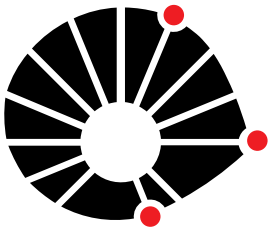

UNICAMP

UNIVERSIDADE ESTADUAL DE CAMPINAS

Instituto de Matemática, Estatística e Computação Científica

STÉFANI CONCOLATO VIEIRA

Propriedades de curvas maximais com dimensão Frobenius 3 sobre Corpo Finito com 64 elementos

Campinas

2021

Stéfani Concolato Vieira

Propriedades de curvas maximais com dimensão Frobenius 3 sobre Corpo Finito com 64 elementos

Tese apresentada ao Instituto de Matemática, Estatística e Computação Científica da Universidade Estadual de Campinas como parte dos requisitos exigidos para a obtenção do título de Doutora em Matemática.

Orientador: Saeed Tafazolian

Este trabalho corresponde à versão final da Tese defendida pela aluna Stéfani Concolato Vieira e orientada pelo Prof. Dr. Saeed Tafazolian.

Campinas

2021

Ficha catalográfica
Universidade Estadual de Campinas
Biblioteca do Instituto de Matemática, Estatística e Computação Científica
Ana Regina Machado - CRB 8/5467

V673p

Vieira, Stéfani Concolato, 1991-
Propriedades de curvas maximais com dimensão Frobenius 3 sobre corpo finito com 64 elementos / Stéfani Concolato Vieira. – Campinas, SP : [s.n.], 2021.

Orientador: Saeed Tafazolian.
Tese (doutorado) – Universidade Estadual de Campinas, Instituto de Matemática, Estatística e Computação Científica.

1. Curva maximal. 2. Corpos finitos (Álgebra). 3. Teoria de Stohr-Voloch. I. Tafazolian, Saeed, 1978-. II. Universidade Estadual de Campinas. Instituto de Matemática, Estatística e Computação Científica. III. Título.

Informações para Biblioteca Digital

Título em outro idioma: Properties of maximal curves with Frobenius dimension three over finite field with 64 elements
Palavras-chave em inglês:
Maximal curve
Finite fields (Algebra)
Stohr-Voloch theory
Área de concentração: Matemática
Titulação: Doutora em Matemática
Banca examinadora:
Saeed Tafazolian [Orientador]
Cícero Fernandes de Carvalho
Guilherme Chaud Tizziotti
Herivelto Martins Borges Filho
Nazar Arakelian
Data de defesa: 28-05-2021
Programa de Pós-Graduação: Matemática

Identificação e informações acadêmicas do(a) aluno(a)
- ORCID do autor: https://orcid.org/0000-0002-7659-0348
- Currículo Lattes do autor: http://lattes.cnpq.br/3490851972237082

Tese de Doutorado defendida em 28 de maio de 2021 e aprovada

pela banca examinadora composta pelos Profs. Drs.

Prof(a). Dr(a). SAEED TAFAZOLIAN

Prof(a). Dr(a). CÍCERO FERNANDES DE CARVALHO

Prof(a). Dr(a). NAZAR ARAKELIAN

Prof(a). Dr(a). HERIVELTO MARTINS BORGES FILHO

Prof(a). Dr(a). GUILHERME CHAUD TIZZIOTTI

A Ata da Defesa, assinada pelos membros da Comissão Examinadora, consta no SIGA/Sistema de Fluxo de Dissertação/Tese e na Secretaria de Pós-Graduação do Instituto de Matemática, Estatística e Computação Científica.

Em memória de Fernando Eduardo Torres Orihuela.

Agradecimentos

Agradeço primeiramente a Deus pode ter me sustentado até este momento nas poderosas mãos Dele. Agradeço aos meus orientadores Fernando e Saeed, por todo o suporte e dedicação, os quais proporcionaram o fruto deste trabalho. Não posso deixar de incluir um agradecimento especial ao professor Fernando e ressaltar o terrível pesar por sua súbita perda. A memória do professor Fernando sempre permancerá viva nos corações de todos aqueles que tiveram a grande honra de conhecê-lo e em toda sua grande obra, a qual sempre abrilhatará a Matemática durante toda a prosperidade. Suas palavras, seus conselhos e ensinamentos sempre estarão presentes na minha memória e em meu coração. Incluo um sincero agredimento ao professor Saeed pelo acolhimento num momento tão difícil e aceite de se tornar meu novo orientador. Seus ensinamentos também foram de grande importância para minha formação.

Agradeço ao apoio da minha família e de amigos, os quais compreenderam minha ausência e distância durante todo esse tempo de estudo e dedicação. Em especial ao meu esposo por todo companheirismo e dedicação expressados.

Agradeço à Universidade Estadual de Campinas, ao Instituto de Matemática, Estatística e Computação Científica, aos professores e companheiros de estudo pela tão grande contribuição para minha formação profissional. Em especial, agradeço aos professores da banca por sua honrosa participação nesta defesa.

O presente trabalho foi realizado com apoio da Coordenação de Aperfeiçoamento de Pessoal de Nível Superior – Brasil (CAPES) – Código de Financiamento 001. Também agradeço pelo apoio financeiro do Conselho Nacional de Desenvolvimento Científico e Tecnológico (CNPq), processo 141167/2019-0.

"Evidentemente, grande é o mistério da piedade:
Aquele que foi manifestado na carne
foi justificado em espírito,
contemplado por anjos, pregado entre os gentios,
crido no mundo, recebido na glória."
(Bíblia Sagrada, I Timóteo 3:16 - ARA)

Resumo

Neste trabalho, abordamos as principais propriedades de curvas maximais sobre corpos finitos cuja dimensão de Frobenius é igual a 3, principalmente as propriedades relacionadas ao comportamento de suas ordens genéricas. Como a maximalidade ocorre sobre corpos finitos com q^2 elementos, onde q é uma potência de um número primo, explicitamos uma classificação através dos gêneros possíveis de tais curvas com comportamento de ordens genéricas diferenciado, com $q \leqslant 29$.

Motivados pelos trabalhos de Fanali-Giulietti-Platoni, no mesmo contexto de curvas maximais com dimensão Frobenius 3, exibimos uma classificação para tais curvas sobre os corpos finitos, com 49 e com 64 elementos, em certas hipóteses através de recursos computacionais.

Palavras-chave: Curvas maximais. Corpos finitos. Dimensão Frobenius.

Abstract

In this work, we present an approach to the main properties of maximal curves over finite fields whose Frobenius dimension is equal to 3, specially the properties related to the behavior of their generic orders. Since maximality occurs over finite fields with q^2 elements, where q is a power of a prime number, we give a characterization through the genus of such curves which generic order behavior is special, with $q \leqslant 29$. In view of the Fanali-Platoni-Giulietti work's, in the same context of maximal curves with Frobenius dimension three, we show a classification for such curves on finite fields, with 49 and 64 elements, in certain hypotheses through computer softwares.

Keywords: Maximal curves. Finite Fields. Frobenius dimension.

Sumário

Introdução

O objeto curva, já conhecido no contexto de Geometria Algébrica sobre corpos algebricamente fechados, pode ser visto num contexto de Corpos Finitos. As aplicações nesta nova abordagem são interessantes em Teoria de Códigos, Criptografia e Geometria Finita. Para mais detalhes citamos os livros (HIRSCHFELD; KORCHMÁROS; TORRES, 2008), (HURT, 2003) e (STICHTENOTH, 2009). Denotaremos um corpo finito com l elementos por $\mathbb{F}_l$, onde l será uma potência de um número primo p, e $\overline{\mathbb{F}}_l$ o respectivo fecho algébrico. Assumiremos hipóteses adicionais para as curvas que serão nosso objeto de estudo aqui, a saber, uma curva sempre será algébrica, projetiva, não singular, geometricamente irredutível definida sobre $\mathbb{F}_l$. Um problema natural e central neste contexto é estimar a quantidade de elementos no conjunto de pontos de uma dada curva $\mathcal{X}$ em $\mathbb{P}^r(\mathbb{F}_l)$, denominado por conjunto de pontos $\mathbb{F}_l-$racionais, ao se considerar $\mathcal{X}$ mergulhada em $\mathbb{P}^r(\overline{\mathbb{F}}_l)$. Outro problema interessante é construir curvas com a propriedade de possuir "muitos pontos" $\mathbb{F}_l-$racionais. Devido aos trabalhos, em 1933 do matemático alemão Helmut Hasse e em 1940 do matemático francês André Weil, existe uma cota para a quantidade de pontos $\mathbb{F}_l-$racionais de uma curva e tal cota depende de um invariante da curva, denominado gênero. Enunciamos aqui o célebre resultado conhecido como *Cota de Hasse-Weil*: Se $\mathcal{X}$ é uma curva de gênero g então

$$\#\mathcal{X}(\mathbb{F}_l) \leqslant 1 + l + 2g\sqrt{l},$$

onde $\mathcal{X}(\mathbb{F}_l)$ é o conjunto de pontos $\mathbb{F}_l-$racionais de $\mathcal{X}$. Em particular, se uma curva atingir tal cota superior dizemos que esta curva é *maximal* sobre $\mathbb{F}_l$. Restringimos nosso foco neste trabalho apenas para curvas maximais, portanto assumiremos $l = q^2$, onde $q := p^m$, $m \in \mathbb{N}$.

Na literatura, podemos encontrar vários exemplos de curvas maximais. O problema de encontrar curvas maximais de um dado gênero sobre um corpo fixo $\mathbb{F}_{q^2}$, é conhecido na teoria como a determinação do *Espectro dos Gêneros* sobre $\mathbb{F}_{q^2}$, isto é, descrever o seguinte conjunto

$$\mathbf{M}(q^2) = \{g \in \mathbb{N}_0 : \text{ existe uma curva } k - \text{maximal de gênero } g\}.$$

Outro questionamento interessante é o conhecimento de possíveis equações, a menos de $\mathbb{F}_{q^2}-$isomorfismo, para curvas com gênero $g \in \mathbf{M}(q^2)$. Sobre tais problemas, muitas perguntas já foram respondidas. Podemos citar, por exemplo em (IHARA, 1981), Ihara utilizando da veracidade da Hipótese de Riemann para curvas sobre Corpos Finitos, observou a seguinte inclusão

$$\mathbf{M}(q^2) \subseteq [0, g_0],$$

onde $g_0 = q(q-1)/2$. Isto restrigiu a quantidade de gêneros possíveis em $\mathbf{M}(q^2)$, descartando vários valores. A respeito das equações possíveis para uma curva com gênero g_0, em (RÜCK; STICHTENOTH, 1994), os matemáticos Rück e Stichtenoth mostraram que a curva Hermitiana $\mathcal{H}_{q+1} : x^q + x = y^{q+1}$ é a única curva maximal, a menos de isomorfismo, com tal gênero.

No primeiro capítulo deste trabalho, apresentamos algumas ferramentas para obter outros tipos de refinamento da inclusão do Espectro dos gêneros. O uso de séries lineares nos permite atacar tal problema a partir de um ponto de vista mais geométrico, pois podemos associá-la a certos invariantes, os quais fornecem propriedades algébricas interessantes para caracterizar propriedades de uma curva maximal. A teoria desenvolvida em (STÖHR; VOLOCH, 1986) é aplicada para uma série particular com boas propriedades, a saber, a série Frobenius $\mathcal{D} := |(q+1)P_0|$, onde P_0 um ponto $\mathbb{F}_{q^2}-$racional de uma curva $\mathbb{F}_{q^2}-$maximal $\mathcal{X}$. A primeira propriedade interessante de tal série é a independência da escolha do ponto P_0, conhecida como *Equivalência Fundamental*, (RÜCK; STICHTENOTH, 1994). A equivalência natural existente entre uma série linear de dimensão r livre de ponto base e morfismo não degenerado em $\mathbb{P}^r$, nos permite associar $\mathcal{D}$ ao morfismo $\pi : \mathcal{X} \longrightarrow \mathbb{P}^r$. Da teoria, pode-se observar que $r \geqslant 2$ e π é um mergulho ou *embedding*. Com estes conceitos, outra cota para o gênero de uma curva maximal foi obtida por Castelnuovo aplicada a $\pi(\mathcal{X})$:

$$g \leqslant c_0(r, q+1),$$

onde c_0 depende de q e da dimensão Frobenius r de $\mathcal{X}$. Mais detalhes e aplicações destas ferramentas serão apresentados no primeiro capítulo deste texto.

Com tais ferramentas, em (FUHRMANN; TORRES, 1996), foi verificado que

$$\mathbf{M}(q^2) \subseteq [0, g_1] \cup \{g_0\}$$

onde $g_1 := \lfloor (q-1)^2/4 \rfloor$ e em (KORCHMÁROS; TORRES, 2002) foi constatado um refinamento ainda melhor,

$$\mathbf{M}(q^2) \subseteq [0, g_2] \cup \{g_1\} \cup \{g_0\},$$

onde $g_2 := \lfloor (q^2 - q + 4)/6 \rfloor$. Atualmente os valores de $\mathbf{M}(q^2)$ para $q \leqslant 7$ já foram completamente determinados, (ARAKELIAN; TAFAZOLIAN; TORRES, 2018). Para valores de $q \leqslant 29$, em (MONTANUCCI; ZINI, 2018) foi explicitado vários valores de gênero em $\mathbf{M}(q^2)$ para o caso particular de curvas Galois-coberta pela curva Hermitiana.

Fixado a dimensão Frobenius r de uma curva $\mathbb{F}_{q^2}-$maximal, também existe um estudo de classificação através das ordens associadas à série Frobenius. Pela maximalidade, várias restrições algébricas foram construídas para as ordens génericas $\mathcal{E} : \varepsilon_0 < \varepsilon_1 < ... < \varepsilon_r$ e as ordens de Frobenius $\mathcal{V} : \nu_0 < \nu_1 < ... < \nu_{r-1}$. Quando a dimensão Frobenius é igual a 2, já é de conhecimento que a única possibilidade é a curva Hermitiana. No capítulo

2, é feito uma abordagem no comportamento de tais ordens. É conhecido na literatura o conceito do comportamento das ordens denominado *Frobenius-clássica*, isto é, quando $\mathcal{V} = \{0, 1, ..., r-1\}$. Introduzimos um novo conceito de quase-classicalidade, já que curvas maximais não são clássicas a respeito da série Frobenius (FUHRMANN; GARCIA; TORRES, 1997), aqui o conhecimento de semigrupo de Weierstrass é necessário. Mas podemos estudar o comportamento bem parecido, a saber, quando $\mathcal{V} = \{0, 1, ..., r-2, q\}$, o qual chamaremos nesta tese de *Frobenius quase-classicalidade*. Como as ordens génericas estão associadas a ordens Frobenius, também denotaremos uma nomeclatura para o comportamento $\mathcal{E} = \{0, 1, ..., r-1, q\}$, o chamamos de *quase-classicalidade* apenas. Quando a dimensão Frobenius é igual a 2, já é conhecido o comportamento das ordens e, portanto, obtemos ambos tipos de quase-classicalidade. Podemos nos perguntar condições para estes tipos de quase-classicalidade quando a dimensão de Frobenius é maior ou igual a 3. Neste capítulo apresentamos que toda curva $\mathbb{F}_{p^2}-$maximal de gênero $g > 0$ é (Frobenius) quase-clássica, toda curva maximal de $g > 0$ e com dimensão Frobenius igual a 3 é Frobenius quase-clássica. Se $c_0(4, q+1) < g \leqslant c_0(3, q+1)$ e $p \neq 3$ então temos quase-classicalidade. Também apresentamos para quais valores de q menores ou igual a 29, os casos em que pode-se ocorre não quase-classicalidade para dimensão Frobenius igual a 3.

No capítulo 3, apresentamos o caso de Frobenius dimensão 3 para caracterizar modelos planos curvas maximais a partir de curvas computacionais e os trabalhos desenvolvidos em (FANALI; GIULIETTI, 2009), a qual utiliza o conhecido resultado do Teorema do Embedding Natural de curvas maximais (KORCHMÁROS; TORRES, 2001). A classificação é conhecida para $q \leqslant 5$. Quando $q = 7$, apresentamos uma classificação completa, proviente da junção dos trabalhos em (FANALI; GIULIETTI; PLATONI, 2012) e (ARAKELIAN; TAFAZOLIAN; TORRES, 2018). Neste caso, temos apenas duas curvas, $Y^4 = X^7 + X$ de gênero 9 e $Y^7 - YX^4 + \omega X^2 = 0$ com $\omega^8 = -1$ tem gênero 7. Quando $q = 8$, a classificação de curvas maximais com dimensão Frobenius igual a 3 se torna mais árdua. Devido altos custos computacionais, nos adequamos a certas hipóteses aqui. Os possíveis gêneros neste caso são $9, 10$ e 12. Como a unicidade, a menos de isomorfismo, de um modelo para gênero 12 é conhecida, nos restrigimos aos gêneros 9 e 10.

1 Preliminares

Neste capítulo apresentamos as definições e resultados necessários para construção de nossos resultados. Denotamos por $\mathbb{F}_q$ um corpo finito com q elementos de característica $p > 0$ e k o fecho algébrico de $\mathbb{F}_q$. O espaço projetivo $r-$dimensional sobre k será denotado por $\mathbb{P}^r(k)$.

1.1 Alguns aspectos de curvas algébricas

Seja $\mathcal{X}$ uma curva projetiva não singular sobre k. Podemos associar a curva $\mathcal{X}$, a qual é um objeto geométrico, com algumas estruturas algébricas. Tais estruturas algébricas podem ser encontradas em Teoria de Corpos de Funções Algébricas, (STICHTENOTH, 2009). Dependendo da situação poderemos optar em utilizar a abordagem mais algébrica ao invés de uma mais geométrica, pois podemos explicitar uma equivalência entre tais conceitos. Por exemplo, uma destas estruturas algébricas associadas a curva $\mathcal{X}$ é o corpo de funções racionais de $\mathcal{X}$, denotado por $k(\mathcal{X})$. Os pontos de $\mathcal{X}$ se correspondem biunivocamente entre os lugares, ou *places*, de $k(\mathcal{X})$ via o mapa

$$P \in \mathcal{X} \mapsto M_P(\mathcal{X}),$$

onde $M_P(\mathcal{X})$ é o ideal maximal do anel local de $\mathcal{O}_P(\mathcal{X}) := \{f \in k(\mathcal{X}) : f \text{ é definida em } P\}$. Outra correspondência que utilizaremos é para o invariante gênero. O gênero do corpo de funções $k(\mathcal{X})$ coincide com o gênero da curva $\mathcal{X}$. Apresentamos nesta seção alguns destes conceitos algébricos.

Neste texto quando nos referirmos ao termo **curva** estamos assumindo uma curva algébrica projetiva não singular, absolutamente irredutível definida sobre k.

Alguns resultados de Teoria Corpos de Funções Algébricas

Utilizando a linguagem de Teoria de Corpos de Funções Algébricas, iremos enxergar o estudo de curvas de um ponto de vista algébrico. Reservamos esta subseção para explanar alguns resultados e definições importantes para apresentação dos resultados principais da tese.

Para uma curva $\mathcal{X}$, vamos denotar $F = k(\mathcal{X})$ o corpo de funções de $\mathcal{X}$ e $\mathbb{P}_F$ o conjunto de pontos de $\mathcal{X}$. Em Teoria de Corpos de Funções Algébricas, $\mathbb{P}_F$ é conhecido como conjunto de lugares da extensão $F|k$.

Definição 1.1. *Um **divisor** é uma soma formal* $D = \sum_{P \in \mathcal{X}} n_P P$, *com* $n_P \in \mathbb{Z}$ *e* $n_P = 0$ *para todos menos um número finito de pontos* $P \in \mathcal{X}$. *O **grau de** D é o valor* $\deg D := \sum n_P$ *e o **suporte** de um divisor é o conjunto de pontos com coeficientes não nulos.*

Sejam $D = \sum n_p P$ e $D' = \sum n'_P P'$ dois divisores de $\mathcal{X}$. Definimos a soma de $D + D'$ sendo

$$\sum_{P \in \mathcal{X}} (n_P + n'_p) P$$

e o divisor zero como $0 := \sum_P r_P P, \quad$ com $r_P = 0$ para todo P. Chamamos de **grupo de divisores** de $\mathcal{X}$, denotado por $Div(\mathcal{X})$, o grupo abeliano livre formado pelos divisores de $\mathcal{X}$. No caso especial em que os coeficientes de um divisor são todos não negativos, dizemos que o divisor é **efetivo**. Usando este conceito podemos definir uma ordenação parcial em $Div(\mathcal{X})$, a saber, dizemos que $D \geqslant D'$ se $D - D'$ é efetivo.

Outro tipo interessante de divisores são aqueles relacionados com funções racionais.

Definição 1.2. *Se f é uma função racional em $\mathcal{X}$, não identicamente nula, o **divisor de** f sendo*

$$div(f) = \sum_{P \in \mathcal{X}} v_P(f) P$$

*onde v_p denota a valorização discreta de f. O divisor de uma função racional é chamado **divisor principal**. O **divisor de pólo** de f é $div_\infty(f) := \sum_{P \in \mathcal{X}, v_P(P) < 0} v_p(f) P$ e o **divisor de zeros** de f é $div_\infty(f) := \sum_{P \in \mathcal{X}, v_P(P) > 0} v_p(f) P$.*

O conjunto dos divisores principais é chamado de **grupo dos divisores principais** e denotado por $Prin(\mathcal{X})$. Com esta noção de divisor principal, podemos particionar o grupo $Div(\mathcal{X})$ com a seguinte relação de equivalência. Denotamos $D \sim D'$ e dizemos D é **linearmente equivalente** a D' se $D - D'$ é um divisor principal. Para cada divisor em $Div(\mathcal{X})$ podemos associar um espaço vetorial. Este está relacionado ao estudo de série lineares e também está profundamente asssociado à construção de um invariante de $\mathcal{X}$, o qual será definido posteriormente.

Definição 1.3. *Para cada $D \in Div(\mathcal{X})$, considere o espaço vetorial sobre k dado por*

$$\mathcal{L}(D) := \{f \in k(\mathcal{X})^* : \ div(f) + D \geqslant 0\} \cup \{0\}.$$

*Chamamos-o de **espaço de Riemann-Roch** associado ao divisor D e denotamos $l(D) := dim_k(\mathcal{L}(D))$.*

Note que se escrevermos $D = \sum_{i=1}^{r} n_i P_i - \sum_{j=1}^{s} m_j Q_j$ com $n_i, m_j > 0$, então o espaço $\mathcal{L}(D)$ é formado pelas funções em $k(\mathcal{X})$, as quais possuem zeros de multiplicidade pelo menos m_j em Q_j e que tais funções não têm polos, exceto possivelmente nos pontos P_i, com ordem no máximo n_i.

Podemos relacionar o grau de um divisor e a dimensão do espaço de Riemann-Roch associado a esse divisor.

Teorema 1.4. *(i) Se deg* $D < 0$*, então* $l(D) = 0$;

(ii) $l(D) \leqslant 1 + deg\ D$;

(iii) existe $\gamma \in \mathbb{Z}$ *tal que deg* $A - l(A) \leqslant \gamma$*, para todo* $A \in Div(\mathcal{X})$.

Demonstração: Para os itens (i) e (ii) veja Corolário 1.4.12 e para o item (iii) veja Proposição 1.4.14 em (STICHTENOTH, 2009). ▫

Pelo resultado anterior podemos assumir o máximo do valor $degA - l(A) + 1$ percorrendo todos os divisores A de $\mathcal{X}$ e definir o **gênero** de $k(\mathcal{X})$ como

$$g := max\{deg\ A - l(A) + 1 : A \in Div(F)\}.$$

Observamos que usando o divisor nulo obtemos que o gênero é sempre não negativo. Quando um divisor $W \in Div(\mathcal{X})$ satisfaz $deg\ W = 2g - 2$ e $l(W) = g$, dizemos que W é um divisor **canônico**. Este divisor é extremamente importante para cálculo da dimensão de um espaço de Riemann-Roch.

Teorema 1.5 (Teorema de Riemann-Roch)**.** *Se* $D \in Div(\mathcal{X})$*, então para qualquer divisor canônico* W *temos*

$$l(D) = 1 + deg\ D - g + l(W - D),$$

onde g *é o gênero* $\mathcal{X}$.

Demonstração: Ver Teorema 1.5.15 em (STICHTENOTH, 2009). ▫

Em particular o cálculo da dimensão de espaços de Riemann-Roch associado a divisores com grau maior estrito que $2g - 2$, como no resultado a seguir.

Corolário 1.6. *Seja* $D \in Div(\mathcal{X})$ *de gênero* g *e deg* $D > 2g - 2$*. Então*

$$l(D) = deg\ D + 1 - g.$$

Demonstração: Seja W um divisor canônico. Como $deg\ D \geqslant 2g-1$ e $deg\ W = 2g-2$ segue que $deg(W - D) < 0$. Aplicando o Teorema 1.4 obtemos $l(W - D) = 0$ e aplicando o Teorema 1.5 obtemos o resultado. ▫

Semigrupo de Weierstrass

Para uma curva $\mathcal{X}$, em geral temos

$$l(mP) \leqslant l((m-1)P) + 1,$$

para todo $P \in \mathcal{X}$ e $m \in \mathbb{N} \cup \{0\}$ (ver Lema 1.4.8, (STICHTENOTH, 2009)). Quando ocorre a igualdade, dizemos que m é uma **não-lacuna**, ou *non-gap*, de P. Caso contrário, dizemos que m é uma **lacuna** de P. Consideramos para cada $P \in \mathcal{X}$, o conjunto

$$H(P) := \{m \in \mathbb{N} : m \text{ é uma não-lacuna em } P\} \cup \{0\}.$$

Observamos que m é uma não-lacuna em P se, e somente se, existe uma função racional com polo de ordem m em P e não possui outros polos em $\mathcal{X}$ além de P. Logo se $m_1, m_2 \in H(P)$ então existem funções racionais f_1, f_2 em $\mathcal{X}$ tais que $v_P(f_1) = -m_1$ e $v_P(f_2) = -m_2$, assim $f_1 \cdot f_2$ é uma função racional em $\mathcal{X}$ tal que $v_P(f_1 f_2) = v_P(f_1) + v_P(f_2) = -(m_1 + m_2)$ então $m_1 + m_2 \in H(P)$. Isto é, $H(P)$ é fechado em relação à soma. Convencionamos uma escrita para os elementos de $H(P)$, como uma sequência ordenada $(m_i)_{i \geqslant 0}$, onde $m_0 = 0$ e $m_{i-1} < m_i$ para $i \in \mathbb{N}_0$. O resultado a seguir mostra que o conjunto de lacunas num ponto $P \in \mathcal{X}$ é finito.

Teorema 1.7 (Teorema das lacunas de Weierstrass)**.** *O número de lacunas de $P \in \mathcal{X}$ é igual ao gênero g da curva $\mathcal{X}$.*

Demonstração: Com efeito, se $i > 2g - 2$ então pelo Corolário 1.6 temos $l(iP) = i + 1 - g$. Daí

$$l(iP) = i + 1 - g = l((i-1)P) + 1 \text{ para } i > 2g - 1$$

logo $[2g, +\infty) \subseteq H(P)$. Como $1 = l(0) \leqslant l(P) \leqslant ... \leqslant l((2g-1)P) = g$ segue que as desigualdades são estritas, isto é, temos g números que são lacunas em P. ▫

O teorema acima, garante que o conjunto $H(P)$ é um semigrupo de $\mathbb{N} \cup \{0\}$ e é chamado de **semigrupo de Weierstrass** em P. Os semigrupos de Weierstrass fornecem propriedades interessantes de curvas, principalmente no contexto de corpos finitos que estamos interessados.

1.2 Mergulhos Projetivos e Sistemas Lineares

Seja $\mathcal{X}$ uma curva projetiva, irredutível e não singular sobre um corpo algebricamente fechado k. Como uma curva é um tipo particular de variedade projetiva não singular, podemos associá-la aos sistemas lineares.

Denotamos por $k(\mathcal{X})$ o corpo de funções de $\mathcal{X}$ e $Div(\mathcal{X})$ o conjunto dos divisores de $\mathcal{X}$. Seja $E \in Div(\mathcal{X})$. Definimos um **sistema linear** em $\mathcal{X}$ como um subconjunto da forma

$$\{E + div(f) : f \in \mathcal{D}'\backslash\{0\}\},$$

para algum $\mathcal{D}'$ é um $k-$subespaço de $\mathcal{L}(E)$. Em particular, se $\mathcal{D}' = \mathcal{L}(E)$ dizemos é um **sistema linear completo** de $\mathcal{X}$ e denotamos por $|E|$. O sistema linear completo $|E|$ é dito **canônico**, se E é um divisor canônico de $\mathcal{X}$. A **dimensão projetiva** de $\mathcal{D}$ é definida como $dim(\mathcal{D}) := dim(\mathcal{D}') - 1$ e o **grau** de $\mathcal{D}$ é igual ao grau de E. Podemos denotar uma série linear $r-$dimensional de grau d por g^r_d.

Seja $\mathcal{D}$ um sistema linear g^r_d. Para cada $i \in \mathbb{N} \cup \{0\}$ e $P \in \mathcal{X}$, consideramos o conjunto

$$\mathcal{D}_i(P) := \{D \in \mathcal{D} : D \geq iP\}.$$

Logo $\mathcal{D} = \mathcal{D}_0(P) \supseteq \mathcal{D}_1(P) \supseteq ... \supseteq \mathcal{D}_i(P) \supseteq \mathcal{D}_{i+1}(P) \supseteq ...$ e se d é o grau de $\mathcal{D}$ então $\mathcal{D}_i = \varnothing$ para $i > d$. Assim para cada $P \in \mathcal{X}$ tem-se

$$\mathcal{D}_i(P) = \{E + div(f) : f \in \mathcal{D}'_i(P)\backslash\{0\}\}$$

onde $\mathcal{D}'_i(P) := \mathcal{D}' \cap \mathcal{L}(E - iP)$, portanto $\mathcal{D}_i(P)$ é uma série linear e é um subespaço de $\mathcal{D}$.

Lema 1.8. *Para cada $P \in \mathcal{X}$ temos $dim\ \mathcal{D}_i(P) \leqslant dim\ \mathcal{D}_{i+1}(P) + 1$ para todo $i \in \mathbb{N} \cup \{0\}$.*

Demonstração: Como para cada $P \in \mathcal{X}$ temos o $k-$isomorfismo entre $\mathcal{D}'_i(P)/\mathcal{D}'_{i+1}(P)$ ao $k-$espaço $\mathcal{L}(E - iP)/\mathcal{L}(E - (i+1)P)$, o qual tem dimensão menor ou igual a 1. ▫

Para cada ponto $P \in \mathcal{X}$, definimos a **multiplicidade** de $\mathcal{D}$ em P por $b(P) := min\{v_P(D) : D \in \mathcal{D}\}$. Se um divisor efetivo $B \in \mathcal{D}$ satisfaz $v_P(B) = b(P)$ chamamos B de **base local** para $\mathcal{D}$. Um divisor efetivo é chamado de **ponto base** para $\mathcal{D}$ se pertencer ao suporte de cada $D \in \mathcal{D}$. No caso particular que $B = 0$ dizemos que a série $\mathcal{D}$ é **livre de ponto base**.

Observação 1.9. *Se B é uma base local de $\mathcal{D}$, segue pela ordenação em $Div(\mathcal{X})$ que $D \geqslant B$ para todo $D \in \mathcal{D}$. Definimos o subconjunto de divisores efetivos*

$$\mathcal{D}^B := \{D - B : D \in \mathcal{D}\}$$

que é uma série linear $r-$dimensional livre de ponto base de grau $d - degB$.

Associando um Sistema Linear a um dado morfismo

Seja $f : \mathcal{X} \longrightarrow \mathbb{P}^r(k)$ um morfismo não degenerado, isto é, $f(\mathcal{X})$ não está contida num hiperplano de $\mathbb{P}^r(k)$. Considere

$$f = (f_0 : \cdots : f_r)$$

onde $f_0, ..., f_r \in k(\mathcal{X})$. Como as funções f_i são unicamente determinadas por f via um fator de proporcionalidade em $k(\mathcal{X})\backslash\{0\}$, o morfismo f corresponde a um ponto de $\mathbb{P}^r(k(\mathcal{X}))$. Para cada ponto $P \in \mathcal{X}$ seja t é uma função racional em $k(\mathcal{X})$ tal que $v_P(t) = 1$, isto é, t é o **parâmetro local em** P de $\mathcal{X}$. Assim para cada $P \in \mathcal{X}$ então

$$f(P) = ((t^{e_P} f_0)(P) : \ldots : (t^{e_P} f_r)(P))$$

onde $e_P := -min\{v_P(f_0), ..., v_P(f_r)\}$.

Iremos considerar $f : \mathcal{X} \longrightarrow \mathbb{P}^r(k)$ como uma curva parametrizada em $\mathbb{P}^r(k)$ e os pontos de $\mathcal{X}$ serão vistos como seus ramos, isto é, para cada $Q \in f(\mathcal{X})$ os pontos das fibras de $f^{-1}(Q)$ são os **ramos de** $f(\mathcal{X})$ **centrados em** Q. Dizemos que o **grau do morfismo** f é

$$deg(f) := [k(\mathcal{X}) : k(f(\mathcal{X}))].$$

Em particular, quando $deg(f) = 1$ dizemos que f é **birracional** e quando $\mathcal{X}$ é $k-$isomorfa a $f(\mathcal{X})$, dizemos que f é um *embedding* ou **mergulho**. Em ambos casos, dizemos que $\mathcal{X}$ é o *modelo não singular* de $f(\mathcal{X})$.

Queremos estudar os divisores de interseção de $f(\mathcal{X})$ e hiperplanos de $\mathbb{P}^r(k)$. Considere $H := \left\{ (x_0 : \ldots : x_r) \in \mathbb{P}^r(k) : \sum_{i=0}^{r} a_i x_i = 0 \right\}$. O hiperplano H intersecta o ramo $P \in \mathcal{X}$ com multiplicidade $v_P\left(\sum_{i=0}^{r} a_i f_i\right) + e_p$. Então o divisor de interseção $f^{-1}(H)$ da curva parametrizada por f e o hiperplano H é dado por

$$f^{-1}(H) = div\left(\sum_{i=0}^{r} a_i f_i\right) + E$$

onde $E := \sum e_P P$. Portanto, associamos o morfismo f ao sistema

$$\left\{ f^{-1}(H) : H \text{ hiperplano em } \mathbb{P}^r(k) \right\}$$

chamado de **sistema linear de seções de hiperplanos**. Caso $\mathcal{X} \subset \mathbb{P}^r(k)$, podemos considerar o morfismo identidade, então o sistema linear de seções de hiperplanos coincide com o conjunto de divisores de interseção entre $\mathcal{X}$ e os hiperplanos de $\mathbb{P}^r(k)$.

Observação 1.10. *O sistema linear de seções de hiperplanos é livre de pontos base.*

Associando um morfismo a um dado sistema linear de livre de ponto-base

Seja $\mathcal{D}$ sistema linear de divisores de $\mathcal{X}$, que é livre de pontos base de dimensão r. Então

$$\mathcal{D} = \{E + div(f) : f \in \mathcal{D}'\backslash\{0\}\}$$

para algum $\mathcal{D}'$ um $k-$subespaço de $\mathcal{L}(E)$ e algum $E \in Div(\mathcal{X})$. Vamos construir um morfismo não degenerado associado a $\mathcal{D}$. Como $dim\mathcal{D}' = r+1$ asumimos $\mathcal{D}' := \langle f_0, ..., f_r \rangle$ com $f_i \in k(\mathcal{X})$. Pode-se verificar a seguinte relação

$$v_P(E) = b(P) - min\{v_P(f_0), ..., v_P(f_r)\}. \tag{1.1}$$

Construímos o morfismo a seguir,

$$\begin{array}{rcl} \mathcal{X} & \longrightarrow & \{\mathcal{D}_{b(P)+1} : P \in \mathcal{X}\} \\ P & \mapsto & \mathcal{D}_{b(P)+1} \end{array}$$

Como $\mathcal{D}_{b(P)+1} \subsetneq \mathcal{D}_{b(P)} = \mathcal{D}$ então $dim\ \mathcal{D}_{b(P)+1} = r-1$. Para cada $P \in \mathcal{X}$, seja um parâmetro local t em P e considere o mapa entre $\mathcal{D}_{b(P)+1}(P) \longrightarrow \mathbb{P}^r(k)$ dado por

$$E + div\left(\sum_{i=0}^{r} a_i f_i\right) \longmapsto \left\{(a_0 : a_1 : ... : a_r) : \sum_{i=0}^{r} \left(t^{v_P(E)-b(P)} f_i\right)(P) a_i = 0\right\}.$$

Seja $f \in \mathcal{D}' \backslash \{0\}$, então $f = \sum_{i=0}^{r} a_i f_i$ com $a_0, a_1, ..., a_r \in k$ e algum $a_i \neq 0$. Note que $E + div\left(\sum_{i=0}^{r} a_i f_i\right) \in \mathcal{D}_{b(P)+1}(P)$ se, e somente se, $E + div\left(\sum_{i=0}^{r} a_i f_i\right) \geq (b(P)+1)P$ se, e somente se, $v_P\left(E + div\left(\sum_{i=0}^{r} a_i f_i\right)\right) \geqslant b(P)+1$. Por isto e por (1.1), segue que $E + div\left(\sum_{i=0}^{r} a_i f_i\right) \in \mathcal{D}_{b(P)+1}(P)$ se, e somente se, $v_P\left(\sum_{i=0}^{r} a_i t^{v_P(E)-b(P)} f_i\right) \geqslant 1$ se, e somente se, $\sum_{i=0}^{r} a_i t^{v_P(E)-b(P)} f_i(P) = 0$. Logo $\mathcal{D}_{b(P)+1}(P) \cong \left\{(a_0 : a_1 : ... : a_r) : \sum_{i=0}^{r} \left(t^{v_P(E)-b(P)} f_i\right)(P) a_i = 0\right\}$. Então associamos a $\mathcal{D}$ o morfismo

$$\begin{array}{rcl} \phi_{\mathcal{D}} : \mathcal{X} & \longrightarrow & \mathbb{P}^r(k) \\ P & \longmapsto & \left((t^{v_P(E)-b(P)} f_0)(P), ..., (t^{v_P(E)-b(P)} f_r)(P)\right) \end{array}$$

Segue de (1.1) que $\phi_{\mathcal{D}}(P) = (t^{e_P} f_0(P) : ... : t^{e_P} f_r(P))$ para $P \in \mathcal{X}$, isto é, $\phi_{\mathcal{D}} = (f_0 : f_1 : ... : f_r)$ é unicamente determinado, via equivalência projetiva.

Observação 1.11. *O morfismo $\phi_{\mathcal{D}}$ é não degenerado, já que $f_0, ..., f_r$ é uma base de $\mathcal{D}$.*

Seja $\mathcal{L}_r$ conjunto das séries lineares $\mathcal{D}^B$ onde $\mathcal{D}$ é uma série $r-$dimensional em $\mathcal{X}$. Para cada morfismo $\phi : \mathcal{X} \longrightarrow \mathbb{P}^r(k)$ não degenerado, consideramos a classe respectiva por $\overline{\phi} := \{T \circ \phi : T \in Aut(\mathbb{P}^r(k))\}$. Com esta relação de equivalência definida, seja $\mathcal{M}_r$ o conjunto das classes de morfismos não degenerados. O resultado a seguir nos permite transitar entre as séries lineares livres de ponto-base e os morfismos não degenerados.

Teorema 1.12. *O conjunto das séries lineares $r-$dimensionais livres de ponto base em $\mathcal{X}$ é equivalente ao conjunto das classes de morfismos $\mathcal{X} \longrightarrow \mathbb{P}^r(k)$ não degenerado via equivalência projetiva.*

Demonstração: Defina para cada $r > 0$ os mapas

$$\begin{array}{rccl} \Theta_r: & \tilde{\mathcal{L}}_r & \longrightarrow & \mathcal{M}_r \\ & \mathcal{D} & \mapsto & \overline{\text{representação em coordenadas de } \phi_{\mathcal{D}}} \end{array} \qquad \text{e}$$

$$\begin{array}{rccl} \Gamma_r: & \mathcal{M}_r & \longrightarrow & \mathcal{L}_r \\ & \overline{\phi} & \mapsto & \mathcal{D}_{\phi} \end{array}$$

onde $\tilde{\mathcal{L}}_r$ é o subconjunto de $\mathcal{L}_r$ das séries lineares livres de ponto base. Seja $\mathcal{D}$ uma série livre de ponto base, onde $\{f_0, f_1, ..., f_r\}$ é uma base de $\mathcal{D}'$. Daí

$$\begin{aligned} \Gamma_r \circ \Theta_r(\mathcal{D}) &= \Gamma(\overline{\text{representação em coordenadas de } \phi_{\mathcal{D}}}) = \mathcal{D}_{\phi_{\mathcal{D}}} = \mathcal{D} = Id_{\mathcal{L}_r} \text{ e} \\ \Theta_r \circ \Gamma_r(\overline{\phi}) &= \Theta_r(\mathcal{D}_{\phi}) = \overline{\text{representação em coordenadas de } \phi_{\mathcal{D}_{\phi}}} = \overline{\phi} = Id_{\mathcal{M}_r}. \quad \square \end{aligned}$$

Invariantes Hermitianos

Seja $\mathcal{D}$ um sistema linear em $\mathcal{X}$ de dimensão r e grau d.

Definição 1.13. *Um inteiro não negativo j é dito uma $(\mathcal{D}, P)-$**ordem** se $\mathcal{D}_{j+1}(P) \subsetneq \mathcal{D}_j(P)$.*

Podemos observar que $\mathcal{D}_i$ é vazio quando $i > d$. No caso em que $\mathcal{D}$ é um sistema linear de seções de hiperplanos, um inteiro j é um $P-$**invariante hermitiano de** $\mathcal{D}$ ou simplesmente uma $(\mathcal{D}, P)-$**ordem** se existe $D \in \mathcal{D}$ tal que $v_P(D) = j$. Isto significa que existe um hiperplano intersectando o ramo P com multiplicidade j. Pelo Lema 1.8, para cada $P \in \mathcal{X}$ existem exatamente $r+1$ inteiros $(\mathcal{D}, P)-$ordens. Vamos denotá-las por

$$j_0(P) < j_1(P) < ... < j_{r-1}(P) < j_r(P).$$

Observação 1.14. *(a) $j_r(P) \leqslant d$;*

(b) Quando P não é um ponto-base de $\mathcal{D}$, obtemos $j_0(P) = 0$.

(c) $j_1(P) = 1$.

Se o sistema linear $\mathcal{D}$ for completo então, pelo Teorema 1.5, obtemos

$$r = d - g \quad \text{ se } d > 2g - 2$$

e $dim\ \mathcal{D}_i = d - i - g$ se $0 \leqslant i \leqslant d - 2g + 1$. Portanto $j_i(P) = i$ quando $i \leqslant d - 2g$ para todo $P \in \mathcal{X}$.

Para cada $P \in \mathcal{X}$, as $(\mathcal{D}, P)-$ordens nos dão informações geométricas sobre a existência de hiperplanos intersectando em P e suas respectivas multiplicidades. Queremos descrever de maneira algébrica essas informações. Primeiramente utilizaremos uma parametrização local t em P. Observamos que para cada $l \in \{0, 1, ...r\}$ existe $f_l \in k(\mathcal{X})$ tal que

$$v_P(t^{v_P(E)} f_l) = j_l(P).$$

O conjunto $\{f_0, \ldots, f_r\}$ é uma base para $\mathcal{D}'$, a qual é chamada **base** $(\mathcal{D}, P)-$**Hermitiana** ou $(\mathcal{D}, P)-$base. Como $D_{j_i}(P) = \left\{ E + div\left(\sum_{l=i}^{r} a_l f_l\right) : (a_i : \ldots : a_r) \in \mathbb{P}^{r-i}(k) \right\}$ temos $j_i(P) = min\left\{ v_P\left(\sum_{l=1}^{r} a_l f_l t^{v_P(E)}\right) : (a_i : \ldots : a_r) \in \mathbb{P}^{r-i}(k) \right\}$.

Como estamos interessados em corpos com característica positiva e os planos osculadores dependem das derivadas das funções coordenadas f_i, usaremos derivadas de Hasse. Relembramos que a $i-$ésima Derivada de Hasse em relação a t, denotada por $D_t^{(i)}$, é definida em $k[t]$ por

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

Esta se estende naturalmente ao $k(t)$ e para cada extensão de corpos finita separável de $k(t)$.

Para cada $l \in \mathbb{N}_0$ consideramos o vetor $D_t^{(l)} f := (D_t^{(l)} f_0, \ldots, D_t^{(l)} f_r)$. Como cada coordenada deste vetor é regular em P, também definimos

$$(D_t^{(l)} f)(P) := (D_t^{(l)} f_0(P), \ldots, D_t^{(l)} f_r(P)).$$

Queremos construir uma sequência de inteiros $0 \leqslant m_0 < ... < m_r$ tais que

$$D_t^{(m_0)} f(P), \ldots, D_t^{(m_r)} f(P)$$

são $k(\mathcal{X})-$linearmente independentes. Definimos o conjunto $\mathcal{A}(g_0, \ldots, g_r; t)$ sendo

$$\left\{ (n_0, \ldots, n_r) \in \mathbb{N}_0^{r+1} : n_0 < ... < n_r \text{ e } W_{g_0,\ldots,g_r;t}^{n_0,\ldots,n_r} := det(D_t^{(n_i)} g_j)_{0 \leqslant i,j \leqslant r} \neq 0 \right\}$$

onde $g_l := t^{v_P(E)} f_l$ para $l = 0, ..., r$. Denotamos também

$$D_t^{(l)} g := (D_t^{(l)} g_0 : \ldots : D_t^{(l)} g_r).$$

O resultado a seguir nos fornece um critério aritmético para obter vetores em $\mathcal{A}(g_0, ..., g_r; t)$.

Lema 1.15. *Se $m_0 < \ldots < m_r$ é uma sequência de inteiros não negativos tais que*

$$det\left(\binom{j_l(P)}{m_i}\right)_{0 \leqslant i,l \leqslant r} \not\equiv 0 \ mod\ p,$$

então $(m_0, \ldots, m_r) \in \mathcal{A}(g_0, \ldots, g_r; t)$.

Demonstração: Para cada $l \in \{0,1,...,r\}$, seja $g_l = \sum_{s=j_l}^{\infty} c_s^l t^s$ com $c_{j_l}^l \neq 0$ a expansão local de g_l em P. Então

$$\begin{aligned} W_{g_0,\ldots,g_r;t}^{m_0,\ldots,m_r} &= det\left(\sum_{s=j_l}^{\infty}\binom{s}{m_i}c_s^l t^{s-m_i}\right)_{0\leqslant i,l\leqslant r} = Ct^{-\sum_i m_i} det\left(\sum_{s=j_l}^{\infty}\frac{c_s^l}{m_i!}t^s\right)_{0\leqslant i,l\leqslant r} \\ &= Cdet\left(\binom{j_l}{m_i}\right)_{0\leqslant i,l\leqslant r} t^{\sum_i (j_i-m_i)} + \cdots \neq 0. \end{aligned}$$

onde $C := \prod_{l=0}^{r} c_{j_l}^l$. □

Portanto, a $r-$upla $(m_0,\ldots,m_r) \in \mathcal{A}(g_0,...,g_r;t)$ se, e somente se, os vetores $D_t^{(m_0)}g(P),\ldots,D_t^{(m_r)}g(P)$ são $k(\mathcal{X})-$linearmente independentes.

Corolário 1.16. *Os vetores* $(D_t^{(j_0(P))}g)(P), \quad \ldots, \quad (D_t^{(j_r(P))}g)(P)$ *são linearmente independentes.*

Podemos nos perguntar se existe uma sequência $(m_0,...,m_r)$, com $m_{i-1} < m_i$ para $i \in \{1,...,r\}$, com a propriedade de minimalidade com respeito a sequência

$$(D_t^{(m_0)}g)(P), \quad \ldots, \quad (D_t^{(m_r)}g)(P)$$

ser linearmente independente. O resultado a seguir garante que os $j_i(P)$'s satisfazem essa propriedade de forma minimal.

Teorema 1.17 (Minimalidade)**.** *Seja t um parâmetro local em P. Então $j_i(P)$ é igual ao mínimo do conjunto*

$\{s > j_{i-1}(P) : (D_t^{(j_0(P))}g)(P),\ldots,(D_t^{(j_{i-1}(P))}g)(P),(D_t^{(s)}g)(P)$ *são linearmente independentes*$\}$.

Demonstração: Do Corolário 1.16 segue que os vetores

$$D_t^{(j_0(P))}g(P), D_t^{(j_1(P))}g(P),\ldots,D_t^{(j_{i-1}(P))}g(P), D_t^{(j_i(P))}g(P)$$

são linearmente independentes. Fixe $j_{i-1}(P) < s < j_i(P)$. Para cada $l \in \{0,1,...,r\}$, seja $g_l = \sum_{u=j_l(P)}^{\infty} c_u^l t^u$ com $c_{j_l(P)}^l \neq 0$. Como para $l = 0,1,\ldots,i-1$ temos os vetores

$$\begin{aligned} (D_t^{(j_0(P))}g)(P) &= (c_{j_0(P)}^1, 0,\ldots,0,\ldots,0) \\ (D_t^{(j_1(P))}g)(P) &= (\star, c_{j_1(P)}^2, 0,\ldots,0,\ldots,0) \\ \vdots &= \quad \vdots \\ (D_t^{(j_{i-1}(P))}g)(P) &= (\star,\star,\ldots,\star, c_{j_{i-1}(P)}^{i-1}, 0,\ldots,0) \\ (D_t^{(s)}g)(P) &= (c^1, c^2, ..., c^{i-2}, c^{i-1}, 0,\ldots,0) \end{aligned}$$

formam uma matriz triangular e tem elementos não nulos na diagonal. Logo, $(D_t^{(s)}f)(P)$ é combinação linear de $(D_t^{(j_0(P))}g)(P), \ldots, (D_t^{(j_{i-1}(P))}g)(P)$. ▫

Outro conceito de minimalidade das $(\mathcal{D}, P)-$ordens também ocorre.

Corolário 1.18. *Sejam $0 \leqslant m_0 < m_1 < ... < m_r$ inteiros tais que os pontos $(D_t^{(m_0)}g)(P)$, ..., $(D_t^{(m_r)}g)(P)$ são linearmente independentes. Então $j_i(P) \leqslant m_i$ para $i = 0, ..., r$.*

Demonstração: Fixe $i \in [1, r]$. Como os vetores $(D_t^{(m_0)}g)(P)$, ..., $(D_t^{(m_i(P))}g)(P)$ são linearmente independentes, segue do Teorema 1.17 que $j_i(P) \leqslant m_i$. ▫

Definição 1.19. *Seja $L_i := L_i(P)$ a interseção de todos os hiperplanos em $\mathbb{P}^r(k)$ que intersectam em P com multiplicidade no mínimo $j_{i+1}(P)$. Dizemos que L_i é o $i-$**ésimo plano osculador** em P e L_{r-1} é o **hiperplano osculador** em P.*

Corolário 1.20. *O $i-$ésimo plano osculador em P é gerado pelos vetores*

$$(D_t^{(j_0(P))}g)(P), \ldots, (D_t^{(j_{i-1}(P))}g)(P), (D_t^{(j_i(P))}g)(P).$$

Em particular, podemos explicitar uma equação para a hiperplano osculador em P através das funções coordenadas.

Corolário 1.21. *O hiperplano osculador em P é dado pela equação*

$$det \begin{pmatrix} X_0 & \ldots & X_r \\ (D_t^{(j_0)}g_0)(P) & \ldots & (D_t^{(j_0)}g_r)(P) \\ \vdots & & \vdots \\ (D_t^{(j_{r-1})}g_0)(P) & \ldots & (D_t^{(j_{r-1})}g_r)(P) \end{pmatrix} = 0.$$

Um caso interessante de interseção ocorre quando existe um hiperplano com multiplicidade maior que r.

Definição 1.22. *Se $j_r(P) > r$, dizemos que P é um **ponto osculante** (ou mais precisamente, um ponto $\mathcal{D}-$osculante).*

As ordens do morfismo

Queremos repetir a caracterização induzida pelo Teorema 1.17, utilizando os determinantes de Wroskianos generalizados mas com uma parametrização num ponto geral, isto é, t será uma variável separável mas não necessariamente um parâmetro local. O objetivo é definir uma sequência $\mathcal{E} : \varepsilon_0 < \varepsilon_1 < ... < \varepsilon_r$ em $\mathcal{A}(g_0, ..., g_r; t)$ com propriedade minimal. Escolheremos $\varepsilon_0, ..., \varepsilon_r$ minimalmente na ordem lexicográfica, isto é, $\varepsilon_0 = 0$ e por

indução escolhemos ε_i como o menor inteiro tal que as linhas $(D_t^{(\varepsilon_j)}f_0, ..., D_t^{(\varepsilon_j)}f_r)$ com $j = 0, ..., i$ são linearmente independentes em $k(\mathcal{X})$.

Assumindo a existência da sequência $\mathcal{E}$, o resultado a seguir garante que ela só dependerá do sistema linear $\mathcal{D}$.

Proposição 1.23. *(a) Se* $g_i = \sum_j a_{ij}f_j$ *com* $(a_{ij})_{0\leqslant i,j\leqslant r} \in GL_{r+1}(k)$, *então*

$$det(D_t^{(\varepsilon_i)}g_j)_{0\leqslant i,j\leqslant r} = det(a_{ij}) \cdot det(D_t^{(\varepsilon_i)}f_j)_{0\leqslant i,j\leqslant r}.$$

(b) Se $h \in k(\mathcal{X})$, *então* $det(D_t^{(\varepsilon_i)}(hf_j))_{0\leqslant i,j\leqslant r} = h^{r+1}det(D_t^{(\varepsilon_i)}f_j)_{0\leqslant i,j\leqslant r}$.

(c) Se x *é uma variável separável, então*

$$det(D_x^{(\varepsilon_i)}f_j)_{0\leqslant i,j\leqslant r} = \left(\frac{dt}{dx}\right)^{\varepsilon_1+\cdots+\varepsilon_r} det(D_t^{(\varepsilon_i)}f_j)_{0\leqslant i,j\leqslant r}.$$

Demonstração: Lema 8.47 em (HIRSCHFELD; KORCHMÁROS; TORRES, 2008). □

Definição 1.24. *A sequência* $\varepsilon_0, ..., \varepsilon_r$ *é dita* $\mathcal{D}-$***ordens*** *ou as* ***ordens*** *do morfismo* f. *Em particular, se* $\varepsilon_i = i$ *para* $i = 0, 1, ..., r$ *dizemos que* $\mathcal{D}$ *é* ***clássica***.

Ainda falta verificar a existência dessa sequência de $\mathcal{D}-$ordens. Como não depende da parametrização, basta tomar t um parâmetro local no ponto $P \in \mathcal{X}$ com $e_P = 0$ e aplicar o Teorema 1.17. Por causa minimalidade das $\mathcal{D}-$ordens e do Teorema 1.18 para todo $P \in \mathcal{X}$ obtemos

$$\varepsilon_i \leqslant j_i(P) \quad \text{para cada } i \in \{0, 1, ..., r\}. \tag{1.2}$$

Considere o divisor

$$R := div(det(D_t^{(\varepsilon_i)}f_j)) + (\varepsilon_1 + \cdots + \varepsilon_r)div(dt) + (r+1)E$$

chamado o **divisor de ramificação** de $\mathcal{D}$, onde $E = \sum_P e_P P$. Observe que R depende somente do sistema linear $\mathcal{D}$ e seu grau é

$$deg\ R = (\varepsilon_1 + \cdots + \varepsilon_r)(2g-2) + (r+1)d, \tag{1.3}$$

onde $d = deg\ \mathcal{D}$.

Definição 1.25. *O* ***peso*** *de* $P \in \mathcal{X}$ *é o valor* $v_P(R)$.

Iremos apresentar cotas para o peso de pontos em $\mathcal{X}$ através das $(\mathcal{D}, P)-$ordens e das $\mathcal{D}-$ordens.

Teorema 1.26. *Seja $P \in \mathcal{X}$ e sejam $j_0(P), ..., j_r(P)$ as $(\mathcal{D}, P)-$ordens. Então*

$$v_P(R) \geqslant \sum_{i=0}^{r}(j_i(P) - \varepsilon_i).$$

A igualdade ocorre se, e somente se, $det\left(\binom{j_i(P)}{\varepsilon_l}\right)_{0\leqslant i,j\leqslant r} \not\equiv 0 \ mod\ p.$

Demonstração: Seja $P \in \mathcal{X}$ e t o parâmetro local em P. Dividindo as funções coordenadas projetivas por t^{e_P}, podemos assumir que $e_P = 0$. Então $v_P(R) = v_P(det(D_t^{(\varepsilon_l)} f_i)_{0\leqslant i,j\leqslant r})$. Depois de uma transformação projetiva, como na demonstração do Teorema 1.17, podemos assumir que $f_i = t^{j_i} + ...$ para cada i, onde os pontos indicam termos de ordem alta. Então

$$\begin{aligned} det(D_t^{(\varepsilon_l)} f_i) &= det\left(\binom{j_i}{\varepsilon_l} t^{j_i-\varepsilon_l} + \cdots\right) = det\left(\binom{j_i}{l} t^{j_i} + \cdots\right) t^{-\varepsilon_0-\cdots-\varepsilon_r} \\ &= det\left(\binom{j_i}{l}\right) t^{j_0+\ldots+j_r-\varepsilon_0-\ldots-\varepsilon_r} + \ldots \end{aligned}$$

Assim
$v_P(det(D_t^{(\varepsilon_l)} f_i)) \geqslant \sum_{i=0}^{r}(j_i(P) - \varepsilon_i)$ e a igualdade ocorre se, e somente se, $det\left(\binom{j_i(P)}{\varepsilon_l}\right) \not\equiv 0 \ mod\ p.$ □

Como $j_i(P) \geqslant \varepsilon_i$ para cada $i \in \{0, 1, .., r\}$ e para cada $P \in \mathcal{X}$, segue que o divisor de ramificação R é efetivo.

Corolário 1.27. *Seja $P \in \mathcal{X}$. Então $v_P(R) = 0$ se, e somente se, $j_i(P) = \varepsilon_i$ para cada $i \in \{0, 1, .., r\}$.*

Portanto, em particular para quase todo $P \in \mathcal{X}$, o conjunto de $(\mathcal{D}, P)$-ordens é igual a $\mathcal{E}$.

Definição 1.28. *Um ponto $P \in \mathcal{X}$ é $\mathcal{D}-$**ordinário** se $j_i(P) = \varepsilon_i$, para $i = 0, 1, ..., r$. Caso contrário, o ponto P é dito $\mathcal{D}-$**Weierstrass**. Quando $\mathcal{D}$ é canônico, dizemos simplesmente pontos de Weierstrass.*

Observamos que :

- O número de pontos $\mathcal{D}-$Weierstrass, contado com seus pesos, é igual ao grau do divisor de Ramificação R.
- Se $\mathcal{D}$ é clássica então os pontos $\mathcal{D}-$Weierstrass são exatamente os pontos $\mathcal{D}-$osculantes.
- Se $\mathcal{D}$ for não clássica, então todo ponto é $\mathcal{D}-$osculante.

Queremos dar um critério para decidir quando o sistema linear $\mathcal{D}$ é clássico. Para isto, começamos refinando a estimativa $\varepsilon_i \leqslant j_i(P)$ assim como na demonstração do Teorema 1.26.

Proposição 1.29. *Seja $P \in \mathcal{X}$ e sejam $j_0, ..., j_n$ a sequência $(\mathcal{D}, P)-$ordens. Se $m_0, ..., m_r$ são inteiros tais que $0 \leqslant m_0 < ... < m_r$ e $det\left(\binom{j_i}{m_n}\right) \not\equiv 0$ mod p, então*

$$\varepsilon_i \leqslant m_i \text{ para } i = 0, 1, ..., r.$$

Observamos que a melhor escolha para os inteiros $m_0, ..., m_r$ na Proposição 1.29 são as ordens do morfismo $\mathbb{P}^1 \longrightarrow \mathbb{P}^r(k)$ dado por $(1 : x) \longmapsto (x^{j_0} : ... : x^{j_r})$, isto é, $m_0 = 0$ e se $m_0, ..., m_{i-1}$ são dados, então escolhemos m_i sendo o mínimo tal que os vetores

$$\left(\binom{j_0}{m_0}, ..., \binom{j_r}{m_0}\right), \ldots, \left(\binom{j_0}{m_i}, ..., \binom{j_n}{m_i}\right)$$

são linearmente independentes sobre o corpo primo $\mathbb{F}_p$.

Corolário 1.30. *Seja $P \in \mathcal{X}$. Se o inteiro*

$$\prod_{i>s} \frac{j_i(P) - j_s(P)}{i - s}$$

não for divisível por p, então $\mathcal{D}$ é clássica e o peso de P é igual a $\sum_{i=0}^{r}(j_i(P) - i)$.

Demonstração: Temos

$$det\left(\binom{j_i(P)}{r}\right) = det\left(\left(\frac{j_i(P)^r}{i!}\right) + ...\right) = \frac{det(j_i(P)^r)}{1!2!\cdots r!} = \prod_{i>s} \frac{(j_i(P) - j_s(P))}{i - s}.$$

Assim pela hipótese $det\left(\binom{j_i}{r}\right) \not\equiv 0$ *mod* p. Pela Proposição 1.29, segue que $\varepsilon_i = i$ para cada i. Portanto, segue do Teorema 1.26 que $v_P(R) = \sum_{i=0}^{r}(j_i(P) - i)$. □

A hipótese do corolário é satisfeita se para $i \neq s$ tivermos $j_i(P) \not\equiv j_s(P)$ *mod* p. Em particular, como $j_r(P) \leqslant d$, obtemos:

Corolário 1.31. *Se $p > d = deg(\mathcal{D})$ ou $p = 0$ então $\mathcal{D}$ é clássica. Além disso, $v_P(R) = \sum_{i=0}^{r}(j_i(P) - i)$.*

Aplicando a Proposição 1.29 a um ponto $\mathcal{D}-$ordinário, obtemos:

Corolário 1.32 (Critério $p-$ádico)**.** *Seja ε alguma $\mathcal{D}-$ordem e seja μ um inteiro tal que*

$$\binom{\varepsilon}{\mu} \not\equiv 0 \ mod\ p.$$

Então μ é também uma $\mathcal{D}-$ordem. Em particular, se ε é uma $\mathcal{D}-$ordem menor do que p, então os inteiros $0, 1, ..., \varepsilon - 1$ são também $\mathcal{D}-$ordens.

Demonstração: Como $\binom{\varepsilon}{\mu} \neq 0$, temos que $0 \leqslant \mu \leqslant \varepsilon$. Podemos supor que $\mu > 0$. Seja r o maior inteiro tal que $\varepsilon_r < \mu$. A matriz

$$\begin{pmatrix} \binom{\varepsilon_0}{\varepsilon_0} & \cdots & \binom{\varepsilon_r}{\varepsilon_0} & \binom{\varepsilon}{\varepsilon_0} \\ \vdots & & \vdots & \vdots \\ \binom{\varepsilon_0}{\varepsilon_r} & \cdots & \binom{\varepsilon_r}{\varepsilon_r} & \binom{\varepsilon}{\varepsilon_r} \\ \binom{\varepsilon_0}{\mu} & \cdots & \binom{\varepsilon_r}{\mu} & \binom{\varepsilon}{\mu} \end{pmatrix}$$

é triangular com as entradas na diagonal $1, ..., 1, \binom{\varepsilon}{\mu}$ e portanto as linhas são linearmente independentes sobre o corpo primo $\mathbb{F}_p$. Então pela Proposição 1.29 temos $\varepsilon_r \leqslant \mu$. Portanto, pela definição de r segue que $\mu = \varepsilon_r$. ▫

Observação 1.33. *Note que $\binom{\varepsilon}{\mu} \not\equiv 0 \ mod\ p$ se, e somente se, $\mu \geqslant 0$ e μ é o $p-$**adicamente menor** do que ε.*

1.3 Teoria de Stöhr-Voloch

Seja k um corpo finito com q elementos e seja $\overline{k}$ seu fecho algébrico. Seja $\mathcal{X}$ uma curva de gênero g definida sobre k. Consideramos $\mathcal{X}$ uma curva munida com a ação da aplicação de Frobenius, a saber, $\phi : \mathcal{X} \longrightarrow \mathcal{X}$ definida por $\phi(x_0 : .. : x_s) = (x_0^q : ... : x_s^q)$.

Seja $f : \mathcal{X} \longrightarrow \mathbb{P}^r(k)$ um $k-$morfismo, digamos $f = (f_0 : ... : f_r)$, onde $f_0, ..., f_r$ são funções $k-$racionais em $\mathcal{X}$. Lembramos que os pontos $k-$racionais são fixados pelo morfismo Frobenius ϕ. Podemos aplicar a teoria de séries lineares para $\overline{k}$. Escrevemos o sistema linear associado $\mathcal{D} \cong \mathbb{P}^r(\mathcal{D}') \subseteq |E|$. Neste caso o divisor E e o sistema linear $\mathcal{D}$ são definidos sobre k, isto é, são invariantes pela ação de Frobenius.

Para cada ponto $P \in \mathcal{X}$ consideramos π_P o hiperplano osculador em P. Seja

$$H = \{P \in \mathcal{X} : \phi(f(P)) \in \pi_P\}.$$

Pelo Corolário 1.21, um ponto P de $\mathcal{X}$ com $e_P = 0$ pertence a H_P se, e somente se,

$$det \begin{pmatrix} f_0(P)^q & \dots & f_r(P)^q \\ (D_t^{(j_0)} f_0)(P) & \dots & (D_t^{(j_0)} f_r)(P) \\ \vdots & & \vdots \\ (D_t^{(j_{r-1})} f_0)(P) & \dots & (D_t^{(j_{r-1})} f_r)(P) \end{pmatrix} = 0,$$

onde t é um parâmetro local em P.

Com o intuito de obter uma cota superior para o número de pontos racionais de $\mathcal{X}$, analisamos o conjunto H, o qual é possivelmente maior. Pela equivalência anterior, vamos estudar os determinantes do tipo

$$W_t^{\nu_0,\dots,\nu_{r-1}}(f_0,...,f_r) := det \begin{pmatrix} f_0^q & \dots & f_r^q \\ D_t^{(\nu_0)} f_0 & \dots & D_t^{(\nu_0)} f_r \\ \vdots & & \vdots \\ D_t^{(\nu_{r-1})} f_0 & \dots & D_t^{(\nu_{r-1})} f_r \end{pmatrix}.$$

onde t é uma variável separável de $k(\mathcal{X})/k$ e $\nu_0, ..., \nu_{r-1}$ são inteiros não negativos.

Proposição 1.34. *Existem inteiros $\nu_0, .., \nu_{r-1}$ com $0 \leqslant \nu_0 < .. < \nu_{r-1}$ tais que*

$$W_t^{\nu_0,..,\nu_{r-1}}(f_0,...,f_r) \neq 0.$$

Escolha os inteiros ν_i's minimalmente na ordem lexiocográfica. Então existe um inteiro I com $0 < I \leqslant r$ tal que

$$\nu_i = \begin{cases} \varepsilon_i, & se \quad i < I \\ \varepsilon_{i+1}, & se \quad i \geqslant I \end{cases}$$

Demonstração: Para a parte da existência, basta considerar $\nu_0 = 0$ e

$\nu_i = min\{s > \nu_{i-1} : f^q, D_t^{(\nu_0)} f, \dots, D_t^{(\nu_{i-1})} f, D_t^{(s)} f$ linearmente independentes sobre $\overline{k}(\mathcal{X})\}$.

Um raciocínio análogo da demonstração do Teorema 1.17. Seja I o menor inteiro tal que a linha $(f_0^q, ..., f_r^q)$ é combinação linear dos vetores $(D_t^{(\varepsilon_i)} f_0, ..., D_t^{(\varepsilon_i)} f_r)$ com $i = 0, .., I$. Como $f_0, \dots, f_r$ é uma $k-$base de $\mathcal{D}'$ segue que $I > 0$ e $\{\nu_0, ..., \nu_{r-1}\} = \{\varepsilon_0, ..., \varepsilon_r\} \backslash \{\varepsilon_I\}$. Pela minimalidade $\varepsilon_i = \nu_i$ para cada $i < I$ e $\varepsilon_{i+1} = \nu_i$ para $i \geqslant I$. □

Na Proposição acima temos um sentido minimalmente para os ν_i's. A minimalidade também se mantém no sentido forte, isto é, se $m_0, .., m_r$ são inteiros com $0 \leqslant m_0 < ... < m_r$ tais que as linhas da matriz

$$\begin{pmatrix} f_0^q & \dots & f_r^q \\ D_t^{(m_0)} f_0 & \dots & D_t^{(m_0)} f_r \\ \vdots & & \vdots \\ D_t^{(m_r)} f_0 & \dots & D_t^{(m_r)} f_r \end{pmatrix}$$

são linearmente independentes, então $\nu_i \leqslant m_i$ para cada $i = 0, ..., r$. De fato, se $\nu_i \leqslant m_i$ a matriz $\begin{pmatrix} f_0^q & \dots & f_r^q \\ D_t^{(\nu_0)} f_0 & \dots & D_t^{(\nu_0)} f_r \\ \vdots & & \vdots \\ D_t^{(\nu_{r-1})} f_0 & \dots & D_t^{(\nu_{r-1})} f_r \end{pmatrix}$ tem posto $r+1$. Veja Corolário 8.44 em (HIRSCHFELD; KORCHMÁROS; TORRES, 2008) para mais detalhes.

Proposição 1.35 (Lema 8.47, (HIRSCHFELD; KORCHMÁROS; TORRES, 2008))**.**

(a) Se $g_i = \sum_j a_{ij} f_j$ *com* $(a_{ij}) \in GL(k)$*, então*

$$W_t^{\nu_0,\dots,\nu_{r-1}}(g_0, ..., g_r) = det(a_{ij}) \cdot W_t^{\nu_0,\dots,\nu_{r-1}}(f_0, ..., f_r).$$

(b) Se $h \in k(\mathcal{X})$*, então* $W_t^{\nu_0,\dots,\nu_{r-1}}(hf_0, .., hf_r) = h^{q+r} W_t^{\nu_0,\dots,\nu_{r-1}}(f_0, ...f_r)$

(c) Se x *é outra variável separável de* $k(\mathcal{X})/k$*, então*

$$W_t^{\nu_0,\dots,\nu_{r-1}}(g_0, ..., g_r) = \frac{dt}{dx}^{\nu_1+\dots+\nu_{r-1}} W_t^{\nu_0,\dots,\nu_{r-1}}(f_0, ...f_r).$$

Pela Proposição 1.35, os inteiros $\nu_0, ..., \nu_{r-1}$ e o divisor

$$S := div(W_t(f_0, ..., f_r)) + (\nu_1 + ... + \nu_{r-1}) div(dt) + (q+r)E \tag{1.4}$$

dependem somente do sistema linear $\mathcal{D}$, o qual é conhecido como **divisor de Frobenius** ou **divisor de Stöhr-Voloch**.

Definição 1.36. *Chamamos* $\nu_0, ..., \nu_{r-1}$ *as* ***ordens de Frobenius*** *de* $\mathcal{D}$*.*

Como $deg(E) = d$, $deg\ div(dt) = 2g-2$ (Definição 5.55 em (HIRSCHFELD; KORCHMÁROS; TORRES, 2008)) e $deg\ div(W_t(f_0, ..., f_r)) = 0$ (Corolário 5.35 em (HIRSCHFELD; KORCHMÁROS; TORRES, 2008)) então

$$deg(S) = (\nu_1 + ... + \nu_{r-1})(2g-2) + (q+r)d. \tag{1.5}$$

Dividindo as funções coordenadas projetivas $f_0, ..., f_r$ por f_0, podemos assumir que $f_0 = 1$ e $f_1, ..., f_r$ podem ser consideradas como funções coordenadas afins. Como $\nu_0 = 0$, obtemos

$$W_t(1, f_1, ..., f_r) = det \begin{pmatrix} f_1 - f_1^q & \dots & f_r - f_r^q \\ D_t^{(\nu_1)} f_1 & \dots & D_t^{(\nu_1)} f_r \\ \vdots & & \vdots \\ D_t^{(\nu_{n-1})} f_1 & \dots & D_t^{(\nu_{n-1})} f_r \end{pmatrix}.$$

Note que $D_t^{(\nu_i)}(f_j^q) = 0$ se ν_i não é um múltiplo de q. Portanto, se $\nu_i < q$ então $\nu_0, ..., \nu_i$ são as $i+1$ primeiras ordens do morfismo

$$((f_1 - f_1^q) : ... : (f_r - f_r^q)) : \mathcal{X} \longrightarrow \mathbb{P}^{r-1}.$$

Podemos aplicar o Corolário 1.32 e obtemos

Proposição 1.37. *Se v é uma ordem de Frobenius de $\mathcal{D}$ menor que q, então cada inteiro não negativo $p-$adicamente menor do que v é também uma ordem de Frobenius de $\mathcal{D}$. Em particular, se $\nu_i < p$ então $(\nu_0, ..., \nu_i) = (0, ..., i)$.*

Agora iremos estudar o divisor S localmente num ponto $P \in \mathcal{X}$. Seja $t \in k(\mathcal{X})$ um parâmetro local em P. Dividindo as funções coordenadas projetivas $f_0, .., f_n$ por t^{e_P}, podemos supor $e_P = 0$. Assim

$$v_P(S) = v_P(W_t(f_0, ..., f_r)) \geqslant 0.$$

Em particular, obtemos o resultado importante que S é um divisor positivo.

Observação 1.38. *O ponto $P \in Supp(S)$ se, e somente se, $W_t(f_0, ..., f_r)(P) = 0$.*

- *Se $\nu_i = j_i(P)$ para cada i, então $P \in Supp(S)$ se, e somente se, a imagem de $f(P)$ via a aplicação de Frobenius está contida no hiperplano osculante em P.*
- *Se $\nu_i < j_i(P)$ para algum i, então $P \in Supp(S)$.*

Como para $P \in \mathcal{X}(k)$ as primeiras duas linhas de $W_t(f_0, .., f_r)$ coincidem, concluímos que todos os pontos racionais estão no suporte de S.

Agora iremos analisar resultados quantitativos.

Proposição 1.39. *(a) Se P é um ponto racional de $\mathcal{X}$ com as $(\mathcal{D}, P)-$ordens $j_0(P), ..., j_r(P)$ então*

$$v_P(S) \geqslant \sum_{i=1}^{r} (j_i(P) - \nu_{i-1}).$$

A igualdade ocorre se, e somente se, $\det\left(\binom{j_i(P)}{\nu_l}\right)_{0 \leqslant l \leqslant r-1, 1 \leqslant i \leqslant r} \not\equiv 0 \ mod\ p$.

(b) Se P é um ponto não racional de $\mathcal{X}$ então

$$v_P(S) \geqslant \sum_{i=1}^{r-1} (j_i(P) - \nu_i).$$

Além disso, se $\det\left(\binom{j_i(P)}{\nu_n}\right)_{0 \leqslant n \leqslant r-1, 1 \leqslant i \leqslant r} \equiv 0 \ mod\ p$ então a desigualdade é estrita.

Demonstração:

(a) Como P é racional, os planos osculadores em P são definidos sobre k. Então, depois de uma transformação projetiva com coeficientes em k, podemos assumir que $f_i = t^{j_i} + ...$ para cada i. Dividindo por f_0, podemos assumir que $f_0 = 1$. Assim

$$W_t^{\nu_0,...,\nu_{n-1}}(1, f_1, ..., f_n) = det \begin{pmatrix} f_1 - f_1^q & \dots & f_n - f_n^q \\ D_t^{(\nu_1)} f_1 & \dots & D_t^{(\nu_1)} f_n \\ \vdots & & \vdots \\ D_t^{(\nu_{n-1})} f_1 & \dots & D_t^{(\nu_{n-1})} f_n \end{pmatrix}.$$

Como $\nu_0 = 0$ e $j_i > 0$ para $i = 1, .., r$, obtemos que

$$W_t^{\nu_0,..,\nu_{r-1}} = det \left(\binom{j_i}{\nu_l} t^{j_i - \nu_l} + \dots \right) = det \left(\binom{j_i}{\nu_l} \right) t^{j_1 + ... + j_r - \nu_0 - ... - \nu_{r-1}} + ..$$

(b) Aplicando uma transformação projetiva com coeficientes no corpo algebricamente fechado k, obtemos funções $k-$racionais $g_i = \sum_{j=0}^{r} a_{ij} f_j$ onde $(a_{ij}) \in GL_{r+1}(\overline{k})$ tal que $f_i = t^{j_i} + ...$ para cada i. Seja $h_i := \sum_{j=0}^{r} a_{ij} f_j^q$. Em contraste a parte (a), não podemos afirmar que $h_i = g_i^q$. Logo $v_P(h_i) \geqslant 0$ para cada i. Temos

$$W_t(f_0, f_1, ..., f_r) det(a_{ij}) = det \begin{pmatrix} h_0 & \dots & h_r \\ D_t^{(\nu_0)} g_0 & \dots & D_t^{(\nu_0)} g_r \\ \vdots & & \vdots \\ D_t^{(\nu_{r-1})} g_0 & \dots & D_t^{(\nu_{r-1})} g_r \end{pmatrix} = \sum_{i=0}^{r} (-1)^i h_i d_i,$$

onde os d_i são os determinantes obtidos pela regra de Cramer, a saber,

$$d_i = det \left(\binom{j_i(P)}{\nu_l}_{i=0,..,r-1, l \neq i} t^{\sum j_l - \nu_l - j_i(P)} + \dots \right).$$

Assim $v_P(d_i) \geqslant \sum_{l=0}^{r-1} j_l(P) - \nu_l - j_1(P) + j_r(P)$ para todo i, isto é, $v_P(S) \geqslant min\{v_P(d_0), ..., v_P(d_r)\}$. Como $j_0(P) < j_1(P) < ... < j_r(P)$ então $min_i v_P(d_i) = v(d_r)$. Portanto $v_P(S) \geqslant j_0 + ... + j_r - j_i - \nu_0 - ... - \nu_{r-1}$. Em particular, se $det \left(\binom{j_i}{\nu_l} \right)_{i,l=0,..,r-1} \equiv 0 \ mod \ p$, então $v_P(d_r) > j_0 + ... + j_{r-1} - \nu_0 - ... - \nu_{r-1}$. □

Agora procuramos as relações entre as ordens de Frobenius $\nu_0, .., \nu_{r-1}$ e os invariantes hermitianos $j_0(P), ..., j_r(P)$ de um ponto P racional.

Proposição 1.40. *Seja P um ponto racional de $\mathcal{X}$ e sejam $j_0(P), .., j_r(P)$ a sequência de $(\mathcal{D}, P)-$ordens. Se $m_0, ..., m_{r-1}$ são inteiros tais que $0 \leqslant m_0 < ... < m_{r-1}$ e*

$$det\left(\binom{j_i(P) - j_1(P)}{m_l}\right)_{0\leqslant l\leqslant r-1, 1\leqslant i\leqslant r} \not\equiv 0 \ mod\ p,$$

então $\nu_i \leqslant m_i$ para cada i.

Demonstração: As melhores escolhas para os inteiros m_i são as ordens do morfismo $\mathbb{P}^1 \longrightarrow \mathbb{P}^{r-1}$ definido por

$$(1 : x) \longmapsto (1 : x^{j_2-j_1} : ... : x^{j_n-j_1}) = (x^{j_1} : x^{j_2} : ... : x^{j_n}).$$

Podemos supor que $m_0 = 0$ e $det\left(\binom{j_i}{m_r}_{0\leqslant r\leqslant n-1, 1\leqslant i\leqslant n}\right) \not\equiv 0 \ mod\ p$. Podemos assumir novamente que $f_0 = 1$ e $f_i = t^{j_i} + ...$ para cada i. Assim, como na demonstração da Proposição 1.39, item (a), obtemos

$$W_t^{m_0,...,m_{r-1}}(f_0, ..., f_r) = det\left(\binom{j_i}{m_r}\right) t^{j_1+...+j_n-m_0-...-m_{n-1}} + ... \neq 0.$$

Portanto pela minimalidade de ν_i tem-se $\nu_i \leqslant m_i$. □

Como uma consequência da Proposição 1.40 e 1.39, item (a), obtemos:

Corolário 1.41. *Se $P \in \mathcal{X}(k)$ então*

$$\nu_i \leqslant j_{i+1}(P) - j_1(P) \quad \textit{para cada } i \textit{ e } v_P(S) \geqslant r j_1(P).$$

Aplicando a Proposição 1.40 no caso em que $m_i = \varepsilon_i$, obtemos

Corolário 1.42. *Se a sequência de ordem de Frobenius $\nu_0, ..., \nu_{r-1}$ difere da sequência $\varepsilon_0, ..., \varepsilon_{r-1}$, então cada ponto racional de $\mathcal{X}$ é um ponto $\mathcal{D}-$Weierstrass.*

Demonstração: Se existe um ponto racional $\mathcal{D}-$ordinário, então pelo Corolário 1.41 segue que $\nu_i \leqslant \varepsilon_{i+1} - \varepsilon_1$. Assim pela Proposição 1.34 temos $\nu_i = \varepsilon_i$ para cada i. □

Corolário 1.43. *Se $\mathcal{D}$ é completa e se existe um ponto racional, então $\nu_i = i$ quando $i < d - 2g$.*

Demonstração: Seja $P \in \mathcal{X}(k)$ com as $(\mathcal{D}, P)-$ordens $j_0, ..., j_r$. Como $\mathcal{D}$ é completa segue, como observado na primeira seção que $j_i = i$ quando $i \leqslant d - 2g$. Portanto, pelo Corolário 1.41, obtemos que $\nu_i = i$ quando $i < d - 2g$. □

Corolário 1.44. *Se existe um ponto P racional em $\mathcal{X}$, então $\nu_i \leqslant i + d - r$ para cada i.*

Demonstração: Como $j_r(P) \leqslant d$ temos $j_i \leqslant i + d - r$ para cada i e aplicamos o Corolário 1.41. ▫

Agora apresentamos o resultado principal de Stöhr e Voloch.

Teorema 1.45 ((STÖHR; VOLOCH, 1986)). *Seja $\mathcal{X}$ uma curva de gênero g definida sobre $\mathbb{F}_q$ e seja N o número de seus pontos $\mathbb{F}_q-$racionais. Se existe em $\mathcal{X}$ um sistema linear de ponto-base-livre definida sobre $\mathbb{F}_q$ de grau d, dimensão r e com a sequência de ordens de Frobenius $\nu_0, \nu_1, ..., \nu_{r-1}$ então*

$$N \leqslant \frac{(\nu_1 + \ldots + \nu_{r-1})(2g-2) + (q+r)d}{r}.$$

Corolário 1.46 (Weil). *Seja $\mathcal{X}$ uma curva de gênero g definida sobre $\mathbb{F}_q$ e seja N o número de seus pontos $\mathbb{F}_q-$racionais. Se q é um quadrado tal que $q > 4g^4(g-1)^2$ então*

$$N \leqslant q + 1 + 2g\sqrt{q}.$$

Demonstração: Se $\mathcal{X}(\mathbb{F}_q) = \varnothing$ então não o que provar. Suponha que $\mathcal{X}$ tem um ponto $\mathbb{F}_q-$racional P. Dado d um inteiro tal que $d \geqslant 2g$. Considere $\mathcal{D} := |dP|$. Assim $\mathcal{D}$ é um sistema linear completo, livre de pontos-base sobre $\mathbb{F}_q$ de grau d. Seja r a dimensão de $\mathcal{D}$. Segue do Teorema de Riemann-Roch que $r = d - g \geqslant g$. Pelos Corolários 1.43 e 1.44, obtemos que $\nu_i = i$ quando $i < r - g$ e $\nu_i \leqslant i + g$ para cada $i = r - g, ..., r - 1$. Aplicando o Teorema 1.45 obtemos que

$$N \leqslant q + 1 + \left(r + \frac{q}{r}\right) g + 2g^2 \frac{(g-1)}{r}$$

para cada inteiro r tal que $r \geqslant g$. Como q é um quadrado tal que $q > 4g^4(g-1)^2$, basta tomar $r = \sqrt{q}$ para obtemos que $N \leqslant q + 1 + 2g\sqrt{q}$. ▫

1.4 Curvas maximais sobre Corpos Finitos

O interesse sobre curvas sobre corpos finitos foi reavivado depois de Goppa, quando este mostrou como aplicá-las em Teoria de Códigos, (GOPPA, 1983). Em (STICHTENOTH, 2009), Capítulo 2, podemos encontrar uma coleção de resultados sobre códigos lineares, entre estes, é o fato que códigos lineares provenientes de curvas possuem uma limitação para sua distância mínima. Esta limitação inferior é significativa somente se a curva tem muitos pontos racionais. Desta maneira, o estudo de curvas com tais características é bem interessante, em particular o conceito de maximalidade. Com o objetivo de cotar a quantidade de pontos racionais de uma curva, primeiramente o matemático Hasse determinou uma cota para o caso particular de curvas com gênero 1. Posteriormente, Weil determinou uma cota para curvas com gênero $g > 1$.

Teorema 1.47 (Cota de Hasse-Weil)**.** *Seja $\mathcal{X}$ uma curva definida sobre $\mathbb{F}_q$ de gênero g. Então*

$$|N_n - q^n - 1| \leqslant 2g\sqrt{q^n} \tag{1.6}$$

onde N_n é o número de pontos $\mathbb{F}_{q^n}-$racionais de $\mathcal{X}$.

Para demonstrá-la, pode-se utilizar como ferramentas a Teoria de Stöhr-Voloch (para a cota superior: Corolário 1.46) e a Teoria de Galois (para cota inferior). Uma aplicação da Cota de Hasse-Weil muitíssimo interessante é veracidade da Hipótese de Riemann para Corpos de Funções sobre Corpos Finitos, através de Função Zeta

$$\zeta_{\mathcal{X},q}(t) := exp\left(\sum_{i=0}^{\infty} \frac{N_i}{i} t^i\right) \tag{1.7}$$

para uma curva $\mathcal{X}$. Para mais detalhes veja Capítulo 9, em (HIRSCHFELD; KORCHMÁROS; TORRES, 2008).

Definição 1.48. *Uma curva $\mathcal{X}$ é dita **maximal** sobre $\mathbb{F}_l$ se a quantidade de seus pontos $\mathbb{F}_l-$racionais atinge a cota superior de Hasse-Weil.*

Para haver maximalidade, o número l deve ser um quadrado, digamos $l = q^2$. Podemos calcular a quantidade de pontos racionais de uma curva maximal em cada extensão de $\mathbb{F}_{q^2}$, através das raízes de um certo polinômio associado a curva. Para isto é aplicado o Teorema 1.5, para garantir a existência de um polinômio $P(t) := \sum_{i=0}^{2g} a_i t^i \in \mathbb{Z}[t]$ tal que $\zeta_{\mathcal{X},q}(t) = \dfrac{P(t)}{(1-t)(1-qt)}$. Definimos o $L-$**polinômio** de $\mathcal{X}$ de gênero g como

$$L(t) = 1 + \sum_{i=1}^{2g-1} a_i t^i + q^g t^{2g}$$

se $g \geqslant 1$ e $L(t) = 1$ se $g = 0$. Tal polinômio possui propriedades que auxiliam na demonstração do resultado a seguir.

Lema 1.49 (Lema 9.20, (HIRSCHFELD; KORCHMÁROS; TORRES, 2008))**.** *Seja $\mathcal{X}$ uma curva maximal sobre $\mathbb{F}_{q^2}$ de gênero g definida sobre $\mathbb{F}_q$. Então*

$$\#\mathcal{X}(\mathbb{F}_{q^i}) = \begin{cases} q^i + 1, & i \equiv 1 \ mod\ 2 \\ q^i + 1 + 2g\sqrt{q^i}, & i \equiv 2 \ mod\ 4 \\ q^i + 1 - 2g\sqrt{q^i}, & i \equiv 0 \ mod\ 4 \end{cases}$$

Vamos estudar curvas maximais sobre um corpo fixado $\mathbb{F}_{q^2}$, através do gênero, suas sequências de ordens e semigrupo de Weierstrass. Sabemos que toda curva

é birracionalmente equivalente a uma curva plana (Teorema 7.17, em (HIRSCHFELD; KORCHMÁROS; TORRES, 2008)), assim vamos trabalhar com modelos planos para buscar exemplos de curvas maximais. Relembramos a seguir a definição de equivalência birracional neste contexto a partir da linguagem de corpos de funções.

Definição 1.50. *Duas curvas planas são ditas* ***birracionalmente equivalente*** *se os corpos de funções delas são isomorfos sobre k.*

Curva Hermitiana

Seja $\mathbb{F}_{q^2}$ com $q = p^h > 2$. Considere $\mathcal{H}_q$ a curva plana irredutível definida sobre $\mathbb{F}_{q^2}$ dada pela equação

$$Y^q + Y = X^{q+1}. \tag{1.8}$$

Definição 1.51. *Uma* ***curva Hermitiana*** *definida sobre $\mathbb{F}_{q^2}$ é qualquer curva algébrica birracionalmente equivalente a curva $\mathcal{H}_q$.*

Podemos escrever as formas equivalentes da curva Hermitiana em coordenadas projetivas. As equações são dadas por $F_i(X_0, X_1, X_2) = 0$, para $i = 1, 2, 3, 4$, onde

(i) $F_1(X_0, X_1, X_2) = X_0^{q+1} + X_1^{q+1} + X_2^{q+1}$;

(ii) $F_2(X_0, X_1, X_2) = X_2^q X_0 - X_2 X_0^q + \omega X_1^{q+1}$, onde $\omega^{q-1} = -1$;

(iii) $F_3(X_0, X_1, X_2) = X_1 X_2^q - X_1^q X_2 + \omega X_0^{q+1}$, onde $\omega^{q-1} = -1$;

(iv) $F_4(X_0, X_1, X_2) = X_0^q X_1 + X_1^q X_2 + X_2^q X_0$.

Cada umas três primeiras equações são obtidas de (1.8) por uma substituição linear definida sobre $\mathbb{F}_{q^2}$. Para obter (iv) é necessário uma transformação sobre $\mathbb{F}_{q^3}$.

Teorema 1.52 ((HIRSCHFELD; KORCHMÁROS; TORRES, 2008))**.** *A curva $\mathcal{H}_q$ é uma curva não singular, com P_∞ o lugar associado ao ramo centrado no ponto $P_\infty = (0 : 0 : 1)$ e tem as seguintes propriedades:*

(i) $div(dx) = (q + 1)(q - 2)P_\infty$;

(ii) $\mathcal{H}_q$ *tem gênero* $\dfrac{q(q-1)}{2}$;

(iii) $\#\mathcal{H}_q(\mathbb{F}_{q^2}) = q^3 + 1$;

(iv) o grupo de $K-$automorfismo de $\mathcal{H}_q$ é $\mathbb{F}_{q^2}-$racional e é isomorfo ao grupo $PGU(3, q)$, o qual age projetivamente sobre $\mathcal{H}_q(\mathbb{F}_{q^2})$.

Cota de Ihara

Teorema 1.53 ((IHARA, 1981)). *Se $\mathcal{X}$ é uma curva maximal de gênero g sobre $\mathbb{F}_{q^2}$ então*

$$2g \leqslant (q-1)q.$$

Demonstração: Seja $\mathcal{X}$ é uma curva $\mathbb{F}_{q^2}-$maximal de gênero g. Como $\mathcal{X}(\mathbb{F}_{q^2}) \subseteq \mathcal{X}(\mathbb{F}_{q^4})$, então $\#\mathcal{X}(\mathbb{F}_{q^2}) \leqslant \#\mathcal{X}(\mathbb{F}_{q^4})$. Aplicando o Lema 1.49, obtemos

$$q^2 + 1 + 2gq \leqslant q^4 + 1 - 2gq^2,$$

isto implica que $2g \leqslant q(q-1)$. ▫

Equivalência Fundamental

Queremos estudar algumas propriedade aritméticas e geométricas das curvas maximais. Primeiramente, vamos relembrar alguns resultados de Jacobianos. Para mais detalhes veja (TATE, 1966), (MUMFORD; FOGARTY; KIRWAN, 1993), (RÜCK; STICHTENOTH, 1994).

Seja $\mathcal{X}$ uma curva $\mathbb{F}_q-$maximal com gênero g e $P_0 \in \mathcal{X}$ um ponto $\mathbb{F}_q-$racional. Seja $\mathcal{J}$ o Jacobiano de $\mathcal{X}$, o qual é uma variedade abeliana isomorfa ao Grupo de Picard. Podemos definir uma aplicação $f = f^{P_0} : \mathcal{X} \longrightarrow \mathcal{J}$ dada por

$$f(P) = [P - P_0].$$

Vamos construir o **Módulo Tate** asssociado a $\mathcal{J}$. Fixe l primo, $l \neq char(\mathbb{F}_q)$.

Definimos para cada $i \in \mathbb{N}$ a aplicação $\psi_i : \mathcal{J} \longrightarrow \mathcal{J}$ dada por $\psi_i(P) := l^i P$.

Observação 1.54. *A aplicação ψ_i é uma **isogenia**. Para verificar este fato, devemos mostrar que ψ_i é um morfismo de grupos algébricos com núcleo finito. Seja*

$$\mathcal{J}_{l^i} := Ker\psi_i = \{[P] \in \mathcal{J} : [l^i P] = [0]\}.$$

Um resultado em (MUMFORD; FOGARTY; KIRWAN, 1993), nos garante que $\#\mathcal{J}_{l^i} = (l^i)^{2g}$.

Definimos para cada $i \in \mathbb{N}$ a aplicação

$$\begin{aligned} \alpha_{i+1} : \mathcal{J}_{l^{i+1}} &\longrightarrow \mathcal{J}_{l^i} \\ P &\longrightarrow lP. \end{aligned}$$

Definição 1.55. *O **módulo Tate** $T_l(\mathcal{J})$ associado a $\mathcal{J}$ com respeito a l é o limite inverso dos grupos J_{l^i} com respeito as aplicações α_i, isto é, o conjunto de todas as sequências $(a_n)_n$ tais que $a_i \in \mathcal{J}_{l^i}$ e $\alpha_{i+1}(a_{i+1}) = a_i$.*

O módulo $T_l(\mathcal{J})$ é um módulo livre de posto $2g$ sobre $\mathbb{Z}_l$. Considere Fr o morfismo de Frobenius associado ao corpo $\mathbb{F}_q$ induzido na curva $\mathcal{X}$ e $Fr_{\mathcal{J}}$ o morfismo induzido por Fr em $\mathcal{J}$. Vamos analisar o seguinte diagrama.

$$\begin{array}{ccc} \mathcal{X} & \xrightarrow{Fr} & \mathcal{X} \\ {\scriptstyle f}\downarrow & & \downarrow{\scriptstyle f} \\ \mathcal{J} & \xrightarrow{Fr_{\mathcal{J}}} & \mathcal{J} \end{array}$$

Como $Fr(P_0) = P_0$ então

$$f \circ Fr(P) = [Fr(P) - P_0] = Frob_{\mathcal{J}}([P - P_0]) = Fr_{\mathcal{J}} \circ f(P) \tag{1.9}$$

para todo $P \in \mathcal{X}$. Queremos induzir o mapa $Fr_{\mathcal{J}}$ no módulo Tate $T_l(\mathcal{J})$. Sabemos que a aplicação

$$\theta_l : \mathbb{Z}_l \otimes End_{\mathbb{F}_q}(\mathcal{J}) \longrightarrow End_G(T_l(\mathcal{J}))$$

é uma bijetora por teorema principal em (TATE, 1966)), onde G é o grupo de Galois da extensão $\overline{\mathbb{F}}_q|\mathbb{F}_q$. Logo a representação $End_G(T_l(\mathcal{J})) \longrightarrow End_{\mathbb{F}_q}(\mathcal{J})$ que associa $f \mapsto \theta_l(1, f)$ é fiel. Se $[a_i] \in \mathcal{J}_{l^i}$ então

$$\psi_i \circ Fr_{\mathcal{J}}([a_i]) = [l^i Fr_{\mathcal{J}}(a_i)] = [l^{i-1} \cdot lFr_{\mathcal{J}}(a_i)] = [l^{i-1}] \cdot [0] = [0]$$

Logo $Fr_{\mathcal{J}}([a_i]) \in Ker(\psi_i) = \mathcal{J}_{l^i}$. Portanto $Fr_{\mathcal{J}}(\mathcal{J}_{l^i}) \subseteq \mathcal{J}_{l^i}$. A aplicação induzida

$$\begin{array}{rcl} Fr_{\mathcal{J}} : T_l(\mathcal{J}) & \longrightarrow & T_l(\mathcal{J}) \\ (a_n)_n & \longmapsto & (Fr_{\mathcal{J}}(a_n))_n \end{array}$$

Assim $Fr_{\mathcal{J}}$ age como uma aplicação linear em $T_l(\mathcal{J})$. Um fato interessante aqui é que o polinômio característico de $T_l(\mathcal{J})$ não depende de l.

Lema 1.56 ((RÜCK; STICHTENOTH, 1994)). *A aplicação de Frobenius do Jacobiano de uma curva maximal sobre $\mathbb{F}_{q^2}$ age como multiplicação por $(-q)$ em $\mathcal{J}$.*

Demonstração: Pelo Teorema 2 em (TATE, 1966), segue que a álgebra $\mathbb{Q} \times End_{\mathbb{F}_q}(\mathcal{J})$ é semi-simples e seu centro é $\mathbb{Q}[Fr_{\mathcal{J}}]$. Seja $h(t)$ o polinômio característico de $Fr_{\mathcal{J}}$. Assim $Fr_{\mathcal{J}}$ é aplicação diagonalizável e com todos os autovalores iguais a $-\sqrt{q}$. Logo $h(t) = (t + \sqrt{q})^{2g}$. Então

$$(Fr_{\mathcal{J}} - \sqrt{q}Id)^{2g} = h(Fr_{\mathcal{J}}) = 0.$$

isto é, $Fr_{\mathcal{J}} = -\sqrt{q}Id$. □

Lema 1.57 ((RÜCK; STICHTENOTH, 1994)). *Seja $\mathcal{X}$ uma curva $\mathbb{F}_{q^2}-$maximal de gênero g. Então o grupo das classes dos divisores de grau zero é isomorfo a $(\mathbb{Z}_{q+1})^{2g}$.*

Demonstração: Considere $\gamma : \mathcal{J} \longrightarrow \mathcal{J}$ dada por $\gamma(P) = (q+1)P$. Assim se $P \in \mathcal{J}$ satisfaz $(q+1)P = 0$ se, e somente se, $P = -qP = Fr_{\mathcal{J}}(P)$ se, e somente se, $P \in \mathcal{J}(\mathbb{F}_{q^2})$. Portanto

$$Ker\ \gamma = \mathcal{J}(\mathbb{F}_{q^2}).$$

Assim $Pic^0 \cong \mathcal{J}(\mathbb{F}_{q^2}) = Ker\ \gamma$. Como $dim\mathcal{J} = 2g$ então considere $\{e_1, ..., e_{2g}\}$ uma base para $\mathcal{J}$. Associamos a cada ponto de $\mathcal{J}$ escrito nesta base um vetor em $\mathbb{Z}_{q+1}$:

$$(k_1, ..., k_{2g}) \mapsto (k_1 + (q+1)\mathbb{Z}, ..., k_{2g} + (q+1)\mathbb{Z}).$$

Portanto $Pic^0 \cong ker\ \gamma \cong (Z_{q+1})^{2g}$. ▫

Corolário 1.58. *Para uma curva maximal $\mathcal{X}$ sobre k temos $qP + Fr(P) \sim (q+1)P_0$ para todo ponto $P \in \mathcal{X}$.*

Demonstração: Para $P \in \mathcal{X}$, temos por (1.9) que

$$[Fr(P) - P_0] = f \circ Fr(P) = Fr_{\mathcal{J}} \circ f(P) = -q[P - P_0]$$

então $Fr(P) + qP \sim (q+1)P_0$. ▫

Aplicando o resultado anterior apenas em pontos $\mathbb{F}_{q^2}-$racionais, obtemos a equivalência a seguir.

Corolário 1.59 (Equivalência Fundamental: (RÜCK; STICHTENOTH, 1994))**.** *Seja $\mathcal{X}$ uma curva maximal sobre k e sejam $P_0, P_1 \in \mathcal{X}(k)$. Então*

$$(q+1)P_1 \sim (q+1)P_0.$$

Corolário 1.60. *Se $\mathcal{X}$ é uma curva $\mathbb{F}_{q^2}-$maximal com $\mathcal{D} = |(q+1)P_0| = g^r_{q+1}$ o sistema de Frobenius de $\mathcal{X}$ num P_0 um ponto $\mathbb{F}_{q^2}-$racional, então $\mathcal{D}$ não depende do ponto racional escolhido e $r \geqslant 2$.*

Demonstração: Segue imediatamente do Corolário 1.59.

Cota de Castelnuovo

Seja $\mathcal{X}$ uma curva $\mathbb{F}_{q^2}-$maximal de gênero g. Considere $\mathcal{D}_0 = |(q+1)P_0|$ onde P_0 é um ponto $\mathbb{F}_{q^2}-$racional de $\mathcal{X}$. Pela Equivalência Fundamental o sistema não depende do ponto racional fixado P_0. Seja r a dimensão de Frobenius de $\mathcal{X}$. A dimensão r controla o gênero através da cota de Castelnuovo aplicada ao morfismo $\pi : \mathcal{X} \longrightarrow \mathbb{P}^r(k)$ associado a $\mathcal{D}_0$, a saber

Teorema 1.61 (Castelnuovo, Corolário 10.25, (HIRSCHFELD; KORCHMÁROS; TORRES, 2008))**.**

$$g \leqslant c_0(r, q+1) := \begin{cases} \dfrac{(2q-(r-1))^2 - 1)}{8(r-1)}, & \text{se } r \text{ é par} \\ \dfrac{(2q-(r-1))^2}{8(r-1)}, & \text{se } r \text{ é ímpar} \end{cases} \tag{1.10}$$

Cota de Furhmann-Torres

Esta sessão é dedicada ao artigo (FUHRMANN; TORRES, 1996), o qual prova o resultado que foi conjecturado por Stichtenoth e Xing, a saber: seja g o gênero de uma curva algébrica não singular irredutível e projetiva sobre o corpo finito $\mathbb{F}_{q^2}$, cujo número de pontos $\mathbb{F}_{q^2}-$racionais atinge a cota de Hasse-Weil, então

$$4g \leqslant (q-1)^2 \quad \text{ou} \quad 2g = (q-1)q.$$

O ponto de partida para a demonstração é consequência de um resultado de Stichenoth e Xing, o qual afirma que existe um ponto $k-$racional $P_0 \in \mathcal{X}$ tal que q e $q+1$ são não lacunas em P_0, ver em (XING; STICHTENOTH, 1995). Então o sistema linear $\mathcal{D} = g^r_{q+1} := |(q+1)P_0|$ é simples. Por Teorema 1.61 segue que se $r \geqslant 3$ então

$$4g \leqslant (q-1)^2. \tag{1.11}$$

Vamos considerar $r = 2$. Aplicamos a Teoria de Stöhr-Voloch ao sistema linear $\mathcal{D} = g^2_{q+1} = |(q+1)P_0|$. Para $P \in \mathcal{X}$, seja $0 = j_0(P) < j_1(P) < j_2(P) \leqslant q+1$ as $(\mathcal{D}, P)-$ordens. O fato que q e $q+1$ são não lacunas em P_0 implica que $j_1(P_0) = 1 \quad$ e $\quad j_2(P_0) = q+1$. Para calcular $j_2(P)$ para $P \in \mathcal{X}(k)$, usamos um resultado de Rück e Stichenoth, o Corolário 1.59. Então para todo $P \in \mathcal{X}(k)$ temos

$$j_2(P) = q+1. \tag{1.12}$$

Seja $0 = \nu_0 < \nu_1$ a sequência de ordens $k-$Frobenius de $\mathcal{D}$, reveja a Proposição 1.34. Pelo Corolário 1.41, segue que ν_1 satisfaz

$$\nu_1 \leqslant j_2(P) - j_1(P) = q + 1 - j_1(P) \tag{1.13}$$

para todo $P \in \mathcal{X}(k)$. Aplicando a relação (1.5) para $\mathcal{D}$, obtemos o grau do divisor de Frobenius

$$deg(S) = \nu_1(2g-2) + (q^2+2)(q+1) \tag{1.14}$$

cujo suporte está contido em $\mathcal{X}(k)$ (isto é consequência da Observação 1.38). Além disso, pela Proposição 1.39, temos para $P \in \mathcal{X}(k)$ vale a seguinte desigualdade

$$v_P(S) \geqslant j_1(P) + (j_2(P) - \nu_1) \geqslant q + 1 - \nu_1. \tag{1.15}$$

Proposição 1.62. *Suponha que* $4g > (q-1)^2$. *Então*

(i) $\nu_1 = q$.

(ii) $j_1(Q) = 1$ *para todo* $Q \in \mathcal{X}(k)$.

Demonstração: Obtemos a afirmação (ii) ao assumir (i) e usando a desigualdade (1.13). Para verificar (i), primeiramente observamos que $\nu_1 \leqslant q$. Usando (1.15) e (1.14) obtemos que

$$\begin{aligned} \nu_1(2g-2) + (q^2+2)(q+1) &= deg(S) \geqslant (q+1-\nu_1)\cdot \#\mathcal{X}(k) \\ &= (q+1-\nu_1)\cdot(q^2+1+2qg). \end{aligned}$$

Assim $(q^2-1)\nu_1 - q(q-1) \geqslant 2(q-1)^2q^2 - \nu_1(q-1)^2q + 4q(q-1)^2$ logo obtemos $\nu_1 \geqslant q$ pois $\nu_1(q^3-q^2+q-1) = \nu_1(q^2-1+q(q-1)^2) \geqslant 2(q-1)^2(q+q^2)$. ▫

Teorema 1.63 (Furhmann-Torres)**.** *Seja $\mathcal{X}$ uma curva $\mathbb{F}_{q^2}-$maximal de gênero g. Então*

$$4g \leqslant (q-1)^2 \quad ou \quad 2g = (q-1)q.$$

Demonstração: Suponha que $4g > (q-1)^2$. Como q e $q+1$ são não lacunas em algum ponto $P_0 \in \mathcal{X}(k)$, então $\langle q, q+1\rangle \subset H(P)$, logo g é menor ou igual ao $\langle q, q+1\rangle$. Assim segue que $2g \leqslant (q-1)q$. Considere R o divisor de $\mathcal{X}$ de ramificação de $\mathcal{D} = |(q+1)\cdot P_0|$. Então o grau do divisor R é dado por

$$deg(R) = (1+q)(2g-2) + 3(q+1),$$

pois da Proposição 1.62 temos $\varepsilon_1 = 1$. Pelo Teorema 1.26 e pela relação (1.12) temos $v_P(R) \geqslant 1$ para todo $P \in \mathcal{X}(k)$. Assim $deg(R) \geqslant \#\mathcal{X}(k)$ e pela maximalidade segue que $2g \geqslant q(q-1)$. ▫

Para buscar um modelo não singular para uma curva maximal de gênero $q(q-1)/2$ podemos utilizar a existência de um ponto $\mathbb{F}_{q^2}-$racional P_0 e funções x, y $\mathbb{F}_{q^2}-$racionais da curva tais que $di\nu_\infty(x) = qP_0$ e $di\nu_\infty(y) = (q+1)P_0$. O espaço

$$\left\{x^iy^j : (i,j) \in \mathbb{N}_0 \times \mathbb{N}_0,\ iq + j(q+1) \leqslant q(q+1)\right\}$$

que tem $1 + (q+1)(q+2)/2$ elementos induz uma combinação $\mathbb{F}_{q^2}-$linear não trivial. O resultado a seguir garante que através desse processo obtemos um $\mathbb{F}_{q^2}-$isomorfismo com a curva Hermitiana.

Teorema 1.64 ((FUHRMANN; TORRES, 1996))**.** *Uma curva $\mathbb{F}_{q^2}-$maximal de gênero $g = q(q-1)/2$ é $\mathbb{F}_{q^2}-$isomorfa a uma curva Hermitiana, a qual é definida por uma equação do tipo*

$$y^q + y = x^{q+1}.$$

Comportamento das ordens da série Frobenius

Os resultados a seguir foram construídos por Furhmann, Garcia e Torres, os quais explicitam o comportamento das ordens do sistema Frobenius e o comportamento das não-lacunas em determinados pontos para curva maximais.

O comportamento das ordens da série de Frobenius de curvas maximais, o qual foi observado em Proposição 1.62, é estendido para qualquer dimensão Frobenius r e gênero, isto é, decorre da maximalidade.

Teorema 1.65 (Teorema 1.4, (FUHRMANN; GARCIA; TORRES, 1997)). *Sejam $\mathcal{X}$ uma curva $\mathbb{F}_{q^2}-$maximal e $\mathcal{D}$ sua série de Frobenius com dimensão r. Considere $\varepsilon_0 < \varepsilon_1 < ... < \varepsilon_r$ sua sequência de ordens da série de Frobenius e $j_i(P)$ a $i-$ésima $(\mathcal{D}, P)-$ordem. Então,*

(i) $\varepsilon_r = q$;

(ii) $j_r(P) = q + 1$ *se* $P \in \mathcal{X}(\mathbb{F}_{q^2})$ *e* $j_r(P) = q$ *se* $P \notin \mathcal{X}(\mathbb{F}_{q^2})$.

(iii) $j_1(P) = 1$ *para todos pontos* $P \in \mathcal{X}$. *Em particular,* $\varepsilon_1 = 1$.

O comportamento das não lacunas em pontos de uma curva maximal pode ser relacionado com a série de Frobenius associada. Em especial, as não lacunas em pontos $k-$racionais da curva possuem propriedades interessantes, as quais iremos sempre recorrer neste trabalho.

Proposição 1.66 (Proposição 1.5, (FUHRMANN; GARCIA; TORRES, 1997)). *Sejam $\mathcal{X}$ uma curva $\mathbb{F}_{q^2}-$maximal e $\mathcal{D}$ sua série de Frobenius com dimensão r. Para $P \in \mathcal{X}$ seja $m_i(P)$ a $i-$ésima não-lacuna em P. Então,*

(i) para cada $P \in \mathcal{X}$ *temos*

$$0 < m_1(P) < ... < m_{r-1}(P) \leqslant q < m_r(P);$$

(ii) se $P \notin \mathcal{X}(\mathbb{F}_{q^2})$, *então os números* $0 \leqslant q - m_{r-1}(P) < ... < q - m_1(P) < q$ *são* $(\mathcal{D}, P)-$*ordens;*

(iii) se $P \in \mathcal{X}(\mathbb{F}_{q^2})$, *então as* $(\mathcal{D}, P)-$*ordens são*

$$0 < q + 1 - m_{r-1}(P) < ... < q + 1 - m_1(P) < q + 1;$$

(iv) se $P \in \mathcal{X}(\mathbb{F}_{q^2})$, *então* q *e* $q + 1$ *são não-lacunas em* P.

Cota de Korchmáros-Torres

A cota de Furhmann e Torres para gêneros de curvas $\mathbb{F}_{q^2}-$maximais foi melhorada por Korchmáros e Torres ao explicitar o terceiro maior gênero possível. Este valor depende de propriedades aritméticas de q.

Teorema 1.67. *(KORCHMÁROS; TORRES, 2002) Seja $\mathcal{X}$ uma curva $\mathbb{F}_{q^2}-$maximal de gênero g. Então,*

$$g \leqslant g_2, \quad g = g_1 \quad ou \quad g = g_0, \tag{1.16}$$

onde $g_0 := q(q-1)/2$, $g_1 := \lfloor (q-1)^2/4 \rfloor$ *e* $g_2 := \lfloor (q^2 - q + 4)/6 \rfloor$. *Além disso,*

(i) para $q \equiv 1 \ mod\ 3$, $q \geqslant 13$, *não existe curva* $\mathbb{F}_{q^2}-$*maximal de gênero igual a* $(q-1)(q-2)/6$;

(ii) para $q \equiv 2 \ mod\ 3$, $q \geqslant 11$, *a curva não singular dada pela equação* $y^q + y = x^{(q+1)/3}$ *é a única curva* $\mathbb{F}_{q^2}-$*maximal de gênero* $(q-1)(q-2)/6$.

Exemplos de curvas maximais não cobertas pela Hermitiana

A maioria dos exemplos de curvas maximais provem de coberturas da curva Hermitiana.

Definição 1.68. *Seja* $\mathcal{F}$ *uma curva plana definida sobre* $\mathbb{F}_q$.

(i) Uma ***transformação racional de*** $K(\mathcal{F})$ *é um mapa* $\omega : \mathbb{F}_q(\mathcal{F}) \longrightarrow \mathbb{F}_q(\mathcal{F})$ *que é uma transformação* $\mathbb{F}_q-$*racional e* $\omega(K(\mathcal{F}))$ *é um corpo de funções* $\mathbb{F}_q-$*racionais;*

(ii) Se $\mathcal{F}'$ *é a imagem de* $\mathcal{F}$ *via uma transformação* $\mathbb{F}_q-$*racional, então* $\mathcal{F} \longrightarrow \mathcal{F}'$ *é dito um* ***cobrimento*** $\mathbb{F}_q-$***racional***.

Existem exemplos conhecidos de curvas que são maximais mas não são cobertas pela curva Hermitiana.

Exemplo 1.69. *Seja* $q = n^3$ *com* n *potência de um primo* p. *A* ***curva GK*** *é dada pela equações*

$$Z^{n^2-n+1} = Yh(X) \ e \ X^n + X = Y^{n+1}.$$

Ela maximal sobre $\mathbb{F}_{q^2}$ *de gênero* $\dfrac{1}{2}(n^3+1)(n^2-2)+1$, *onde*

$$h(X) = \sum_{i=0}^{n} (-1)^{i+1} X^{i(n-1)}.$$

Este é um exemplo de curva que não é Galois-coberta pela curva Hermitiana para $n > 2$. *Mais informações podem ser encontradas em (GIULIETTI; KORCHMÁROS, 2009).*

Exemplo 1.70. *A* ***curva GGS*** *ou* ***curva GK-generalizada*** $\mathcal{C}_n$ *é o modelo não singular sobre* $\mathbb{F}_{q^{2n}}$ *da curva definida pelas equações afins*

$$v^{q+1} = u^q + u \quad e \quad w^{\frac{q^n+1}{q+1}} = v^{q^2} - v$$

e o gênero $\dfrac{q^{n+2} - q^n - q^3 + q^2}{2}$. *Em (DUURSMA; MAK, 2012) observaram que* $\mathcal{C}_n$ *não pode ser Galois-coberta pela curva Hermitiana sobre* $\mathbb{F}_{q^{2n}}$ *quando* $n > 3$ *e* $q > 2$. *Em (GIULIETTI; MONTANUCCI; ZINI, 2016), é observado que a curva não é Galois-coberta pela Hermitiana nos casos* $q = 2$ *e* $n \geqslant 5$.

Exemplo 1.71. *Seja $n \geqslant 3$ é um inteiro ímpar, q é uma potência de um primo e $s \geqslant 1$ um divisor de $(q^n+1)/(q+1)$. Seja $\mathcal{C}_n$ a curva GGS e considere o morfismo $\varphi_{n,s} : \mathcal{C}_n \longrightarrow \mathbb{P}^3$ dado por*

$$\varphi(u,v,w,1) \longrightarrow (x,y,z,1) := (u,v,w^s,1).$$

Considere a curva $\mathcal{Y}_{n,s}$ o modelo não singular sobre $\mathbb{F}_{q^{2n}}$ de $\varphi_{n,s}(\mathcal{C}_n)$, o qual é dado pelo modelo

$$y^{q+1} = x^q + x \quad e \quad z^M = y^{q^2} - y, \tag{1.17}$$

onde $M = \dfrac{q^n+1}{s(q+1)}$. Esta curva é $\mathbb{F}_{q^{2n}}-$maximal de gênero $\dfrac{q^{n+2}-q^n-sq^3+q^2+s-1}{2s}$. Em (TAFAZOLIAN; TEHERÁN-HERRERA; TORRES, 2016) foi observado que fixando $n=3$ e s divisor de q^2-q+1, a curva $\mathcal{Y}_{3,s}$ não pode coberta pela curva Hermitiana $\mathcal{H}_3$ sobre $\mathbb{F}_{q^6}$ para $q > s(s+1)$.

1.5 O Problema de determinação do Espectro dos Gêneros

Seja q a potência de um número primo p. Consideramos o corpo $k = \mathbb{F}_{q^2}$ o corpo finito com q^2 elementos. Estamos interessados em determinar o conjunto

$$\mathbf{M}(q^2) := \{ \quad g \in \mathbb{N}_0 : \text{existe uma curva } k-\text{maximal de gênero } g \quad \},$$

chamado de **Espectro dos Gêneros** sobre k. Dado $g \in \mathbf{M}(q^2)$, outro problema interessante é saber quantas curvas $k-$maximais de gênero g existem, a menos de isomorfismo.

Usando os resultados já conhecidos de curvas maximais sobre k, podemos responder estes problemas para alguns valores de q. Usando o Teorema 1.63 e o Teorema 1.67 obtemos o resultado a seguir.

Teorema 1.72 ((KORCHMÁROS; TORRES, 2002))**.**

$$\boldsymbol{M}(q^2) \subseteq [0, g_2] \cup \{g_1\} \cup \{g_0\}, \tag{1.18}$$

onde $g_0 := q(q-1)/2$, $g_1 := \lfloor (q-1)^2/4 \rfloor$ e $g_2 := \lfloor (q^2-q+4)/6 \rfloor$.

Aplicando o teorema anterior podemos explicitar o espectro de gêneros para $q \leqslant 5$.

Corolário 1.73. *(i)* $\boldsymbol{M}(2^2) = \{0,1\}$.

(ii) $\boldsymbol{M}(3^2) = \{0,1,3\}$.

(iii) $\boldsymbol{M}(4^2) = \{0,1,2,6\}$;

(iv) $\boldsymbol{M}(5^2) = \{0,1,2,3,4,10\}$;

(v) $\mathbf{M}(7^2) \subseteq [0,7] \cup \{9\} \cup \{21\}$.

Em (ARAKELIAN; TAFAZOLIAN; TORRES, 2018) foi determinado

$$\mathbf{M}(7^2) = \{0,1,2,3,5,7,9,21\}.$$

Observação 1.74. *Utilizando o exemplo 1.69 obtemos:* $99 \in \boldsymbol{M}(27^2)$. *Segue do Teorema 1.67 segue que:* $22 \notin \boldsymbol{M}(13^2)$, $35 \notin \boldsymbol{M}(16^2)$, $51 \notin \boldsymbol{M}(19^2)$, $92 \notin \boldsymbol{M}(25^2)$.

Usando a dimensão de Frobenius podemos descartar alguns valores de gênero no Espectro.

Proposição 1.75 (Prop 3.1, (ARAKELIAN; TAFAZOLIAN; TORRES, 2018))**.** *Seja $\mathcal{X}$ uma curva $\mathbb{F}_{q^2}-$maximal de gênero g com dimensão Frobenius igual a r. Se alguma das condições é satisfeita:*

(a) $q \equiv 0 \ mod\ 3$ *e* $(3q-1)(2g-2) > (q+1)(q^2-4q-1)$ *ou*

(b) $q \not\equiv 0 \ mod\ 3$, $r = 3$ *e* $(4q-1)(2g-2) > (q+1)(q^2-5q-2)$

então

$$g \geqslant c_1(q) := \frac{q^2-2q+3}{6}. \tag{1.19}$$

Corolário 1.76 ((ARAKELIAN; TAFAZOLIAN; TORRES, 2018))**.** *Seja $q \not\equiv 0 \ mod\ 3$. Seja $\mathcal{X}$ uma curva $\mathbb{F}_{q^2}-$maximal de gênero g com $g > \frac{(q-1)(q-2)}{6}$. Então*

$$g \geqslant c_1(q). \tag{1.20}$$

Demonstração: Seja r a dimensão de Frobenius de $\mathcal{X}$. Se $r \geqslant 4$ então $g \leqslant (q-1)(q-2)/6$ o que contradiz a hipótese. Logo $r \leqslant 3$. Se $r = 2$ segue que $g = (q-1)q/2$ portanto vale 1.20. Se $r = 3$ então aplicando a hipótese sobre g temos

$$\begin{aligned}(4q-1)(2g-2) &> (4q-1)\frac{(q-1)(q-2)-6}{3} = (4q-1)\frac{(q+1)(q-4)}{3} \\ &= (q+1)\frac{(4q^2-17q+4)}{3} > (q+1)(q^2-5q-2)\end{aligned}$$

Aplicando a Proposição 1.75, segue que $g \geqslant c_1(q)$. ▫ Em (ARAKELIAN; TAFAZOLIAN; TORRES, 2018) são aplicados para $q \leqslant 16$, a saber,

$6 \notin \mathbf{M}(7^2), 8 \notin \mathbf{M}(8^2), 10 \notin \mathbf{M}(9^2), 16 \notin \mathbf{M}(11^2), 23, 24 \notin \mathbf{M}(13^2)$ e $36, 37 \notin \mathbf{M}(16^2)$.

Explicitamos para $q \leqslant 29$ no resultado a seguir.

Corolário 1.77. *(i)* $41, 42 \notin \boldsymbol{M}(17^2)$;

(ii) $52, 53, 54 \notin \boldsymbol{M}(19^2)$;

(iii) $78, 79, 80 \notin \boldsymbol{M}(23^2)$*;*

(iv) $93, 94, 95, 96 \notin \boldsymbol{M}(25^2)$*;*

(v) $110, 111, 112 \notin \boldsymbol{M}(27^2)$*;*

(vi) $127, 128, 129, 130 \notin \boldsymbol{M}(29^2)$.

Além disso, encontramos para $8 \leqslant q \leqslant 29$ as seguintes informações:

(i) $\{0, 1, 2, 3, 4, 6, 7, 9, 10, 12, 28\} \subseteq \mathbf{M}(8^2) \subseteq [0, 10] \cup \{12\} \cup \{28\}$;

(ii) $\{0, 1, 2, 3, 4, 6, 8, 9, 12, 16, 36\} \subseteq \mathbf{M}(9^2) \subseteq [0, 12] \cup \{16\} \cup \{36\}$;

(iii) $\{0, 1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 13, 15, 18, 19, 25, 55\} \subseteq \mathbf{M}(11^2) \subseteq [0, 19] \cup \{25\} \cup \{55\}$;

(iv) $\{0, 1, 2, 3, 4, 5, 6, 9, 10, 12, 15, 18, 26, 36, 78\} \subseteq \mathbf{M}(13^2) \subseteq [0, 21] \cup [23, 26] \cup \{36\} \cup \{78\}$;

(v) $\{0, 1, 2, 4, 6, 8, 12, 16, 24, 28, 40, 56, 120\} \subseteq \mathbf{M}(16^2) \subseteq [0, 34] \cup [36, 40] \subseteq \{56\} \cup \{120\}$;

(vi) $\{0, 1, 2, 3, 4, 5, 6, 7, 8, 10, 11, 12, 14, 16, 19, 22, 28, 32, 40, 45, 46, 64, 136\} \subseteq \mathbf{M}(17^2) \subseteq [0, 46] \cup \{64\} \cup \{136\}$;

(vii) $\{0, 1, 2, 3, 4, 5, 6, 7, 8, 9, 12, 13, 14, 16, 17, 18, 19, 21, 24, 27, 35, 36, 41, 57, 81, 171\} \subseteq \mathbf{M}(19^2) \subseteq [0, 57] \cup \{81\} \cup \{171\}$;

(viii) $\{0, 1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 13, 15, 16, 17, 19, 21, 22, 23, 25, 28, 31, 33, 37, 41, 55, 61, 77, 84, 85, 121, 253\} \subseteq \mathbf{M}(23^2) \subseteq [0, 85] \cup \{121\} \cup \{253\}$;

(ix) $\{0, 1, 2, 3, 4, 6, 8, 10, 12, 18, 22, 24, 30, 36, 44, 48, 50, 60, 66, 72, 100, 144, 300\} \subseteq \mathbf{M}(25^2) \subseteq [0, 100] \cup \{144\} \cup \{300\}$;

(x) $\{0, 1, 3, 4, 6, 7, 9, 10, 12, 13, 15, 16, 17, 18, 19, 24, 25, 26, 27, 39, 43, 51, 52, 78, 85, 108, 117, 169, 351\} \subseteq \mathbf{M}(27^2) \subseteq [0, 117] \cup \{169\} \cup \{351\}$;

(xi) $\{0, 1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 16, 17, 18, 19, 20, 21, 22, 24, 26, 28, 31, 33, 34, 36, 40, 42, 45, 49, 56, 58, 61, 66, 70, 82, 91, 98, 126, 135, 136, 196, 406\} \subseteq \mathbf{M}(29^2) \subseteq [0, 136] \cup \{196\} \cup \{406\}$.

Algumas perguntas ainda sem resposta:

(i) $5 \in \mathbf{M}(8^2)$?

(ii) $5, 7, 11 \in \mathbf{M}(9^2)$?

(iii) $12, 14, 17 \in \mathbf{M}(11^2)$?

(iv) $7, 8, 11, 13, 14, 16, 17, 19, 20, 21, 25 \in \mathbf{M}(13^2)$?

(v) $3, 5, 7, 9, 10, 11, 13, 14, 15, 17, 18, 19, 20, 21, 22, 23, 25, 26, 27, 29, 30, 31, 32, 33, 34, 38, 39 \in \mathbf{M}(16^2)$?

(vi) $9, 13, 15, 17 \in \mathbf{M}(17^2)$?

(vii) $10, 11, 15 \in \mathbf{M}(19^2)$?

(viii) $5, 7, 9, 11 \in \mathbf{M}(25^2)$?

Em (MONTANUCCI; ZINI, 2018) foi mostrado que estes casos restantes não podem ser satisfeitos por curvas Galois-coberta pela curva Hermitiana sobre $\mathbb{F}_{q^2}$.

1.6 Classificação de curvas maximais com dimensão Frobenius 3

Nesta seção iremos introduzir as ferramentas necessárias para classificar uma curva $\mathbb{F}_{q^2}-$maximal com dimensão Frobenius 3 via modelos $\mathbb{F}_{q^2}-$birracionais. Uma das ferramentas fundamentais aqui é um fato mais geral, o qual afirma que curvas maximais estão mergulhadas numa superfície Hermitiana.

Teorema 1.78 (Natural Embedding Theorem, (HIRSCHFELD; KORCHMÁROS; TORRES, 2008))**.** *Seja $\mathcal{X}$ uma curva $\mathbb{F}_{q^2}-$maximal com dimensão de Frobenius r. Então $\mathcal{X}$ é isomorfa sobre $\mathbb{F}_{q^2}$ a uma curva em $\mathbb{P}^m(\overline{\mathbb{F}}_{q^2})$ de grau $q+1$ pertencendo a uma variedade Hermitiana $\mathcal{H}_m$ definida sobre $\mathbb{F}_{q^2}$ com $m \leqslant r$. Além disso, o hiperplano osculador de $\mathcal{X}$ em todo ponto $P \in \mathcal{X}$ coincide com o hiperplano tangente em P em $\mathcal{H}_m$.*

Aplicando em particular para dimensão Frobenius igual a 3, obtemos a dimensão da variedade Hermitiana.

Corolário 1.79. *Seja $\mathcal{X}$ uma curva $\mathbb{F}_{q^2}-$maximal de dimensão Frobenius 3. Então $\mathcal{X}$ é isomorfa sobre $\mathbb{F}_{q^2}$ a uma curva em $\mathbb{P}^3(\overline{\mathbb{F}}_{q^2})$ de grau $q+1$ pertencendo a uma variedade Hermitiana $\mathcal{H}_3$ definida sobre $\mathbb{F}_{q^2}$. Além disso, o hiperplano osculador de $\mathcal{X}$ em todo ponto $P \in \mathcal{X}$ coincide com o hiperplano tangente em P em $\mathcal{H}_3$.*

Demonstração: Do Teorema 1.78 segue que $m \leqslant 3$. Se $m = 2$ então $\mathcal{X}$ é isomorfa a curva Hermitiana $\mathcal{H}_2$, logo $r = 2$ um absurdo. Logo $m = 3$. ▫

Tendo em vista estes resultados, a classificação de uma curva $\mathbb{F}_{q^2}-$maximal de dimensão Frobenius 3, via (FANALI; GIULIETTI; PLATONI, 2012), utiliza a existência de uma curva em $\mathbb{P}^3(\overline{\mathbb{F}}_{q^2})$ de grau $q+1$ pertencendo a uma variedade Hermitiana $\mathcal{H}_3$ definida sobre $\mathbb{F}_{q^2}$, a qual é isomorfa a curva inicial sobre $\mathbb{F}_{q^2}$.

1.6.1 Trabalhos de Fanali-Giulietti-Platoni

Em (FANALI; GIULIETTI, 2009), Fanali e Giulietti observaram que dada uma curva $\mathbb{F}_{q^2}-$maximal com dimensão Frobenius 3, suas ordens de contatos com planos tangentes não osculantes nos permitiriam caracterizar uma família de modelos $\mathbb{F}_{q^2}-$birracionais para tal curva. Foram construídas projetividades que preservavam características convenientes em tais planos e como tais fatos afetam nos modelos da curva em (FANALI; GIULIETTI; PLATONI, 2012).

Seja $\mathcal{X}$ uma curva maximal sobre $\mathbb{F}_{q^2}$ com dimensão Frobenius 3. Seja m_P a primeira não-lacuna em P um ponto $\mathbb{F}_{q^2}-$racional de $\mathcal{X}$. Vamos considerar as coordenadas de $\mathbb{P}^3(\overline{\mathbb{F}}_{q^2})$ como $(t : x : y : z)$.

Observação 1.80. *Como o grupo de transformações lineares preservando $\mathcal{H}_3$ age transitivamente em $\mathcal{H}_3(\mathbb{F}_{q^2})$, podemos assumir que $P = (0 : 1 : 0 : 0) \in \mathcal{X}$. Além diso, o plano osculante a $\mathcal{X}$ no ponto P é dado pela equação $T = 0$, o qual coincide com o plano tangente a $\mathcal{H}_3$ no ponto P.*

Lema 1.81 (Lema 1, (FANALI; GIULIETTI; PLATONI, 2012))**.** *Existe uma projetividade que mapeia a reta tangente de $\mathcal{X}$ em P na reta com equação $Y = 0$, $T = 0$ e preservando $\mathcal{H}_3$, o ponto P e o plano $T = 0$.*

Demonstração: Seja l a reta tangente a $\mathcal{X}$ no ponto P. Como l está contida no plano osculante a $\mathcal{X}$ em P, temos que l pode ser definida pelas equações

$$aY - bZ = 0 \quad \text{e} \quad T = 0$$

para certos $a, b \in \mathbb{F}_{q^2}$. Se $b = 0$ não há o que provar. Se $a = 0$ trocamos Z por Y. Se $ab \neq 0$, podemos reescrever as equações de l por

$$Y - \mu Z = 0 \quad \text{e} \quad T = 0$$

com $\mu \in \mathbb{F}_{q^2}^*$. Considere $\alpha, \beta, m \in \mathbb{F}_{q^2}$ com $m \neq 0$ e $\alpha\mu \neq \beta$ tais que

$$\begin{aligned} m^{q+1} + (\mu m)^{q+1} &= 1, \\ \alpha^{q+1} + \beta^{q+1} &= 1, \\ \alpha + \beta\mu^q &= 0. \end{aligned} \tag{1.21}$$

Definimos ϕ a transformação linear dada por $X \mapsto X'$, $Y \mapsto \beta Y' + \mu m Z'$, $Z \mapsto \alpha Y' + m Z'$ e $T \mapsto T'$. Pode-ser verificar que o mapa ϕ satisfaz a tese do lema já que a reta $\phi^{-1}(l)$ tem equações

$$Y = 0 \quad \text{e} \quad T = 0.$$

Para verificação da existência de $\alpha, \beta, m \in \mathbb{F}_{q^2}$ satisfazendo (1.21), veja demonstração do Lema 1 em (FANALI; GIULIETTI; PLATONI, 2012). ▫

Pelo resultado anterior podemos sempre assumir que a reta tangente a $\mathcal{X}$ no ponto P tem equações

$$Y = 0 \quad \text{e} \quad T = 0. \tag{1.22}$$

Da mesma maneira, queremos caracterizar os planos tangentes não osculantes a $\mathcal{X}$ em P.

Lema 1.82 (Lema 2, (FANALI; GIULIETTI; PLATONI, 2012))**.** *Para todo plano tangente π não osculante a $\mathcal{X}$ em P, o qual é definido sobre $\mathbb{F}_{q^2}$, existe uma projetividade que mapeia π no plano $Y = 0$ e preserva $\mathcal{H}_3$, o ponto P, o plano $T = 0$ e a reta com equações $Y = 0, T = 0$.*

Demonstração: Seja π um plano tangente não osculante a $\mathcal{X}$ em P, o qual é definido sobre $\mathbb{F}_{q^2}$. Como π contém a reta tangente a $\mathcal{X}$ em P, podemos escrever a equação para π como $Y = nT$ para algum $n \in \mathbb{F}_{q^2}$. Considere $\alpha := n^q$ e $\beta \in \mathbb{F}_{q^2}$ tal que $\beta^q + \beta = n^{q+1}$. Definimos φ a transformação linear dada por $X \mapsto X' + \alpha Y' + \beta T'$, $Y \mapsto Y' + nT'$, $Z \mapsto Z'$ e $T \mapsto T'$. Assim o plano $\varphi^{-1}(\pi)$ tem equações $Y = 0$ e $T = 0$. Pode-se verificar que φ satisfaz a tese. ▫

A descrição de um plano tangente não osculante a $\mathcal{X}$ em P pode ser mais precisa quando sabemos a quantidade de pontos $\mathbb{F}_{q^2}-$racionais de $\mathcal{X}$ neste plano.

Lema 1.83 (Lema 3, (FANALI; GIULIETTI; PLATONI, 2012))**.** *Seja π um plano tangente não osculante que passa por P, o qual é definido sobre $\mathbb{F}_{q^2}$ e que contém pelo menos dois pontos $\mathbb{F}_{q^2}-$racionais distintos de $\mathcal{X}$ e também diferentes de P. Sejam P_1 e P_2 tais pontos. Então podemos assumir $P_1 = (1 : 0 : 0 : 0)$ e algumas das duas possibilidades:*

(a) $P_2 = (1 : B : 0 : 1)$ para algum $B \in \mathbb{F}_{q^2}$ com $B^q + B = 1$,

(b) Fixe $W \in \mathbb{F}_{q^2}^*$ tal que $W^q + W = 0$ então $P_2 = (1 : W : 0 : 0)$.

Demonstração: Pelo Lema 1.82 podemos assumir π com equação $Y = 0$. Como $P_1 \in \mathcal{H}_3 \cap \pi$ podemos escrever $P_1 := (1 : A : 0 : B)$ com $A, B \in \mathbb{F}_{q^2}$ tais que $B^{q+1} = A^q + A$. Considere ϕ definida como

$$X \mapsto X' + B^q Z' + AT', \quad Y \mapsto Y', \quad Z \mapsto Z' + BT', \quad T \mapsto T'.$$

Este mapa ϕ preserva $\mathcal{H}_3$, preserva o plano π, o ponto P e a reta com equações $Y = 0$ e $T = 0$. Como $\phi^{-1}(P_1) \in \pi \cap \mathcal{H}_3$ segue que $\phi^{-1}(P_1) = (1 : 0 : 0 : 0)$. Portanto podemos assumir que $P_1 = (1 : 0 : 0 : 0)$. Para o segundo ponto $P_2 \in \mathcal{H}_3(\mathbb{F}_{q^2}) \cap \pi$, considere $P_2 := (1 : C : 0 : \lambda)$ com $\lambda, C \in \mathbb{F}_{q^2}$ tais que $\lambda^{q+1} = C^q + C$. Se $\lambda = 0$, como W é uma raíz de $X^q + X = 0$ em $\mathbb{F}_{q^2}$ segue que $C = sW$ com $s \in \mathbb{F}_q^*$. Seja $t \in \mathbb{F}_{q^2}$ tal que $s = t^{q+1}$. Considere a transformação linear σ dada por

$$X \mapsto sX', \quad Y \mapsto tY', \quad Z \mapsto tZ', \quad T \mapsto T'.$$

Tal mapa preserva $\mathcal{H}_3$, o ponto P, a reta tangente em P, a reta $Y=0, T=0$, o plano π e $(1:0:0:0)$. Além disso, $\sigma^{-1}(P_2)=(1:W:0:0)$. Isto se enquadra no caso (b). Suponha que $\lambda \neq 0$. Consideramos a transformação linear ψ dada por

$$X \mapsto \lambda^{q+1}X', \quad Y \mapsto \lambda Y', \quad Z \mapsto \lambda Z', \quad T \mapsto T'.$$

Logo ψ preserva $\mathcal{H}_3$, o ponto P, a reta tangente em P, a reta $Y=0, T=0$, o plano π e $(1:0:0:0)$. Além disso, $\psi^{-1}(P_2)=(1:C/\lambda^{q+1}:0:1)$. Tomando $B := C/\lambda^{q+1}$ temos o caso (a). ▫

Quando π não contém pontos $\mathbb{F}_{q^2}-$racionais, assumimos uma **ordem total** em toda extensão finita $\mathbb{F}_{q^{2r}}$ de $\mathbb{F}_{q^2}$, a saber:

$$q_1 \preceq_r q_2 \quad \text{se } q_1 \in \mathbb{F}_{q^{2r_1}}, q_2 \in \mathbb{F}_{q^{2r_2}} \text{ com } r_1 \leqslant r_2.$$

Relembramos que o **grau** de um ponto $Q \in \mathcal{X}$ é definido sendo o menor inteiro r tal que $Q \in \mathcal{X}(\mathbb{F}_{q^{2r}})$.

Lema 1.84 (Lema 4, (FANALI; GIULIETTI; PLATONI, 2012))**.** *Seja π um plano tangente não osculante em P definido sobre $\mathbb{F}_{q^2}$, contendo um ponto P_1 tal que $r := deg(P_1) > 1$. Seja $\omega \in \mathbb{F}_{q^{2r}}$ um elemento primitivo sobre $\mathbb{F}_{q^2}$. Então podemos assumir que $P_1 = (1:\overline{X}:0:\overline{Z})$ onde*

(i) $\overline{Z} = \omega^{r-1}$ ou $\overline{Z} = \omega^{i_0} + \sum_{i=i_0+1}^{r-1} \overline{Z}_i \omega^i$, com $0 < i_0 < r-1$ e $\overline{Z}_i \in \mathbb{F}_{q^2}$;

(ii) $\overline{X}$ é a menor raiz do polinômio $T^q + T = \overline{Z}^{q+1}$ com respeito à ordenação $\preceq_r$.

Demonstração: Pelo Lema 1.82 podemos assumir que o plano π tem equação $Y=0$. Podemos escrever $P_1 := (1:A:0:B)$ com $A, B \in \mathbb{F}_{q^{2r}}$ tais que $B^{q+1} = A^q + A$. Como $\omega \in \mathbb{F}_{q^{2r}}$ é um elemento primitivo, temos que $\{1, \omega, .., \omega^{r-1}\}$ é uma base de $\mathbb{F}_{q^{2r}}$ sobre $\mathbb{F}_{q^2}$. Podemos escrever

$$A = \sum_{i=0}^{r-1} A_i \omega^i \quad \text{e} \quad B := \sum_{i=0}^{r-1} B_i \omega^i,$$

com $A_0, A_1, ..., A_{r-1}, B_0, B_1, ..., B_{r-1} \in \mathbb{F}_{q^2}$. Observamos que $B_0 \neq 0$. Seja i_0 o primeiro índice positivo tal que $B_{i_0} \neq 0$.

Sejam $a := 1/B_{i_0}$, $b := -B_0/B_{i_0}$ e $c \in \mathbb{F}_{q^2}$ tal que $c^q + c = b^{q+1}$. Considere θ a transformação linear dada por

$$X' \mapsto a^{q+1}X + ab^qZ + cT, \quad Y' \mapsto aY, \quad Z' \mapsto aZ + bT, \quad T' \mapsto T.$$

O mapa θ preserva $\mathcal{H}_3$, o ponto P, a reta tangente em P, a reta $Y=0, T=0$ e o plano π. Além disso, $\theta(P_1) = \big(1 : a^{q+1}A + ab^qB + c : 0 : aB + b\big)$. Sejam $\tilde{X} := a^{q+1}A + ab^qB + c$ e $\overline{Z} := aB + b$. Daí $\overline{Z} = \dfrac{1}{B_{i_0}} \sum_{i=i_0}^{r-1} B_i \omega^i$. Isto prova o item (i).

Para verificar o item (ii), seja $\overline{X}$ a menor raiz do polinômio $T^q+T=\overline{Z}^{q+1}$, com respeito a ordenação $\preceq_r$. Seja $d:=\tilde{X}-\overline{X}$. Assim $d^q+d=0$. Consideramos novamente uma transformação linear Γ dada por

$$X'\mapsto X+dT,\quad Y'\mapsto Y,\quad Z'\mapsto Z,\quad T'\mapsto T.$$

Assim Γ preserva $\mathcal{H}_3$, o ponto P, a reta tangente em P, a reta $Y=0,T=0$ e o plano π. Além disso, $\Gamma(1:\tilde{X}:0:\overline{Z})=(1:\tilde{X}+d:0:\overline{Z})=(1:\overline{X}:0:\overline{Z})$. Isto prova (ii). ▫

Enfim podemos enunciar o teorema principal dos trabalhos de Fanali-Giulietti-Platoni.

Teorema 1.85 (Teorema 4, (FANALI; GIULIETTI; PLATONI, 2012))**.** *Seja $\mathcal{X}$ uma curva maximal sobre $\mathbb{F}_{q^2}$ com dimensão Frobenius 3. Seja m_P a primeira não-lacuna em P um ponto $\mathbb{F}_{q^2}-$racional de $\mathcal{X}$. Seja π um plano tangente não osculante a $\mathcal{X}$ em P definido sobre $\mathbb{F}_{q^2}$. Assuma que o divisor de interseção de $\mathcal{X}$ e π seja*

$$D=(q+1-m_P)P+m_1P_1+...+m_dP_d$$

com $m_1+...+m_d=m_P$, $P_i\neq P$ e $P_i\neq P_j$ se $i\neq j$. Então $\mathcal{X}$ é $\mathbb{F}_{q^2}-$birracionalmente equivalente a curva plana com equação

$$Z^{q+1}=X^q+X+\lambda\xi(X,Z) \tag{1.23}$$

onde $\lambda\in\mathbb{F}_{q^2}^*$ e $\xi(X,Z)$ é um polinômio definido sobre $\mathbb{F}_{q^2}$ de grau m_P, obtido como o produto de d polinômios $L_1(X,Z)^{m_1},...,L_d(X,Z)^{m_d}$ tais que as retas com equação $L_i(X,Z)=0$ são retas tangentes da curva Hermitiana $Z^{q+1}=X^q+X$ em d pontos (não necessariamente distintos).

Demonstração: Pelo Corolário 1.79 podemos assumir que a curva $\mathcal{X}$ está contida na superfície Hermitiana $\mathcal{H}_3$ com equação $Z^{q+1}+Y^{q+1}=X^qT+XT^q$. Podemos assumir que $P:=(0:1:0:0)$, o plano osculante $\mathcal{X}$ em P tem equação $T=0$ e π tem equação $Y=0$. Sejam x,y,z as coordenadas afins de $\mathcal{X}$, as quais satisfazem

$$z^{q+1}+y^{q+1}=x^q+x. \tag{1.24}$$

Então podemos escrever $div_\infty(y)=m_P,\quad div_\infty(z)=qP$ e $div_\infty(x)=(q+1)P$. Consideramos D o divisor de interseção da curva $\mathcal{X}$ com o plano π. Assim

$$D=(q+1-m_P)P+m_1P_1+...+m_dP_d$$

com $P_i=(1:x_i:0:z_i)$ para algum $x_i,z_i\in\overline{\mathbb{F}}_{q^2}$ com $x_i^q+x_i=z_i^{q+1}$ para $i=1,...,d$. Desta maneira os pontos $Q_i:=(1:x_i:z_i)$ pertencem a $\mathcal{H}_2$ para $i=1,...,d$. A reta tangente

de $\mathcal{H}_2$ em Q_i tem equação $L_i(X,Z)=0$ onde $L_i(X,Z):=z_i^q(Z-z_i)-(X-x_i)$. Logo $div(L_i(x,z))=qP_i+\phi_{q^2}(P_i)-(q+1)P$. Considere

$$\xi(X,Z)=\prod_{i=1}^{d}L_i(X,Z)^{m_i}. \tag{1.25}$$

Como $m_1P+...+m_dP_d$ é um divisor $\mathbb{F}_{q^2}-$racional segue que o polinômio $\xi(X,Z)\in\mathbb{F}_{q^2}[X,Z]$. Além disso, como $div(\xi(X,Z))=(q+1)(m_1P+...+m_dP_d)-m_P(q+1)P=div(y^{q+1})$ obtemos que existe $\lambda\in\overline{\mathbb{F}}_{q^2}$ tal que $y^{q+1}=\lambda\xi(x,z)$. Entretanto como y e $\xi(x,z)$ são funções $\mathbb{F}_{q^2}-$racionais implica que $\lambda\in\mathbb{F}_{q^2}$. Desta forma

$$z^{q+1}+\lambda\xi(x,z)=x^q+x. \tag{1.26}$$

Resta mostrar que a curva dada pela equação (1.26) é $\mathbb{F}_{q^2}-$birracionalmente equivalente a curva $\mathcal{X}$. Para isto, consideramos o mapa racional $\gamma:\mathcal{X}\longrightarrow\mathbb{P}^2(\overline{\mathbb{F}}_{q^2})$ com $\gamma=(1:x:z)$ e seja $\mathcal{C}:=\gamma(\mathcal{X})$ dada pela equação $Z^{q+1}+\lambda\xi(X,Z)=X^q+X$. Vamos mostrar que γ é birracional. Já sabemos que o corpo de funções da curva $\mathcal{X}$ é $\overline{\mathbb{F}}_{q^2}(\mathcal{X})=\overline{\mathbb{F}}_{q^2}(x,y,z)$ e o corpo de funções da curva $\mathcal{C}$ é $\overline{\mathbb{F}}_{q^2}(\mathcal{C})=\overline{\mathbb{F}}_{q^2}(x,z)$. Como $[\overline{\mathbb{F}}_{q^2}(\mathcal{X}):\overline{\mathbb{F}}_{q^2}(\mathcal{C})]=div_\infty(y)$ segue que o morfismo γ é separável. Além disso, γ é totalmente ramificado em P. Seja $\overline{P}:=\gamma(P)$ e seja e_P o índice de ramificação de P. Como

$$e_P\cdot v_{\overline{P}}(x)=v_P(x)=-(q+1)\quad\text{ e }\quad e_P\cdot v_{\overline{P}}(z)=v_P(z)=-q$$

então $e_P=1$. Mas γ é totalmente ramificado logo $deg(\gamma)=e_P=1$. □

Aplicações dos trabalhos de Fanali-Giulietti-Platoni

Com o objetivo de reduzir a quantidade de casos que aparecem na tentativa de explicitar o polinômio $\xi(X,Z)$ no Teorema 1.85, analisa-se quando o plano π possui pontos $\mathbb{F}_{q^2}-$racionais ou não. Assumindo certas hipóteses temos as seguintes constatações.

Proposição 1.86 (Proposição 2, (FANALI; GIULIETTI; PLATONI, 2012))**.** *Assuma as hipóteses do Teorema 1.85 e suponha que π contenha pelo menos dois pontos $\mathbb{F}_{q^2}-$racionais de $\mathcal{X}$ diferentes do ponto P, digamos P_1 e P_2. Então a curva $\mathcal{X}$ é $\mathbb{F}_{q^2}-$birracionalmente equivalente a uma curva plana com equação*

$$Z^{q+1}=X^q+X+\lambda X(X-Z+1-B)\overline{\xi}(X,Z) \tag{1.27}$$

ou

$$Z^{q+1}=X^q+X+\lambda X(X-W)\overline{\xi}(X,Z) \tag{1.28}$$

onde $\lambda\in\mathbb{F}_{q^2}^*$, $B\in\mathbb{F}_{q^2}$ tal que $B^q+B=1$, W um elemento fixo em $\mathbb{F}_{q^2}$ com $W^q+W=0$ e $\overline{\xi}(X,Z)$ um polinômio definido sobre $\mathbb{F}_{q^2}$ de grau m_P-2, obtido como o produto de m_P-2 polinômios lineares $L_3(X,Z),...,L_{m_P}(X,Z)$ tais $L_i(X,Z)=0$ é a reta tangente da curva Hermitiana $Z^{q+1}=X^q+X$ no ponto Q_i com $i\in\{3,...,m_P\}$ (não necessariamente os Q_i's são distintos).

Demonstração: Podemos assumir que $P = (0 : 1 : 0 : 0)$, o plano osculante de $\mathcal{X}$ em P tem equação $T = 0$, π tem equação $Y = 0$, o ponto $P_1 = (1 : 0 : 0 : 0)$ e $P_2 = (1 : B : 0 : 1)$ ou $P_2 = (1 : W : 0 : 0)$ pelo Lema 1.83, onde $B, W \in \mathbb{F}_{q^2}$ tais que $B^q + B = 1$ e $W^q + W = 0$. Daí $L_1(X, Z) := X$ é a reta tangente de $\mathcal{H}_2$ em P e a reta tangente de $\mathcal{H}_2$ em P_2 tem equação $L_2(X, Z) := X - W$ ou $L_2(X, Z) = Z - X + 1 - B$. Na demonstração do Teorema 1.85 obtemos

$$\xi(X, Z) = X \cdot L_2(X, Z) \cdot \overline{\xi}(X, Z)$$

sendo $\overline{\xi}(X, Z) \in \mathbb{F}_{q^2}[X, Z]$ obtido pelos produtos de $m_P - 2$ das retas tangentes de $\mathcal{H}_2$. ▫

Proposição 1.87 (Proposição 3, (FANALI; GIULIETTI; PLATONI, 2012))**.** *Nas hipóteses do Teorema 1.85 e supondo que o plano π contém um ponto P_1 com $r := deg(P) > 1$. Então a curva $\mathcal{X}$ é $\mathbb{F}_{q^2}-$birracionalmente equivalente a uma curva plana com equação*

$$Z^{q+1} = X^q + X + \lambda\overline{\xi}(X, Z)\prod_{i=1}^{r}\left((\overline{Z}^{q^{2i}})^q \cdot (Z - \overline{Z}^{q^{2i}}) - (X - \overline{X}^{q^{2i}})\right), \tag{1.29}$$

onde $\overline{X}$ e $\overline{Z}$ são como no Lema 1.84, $\lambda \in \mathbb{F}_{q^2}^*$ e $\overline{\xi}(X, Z)$ é um polinômio definido sobre $\mathbb{F}_{q^2}$ de grau $m_P - r$, obtido como produtor de $m_P - r$ polinômios lineares $L_{r+1}(X, Z), ..., L_{m_P}(X, Z)$ tais que $L_i(X, Z) = 0$ é a equação da reta tangente da curva Hermitiana $Z^{q+1} = X^q + X$ no ponto Q_i, com $i \in \{r + 1, ..., m_P\}$ (não necessariamente os Q_i's são distintos).

Demonstração: Podemos assumir que $P = (0 : 1 : 0 : 0)$, o plano osculante de $\mathcal{X}$ em P tem equação $T = 0$, o plano π tem equação $Y = 0$ e o ponto $P_1 = (1 : \overline{X} : 0 : \overline{Z})$ pelo Lema 1.84. Seja $P_1^{(i)} := \phi_{q^2}^{(i)}(P_1) = (1 : \overline{X}^{q^{2i}} : 0 : \overline{Z}^{q^{2i}}) \in \pi \cap \mathcal{X}$ para $i = 2, ..., r$. Logo a reta tangente em $P_1^{(i)}$ é

$$(\overline{Z}^{q^{2i}})^q(Z - \overline{Z}^{q^{2i}}) - (X - \overline{X}^{q^{2i}}).$$

Aplicando o Teorema 1.85 segue o resultado. ▫

Partição do conjunto de pontos $\mathbb{F}_{q^2}-$racionais de $\mathcal{H}_2$

Como a equação da curva no Teorema 1.85 dependem das retas tangentes $L_i(X, Z)$ de $\mathcal{H}_2 : Z^{q+1} = X^q + X$ num ponto $Q_i := (1 : x_i : z_i)$, e estas são da forma

$$L_i(X, Z) = z_i^q(Z - z_i) - (X - x_i),$$

vamos particionar o conjunto dos pontos $\mathbb{F}_{q^2}-$racionais da curva Hermitiana $\mathcal{H}_2$ através do morfismo Frobenius ϕ_q associado ao corpo $\mathbb{F}_q$. Considere

$$\mathcal{A}_1 := \{Q \in \mathcal{H}_2(\mathbb{F}_{q^2}) : \phi_q(Q) = Q\}.$$

Quando $\mathcal{A}_1 \subsetneq \mathcal{H}_2(\mathbb{F}_{q^2})$, considere a família $\mathcal{S} := \{S \subseteq \mathcal{H}_2(\mathbb{F}_{q^2}) : \phi_q(Q) \notin S, Q \in S\}$. Logo existiria $Q \in \mathcal{H}_2(\mathbb{F}_{q^2})\backslash\mathcal{A}_1$. Considerando

$S := \{Q\}$, temos que $S \in \mathcal{S}$. Portanto a família $\mathcal{S}$ é não vazia. Considere a ordenação parcial em $\mathcal{S}$:

$$\text{se } S_1 \subset S_2 \text{ então } S_1 \leqslant S_2 \text{ para } S_1, S_2 \in \mathcal{S}.$$

Além disso, seja $S_1 \subsetneq S_2 \subsetneq S_3 \subsetneq \ldots$ com $S_i \in \mathcal{S}$, então $\overline{S} := \bigcup_i S_i$ é elemento maximal dessa cadeia. Suponha que $\overline{S} \notin \mathcal{S}$. Logo existe $Q \in \overline{S}$ tal que $\phi_q(Q) \in \overline{S}$, isto é, existem i_0, j_0 tais que

$$Q \in S_{i_0} \text{ e } \phi_q(Q) \in S_{j_0}.$$

Como $S_{i_0}, S_{j_0} \in \mathcal{S}$ temos $\phi_q(Q) \notin S_{i_0}$ e $Q = \phi_q(\phi_q Q) \notin S_{j_0}$. Logo $i_0 \neq j_0$. Se $j_0 < i_0$ então como $\phi_q(Q) \notin S_{i_0}$ segue que $\phi_q(Q) \notin S_{j_0}$ um absurdo. Logo $j_0 > i_0$. Como $Q \in S_{i_0}$ então $Q \in S_{j_0}$ outro absurdo. Portanto $\overline{S} \in \mathcal{S}$. Portanto, pelo Lema de Zorn, $\mathcal{S}$ admite um elemento maximal, vamos denotá-lo por $\mathcal{A}_2$. Assim o o conjunto dos pontos $\mathbb{F}_{q^2}-$racionais da curva Hermitiana $\mathcal{H}_2$ em três conjuntos disjuntos, a saber, $\mathcal{A}_1$, $\mathcal{A}_2$ e $\mathcal{A}_3 := \{\phi_q(Q) : Q \in \mathcal{A}_2\}$.

1.6.2 Classificação para $\mathbb{F}_{16}$ e $\mathbb{F}_{25}$

Em (FANALI; GIULIETTI, 2009), obtemos as classificações para curvas $\mathbb{F}_{q^2}-$maximais com dimensão Frobenius 3 através de modelos birracionais sobre $\mathbb{F}_{4^2}$ e sobre $\mathbb{F}_{5^2}$, as quais enunciamos a seguir.

Teorema 1.88. *Toda curva $\mathbb{F}_{16}-$maximal com dimensão Frobenius 3 é birracionalmente equivalente sobre $\mathbb{F}_{16}$ à curva plana dada pela equação afim*

$$Y^5 = X^2 + X$$

e tem gênero igual a 2.

Teorema 1.89. *Toda curva $\mathbb{F}_{25}-$maximal com dimensão Frobenius 3 é birracionalmente equivalente sobre $\mathbb{F}_{25}$ à curva plana dada por uma das seguintes equações*

(i) $Y^6 = X^5 + 2X^4 + 3X^3 + 4X^2 + 3XY^3$;

(ii) $Y^5 + Y = X^3$.

e tem gênero igual a 3 ou 4.

2 Quase-classicalidade de curvas maximais

Seja $\mathcal{X}$ uma curva $\mathbb{F}_{q^2}-$maximal de gênero $g > 0$, onde q é uma potência de um primo p. Considere a série Frobenius linear $\mathcal{D}_0 := |(q+1) \cdot P_0|$ de $\mathcal{X}$, com P_0 ponto $\mathbb{F}_{q^2}-$racional. Digamos que sua dimensão projetiva seja r. O sistema $\mathcal{D}_0$ não depende do ponto P_0, pois satisfaz a Equivalência Fundamental

$$(q+1) \cdot P_0 \sim qP + \phi(P),$$

onde $\phi : \mathcal{X} \to \mathcal{X}$ é o morfismo de Frobenius relativo a $\mathbb{F}_{q^2}$. Além disso, neste caso de maximalidade segue $r \geqslant 2$. A partir da teoria de série lineares podemos associar a um sistema $\mathcal{D} = g^r_d$ a sequência de ordens de Frobenius $\mathcal{V} : \quad 0 = \nu_0 < \nu_1 < \nu_2 < ... < \nu_{r-1}$ e a sequência de $\mathcal{D}-$ordens $\mathcal{E} : \quad 0 = \varepsilon_0 < \varepsilon_1 < ... < \varepsilon_r$. Sabemos da Proposição 1.34 que existe um número inteiro $I \leqslant r-1$ tal que

$$\nu_i = \varepsilon_i \text{ para } i < I, \quad \nu_i = \varepsilon_{i+1} \text{ para } i \geqslant I. \tag{2.1}$$

Em geral, um dado sistema linear de dimensão r é dito **Frobenius clássico** quando a sequência de ordens de Frobenius de tal sistema é $\mathcal{V} = \{0, 1, ..., r-1\}$. Observamos que as ordens de $\mathcal{D}_0$ satisfaz $\nu_{r-1} = \varepsilon_r = q$ (ver Teorema 1.4 em (FUHRMANN; GARCIA; TORRES, 1997)) e neste caso $r = q+1$ se, e somente se, $g = 0$. Portanto $\mathcal{D}_0$ é sempre Frobenius não-clássica. Entretanto pode ocorrer uma condição mais fraca sobre a noção de Frobenius classicalidade de $\mathcal{D}_0$.

Definição 2.1. *Seja $\mathcal{X}$ uma curva definida sobre $\mathbb{F}_{q^2}$ e $\mathcal{D}_0$ sua série Frobenius de dimensão r. Dizemos que $\mathcal{X}$ é*

(a) ***Frobenius quase-clássica*** *se a sequência de $\mathcal{D}_0-$ordens Frobenius é $\nu_i = i$ para $i \leqslant r-2$ e $\nu_{r-1} = q$.*

(b) ***quase-clássica*** *se a sequência de $\mathcal{D}_0-$ordens for $\varepsilon_i = i$ para $i \leqslant r-1$ e $\varepsilon_r = q$.*

Existe na literatura muitos resultados sobre o comportamento das ordens e da dimensão de $\mathcal{D}_0$. Ao fixarmos q na Cota de Castelnuovo (Teorema 1.61) podemos verificar um comportamento de monotocidade de c_0 em função de r.

Observação 2.2. *Se $r \geqslant s$ temos $c_0(r, q+1) \leqslant c_0(s, q+1)$.*

Quando a dimensão Frobenius é igual a 2 então temos um único modelo de curva maximal, a menos de isomorfismo. Além disso, podemos explicitar o comportamento das ordens genéricas e das ordens de Frobenius e também do gênero.

Teorema 2.3 ((FUHRMANN; TORRES, 1996)). *Seja $\mathcal{X}$ uma curva $\mathbb{F}_{q^2}-$maximal de gênero g com dimensão Frobenius 2. Então as seguintes condições são equivalentes:*

(a) $r = 2$;

(b) $2g = q(q-1)$;

(c) a curva $\mathcal{X}$ deve ser isomorfa à curva Hermitiana $\mathcal{H}_q$: $y^{q+1} = x^q + x$.

(d) $g > \lfloor \frac{(q-1)^2}{4} \rfloor$.

(e) $\nu_1 > 1$.

Por meio do resultado anterior, o estudo de quase-classicalidade para a dimensão Frobenius 2 se torna trivial.

Corolário 2.4. *Toda curva $\mathbb{F}_{q^2}-$maximal de gênero g com dimensão Frobenius 2 é quase-clássica e Frobenius quase-clássica.*

O estudo de quase-classicalidade para corpos do tipo $\mathbb{F}_{p^2}$, com p primo, é simples e independe de qual for o valor da dimensão de Frobenius analisada. Isto decorre simplesmente por critérios aritméticos do comportamento das ordens. As curvas $\mathbb{F}_{p^2}-$maximais serão exemplos de quase-classicalidade e Frobenius quase-classicalidade.

Teorema 2.5. *Seja $\mathcal{X}$ uma curva $\mathbb{F}_{p^2}-$maximal com de gênero $g > 0$ e dimensão de Frobenius $r > 2$. Então $\mathcal{X}$ é quase-clássica e Frobenius quase-clássica.*

Demonstração: Temos pela maximalidade $\varepsilon_r = p$. Como $r > 2$ então $p > 2$. Então $\varepsilon_{r-1} = p - k$ com $k \in \{1, 2, ..., p-1\}$. Pelo Critério $p-$ádico segue que $\{0, 1, ..., p-k-1, p-k\} \subset \mathcal{E}$ logo $k = p - r + 1$. Assim $\varepsilon_i = i$ para $i \leqslant r-1$, isto é, $\mathcal{X}$ é quase-clássica. Segue do teorema 2.3 que $\nu_1 = 1$. Como $\nu_{r-1} = \varepsilon_r = p$ e (2.1) segue que $I < r$. Assim $\nu_i = i$ para $i < I$ e $\nu_i = i + 1$ para $I \leqslant i < r$. Suponha $I \leqslant r-2$. Como $I < I + 1 \leqslant r - 1$ então $I + 1 = \nu_I < \nu_{r-1} = p$. Se $I + 1 = pk$ com $k \in \mathbb{N}$, como $pk - 1 = I = \varepsilon_I < \varepsilon_r = p$ obtemos que $k = 1$, isto é, $I = p - 1$. Como $p + 1 = \nu_p = \nu_I < \nu_{r-1} = p$ obtemos um absurdo. Logo $I + 1 \not\equiv 0 \ mod\ p$. Daí como $I + 1 = \nu_I$, usando o Critério $p-$ádico teremos que $I \in \mathcal{V}$. Contradizendo o fato que $\mathcal{V} = \{0, 1, ..., I-1, I+1, ...,\}$. Portanto $I = r - 1$. Assim $\nu_i = i$ para $i = 1, .., r-2$ e $\nu_{r-1} = p$, isto é, $\mathcal{X}$ é Frobenius quase-clássica. □

Em busca de encontrar exemplos de curvas maximais que não satisfazem a propriedade de quase-classicalidade, vamos analisar propriedades que podem ser obtidas em casos particulares de dimensão Frobenius 3 e dimensão Frobenius 4. Em particular queremos dar uma classificação para curvas $\mathbb{F}_{q^2}-$maximais com dimensão Frobenius 3 através do invariante gênero, tendo em vista o problema de determinação do Espectro dos Gêneros $\mathbf{M}(q^2)$, onde $q \leqslant 29$ e q potência de um número primo. Tais propriedades serão usadas no capítulo seguinte.

2.1 Dimensão Frobenius 3

Através do Teorema 1.61 obtemos uma cota superior para o gênero de curvas $\mathbb{F}_{q^2}-$maximais, a saber,

$$g \leqslant c_0(3) := \frac{(q-1)^2}{4} \tag{2.2}$$

onde g denota o gênero. Esta cota é ótima, pois é possível explicitar um único modelo para cada q, a menos de isomorfismo, de uma curva $\mathbb{F}_{q^2}-$maximal com tal gênero. O modelo para característica ímpar foi encontrado por Fuhrmann, Garcia e Torres, já o modelo para característica 2 foi encontrado por Abdón e Torres. Segue da Proposição 1.66 que

$$m_2(P) = q \quad \text{e } m_3(P) = q+1 \quad \text{para todo } P \text{ ponto } \mathbb{F}_{q^2} - \text{racional} \tag{2.3}$$

de uma curva maximal sobre $\mathbb{F}_{q^2}$ com dimensão Frobenius 3. Usaremos este fato nesta seção.

Teorema 2.6 ((FUHRMANN; GARCIA; TORRES, 1997), (ABDÓN; TORRES, 1999))**.** *Seja $\mathcal{X}$ é uma curva $\mathbb{F}_{q^2}-$maximal de gênero g. Então $g = \lfloor c_0(3) \rfloor$ se, e somente se, a curva $\mathcal{X}$ é unicamente determinada pelos tipos:*

(i) $Y^{(q+1)/2} = X^q + X$, *se q é ímpar;*

(ii) $Y^{q+1} = X^{q/2} + ... + X$, *se q é par.*

Quando a dimensão Frobenius é 3, a propriedade de Frobenius quase-classicalidade para curvas $\mathbb{F}_{q^2}-$maximais é sempre satisfeita. Entretanto curvas $\mathbb{F}_{q^2}-$maximal com tal dimensão Frobenius não necessariamente serão quase-clássicas. A curva GK (veja exemplo 1.69) é um exemplo de curva que não satisfaz a propriedade de quase-classicalidade em certos corpos.

Exemplo 2.7. *A curva Giulietti-Korchmáros é uma curva $\mathbb{F}_{q^6}-$maximal de gênero igual a $1 + (q^3+1)(q^2-2)/2$ com dimensão Frobenius 3. Em (FANALI; GIULIETTI, 2010), é verificado que $\varepsilon_2 = q$. Este é um exemplo de uma curva não quase-clássica para $q \neq 2$.*

Queremos responder quando uma curva maximal tem a propriedade de quase-classicalidade ou não através de intervalos de possibilidade para o gênero de tal curva. Quando a maximalidade ocorre num corpo $\mathbb{F}_{p^2}$, com p primo, o Teorema 2.5 já responde nossos questionamentos de uma não dependência para o gênero, além de (2.2).

Teorema 2.8. *Seja $\mathcal{X}$ uma curva $\mathbb{F}_{q^2}-$maximal com dimensão Frobenius 3. Então $\mathcal{X}$ é Frobenius quase-clássica. Se $\mathcal{X}$ é quase-clássica então $c_1(q) \leqslant g \leqslant c_0(3)$, onde*

$$c_1(q) := \frac{q^2 - 2q + 3}{6}. \tag{2.4}$$

Além disso, se $q \not\equiv 0 \ mod\ 3$, então $\mathcal{X}$ quase-clássica se, e somente se, $c_1(q) \leqslant g \leqslant c_0(3)$.

Demonstração: Pela Cota de Castelnuovo, temos $g \leqslant c_0(3)$. Segue da maximalidade que $0 = \nu_0 < \nu_1 = 1 < \nu_2 = q$. Suponha que $\mathcal{X}$ é quase-clássica. Seja R o divisor de ramificação de $\mathcal{D}_0$. Sabemos que R satisfaz $deg(R) \geqslant \#\mathcal{X}(\mathbb{F}_{q^2})$ então $3(2g-2) \geqslant (q+1)(q-3)$, isto é, $g \geqslant c_1(q)$. Para a recíproca, suponha que $g > c_1(q)$. Se $\varepsilon_2 \geqslant 4$ então o divisor de Frobenius de $\mathcal{D}_0$ implica que

$$(1+q)(2g-2) + (q^2+3)(q+1) \geqslant 5\left((2g-2)q + (1+q)^2\right) \tag{2.5}$$

uma contradição com $g > c_1(q)$. Portanto $\varepsilon_2 = \{2, 3\}$. Como a característica de $\mathbb{F}_{q^2}$ é diferente de 3, pelo Critério $p-$ádico segue que $\varepsilon_2 = 2$. □

O Exemplo 2.7 satisfaz a condição $g \leqslant c_1(q)$, para $q \neq 2$, isto reafirma a não quase-classicalidade. Observamos que em alguns casos o conhecimento do gênero da curva pode nos fornecer a não quase-classicalidade sem o cálculo explícito das ordens genéricas de sua série linear Frobenius.

Exemplo 2.9. *De (TAFAZOLIAN; TEHERÁN-HERRERA; TORRES, 2016), sabemos que a curva $\mathcal{Y}_{3,1}$, dada por*

$$\mathcal{Y}_{3,1}: \quad y^4 = x^3 + x, \quad y^9 - y = z^7, \tag{2.6}$$

é $\mathbb{F}_{27^2}-$maximal e não é coberta pela Hermitiana $\mathcal{H}_3$ sobre $\mathbb{F}_{27^2}$ e tem gênero 99. Este é um caso particular do Exemplo 1.71. Seja r sua dimensão de Frobenius. Como existe um ponto $P \in \mathcal{Y}_{3,1}(\mathbb{F}_{27^2})$ tal que o semigrupo de Weierstrass em P é da forma $\langle 21, 27, 28\rangle$, segue que $m_3(P) = 27$ e pela maximalidade, segue que sua dimensão Frobenius é igual a 3. A não quase-classicalidade segue do Teorema 2.8.

Novamente um exemplo de curva não quase-clássica com a propriedade de não ser Galois-coberta pela curva Hermitiana. Poderíamos nos perguntar se esta propriedade de cobertura é necessária para obter curvas não quase-clássica. Isso não é necessariamente verdadeiro sobre corpos $\mathbb{F}_{p^2}$, como observado. Um exemplo de existência de uma curva com tais propriedades é a curva Fricke-Macbeath de gênero 7, a qual é $\mathbb{F}_{71^2}-$maximal e não é Galois-coberta pela curva Hermitiana $\mathcal{H}_{72}$ (BARTOLI; MONTANUCCI; TORRES, 2010). Esta curva tem dimensão Frobenius 65.

Em relação ao gênero, também há um bom comportamento em relação aos valores $c_0(3)$ e $c_0(4)$.

Corolário 2.10. *Seja $q \not\equiv 0$ mod 3. Se $\mathcal{X}$ é uma curva $\mathbb{F}_{q^2}-$maximal de gênero g tal que*

$$c_0(4) < g \leqslant c_0(3)$$

então $\mathcal{X}$ é quase-clássica com dimensão Frobenius igual a 3 e g não pertence ao intervalo aberto $]c_0(4), c_1(q)[$.

Demonstração: Seja r a dimensão Frobenius de $\mathcal{X}$. De fato se $r \geqslant 4$ então $g \leqslant c_0(4)$ um absurdo. Logo $r = 3$. Supondo $c_0(4) < g < c_1(q)$ segue do Teorema 2.8 a não quase-classicalidade. Usando (2.5) e $g > c_0(4)$ obtemos uma contradição. Portanto, $g \geqslant c_1(q)$ e usando novamente o Teorema 2.8 obtemos $\mathcal{X}$ quase-clássica. ▫

Observamos que em geral curvas $\mathbb{F}_{q^2}-$maximais com gênero igual a $c_0(4)$ não necessariamente implica que sua dimensão Frobenius é igual a 3. Toda curva $\mathbb{F}_{q^2}-$maximal de gênero $c_0(4)$ com a hipótese $q \equiv 1, 2 \ mod \ 3$ tem dimensão Frobenius igual a 4. Este resultado pode ser visto com mais detalhes em Lema 10.50 de (HIRSCHFELD; KORCHMÁROS; TORRES, 2008). Com o objetivo de eliminar alguns valores de gênero g para dimensão Frobenius 3 enunciamos o resultado a seguir.

Proposição 2.11. *Seja $q \not\equiv 0 \ mod \ 3$. Seja $\mathcal{X}$ uma curva $\mathbb{F}_{q^2}-$maximal de gênero g tal que*

$$3(q+1)(q^2-5q-2) < 3(2g-2)(4q-1) < (q^2-2q-3)(4q-1). \tag{2.7}$$

Então a dimensão Frobenius é maior ou igual a 4.

Demonstração: Da hipótese obtemos que $g < c_1(q)$. Logo $r > 2$. Se $r = 3$, segue da Proposição 1.75 que $g \geqslant c_1(q)$. Absurdo. Logo $r \geqslant 4$. ▫.

2.1.1 Não quase-classicalidade em dimensão Frobenius 3

Nosso objetivo nesta subseção é classificar através do gênero quando obtemos a não quase-classicalidade para curvas $\mathbb{F}_{q^2}-$maximais com $q \leqslant 29$ e $q = p^h$, onde p é um primo e $h \geqslant 1$. Como esta propriedade não ocorre sobre corpos $\mathbb{F}_{p^2}$, com p primo, vamos analisar o comportamento das ordens genéricas sobre $\mathbb{F}_{p^4}$ e $\mathbb{F}_{p^6}$.

Proposição 2.12. *Seja $\mathcal{X}$ uma curva $\mathbb{F}_{q^2}-$maximal, dimensão Frobenius igual a 3 e não quase-clássica. Se $c_1(q) \leqslant g$ então $q = 3^h$ com $h \geqslant 2$.*

Demonstração: Suponha que $c_1(q) \leqslant g$. Como a dimensão Frobenius é igual a 3 então $c_1(q) \leqslant g \leqslant c_0(3)$. Se $q \not\equiv 0 \ mod \ 3$ então $\mathcal{X}$ é quase-clássica pelo Teorema 2.8, uma contradição. Logo $q \equiv 0 \ mod \ 3$. Pela hipótese de quase-classicalidade segue que $q \neq 3$. ▫

Para alcançar a classificação desejada, refinamos as possibilidades para ε_2, o qual inicialmente satisfaz $3 \leqslant \varepsilon_2 < q$ utilizando propriedades do divisor de ramificação de $\mathcal{D}_0$, o divisor de Frobenius e propriedades aritméticas. Desta última, citamos o "Lema de Lucas".

Lema 2.13 (Lema A.6 em (HIRSCHFELD; KORCHMÁROS; TORRES, 2008))**.**

$$\binom{np^h}{p^h} \equiv n \ mod \ p.$$

O conhecimento de um semigrupo de Weierstrass em pontos $\mathbb{F}_{q^2}-$maximais, também é outro método para calcular ε_2.

Proposição 2.14. *Seja $\mathcal{X}$ uma curva $\mathbb{F}_{q^2}-$maximal com dimensão de Frobenius igual a 3. Se $\mathcal{X}$ é não quase-clássica então existe $Q \in \mathcal{X}(\mathbb{F}_{q^2})$ tal que $m_1(Q) \leqslant q-2$.*

Demonstração: Pelo Lema 3.7 em (COSSIDENTE; KORCHMÁROS; TORRES, 1999) existe um ponto $P \in \mathcal{X}(\mathbb{F}_{q^2})$ tal que $m_1(P) = q+1-\varepsilon_2$. Como $\mathcal{X}$ é não quase-clássico então $\varepsilon_2 \geqslant 3$. Portanto $m_1(P) \leqslant q-2$. □

Observamos que a recíproca não é válida no resultado acima, isto é, se existe um ponto $\mathbb{F}_{q^2}-$maximal com primeira não-gap igual a $q-2$ não necessariamente teremos não quase-classicalidade. Basta considerar a curva GK sobre $\mathbb{F}_{64}$, a qual tem dimensão Frobenius 3, existe um ponto com semigrupo de Weierstrass gerado por $\langle 6, 8, 9\rangle$ mas é quase-clássica.

$\mathbb{F}_{p^h}-$maximalidade e não quase-classicalidade, com $h = 4, 6$

Quando nos restringimos a estudar curvas $\mathbb{F}_{p^4}-$maximais ou $\mathbb{F}_{p^6}-$maximais com dimensão Frobenius 3 não quase-clássicas podemos explicitar o valor de ε_2, onde p é um primo.

Proposição 2.15. *Seja $\mathcal{X}$ uma curva $\mathbb{F}_{p^4}-$maximal de gênero $g > 0$ com dimensão Frobenius 3 que não é quase-clássica. Então $\varepsilon_2 = p$ e $p \geqslant 3$.*

Demonstração: Por hipótese $3 \leqslant \varepsilon_2 < p^2$. Se $p = 2$ então segue que $\varepsilon_2 = 3$. Pela Proposição 2.10, $g = 1$. Assim $deg(S) = 95$, $\#\mathcal{X}(\mathbb{F}_{16}) = 25$ e $v_P(S) \geqslant 4$ para todo P racional de $\mathcal{X}$. Uma contradição, pois $deg(S) \geqslant 4 \cdot 25$. Suponha $p \geqslant 3$. Se $\varepsilon_2 < p$ então teríamos $\varepsilon_2 - 1, \varepsilon_2 - 2, ..., 1 \in \mathcal{E}$, isto é, $\varepsilon_2 = 2$, uma contradição. Portanto $\varepsilon_2 \geqslant p$. Seja $\varepsilon_2 = ps + r$ com $s, r \in \mathbb{N}$ tal que $0 \leqslant r < p$. Se $r > 0$ então $\varepsilon_2 - 1 \in \mathcal{E}$, pois $\binom{\varepsilon_2}{\varepsilon_2 - 1} = \varepsilon_2 = ps + r \not\equiv 0 \ mod\ p$. Portanto $\varepsilon_2 = ps$. Como $\varepsilon_2 < \varepsilon_3 = p^2$ então $s < p$. Se $s \geqslant 2$, usando o Lema 2.13 segue que $\binom{ps}{p} \not\equiv 0 \ mod\ p$ então $p \in \mathcal{E} = \{0, 1, ps, p^2\}$ uma contradição. Logo $\varepsilon_2 = p$. □

Proposição 2.16. *Seja $\mathcal{X}$ uma curva $\mathbb{F}_{p^6}-$maximal de gênero $g > 0$ com dimensão Frobenius 3 que não é quase-clássica. Então $\varepsilon_2 = p$ ou $\varepsilon_2 = p^2$.*

Demonstração: Por hipótese, $\varepsilon_2 \geqslant p$. Seja $\varepsilon_2 = ps + r$ com $s \in \mathbb{N}$ tal que $0 \leqslant r < p$. Se $r > 0$ então $\varepsilon_2 - 1 \in \mathcal{E}$, pois $\binom{\varepsilon_2}{\varepsilon_2 - 1} = \varepsilon_2 = ps + r \not\equiv 0 \ mod\ p$. Portanto $\varepsilon_2 = ps$. Como $\varepsilon_2 < \varepsilon_3 = p^3$ então $s < p^2$. Suponha que $1 < s < p$ então $\binom{ps}{p} \not\equiv 0 \ mod\ p$, isto é, $p \in \mathcal{E} = \{0, 1, ps, p^3\}$. Uma contradição. Portanto $s = 1$ ou $s \geqslant p$. Logo $\varepsilon_2 = p$ ou

$\varepsilon_2 \geqslant p^2$. Suponha que $\varepsilon_2 \geqslant p^2$. Seja $\varepsilon_2 = p^2h + t$ com $h \in \mathbb{N}$ e $0 \leqslant t < p^2$. Se $p \leqslant h$, como $\varepsilon_2 < \varepsilon_3 = p^3$ daí $t < p^2(p-h) \leqslant 0$. Absurdo. Logo $p > h$.

- Suponha que $t > 0$. Se $t < p$ assim $\binom{\varepsilon_2}{\varepsilon_2 - 1} = p^2h + t \not\equiv 0 \ mod\ p$ logo $\varepsilon_2 - 1 \in \mathcal{E} = \{0, 1, \varepsilon_2, p^3\}$. Um absurdo. Portanto $t \geqslant p$. Escrevendo $t = pa + b$ com $a \in \mathbb{N}$ e $0 \leqslant b < p$. Daí $\varepsilon_2 = p^2h + t = p^2h + pa + b$. Se $b > 0$ teremos $\binom{\varepsilon_2}{\varepsilon_2 - 1} \equiv b \ mod\ p$, isto é, $\varepsilon_2 - 1 \in \mathcal{E} = \{0, 1, \varepsilon_2, p^3\}$ uma contradição. Logo $\varepsilon_2 = p^2h + pa$ com $1 \leqslant a < p(p-h)$. Como $\binom{p^2h + pa}{pa} \not\equiv 0 \ mod\ p$ teríamos $pa \in \mathcal{E}$, isto é, $t = a = 0$, um absurdo.

Logo $t = 0$ então teríamos $\binom{p^2h}{p^2} \not\equiv 0 \ mod\ p$ o que implicaria $p^2 \in \mathcal{E} = \{0, 1, p^2h, p^3\}$. Portanto $\varepsilon_2 = p^2$. □

Com a classificação a seguir podemos tentar construir curvas computacionalmente utilizando os resultados de Fanali-Giulietti-Platoni, em busca de construir mais exemplos de curvas maximais não quase-clássicas, para q pequeno, ou verificar a não existência de tais curvas.

Teorema 2.17. *Seja $\mathcal{X}$ uma curva $\mathbb{F}_{q^2}-$maximais com dimensão Frobenius 3 com $q \leqslant 29$, q potência de um primo. Considere as seguintes situações*

(i) *se $q = g = 9$;*

(ii) *se $q = 16$ e $g = 24$;*

(iii) *se $q = 25$ e $g \in \{49, 50\}$;*

(iv) *se $q = 27$ e $g \in [85, 109]$.*

Se não estamos em nenhum dos casos anteriores, então $\mathcal{X}$ é quase-clássica.

Demonstração: Como $\mathcal{X}$ é sempre Frobenius quase-clássica temos que o divisor de Frobenius implica que

$$(1+q)(2g-2) + (q^2+3)(q+1) \geqslant (\varepsilon_2 + 1)\left((2g-2)q + (q+1)^2\right) \tag{2.8}$$

e o divisor de ramificação R implica que

$$g \geqslant \frac{(1+q)(q-3)}{2(1+\varepsilon_2)} + 1 \tag{2.9}$$

Suponha que $q = p^2$ então pela Proposição 2.15 teremos $\varepsilon_2 = p$ assim em (2.8) obtemos

$$g \leqslant \frac{(p^2+1)(p^4 - p^3 - p^2 - p + 2)}{2(p^3-1)} + 1 \tag{2.10}$$

Aplicando (2.9) e (2.10) para $p = 3$ obtemos $g = 9$ e $p = 5$ temos $g \in \{49, 50\}$. Suponha que $q = p^3$ então segue da Proposição 2.15 que $\varepsilon_2 = p$ ou $\varepsilon_2 = p^2$. Se $\varepsilon_2 = p$ então

$$\frac{p^6 - 2p^3 + 3}{2(1+p)} + 1 \leqslant g \leqslant \frac{(p^3+1)(p^6 - p^4 - p^3 - p + 2)}{2(p^4 - 1)} + 1. \tag{2.11}$$

Observamos que para $q = 16$ temos

$$\mathbf{M}(16^2) \subseteq [0, 34] \cup [36, 40] \cup \{56\} \cup \{120\}.$$

Além disso, Proposição 4.2 de (ARAKELIAN; TAFAZOLIAN; TORRES, 2018), sabemos que $36, 37 \notin \mathbf{M}(16^2)$. Então $\varepsilon_2 \in \{2, 4, 8\}$. Assim $14 \leqslant g \leqslant 56$. Suponha $\varepsilon_2 = 8$ então $deg(S) \geqslant 9 \cdot \#\mathcal{X}(\mathbb{F}_{16^2})$, isto é, $g \leqslant 8$, um absurdo. Portanto $\varepsilon_2 \in \{2, 4\}$. Segue de (2.7) que $g \notin [25, 37]$. Para $g \in \{38, 39, 40, 56\}$ aplicamos o Teorema 2.8 e obtemos quase-classicalidade. (Observamos que os casos $g = 38, 39$ ainda não se sabe se tais curvas existem, mas se existirem serão quase-clássicas com dimensão Frobenius 3). Suponha não quase-classicalidade. Então $\varepsilon_2 = 4$. Usando o divisor de Ramificação temos $g \geqslant \dfrac{q^2 - 2q + 7}{10}$. Logo $g = 24$. ▫

Observação 2.18. *Seja $\mathcal{X}$ uma curva $\mathbb{F}_{81}-$maximal de gênero 9. Então temos duas possibilidades para sua dimensão Frobenius r, a saber, $r = 3$ ou 4. Em (ABDÓN; TORRES, 2005) é observado que:*

(i) se $r = 3$ então $\mathcal{X}$ é não quase-clássico ($\varepsilon_2 = 3$);

(ii) se $r = 4$ então $\mathcal{X}$ é quase-clássico.

No caso (ii) sabemos que existe um exemplo de curva definida pela equação

$$X^3 + X = aZ^{10}$$

com $a \in \mathbb{F}_{81}$ tal que $a^8 = -1$. No caso (i) ainda não é conhecido um exemplo de curva para esta situação. Uma alternativa para tentar construir uma curva satisfazendo (i) é utilizar os resultados em (FANALI; GIULIETTI; PLATONI, 2012) (a ser exposta no Capítulo 3). Seja $\mathcal{X}$ tal curva. Usando o Lema 2.14, existe um ponto P em $\mathcal{X}$ que é $\mathbb{F}_{81}-$racional tal que a primeira não-gap não nula em P é igual a 7. Seja π um plano tangente não osculante a $\mathcal{X}$ definido sobre $\mathbb{F}_{81}$. Então pelos resultados teríamos que a curva $\mathcal{X}$ é $\mathbb{F}_{81}-$birracionalmente equivalente a curva plana com equação $Z^{10} = X^9 + X + \lambda\xi(X, Z)$ onde $\lambda \in \mathbb{F}_{81}^*$ e $\xi(X, Z)$ é um polinômio definido sobre $\mathbb{F}_{81}$ de grau 7, obtido como o produto de polinômios lineares $L_1(X, Z)^{m_1}, ..., L_d(X, Z)^{m_d}$ onde as retas com equação $L_i(X, Z) = 0$ são as retas tangentes da curva Hermitiana $Z^{10} = X^9 + X$ em certos $d(> 0)$ pontos (não necessariamente distintos) e satisfazendo $m_1 + ... + m_d = 7$.

2.2 Dimensão Frobenius 4

Seja $\mathcal{X}$ uma curva $\mathbb{F}_{q^2}-$maximal e seja $\mathcal{D}$ sua série de Frobenius de dimensão 4. As ordens de Frobenius neste caso são $\mathcal{V}: \quad \nu_0 = 0 < \nu_1 = 1 < \nu_2 < \nu_3 = q$ e as $\mathcal{D}-$ordens são $0 = \varepsilon_0 < 1 = \varepsilon_1 < \varepsilon_2 < \varepsilon_3 < \varepsilon_4 = q$.

2.2.1 Condições necessárias para não quase-classicalidade

Sabemos que existe $1 < I \leqslant 3$ tal que $\mathcal{V} = \mathcal{E}\backslash\{\varepsilon_I\}$, isto é, podemos ter um dos dois casos:

(i) $\nu_2 = \varepsilon_2$.

(ii) $\nu_2 = \varepsilon_3$.

Observação 2.19. *Se temos Frobenius quase-classicalidade então estamos no caso (i). Se estamos na situação (ii) então temos não Frobenius quase-classicalidade.*

Observação 2.20. *Seja $\mathcal{X}$ uma curva $\mathbb{F}_{p^2}-$maximal com dimensão Frobenius 4. Supondo o caso (ii), obtemos $\varepsilon_3 = pm$ com $1 \leqslant m < p$. Primeiramente observamos que $p > 2$. Pelo Critério $p-$ádico e Lema de Lucas segue que $p \in \mathcal{E}$. Temos as possibilidades:*

(iia) $\varepsilon_2 = p, \varepsilon_3 = pm$ com $1 < m < p$, isto é, não quase-classsicalidade. Como $p \neq 2$, como $\binom{mp}{(m-1)p} \not\equiv 0 \ mod\ p$ aplicando o Critério $p-$ádico vemos que então $m = 2$, isto é, $\varepsilon_3 = 2p$.

(iib) $p = 3$ e quase-classicalidade.

O resultado a seguir caracteriza quando maximalidade e quase-classicalidade implicam Frobenius quase-classicalidade para dimensão Frobenius igual a 4.

Lema 2.21. *Seja $q \not\equiv 0 \ mod\ 3$. Seja $\mathcal{X}$ uma curva $\mathbb{F}_{q^2}-$maximal quase-clássica de gênero g e dimensão Frobenius 4. Então $\mathcal{X}$ é Frobenius quase-clássica.*

Demonstração: No caso (ii) teríamos $\nu_2 = 3$ e como $q \not\equiv 0 \ mod\ 3$ então teríamos $2 \in \mathcal{V}$ o que seria um absurdo. Logo estamos na situação (i), isto é, $\nu_2 = \varepsilon_2 = 2$. A maximalidade implica $\nu_3 = q$. □

Seja S o divisor de Frobenius de $\mathcal{X}$. Para cada $P \in \mathcal{X}(\mathbb{F}_{q^2})$ temos

$$v_P(S) \geqslant \varepsilon_2 + \varepsilon_3 - \nu_2 + 1.$$

No caso (i) teremos $v_P(S) \geqslant \varepsilon_3 + 1$ e no caso (ii) teremos $v_P(S) \geqslant \varepsilon_2 + 1$ para cada $P \in \mathcal{X}(\mathbb{F}_{q^2})$.

Lema 2.22. *Seja $\mathcal{X}$ uma curva $\mathbb{F}_{q^2}-$maximal com dimensão Frobenius 4 e Frobenius quase-clássica de gênero g. Se*

$$g < \frac{q^2-3q+8}{12}.$$

então $\mathcal{X}$ é não quase-clássica.

Demonstração: Por hipótese estamos no caso (i). Neste caso $\varepsilon_2 = 2$. Suponha que temos quase-classicalidade, isto é, $\varepsilon_i = i$ para $0 \leqslant i \leqslant 3$ e $\varepsilon_4 = q$. Então usando (1.3), grau o divisor de ramificação de $\mathcal{D}_0 = g^4_{q+1}$ será $deg(R) = (6+q)(2g-2) + 5(q+1)$ e usando a maximalidade obtemos $6(2g-2) \geqslant (1+q)(q-4)$. □

Proposição 2.23. *Seja $q \not\equiv 0 \bmod 2$. Seja $\mathcal{X}$ uma curva $\mathbb{F}_{q^2}-$maximal Frobenius quase-clássica de gênero $g > 1$ com dimensão Frobenius 4. Se*

$$(5q-3)(2g-2) > (1+q)(q^2-6q-2)$$

então $\mathcal{X}$ é quase-clássica.

Demonstração: Estamos na situação (ii), logo para todo $P \in \mathcal{X}(\mathbb{F}_{q^2})$ temos $v_P(S) \geqslant \varepsilon_3 + 1$. Se $\mathcal{X}$ for não quase-clássica então $\varepsilon_3 \geqslant 4$. Como q é ímpar então $\varepsilon_3 \geqslant 5$. Logo $v_P(S) \geqslant 6$ para todo P racional de $\mathcal{X}$. Logo

$$(3+q)(2g-2) + (q^2+4)(q+1) \geqslant 6q(2g-2) + 6(1+q)^2.$$

Isto implica que $(5q-3)(2g-2) \leqslant (1+q)(q^2-6q-2)$. Absurdo. Logo $\mathcal{X}$ é quase-clássica. □

Analisando o semigrupo de Weierstrass, segue da Proposição 1.66 que

$$m_3(P) = q \quad \text{e} \quad m_4(P) = q+1 \quad \text{para todo } P \text{ ponto } \mathbb{F}_{q^2} - \text{racional} \tag{2.12}$$

de uma curva maximal sobre $\mathbb{F}_{q^2}$ com dimensão Frobenius 4.

Exemplo 2.24. *A curva dada pela equação*

$$Y^{51} = X(X+1)^{15}$$

tem gênero 24 é $\mathbb{F}_{16^2}-$maximal e existe P ponto $\mathbb{F}_{16^2}-$racional com semigrupo de Weierstrass igual $\langle 10, 13, 16, 17\rangle$. Assim de (2.12) segue que $m_3(P) = 16$ logo sua dimensão Frobenius é 4. Neste caso, $j_0(P) = 0$, $j_1(P) = 1$, $j_2(P) = 4$, $j_3(P) = 7$ e $j_4(P) = 17$. Segue do Corolário 1.41 que

$$\nu_2 \leqslant j_3(P) - 1 = 6.$$

Como a característica é 2 temos $\nu_2 = 2$. Sabemos que $\varepsilon_2 = 2$ e como $\varepsilon_3 \leqslant j_3(P) = 7$ então $\varepsilon_3 \in \{3, 4\}$.

Um comportamento como observado na Proposição 2.10, entre o números de Castelunovo, não se mantem de maneira análoga: se $c_0(5) < g \leqslant c_0(4)$ não necessariamente teremos dimensão Frobenius 4. Observamos que $c_0(4) = \dfrac{(q-1)(q-2)}{6}$ e $c_0(5) := \dfrac{(q-2)^2}{8}$.

Teorema 2.25. *Seja $\mathcal{X}$ uma curva maximal sobre $\mathbb{F}_{q^2}$ de gênero g tal que $c_0(5) < g \leqslant c_0(4)$. Se $q \not\equiv 0 \ mod\ 3$ e*

$$(4q-1)(2g-2) > (q+1)(q^2-5q-2)$$

então $\mathcal{X}$ tem dimensão Frobenius igual a 4. Em particular, quando $q \equiv 0 \ mod\ 3$ então $(3q-1)(2g-2) \leqslant (q+1)(q^2-4q-1)$.

Demonstração: Seja r a dimensão Frobenius de $\mathcal{X}$. Por Teorema 2.3 temos $r \neq 2$. Se $r \geqslant 5$ então pela Cota de Castelnuovo temos que $g \leqslant c_0(5)$. Absurdo. Nas hipóteses iniciais sobre q, se $r = 3$ então pela Proposição 1.75 obtemos $g \geqslant c_0(4) + \dfrac{q+1}{6}$, o que seria uma contradição. Logo $r = 4$. Se $q \equiv 0 \ mod\ 3$ e $(3q-1)(2g-2) > (q+1)(q^2-4q-1)$, segue o resultado pela Proposição 1.75. ▫

Assumindo quase-classicalidade podemos obter a existência de um ponto $\mathbb{F}_{q^2}-$racional com semigrupo de Weierstrass específico, como no resultado a seguir.

Proposição 2.26. *Seja $q \geqslant 7$. Seja $\mathcal{X}$ uma curva $\mathbb{F}_{q^2}-$maximal quase-clássica de gênero $g > 1$ com dimensão Frobenius 4. Então existe $P \in \mathcal{X}(\mathbb{F}_{q^2})$ tal que*

$$m_1(P) = q-2 \quad e \quad m_2(P) = q-1.$$

Em particular, $q - 3 \leqslant g \leqslant c_0(4)$.

Demonstração: Para todo $P \in \mathcal{X}(\mathbb{F}_{q^2})$ temos $v_P(R) \geqslant 2(q-1) - (m_1(P) + m_2(P))$. Suponha que $m_1(P) + m_2(P) \leqslant 2q-4$ para todo $P \in \mathcal{X}(\mathbb{F}_{q^2})$. Assim $v_P(R) \geqslant 2$ para todo $P \in \mathcal{X}(\mathbb{F}_{q^2})$. Pela quase-classicalidade temos $deg(R) = (6+q)(2g-2) + 5(q+1)$. Disto segue que $(2g-2)(q-6) < (1+q)(3-2q) < 0$ isto é, $q < 6$ um absurdo. Portanto existe $P' \in \mathcal{X}(\mathbb{F}_{q^2})$ tal que $m_1(P') + m_2(P') \geqslant 2q-3$. Pela maximalidade $m_3(P') = q$ assim

$$2q-3 \leqslant m_1(P') + m_2(P') \leqslant m_1(P') + q - 1$$

logo $m_1(P') \geqslant q-2$. Portanto $m_1(P') = q-2$ e $m_2(P') = q-1$. Como a dimensão Frobenius é igual a 4 então $g \leqslant c_0(4)$. Pelo Teorema 2.25 existe $P \in \mathcal{X}(\mathbb{F}_{q^2})$ tal que $m_1(P) = q-2$, $m_2(P) = q-1$ e $m_3(P) = q$. Logo $[1, q-3] \subseteq G(P)$. ▫

Alguns casos em que o gênero é igual a $q-3$, ainda não sabemos se existe uma curva $\mathbb{F}_{q^2}-$maximal com tal gênero. Observamos que para o caso $q = 7$, já se sabe que $4 \notin \mathbf{M}(7^2)$, por (KUDO; HARASHITA, 2017). Já é conhecido que

$$\{0,1,2,3,4,6,7,9,10,12,28\} \subseteq \mathbf{M}(8^2) \subseteq [0,10] \cup \{12\} \cup \{28\}$$

Resta saber se 5 pertence ou não a $\mathbf{M}(8^2)$. Mas se tal curva existir podemos obter algumas informações sobre ela, estudando a família de curvas $\mathbb{F}_{q^2}-$maximais de gênero $q-3$.

Observação 2.27. *Considere $\mathcal{X}$ curva $\mathbb{F}_{q^2}-$maximal de gênero $q-3$ e dimensão de Frobenius igual a 4. Então se $q \geqslant 13$ teremos não quase-classicalidade. De fato, caso contrário teríamos uma contradição com $deg(R) \geqslant \#\mathcal{X}(\mathbb{F}_{q^2})$. Em geral*

$$(1+\nu_2+q)2(q-4)+(q^2+4)(q+1) \geqslant (\varepsilon_2+\varepsilon_3-\nu_2+1)\left(2(q-4)q+(1+q)^2\right).$$

Para $q \leqslant 11$ com não quase-clássica temos apenas $q=9$ e $\mathcal{E}=\{0,1,3,4,9\}$ e $\mathcal{V}=\{0,1,3,9\}$. Além disso, pela Proposição 2.26, segue que existe $P' \in \mathcal{X}(\mathbb{F}_{q^2})$ tal que $m_1(P')=g+1$ e $m_2(P')=g+2$. Portanto, estas curvas quase-clássicas também serão clássicas (com respeito ao sistema canônico).

Algumas família de curvas que podem ser estudadas para tentar responder se existe uma curva $\mathbb{F}_{64}-$maximal de gênero 5. Por exemplo, as curvas trigonais $\mathbb{F}_{64}-$maximais, já que estas são clássicas (VIANA, 1989).

Corolário 2.28. *Seja $\mathcal{X}$ uma curva $\mathbb{F}_{64}-$maximal de gênero 5. Então $\mathcal{X}$ é não hiperelíptica com dimensão Frobenius 4, quase-clássica, Frobenius quase-clássica e clássica com respeito ao sistema canônico.*

2.3 Curvas Hurwitz: quase-classicalidade e não quase-classicalidade

Considere q uma potência de um primo $p>0$. A **curva Hurwitz** de grau $n+1$ é uma curva plana não singular dada pela equação

$$\mathcal{C}_n: \quad XY^n+YZ^n+X^nZ=0$$

onde $(n^2-n+1) \not\equiv 0 \ mod\ p$. Sabemos que quando $q+1 \equiv 0 \ mod\ (n^2-n+1)$, a curva $\mathcal{C}_n$ é coberta sobre $\mathbb{F}_{q^2}$ pela curva Hermitiana $\mathcal{H}_q$. Em particular, $\mathcal{C}_n$ é $\mathbb{F}_{q^2}-$maximal nesta hipótese. Além disso, o semigrupo de Weierstrass de $\mathcal{C}_n$ no ponto $(0,1,0)$ é gerado pelo conjunto $S:=\{s(n-1)+1 : s=1,...,n\}$, veja Lema 10.76 e Lema 10.77 em (HIRSCHFELD; KORCHMÁROS; TORRES, 2008). Quando $n=p$, segue de tais lemas que a curva $\mathcal{C}_p$ é $\mathbb{F}_{p^6}-$maximal de gênero $p(p-1)/2$ e tem semigrupo de Weierstrass em $P_0:=(0,1,0)$ gerado pelo conjunto

$$\{0,p,2p-1,3p-2,4p-3,...,p^2-(p-1)\}. \tag{2.13}$$

Seja $\mathcal{D}_0=g^r_{p^3+1}$ a série de Frobenius de $\mathcal{C}_p$ sobre $\mathbb{F}_{p^6}$. Queremos estudar o comportamento de suas $\mathcal{D}_0-$ordens. Vamos mostrar que

$$\varepsilon_i=i \text{ para } i \leqslant r-g+2p-4 \text{ e } \nu_i=i \text{ para } i \leqslant r-g+p-3 \text{ para a curva } \mathcal{C}_p.$$

Observamos que segue da Proposição 1.6.6, em (STICHTENOTH, 2009), que neste caso teremos

$$m_g(P)=2g=p^2-p, \text{ para todo } P \text{ ponto } \mathbb{F}_{p^6}-\text{racional de } \mathcal{C}_p. \tag{2.14}$$

Proposição 2.29. *A série Frobenius da curva $\mathcal{C}_p$ sobre $\mathbb{F}_{p^6}$ temos dimensão igual a p^3-g+1 e grau p^3+1.*

Demonstração: Seja r a dimensão Frobenius de $\mathcal{C}_p$. Observamos que se $r-1 \leqslant g$ então para todo $P \in \mathcal{C}_p$ teríamos pela maximalidade que

$$p^3 = m_{r-1}(P) \leqslant m_g(P).$$

Mas segue de (2.14), um absurdo. Portanto $r-1 > g$, assim $m_{r-1}(P) = 2g+(r-1-g) = g+r-1$ para todo $P \in \mathcal{C}_p$. Novamente pela maximalidade obtemos $r = p^3-g+1$. ▫

Como $P_0 \in \mathcal{C}_p$ e $m_1(P_0) = p$ então pela maximalidade $j_{r-1}(P_0) = p^3+1-m_1(P_0) = p^3-p+1$. Além disso, $p^3-p(p-1)/2 = r-1 \leqslant \varepsilon_{r-1} \leqslant j_{r-1}(P_0) = p^3-p+1$ logo $2p^3-p(p-1) \leqslant 2\varepsilon_{r-1} \leqslant 2p^3-2p+2$, isto é,

$$p(3-p) = 2p-p(p-1) \leqslant 2\varepsilon_{r-1}-2p^3+2p \leqslant 2. \tag{2.15}$$

Proposição 2.30. *As curvas $\mathcal{C}_p$ são quase-clássica sobre $\mathbb{F}_{p^6}$ com $p \in \{2,3\}$.*

Demonstração: Como $p=2$ então por (2.15) temos $\varepsilon_7 = 7$. Portanto, $\varepsilon_i = i$, $i \leqslant r-1$. Como $p=3$ então por (2.15) temos $\varepsilon_{r-1} = p^3-p$ ou $\varepsilon_{r-1} = p^3-p+1$, isto é, $\varepsilon_{24} = 24$ ou 25. Como $H(P_0) = \langle 3,5,7\rangle$ então para $i \geqslant 2$ temos

$$j_{25-i}(P_0) = 28-m_i(P_0) = 28-(g+i) = 25-i$$

então $\varepsilon_{25-i} \leqslant j_{25-i}(P_0) = 25-i$ para $i \geqslant 2$, isto é, $\varepsilon_i = i$ para $i = 0,1,2,3,...,23$. Suponha que $\varepsilon_{24} = 25$. Pelo Critério $p-$ádico segue que $\varepsilon_{23} = 24$. Absurdo. Logo $\varepsilon_{24} = 24$. Além disso, pela maximalidade $\varepsilon_{25} = p^3 = 27$. Portanto, $\mathcal{C}_3$ é quase-clássica. ▫

Vamos assumir $p \geqslant 5$. Sabemos que $[1,p-1] \subseteq G(P_0)$ e

$$[kp+1,(k+1)p-(k+1)] \subseteq G(P_0), \text{ para } 1 \leqslant k \leqslant p-3.$$

Por contagem obtemos

$$G(P_0) = [1,p-1] \cup [p+1,2p-2] \cup [2p+1,3p-3] \cup ... \cup [p^2-3p+1,p^2-3p+2] \cup \{p^2-2p+1\}.$$

Proposição 2.31. *A curva $\mathcal{C}_p$ tem o seguinte comportamento das $\mathcal{D}_0-$ordens:*

$$\varepsilon_i = i, \text{ para } i = 0,1,...,r-g.$$

As Frobenius ordens satisfazem $\nu_i = i$, para $i = 0,1,...,r-g-1$.

Demonstração: Em geral, para a curva $\mathcal{C}_p$ temos para $i \geqslant g$

$$j_{r-i}(P_0) \;=\; p^3+1-m_{g+(i-g)}(P_0) = p^3+1-i-g = r-i.$$

Como $\varepsilon_{r-i} \leqslant j_{r-i}(P_0) = r-i$ para $g \leqslant i \leqslant r$ e como $\nu_{r-i-1} \leqslant j_{r-i}(P_0)-j_1(P_0) = r-i-1$. Assim $\varepsilon_{r-i} = r-i$ para $g \leqslant i \leqslant r$ e $\nu_{r-i-1} = r-i-1$ para $g \leqslant i \leqslant r-1$. ▫

Teorema 2.32. *Seja $p > 3$. A curva $\mathcal{C}_p$ tem a seguinte propriedade para as $\mathcal{D}_0-$ordens:*

$$\varepsilon_i = i \text{ para } i \leqslant r - g + 2p - 4.$$

As Frobenius ordens satisfazem $\nu_i = i$ para $i \leqslant r - g + p - 3$. Além disso, $\mathcal{V} = \mathcal{E}\backslash\{\varepsilon_I\}$ com $I = r - g + p - 2$ ou $I > r - g + 2p - 5$ e $\varepsilon_{r-g+2p-3} \in \{r - g + 2p - 3, r - g + 2p - 1\}$, $\nu_{r-g+2p-4} \in \{r - g + 2p - 4, r - g + 2p - 3, r - g + 2p - 2, r - g + 2p - 1\}$.

Demonstração: Sabemos que para $1 \leqslant k \leqslant p - 1$ temos que

$$(p - (k + 1))p, \quad k(p - 1) + 1 \in H(P_0)$$

logo $p^2 - p - (k - 1) = (p - k - 1)p + k(p - 1) + 1 \in H(P_0)$. Como $m_g(P_0) = p^2 - p$, por (2.14), então $m_{g-1}(P_0) = p^2 - p - 1$, $m_{g-2}(P_0) = p^2 - p - 2, ..., m_{g-(p-2)}(P_0) = p^2 - 2p + 2$. Portanto para $k = 1, 2, ..., p - 1$ temos $m_{g-k}(P_0) = p^2 - p - k = 2g - k, \quad k = 0, 1, ..., p - 2$. Isto implica que para $k = 0, 1, 2, ..., p - 2$ temos

$$j_{r-g+k}(P_0) \;\; = \;\; p^3 + 1 - m_{g-k}(P_0) = 1 + p^3 - 2g + k = r - g + k.$$

Portanto $\varepsilon_{r-g+k} = r - g + k$ para $k = 0, 1, 2, ..., p - 2$. Além disso, para $k = 0, 1, ..., p - 2$ temos

$$\nu_{r-g+k-1} \leqslant j_{r-g+k}(P_0) - 1 = r - g + k - 1,$$

logo $\nu_{r-g+k-1} = r - g + k - 1$ para $k = 0, 1, ..., p - 2$. Isto é,

$$\nu_i = i, \text{ para } i = r - g - 1, r - g, ..., r - g + p - 3.$$

Observamos que o intervalo $[p^2 - 3p + 3, p^2 - 2p] \subset H(P_0)$ e $m_{g-p+2}(P_0) = p^2 - 2p + 2$ é o condutor de $H(P_0)$, logo $m_{g-2p+k}(P_0) = 2g - 2p + (k - 1)$, para $k = 4, ..., p + 1$. Assim para $k = 4, ..., p + 1$ temos

$$j_{r-g+2p-k}(P_0) \;\; = \;\; 1 + p^3 - m_{g-2p+k}(P_0) = r + g - 2g + 2p - k + 1 = r - g + 2p - k + 1.$$

Isto é, $j_i(P_0) = i + 1$ para $i \in \{r - g + 2p - 3, ..., r - g + p\}$. Portanto $\varepsilon_{r-g+2p-k} \in \{r - g + 2p - k, r - g + 2p - k + 1\}$ para $k = 4, ..., p + 1$. Em particular, $\varepsilon_{r-g+p-1} \in \{r - g + p - 1, r - g + p\}$. Se supormos que $\varepsilon_{r-g+p-1} = r - g + p$ então como

$$\binom{r - g + p}{r - g + p - 1} = r - g + p = p^3 - p^2 + 2p + 1 \equiv 1 \; mod \; p$$

segue que $r - g + p - 1 \in \mathcal{E}$, isto é, $\varepsilon_{r-g+p-2} = r - g + p - 1$. Uma contradição, pois $\varepsilon_{r-g+p-2} = r - g + p - 2$. Portanto, $\varepsilon_{r-g+p-1} = r - g + p - 1$. Analogamente, $\varepsilon_{r-g+p+i} = r - g + p + i$ com $i = 0, 1, ..., p - 4$. Além disso, para $k = 4, ..., p + 1$ temos $\nu_{r-g+2p-k-1} \in \{r - g + 2p - k - 1, r - g + 2p - k.\}$. Note que se $\nu_{r-g+p-2} = r - g + p - 1$ então $\nu_{r-g+2p-k-1} = r - g + 2p - k$ para $k = 4, ..., p$. Logo se $I = r - g + p - 2$ então $\nu_i = i + 1$ para $i \in \{r - g + p - 2, ..., r - g + 2p - 5\}$.

Como $[p^2-4p+4, p^2-3p] \subset H(P_0)$ e como $m_{g-2p+4}(P_0) = 2g-2p+3 = p^2-3p+3$ então $m_{g-2p+3-k}(P_0) = 2g-2p-k$ para $k = 0, 1, ..., p-4$. Assim para $k = 0, 1, ..., p-4$ tem-se

$$j_{r-g+2p-3+k}(P_0) \;=\; 1 + p^3 - m_{g-2p+3-k} = r + g - 2g + 2p + k = r - g + 2p + k.$$

Isto é, $j_i(P_0) = i+3 \quad$ para $i = r-g+2p, ..., r-g+3p-4$. Portanto para $k = 0, 1, ..., p-4$ temos

$$\varepsilon_{r-g+2p+k-3} \in \{r-g+2p+k-3, r-g+2p+k-2, ..., r-g+2p-1, r-g+2p\}.$$

Em particular,

$$\varepsilon_{r-g+2p-3} \in \{r-g+2p-3, r-g+2p-2, r-g+2p-1, r-g+2p\}, \quad (2.16)$$

$$\varepsilon_{r-g+2p-2} \in \{r-g+2p-2, r-g+2p-1, r-g+2p, r-g+2p+1\}, \quad (2.17)$$

$$\varepsilon_{r-g+2p-1} \in \{r-g+2p-1, r-g+2p, r-g+2p+1, r-g+2p+2\}, \quad (2.18)$$

$$\varepsilon_{r-g+2p} \in \{r-g+2p, r-g+2p+1, r-g+2p+2\}. \quad (2.19)$$

Supondo que $\varepsilon_{r-g+2p-3} = r-g+2p$, como

$$\binom{r-g+2p}{r-g+2p-1} = r-g+2p = p^3-p^2+3p+1 \equiv 1 \; mod \; p.$$

logo $\varepsilon_{r-g+2p-4} = r-g+2p-1$ uma contradição. Se admitimos que $\varepsilon_{r-g+2p-3} = r-g+2p-2$, então

$$\binom{r-g+2p-2}{r-g+2p-3} = r-g+2p-2 = p^3-p^2+3p-1 \equiv -1 \; mod \; p$$

segue que $\varepsilon_{r-g+2p-4} = r-g+2p-3$ uma contradição. Portanto $\varepsilon_{r-g+2p-3} \in \{r-g+2p-3, r-g+2p-1\}$. Note que $\nu_{r-g+2p-4} \in \{r-g+2p-4, r-g+2p-3, r-g+2p-2, r-g+2p-1\}$. □

Casos particulares

Observação 2.33. *Se $p = 5$ então $\varepsilon_i = i$ para $i \leqslant 112$ e $\nu_i = i$ para $i \leqslant 108$. Sabemos que*

$$H(P_0) = \{0, 5, 9, 10, 13, 14, 15, 17, \mapsto\}.$$

Assim $j_{110}(P_0) = 111$, $j_{111}(P_0) = 112$, $j_{112}(P_0) = 113$, $j_{113}(P_0) = 116$, $j_{114}(P_0) = 117$ e $j_{115}(P_0) = 121$. Pelo Critério p−ádico temos $\varepsilon_{113} = 113$, $\varepsilon_{114} \in \{114, 115, 116\}$ e $\varepsilon_{115} \in \{115, 116, 117, 120\}$. E $\nu_{109} = 109$, $\nu_{110} = 110$, $\nu_{111} = 111$, $\nu_{112} = 112$, $\nu_{113} \in \{113, 115, 116\}$ e $\nu_{114} \in \{114, 115, 116, 117, 120\}$. Assim $\varepsilon_{113} = 113$, $\varepsilon_{114} \neq 116$.

Se $\nu_{112} = 115$ então $\nu_{113} = 116$ e $\nu_{114} \in \{117, 120\}$. Como

$$(\{0, 1, ..., 113\} \cup \{\varepsilon_{114}, \varepsilon_{115}, 125\}) \setminus \{\varepsilon_I\} = \mathcal{E} \setminus \{\varepsilon_I\} = \{0, 1, ..., 111\} \cup \{115, 116, \nu_{114}, 125\}$$

segue um absurdo. Logo $\nu_{112} = 112$. *Assim* $\nu_{113} \in \{113, 115\}$. *Suponha que* $\nu_{113} = 113$ *então* $\nu_{114} \in \{114, 115\}$. *Logo* $\nu_{114} = \varepsilon_{115} = 115$ *ou* $\nu_{114} = \varepsilon_{114} = 114$. *Suponha que* $\nu_{113} = 115$ *então* $\varepsilon_{114} = \nu_{113} = 115$ *e* $\nu_{114} = \varepsilon_{115} \in \{116, 120\}$. *Daí*

$$\begin{aligned} &\mathcal{E} : \{0, 1, ..., 113, 114, 115\} \cup \{125\} \quad e \quad \mathcal{V} : \mathcal{E}\backslash\{\gamma\} \text{ com } \gamma \in \{114, 115\} \\ ou \quad &\mathcal{E} : \{0, 1, ..., 113\} \cup \{115, \mu, 125\} \quad e \quad \mathcal{V} : \mathcal{E}\backslash\{113\} \text{ com } \mu \in \{116, 120\} \end{aligned}$$

Portanto se $\mathcal{C}_5$ *é quase clássica então* $\gamma = 115$.

Corolário 2.34. *Se* $p > 5$ *então* $r - g + 2p - 1, r - g + 2p, ..., r - g + 3p - 7 \in \mathcal{E}$. *Se* $p = 7$ *então* $[0, 1, ..., 312\} \cup \{315, 316\} \subseteq \mathcal{E}$.

Demonstração: Se $\varepsilon_{r-g+3p-7} = r - g + 3p - 7$ então $\varepsilon_i = i$ para $i \leqslant r - g + 3p - 7$.

Suponha que $\varepsilon_{r-g+3p-7} = r - g + 3p - 6$. Assim $\varepsilon_{r-g+3p-k} = r - g + 3p - k + 1$, para $8 \leqslant k \leqslant p + 1$. Em particular, $\varepsilon_{r-g+2p-1} = r - g + 2p$. Logo $\varepsilon_{r-g+2p-2} = r - g + 2p - 1$. Suponha que $\varepsilon_{r-g+3p-7} = r - g + 3p - 5$. Assim $\varepsilon_{r-g+3p-k} = r - g + 3p - k + 2$, para $8 \leqslant k \leqslant p + 2$. Em particular, $\varepsilon_{r-g+2p-2} = r - g + 2p$. Logo $\varepsilon_{r-g+2p-3} = r - g + 2p - 1$. Suponha que $\varepsilon_{r-g+3p-7} = r - g + 3p - 4$. Assim $\varepsilon_{r-g+3p-k} = r - g + 3p - k + 3$ para $8 \leqslant k \leqslant p + 3$. Em particular, $\varepsilon_{r-g+2p-3} = r - g + 2p$. Logo $\varepsilon_{r-g+2p-4} = r - g + 2p - 1$. Contradizendo o Teorema 2.32. ▫

Corolário 2.35. *Se* $p > 7$ *então* $r - g + 3p - 1, r - g + 3p, ..., r - g + 4p - 10 \in \mathcal{E}$.

Demonstração: Segue da demonstração do Teorema 2.32 que $m_{g-3p+6}(P_0) = p^2 - 4p$ e que $[p^2 - 5p + 4, p^2 - 4p] \subseteq H(P_0)$. Assim segue que $m_{g-4p+10+k}(P_0) = p^2 - 5p + 4 + k$, com $k \in \{0, 1, ..., p - 4\}$. Logo para $k \in \{0, 1, ..., p - 4\}$ temos

$$j_{r-g+4p-10-k}(P_0) \;=\; 1 + p^3 - p^2 + 5p - 4 - k = (r - g + 4p - 10 - k) + 6.$$

Assim para $k \in \{0, 1, ..., p - 4\}$ obtemos $\varepsilon_{r-g+4p-10-k} \in \{r - g + 4p - 10 - k, ..., r - g + 4p - 10 - k + 6\}$. Em particular, $\varepsilon_{r-g+3p-6} \in \{r - g + 3p - 6, ..., r - g + 3p\}$. Se $\varepsilon_{r-g+4p-10} = r - g + 4p - 10$ então $\varepsilon_i = i$ para $i \leqslant r - g + 4p - 10$.

- Suponha que $\varepsilon_{r-g+4p-10} = r - g + 4p - 9$. Então

  $$\varepsilon_{r-g+4p-k} = r - g + 4p - k + 1, \quad \text{com } 11 \leqslant k \leqslant p + 1.$$

  Em particular, $\varepsilon_{r-g+3p-1} = r - g + 3p$. Logo $\varepsilon_{r-g+3p-2} = r - g + 3p - 1$.

- Suponha que $\varepsilon_{r-g+4p-10} = r - g + 4p - 8$. Então

  $$\varepsilon_{r-g+4p-k} = r - g + 4p - k + 2, \quad \text{com } 11 \leqslant k \leqslant p + 2.$$

  Em particular, $\varepsilon_{r-g+3p-2} = r - g + 3p$. Logo $\varepsilon_{r-g+3p-3} = r - g + 3p - 1$.

- Suponha que $\varepsilon_{r-g+4p-10} = r-g+4p-7$. Então

$$\varepsilon_{r-g+4p-k} = r-g+4p-k+3, \quad \text{com } 11 \leqslant k \leqslant p+3.$$

Em particular, $\varepsilon_{r-g+3p-3} = r-g+3p$. Logo $\varepsilon_{r-g+3p-4} = r-g+3p-1$.

- Suponha que $\varepsilon_{r-g+4p-10} = r-g+4p-6$. Então

$$\varepsilon_{r-g+4p-k} = r-g+4p-k+4, \quad \text{com } 11 \leqslant k \leqslant p+4.$$

Em particular, $\varepsilon_{r-g+3p-4} = r-g+3p$. Logo $\varepsilon_{r-g+3p-5} = r-g+3p-1$.

- Suponha que $\varepsilon_{r-g+4p-10} = r-g+4p-5$. Então

$$\varepsilon_{r-g+4p-k} = r-g+4p-k+5, \quad \text{com } 11 \leqslant k \leqslant p+5.$$

Em particular, $\varepsilon_{r-g+3p-5} = r-g+3p$. Logo $\varepsilon_{r-g+3p-6} = r-g+3p-1$.

- Suponha que $\varepsilon_{r-g+4p-10} = r-g+4p-4$. Então

$$\varepsilon_{r-g+4p-k} = r-g+4p-k+6, \quad \text{com } 11 \leqslant k \leqslant p+6.$$

Em particular, $\varepsilon_{r-g+3p-6} = r-g+3p$. Logo $\varepsilon_{r-g+3p-7} = r-g+3p-1$. □

Considere o intervalo

$$I_k = [r-g+kp-1, r-g+(k+1)p-(3k+1)] \tag{2.20}$$

para $2 \leqslant k < \dfrac{p}{3}$.

Lema 2.36. *Se $p > 5$ então $I_k \subseteq H(P)$ para $2 \leqslant k < \dfrac{p}{3}$.*

Demonstração: Para $1 \leqslant k < p$ considere $H_k := [p^2-kp+k, p^2-(k-1)p]$. Segue de (2.13) e da demonstração do Teorema 2.32 que $H_k \subset H(P)$ para $1 \leqslant k < p$ e como

$$\begin{aligned}
m_{g-p+1-j}(P_0) &= (g-p+1-j)+(g-1) \text{ para } 0 \leqslant j \leqslant p-3,\\
m_{g-p+1-j}(P_) &= (g-p+1-j)+(g-3) \text{ para } p-2 \leqslant j \leqslant 2p-6,\\
m_{g-p+1-j}(P_0) &= (g-p+1-j)+(g-6) \text{ para } 2p-5 \leqslant j \leqslant 3p-10,\\
&\vdots\\
m_{g-p+1-j}(P_0) &= (g-p+1-j)+(g-(g-2p+3)) \text{ para } g-p-2 \leqslant j \leqslant g-p-1\\
m_1(P_0) &= (g-p+1-j)+(g-(g-2p+2)) = p.
\end{aligned}$$

Assim para $k = 0, 1, ..., p-4$ tem-se

$$j_{r-g+2p-3+k}(P_0) = 1+p^3-m_{g-2p+3-k} = r+g-2g+2p+k = r-g+2p+k.$$

Isto é, $j_i(P_0) = i+3 \quad$ para $i = r-g+2p, ..., r-g+3p-4$. Portanto para $k = 0, 1, ..., p-4$ temos $\varepsilon_{r-g+2p+k-3} \in \{r-g+2p+k-3, r-g+2p+k-2, ..., r-g+2p-1, r-g+2p\}$. Em particular,

$$\begin{aligned}
\varepsilon_{r-g+2p-3} &\in \{r-g+2p-3, r-g+2p-2, r-g+2p-1, r-g+2p\},\\
\varepsilon_{r-g+2p-2} &\in \{r-g+2p-2, r-g+2p-1, r-g+2p, r-g+2p+1\},\\
\varepsilon_{r-g+2p-1} &\in \{r-g+2p-1, r-g+2p, r-g+2p+1, r-g+2p+2\},\\
\varepsilon_{r-g+2p} &\in \{r-g+2p, r-g+2p+1, r-g+2p+2\}.
\end{aligned}$$

Supor que $\varepsilon_{r-g+2p-3} = r-g+2p$. Como

$$\binom{r-g+2p}{r-g+2p-1} = r-g+2p = p^3-p^2+3p+1 \equiv 1 \ mod\ p.$$

logo $\varepsilon_{r-g+2p-4} = r-g+2p-1$ uma contradição. Supor que $\varepsilon_{r-g+2p-3} = r-g+2p-2$. Como

$$\binom{r-g+2p-2}{r-g+2p-3} = r-g+2p-2 = p^3-p^2+3p-1 \equiv -1 \ mod\ p$$

logo $\varepsilon_{r-g+2p-4} = r-g+2p-3$ uma contradição. Portanto $\varepsilon_{r-g+2p-3} \in \{r-g+2p-3, r-g+2p-1\}$. Se $\varepsilon_{r-g+3p-7} = r-g+3p-7$ então $\varepsilon_i = i$ para $i \leqslant r-g+3p-7$. Suponha que $\varepsilon_{r-g+3p-7} = r-g+3p-6$. Assim

$$\varepsilon_{r-g+3p-k} = r-g+3p-k+1, \quad \text{para } 8 \leqslant k \leqslant p+1.$$

Em particular, $\varepsilon_{r-g+2p-1} = r-g+2p$. Logo $\varepsilon_{r-g+2p-2} = r-g+2p-1$. Suponha que $\varepsilon_{r-g+3p-7} = r-g+3p-5$. Assim

$$\varepsilon_{r-g+3p-k} = r-g+3p-k+2, \quad \text{para } 8 \leqslant k \leqslant p+2.$$

Em particular, $\varepsilon_{r-g+2p-2} = r-g+2p$. Logo $\varepsilon_{r-g+2p-3} = r-g+2p-1$. Suponha que $\varepsilon_{r-g+3p-7} = r-g+3p-4$. Assim

$$\varepsilon_{r-g+3p-k} = r-g+3p-k+3, \quad \text{para } 8 \leqslant k \leqslant p+3.$$

Em particular, $\varepsilon_{r-g+2p-3} = r-g+2p$. Logo $\varepsilon_{r-g+2p-4} = r-g+2p-1$. Contradizendo o Teorema 2.32. Portanto o intervalo definido em (2.20), satisfaz $I_2 \subseteq H(P)$. ▫

Teorema 2.37. *Seja $p > 5$ primo. Se*

$$I \neq r-g+2p+kp-2 \quad \textit{para todo } k \in \mathbb{Z},\ 2k \leqslant p-5$$

então $\mathcal{C}_p$ é não quase-clássica.

Demonstração: Suponha que $\mathcal{C}_p$ seja quase-clássica. Suponha que $I \leqslant r-g+2p-4$.

- Se $I = r - g + p - 2$ então como $I + p \leqslant r - 2$ segue que $\nu_{I+p-1} = \varepsilon_{I+p} = I + p$. Pelo Critério $p-$ádico segue que $\binom{I+p}{I} \not\equiv 0 \ mod\ p$, assim $I \in \mathcal{V}$ absurdo.

- Se $I = r - g + p - 1$ então $\nu_I = I + 1 \equiv 1 \ mod\ p$ e pelo Critério $p-$ádico segue que $I \in \mathcal{V}$. Absurdo.

- Se $I = r - g + p$ então $\nu_I = I + 1 \equiv 2 \ mod\ p$ e pelo Critério $p-$ádico segue que $I \in \mathcal{V}$. Absurdo.

- Se $I = r - g + p + l$ com $l \in \{1, ..., p - 4\}$ e $l + 1 \not\equiv 0 \ mod\ p$ então $\nu_I = I + 1 = p^3 - 2g + p + (l + 1) \not\equiv 0 \ mod\ p$ e pelo Critério $p-$ádico segue que $I \in \mathcal{V}$. Absurdo.

Portanto $I \neq r-g+p+l$ com $l \in \{-1, 0, 1, ..., p-4\}$ e $l+1 \not\equiv 0 \ mod\ p$. Isto é, $I = r-g+p+l$ com $l \in \{-1, 0, 1, ..., p - 4\}$ e $l + 1 \equiv 0 \ mod\ p$, um absurdo.

Assim $I > r - g + 2p - 4$. Daí $I = r - g + 2p - 3 + l$ para $l \in \{0, 1, ..., g - 2p + 1\}$.

- Se $I = r - g + 2p - 3 + l$ para $l \in \{0, 1, ..., g - 2p + 1\}$ com $l - 1 \not\equiv 0 \ mod\ p$, então $\nu_I = I + 1 \equiv (l - 1) \ mod\ p$ e pelo Critério $p-$ádico segue que $I \in \mathcal{V}$. Absurdo.

Então $I = r - g + 2p - 3 + l$ para $l \in \{0, 1, ..., g - 2p + 1\}$ com $l - 1 \equiv 0 \ mod\ p$. Portanto $l = sp + 1$ com $k \in \mathbb{N}$ e $kp + 1 \in \{0, 1, ..., g - 2p + 1\}$, logo

$$I = r - g + 2p + kp - 2 \quad \text{com } 2k \leqslant p - 5, k \in \mathbb{N}.$$

Em particular para $p > 5$ se tivermos $I = r - g + 2p - 2$, segue que $\nu_{I+p-1} = \varepsilon_{I+p} = I + p$ pois $I + p \leqslant r - 2$. Como neste caso $\binom{I+p}{I} \not\equiv 0 \ mod\ p$ segue que $I \in \mathcal{V}$. Absurdo. □

3 Mais propriedades de curvas maximais com dimensão Frobenius 3 sobre $\mathbb{F}_{q^2}$, $q \geqslant 7$

Este capítulo é motivado pela classificação de curvas maximais com dimensão Frobenius igual a 3 através de modelos birracionalmente equivalentes sobre um corpo finito previamente fixado, a qual surge em (FANALI; GIULIETTI, 2009). Obtemos nesta literatura uma classificação completa sobre os corpos $\mathbb{F}_{16}$ e $\mathbb{F}_{25}$. Apresentaremos neste capítulo uma classificação completa para curvas $\mathbb{F}_{49}-$maximais com dimensão Frobenius 3 através de modelos birracionais sobre $\mathbb{F}_{49}$ ao utilizar resultados já conhecidos de (FANALI; GIULIETTI; PLATONI, 2012), (KUDO; HARASHITA, 2017) e (ARAKELIAN; TAFAZOLIAN; TORRES, 2018). Um caminho natural a se seguir é a classificação completa para curvas $\mathbb{F}_{64}-$maximais com dimensão Frobenius 3 através de modelos birracionais sobre $\mathbb{F}_{64}$. Com este intuito, também apresentaremos neste capítulo uma classificação para curvas $\mathbb{F}_{64}-$maximais de gênero igual a 9 ou 10, sob certas hipóteses. Enfatizamos que a extrema importância do uso de ferramentas computacionais para tais classificações. Neste trabalho foi utilizado o software Magma, (BOSMA; CANNON; PLAYOUST, 1997).

3.1 $\mathbb{F}_{49}$

Agora vamos trabalhar sobre o corpo $\mathbb{F}_{49}$. Seja $\mathcal{X}$ uma curva $\mathbb{F}_{49}-$maximal de gênero g com dimensão Frobenius igual a 3 e seja $P_0 \in \mathcal{X}(\mathbb{F}_{49})$. Pela Proposição 1.66 segue que $m_2(P_0) = 7$ e $m_1(P_0) = 4, 5$ ou 6. Então $g \geqslant 5$. Neste caso $g \leqslant c_0(3) = 9$ pela Cota de Castelnuovo. Então $g \in \{5, 6, 7, 8, 9\}$. Pela Proposição 1.75 deveríamos ter $g > 6$. Portanto $g \in \{7, 8, 9\}$. Quando $g = 7$ segue por (FANALI; GIULIETTI; PLATONI, 2012) que $\mathcal{X}$ é birracionalmente equivalente sobre $\mathbb{F}_{49}$ a curva plana dada por

$$Y^7 - YX^4 + \omega X^2 = 0,$$

com $\omega^8 = -1$. Este resultado é obtido através de cálculos computacionais via Magma. Quando $g = 9 = \lfloor c_0(3) \rfloor$, já é conhecido pelo Teorema 2.6 que a curva $\mathcal{X}$ é birracionalmente equivalente sobre $\mathbb{F}_{49}$ à curva plana dada por

$$Y^4 = X^7 + X.$$

Entretanto, somente em (ARAKELIAN; TAFAZOLIAN; TORRES, 2018) conhecemos a completa determinação do espectro de gêneros sobre $\mathbb{F}_{49}$, a saber, $\mathbf{M}(7^2) = \{0, 1, 2, 3, 5, 7, 9, 21\}$, logo $g \in \{7, 9\}$. Estes fatos nos permitem classificar as curvas $\mathbb{F}_{49}-$maximais com dimensão Frobenius igual a 3.

Teorema 3.1. *Seja $\mathcal{X}$ uma curva $\mathbb{F}_{49}-$maximal de gênero g com dimensão Frobenius igual a 3. Então $\mathcal{X}$ é birracionalmente equivalente sobre $\mathbb{F}_{49}$ à curva plana dada por*

(i) $Y^4 = X^7 + X$ *e tem gênero 9 ou*

(ii) $Y^7 - YX^4 + \omega X^2 = 0$ *com* $\omega^8 = -1$ *e tem gênero 7.*

3.2 $\mathbb{F}_{64}$

Sobre $\mathbb{F}_{64}$ existem apenas alguns valores possíveis de gênero para curvas maximais. Sabemos que

$$\{0, 1, 2, 3, 4, 6, 7, 9, 10, 12, 28\} \subseteq M(8^2) \subseteq [0, 10] \cup \{12\} \cup \{28\}.$$

Aqui o único valor de gênero ainda não conhecido é o igual a 5.

Proposição 3.2. *Seja $\mathcal{X}$ uma curva $\mathbb{F}_{64}-$maximal de gênero g e dimensão Frobenius 3. Então $g \in \{9, 10, 12\}$.*

Demonstração: Primeiramente pela Cota de Castelnuovo temos que $g \leqslant c_0(3) < 13$. Seja $P_0 \in \mathcal{X}(\mathbb{F}_{64})$. Pela maximalidade $m_2(P_0) = 8$, veja Proposição 1.66. Como $4 \leqslant m_1(P_0) \leqslant 7$ então $g \geqslant 6$. Então $g \in [6, 12]$. Observe que se $g = 6$ ou 7 então pelo Teorema 2.25 segue que $r = 4$. Como $8, 11 \notin M(8^2)$ logo $g \in \{9, 10, 12\}$. ▫

No caso em que o gênero é igual a 12, pelo Teorema 2.6 sabemos que existe uma única curva, a menos de isomorfismo.

Teorema 3.3. *Toda curva $\mathbb{F}_{64}-$maximal de gênero 12 é $\mathbb{F}_{64}-$birracionalmente equivalente a curva plana com equação*

$$Y^9 = X^4 + X^2 + X. \tag{3.1}$$

Podemos nos perguntar se é possível uma classificação para os gêneros iguais aos valores 9 e 10 para que desta forma possamos dar uma classificação completa sobre $\mathbb{F}_{64}$. Sabemos que existe um único modelo, a menos de isomorfismo, em cada caso ao se assumir a hipótese de tais curvas serem Galois-cobertas pela curva Hermitiana.

Teorema 3.4 (Teorema 2.1, (COSSIDENTE; KORCHMÁROS; TORRES, 2000))**.** *Toda curva $\mathbb{F}_{64}-$maximal Galois-coberta pela curva Hermitiana de gênero 9 é $\mathbb{F}_{64}-$birracionalmente equivalente a curva $\mathcal{F}_0'$ dada por*

$$Y^8 = YX^2 + X^5 \tag{3.2}$$

Sabemos que esta curva $\mathcal{F}_0'$ satisfaz:

(i) $j_2(P) = 2$ para todo P racional;

(ii) Existem P_1, P_2, P_3 pontos que não são $\mathbb{F}_{64}-$racionais tais que $j_2(P_i) = 3$ para $i = 1, 2, 3$;

(iii) $j_2(P) = 2$ para $P \notin \{P_1, P_2, P_3\}$ não $\mathbb{F}_{64}-$racional.

Para mais informações veja Seção 6, (COSSIDENTE; KORCHMÁROS; TORRES, 1999).

Teorema 3.5 (Teorema 2.1, (COSSIDENTE; KORCHMÁROS; TORRES, 2000))**.** *Toda curva $\mathbb{F}_{64}-$maximal de gênero igual a* 10 *que é Galois-coberta pela curva Hermitiana é $\mathbb{F}_{64}-$birracionalmente equivalente a curva $\mathcal{F}_0$ dada por*

$$v^9 = u^6 + u^3. \tag{3.3}$$

Com estes resultados podemos enunciar uma classificação para curvas $\mathbb{F}_{64}-$maximais com dimensão Frobenius 3, quando estas são Galois-coberta pela curva Hermitiana.

Teorema 3.6. *Seja $\mathcal{X}$ uma curva $\mathbb{F}_{64}-$maximal com dimensão Frobenius* 3 *e Galois-coberta pela curva Hermitiana. Então $\mathcal{X}$ é $\mathbb{F}_{64}-$birracionalmente equivalente a alguma das curvas a seguir*

(i) a curva dada por (3.1) com gênero 12;

(ii) a curva dada por (3.3) com gênero 10;

(iii) a curva dada por (3.2) com gênero 9.

Queremos um resultado similar do Teorema 3.6 sem a hipótese da Galois-cobertura pela curva Hermitiana. Este resultado seria possível se soubéssemos a existência ou não existência de curvas $\mathbb{F}_{64}-$maximais de gênero 9 ou 10 que não são Galois-cobertas, já que a classificação gênero 12 não depende de Galois-cobertura. Em geral, a curva definida por Giulietti-Korchmáros em (GIULIETTI; KORCHMÁROS, 2009) é um exemplo de curva maximal que não é Galois-coberta pela curva Hermitiana sobre certos corpos. Entretanto sobre o corpo $\mathbb{F}_{64}$, esta curva é um exemplo de curva maximal de gênero 10, dada pelas equações

$$Z^3 = Y(1 + X + X^2), \quad Y^3 = X^2 + X, \tag{3.4}$$

e coberta pela curva Hermitiana $U^9 + V^9 + 1 = 0$. Para construir tal cobertura, basta considerar $\varepsilon \in \mathbb{F}_{64}$ uma raiz cúbica primitiva, $X := \dfrac{U^3}{U^3 + V^3} + \varepsilon$ e $Z := \dfrac{UV}{U^3 + V^3}$. Desta maneira, obtemos a curva $Z^9 = X^8 + X - (X^2 + X)^3$ a qual é $\mathbb{F}_{64}-$birracionalmente

equivalente a curva dada por (3.4) (ver Teorema 4, em (GIULIETTI; KORCHMÁROS, 2009)).

Assim a curva dada por (3.4) é $\mathbb{F}_{64}-$birracionalmente equivalente a curva dada por (3.3). Explicitamos este morfismo na observação a seguir.

Observação 3.7. *Considere o corpo $\mathbb{F}_{64}$. Seja C_1 a curva dada pelas equações $f_1 = f_0 = 0$ onde*

$$f_0 := y^3 + x^2t + xt^2 \text{ e } f_1 := z^3 + x^2y + xyt + t^2y.$$

Seja C_2 a curva dada pela equação $v^9 = u^3w^6 + u^6w^3$. Vamos mostrar que C_1 é o modelo não singular de C_2. Considere o morfismo $\pi : C_2 \longrightarrow \mathbb{P}^3$ dado por $\pi(u : v : w) = (g_0(u, v, w) : g_1(u, v, w) : g_2(u, v, w) : g_3(u, v, w))$ onde

$$\begin{aligned} g_0 &:= a^{21}u^5w^4 + a^{21}u^4v^3w^2 + a^{42}u^4w^5 + a^{42}u^3v^3w^3 + u^3w^6 + u^2v^3w^4 + v^9; \\ g_1 &:= u^4v^3w^2 + a^{21}u^3v^3w^3 + a^{42}u^2v^3w^4 + a^{42}v^9; \\ g_2 &:= a^{49}u^5vw^3 + a^7u^4vw^4 + a^{28}u^3vw^5; \\ g_3 &:= v^9. \end{aligned}$$

Assim

$$\begin{aligned} g_1^3 &+ g_0^2g_3 + g_0g_3^2 = v^9[u^{12}w^6 + a^{21}u^{11}w^7 + a^{42}u^{10}w^8 + u^9w^9 + a^{21}u^8w^{10} + a^{42}u^7w^{11}] \\ &+ v^{18}[a^{21}u^5w^4 + a^{42}u^4w^5 + u^3w^6] + v^{27} \\ &= (u^3w^6 + u^6w^3)[u^{12}w^6 + a^{21}u^{11}w^7 + a^{42}u^{10}w^8 + u^9w^9 + a^{21}u^8w^{10} + a^{42}u^7w^{11}] \\ &+ (u^3w^6 + u^6w^3)^2[a^{21}u^5w^4 + a^{42}u^4w^5 + u^3w^6] + (u^3w^6 + u^6w^3)^3 \\ &= 0 \qquad e \end{aligned}$$

$$\begin{aligned} g_1^4 + g_2^3g_3 &+ g_1g_3^3 = v^{12}[u^{16}w^8 + a^{21}u^{15}w^9 + a^{42}u^{14}w^{10} + u^{10}w^{14} + a^{21}u^9w^{15} + a^{42}u^8w^{16}] \\ &+ v^{30}[u^4w^2 + a^{21}u^3w^3 + a^{42}u^2w^4] \\ &= v^3(u^3w^6 + v^6w^3)[u^{16}w^8 + a^{21}u^{15}w^9 + a^{42}u^{14}w^{10} + u^{10}w^{14} + a^{21}u^9w^{15} \\ &+ a^{42}u^8w^{16}] + v^3(u^3w^6 + v^6w^3)^3[u^4w^2 + a^{21}u^3w^3 + a^{42}u^2w^4] \\ &= 0. \end{aligned}$$

Para $v \neq 0$ temos que $g_2^3 = \dfrac{g_1^4}{g_3} + g_1g_3^2 = \dfrac{g_1}{g_3}(g_0^2g_3 + g_0g_3^2) + g_1g_3^2 = g_0^2g_1 + g_0g_1g_3 + g_1g_3^2$. Para $v = 0$ temos $\pi(u : 0 : w) = (g_0 : 0 : 0 : 0) = (1 : 0 : 0 : 0 : 0)$. Logo $\pi(C_2) \subseteq C_1$. Considere agora o morfismo $\phi : C_1 \longrightarrow \mathbb{P}^2$ dado por $\phi(x : y : z : t) = (G_0(x : y : z : t) : G_1(x : y : z : t) : G_2(x : y : z : t))$ onde

$$\begin{aligned} G_0(x, y, z, t) &:= a^{21}xt^2 + a^{21}y^3 + y^2t + a^{21}t^3; \\ G_1(x, y, z, t) &:= a^{35}xzt + a^{56}yzt + a^{35}zt^2; \\ G_2(x, y, z, t) &:= y^3 + a^{42}y^2t + a^{21}yt^2; \end{aligned}$$

Usando $f_0 = f_1 = 0$ obtemos $G_1^9 + G_0^3 G_3^6 + G_0^6 G_3^3 = 0$. Portanto $\phi(C_1) \subseteq C_2$. Agora observamos que

$$\phi \circ \pi(u : v : w) \quad = \quad \phi(g_0(u,v,w) : g_1(u,v,w) : g_2(u,v,w) : g_3(u,v,w)) = (H_0 : H_1 : H_2)$$

onde $H_i := G_i(g_0(u,v,w) : g_1(u,v,w) : g_2(u,v,w) : g_3(u,v,w))$ para $i = 0, 1, 2$. Mas

$$\begin{aligned}
H_0 &= v^9[a^{21}u^{12}w^6 + a^{42}u^{11}w^7 + a^{21}u^9w^9 + u^7w^{11} + a^{21}u^6w^{12}] \\
&+ v^{18}[a^{42}u^5w^4 + u^4w^5 + a^{21}u^3w^6] \\
&= u[a^{21}u^{17}w^9 + u^{15}w^{11} + a^{21}u^{14}w^{12} + a^{42}u^{13}w^{13} + u^{12}w^{14} + a^{42}u^{10}w^{16}] \\
H_1 &= v^{10}[a^{42}u^{10}w^7 + a^{21}u^8w^9 + u^6w^{11}] + v^{19}[a^{21}u^5w^3 + a^{42}u^4w^4 + u^3w^5] \\
&= v[a^{21}u^{17}w^9 + u^{15}w^{11} + a^{21}u^{14}w^{12} + a^{42}u^{13}w^{13} + u^{12}vw^{14} + a^{42}u^{10}w^{16}] \\
H_2 &= v^9[u^{12}w^6 + a^{21}u^{11}w^7 + u^9w^9 + a^{42}u^7w^{11} + u^6w^{12}] + v^{27} \\
&= w[a^{21}u^{17}w^9 + u^{15}w^{11} + a^{21}u^{14}w^{12} + a^{42}u^{13}w^{13} + u^{12}w^{14} + a^{42}u^{10}w^{16}]
\end{aligned}$$

Portanto $\phi \circ \pi = Id$. Logo $\phi : C_1 \longrightarrow C_2$ é sobrejetora. Em particular ϕ é birracional, pois aplicando a Fórmula de Riemann-Hurwitz temos $2g(C_2) - 2 \geqslant (2g(C_1) - 2)d$ segue que $d = 1$. Portanto C_1 é o modelo não singular de C_2.

Como a classificação via Fanali-Giulietti-Platoni dos modelos dependem dos pontos $\mathbb{F}_{q^n}$-racionais da Hermitiana, citamos o resultado a seguir.

Observação 3.8. *Aplicando o Teorema 9.25 em (HIRSCHFELD; KORCHMÁROS; TORRES, 2008) para a curva Hermitiana $\mathcal{H}_2$ temos $\mathcal{H}_2(\mathbb{F}_{q^4}) \backslash \mathcal{H}_2(\mathbb{F}_{q^2}) = \varnothing$.*

3.3 Curvas maximais de gênero 9 e 10 sobre $\mathbb{F}_{64}$

Seja $\mathcal{X}$ uma curva $\mathbb{F}_{64}-$maximal com dimensão Frobenius 3 e gênero g. Já vimos que se $g = 12$ então $\mathcal{X}$ é $\mathbb{F}_{64}-$birracionalmente equivalente a curva dada por (3.1). Portanto, vamos considerar g diferente de 12, isto é $g \in \{9, 10\}$. Assim as $(\mathcal{D}, P)-$ordens num ponto P racional de $\mathcal{X}$ são

$$j_0(P) = 0 < j_1(P) = 1 < j_2(P) < j_3(P) = 9.$$

Pela Proposição 1.66, associamos estas ordens em P com o semigrupo de Weierstrass $H(P)$ temos que $j_2(P) = 9 - m_1(P)$ e $m_2(P) = 8$, $m_3(P) = 9$.

Proposição 3.9. *Seja $\mathcal{X}$ uma curva $\mathbb{F}_{64}-$maximal de gênero $g < 12$ com dimensão Frobenius 3. Então temos duas possibilidades:*

(A) $j_2(P) = 3$ para algum $P \in \mathcal{X}(\mathbb{F}_{64})$;

(B) $j_2(P) = 2$ para todo $P \in \mathcal{X}(\mathbb{F}_{64})$.

Demonstração: Pelo Teorema 2.17 segue que $\mathcal{X}$ é quase-clássica, isto é, $\varepsilon_2 = 2$. Logo pelo Lema 3.7 em (COSSIDENTE; KORCHMÁROS; TORRES, 1999) existe um ponto $P \in \mathcal{X}(\mathbb{F}_{q^2})$ tal que $j_2(P) = 2$. Vamos mostrar que se existe P ponto $\mathbb{F}_{64}-$racional de $\mathcal{X}$ tal que $j_2(P) \neq 2$ então $j_2(P) = 3$. Observamos que para tal ponto P temos $3 \leqslant j_2(P) \leqslant 8$. Como $m_2(P) = 8$ então $m_1(P) \geqslant 4$. Logo $j_2(P) \leqslant 5$. Se $j_2(P) = 5$ então $m_1(P) = 4$ e segue que $g = 12$ via Proposição 2.4 de (ABDÓN; TORRES, 1999). Uma contradição. Se $j_2(P) = 4$ então $m_1(P) = 5$ daí g é menor ou igual ao gênero do semigrupo $\langle 5, 8, 9\rangle$, o qual é igual a 8, outra contradição. ▫

Existem exemplos em que as situações (A) e (B) acontecem. A curva dada em (3.2) satisfaz o caso (B) e a curva dada por (3.3) satisfaz o caso (A). Vamos utilizar o Teorema 1.85 em cada uma das situações para curvas com gêneros 9 e 10.

Caso (A): $j_2(P) = 3$ para algum P racional

Suponha que $\mathcal{X}$ é uma curva $\mathbb{F}_{64}-$maximal de gênero $g \in \{9, 10\}$ e $j_2(P) = 3$ para algum ponto $P \in \mathcal{X}(\mathbb{F}_{64})$. Dos resultados de Fanali-Giulietti-Platoni, podemos assumir que $\mathcal{X}$ é:

- uma curva de grau 9 contida na superfície Hermitiana com equação

$$\mathcal{H}_3 : \quad Z^9 + Y^9 = X^8 + X, \qquad \text{por Corolário 1.79 ;}$$

- $P = (0 : 1 : 0 : 0) \in \mathcal{X}$, pela Observação 1.80;
- o plano osculante a $\mathcal{X}$ em P tem equação $T = 0$, (coincide com o plano tangente em P em $\mathcal{H}_3$ por Corolário 1.79);
- a reta tangente de $\mathcal{X}$ em P é a reta com equações $Y = 0, \quad T = 0$, por Lema 1.81, e
- os planos tangentes não-osculantes de $\mathcal{X}$ em P são aqueles com equação

$$Y - bT = 0, \text{ com } b \in \overline{\mathbb{F}}_{64},$$

pelo Lema 1.82.

Como $j_2(P) = 3$ então $m_P := 6$ é a primeira non-gap não nula em P e todo plano π_b com equação $Y - bT = 0$ com $b \in \overline{\mathbb{F}}_{64}$ intersecta $\mathcal{X}$ em P com multiplicidade 3. Como o grau de $\mathcal{X}$ é igual a 9, existem 6 pontos afins de $\mathcal{X}$ pertencendo aos planos π_b com $b \in \overline{\mathbb{F}}_{64}$. Vamos mostrar a existência de um plano da forma π_b tal que sua multiplicidade da interseção com a curva $\mathcal{X}$ em algum ponto distinto de P é maior do que 1.

Proposição 3.10. *Existe um plano*

$$\pi_0 : \quad Y - b_0 T = 0$$

para algum $b_0 \in \mathbb{F}_{64}$ *contendo no máximo* 5 *pontos distintos* $\mathbb{F}_{64}-$*racionais (afins) de* $\mathcal{X}$.

Demonstração: Suponha que todo plano π_b da forma $Y - bT = 0$ com $b \in \mathbb{F}_{64}$ intersecta em 6 pontos afins distintos a curva $\mathcal{X}$. Mas os planos π_b particionam o conjunto de pontos afins $\mathbb{F}_{64}-$racionais de $\mathbb{P}^3(\overline{\mathbb{F}}_{64})$ então

$$\sum_{b\in\mathbb{F}_{64}} [\pi_b \cap \mathcal{X}(\mathbb{F}_{64})] = 64 + 16g$$

o que resulta num contradição com o gênero. □

Proposição 3.11. *Suponha (A) e que o plano π_0 da Proposição 3.10 não intersecte nenhum ponto $\mathbb{F}_{64}-$racional afim de $\mathcal{X}$. Então existem $P_1, P_2 \in \mathcal{X}$ afins distintos com $deg(P_1) = deg(P_2) = 3$.*

Demonstração: Temos então a possibilidade para o divisor de interseção

i) $D = 3P+P_1+\phi_{64}(P_1)+\phi_{64}^2(P_1)+P_2+\phi_{64}(P_2)+\phi_{64}^2(P_2)$, com $deg(P_1) = deg(P_2) = 3$;

ii) $D = 3P + 2R + 2\phi_{64}(R) + 2\phi_{64}^2(R)$ com $deg(R) = 3$.

utilizando o fato da Observação 3.8. Em (ii) podemos assumir pelo Lema 1.84 que $R = (1 : \overline{X} : 0 : \overline{Z})$, onde $\overline{X}$ é a menor raiz do polinômio $T^8 + T = \overline{Z}^9$ (com respeito à ordenação $\preceq_3$) e $\omega \in \mathbb{F}_{64^3}$ elemento primitivo sobre $\mathbb{F}_{64}$.

Aplicando o Teorema 1.85 obtemos $\xi(X, Z) := \prod_{i=1}^{3}((\overline{Z}^{8^{2i}})^8(Z - \overline{Z}^{8^{2i}}) - (X - \overline{X}^{8^{2i}}))^2$, com as duas possibilidades:

(I) $\overline{Z} = \omega^2$ com $\omega \in \mathbb{F}_{64^3}$ elemento primitivo sobre $\mathbb{F}_{64}$.

(II) $\overline{Z} = \omega + \overline{Z}_2\omega^2$ com $\overline{Z}_2 \in \mathbb{F}_{64}$ e $\omega \in \mathbb{F}_{64^3}$ elemento primitivo sobre $\mathbb{F}_{64}$.

Observamos que em ambos os casos (I), (II) a curva dada por $Z^9 = X^8 + X + \lambda\xi(X, Z)$ é não singular, logo tal curva tem gênero igual a 28.

Para (i) temos a curva

$$Z^9 = X^8 - X + \lambda\xi(X, Z)\mu(X, Z) \tag{3.5}$$

onde $\xi(X, Z) := \prod_{i=1}^{3}((\overline{Z}^{8^{2i}})^8(Z - \overline{Z}^{8^{2i}}) - (X - \overline{X}^{8^{2i}}))$ satisfazendo (I) ou (II), e $\mu(X, Z) = \prod_{i=1}^{3}((z_2^{8^{2i}})^8(Z - z_2^{8^{2i}}) - (X - x_2^{8^{2i}}))$ com $x_2^8 + x_2 = z_2^9$, $x_2, z_2 \in \mathbb{F}_{64^3}$. □

Portanto o caso (A) se resume em duas possibilidades:

A1) O plano π_0 intersecta a curva em dois pontos P_1 e P_2 distintos afins não $\mathbb{F}_{64}-$racionais de $\mathcal{X}$, com $deg(P_1) = deg(P_2) = 3$.

A2) O plano π_0, intersecta em pelo menos um ponto $\mathbb{F}_{64}-$racional afim de $\mathcal{X}$ com multiplicidade maior ou igual a 2.

Algumas partições no conjunto dos pontos $\mathbb{F}_{64}-$racionais da curva Hermitiana $\mathcal{H}_2$ podem facilitar o tempo das rotinas no Magma.

Observação 3.12. *Considere a partição do conjunto* $\mathbb{F}_{64}^* := \langle a \rangle$ *a partir dos seguintes conjuntos,*

$$\begin{aligned}
B_0 &:= \{1, a^7, a^{14}, a^{21}, a^{28}, a^{35}, a^{42}, a^{49}, a^{56}\};\\
B_1 &:= \{a, a^8, a^{15}, a^{22}, a^{29}, a^{36}, a^{43}, a^{50}, a^{57}\};\\
B_2 &:= \{a^2, a^9, a^{16}, a^{23}, a^{30}, a^{37}, a^{44}, a^{51}, a^{58}\};\\
B_3 &:= \{a^3, a^{10}, a^{17}, a^{24}, a^{31}, a^{38}, a^{45}, a^{52}, a^{59}\};\\
B_4 &:= \{a^4, a^{11}, a^{18}, a^{25}, a^{32}, a^{39}, a^{46}, a^{53}, a^{60}\};\\
B_5 &:= \{a^5, a^{12}, a^{19}, a^{26}, a^{33}, a^{40}, a^{47}, a^{54}, a^{61}\};\\
B_6 &:= \{a^6, a^{13}, a^{20}, a^{27}, a^{34}, a^{41}, a^{48}, a^{55}, a^{62}\}.
\end{aligned}$$

Observamos que se $b \in B_i$ *então as raízes do polinômio* $x^8 + x - b^9$ *sobre* $\mathbb{F}_{64}$ *estão em* C_i *para* $i \in \{0, ..., 6\}$ *onde*

$$\begin{aligned}
C_0 &:= \{a^{21}, a^{31}, a^{42}, a^{47}, a^{55}, a^{59}, a^{61}, a^{62}\};\\
C_1 &:= \{a, a^5, a^7, a^8, a^{30}, a^{40}, a^{51}, a^{56}\};\\
C_2 &:= \{a^2, a^{10}, a^{14}, a^{16}, a^{17}, a^{39}, a^{49}, a^{60}\};\\
C_3 &:= \{a^6, a^{11}, a^{19}, a^{23}, a^{25}, a^{26}, a^{48}, a^{58}\};\\
C_4 &:= \{a^4, a^{15}, a^{20}, a^{28}, a^{32}, a^{34}, a^{35}, a^{57}\};\\
C_5 &:= \{a^3, a^{13}, a^{24}, a^{29}, a^{37}, a^{41}, a^{43}, a^{44}\};\\
C_6 &:= \{a^{12}, a^{22}, a^{33}, a^{38}, a^{46}, a^{50}, a^{52}, a^{53}\}.
\end{aligned}$$

Portanto um ponto $(c, b) \in \mathcal{H}_2(\mathbb{F}_{64})$ *satisfaz* $(b, c) \in B_i \times C_i$, *se* $b, c \neq 0$ *para algum* $i \in \{0, 1, 2, 3, 4, 5, 6\}$ *ou* $b = 0$ *e* $c \in J := \{0, 1, a^9, a^{18}, a^{27}, a^{36}, a^{45}, a^{54}\}$.

Observação 3.13. *Vamos explicitar as raízes do polinômio* $X^{64} + X$ *sobre o corpo* $\mathbb{F}_{64^3}$. *Denotando* $\mathbb{F}_{64^3}^* = \langle c \rangle$, *considere o conjunto* H *definido pelas raízes da equação* $X^{64} + X = 0$ *em* $\mathbb{F}_{64^3}$. *Utilizando o software Magma percebemos que* H *é formado pelos elementos* 0 *e* c^i

onde i percorre o conjunto

$$\begin{array}{llllllllll}
\{0, & 4161, & 8322, & 12483, & 16644, & 20805, & 24966, & 29127, & 33288, & 37449, \\
& 41610, & 45771, & 49932, & 54093, & 58254, & 62415, & 66576, & 70737, & 74898, \\
& 79059, & 83220, & 87381, & 91542, & 95703, & 99864, & 104025, & 108186, & 112347, \\
& 116508, & 120669, & 124830, & 128991, & 133152, & 137313, & 141474, & 145635, & 149796, \\
& 153957, & 158118, & 162279, & 166440, & 170601, & 174762, & 178923, & 183084, & 187245, \\
& 191406, & 195567, & 199728, & 203889, & 208050, & 212211, & 216372, & 220533, & 224694, \\
& 228855, & 233016, & 237177, & 241338, & 245499, & 249660, & 253821, & 257982 & \}.
\end{array}$$

Assim $\mathbb{F}_{64}$ *pode ser identificado com* H *e pode ser considerado como um subcorpo de* $\mathbb{F}_{64^3}$. *Como* $\mathbb{F}_{2^{18}}$ *é o menor subcorpo que contém* c *e* $\mathbb{F}_{2^6}$ *segue que* $\mathbb{F}_{2^{18}} = \mathbb{F}_{2^6}[c]$.

Agora vamos observar que o polinômio $X^8 + X - 1$ *tem as seguintes raízes em* $\mathbb{F}_{64^3}$ *no conjunto*

$$I := \{c^{87381}, c^{128991}, c^{174762}, c^{195567}, c^{228855}, c^{245499}, c^{253821}, c^{257982}\}. \tag{3.6}$$

Proposição 3.14. *Suponha a Condição (A2) verdadeira. Então na interseção* π *e* $\mathcal{X}$ *contém pelo menos 2 pontos* $\mathbb{F}_{64}-$*racionais afins distintos e nenhum ponto não* $\mathbb{F}_{64}-$*racional.*

Demonstração: Observamos primeiramente que não podemos ter apenas um ponto $\mathbb{F}_{64}-$racional afim R nesta interseção de $\mathcal{X}$ e π. De fato, o divisor de interseção seria da forma $3P + 6R$ e como R é um ponto $\mathbb{F}_{64}-$racional, podemos escrever $R := (1 : x : 0 : z)$ com $z^9 = x^8 + x$, e aplicar o Teorema 1.85. Logo a curva $\mathcal{X}$ é $\mathbb{F}_{64}-$birracionalmente equivalente à curva dada pela equação

$$Z^9 = X^8 + X + \lambda(z^8 Z - X + x^8)^6,$$

com $\lambda \in \mathbb{F}_{64}$. Esta curva é não singular, portanto possui gênero 28. Como o gênero de $\mathcal{X}$ é igual a $g \in \{9, 10\}$ e o gênero é um invariante birracional segue uma contradição. Se tal plano π intersectar a curva $\mathcal{X}$ em algum ponto não $\mathbb{F}_{64}-$racional então podemos aplicar o Lema 1.84. Neste caso, teríamos as seguintes possibilidades para o divisor D de interseção:

(i)

$$D = 3P + 2R + P_2 + P_3 + \phi_{64}(P_3) + \phi_{64}^2(P_3) \tag{3.7}$$

com $P_2 \in \mathcal{X}(\mathbb{F}_{64})$ e $P_3 \notin \mathcal{X}(\mathbb{F}_{64})$ com $deg(P_3) = 3$;

(ii)

$$D = 3P + 3R + P_3 + \phi_{64}(P_3) + \phi_{64}^2(P_3) \tag{3.8}$$

com $P_3 \notin \mathcal{X}(\mathbb{F}_{64})$ e $deg(P_3) = 3$.

Com o suporte do Magma, iremos observar que (i) e (ii) não podem acontecer. Se temos (3.7) poderemos assumir que $P_3 = (1 : \overline{X} : 0 : \overline{Z})$ como no Lema 1.84 com $\omega = c$ (ver Observação 3.13). Daí $\overline{X}$ é a menor raiz do polinômio $T^8 + T = \overline{Z}^9$ com respeito à ordenação $\preceq_3$. Utilizando o Magma, observamos que o polinômio $T^8 + T - \overline{Z}^9$ não temos raízes sobre $\mathbb{F}_{64^3}$ quando $\overline{Z} = \omega^2$. Portanto

$$\overline{Z} = \omega + \overline{Z}_2\omega^2 \text{ com } \overline{Z}_2 \in \mathbb{F}_{64}. \tag{3.9}$$

Note que o polinômio $T^8 + T - (\omega + \overline{Z}_2\omega^2)^9$ apenas temos raízes sobre $\mathbb{F}_{64^3}$ quando

$$\overline{Z}_2 \in \{c^{58254}, c^{66576}, c^{79059}, c^{91542}, c^{99864}, c^{174762}, c^{178923}, c^{241338}, c^{245499}\}. \tag{3.10}$$

Pelo Lema 1.83, podemos assumir uma das duas possibilidades:

(a) $\xi(X, Z) = X^2 L_2(X, Z) \cdot \overline{\xi}(X, Z)$,

(b) $\xi(X, Z) = X L_2(X, Z)^2 \cdot \overline{\xi}(X, Z)$,

onde $L_2(X, Z) = X + 1$ ou $L_2(X, Z) = Z - X + B - 1$ e $\overline{\xi}(X, Z)$ sendo igual a

$$((\omega + \overline{Z}_2\omega^2)^{2^9} Z - X - \overline{X}^{2^9})((\omega + \overline{Z}_2\omega^2)^{2^{15}} Z - X - \overline{X}^{2^{15}})((\omega + \overline{Z}_2\omega^2)^8 Z - X - \overline{X}^8) \tag{3.11}$$

satisfazendo $\overline{X}^8 + \overline{X} = \overline{Z}^9$ e $B \in I$ como em (3.6). Supondo (a) temos os gêneros $26, 27, 28$. Supondo (b) e $L_2(X, Z) = X + Z + 1 - B$ temos os gêneros $25, 26, 27, 28$. Suponha (b) e $L_2(X, Z) = X + 1$ temos os gêneros $26, 27, 28$.

Supondo (3.8), podemos assumir que $R = (1 : 0 : 0 : 0)$ então teremos $\xi(X, Z) = X^3 \cdot \overline{\xi}(X, Z)$ com $\overline{\xi}(X, Z)$ como em (3.11). Utilizando o Magma as possíveis curvas singulares tem gêneros 26 e 27. ▫

Desta forma o caso (A2) se resume em analisar as possíveis interseções da curva $\mathcal{X}$ com o plano π que contém apenas pontos $\mathbb{F}_{64}-$racionais. Então existem pelo menos 2 e no máximo 5 pontos $\mathbb{F}_{64}-$racionais afins distintos e diferentes de P. Sejam P_i, $i = 1, 2, 3, 4, 5$ tais pontos. Podemos supor $P_1 = (1 : 0 : 0 : 0)$ e $P_2 = (1 : 1 : 0 : 0)$ ou $P_2 = (1 : B : 0 : 1)$ satisfazendo $B^8 + B = 1$. Então supondo (A2) temos dos resultados de Fanali-Giulietti-Platoni que a curva $\mathcal{X}$ é $\mathbb{F}_{64}-$birracionalmente equivalente a curva dada pela equação plana

$$Z^9 = X^8 + X + \lambda\xi(X, Z),$$

com

$$\xi(X, Z) = X^{m_1} L_2(X, Z)^{m_2} L_3(X, Z)^{m_3} \cdots L_t(X, Z)^{m_t} \tag{3.12}$$

onde $L_2(X, Z) = X + 1$ ou $L_2(X, Z) = X + Z + 1 - B$, $\lambda \in \mathbb{F}_{64}^*$ e com $3 \leqslant t \leqslant 5$, $m_1 \geqslant 1$, $m_2 \geqslant 1$, $m_i \geqslant 0$, $m_3 + ... + m_t = 4$, $L_i(X, Z) := z_i^8(Z - z_i) - (X - x_i)$, com

$x_i, z_i \in \mathbb{F}_{64}$ satisfazendo $x_i^8 + x_i = z_i^9$ para $i = 3, ..., t$. Observamos que existe o ponto R na interseção entre a curva $\mathcal{X}$ e o plano π com multiplicidade maior ou igual a 2. Logo existe $j \in \{1, 2, 3, ..., t\}$ tal que $m_j \geqslant 2$. Vamos analisar a quantidade máxima de pontos $\mathbb{F}_{64}-$racionais que podem aparecer nesta interseção $\mathcal{X} \cap \pi$.

Teorema 3.15. *Seja* $\mathcal{X}$ *uma curva* $\mathbb{F}_{64}-$*maximal com dimensão Frobenius igual a* 3*, com* $g \in \{9, 10\}$*. Suponha que a condição (A2) é válida. Então* $\mathcal{X}$ *tem gênero* 10 *e é* $\mathbb{F}_{64}-$*birracionalmente equivalente a curva dada em (3.3).*

Demonstração: Suponha que a interseção de $\mathcal{X}$ com π tem exatamente 5 pontos $\mathbb{F}_{64}-$racionais afins, então a curva $\mathcal{X}$ é isomorfa a curva dada pela equação $Z^9 = X^8 + X + \lambda\xi(X, Z)$ com $\lambda \in \mathbb{F}_{64}^*$ e $\xi(X, Z)$ como a seguir

a') $\xi(X, Z) = X^2 L_2(X, Z)L_3(X, Z)L_4(X, Z)L_5(X, Z)$;

b') $\xi(X, Z) = XL_2(X, Z)L_3(X, Z)^2 L_4(X, Z)L_5(X, Z)$;

c') $\xi(X, Z) = XL_2(X, Z)^2 L_3(X, Z)L_4(X, Z)L_5(X, Z)$;

com $L_i(X, Z) \neq L_j(X, Z)$ para $i \neq j$ e $L_i(X, Z) \neq X$ para $i \in \{2, 3, 4, 5\}$.

Novamente utilizamos o Magma nos casos (a'), (b') e (c'), verificamos que não ocorre nenhuma curva neste formato de gênero igual a 9 e nem 10. Logo a interseção de $\mathcal{X}$ com π tem no máximo 4 pontos $\mathbb{F}_{64}-$racionais afins então em (3.12) podemos supor $t = 4$. Sem perda de generalidade suponha $m_3 \geqslant 2$. Admita que $m_3 \geqslant 2$. Se $R = P_1$ então podemos escrever

$$\xi(X, Z) = X^2 L_2(X, Z)L_3(X, Z)^2 L_4(X, Z).$$

Se $R = P_2$ então podemos escrever $\xi(X, Z) = XL_2(X, Z)^2 L_3(X, Z)^2 L_4(X, Z)$. Se $R \notin \{P_1, P_2\}$ então temos as possibilidades:

a) $\xi(X, Z) = XL_2(X, Z)L_3(X, Z)^2 L_4(X, Z)^2$;

b) $\xi(X, Z) = XL_2(X, Z)L_3(X, Z)^3 L_4(X, Z)$;

c) $\xi(X, Z) = XL_2(X, Z)^2 L_3(X, Z)^2 L_4(X, Z)$;

d) $\xi(X, Z) = X^2 L_2(X, Z)L_3(X, Z)^2 L_4(X, Z)$.

Se $m_1 \geqslant 2$ ou $m_2 \geqslant 2$ então teremos os casos anteriores e só falta analisar quando

e) $\xi(X, Z) = X^2 L_2(X, Z)^2 L_3(X, Z)L_4(X, Z)$.

Pelas hipóteses segue que a curva $\mathcal{X}$ é isomorfa a curva dada pela equação $Z^9 = X^8 + X + \lambda\xi(X,Z)$ com $\lambda \in \mathbb{F}_{64}^*$ e $\xi(X,Z)$ como nos casos (a), (b), (c), (d) e (e) citados anteriormente. Utilizando o software Magma, com cálculos exaustivos, verificamos que não ocorre nenhuma curva de gênero igual a 9. Para gênero igual a 10 ocorre apenas quando $L_2(X,Z) = X + 1$ (em todas equações citadas, exceto na equação (b)) e temos apenas uma única curva, a qual é dada por

$$Z^9 = X^8 + X + X^3(X+1)^3 = X^8 + X^6 + X^5 + X^4 + X^3 + X.$$

Esta curva é $\mathbb{F}_{64}-$maximal e isomorfa a curva dada em (3.3). ▫

Damos uma classificação para as curvas $\mathbb{F}_{64}-$maximais satisfazendo a hipótese (A). Para um refinamento deste resultado é necessário um grande gasto computacional. Observamos que quanto mais pontos temos na interseção com algum plano racional, mais gastos computacionais são requisitados.

Teorema 3.16. *Seja $\mathcal{X}$ uma curva $\mathbb{F}_{64}-$maximal com Frobenius dimensão 3 com $g \in \{9,10\}$. Se existe P ponto $\mathbb{F}_{64}-$racional de $\mathcal{X}$ tal que $j_2(P) = 3$ então $\mathcal{X}$ é $\mathbb{F}_{64}-$birracionalmente equivalente a curva (3.3) ou a curva dada pelo modelo (3.5).*

Escrevendo $\mathbb{F}_{64^3}^* = \langle c \rangle$, observamos que o modelo (3.5) pode ser escrito usando parte da demonstração da Proposição 3.14, isto é,

$$Z^9 = X^8 + X + \lambda\xi(X,Z)\mu(X,Z)$$

onde $\lambda \in \mathbb{F}_{64}^*$, $\xi(X,Z) = ((c+\overline{Z}_2c^2)^{2^9}Z - X - \overline{X}^{2^9})((c+\overline{Z}_2c^2)^{2^{15}}Z - X - \overline{X}^{2^{15}})((\omega+\overline{Z}_2c^2)^8Z - X - \overline{X}^8)$ com $\overline{X}$ sendo a menor raiz em $\mathbb{F}_{64^3}$ do polinômio $T^8 + T - (c+\overline{Z}_2c^2)^9$ e

$$\overline{Z}_2 \in \{c^{58254}, c^{66576}, c^{79059}, c^{91542}, c^{99864}, c^{174762}, c^{178923}, c^{241338}, c^{245499}\}.$$

Caso (B): $j_2(P) = 2$ para todo P racional

Seja $\mathcal{X}$ uma curva $\mathbb{F}_{64}-$maximal de gênero $g \in \{9,10\}$ tal que a condição (B) é válida. Neste caso a primeira non-gap não nula $m_P = 7$ e todo plano π_b com equação $Y - bT = 0$ com $b \in \overline{\mathbb{F}}_{64}$ intersecta $\mathcal{X}$ em P com multiplicidade 2. Como o grau de $\mathcal{X}$ é 9, existem no máximo 7 pontos afins de $\mathcal{X}$ pertencendo a π_b. Assim o divisor de interseção entre $\mathcal{X}$ e π_b é da forma

$$2P + m_1P_1 + m_2P_2 + ... + m_7P_7.$$

Proposição 3.17. *Seja $\mathcal{X}$ uma curva $\mathbb{F}_{64}-$maximal de gênero $g \in \{9,10\}$ tal que $j_2(P) = 2$ para todo P ponto $\mathbb{F}_{64}-$racional de $\mathcal{X}$. Então existe plano $\pi_0 : \quad Y - b_0T = 0$ para algum $b_0 \in \mathbb{F}_{64}$ contendo um ponto $R \in \mathcal{X}$ de grau $deg(R) \geqslant 3$.*

Demonstração: Podemos assumir que $\mathcal{X}$ é uma curva de grau 9 contida na superfície Hermitiana com equação afim $Z^9+Y^9 = X^8+X$, $P = (0:1:0:0) \in \mathcal{X}$, o plano osculante a $\mathcal{X}$ em P tem equação $T = 0$, a reta tangente a $\mathcal{X}$ em P é a reta com equação $Y = 0, T = 0$, e os planos tangentes não osculantes a $\mathcal{X}$ em P são aqueles cuja equação é da forma

$$Y - bT = 0, \quad b \in \overline{\mathbb{F}}_{64}.$$

Suponha que todo plano racional $\pi : Y - bT = 0$ com $b \in \mathbb{F}_{64}$ intersecta a curva $\mathcal{X}$ em mais do que 3 pontos $\mathbb{F}_{64}-$racionais afins. Então

$$64 + 16g = \#[\mathcal{X}(\mathbb{F}_{64})\backslash\{P\}] = \sum_{b\in\mathbb{F}_{64}} \#(\mathcal{X}(\mathbb{F}_{64}) \cap \{Y - bT = 0\}) \geqslant 4 \cdot 64 = 256$$

um absurdo. Logo existe $b_0 \in \mathbb{F}_{64}$ tal que $\#(\mathcal{X}(\mathbb{F}_{64}) \cap \{Y - b_0T = 0\}) \leqslant 3$. Vamos mostrar que existe plano π_0 não contém nenhum ponto $\mathbb{F}_{64}-$racional afim de $\mathcal{X}$. Se $\#(\mathcal{X}(\mathbb{F}_{64}) \cap \pi_0) = 1$ então a curva $\mathcal{X}$ é uma $\mathbb{F}_{64}-$birracionalmente equivalente a curva dada pela equação

$$Z^9 = X^8 + X + \lambda X^7$$

com $\lambda \in \mathbb{F}_{64}$. Tal curva é não singular e portanto possui gênero 28. Contradizendo que $g \in \{9, 10\}$. Suponha que temos apenas dois pontos $\mathbb{F}_{64}-$racionais afins distintos nesta interseção. Logo temos que $\mathcal{X}$ é $\mathbb{F}_{64}-$birracionalmente equivalente a curva dada por

$$Z^9 = X^8 + X + \lambda X^{m_1} L_2(X, Z)^{m_2} \tag{3.13}$$

onde $m_1, m_2 \in \mathbb{N}$ com $m_1+m_2 = 7$, $\lambda \in \mathbb{F}_{64}$, $L_2(X, Z) = X+1$ ou $L_2(X, Z) = X+Z+1-B$, com $B^8 + B = 1$. Na terceira opção, teríamos $\mathcal{X}$ é $\mathbb{F}_{64}-$birracionalmente equivalente a curva dada por

$$Z^9 = X^8 + X + \lambda X^{m_1} L_2(X, Z)^{m_2} (b^8Z - X - c^8)^{m_3} \tag{3.14}$$

onde $m_1, m_2, m_3 \in \mathbb{N}$ com $m_1 + m_2 + m_3 = 7$, $\lambda \in \mathbb{F}_{64}$, $L_2(X, Z) = X + 1$ ou $L_2(X, Z) = X + Z + 1 - B$ e $b \in \mathbb{F}_{64}\backslash\{0, 1\}$, $c \in \mathbb{F}_{64}\backslash\{0, B\}$ satisfazendo $c^8 + c = b^9$. Usando o software Magma verificamos que não ocorrem os gêneros 9 e nem a 10 para este modelo de curva (3.13) e (3.14). Portanto existe $R \in \pi_0$ e $R \notin \mathcal{X}(\mathbb{F}_{64})$ tal que $deg(R) := r \geqslant 3$. ▫

Segue da Proposição 3.17 que existe $R \in \pi_0$ e $R \notin \mathcal{X}(\mathbb{F}_{64})$ tal que $deg(R) := r \geqslant 3$. O divisor de interseção entre o plano π_0 e $\mathcal{X}$ é da forma

$$2P + P_1 + \phi(P_1) + \phi^2(P_1) + P_2 + \phi(P_2) + \phi^2(P_2) + \phi^3(P_2)$$

com $deg(P_1) = 3$ e $deg(P_2) = 4$. Sabemos que o modelo conhecido de gênero 9 dado em (3.2) satisfaz a hipótese (B). Muitos cálculos computacionais foram realizados neste caso e em nenhum deles apareceram exemplos de curvas de gênero 10 e as curvas de gênero 9

obtidas são $\mathbb{F}_{64}-$birracionalmente equivalentes ao modelo (3.2). Um objetivo de trabalhos futuros é terminar toda a classificação para curvas $\mathbb{F}_{64}-$maximais com dimensão Frobenius 3. Com isto também poderíamos afirmar se existem modelos não Galois-cobertos pela curva Hermitiana $\mathcal{H}_2$ com dimensão Frobenius 3 sobre o corpo $\mathbb{F}_{64}$.

Referências

ABDÓN, M.; TORRES, F. On maximal curves in characteristic two. *Manuscr. Math.*, Springer, Berlin/Heidelberg, v. 99, n. 1, p. 39–53, 1999. ISSN 0025-2611. Citado 2 vezes nas páginas 57 e 79.

_____. On F_{q^2}-maximal curves of genus $\frac{1}{6}(q-3)q$. *Beitr. Algebra Geom.*, Springer, Berlin/Heidelberg, v. 46, n. 1, p. 241–260, 2005. ISSN 0138-4821. Citado na página 62.

ARAKELIAN, N.; TAFAZOLIAN, S.; TORRES, F. On the spectrum for the genera of maximal curves over small fields. *Adv. Math. Commun.*, American Institute of Mathematical Sciences (AIMS), Springfield, MO; Shandong University, Jinan, v. 12, n. 1, p. 143–149, 2018. ISSN 1930-5346. Citado 5 vezes nas páginas 12, 13, 45, 62 e 74.

BARTOLI, D.; MONTANUCCI, M.; TORRES, F. $\mathbb{F}_{p^2}-$maximal curves with many automorphisms are galois-covered by the hermitian curve. *preprint*, 2010. Citado na página 58.

BOSMA, W.; CANNON, J.; PLAYOUST, C. The Magma algebra system. I: The user language. *J. Symb. Comput.*, Elsevier (Academic Press), London, v. 24, n. 3-4, p. 235–265, 1997. ISSN 0747-7171. Citado na página 74.

COSSIDENTE, A.; KORCHMÁROS, G.; TORRES, F. On curves covered by the Hermitian curve. *J. Algebra*, Elsevier (Academic Press), San Diego, CA, v. 216, n. 1, p. 56–76, 1999. ISSN 0021-8693. Citado 3 vezes nas páginas 60, 76 e 79.

_____. Curves of large genus covered by the Hermitian curve. *Commun. Algebra*, Taylor & Francis, Philadelphia, PA, v. 28, n. 10, p. 4707–4728, 2000. ISSN 0092-7872. Citado 2 vezes nas páginas 75 e 76.

DUURSMA, I.; MAK, K.-H. On maximal curves which are not Galois subcovers of the Hermitian curve. *Bull. Braz. Math. Soc. (N.S.)*, Springer, Berlin/Heidelberg; Sociedade Brasileira de Matemática, Rio de Janeiro, v. 43, n. 3, p. 453–465, 2012. ISSN 1678-7544. Citado na página 43.

FANALI, S.; GIULIETTI, M. On maximal curves with Frobenius dimension 3. *Des. Codes Cryptography*, Springer US, New York, NY, v. 53, n. 3, p. 165–174, 2009. ISSN 0925-1022. Citado 4 vezes nas páginas 13, 48, 54 e 74.

_____. On some open problems on maximal curves. *Des. Codes Cryptography*, Springer US, New York, NY, v. 56, n. 2-3, p. 131–139, 2010. ISSN 0925-1022. Citado na página 57.

FANALI, S.; GIULIETTI, M.; PLATONI, I. On maximal curves over finite fields of small order. *Adv. Math. Commun.*, American Institute of Mathematical Sciences (AIMS), Springfield, MO; Shandong University, Jinan, v. 6, n. 1, p. 107–120, 2012. ISSN 1930-5346. Citado 10 vezes nas páginas 13, 47, 48, 49, 50, 51, 52, 53, 62 e 74.

FUHRMANN, R.; GARCIA, A.; TORRES, F. On maximal curves. *J. Number Theory*, Elsevier (Academic Press), San Diego, CA, v. 67, n. 1, p. 29–51, 1997. ISSN 0022-314X. Citado 4 vezes nas páginas 13, 42, 55 e 57.

FUHRMANN, R.; TORRES, F. The genus of curves over finite fields with many rational points. *Manuscr. Math.*, Springer, Berlin/Heidelberg, v. 89, n. 1, p. 103–106, 1996. ISSN 0025-2611. Citado 4 vezes nas páginas 12, 40, 41 e 56.

GIULIETTI, M.; KORCHMÁROS, G. A new family of maximal curves over a finite field. *Math. Ann.*, Springer, Berlin/Heidelberg, v. 343, n. 1, p. 229–245, 2009. ISSN 0025-5831. Citado 3 vezes nas páginas 43, 76 e 77.

GIULIETTI, M.; MONTANUCCI, M.; ZINI, G. On maximal curves that are not quotients of the Hermitian curve. *Finite Fields Appl.*, Elsevier (Academic Press), San Diego, CA, v. 41, p. 72–88, 2016. ISSN 1071-5797. Citado na página 43.

GOPPA, V. D. Algebraico-geometric codes. *Math. USSR, Izv.*, American Mathematical Society (AMS), Providence, RI, v. 21, p. 75–91, 1983. ISSN 0025-5726. Citado na página 34.

HIRSCHFELD, J. W. P.; KORCHMÁROS, G.; TORRES, F. Algebraic curves over a finite field. *Princeton Ser. Appl. Math.*, Princeton, NJ: Princeton University Press, p. xx + 696, 2008. Citado 10 vezes nas páginas 11, 25, 30, 35, 36, 39, 47, 59, 66 e 78.

HURT, N. E. Many rational points. Coding theory and algebraic geometry. *Math. Appl., Dordr.*, Dordrecht: Kluwer Academic Publishers, v. 564, p. xxii + 346, 2003. ISSN 0921-3791. Citado na página 11.

IHARA, Y. Some remarks on the number of rational points of algebraic curves over finite fields. *J. Fac. Sci., Univ. Tokyo, Sect. I A*, University of Tokyo, Tokyo, v. 28, p. 721–724, 1981. ISSN 0040-8980. Citado 2 vezes nas páginas 11 e 37.

KORCHMÁROS, G.; TORRES, F. Embedding of a maximal curve in a Hermitian variety. *Compos. Math.*, Cambridge University Press, Cambridge; London Mathematical Society, London, v. 128, n. 1, p. 95–113, 2001. ISSN 0010-437X. Citado na página 13.

_____. On the genus of a maximal curve. *Math. Ann.*, Springer, Berlin/Heidelberg, v. 323, n. 3, p. 589–608, 2002. ISSN 0025-5831. Citado 3 vezes nas páginas 12, 42 e 44.

KUDO, M.; HARASHITA, S. Superspecial curves of genus 4 in small characteristic. *Finite Fields Appl.*, Elsevier (Academic Press), San Diego, CA, v. 45, p. 131–169, 2017. ISSN 1071-5797. Citado 2 vezes nas páginas 65 e 74.

MONTANUCCI, M.; ZINI, G. On the spectrum of genera of quotients of the Hermitian curve. *Commun. Algebra*, Taylor & Francis, Philadelphia, PA, v. 46, n. 11, p. 4739–4776, 2018. ISSN 0092-7872. Citado 2 vezes nas páginas 12 e 47.

MUMFORD, D.; FOGARTY, J.; KIRWAN, F. Geometric invariant theory. *Ergeb. Math. Grenzgeb., 3. Folge*, Berlin: Springer-Verlag, v. 34, p. 320, 1993. ISSN 0071-1136. Citado na página 37.

RÜCK, H.-G.; STICHTENOTH, H. A characterization of Hermitian function fields over finite fields. *J. Reine Angew. Math.*, De Gruyter, Berlin, v. 457, p. 185–188, 1994. ISSN 0075-4102. Citado 4 vezes nas páginas 12, 37, 38 e 39.

STICHTENOTH, H. Algebraic function fields and codes. *Grad. Texts Math.*, Berlin: Springer, v. 254, p. xiii + 355, 2009. ISSN 0072-5285. Citado 6 vezes nas páginas 11, 14, 16, 17, 34 e 66.

STÖHR, K.-O.; VOLOCH, J. F. Weierstrass points and curves over finite fields. *Proc. Lond. Math. Soc. (3)*, John Wiley & Sons, Chichester; London Mathematical Society, London, v. 52, p. 1–19, 1986. ISSN 0024-6115. Citado 2 vezes nas páginas 12 e 34.

TAFAZOLIAN, S.; TEHERÁN-HERRERA, A.; TORRES, F. Further examples of maximal curves which cannot be covered by the Hermitian curve. *J. Pure Appl. Algebra*, Elsevier (North-Holland), Amsterdam, v. 220, n. 3, p. 1122–1132, 2016. ISSN 0022-4049. Citado 2 vezes nas páginas 44 e 58.

TATE, J. Endomorphisms of Abelian varieties over finite fields. *Invent. Math.*, Springer, Berlin/Heidelberg, v. 2, p. 134–144, 1966. ISSN 0020-9910. Citado 2 vezes nas páginas 37 e 38.

VIANA, P. *Classicality of trigonal curves of genus five*. 1989. Computers and mathematics, Proc. Conf., Cambridge/Mass. 1989, 60-65 (1989). Citado na página 66.

XING, C.; STICHTENOTH, H. The genus of maximal function fields over finite fields. *Manuscr. Math.*, Springer, Berlin/Heidelberg, v. 86, n. 2, p. 217–224, 1995. ISSN 0025-2611. Citado na página 40.