WALTEIR DE PAULA FERREIRA

Um estudo sobre o número máximo de pontos $\mathbb{F}_q$ - racionais em uma hipersuperfície de $\mathbb{P}^n$

UNIVERSIDADE FEDERAL DE UBERLÂNDIA
FACULDADE DE MATEMÁTICA
2021

WALTEIR DE PAULA FERREIRA

Um estudo sobre o número máximo de pontos $\mathbb{F}_q$ - racionais em uma hipersuperfície de $\mathbb{P}^n$

Dissertação apresentada ao Programa de Pós-Graduação em Matemática da Universidade Federal de Uberlândia, como parte dos requisitos para obtenção do título de **MESTRE EM MATEMÁTICA.**

Área de Concentração: Matemática.
Linha de Pesquisa: Geometria Algébrica.

Orientador: Prof. Dr. Victor Gonzalo Lopez Neumann.

UBERLÂNDIA - MG
2021

Ficha Catalográfica Online do Sistema de Bibliotecas da UFU
com dados informados pelo(a) próprio(a) autor(a).

F383 2021

Ferreira, Walteir de Paula, 1997-
Um estudo sobre o número máximo de pontos F_q - racionais em uma hipersuperfície de P^n [recurso eletrônico] / Walteir de Paula Ferreira. - 2021.

Orientador: Victor Gonzalo Lopez Neumann.
Dissertação (Mestrado) - Universidade Federal de Uberlândia, Pós-graduação em Matemática.
Modo de acesso: Internet.
Disponível em: http://doi.org/10.14393/ufu.di.2021.56
Inclui bibliografia.

1. Matemática. I. Neumann, Victor Gonzalo Lopez,1974-, (Orient.). II. Universidade Federal de Uberlândia. Pós-graduação em Matemática. III. Título.

CDU: 51

Bibliotecários responsáveis pela estrutura de acordo com o AACR2:

Gizele Cristine Nunes do Couto - CRB6/2091

UNIVERSIDADE FEDERAL DE UBERLÂNDIA
Coordenação do Programa de Pós-Graduação em Matemática
Av. João Naves de Ávila, 2121, Bloco 1F, Sala 1F 160 - Bairro Santa Mônica, Uberlândia-MG, CEP 38400-902
Telefone: (34) 3239-4209/4154 - www.posgrad.famat.ufu.br - pgmat@famat.ufu.br

ATA DE DEFESA - PÓS-GRADUAÇÃO

Programa de Pós-Graduação em:	Matemática				
Defesa de:	Dissertação de Mestrado Acadêmico, nº 90, PPGMAT				
Data:	18 de fevereiro de 2021	Hora de início:	10:00	Hora de encerramento:	11:30
Matrícula do Discente:	11912MAT010				
Nome do Discente:	Walteir de Paula Ferreira				
Título do Trabalho:	Um estudo sobre o número máximo de pontos F_q-racionais em uma hipersuperfície de P^n				
Área de concentração:	Matemática				
Linha de pesquisa:	Geometria Algébrica				
Projeto de Pesquisa de vinculação:	Códigos cartesianos afins				

Reuniu-se em web conferência pela plataforma Mconf-RNP, em conformidade com a PORTARIA Nº 36, DE 19 DE MARÇO DE 2020 da COORDENAÇÃO DE APERFEIÇOAMENTO DE PESSOAL DE NÍVEL SUPERIOR - CAPES, pela Universidade Federal de Uberlândia, a Banca Examinadora, designada pelo Colegiado do Programa de Pós-graduação em Matemática, assim composta: Professores Doutores: Herivelto Martins Borges Filho - ICMC/USP; Cícero Fernandes de Carvalho - FAMAT/UFU e Victor Gonzalo Lopez Neumann - FAMAT/UFU orientador do candidato.

Iniciando os trabalhos o presidente da mesa, Dr. Victor Gonzalo Lopez Neumann, apresentou a Comissão Examinadora e o candidato, agradeceu a presença do público, e concedeu ao Discente a palavra para a exposição do seu trabalho. A duração da apresentação do Discente e o tempo de arguição e resposta foram conforme as normas do Programa.

A seguir o senhor(a) presidente concedeu a palavra, pela ordem sucessivamente, aos(às) examinadores(as), que passaram a arguir o(a) candidato(a). Ultimada a arguição, que se desenvolveu dentro dos termos regimentais, a Banca, em sessão secreta, atribuiu o resultado final, considerando o(a) candidato(a):

Aprovado.

Esta defesa faz parte dos requisitos necessários à obtenção do título de Mestre.

O competente diploma será expedido após cumprimento dos demais requisitos, conforme as normas do Programa, a legislação pertinente e a regulamentação interna da UFU.

Nada mais havendo a tratar foram encerrados os trabalhos. Foi lavrada a presente ata que após lida e achada conforme foi assinada pela Banca Examinadora.

Documento assinado eletronicamente por **Herivelto Martins Borges Filho**, **Usuário Externo**, em 18/02/2021, às 11:29, conforme horário oficial de Brasília, com fundamento no art. 6º, § 1º, do Decreto nº 8.539, de 8 de outubro de 2015.

Documento assinado eletronicamente por **Victor Gonzalo Lopez Neumann**, **Professor(a) do Magistério Superior**, em 18/02/2021, às 11:46, conforme horário oficial de Brasília, com fundamento no art. 6º, § 1º, do Decreto nº 8.539, de 8 de outubro de 2015.

Documento assinado eletronicamente por **Cícero Fernandes de Carvalho**, **Professor(a) do Magistério Superior**, em 18/02/2021, às 13:09, conforme horário oficial de Brasília, com fundamento no art. 6º, § 1º, do Decreto nº 8.539, de 8 de outubro de 2015.

A autenticidade deste documento pode ser conferida no site https://www.sei.ufu.br/sei/controlador_externo.php?acao=documento_conferir&id_orgao_acesso_externo=0, informando o código verificador **2512378** e o código CRC **3D45CEEB**.

Dedicatória

Dedico este trabalho a todos os jovens (de corpo ou de alma) que apesar de todas as dificuldades jamais desistiram dos seus sonhos.

Agradecimentos

Agradeço, imensamente, a orientação impecável do professor Victor Gonzalo Lopez Neumann por trazer luz nos dias de escuridão. Agradeço também todos aqueles que contribuíram de forma direta ou indireta com minha formação, em especial, agradeço aos nobres colegas Paulo Victor, Fernando Augusto, Heyssen Billy, João Paulo, Juan Estuardo, Mariana Rosas, Pedro Manuel e Wendy Díaz, por tornarem essa caminhada tão prazerosa.

Por fim, não menos importante, agradeço à CAPES pelo aporte financeiro nesses dois anos de mestrado, que tornou possível a realização deste sonho.

FERREIRA, W. P. *Um estudo sobre o número máximo de pontos $\mathbb{F}_q$ - racionais em uma hipersuperfície de $\mathbb{P}^n$*. 2021. 58+x p. Dissertação de Mestrado, Universidade Federal de Uberlândia, Uberlândia-MG.

Resumo

Neste trabalho, realizamos um estudo sobre o número máximo de pontos $\mathbb{F}_q$ - racionais em uma hipersuperfície de $\mathbb{P}^n$. Como alguns exemplos peculiares acontecem no contexto geral, hipersuperfícies de grau $d \geq q$ que se anulam em todos os pontos $\mathbb{F}_q$ - racionais, nos parece razoável analisar separadamente o caso de hipersuperfícies não singulares de grau d. Contudo, isso torna o problema bem mais complicado. Para o caso $n = 2$ enunciamos o teorema de Hasse-Weil. Finalizamos o trabalho apresentando a resposta, recentemente, apresentada por Mrinmoy Datta em [9] para o caso $n = 4$ e sobre algumas condições para d.

Palavras-chaves: Espaço projetivo, Hipersuperfícies, Pontos $\mathbb{F}_q$ - racionais.

FERREIRA, W. P. *A study on the maximum number of* $\mathbb{F}_q$ *- rational points on a hypersurface of* $\mathbb{P}^n$. 2021. 58+x p. M. Sc. Dissertation, Federal University of Uberlândia, Uberlândia-MG.

Abstract

In this work, we study the maximum number of $\mathbb{F}_q$-rational points on a hypersurface of $\mathbb{P}^n$. Given that some particular examples occur on general context, hypersurfaces of degree $d \geq q$ that vanish on all $\mathbb{F}_q$-rational points, it seems reasonable to analyze separately the case of non-singular hypersurfaces of degree d, but it makes our problem much more difficult. For the case $n = 2$, we present the well-known Hasse-Weil Theorem. We finish the work presenting the answer given, recently, by Mrinmoy Datta at [9] for the case $n = 4$ and under some restrictions on d.

Keywords: projective space, hypersurfaces, $\mathbb{F}_q$-rational points

Sumário

Introdução

O estudo de raízes de um polinômio vem intrigando matemáticos desde os primórdios. Nas séries iniciais do ensino fundamental II são apresentados os primeiros problemas envolvendo equações polinomiais com uma variável de grau 1 sobre o corpo dos números reais, que com simples manipulações algébricas obtemos as soluções:

$$aX + b = 0 \text{ com } a \neq 0 \Rightarrow X = -ba^{-1}. \tag{1}$$

Posteriormente, já no final do ensino fundamental II, aprendemos sobre equações de grau 2, momento que é ensinada a "amada" fórmula para resolver equações quádricas (Bhaskara):

$$aX^2 + bX + c = 0 \text{ com } a \neq 0 \Rightarrow X = \frac{-b \pm \sqrt{b^2 - 4ac}}{2a}. \tag{2}$$

Em um nível mais avançado, alguns têm a oportunidade de estudar a teoria de Galois, na qual uma das aplicações nos mostra a impossibilidade de obter uma fórmula envolvendo apenas as operações básicas que nos descreve as soluções para equações de grau maior ou igual a 5 partindo dos coeficientes. Determinar com exatidão quem são as raízes de um polinômio, como as equações (1) e (2) nos fornecem, não é uma tarefa nada fácil. Desse modo, não estamos interessados em determinar quem são as raízes do polinômio, mas estudar qual é o número máximo de raízes que polinômios de grau de d com n variáveis com coeficiente em um corpo finito possuem, considerando também alguns *zeros especiais* (no infinito).

Uma maneira de realizar o estudo de raízes de um polinômio de n variáveis com coeficientes em um corpo é por meio de uma relação entre álgebra abstrata (mais especificamente álgebra comutativa) e geometria, subárea da matemática conhecida como geometria algébrica clássica. Desse modo, no primeiro capítulo abordamos brevemente o conceito de variedades afins e apresentamos o enunciado de alguns resultados quando o corpo base é algebricamente fechado, tendo como principal referência o livro [1]. Esses resultados justificam, parcialmente, o motivo de sempre considerarmos, a menos que seja mencionado o contrário, um corpo que seja algebricamente fechado e, assim, estaremos também considerando as raízes do polinômio no fecho algébrico. Além dos pontos no fecho algébrico, algumas experiências nos fazem acreditar que existe algo interessante no *infinito* a ser analisado, por exemplo, a sensação que retas paralelas se interceptam no horizonte:

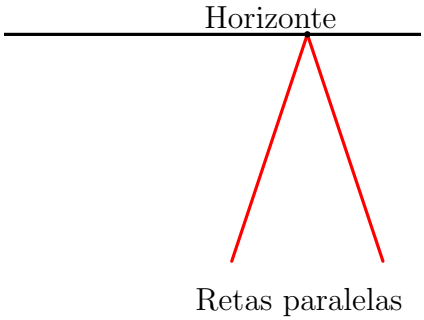

Figura 1: Comportamento de retas paralelas no infinito.

Para trabalharmos com esses pontos no *infinito*, definimos um novo espaço que, grosso modo, pode ser considerado como sendo o espaço afim com alguns pontos adicionais, chamado espaço projetivo. Posteriormente, para finalizar este primeiro capítulo, falamos sobre mudança linear no sistema de coordenada para simplificar alguns problemas.

No capítulo dois, estendemos a definição de variedades para o caso projetivo e mostramos uma versão do teorema Nullstellensatz Projetivo, o qual nos possibilita caracterizar as variedades projetivas geradas por um único polinômio homogêneo, chamadas hipersuperfícies. Quando consideramos um corpo finito várias indagações surgem naturalmente. O presente trabalho está interessado em realizar um estudo sobre o número máximo de pontos em uma hipersuperfície de grau d no espaço projetivo definido sobre um corpo finito. Para isso, definimos as variedades Hermitianas, que desempenham um papel central no estudo realizado devido a um resultado sobre o número de pontos em uma variedade Hermitiana não degenerada, apresentado por Bose e Chakravarti em [2]. Posteriormente, falamos um pouco sobre o comportamento de uma hipersuperfície quando fazemos uma mudança linear no sistema de coordenadas. Para finalizar o capítulo, falamos sobre o espaço tangente com o intuito de analisar separadamente as hipersuperfícies não singulares no próximo capítulo e enunciamos o teorema de Bezout sobre o número de pontos na interseção de duas curvas projetivas sem componentes em comum.

Por fim, no último capítulo, apresentamos a resposta dada por Serre em [3] para o número máximo de pontos $\mathbb{F}_q$ - racionais em uma hipersuperfície definida sobre $\mathbb{F}_q$. Posteriormente, falamos sobre a conjectura de Sziklai apresentada em [4] e provada em uma série de três artigo [5, 6, 7] por Homma e Kim sobre o número máximo de pontos em uma curva não singular definida sobre $\mathbb{F}_q$ que não contém uma reta definida sobre $\mathbb{F}_q$, depois uma generalização provada pelos mesmos autores em [8] sobre o número máximo de pontos $\mathbb{F}_q$ - racionais em uma hipersuperfície definida sobre $\mathbb{F}_q$ e sem componente $\mathbb{F}_q$ - linear. Esses resultados possibilitaram Datta em [9] determinar o número máximo de pontos $\mathbb{F}_q$ - racionais em uma hipersuperfície de grau d definida sobre $\mathbb{F}_q$ em $\mathbb{P}^4$, sobre algumas condições para d. Finalizamos o trabalho apresentando a demonstração desse resultado.

Walteir de Paula Ferreira
Uberlândia-MG, 18 de fevereiro de 2021.

Capítulo 1

Prolegômenos algébricos

Imaginamos que o leitor que inicia sua maravilhosa aventura por este singelo trabalho esteja familiarizado com os conceitos iniciais da álgebra comutativa e geometria algébrica clássica, de tal modo que este primeiro capítulo não apresente nenhuma grande dificuldade e sirva tão somente para fixar a terminologia usada pelo autor. Desse modo, as demonstrações que requerem uma explanação melhor da teoria aqui apresentada, para uma boa compreensão, serão omitidas e as devidas referências para elas são dadas. Antes, vamos fixar algumas notações:

- A menos que seja mencionado o contrário, denotaremos por k um corpo algebricamente fechado [1] e $k[X_1, ..., X_n]$ denotará o anel de polinômios nas n indeterminadas $X_1, ..., X_n$ com coeficientes no corpo k.

- Vamos denotar por q a potência positiva de um primo positivo, isto é, $q = p^m$ para algum primo $0 < p \in \mathbb{Z}$ e m inteiro positivo. Um dos resultados iniciais sobre a teoria dos corpos finitos é que existe um único corpo finito com q elementos, a menos de isomorfismo, esse corpo será denotado por $\mathbb{F}_q$. Para os leitores pouco familiarizado com as noções básicas sobre corpos finitos indicamos a leitura de [10].

Como existe uma boa discussão na matemática se o número zero é ou não natural, nos parece razoável informar que durante este trabalho vamos considerar como conjunto dos números naturais como sendo $\mathbb{N} := \{1, 2, 3, ...\}$ e n denotará um número natural qualquer.

1.1 Geometria no espaço afim

O conceito de variedade é um dos principais objetos de estudo da geometria algébrica clássica. Uma variedade consiste no lugar geométrico onde uma coleção de equações polinomiais é satisfeita. Nesta seção, faremos uma breve introdução sobre variedades no espaço afim e apresentaremos alguns resultados necessários para as próximas seções. Esta seção tem como principal referência [1].

Definição 1.1. Seja k um corpo arbitrário. O **espaço afim de dimensão** n **sobre** k, denotado por $\mathbb{A}^n(k)$, é definido por $\mathbb{A}^n(k) := k^n = \{(x_1, ..., x_n);\ x_1, ..., x_n \in k\}$.

Neste momento, o leitor poderia se indagar sobre o fato de não utilizarmos simplesmente a notação k^n para representar o espaço afim de dimensão n sobre k. Pois bem, está notação usualmente é utilizada para representar o k-espaço vetorial k^n, porém, no momento, não estamos interessados na estrutura vetorial do conjunto. Desse modo, a origem não desempenhará nenhum papel central, como desempenha na álgebra linear.

[1] Todo polinômio de grau positivo em $k[X]$ possui raiz em k.

Uma das grandes belezas da geometria algébrica clássica é que ela estabelece uma ponte entre álgebra e geometria. Para isso, primeiramente, enunciamos um resultado:

Teorema 1.1 (Base de Hilbert)**.** *Todo ideal de* $k[X_1, ..., X_n]$ *é finitamente gerado.*

Demonstração. Veja [1, teorema 4 - seção 2.5]. ■

Vamos considerar um polinômio $f \in k[X_1, ..., X_n]$ também como sendo uma função de $\mathbb{A}^n(k)$ em k que associa a cada ponto $(x_1, ..., x_n) \in \mathbb{A}^n(k)$ o elemento $f(x_1, ..., x_n) \in k$. Agora vamos associar a cada subconjunto do espaço afim um ideal de $k[X_1, ..., X_n]$:

Lema 1.1. *Sejam* k *um corpo arbitrário e* $S \subseteq \mathbb{A}^n(k)$*. O conjunto*

$$\mathbb{I}(S) := \{f \in k[X_1, ..., X_n]; \quad f(x) = 0 \quad \textit{para todo} \quad x \in S\} \subseteq k[X_1, ..., X_n]$$

é um ideal, chamado de ***ideal polinomial que se anula em*** S*.*

Demonstração. Claramente, o polinômio identicamente nulo está em $\mathbb{I}(S)$. Sejam $f, g \in \mathbb{I}(S)$ e $h \in k[X_1, ..., X_n]$. Dado $a \in S$ temos $f(a) = g(a) = 0$ pela definição de $\mathbb{I}(S)$. Desse modo,

$$(f + g)(a) := f(a) + g(a) = 0 + 0 = 0 \quad \text{e} \quad (hf)(a) := h(a)f(a) = h(a) \cdot 0 = 0.$$

Sendo a um ponto arbitrário de S então $f + g$ e hf pertencem a $\mathbb{I}(S)$. Portanto, $\mathbb{I}(S)$ é um ideal de $k[X_1, ..., X_n]$.

■

Dada uma coleção $\mathcal{B} \subseteq k[X_1, ..., X_n]$, denotaremos por $\langle \mathcal{B} \rangle$ o ideal gerado por $\mathcal{B}$, isto é, o menor ideal de $k[X_1, ..., X_n]$ que contém a coleção $\mathcal{B}$. Um exercício interessante, o qual deixamos para o leitor escrever os detalhes, é que

$$\langle \mathcal{B} \rangle = \{h_1 f_1 + \cdots + h_m f_m; \ m \geq 1, f_j \in \mathcal{B} \ e \ h_j \in k[X_1, ..., X_n] \ \forall j = 1, ..., m\}.$$

Com essa notação, o teorema da base de Hilbert 1.1 nos diz que se I é um ideal de $k[X_1, ..., X_n]$, então existem $f_1, ..., f_m \in k[X_1, ..., X_n]$ tais que $I = \langle f_1, ..., f_m \rangle$.

Exemplo 1.1. Sejam k um corpo arbitrário e $S = \{(0, 0)\} \subseteq \mathbb{A}^2(k)$. Então $\mathbb{I}(S) = \langle X, Y \rangle$, de fato: como $X, Y \in \mathbb{I}(S)$, então $\langle X, Y \rangle \subseteq \mathbb{I}(S)$. Dado $f \in \mathbb{I}(S)$ tem-se $f(0, 0) = 0$, ou seja, o termo independente de f é nulo e assim podemos escrever $f = X \cdot f_1(X, Y) + Y \cdot f_2(X, Y)$ com $f_1, f_2 \in k[X, Y]$, consequentemente, $f \in \langle X, Y \rangle$. Segue daí que $\mathbb{I}(S) \subseteq \langle X, Y \rangle$.

Com isso, temos a seguinte função

$$\begin{array}{ccc} \{ \text{ subconjuntos de } \mathbb{A}^n(k) \ \} & \longrightarrow & \{ \text{ ideais de } k[X_1, ..., X_n] \ \} \\ S & \longmapsto & \mathbb{I}(S) \end{array}.$$

No próximo objetivo é fazer o caminho inverso, associar um ideal qualquer de $k[X_1, ..., X_n]$ a um subconjunto de $\mathbb{A}^n(k)$.

Definição 1.2. Seja k um corpo arbitrário. Uma **variedade afim** é o lugar geométrico em $\mathbb{A}^n(k)$ onde uma coleção de equações polinomiais é satisfeita.

Dada uma coleção de polinômios $\mathcal{B} \subseteq k[X_1, ..., X_n]$, denotaremos por $\mathbb{V}(\mathcal{B})$ a variedade afim associada à coleção $\mathcal{B}$, ou seja,

$$\mathbb{V}(\mathcal{B}) := \{(a_1, ..., a_n) \in \mathbb{A}^n(k); \ f(a_1, ..., a_n) = 0 \ \ \forall \ f \in \mathcal{B}\}.$$

Quando $\mathcal{B} = \{f_1, ..., f_m\}$ é finito, denotaremos $\mathbb{V}(\mathcal{B})$ simplesmente por $\mathbb{V}(f_1, ..., f_m)$.

Exemplo 1.2. Considere $f = Y - X^2 \in \mathbb{R}[X, Y]$. Assim

$$\mathbb{V}(f) = \{(x, y) \in \mathbb{A}^2(\mathbb{R});\ y = x^2\},$$

ou seja, $\mathbb{V}(f)$ é o gráfico de uma parábola em $\mathbb{A}^2(\mathbb{R}) = \mathbb{R}^2$:

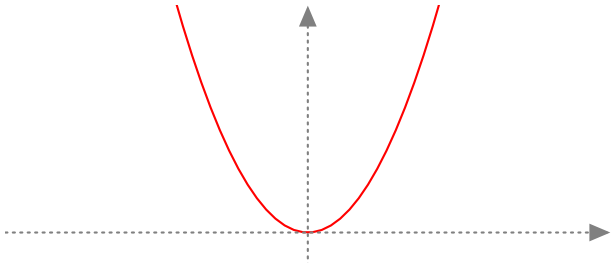

Figura 1.1: Representação gráfica da parábola $y = x^2$ em $\mathbb{R}^2$.

O próximo resultado que vamos enunciar nos diz que não precisamos considerar variedades afins geradas por subconjuntos quaisquer de $k[X_1, ..., X_n]$, pois é suficiente apenas considerar as variedade geradas por ideais.

Proposição 1.1. *Seja $\mathcal{B} \subseteq k[X_1, ..., X_n]$. Se I é o ideal gerado por $\mathcal{B}$, então $\mathbb{V}(I) = \mathbb{V}(\mathcal{B})$.*

Demonstração. Seja $a \in \mathbb{V}(I)$. Assim, para todo $f \in I$ temos $f(a) = 0$. Em particular, para todo $f \in \mathcal{B} \subseteq I$ vale $f(a) = 0$, consequentemente, $a \in \mathbb{V}(\mathcal{B})$. Desse modo, $\mathbb{V}(I) \subseteq \mathbb{V}(\mathcal{B})$.

Para a inclusão revesa considere $a \in \mathbb{V}(\mathcal{B})$ e $f \in I$. Como I é gerado por $\mathcal{B}$ existem polinômios $f_1, ..., f_m \in \mathcal{B}$ e $g_1, ..., g_m \in k[X_1, ..., X_n]$ tais que $f = \sum_{j=1}^{m} g_j f_j$. Segue daí que

$$f(a) = \sum_{j=1}^{m} g_j(a) \cdot f_j(a) = \sum_{j=1}^{m} g_j(a) \cdot 0 = 0.$$

Sendo f um polinômio arbitrário de I, então $a \in \mathbb{V}(I)$. Logo, $\mathbb{V}(\mathcal{B}) \subseteq \mathbb{V}(I)$.

■

Esta proposição nos diz que toda variedade afim pode ser gerada por um ideal. Por outro lado, sabemos pelo teorema da base de Hilbert 1.1 que todo ideal em $k[X_1, ..., X_n]$ é finitamente gerado. Desse modo, toda variedade afim pode ser gerada por uma coleção finita de polinômios. No caso particular, quando a variedade é gerada por um único polinômio de grau d, dizemos que ela é uma **hipersuperfície afim de grau** d. Se $n = 2$ ou $n = 3$, podemos nos referir a uma hipersuperfície de grau d por **curva de grau** d ou **superfície de grau** d, respectivamente.

Com isso, temos a seguinte função

$$\begin{array}{ccc} \{ \text{ ideais de } k[X_1, ..., X_n] \ \} & \longrightarrow & \{ \text{ subconjuntos de } \mathbb{A}^n(k) \ \} \\ I & \longmapsto & \mathbb{V}(I) \end{array}.$$

De modo geral, se $\mathbb{V}(I)$ é a variedade afim gerada pelo ideal $I \subseteq k[X_1, ..., X_n]$, nem sempre temos $\mathbb{I}(\mathbb{V}(I)) = I$. Vejamos um exemplo a seguir onde isso não acontece.

Exemplo 1.3. Sejam $f = X^2 + Y^2 \in \mathbb{R}[X, Y]$ e $I = \langle f \rangle$. Assim, pela proposição 1.1, temos $\mathbb{V}(I) = \mathbb{V}(f) = \{(0, 0)\}$. Além disso, $\mathbb{I}(\mathbb{V}(I)) = \mathbb{I}(\{(0, 0)\}) = \langle X, Y \rangle$ (veja, exemplo 1.1).

Observação 1.1. Um dos principais motivos pelos quais consideramos k um corpo algebricamente fechado, a menos que seja mencionado o contrário como em algumas definições acima, é pelo fato de que exemplos peculiares como $\mathbb{V}(X^2 + Y^2 + 1) = \emptyset$ em $\mathbb{A}^2(\mathbb{R})$ só acontecem em um caso bem específico (teorema 1.2). Além disso, quando $n \geq 2$, uma hipersuperfície no espaço afim de dimensão n sobre um corpo algebricamente fechado tem infinitos pontos.

Por outro lado, por definição, sempre vale $I \subseteq \mathbb{I}(\mathbb{V}(I))$. Como veremos, não vale a igualdade nem quando k é algebricamente fechado, entretanto, neste caso existe um resultado da geometria algébrica que nos descreve $\mathbb{I}(\mathbb{V}(I))$ em termos de I. Antes de enunciá-lo, vejamos um resultado e mais algumas definições necessárias.

Teorema 1.2 (Weak Nullstellensatz)**.** *Se* $\mathbb{V}(I) = \emptyset$*, então* $I = k[X_1, ..., X_n]$.

Demonstração. Veja [1, teorema 1 - seção 4.1]. ■

De modo equivalente, o teorema Weak Nullstellensatz 1.2 nos diz que se I é um ideal próprio de $k[X_1, ..., X_n]$, então $\mathbb{V}(I) \neq \emptyset$. No caso $k = \mathbb{C}$ ele pode ser considerado como uma generalização mais forte do teorema fundamental da álgebra [2] para polinômios de várias variáveis. Com efeito, dado $f \in \mathbb{C}[X_1, ..., X_n]$ não constante, temos $\langle f \rangle \neq \langle 1 \rangle$. Assim, por Weak Nullstellensatz, $\mathbb{V}(f) \neq \emptyset$, isto é, existe $(x_1, ..., x_n) \in \mathbb{C}^n$ tal que $f(x_1, ..., x_n) = 0$. Mais ainda, ele consegue garantir quando um sistema de equações polinomiais com coeficientes em $\mathbb{C}$ possui solução.

Definição 1.3. Dado um ideal $I \subseteq k[X_1, ..., X_n]$, defina-se o radical de I, denotado por $\text{rad}(I)$, como sendo

$$\text{rad}(I) := \{f \in k[X_1, ..., X_n];\ f^m \in I \text{ para algum } m \geq 1\}.$$

Proposição 1.2. *O subconjunto* $\text{rad}(I)$ *é um ideal de* $k[X_1, ..., X_n]$.

Demonstração. Claramente, $0 \in \text{rad}(I)$. Sejam $f, g \in \text{rad}(I)$ e $h \in k[X_1, ..., X_n]$. Assim, existe $m, l \geq 1$ tal que $f^m, g^l \in I$. Desse modo, tem-se $(hf)^m = h^m f^m \in I$, consequentemente, $hf \in \text{rad}(I)$. Além disso, segue do teorema binomial para anéis que

$$(f+g)^{m+l-1} = \sum_{k=0}^{m+l-1} \binom{m+l-1}{k} f^{m+l-1-k} g^k$$

- Se $k \geq l$ tem-se $f^{m+l-1-k} g^k \in I$.
- Se $k < l$ então $m - 1 < m + l - 1 - k$, assim $f^{m+l-1-k} g^k \in I$.

Logo, $(f+g)^{m+l-1} \in I$ e assim $f + g \in \text{rad}(I)$. Portanto, $\text{rad}(I)$ é um ideal em $k[X_1, ..., X_n]$. ■

Observação 1.2. Para todo ideal I de $k[X_1, ..., X_n]$ vale $I \subseteq \text{rad}(I)$.

Exemplo 1.4. Seja $\mathfrak{p}$ um ideal primo de $k[X_1, ..., X_n]$. Afirmamos que $\text{rad}(\mathfrak{p}) = \mathfrak{p}$. Com efeito, pela observação acima, temos $\mathfrak{p} \subseteq \text{rad}(\mathfrak{p})$. Seja $f \in \text{rad}(\mathfrak{p})$, assim existe $m \geq 1$ tal que $f^m \in \mathfrak{p}$. Como $\mathfrak{p}$ é um ideal primo, tem-se $f \in \mathfrak{p}$, consequentemente, $\text{rad}(\mathfrak{p}) \subseteq \mathfrak{p}$. Portanto, $\text{rad}(\mathfrak{p}) = \mathfrak{p}$.

Exemplo 1.5. Seja $I = \langle X^m, Y^n \rangle$ ideal em $k[X, Y]$ com $m, n \geq 1$. Então, $\text{rad}(I) = \langle X, Y \rangle$, de fato: Seja $f \in \text{rad}(I)$, assim existe $r \geq 1$ tal que $f^r \in I = \langle X^m, Y^n \rangle \subseteq \langle X, Y \rangle$. Como $\langle X, Y \rangle$ é um ideal primo tem-se $f \in \langle X, Y \rangle$. Logo, $\text{rad}(I) \subseteq \langle X, Y \rangle$. Além disso, observe que $X, X \in \text{rad}(I)$, pois $X^m, Y^n \in I$, assim $\langle X, Y \rangle \subseteq \text{rad}(I)$. Portanto, $\text{rad}(I) = \langle X, Y \rangle$.

Com esta definição de radical de um ideal podemos enunciar um teorema que caracteriza os ideais gerados por variedades afins:

Teorema 1.3 (Nullstellensatz)**.** *Seja* I *ideal de* $k[X_1, ..., X_n]$*, então* $\mathbb{I}(\mathbb{V}(I)) = \text{rad}(I)$.

Demonstração. Veja [1, teorema 6 - seção 4.2]. ■

[2] O teorema fundamental da álgebra afirma que o corpo dos números complexo é algebricamente fechado.

Como sabemos, $k[X_1, ..., X_n]$ é um domínio de fatoração única. Assim, uma consequência quase imediata do teorema Nullstellensatz 1.3 é o seguinte:

Corolário 1.1. *Dado $f \in k[X_1, ..., X_n]$ não constante, seja $f = cf_1^{a_1} \cdots f_s^{a_s}$ a decomposição de f em distintos polinômios irredutíveis em $k[X_1, ..., X_n]$ com $c \in k$. Então $\mathbb{I}(\mathbb{V}(f)) = \langle f_1 \cdots f_r \rangle$.*

Demonstração. Considere $I = \langle f \rangle$. Assim, pelo teorema Nullstellensatz 1.3, é suficiente mostrar que $\text{rad}(I) = \langle f_1 \cdots f_s \rangle$. Seja $N = max\{a_1, ..., a_s\}$ então

$$(f_1 \cdots f_s)^N = f_1^{N-a_1} \cdots f_s^{N-a_s} f \in I,$$

assim $f_1 \cdots f_s \in \text{rad}(I)$, consequentemente, $\langle f_1 \cdots f_s \rangle \subseteq \text{rad}(I)$. Para a inclusão reversa, dado $g \in \text{rad}(I)$ existe $m \geq 1$ tal que $g^m \in I = \langle f \rangle$. Segue daí que

$$g^m = hf = chf_1^{a_1} \cdots f_s^{a_s},$$

para algum $h \in k[X_1, ..., X_n]$. Desse modo, $f_1, ..., f_s$ são fatores irredutíveis de g^m. Por outro lado, a fatoração de g^m em polinômios irredutíveis são potências m-ésima dos fatores irredutíveis de g. Logo $f_1, ..., f_s$ são fatores irredutíveis de g, consequentemente, $g \in \langle f_1 \cdots f_s \rangle$ e assim $\text{rad}(I) \subseteq \langle f_1 \cdots f_s \rangle$. Portanto, $\text{rad}(I) = \langle f_1 \cdots f_s \rangle$.

■

Desse modo, o corolário acima nos diz que, quando o corpo é algebricamente fechado, a dificuldade de encontrar $\mathbb{I}(\mathbb{V}(f))$ está relacionado com a dificuldade de encontrar os fatores irredutíveis de f em $k[X_1, ..., X_n]$.

Teorema 1.4. (Correspondência Ideal-Variedade)

i) Sejam I e J ideais de $k[X_1, ..., X_n]$. Se $I \subseteq J$, então $\mathbb{V}(I) \supseteq \mathbb{V}(J)$.

ii) Sejam V e W variedades afins de $\mathbb{A}^n(k)$. Se $V \subseteq W$, então $\mathbb{I}(V) \supseteq \mathbb{I}(W)$

iii) Se V é uma variedade de $\mathbb{A}^n(k)$, então $\mathbb{V}(\mathbb{I}(V)) = V$.

Demonstração. Os itens (i) e (ii) são imediatos. Deixamos os detalhes para o leitor.

(iii) A inclusão $V \subseteq \mathbb{V}(\mathbb{I}(V))$ segue da definição. Para a inclusão reversa, considere I ideal de $k[X_1, ..., X_n]$ tal que $V = \mathbb{V}(I)$. Se $f \in I$, então f se anula em V, assim $f \in \mathbb{I}(V)$. Deste modo, temos $I \subseteq \mathbb{I}(V)$. Segue do item (i) que $\mathbb{V}(\mathbb{I}(V)) \subseteq \mathbb{V}(I) = V$. Portanto, $\mathbb{V}(\mathbb{I}(V)) = V$.

■

Com essa correspondência ideal-variedade e o corolário do teorema Nullstellensatz temos a seguinte caracterização para hipersuperfícies afim:

Proposição 1.3. *Seja V uma variedade afim em $\mathbb{A}^n(k)$. Então V é uma hipersuperfície se, e somente se, $\mathbb{I}(V)$ é principal.*

Demonstração. Suponha que $V = \mathbb{V}(f)$ para algum $f \in k[X_1, .., X_n]$. Segue do corolário do teorema de Nullstellensatz 1.3 que

$$\mathbb{I}(V) = \mathbb{I}(\mathbb{V}(f)) = rad(\langle f \rangle) = \langle f_1 \cdots f_r \rangle,$$

onde $f_1, ..., f_r$ são os fatores irredutíveis não associados de f em $k[X_1, ..., X_n]$.

Reciprocamente, suponha que $\mathbb{I}(V) = \langle g \rangle$ para algum $g \in k[X_1, ..., X_n]$. Pelo item (iii) do teorema Correspondência Ideal-Variedade 1.4 temos

$$V = \mathbb{V}(\mathbb{I}(V)) = \mathbb{V}(\langle g \rangle) = \mathbb{V}(g).$$

■

Observação 1.3. A hipótese de k ser algebricamente fechado é essencial para a veracidade da implicação ($\Rightarrow$) da proposição anterior, veja o exemplo 1.3.

Para finalizar a seção vamos munir o espaço afim com uma topologia[3]. Antes disso, vamos ver mais duas propriedades que o conjunto das variedades afins possui:

Proposição 1.4. *Para qualquer espaço afim $\mathbb{A}^n(k)$ temos:*

i) A interseção de qualquer coleção de variedades afins é uma variedade afim.

ii) A reunião finita de variedades afins é uma variedade afim.

Demonstração.

i) Seja $\{V_\alpha\}_\alpha$ uma coleção de variedades afins. Para cada α existe um ideal $I_\alpha \subseteq k[X_1, ..., X_n]$ tal que $V_\alpha = \mathbb{V}(I_\alpha)$. Afirmamos que

$$\bigcap_\alpha V_\alpha = \mathbb{V}\left(\bigcup_\alpha I_\alpha\right).$$

Com efeito, sejam $a \in \bigcap_\alpha V_\alpha$ e $f \in \bigcup_\alpha I_\alpha$. Assim, existe α tal que $f \in I_\alpha$. Como $a \in V_\alpha = \mathbb{V}(I_\alpha)$ tem-se $f(a) = 0$. Logo, $a \in \mathbb{V}\left(\bigcup_\alpha I_\alpha\right)$, consequentemente, $\bigcap_\alpha V_\alpha \subseteq \mathbb{V}\left(\bigcup_\alpha I_\alpha\right)$. Para a inclusão reversa, seja $a \in \mathbb{V}\left(\bigcup_\alpha I_\alpha\right)$. Assim, para todo α e $f \in I_\alpha$ temos $f(a) = 0$, isto é, $a \in \mathbb{V}(I_\alpha) = V_\alpha$ para todo α. Logo, $a \in \bigcap_\alpha V_\alpha$, consequentemente, $\mathbb{V}\left(\bigcup_\alpha I_\alpha\right) \subseteq \bigcap_\alpha V_\alpha$.

ii) Sejam V e W variedades. Assim, existem ideias $I, J \subseteq k[X_1, ..., X_n]$ tais que $V = \mathbb{V}(I)$ e $W = \mathbb{V}(J)$. Afirmamos que

$$V \cup W = \mathbb{V}(\{fg;\ f \in I \ \ e \ \ g \in J\})$$

Com efeito, sejam $a \in V \cup W$, $f \in I$ e $g \in J$. Se $a \in V$ então $f(a) = 0$ e assim $(fg)(a) = f(a)g(a) = 0$. Se $a \in W$, então $g(a) = 0$ e assim $(fg)(a) = f(a)g(a) = 0$. Deste modo, em ambos os caso temos $a \in \mathbb{V}(\{fg;\ f \in I \ \ e \ \ g \in J\})$, consequentemente,

$$V \cup W \subseteq \mathbb{V}(\{fg;\ f \in I \ \ e \ \ g \in J\}).$$

Para a inclusão reversa, seja $a \in \mathbb{V}(\{fg;\ f \in I \ \ e \ \ g \in J\})$. Se $g(a) = 0$ para todo $g \in J$, então $a \in W$, consequentemente, $\mathbb{V}(\{fg;\ f \in I \ \ e \ \ g \in J\}) \subseteq V \cup W$. Suponha que exista $g \in J$ tal que $g(a) \neq 0$, assim para todo $f \in I$ tem-se $f(a)g(a) = (fg)(a) = 0$, implicando $f(a) = 0$. Logo, $a \in V$ e assim $\mathbb{V}(\{fg;\ f \in I \ \ e \ \ g \in J\}) \subseteq V \cup W$. O resultado segue usando indução finita sobre n.

■

Desse modo, usando as leis De Morgan da teoria dos conjuntos, o resultado anterior nos possibilita adicionar uma estrutura topológica no espaço afim, basta definir como subconjunto aberto o complementar de uma variedade afim. Essa topologia é chamada de ***topologia de Zariski*** em $\mathbb{A}^n(k)$. O fecho de Zariski de um subconjunto de $\mathbb{A}^n(k)$ é facilmente caracterizado:

Proposição 1.5. *Seja $S \subseteq \mathbb{A}^n(k)$. Então $\overline{S} = \mathbb{V}(\mathbb{I}(S))$.*

Demonstração. Por definição, temos $S \subseteq \mathbb{V}(\mathbb{I}(S))$. Sendo $\overline{S}$ o menor fechado que contém S, tem-se $\overline{S} \subseteq \mathbb{V}(\mathbb{I}(S))$. Como $S \subseteq \overline{S}$ segue do teorema Correspondência Ideal-Variedade 1.4 que $\mathbb{V}(\mathbb{I}(S)) \subseteq \mathbb{V}(\mathbb{I}(\overline{S})) = \overline{S}$. Portanto, $\overline{S} = \mathbb{V}(\mathbb{I}(S))$. ■

[3]Para as noções topológicas básicas, indicamos a leitura do famoso livro de topologia do Munkres [11].

1.2 Algumas considerações sobre $\mathbb{A}^n(\mathbb{F}_q)$

Quando consideramos hipersuperfícies no espaço afim sobre um corpo finito $\mathbb{F}_q$, podemos nos questionar sobre a cardinalidade máxima desse conjunto com relação ao grau da hipersuperfície, dimensão do espaço e q. Desse modo, esta seção tem por objetivo dar uma resposta para esta indagação.

Teorema 1.5. *Seja $f \in \mathbb{F}_q[X_1, ..., X_n]$ com $deg(f) = d \geq 0$. Então*

$$|\mathbb{V}(f)| \leq dq^{n-1}.$$

Demonstração. Se $d = 0$, então f é constante e diferente do polinômio identicamente nulo, o resultado segue. Se $d = 1$, então

$$f = a_0 + a_1X_1 + \cdots + a_nX_n.$$

Como $deg(f) = 1$ tem-se $a_j \neq 0$ para algum $j = 1, ..., n$. Fazendo $f = 0$ temos

$$X_j = -a_j^{-1}(a_0 + a_1X_1 + \cdots + a_{j-1}X_{j-1} + a_{j+1}X_{j+1} + \cdots + a_nX_n).$$

Assim, para cada $i \neq j$ existem q possibilidades para X_i, consequentemente, $|\mathbb{V}(f)| = q^{n-1}$. Sabemos que o resultado é verdadeiro para $n = 1$. Assim, mostramos que o teorema é verdadeiro para os casos $d \leq 1$ ou $n = 1$. Prosseguimos usando indução duas vezes. Suponha que seja verdadeiro para todo polinômio de grau d' com $0 \leq d' < d$ e no máximo n variáveis. Vamos provar que é verdadeiro para um polinômio $f(X_1, ..., X_n)$ com n indeterminadas de grau d dividindo a prova em dois casos:

***Caso 1**: Suponha que f seja divisível por $X_1 - c$ para algum $c \in \mathbb{F}_q$.* Temos

$$f = (X_1 - c)g$$

para algum $g \in \mathbb{F}_q[X_1, ..., X_n]$ com $deg(g) = d - 1 < d$. Pela hipótese de indução

$$|\mathbb{V}(g)| \leq (d - 1)q^{n-1}.$$

Deste modo, tem-se $|\mathbb{V}(f)| \leq |\mathbb{V}(X_1 - c)| + |\mathbb{V}(g)| = q^{n-1} + (d - 1)q^{n-1} = dq^{n-1}$.

Suponha agora que seja verdadeiro para todo polinômio com m variáveis, $1 \leq m < n$, e de grau no máximo d.

***Caso 2**: Suponha que f não seja divisível por $X_1 - c$ para todo $c \in \mathbb{F}_q$.* Assim, para todo $c \in \mathbb{F}_q$ tem-se $g(X_2, ..., X_n) = f(c, X_2, ..., X_n)$ é um polinômio com $n - 1$ variáveis, não nulo e de grau no máximo d. Pela hipótese de indução $|\mathbb{V}(g)| \leq dq^{n-2}$ em $\mathbb{A}^{n-1}(\mathbb{F}_q)$. Como existe q escolhas possíveis para c, então

$$|\mathbb{V}(f)| \leq q \cdot dq^{n-2} = dq^{n-1}.$$

■

Teorema 1.6. *Sejam $n \geq 2$ e $\mathbb{V}(f) \subseteq \mathbb{A}^n(\mathbb{F}_q)$ uma hipersuperfície de grau d, com $2 \leq d < q$. Se $|\mathbb{V}(f)| < dq^{n-1}$, então*

$$|\mathbb{V}(f)| \leq dq^{n-1} - (d - 1)q^{n-2}.$$

Demonstração. Veja [12, proposição 2]. ■

1.3 Espaço projetivo: ao infinito e além!

Na geometria euclidiana plana dizemos que duas retas distintas são concorrentes se possuem um único ponto em comum e são ditas paralelas se não possuem nenhum ponto em comum. Entretanto, por experiências cotidianas, todos nós já tivemos aquela leve sensação que retas paralelas se interceptam no "infinito". Um exemplo simples deste fenômeno ocorre quando viajamos de carro sobre uma estrada reta; existe uma leve sensação que todas as retas paralelas que constituem a estrada se encontram no horizonte. Outra questão pertinente, que nos leva a acreditar que exista algo interessante no "infinito" a ser analisado, é o comportamento assintótico de algumas curvas planas. Por exemplo, a hipérbole $X^2 - Y^2 = 1$ no plano $\mathbb{R}^2$ possui duas assíntotas $Y = X$ e $Y = -X$ (direções assintóticas). Essas retas no plano nunca se interceptam com a hipérbole, porém, no infinito, temos a sensação que a hipérbole intercepta cada reta em dois pontos distintos:

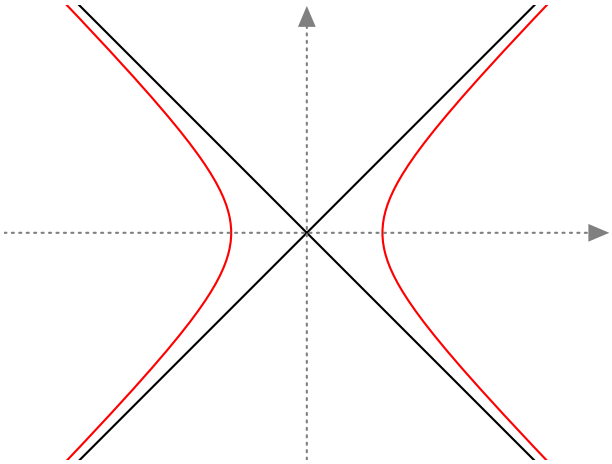

Figura 1.2: Direções assintóticas da hipérbole $X^2 - Y^2 = 1$ em $\mathbb{R}^2$

O conceito de espaço projetivo originou-se deste efeito visual, onde retas paralelas parecem se encontrar no "infinito". Grosso modo, podemos imaginar o espaço projetivo como sendo o espaço afim com esses pontos no infinito. Esta ideia ficará mais clara adiante.

Definição 1.4. Seja k um corpo arbitrário. O **espaço projetivo de dimensão n sobre k**, denotado por $\mathbb{P}^n(k)$, é definido como sendo o conjunto das retas em $\mathbb{A}^{n+1}(k)$ que passam pela origem.

Dado $(a_0, ..., a_n) \in \mathbb{A}^{n+1}(k)$, considere

$$\text{span}(a_0, ..., a_n) := \{\lambda(a_0, ..., a_n);\ \lambda \in k\}.$$

Com isso, podemos escrever

$$\mathbb{P}^n(k) = \{\text{span}(a_0, ..., a_n);\ a_0, ..., a_n \in \mathbb{A}^n(k) \text{ não são todos nulos}\}.$$

Comumente, os elementos de $\mathbb{P}^n(k)$ serão chamados de pontos.

Por mais estranho que possa parecer a definição de espaço projetivo dada em 1.4, em relação as observações feitas no início desta seção, mostraremos que podemos identificar ele como sendo o espaço afim de dimensão n com alguns pontos no infinito, o qual justifica parcialmente o motivo de darmos preferência em trabalhar no espaço projetivo do que no afim para o estudo de hipersuperfícies. Antes disso, uma indagação que surge naturalmente quando se considera o espaço projetivo sobre um corpo finito é sua cardinalidade, que é obviamente finita:

Proposição 1.6. $|\mathbb{P}^n(\mathbb{F}_q)| = q^n + \cdots + q + 1$.

Demonstração. Dado $(a_0, ..., a_n) \in \mathbb{A}^{n+1}(\mathbb{F}_q)$ não nulo, tem-se

$$|\text{span}(a_0, ..., a_n)| = |\{\lambda \cdot (a_0, ..., a_n);\ \lambda \in \mathbb{F}_q\}| = q,$$

isto é, cada reta que contém a origem em $\mathbb{A}^{n+1}(\mathbb{F}_q)$ tem exatamente q pontos. Além disso, sabemos que $|\mathbb{A}^{n+1}(\mathbb{F}_q)| = |\mathbb{F}_q^{n+1}| = q^{n+1}$, assim as retas que contém a origem devem passar em todos os outros $q^{n+1} - 1$ pontos do espaço. Deste modo, existem $q^{n+1} - 1$ retas, entretanto, cada reta foi contada $q - 1$ vezes. Segue daí que

$$|\mathbb{P}^n(\mathbb{F}_q)| = \frac{q^{n+1} - 1}{q - 1} = \frac{(q-1)(q^n + \cdots + q + 1)}{q - 1} = q^n + \cdots + q + 1.$$

■

Devido ao fato de que o número $|\mathbb{P}^n(\mathbb{F}_q)| = q^n + \cdots + q + 1$ vai aparecer várias vezes no capítulo 3, vamos fixar uma notação para facilitar a leitura e escrita. Defina $\theta_q : \mathbb{Z} \to \{0\} \cup \mathbb{N}$ por

$$\theta_q(z) = \begin{cases} |\mathbb{P}^z(\mathbb{F}_q)| & \text{se } z \geq 0 \\ \\ 0 & \text{caso contrário} \end{cases}$$

Para visualizar o espaço projetivo como sendo o espaço afim com alguns pontos no infinito, primeiramente, vamos identificar ele como sendo o quociente de uma relação de equivalência: defina-se em $\mathbb{A}^{n+1}(k)$ a seguinte relação $(a_0, ..., a_n) \sim (a'_0, ..., a'_n)$ *se* $(a_0, ..., a_n) = \lambda \cdot (a'_0, ..., a'_n)$ para algum $\lambda \in k$ não nulo.

Proposição 1.7. *A relação* $\sim$ *em* $\mathbb{A}^{n+1}(k)$ *é uma relação de equivalência.*

Demonstração.

- *Reflexibilidade*: Como $(a_0, ..., a_n) = 1 \cdot (a_0, ..., a_n)$ tem-se $(a_0, ..., a_n) \sim (a_0, ..., a_n)$.
- *Simetria*: Suponha que $(a_0, ..., a_n) \sim (a'_0, ..., a'_n)$. Logo existe $\lambda \in k$ não nulo tal que $(a_0, ..., a_n) = \lambda \cdot (a'_0, ..., a'_n)$. Assim, λ^{-1} é não nulo e vale $(a'_0, ..., a'_n) = \lambda^{-1} \cdot (a_0, ..., a_n)$, consequentemente, $(a'_0, ..., a'_n) \sim (a_0, ..., a_n)$.
- *Transitividade*: Suponha que $(a_0, ..., a_n) \sim (a'_0, ..., a'_n)$ e $(a'_0, ..., a'_n) \sim (a''_0, ..., a''_n)$. Logo, existem $\lambda, \beta \in k$ não nulos tais que $(a_0, ..., a_n) = \lambda \cdot (a'_0, ..., a'_n)$ e $(a'_0, ..., a'_n) = \beta \cdot (a''_0, ..., a''_n)$. Segue daí que $\lambda \cdot \beta$ é não nulo e vale $(a_0, ..., a_n) = \lambda \cdot (a'_0, ..., a'_n) = \lambda \cdot \beta \cdot (a''_0, ..., a''_n)$. Deste modo, $(a_0, ..., a_n) \sim (a''_0, ..., a''_n)$.

■

Assim, de maneira natural, podemos identificar o n-ésimo espaço projetivo como sendo o conjunto da classes de equivalência $\mathbb{P}^n(k) \simeq (\mathbb{A}^{n+1}(k) - \{0\})/\sim$. Essa identificação nos leva a seguinte definição: dizemos que um subconjunto de $\mathbb{P}^n(k)$ é um **subespaço de dimensão** m se ele é o conjunto das classes de um subespaço vetorial de dimensão $m + 1$ em $\mathbb{A}^{n+1}(k)$ menos a origem; denotaremos por dim(S) a dimensão do subespaço S de $\mathbb{P}^n(k)$. Os subespaço de dimensão 1 e 2 em $\mathbb{P}^n(k)$ são chamados de **retas** e **planos**, respectivamente. Uma vez definido reta no espaço projetivo é de imediata verificação que duas retas distintas em $\mathbb{P}^2(k)$ se interceptam em um único ponto, pois dois subespaços vetoriais distintos de dimensão 2 em $\mathbb{A}^3(k) = k^3$ se interceptam em um subespaço de dimensão 1. Dado um subespaço $S \subseteq \mathbb{P}^n(k)$ de dimensão m definimos a **codimensão** de S, denotada por codim(S), com sendo

$$\text{codim(S)} := \dim(\mathbb{P}^n(k)) - \dim(\text{S}) = n - m.$$

Em particular, quando $k = \mathbb{F}_q$, a cardinalidade de um subespaço de dimensão m de $\mathbb{P}^n(\mathbb{F}_q)$ é facilmente calculado.

Proposição 1.8. *Se S é um subespaço de dimensão m em $\mathbb{P}^n(\mathbb{F}_q)$, então $|S| = \theta_q(m)$. Em particular, uma reta e um plano em $\mathbb{P}^n(\mathbb{F}_q)$ têm $q+1$ e q^2+q+1 pontos, respectivamente.*

Demonstração. Basta observar que S corresponde a um subespaço vetorial de dimensão $m+1$ de $\mathbb{A}^{n+1}(\mathbb{F}_q)$, o qual sabemos ser isomorfo a $\mathbb{A}^{m+1}(\mathbb{F}_q)$. O resultado segue.

■

Exemplo 1.6. Sejam $P = [u_0 : \cdots : u_n], Q = [v_0 : \cdots : v_n] \in \mathbb{P}^n(k)$ com $P \neq Q$. Considere os vetores $u = (u_0, ..., u_n)$ e $v = (v_0, ..., v_n)$. Claramente, u e v são ambos não nulos e linearmente independente ($P \neq Q$). Deste modo, o subespaço vetorial gerado por u e v, denotado por $span(u, v)$, tem dimensão 2 e

$$span(u, v) = \{\alpha u + \beta v;\ \alpha, \beta \in k\}.$$

Assim, a reta em $\mathbb{P}^n(k)$ que contém os pontos P e Q, denotada por $l(P, Q)$, é o conjunto

$$l(P,Q) = \{[\alpha u_0 + \beta v_0 : \cdots : \alpha u_n + \beta v_n] \in \mathbb{P}^n(k);\ \alpha, \beta \in k \text{ não são ambos nulos}\}$$

Observe que se $(a'_0, ..., a'_n) \sim (a_0, ..., a_n)$, então $\text{span}(a_0, ..., a_n) = \text{span}(a'_0, ..., a'_n)$. Assim, sem nenhuma ambiguidade, o ponto $P = \text{span}(a_0, ..., a_n) \in \mathbb{P}^n(k)$ será denotado simplesmente por $[a_0 : \cdots : a_n]$ e chamamos $a_0, ..., a_n$ de **coordenadas homogêneas** do ponto P.

Estamos quase no momento de identificar o espaço projetivo como sendo o espaço afim com alguns pontos no infinito. Claramente, não queremos uma simples identificação. Em nosso contexto, seria interessantes se o espaço afim fosse mergulhado, preservando a estrutura algébrica afim. Para isso, podemos, de forma natural, parametrizar a maioria das retas em $\mathbb{A}^{n+1}(k)$ por um espaço afim de dimensão n. Para cada $i = 0, ..., n$ defina

$$U_i := \{[a_0 : \cdots : a_n] \in \mathbb{P}^n(k);\ a_i \neq 0\},$$

chamada de **i-ésima carta afim**.

Lema 1.2. *Para cada $i = 0, ..., n$ a seguinte relação $\varphi_i : U_i \to \mathbb{A}^n(k)$ definida por*

$$\varphi_i([a_0 : \cdots : a_n]) = \left(\frac{a_0}{a_i}, ..., \frac{a_{i-1}}{a_i}, \frac{a_{i+1}}{a_i}, ..., \frac{a_n}{a_i}\right)$$

é uma função bijetora. A inversa de φ_i é dada por $\psi_i : \mathbb{A}^n(k) \to U_i$ definida por

$$\psi_i(a_0, ..., a_{i-1}, a_{i+1}, ...a_n) = [a_0 : \cdots : a_{i-1} : 1 : a_{i+1} : \cdots : a_n].$$

Demonstração. Para simplificar a notação, consideremos $i = 0$.

Seja $[a_0 : \cdots : a_n] = [a'_0 : \cdots : a'_n] \in U_0$. Existe, por definição, $\lambda \in k$ não nulo tal que $(a'_0, ..., a'_n) = \lambda \cdot (a_0, ..., a_n)$. Segue daí que

$$\varphi_0([a_0 : \cdots : a_n]) = \left(\frac{a_1}{a_0}, ..., \frac{a_n}{a_0}\right) = \left(\frac{\lambda a_1}{\lambda a_0}, ..., \frac{\lambda a_n}{\lambda a_0}\right) = \left(\frac{a'_1}{a'_0}, ..., \frac{a'_n}{a'_0}\right) = \varphi_0([a'_0 : \cdots : a'_n]).$$

Assim, a relação φ_0 está bem definida como função. Para verificar que φ_0 é uma bijeção, com inversa ψ_0, basta observar que

$$(\varphi_0 \circ \psi_0)(a_1, ..., a_n) = \varphi_0(\psi_0(a_1, ..., a_n)) = \varphi_0([1 : a_1 : \cdots : a_n]) = (a_1, ..., a_n)$$

$$(\psi_0 \circ \varphi_0)([a_0 : \cdots : a_n]) = \psi_0\left(\frac{a_1}{a_0}, ..., \frac{a_n}{a_0}\right) = \left[1, \frac{a_1}{a_0} : \cdots : \frac{a_n}{a_0}\right] = [a_0 : \cdots : a_n]$$

Portanto, φ_0 é uma função bijetora com inversa ψ_0.

■

Dessa maneira, para cada $i = 0, ..., n$, podemos identificar $U_i \simeq \mathbb{A}^n(k)$. Observe que para cada ponto $[a_0 : \cdots : a_n] \in \mathbb{P}^n(k)$ existe, por definição, $a_i \neq 0$ e assim $[a_0 : \cdots : a_n] \in U_i$. Portanto, podemos escrever

$$\mathbb{P}^n(k) = U_0 \cup \cdots \cup U_n, \text{ com } U_i \simeq \mathbb{A}^n(k).$$

No próximo capítulo, veremos, de forma análoga ao caso afim, que podemos munir o espaço projetivo com uma noção topológica usando as variedades projetivas (a serem definidas). Com esta topologia, a função do lema 1.2 torna-se um homeomorfismo [4] entre os espaços topológicos U_i e $\mathbb{A}^n(k)$ (proposição 2.9). Assim, deixaremos de apenas identificá-los e passaremos a considerar uma igualdade, pois eles possuem a mesma estrutura que estamos investigando.

Exemplo 1.7. As retas $span(a_0, a_1) \subseteq \mathbb{A}^2(\mathbb{R})$ são definidas pela equação linear

$$a_0X - a_1Y = 0.$$

Quando $a_0 \neq 0$ ao dividir tudo por a_0, temos

$$X = \frac{a_1}{a_0} \cdot Y,$$

esses são os elementos de U_0. Quando $a_1 \neq 0$ ao dividir tudo por a_1, temos

$$Y = \frac{a_0}{a_1} \cdot X,$$

esses são os elementos de U_1.

Considere $H_i = \mathbb{P}^n(k) \backslash U_i = \{[a_0 : \cdots : a_n];\ a_i = 0 \quad e \quad (a_0, ..., a_{i-1}, a_{i+1}, ..., a_n) \neq 0\}$. Assim, podemos identificar H_i como sendo $\mathbb{P}^{n-1}(k)$

$$[a_0 : \cdots : a_{i-1} : 0 : a_{i+1} : \cdots : a_n] \in H_i \longleftrightarrow [a_0 : \cdots : a_{i-1} : a_{i+1} : \cdots : a_n] \in \mathbb{P}^{n-1}(k).$$

Portanto, podemos expressar

$$\mathbb{P}^n(k) = U_i \cup H_i = \mathbb{A}^n(k) \cup \mathbb{P}^{n-1}(k),$$

onde identificamos $\mathbb{P}^0(k)$ como um ponto. Os pontos em $\mathbb{P}^{n-1}(k)$ são chamados de ***pontos no infinito*** de $\mathbb{P}^n(k)$.

Exemplo 1.8. Considerando a carta afim U_0 e escolhendo um representante para cada classe, pelo exposto acima, podemos escrever

$$\mathbb{P}^n(k) = \{(1, x_1, ..., x_n),\ (x_1, ..., x_n) \in \mathbb{A}^n(k)\} \cup \mathbb{P}^{n-1}(k).$$

O primeiro conjunto da reunião é identificado como sendo $\mathbb{A}^n(k)$. Por exemplo, no caso $k = \mathbb{R}$, podemos escrever $\mathbb{P}^2(\mathbb{R}) = \{(1, a, b);\ (a, b) \in \mathbb{R}^2\} \cup \{(0, 1, c);\ c \in \mathbb{R}\} \cup \{(0, 0, 1)\}$ e os pontos com primeira coordenada nula são os pontos no infinito.

Para finalizar está seção, apresentamos outra maneira de identificar o espaço projetivo, o qual nos auxiliará em alguns resultados no capítulo 3.

Definição 1.5. Seja k um corpo arbitrário. O **espaço projetivo dual de dimensão** n **sobre** k, denotado por $\check{\mathbb{P}}^n(k)$, é definido como sendo o conjunto de todos os subespaços de dimensão n do espaço vetorial $\mathbb{A}^{n+1}(k) = k^{n+1}$.

[4] Uma bijeção contínua com inversa contínua.

Sabemos da álgebra linear que os subespaços vetoriais de dimensional n de $\mathbb{A}^{n+1}(k)$ podem ser expressos da seguinte forma $\mathrm{H}(p_0,...,p_n) = \{(x_0,...,x_n) \in \mathbb{A}^{n+1}(k);\ x_0p_0 + \cdots + x_np_n = 0\}$, para algum $(p_0,...,p_n) \neq 0$. Além disso, temos

$$\mathrm{H}(p_0,...,p_n) = \mathrm{H}(p'_0,...,p'_n) \Leftrightarrow [p_0 : \cdots : p_n] = [p'_0 : \cdots : p'_n] \in \mathbb{P}^n(k).$$

Deste modo, $H(p_0,...,p_n) \longleftrightarrow [p_0,...,p_n]$ identifica $\mathbb{P}^n(k)$ com $\check{\mathbb{P}}^n(k)$.

Proposição 1.9. *Dado $P = [p_0 : \cdots : p_n], P' = [p'_0 : \cdots : p'_n] \in \mathbb{P}^n(\mathbb{F}_q)$ distintos, então*

$$|\{H \in \check{\mathbb{P}}^n(\mathbb{F}_q);\ P, Q \in H\}| = \theta_q(n-2)$$

Demonstração. Para as coordenadas homogêneas de P e P' pertencerem ao conjunto $H(a_0,...,a_n)$, devemos ter

$$p_0a_0 + \cdots + p_na_n = p'_0a_0 + \cdots + p'_na_n = 0.$$

O conjunto solução $a_0,...,a_n$ forma um subespaço vetorial de dimensão $n-1$ em $\mathbb{A}^{n+1}(k)$, o qual corresponde em $\mathbb{P}^n(k)$ como sendo um subespaço de codimensão 2.

■

Observação 1.4. Dado $P \in \mathbb{P}^n(k)$, com um argumento análogo feito na proposição anterior, tem-se

$$|\{H \in \check{\mathbb{P}}^n(\mathbb{F}_q);\ P \in H\}| = \theta_q(n-1).$$

1.3.1 Mudança linear no sistema de coordenadas projetivas

Depois de definido um novo espaço é comum estudar os automorfismos existentes. Por exemplo, considerando $E = k^{n+1}$ como um k-espaço vetorial, estudamos na álgebra linear as funções bijetoras $A : E \to E$ tais que

$$A(\alpha x + y) = \alpha A(x) + A(y)$$

para todo $x, y \in E$ e $\alpha \in k$, chamadas de **transformações lineares** (bijetoras). Uma vez fixado em E a base canônica, existe um isomorfismo natural entre o conjunto das transformações lineares $A : E \to E$ e o conjunto das matrizes inversíveis de ordem $n+1$ com coeficientes em k, chamado **grupo linear geral** e denotado por $GL_{n+1}(k)$. Sendo assim, ao considerarmos $A : E \to E$ uma transformação linear, denotaremos também por A a matriz associada em $GL_{n+1}(k)$ em relação à base canônica e vice-versa. Como no caso do espaço afim $\mathbb{A}^{n+1}(k)$, não consideramos a estrutura vetorial existente, assim a origem não desempenha nenhum papel central. Os automorfismos que consideramos neste caso são $T : \mathbb{A}^{n+1}(k) \to \mathbb{A}^{n+1}(k)$ tais que $T(x) = A(x) + b$, onde $A : E \to E$ é uma transformação linear e $b \in \mathbb{A}^{n+1}(k)$, chamada de **transformação afim** (ou **afinidade**). Para o caso projetivo, primeiramente, observe que as retas de E que passam pela origem (subespaços vetoriais unidimensionais) são da forma $r = \{\alpha v; \alpha \in k\}$ para algum $v \in E$ não nulo. Segue daí que $A(r) = \{\alpha A(v);\ \alpha \in k\}$ é uma reta em E. Deste modo, fica bem definido

$$\mathrm{T} :\ \mathbb{P}^n(k) \to \mathbb{P}^n(k), \quad \text{com } \mathrm{T}([x_0 : \cdots : x_n]) = A \cdot \begin{bmatrix} x_0 \\ \vdots \\ x_n \end{bmatrix},$$

onde $A \in GL_{n+1}(k)$, isto é, se $A = (a_{ij})_{0 \leq i,j \leq n}$ então

$$\mathrm{T}([x_0 : \cdots : x_n]) = \left[\sum_{j=0}^{n} a_{0j}x_j : \cdots : \sum_{j=0}^{n} a_{nj}x_j \right],$$

chamada **transformação projetiva** (ou **projetividade**). Observe que uma transformação projetiva diz respeito a uma mudança linear no sistema de coordenada de $\mathbb{P}^n(k)$, considerando

$$(y_0, ..., y_n) = \left(\sum_{j=0}^{n} a_{0j}x_j, ..., \sum_{j=0}^{n} a_{nj}x_j \right),$$

então $y_0, ..., y_n$ são as novas coordenadas homogêneas de $\mathbb{P}^n(k)$.

Claramente, $A, B \in GL_{n+1}(k)$ definem a mesma transformação projetiva se, e somente se, $A = \lambda B$ para algum $\lambda \in k$ não nulo. Segue daí que o grupo das transformações projetivas é isomorfo à

$$PGL_n(k) := \frac{GL_{n+1}(k)}{\{\lambda Id\}},$$

chamado de **grupo linear projetivo**.

Antes de prosseguirmos com mais algumas questões sobre mudança linear no sistema de coordenadas, precisamos de algumas definições da álgebra comutativa.

Definição 1.6. Seja $R \neq \{0\}$ um anel comutativo com unidade. Dizemos que R é uma k **- álgebra** se existe um homomorfismo de anéis $f : k \to R$. Neste caso, como os únicos ideais de k são os triviais e $f(1) = 1$, f é injetivo e podemos considerar k como subanel de R.

Observação 1.5. $(a, r) \in k \times R \longmapsto f(a) \cdot r \in R$ torna o anel R um k - espaço vetorial.

Exemplo 1.9. O anel do polinômio em $n + 1$ indeterminadas $k[X_0, ..., X_n]$ é uma k-álgebra com o homomorfismo natural $f : k \to k[X_0, ..., X_n]$ dada por $a \longmapsto f_a(X_0, ..., X_n) = a$.

Definição 1.7. Sejam R e R' duas k-álgebras. Dizemos que $f : R \to R'$ é um homomorfismo de k-álgebras se:

i) $f : R \to R'$ é um homomorfismo de anéis.

ii) $f : R \to R'$ é uma transformação linear ao considerarmos R e R' como sendo k-espaços vetoriais (veja, observação 1.5).

Além disso, se f for bijetora dizemos que ela é um k**-isomorfismo**.

Cada matriz $A \in GL_{n+1}(k)$ induz um k-isomorfismo

$$A^* : k[Y_0, ..., Y_n] \to k[X_0, ..., X_n],$$

onde para cada $f \in k[Y_0, ..., Y_n]$ a função A^* associa o polinômio A^*f tal que

$$(A^*f)(x_0, ..., x_n) = f(A^{-1}(x_0, ..., x_n))$$

para todo $(x_0, ..., x_n) \in k^{n+1}$. Mais explicitamente, se $A^{-1} = (b_{ij})_{0 \leq i,j \leq n}$ é a inversa de A, então

$$(A^*f)(X_0, ..., X_n) = f\left(\sum_{j=0}^{n} b_{0j}X_j, ..., \sum_{j=0}^{n} b_{nj}X_j \right).$$

Exemplo 1.10. Considere

$$A = \begin{pmatrix} 1 & 2 & 3 \\ 0 & 1 & 2 \\ 0 & 0 & 1 \end{pmatrix} \in GL_3(\mathbb{C})$$

cuja inversa é dada por

$$A^{-1} = \begin{pmatrix} 1 & -2 & 1 \\ 0 & 1 & -2 \\ 0 & 0 & 1 \end{pmatrix}.$$

Deste modo, se $T : \mathbb{P}^2(\mathbb{C}) \to \mathbb{P}^2(\mathbb{C})$ é definida por A, então

$$T([x_0 : x_1 : x_2]) = [x_0 + 2x_1 + 3x_2 : x_1 + 2x_2 : x_2]$$

e $A^* : k[Y_0, Y_1, Y_2] \to k[X_0, X_1, X_2]$ é definido por

$$(A^* f)(X_0, X_1 X_2) = f(X_0 - 2X_1 + X_2, X_1 - 2X_2, X_2)$$

Po exemplo, considere a parábola projetiva $f = Y_1 Y_2 - Y_0^2$ então

$$\begin{aligned}
(A^* f) &= f(X_0 - 2X_1 + X_2, X_1 - 2X_2, X_2) \\
&= (X_1 - 2X_2)X_2 - (X_0 - 2X_1 + X_2)^2 \\
&= X_1 X_2 - 2X_2^2 - ((X_0 - 2X_1)^2 + 2(X_0 - 2X_1)X_2 + X_2^2) \\
&= X_1 X_2 - 2X_2^2 - (X_0^2 - 4X_0 X_1 + 4X_1^2 + 2X_0 X_2 - 4X_1 X_2 + X_2^2) \\
&= X_1 X_2 - 2X_2^2 - X_0^2 + 4X_0 X_1 - 4X_1^2 - 2X_0 X_2 + 4X_1 X_2 - X_2^2 \\
&= 5X_1 X_2 - 3X_2^2 - X_0^2 + 4X_0 X_1 - 4X_1^2 - 2X_0 X_2.
\end{aligned}$$

Capítulo 2

Variedades no espaço projetivo

Como já havíamos mencionado, o conceito de variedades é um dos principais objetos de estudo da geometria algébrica clássica. No caso afim, ela consiste no lugar geométrico onde uma coleção de equações polinomiais é satisfeita. Neste capítulo, estamos interessados em estender esta definição para o caso projetivo, entretanto, uma vez que o espaço projetivo é o quociente de uma relação de equivalência, o mínimo que esperamos é que a definição de variedades no espaço projetivo não dependa da escolha do representante da classe. Claramente, isso não acontece para todo polinômio. Desse modo, na primeira seção deste capítulo, definimos uma classe muito especial de polinômio (homogêneos) e associamos a cada polinômio com n variáveis um polinômio homogêneo com $n+1$ variáveis (homogenização). Posteriormente, definimos variedades no espaço projetivo e apresentamos uma versão do teorema Nullstellensatz no caso projetivo, que nos possibilita caracterizar as hipersuperfícies de forma análoga do caso afim. Para finalizar o capítulo, falamos sobre hipersuperfícies equivalentes, espaço tangente de uma variedade projetiva em um ponto e o teorema de Bezout.

2.1 Polinômios homogêneos e homogenização

Tendo em vista a definição de variedades no espaço afim, poderíamos, de forma ingênua, tentar definir de modo semelhante variedades no espaço projetivo. Entretanto, ao definir um novo conceito em um espaço de classes de equivalência, em geral, é utilizado um elemento como representante de cada classe, mas, para uma boa definição, sempre é indispensável que o conceito não dependa da escolha do representante. Vejamos, por meio de um exemplo, como em geral o conjunto dos zeros de um polinômio no espaço projetivo não está bem definido para todo polinômio: considere o polinômio $f(X,Y) = X^2 + Y^2 - 2 \in \mathbb{C}[X,Y]$. Temos $[1:1] = [2:2]$ em $\mathbb{P}^1(\mathbb{C})$. Observe que $f(1,1) = 0 \neq 6 = f(2,2)$. Deste modo, o conjunto dos zeros de $f = X^2 + Y^2 - 2$ em $\mathbb{P}^1(\mathbb{C})$ não está bem definido, pois neste caso a equação $f = 0$ depende da escolha do representado da classe.

Definição 2.1. Seja k um corpo arbitrário. Dizemos que um polinômio $f \in k[X_0, ..., X_n]$ é **homogêneo de grau** $d \geq 0$ se todos os seus monômios não nulos têm o mesmo grau total igual a d.

Exemplo 2.1. Para todo $d \geq 0$ o polinômio $f = X_0^d + \cdots + X_n^d$ é homogêneo de grau d.

Talvez, experiências com cálculo ou equações diferenciais faça o leitor estranhar a definição de polinômio homogêneo. Pois bem, mostraremos a seguir que a definição dada acima é equivalente à definição que geralmente aparece no mercado.

Proposição 2.1. *Seja $f \in k[X_0, ..., X_n]$ não nulo. Então f é homogêneo de grau $d \geq 0$ se, e somente se, $f(\lambda X_0, ..., \lambda X_n) = \lambda^d f(X_0, ..., X_n)$ para todo $\lambda \in k$.*

Demonstração. Suponha que f seja homogêneo de grau d. Assim, podemos escrever

$$f = \sum_{j=1}^{m} a_j X_0^{\alpha_j^0} \cdots X_n^{\alpha_j^n},$$

onde $\alpha_j^0 + \cdots + \alpha_j^n = d$ e $a_j \in k$ para todo $j = 1, ..., m$. Logo, para todo $\lambda \in k$ vale

$$\begin{aligned} f(\lambda X_0, ..., \lambda X_n) &= \sum_{j=1}^{m} a_j (\lambda X_0)^{\alpha_j^0} \cdots (\lambda X_n)^{\alpha_j^n} \\ &= \sum_{j=1}^{m} a_j \lambda^{\alpha_j^0} X_0^{\alpha_j^0} \cdots \lambda^{\alpha_j^n} X_n^{\alpha_j^n} \\ &= \sum_{j=1}^{m} a_j \ \lambda^{\alpha_j^0 + \cdots + \alpha_j^n} \ X_0^{\alpha_j^0} \cdots X_n^{\alpha_j^n} \\ &= \lambda^d f(X_0, ..., X_n). \end{aligned}$$

Reciprocamente, suponha que $f(\lambda X_0, ..., \lambda X_n) = \lambda^d f(X_0, ..., X_n)$ para todo $\lambda \in k$. Seja $a_\alpha X^\alpha$ um termo monomial não nulo de f, com $\alpha = (\alpha_1, ..., \alpha_n)$ e $X = X_0 \cdots X_n$. Assim, por hipótese, tem-se

$$a_\alpha (\lambda X_0)^{\alpha_1} \cdots (\lambda X_n)^{\alpha_n} = \lambda^d a_\alpha X^\alpha.$$

Deste modo, devemos ter $\lambda^{\alpha_1} \cdots \lambda^{\alpha_n} = \lambda^d$, consequentemente, $\alpha_1 + \cdots + \alpha_n = d$. Portanto, f é um polinômio homogêneo de grau d.

■

Seja h o polinômio identicamente nulo em $k[X_0, ..., X_n]$. Como h não possui monômios não nulo é natural, por vacuidade, considerar h como sendo homogêneo de grau d para todo $d \geq 0$. Esta simples convenção nos possibilita decompor cada polinômio $f \in k[X_0, ..., X_n]$ não identicamente nulo como uma soma de polinômios homogêneos $f = f_0 + f_1 + \cdots + f_d$, onde $d = grau(f)$ e cada f_j é um polinômio homogêneo de grau j em $k[X_0, ..., X_n]$. Basta agrupar os monômios com mesmo grau total. Chamamos de **componentes homogêneas de** f os polinômios $f_0, ..., f_d$.

Exemplo 2.2. As componentes homogêneas de $f = 2X^2 + XY^2 + 5XZ + 3Z^3 \in \mathbb{C}[X, Y, Z]$ são $f_0 = 0$, $f_1 = 0$, $f_2 = 2X^2 + 5XZ$ e $f_3 = XY^2 + 3Z^3$.

Definição 2.2. Dizemos que um ideal $I \subseteq k[X_0, ..., X_n]$ é homogêneo se admite uma coleção de geradores homogêneos.

Observação 2.1. Ao considerarmos um ideal homogêneo $I = \langle F_1, ..., F_m \rangle \subseteq k[X_0, ..., X_n]$ ficará subentendido que $F_1, ..., F_m$ são polinômios homogêneos de $k[X_0, ..., X_n]$.

Lema 2.1. *Sejam $f, g \in k[X_0, ..., X_n]$ ambos não identicamente nulo. Sejam $f_0, ..., f_m$ e $g_0, ..., g_s$ as componentes homogêneas de f e g, respectivamente.*

i) Se $m = s$, então $f = g$ se, e somente se, $f_j = g_j$ para todo $j = 0, ..., m$.

ii) Se $h = fg$, então as componentes homogêneas de h são dadas por $h_l = \sum_{i+j=l} f_i g_j$.

Demonstração. O item (i) segue diretamente da definição de igualdade de polinômios. Deixamos os detalhes para o leitor.

ii) Temos

$$h = fg = \left(\sum_i f_i\right)\left(\sum_j g_j\right) = \sum_{i,j} f_i g_j.$$

Observe que $f_i g_j$ é homogêneo de grau $i+j$. Segue do item (i) que $h_l = \sum_{i+j=l} f_i g_j$ são as componentes homogêneas de h.

■

Proposição 2.2. *O ideal $I \subseteq k[X_0, ..., X_n]$ é homogêneo se, e somente se, para todo $g \in I$ as componentes homogêneas de g pertencem a I.*

Demonstração. Suponha que $I \subseteq k[X_0, ..., X_n]$ seja um ideal homogêneo. Assim, existem $f_1, ..., f_m$ em $k[X_0, ..., X_n]$ homogêneos não nulos de grau $d_1, ..., d_m$, respectivamente, tais que $I = \langle f_1, ..., f_m \rangle$.

Dado $g \in I$ existem $g_1, ..., g_m \in k[X_0, ..., X_n]$ tais que

$$g = g_1 f_1 + \cdots + g_m f_m.$$

Como f_j é homogêneo de grau d_j, existe apenas uma componente homogênea não nula a saber: $f_{d_j} = f_j$. Sejam $g_{j_1}, ..., g_{j_s}$ componentes homogêneas de g_j. Segue do lema 2.1 que

$$g_l = g_{1'_r} f_1 + \cdots + g_{j'_r} f_m \in I,$$

onde $1'_r + d_1 = \cdots = j'_r + d_m = l$ são as componentes homogêneas de g.

Reciprocamente, suponha que para todo $g \in I$ as componentes homogêneas de g pertencem a I. Pelo teorema da base de Hilbert 1.1, existem $f_1, ..., f_m \in I$ (não necessariamente homogêneos) tais que $I = \langle f_1, ..., f_m \rangle$. Escreva f_j como soma das suas componentes homogêneas $f_j = \sum_i f_{ji}$, com $j = 1, ..., m$. Por hipótese, tem-se $f_{ji} \in I$ para todo i, j. Deste modo, se J é o ideal gerado pelas componentes homogêneas dos polinômios $f_1, ..., f_m$, então $I \subseteq J$. Por outro lado, como cada componente está em I temos $J \subseteq I$. Logo, $I = J$ é homogêneo.

■

Proposição 2.3. *Seja k um corpo infinito. Sejam $F \in k[X_0, ..., X_n]$ e $F_0, ..., F_m$ as componentes homogêneas de F. Se F se anula em todas coordenadas homogêneas de $P \in \mathbb{P}^n(k)$, então*

$$F_0(P) = \cdots = F_m(P) = 0.$$

Demonstração. Sejam $a_0, ..., a_n$ coordenadas homogêneas de P. Defina o polinômio

$$G(X) = f(Xa_0, ..., Xa_n) \in k[X].$$

Por hipótese, temos $G(x) = 0$ para todo $x \neq 0$. Sendo k infinito, tem-se que G é o polinômio identicamente nulo, pois um polinômio não nulo de uma variável tem apenas finitas raízes em k. Além disso, temos

$$\begin{aligned} G(X) &= f(Xa_1, ..., Xa_n) \\ &= \sum_{i=0}^{m} F_i(Xa_0, ..., Xa_n) \\ &= \sum_{i=0}^{m} X^i F_i(a) \end{aligned}$$

Portanto, $F_0(a) = \cdots = F_m(a) = 0$. ■

Para finalizar esta seção, vamos falar brevemente sobre homogenização e desomogenização de polinômios.

Proposição 2.4. *A função* $\Phi_i : k[X_0, ..., X_n] \to k[Y_0, ..., Y_{i-1}, Y_{i+1}, ..., Y_n]$ *definida por*

$$\begin{array}{rcl} X_i & \longmapsto & 1 \\ X_j & \longmapsto & Y_j \quad se\ j \neq i \end{array}$$

é um homomorfismo de anéis.

Demonstração. Basta observar que a função é o seguinte homomorfismo de avaliação

$$f(X_0, ..., X_n) \longmapsto f(Y_0, ..., Y_{i-1}, 1, Y_{i+1}, ..., Y_n).$$

■

O polinômio $\Phi_i(f)$ é chamado **desomogenização** de f em relação à variável X_i.
Para $f \in k[Y_0, ..., Y_{i-1}, Y_{i+1}, ..., Y_n]$ temos

$$\Phi_i^{-1}(f) = \left\{ X_i^D \cdot f\left(\frac{X_0}{X_i}, ..., \frac{X_{i-1}}{X_i}, \frac{X_{i+1}}{X_i}, ..., \frac{X_n}{X_i}\right);\ D \geq grau(f) \right\}$$

Definição 2.3. Dado $f \in k[Y_0, ..., Y_{i-1}, Y_{i+1}, ..., Y_n]$, defina-se a **homogenização** de f com respeito à variável X_i como sendo o polinômio

$$F(X_0, ..., X_n) = X_i^{grau(f)} \cdot f\left(\frac{X_0}{X_i}, ..., \frac{X_{i-1}}{X_i}, \frac{X_{i+1}}{X_i}, ..., \frac{X_n}{X_i}\right)$$

Vale observar que a F é um polinômio homogêneo de grau $d = grau(f)$. Com efeito, para facilitar a notação considere a homogeneização de f em relação à variável X_0, isto é,

$$F = X_0^{grau(f)} \cdot f\left(\frac{X_1}{X_0}, ..., \frac{X_n}{X_0}\right)$$

Seja $X = (X_1, ..., X_n)$. Se $a \cdot Y^\alpha = a \cdot Y_1^{\alpha_1} \cdots Y_n^{\alpha_n}$ é um termo monomial de f, então $|\alpha| := \alpha_1 + \cdots + \alpha_n \leq d$ e os termos monomiais de F são do tipo

$$a \cdot X_0^d \cdot \frac{X^\alpha}{X_0^{|\alpha|}} = a \cdot X_0^{d-|\alpha|} \cdot X^\alpha.$$

Portanto, F é um polinômio homogêneo de grau d.

Exemplo 2.3. Considere $f = Y - X^2 \in k[X, Y]$. Então a homogenização de f em relação à variável Z é, por definição, o polinômio homogêneo

$$F(X, Y, Z) = Z^2 f\left(\frac{X}{Z}, \frac{Y}{Z}\right) = Z^2\left(\frac{Y}{Z} - \frac{X^2}{Z^2}\right) = YZ - X^2.$$

2.2 Variedades projetivas

Em geral, o valor de um polinômio em um ponto do espaço projetivo não esta bem definido. Por outro lado, pela proposição 2.1, o conjunto de zeros no espaço projetivo de um polinômio está bem definido desde que ele seja homogêneo. Isso nos leva a seguinte definição:

Definição 2.4. Sejam k um corpo arbitrário e $F \in k[X_0, ..., X_n]$ homogêneo:

i) Uma **hipersuperfície** em $\mathbb{P}^n(k)$ definida por F, denotada por $\mathbf{v}(F)$, é definida por

$$\mathbf{v}(F) := \{[x_0 : \cdots : x_n] \in \mathbb{P}^n(k); \quad F(x_0, ..., x_n) = 0\}.$$

ii) O **grau da hipersuperfície** $\mathbf{v}(F)$, denotado por $deg(\mathbf{v}(F))$, é o grau do polinômio F.

iii) Se $G \in k[X_0, ..., X_n]$ é irredutível e divide F, dizemos que a hipersuperfície $\mathbf{v}(G) \subseteq \mathbb{P}^n(k)$ é uma **componente** de $\mathbf{v}(F)$. (Observação: Se $G|F$, então G é homogêneo).

iv) Uma hipersuperfície H de grau 1 é chamado de **hiperplano**, isto é,

$$H = \mathbf{v}(a_0X_0 + \cdots + a_nX_n) \subseteq \mathbb{P}^n(k),$$

onde $a_0, ..., a_n \in k$ não são todos nulos.

Todo hiperplano é um subespaço de codimensão 1 em $\mathbb{P}^n(k)$, pois o conjunto solução de $a_0X_0 + \cdots + a_nX_n = 0$ em $\mathbb{A}^{n+1}(k)$ é um subespaço de dimensão n. Em particular, quando $k = \mathbb{F}_q$, todo hiperplano em $\mathbb{P}^n(\mathbb{F}_q)$ tem $\theta_q(n-1)$ pontos. De modo Geral, podemos definir:

Definição 2.5. Seja k um corpo arbitrário e sejam $F_1, ..., F_m \in k[X_0, ..., X_n]$ homogêneos. Chamamos

$$\mathbf{v}(F_1, ..., F_m) := \{[a_0 : \cdots : a_n] \in \mathbb{P}^n(k); \ F_1(a_0, ..., a_n) = \cdots = F_m(a_0, ..., a_n) = 0\}$$

de **variedade projetiva** definida por $F_1, ..., F_m$.

Em particular, quando os polinômios são homogêneo de grau 1, dizemos também que a variedade projetiva é **linear**. Claramente, as variedades projetivas lineares são subespaços de $\mathbb{P}^n(k)$, além disso, qualquer subespaço de dimensão m de $\mathbb{P}^n(k)$ pode ser visto como sendo uma variedade linear.

Exemplo 2.4. Identificando o espaço projetivo como no exemplo 1.8, uma hipersuperfície $\mathcal{X}$ em $\mathbb{P}^n(k)$, definida pelo polinômio homogêneo $F \in k[X_0, ..., X_n]$, pode ser escrita por

$$\mathcal{X} = \{(1, x_1, ..., x_n); \ F(1, x_1, ..., x_n) = 0\} \cup \{(0, a_1, ..., a_n); F(0, a_1, ..., a_n) = 0\}.$$

Observe que $f = F(1, X_0, ..., X_n)$ é a desomogenização em relação à variável X_0, além disso, existe uma correspondência natural entre $\mathbb{V}(f) \subseteq \mathbb{A}^n(k)$ e

$$\{(1, x_1, ..., x_n); \ F(1, x_1, ..., x_n) = 0\}.$$

Desse modo, pelos processos de homogenização e desomogenização, uma hipersuperfície no espaço projetivo está intimamente relacionado com uma hipersuperfície no espaço afim, de modo que no contexto projetivo apenas estamos considerando os pontos no infinito discutido no início da seção 3 do primeiro capítulo.

Uma vez definido variedades no espaço projetivo, nosso próximo objetivo é apresentar uma versão do teorema Nullstellensatz no caso projetivo. Para tal propósito, vamos associar a cada ideal homogêneo uma variedade projetiva: segue da proposição 2.2, que dado $I \subseteq k[X_0, ..., X_n]$ ideal homogêneo, o conjunto

$$\mathbf{v}(I) := \{[x_0 : \cdots : x_n] \in \mathbb{P}^n(k); \ F(x_0, ..., x_n) = 0 \ \forall F \in I\}$$

está bem definido. Vamos mostrar que $\mathbf{v}(I)$, tendo como base a definição 2.5, é uma variedade projetiva, chamada de **variedade projetiva gerada por** I.

Proposição 2.5. *Dado $I = \langle F_1, ..., F_m \rangle \subseteq k[X_0, ..., X_n]$ um ideal homogêneo. Então*

$$\mathbf{v}(I) = \mathbf{v}(F_1, ..., F_m).$$

Demonstração. Claramente, por definição, temos $\mathbf{v}(I) \subseteq \mathbf{v}(F_1, ..., F_m)$.

Sejam $[x_0 : \cdots : x_n] \in \mathbf{v}(F_1, ..., F_m)$ e $F \in I$. Assim existem $G_1, ..., G_m \in k[X_0, ..., X_n]$, não necessariamente homogêneos, tais que

$$F = G_1F_1 + \cdots + G_mF_m.$$

A equação $G_j = 0$ pode depender da escolha do representante da classe. Por outro lado, a equação $G_jF_j = 0$ é igual a zero para toda coordenada homogênea do ponto $[x_0 : \cdots : x_n]$, pois $F_j = 0$ independente da escolha. Considerando $x = (x_0, ..., x_n)$, temos

$$F(x) = G_1(x)F_1(x) + \cdots G_m(x)F_m(x) = 0,$$

consequentemente, $[x_0 : \cdots : x_n] \in \mathbf{v}(I)$ e assim $\mathbf{v}(F_1, ..., F_m) \subseteq \mathbf{v}(I)$.

Portanto, $\mathbf{v}(I) = \mathbf{v}(F_1, ..., F_m)$.

■

Para não houver possibilidade de confusão lembre-se que, a menos que seja mencionado o contrário, estamos sempre considerando k um corpo algebricamente fechado. Um resultado simples que vai nos possibilitar, juntamente com a proposição 2.3, gerar ideais homogêneos com subconjuntos do espaço projetivo é que todo corpo algebricamente fechado é infinito:

Proposição 2.6. *Se k é um corpo algebricamente fechado, então k é infinito.*

Demonstração. Suponha que k seja finito, digamos $k = \{a_1, ..., a_m\}$. Considere o polinômio

$$f(x) = 1 + \prod_{j=1}^{m}(x - a_j) \in k[x].$$

Assim, para todo $j = 1, ..., m$ tem-se $f(a_j) = 1$, ou seja, f não possui raiz em k. Contrariando o fato de k ser algebricamente fechado. Portanto, k é infinito.

■

Uma maneira, natural, de gerar ideais homogêneos usando variedades projetivas é definir o ideal gerado pelos polinômios que geram a variedade, isto é, se $\mathbf{v}(F_1, ..., F_n)$ é uma variedade projetiva, então $\langle F_1, ..., F_m \rangle$ é um ideal é homogêneo. Existe também outra maneira de uma variedade projetiva gerar um ideal homogêneo. Primeiramente, convencionamos que dado $S \subseteq \mathbb{P}^n(k)$, ao considerarmos $F \in k[X_0, ..., X_n]$ tal que $F(x_0, ..., x_n) = 0$ para algum $[x_0 : \cdots : x_n] \in S$ ficará subentendido que a expressão $F = 0$ independe da escolha do representada da classe.

Proposição 2.7. *Seja $S \subseteq \mathbb{P}^n(k)$. O seguinte conjunto é um ideal homogêneo*

$$\mathbb{J}(S) := \{F \in k[X_0, ..., X_n];\ F(x_0, ..., x_n) = 0 \ \ \forall [x_0 : \cdots : x_n] \in S\}.$$

Demonstração. Análogo ao caso afim, feito na proposição 1.1, tem-se que $\mathbb{J}(S)$ é um ideal de $k[X_0, ..., X_n]$.

Sejam $F \in \mathbb{J}(S)$ e $F_0, ..., F_m$ as componente homogêneas de F. Dado $[x_0 : \cdots : x_n] \in S$ temos $F(x_0, ..., x_n) = 0$. Pela proposição 2.3, tem-se

$$F_0(x_0, ..., x_n) = \cdots = F_m(x_0, ..., x_n) = 0.$$

Assim, $F_0, ..., F_m \in \mathbb{J}(S)$. Portanto, pela proposição 2.2, $\mathbb{J}(S)$ é um ideal homogêneo.

■

No caso afim, por meio do teorema Nullstellensatz 1.2 é possível verificar que o ideal gerado por uma variedade afim é igual ao radical do ideal que gera a variedade. Como no contexto projetivo, as variedade são geradas por ideais homogêneos seria interessante se o radical de um ideal homogêneo fosse também um idel homogêneo. Felizmente, isso acontece:

Lema 2.2. *Seja I ideal homogêneo em $k[X_0, ..., X_n]$. Então rad(I) é um ideal homogêneo.*

Demonstração. Seja $f \in \text{rad}(I)$. Assim, existe $m \geq 1$ tal que $f^m \in I$. Se $f \neq 0$ decomponha f como soma das suas componentes homogêneas

$$f = \sum_j f_i = f_{max} + \sum_{j<max} f_i,$$

onde f_{max} é a componente homogênea não nula de grau total igual ao grau de f. Expandindo f^m, tem-se

$$(f^m)_{max} = (f_{max})^m.$$

Sendo I um ideal homogêneo tem-se, pela proposição 2.2, que as componentes homogêneas de f^m pertencem a I, consequentemente, $(f_{max})^m = (f^m)_{max} \in I$. Assim, $f_{max} \in \text{rad}(I)$. Considere $g = f - f_{max} \in \text{rad}(I)$. Com o mesmo argumento feito anteriormente, tem-se $g_{max} \in \text{rad}(I)$. Observe que g_{max} é uma componente homogênea de f. Aplicando esse raciocínio repetidamente, obtemos que as componentes homogêneas de f estão em rad(I). Portanto, segue da proposição 2.2, que rad(I) é um ideal homogêneo em $k[X_0, ..., X_n]$.

■

Teorema 2.1 (Nullstellensatz projetivo)**.** *Seja I ideal homogêneo de $k[X_0, ..., X_n]$. Se $\mathbf{v}(I)$ é um conjunto não vazio, então*

$$\mathbb{J}(\mathbf{v}(I)) = \text{rad}(I).$$

Demonstração. Seja $V = \mathbb{V}(I) \subseteq \mathbb{A}^{n+1}(k)$. Afirmamos que

$$\mathbb{I}(V) = \mathbb{J}(\mathbf{v}(I)).$$

Com efeito, seja $F \in \mathbb{I}(V)$. Dado $P \in \mathbf{v}(I)$, as coordenada homogêneas de P estão em V, assim $F(P) = 0$, consequentemente, $\mathbb{I}(V) \subseteq \mathbb{J}(\mathbf{v}(I))$. Seja $F \in \mathbb{J}(\mathbf{v}(I))$. Dado $(a_0, ..., a_n) \in V$ não nulo, tem-se $P = [a_0, ..., a_n] \in \mathbf{v}(I)$. Deste modo, resta mostrar que $F(0, ..., 0) = 0$. Seja F_0 a componente homogênea de grau zero de F, isto é, $F_0 = F(0, ..., 0)$. Como $\mathbb{J}(\mathbf{v}(I))$ é um ideal homogêneo tem-se $F_0 \in \mathbb{J}(\mathbf{v}(I))$. Sendo $\mathbf{v}(I) \neq \emptyset$ devemos ter $F_0 = 0$. Logo, $\mathbb{J}(\mathbf{v}(I)) \subseteq \mathbb{I}(V)$.

Portanto, $\mathbb{I}(V) = \mathbb{J}(\mathbf{v}(I))$. Segue do teorema Nullstellensatz 1.2 que

$$\text{rad}(I) = \mathbb{I}(\mathbb{V}(I)) = \mathbb{I}(V) = \mathbb{J}(\mathbf{v}(I)).$$

■

Com esta versão de Nullstellensatz no caso projetivo, podemos, de maneira semelhante ao caso afim, caracterizar as hipersuperfícies em $\mathbb{P}^n(k)$. Antes, precisamos de dois lemas:

Lema 2.3. *Sejam $F, G, H \in k[X_0, ..., X_n]$ polinômios não nulos. Se F é homogêneo de grau $d \in \mathbb{N}$ e $F = GH$, então G e H são homogêneos.*

Demonstração. Como F é homogêneo de grau d, temos apenas uma componente homogênea a saber: $F_d = F$. Sejam $G_0, ..., G_s$ e $H_0, ..., H_r$ as componentes homogêneas de G e H, respectivamente. Segue do lema 2.1 item (ii) que

$$G_s H_r = F_d = F = GH = (G_0 + \cdots + G_s)(H_0 + \cdots + H_r).$$

Portanto, $G = G_s$ e $H = H_r$ são homogêneos.

■

Corolário 2.1. *Se $F_1, ..., F_m$ são as componentes irredutíveis de um polinômio homogêneo F em $k[X_0, ..., X_n]$, então $F_1, ..., F_m$ são homogêneos, consequentemente, $F_1 \cdots F_m$ é homogêneo.*

Lema 2.4. *Seja $\mathbf{v}(I)$ uma variedade projetiva, então $\mathbf{v}(\mathbb{J}(\mathbf{v}(I))) = \mathbf{v}(I)$.*

Demonstração. Análogo ao caso afim (proposição 1.4).

■

Proposição 2.8. *Seja $I \subseteq k[X_0, ..., X_n]$ um ideal homogêneo. Então $\mathbf{v}(I)$ é uma hipersuperfície se, e somente se, $\mathbb{J}(\mathbf{v}(I)) = \langle G \rangle$ para algum $G \in k[X_0, ..., X_n]$ homogêneo.*

Demonstração. Suponha que $\mathbf{v}(I) = \mathbf{v}(F)$ para algum polinômio $F \in k[X_0, ..., X_n]$ homogêneo. Como k é algebricamente fechado, temos $\mathbf{v}(I) = \mathbf{v}(F) \neq \emptyset$. Segue do teorema Nullstellensatz projetivo 2.1 que

$$\mathbb{J}(\mathbf{v}(I)) = \mathbb{J}(\mathbf{v}(F)) = rad(\langle F \rangle) = \langle F_1 \cdots F_m \rangle,$$

onde $F_1, ..., F_m$ são as componentes irredutíveis de F em $k[X_0, ..., X_n]$ (Para a última igualdade, veja a demostração do corolário do Nullstellensatz 1.3). Além disso, pelo corolário do lema 2.3, temos $F_1 \cdots F_m$ é homogêneo.

Reciprocamente, suponha que $\mathbb{J}(\mathbf{v}(I)) = \langle G \rangle$ para algum $G \in k[X_0, ..., X_n]$ homogêneo. Assim, pela proposição 2.4, temos

$$\mathbf{v}(I) = \mathbf{v}(\mathbb{J}(\mathbf{v}(I))) = \mathbf{v}(\langle G \rangle) = \mathbf{v}(G).$$

■

Com a definição de variedades no espaço projetivo e os resultados anteriores, podemos, de forma completamente análoga ao caso afim, munir o espaço projetivo com um topologia, bastando considerar como conjunto aberto o complementar de uma variedade projetiva. Esta topologia é comumente chamada de **topologia de Zariski em** $\mathbb{P}^n(k)$. Além disso, o fecho projetivo de Zariski é caracterizado da mesma maneira do caso afim.

Para finalizar esta seção, como prometido, vamos mostrar agora que a função φ_i do lema 1.2 é um homeomorfismo entre espaços topológicos.

Proposição 2.9. *Para cada $i = 0, ..., n$ a função $\varphi_i : U_i \to \mathbb{A}^n(k)$ definida por*

$$\varphi_i([a_0 : \cdots : a_n]) = \left(\frac{a_0}{a_i}, \cdots, \frac{a_{i-1}}{a_i}, \frac{a_{i+1}}{a_i}, ..., \frac{a_n}{a_i} \right)$$

é um homeomorfismo.

Demonstração. Sabemos que φ_i é uma bijeção. Para provar que φ_i é um homeomorfismo, basta mostrar que ela e sua inversa são funções fechadas (levam conjunto fechado em conjunto fechado). Para simplificar a notação, considere $i = 0$. Seja $X \subseteq U_0$ um conjunto fechado. Se $\overline{X}$ denota o fecho projetivo de X em $\mathbb{P}^n(k)$, existe um ideal homogêneo J tal que $\overline{X} = \mathbf{v}(J)$. Considere $J_0 = \{\Phi_0(f);\ f \in J\}$ onde $\Phi_0(f)$ é a desomogenização de f em relação à variável X_0. Claramente, temos $\varphi_0(X) = \mathbb{V}(J_0)$. Para inclusão reversa, seja $V \subseteq \mathbb{A}^n(k)$ fechado. Assim existe um ideal I tal que $V = \mathbb{V}(I)$. Considere $I_0 = \{f^*;\ f \in I\}$ onde f^* é a homogenização de f em relação à variável X_0. Observe que $\varphi_0^{-1}(V) = U_0 \cap \mathbf{v}(I_0)$. O resultado segue.

■

2.2.1 Variedades Hermitianas em $\mathbb{P}^n(\mathbb{F}_{q^2})$

Existe uma coleção especial de variedades que desempenham um papel central no estudo sobre o número máximo de pontos de uma hipersuperfícies de grau d no espaço projetivo sobre um corpo finito, chamadas variedades Hermitianas. Nesta seção, estamos interessando no número de pontos que uma variedade Hermitiana não degenerada possui. Para um estudo detalhado sobre variedades Hermitianas indicamos a leitura de [2]. Antes, precisamos de um resultado sobre corpos finitos:

Proposição 2.10. *Para todo $x \in \mathbb{F}_q$ vale $x^q = x$.*

Demonstração. O caso $x = 0$ é óbvio. Sendo $\mathbb{F}_q$ um corpo, tem-se que $\mathbb{F}_q^* = \mathbb{F}_q \backslash \{0\}$ é um grupo multiplicativo de ordem $q-1$. Segue daí que para todo $x \in \mathbb{F}_q^*$ vale $x^{q-1} = 1$ e assim, multiplicando ambos os lados por x, obtemos $x^q = x$.

■

Dado $x \in \mathbb{F}_{q^2}$, o seu conjugado é definido como sendo x^q. Observe que, pela proposição 2.10, x é o conjugado de x^q. Denotaremos simplesmente por $\overline{x}$ o conjugado de x em $\mathbb{F}_{q^2}$. Dado $\mathrm{x} = (x_0, x_1, ..., x_n) \in \mathbb{A}^{n+1}(\mathbb{F}_{q^2})$, considere

$$\mathrm{x}^q = \begin{bmatrix} x_0^q \\ \vdots \\ x_n^q \end{bmatrix}. \tag{2.1}$$

Definição 2.6.

i) Uma matriz quadrada $\mathcal{H} = (h_{ij})$, com coeficientes em $\mathbb{F}_{q^2}$, é dita **hermitiana** se $h_{ij} = \overline{h_{ji}}$ para todo i, j.

ii) Uma **variedade hermitiana** $\mathcal{H}_{n-1}$ no espaço projetivo finito $\mathbb{P}^n(\mathbb{F}_{q^2})$ é definida como sendo o conjunto dos pontos $\mathrm{x} = [x_0 : x_1 : \cdots : x_n] \in \mathbb{P}^n(\mathbb{F}_{q^2})$ tais que $\mathrm{x}\mathcal{H}\mathrm{x}^q = 0$, onde $\mathcal{H} = (h_{ij})_{0 \le i,j \le n}$ é uma matriz hermitiana de ordem $n+1$ e x^q é o vetor coluna dado em (2.1), isto é, a variedade definida pelo polinômio homogêneo de ordem $q+1$

$$[X_0, \cdots, X_n]\mathcal{H} \begin{bmatrix} X_0^q \\ \vdots \\ X_n^q \end{bmatrix} = h_{00}X_0^{q+1} + \cdots + h_{0n}X_0X_n^q + \cdots + h_{n1}X_nX_0^q + \cdots + h_{nn}X_n^{q+1},$$

onde $h_{ij} = \overline{h_{ji}}$. Além disso, se posto$(\mathcal{H}) = n+1$, dizemos que $\mathcal{H}_{n-1}$ é uma **variedade hermitiana não degenerada**.

Exemplo 2.5. Claramente, a matriz identidade $\mathcal{H} = Id_{n+1}$ é hermitiana com posto $n+1$, assim, a variedade projetiva em $\mathbb{P}^n(\mathbb{F}_{q^2})$ associada é definida pelo polinômio

$$[X_0, \cdots, X_n]\mathcal{H} \begin{bmatrix} X_0^q \\ \vdots \\ X_n^q \end{bmatrix} = X_0^{q+1} + \cdots + X_n^{q+1},$$

ou seja, $\mathbf{v}(X_0^{q+1} + \cdots + X_n^{q+1})$ é uma variedade Hermitiana não degenerada em $\mathbb{P}^n(\mathbb{F}_{q^2})$.

Nosso próximo objetivo é apresentar o número de pontos em um variedade Hermitiana não degenerada, apresentado por Bose e Chakravarti em [2]. Antes disso, precisamos de mais algumas considerações sobre corpos finitos.

Teorema 2.2. *Para todo corpo finito $\mathbb{F}_q$, o grupo multiplicativo $\mathbb{F}_q^* = \mathbb{F}_q \backslash \{0\}$ é cíclico.*

Demonstração. Veja [10, teorema 2.8]. ■

Definição 2.7. Um gerador do grupo multiplicativo $\mathbb{F}_q^*$ é dito **elemento primitivo** de $\mathbb{F}_q$.

Exemplo 2.6. No corpo $\mathbb{Z}/(3) = \mathbb{F}_3 = \{0, 1, 2\}$ o elemento 2 é primitivo. Em geral, o corpo finito $\mathbb{F}_q$ possui $\Phi(q-1)$ elementos primitivos, onde Φ é a função de Euler.

Considere a extensão de corpo $\mathbb{F}_{q^2}$ de $\mathbb{F}_q$. Segue da proposição 2.10 que todo elemento não nulo $x \in \mathbb{F}_{q^2}$ satisfaz a equação $x^{q^2-1} = 1$. Se $\theta \in \mathbb{F}_{q^2}$ é um elemento primitivo então

$$0, \theta, \theta^2, ..., \theta^{q^2-1} = 1$$

são todos os elementos de $\mathbb{F}_{q^2}$. Considere $\phi = \theta^{q+1}$, temos

$$\phi^q = \theta^{q^2+q} = \theta^{q+1} = \phi.$$

Assim $\phi \in \mathbb{F}_q$, pois $\mathbb{F}_q$ é o corpo de raízes de $x^q - x$ sobre $\mathbb{F}_p$ onde $q = p^m$ e p é primo. Além disso,

$$0, \phi, \phi^2, ..., \phi^{q-1} = 1 \tag{2.2}$$

são todos distintos e elementos de $\mathbb{F}_q$. Segue daí que os elementos de $\mathbb{F}_q$ são descritos em (2.2) e ϕ é um elemento primitivo de $\mathbb{F}_q$. Deste modo, dado $x \in \mathbb{F}_{q^2}$ existe um único elemento $y \in \mathbb{F}_q$ com $y = x^{q+1}$. Mais ainda, se $y \in \mathbb{F}_q$ é não nulo existe precisamente $q+1$ elementos $x \in \mathbb{F}_{q^2}$ tais que $x^{q+1} = y$. Com efeito, se

$$y = \phi^i = \theta^{i(q+1)}, \quad 1 \leq i \leq q-1$$

então

$$x = \theta^{i+j(q-1)}, \quad j = 1, ..., q+1.$$

Se y é nulo então o correspondente em $\mathbb{F}_{q^2}$ é nulo.

Teorema 2.3 (Bose-Chakravarti)**.** *Se $\mathcal{X} = \mathbf{v}(X_0^{q+1} + \cdots + X_n^{q+1}) \subseteq \mathbb{P}^n(\mathbb{F}_{q^2})$, então*

$$|\mathcal{X}| = \frac{[q^{n+1} - (-1)^{n+1}][q^n - (-1)^n]}{q^2 - 1}.$$

Demonstração. Dado um corpo arbitrário k, denotaremos por $\mathrm{V}(n, k)$ o k - espaço vetorial k^n. Seja $\varphi : V(n, \mathbb{F}_{q^2}) \to V(n, \mathbb{F}_q)$ a função que associa o vetor $\mathbf{x}^T = (x_0, x_1, ..., x_n) \in \mathrm{V}(n, \mathbb{F}_{q^2})$ ao vetor $\mathbf{y}^T = (y_0, y_1, ..., y_n) \in \mathrm{V}(n, \mathbb{F}_q)$ onde $y_i = x_i^{q+1}$ com $i = 0, ..., n$. Observe que pelo exposto anteriormente, se $\mathbf{y}^T$ tem r coordenadas não nulas existem $(q+1)^r$ vetores $\mathbf{x}^T \in \mathrm{V}(n, \mathbb{F}_{q^2})$ que corresponde a $\mathbf{y}^T$.

Seja $X \in \mathbb{P}^n(\mathbb{F}_{q^2})$ o elemento gerada pelo vetor linha $\mathbf{x}^T$ com r coordenadas não nulas. Assim, qualquer um dos $q^2 - 1$ vetores linhas $\rho\mathbf{x}^T \in \mathrm{V}(n, \mathbb{F}_{q^2})$ representa o ponto X, onde ρ é um ponto não nulo de $\mathbb{F}_{q^2}$. Se $\mathbf{y}^T = \varphi(\mathbf{x}^T)$ e $Y \in \mathbb{P}^n(\mathbb{F}_q)$ é o elemento gerado pelo vetor linha $\mathbf{y}^T$, então dizemos que Y corresponde a X. Deste modo, o ponto $Y \in \mathbb{P}^n(\mathbb{F}_q)$ é determinado pelo ponto $X \in \mathbb{P}^n(\mathbb{F}_{q^2})$; como cada vetor $\rho\mathbf{x}^T$ representa o ponto X então o correspondente $a\mathbf{y}^T$, com $a = \rho^{q+1}$, representa o mesmo ponto em $\mathbb{P}^n(\mathbb{F}_q)$ que $\mathbf{y}^T$. Logo, Y é unicamente determinado por X. Inversamente, seja $\mathbf{y}^T \in \mathrm{V}(n, \mathbb{F}_q)$ representando o ponto $Y \in \mathbb{P}^n(\mathbb{F}_q)$. Se $\mathbf{y}^T$ tem r coordenadas não nulas existem $(q+1)^r$ vetores em $\mathrm{V}(n, \mathbb{F}_{q^2})$ correspondendo a $\mathbf{y}^T$. O ponto Y pode ser representando por $q-1$ vetores $a\mathbf{y}^T \in \mathrm{V}(n, \mathbb{F}_{q^2})$, onde $a \in \mathbb{F}_q$ é não nulo. Cada vetor corresponde a $(q+1)^r$ vetores de $\mathrm{V}(n, \mathbb{F}_{q^2})$. Como temos $q-1$ vetores $a\mathbf{y}^T$ isso

corresponde a $(q-1)(q+1)^r$ vetores em $\mathrm{V}(n,\mathbb{F}_{q^2})$. Segue do fato que existe q^2-1 vetores linha que representam o mesmo ponto em $\mathbb{P}^n(\mathbb{F}_{q^2})$, que cada ponto em $\mathbb{P}^n(\mathbb{F}_q)$ com r coordenadas não nulas corresponde a

$$\frac{(q-1)(q+1)^r}{q^2+1} = (q+1)^{r-1}$$

pontos em $\mathbb{P}^n(\mathbb{F}_{q^2})$.

A variedade hermitiana $\mathcal{X}$ consiste no conjunto de pontos $[x_0 : x_1 : \cdots : x_n] \in \mathbb{P}^n(\mathbb{F}_{q^2})$ tais que

$$\sum_{i=0}^{n} x_i\overline{x_i} = 0 \Leftrightarrow \sum_{i=0}^{n} x_i^{q+1} = 0.$$

Seja H o hiperplano em $\mathbb{P}^n(\mathbb{F}_q)$ com equação $y_0 + y_1 + \cdots + y_n = 0$. Pela correspondência entre pontos de $\mathbb{P}^n(\mathbb{F}_q)$ e $\mathbb{P}^n(\mathbb{F}_{q^2})$ descrito acima, temos $X \in \mathcal{X}$ se, e somente se, $Y \in H$.

Agora vamos determinar o número de pontos em H com exatamente r coordenadas não nulas. Dado $[y_0 : y_1 : \cdots : y_n] \in H$, com $y_0 + y_1 + \cdots + y_n = 0$, existem

$$\binom{n+1}{r}$$

possibilidade de escolher r coordenadas não nulas. Deste modo, basta saber quantos pontos existem com $y_1, ..., y_r$ não nulos tais que

$$y_1 + \cdots + y_r = 0. \tag{2.3}$$

Sabemos que existem $\theta_q(r-2)$ pontos projetivos satisfazendo (2.3). Com um argumento análoga obtemos

$$\binom{r}{1}\theta_q(r-3)$$

pontos com pelo menos uma coordenada não nula, porém, contamos duas vezes pontos com pelo menos duas coordenadas não nulas. Existem

$$\binom{r}{2}\theta_q(r-4)$$

pontos com pelo menos duas coordenadas não nula. Seguindo, usando o principio de inclusão e exclusão, existem

$$\binom{n+1}{r}\left[\theta(r-2) - \binom{r}{1}\theta_q(r-3) + \binom{r}{2}\theta_q(r-4) + \cdots + (-1)^{r-2}\binom{r}{r-2}\theta_q(0)\right] \tag{2.4}$$

pontos em H com r coordenadas não nulas. Considere

$$\begin{aligned}
A &= \theta(r-2) - \binom{r}{1}\theta_q(r-3) + \binom{r}{2}\theta_q(r-4) + \cdots + (-1)^{r-2}\binom{r}{r-2}\theta_q(0) \\
&= \sum_{i=0}^{r-2}(-1)^i\binom{r}{i}\theta_q(r-2-i) \\
&= \frac{1}{q-1}\sum_{i=0}^{r-2}(-1)^i\binom{r}{i}(q^{r-2-i+1}-1) \\
&= \frac{1}{q-1}\left(\sum_{i=0}^{r-2}(-1)^i\binom{r}{i}q^{r-1-i} - \sum_{i=0}^{r-2}\binom{r}{i}(-1)^i\right).
\end{aligned}$$

Segue do binômio de Newton para anéis que

$$0 = (1-1)^r = \sum_{i=0}^{r} \binom{r}{i}(-1)^i = \binom{r}{r}(-1)^r + \binom{r}{r-1}(-1)^{r-1} + \sum_{i=0}^{r-2} \binom{r}{i}(-1)^i$$

$$\Rightarrow \sum_{i=0}^{r-2} \binom{r}{i}(-1)^i = (-1)^r(r-1)$$

e

$$(q-1)^r = \sum_{i=0}^{r}(-1)^i \binom{r}{i} q^{r-i} = qr(-1)^{r-1} + (-1)^r + q\sum_{i=0}^{r-2}(-1)^i \binom{r}{i} q^{r-i-1}$$

$$\Rightarrow \sum_{i=0}^{r-2}(-1)^i \binom{r}{i} q^{r-i-1} = \frac{(q-1)^r + qr(-1)^r + (-1)^{r+1}}{q} = \frac{(q-1)^r}{q} + r(-1)^r + \frac{(-1)^{r+1}}{q}$$

Logo,

$$\begin{aligned} A &= \frac{1}{q-1}\left(\frac{(q-1)^r}{q} + r(-1)^r + \frac{(-1)^{r+1}}{q} - (-1)^r(r-1)\right) \\ &= \frac{1}{q(q-1)}((q-1)^r + (-1)^r(q-1)) \\ &= \frac{(q-1)^{r-1} - (-1)^{r-1}}{q}. \end{aligned}$$

Deste modo, segue da equação (2.4) que o número de pontos em H com r coordenadas não nulas é

$$\binom{n+1}{r} A = \binom{n+1}{r} \frac{(q-1)^{r-1} - (-1)^{r-1}}{q}.$$

Como cada ponto com r coordenadas não nulas em $\mathbb{P}^n(\mathbb{F}_q)$ corresponde a $(q+1)^{r-1}$ pontos em $\mathbb{P}^n(\mathbb{F}_{q^2})$ então o número de pontos em $\mathcal{X}$ é

$$\begin{aligned} |\mathcal{X}| &= \sum_{r=1}^{n+1} \binom{n+1}{r} \frac{((q-1)^{r-1} - (-1)^{r-1})(q+1)^{r-1}}{q} \\ &= \frac{1}{q}\left(\sum_{r=1}^{n+1} \binom{n+1}{r}(q^2-1)^{r-1} - \sum_{r=1}^{n+1} \binom{n+1}{r}(-q-1)^{r-1}\right). \end{aligned}$$

Novamente, pelo binômio de Newton para anéis temos

$$q^{2(n+1)} = (q^2-1+1)^{n+1} = \sum_{r=0}^{n+1} \binom{n+1}{r}(q^2-1)^r = 1 + (q^2-1)\sum_{r=1}^{n+1} \binom{n+1}{r}(q^2-1)^{r-1}$$

$$\Rightarrow \sum_{r=1}^{n+1} \binom{n+1}{r}(q^2-1)^{r-1} = \frac{q^{2(n+1)} - 1}{q^2-1}$$

e

$$(-q-1+1)^{n+1} = \sum_{r=0}^{n+1} \binom{n+1}{r}(-q-1)^r = 1 + (-q-1)\sum_{r=1}^{n+1} \binom{n+1}{r}(-q-1)^{r-1}$$

$$\Rightarrow \sum_{r=1}^{n+1} \binom{n+1}{r}(-q-1)^{r-1} = -\frac{(-1)^{n+1}q^{n+1}-1}{q+1}.$$

Portanto,

$$\begin{aligned}
|\mathcal{X}| &= \frac{1}{q}\left(\frac{q^{2(n+1)}-1}{q^2-1} + \frac{(-1)^{n+1}q^{n+1}-1}{q+1}\right) \\
&= \frac{1}{q(q^2-1)}(q^{2(n+1)} - 1 + (q-1)((-1)^{n+1}q^{n+1}-1) \\
&= \frac{1}{q(q^2-1)}(q^{2(n+1)} - 1 + (-1)^{n+1}q^{n+2} - q - (-1)^{n+1}q^{n+1} + 1) \\
&= \frac{1}{q^2-1}(q^{2n+1} - (-1)^n q^{n+1} - (-1)^{n+1}q^n - 1) \\
&= \frac{(q^{n+1}-(-1)^{n+1})(q^n-(-1)^n)}{q^2-1}.
\end{aligned}$$

■

O caso geral, número de pontos em uma variedade Hermitiana não degenerada, decorre do fato que toda variedade Hermitiana não degenerada em $\mathbb{P}^n(k)$ é *projetivamente equivalente* a $\mathbf{v}(X_0^{q+1} + \cdots + X_n^{q+1})$, assunto da próxima seção.

2.3 Hipersuperfícies projetivamente equivalentes

Nesta seção, vamos falar sobre o comportamento de uma hipersuperfície quando realizamos uma mudança linear no sistema de coordenadas projetivo.

Definição 2.8. Dizemos que duas hipersuperfícies $\mathcal{X}_0$ e $\mathcal{X}_1$ em $\mathbb{P}^n(k)$ são **projetivamente equivalentes** se existir uma projetividade $T : \mathbb{P}^n(k) \to \mathbb{P}^n(k)$ tal que $T(\mathcal{X}_0) = \mathcal{X}_1$.

Sejam $\mathcal{X}_0 = \mathbf{v}(F), \mathcal{X}_1 = \mathbf{v}(G) \subset \mathbb{P}^n(k)$, com $F, G \in k[X_0, ..., X_n]$ homogêneos. Se existir $A = (a_{ij})_{0\leq i,j\leq n} \in GL_{n+1}(k)$ tal que

$$F(X_0, ..., X_n) = G\left(\sum_{j=0}^{n} a_{0j}X_j, ..., \sum_{j=0}^{n} a_{nj}X_j\right) \tag{2.5}$$

então a projetividade $T : \mathbb{P}^n(k) \to \mathbb{P}^n(k)$ definida por A satisfaz $T(\mathcal{X}_0) = \mathcal{X}_1$. Com efeito, dado $[x_0 : \cdots : x_n] \in \mathcal{X}_0$ temos

$$G(A(x_0, ..., x_n)) = G\left(\sum_{j=0}^{n} a_{0j}x_j, ..., \sum_{j=0}^{n} a_{nj}x_j\right) = F(x_0, ..., x_n) = 0,$$

ou seja, $T([x_0 : \cdots : x_n]) \in \mathcal{X}_1$, consequentemente, $T(\mathcal{X}_0) \subseteq \mathcal{X}_1$. Reciprocamente, dado $[x_0' : \cdots : x_n'] \in \mathcal{X}_1$ existe, pelo fato de T ser bijetora, $[x_0 : \cdots : x_n] \in \mathbb{P}^n(k)$ tal que

$$T([x_0 : \cdots : x_n]) = [x_0' : \cdots : x_n'].$$

Segue daí que

$$F(x_0, ..., x_n) = G\left(\sum_{j=0}^{n} a_{0j}x_j, ..., \sum_{j=0}^{n} a_{nj}x_j\right) = G(A(x_0, ..., x_n)) = G(\lambda x_0', ..., \lambda x_n') = 0,$$

ou seja, $[x_0 : \cdots : x_n] \in \mathcal{X}_0$, consequentemente, $\mathcal{X}_1 \subseteq T(\mathcal{X}_0)$.

Lema 2.5. *A relação $\sim$ em $\mathbb{P}^n(k)$ que identifica duas hipersuperfícies projetivamente equivalentes é uma relação de equivalência.*

Demonstração. Sejam $\mathcal{X}_0, \mathcal{X}_1, \mathcal{X}_2 \in \mathbb{P}^n(k)$ hipersuperfícies.

- *Reflexiva*: Se $T : \mathbb{P}^n(k) \to \mathbb{P}^n(k)$ é a projetividade definida pela matriz identidade de $GL_{n+1}(k)$ então $T(\mathcal{X}_0) = \mathcal{X}_0$, consequentemente, $\mathcal{X}_0 \sim \mathcal{X}_0$.
- *Simétrica*: Suponha que $\mathcal{X}_0 \sim \mathcal{X}_1$. Assim existe uma projetividade $T : \mathbb{P}^n(k) \to \mathbb{P}^n(k)$ tal que $T(\mathcal{X}_0) = \mathcal{X}_1$, consequentemente, a projetividade inversa satisfaz $T^{-1}(\mathcal{X}_1) = \mathcal{X}_0$, assim $\mathcal{X}_1 \sim \mathcal{X}_0$.
- *Transitividade*: Suponha que $\mathcal{X}_0 \sim \mathcal{X}_1$ e $\mathcal{X}_1 \sim \mathcal{X}_2$. Deste modo, existem projetividades $T_0, T_1 : \mathbb{P}^n(k) \to \mathbb{P}^n(k)$ tais que $T_0(\mathcal{X}_0) = \mathcal{X}_1$ e $T_1(\mathcal{X}_1) = \mathcal{X}_2$. Segue daí que a projetividade dada pela composição $(T_1 \circ T_0) : \mathbb{P}^n(k) \to \mathbb{P}^n(k)$ satisfaz $(T_1 \circ T_0)(\mathcal{X}_0) = T_1(T_0(\mathcal{X}_0)) = T_1(\mathcal{X}_1) = \mathcal{X}_2$, assim $\mathcal{X}_0 \sim \mathcal{X}_2$.

■

Exemplo 2.7. Qualquer variedade Hermitiana não degenerada em $\mathbb{P}^n(\mathbb{F}_{q^2})$ é projetivamente equivalente a $\mathbf{v}(X_0^{q+1} + \cdots + X_n^{q+1})$ (veja, por exemplo, [13, teorema 5.1.5]).

Exemplo 2.8. Qualquer quádrica não singular em $\mathbb{P}^4(\mathbb{F}_q)$ é projetivamente equivalente a $\mathbf{v}(X_0^2 + X_1X_2 + X_3X_4)$ (veja, por exemplo, [13, teorema 5.2.4]).

Para finalizar está seção, vamos fazer uma mudança no sistema de coordenadas que vai simplificar a demonstração de um teorema no último capítulo. Antes disso, precisamos de um resultado.

Proposição 2.11. *Se $F_1, ..., F_r \in k[X_0, ..., X_n]$ são $r \leq n$ polinômios homogêneos, então*

$$\mathbf{v}(F_1) \cap \cdots \cap \mathbf{v}(F_r) \neq \emptyset.$$

Demonstração. Veja [14, seção 6.2] ■

Exemplo 2.9. Seja $P = [p_0 : p_1 : p_2 : p_3] \in \mathbb{P}^3(k)$ e $\Pi = \mathbf{v}(a_0X_0 + a_1X_1 + a_2X_2 + a_3X_3)$ um hiperplano em $\mathbb{P}^3(k)$ tal que $P \notin \Pi$. Vamos construir uma matriz invertível $B = (b_{ij})$ tal que a projetividade dada por ela leva P em $[1 : 0 : 0 : 0]$ e Π em $\mathbf{v}(X_0)$. Para isso, vamos determinar a matriz $A = (a_{ij})$ inversa de B: queremos

$$\lambda \begin{bmatrix} p_0 \\ p_1 \\ p_2 \\ p_3 \end{bmatrix} = \begin{bmatrix} a_{11} & a_{12} & a_{13} & a_{14} \\ a_{21} & a_{22} & a_{23} & a_{24} \\ a_{31} & a_{32} & a_{33} & a_{34} \\ a_{41} & a_{42} & a_{43} & a_{44} \end{bmatrix} \begin{bmatrix} 1 \\ 0 \\ 0 \\ 0 \end{bmatrix} = \begin{bmatrix} a_{11} \\ a_{21} \\ a_{31} \\ a_{41} \end{bmatrix}.$$

Assim, devemos ter $a_{11} = \lambda p_0, a_{21} = \lambda p_1, a_{31} = \lambda p_2$ e $a_{41} = \lambda p_3$. Considere

$$f = a_0X_0 + a_1X_1 + a_2X_2 + a_3X_3.$$

Queremos

$$\begin{aligned} X_0' = B^*(f) &= \sum_{j=0}^{3} a_0a_{1(j+1)}X_j' + \sum_{j=0}^{3} a_1a_{2(j+1)}X_j' + \sum_{j=0}^{3} a_2a_{3(j+1)}X_j' + \sum_{j=0}^{3} a_3a_{4(j+1)}X_j' \\ &= \lambda(a_0p_0 + a_1p_1 + a_2p_2 + a_3p_3)X_0' + (a_0a_{12} + a_1a_{22} + a_2a_{32} + a_3a_{42})X_1' + \\ &\quad + (a_0a_{13} + a_1a_{23} + a_2a_{33} + a_3a_{43})X_2' + (a_0a_{14} + a_1a_{24} + a_2a_{34} + a_3a_{44})X_3'. \end{aligned}$$

Como $P \notin \Pi$ tem-se $a_0p_0 + a_1p_1 + a_2p_2 + a_3p_3 \neq 0$. Assim, considere

$$\lambda = (a_0p_0 + a_1p_1 + a_2p_2 + a_3p_3)^{-1}.$$

Resta satisfazer a seguinte condição dada abaixo de modo que a matriz B seja invertível:

$$\begin{aligned} a_0a_{12} + a_1a_{22} + a_2a_{32} + a_3a_{42} &= 0 \\ a_0a_{13} + a_1a_{23} + a_2a_{33} + a_3a_{43} &= 0 \\ a_0a_{14} + a_1a_{24} + a_2a_{34} + a_3a_{44} &= 0. \end{aligned}$$

Em um caso particular, isso é facilmente obtido. Desse modo, apenas vamos garantir que exista uma solução de modo que a matriz B seja invertível. Para isso, basta observar que as três equações acimas, juntamente com $det(A) = 1$, considerando $det(A)$ como um polinômio com 12 variáveis, é um sistema com mais variáveis que equações.

Por exemplo, seja $P = [0 : 13 : 2 : 4]$ e $\Pi = \mathbf{v}(5X_0 + X_1 - 3X_3)$ em $\mathbb{P}^3(k)$. Primeiramente, observe que $P \notin \Pi$. Usando a estratégia acima, considere

$$\lambda = (13 - 12)^{-1} = (1)^{-1} = 1$$

e

$$\begin{aligned} 5a_{12} + a_{22} - 3a_{42} &= 0 \\ 5a_{13} + a_{23} - 3a_{43} &= 0 \\ 5a_{14} + a_{24} - 3a_{44} &= 0. \end{aligned}$$

Tome $a_{12} = a_{13} = -a_{14} = 1$ e $a_{42} = a_{43} = -2a_{44} = 2$, assim $a_{23} = a_{22} = 1$ e $a_{24} = 2$. Temos

$$1 = det \begin{bmatrix} 0 & 1 & 1 & -1 \\ 13 & 1 & 1 & 2 \\ 2 & a_{32} & a_{33} & a_{34} \\ 4 & 2 & 2 & -1 \end{bmatrix} = a_{32} - a_{33}.$$

Assim podemos considerar $a_{33} = a_{34} = 0$ e $a_{32} = 1$. Logo,

$$A = \begin{bmatrix} 0 & 1 & 1 & -1 \\ 13 & 1 & 1 & 2 \\ 2 & 1 & 0 & 0 \\ 4 & 2 & 2 & -1 \end{bmatrix} \Rightarrow B = \begin{bmatrix} 5 & 1 & 0 & -3 \\ -10 & -2 & 1 & 6 \\ -11 & -2 & -1 & 7 \\ -22 & -4 & 0 & 13 \end{bmatrix}.$$

Se $T : \mathbb{P}^3(k) \to \mathbb{P}^3(k)$ é a projetividade definida por B, então, pelo exposto acima, tem-se $T(P) = [1 : 0 : 0 : 0]$ e $B^*(5X_0 + X_1 - 3X_3) = X_0$.

2.4 Espaço tangente e hipersuperfícies suaves

O conceito de reta e plano tangente no cálculo diferencial desempenha um papel fundamental para estudar o comportamento de algumas funções em um ponto. Desse modo, o principal objetivo desta seção é definir o conceito de espaço tangente associado a um ponto de uma variedade afim e projetiva. Para isso, considere a derivada parcial formal de um polinômio em relação à variável X_j definida por

$$\frac{\partial}{\partial X_j}\left(\sum_{\alpha_1,\ldots,\alpha_n} C_{\alpha_1,\ldots,\alpha_n}\, X_1^{\alpha_1}\cdots X_n^{\alpha_n}\right) = \sum_{\alpha_1,\ldots,\alpha_n} C_{\alpha_1,\ldots,\alpha_n}\, \alpha_j\, X_1^{\alpha_1}\cdots X_j^{\alpha_j-1}\cdots X_n^{\alpha_n}.$$

Definição 2.9. Sejam V uma variedade afim e $p = (a_1, ..., a_n) \in \mathbb{A}^n(k)$:

(i) Seja $f \in k[X_1, ..., X_n]$. A ***parte linear*** de f em p, denotada por $d_p(f)$, é definida pelo seguinte polinômio de grau 1

$$d_p(f)(X_1, ..., X_n) := \frac{\partial f}{\partial X_1}(p)(X_1 - a_1) + \cdots + \frac{\partial f}{\partial X_n}(p)(X_n - a_n).$$

(ii) Se $p \in V$ definimos o **espaço tangente** de V em p, denotado por $T_p(V)$, como sendo a seguinte variedade afim

$$T_p(V) := \mathbb{V}(d_p(f);\ f \in \mathbb{I}(V)).$$

Lema 2.6. *Sejam $f, g \in k[X_1, ..., X_n]$ e $p \in \mathbb{A}^n(k)$. Então $d_p(fg) = d_p(f) \cdot g(p) + f(p) \cdot d_p(g)$.*

Demonstração. Suponha que

$$f = \sum_{i=1}^{m} a_i X_1^{\alpha_1^i} \cdots X_n^{\alpha_n^i} \quad e \quad g = \sum_{s=1}^{r} b_s X_1^{\beta_1^s} \cdots X_n^{\beta_n^s}.$$

Temos

$$fg = \sum_{s=1}^{r} \sum_{i=1}^{m} a_i b_s X_1^{\beta_1^s + \alpha_1^i} \cdots X_n^{\beta_n^s + \alpha_n^i}.$$

Logo,

$$\begin{aligned}
\frac{\partial(fg)}{\partial X_j}(p) &= \sum_{s=1}^{r} \sum_{i=1}^{m} a_i b_s (\beta_j^s + \alpha_j^i)\ p_1^{\beta_1^s + \alpha_1^i} \cdots p_j^{\beta_j^s + \alpha_j^i - 1} \cdots p_n^{\beta_n^s + \alpha_n^i} \\
&= \sum_{s=1}^{r} \sum_{i=1}^{m} a_i b_s \beta_j^s\ p_1^{\beta_1^s + \alpha_1^i} \cdots p_j^{\beta_j^s + \alpha_j^i - 1} \cdots p_n^{\beta_n^s + \alpha_n^i} \\
&\quad + \sum_{s=1}^{r} \sum_{i=1}^{m} a_i b_s \alpha_j^i\ p_1^{\beta_1^s + \alpha_1^i} \cdots p_j^{\beta_j^s + \alpha_j^i - 1} \cdots p_n^{\beta_n^s + \alpha_n^i} \\
&= \frac{\partial(f)}{\partial X_j}(p) \cdot g(p) + f(p) \cdot \frac{\partial(g)}{\partial X_j}(p).
\end{aligned}$$

O resultado segue. ■

Proposição 2.12. *Sejam $V \subseteq \mathbb{A}^n(k)$ uma variedade afim e $p = (a_1, ..., a_n) \in V$. Se $\mathbb{I}(V) = \langle f_1, ..., f_m \rangle$, então $T_p(V) = \mathbb{V}(d_p(f_1), ..., d_p(f_m))$.*

Demonstração. Dado $g \in \mathbb{I}(V) = \langle f_1, ..., f_m \rangle$ existem $h_1, ..., h_m \in k[X_1, ..., X_n]$ tais que

$$g = \sum_{j=1}^{m} h_j f_j$$

Segue do lema 2.6 que

$$d_p(g) = \sum_{j=1}^{m} d_p(h_j f_j) = \sum_{j=1}^{m} h_j(p) d_p(f_j).$$

Portanto, $T_p(V) = \mathbb{V}(d_p(f_1), ..., d_p(f_m))$. ■

Exemplo 2.10. Seja $V = \mathbb{V}(f)$ com $f = Y - X^2 \in k[X,Y]$. Observe que $k[X,Y]/\langle f\rangle$ é isomorfo à $k[Z]$ dado por $g(X,Y) \longmapsto g(Z,Z^2)$. Assim, $\langle f\rangle$ é um ideal primo, implicando que f é irredutível. Segue do corolário 1.1 que $\mathbb{I}(V) = \langle f\rangle$. Dado $p = (a,a^2) \in V$ com $a \in k$, pela proposição 2.12, o espaço tangente de V em p é

$$T_p(V) = \mathbb{V}(-2a(X-a) + (Y-a^2)) = \mathbb{V}(Y - 2aX + 2a^2 - a^2).$$

Por exemplo, se $k = \mathbb{C}$, os pontos reais de $\mathbb{V}(f)$ e $T_P(V)$ no ponto $p = (1,1)$ no plano $\mathbb{R}^2$ são

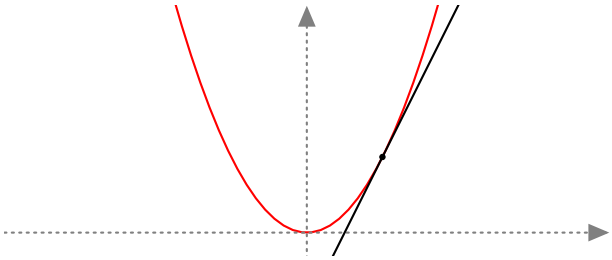

Figura 2.1: Pontos reais da variedade $\mathbb{V}(Y - X^2)$ e do espaço tangente em $(1,1)$.

Para o caso projetivo precisamos da fórmula de Euler.

Lema 2.7 (Fórmula de Euler)**.** *Seja $F \in k[X_0,...,X_n]$ homogêneo de grau d, então*

$$d \cdot F = \sum_{i=1}^{n} X_i \cdot \frac{\partial F}{\partial X_i}.$$

Demonstração. Seja $X^\alpha = a \cdot X_1^{\alpha_1} \cdots X_n^{\alpha_n}$ um termo monomial de F. Como F é homogêneo de grau d, então $\alpha_1 + \cdots + \alpha_n = d$. Temos

$$\sum_{i=1}^{n} X_i \frac{\partial}{\partial X_i}(X^\alpha) = \sum_{i=1}^{n} \alpha_i \; X^\alpha = X^\alpha \sum_{i=1}^{n} \alpha_i = d \cdot X^\alpha.$$

O resultado segue daí. ■

Dada uma hipersuperfície $\mathcal{X} \subsetneq \mathbb{P}^n(k)$, existe, pelo corolário 2.8, $F \in k[X_0,...,X_n]$ homogêneo tal que $\mathbb{J}(\mathcal{X}) = \langle F\rangle$. Por simplicidade, considere a carta afim U_0, assim a hipersuperfície afim $\mathcal{X} \cap U_0 \subsetneq U_0 \simeq \mathbb{A}^n(k)$ é tal que $\mathbb{I}(\mathcal{X} \cap U_0) = \langle f\rangle$, onde $f = F(1,X_1,...,X_n)$ é a desomogenização de F em relação à variável X_0. Como efeito, pela lema 2.4, temos

$$\mathcal{X} = \mathbf{v}(\mathbb{J}(\mathcal{X})) = \mathbf{v}(F).$$

Assim, segue do exemplo 2.4, que $\mathcal{X} \cap U_0 = \mathbb{V}(f)$ com $f = F(1,X_1,...,X_n)$. Como $\mathbb{J}(\mathcal{X}) = \langle F\rangle$ então $F = G_1 \cdots G_s$ onde $G_1,...,G_s \in k[X_0,...,X_n]$ são irredutíveis não associados (veja, demonstração da proposição 2.8). Como o processo de desomogenização é um homomorfismo de anéis, temos

$$f = F(1,X_1,...,X_n) = G_1(1,X_1,...,X_n) \cdots G_s(1,X_1,...,X_n).$$

Como G_i é irredutível,s então $G_i(1,X_1,...,X_n)$ é constante ou irredutível. Assim, $\mathbb{I}(\mathcal{X} \cap U_0) = \langle f\rangle$ (veja, demonstração da proposição 1.3). Dado $P = [1 : a_1 : \cdots : a_n] \in \mathcal{X}$, o espaço tangente afim de $\mathcal{X} \cap U_0$ em $p = \varphi_0(P)$ é a variedade afim definida pelo polinômio

$$\frac{\partial f}{\partial X_1}(p)(X_1 - a_1) + \cdots + \frac{\partial f}{\partial X_n}(p)(X_n - a_n). \tag{2.6}$$

Como $f = F(1, X_1, ..., X_n)$ então

$$\frac{\partial f}{\partial X_j} = \frac{\partial F}{\partial X_j}(1, X_1, ..., X_n)$$

para todo $j = 1, ..., n$. Deste modo, homogenizando o polinômio (2.6), definimos o espaço tangente projetivo de $\mathcal{X}$ em P como sendo a variedade projetiva definida pelo polinômio

$$\frac{\partial F}{\partial X_1}(1, a_1, ..., a_n)(X_1 - a_1X_0) + \cdots + \frac{\partial F}{\partial X_n}(1, a_1, ..., a_n)(X_n - a_nX_0). \tag{2.7}$$

Como $F(1, a_1, ..., a_n) = 0$, segue do lema 2.7 que

$$\frac{\partial F}{\partial X_0}(1, a_1, ..., a_n)X_0 = \sum_{j=1}^{n} \frac{\partial F}{\partial X_i}(1, a_1, ..., a_n)(-a_iX_0).$$

Portanto, substituindo na equação (2.7), obtemos o polinômio

$$\sum_{i=0}^{n} X_i \cdot \frac{\partial F}{\partial X_i}(1, a_1, ..., a_n). \tag{2.8}$$

A equação (2.8) nos leva à seguinte definição.

Definição 2.10. Seja $\mathcal{X}$ uma hipersuperfície em $\mathbb{P}^n(k)$ com $\mathbb{J}(\mathcal{X}) = \langle F \rangle$, onde $F \in k[X_0, ..., X_n]$ é um polinômio homogêneo. Dado $P = [a_0 : \cdots : a_n] \in \mathcal{X}$, defina-se o ***espaço tangente projetivo*** de $\mathcal{X}$ em P, denotado por $\mathbb{T}_P(\mathcal{X})$, como sendo

$$\mathbb{T}_P(\mathcal{X}) := \left\{ [x_0 : \cdots : x_n] \in \mathbb{P}^n(k);\ \sum_{i=0}^{n} x_i \cdot \frac{\partial F}{\partial X_i}(a_0, ..., a_n) = 0 \right\},$$

Quando $\mathbb{T}_P(\mathcal{X}) = \mathbb{P}^n(k)$, dizemos que P é um ponto **singular** de $\mathcal{X}$. Caso contrário, dizemos que P é **não singular** (ou **suave**) de $\mathcal{X}$. Se todos os pontos de $\mathcal{X}$ são não singulares, dizemos que $\mathcal{X}$ é uma hipersuperfície não singular (ou suave).

Exemplo 2.11. Considere a parábola projetiva $\mathcal{X} = \mathbf{v}(X_0^2 - X_1X_2) \subseteq \mathbb{P}^2(k)$. Segue da irredutibilidade de $X_0^2 - X_1X_2$ que $\mathbb{J}(\mathcal{X}) = \langle F \rangle$, onde $F = X_0^2 - X_1X_2$. Temos

$$\frac{\partial F}{\partial X_0} = 2X_0, \quad \frac{\partial F}{\partial X_1} = -X_2 \quad \text{e} \quad \frac{\partial F}{\partial X_2} = -X_1.$$

Considerando $P = [1 : 1 : 1] \in \mathcal{X}$ então

$$\mathbb{T}_P(\mathcal{X}) = \left\{ [x_0 : x_1 : x_2] \in \mathbb{P}^2(k);\ 2x_0 - x_1 - x_2 = 0 \right\}.$$

2.5 Teorema de Bezout: sobre o número de interseções

Se consideramos como curva afim apenas o conjunto de pontos, então $\mathbb{V}(f) = \mathbb{V}(f^n)$ para todo $n \in \mathbb{N}$, onde $f \in k[X, Y]$. Entretanto, ao analisarmos um zero de um polinômio f é interessante levar em consideração a *multiplicidade*. Isso nos leva a redefinir o que entendemos como curva afim.

Definição 2.11. Considere a relação de equivalência $f \cong g \Leftrightarrow f = \lambda g$ para algum $\lambda \in k^*$, onde $f, g \in K[X, Y]$. Uma **curva algébrica plana afim** (ou **curva afim**) é uma classe de equivalência no conjunto dos polinômios em $k[X, Y]$ não constantes. Denotaremos por f ou $f = 0$ a curva algébrica plana afim associada ao polinômio não constante f, isto é, a classe de f. O **traço** da curva algébrica afim plana f é a variedade afim $\mathbb{V}(f)$.

Observação 2.2. Dados $f, g \in k[X, Y]$ a notação $(a, b) \in f$ significa $(a, b) \in \mathbb{V}(f)$ e $f \cap g$ representará a interseção dos traços, isto é, $\mathbb{V}(f) \cap \mathbb{V}(g)$.

Seja $f \in k[X, Y]$ de grau $d \geq 1$. Se $f = cf_1^{s_1} \cdots f_m^{s_m}$ é a decomposição de f em fatores irredutíveis não associados em $k[X, Y]$, então as curvas afins $f_1, ..., f_m$ são ditas **componentes irredutíveis** de f com multiplicidades $s_1, ..., s_m$, respectivamente.

Para ficar claro o que estamos interessados em apresentar nesta seção e um dos motivos de considerarmos k um corpo algebricamente fechado, vejamos alguns exemplos no plano $\mathbb{R}^2$:

Exemplo 2.12. Considere as curvas afins $f = Y - X^2$ e $g_\lambda = X^2 + 4(Y - \lambda)^2 - 4$. Vamos analisar $f \cap g$ para certos valores de λ. No caso $\lambda = 2$, temos 4 pontos reais na interseção; basta calcular as raízes da equação $Y + 4(Y - 2)^2 = 4$ com $Y = X^2$:

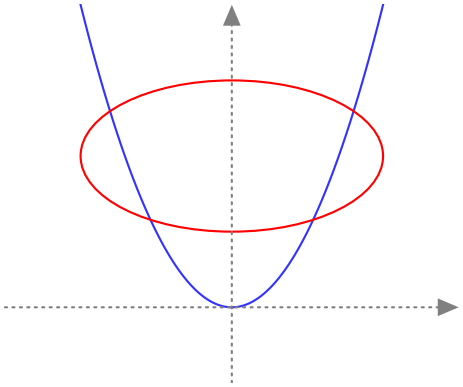

Figura 2.2: Representação gráfica de $y = x^2$ e $x^2 + 4(y - 2)^2 = 4$.

Neste caso, o número de pontos na interseção das curvas é exatamente $deg(f) \cdot deg(g_2)$. No caso $\lambda = 1$, encontramos apenas três pontos reais na interseção:

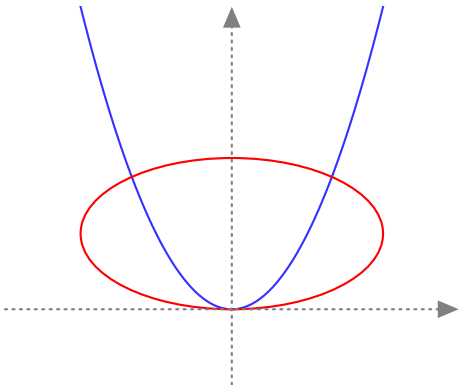

Figura 2.3: Representação gráfica de $y = x^2$ e $x^2 + 4(y - 1)^2 = 4$.

Entretanto, observe que o ponto $(0, 0)$ é "especial", pois o espaço tangente das curvas neste ponto coincide. Assim, existe uma "multiplicidade" a ser considerada. No caso $\lambda = 0$, encontramos apenas dois pontos reais na interseção:

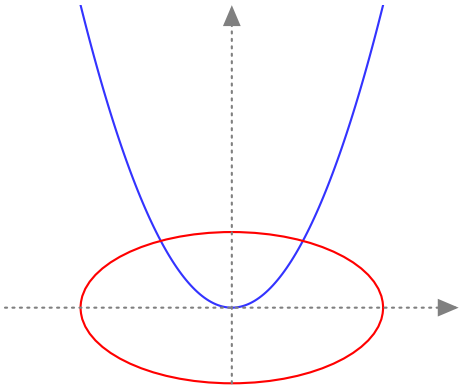

Figura 2.4: Representação gráfica de $y = x^2$ e $x^2 + 4y^2 = 4$.

Entretanto, as equações $Y = X^2$ e $X^2 - 4Y^2 = 4$ nos fornecem quatro soluções, duas delas estão em $\mathbb{C}$ (fecho algébrico de $\mathbb{R}$).

Além dos pontos na interseção no plano, existem outras interseções a serem consideradas, aquelas no infinito discutidas no início da seção 3 do capítulo 1.

Exemplo 2.13. Homogenizando o polinômio $f = X^2 - Y^2 - 1$ em relação à variável Z obtemos $F = X^2 - Y^2 - Z^2$. Seja $\mathcal{X} = \mathbf{v}(F) \subseteq \mathbb{P}^2(k)$ a hipersuperfície gerada por F (hipérbole projetiva). Cada hiperplano (neste caso são retas) $H_0 = \mathbf{v}(Y + X)$ e $H_1 = \mathbf{v}(Y - X)$ de $\mathbb{P}^2(k)$ intercepta $\mathcal{X}$ em um ponto com multiplicidade, de fato: Considerando $Y = X$, obtemos de $X^2 - Y^2 - Z^2$ à solução $P_1 = [1 : 1 : 0]$ e, no caso $Y = -X$, obtemos à solução $P_0 = [1 : -1 : 0]$. Além disso, o espaço tangente de $\mathcal{X}$ nos pontos P_0 e P_1 são, respectivamente, H_0 e H_1.

Observe, nos exemplos anteriores, a sútil relação entre o produto dos graus das curvas e número de pontos na interseções (contando as no infinito). Isso não é um mera coincidência, pois, se contarmos o número de pontos na interseção, considerando as *multiplicidades* e as no infinito, o resultado é sempre o produto dos graus, desde que nós garantamos que o número na interseção é finito. Esse resultado é conhecido como teorema de Bezout é será enunciado no final desta seção. Antes disso, formalizemos alguns conceitos:

Definição 2.12. Dadas duas curvas afins f e g, o **número de interseção** de f e g no ponto $p = (a, b)$, denotado por $I(p, f \cap g)$, é definido pelos seguintes axiomas:

$I_1)$ $0 \leq I(p, f \cap g) \in \mathbb{Z}$ se f e g não possuem componente comum contendo o ponto p;

$I_2)$ $I(p, f \cap g) = \infty$ se f e g possuem componente comum contendo o ponto p;

$I_3)$ $I(p, f \cap g) = 0$ se, e somente se, $p \notin f \cap g$.

$I_4)$ $I(p, F \cap G) = 1$ se f e g são duas retas distintas passando em p;

$I_5)$ $I(p, f \cap g) = I(p, g \cap f)$;

$I_6)$ $I(p, f \cap (g + hf)) = I(p, f \cap g)$ para qualquer $h \in k[X, Y]$.

$I_7)$ $I(p, f \cap gh) = I(p, f \cap g) + I(p, f \cap h)$ para qualquer curva afim h.

Teorema 2.4. *Para duas curvas afins f e g existe no máximo uma função $I(p, f \cap g)$ satisfazendo os axiomas $I_1 - I_7$.*

Demonstração. Veja [15, teorema 3.8]. ■

Teorema 2.5. *Existe uma função $I(p, f \cap g)$ satisfazendo os axiomas $I_1 - I_7$.*

Demonstração. Veja [15, teorema 3.9]. ■

Com isso,s podemos definida multiplicidade de um ponto em uma curva.

Definição 2.13. Sejam f uma curva afim e $p_0 \in f$. A **multiplicidade** de p_0 em f, denotada por $m_{p_0}(f)$, é definida por

$$m_{p_0}(f) := min\{I(p_0, f \cap l);\ l \text{ é uma reta tal que } p_0 \in l\}.$$

Pelo mesmo motivo discutido no início da seção, vamos redefinir o que entendemos como curva projetiva.

Definição 2.14. Considere a relação de equivalência $F \simeq G \Leftrightarrow F = \lambda G$ para algum $\lambda \in k^*$, onde $F, G \in k[X, Y, Z]$. Uma **curva algébrica projetiva plana** (ou **curva projetiva**) é uma classe de equivalência de polinômios homogêneos não constantes de $k[X, Y, Z]$. Denotaremos por F ou $F = 0$ a curva projetiva associada ao polinômio homogêneo não constante F e definimos o seu traço como sendo $\mathbf{v}(F)$.

Definição 2.15. Para duas curva planas projetivas $F, G \in k[X, Y, Z]$ e o ponto $O = [1 : 0 : 0]$ definimos o número de interseção de F e G em O, denotado por $I(O, F \cap G)$, como sendo

$$I(O, F \cap G) := I((0, 0), f \cap g),$$

onde f e g são as desomogenização de F e G em relação à variável X.

O número de interseção das curvas projetivas F e G em um ponto P é calculado por meio de uma transformação projetiva que leva P em $[1 : 0 : 0]$. A multiplicidade de um ponto em uma curva projetiva também é definida desta maneira.

Teorema 2.6 (Bezout)**.** *Se as curvas projetivas F e G são de graus m e n, respectivamente, e não possuem componentes em comum, então*

$$\sum I(P, F \cap G) = mn.$$

Demonstração. Veja [15, teorema 3.14]. ■

Observação 2.3. O teorema de Bezout 2.6 conta as multiplicidades, assim o número de pontos na interseção de duas curvas planas projetivas que não possuem componentes em comum é sempre menor ou igual ao produto dos graus.

Capítulo 3

Hipersuperfícies no espaço projetivo

Várias indagações surgem, naturalmente, quando consideramos o espaço projetivo sobre um corpo finito. Entre as diversas indagações existentes, estamos particularmente interessados no problema de determinar o número máximo de pontos em uma hipersuperfície arbitrária de grau d de $\mathbb{P}^n(\mathbb{F}_q)$. Buscando analisar essa indagação, na primeira seção deste capítulo fazemos algumas considerações para que o problema esteja definido no espaço projetivo sobre o fecho algébrico de $\mathbb{F}_q$, o qual sabemos ser algebricamente fechado. Essa abordagem nos abre um leque de possibilidades para analisar o problema. Posteriormente, apresentamos a resposta dada por Serre para essa indagação. Além disso, devido ao fato de que alguns exemplos peculiares acontecem no contexto geral, nos parece razoável analisar separadamente o caso de hipersuperfícies não singulares de grau d, entretanto, isso torna o problema bem mais complicado. Para o caso $n = 2$, existe o teorema de Hasse-Weil. Recentemente, Mrinmoy Datta em [9] apresenta uma resposta para o caso $n = 4$ com algumas condições para d, isso será apresentado com detalhes na última seção do capítulo.

3.1 Algumas considerações iniciais

Doravante, denotaremos por $K = \overline{\mathbb{F}_q}$ o fecho algébrico de $\mathbb{F}_q$, ou seja, K denotará o menor corpo algebricamente fechado, a menos de isomorfismo, que contém $\mathbb{F}_q$. Um resultado interessante sobre o fecho algébrico do corpo finito $\mathbb{F}_q$ é que $K = \bigcup_{i\in\mathbb{N}} \mathbb{F}_{q^i}$. Assim, de forma natural, podemos considerar que o espaço projetivo $\mathbb{P}^n(K)$ contém o espaço projetivo finito $\mathbb{P}^n(\mathbb{F}_{q^i})$ para todo $i \geq 1$. Isso nos possibilita realizar um estudo sobre o número máximo de pontos de uma hipersuperfície em $\mathbb{P}^n(\mathbb{F}_q)$ com um olhar em $\mathbb{P}^n(K)$. Para isso, precisamos de algumas definições:

Definição 3.1.

i) Dizemos que uma hipersuperfície $\mathbf{v}(F) \subseteq \mathbb{P}^n(K)$ é definida sobre $\mathbb{F}_q$ se existir $c \in \mathbb{F}_q$ tal que $cF \in \mathbb{F}_q[X_0, ..., X_n]$.

ii) Dizemos que $P \in \mathbb{P}^n(K)$ é um ponto $\mathbb{F}_q$ - racional se existirem $x_0, ..., x_n \in \mathbb{F}_q$ tais que $P = [x_0 : \cdots : x_n]$.

iii) Dado $S \subseteq \mathbb{P}^n(K)$ denotaremos por $S(\mathbb{F}_q)$ o conjunto dos pontos $\mathbb{F}_q$-racionais em S.

Exemplo 3.1. Seja $F \in \mathbb{F}_q[X_0, ..., X_n]$ homogêneo. Claramente, $\mathcal{X} = \mathbf{v}(F) \subseteq \mathbb{P}^n(K)$ é uma hipersuperfície definida sobre $\mathbb{F}_q$. Além disso, se $x_0, ..., x_n \in \mathbb{F}_q$ não são todos nulos e $F(x_0, ..., x_n) = 0$, então $[x_0 : \cdots : x_n] \in \mathcal{X}(\mathbb{F}_q)$.

Como todo corpo é um domínio de integridade, tem-se para todo polinômio homogêneo $F \in k[X_0, ..., X_n]$ e $m \in \mathbb{N}$ que $\mathbf{v}(F) = \mathbf{v}(F^m)$. Sendo assim, podemos considerar o polinômio de menor grau que gera o conjunto $\mathbf{v}(F)$. Isso é feito da seguinte maneira: doravante, quando considerarmos uma hipersuperfície $\mathcal{X} = \mathbf{v}(F)$ de grau d ficará subentendido que $\mathbb{J}(\mathcal{X}) = \langle F \rangle$.

Proposição 3.1. *Sejam $\mathbf{v}(G)$ e $\mathbf{v}(F)$ hipersuperfícies de grau $d' \geq 1$ e $d \geq 1$, respectivamente, tais que $\mathbf{v}(G) \subseteq \mathbf{v}(F)$:*

i) Se $d' = d$ então $\mathbf{v}(G) = \mathbf{v}(F)$.

ii) Se $d' < d$ existe uma hipersuperfície $\mathcal{X}$ de grau no máximo $d - d'$ tal que $\mathbf{v}(F) = \mathbf{v}(G) \cup \mathcal{X}$.

Demonstração. Temos $\langle F \rangle = \mathbb{J}(\mathbf{v}(F)) \subseteq \mathbb{J}(\mathbf{v}(G)) = \langle G \rangle$. Assim, existe $H \in k[X_0, ..., X_n]$ não nulo e homogêneo tal que $F = GH$. Segue daí que $\mathbf{v}(F) = \mathbf{v}(G) \cup \mathbf{v}(H)$.

i) Se $d' = d$ então $deg(H) = 0$ e assim $\mathbf{v}(H) = \emptyset$.

ii) Se $d' < d$ então $deg(H) = d - d' > 0$. Se $H = H_1^{s_1} \cup \cdots \cup H_m^{s_m}$ é a decomposição de H em fatores irredutíveis não associado considere $\mathcal{X} = \mathbf{v}(H_1 \cdots H_m)$. Assim, $deg(\mathcal{X})$ é no máximo $d - d'$, $\mathbf{v}(F) = \mathbf{v}(G) \cup \mathcal{X}$ e $\mathbb{J}(\mathcal{X}) = \langle H_1 \cdots H_m \rangle$.

■

Com isso, enunciamos o problema principal que este trabalho está interessado em analisar é o seguinte:
Problema 1: Seja $\mathcal{X}$ uma hipersuperfície (não singular) de grau $d \geq 1$ em $\mathbb{P}^n(K)$ definida sobre $\mathbb{F}_q$. Qual é o número máximo de pontos $\mathbb{F}_q$ - racionais em $\mathcal{X}$?

A quantidade de pontos $\mathbb{F}_q$ - racionais em $\mathbb{P}^n(K)$ é uma cota superior para o problema 1 e, obviamente, é igual a $\theta_q(n)$. Além disso, se $d \geq q + 1$, essa cota é atingida por algumas hipersuperfícies de grau d:

Exemplo 3.2. Considere $d \geq q + 1$ e seja

$$F = G(X_0, X_1)[X_0^q X_1 - X_0 X_1^q] = X_0^{d-1} X_1 - X_0^{d-q} X_1^q \in \mathbb{F}_q[X_0, X_1, ..., X_n],$$

onde $G(X_0, X_1)$ é um polinômio homogêneo e irredutível de grau $d - q - 1$. Claramente, F é homogêneo de grau d. Se P é um ponto $\mathbb{F}_q$ - racional, com coordenadas homogêneas $x_0, x_1, ..., x_n \in \mathbb{F}_q$, segue da proposição 2.10 que

$$F(x_0, x_1, ..., x_n) = G(x_0, x_1)[x_0^q x_1 - x_0 x_1^q] = G(x_0, x_1)[x_0 x_1 - x_0 x_1] = 0.$$

Portanto, considerando $\mathcal{X} = \mathbf{v}(F) \subseteq \mathbb{P}^n(K)$ tem-se $|\mathcal{X}(\mathbb{F}_q)| = \theta_q(n)$.

Exemplo 3.3. Seja $\mathcal{X} = \mathbf{v}(x_1^q x_3 - x_1 x_3^q + x_0^q x_2 - x_0 x_2^q)$ em $\mathbb{P}^3(K)$. Então $\mathcal{X}$ é uma superfície irredutível, não singular e com $q^3 + q^2 + q + 1$ pontos $\mathbb{F}_q$-racionais (veja, artigo [16]).

Assim, no problema 1, quando consideramos hipersuperfícies de modo geral, não precisamos mais considerar os casos $d \geq q + 1$. Os casos $d \leq q$ foram respondidos por Serre e sobre quais condições esse limite é atingido, isso será apresentado na próxima seção (teorema 3.2). Quando apenas consideramos hipersuperfícies não singulares de grau d, o problema 1 torna-se um pouco mais complicado. Para o caso $n = 2$, existe o teorema de Hasse-Weil:

Teorema 3.1 (Hasse-Weil)**.** *Seja $\mathcal{C}$ uma curva não singular de grau d em $\mathbb{P}^2(K)$ definida sobre $\mathbb{F}_q$. Então*

$$|\mathcal{C}(\mathbb{F}_q)| \leq 1 + q + (d - 1)(d - 2)\sqrt{q}.$$

Demonstração. Veja [15, teorema 9.18]. ■

Exemplo 3.4. Seja $q = 2^2$. Considere a curva Hermitiana $\mathcal{H} = \mathbf{v}(X_0^3 + X_1^3 + X_2^3)$. Segue do teorema 2.3 que

$$|\mathcal{H}(\mathbb{F}_q)| = \frac{[2^3 - (-1)^3][2^2 - (-1)^2]}{2^2 - 1} = 9 = 1 + 2^2 + (3-1)(3-2)2.$$

Geralmente, o teorema de Hasse-Weil é apresentado em relação ao gênero da curva, conceito não definido aqui, o qual consegue extrair algumas informações da curva melhor que o grau, mas para fins deste primeiro trabalho utilizamos apenas o conceito de grau. Para um estudo detalhado sobre curvas, indicamos a leitura do livro [15].

No caso $n = 3$, a quantidade de pontos $\mathbb{F}_q$-racionais em uma superfície $\mathcal{X}$ não singular e definida sobre $\mathbb{F}_q$ satisfaz

$$|\mathcal{X}(\mathbb{F}_q)| = q^2 + tq + 1, \tag{3.1}$$

onde $-2 \leq t \leq 7$ e $t \neq 6$. Além disso, a igualdade (3.1) é possível exceto quando $q = 2, 3$ ou 5 (veja, artigo [17]).

Sobre algumas condições adicionais, Homma e Kim, em uma sequência de três artigos [5, 6, 7], conseguem provar a conjectura Sziklai, apresentada por Peter Sziklai em [4], que melhora o limite do teorema de Serre para curvas que não contém uma reta definida sobre $\mathbb{F}_q$. Posteriormente, no artigo [8], temos uma generalização para hipersuperfícies sem componentes $\mathbb{F}_q$-lineares, limite considerado elementar pelos próprios autores. Esses resultados possibilitaram a Mrinmoy Datta em [9] apresentar uma resposta para o problema 1 no caso de uma hipersuperfície não singular de grau d em $\mathbb{P}^4(K)$, sobre algumas condições para d. Isso será apresentado com detalhes na última seção do capítulo.

3.2 Teorema de Serre

Nesta seção, apresentaremos a resposta dada por Serre em [3] para o problema 1 para os casos $d \leq q + 1$ e sobre quais condições esse limite é atingido. Antes disso, para uma melhor compreensão, precisamos de uma proposição e um exemplo:

Proposição 3.2. *Sejam $\mathcal{X} = \mathbf{v}(F)$ uma hipersuperfície e $H = \mathbf{v}(a_0X_0 + \cdots + a_nX_n)$ um hiperplano em $\mathbb{P}^n(K)$ definidas sobre $\mathbb{F}_q$:*

i) Se F restrito a H não é identicamente nulo, então $\mathcal{X} \cap H$ é uma hipersuperfície de grau d em $H \simeq \mathbb{P}^{n-1}(K)$ definida sobre $\mathbb{F}_q$.

ii) Se $\mathcal{X}$ não contém uma componente $\mathbb{F}_q$-linear, então $\mathcal{X} \cap H$ é uma hipersuperfície de grau d em $H \simeq \mathbb{P}^{n-1}(K)$ definida sobre $\mathbb{F}_q$. Além disso, se $\mathcal{X}$ não contém um subespaço de codimensão 2, então $\mathcal{X} \cap H$ não contém uma componente $\mathbb{F}_q$ - linear.

Demonstração.

i) Sem perda de generalidade, suponha que $F \in \mathbb{F}_q[X_0, ..., X_n]$ e $a_0, ..., a_n \in \mathbb{F}_q$. Como H é um hiperplano, existe $a_j \neq 0$. Para simplificar as notações, considere $j = 0$. Assim, o hiperplano H é definido pela equação $X_0 = -a_0^{-1}(a_1X_1 + \cdots + a_nX_n)$. Deste modo, se $[x_0 : \cdots : x_n] \in H$ então $(x_1, ..., x_n) \neq 0$, pois caso contrário teríamos $(x_0, ..., x_n) = 0$. Segue daí que existe uma correspondência natural entre H e $\mathbb{P}^{n-1}(K)$, dada por

$$[x_0 : x_1 : \cdots : x_n] \in H \longleftrightarrow [x_1 : \cdots : x_n] \in \mathbb{P}^{n-1}(K). \tag{3.2}$$

Defina

$$G(X_1,...,X_n) = F\left(-a_0^{-1}(a_1X_1+\cdots+a_nX_n), X_1,...,X_n\right) \in \mathbb{F}_q[X_1,...,X_n].$$

Como F restrito a H não é identicamente nulo, tem-se $G \neq 0$. Seja $\lambda \in K$, temos

$$\begin{aligned} G(\lambda X_1,...,\lambda X_n) &= F\left(-a_0^{-1}(a_1\lambda X_1+\cdots+a_n\lambda X_n), \lambda X_1,...,\lambda X_n\right) \\ &= F\left(-\lambda a_0^{-1}(a_1X_1+\cdots+a_nX_n), \lambda X_1,...,\lambda X_n\right) \\ &= \lambda^d F\left(-a_0^{-1}(a_1X_1+\cdots+a_nX_n), X_1,...,X_n\right) \\ &= \lambda^d G(X_1,...,X_n). \end{aligned}$$

Segue da proposição 2.1 que G é homogêneo de grau d. Além disso, com a identificação (3.2), tem-se $\mathcal{X} \cap H \simeq \mathbf{v}(G)$.

ii) A primeira afirmação segue do item (i), pois nenhum hiperplano definida sobre $\mathbb{F}_q$ é uma componente de $\mathcal{X}$. Além disso, se a hipersuperfície $\mathcal{X} \cap H$ em $H \simeq \mathbb{P}^{n-1}(K)$ contém uma componente $\mathbb{F}_q$ - linear, então $\mathcal{X}$ contém um subespaço $\mathbb{F}_q$ - linear de codimensão 2.

■

No próximo exemplo estabelecemos a quantidade de pontos $\mathbb{F}_q$-racionais na união de d hiperplanos em $\mathbb{P}^n(K)$ definidos sobre $\mathbb{F}_q$ e sobre algumas condições.

Exemplo 3.5. Considere d um número natural com $d \leq q$. Sejam $H_1,...,H_d$ hiperplanos distintos em $\mathbb{P}^n(K)$ definidos sobre $\mathbb{F}_q$ tais que a interseção contém um subespaço S definido sobre $\mathbb{F}_q$ de codimensão 2. Como $|H_j(\mathbb{F}_q)| = q^{n-1} + |S(\mathbb{F}_q)|$ para todo $j = 1,...,d$, então cada hiperplano tem q^{n-1} pontos $\mathbb{F}_q$-racionais que não pertencem a $S(\mathbb{F}_q)$, além disso, todos esses pontos são distintos, pois dado um subespaço de codimensão 2 e um ponto fora dele existe um único hiperplano que contém o subespaço e o ponto. Como temos d hiperplanos, então $|(H_1 \cup \cdots \cup H_d)(\mathbb{F}_q)| = dq^{n-1} + |S(\mathbb{F}_q)| = dq^{n-1} + \theta_q(n-2)$.

Teorema 3.2 (Serre)**.** *Seja $\mathcal{X}$ uma hipersuperfície de grau d em $\mathbb{P}^n(K)$ definida sobre $\mathbb{F}_q$. Se $d \leq q+1$, então*

$$|\mathcal{X}(\mathbb{F}_q)| \leq dq^{n-1} + \theta_q(n-2).$$

Além disso, se $d \leq q$, o limite é atingido por uma hipersuperfície $\mathcal{X}$ se, e somente se, $\mathcal{X}$ é a união de d hiperplanos definidos sobre $\mathbb{F}_q$ tais que a interseção dos hiperplanos contém um subespaço de codimensão 2 definido sobre $\mathbb{F}_q$.

Demonstração. Seja $F \in \mathbb{F}_q[X_0, X_1, ..., X_n]$ homogêneo de grau d tal que $\mathcal{X} = \mathbf{v}(F)$. Se $d = q+1$, tem-se

$$dq^{n-1} + \theta_q(n-2) = q^n + q^{n-1} + \theta_q(n-2) = \theta_q(n),$$

consequentemente, a cota superior dada pelo teorema é trivial. Suponha $d \leq q$. Provemos o resultado usando o princípio da indução finita sobre n: para $n = 1$ considere

$$f(X_1) = F(1, X_1)$$

a desomogenização de F em relação à variável X_0. Sendo K um corpo algebricamente fechado, existem $c, \alpha_1, ..., \alpha_m \in K$, com $m \leq d$, tais que

$$f(X_1) = c\prod_{j=1}^{m}(X_1 - \alpha_j)^{\beta_j}$$

onde $\beta_j \geq 1$ para todo $j = 1, ..., m$. Homogenizando f em relação à variável X_0 obtemos

$$c\prod_{j=1}^{m}(X_1 - \alpha_j X_0)^{\beta_j}.$$

Assim devemos ter

$$F = c\ X_0^e \prod_{j=1}^{m}(X_1 - \alpha_j X_0)^{\beta_j},$$

para algum $e \geq 0$. O resultado segue. Suponha agora $n \geq 2$. Sejam $G_1, ..., G_s$ os distintos fatores lineares de F em $\mathbb{F}_q[X_0, ..., X_n]$. Para cada $j = 1, ..., s$, considere o hiperplano

$$H_j = \mathbf{v}(G_j).$$

Seja $Y_s = H_1 \cup \cdots \cup H_s$ (caso não existam fatores lineares considere $Y_0 = \emptyset$). Claramente, $Y_s \subseteq \mathcal{X}$. Vamos dividir a prova em dois casos:

***Caso 1**: Suponha que $Y_s = \mathcal{X}$.* Neste caso $s \neq 0$ e provemos por indução sobre s que vale

$$|Y_s(\mathbb{F}_q)| \leq sq^{n-1} + \theta_q(n-2). \tag{3.3}$$

Para $s = 1$, temos

$$|Y_1(\mathbb{F}_q)| = |H_1(\mathbb{F}_q)| = \theta_q(n-1) = q^{n-1} + \theta_q(n-2).$$

Suponha verdadeiro para algum $s \geq 1$. Sabemos que H_{s+1} tem $\theta_q(n-1) = q^{n-1} + \theta_q(n-2)$ pontos $\mathbb{F}_q$ - racionais e $|(H_{s+1} \cap Y_s)(\mathbb{F}_q)| \geq \theta_q(n-2)$, pois trata-se da interseção de um hiperplano com um conjunto que contém um hiperplano. Logo, pela hipótese de indução, tem-se

$$\begin{aligned} |Y_{s+1}(\mathbb{F}_q)| &= |Y_s(\mathbb{F}_q)| + |H_{s+1}(\mathbb{F}_q)| - |(H_{s+1} \cap Y_s)(\mathbb{F}_q)| \\ &\leq sq^{n-1} + \theta_q(n-2) + q^{n-1} + \theta_q(n-2) - \theta_q(n-2) \\ &= (s+1)q^{n-1} + \theta_q(n-2). \end{aligned}$$

Como $s \leq d$, segue da desigualdade (3.3) que

$$|\mathcal{X}(\mathbb{F}_q)| = |Y_s(\mathbb{F}_q)| \leq sq^{n-1} + \theta_q(n-2) \leq dq^{n-1} + \theta_q(n-2).$$

Além disso, vale a igualdade apenas quando $s = d$ e a interseção dos hiperplanos contém um subespaço de codimensão 2 definido sobre $\mathbb{F}_q$ (veja, exemplo 3.5).

***Caso 2**: Suponha que $Y_s \subsetneq \mathcal{X}$.* Seja $P_0 \in \mathcal{X}$ tal que $P_0 \notin Y_s$. Se H é um hiperplano definido sobre $\mathbb{F}_q$ que contém o ponto P_0, então F restrito a H não é identicamente nulo, pois caso contrário $H \subseteq Y_s$. Assim, pela proposição 3.2 item (i), tem-se que $\mathcal{X} \cap H$ é uma hipersuperfície de grau d em $H \simeq \mathbb{P}^{n-1}(K)$ definida sobre $\mathbb{F}_q$. Pela hipótese de indução, temos

$$|(\mathcal{X} \cap H)(\mathbb{F}_q)| \leq dq^{n-2} + \theta_q(n-3). \tag{3.4}$$

Considere $\check{\mathbb{P}}_0 = \{H \in \check{\mathbb{P}}^n(K);\ H \text{ é definido sobre } \mathbb{F}_q \text{ e } P_0 \in H\}$. Defina

$$\mathcal{P} = \{(P', H) \in (\mathcal{X}(\mathbb{F}_q) - \{P_0\}) \times \check{\mathbb{P}}_0;\ P' \in H\}.$$

Para cada $P' \in \mathcal{X}(\mathbb{F}_q) - \{P_0\}$ existem, pela proposição 1.9, $\theta_q(n-2)$ hiperplanos definidos sobre $\mathbb{F}_q$ contendo P_0 e P', consequentemente,

$$|\mathcal{P}| = (|\mathcal{X}(\mathbb{F}_q)| - 1)\theta_q(n-2).$$

Além disso, pela equação (3.4), para cada hiperplano $H \in \check{\mathbb{P}}_0$ o número de $P' \in \mathcal{X}(\mathbb{F}_q) - \{P_0\}$ satisfaz

$$|(\mathcal{X} \cap H)(\mathbb{F}_q)| - 1 \leq dq^{n-2} + \theta_q(n-3) - 1$$

e, pela observação 1.4, temos $|\check{\mathbb{P}}_0| = \theta_q(n-1)$. Assim,

$$|\mathcal{P}| \leq \theta_q(n-1)(dq^{n-2} + \theta_q(n-3) - 1).$$

Logo, vale

$$(|\mathcal{X}(\mathbb{F}_q)| - 1)\theta_q(n-2) = |\mathcal{P}| \leq \theta_q(n-1)(dq^{n-2} + \theta_q(n-3) - 1),$$

consequentemente, temos

$$\begin{aligned}
|\mathcal{X}(\mathbb{F}_q)| &\leq 1 + \frac{\theta_q(n-1)}{\theta_q(n-2)}(dq^{n-2} + \theta_q(n-3) - 1) \\
&= 1 + \frac{q\theta_q(n-2)+1}{\theta_q(n-2)}(dq^{n-2} + \theta_q(n-3) - 1) \\
&= 1 + dq^{n-1} + q\theta_q(n-3) - q + \frac{1}{\theta_q(n-2)}(dq^{n-2} + \theta_q(n-3) - 1) \\
&= dq^{n-1} + \theta_q(n-2) - \frac{1}{\theta_q(n-2)}(q\theta_q(n-2) - dq^{n-2} - \theta_q(n-3) + 1).
\end{aligned}$$

Observe que

$$q\theta_q(n-2) - \theta_q(n-3) + 1 = (q^{n-1} + \cdots + q) - (q^{n-3} + \cdots + q + 1) + 1 = q^{n-1} + q^{n-2}.$$

Como $d \leq q < q+1$ então $q + 1 - d > 0$, assim

$$\frac{1}{\theta_q(n-2)}(q\theta_q(n-2) - dq^{n-2} - \theta_q(n-3) + 1) = \frac{q^{n-2}}{\theta_q(n-2)}(q + 1 - d) > 0.$$

Portanto,

$$|\mathcal{X}(\mathbb{F}_q)| < dq^{n-1} + \theta_q(n-2).$$

■

Pelo exemplo 3.2, se $d \geq q+1$, existe uma hipersuperfície de grau d com $\theta_q(n)$ pontos $\mathbb{F}_q$-racionais. Além disso, quando $d \geq q+1$, tem-se

$$dq^{n-1} + \theta_q(n-2) \geq (q+1)q^{n-1} + \theta_q(n-2) = \theta_q(n).$$

Deste modo,

$$M_q(d,n) := min\{\theta_q(n),\ dq^{n-1} + \theta_q(n-2)\}$$

é o número máximo de pontos $\mathbb{F}_q$-racionais de uma hipersuperfície de grau d em $\mathbb{P}^n(K)$ definida sobre $\mathbb{F}_q$. Além disso, se $d \geq q+1$, o limite é atingido pela hipersuperfície dada no exemplo 3.2 e, se $d \leq q$, o limite é atingido pela união de d hiperplanos tal que a interseção contém um subespaço de codimensão 2 (veja, exemplo 3.5).

3.3 Hipersuperfícies sem componentes $\mathbb{F}_q$ - lineares

Nosso próximo objetivo consiste em enunciar a resposta dada por Homma e Kim em uma séries de três artigos [5, 6, 7] para a conjectura de Sziklai, apresentada por Peter Skizlai em [4], sobre o número máximo de pontos $\mathbb{F}_q$-racional em uma curva de grau d que não contém um reta definida sobre $\mathbb{F}_q$, necessária para a seção final. Posteriormente, apresentamos uma versão mais geral, considerando uma hipersuperfície de grau d definida sobre $\mathbb{F}_q$ sem componente $\mathbb{F}_q$-linear, provada pelos mesmos autores em [8].

Teorema 3.3 (Limite de Sziklai)**.** *Seja $\mathcal{C}$ uma curva plana de grau d em $\mathbb{P}^2(K)$ definida sobre $\mathbb{F}_q$ que não contém uma reta definida sobre $\mathbb{F}_q$, então*

$$|\mathcal{C}(\mathbb{F}_q)| \leq (d-1)q + 1.$$

Exceto para uma curva em $\mathbb{F}_4$ projetivamente equivalente à curva definida por

$$(X+Y+Z)^4 + (XY+YZ+ZX)^2 + XYZ(X+Y+Z) = 0. \tag{3.5}$$

Demonstração. Veja os artigos [5, 6, 7]. ■

Observação 3.1. No artigo [5] é provado o caso $d = q+1$ e que a curva dada pela expressão (3.5) tem 14 pontos $\mathbb{F}_4$-racionais. Em [7] é provado o caso para curvas irredutíveis, não clássicas q-Frobenius. Os demais casos são feitos em [6].

Nestas condições a cota superior dada pelo teorema anterior é melhor que a do teorema de Serre 3.2, pois $(d-1)q + 1 = dq - q + 1 < dq + 1$. Pouco tempo depois, Homma e Kim publicaram um artigo com uma versão mais geral. Primeiramente, para uma boa compreensão, precisamos de uma definição e alguns resultados.

Definição 3.2. Para $S \subseteq \mathbb{P}^n(\mathbb{F}_q)$ o i-ésimo s-grau de S, denotado por $d_i(S)$, é definido por

$$d_i(S) := max\{|S \cap M_i|;\ M_i \text{ é um subespaço } \mathbb{F}_q\text{-linear de codimensão } i\}.$$

O i-ésimo s-grau só faz sentido quando $0 \leq i \leq n$.

Lema 3.1. *Sejam $S \subseteq \mathbb{P}^n(\mathbb{F}_q)$ e $d_1 = d_1(S)$. Então*

$$|S| \leq (d_1 - 1)q + 1 + \left\lfloor \frac{d_1 - 1}{\theta_q(n-2)} \right\rfloor.$$

Demonstração. Fixe um ponto $P_0 \in S$. Seja $\check{\mathbb{P}}_0 = \{H \in \check{\mathbb{P}}^n(\mathbb{F}_q);\ P_0 \in H\}$. Defina

$$\mathcal{P} := \{(P, H) \in (S - \{P_0\}) \times \check{\mathbb{P}}_0;\ P \in H\}.$$

Segue da proposição 1.9 que para cada $P \in (S - \{P_0\})$ existem $\theta_q(n-2)$ hiperplanos contendo P e P_0. Segue daí que

$$|\mathcal{P}| = (|S| - 1)\theta_q(n-2). \tag{3.6}$$

Além disso, se $d_1 = d_1(S)$, então $|(S - \{P_0\}) \cap H| \leq d_1 - 1$ para todo $H \in \check{\mathbb{P}}_0$ e, pela observação 1.4, temos $|\check{\mathbb{P}}_0| = \theta_q(n-1)$. Assim,

$$|\mathcal{P}| \leq (d_1 - 1)|\check{\mathbb{P}}_0| = (d_1 - 1)\theta_q(n-1). \tag{3.7}$$

Segue da igualdade (3.6) e da desigualdade (3.7) que

$$(|S| - 1)\theta_q(n-2) = |\mathcal{P}| \leq (d_1 - 1)\theta_q(n-1).$$

Logo, tem-se

$$\begin{aligned} |S| &\leq 1 + \frac{\theta_q(n-1)}{\theta_q(n-2)}(d_1 - 1) \\ &= 1 + \frac{q\theta_q(n-2) + 1}{\theta_q(n-2)}(d_1 - 1) \\ &= (d_1 - 1)q + 1 + \frac{d_1 - 1}{\theta_q(n-2)}. \end{aligned}$$

■

O leitor mais atento deve ter percebido que o argumento usado para provar o lema anterior já apareceu na demonstração de outro resultado (por exemplo, demonstração do caso 2 no teorema 3.2). Pois bem, este argumento é muito utilizado em geometria algébrica sobre corpos finitos e na teoria de códigos corretores de erros para determinar cotas.

Lema 3.2. *Sejam $S \subseteq \mathbb{P}^n(\mathbb{F}_q)$, $d_1 = d_1(S)$ e $d_2 = d_2(S)$. Então*

$$|S| \leq (d_1 - d_2)q + d_1.$$

Demonstração. Sejam L_0 um subespaço linear de codimensão 2 tal que $|S \cap L_0| = d_2$ e L_0^* o conjunto dos hiperplanos em $\mathbb{P}^n(\mathbb{F}_q)$ contendo L_0. Como $|H \cap S| \leq d_1$ para todo hiperplano e existem $q+1$ hiperplanos contendo L_0, então

$$\begin{aligned} |S| &= \sum_{H \in L_0^*} (|H \cap S| - d_2) + d_2 \\ &\leq (d_1 - d_2)(q+1) + d_2 = (d_1 - d_2)q + d_1. \end{aligned}$$

■

Com isso, quando considerarmos hipersuperfícies sem componente $\mathbb{F}_q$-linear, é possível melhorar a cota superior dada pelo teorema Serre 3.2. Essa cota é apresentada em [8] e é considerada elementar pelos próprios autores:

Teorema 3.4 (Homma-Kim)**.** *Seja $\mathcal{X} \subset \mathbb{P}^n(K)$, com $n \geq 2$, uma hipersuperfície de grau d definida sobre $\mathbb{F}_q$. Se $\mathcal{X}$ não contém uma componente $\mathbb{F}_q$-linear, então*

$$|\mathcal{X}(\mathbb{F}_q)| \leq (d-1)q^{n-1} + dq^{n-2} + \theta_q(n-3).$$

Demonstração. Se $d \geq q+1$, então

$$(d-1)q^{n-1} + dq^{n-2} + \theta_q(n-3) \geq q^n + (q+1)q^{n-2} + \theta_q(n-3) = \theta_q(n),$$

consequentemente, a cota superior é trivial. Suponha que $d \leq q+1$. Provemos o resultado usando o princípio de indução finita sobre n: para $n = 2$, segue do teorema 3.3, que

$$|\mathcal{X}(\mathbb{F}_q)| \leq (d-1)q + 2 \leq (d-1)q + d.$$

Para $n \geq 3$, vamos dividir a prova em dois casos:

Caso 1*: Suponha que exista um subespaço $\mathbb{F}_q$-linear de codimensão 2 em $\mathbb{P}^n(K)$ contido em $\mathcal{X}$.* Deste modo, o segundo s-grau de $\mathcal{X}(\mathbb{F}_q)$ é $\theta_q(n-2)$. Como $\mathcal{X}$ não contém um componente $\mathbb{F}_q$-linear, então para todo hiperplano H em $\mathbb{P}^n(K)$ definido sobre $\mathbb{F}_q$ tem-se, pela proposição 3.2 item (ii), que $\mathcal{X} \cap H$ é uma hipersuperfície definida sobre $\mathbb{F}_q$ de grau d em $H \simeq \mathbb{P}^{n-1}(K)$. Segue do teorema Serre 3.2 que

$$|(\mathcal{X} \cap H)(\mathbb{F}_q)| \leq dq^{n-2} + \theta_q(n-3).$$

Assim, o primeiro s-grau de $\mathcal{X}(\mathbb{F}_q)$ é no máximo $dq^{n-2} + \theta_q(n-3)$. Pelo lema 3.2, temos

$$\begin{aligned} |\mathcal{X}(\mathbb{F}_q)| &\leq (dq^{n-2} + \theta_q(n-3) - \theta_q(n-2))q + dq^{n-2} + \theta_q(n-3) \\ &= (dq^{n-2} - q^{n-2})q + dq^{n-2} + \theta_q(n-3) \\ &= (d-1)q^{n-1} + dq^{n-2} + \theta_q(n-3). \end{aligned}$$

Caso 2*: Suponha que não exista um subespaço $\mathbb{F}_q$-linear de codimensão 2 em $\mathbb{P}^n(K)$ contido em $\mathcal{X}$.* Assim, se H é um hiperplano em $\mathbb{P}^n(K)$ definido sobre $\mathbb{F}_q$, pela proposição 3.2 item (ii),

tem-se que $\mathcal{X} \cap H$ é uma hipersuperfície de grau d em $H \simeq \mathbb{P}^{n-1}(K)$ sem componente $\mathbb{F}_q$-linear. Por hipótese de indução, temos

$$|(\mathcal{X} \cap H)(\mathbb{F}_q)| \leq (d-1)q^{n-2} + dq^{n-3} + \theta_q(n-4).$$

Assim, o primeiro s-grau de $\mathcal{X}(\mathbb{F}_q)$ é no máximo $(d-1)q^{n-2} + dq^{n-3} + \theta_q(n-4)$. Segue do lema 3.1 que

$$|\mathcal{X}(\mathbb{F}_q)| \leq ((d-1)q^{n-2} + dq^{n-3} + \theta_q(n-4) - 1)q + 1 + \left\lfloor \frac{(d-1)q^{n-2} + dq^{n-3} + \theta_q(n-4) - 1}{\theta_q(n-2)} \right\rfloor.$$

Como

$$\begin{aligned}
&(d-1)q^{n-2} + dq^{n-3} + \theta_q(n-4) - 1 \\
&= (d-1)(q^{n-2} + q^{n-3} + \theta_q(n-4)) + q^{n-3} - (d-2)\theta_q(n-4) - 1 \\
&= (d-1)\theta_q(n-2) + q^{n-3} - ((d-2)\theta_q(n-4) + 1) \\
&< (d-1)\theta_q(n-2) + q^{n-3},
\end{aligned}$$

temos

$$\left\lfloor \frac{(d-1)q^{n-2} + dq^{n-3} + \theta_q(n-4) - 1}{\theta_q(n-2)} \right\rfloor \leq \left\lfloor d - 1 + \frac{q^{n-3}}{\theta_q(n-2)} \right\rfloor = d - 1.$$

Portanto, como $d - q \leq 1$, temos

$$\begin{aligned}
|\mathcal{X}(\mathbb{F}_q)| &\leq ((d-1)q^{n-2} + dq^{n-3} + \theta_q(n-4) - 1)q + 1 + (d-1) \\
&= (d-1)q^{n-1} + dq^{n-2} + \theta_q(n-4)q + (d-q) \\
&\leq (d-1)q^{n-1} + dq^{n-2} + \theta_q(n-4)q + 1 \\
&= (d-1)q^{n-1} + dq^{n-2} + \theta_q(n-3).
\end{aligned}$$

■

Para o caso $n = 2$, a cota superior dada pelo teorema de Homma-Kimm 3.4 não é muito boa, mas se $n \geq 3$ o limite é alcançado por algumas hipersuperfícies.

Exemplo 3.6. Segue do teorema 2.3 que a superfície Hermitiana

$$\mathcal{H} = \mathbf{v}(X_0^{q+1} + X_1^{q+1} + X_2^{q+1} + X_3^{q+1})$$

em $\mathbb{P}^3(K)$ tem $(q^2+1)(q^3+1)$ pontos $\mathbb{F}_{q^2}$ - racional. Além disso, observe que

$$((q+1) - 1)q^4 + (q+1)q^2 + \theta_q(0) = (q^2+1)(q^3+1).$$

Observe que sobre tais condições essa cota é melhor que a cota do teorema de Serre 3.2: considere $d \leq q$, temos

$$dq^{n-1} + \theta_q(n-2) - (q+1-d) - ((d-1)q^{n-1} + dq^{n-2} + \theta_q(n-3)) = (q+1-d)(q^{n-2} - 1).$$

Assim

$$dq^{n-1} + \theta_q(n-2) - (q+1-d) = (d-1)q^{n-1} + dq^{n-2} + \theta_q(n-3) + (q+1-d)(q^{n-2} - 1),$$

consequentemente,

$$dq^{n-1} + \theta_q(n-2) > (d-1)q^{n-1} + dq^{n-2} + \theta_q(n-3).$$

3.4 Hipersuperfícies não singulares em $\mathbb{P}^4$

Para finalizar este ultimo capítulo, vamos apresentar a resposta dada por Mrinmoy Datta em [9] sobre o número máximo de pontos $\mathbb{F}_q$-racionais em uma hipersuperfície $\mathcal{X}$ não singular de grau d em $\mathbb{P}^4(K)$ definida sobre $\mathbb{F}_q$, com $(d,q) \neq (4,4)$ e $2 \leq d \leq q$. Mais explicitamente, Datta mostra que

$$|\mathcal{X}(\mathbb{F}_q)| \leq (d-1)q^3 + (d-1)q^2 + q + 1. \tag{3.8}$$

Antes de prosseguir com os resultados necessários para provar a desigualdade (3.8), vamos fixar algumas notações que iremos utilizar durante está seção:

i) A menos que seja mencionado o contrário, d vai representar um número natural tal que $2 \leq d \leq q$ e $\mathcal{X}$ uma hipersuperfície não singular de grau d em $\mathbb{P}^4(K)$ definida sobre $\mathbb{F}_q$.

ii) Dado $P \in \mathcal{X}(\mathbb{F}_q)$, defina

$$\mathcal{L}(P,\mathcal{X}) := \textit{o conjunto das retas } l \textit{ satisfazendo } P \in l \subset \mathcal{X}$$

$$\mathcal{L}_q(P,\mathcal{X}) := \textit{o conjunto das retas } l \textit{ definidas sobre } \mathbb{F}_q \textit{ satisfazendo } P \in l \subset \mathcal{X}.$$

iii) Para uma reta $l \subseteq \mathbb{P}^4(K)$ definida sobre $\mathbb{F}_q$ defina

$$\mathcal{B}(l) := \textit{ o conjunto dos planos } \Pi \subseteq \mathbb{P}^4(K) \textit{ definidos sobre } \mathbb{F}_q \textit{ satisfazendo } l \subseteq \Pi.$$

A cardinalidade de $\mathcal{B}(l)$ é facilmente calculada.

Proposição 3.3. $|\mathcal{B}(l)| = q^2 + q + 1$.

Demonstração. Para cada $Q \in \mathbb{P}^4(\mathbb{F}_q) \backslash l(\mathbb{F}_q)$ existe um único plano Π definido sobre $\mathbb{F}_q$ contendo l e Q. Como $|l(\mathbb{F}_q)| = q+1$, temos $q^4+q^3+q^2$ planos definidos sobre $\mathbb{F}_q$ que contém l. Entretanto, cada plano foi contado q^2 vezes, pois um plano tem q^2+q+1 pontos $\mathbb{F}_q$ - racionais, assim

$$|\mathcal{B}(l)| = \frac{q^4+q^3+q^2}{q^2} = \frac{q^2(q^2+q+1)}{q^2} = q^2+q+1.$$

■

Além disso, claramente, temos

$$\mathbb{P}^4(\mathbb{F}_q) = \bigcup_{\Pi \in \mathcal{B}(l)} \Pi(\mathbb{F}_q).$$

Agora vamos apresentar um invariante que as hipersuperfícies não singulares em $\mathbb{P}^n(K)$ definidas sobre $\mathbb{F}_q$ possuem:

Definição 3.3. O **invariante de Koen Thas** de uma hipersuperfície $\mathcal{X}$ em $\mathbb{P}^n(K)$ definida sobre $\mathbb{F}_q$, denotado por $k_{\mathcal{X}}$, é definida por

$$k_{\mathcal{X}} := max\{dim(L);\ L \subseteq \mathcal{X} \textit{ e } L \textit{ é um subespaço linear de } \mathbb{P}^n(K) \textit{ definido sobre } \mathbb{F}_q\ \}$$

O termo "invariante" na definição é devido ao seguinte teorema:

Teorema 3.5. *Se $\mathcal{X}$ é uma hipersuperfície não singular grau $d \geq 2$ em $\mathbb{P}^n(K)$ definida sobre $\mathbb{F}_q$, então*

$$k_{\mathcal{X}} \leq \lfloor (n-1)/2 \rfloor.$$

Demonstração. Seja $L \subseteq \mathcal{X}$ um subespaço linear de $\mathbb{P}^n(K)$ definido sobre $\mathbb{F}_q$. Seja $r = dim(L)$. Escolha um sistema de coordenadas $X_0, ..., X_n$ em $\mathbb{P}^n$ tal que L é definido por $X_0 = \cdots = X_{n-r-1} = 0$. Como $L \subseteq \mathcal{X}$ a equação de $\mathcal{X}$ é da forma

$$F(X_0, ..., X_n) = \sum_{i=0}^{n-r-1} f_i(X_0, ..., X_n)X_i = 0.$$

Como $deg(\mathcal{X}) \geq 2$, cada f_i é um polinômio homogêneo não constante. Considere as equações simultâneas

$$F = \frac{\partial F}{\partial X_0} = \cdots = \frac{\partial F}{\partial X_n} = 0,$$

mais explicitamente,

$$\begin{aligned}
F &= \sum_{i=0}^{n-r-1} f_i(X_0, ..., X_n)X_i = 0 \\
\frac{\partial F}{\partial X_0} &= \sum_{i=0}^{n-r-1} \frac{\partial f_i}{\partial X_0}X_i + f_0 = 0 \\
&\vdots \\
\frac{\partial F}{\partial X_{n-r-1}} &= \sum_{i=0}^{n-r-1} \frac{\partial f_i}{\partial X_{n-r-1}}X_i + f_{n-r-1} = 0 \\
\frac{\partial F}{\partial X_{n-r}} &= \sum_{i=0}^{n-r-1} \frac{\partial f_i}{\partial X_{n-r}}X_i = 0 \\
&\vdots \\
\frac{\partial F}{\partial X_n} &= \sum_{i=0}^{n-r-1} \frac{\partial f_i}{\partial x_n}X_i = 0.
\end{aligned}$$

Podemos ver o conjunto $\{X_{n-r}, ..., X_n\}$ como sistema de coordenadas de $L = \mathbb{P}^r(K)$. Suponha que $n - r \leq r$. Pela proposição 2.11, as $n - r$ equações

$$\begin{cases}
f_0(0, ..., 0, X_{n-r}, ..., X_n) = 0 \\
\vdots \\
f_{n-r-1}(0, ..., 0, X_{n-r}, ..., X_n) = 0
\end{cases}$$

admitem solução $[\alpha_{n-r} : \cdots : \alpha_n] \in \mathbb{P}^r(K)$. Claramente, $[0 : \cdots : 0 : \alpha_{n-r} : \cdots : \alpha_n] \in L \subseteq \mathcal{X}$ é um ponto singular de $\mathcal{X}$, absurdo. Portanto, $n - r > r$ e assim $r \leq (n-1)/2$.

■

Para finalizar está seção, apresentamos um resultado sobre o limite superior do número de retas que passam por um ponto em uma superfície, correspondente ao teorema 3.1 do artigo [9]. Sabemos pelo teorema 3.5 que nenhuma superfície não singular de grau $d \geq 2$ em $\mathbb{P}^3(K)$ definida sobre $\mathbb{F}_q$ contém um plano definido sobre $\mathbb{F}_q$, assim, vamos reformulamos o teorema e fazer algumas pequenas modificações na demonstração. Antes, precisamos definir o que é um cone sobre uma curva plana.

Definição 3.4. Sejam $\mathcal{Y}$ uma curva plana (contida em um plano) em $\mathbb{P}^n(K)$ e $P \in \mathbb{P}^n(K)$. O cone sobre a curva plana $\mathcal{Y}$ com centro em P, denotado por $C(\mathcal{Y}, P)$, é definido como sendo a reunião das retas $l(P, Q)$ com $Q \in \mathcal{Y}$.

Observação 3.2. Seja $\mathcal{Y}$ uma curva plana de grau d em $\mathbb{P}^3(K)$. Assim, por definição, existem um plano Π e uma hipersuperfície $\mathcal{X} = \mathbf{v}(F)$ de grau d em $\mathbb{P}^3(K)$ tal que $\mathcal{Y} = \Pi \cap \mathcal{X}$. Dado $P \in \mathbb{P}^3(K)\backslash\Pi$ podemos assumir que $P = [1 : 0 : 0 : 0]$ e $\Pi = \mathbf{v}(X_0)$ (veja, exemplo 2.9). Considere $G(X_1, X_2, X_3) = F(0, X_1, X_2, X_3)$. Claramente, G é homogêneo de grau d. Afirmamos que

$$C(\mathcal{Y}, P) = \{[x_0 : x_1 : x_2 : x_3] \in \mathbb{P}^3(K);\ G(x_1, x_2, x_3) = 0\}.$$

Com efeito, dado $Q = [0 : x_1 : x_2 : x_3] \in \mathcal{Y}$, tem-se $G(\beta x_1, \beta x_2, \beta x_3) = \beta^d G(x_1, x_2, x_3) = 0$. Assim, $l(P, Q) \subseteq \{[x_0 : x_1 : x_2 : x_3] \in \mathbb{P}^3(K);\ G(x_1, x_2, x_3) = 0\}$, consequentemente,

$$C(\mathcal{Y}, P) \subseteq \{[x_0 : x_1 : x_2 : x_3] \in \mathbb{P}^3(K);\ G(x_1, x_2, x_3) = 0\}.$$

Para a inclusão reversa, considere $P_0 = [x_0 : x_1 : x_2 : x_3]$ tal que $G(x_1, x_2, x_3) = 0$. Se $x_0 = 0$, então $P_0 \in \mathcal{Y} = \Pi \cap \mathcal{X} \subseteq C(\mathcal{Y}, P)$. Se $x_0 \neq 0$, então

$$P_0 = [1 : x_1x_0^{-1} : x_2x_0^{-1} : x_2x_0^{-1}] \in l(P, [0 : x_1 : x_2 : x_3]) \subseteq C(\mathcal{Y}, P),$$

assim $\{[x_0 : x_1 : x_2 : x_3] \in \mathbb{P}^3(K);\ G(x_1, x_2, x_3) = 0\} \subseteq C(\mathcal{Y}, P)$. Portanto, $C(\mathcal{Y}, P)$ é uma hipersuperfície de grau d em $\mathbb{P}^3(K)$.

Teorema 3.6. *Seja $\mathcal{S} \subseteq \mathbb{P}^3(K)$ uma superfície de grau $d \geq 2$ definida sobre $\mathbb{F}_q$ e $P \in \mathcal{S}(\mathbb{F}_q)$. Então, um dos seguintes itens é válido:*

(a) $\mathcal{S}$ contém um cone sobre uma curva plana definida sobre $\mathbb{F}_q$, com centro em P.

(b) $|\{l \subseteq \mathbb{P}^3(K);\ l$ é uma reta tal que $P \in l \subseteq \mathcal{S}\}| \leq d(d-1)$.

Demonstração. Suponha que a condição (a) não seja satisfeita.

Seja $\Pi \subseteq \mathbb{P}^3(K)$ um plano definido sobre $\mathbb{F}_q$ que não passa pelo ponto P. Fazendo uma mudança linear no sistema de coordenada podemos assumir que $P = [1 : 0 : 0 : 0]$ e $\Pi = \mathbf{v}(X_0)$ (veja, exemplo 2.9). Suponha que $\mathcal{S} = \mathbf{v}(F)$, com $F \in \mathbb{F}_q[X_0, X_1, X_2, X_3]$ de grau d. Sendo F um polinômio homogêneo de grau d, podemos escrever

$$F(X_0, X_1, X_2, X_3) = c \cdot X_0^d + X_0^{d-1}F_1(X_1, X_2, X_3) + \cdots + F_d(X_1, X_2, X_3),$$

onde $F_i \in \mathbb{F}_q[X_1, X_2, X_3]$ é um polinômio homogêneo de grau i, com $i = 1, ..., d$. Como $P \in \mathcal{S}$, tem-se $0 = F(P) = F(1, 0, 0, 0) = c + F_1(0, 0, 0) + \cdots + F_d(0, 0, 0) = c$. Assim,

$$F(X_0, X_1, X_2, X_3) = X_0^{d-1}F_1(X_1, X_2, X_3) + \cdots + F_d(X_1, X_2, X_3).$$

Observe que $F_d \neq 0$, pois caso contrário teríamos $\Pi \subseteq \mathcal{X}$, contrariando o invariante de Koen Thas. Além disso, $(F_1, ..., F_{d-1}) \neq (0, ..., 0)$, de fato: Suponha que $F_1 = \cdots = F_{d-1} = 0$, assim $F = F_d$. Considere a curva plana $\mathbf{v}(X_0, F_d)$. Seja $Q = [0 : x_1 : x_2 : x_3] \in \mathbf{v}(X_0, F_d)$. Para todo $\alpha, \beta \in K$ vale

$$F(\alpha, \beta x_1, \beta x_2, \beta x_3) = F_d(\beta x_1, \beta x_2, \beta x_3) = \beta^d F_d(x_1, x_2, x_3) = 0,$$

ou seja, $\mathcal{S}$ contém o cone sobre a curva plana $\mathbf{v}(X_0, F_d)$ definida sobre $\mathbb{F}_q$, com centro em P, contrariando nossa hipótese inicial. Logo, $(F_1, ..., F_{d-1}) \neq (0, ..., 0)$. Temos também que $F_1, ..., F_d$ são coprimos. Com efeito, suponha que exista $G \in \mathbb{F}_q[X_1, X_2, X_3]$ homogêneo de grau d_G tal que $G|F_i$ para cada $i = 1, ..., d$, assim $F_i = G_i \cdot G$ para algum $G_i \in \mathbb{F}_q[X_1, X_2, X_3]$.

Considere a curva plana $\mathbf{v}(X_0, G)$. Seja $Q = [0 : x_1 : x_2 : x_3] \in \mathbf{v}(X_0, G)$. Para todo $\alpha, \beta \in K$ vale

$$\begin{aligned} F(\alpha, \beta x_1, \beta x_2, \beta x_3) &= \alpha^{d-1} F_1(\beta x_1, \beta x_2, \beta x_3) + \cdots + F_d(\beta x_1, \beta x_2, \beta x_3) \\ &= [\alpha^{d-1} G_1(\beta x_1, \beta x_2, \beta x_3) + \cdots G_d(\beta x_1, \beta x_2, \beta x_3)] G(\beta x_1, \beta x_2, \beta x_3) \\ &= [\alpha^{d-1} G_1(\beta x_1, \beta x_2, \beta x_3) + \cdots G_d(\beta x_1, \beta x_2, \beta x_3)] \beta^{d_G} G(x_1, x_2, x_3) \\ &= 0 \end{aligned}$$

isto é, $\mathcal{S}$ contém o cone sobre a curva plana $\mathbf{v}(X_0, G)$ definida sobre $\mathbb{F}_q$, com centro em P, contrariando nossa hipótese inicial. Logo, $F_1, ..., F_d$ são coprimos. Defina

$$\mathcal{L}^{\mathcal{S}}(P) := \{l \subseteq \mathbb{P}^3;\ l \text{ é uma reta tal que } P \in l \subseteq \mathcal{S}\}.$$

Observe que para cada reta l com $P \in l \subseteq \mathcal{S}$ tem-se $|l \cap \Pi| = 1$, pois $P \notin \Pi$. Defina

$$A = \left(\bigcup_{l \in \mathcal{L}^{\mathcal{S}}(P)} l \right) \cap \Pi.$$

Pela observação feita acima, existe uma bijeção natural entre $\mathcal{L}^{\mathcal{S}}(P) \longleftrightarrow A$. Desse modo, basta mostrar que $|A| \leq d(d-1)$. Afirmamos que $A = \mathbf{v}(F_1, ..., F_d, X_0)$. Com efeito, seja $Q = [0 : x_1 : x_2 : x_3] \in A$. Assim, a linha

$$l(P, Q) = \{[t : ux_0 : ux_1 : ux_2];\ t, u \in K \text{ não são ambos nulos}\}$$

que contém os pontos P e Q está contida em $\mathcal{S}$, logo $[t : x_1 : x_2 : x_3] \in \mathcal{S}$ para todo $t \in K$. Em particular, $F(t, x_1, x_2, x_3) = 0$ para todo $t \in K$. Como $F(T, x_1, x_2, x_3)$ é um polinômio na variável T com grau no máximo $d-1$, então $F_i(x_1, x_2, x_3) = 0$ para todo $i = 1, ..., d$. Segue daí que $A \subseteq \mathbf{v}(F_1, ..., F_d, X_0)$. Inversamente, seja $Q = [0, x_1, x_2, x_3] \in \mathbf{v}(F_1, ..., F_d, X_0)$. Claramente, $P \neq [0 : x_1 : x_2 : x_3] \in \Pi$ e a linha

$$l(P, Q) = \{[t : ux_0 : ux_1 : ux_2];\ t, u \in K \text{ não são ambos nulos}\} \in \mathcal{L}^{\mathcal{S}}(P),$$

consequentemente, $[0 : x_1 : x_2 : x_3] \in A$ e assim $\mathbf{v}(F_1, ..., F_d, X_0) \subseteq A$. Portanto,

$$A = \mathbf{v}(F_1, ..., F_d, X_0).$$

Considere $F_d = G_1 \cdots G_r$, com $r \geq 1$ e $G_j \in \mathbb{F}_q[X_1, X_2, X_3]$ irredutível. Como $F_1, ..., F_d$ são coprimos, para cada $i = 1, ..., r$ existe $1 \leq j_i \leq d-1$ tal que G_i e F_{j_i} são coprimos. Segue do Teorema de Bezout 2.6 que

$$|\mathbf{v}(X_0, G_i, F_{j_i})| \leq deg(G_i) deg(F_{j_i}) \leq deg(G_i)(d-1).$$

Segue daí que

$$\begin{aligned} |A| = |\mathbf{v}(X_0, F_1, ..., F_d)| &\leq \sum_{i=1}^{r} |\mathbf{v}(X_0, F_1, ..., F_{d-1}, G_i)| \\ &\leq \sum_{i=1}^{r} |\mathbf{v}(X_0, G_i, F_{j_i})| \\ &= \sum_{i=1}^{r} deg(G_i)(d-1) = d(d-1). \end{aligned}$$

Portanto, $|\{l \subseteq \mathbb{P}^3(K);\ l \text{ é uma linha tal que } P \in l \subseteq \mathcal{S}\}| \leq d(d-1)$.

■

Para fins deste trabalho, o teorema 3.6 foi provado para corpos finitos. Entretanto, o leitor deve ter observado que não utilizamos nenhuma propriedade adicional que um corpo finito possa ter, apenas utilizar a propriedade algébrica de ser um corpo. Assim, o teorema contínua válido se substituímos $\mathbb{F}_q$ por um corpo arbitrário k.

3.4.1 Número máximo de pontos $\mathbb{F}_q$-racionais

Por fim, nesta última seção, vamos provar a desigualdade 3.8. Começando com o caso $d = 2$ e alguns resultados necessários para o caso geral.

Teorema 3.7. *Seja $\mathcal{X}$ uma hipersuperfície quádrica não singular em $\mathbb{P}^4(K)$ sobre $\mathbb{F}_q$, então*

$$|\mathcal{X}(\mathbb{F}_q)| = q^3 + q^2 + q + 1.$$

Demonstração. Como toda quádrica não singular em $\mathbb{P}^4(\mathbb{F}_q)$ é projetivamente equivalente a $\mathcal{X}_0 = \mathbf{v}(X_0^2 + X_1X_2 + X_3X_4)$ (veja, exemplo 2.8), basta observar que

$$|\mathcal{X}_0(\mathbb{F}_q)| = q^3 + q^2 + q + 1.$$

Com efeito, considerando $P = [x_0 : x_1 : x_2 : x_3 : x_4] \in \mathcal{X}_0$, vamos dividir a prova em dois caso:

***Caso 1**: Considere $x_4 \neq 0$.* Neste caso, como estamos considerando pontos projetivos, podemos assumir $x_4 = 1$. Assim

$$x_3 = -(x_0^2 + x_1x_2).$$

Segue daí que $P = [x_0 : x_1 : x_2 : -(x_0^2 + x_1x_2) : 1]$ e assim temos q^3 pontos $\mathbb{F}_q$-racionais.

***Caso 2**: Considere $x_4 = 0$.* Assim temos $x_0^2 + x_1x_2 = 0$ e x_3 qualquer. Vamos considerar dois subcasos:

***Subcaso 1**: Considere $x_1 \neq 0$.* Neste caso, como estamos considerando pontos projetivos, podemos assumir $x_1 = 1$, assim $x_2 = -x_0^2$. Segue daí que $P = [x_0 : 1 : -x_0^2 : x_3]$ e assim temos q^2 pontos $\mathbb{F}_q$-racionais.

***Subcaso 2**: Considere $x_1 = 0$.* Assim $x_0^2 = 0$ e existe uma bijeção natural

$$[0 : 0 : x_2 : x_3 : 0] \in \mathcal{X}_0 \longleftrightarrow [x_2 : x_3] \in \mathbb{P}^1(K).$$

Segue dai que temos $q + 1$ pontos $\mathbb{F}_q$-racionais.

Portanto, $|\mathcal{X}_0(\mathbb{F}_q)| = q^3 + q^2 + q + 1$.

■

Para as próximas três proposições, considere $P \in \mathcal{X}(\mathbb{F}_q)$.

Proposição 3.4. $|\mathbb{T}_P(\mathcal{X})(\mathbb{F}_q)| = \theta_q(3)$.

Demonstração. Como P é um ponto não singular e $\mathcal{X}$ é uma hipersuperfície definida sobre $\mathbb{F}_q$, então $\mathbb{T}_P(\mathcal{X})$ é um hiperplano definido sobre $\mathbb{F}_q$. Segue daí que

$$|\mathbb{T}_P(\mathcal{X})(\mathbb{F}_q)| = \theta_q(3).$$

■

Proposição 3.5. *Se S é o conjunto das retas definidas sobre $\mathbb{F}_q$ que passam por P e não estão contidas em $\mathbb{T}_P(\mathcal{X})$, então $|S| = q^3$.*

Demonstração. Segue da proposição 3.4 que $|\mathbb{T}_P(\mathcal{X})(\mathbb{F}_q)| = \theta_q(3)$. Assim $|\mathbb{T}_P(\mathcal{X})^C(\mathbb{F})_q| = q^4$. Os elementos de S são da forma $l(P, Q)$ com $Q \in \mathbb{T}_P(\mathcal{X})^C(\mathbb{F}_q)$. Logo, temos q^4 retas, entretanto, cada reta foi contado q vezes. Portanto,

$$|S| = \frac{q^4}{q} = q^3.$$

■

Proposição 3.6. *Se U denota o conjunto das retas sobre $\mathbb{F}_q$ que passam por P e estão contidas em $\mathbb{T}_P(\mathcal{X})$, então*

$$|U| = q^2 + q + 1.$$

Demonstração. Os elementos de U são da forma $l(P,Q)$ com $Q \in \mathbb{T}_P(\mathcal{X})(\mathbb{F}_q)\backslash\{P\}$. Deste modo, temos $|\mathbb{T}_P(\mathcal{X})(\mathbb{F}_q)| - 1$ retas. Entretanto, cada reta foi contada q vezes, assim

$$|U| = \frac{q^3 + q^2 + q}{q} = q^2 + q + 1.$$

■

Lema 3.3. *Seja $P \in \mathcal{X}(\mathbb{F}_q)$, então $|\mathcal{X}(\mathbb{F}_q) \cap \mathbb{T}_P(\mathcal{X})^C| \leq (d-1)q^3$.*

Demonstração. Denotaremos por S o conjunto de todas as retas definidas sobre $\mathbb{F}_q$ que contêm o ponto P e não estão contidas em $\mathbb{T}_P(\mathcal{X})$. Afirmamos que

$$\mathbb{T}_P(\mathcal{X})^C(\mathbb{F}_q) = \bigsqcup_{l \in S} (l(\mathbb{F}_q)\backslash\{P\}).$$

Com efeito, dado $Q \in \mathbb{T}_P(\mathcal{X})^C(\mathbb{F}_q)$, tem-se $Q \neq P$ e $l(P,Q) \in S$. Assim

$$T_P(\mathcal{X})^C(\mathbb{F}_q) \subset \bigsqcup_{l \in S} (l(\mathbb{F}_q)\backslash\{P\}).$$

Seja $Q \in \bigsqcup_{l\in S}(l(\mathbb{F}_q)\backslash\{P\})$. Logo, existe $l \in S$ tal que $Q \in l(\mathbb{F}_q)\backslash\{P\}$. Como l não está contida em $\mathbb{T}_p(\mathcal{X})$ devemos ter $Q \in \mathbb{T}_P(\mathcal{X})^C$. Sendo Q um ponto $\mathbb{F}_q$-racional, tem-se $Q \in \mathbb{T}_P(\mathcal{X})^C(\mathbb{F}_q)$. Assim

$$\bigsqcup_{l \in S} (l(\mathbb{F}_q)\backslash\{P\}) \subset T_P(X)^C(\mathbb{F}_q).$$

Deste modo, tem-se

$$|\mathcal{X}(\mathbb{F}_q) \cap \mathbb{T}_P(\mathcal{X})^C| = \sum_{l \in S} |\mathcal{X}(\mathbb{F}_q) \cap (l\backslash\{P\})|$$

Para cada $l \in S$,tem-se $l \nsubseteq \mathcal{X}$, pois caso contrário teríamos $l \subset \mathbb{T}_P(\mathcal{X})$. Segue do teorema de Bezout 2.6 que $|\mathcal{X} \cap l| \leq d$, consequentemente,

$$|\mathcal{X} \cap (l\backslash\{P\})| \leq d - 1.$$

Pela proposição 3.5, temos $|S| = q^3$. Portanto,

$$|\mathcal{X}(\mathbb{F}_q) \cap \mathbb{T}_p(\mathcal{X})^C| = \sum_{l \in S} |\mathcal{X}(\mathbb{F}_q) \cap (l\backslash\{P\})| \leq (d-1)q^3.$$

■

Com o lema 3.3 é possível provar a conjectura no caso em que $\mathcal{L}_q(P,\mathcal{X}) = \emptyset$ para algum ponto $P \in \mathcal{X}(\mathbb{F}_q)$. Neste caso, a desigualdade é estrita:

Lema 3.4. *Seja $P \in \mathcal{X}(\mathbb{F}_q)$. Se $\mathcal{L}_q(P,\mathcal{X}) = \emptyset$, então*

$$|\mathcal{X}(\mathbb{F}_q)| < (d-1)q^3 + (d-1)q^2 + q + 1.$$

Demonstração. Segue do lema 3.3 que

$$|\mathcal{X}(\mathbb{F}_q)| = |\mathcal{X}(\mathbb{F}_q) \cap \mathbb{T}_P(\mathcal{X})| + |\mathcal{X}(\mathbb{F}_q) \cap \mathbb{T}_P(\mathcal{X})^C| \leq |\mathcal{X}(\mathbb{F}_q) \cap \mathbb{T}_P(\mathcal{X})| + (d-1)q^3.$$

Assim, basta mostrar que $|\mathcal{X}(\mathbb{F}_q) \cap \mathbb{T}_P(\mathcal{X})| < (d-1)q^2 + q + 1$. Como P é um ponto singular de $\mathcal{X} \cap \mathbb{T}_P(\mathcal{X})$ e $\mathcal{L}_q(P, \mathcal{X}) = \emptyset$ para cada reta l definida sobre $\mathbb{F}_q$ tal que $P \in l \subset \mathbb{T}_P(\mathcal{X})$, tem-se

$$|\mathcal{X} \cap (l \setminus \{P\})| \leq d - 2.$$

Pela proposição 3.6, existem $q^2 + q + 1$ retas sobre $\mathbb{F}_q$ em $\mathbb{T}_P(\mathcal{X})$ contendo o ponto P. Assim

$$\begin{aligned} |\mathcal{X}(\mathbb{F}_q) \cap \mathbb{T}_P(\mathcal{X})| &\leq 1 + (d-2)(q^2+q+1) \\ &= (d-2)q^2 + (d-2)q + d - 1 \\ &= ((d-1)q^2 + q + 1) - q^2 + (d-3)q + d - 2. \end{aligned}$$

Logo, basta mostrar que $-q^2 + (d-3)q + d - 2 < 0$: temos $d \leq q$, logo

$$\begin{aligned} (d-3)q \leq (q-3)q = q^2 - 3q \\ \Rightarrow (d-3)q + d - 2 < (d-3)q + 3q \leq q^2 \\ \Rightarrow -q^2 + (d-3)q + d - 2 < 0. \end{aligned}$$

■

Definição 3.5. Sejam $P \in \mathcal{X}(\mathbb{F}_q)$ e $l \in \mathcal{L}_q(P, \mathcal{X})$. Para cada $Q \in l(\mathbb{F}_q)$, defina

$$\Omega_l(Q) := \{\Pi \in \mathcal{B}(l);\ \mathcal{X} \cap \Pi = l \cup l_1 \cup \cdots \cup l_{d-1},\ l_i \in \mathcal{L}_q(Q, \mathcal{X})\}$$

e

$$\Omega(l) := \bigcup_{Q \in\ l(\mathbb{F}_q)} \Omega_l(Q).$$

Lema 3.5. *Seja $P \in \mathcal{X}(\mathbb{F}_q)$. Suponha que exista $l \in \mathcal{L}_q(P, \mathcal{X})$ tal que para todo ponto $Q \in l(\mathbb{F}_q)$ a superfície $\mathcal{X} \cap \mathbb{T}_Q(\mathcal{X})$ não contém um cone sobre uma curva plana definida em $\mathbb{F}_q$ com centro em Q. Então, para todo $Q \in l(\mathbb{F}_q)$, tem-se*

$$|\Omega_l(Q)| \leq d - 1.$$

Consequentemente, $|\Omega(l)| \leq (d-1)(q+1)$.

Demonstração. Sejam $Q \in l(\mathbb{F}_q)$ e $t_Q = |\Omega_l(Q)|$. Deste modo, existem t_Q planos, digamos $\Pi_1, ..., \Pi_{t_Q}$, cada um definido sobre $\mathbb{F}_q$ contendo $d-1$ retas diferentes de l definidas sobre $\mathbb{F}_q$ que passam por Q e estão contidas em $\mathcal{X}$. Assim

$$|\mathcal{L}_q(Q, X)| \geq (d-1)t_Q + 1.$$

Se $t_Q \geq d$, então $|\mathcal{L}_q(Q, X)| \geq (d-1)d + 1 > d(d-1)$, contrariando o teorema 3.6, pois, por hipótese, $\mathcal{X} \cap \mathbb{T}_Q(\mathcal{X})$ não contém um cone sobre uma curva plana definida em $\mathbb{F}_q$ com centro em Q. Logo,

$$|\Omega_l(Q)| = t_Q \leq d - 1.$$

Consequentemente, tem-se

$$|\Omega(l)| = \sum_{P \in\ l(\mathbb{F}_q)} |\Omega_l(P)| \leq (d-1)(q+1).$$

■

Observação 3.3. Se existir $l \in \mathcal{L}_q(P, \mathcal{X})$ tal que para todo $Q \in l(\mathbb{F}_q)$ a superfície $\mathcal{X} \cap \mathbb{T}_Q(\mathcal{X})$ não contém um cone sobre um curva plana definida sobre $\mathbb{F}_q$ com centro em Q, então, usando o teorema 3.6 e um argumento semelhante ao do lema 3.5, tem-se

$$|\mathcal{G}(l)| \leq d(q+1) - 1,$$

onde $\mathcal{G}(l) := \{\Pi \in \mathcal{B}(l);\ \mathcal{X} \cap \Pi$ *é a união de* d *retas definidas sobre* $\mathbb{F}_q\}$. Além disso, se $d = 3$ e $\Pi \in \mathcal{B}(l) \backslash \mathcal{G}(l)$, então identificando $\Pi \simeq \mathbb{P}^2(K)$ de modo que a reta l sejam os pontos no infinito tem-se que $\mathcal{X} \cap (\Pi \backslash l)$ é uma curva afim de grau 2 definida sobre $\mathbb{F}_q$ que não contém uma reta definida sobre $\mathbb{F}_q$, pois, caso contrário, $\mathcal{X} \cap \Pi$ seria a reunião de três retas definidas sobre $\mathbb{F}_q$. Segue do teorema 3.3 que $|\mathcal{X}(\mathbb{F}_q) \cap (\Pi \backslash l)| \leq q + 1$.

Lema 3.6. *Para cada* $\Pi \in \mathcal{B}(l)$, *tem-se*

$$|\mathcal{X}(\mathbb{F}_q) \cap (\Pi \backslash l)| = (d-1)q \quad \textit{se} \quad \Pi \in \Omega(l)$$

$$e$$

$$|\mathcal{X}(\mathbb{F}_q) \cap (\Pi \backslash l)| \leq (d-1)q - (d-2) \quad \textit{se} \quad \Pi \in \mathcal{B}(l) \backslash \Omega(l).$$

Demonstração. Seja $\Pi \in \Omega(l)$. Assim, existe $Q \in l(\mathbb{F}_q)$ tal que

$$\mathcal{X} \cap \Pi = l \cup l_1 \cup \cdots \cup l_{d-1},$$

onde cada $l_i \in \mathcal{L}_q(Q, \mathcal{X})$. Claramente, tem-se

$$|\mathcal{X}(\mathbb{F}_q) \cap \Pi| = dq + 1,$$

consequentemente, $|\mathcal{X}(\mathbb{F}_q) \cap \Pi \backslash l| = |\mathcal{X}(\mathbb{F}_q) \cap \Pi| - |l(\mathbb{F}_q)| = dq + 1 - q - 1 = (d-1)q$.

Para a segunda afirmação, seja $\Pi \in \mathcal{B}(l) \backslash \Omega(l)$. Então $\mathcal{X} \cap \Pi$ não se escreve como reunião de d retas com um ponto em comum. Segue da segunda afirmação do teorema de Serre 3.2 que $|\mathcal{X}(\mathbb{F}_q) \cap \Pi| < dq + 1$. Além disso, $\mathcal{X} \cap (\Pi \backslash l)$ é uma curva afim de grau $d-1$ com

$$|\mathcal{X}(\mathbb{F}_q) \cap (\Pi \backslash l)| = |\mathcal{X}(\mathbb{F}_q) \cap \Pi| - |l(\mathbb{F}_q)| < dq + 1 - q - 1 = (d-1)q$$

Como $d - 1 \leq q - 1$, segue do teorema 1.6 que $|\mathcal{X}(\mathbb{F}_q) \cap (\Pi \backslash l)| \leq (d-1)q - (d-2)$.

■

Teorema 3.8. (Datta) *Seja* d *um natural, com* $2 \leq d \leq q$. *Seja* $\mathcal{X} \subset \mathbb{P}^4$ *uma hipersuperfície não singular de grau* d *sobre* $\mathbb{F}_q$. *Se* $(d, q) \neq (4, 4)$, *então*

$$|\mathcal{X}(\mathbb{F}_q)| \leq (d-1)q^3 + (d-1)q^2 + q + 1.$$

Além disso, o limite é atingido por uma hipersuperfície $\mathcal{X}$ *de grau* d *se existe um ponto* $P \in \mathcal{X}(\mathbb{F}_q)$ *tal que* $\mathcal{X} \cap \mathbb{T}_P(\mathcal{X})$ *é um cone com centro em* P *sobre uma curva plana* $\mathcal{C}$ *de grau* d *definida sobre* $\mathbb{F}_q$ *que não contém uma linha definida sobre* $\mathbb{F}_q$ *e* $|\mathcal{C}(\mathbb{F}_q)| = (d-1)q + 1$.

Demonstração. O caso $d = 2$ segue do teorema 3.7. Suponha $d \geq 3$. Se $\mathcal{X}(\mathbb{F}_q) = \emptyset$ não temos nada para fazer. Escolha $P \in \mathcal{X}(\mathbb{F}_q)$. Se $\mathcal{L}_q(P, \mathcal{X}) = \emptyset$, então o resultado segue do lema 3.4. Logo, podemos assumir que $\mathcal{L}_q(P, \mathcal{X}) \neq \emptyset$. Seja $l \in \mathcal{L}_q(P, \mathcal{X})$. Vamos dividir a prova em dois casos:

Caso 1*: suponha que exista* $Q \in l(\mathbb{F}_q)$ *tal que* $\mathcal{X} \cap \mathbb{T}_Q(\mathcal{X})$ *contém um cone sobre uma curva plana* $\mathcal{C}$ *definida sobre* $\mathbb{F}_q$ *com centro em* Q. Seja Π um plano definido sobre $\mathbb{F}_q$ tal que $\mathcal{C} \subset \Pi$. Seja $d_1 = deg(\mathcal{C})$. Primeiramente, observe que $\mathcal{C}$ não contém uma reta definida sobre $\mathbb{F}_q$, pois, caso contrário, $\mathcal{X} \cap \mathbb{T}_Q(\mathcal{X})$ conteria um plano definido sobre $\mathbb{F}_q$, contrariando o invariante de

Koen Thas do teorema 3.5. Como $d_1 \leq d$ e $(d,q) \neq (4,4)$, então $(d_1,q) \neq (4,4)$. Segue do teorema 3.3 que $|\mathcal{C}(\mathbb{F}_q)| \leq (d_1-1)q+1$. Seja $\mathcal{C}^*$ o cone sobre a curva $\mathcal{C}$ com centro em Q. Como cada reta que constitui o cone tem $q+1$ pontos $\mathbb{F}_q$-racional e apenas o ponto Q em comum, assim

$$|\mathcal{C}^*(\mathbb{F}_q)| \leq ((d_1-d)q+1)q+1 = (d_1-d)q^2+q+1.$$

Segue da proposição 3.1 e observação 3.2 que: se $d_1 = d$ então $\mathcal{X} \cap \mathbb{T}_Q(\mathcal{X}) = \mathcal{C}^*$. Deste modo, temos $|\mathcal{X}(\mathbb{F}_q) \cap \mathbb{T}_Q(\mathcal{X})| \leq (d-1)q^2+q+1$. Segue do lema 3.3 que

$$\begin{aligned} |\mathcal{X}(\mathbb{F}_q)| &\leq |\mathcal{X}(\mathbb{F}_q) \cap \mathbb{T}_Q(\mathcal{X})| + |\mathcal{X}(\mathbb{F}_q) \cap \mathbb{T}_Q(\mathcal{X})^C| \\ &\leq (d-1)q^3+(d-1)q^2+q+1. \end{aligned}$$

Se $d_1 < d$, existe uma superfície Z de grau no máximo $d-d_1$ tal que $\mathcal{X} \cap \mathbb{T}_Q(\mathcal{X}) = \mathcal{C}^* \cup Z$. Observe que Z não contém um plano definido sobre $\mathbb{F}_q$, pois, caso contrário, $\mathcal{X} \cap \mathbb{T}_Q(\mathcal{X})$ também conteria, o que contraria o invariante de Koen Thas do teorema 3.5. Pelo teorema 3.4 temos

$$|Z(\mathbb{F}_q)| \leq (d-d_1-1)q^2+(d-d_1)q+1.$$

Segue daí que

$$\begin{aligned} |\mathcal{X}(\mathbb{F}_q) \cap \mathbb{T}_Q(\mathcal{X})| &\leq |\mathcal{C}^*| + |Z| \\ &\leq (d_1-1)q^2+q+1+(d-d_1-1)q^2+(d-d_1)q+1 \\ &= (d-1)q^2+q+1+(-q^2+(d-d_1)q+1). \end{aligned}$$

Como $d_1 \geq 1$, tem-se $d-d_1 \leq q-1$, assim

$$(d-d_1)q+1 < (d-d_1)q+q \leq q^2$$

$$\Rightarrow -q^2+(d-d_1)q+1 < 0.$$

Deste modo, vale

$$|\mathcal{X}(\mathbb{F}_q) \cap \mathbb{T}_Q(\mathcal{X})| < (d-1)q^2+q+1.$$

Assim, segue do lema 3.3 que

$$\begin{aligned} |\mathcal{X}(\mathbb{F}_q)| &\leq |\mathcal{X}(\mathbb{F}_q) \cap \mathbb{T}_Q(\mathcal{X})| + |\mathcal{X}(\mathbb{F}_q) \cap \mathbb{T}_Q(\mathcal{X})^C| \\ &< (d-1)q^3+(d-1)q^2+q+1. \end{aligned}$$

Caso 2*: para cada $Q \in l(\mathbb{F}_q)$ a superfície correspondente $\mathcal{X} \cap \mathbb{T}_Q(\mathcal{X})$ não contém um cone sobre uma curva plana definida sobre $\mathbb{F}_q$ com centro em Q.* Primeiramente, considere o caso $(d,q) \neq (3,3)$. Seja $r = |\mathcal{B}(l) \backslash \Omega(l)|$. Segue do lema 3.5 que $r \geq q^2+q+1-(d-1)(q+1)$. Pelo lema 3.6 temos

$$\begin{aligned} |\mathcal{X}(\mathbb{F}_q)| &= |l(\mathbb{F}_q)| + \sum_{\Pi \in \mathcal{B}(l)} |\mathcal{X}(\mathbb{F}_q) \cap (\Pi \backslash l)| \\ &= |l(\mathbb{F}_q)| + \sum_{\Pi \in \Omega(l)} |\mathcal{X}(\mathbb{F}_q) \cap (\Pi \backslash l)| + \sum_{\Pi \in \mathcal{B}(l) \backslash \Omega(l)} |\mathcal{X}(\mathbb{F}_q) \cap (\Pi \backslash l)| \\ &\leq q+1+(q^2+q+1-r)(d-1)q + r((d-1)q-(d-2)) \\ &= (d-1)q^3+(d-1)q^2+q+1+((d-1)q-r(d-2)). \end{aligned}$$

Assim, basta mostrar que $r(d-2)+(1-d)q > 0$.

Subcaso 1: Se $d \leq q-1$, então

$$(1-d)(q+1) \geq (2-q)(q+1) = -(q^2-q-2).$$

Deste modo, tem-se

$$r \geq q^2+q+1+(1-d)(q+1) \geq q^2+q+1-(q^2-q-2) = 2q+3.$$

Logo, vale

$$r(d-2)+(d-1)q \geq (2q+3)(d-2)+(d-1)q > 0.$$

Subcaso 2: Se $d=q$, então $(1-d)(1+q) = 1-q^2$. Assim

$$r \geq q^2+q+1+(1-d)(q+1) = q+2.$$

Como $q=d\geq 3$, $(d,q)\neq(3,3)$ e $(d,q)\neq(4,4)$, então

$$r(d-2)+(1-d)q \geq (d-2)(q+2)+(1-d)q = q^2-4-q^2+q = q-4 > 0.$$

Considere agora $(d,q)=(3,3)$. Seja $r=|\mathcal{B}(l)\backslash\Omega(l)|$ e $s=|\mathcal{B}(l)\backslash\mathcal{G}(l)|$ (veja, lema 3.3). Deste modo, $s \geq q^2+q+1-d(q+1)+1 = q^2+(q+1)(1-d)+1$. Assim, quando $(d,q)=(3,3)$ temos $r\geq 5$ e $s\geq 2$. Observe que $\Omega(l)\subset\mathcal{G}(l)$, consequentemente,

$$\mathcal{B}(l) = \Omega(l) \sqcup (\mathcal{G}(l)\backslash\Omega(l)) \sqcup (\mathcal{B}(l)\backslash\mathcal{G}(l))$$

Considere $A=\Omega(l), B=(\mathcal{G}(l)\backslash\Omega(l))$ e $C=(\mathcal{B}(l)\backslash\mathcal{G}(l))$. Deste modo, tem-se

$$\begin{aligned}
|\mathcal{X}(\mathbb{F}_q)| &= |l(\mathbb{F}_q)| + \sum_{\Pi\in\mathcal{B}(l)} |\mathcal{X}(\mathbb{F}_q)\cap(\Pi\backslash l)| \\
&= |l(\mathbb{F}_q)| + \sum_{\Pi\in A} |\mathcal{X}(\mathbb{F}_q)\cap(\Pi\backslash l)| + \sum_{\Pi\in B} |\mathcal{X}(\mathbb{F}_q)\cap(\Pi\backslash l)| + \sum_{\Pi\in C} |\mathcal{X}(\mathbb{F}_q)\cap(\Pi\backslash l)| \\
&\leq q+1+(q^2+q+1-r)2q+(r-s)(2q-1)+s(q+1) \\
&= 2q^3+2q^2+q+1+(2q(1-r)+(r-s)(2q-1)+s(q+1)).
\end{aligned}$$

Assim, basta mostrar que $(2q(1-r)+(r-s)(2q-1)+s(q+1)) < 0$. Com efeito, como $q=3$, $r\geq 5$ e $s\geq 2$, temos

$$(2q(1-r)+(r-s)(2q-1)+s(q+1)) = 6-(r+s) < 0.$$

■

Sabemos, pelo teorema 3.7, que toda quádrica não singular atinge o limite do teorema 3.8. Além disso, ele também é alcançado por algumas hipersuperfícies hermitianas:

Exemplo 3.7. Considere a hipersuperfície Hermitiana

$$\mathcal{H} = \mathbf{v}(X_0^{q+1}+X_1^{q+1}+X_2^{q+1}+X_3^{q+1}+X_4^{q+1})$$

em $\mathbb{P}^4(K)$ definida sobre $\mathbb{F}_{q^2}$. Pelo teorema 2.3, temos

$$|\mathcal{H}(\mathbb{F}_{q^2})| = \frac{(q^5+1)(q^4-1)}{q^2-1} = (q^5+1)(q^2+1) = q(q^6)+q(q^4)+q^2+1,$$

isto é, a hipersuperfície $\mathcal{H}$ atinge o limite dado pelo teorema 3.8.

Para finalizar o trabalho, vejamos uma simples comparação entre as cotas superiores quando $d\leq q$. Defina $\mathfrak{B}(d) := (d-1)q^3+(d-1)q^2+q+1$ (teorema 3.8), $\mathfrak{L}(d,4) := dq^3+q^2+q+1$ (teorema 3.2) e $\mathcal{E}(d,4) := (d-1)q^3+dq^2+q+1$ (teorema 3.4). Claramente, tem-se

$$\mathfrak{B}(d) < \mathcal{E}(d,4) < \mathfrak{L}(d,4).$$

Referências Bibliográficas

[1] COX, David; LITTLE, John; OSHEA, Donal. **Ideals, varieties, and algorithms: an introduction to computational algebraic geometry and commutative algebra**. Springer Science and Business Media, 2015.

[2] BOSE, Raj Chandra; CHAKRAVARTI, I. M. **Hermitian varietis in a finite projective space PG**(N, q^2). Can. J. Math. 18 (1966) 1161–1182.
https://doi.org/10.4153/CJM-1966-116-0

[3] SERRE, Jean-Pierre. **Lettre à M. Tsfasman**, Journées Arithmétiques, 1989 (Luminy 1990) Astérisque 198—200 (1991) 1, Astérisque 351—353 (1992).
Local: http://www.numdam.org/item/AST_1991__198-199-200__351_0

[4] SZIKLAI, Peter. **A bound on the number of points of a plane curve**, Finite Fields Appl. 14 (2008) 41–43.
https://doi.org/10.1016/j.ffa.2007.09.004

[5] HOMMA, Masaaki. KIM, Seon Jeon, **Around Sziklai's conjecture on the number of points of a plane curve over a finite field**, Finite Fields Appl. 15 (2009) 468–474.
https://doi.org/10.1016/j.ffa.2009.02.008

[6] HOMMA, Masaaki. KIM, Seon Jeon, **Sziklai's conjecture on the number of points of a plane curve over a finite field II**, in: G. McGuire, G.L. Mullen, D. Panario, I.E. Shparlinski (Eds.), Finite Fields: Theory and Applications, in: Contemp. Math., vol. 518, AMS, Providence, 2010, pp. 225–234.
https://doi.org/10.1090/conm/518/10208

[7] HOMMA, Masaaki. KIM, Seon Jeon, **Sziklai's conjecture on the number of points of a plane curve over a finite field III**, Finite Fields Appl. 16 (2010) 315–319.
https://doi.org/10.1016/j.ffa.2010.05.001

[8] HOMMA, Masaaki. KIM, Seon Jeong. **An elementary bound for the number of points of a hypersurface over a finite field**, Finite Fields Appl. 20 (2013) 76–83.
https://doi.org/10.1016/j.ffa.2012.11.002

[9] DATTA, Mrinmoy. **Maximum number of $\mathbb{F}_q$ - rational points on nonsingular threefolds in $\mathbb{P}^4$**. Finite Fields and Their Applications 59 (2019) 86–96.
https://doi.org/10.1016/j.ffa.2019.05.006

[10] LIDL, Rudolf; NIEDERREITER, Harald. **Introduction to finite fields and their applications**. Cambridge university press, 1986.

[11] MUNKRES, James R. **Topology: a First Course**. Prentice-Hall, 1974.

[12] GEIL, Olav. **On the second weight of generalized Reed-Muller codes**. Designs, Codes and Cryptography. 48, 323–330 (2008). https://doi.org/10.1007/s10623-008-9211-9

[13] HIRSCHFELD, James. **Projective geometries over finite fields**. Oxford University Press, 1980.

[14] SHAFAREVICH, Igor R. REID, Miles. **Basic algebraic geometry 1: Varieties in Projective Space**. Berlin: Springer-verlag, 2013.

[15] HIRSCHFELD, James; KORCHMÁROS, Gábor; TORRES, Fernando. **Algebraic Curves over a Finite Field**, Princeton University Press, 2008.

[16] VOLOCH, José Felipe. **Surfaces in $\mathbb{P}^3$ over finite fields**. Topics in algebraic and noncommutative geometry (Lumimy/Annapolis, MD, 2001), 219–226, Contemp. Math. 324, Amer. Math. Soc., Providence, RI, 2003.

[17] SWINNERTON–DYER, PETER. **Cubic surfaces over finite fields**. In: Mathematical Proceedings of the Cambridge Philosophical Society. Cambridge University Press, 2010. p. 385-388.

https://doi.org/10.1017/S0305004110000320