x^2 + a_2xy + a_3y^2 + a_4xz + a_5yz + a_6z^2 = 0.$$

De fato, como $a_1a_3a_6 \neq 0$, temos que $(1 : 0 : 0), (0 : 1 : 0), (0 : 0 : 1) \notin \mathcal{E}$. Portanto $\mathcal{Y}$ é a imagem de $\mathcal{E}$ pela transformação standart de Cremona $(x : y : z) \mapsto (yz : xz : xy)$. Como $\mathcal{E}$ é irredutítvel (pois se fosse redutível, $\mathcal{X}$ também seria), temos que $\mathcal{Q}'_P$ é irredutível.

Agora, para todo $P = (u : w : 1) \in \mathcal{X}$ com $uw \neq 0$, no corpo de funções da curva $\mathcal{X}$ temos

$$\begin{aligned} s(x,y) &= s(x,y) - f(x,y)x^2y^2 \\ &= a_5(w^m - y^m)^{p^v}x^2y + a_4(u^m - x^m)^{p^v}xy^2 + a_3(w^{2m} - y^{2m})^{p^v}x^2 \\ &+ a_2(u^mw^m - y^my^m)^{p^v}xy + a_1(u^{2m} - x^{2m})^{p^v}y^2. \end{aligned}$$

Da última igualdade, temos que $v_P(\mathcal{Q}'_P) \geq p^v$, e portanto $I(P, \mathcal{Q}'_P \cap \mathcal{X}) \geq p^v \geq 11$. Assim, como no caso anterior, se $\mathcal{H}^2_P$ é a cônica osculadora a $\mathcal{X}$ em P, temos que $I(P, \mathcal{H}^2_P \cap \mathcal{X}) \geq p^d \geq 11$, e mais uma vez, pelo Teorema de Bézout teríamos que a cônica $\mathcal{H}^2_P$ é uma componente de $\mathcal{Q}'_P$, o que contradiz a irredutibilidade desta última. Portanto, a curva $\mathcal{X}$ é clássica. □

Lema 2.2.6. *Se $p|n - 1$, então $\mathcal{X}$ é não clássica com relação a $\mathcal{D}_2$.*

Demonstração. Suponhamos $n = mp^v + 1$, com mdc(m, p)=1. De $f(x, y) = 0$ obtemos

$$\begin{aligned} 0 &= a_1x^{2n} + a_2x^ny^n + a_3y^{2n} + a_4x^n + a_5y^n + a_6 \Longrightarrow \\ 0 &= a_1(x^{2m})^{p^v}x^2 + a_2(x^my^m)^{p^v}xy + a_3(y^{2m})^{p^v}y^2 + a_4(x^m)^{p^v}x + a_5(y^m)^{p^v}y + a_6. \end{aligned}$$

Pelo Teorema 1.2.10, temos o resultado. □

Assim, o Teorema 2.2.3 segue dos Lemas 2.2.4, 2.2.5 e 2.2.6. Estabeleceremos agora o resultado principal desta seção.

Teorema 2.2.7. *Suponha que $p \nmid 2n - 1$. Então $\mathcal{X}$ é $\mathbb{F}_q$-Frobenius não clássica com relação a $\mathcal{D}_2$ se, e somente se, $n = \frac{p^h-1}{p^v-1}$, com $h > v$, $v|h$ e $a_i \in \mathbb{F}_{p^v}$, para $i = 1, 2, 3, 4, 5, 6$.*

Demonstração. Se $p|n - 1$ e $n = \frac{p^h-1}{p^v-1}$, com $h > v$, $v|h$ e $a_i \in \mathbb{F}_{p^v}$, para $i = 1, 2, 3, 4, 5, 6$, pelo Corolário 2.1.4 aplicado a $s = 2$, temos que $\mathcal{X}$ é $\mathbb{F}_q$-Frobenius não clássica com relação a $\mathcal{D}_2$. Reciprocamente, suponhamos que $\mathcal{X}$ é $\mathbb{F}_q$-Frobenius não clássica para $\mathcal{D}_2$. Em particular, pela Proposição 1.3.9, $\mathcal{X}$ é não clássica para $\mathcal{D}_2$. Logo, pelo Teorema 2.2.3, temos que $p|n - 1$. Sejam

$(0,1,2,3,4,\epsilon)$ a sequência de $\mathcal{D}_2$-ordens de $\mathcal{X}$ e $(\nu_0,\nu_1,\nu_2,\nu_3,\nu_4)$ a sequência de $\mathbb{F}_q$-ordens de Frobenius de $\mathcal{X}$ para $\mathcal{D}_2$. Como a sequência $(\nu_0,\nu_1,\nu_2,\nu_3,\nu_4)$ é não clássica, temos

$$\det\begin{pmatrix} 1 & x^q & y^q & x^{2q} & x^qy^q & y^{2q} \\ 1 & x & y & x^2 & xy & y^2 \\ 0 & D_\tau^{(1)}(x) & D_\tau^{(1)}(y) & D_\tau^{(1)}(x^2) & D_\tau^{(1)}(xy) & D_\tau^{(1)}(y^2) \\ 0 & D_\tau^{(2)}(x) & D_\tau^{(2)}(y) & D_\tau^{(2)}(x^2) & D_\tau^{(2)}(xy) & D_\tau^{(2)}(y^2) \\ 0 & D_\tau^{(3)}(x) & D_\tau^{(3)}(y) & D_\tau^{(3)}(x^2) & D_\tau^{(3)}(xy) & D_\tau^{(3)}(y^2) \\ 0 & D_\tau^{(4)}(x) & D_\tau^{(4)}(y) & D_\tau^{(4)}(x^2) & D_\tau^{(4)}(xy) & D_\tau^{(4)}(y^2) \end{pmatrix} = 0,$$

onde τ é uma variável separante em $\mathbb{F}_q(\mathcal{X})$. Como $(0,1,2,3,4,\epsilon)$ é a sequência de $(\mathcal{D}_2,P)$-ordens para quase todo ponto $P \in \mathcal{X}$, pelo Corolário 1.2.4, temos que $\Phi_q(P)$ pertence ao hiperplano osculador a $\phi_2(\mathcal{X})$ em P para infinitos pontos $P \in \mathcal{X}$. Portanto, $\Phi_q(P) \in \mathcal{H}_P^2$ para infinitos pontos $P \in \mathcal{X}$, onde $\mathcal{H}_P^2$ é a cônica osculadora a $\mathcal{X}$ em P. Logo, pelo Teorema 2.1.3, $n = \frac{p^h-1}{p^v-1}$, com $h > v$, $v|h$ e $a_i \in \mathbb{F}_{p^v}$, para $i = 1,2,3,4,5,6$. □

2.2.1 O caso $p|2n-1$

Seja $\mathcal{X}$ a curva plana não singular definida por $F(x,y,z) = 0$ como na seção 2.2. Provamos que se $\mathcal{X}$ é não clássica com relação a $\mathcal{D}_2$, então $p|(n-1)(2n-1)$, e a recíproca é verdadeira se $p|n-1$. Nesta seção, discutiremos a classicalidade de $\mathcal{X}$ para o caso $p|2n-1$. Suponhamos então $2n = mp^v + 1$ para certos $m, v > 0$ com $\mathrm{mdc}(m,p) = 1$. Existem alguns casos para os quais a curva $\mathcal{X}$ é não clássica com relação a $\mathcal{D}_2$. Listemos alguns destes casos:

- A curva $\mathcal{X}$ dada por $F(x,y,z) = 0$, onde $F(x,y,z) = a_1x^{2n} + a_3y^{2n} + a_4x^nz^n + a_6z^{2n}$ (ou seja, $a_2 = a_5 = 0$), é não clássica para $\mathcal{D}_2$. De fato, temos em $\mathbb{K}(\mathcal{X})$ que

$$\begin{aligned} 0 &= a_1x^{2n} + a_3y^{2n} + a_4x^n + a_6 \Longrightarrow \\ -a_4x^n &= a_1(x^m)^{p^v}x + a_3(y^m)^{p^v}y + a_6 \Longrightarrow \\ a_4^2(x^m)^{p^v}x &= (a_1(x^m)^{p^v}x + a_3(y^m)^{p^v}y + a_6)^2; \end{aligned}$$

  logo, pelo Teorema 1.2.10, temos que $\mathcal{X}$ é não clássica para D_2.

- A curva $\mathcal{X}$ dada por $F(x,y,z) = 0$, onde $F(x,y,z) = a_1x^{2n} + a_2x^ny^n + a_3y^{2n} + a_6z^{2n}$ (ou seja, $a_4 = a_5 = 0$), é não clássica para $\mathcal{D}_2$. De fato,

$$\begin{aligned} 0 &= a_1x^{2n} + a_2x^ny^n + a_3y^{2n} + a_6 \Longrightarrow \\ -a_2x^ny^n &= a_1(x^m)^{p^v}x + a_3(y^m)^{p^v}y + a_6 \Longrightarrow \\ a_2^2(x^my^m)^{p^v}xy &= (a_1(x^m)^{p^v}x + a_3(y^m)^{p^v}y + a_6)^2, \end{aligned}$$

  e novamente temos o resultado pelo Teorema 1.2.10 para este caso.

- O mesmo argumento dos itens acima mostra que a curva dada por $a_1x^{2n}+a_3y^{2n}+a_5y^nz^n+a_6z^{2n}=0$ também é não clássica para $\mathcal{D}_2$.

Por outro lado, existem casos para os quais $\mathcal{X}$ é classica para $\mathcal{D}_2$. Por exemplo, considere a curva $\mathcal{X}_1$ dada por $H(x,y,z)=0$, onde $H(x,y,z)=x^{2n}+x^ny^n+y^{2n}+x^nz^n+y^nz^n+z^{2n}$. A curva $\mathcal{X}_1$ é não singular se $p\geq 7$ (veja o Lema 2.3.1 na próxima seção). Seja $h(x,y)=H(x,y,1)$. Como $h(x,y)=0$ em $\mathbb{K}(\mathcal{X})$, temos

$$\begin{aligned}(x^{2n}+x^ny^n+y^{2n}+x^n+y^n+1)(x^{2n}-x^ny^n+y^{2n}-x^n+y^n+1) &= 0\\ \Longrightarrow x^{4n}+x^{2n}y^{2n}+y^{4n}+x^{2n}+3y^{2n}+1 &= -2(y^{3n}+y^n).\end{aligned}$$

Elevando ao quadrado os dois lados da última igualdade e fazendo algumas manipulações, obtemos

$$\begin{aligned}0 &= x^{8n}+y^{8n}+2x^{6n}y^{2n}+2x^{2n}y^{6n}+3x^{4n}y^{4n}+2x^{6n}+2y^{6n}+8x^{2n}y^{4n}+8x^{4n}y^{2n}\\ &+ 3x^{4n}+3y^{4n}+8x^{2n}y^{2n}+2x^{2n}+2y^{2n}+1,\end{aligned} \tag{2.2.2}$$

isto é,

$$\begin{aligned}0 &= (x^{4m})^{p^v}x^4+(y^{4m})^{p^v}y^4+(\eta x^{3m}y^m)^{p^v}x^3y+(\eta x^my^{3m})^{p^v}xy^3+(\xi x^{2m}y^{2m})^{p^v}x^2y^2\\ &+ (\eta x^{3m})^{p^v}x^3+(\eta y^{3m})^{p^v}y^3+(\eta^3x^my^{2m})^{p^v}xy^2+(\eta^3x^{2m}y^m)^{p^v}x^2y+(\xi x^{2m})^{p^v}x^2\\ &+ (\xi y^{2m})^{p^v}y^2+(\eta^3x^my^m)^{p^v}xy+(\eta x^m)^{p^v}x+(\eta y^m)^{p^v}y+1,\end{aligned} \tag{2.2.3}$$

onde $\eta=2^{1/p^v}$ e $\xi=3^{1/p^v}$. Seja $P=(u:w:1)\in\mathcal{X}_1$ com $uw\neq 0$ e seja $\mathcal{Q}_P$ o fecho projetivo da quártica dada por $r(x,y)=0$, onde

$$\begin{aligned}r(x,y) &= (u^{4m})^{p^v}x^4+(w^{4m})^{p^v}y^4+(\eta u^{3m}w^m)^{p^v}x^3y+(\eta u^mw^{3m})^{p^v}xy^3+(\xi u^{2m}w^{2m})^{p^v}x^2y^2\\ &+ (\eta u^{3m})^{p^v}x^3+(\eta w^{3m})^{p^v}y^3+(\eta^3u^mw^{2m})^{p^v}xy^2+(\eta^3u^{2m}w^m)^{p^v}x^2y+(\xi u^{2m})^{p^v}x^2\\ &+ (\xi w^{2m})^{p^v}y^2+(\eta^3u^mw^m)^{p^v}xy+(\eta u^m)^{p^v}x+(\eta w^m)^{p^v}y+1.\end{aligned} \tag{2.2.4}$$

A quártica $\mathcal{Q}_P$ é isomorfa à curva $\mathcal{G}$ dada por $G(x,y,z)=0$, onde

$$\begin{aligned}G(x,y,z) &= x^4+y^4+2x^3y+2xy^3+3x^2y^2+2x^3z+2y^3z+8xy^2z+8x^2yz\\ &+ 3x^2z^2+3y^2z^2+8xyz^2+2xz^3+2yz^3+z^4,\end{aligned} \tag{2.2.5}$$

e o isomorfismo é dado por $(x:y:z)\mapsto(u^{mp^v}x:w^{mp^v}y:z)$. Afirmamos que $\mathcal{G}$ é irredutível. De fato, observe primeiro que um ponto de interseção de duas componentes de uma curva redutível é um ponto singular da mesma. Não é difícil mostrar que os pontos singulares de $\mathcal{G}$ são $P_1=(-1:-1:1)$, $P_2=(1:-1:1)$ e $P_3=(-1:1:1)$, e tais pontos são singularidades ordinárias duplas. Como P_1, P_2 e P_3 não são colineares, temos que $\mathcal{G}$ não pode ser a união de uma reta com uma cúbica. Como $\mathcal{G}$ possui apenas singularidades duplas, se $\mathcal{G}$ fosse a união de duas cônicas,

pelo Teorema de Bézouts teríamos que $\mathcal{G}$ possui pelo menos quatro singularidades ordinárias ou pelo menos uma singularidade não ordinária. Logo, $\mathcal{G}$ é irredutível, e portanto, $\mathcal{Q}_P$ também é.

Portanto, pelos mesmos argumentos da prova do Lema 2.2.5, temos que $I(P, \mathcal{Q}_P \cap \mathcal{X}_1) \geq p$. Suponha que $\mathcal{X}_1$ seja não clássica para $\mathcal{D}_2$. Como $\mathcal{X}_1$ é classica para $\mathcal{D}_1$, pela Proposição 1.2.9, a sequência de $\mathcal{D}_2$-ordens de $\mathcal{X}$ é $(0, 1, 2, 3, 4, p^l)$, para algum $l > 0$. Portanto, se $\mathcal{H}_P^2$ é a cônica osculadora a $\mathcal{X}_1$ em P, temos $I(P, \mathcal{H}_P^2 \cap \mathcal{X}_1) \geq p^l$. Pelo Lema 2.1.1, $I(P, \mathcal{H}_P^2 \cap \mathcal{Q}_p) \geq p > 8 = \deg(\mathcal{H}_P^2) \cdot \deg(\mathcal{Q}_p)$, contradizendo o Teorema de Bézout (uma vez que $\mathcal{Q}_P$ é irredutível). Logo $\mathcal{X}_1$ é classica para $\mathcal{D}_2$.

Apesar de existirem exemplos de curvas não clássicas com relação a $\mathcal{D}_2$ quando $p|2n-1$, cálculos realizados para inúmeros casos particulares usando o software "Magma Calculator"nos levam a suspeitar que não existem curvas Frobenius não clássicas com relação a $\mathcal{D}_2$ neste caso, ou seja, suspeitamos que a hipótese "$p \nmid 2n-1$"do Teorema 2.2.7 pode ser dispensada.

2.3 Curvas não clássicas

Na seção 2.1, apresentamos condições para que uma curva $\mathcal{X} : F(x, y, z) = 0$ seja $\mathbb{F}_q$-Frobenius não clássica com relação a $\mathcal{D}_s$ sob certas hipóteses, dentre as quais, $\mathcal{X}$ ser não singular e $p|n-1$. Pela Proposição 1.3.9, os candidatos naturais a serem curvas $\mathbb{F}_q$-Frobenius não clássicas para $\mathcal{D}_s$ são as curvas não clássicas para a mesma série linear. Nesta seção, exibiremos uma condição necessária para que um certo exemplo de curva seja não clássico, e consequentemente, $\mathbb{F}_q$-Frobenius não clássico para $\mathcal{D}_s$.

Considere a curva $\mathcal{X}_1 : H(x, y, z) = 0$ de grau sn, onde $s(n-1) \geq 3$, $p \nmid n$ e

$$H(x, y, z) := \sum_{i+j+t=s} x^{in} y^{jn} z^{tn}. \tag{2.3.1}$$

Lema 2.3.1. *A curva $\mathcal{X}_1$ é não singular se $p \geq \binom{s+2}{2}$.*

Demonstração. Note que $H(x, y, z) = G_s(x^n, y^n, z^n)$, onde

$$G_s(x, y, z) = \sum_{i+j+k=s} x^i y^j z^k.$$

Como $H(x, y, z)$ é um polinômio simétrico (ou seja, $H(x, y, z)$ é invariante pela permutação de suas coordenadas projetivas x, y e z), podemos trabalhar apenas com os pontos afins. Seja $h(x, y) = H(x, y, 1)$ e suponha que exista um ponto singular $P = (a, b)$ na curva afim dada por $h(x, y) = 0$. Daí temos

$$\begin{aligned} 0 &= G_s(a^n : b^n : 1) \\ 0 &= h_x(a, b) = (G_s)_x(a^n : b^n : 1) n a^{n-1} \\ 0 &= h_y(a, b) = (G_s)_y(a^n : b^n : 1) n b^{n-1}, \end{aligned}$$

onde F_x e F_y denotam as derivadas parciais de um polinômio F com relação às variáveis x e y, respectivamente.

Se $ab \neq 0$, temos que $h(a,b) = (G_s)_x(a^n : b^n : 1) = (G_s)_y(a^n : b^n : 1) = 0$, e portanto $(a^n : b^n : 1)$ é um ponto singular da curva $\mathcal{F}$ dada por $G_s(x : y : z) = 0$. Mas como $p \geq \binom{s+2}{2} = (s+2)(s+1)/2$, temos que $p \nmid (s+2)(s+1)$ e portanto por [32, Teorema 1], a curva $\mathcal{F}$ é não singular; logo este caso não ocorre.

Suponhamos então sem perda de generalidade $b = 0$. Neste caso, temos que $a \neq 0$ e, desta forma, temos $0 = h(a,0) = h_x(a,b)$. Mas

$$h(x,0) = \frac{(x^n)^{s+1} - 1}{x^n - 1},$$

e portanto a é uma raiz $n(s+1)$-ésima de 1, e estas são todas distintas, uma vez que p não divide $n(s+1)$. Logo, a equação $h_x(a,b) = 0$ fornece uma contradição. □

Lema 2.3.2. *Suponha que $p \geq \binom{s+2}{2}$. Os pontos $P \in \mathcal{X}_1$ com $xyz = 0$ são pontos de inflexão, e sua sequência de $(\mathcal{D}_1, P)$-ordens é $(0,1,n)$.*

Demonstração. Suponhamos sem perda de generalidade que o ponto é $P = (a : 0 : 1)$. Daí temos que $a^{sn} + a^{(s-1)n} + \ldots + a^n + 1 = 0$ e a reta tangente a $\mathcal{X}_1$ em P é dada por $l_P : x - az = 0$. Um cálculo simples verifica que $h(a,y) = y^n t(y)$, onde $y \nmid t(y)$. Portanto, temos que $I(P, l_P \cap \mathcal{X}) = n$. □

Daremos agora uma condição necessária para que $\mathcal{X}_1$ seja $\mathbb{F}_q$-Frobenius não clássica com relação a $\mathcal{D}_s$.

Proposição 2.3.3. *Suponha que $p \geq \binom{s+2}{2}$. Se $\mathcal{X}_1$ é não clássica com relação a $\mathcal{D}_s$, então p divide $\prod_{r=1}^{s} \prod_{t=-s}^{s-r} (rn + t)$.*

Demonstração. Se P é um ponto $\mathcal{X}_1$ com $xyz = 0$, o Lema 2.3.2 diz que 0, 1 e n são todas as possíveis multiplicidades de interseção de $\mathcal{X}_1$ com uma reta em $\mathbb{P}^2(\mathbb{K})$. Logo, temos que o conjunto de todas as possíveis multiplicidades de interseção de $\mathcal{X}_1$ com uma curva plana de grau s é dado por $\{an + b \mid a + b \leq s\}$. Pela Proposição 1.2.7, segue o resultado. □

Capítulo 3

Pontos racionais em curvas sobre corpos finitos

3.1 Introdução

Como mencionado no capítulo 1, em [29] Störh e Voloch obtiveram cotas para o número de pontos racionais em uma curva $\mathcal{X}$ definida sobre um corpo finito $\mathbb{F}_q$ através de funções que se anulam nos pontos $P \in \mathcal{X}$ tais que a imagem pelo mapa $\mathbb{F}_q$-Frobenius do ponto $\phi(P)$ pertence ao hiperplano osculador a $\phi(\mathcal{X})$ em P, onde $\phi : \mathcal{X} \longrightarrow \mathbb{P}^n(\mathbb{K})$ é um morfismo definido sobre $\mathbb{F}_q$, com $n \geq 2$.

Sejam u, m dois inteiros tais que $m > u$ e $\text{mdc}(u, m) = 1$, e sejam $\Phi_{q^m}, \Phi_{q^u} : \phi(\mathcal{X}) \longrightarrow \phi(\mathcal{X})$ respectivamente os $\mathbb{F}_{q^m}$ e $\mathbb{F}_{q^u}$ mapas de Frobenius definidos em $\phi(\mathcal{X})$. Inspirados na idéia de [29], neste trabalho obteremos novas cotas maximais através de funções que se anulam nos pontos $P \in \mathcal{X}$ tais que existe uma reta em $\mathbb{P}^n(\mathbb{K})$ passando por $\Phi_{q^u}(\phi(P))$ e $\Phi_{q^m}(\phi(P))$ que intersecta o espaço $(n-2)$-osculador a $\phi(\mathcal{X})$ em P.

3.2 O divisor (q^u, q^m)-Frobenius

Sejam $\mathcal{X}$ uma curva não singular irredutível de gênero g definida sobre $\mathbb{F}_q$ e $\phi = (f_0 : ... : f_n) \in \mathbb{P}^n(\mathbb{F}_q(\mathcal{X}))$ $(n \geq 2)$ um morfismo definido sobre $\mathbb{F}_q$, ou seja, $\phi = (f_0 : ... : f_n) : \mathcal{X} \longrightarrow \mathbb{P}^n(\mathbb{K})$, com $f_0, ..., f_n \in \mathbb{F}_q(\mathcal{X})$ tais que $\{f_0, ..., f_n\}$ é linearmente independente sobre $\mathbb{K}$. Sejam $P \in \mathcal{X}$, $t \in \mathbb{K}(\mathcal{X})$ um parâmetro local em P e $e_P = -min\{v_P(f_0), ..., v_P(f_n)\}$. Sabemos pelo Teorema 1.2.3, supondo que $e_P = 0$ (multiplicando cada f_i por t^{e_P}), que o plano $(n-2)$-osculador a $\phi(\mathcal{X})$ em P é gerado pelos pontos

$$((D_t^{(j_i)} f_0)(P) : ... : (D_t^{(j_i)} f_n)(P)), \quad i = 0, ..., n-2,$$

onde $D_t^{(l)}$ é a l-ésima derivada de Hasse com relação a t e j_i é a i-ésima $(\mathcal{D}, P)$-ordem de $\mathcal{X}$, onde $\mathcal{D}$ é a série linear correspondente ao morfismo ϕ.

O nosso objetivo é contar os pontos P de $\mathcal{X}$ tais que exista uma reta em $\mathbb{P}^n(\mathbb{K})$ passando por

$\Phi_{q^u}(\phi(P))$ e $\Phi_{q^m}(\phi(P))$ que intersecte o plano $(n-2)$-osculador a $\phi(\mathcal{X})$ em P. Dado $P \in \mathcal{X}$, existe uma reta em $\mathbb{P}^n(\mathbb{K})$ passando por $\Phi_{q^u}(\phi(P))$ e $\Phi_{q^m}(\phi(P))$ que intersecta o plano $(n-2)$-osculador a $\phi(\mathcal{X})$ em P se, e somente se,

$$\det \begin{pmatrix} f_0(P)^{q^m} & f_1(P)^{q^m} & \dots & f_n(P)^{q^m} \\ f_0(P)^{q^u} & f_1(P)^{q^u} & \dots & f_n(P)^{q^u} \\ (D_t^{(j_0)}f_0)(P) & (D_t^{(j_0)}f_1)(P) & \dots & (D_t^{(j_0)}f_n)(P) \\ \vdots & \vdots & \dots & \vdots \\ (D_t^{(j_{n-2})}f_0)(P) & (D_t^{(j_{n-2})}f_1)(P) & \dots & (D_t^{(j_{n-2})}f_n)(P) \end{pmatrix} = 0.$$

Tal fato motiva o estudo deste determinante num ponto genérico de $\mathcal{X}$. Considere $t \in \mathbb{F}_q(\mathcal{X})$ uma variável separante. Estudaremos as funções do tipo

$$A_t^{\rho_0,\dots,\rho_{n-2}}(f_0,\dots,f_n) := \det \begin{pmatrix} f_0^{q^m} & f_1^{q^m} & \dots & f_n^{q^m} \\ f_0^{q^u} & f_1^{q^u} & \dots & f_n^{q^u} \\ D_t^{(\rho_0)}f_0 & D_t^{(\rho_0)}f_1 & \dots & D_t^{(\rho_0)}f_n \\ \vdots & \vdots & \dots & \vdots \\ D_t^{(\rho_{n-2})}f_0 & D_t^{(\rho_{n-2})}f_1 & \dots & D_t^{(\rho_{n-2})}f_n \end{pmatrix} \tag{3.2.1}$$

em $\mathbb{F}_q(\mathcal{X})$, onde $\rho_0, \rho_1, \dots, \rho_{n-2}$ são inteiros não negativos. Começaremos mostrando que funções não nulas dadas por (3.2.1) de fato existem em $\mathbb{F}_q(\mathcal{X})$.

Proposição 3.2.1. *Existem inteiros não negativos $\kappa_0, \dots, \kappa_{n-2}$, com $\kappa_0 < \dots < \kappa_{n-2}$, tais que a função $A_t^{\kappa_0,\dots,\kappa_{n-2}}(f_0,\dots,f_n)$ não se anula em $\mathcal{X}$.*

Demonstração. Como ϕ é não degenerado, observe que $(f_0^{q^u} : \dots : f_n^{q^u}) \neq (f_0^{q^m} : \dots : f_n^{q^m})$. Sejam $\nu_0 < \nu_1 < \dots < \nu_{n-1}$ as ordens $\mathbb{F}_{q^u}$-Frobenius de $\mathcal{X}$ com relação a ϕ. Se as $n+1$-uplas $(f_0^{q^m},\dots,f_n^{q^m}), (f_0^{q^u},\dots,f_n^{q^u}), (D_t^{(\nu_i)}f_0,\dots,D_t^{(\nu_i)}f_n)$, com $i = 0,\dots,n-2$, são linearmente independentes sobre $\mathbb{F}_q$, o resultado está provado. Caso contrário, seja $I \in \{0,\dots,n-2\}$ o menor inteiro tal que a $n+1$-upla $(f_0^{q^m},\dots,f_n^{q^m})$ seja combinação linear de $(f_0^{q^u},\dots,f_n^{q^u})$ e $(D_t^{(\nu_i)}f_0,\dots,D_t^{(\nu_i)}f_n)$, para $i = 0,\dots,I$. Suponha que existe $I_2 \in \{I+1,\dots,n-1\}$ tal que $(f_0^{q^m},\dots,f_n^{q^m})$ seja uma combinação linear de $(f_0^{q^u},\dots,f_n^{q^u})$ e $(D_t^{(\nu_i)}f_0,\dots,D_t^{(\nu_i)}f_n)$, com $i \in \{0,\dots,I_2\}\backslash\{I\}$. Daí temos que o conjunto formado por $(f_0^{q^u},\dots,f_n^{q^u})$ e $(D_t^{(\nu_i)}f_0,\dots,D_t^{(\nu_i)}f_n)$, para $i = 0,\dots,I_2$, é linearmente dependente, o que contradiz a definição da sequência $\{\nu_0,\dots,\nu_{n-1}\}$. Portanto, temos que $\{\kappa_0,\dots,\kappa_{n-2}\} = \{\nu_0,\dots,\nu_{n-1}\}\backslash\{\nu_I\}$ são tais que $A_t^{\kappa_0,\dots,\kappa_{n-2}}(f_0,\dots,f_n) \neq 0$. □

Escolheremos sempre os inteiros $0 \leq \kappa_0 < \dots < \kappa_{n-2}$ minimalmente na ordem lexicográfica, isto é, κ_0 é o menor inteiro tal que as $n+1$-uplas $(f_0^{q^u},\dots,f_n^{q^u})$, $(f_0^{q^m},\dots,f_n^{q^m})$ e $(D_t^{(\kappa_0)}f_0,\dots,D_t^{(\kappa_0)}f_n)$ são linearmente independentes sobre $\mathbb{F}_q$ e, se $\kappa_0,\dots,\kappa_{l-1}$ são conhecidos, então κ_l é o menor inteiro tal que as $n+1$-uplas $(f_0^{q^u},\dots,f_n^{q^u})$, $(f_0^{q^m},\dots,f_n^{q^m})$,...,$(D_t^{(\kappa_i)}f_0,\dots,D_t^{(\kappa_i)}f_n)$, para $i = 0,\dots,l$, são linearmente independentes sobre $\mathbb{F}_q$.

Repare que na proposição anterior, poderiamos ter feito o mesmo procedimento usando as

ordens $\mathbb{F}_{q^m}$-Frobenius de $\mathcal{X}$ com relação a ϕ, digamos $\mu_0, ...\mu_{n-1}$. Assim, temos o seguinte resultado.

Corolário 3.2.2. *Existem inteiros positivos I e J tais que $\{\kappa_0, ..., \kappa_{n-2}\} = \{\nu_0, ..., \nu_{n-1}\}\backslash\{\nu_I\} = \{\mu_0, ..., \mu_{n-1}\}\backslash\{\mu_J\}$. Em particular, temos que $\kappa_i \geq max\{\nu_i, \mu_i\}$ para todo $i = 0, ..., n-2$.*

A próxima proposição mostra que a minimalidade dos inteiros $\kappa_0, ..., \kappa_{n-2}$ vale em um sentido ainda mais forte.

Proposição 3.2.3. *Se $m_0, ..., m_s$ são inteiros com $0 \leq m_0 < ... < m_s$ tais que as linhas da matriz*

$$\begin{pmatrix} f_0^{q^m} & f_1^{q^m} & ... & f_n^{q^m} \\ f_0^{q^u} & f_1^{q^u} & ... & f_n^{q^u} \\ D_t^{(m_0)} f_0 & D_t^{(m_0)} f_1 & ... & D_t^{(m_0)} f_n \\ \vdots & \vdots & ... & \vdots \\ D_t^{(m_s)} f_0 & D_t^{(m_s)} f_1 & ... & D_t^{(m_s)} f_n \end{pmatrix} \tag{3.2.2}$$

são linearmente independentes, então $\kappa_i \leq m_i$ para cada $i = 0, ..., s$.

Demonstração. Pela definição de κ_i, para $i = 0, ..., n-2$, as $\kappa_s + 2$ linhas da matriz

$$\begin{pmatrix} f_0^{q^m} & f_1^{q^m} & ... & f_n^{q^m} \\ f_0^{q^u} & f_1^{q^u} & ... & f_n^{q^u} \\ D_t^{(0)} f_0 & D_t^{(0)} f_1 & ... & D_t^{(0)} f_n \\ D_t^{(1)} f_0 & D_t^{(1)} f_1 & ... & D_t^{(1)} f_n \\ \vdots & \vdots & ... & \vdots \\ D_t^{(\kappa_s - 1)} f_0 & D_t^{(\kappa_s - 1)} f_1 & ... & D_t^{(\kappa_s - 1)} f_n \end{pmatrix}$$

geram um subespaço vetorial de $\mathbb{K}(\mathcal{X})^{n+1}$ de dimensão $s+2$. Como as linhas da matriz (3.2.2) geram um subespaço de dimensão $s+3$ de $\mathbb{K}(\mathcal{X})^{n+1}$, temos que $\kappa_s - 1 < m_s$, ou seja, $\kappa_s \leq m_s$. □

Proposição 3.2.4. *(a) Se $g_i = \sum a_{ij} f_j$ com $(a_{ij}) \in GL_{n+1}(\mathbb{F}_q)$, então*

$$A_t^{\kappa_0, ..., \kappa_{n-2}}(g_0, ..., g_n) = \det(a_{ij}) A_t^{\kappa_0, ..., \kappa_{n-2}}(f_0, ..., f_n).$$

(b) Se $h \in \mathbb{F}_q(\mathcal{X})^*$, então

$$A_t^{\kappa_0, ..., \kappa_{n-2}}(hf_0, ..., hf_n) = h^{q^m + q^u + n - 1} A_t^{\kappa_0, ..., \kappa_{n-2}}(f_0, ..., f_n).$$

(c) Se x é outra variável separante de $\mathbb{F}_q(\mathcal{X})$, então

$$A_x^{\kappa_0, ..., \kappa_{n-2}}(f_0, ..., f_n) = \left(\frac{dt}{dx}\right)^{\kappa_0 + \kappa_1 + ... + \kappa_{n-2}} A_t^{\kappa_0, ..., \kappa_{n-2}}(f_0, ..., f_n).$$

Demonstração. (a) Segue facilmente usando propriedades de determinante, e não depende da minimalidade dos κ_i.

(b) Pela regra do produto da derivada de Hasse,

$$D_t^{(\kappa_i)}(hf_j) = h \cdot D_t^{(\kappa_i)} f_j + \sum_{s=1}^{\kappa_i} (D_t^{(s)} h) \cdot (D_t^{(\kappa_i - s)} f_j).$$

Na primeira e segunda linhas de $A_t^{\kappa_0,\ldots,\kappa_{n-2}}(hf_0, ..., hf_n)$, todo elemento tem respectivamente h^{q^m} e h^{q^u} como fator. A terceira linha é dada por

$$(h \cdot D_t^{(\kappa_0)} f_0 + \cdots, ..., h \cdot D_t^{(\kappa_0)} f_r + \cdots),$$

onde as reticências em cada entrada indicam termos que são coordenadas de um vetor w que é uma combinação linear dos vetores $(D_t^{(c)} f_0, ..., D_t^{(c)} f_r)$ com $0 \leq c < \kappa_0$. Pela minimalidade de κ_0, temos que w pode ser omitido do determinante, e novamente h é um fator da segunda linha. Repetindo os mesmos argumentos para as demais linhas de $A_t^{\kappa_0,\ldots,\kappa_{n-2}}(hf_0, ..., hf_n)$, temos o resultado.

(c) Por [18, Teorema 5.82], para cada $i = 0, ...n-2$ temos que

$$D_x^{(\kappa_i)} f = \left(\frac{dt}{dx}\right)^{\kappa_i} D_t^{(\kappa_i)} f + \sum_{j=1}^{\kappa_i - 1} d_j D_t^{(j)} f.$$

onde $d_1, .., d_{\kappa_i - 1} \in \mathbb{F}_q(\mathcal{X})$ que são polinômios nas indeterminadas $D_x^{(j)} t$ para $1 \leq j \leq \kappa_i$. Usando novamente a regra do produto da derivada de Hasse, o resultado segue por procedimento análogo ao do ítem (b).

□

Pela Proposição 3.2.4, a sequência de inteiros $(\kappa_0, ..., \kappa_{n-2})$ está totalmente determinada pela morfismo ϕ, e portanto também pela série $\mathcal{D}$ associada ao mesmo. Chamaremos os inteiros $0 \leq \kappa_0 < ... < \kappa_{n-2}$ de ordens (q^u, q^m)-Frobenius de $\mathcal{X}$ com relação a ϕ (ou com relação a $\mathcal{D}$). Quando $\kappa_i = i$ para $i = 0, 1, ..., n-2$, diremos que $\mathcal{X}$ é (q^u, q^m)-Frobenius clássica com relação ao morfismo ϕ (à série linear $\mathcal{D}$), ou simplesmente que $\mathcal{X}$ é (q^u, q^m)-Frobenius clássica. Se $\kappa_i \neq i$ para algum i, diremos que $\mathcal{X}$ é (q^u, q^m)-Frobenius não clássica. Convém observarmos que todas as definições e resultados obtidos até aqui valem mesmo se ϕ não for birracional.

Definição 3.2.5. *O divisor (q^u, q^m)-Frobenius de $\mathcal{D}$ é definido por*

$$T_{u,m} = div(A_t^{\kappa_0,\ldots,\kappa_{n-2}}(f_0, ..., f_n)) + (\kappa_0 + \kappa_1 + ... + \kappa_{n-2}) div(dt) + (q^m + q^u + n - 1)E,$$

onde t é uma variável separante de $\mathbb{F}_q(\mathcal{X})$ e $E = \sum_{P \in \mathcal{X}} e_P P$, com $e_P = -min\{v_P(f_0), ..., v_P(f_n)\}$.

Novamente pela Proposição 3.2.4, o divisor $T_{u,m}$ está bem definido e depende apenas do morfismo ϕ (da série linear $\mathcal{D}$). Além disso, o grau de $T_{u,m}$ é

$$\deg(T_{u,m}) = (\kappa_0 + \kappa_1 + ... + \kappa_{n-2})(2g-2) + (q^m + q^u + n - 1)d, \tag{3.2.3}$$

onde $d = \deg(\mathcal{D}) = \deg(E)$.

Proposição 3.2.6. *Sejam $\phi = (f_0 : ... : f_n) : \mathcal{X} \longrightarrow \mathbb{P}^n(\mathbb{K})$ um morfismo definido sobre $\mathbb{F}_q$ e $\kappa_0, ..., \kappa_{n-2}$ as ordens (q^u, q^m)-Frobenius associadas a ϕ. Suponha que $\kappa_0 > 0$. Então $\mathbb{F}_q(x,y) \subseteq \mathbb{F}_q(\mathcal{X}) \subseteq \mathbb{E}$, onde $\mathbb{F}_q(x,y)$ é o corpo de funções da curva definida por $h(x,y) = 0$, para*

$$h(x,y) = \frac{(x^{q^m} - x)(y^{q^u} - y) - (y^{q^m} - y)(x^{q^u} - x)}{(x^{q^2} - x)(y^q - y) - (y^{q^2} - y)(x^q - x)}, \tag{3.2.4}$$

[1]

e $\mathbb{E}$ é o fecho Galoisiano de $\mathbb{F}_q(x,y)/\mathbb{F}_q(x)$. Em particular, existe um número finito de curvas (a menos de transformação birracional) que admitem um modelo projetivo para o qual $\kappa_0 > 0$.

Demonstração. Dividindo todas as funções coordenadas de ϕ por f_0, podemos assumir que $\phi = (1 : f_1 : f_2, ... : f_n)$. Além disso, a menos de uma mudança de coordenadas projetivas sobre $\mathbb{F}_q$, podemos assumir que $x := f_1$ é uma variável separante de $\mathbb{F}_q(\mathcal{X})/\mathbb{F}_q$. Sejam $v_1 = (1, f_1, ..., f_n), v_2 = (1, f_1^{q^u}, ..., f_n^{q^u})$ e $v_3 = (1, f_1^{q^m}, ..., f_n^{q^m})$. Como ϕ é não degenerado, sabemos que v_1, v_2 e v_3 são dois a dois linearmente independentes sobre $\mathbb{K}$. Suponhamos que $\kappa_0 > 0$. Pela definição de κ_0, temos então que o conjunto $\{v_1, v_2, v_3\}$ é linearmente dependente sobre $\mathbb{K}(\mathcal{X})$, ou seja, a matriz

$$U = \begin{pmatrix} 1 & f_1^{q^m} & f_2^{q^m} & ... & f_n^{q^m} \\ 1 & f_1^{q^u} & f_2^{q^u} & ... & f_n^{q^u} \\ 1 & f_1 & f_2 & ... & f_n \end{pmatrix}$$

tem posto igual a 2. Sendo assim, todas as matrizes 3×3 obtidas escolhendo-se três colunas distintas de U têm determinante nulo. Em particular, temos para cada $i = 2, ..., n$ que $g(x, f_i) = 0$, onde

$$g(x, f_i) = (x^{q^m} - x)(f_i^{q^u} - f_i) - (f_i^{q^m} - f_i)(x^{q^u} - x). \tag{3.2.5}$$

Por [4, Teorema 1.1], para cada i temos que $g(x, f_i) = g_1(x, f_i)h(x, f_i)$, onde $g_1(x, f_i) = (x^{q^2} - x)(f_i^q - f_i) - (f_i^{q^2} - f_i)(x^q - x)$ é o produto de todos os fatores lineares não nulos de $\mathbb{F}_q[x, f_i]$ e $h(x, f_i)$ é irredutível. Como o morfismo ϕ é não degenerado, temos que $g_1(x, f_i) \neq 0$. Portanto $h(x, f_i) = 0$ em $\mathbb{K}(\mathcal{X})$, e assim, para quaisquer $i, j \in \{2, ..., n\}$, os elementos f_i e f_j são conjugados sobre $\mathbb{F}_q(x)$. Logo, $\mathbb{F}_q(\mathcal{X}) \subseteq \mathbb{E}$. □

Seja $\mathcal{F}$ o fecho projetivo da curva dada pela equação $h(x,y) = 0$, onde $h(x,y)$ é definido por (3.2.4). A curva $\mathcal{F}$ é amplamente estudada em [4]; lá, dentre outras coisas, é exibida a sua

[1] Pode-se verificar que $h(x,y)$ de fato é um polinômio.

quantidade de pontos $\mathbb{F}_{q^r}$-racionais, para $r = 1, u, m, m-u$ ([4, Teorema 4.4]). Além disso, a curva $\mathcal{F}$ é não clássica com relação ao morfismo $\phi_1 = (1 : x : y) : \mathcal{X} \longrightarrow \mathbb{P}^2(\mathbb{K})$ com sequência de $\mathcal{D}_1$-ordens $(0, 1, q^u)$ ([4, Teorema 2.6]) e é a única curva simultaneamente $\mathbb{F}_{q^u}$ e $\mathbb{F}_{q^m}$-Frobenius não clássica com relação a ϕ_1 ([4, Teorema 3.4]). Assim, pela demonstração da Proposição 3.2.6 e pelo Corolário 3.2.2, temos que $\mathcal{F}$ é a única curva (q^u, q^m)-Frobenius não clássica para ϕ_1 e sua ordem (q^u, q^m)-Forbenius é $\kappa_0 = q^u$. Com estes fatos em mãos, facilmente verificamos o seguinte resultado.

Corolário 3.2.7. *Para um morfismo arbitrário $\phi : \mathcal{X} \longrightarrow \mathbb{P}^n(\mathbb{K})$ sobre $\mathbb{F}_q$, se $\kappa_0 > 0$, então $\kappa_0 = q^u$.*

Sejam $\mathcal{X}$ e ϕ como no enunciado da Proposição 3.2.6, ou seja, suponha que $\kappa_0 > 0$. Considere $\mathbb{F}_q(\mathcal{F})$ o corpo de funções de $\mathcal{F}$ sobre $\mathbb{F}_q$ e seja $s = [\mathbb{F}_q(\mathcal{X}) : \mathbb{F}_q(\mathcal{F})]$. Como todo ponto $\mathbb{F}_{q^r}$-racional de $\mathcal{X}$ está sobre um único ponto $\mathbb{F}_{q^r}$-racional de $\mathcal{F}$, temos que $N_r \leq s \cdot \#(\mathcal{F}(\mathbb{F}_{q^r}))$ para $r = 1, u, m, m-u$; em particular, por [4, Teorema 4.4], temos $N_1 = 0$. No que segue, sempre vamos supor que $\kappa_0 = 0$.

Dado um ponto $P \in \mathcal{X}$ qualquer, seja $t \in \mathbb{K}(\mathcal{X})$ um parâmetro local em P. Multiplicando cada função coordenada $f_0, ..., f_n$ de ϕ por t^{e_P}, podemos supor que $e_P = 0$, e como tal operação não altera o divisor $T_{u,m}$, temos que

$$v_P(T_{u,m}) = v_P(A_t^{\kappa_0,...,\kappa_{n-2}}(f_0, ..., f_n)) \geq 0,$$

uma vez que $v_P(div(dt)) = 0$. Em particular, temos que $T_{u,m}$ é um divisor efetivo.

Observação 3.2.8. *Note que se P é um ponto $\mathbb{F}_{q^u}$-racional ou $\mathbb{F}_{q^m}$-racional (e em particular, se P é um ponto $\mathbb{F}_q$-racional), temos que $A_t^{\kappa_0,...,\kappa_{n-2}}(f_0, ..., f_n)(P) = 0$, ou seja, todo ponto $\mathbb{F}_{q^u}$-racional e $\mathbb{F}_{q^m}$-racional pertence ao suporte de $T_{u,m}$. Além destes, o suporte de $T_{u,m}$ conta também com os pontos $\mathbb{F}_{q^{(m-u)}}$-racionais de $\mathcal{X}$, já que neste caso $f_i(P)^{q^u} = f_i(P)^{q^m}$ para $i = 0, ..., n$.*

Queremos agora estudar as propriedades de $T_{u,m}$. Nas próximas proposições, estimaremos o peso de certos tipos de pontos de $\mathcal{X}$ no divisor $T_{u,m}$.

Proposição 3.2.9. *Seja $P \in \mathcal{X}$ um ponto $\mathbb{F}_q$-racional com $(\mathcal{D}, P)$-ordens $j_0, j_1, ..., j_n$. Então*

$$v_P(T_{u,m}) \geq q^u j_1 + \sum_{i=0}^{n-2} (j_{i+2} - \kappa_i),$$

e vale a igualdade se, e somente se,

$$\det\left(\binom{j_i}{\kappa_s}\right)_{2 \leq i \leq n, 0 \leq s \leq n-2} \not\equiv 0 \mod p.$$

Demonstração. Sejam $P \in \mathcal{X}$ um ponto $\mathbb{F}_q$-racional e t um parâmetro local em P. Multiplicando todas as funções coordenadas f_i por t^{e_P}, podemos supor $e_P = 0$. Sabemos que o i-ésimo plano

osculador L_i no ponto $P \in \mathcal{X}$ é gerado pelos pontos $((D_t^{(j_s)} f_0)(P) : ... : (D_t^{(j_s)} f_n)(P))$, para $s = 0, ..., i$. Como P é um ponto $\mathbb{F}_q$-racional, temos que os planos osculadores em P estão definidos sobre $\mathbb{F}_q$. Podemos assim fazer uma mudança de coordenadas projetivas cuja imagem de L_i é $\{(x_0 : ... : x_n) \in \mathbb{P}^n(\mathbb{K}) \mid x_{i+1} = ... = x_n = 0\}$.

Logo, esta mudança de coordenadas é dada por uma matriz com coeficientes em $\mathbb{F}_q$, e portanto pelo ítem (a) da Proposição 3.2.4 podemos assumir que $f_i = t^{j_i} + ...$ é a expansão local de cada função coordenada de ϕ em P, onde todos os coeficientes desta expansão pertencem a $\mathbb{F}_q$. Dividindo todas as funções coordenadas de ϕ por f_0, podemos também supor que $f_0 = 1$. Assim $A_t^{\kappa_0,...,\kappa_{n-2}}(f_0, ..., f_n) =$

$$\det \begin{pmatrix} 1 & t^{q^m j_1} + ... & t^{q^m j_2} + ... & ... & t^{q^m j_n} + ... \\ 1 & t^{q^u j_1} + ... & t^{q^u j_2} + ... & ... & t^{q^u j_n} + ... \\ 1 & c_{10} t^{j_1 - \kappa_0} + ... & c_{20} t^{j_2 - \kappa_0} + ... & ... & c_{n0} t^{j_n - \kappa_0} + ... \\ 0 & c_{11} t^{j_1 - \kappa_1} + ... & c_{21} t^{j_2 - \kappa_1} + ... & ... & c_{n1} t^{j_n - \kappa_1} + ... \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 0 & c_{1(n-2)} t^{j_1 - \kappa_{n-2}} + ... & c_{2(n-2)} t^{j_2 - \kappa_{n-2}} + ... & ... & c_{n(n-2)} t^{j_n - \kappa_{n-2}} + ... \end{pmatrix},$$

onde $c_{is} = \binom{j_i}{\kappa_s}$. Logo $A_t^{\kappa_0,...,\kappa_{n-2}}(f_0, ..., f_n) = A_1 - A_2 + A_3$, onde A_1, A_2 e A_3 são os determinantes obtidos pelo desenvolvimento de Laplace usando a primeira coluna. Analisaremos cada um destes três determinantes.

$$A_1 = \det \begin{pmatrix} t^{q^u j_1} + ... & t^{q^u j_2} + ... & ... & t^{q^u j_n} + ... \\ c_{10} t^{j_1 - \kappa_0} + ... & c_{20} t^{j_2 - \kappa_0} + ... & ... & c_{n0} t^{j_n - \kappa_0} + ... \\ c_{11} t^{j_1 - \kappa_1} + ... & c_{21} t^{j_2 - \kappa_1} + ... & ... & c_{n1} t^{j_n - \kappa_1} + ... \\ \vdots & \vdots & \ddots & \vdots \\ c_{1(n-2)} t^{j_1 - \kappa_{n-2}} + ... & c_{2(n-2)} t^{j_2 - \kappa_{n-2}} + ... & ... & c_{n(n-2)} t^{j_n - \kappa_{n-2}} + ... \end{pmatrix}$$

$$= t^{q^u j_1 + \sum_{i=0}^{n-2} (j_1 - \kappa_i)} \cdot \det \begin{pmatrix} 1 + ... & t^{q^u (j_2 - j_1)} + ... & ... & t^{q^u (j_n - j_1)} + ... \\ c_{10} + ... & c_{20} t^{j_2 - j_1} + ... & ... & c_{n0} t^{j_n - j_1} + ... \\ c_{11} + ... & c_{21} t^{j_2 - j_1} + ... & ... & c_{n1} t^{j_n - j_1} + ... \\ \vdots & \vdots & \ddots & \vdots \\ c_{1(n-2)} + ... & c_{2(n-2)} t^{j_2 - j_1} + ... & ... & c_{n(n-2)} t^{j_n - j_1} + ... \end{pmatrix}$$

$$= t^{q^u j_1 + \sum_{i=0}^{n-2} (j_{i+2} - \kappa_i)} \cdot \det \begin{pmatrix} 1 + ... & t^{(q^u - 1)(j_2 - j_1)} + ... & ... & t^{(q^u - 1)(j_n - j_1)} + ... \\ c_{10} + ... & c_{20} + ... & ... & c_{n0} + ... \\ c_{11} + ... & c_{21} + ... & ... & c_{n1} + ... \\ \vdots & \vdots & \ddots & \vdots \\ c_{1(n-2)} + ... & c_{2(n-2)} + ... & ... & c_{n(n-2)} + ... \end{pmatrix}.$$

Daí

$$A_1 = \det\left(\binom{j_i}{\kappa_s}\right)_{2\le i\le n, 0\le s\le n-2} \cdot t^{q^u j_1 + \sum_{i=0}^{n-2}(j_{i+2}-\kappa_i)} + ..., \tag{3.2.6}$$

onde as reticências indicam os termos de grau superior em t. Analogamente, temos que

$$A_2 = t^{q^m j_1 + \sum_{i=0}^{n-2}(j_{i+2}-\kappa_i)} \cdot \det \begin{pmatrix} 1+... & t^{(q^m-1)(j_2-j_1)}+... & ... & t^{(q^m-1)(j_n-j_1)}+... \\ c_{10}+... & c_{20}+... & ... & c_{n0}+... \\ c_{11}+... & c_{21}+... & ... & c_{n1}+... \\ \vdots & \vdots & \ddots & \vdots \\ c_{1(n-2)}+... & c_{2(n-2)}+... & ... & c_{n(n-2)}+... \end{pmatrix},$$

e também

$$A_3 = t^{(q^m+q^u-1)j_1+\sum_{i=0}^{n-2}(j_{i+2}-\kappa_i)} \cdot \det \begin{pmatrix} 1+... & t^{(q^m-1)(j_2-j_1)}+... & ... & t^{(q^m-1)(j_n-j_1)}+... \\ 1+... & t^{(q^u-1)(j_2-j_1)}+... & ... & t^{(q^u-1)(j_n-j_1)}+... \\ c_{11}+... & c_{21}+... & ... & c_{n1}+... \\ \vdots & \vdots & \ddots & \vdots \\ c_{1(n-2)}+... & c_{2(n-2)}+... & ... & c_{n(n-2)}+... \end{pmatrix}.$$

Assim,

$$A_t^{\kappa_0,...,\kappa_{n-2}}(f_0,...,f_n) = A_1 - A_2 + A_3 = \det\left(\binom{j_i}{\kappa_s}\right)_{2\le i\le n, 0\le s\le n-2} \cdot t^{q^u j_1 + \sum_{i=0}^{n-2}(j_{i+2}-\kappa_i)} + ...,$$

onde novamente temos que as reticências indicam os termos de grau superior em t. Como $v_P(T_{u,m}) = v_P(A_t^{\kappa_0,...,\kappa_{n-2}}(f_0,...,f_n))$, temos o resultado. □

Proposição 3.2.10. *Seja $P \in \mathcal{X}$ um ponto arbitrário com $(\mathcal{D}, P)$-ordens $j_0, j_1, ..., j_n$. Então*

$$v_P(T_{u,m}) \ge \sum_{i=0}^{n-2}(j_i - \kappa_i),$$

e se

$$\det\left(\binom{j_i}{\kappa_s}\right)_{0\le i,s\le n-2} \equiv 0 \mod p,$$

vale a desigualdade estrita.

Demonstração. Podemos novamente supor $e_P = 0$. Como na prova da Proposição 3.2.9, aplicamos uma transformação projetiva de $\mathbb{P}^n(\mathbb{K})$ obtendo $g_i = \sum_{j=0}^{n} a_{ij} f_j$ tal que $g_i = t^{j_i} + ...$ é a expansão local de g_i em P (onde t é um parâmetro local em P). Mas desta vez, como P é arbitrário, temos que $a_{ij} \in \mathbb{K}$ para todo i, j, mas estes coeficientes não são necessariamente elementos de $\mathbb{F}_q$; assim não podemos aplicar o ítem (a) da Proposição 3.2.4. Sejam então $b_i = \sum a_{ij} f_j^{q^m}$ e

$h_i = \sum a_{ij} f_j^{q^u}$. Temos

$$A_t^{\kappa_0,\ldots,\kappa_{n-2}}(f_0,\ldots,f_n)\det(a_{ij}) = \det\begin{pmatrix} b_0 & b_1 & \ldots & b_n \\ h_0 & h_1 & \ldots & h_n \\ D_t^{(\kappa_0)}g_0 & D_t^{(\kappa_0)}g_1 & \ldots & D_t^{(\kappa_0)}g_n \\ D_t^{(\kappa_1)}g_0 & D_t^{(\kappa_1)}g_1 & \ldots & D_t^{(\kappa_1)}g_n \\ \vdots & \vdots & \ddots & \vdots \\ D_t^{(\kappa_{n-2})}g_0 & D_t^{(\kappa_{n-2})}g_1 & \ldots & D_t^{(\kappa_{n-2})}g_n \end{pmatrix} = \sum_{i=0}^{n}(-1)^i b_i d_i,$$

onde

$$d_i = \sum_{k\in\{0,\ldots,n\}\setminus\{i\}} (-1)^{\alpha_{ki}} h_k l_{ki}, \qquad \alpha_{ki} = \begin{cases} k, & \text{se } k < i \\ k+1, & \text{se } k > i \end{cases}$$

e l_{ki} são os menores $(n-1)\times(n-1)$ obtidos pela matriz acima, omitindo-se suas duas primeiras linhas e as k-ésima e i-ésima colunas. Logo

$$A_t^{\kappa_0,\ldots,\kappa_{n-2}}(f_0,\ldots,f_n)\det(a_{ij}) = \sum_{i=0}^{n}\sum_{k\neq i}(-1)^{i+\alpha_{ki}} b_i h_k l_{ki}.$$

Como $f_0,\ldots,f_n$ são regulares em P, temos que $v_P(b_i) \geq 0$ para todo i e $v_P(h_k) \geq 0$ para todo k. Portanto, temos que $v_P(T_{u,m}) \geq min\{v_P(l_{ki}) \mid i = 0,\ldots,n,\ k \in \{0,\ldots,n\}\setminus\{i\}\}$. Por procedimento análogo ao cálculo de (3.2.6), temos que

$$\begin{aligned} l_{ki} &= \det\left(\binom{j_r}{\kappa_s} t^{j_r-\kappa_s} + \cdots\right) \\ &= \det\left(\binom{j_r}{\kappa_s}\right) t^{j_0+\ldots+j_n-j_k-j_i-\kappa_0-\ldots-\kappa_{n-2}} + \cdots \end{aligned} \tag{3.2.7}$$

onde $0 \leq s \leq n-2$ e $r \in \{0,\ldots,n\}\setminus\{k,i\}$, e assim

$$v_P(l_{ki}) \geq j_0 + \ldots + j_n - j_k - j_i - \kappa_0 - \ldots - \kappa_{n-2}. \tag{3.2.8}$$

Os menores valores possíveis para o lado direito de (3.2.8) são obtidos quando $k,\ i \in \{n-1, n\}$. Logo, temos a desigualdade enunciada. Por fim, se

$$\det\left(\binom{j_i}{\kappa_s}\right)_{0\leq i,s\leq n-2} \equiv 0 \mod p,$$

temos que $v_P(l_{n-1,n}) > j_0 + \ldots + j_{n-2} - \kappa_0 - \ldots - \kappa_{n-2}$. □

Proposição 3.2.11. *Seja $P \in \mathcal{X}$ um ponto $\mathbb{F}_{q^r}$-racional, para $r = u, m$, com $(\mathcal{D}, P)$-ordens $j_0, j_1, \ldots, j_n$. Então*

$$v_P(T_{u,m}) \geq max\left\{\sum_{i=1}^{n-1}(j_i - \kappa_{i-1}), 1\right\}.$$

Além disso, se

$$\det\left(\binom{j_i}{\kappa_s}\right)_{1\leq i\leq n-1, 0\leq s\leq n-2} \equiv 0 \mod p \quad e \quad \sum_{i=1}^{n-1}(j_i-\kappa_{i-1})\geq 1$$

vale a desigualdade estrita. Em particular, se $\mathcal{X}$ for (q^u,q^m)-Frobenius clássica com relação a ϕ, temos que $v_P(T_{u,m})\geq j_{n-1}\geq n-1$.

Demonstração. Suponhamos, sem perda de generalidade, que P é um ponto $\mathbb{F}_{q^u}$-racional (o caso em que P é $\mathbb{F}_{q^m}$-racional é análogo). Seja t um parâmetro local em P. Novamente, multiplicando todas as funções coordenadas f_i por t^{e_P}, podemos supor que $e_P=0$. Como na prova da Proposição 3.2.9, aplicamos uma transformação projetiva de $\mathbb{P}^n(\mathbb{K})$ obtendo $g_i=\sum_{j=0}^n a_{ij}f_j$ tal que $g_i=t^{j_i}+...$ é a expansão local de g_i em P. Como P é $\mathbb{F}_{q^u}$-racional, os planos osculadores em P estão definidos sobre $\mathbb{F}_{q^u}$. Assim, todos os coeficientes desta expansão são elementos de $\mathbb{F}_{q^u}$ e a matriz (a_{ij}) da transformação projetiva correspondente é tal que $a_{ij}\in\mathbb{F}_{q^u}$. Para cada $i=0,...,n$, seja então $b_i=\sum a_{ij}f_j^{q^m}$. Temos

$$A_t^{\kappa_0,...,\kappa_{n-2}}(f_0,...,f_n)\det(a_{ij})=\det\begin{pmatrix} b_0 & b_1 & ... & b_n\\ g_0^{q^u} & g_1^{q^u} & ... & g_n^{q^u}\\ D_t^{(\kappa_0)}g_0 & D_t^{(\kappa_0)}g_1 & ... & D_t^{(\kappa_0)}g_n\\ D_t^{(\kappa_1)}g_0 & D_t^{(\kappa_1)}g_1 & ... & D_t^{(\kappa_1)}g_n\\ \vdots & \vdots & \ddots & \vdots\\ D_t^{(\kappa_{n-2})}g_0 & D_t^{(\kappa_{n-2})}g_1 & ... & D_t^{(\kappa_{n-2})}g_n \end{pmatrix}=\sum_{i=0}^n(-1)^i b_i d_i,$$

onde

$$d_i=\sum_{k\in\{0,...,n\}\setminus\{i\}}(-1)^{\alpha_{ki}}g_k^{q^u}l_{ki},\qquad \alpha_{ki}=\begin{cases} k, & \text{se } k<i\\ k+1, & \text{se } k>i\end{cases}$$

e os l_{ki} são como na prova da Proposição 3.2.10. Novamente neste caso, como $v_P(b_i)\geq 0$ para todo i, temos que $v_P(T_{u,m})\geq min\{v_P(g_k^{q^u}l_{ki})\mid i=0,...,n,\ k\in\{0,...,n\}\setminus\{i\}\}$. Uma vez que $v_P(g_k^{q^u})=q^u j_k$ e por (3.2.8) $v_P(l_{ki})\geq j_0+...+j_n-j_k-j_i-\kappa_0-...-\kappa_{n-2}$, temos que

$$v_P(g_k^{q^u}l_{ki})\geq q^u j_k+j_0+...+j_n-j_k-j_i-\kappa_0-...-\kappa_{n-2} \tag{3.2.9}$$

para todo $i\in\{0,...,n\}$ e $k\in\{0,...,n\}\setminus\{i\}$. Observe que na soma do lado direito de (3.2.9), o menor valor é obtido quando $k=0$ e $i=n$. Como, por (3.2.7), $v_P(l_{0n})>\sum_{i=1}^{n-1}(j_i-\kappa_{i-1})$ caso $p|\det\left(\binom{j_i}{\kappa_s}\right)$, com $1\leq i\leq n-1$ e $0\leq s\leq n-2$, temos o resultado. □

Vamos agora estimar o peso dos pontos $\mathbb{F}_{q^{(m-u)}}$-racionais de $\mathcal{X}$ em $T_{u,m}$. Começaremos pelo caso de uma curva plana, que nos ajudará posteriormente ao estudo do caso geral.

Lema 3.2.12. *Seja $\mathcal{X}$ um modelo projetivo não singular de uma curva plana irredutível dada por $f(x,y)=0$ definida sobre $\mathbb{F}_q$, com $q=p^h$, e seja $T_{u,m}$ o divisor (q^u,q^m)-Frobenius associado*

ao morfismo $\phi_1 = (1 : x : y) : \mathcal{X} \longrightarrow \mathbb{P}^2(\mathbb{K})$. *Se* $P \in \mathcal{X}$ *é um ponto* $\mathbb{F}_{q^{(m-u)}}$*-racional, então* $v_P(T_{u,m}) \geq q^u$.

Demonstração. Se t é uma variável separante de $\mathbb{F}_q(\mathcal{X})$, temos por (3.2.1) que

$$A_t^0(1, x, y) = g(x, y) = (x^{q^m} - x)(y^{q^u} - y) - (y^{q^m} - y)(x^{q^u} - x). \tag{3.2.10}$$

Como visto na demonstração da Proposição 3.2.6, temos $g(x, y) = g_1(x, y)h(x, y)$, onde

$$g_1(x, y) = \prod_{(a_0:a_1:a_2)\in\mathbb{P}^2(\mathbb{F}_q)} (a_0x + a_1y + a_2),$$

e $h(x, y) \in \mathbb{F}_q[x, y]$ é o polinômio absolutamente irredutível dado por (3.2.4). Assim, para o fecho projetivo $\mathcal{C}$ da curva plana dada por $g(x, y) = 0$, temos $\mathcal{C} = S \cup \mathcal{F}$, onde S é a união de todas as retas de $\mathbb{P}^2(\mathbb{K})$ definidas sobre $\mathbb{F}_q$ e $\mathcal{F}$ é a curva que figura na Proposição 3.2.6 (ou seja, $\mathcal{F}$ é o fecho projetivo da curva afim dada por $h(x, y) = 0$).

Se $P \in \mathcal{X}$ é um ponto $\mathbb{F}_q$-racional, o resultado segue da Proposição 3.2.9. Seja $P \in \mathcal{X}$ um ponto $\mathbb{F}_{q^{(m-u)}}$-racional que não é $\mathbb{F}_q$-racional, centrado em $\phi_1(P) \in \mathbb{P}^2(\mathbb{F}_{q^{(m-u)}})\backslash\mathbb{P}^2(\mathbb{F}_q)$. Por [4, Proposição 3.2], temos que $\phi_1(P)$ tem multiplicidade $q^u - 1$ na curva $\mathcal{F}$ caso $\phi_1(P) \in S$, ou multiplicidade q^u caso $\phi_1(P) \notin S$. Logo, em qualquer um dos casos, $\phi_1(P)$ tem multiplicidade q^u em $\mathcal{C}$. Supondo $e_P = 0$, temos

$$v_P(T_{u,m}) = v_P(A_t^0(1, x, y)) = v_P(g(x, y)) = I(P, \mathcal{X} \cap \mathcal{C}) \geq q^u.$$

□

No Lema 3.2.12 avaliamos o peso dos pontos $\mathbb{F}_{q^{(m-u)}}$-racionais da curva $\mathcal{X}$ no divisor (q^u, q^m)-Frobenius com relação à série linear $\mathcal{D}_1$ obtida pelo corte de $\mathcal{X}$ pelo sistema linear de retas em $\mathbb{P}^2(\mathbb{K})$. Vejamos agora o caso para um morfismo arbitrário.

Teorema 3.2.13. *Seja* $P \in \mathcal{X}$ *um ponto* $\mathbb{F}_{q^{(m-u)}}$*-racional. Então* $v_P(T_{u,m}) \geq q^u$.

Demonstração. Dividindo cada f_i por f_0, para $i = 0, ..., n$, podemos supor que $f_0 = 1$. Seja $P \in \mathcal{X}$ um ponto $\mathbb{F}_{q^{(m-u)}}$-racional e seja $t \in \mathbb{F}_{q^{(m-u)}}$ um parâmetro local em P. Novamente, podemos supor que $e_P = 0$ e assim temos que $v_P(f_i) \geq 0$ para todo $i = 0, ..., n$ e

$$v_P(T_{u,m}) = v_P(A_t^{\kappa_0,...,\kappa_{n-2}}(1, f_1, ..., f_n)).$$

Repare agora que, pelo desenvolvimento de Laplace utilizando as três primeiras linhas,

$$A_t^{\kappa_0,...,\kappa_{n-2}}(1, f_1, ..., f_n) = \sum_{0<i<j\leq n} \Delta_{ij} W_{ij} D_{ij},$$

$$\text{onde } W_{ij} = \det \begin{pmatrix} 1 & f_i^{q^m} & f_j^{q^m} \\ 1 & f_i^{q^u} & f_j^{q^u} \\ 1 & f_i & f_j \end{pmatrix} \quad \text{e} \quad D_{ij} := \det(D_t^{(\kappa_r)} f_s)_{1\leq r\leq n-2,\ 1\leq s\leq n,\ s\neq i,j},$$

sendo $\Delta_{ij} \in \{-1, 1\}$ o sinal correspondente. Como $v_P(D_{ij}) \geq 0$, para $0 < i < j \leq n$, temos $v_P(T_{u,m}) \geq min\{v_P(W_{ij})\}_{0<i<j\leq n}$. Portanto, é suficiente provarmos que $v_P(W_{ij}) \geq q^u$ para $0 < i < j \leq n$.

Dada uma curva $\mathcal{C}$ com corpo de funções $\mathbb{K}(z, w)$, defina $g(z, w) := (z^{q^m} - z)(w^{q^u} - w) - (w^{q^m} - w)(z^{q^u} - z)$ e suponha $g(z, w) \neq 0$. Pela demosntração do Lema 3.2.12, para todo ponto $\mathbb{F}_{q^{(m-u)}}$-racional $P \in \mathcal{C}$ tal que z e w sejam regulares em P, temos $v_P(g(z, w)) \geq q^u$.

Sejam i e j tais que $i < j$ e $W_{ij} \neq 0$, e defina $\xi := f_i$ e $\eta := f_j$. Considere o morfismo $\psi = (1 : \xi : \eta) : \mathcal{X} \longrightarrow \mathbb{P}^2(\mathbb{K})$ definido sobre $\mathbb{F}_q$ e seja $\mathcal{Y} = \psi(\mathcal{X})$. Observe que $\mathbb{K}(\xi, \eta) \subseteq \mathbb{K}(\mathcal{X})$ é o corpo de funções de $\mathcal{Y}$ e a extensão $\mathbb{K}(\mathcal{X})/\mathbb{K}(\xi, \eta)$ é finita. Uma vez que ψ está definido sobre $\mathbb{F}_q$, temos que $Q = \psi(P) \in \mathcal{Y}$ é um ponto $\mathbb{F}_{q^{m-u}}$-racional. Logo, temos que $v_Q(g(\xi, \eta)) \geq q^u$. Portanto

$$v_P(W_{ij}) = v_P(g(\xi, \eta)) = e(P|Q) \cdot v_Q(g(\xi, \eta)) \geq e(P|Q) \cdot q^u,$$

onde $e(P|Q)$ é o índice de ramificação de P sobre Q. □

A estimativa para o peso dos pontos $\mathbb{F}_q$-racionais no divisor $T_{u,m}$ obtida na Proposição 3.2.9 depende das $(\mathcal{D}, P)$-ordens e da sequência de ordens (q^u, q^m)-Frobenius de $\mathcal{X}$ com relação a $\mathcal{D}$. O objetivo dos próximos dois resultados é obter um limitante inferior para tal estimativa.

Proposição 3.2.14. *Seja $P \in \mathcal{X}$ um ponto $\mathbb{F}_q$-racional e sejam $j_0, ..., j_n$ as suas $(\mathcal{D}, P)$-ordens. Se $m_0, ..., m_{n-2}$ são inteiros tais que $0 \leq m_0 < m_1 < ... < m_{n-2}$ e*

$$\det\left(\binom{j_i - j_2}{m_r}\right)_{0\leq r\leq n-2,\ 2\leq i\leq n} \not\equiv 0 \mod p,$$

então $\kappa_i \leq m_i$ para todo i.

Demonstração. A prova é análoga a de [29, Proposição 2.5]. Seja x uma variável separante de $\mathbb{F}_q(\mathcal{X})$ e sejam $\tau_0, ..., \tau_{n-2}$ as ordens do seguinte morfismo:

$$\begin{aligned} \theta : \mathbb{P}^1(\mathbb{K}) &\longrightarrow \mathbb{P}^{n-2}(\mathbb{K}) \\ (1 : x) &\longmapsto (1 : x^{j_3 - j_2} : ... : x^{j_n - j_2}) = (x^{j_2} : x^{j_3} : ... : x^{j_n}). \end{aligned}$$

Como $\det\left(\binom{j_i - j_2}{m_r}\right)_{0\leq r\leq n-2,\ 2\leq i\leq n} \not\equiv 0 \mod p$, temos que $m_0 = 0$ e

$$\det(D_x^{(m_r)} x^{j_i - j_2}) = det\left(\binom{j_i - j_2}{m_r}\right)_{0\leq r\leq n-2,\ 2\leq i\leq n} \cdot x^{\sum_{i=1}^{n-2}(j_{i+2} - m_i) - (n-2)j_2} \neq 0.$$

Assim, pela minimalidade dos τ_i, temos que $\tau_i \leq m_i$ para todo $i = 0, ..., n-2$. Por outro lado, temos que $\kappa_i \leq \tau_i$ para cada i. De fato, como $\tau_0, ..., \tau_{n-2}$ são as ordens de θ, temos que $\det(D_x^{(\tau_r)} x^{j_i}) \neq 0$. Logo,

$$\det\left(\binom{j_i}{\tau_r}\right)_{0\leq r\leq n-2,\ 2\leq i\leq n} \not\equiv 0 \mod p.$$

Como P é $\mathbb{F}_q$-racional, novamente podemos supor que $f_0 = 1$ e $f_i = t^{j_i} + ...$ para cada i. Assim, como na prova da Proposição 3.2.9, temos

$$A_t^{\tau_0,...,\tau_{r-2}}(f_0, ..., f_n) = \det\left(\binom{j_i}{\tau_r}\right)_{2\leq i\leq n, 0\leq r\leq n-2} \cdot t^{q^u j_1 + \sum_{i=0}^{n-2}(j_{i+2}-\tau_i)} + ... \neq 0.$$

Portanto $\kappa_i \leq \tau_i$, pela minimalidade dos κ_i. □

Corolário 3.2.15. *Seja $P \in \mathcal{X}$ um ponto $\mathbb{F}_q$-racional. Então para todo $i \in \{0, 1, ..., n-2\}$ temos $\kappa_i \leq j_{i+2} - j_2$ e, além disso,*

$$v_P(T_{u,m}) \geq q^u + 2(n-1).$$

Demonstração. A primeira afirmação segue da Proposição 3.2.14 fazendo $m_r = j_{r+2} - j_2$. A segunda afirmação segue da primeira, da Proposição 3.2.9, e do fato de que $j_1 \geq 1$ e $j_2 \geq 2$. □

Como consequência imediata do Corolário 3.2.15, temos uma prova alternativa para o seguinte resultado, que já foi obtido antes.

Corolário 3.2.16. *Se $\kappa_0 > 0$, então $\mathcal{X}(\mathbb{F}_q) = \emptyset$ (ou seja, $N_1 = 0$).*

Estamos agora interessados em critérios para a determinação das ordens (q^u, q^m)-Frobenius. Levando em consideração as relações $\epsilon_i \leq \nu_i \leq \kappa_i$, começamos com os seguintes resultados.

Corolário 3.2.17. *Se existir um ponto $P \in \mathcal{X}(\mathbb{F}_q)$ com $(\mathcal{D}, P)$-ordens $j_0, ..., j_n$ tais que*

$$\det\left(\binom{j_i - j_2}{\epsilon_r}\right)_{0\leq r\leq n-2,\ 2\leq i\leq n} \not\equiv 0 \mod p,$$

então $\kappa_i = \epsilon_i$ para todo i.

Corolário 3.2.18. *Sejam $\nu_0, ..., \nu_{n-1}$ as ordens $\mathbb{F}_{q^u}$-Frobenius de $\mathcal{X}$ com relação a $\mathcal{D}$. Se existir um ponto $P \in \mathcal{X}(\mathbb{F}_q)$ com $(\mathcal{D}, P)$-ordens $j_0, ..., j_n$ tais que*

$$\det\left(\binom{j_i - j_2}{\nu_r}\right)_{0\leq r\leq n-2,\ 2\leq i\leq n} \not\equiv 0 \mod p,$$

então $\kappa_i = \nu_i$ para todo i.

O resultado do Corolário 3.2.18 também é válido para μ_i no lugar de ν_i, onde $\mu_0, ..., \mu_{n-1}$ são as ordens $\mathbb{F}_{q^m}$-Frobenius com relação a $\mathcal{D}$. No caso em que $m_i = i$, obtemos o seguinte.

Corolário 3.2.19. *Seja $P \in \mathcal{X}(\mathbb{F}_q)$ e sejam $j_0, ..., j_n$ as $(\mathcal{D}, P)$-ordens. Se o inteiro $\prod_{2\leq i<r\leq n}(j_r - j_i)/(r-i)$ não é divisível por p, então $\kappa_i = i$ para todo $i = 0, ..., n-2$ e*

$$v_P(T_{u,m}) = 2n - 1 + (q^u - 1)j_1 + \sum_{i=1}^{n}(j_i - i).$$

Demonstração. Usando propriedades básicas de determinante, temos

$$\det\left(\binom{j_i}{r}\right)_{0\leq r\leq n-2,\ 2\leq i\leq n} = \det\begin{pmatrix} 1 & j_2 & \frac{j_2(j_2-1)}{2!} & \cdots & \frac{j_2(j_2-1)...(j_2-(n-3))}{(n-2)!} \\ 1 & j_3 & \frac{j_3(j_3-1)}{2!} & \cdots & \frac{j_3(j_3-1)...(j_3-(n-3))}{(n-2)!} \\ 1 & j_4 & \frac{j_4(j_4-1)}{2!} & \cdots & \frac{j_4(j_4-1)...(j_4-(n-3))}{(n-2)!} \\ \vdots & \vdots & \vdots & \cdots & \vdots \\ 1 & j_n & \frac{j_n(j_n-1)}{2!} & \cdots & \frac{j_n(j_n-1)...(j_n-(n-3))}{(n-2)!} \end{pmatrix}$$

$$= \frac{1}{2!3!...(n-2)!} det\begin{pmatrix} 1 & j_2 & j_2^2 - j_2 & \cdots & j_2^{n-2} + ... \\ 1 & j_3 & j_3^2 - j_3 & \cdots & j_2^{n-2} + ... \\ 1 & j_4 & j_4^2 - j_4 & \cdots & j_2^{n-2} + ... \\ \vdots & \vdots & \vdots & \cdots & \vdots \\ 1 & j_n & j_n^2 - j_n & \cdots & j_n^{n-2} + ... \end{pmatrix},$$

onde as reticências na última coluna indicam os termos de potências menores que $n-2$ em j_i. Logo, uma vez que $2!3!...(n-2)! = \prod_{2\leq i<r\leq n}(r-i)$, temos

$$\det\left(\binom{j_i}{r}\right)_{0\leq r\leq n-2,\ 2\leq i\leq n} = \frac{det(j_i^r)}{2!3!...(n-2)!} \overset{\text{det Vandermonde}}{=} \prod_{2\leq i<r\leq n}(j_r - j_i)/(r-i). \quad (3.2.11)$$

Assim, temos que $p \nmid \prod_{2\leq i<r\leq n}(j_r - j_i)/(r-i)$ implica $p \nmid \det\left(\binom{j_i}{r}\right)_{0\leq r\leq n-2,\ 2\leq i\leq n}$. Como $P \in \mathcal{X}(\mathbb{F}_q)$, podemos supor $f_0 = 1$ e $f_i = t^{j_i} + ...$ para cada i. Novamente como na prova da Proposição 3.2.9, temos

$$A_t^{0,...,r-2}(f_0, ..., f_n) = \det\left(\binom{j_i}{r}\right)_{2\leq i\leq n, 0\leq r\leq n-2} \cdot t^{q^u j_1 + \sum_{i=0}^{n-2}(j_{i+2}-i)} + ... \neq 0.$$

Portanto, $\kappa_i = i$ para todo i, e pelo Teorema 3.2.9 temos que

$$v_P(T_{u,m}) = q^u j_1 + \sum_{i=0}^{n-2}(j_{i+2} - i) = 2n - 1 + (q^u - 1)j_1 + \sum_{i=1}^{n}(j_i - i).$$

□

Seja $d = \deg(\mathcal{D})$ e suponha $\mathcal{X}(\mathbb{F}_q) \neq \emptyset$. Como $j_n \leq d$, temos pelo Cororlário 3.2.19 que se

$p \geq d-1$, então $\kappa_i = i$ para todo $i = 0, ..., n-2$, ou seja, a curva $\mathcal{X}$ é (q^u, q^m)-Frobenius clássica com relação a $\mathcal{D}$. O próximo teorema, revela uma característica importante da sequência de ordens (q^u, q^m)-Frobenius. Através dele, em particular, poderemos provar um resultado análogo à afirmação anterior sem precisarmos assumir $\mathcal{X}(\mathbb{F}_q) \neq \emptyset$.

Teorema 3.2.20. *Seja $\phi = (f_0 : f_1 : ... : f_n) : \mathcal{X} \longrightarrow \mathbb{P}^n(\mathbb{K})$, com $n > 2$, um morfismo definido sobre $\mathbb{F}_q$ tal que $\mathcal{X}$ é (q^u, q^m)-Frobenius não clássica com relação a ϕ. Seja $\ell \in \{1, ..., n-2\}$ tal que $\kappa_i = i$ para $i < \ell$ e $\kappa_\ell > \ell$. Então $p | \kappa_\ell$.*

Note que o resultado obtido no Teorema 3.2.20 é análogo ao obtido em [10, Corolário 3], sendo este último relacionado à sequência de ordens $\mathbb{F}_q$-Frobenius.

Corolário 3.2.21. *Sejam $\phi = (f_0 : f_1 : ... : f_n) : \mathcal{X} \longrightarrow \mathbb{P}^n(\mathbb{K})$ um morfismo definido sobre $\mathbb{F}_q$ e $\mathcal{D}$ a sua série linear correspondente. Se $p > d = \deg(\mathcal{D})$, então $\mathcal{X}$ é (q^u, q^m)-Frobenius clássica com relação a $\mathcal{D}$.*

Demonstração. Segue imediatamente do Teorema 3.2.20 e do fato de que $\kappa_{n-2} \leq d$. □

Corolário 3.2.22. *Seja $\phi = (f_0 : f_1 : ... : f_n) : \mathcal{X} \longrightarrow \mathbb{P}^n(\mathbb{K})$ um morfismo definido sobre $\mathbb{F}_q$ e suponha que $p > n-1$. Se $\mathcal{X}$ é (q^u, q^m)-Frobenius não clássica com relação a ϕ, então $\mathcal{X}$ é $\mathbb{F}_{q^r}$-Frobenius não clássica com relação a ϕ, para $r = u, m$. Além disso, se $p > n$, a curva $\mathcal{X}$ é não clássica para ϕ.*

Demonstração. Sejam $(\nu_0, ..., \nu_{n-1})$ e $(\kappa_0, ..., \kappa_{n-2})$ respectivamente as sequências $\mathbb{F}_{q^u}$-Frobenius e (q^u, q^m)-Frobenius de $\mathcal{X}$ com relação a ϕ. Suponhamos que $\mathcal{X}$ é (q^u, q^m)-Frobenius não clássica com relação a ϕ. Pelo Corolário 3.2.2, existe $I \in \{1, ..., n-1\}$ tal que $\{\kappa_0, ..., \kappa_{n-2}\} = \{\nu_0, ..., \nu_{n-1}\} \backslash \{\nu_I\}$. Se $I = n-1$, temos que $(\nu_0, ..., \nu_{n-1}) = (\kappa_0, ..., \kappa_{n-2})$ e imediatamente concluímos que $\mathcal{X}$ é $\mathbb{F}_{q^u}$-Frobenius não clássica para ϕ. Se $I \neq n-1$, uma vez que $p | \kappa_\ell$ para algum $\ell = 1, ..., n-2$ (Teorema 3.2.20), temos que $p | \nu_i$ para algum $i \in \{0, ..., n-1\} \backslash \{I\}$. Como $i \leq n-1 < p$, a curva $\mathcal{X}$ é $\mathbb{F}_{q^u}$-Frobenius não clássica para ϕ. De maneira análoga, prova-se que $\mathcal{X}$ é $\mathbb{F}_{q^m}$-Frobenius não clássica para ϕ. A última afirmação segue da Proposição 1.3.9. □

A fim provarmos o Teorema 3.2.20, precisaremos estabelecer algumas notações e dos dois lemas seguintes. Dados um morfismo $\phi = (f_0 : f_1 : ... : f_n) : \mathcal{X} \longrightarrow \mathbb{P}^n(\mathbb{K})$ definido sobre $\mathbb{F}_q$ e t uma variável separante de $\mathbb{F}_q(\mathcal{X})$, para cada inteiro positivo $r \geq 0$ definimos

$$W_{ijk}^{(r)}(\phi, t) := \det \begin{pmatrix} f_i^{q^m} & f_j^{q^m} & f_k^{q^m} \\ f_i^{q^u} & f_j^{q^u} & f_k^{q^u} \\ D_t^{(r)}(f_i) & D_t^{(r)}(f_j) & D_t^{(r)}(f_k) \end{pmatrix}, \tag{3.2.12}$$

onde $i, j, k \in \{1, ..., n\}$ são distintos. Convencionaremos $W_{ijk}(\phi, t) := W_{ijk}^{(0)}(\phi, t)$. Quando não houver dúvidas quanto ao morfismo e à variável separante em questão, denotaremos apenas $W_{ijk}^{(r)}$

ao invés de $W_{ijk}^{(r)}(\phi,t)$. Também, sejam $f_{s_1},...,f_{s_k} \in \{f_0,...,f_n\}$ onde $1 \leq k \leq n+1$ e sejam $r_1,...,r_k$ inteiros positivos. Definimos

$$M_{s_1,...,s_k}^{r_1,...,r_k}(\phi,t) := \det \begin{pmatrix} D_t^{(r_1)}f_{s_1} & D_t^{(r_1)}f_{s_2} & ... & D_t^{(r_1)}f_{s_k} \\ D_t^{(r_2)}f_{s_1} & D_t^{(r_2)}f_{s_2} & ... & D_t^{(r_2)}f_{s_k} \\ \vdots & \vdots & ... & \vdots \\ D_t^{(r_k)}f_{s_1} & D_t^{(r_k)}f_{s_2} & ... & D_t^{(r_k)}f_{s_k} \end{pmatrix}. \tag{3.2.13}$$

Neste caso, também denotaremos $M_{s_1,...,s_k}^{r_1,...,r_k}$ ao invés de $M_{s_1,...,s_k}^{r_1,...,r_k}(\phi,t)$ quando estiverem claros o morfismo ϕ e a variável separante t em questão. Note que se $r_i = r_s$ para $i,s \in \{1,...,k\}$, temos que $M_{s_1,...,s_k}^{r_1,...,r_k} = 0$.

Lema 3.2.23. *Sejam $\phi = (f_0 : f_1 : ... : f_n) : \mathcal{X} \longrightarrow \mathbb{P}^n(\mathbb{K})$ um morfismo definido sobre $\mathbb{F}_q$ e t uma variável separante de $\mathbb{F}_q(\mathcal{X})$. Então $D_t^{(1)}(W_{ijk}^{(r)}) = (r+1)W_{ijk}^{(r+1)}$ para todo $r \geq 0$.*

Demonstração. Em primeiro lugar, temos que $D_t^{(1)}(g^{q^l}) = 0$ para todo $g \in \mathbb{K}(\mathcal{X})$, com $l > 0$. Para i,j,k fixados, definimos $g_i := f_j^{q^{m-u}}f_k - f_j f_k^{q^{m-u}}$, $g_j := f_i^{q^{m-u}}f_k - f_i f_k^{q^{m-u}}$ e $g_k := f_i^{q^{m-u}}f_j - f_i f_j^{q^{m-u}}$, e observamos que

$$W_{ijk}^{(r)} = D_t^{(r)}(f_i)g_i^{q^u} - D_t^{(r)}(f_j)g_j^{q^u} + D_t^{(r)}(f_k)g_k^{q^u}.$$

Usando a regra do produto das Derivadas de Hasse e o fato de que $D_t^{(1)}(g_\alpha^{q^u}) = 0$, para $\alpha = i,j,k$, temos que

$$\begin{aligned} D_t^{(1)}(W_{ijk}^{(r)}) &= D_t^{(1)}(D_t^{(r)}(f_i)g_i^{q^u}) - D_t^{(1)}(D_t^{(r)}(f_j)g_j^{q^u}) + D_t^{(1)}(D_t^{(r)}(f_k)g_k^{q^u}) \\ &= (r+1)(D_t^{(r+1)}(f_i)g_i^{q^u} - D_t^{(r+1)}(f_j)g_j^{q^u} + D_t^{(r+1)}(f_k)g_k^{q^u}) = (r+1)W_{ijk}^{(r+1)}, \end{aligned}$$

como queríamos. □

Lema 3.2.24. *Sejam $\phi = (f_0 : f_1 : ... : f_n) : \mathcal{X} \longrightarrow \mathbb{P}^n(\mathbb{K})$ um morfismo definido sobre $\mathbb{F}_q$ e t uma variável separante de $\mathbb{F}_q(\mathcal{X})$. Então, para todo $r > 0$ e $k > 0$ temos*

$$D_t^{(1)}(M_{s_1,...,s_k}^{r,...,r+k-1}) = (r+k)\cdot M_{s_1,...,s_k}^{r,...,\widehat{r+k-1},r+k}.$$

Demonstração. Demonstraremos por indução em k. O caso $k=1$ pode ser facilmente checado. Suponhamos que a propriedade é válida para $k \leq n-1$. Pelo o desenvolvimento de Laplace usando a primeira linha, temos que

$$M_{s_1,...,s_k,s_{k+1}}^{r,...,r+k-1,r+k} = \sum_{i=1}^{k+1}(-1)^{i+1}D_t^{(r)}(f_{s_i})\cdot M_{s_1,...,\widehat{s_i},...,s_{k+1}}^{r+1,...,r+k}. \tag{3.2.14}$$

Assim, temos que

$$D_t^{(1)}(M^{r,\dots,r+k-1,r+k}_{s_1,\dots,s_k,s_{k+1}}) = \Lambda + \sum_{i=1}^{k+1}(-1)^{i+1}D_t^{(r)}(f_{s_i})\cdot D_t^{(1)}(M^{r+1,\dots,r+k}_{s_1,\dots,\widehat{s_i},\dots,s_{k+1}}),$$

onde

$$\Lambda := (r+1)\left(\sum_{i=1}^{k+1}(-1)^{i+1}D_t^{(r+1)}(f_{s_i})\cdot M^{r+1,\dots,r+k}_{s_1,\dots,\widehat{s_i},\dots,s_{k+1}}\right).$$

Agora, note que

$$\Lambda = (r+1)\cdot M^{r+1,r+1,\dots,r+k}_{s_1,\dots,s_k,s_{k+1}} = 0,$$

visto que as duas primeiras linhas da matriz cujo determinante é $M^{r+1,r+1,\dots,r+k}_{s_1,\dots,s_k,s_{k+1}}$ se repetem. Por outro lado, pela hipótese de indução, para todo $i = 1, \dots, k+1$, temos

$$D_t^{(1)}(M^{r+1,\dots,r+k}_{s_1,\dots,\widehat{s_i},\dots,s_{k+1}}) = (r+k+1)\cdot M^{r+1,\dots,\widehat{r+k},r+k+1}_{s_1,\dots,\widehat{s_i},\dots,s_{k+1}}.$$

Portanto, temos que $D_t^{(1)}(M^{r,\dots,r+k-1,r+k}_{s_1,\dots,s_k,s_{k+1}}) =$

$$(r+k+1)\left(\sum_{i=1}^{k+1}(-1)^{i+1}D_t^{(r)}(f_{s_i})\cdot M^{r+1,\dots,\widehat{r+k},r+k+1}_{s_1,\dots,\widehat{s_i},\dots,s_{k+1}}\right) = (r+k+1)\cdot M^{r,\dots,r+k-1,r+k+1}_{s_1,\dots,s_i,\dots,s_{k+1}}.$$

□

Demonstração do Teorema 3.2.20. Seja $a \geq 0$ tal que $\kappa_\ell = \ell + a + 1$. Como $\mathcal{X}$ é (q^u, q^m)-Frobenius não clássica com relação a ϕ nas hipóteses do enunciado, temos que $\Gamma^{0,\dots,\ell-1,\ell+a}_{s_0,\dots,s_{\ell+2}} = 0$ para toda sequência $s_0 < \dots < s_{\ell+2}$ tal que $s_i \in \{0, \dots, n\}$, onde

$$\Gamma^{r_0,\dots,r_\ell}_{s_0,\dots,s_{\ell+2}} := \det\begin{pmatrix} f_{s_0}^{q^m} & f_{s_1}^{q^m} & f_{s_2}^{q^m} & \cdots & f_{s_{\ell+2}}^{q^m} \\ f_{s_0}^{q^u} & f_{s_1}^{q^u} & f_{s_2}^{q^u} & \cdots & f_{s_{\ell+2}}^{q^u} \\ D_t^{(r_0)}(f_{s_0}) & D_t^{(r_0)}(f_{s_1}) & D_t^{(r_0)}(f_{s_2}) & \cdots & D_t^{(r_0)}(f_{s_{\ell+2}}) \\ D_t^{(r_1)}(f_{s_0}) & D_t^{(r_1)}(f_{s_1}) & D_t^{(r_1)}(f_{s_2}) & \cdots & D_t^{(r_1)}(f_{s_{\ell+2}}) \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ D_t^{(r_\ell)}(f_{s_0}) & D_t^{(r_\ell)}(f_{s_1}) & D_t^{(r_\ell)}(f_{s_2}) & \cdots & D_t^{(r_\ell)}(f_{s_{\ell+2}}) \end{pmatrix},$$

sendo t é uma variável separante de $\mathbb{F}_q(\mathcal{X})$. Repare que, utilizando o desenvolvimento de Laplace usando as três primeiras linhas, obtemos

$$\Gamma^{r_0,\dots,r_\ell}_{s_0,\dots,s_{\ell+2}} = \sum_{i<j<k}\Delta_{s_is_js_k}W^{(r_0)}_{s_is_js_k}M^{r_1,\dots,r_\ell}_{s_\alpha,\alpha\neq i,j,k}, \tag{3.2.15}$$

onde $\Delta_{s_is_js_k} \in \{1, -1\}$ é o sinal correspondente e $i, j, k \in \{0, \dots, \ell+2\}$. Desta maneira, fixada

uma sequência $s_0 < ... < s_{\ell+2}$ com $s_i \in \{0, ..., n\}$, temos que

$$0 = \Gamma^{0,...,\ell-1,\ell+a}_{s_0,...,s_{\ell+2}} = \sum_{i<j<k} \Delta_{s_i s_j s_k} W_{s_i s_j s_k} M^{1,...,\ell-1,\ell+a}_{s_\alpha, \alpha \neq i,j,k}.$$

Logo, $0 = D_t^{(1)}(\Gamma^{0,...,\ell-1,\ell+a}_{s_0,...,s_{\ell+2}}) = \Lambda_1 + \Lambda_2$, onde

$$\Lambda_1 := \sum_{i<j<k} \Delta_{s_i s_j s_k} D_t^{(1)}(W_{s_i s_j s_k}) M^{1,...,\ell-1,\ell+a}_{s_\alpha, \alpha \neq i,j,k}$$

e

$$\Lambda_2 := \sum_{i<j<k} \Delta_{s_i s_j s_k} W_{s_i s_j s_k} D_t^{(1)}(M^{1,...,\ell-1,\ell+a}_{s_\alpha, \alpha \neq i,j,k}).$$

Agora, pelo Lema 3.2.23, temos que

$$\Lambda_1 = \sum_{i<j<k} \Delta_{s_i s_j s_k} W^{(1)}_{s_i s_j s_k} M^{1,...,\ell-1,\ell+a}_{s_\alpha, \alpha \neq i,j,k} = \Gamma^{1,1,...,\ell-1,\ell+a}_{s_0,...,s_{\ell+2}} = 0, \tag{3.2.16}$$

uma vez que a terceira e a quarta linhas da matriz cujo determinante é $\Gamma^{1,1,...,\ell-1,\ell+a}_{s_0,...,s_{\ell+2}}$ são iguais. Portanto, temos que $\Lambda_2 = 0$. Por outro lado, pelo desenvolvimento de Laplace usando a última linha aplicado a $M^{1,...,\ell-1,\ell+a}_{s_\alpha, \alpha \neq i,j,k}$, obtemos

$$M^{1,...,\ell-1,\ell+a}_{s_\alpha, \alpha \neq i,j,k} = \sum_{r \neq i,j,k} \Delta_r D_t^{(\ell+a)}(f_{s_r}) M^{1,...,\ell-1}_{s_\alpha, \alpha \neq i,j,k,r},$$

onde $r \in \{0, ..., \ell+2\}$ e Δ_r é o sinal correspondente. Utilizando o Lema 3.2.24 temos $D_t^{(1)}(M^{1,...,\ell-1,\ell+a}_{s_\alpha, \alpha \neq i,j,k}) =$

$$= (\ell + a + 1) \cdot \sum_{r \neq i,j,k} \Delta_r D_t^{(\ell+a+1)}(f_{s_r}) M^{1,...,\ell-1}_{s_\alpha, \alpha \neq i,j,k,r} + \ell \cdot \sum_{r \neq i,j,k} \Delta_r D_t^{(\ell+a)}(f_{s_r}) M^{1,...,\ell-2,\ell}_{s_\alpha, \alpha \neq i,j,k,r}$$

$$= (\ell + a + 1) \cdot M^{1,...,\ell-1,\ell+a+1}_{s_\alpha, \alpha \neq i,j,k} + \ell \cdot M^{1,...,\ell-2,\ell,\ell+a}_{s_\alpha, \alpha \neq i,j,k}.$$

Portanto

$$\begin{aligned} \Lambda_2 &= (\ell + a + 1) \cdot \sum_{i<j<k} \Delta_{s_i s_j s_k} W_{s_i s_j s_k} M^{1,...,\ell-1,\ell+a+1}_{s_\alpha, \alpha \neq i,j,k} + \ell \cdot \sum_{i<j<k} \Delta_{s_i s_j s_k} W_{s_i s_j s_k} M^{1,...,\ell-2,\ell,\ell+a}_{s_\alpha, \alpha \neq i,j,k} \\ &= (\ell + a + 1) \cdot \Gamma^{0,...,\ell-1,\ell+a+1}_{s_0,...,s_{\ell+2}} + \ell \cdot \Gamma^{0,...,\ell-2,\ell,\ell+a}_{s_0,...,s_{\ell+2}}. \end{aligned} \tag{3.2.17}$$

Afirmamos que $\Gamma^{0,...,\ell-2,\ell,\ell+a}_{s_0,...,s_{\ell+2}} = 0$ para toda sequência $s_0 < ... < s_{\ell+2}$ tal que $s_i \in \{0, ..., n\}$. De fato: para $a = 0$, a afirmação pode ser facilmente verificada. Suponha $a > 0$ e suponha também que $\Gamma^{0,...,\ell-2,\ell,\ell+a}_{s_0,...,s_{\ell+2}} \neq 0$ para alguma tal sequência. Pela Proposição 3.2.3, teríamos que $\kappa_\ell \leq \ell + a$, uma contradição, já que $\kappa_\ell = \ell + a + 1$. Assim, concluímos que

$$0 = \Lambda_2 = (\ell + a + 1) \cdot \Gamma^{0,...,\ell-1,\ell+a+1}_{s_0,...,s_{\ell+2}} = \kappa_\ell \cdot \Gamma^{\kappa_0,...,\kappa_{\ell-1},\kappa_\ell}_{s_0,...,s_{\ell+2}}.$$

Pela definição da sequência $(\kappa_0, ..., \kappa_{\ell-1}, \kappa_\ell)$, temos que existe uma sequência $s_0 < ... < s_{\ell+2}$, com $s_i \in \{0, ..., n\}$, tal que $\Gamma^{\kappa_0,...,\kappa_{\ell-1},\kappa_\ell}_{s_0,...,s_{\ell+2}} \neq 0$. Portanto, $p|\kappa_\ell$. □

Segue agora o resultado principal deste capítulo.

Teorema 3.2.25. *Seja $\mathcal{X}$ uma curva projetiva irredutível não singular de gênero g definida sobre $\mathbb{F}_q$, e sejam N_r a sua quantidade de pontos $\mathbb{F}_{q^r}$-racionais, para $r = 1, u, m, m-u$. Se existir em $\mathcal{X}$ uma série linear $\mathcal{D}$ definida sobre $\mathbb{F}_q$ simples, livre de ponto base, de grau d, dimensão n e ordens (q^u, q^m)-Frobenius $\kappa_0, \kappa_1, ..., \kappa_{n-2}$, então*

$$(c_1 - c_u - c_m - c_{m-u})N_1 + c_u N_u + c_m N_m + c_{m-u} N_{m-u} \leq (\kappa_0 + \kappa_1 + ... + \kappa_{n-2})(2g-2) + (q^m + q^u + n - 1)d,$$

onde c_r é o peso mínimo dos pontos $P \in \mathcal{X}(\mathbb{F}_{q^r})$ no divisor $T_{u,m}$, para $r = 1, u, m, m-u$. Além disto, $c_{m-u} \geq q^u$ e $c_1 \geq q^u + 2(n-1)$.

Demonstração. Pela Observação 3.2.8 os pontos $\mathbb{F}_{q^r}$-racionais sempre aparecem no suporte de $T_{u,m}$ para $r = 1, u, m, m-u$. Como $\mathrm{mdc}(u, m)=1$, temos que $\mathcal{X}(\mathbb{F}_{q^r}) \bigcap_{r \neq s} \mathcal{X}(\mathbb{F}_{q^s}) = \mathcal{X}(\mathbb{F}_q)$, para $r, s \in \{1, u, m, m-u\}$ (em particular, $N_r \geq N_1$ para cada r). Também, uma vez que $\mathcal{X}(\mathbb{F}_q) \subseteq \mathcal{X}(\mathbb{F}_{q^r})$ para $r \in \{u, m, m-u\}$, temos que $c_1 \geq c_r$ para cada r. Logo, temos

$$c_1 N_1 + c_u(N_u - N_1) + c_m(N_m - N_1) + c_{m-u}(N_{m-u} - N_1) \leq \deg(T_{u,m}).$$

Portanto, a desigualdade enunciada segue de (3.2.3). Os valores mínimos assumidos por c_{m-u} e c_1 seguem respectivamente do Teorema 3.2.13 e do Corolário 3.2.15. □

Observação 3.2.26. *Note que caso $\mathcal{X}$ seja (q^u, q^m)-Frobenius clássica, segue da Proposição 3.2.11 que $c_u \geq n-1$ e $c_m \geq n-1$.*

Repare agora que, se existir um ponto $P \in \mathcal{X}$ no suporte de $T_{u,m}$ que não seja $\mathbb{F}_{q^r}$-racional, para $r = u, m, (m-u)$, podemos somar $v_P(T_{u,m})$ do lado esquerdo da desigualdade exibida no Teorema 3.2.25. Da mesma forma, se existir um ponto $\mathbb{F}_{q^r}$-racional $P \in \mathcal{X}$ no suporte de $T_{u,m}$ tal que $v_P(T_{u,m}) > c_r$, podemos somar $(v_P(T_{u,m}) - c_r)$ do lado esquerdo da mesma desigualdade, onde $r = 1, u, m, m-u$. Assim, usando as Proposições 3.2.9, 3.2.10 e 3.2.11, podemos reescrever o Teorema 3.2.25 da seguinte maneira.

Teorema 3.2.27. *Seja $\mathcal{X}$ uma curva irredutível não singular de gênero g definida sobre $\mathbb{F}_q$, e sejam N_r a sua quantidade de pontos $\mathbb{F}_{q^r}$-racionais, para $r = 1, u, m, m-u$. Se existir em $\mathcal{X}$ uma série linear $\mathcal{D}$ definida sobre $\mathbb{F}_q$ simples, livre de ponto base, de grau d, dimensão n e ordens (q^u, q^m)-Frobenius $\kappa_0, \kappa_1, ..., \kappa_{n-2}$, então*

$$\begin{aligned} & (c_1 - c_u - c_m - c_{m-u})N_1 + c_u N_u + c_m N_m + c_{m-u} N_{m-u} + \sum_{P \in \mathcal{X}} B(P) \\ \leq\ & (\kappa_0 + \kappa_1 + ... + \kappa_{n-2})(2g-2) + (q^m + q^u + n - 1)d, \end{aligned} \tag{3.2.18}$$

onde c_r é o peso mínimo dos pontos $P \in \mathcal{X}(\mathbb{F}_{q^r})$ no divisor $T_{u,m}$, para $r = 1, u, m, m-u$ e

$$B(P) = \begin{cases} q^u j_1 + \sum_{i=0}^{n-2}(j_{i+2} - \kappa_i) - c_1, & \text{para } P \in \mathcal{X}(\mathbb{F}_q); \\ max\left\{0,\ \sum_{i=1}^{n-1}(j_i - \kappa_{i-1}) - c_r\right\} & \text{para } P \in \mathcal{X}(\mathbb{F}_{q^r})\backslash\mathcal{X}(\mathbb{F}_q),\ r{=}u,m; \\ v_P(T_{u,m}) - c_{m-u} & \text{para } P \in \mathcal{X}(\mathbb{F}_{q^{m-u}})\backslash\mathcal{X}(\mathbb{F}_q); \\ max\{0,\ \sum_{i=0}^{n-2}(j_i - \kappa_i)\}, & \text{nos demais casos .} \end{cases}$$

Além disto, $c_{m-u} \geq q^u$ e $c_1 \geq q^u + 2(n-1)$.

Demonstração. Os valores de $B(P)$ seguem da Proposição 3.2.9 caso $P \in \mathcal{X}(\mathbb{F}_q)$, da Proposição 3.2.11 caso $P \in \mathcal{X}(\mathbb{F}_{q^r})\backslash\mathcal{X}(\mathbb{F}_q)$, para $r = u, m$ e da Proposição 3.2.10 caso $P \notin \mathcal{X}(\mathbb{F}_{q^r})$, para $r = 1, u, m, m-u$. O restante da demonstração é análoga à do Teorema 3.2.25. □

3.3 Exemplos

Nesta seção veremos alguns exemplos de aplicações do Teorema 3.2.25, obtendo-se assim novas cotas superiores para pontos racionais em curvas definidas sobre $\mathbb{F}_q$. Compararemos estas novas cotas à cotas já existentes.

Exemplo 3.3.1. *Seja $\mathcal{X}$ um modelo projetivo não singular de uma curva plana de gênero g, grau d, definida por $f(x,y) = 0$ sobre $\mathbb{F}_q$ e considere o morfismo de Veronese*

$$\phi_s = (1 : x : y : x^2 : \ldots : x^i y^j : \ldots : y^s) : \mathcal{X} \longrightarrow \mathbb{P}^M(\mathbb{K}),$$

com $i + j \leq s$, onde $1 \leq s \leq d-3$ e $M = \binom{s+2}{2} - 1 = (s^2+3s)/2$. Sabemos que a série linear $\mathcal{D}_s$ associada ao morfismo ϕ_s é simples, livre de ponto base e $\deg(\mathcal{D}_s) = sd$ (ver 2.0.1). Se $\mathcal{X}$ é (q^u, q^m)-Frobenius clássica para $\mathcal{D}_s$, o Teorema 3.2.25 fornece

$$(M-1)N_u + (M-1)N_m + q^u N_{m-u} \leq (M-1)(M-2)(g-1) + sd(q^m + q^u + M - 1). \quad (3.3.1)$$

Para $s = 1$, temos o morfismo $\phi_1 = (1 : x : y) : \mathcal{X} \longrightarrow \mathbb{P}^2(\mathbb{K})$. Note que neste caso, não é preciso o uso da derivada de Hasse e logo, na construção do divisor (q^u, q^m)-Frobenius $T_{u,m}$, não precisamos do divisor canônico para fazer a "correção" em caso de mudança de variável separante. Portanto, temos que $\mathcal{X}$ é (q^u, q^m)-Frobenius clássica para ϕ_1 e

$$T_{u,m} = div((x^{q^m} - x)(y^q - y) - (y^{q^m} - y)(x^q - x)) + (q^m + q^u + 1)E.$$

Como o grau de $\mathcal{D}_1$ é d, temos $\deg(T_{u,m}) = d(q^m + q + 1)$. Assim, a cota (3.3.1) é dada por

$$N_u + N_m + q^u N_{m-u} \leq d(q^m + q^u + 1). \quad (3.3.2)$$

Sejam $r = u, m, m-u$. Supondo que $\mathcal{X}$ seja $\mathbb{F}_{q^r}$-Frobenius clássica com relação a ϕ_1, temos

que a cota de Stöhr-Voloch fornece

$$2N_r \leq 2(g-1) + d(q^r + 2). \tag{3.3.3}$$

Vejamos o seguinte caso: A curva $\mathcal{X}$ atinge a cota (3.3.3), ou seja, $2N_1 = 2(g-1) + d(q+2)$. Fazendo $u = m-1$, temos por (3.3.2) que

$$q^{m-1}(g - 1 + d(q+2)/2) + N_{m-1} + N_m \leq d(q^m + q^{m-1} + 1);$$

ou seja, temos que

$$2N_m \leq 2(g-1) + d(q^m + 2) - 2(q^{m-1} + 1)(g-1) - 2N_{m-1},$$

que é melhor que a cota (3.3.3) para N_m sempre que $d > 2$. Podemos encontrar exemplos de classes de curvas que atingem a cota (3.3.3) em [3, Teorema 2.1] e [6, Teorema 2].

Para $s = 2$, temos o morfismo $\phi_2 = (1 : x : y : x^2 : xy : y^2) : \mathcal{X} \longrightarrow \mathbb{P}^5(\mathbb{K})$. Se $\mathcal{X}$ for (q^u, q^m)-Frobenius clássica para $\mathcal{D}_2$, a cota (3.3.1) neste caso fornece

$$4N_u + 4N_m + q^u N_{m-u} \leq 12(g-1) + 2d(q^m + q^u + 4). \tag{3.3.4}$$

A cota de Stöhr-Voloch para $\mathcal{X}$ $\mathbb{F}_{q^r}$-Frobenius clássica para $\mathcal{D}_2$ é

$$5N_r \leq 20(g-1) + 2d(q^r + 5). \tag{3.3.5}$$

A cota (3.3.4) para N_m é melhor do que a cota (3.3.2), aproximadamente, se $3d < q^{m-u}$. Se em particular tivermos aproximadamente $N_{m-u} \geq dq^{m-u}/2$, a cota (3.3.4) para N_m também é melhor do que a cota (3.3.5).

Exemplo 3.3.2. *Seja $\mathcal{X}$ uma curva nas hipóteses do exemplo anterior. Para $m = 2$ e $u = 1$, o Teorema 3.2.25 fornece a seguinte cota (associada ao morfismo ϕ_1):*

$$N_2 \leq d(q^2 + q + 1) - (q+1)N_1. \tag{3.3.6}$$

Em [19], trabalhando com a Função Zeta da curva, Ihara observou a seguinte relação entre N_1 e N_2:

$$N_2 \leq q^2 + 1 + 2gq - \frac{(N_1 - q - 1)^2}{g}. \tag{3.3.7}$$

Em algumas situações, dependendo de n, q e N_1, a cota (3.3.6) é melhor do que (3.3.7). Por exemplo, suponha que $\mathcal{X}$ é não singular; se $N_1 \geq dq/2$, temos que (3.3.6) é melhor do que (3.3.7), aproximadamente, se $d \geq q/2 + 3$.

Exemplo 3.3.3. *Considere a curva $\mathcal{X}$ apresentada em [6, Teorema 2] dada pelo fecho projetivo da curva afim definida por*

$$(y+2)^{18} + y^{18} - x^{18} - 1 = 0$$

sobre $\mathbb{F}_{37}$. *Por [6, Teorema 2], temos que* $\mathcal{X}$ *é não singular (portanto seu gênero é* $g = (d-1)(d-2)/2 = 136$*) e* $N_1 = 3(p-1)^2/8 = 486$. *Utilizando o software "Magma Calculator", obtemos que* $N_2 = 2430$. *Através da tabela (3.3.8), podemos comparar a cota (3.3.2) com outras cotas aqui listadas:*

Cota	$N_2 \leq$
Störh-Voloch (3.3.3)	12475
Hasse-Weil (1.0.2)	11434
Ihara (3.3.7)	9959
(3.3.2)	6858

(3.3.8)

Exemplo 3.3.4. *Seja* $\mathcal{X}$ *a curva de grau* 6 *definida sobre* $\mathbb{F}_3$ *dada por*

$$\sum_{r+s+k=6} x^r y^s z^k = 0.$$

Queremos estimar a quantidade de pontos $\mathbb{F}_{27}$*-racionais de* $\mathcal{X}$. *Assim, usaremos a cota (3.3.2) para* $m = 3$ *e* $u = 1$. *Por [3, Teorema 2.1], temos que* $\mathcal{X}$ *é não singular e possui* $d(d+q^2-1)/2 = 42$ *pontos* $\mathbb{F}_9$*-racionais, ou seja,* $N_2 = 42$. *Seu gênero é dado por* $(d-1)(d-2)/2 = 10$. *Usando o software "Magma Calculator", obtemos* $N_1 = 0$ *e* $N_3 = 24$. *Podemos comparar a cota (3.3.2) com as demais através da tabela (3.3.9).*

Cota	$N_3 \leq$
Hasse-Weil (1.0.2)	131
Störh-Voloch (3.3.3)	96
(3.3.2)	60

(3.3.9)

3.4 Curvas $\mathbb{F}_{q^r}$-Frobenius não clássicas, para $r = u, m$

Seja $\mathcal{X}$ uma curva não singular de gênero g irredutível definida sobre $\mathbb{F}_q$. Nesta seção, analisaremos os casos em que a curva $\mathcal{X}$ é (q^u, q^m)-Frobenius clássica e $\mathbb{F}_{q^r}$-Frobenius não clássica com relação a um morfismo ϕ definido sobre $\mathbb{F}_q$, para $r = u, m$, e as consequências que este fato exerce no Teorema 3.2.25. Começaremos por um resultado que estima o peso de um ponto $\mathbb{F}_{q^m}$-racional no divisor $T_{u,m}$, no qual fazemos uso do fato de que os determinantes $A_t^{\kappa_0,\ldots,\kappa_{n-2}}(f_0,\ldots,f_n)$ e $W_t^{\nu_0,\ldots,\nu_{n-1}}(f_0,\ldots,f_n)$ (definido como em (1.3.1) para $\mathbb{F}_{q^m}$) diferem um do outro por apenas uma linha, onde $(\nu_0,\ldots,\nu_{n-1})$ é a sequência não clássica de ordens $\mathbb{F}_{q^u}$-Frobeius de $\mathcal{X}$ com relação ao morfismo ϕ.

Proposição 3.4.1. *Seja* $\mathcal{X}$ *uma curva irredutível não singular* $\mathbb{F}_{q^u}$*-Frobenius não clássica e* (q^u, q^m)*-Frobenius clássica com relação ao morfismo* $\phi = (1 : f_1 : \ldots : f_n)$. *Seja* $P \in \mathcal{X}$ *um ponto* $\mathbb{F}_{q^m}$*-racional com* $(\mathcal{D}, P)$*-ordens* $j_0,\ldots,j_n$ *tais que* $\prod_{0\leq s<r\leq n-1}(j_r - j_s)/(r-s) \not\equiv 0 \mod p$. *Então*

$$v_P(T_{u,m}) \geq j_n + \sum_{i=0}^{n-2}(j_i - i).$$

Caso

$$\det\left(\binom{j_r}{s}\right)_{0\leq s\leq n-1,\ 1\leq r\leq n} \equiv 0 \mod p,$$

vale a desigualdade estrita.

Demonstração. Podemos assumir que $e_P = 0$. Sejam t um parâmetro local em P e $(a_{ij}) \in GL_{n+1}(\mathbb{F}_{q^m})$, com $a_{00} = 1$ e $a_{0r} = 0$ para $r = 1, ..., n$, tal que $g_i := \sum_{j=0}^{n} a_{ij} f_j = t^{j_i} + ...$, para $i = 0, ..., n$, onde $f_0 := 1$. Uma vez que $\mathcal{X}$ é $\mathbb{F}_{q^u}$-Frobenius não clássica e (q^u, q^m)-Frobenius clássica com relação a ϕ, temos que a sequência de ordens $\mathbb{F}_{q^u}$-Frobenius é dada por $(0, 1..., n-2, \epsilon)$, com $\epsilon > n-1$. Assim, temos

$$\det\begin{pmatrix} 1 & f_1^{q^u} & ... & f_n^{q^u} \\ 1 & f_1 & ... & f_n \\ 0 & D_t^{(1)}(f_1) & ... & D_t^{(1)}(f_n) \\ \vdots & \vdots & ... & \vdots \\ 0 & D_t^{(n-1)}(f_1) & ... & D_t^{(n-1)}(f_n) \end{pmatrix} = 0. \tag{3.4.1}$$

Portanto,

$$\det\begin{pmatrix} 1 & f_1^{q^u} & ... & f_n^{q^u} \\ 1 & f_1 & ... & f_n \\ 0 & D_t^{(1)}(f_1) & ... & D_t^{(1)}(f_n) \\ \vdots & \vdots & ... & \vdots \\ 0 & D_t^{(n-1)}(f_1) & ... & D_t^{(n-1)}(f_n) \end{pmatrix} \cdot \det(a_{ij}) = \det\begin{pmatrix} 1 & h_1 & ... & h_n \\ 1 & g_1 & ... & g_n \\ 0 & D_t^{(1)}(g_1) & ... & D_t^{(1)}(g_n) \\ \vdots & \vdots & ... & \vdots \\ 0 & D_t^{(n-1)}(g_1) & ... & D_t^{(n-1)}(g_n) \end{pmatrix} = 0, \tag{3.4.2}$$

onde $h_i = \sum_{j=0}^{n} a_{ij} f_j^{q^u}$. Assim, utilizando o desenvolvimento de Laplace nas colunas do último determinante, para cada $i = 1, ..., n$ obtemos

$$h_i = \sum_{j=0}^{n-1} (-1)^j \frac{\Upsilon_{ij}}{\gamma_i} \cdot D_t^{(j)} g_i, \tag{3.4.3}$$

onde γ_i é o menor $n \times n$ de (3.4.2) obtido omitindo-se a primeira linha e a $i+1$-ésima coluna e Υ_{ij} é o menor $n \times n$ de (3.4.2) obtido omitindo-se a $j+2$-ésima linha e a $i+1$-ésima coluna.

Afirmação: $\Upsilon_{rj}/\gamma_r = \Upsilon_{sj}/\gamma_s$ para todo $r, s \in \{1, ..., n\}$ com $r \neq s$ e $j \in \{0, ..., n-1\}$.

Assumindo a afirmação, temos que $\delta_j := \Upsilon_{ij}/\gamma_i$ para todo $i \in \{1, ..., n\}$ e $j \in \{0, ..., n-1\}$; em particular, $\delta_{n-1} = \Upsilon_{nn-1}/\gamma_n$. Como h_j é regular em P para todo j e

$$\Upsilon_{nn-1} = \det\begin{pmatrix} 1 & h_1 & ... & h_{n-1} \\ 1 & t^{j_1} + \cdots & ... & t^{j_{n-1}} + \cdots \\ 0 & c_{11}t^{j_1-1} + \cdots & ... & c_{(n-1)1}t^{j_{n-1}-1} + \cdots \\ \vdots & \vdots & ... & \vdots \\ 0 & c_{1(n-2)}t^{j_1-(n-2)} + \cdots & ... & c_{(n-1)(n-2)}t^{j_{n-1}-(n-2)} + \cdots \end{pmatrix},$$

onde $c_{ik} = \binom{j_i}{k}$, temos que $v_P(\Upsilon_{nn-1}) \geq \sum_{i=0}^{n-2}(j_i - i)$. Também, como

$$\gamma_n = \det \begin{pmatrix} D_t^{(1)}(g_1) & \dots & D_t^{(1)}(g_n) \\ \vdots & \dots & \vdots \\ D_t^{(n-1)}(g_1) & \dots & D_t^{(n-1)}(g_n) \end{pmatrix} = \det\left(\binom{j_r}{s}\right) t^{\sum_{i=1}^{n-1}(j_i - i)} + \cdots,$$

e $det\left(\binom{j_r}{s}\right)_{1\leq r,s\leq n-1} = \prod_{0\leq s<r\leq n-1}(j_r - j_s)/(r-s) \not\equiv 0 \mod p$, temos $v_P(\gamma_n) = \sum_{i=1}^{n-1}(j_i - i)$. Portanto, $v_P(\delta_{n-1}) \geq -j_{n-1} + n - 1$. Agora, note que

$$(-1)^n A_t^{\kappa_0,\dots,\kappa_{n-2}}(f_0, f_1, \dots, f_n) \cdot \det(a_{ij}) = \det \begin{pmatrix} 1 & g_1^{q^m} & \dots & g_n^{q^m} \\ 1 & g_1 & \dots & g_n \\ 0 & D_t^{(1)}(g_1) & \dots & D_t^{(1)}(g_n) \\ \vdots & \vdots & \dots & \vdots \\ 0 & D_t^{(n-2)}(g_1) & \dots & D_t^{(n-2)}(g_n) \\ 1 & h_1 & \dots & h_n \end{pmatrix}.$$

Através da relação

$$(1, h_1, \dots, h_n) = \sum_{j=0}^{n-1}(-1)^j \delta_j \cdot (D_t^{(j)}(1), D_t^{(j)}(g_1), \dots, D_t^{(j)}(g_{n-1})),$$

onde $\delta_0 := 1$, obtemos $(-1)^n A_t^{\kappa_0,\dots,\kappa_{n-2}}(f_0, f_1, \dots, f_n) \cdot \det(a_{ij}) =$

$$\delta_{n-1} \cdot \det \begin{pmatrix} 1 & g_1^{q^m} & \dots & g_n^{q^m} \\ 1 & g_1 & \dots & g_n \\ 0 & D_t^{(1)}(g_1) & \dots & D_t^{(1)}(g_n) \\ \vdots & \vdots & \dots & \vdots \\ 0 & D_t^{(n-2)}(g_1) & \dots & D_t^{(n-2)}(g_n) \\ 0 & D_t^{(n-1)}(g_1) & \dots & D_t^{(n-1)}(g_n) \end{pmatrix} = \delta_{n-1} \cdot \left(\det\left(\binom{j_i}{s}\right) t^{\sum_{i=1}^{n} j_i - (i-1)} + \cdots\right).$$

Portanto, $v_P(T_{u,m}) = v_P(A_t^{\kappa_0,\dots,\kappa_{n-2}}(f_0, f_1, \dots, f_n)) \geq v_P(\delta_{n-1}) + \sum_{i=1}^{n} j_i - (i-1) = j_n + \sum_{i=0}^{n-2}(j_i - i)$.

Prova da Afirmação: Queremos mostrar que $\gamma_s \Upsilon_{rj} = \gamma_r \Upsilon_{sj}$ para todo $r, s \in \{1, \dots, n\}$ com $r \neq s$ e $j \in \{0, \dots, n-1\}$. Para simplificarmos a exposição, vamos supor que $s = n$ e $r = 1$; não é difícil constatar que os demais casos são análogos. Primeiro, repare que o desenvolvimento de Laplace aplicado a (3.4.2) usando a primeira e a segunda linhas fornece

$$\gamma_1 h_1 = A + \sum_{i=2}^{n}(-1)^i \gamma_i h_i \quad \text{e} \quad \gamma_1 g_1 = A + \sum_{i=2}^{n}(-1)^i \gamma_i g_i,$$

onde A é o menor $n \times n$ de (3.4.2) obtido omitindo-se a primeira linha e a primeira coluna.

Também, usando propriedades básicas de determinantes, verifica-se facilmente que $\gamma_1 D_t^{(r)}(g_1) = \sum_{i=2}^{n}(-1)^i \gamma_i D_t^{(r)}(g_i)$ para todo $r \neq j$. Assim $\gamma_1 \Upsilon_{nj} =$.

$$\gamma_1 \cdot \det \begin{pmatrix} 1 & h_1 & \dots & h_{n-1} \\ 1 & g_1 & \dots & g_{n-1} \\ 0 & D_t^{(1)}(g_1) & \dots & D_t^{(1)}(g_{n-1}) \\ \vdots & \vdots & \dots & \vdots \\ 0 & D_t^{(j-1)}(g_1) & \dots & D_t^{(j-1)}(g_{n-1}) \\ 0 & D_t^{(j+1)}(g_1) & \dots & D_t^{(j+1)}(g_{n-1}) \\ \vdots & \vdots & \dots & \vdots \\ 0 & D_t^{(n-1)}(g_1) & \dots & D_t^{(n-1)}(g_{n-1}) \end{pmatrix} = \det \begin{pmatrix} 1 & \gamma_1 h_1 & \dots & h_{n-1} \\ 1 & \gamma_1 g_1 & \dots & g_{n-1} \\ 0 & \gamma_1 D_t^{(1)}(g_1) & \dots & D_t^{(1)}(g_{n-1}) \\ \vdots & \vdots & \dots & \vdots \\ 0 & \gamma_1 D_t^{(j-1)}(g_1) & \dots & D_t^{(j-1)}(g_{n-1}) \\ 0 & \gamma_1 D_t^{(j+1)}(g_1) & \dots & D_t^{(j+1)}(g_{n-1}) \\ \vdots & \vdots & \dots & \vdots \\ 0 & \gamma_1 D_t^{(n-1)}(g_1) & \dots & D_t^{(n-1)}(g_{n-1}) \end{pmatrix},$$

e portanto

$$\gamma_1 \Upsilon_{nj} = \det \begin{pmatrix} 1 & A + \sum_{i=2}^{n}(-1)^i \gamma_i h_i & h_2 & \dots & h_{n-1} \\ 1 & A + \sum_{i=2}^{n}(-1)^i \gamma_i g_i & g_2 & \dots & g_{n-1} \\ 0 & \sum_{i=2}^{n}(-1)^i \gamma_i D_t^{(1)}(g_i) & D_t^{(1)}(g_2) & \dots & D_t^{(1)}(g_{n-1}) \\ \vdots & \vdots & \vdots & \dots & \vdots \\ 0 & \sum_{i=2}^{n}(-1)^i \gamma_i D_t^{(j-1)}(g_i) & D_t^{(j-1)}(g_2) & \dots & D_t^{(j-1)}(g_{n-1}) \\ 0 & \sum_{i=2}^{n}(-1)^i \gamma_i D_t^{(j+1)}(g_i) & D_t^{(j+1)}(g_2) & \dots & D_t^{(j+1)}(g_{n-1}) \\ \vdots & \vdots & \vdots & \dots & \vdots \\ 0 & \sum_{i=2}^{n}(-1)^i \gamma_i D_t^{(n-1)}(g_i) & D_t^{(n-1)}(g_2) & \dots & D_t^{(n-1)}(g_{n-1}) \end{pmatrix}. \quad (3.4.4)$$

Usando a linearidade na segunda coluna de (3.4.4) e o fato de que os inteiros n e $n-2$ têm a mesma paridade, temos que $\gamma_1 \Upsilon_{nj} = \gamma_n \Upsilon_{1j}$, como queríamos. □

Exemplo 3.4.2. *Seja $\mathcal{F} : f(x,y) = 0$ uma curva plana de grau d e gênero g definida sobre $\mathbb{F}_q$ e seja $\mathcal{X}$ um modelo projetivo não singular de $\mathcal{F}$. Considere o morfismo de Veronese $\phi_s : \mathcal{X} \longrightarrow \mathbb{P}^M(\mathbb{K})$, com $1 \leq s \leq d-3$, onde $M = \binom{s+2}{2} - 1 = (s^2+3s)/2$, tal que $p \geq M-1$. Sabemos que associada a ϕ_s temos a série linear $\mathcal{D}_s$, que é simples, livre de ponto base e tem grau sd. Suponhamos que $\mathcal{X}$ seja (q^u, q^m)-Frobenius clássica com relação a $\mathcal{D}_s$ e $\mathbb{F}_{q^u}$-Frobenius não clássica. Como a sequência $(\kappa_0, ..., \kappa_{M-2}) = (0, ..., M-2)$ é uma subsequência da sequência $\mathbb{F}_{q^u}$-Frobenius $(\nu_0, ..., \nu_{M-1})$, temos pelo Corolário 1.3.4 que $(\nu_0, ..., \nu_{M-1}) = (0, 1, ..., M-2, p^r)$, para algum $r > 0$ ($p^r > M-1$); esta última é uma subsequência da sequência de $\mathcal{D}_s$-ordens $(\epsilon_0, ..., \epsilon_M)$, e assim temos que $\epsilon_i = i$ para $i = 0, ..., M-2$, $\epsilon_{M-1} = M-1$ ou p^r e $\epsilon_M \geq p^r$. Suponhamos também que $\prod_{0 \leq s < r \leq M-1}(j_r(P) - j_s(P))/(r-s) \not\equiv 0 \mod p$ para todo $P \in \mathcal{X}(\mathbb{F}_{q^m}) \backslash \mathcal{X}(\mathbb{F}_q) \cap Supp(R)$, onde R é o divisor de ramificação de $\mathcal{X}$ com relação a $\mathcal{D}_s$.*

Vamos primeiro assumir que $\epsilon_{M-1} = M-1$, e portanto $\epsilon_M = p^r$. Desta maneira, temos que $c_{m-u} \geq q^u$ (Proposição 3.2.13), $c_1 \geq q^u + p^r + M - 1$ (Proposição 3.2.9) e $c_u \geq M-1$ (Proposição 3.2.11). Também, como $\prod_{0 \leq s < r \leq M-1}(j_r(P) - j_s(P))/(r-s) = 1$ para todo $P \notin Supp(R)$, temos

que $c_m \geq p^r$ (Proposição 3.4.1) Pelo Teorema 3.2.25, temos

$$(M-1)N_u + p^r N_m + q^u N_{m-u} \leq (M-1)(M-2)(g-1) + sd(q^m + q^u + M - 1).$$

A cota obtida para N_m é melhor do que a cota de Stöhr-Voloch relativa a série linear $\mathcal{D}_s$ para N_m sempre que, aproximadamente, $(M-1)N_u/q^u + N_{m-u} > sd$. Agora, suponhamos que $\epsilon_{M-1} = p^r$ e assim $\epsilon_M > p^r$. Aqui, temos que $c_{m-u} \geq q^u$ (Proposição 3.2.13), $c_1 \geq q^u + 2p^r$ (Proposição 3.2.9), $c_m \geq p^r$ e $c_u \geq p^r$ (Proposição 3.2.11). Neste caso, O Teorema 3.2.25 fornece

$$p^r N_u + p^r N_m + q^u N_{m-u} \leq (M-1)(M-2)(g-1) + sd(q^m + q^u + M - 1).$$

Aqui, cota obtida para N_m é melhor do que a cota de Stöhr-Voloch relativa a série linear $\mathcal{D}_s$ para N_m sempre que, aproximadamente, $p^r N_u/q^u + N_{m-u} + p^r(2g-2)/q^u > sd$.

Exemplo 3.4.3. *Sejam ε uma potência de um primo p e $r > 0$ um inteiro. As aplicações norma $N : \mathbb{F}_q \longrightarrow \mathbb{F}_\varepsilon$ e traço $T : \mathbb{F}_q \longrightarrow \mathbb{F}_\varepsilon$, onde $q = \varepsilon^r$, são definidas respectivamente por $N(\alpha) = \alpha^{\frac{\varepsilon^r-1}{\varepsilon-1}}$ e $Tr(\alpha) = \alpha^{\varepsilon^{r-1}} + \alpha^{\varepsilon^{r-2}} + ... + \alpha^\varepsilon + \alpha$. A curva norma-traço $\mathcal{F}$ sobre $\mathbb{F}_q$ é definida pelo fecho projetivo da curva afim*

$$N(x) = Tr(y).$$

O grau de $\mathcal{F}$ é $\frac{\varepsilon^r-1}{\varepsilon-1} = \varepsilon^{r-1} + \varepsilon^{r-2} + ... + \varepsilon + 1$. Por [18, Teorema 7.65 (iii)], a curva $\mathcal{F}$ é não clássica para ϕ_1 e sua sequência de $\mathcal{D}_1$-ordens é dada por $(0, 1, \varepsilon)$. Seja $\mathcal{X}$ um modelo projetivo não singular de $\mathcal{F}$. Utilizando-se do fato de que a aplicação traço é linear e sobrejetiva, não é difícil mostrar que $\mathcal{X}$ possui $\varepsilon^{2r-1} + 1$ pontos $\mathbb{F}_q$-racionais. Além disso, como $N(x)$ e $Tr(y)$ são polinômios com o conjunto mínimo de valores, por [5] temos que a curva $\mathcal{X}$ é $\mathbb{F}_q$-Frobenius não clássica para ϕ_1, com sequência $\mathbb{F}_q$-Frobenius $(0, \varepsilon)$. Verifica-se sem dificuldades que $\mathcal{F}$ possui um único ponto singular $P = (0 : 1 : 0)$, que é $\mathbb{F}_q$-racional; sendo assim, $p \nmid j_1(P)$ para todo $P \in \mathcal{X}(\mathbb{F}_{q^m}) \backslash \mathcal{X}(\mathbb{F}_q)$. Utilizando o exemplo 3.4.2 para $s = 1$, $u = 1$ e $m = 2$, temos que

$$N_2 \leq \frac{(\varepsilon^{r-1} + \varepsilon^{r-2} + ... + \varepsilon + 1)(q^2 + q + 1) - (q+1)(\varepsilon^{2r-1} + 1)}{\varepsilon}. \tag{3.4.5}$$

Vejamos o caso em que $\varepsilon = 3$ e $q = \varepsilon^3 = 27$, ou seja, $r = 3$. Neste caso, temos que a curva $\mathcal{X}$ é dada por $x^{13} = y^9 + y^3 + y$. Através do software "Magma Calculator", calculamos $N_2 = 946$. Utilizando a tabela (3.4.6), podemos comparar a cota (3.4.5) com outras cotas para N_2.

Cota	$N_2 \leq$
Hasse-Weil (1.0.2)	3322
Störh-Voloch (1.3.2)	3261
Ihara (3.3.7)	2350
(3.4.5)	1003

(3.4.6)

Teorema 3.4.4. *Seja $\mathcal{X}$ uma curva plana não singular de grau d definida sobre $\mathbb{F}_q$, com $q = p^h$.*

Suponha que $\mathcal{X}$ é $\mathbb{F}_q$-Frobenius não clássica com relação ao sistema linear de retas em $\mathbb{P}^2(\mathbb{K})$. Então

$$p^s N_m + qN_{m-1} \leq d(q^m + d - 1), \tag{3.4.7}$$

para algum $s > 0$.

Demonstração. Suponha que $\mathcal{X}$ é o fecho projetivo da curva dada por $f(x, y) = 0$, com $f(x, y) \in \mathbb{F}_q[x, y]$. Considere o morfismo $\phi_1 = (1 : x : y) : \mathcal{X} \longrightarrow \mathbb{P}^2(\mathbb{K})$ e $\mathcal{D}_1$ a série linear correspondente. Pela Proposição 3.2.6, temos que a única ordem (q, q^m)-Frobenius de $\mathcal{X}$ associada a $\mathcal{D}_1$ é $\kappa_0 = 0$. Como $\mathcal{X}$ é $\mathbb{F}_q$-Frobenius não clássica para ϕ_1, temos em particular que ela é não clássica, e suas sequência de $\mathcal{D}_1$-ordens e sequência de ordens $\mathbb{F}_q$-Frobenius são $(0, 1, \epsilon)$ e $(0, \epsilon)$ respectivamente, onde $\epsilon = p^s$ para algum $s > 0$ (Corolário 1.2.9). Além disto, como $\mathcal{X}$ é não singular, temos que $j_1(P) = 1$ para todo $P \in \mathcal{X}$ e, pelo Teorema 1.3.8, temos $N_1 = d(q - d + 2)$. Por [29, Corolário 2.10], todo ponto $\mathbb{F}_q$-racional de $\mathcal{X}$ é um ponto $\mathcal{D}_1$-Weierstrass, ou seja, todo ponto $\mathbb{F}_q$-racional de $\mathcal{X}$ pertence ao suporte do divisor de ramificação R de $\mathcal{D}_1$. Assim, dado $P \in \mathcal{X}(\mathbb{F}_q)$, temos que $j_2(P) \geq p^s + 1$.

Portanto, pela Proposição 3.2.9 e pela Proposição 3.4.1, temos que $v_P(T_{1,m}) \geq qj_1(P) + j_2(P) = q + p^s + 1$ se P é um ponto $\mathbb{F}_q$-racional e $v_P(T_{1,m}) \geq j_2(P) = p^s$ se P é um ponto $\mathbb{F}_{q^m}$-racional. Também, se P é um ponto $\mathbb{F}_{q^{m-1}}$-racional, temos pelo Teorema 3.2.13 que $v_P(T_{1,m}) \geq q$. Aplicando o Teorema 3.2.25 com $c_1 = q + p^s + 1$, $c_m = p^s$, $c_{m-1} = q$ e efetuando os cálculos, chegamos à cota superior desejada. □

Seja $\mathcal{X}$ uma curva como no enuciado do teorema anterior. Como $\mathcal{X}$ é $\mathbb{F}_q$-Frobenius não clássica, temos que $\mathcal{X}$ é $\mathbb{F}_{q^m}$-Frobenius clássica para ϕ_1 ([4, Teorema 1.1]); porém, esta é não clássica com sequência de $\mathcal{D}_1$-ordens $(0, 1, p^s)$. Logo, a cota de Stöhr-Voloch para N_m com relação ao morfismo ϕ_1 é

$$N_m \leq \frac{d(d + q^m - 1)}{p^s}. \tag{3.4.8}$$

A cota (3.4.7) é melhor do que a cota de Stöhr-Voloch acima sempre que $N_{m-1} \neq 0$. Isto acontece, em particular, se $d \neq q + 2$. Caso $N_{m-1} = 0$, as cotas coincidem. Em algumas situações, a cota (3.4.7) também é melhor do que a cota de Hasse-Weil. Por exemplo, caso $m = 2$, temos que a cota (3.4.7) é melhor do que a cota de Ihara (3.3.7) (que é melhor do que a cota de Hasse-Weil) se, aproximadamente, $d \geq q/p^s$.

Exemplo 3.4.5. *Seja $p = 5$, $q = 5^3 = 125$ e considere a curva $\mathcal{X}$ de grau $p^2 + p + 1 = 31$ sobre $\mathbb{F}_{125}$ dada pelo fecho projetivo da curva definida por*

$$y^{31} - (x^6 + 1)^5 x - (x^5 + x)^5 = 0.$$

Por [9, Seção 3], a curva $\mathcal{X}$ é $\mathbb{F}_q$-Frobenius não clássica com relação a $\phi_1 = (1 : x : y)$. Por [18, Teorema 7.65 (iii)], temos que a sequência de $\mathcal{D}_1$-ordens de $\mathcal{X}$ é $(0, 1, 5)$. Não é difícil mostrar que a curva $\mathcal{X}$ é não singular. Utilizando o software "Magma Calculator", obtemos que $N_2 = 22196$,

ou seja, $\mathcal{X}$ possui 22196 *pontos $\mathbb{F}_{125^2}$-racionais. Utilizando a tabela (3.4.9), podemos comparar a cota (3.4.7) com outras cotas para N_2.*

Cota	$N_2 \leq$
Hasse-Weil (1.0.2)	124376
Ihara (3.3.7)	105703
Störh-Voloch (3.4.8)	97061
(3.4.7)	22661

(3.4.9)

Exemplo 3.4.6. *Vejamos um exemplo de curva que atinge a cota (3.4.7). Seja $\mathcal{X}$ a curva definida sobre $\mathbb{F}_{q^2}$ dada pela equação*

$$x^{q+1} + y^{q+1} + z^{q+1} = 0,$$

ou seja, a curva $\mathcal{X}$ é a Curva Hermitiana sobre $\mathbb{F}_{q^2}$. A curva $\mathcal{X}$ é uma curva maximal (ou seja, a curva $\mathcal{X}$ atinge a cota de Hasse-Weil) e seu gênero é dado por $g = q(q-1)/2$ (ver [28, Exemplo 6.3.6]). Caso $q \neq 2$, por [18, Teorema 7.65 (iii)] temos que $\mathcal{X}$ é $\mathbb{F}_{q^2}$-Frobenius não clássica com relação a ϕ_1, e sua sequência de $\mathcal{D}_1$-ordens é dada por $(0, 1, q)$. Por [28, Corolário 5.1.16], temos que

$$N_r = q^{2r} + 1 - \sum_{i=1}^{2g} \alpha_i^r, \tag{3.4.10}$$

onde $\alpha_1, ..., \alpha_{2g} \in \mathbb{C}$ são os inversos das raízes do L-polinômio (o numerador da Função Zeta) de $\mathcal{X}$ sobre $\mathbb{F}_{q^2}$ (esta igualdade é verdadeira para curvas em geral, e não só para curvas maximais). Pelo Teorema de Hasse-Weil ([28, Teorema 5.2.1]), temos que $|\alpha_i| = q$ e, pela maximalidade de $\mathcal{X}$, temos que $N_1 = q^2 + 1 + 2gq$. Com isso e usando (3.4.10), temos que $\alpha_i = -q$, para $i = 1, ..., 2g$.

Agora seja $m > 1$ e suponha, sem perda de generalidade, que m é par. Pela equação (3.4.10), temos

$$N_m = q^{2m} + 1 - 2g(-q^m) = q^{2m} + 1 - q^{m+1}(q-1).$$

Também, temos que $m-1$ é ímpar e novamente por (3.4.10), temos

$$N_{m-1} = q^{2(m-1)} + 1 + q^m(q-1).$$

Portanto, obtemos

$$\begin{aligned} qN_m + q^2N_{m-1} &= q(q^{2m} + 1 - q^{m+1}(q-1)) + q^2(q^{2(m-1)} + 1 + q^m(q-1)) \\ &= q^{2m+1} + q^{2m} + q^2 + q = (q+1)(q^{2m} + q) \\ &= d(q^{2m} + d - 1), \end{aligned} \tag{3.4.11}$$

onde $d = q + 1$ é o grau da curva $\mathcal{X}$.

Finalizamos esta seção observando que na Proposição 3.4.1 e no Exemplo 3.4.2 supusemos que $\mathcal{X}$ é $\mathbb{F}_{q^u}$-Forbenius não clássica com relação a ϕ e tomamos um ponto $\mathbb{F}_{q^m}$-racional $P \in \mathcal{X}$ para estimar seu peso em $T_{u,m}$. Se supuséssemos que $\mathcal{X}$ é $\mathbb{F}_{q^m}$-Forbenius não clássica com relação a ϕ e tomássemos um ponto $P \in \mathcal{X}$ que fosse $\mathbb{F}_{q^u}$-racional, obteríamos resultados equivalentes (trocando a sequência de ordens $\mathbb{F}_{q^u}$-Frobenius $(\nu_0, ..., \nu_{n-1})$ pela sequência de ordens $\mathbb{F}_{q^m}$-Frobenius $(\mu_0, ..., \mu_{n-1})$). Todas as demonstrações são análogas.

3.5 Aplicação a uma curva de Fermat

Seja $\mathcal{X} := \mathcal{X}_d(a,b)$ uma curva de Fermat de grau d definida sobre $\mathbb{F}_q$ $(q = p^h)$, ou seja, a curva $\mathcal{X}$ é dada por uma equação do tipo $ax^d + by^d = z^d$, com $a, b \in \mathbb{F}_q$, onde $p \nmid d$. Em [12], são apresentadas cotas superiores para N_1 quando a curva $\mathcal{X}$ é $\mathbb{F}_q$-Frobenius clássica com relação ao morfismo de Veronese ϕ_s, com $1 \leq s \leq d-3$ e, para os casos $s = 1$ e $s = 2$, o valor exato de N_1 é determinado quando $\mathcal{X}$ é $\mathbb{F}_q$-Frobenius não clássica.

Aqui aplicaremos o Teorema 3.2.27 aos morfismos de Veronese em curvas de Fermat definidas sobre $\mathbb{F}_q$. Para os casos em que tais curvas são $\mathbb{F}_q$-Frobenius não clássicas, porém (q, q^m)-Frobenius clássicas para $s = 1$ e $s = 2$, daremos novas cotas superiores para o número de pontos racionais de $\mathcal{X}$ em uma extensão de $\mathbb{F}_q$, que melhoram as cotas obtidas pelo Teorema de Stöhr-Voloch.

Considere novamente o morfismo de Veronese $\phi_s : \mathcal{X} \longrightarrow \mathbb{P}^M$, com $M = \binom{s+2}{2} - 1 = (s^2+3s)/2$, $1 \leq s \leq d-3$, onde $\phi_s = (1 : x : y : x^2 : ... : x^iy^j : ... : y^s)$, tal que $i + j \leq s$ e $\mathcal{D}_s$ a série linear associada ao mesmo.

Teorema 3.5.1. *Sejam $\mathcal{X} = \mathcal{X}_d(a,b)$ uma curva de Fermat irredutível definida sobre $\mathbb{F}_q$ e s um inteiro tal que $1 \leq s \leq d-3$. Se $\mathcal{X}$ é (q, q^m)-Frobenius clássica com relação a $\mathcal{D}_s$, então*

$$\begin{aligned} & (c_1 - c_m - c_{m-1})N_1 + c_mN_m + c_{m-1}N_{m-1} + R(E_1 + 2E_2 + c_m + c_{m-1} - c_m^* - c_{m-1}^*) \\ + \;& 3dE_2 + R_m(c_m^* - c_m - E_2) + R_{m-1}(c_{m-1}^* - c_{m-1} - E_2) \\ \leq \;& (M-2)(M-1)(g-1) + sd(q^m + q + M - 1), \end{aligned} \tag{3.5.1}$$

com $c_1 \geq q + 2(M-1)$, $c_{m-1} \geq q$, $c_m \geq (M-1)$, onde

$$M = \binom{s+2}{2} - 1, \qquad E_1 = q + d(2s-1) - c_1,$$

$$E_2 = \frac{1}{6}\left((d-s-1)s(s-1)(s+4) + \frac{s(s-1)(s-2)(s+5)}{4}\right) - \frac{2(s-1)d - (s+2)(s+1) + 6}{2},$$

R é o número de pontos $\mathbb{F}_q$-racionais de $\mathcal{X}$ com $xyz = 0$, R_r é o número de pontos $\mathbb{F}_{q^r}$-racionais de $\mathcal{X}$ com $xyz = 0$ e c_r^* é o peso mínimo dos pontos $P \in \mathcal{X}(\mathbb{F}_{q^r}) \backslash \mathcal{X}(\mathbb{F}_q)$ com $xyz = 0$ no divisor $T_{1,m}$, para $r = m, (m-1)$.

Demonstração. Sabemos por [12, Teorema 1] que um ponto $P \in \mathcal{X}$ é ponto de inflexão total (isto é, a multiplicidade de interseção de $\mathcal{X}$ com sua reta tangente em P é d) se, e somente se, $P \in \mathcal{C} : xyz = 0$. A idéia é aplicarmos o Teorema 3.2.27 ao morfismo ϕ_s, calculando o valor de $B(P)$ nestes pontos de inflexão total. Como as possíveis multiplicidades de interseção de retas com a curva $\mathcal{X}$ em um ponto de inflexão total são $0, 1, d$, temos que as $(\mathcal{D}_s, P)$-ordens nestes pontos são $\{j_0, j_1, ..., j_M\} = \{i + dj \mid i, j \geq 0,\ i + j \leq s\}$.

Temos assim $3d$ pontos de inflexão total em $\mathcal{X}$, sendo R deles $\mathbb{F}_q$-racionais, R_{m-1} deles $\mathbb{F}_{q^{m-1}}$-racionais e R_m deles $\mathbb{F}_{q^m}$-racionais. Logo, tendo em vista que as ordens (q, q^m)-Frobenius são $0, 1, 2, ..., M-2$, calculando $B(P)$ para estes pontos e aplicando o Teorema 3.2.27 obtemos

$$\begin{aligned} & (c_1 - c_m - c_{m-1})N_1 + c_m N_m + c_{m-1}N_{m-1} + (3d - R_m - R_{m-1} + R)(\sum_{i=0}^{M-2}(j_i - i)) \\ + \quad & (R_m - R)(c_m^* - c_m) + (R_{m-1} - R)(c_{m-1}^* - c_{m-1}) + R(qj_1 + \sum_{i=0}^{M-2}(j_{i+2} - i) - c_1) \\ \leq \quad & (M-1)(M-2)(g-1) + sd(q^m + q + M - 1). \end{aligned}$$

Em [12, Corolário 1], é mostrado que

$$\sum_{i=0}^{M-1}(j_i - i) = \frac{1}{6}\left((d - s - 1)s(s-1)(s+4) + \frac{s(s-1)(s-2)(s+5)}{4}\right).$$

Logo, como $j_{M-1} = (s-1)d + 1$, temos que

$$\sum_{i=0}^{M-2}(j_i - i) = \sum_{i=0}^{M-1}(j_i - i) - (j_{M-1} - (M-1)) = E_2.$$

Assim, reescrevemos a desigualdade acima:

$$\begin{aligned} & (c_1 - c_m - c_{m-1})N_1 + c_m N_m + c_{m-1}N_{m-1} + 3dE_2 + (R_{m-1} - R)(c_{m-1}^* - c_{m-1} - E_2) \\ + \quad & R(q + \sum_{i=0}^{M-2}(j_{i+2} - i) - \sum_{i=0}^{M-2}(j_i - i) - c_1) + (R_m - R)(c_m^* - c_m - E_2) \\ \leq \quad & (M-1)(M-2)(g-1) + sd(q^m + q + M - 1). \end{aligned}$$

Uma vez que $j_1 = 1$, $j_M = sd$ e $j_{M-1} = (s-1)d + 1$, temos

$$q + \sum_{i=0}^{M-2}(j_{i+2} - i) - \sum_{i=0}^{M-2}(j_i - i) - c_1 = E_1,$$

e assim obtemos o resultado. □

Observação 3.5.2. *Para $c_1 = q + 2(M-1)$, temos que $E_1 = s(2d - s - 3) - d + 2$.*

Vamos agora estudar o Teorema 3.5.1 sob a hipótese de $\mathcal{X}$ ser $\mathbb{F}_q$-Frobenius não clássica para o morfismo $\phi_1 = (1 : x : y)$. Por [12, Teorema 2], se $p \neq 2$, a curva $\mathcal{X}$ é $\mathbb{F}_q$-Frobenius não clássica para ϕ_1 se, e somente se, $d = (p^h - 1)/(p^r - 1)$ para algum $r|h$ e $a, b \in \mathbb{F}_{p^r}$ (lembrando que $q = p^h$), e neste caso a sequência de $\mathcal{D}_1$-ordens de $\mathcal{X}$ é $(0, 1, p^r)$ ([18, Teorema 7.65 (iii)]). Além disso, temos que todos os pontos de inflexão total de $\mathcal{X}$ são pontos $\mathbb{F}_q$-racionais. Logo, para este caso, temos que $R = R_m = R_{m-1} = 3d$.

Teorema 3.5.3. *Suponha $p > 2$ e seja $\mathcal{X} = \mathcal{X}_d(a, b)$ uma curva de Fermat definida sobre $\mathbb{F}_q$. Se $\mathcal{X}$ é $\mathbb{F}_q$-Frobenius não clássica com relação ao morfismo $\phi_1 = (1 : x : y)$, então existe $r > 0$ tal que*

$$N_m \leq \frac{d(q^m + d - 1) - 3d(d - p^r) - qN_{m-1} + 3d}{p^r}. \tag{3.5.2}$$

Demonstração. Como observamos acima, $\mathcal{X}$ é não clássica para ϕ_1 e a sequência de $\mathcal{D}_1$-ordens de $\mathcal{X}$ é $(0, 1, p^r)$, para algum $r > 0$ (precisamente, o inteiro r é tal que $d = (p^h - 1)/(p^r - 1)$). Logo, a sequência de ordens $\mathbb{F}_q$-Frobenius de $\mathcal{X}$ com relação a ϕ_1 é $(0, p^r)$. Como a $\mathcal{X}$ é não singular, temos pela Proposição 3.4.1 que $c_m \geq p^r$. Agora, se $P \in \mathcal{X}(\mathbb{F}_q)$, temos que $j_2(P) \geq p^r + 1$ ([29, Corolário 2.10]) e assim, pela Proposição 3.2.9, obtemos $c_1 \geq q + p^r + 1$. Também, pelo Lema 3.2.12, temos que $c_{m-1} \geq q$.

Do fato de $\mathcal{X}$ ser não singular, segue também que $g = (d-2)(d-1)/2$, e pelo Teorema 1.3.8, temos $N_1 = d(q-d+2)$. Por fim, $E_1 = d - p^r - 1$ e $E_2 = 0$. Aplicando o Teorema 3.5.1 (levando em conta que $R = R_m = R_{m-1} = 3d$), temos a desigualdade procurada. □

A cota para N_m usando a técnica apresentada em [12] para ϕ_1 é

$$N_m \leq \frac{d(q^m + d - 1) - 3d(d - p^r)}{p^r}. \tag{3.5.3}$$

A cota (3.5.2) é sempre melhor do que a cota (3.5.3).

Exemplo 3.5.4. *A Curva Hermitiana $\mathcal{X}$ apresentada no exemplo 3.4.6 também atinge a cota (3.5.2), pois esta e a cota (3.4.7) são a mesma neste caso, uma vez que $d = q+1$ e $p^r = q$ (visto que a sequência de $\mathcal{D}_1$-ordens de $\mathcal{X}$ é $(0, 1, q)$).*

Exemplo 3.5.5. *Seja $p = 7$, $q = 7^3 = 343$ e considere a curva de Fermat de grau $d = p^2+p+1 = 57$*

$$\mathcal{X} : x^{57} + y^{57} = z^{57}$$

definida sobre $\mathbb{F}_{343}$. Sua sequência de $\mathcal{D}_1$-ordens é $(0, 1, 7)$, e como $\mathcal{X}$ é $\mathbb{F}_q$-Frobenius não clássica para ϕ_1, temos pelo Teorema 1.3.8 que $N_1 = d(q - 1) - d(d - 3) = 16416$. Usando o software "Magma Calculator", obtemos que $N_2 = 152874$. Através da tabela (3.5.4), comparamos a cota

(3.5.2) a outras cotas para N_2.

Cota	$N_2 \leq$
Hasse-Weil (1.0.2)	1154882
Ihara (3.3.7)	1006356
Garcia-Voloch (3.5.3)	957233
(3.5.2)	152874

(3.5.4)

Ou seja, a curva $\mathcal{X}$ *atinge a cota (3.5.2).*

Suponhamos agora que $p > 5$, que $\mathcal{X}$ seja (q, q^m)-Frobenius clássica para $\phi_2 = (1 : x : y : x^2 : xy : y^2)$ e também que $\mathcal{X}$ seja $\mathbb{F}_q$-Frobenius não clássica para ϕ_2, porém clássica para ϕ_1. Por [12, Teorema 3], temos que $\mathcal{X}$ atende a uma das três seguintes propriedades:

(1) $p|(d-2)$ e $d = 2(p^h - 1)/(p^r - 1)$ com $r < h$, $r|h$ e $a, b \in \mathbb{F}_{p^r}$.

(2) $p|(2d-1)$ e $d = (p^h - 1)/2(p^r - 1)$ com $h = tr$ (t par) e $a^2, b^2 \in \mathbb{F}_{p^r}$.

(3) $q = d + 1$ e $a + b = 1$ (ver Observação 3.5.7).

Além disso, temos nos três casos que todo ponto de inflexão total de $\mathcal{X}$ é $\mathbb{F}_q$-racional (e portanto $R = R_m = R_{m-1} = 3d$). Seja $e := (p^h - 1)/(p^r - 1)$. Por [12, seção 2], temos que

$$N_1 = \begin{cases} (q-1)^2 & \text{no caso (3);} \\ (e^2/4)(p^r - 2) + 3e/2 & \text{no caso (2);} \\ e^2(p^r + 1 - 2(\vartheta(a) + \vartheta(b) + \vartheta(-ab))) + 2e(\vartheta(a) + \vartheta(b) + \vartheta(-ab)) & \text{no caso (1),} \end{cases}$$

onde $\vartheta : \mathbb{F}_{q^r}^* \longrightarrow \{0, 1\}$ é dada por $\vartheta(\alpha) = 1$ se, e somente se, $\alpha \in H$, onde H é o subgrupo de $\mathbb{F}_{p^r}^*$ de índice 2.

Por [11, Teorema 1] e [18, Teorema 7.65 (iii)], temos que $\mathcal{X}$ é não clássica para ϕ_2 e sua sequência de $\mathcal{D}_2$-ordens é $(\epsilon_0, ..., \epsilon_5) = (0, 1, 2, 3, 4, p^r)$. Como a sequência (q, q^m)-Frobenius é $(0, 1, 2, 3)$, temos que e a sequência $\mathbb{F}_q$-Frobenius para ϕ_2 é $(0, 1, 2, 3, p^r)$. Seja $P \in \mathcal{X}(\mathbb{F}_{q^m}) \backslash \mathcal{X}(\mathbb{F}_q)$. Uma vez que todas as inflexões de $\mathcal{X}$ são $\mathbb{F}_q$-racionais, temos que as $(\mathcal{D}_1, P)$-ordens são $(0, 1, 2)$. Portanto, existem cônicas (degeneradas) que intersectam $\mathcal{X}$ em P com multiplicidades $0, 1, 2, 3$ e 4, de onde concluímos que a sequência de $(\mathcal{D}_2, P)$-ordens é $(j_0, j_1, j_2, j_3, j_4, j_5) = (0, 1, 2, 3, 4, j_5)$ e, consequentemente, $\prod_{0 \leq s < r \leq 4}(j_r - j_s)/(r - s) = 1$. Assim, para tais pontos, temos pela Proposição 3.4.1 que $v_P(T_{1,m}) \geq p^r$. Por [29, Corolário 2.10], temos para todo $P \in \mathcal{X}(\mathbb{F}_q)$ que $j_i(P) \geq \epsilon_i + 1$ para algum $i = 2, ..., 5$. Logo, pela Proposição 3.2.9, se P é um ponto $\mathbb{F}_q$-racional de $\mathcal{X}$, temos $v_P(T_{1,m}) \geq q + p^r + 4$ e pelo Teorema 3.2.13, se P é um ponto $\mathbb{F}_{q^{(m-1)}}$-racional, temos $v_P(T_{1,m}) \geq q$. Como $E_1 = 3d - p^r - 4$ e $E_2 = d - 3$, o Teorema 3.5.1 fornece

$$N_m \leq \frac{2d(2d + q^m + q - 2) - 4N_1 - qN_{m-1}}{p^r} - \frac{3d(4d - p^r - 7)}{p^r}. \tag{3.5.5}$$

Reescrevendo a desigualdade (3.5.5), obtems o seguinte.

Teorema 3.5.6. *Seja $\mathcal{X} = \mathcal{X}_d(a,b)$ uma curva de Fermat definida sobre $\mathbb{F}_q$, onde $q = p^h$ e $p > 5$. Suponha que $\mathcal{X}$ seja (q, q^m)-Frobenius clássica para ϕ_2. Suponha também que $\mathcal{X}$ seja $\mathbb{F}_q$-Frobenius não clássica para ϕ_2, porém clássica para ϕ_1. Então existe $r > 0$ tal que*

$$N_m \leq \frac{2d(2d+q^m-1)-3d(2d-p^r)}{p^r} - \frac{4N_1+qN_{m-1}+3d(2d-7)-2d(q-1)}{p^r}. \tag{3.5.6}$$

A cota para N_m usando a técnica apresentada em [12] para ϕ_2 é

$$N_m \leq \frac{2d(2d+q^m-1)-3d(2d-p^r)}{p^r}. \tag{3.5.7}$$

Um cálculo simples mostra que $4N_1 > 2d(q-1)$. Logo, a cota (3.5.6) é melhor do que a cota (3.5.7) em todos os três casos possíveis.

Observação 3.5.7. *Apesar de não citada em [12, Teorema 3], a curva $\mathcal{X} : ax^{q-1}+(1-a)y^{q-1}-1 = 0$, com $a \in \mathbb{F}_q^*$, é $\mathbb{F}_q$-Frobenius não clássica para ϕ_2. Na prova do referido Teorema, é analisado o caso em que $p|d+1$, onde d é o grau da curva de Fermat $\mathcal{X} = \mathcal{X}_d(a,b)$ definida sobre $\mathbb{F}_q$. Lá, supõe-se que x é uma variável separante de $\mathbb{F}_q(\mathcal{X})$ e, desta maneira, é mostrado que*

$$W_x^{0,1,2,3,4}(1,x,y,x^2,xy,y^2) = F \cdot G \neq 0, \tag{3.5.8}$$

onde $G := x^q y^q - ax^{d+1}y^q - by^{d+1}x^q$ e $F \in \mathbb{F}_q(\mathcal{X})^*$. Na verdade, uma situação deixou de ser considerada em [12, Teorema 3]. Suponha que $\mathcal{X}$ é $\mathbb{F}_q$-Frobenius não clássica para ϕ_2, ou seja, que $G = 0$. Escreva $d+1 = p^r l$, onde p não divide l. Se $r > h$, tomando a raiz p^h-ésima de G, obtemos

$$xy - a^{1/p^h}x^{p^{r-h}l}y - b^{1/p^h}y^{p^{r-h}l}x = 0,$$

que é uma equação relacionando x e y de grau menor que d, uma contradição. Suponha então que $r < h$ e tome a raiz p^r-ésima de G

$$x^{p^{h-r}}y^{p^{h-r}} - a^{1/p^r}x^l y^{p^{h-r}} - b^{1/p^r}y^l x^{p^{h-r}} = 0.$$

Aplicando a primeira derivada de Hasse com relação a x dos dois lados desta última equação, obtemos

$$-a^{1/p^r} + b^{1/p^r}\frac{a}{b}\left(\frac{x}{y}\right)^{p^{h-r}+d-l} = 0,$$

e assim $p^{h-r}+d-l = 0$, o que também é uma contradição, uma vez que $d+1 > l$.

Resta então olharmos para o caso $r = h$, ou seja, $d+1 = ql$. Neste caso, temos que $G = 0$ fornece

$$x^q y^q(1 - ax^{q(l-1)} - by^{q(l-1)}) = 0,$$

e portanto $1 - ax^{l-1} - by^{l-1} = 0$. Se $l > 1$, teríamos que uma equação de grau menor que d relacionando x e y, um absurdo. Logo $l = 1$, ou seja, $a+b = 1$. Assim, temos que a hipótese de

que as $\mathcal{D}_2$-ordens de Frobenius são não clássicas e $p|(d+1)$ nos forenece $d = q-1$ e $b = 1-a$. A recíproca deste caso pode ser verificada sem dificuldades.

Finalizaremos a seção mostrando que a classe que curvas de Fermat que atendem as hipóteses do Teorema 3.5.6 é não vazia, isto é, mostrando que existem curvas (q, q^m)-Frobenius clássicas para ϕ_2 que sejam $\mathbb{F}_q$-Frobenius não clássicas para ϕ_2, porém clássicas para ϕ_1. Para isso, faremos uso da seguinte Proposição.

Proposição 3.5.8. *Seja $\mathcal{X}_d(a,b) = \mathcal{X}$ uma curva de Fermat definida sobre $\mathbb{F}_q$, com $q = p^h$ ($p > 5$), e seja R o número de pontos $\mathbb{F}_q$-racionais de $\mathcal{X}$ tais que $xyz = 0$. Se $R \neq 0$ e $\mathcal{X}$ é (q, q^m)-Frobenius não clássica com relação a ϕ_2, então $p|(d-1)(d-2)$.*

Demonstração. Seja $P \in \mathcal{X}$ um ponto $\mathbb{F}_q$-racional tal que $xyz = 0$. As ordens de P com relação a ϕ_1 são $0, 1$ e d; logo, as $(\mathcal{D}_2, P)$-ordens são $0, 1, 2, d, d+1$ e $2d$. Como $\mathcal{X}$ é (q, q^m)-Frobenius não clássica com relação a ϕ_2, pelo Corolário 3.2.19 temos que $p|\prod_{2\leq i<r\leq 5}(j_r - j_i)/(r-i)$. Logo, $p|d(d-1)(d-2)$. Como $p \nmid d$, temos portanto que $p|(d-1)(d-2)$. □

Pela Proposição 3.5.8, existem curvas que atendem as hipóteses do Teorema 3.5.6. De fato, seja $\mathcal{X}$ a curva definida por $ax^d + by^d = z^d$, com $a, b \in \mathbb{F}_{p^r}$, onde $d = e/2$ e $p > 5$. Como observado antes, temos neste caso que $R = 3d \neq 0$; entretanto, $p \nmid (d-1)(d-2)$. Logo, $\mathcal{X}$ é (q, q^m)-Frobenius clássica com relação a ϕ_2.

Referências Bibliográficas

[1] A. Aguglia, G. Korchmáros, On the algebraic curves over a finite field with many rational points, Bull. Belg. Math. Soc. 7(2000) 333-342.

[2] A. Aguglia, G. Korchmáros, F. Torres, Plane maximal curves, Acta Arith. 98(2001) 165-179.

[3] H. Borges, On complete (N, d)-arcs derived from plane curves, Finite Fields and Their Applications, 15(2009) 82-96.

[4] H. Borges, On multi-Frobenius non-classical plane curves, Arch. Math. (Basel) 93(2009), no. 6, 541-553.

[5] H. Borges, On the Frobenius non-classical components of $f(x) = g(y)$, preprint.

[6] M.L. Carlin, J.F. Voloch, Plane curves with many points over finite fields, Rocky Montain J. Math., 34(2004) 1255-1259.

[7] A. Cossidente, J.W.P. Hirshfeld, G. Korchmáros, F. Torres, On plane maximal curves, Compositio Math, 121(2000) 163-181.

[8] W. Fulton, Algebraic curves, W. A. Benjamin INC, New York (1969).

[9] A. Garcia, The curves $y^n = f(x)$ over finite fields, Arch. Math. 54(1990) 36-44.

[10] A. Garcia, M. Homma, Frobenius order sequences of curves, Algebra and Number Theory, eds. G. Frey and J. Ritter (Walter Gruyter Co., 1994) 27-41.

[11] A. Garcia, J.F. Voloch, Wronskians and linear independence in fields of prime characteristic, Manuscripta Math. 59(1987) 457-469.

[12] A. Garcia, J.F. Voloch, Fermat Curves over finite fields, Journal of Number Theory 30(1988) 345-356.

[13] M. Giulietti, On the number of rational points of a plane algebraic curve, preprint.

[14] A. Hefez, J.F. Voloch, Frobenius non-classical curves, Arch. Math. 54 (1990) 263-273.

[15] J.W.P. Hirshfeld, Projective geometries over finite fields, 2nd edn, Oxford University Press, 1998.

[16] J.W.P. Hirshfeld, G. Korchmáros, On the embedding of an arc into a conic in a finite plane, Finite Fields and Their Applications 2(1996) 274-292.

[17] J.W.P. Hirshfeld, G. Korchmáros, On the number of rational points on an algebraic curve over a finite field, Bull. Belg. Math. Soc. 5(1998) 313-340.

[18] J.W.P. Hirshfeld, G. Korchmáros, F.Torres, Algebraic curves over a finite field, Princeton Series in Applied Mathematics, 2008.

[19] Y. Ihara, Some Remarks on the number of rational points of algebraic curves over finite fields, J. Fac. Sci. Univ. Tokyo, Sect. IA Math. 28(1981) 721-724.

[20] G. Korchmáros, T. Szönyi, Fermat Curves over finite fields and cyclic subsets in high-dimensional projective spaces, Finite Fields and Their Applications, 5(1999) 206-217

[21] S. Lang, Algebra, *3rd* edition, Graduate Texts in Math. 211, Springer-Verlag, New York (2002).

[22] D. Levcovitz, Bounds for the number of fixed points of automorphisms of curves, Proc. London Math. Soc. (3) 62(1991), no. 1, 133-150.

[23] R. Lidl, H. Niederreiter, Finite fields, Cambridge University Press, 1988.

[24] R. Miranda, Algebraic curves and Riemann Surfaces, Graduate Studies in Mathematics series, No. 5, AMS (1995).

[25] M. Namba, Geometry of projective algebraic curves, Pure and Applied Mathematics, Marcel Dekker Inc. (1984).

[26] R. Pardini, Some remarks on plane curves over fields of positive characteristic, Compositio Math. 60(1986) 3-17.

[27] J-P. Serre, Sur le noumbre des points rationnels d'une courbe algébrique sur un corps fini, C.R. Acad. Sci. Paris Sér *I* Math., 296(1983) 397-402.

[28] H. Stichtenoth, Algebraic function fields and codes, Springer, Berlin, 1993.

[29] K.O. Stöhr, J.F. Voloch, Weierstrass points on curves over finite fields, Proc. London Math. Soc. 52(1986) 1-19.

[30] T. Szönyi, On cyclic caps in projective spaces, Des. Codes Cryptogr. 8(1996) 327-332.

[31] F. Torres, The approach of Stöhr-Voloch to the Hasse-Weil bound with applications to optimal curves and plane arcs: Expanded version of lectures given at Essen (April 1997) and Perugia (February 1998), IMECC-UNICAMP/November 2000.

[32] F. Rodriguez Villegas, J.F. Voloch, D. Zagier, Constructions of plane curves with many points, Acta Arith. 99(2001) 85-96.

Índice Remissivo

$(\mathcal{D}, P)$-ordem, 4
i-ésimo plano osculador, 4
índice $\mathbb{F}_q$-Frobenius, 7

Curva (q^u, q^m)-Frobenius não clássica, 30
Curva $\mathbb{F}_q$-Frobenius não clássica, 7
Curva s-osculadora, 11
Curva de Fermat, 12
Curva Hermitiana, 1
Curva não clássica, 5
Curvas maximais, 1

Derivada de Hasse, 4
Divisor (q^u, q^m)-Frobenius, 30
Divisor de Frobenius, 7
Divisor de ramificação, 5

Hiperplano osculador, 4

Mapa $\mathbb{F}_q$-Frobenius, 2
Morfismo, 2
Morfismo birracional, 3
Morfismo de Veronese, 11

Ordens (q^u, q^m)-Frobenius, 30
Ordens $\mathbb{F}_q$-Frobenius, 7

Pontos $\mathcal{D}$-Weierstrass, 5

Série linear, 3
Série linear simples, 3
Sequência de $\mathcal{D}$-ordens, 5
Sistema linear de curvas, 11

Teorema de Garcia-Voloch, 6
Teorema de Hasse-Weil, 1
Teorema de Hefez-Voloch, 9
Teorema de Stöhr-Voloch, 8