Universidade Estadual de Campinas

INSTITUTO DE MATEMÁTICA, ESTATÍSTICA E COMPUTAÇÃO CIENTÍFICA

Departamento de Matemática

Sobre o Número de Soluções de Equações Polinomiais em Corpos Finitos

Marcelo Oliveira Veloso [†]

Mestrado em Matemática - Campinas - SP

Orientador: Prof. Dr. Paulo Roberto Brumatti

[†]Este trabalho contou com apoio financeiro do CNPq.

FICHA CATALOGRÁFICA ELABORADA PELA BIBLIOTECA DO IMECC DA UNICAMP

Veloso, Marcelo Oliveira

V546s Sobre o número de soluções de equações polinomiais em corpos finitos / Marcelo Oliveira Veloso -- Campinas, [S.P. :s.n.], 2005.

Orientador : Paulo Roberto Brumatti

Dissertação (mestrado) - Universidade Estadual de Campinas, Instituto de Matemática, Estatística e Computação Científica.

1. Álgebra comutativa. 2. Geometria algébrica. 3. Formas quadráticas. I. Brumatti, Paulo Roberto. II. Universidade Estadual de Campinas. Instituto de Matemática, Estatística e Computação Científica. III. Título.

Título em inglês: On the number of solutions of polynomial equations on finite fields.

Palavras-chave em inglês (keywords): 1. Commutative algebra. 2. Algebraic geometry. 3. Quadratic forms.

Área de concentração: Álgebra

Titulação: Mestre em matemática

Banca examinadora: Prof. Dr. Paulo Roberto Brumatti (UNICAMP)
Prof. Dr. Cícero Fernandes de Carvalho (UFU)
Prof. Dr. Antônio José Engler (UNICAMP)

Data da defesa: 16/02/2005

Sobre o Número de Pontos de uma Curva Algébrica em Corpos finitos

Este exemplar corresponde à redação final da dissertação devidamente corrigida e defendida por **Marcelo Oliveira Veloso** e aprovada pela comissão julgadora.

Campinas, 16 de Fevereiro de 2005.

Prof. Dr. Paulo Roberto Brumatti

Banca examinadora:

Prof. Dr. Paulo Roberto Brumatti.

Prof. Dr. Cícero Fernandes de Carvalho.

Prof. Dr. Antônio José Engler.

Dissertação apresentada ao Instituto de Matemática, Estatística e Computação Científica, UNICAMP como requisito parcial para obtenção do título de **Mestre em Matemática**.

O Homem do São Francisco

(Letra & Música: Jorge Silva)

Quem lançar seu olhar sobre as águas do meu São Francisco
Bem verá sobre ondas tranqüilas um barco a vagar
Levar um homem que tem sua pele bastante curtida
Pelo sol e também pelo vento daquele lugar
...
Navegante, o vagar pelas águas te deu braços fortes
Uma crença, mil lendas
E voz para sempre cantar
Todas cores brilhantes do rio com o sol ao nascente
Ou a triste lembrança que ás vezes te nubla o olhar

Quantas vezes, em noites bem claras, do alto as estrelas
Contemplaram o homem fazendo da praia seu leito?
Quantas vezes os pingos da chuva cobriram seu rosto
Ocultando o pranto nascido de coisas do peito

Certa vez, o cansaço envolveu sua mente e seu corpo
Resolveu esquecer sua vida de navegador
Mas o sangue que corre nas veias do bom pescador
Não achou ambiente igual e o homem voltou

Navegante...

À memória da minha avó
Nicinha, do meu tio
Zé de Iaiá, e do meu
primo-sobrinho Lucas.

AGRADECIMENTOS

- A Jeová, Deus;
- A minha esposa Gilcélia;
- A minha mãe Lindaura;
- Ao Prof. Brumatti e aos professores da Graduação Helder Cândido e Cristina Marques;
- Aos amigos que tanto contribuiram nesta caminhada Dadam, Rinaldo, Marcelo, Evandro, Fábio, Júlio César; a todos membros do Departamento de Futebol do IMECC e demais companheiros de curso;
- Aos amigos da graduação Fábio, Jean, Cris, Alexandre, Aninha, Gil, Leandro e Ivanildo;
- Aos tios Esdras, Lika, Nicinha, Carminha, Osvaldo, Hélio, Waltércio, Chica, Vilmar, Cremilda, Manoelina e Ronildo.
- Aos irmãos Rodrigo, Ricardo, Fabiana, Jose e Dinha;
- Aos primos Douglas, Dilson, Cris, Viviane, Reinaldinho, Lu, Leninha, Juninho e sobrinhos Magno, Alisson, Layla e Rodriguinho;
- e não podia faltar minha querida avó Teodolina.

RESUMO

O objetivo principal deste trabalho é o estudo do número de soluções de equações polinomiais definidas sobre corpos finitos. Para isto utilizamos resultados básicos sobre a soma de Caracteres e resultados sobre o número de soluções de uma Forma Quadrática. Na nossa abordagem procuramos utilizar técnicas bem elementares, apesar disto implicar num número maior de cálculos. Contudo este metodo permitiu estudar e determinar fórmulas para o número de soluções de determinadas equações polinomiais muito estudadas, sem a necessidade de ferramentas mais elaboradas.

Dentre as aplicações das fórmulas obtidas, temos alguns exemplos de curvas algébricas planas cujo número de pontos racionais atingem a cota de Weil, ou seja, curvas maximais que são de grande interesse em teoria dos códigos. Também conseguimos exemplos de variedades projetivas sobre corpos finitos cujo número de pontos atingem a cota de Weil-Deligne.

ABSTRACT

The main objective of this work is to study the number of solutions of polynomial equations over finite fields. For that we used basic results on Character sums and on the number of solutions of a Quadratic Form. This approach uses elementary techniques even considering the increasing on computations. Therefore this method allowed us to study and determine formulae for the number of solutions of certain polynomial equations well known, without the need of more sophisticated tools.

Among the applications of the obtained formulae, we have some examples of plane algebraic curves which number of rational points achieve the Weil bound, that is, maximal curves which are of great interest in code theory. In addition, other examples were obtained of projective manifolds over finite fields which number of points achieve the Weil-Deligne bound.

SUMÁRIO

Introdução

Estudar as soluções de equações polinomiais (também conhecidas como algébricas) é, sem dúvida, um questão de grande relevância na matemática. Problemas famosos consistem em analisar as soluções de uma equação algébrica. Como

- Verificar que o corpo dos números complexos é algebricamente fechado. Este resultado foi provado por F. Gauss.
- O chamado "Último Teorema de Fermat" que afirma que a equação

  $$X^n + Y^n = Z^n,$$

  com $n \geq 3$, não possui solução $(x, y, z) \in \mathbb{Z}^3$, tal que $xyz \neq 0$. Resultado provado recentemente por A. Wiles.
- A caracterização dos polinômios $f(x)$ em $\mathbb{Q}[x]$ que são solúveis por radicais. Resultado devido a E. Galois.
- Uma aplicação bem mais recente de tal teoria é o fato de que o conjunto solução de uma equação polinomial em duas variáveis (curva algébrica plana) pode gerar bons códigos corretores de erros, os chamados códigos geométricos de Goppa. Veja [9].

Neste texto estamos interessados no número de soluções, em $\mathbb{F}_{q^k}$, das equações polinomiais $f(x_1, \ldots, x_n) = 0$, com $f(x_1, \ldots, x_n) \in \mathbb{F}_{q^k}[x_1, \ldots, x_n]$, onde $\mathbb{F}_{q^k}$ é o corpo finito com q^k elementos. Uma solução desta equação algébrica é uma n-upla $(a_1, \ldots, a_n)$ em $\mathbb{F}_{q^k}^n$ que satisfaz

$f(a_1, \ldots, a_n) = 0$. Em certas condições é possível determinar o número de soluções de certas equações algébricas. Por exemplo: a equação polinômial (veja Exemplo 2.2)

$$y^3 - y = x^4$$

possui 3.486.430.107 soluções sobre $\mathbb{F}_{3^{20}}$.

Nosso principal objetivo neste texto é apresentar resultados que determinem o número de soluções de uma equação polinômial e suas conseqüências. Uma destas conseqüências é o exemplo acima que decorrre diretamente do Corolário 2.5. São resultados já conhecidos, e para determiná-los procuramos utilizar técnicas mais elementares, apesar de serem mais intricadas.

No primeiro capítulo é feito uma pequena introdução à teoria dos caracteres e à teoria das formas quadráticas. Obtemos alguns resultados clássicos sobre a soma de caracteres sobre um corpo finito, equivalência de formas quadráticas sobre um corpo finito e encerramos o capítulo com um resultado bem conhecido, Teorema 1.18, sobre o número de soluções de uma forma quadrática. A referência principal é [3].

Ao longo do segundo capítulo temos exemplos de algumas curvas maximais, isto é, curvas que atingem a cota de Weil que é o número máximo de soluções possíveis. Um destes exemplos é a bastante conhecida curva de Hermite (Exemplo 2.1), os outros são obtidos a partir do resultado que determina o número de soluções da equação $y^q - y = ax^s + b$ sobre um corpo finito. Sendo este o principal resultado exposto neste texto, Teorema 2.3, devido a J. Wolfmann [5].

Começamos o terceiro capítulo com alguns resultados, bem conhecidos, sobre o número de soluções de equações diagonais com expoente constante sobre corpos finitos, ou seja, equações da forma $a_1x_1^d + \cdots + a_nx^d = b$ onde b e os a_i estão em $\mathbb{F}_{q^k}$, e d é um inteiro positivo. Depois determinamos o número destas soluções em determinados casos, Teorema 3.4, resultado devido a J. Wolfmann [6], donde é possível obter exemplos de variedades projetivas que atingem a cota de Weil-Deligne.

Finalizamos o texto com dois apêndices. O primeiro sobre os corpos finitos onde listamos suas principais propriedades e resultados usados ao longo deste texto. O segundo fala sobre curvas algébricas sobre corpos finitos onde fornecemos definições e resultados básicos sobre curvas e variedades utilizados ao longo deste texto.

CAPÍTULO 1

Conceitos Fundamentais

Neste capítulo inicial faremos uma breve introdução de alguns conceitos e resultados sobre Caracteres e Formas Quadráticas. Para um estudo inicial desses tópicos recomendamos as referências [10] e [4], respectivamente. Contudo nossa principal referência, para essas notas, é o livro-texto [3].

Durante todo o texto, $\mathbb{F}_{q^k}$ denota o corpo finito com q^k elementos, onde q é uma potência de um primo p e k um inteiro positivo.

Encerramos o capítulo com a apresentação de alguns resultados fundamentais a respeito do número de soluções, em $\mathbb{F}_{q^n}$, da equação $f(x_1, \ldots, x_n) = b$ onde $b \in \mathbb{F}_q$ e f é uma forma quadrática em $\mathbb{F}_q[x_1, \ldots, x_n]$.

1.1 Caracteres

Nesta seção vamos estudar alguns resultados sobre caracteres, em particular estamos interessados em resultados referentes a somas de alguns caracteres sobre $\mathbb{F}_q$.

Sejam G um grupo abeliano multiplicativo com ordem, $|G|$, finita e $\mathbb{C}$ corpo dos números complexos.

Definição 1.1 (Caractere de G)

Todo homomorfismo multiplicativo $\chi : G \to \mathbb{C}^*$ é chamado de caractere de G. □

Observe que $\chi(1_G) = \chi(1_G 1_G) = \chi(1_G)\chi(1_G)$, logo $\chi(1_G) = 1$, onde 1 é a unidade de $\mathbb{C}$. Portanto pelo Teorema de Lagrange para grupos finitos $\chi(g)^{|G|} = \chi(g^{|G|}) = \chi(1_G) = 1$, para todo $g \in G$. Assim $\chi(g)$ é uma $|G|$-ésima raíz da unidade, para todo $g \in G$. Logo a imagem, $\chi(G)$, de um carectere, χ, de G é um subgrupo do subgrupo multiplicativo dos números complexos com norma um, o qual denotaremos por U. Na verdade $\chi(G)$ é subgrupo do subgrupo cíclico das $|G|$-ésimas raizes da unidade e portanto cíclico.

Veja também que $\chi(g)\chi(g^{-1}) = 1$, logo $\chi(g^{-1}) = \chi(g)^{-1} = \overline{\chi(g)}$, para todo $g \in G$, onde a barra denota o complexo conjugado. Observe ainda que o conjunto dos caracteres de G, que vamos denotar por $\hat{G}$, é um grupo multiplicativo com a operação multiplicação ponto a ponto. Pela observação acima tem-se que a ordem de $\hat{G}$ é finita.

EXEMPLO 1.1 *Seja G um grupo cíclico de ordem n. Tome g um gerador deste grupo, fixe um inteiro $j \in [0, n-1]$ e defina*

$$\chi_j(g^k) = e^{\frac{2\pi jki}{n}}$$

Não é difícil ver que χ_j é um caractere de G.

Agora suponha que χ é um caractere de G. Então $\chi(g)$ deve ser uma raíz n-ésima da unidade e portanto $\chi(g) = e^{\frac{2\pi ji}{n}}$ para algun inteiro $j \in [0, n-1]$. Portanto temos que $\chi_j(g^k) = e^{\frac{2\pi jki}{n}}$, isto é, $\hat{G} = \{\chi_0, \chi_1, \ldots, \chi_{n-1}\}$. ♢

EXEMPLO 1.2 *Defina $\chi(g) = 1$ para todo $g \in G$. Este é chamado de caractere trivial de G.*

♢

Definição 1.2 (Caracteres Multiplicativos)

Seja $G = \mathbb{F}_q^*$. Os caracteres de G são chamados de caracteres multiplicativos de $\mathbb{F}_q^*$.

□

EXEMPLO 1.3 *Defina $\eta : \mathbb{F}_q^* \to U$ como $\eta(a) = 1$ se a é um quadrado em $\mathbb{F}_q^*$, e $\eta(a) = -1$ caso contrário. Claramente η é um caractere multiplicativo sobre $\mathbb{F}_q$.*

♢

Definição 1.3 (Caractere Quadrático)

O caractere multiplicativo do Exemplo 1.3 *é chamado de caractere quadrático de $\mathbb{F}_q$.*

□

Veja que todo caractere multiplicativo θ está definido somente para os elementos de $\mathbb{F}_q^*$. Iremos convencionar que a extensão de θ para $\mathbb{F}_q$ será dada por $\theta(0) = 1$ se θ for trivial e $\theta(0) = 0$ caso contrário. Com esta convenção quando referirmos ao caractere multiplicativo estaremos fazendo referência a sua extensão. Apresentamos, a seguir, dois resultados sobre caracteres multiplicativos:

Lema 1.1 *Seja θ um caracter multiplicativo. Então*

$$\sum_{c\in\mathbb{F}_q} \theta(c) = \begin{cases} q \text{ se } \theta \text{ é trivial} \\ 0 \text{ se } \theta \text{ é não trivial.} \end{cases}$$

Demonstração:
Se θ é trivial o resultado é imediato. Caso θ seja não trivial existe $b \in \mathbb{F}_q^*$ tal que $\theta(b) \neq 1$. Logo

$$\theta(b)\sum_{c\in\mathbb{F}_q^*} \theta(c) = \sum_{c\in\mathbb{F}_q^*} \theta(bc) = \sum_{c\in\mathbb{F}_q^*} \theta(c),$$

visto que bc percorre todo $\mathbb{F}_q^*$ quando c percorre $\mathbb{F}_q^*$. Donde temos

$$(\theta(b) - 1)(\sum_{c\in\mathbb{F}_q^*} \theta(c)) = 0$$

e então $\sum_{c\in\mathbb{F}_q^*} \theta(c) = 0$, visto que $\theta(b) \neq 1$. □

Teorema 1.2 *Seja $f(X) = a_2X^2 + a_1X + a_0 \in \mathbb{F}_q[X]$ com q ímpar e $a_2 \neq 0$. Tome $d = a_1^2 - 4a_0a_2$ e seja η o caracter quadrático de $\mathbb{F}_q$. Então*

$$\sum_{c\in\mathbb{F}_q} \eta(f(c)) = \begin{cases} -\eta(a_2) \text{ se } d\neq 0 \\ (q-1)\eta(a_2) \text{ se } d=0 \end{cases}$$

Demonstração:
Temos que $\eta(4a_2^2) = 1$. Logo

$$\begin{aligned}
\sum_{c\in\mathbb{F}_q}\eta(f(c)) &= \eta(4a_2^2)\sum_{c\in\mathbb{F}_q}\eta(a_2c^2+a_1c+a_0)\\
&= \eta(a_2)\sum_{c\in\mathbb{F}_q}\eta(4a_2)\eta(a_2c^2+a_1c+a_0)\\
&= \eta(a_2)\sum_{c\in\mathbb{F}_q}\eta(4a_2^2c^2+4a_1a_2c+4a_0a_2)\\
&= \eta(a_2)\sum_{c\in\mathbb{F}_q}\eta(4a_2^2c^2+4a_1a_2c+a_1^2-a_1^2+4a_0a_2)\\
&= \eta(a_2)\sum_{c\in\mathbb{F}_q}\eta((2a_2c+a_1)^2-d)\\
&= \eta(a_2)\sum_{b\in\mathbb{F}_q}\eta(b^2-d).
\end{aligned}$$

Caso $d=0$ temos $\eta(b^2)=1$ para todo $b\in\mathbb{F}_q^*$ e temos a segunda igualdade. Agora suponha $d\neq 0$ e considere a seguinte igualdade

$$\sum_{b\in\mathbb{F}_q}\eta(b^2-d) = -q+\sum_{b\in\mathbb{F}_q}(1+\eta(b^2-d)).$$

Veja que se b^2-d não é um quadrado, em $\mathbb{F}_q$, então $1+\eta(b^2-d)=1-1=0$. Logo $\sum_{b\in\mathbb{F}_q}(1+\eta(b^2-d))$ é o número dos $c\in\mathbb{F}_q$ tais que $c^2=b^2-d$, donde temos

$$\sum_{b\in\mathbb{F}_q}\eta(b^2-d) = -q+\#(S(d)),$$

sendo $S(d)=\{(b,c)\in\mathbb{F}_q\times\mathbb{F}_q : b^2-c^2=d\}$. Considere o seguinte conjunto $D=\{(u,v)\in\mathbb{F}_q\times\mathbb{F}_q : uv=d\}$. Como consideramos $d\neq 0$, é fácil ver que $\#(D)=q-1$. Observe agora que $\varphi(u,v)=(\frac{u+v}{2},\frac{u-v}{2})$ é uma bijeção entre D e $S(d)$. Segue então que $\#(D)=\#(S(d))$ e temos o resultado. □

1.2 Formas Quadráticas

Nesta seção vamos estudar um pouco sobre formas quadráticas e as formas bilineares associadas.

Seja f uma forma quadrática em $\mathbb{F}_q$. Nosso objetivo consiste em obtermos uma representação equivalente para f mais simples (com menos variáveis), quando for possível, por meio de uma mudança de variáveis.

Lembramos que $\mathbb{F}_{q^n}$ é um $\mathbb{F}_q$-espaço vetorial de dimensão n. Tendo isto em mente a seguir apresentamos três definições que estão intrinsicamente ligadas.

Definição 1.4 (Forma Bilinear)

Uma forma bilinear em $\mathbb{F}_{q^n}$ é uma função

$$\begin{array}{rccc} B & : & \mathbb{F}_{q^n} \times \mathbb{F}_{q^n} & \longrightarrow & \mathbb{F}_q \\ & & (x,y) & \longmapsto & B(x,y) \end{array}$$

tal que B é uma aplicação $\mathbb{F}_q$-linear de $\mathbb{F}_{q^n}$ em $\mathbb{F}_q$ quando fixamos x, isto é, linear na segunda variável, e linear na primeira variável quando fixamos y. Caso $B(x,y) = B(y,x)$, para todos $x, y \in \mathbb{F}_{q^n}$, dizemos que B é bilinear simétrica. □

EXEMPLO 1.4 *Seja $\mathbb{A}$ uma matriz $n \times n$ com entradas em $\mathbb{F}_q$, e $\beta = \{\beta_1, \ldots, \beta_n\}$ uma $\mathbb{F}_q$-base de $\mathbb{F}_{q^n}$ e para $x \in \mathbb{F}_{q^n}$ considere $[x] = (x_1, \ldots, x_n)$ tal que $x = \sum_{i=1}^{n} x_i\beta_i$, com $x_i \in \mathbb{F}_q$. Agora defina $B(x,y) = [x]\mathbb{A}[y]^t$. É claro que B é bilinear. Caso tenhamos $\mathbb{A} = \mathbb{A}^t$ temos que B é bilinear simétrica.* ♢

Definição 1.5 (Forma Quadrática)

Um polinômio $f \in \mathbb{F}_q[x_1, \ldots, x_n]$ é dito uma forma quadrática sobre $\mathbb{F}_q$ se f é nulo ou homogêneo de grau 2. Portanto toda forma quadrática tem a seguinte representação

$$f(x_1, \ldots, x_n) = \sum_{i,j=1}^{n} a_{ij}x_ix_j \text{ com } a_{ij} \in \mathbb{F}_q. \tag{1.1}$$

Muitas vezes nos referimos a f como n-ésima forma quadrática sobre $\mathbb{F}_q$. □

Seja $f \in \mathbb{F}_q[x_1, \ldots, x_n]$ uma forma quadrática, então $f(x_1, \ldots, x_n) = \sum_{i,j=1}^{n} a_{ij}x_ix_j$ com $a_{ij} \in \mathbb{F}_q$. Considere a matriz $\mathbb{B}$, $n \times n$, cujas entradas são precisamente os a_{ij}. É fácil ver que

$$f(x_1, \ldots, x_n) = (x_1, \ldots, x_n)\mathbb{B}\begin{pmatrix} x_1 \\ \vdots \\ x_n \end{pmatrix}. \tag{1.2}$$

Portanto toda forma quadrática possui uma representação matricial dada por (1.2).

EXEMPLO 1.5 *Seja $f(x,y) = 3x^2 + 2xy + 4y^2$ em $\mathbb{F}_7[X,Y]$. Como f é um polinômio homogêneo de grau 2 temos que f é uma forma quadrática sobre $\mathbb{F}_7$ cuja matriz da representação matricial é*

$$\begin{pmatrix} 3 & 2 \\ 0 & 4 \end{pmatrix}.$$

Agora considere a seguinte matriz com entradas em $\mathbb{F}_7$:

$$\begin{pmatrix} 3 & 1 \\ 1 & 4 \end{pmatrix}.$$

Utilizando esta matriz obtemos outra representação matricial para f:

$$f(x,y) = (x,y)\begin{pmatrix} 3 & 1 \\ 1 & 4 \end{pmatrix}(x,y)^t.$$

Onde a matriz desta representação é simétrica. ♢

Dado uma forma quadrática $f(x_1,\ldots,x_n) = \sum_{i,j=1}^{n} a_{ij}x_ix_j$ sobre $\mathbb{F}_q$, supondo q ímpar, é sempre possível obter uma representação matricial com uma matriz simétrica, como vimos no exemplo anterior. Faça $b_{ij} = \frac{(a_{ij}+a_{ji})}{2}$ e temos $f(x_1,\ldots,x_n) = \sum_{i,j=1}^{n} b_{ij}x_ix_j$. Considerando a matriz cujos entradas são (b_{ij}), observe que por definição $b_{ij} = b_{ji}$, temos uma matriz que é igual a sua transposta, ou seja, a matriz com coeficientes (b_{ij}) é simétrica. Esta matriz simétrica, unicamente determinada pela forma quadrática f, quando q é ímpar, vamos denotar por $\mathbb{M}_f$ e iremos referir a ela como matriz dos coeficientes de f.

Neste caso, sendo x um vetor coluna em n indeterminadas $x_1,\ldots,x_n$, é fácil ver que

$$f(x) = x^t\mathbb{M}_f x. \tag{1.3}$$

Observe que a equação (1.1) sempre pode ser reescrita como

$$f(x_1,\ldots,x_n) = \sum_{i}^{n} a_{ii}x_i^2 + \sum_{i<j}(a_{ij}+a_{ji})x_ix_j.$$

Logo podemos assumir que a matriz dos coeficientes de f é triangular superior quando q é par. Em linguagem matricial temos

$$f(x) = x^t \mathbb{A} x, \tag{1.4}$$

sendo $\mathbb{A}$ uma matriz, $n \times n$, triangular superior com coeficientes em $\mathbb{F}_q$. Iremos denotar por $\mathbb{A}_f$ a matriz triangular superior dos coeficientes de f.

Dado f uma n-ésima forma quadrática sobre $\mathbb{F}_q$ sempre podemos pensar na função

$$\begin{array}{rccc} Q_f & : & \mathbb{F}_{q^n} & \longrightarrow & \mathbb{F}_q \\ & & x & \longmapsto & f(x) \end{array}$$

onde x é um vetor coluna no $\mathbb{F}_q$-espaço vetorial $\mathbb{F}_{q^n}$. Observe que

$$Q_f(\alpha x) = \alpha^2 Q_f(x)$$

para todo $\alpha \in \mathbb{F}_q$ e qualquer $x \in \mathbb{F}_{q^n}$. Se que q for ímpar temos

$$\begin{aligned} B_f(x,y) \stackrel{\text{def}}{=} Q_f(x+y) - Q_f(x) - Q_f(y) &= (x+y)^t \mathbb{M}_f (x+y) - x^t \mathbb{M}_f x - y^t \mathbb{M}_f y \\ &= x^t \mathbb{M}_f y + y^t \mathbb{M}_f x \\ &= x^t \mathbb{M}_f y + (y^t \mathbb{M}_f x)^t \\ &= x^t \mathbb{M}_f y + x^t \mathbb{M}_f y \\ &= x^t (2\mathbb{M}_f) y, \end{aligned}$$

pois $\mathbb{M}_f$ é simétrica. Se que q for par temos

$$\begin{aligned} B_f(x,y) = Q_f(x+y) + Q_f(x) + Q_f(y) &= (x+y)^t \mathbb{A}_f (x+y) + x^t \mathbb{A}_f x + y^t \mathbb{A}_f y \\ &= x^t \mathbb{A}_f y + y^t \mathbb{A}_f x \\ &= x^t \mathbb{A}_f y + (y^t \mathbb{A}_f x)^t \\ &= x^t \mathbb{A}_f y + x^t \mathbb{A}_f^t y \\ &= x^t (\mathbb{A}_f + \mathbb{A}_f^t) y \end{aligned}$$

e obtemos B_f bilinear simétrica em ambos os casos. Logo a função Q_f possui as seguintes propriedades:

1. Dado $x \in \mathbb{F}_{q^n}$, $Q_f(\alpha x) = \alpha^2 Q_f(x)$ para todo $\alpha \in \mathbb{F}_q$ e
2. a função

$$\begin{array}{rccc} B_f & : & \mathbb{F}_{q^n} \times \mathbb{F}_{q^n} & \longrightarrow & \mathbb{F}_q \\ & & (x,y) & \longmapsto & Q_f(x+y) - Q_f(x) - Q_f(y) \end{array}$$

é $\mathbb{F}_q$-bilinear simétrica.

Devido a importância das propriedades (1) e (2) satisfeitas por Q_f dizemos que uma função que satifaz estas propriedades é uma *função quadrática*. Também devido a importância da função B_f definimos:

Definição 1.6 (Forma Bilinear Associada)

Seja $f \in \mathbb{F}_q[x_1, \ldots, x_n]$ uma forma quadrática. Então a função definida por

$$B_f(v, w) \stackrel{def}{=} Q_f(v + w) - Q_f(v) - Q_f(w)$$

é dita forma bilinear simétrica associada a f, onde Q_f é a função quadrática induzida por f. Como vimos B_f é sempre simétrica, dessa forma iremos nos referir a B_f simplesmente como forma bilinear associada a f. □

É importante observar que quando q é ímpar a forma matricial de B_f é dada por $2\mathbb{M}_f$. E quando q é par a forma matricial de B_f é $\mathbb{A}_f + \mathbb{A}_f^t$.

Até aqui vimos que dado uma forma quadrática f é possível associar uma função quadrática. Agora vamos ver que este processo é reversível, ou seja, dado uma função quadrática é possível associar uma forma quadrática. De fato, considere $h : \mathbb{F}_{q^n} \longrightarrow \mathbb{F}_q$ uma função quadrática sobre $\mathbb{F}_q$. Novamente vamos separar em dois casos um quando q for ímpar e o outro quando q for par. Seja $\{e_1, \ldots, e_n\}$ a base canônica de $\mathbb{F}_{q^n}$ sobre $\mathbb{F}_q$.

- No caso ímpar defina

  $$b_{ij} = \frac{B_h(e_i, e_j)}{2}$$

  e temos a seguinte forma quadrática

  $$f(x_1, \ldots, x_n) = \sum_{i,j=1}^{n} b_{ij} x_i x_j.$$

  Claramente Q_f é igual a função quadrática h.

- No caso par defina

  $$a_{ij} = \begin{cases} h(e_i), & \text{se} \quad i = j \\ B_h(e_i, e_j), & \text{se} \quad i < j \\ 0, & \text{se} \quad i > j \end{cases}$$

temos então a seguinte forma quadrática

$$f(x_1, \ldots, x_n) = \sum_{i,j=1}^{n} a_{ij} x_i x_j.$$

Por definição temos $Q_f(e_i) = h(e_i)$. Vamos verificar, por indução no número de variáveis n, que $Q_f(\alpha_1 e_1 + \cdots + \alpha_n e_n) = h(\alpha_1 e_1 + \cdots + \alpha_n e_n)$ onde $\alpha_i \in \mathbb{F}_q$ com $i \in \{1, \ldots, n\}$. Disto teremos Q_f igual a função quadrática h. De fato:
Quando $n = 1$ o resultado é imediato. Suponha que para $n = k > 1$ tenhamos
$Q_f(\alpha_1 e_1 + \cdots + \alpha_k e_k) = h(\alpha_1 e_1 + \cdots + \alpha_k e_k)$. Vamos verificar que esta igualdade também é válida para $n = k + 1$ e o resultado seguirá por indução finita. Observe que $B_f(x, y) = Q_f(x + y) + Q_f(x) + Q_f(y)$ logo

$$Q_f(\sum_{i=1}^{k+1} \alpha_i e_i) = B_f(\sum_{i=1}^{k} \alpha_i e_i, \alpha_{k+1} e_{k+1}) + Q_f(\sum_{i=1}^{k} \alpha_i e_i) + Q_f(\alpha_{k+1} e_{k+1}). \tag{1.5}$$

Por hipótese de indução $Q_f(\sum_{i=1}^{k} \alpha_i e_i) = h(\sum_{i=1}^{k} \alpha_i e_i)$ e $Q_f(\alpha_{k+1} e_{k+1}) = h(\alpha_{k+1} e_{k+1})$ como

$$\begin{aligned}
B_f(\alpha_1 e_1 + \cdots + \alpha_k e_k, \alpha_{k+1} e_{k+1}) &= B_f(\alpha_1 e_1, \alpha_{k+1} e_{k+1}) + \cdots + B_f(\alpha_k e_k, \alpha_{k+1} e_{k+1}) \\
&= \alpha_1 \alpha_{k+1} B_f(e_1, e_{k+1}) + \cdots + \alpha_k \alpha_{k+1} B_f(e_k, e_{k+1}) \\
&= \alpha_1 \alpha_{k+1} a_{1(k+1)} + \cdots + \alpha_k \alpha_{k+1} a_{k(k+1)} \\
&= \alpha_1 \alpha_{k+1} B_h(e_1, e_{k+1}) + \cdots + \alpha_k \alpha_{k+1} B_h(e_k, e_{k+1}) \\
&= B_h(\alpha_1 e_1 + \cdots + \alpha_k e_k, \alpha_{k+1} e_{k+1}),
\end{aligned}$$

substituindo estas igualdades em (1.5), obtemos

$$Q_f(\sum_{i=1}^{k+1} \alpha_i e_i) = B_h(\sum_{i=1}^{k} \alpha_i e_i) + h(\sum_{i=1}^{k} \alpha_i e_i) + h(\alpha_{k+1} e_{k+1}) = h(\sum_{i=1}^{k+1} \alpha_i e_i)$$

e obtemos, por indução matemática a igualdade desejada.

Portanto dado uma função quadrática existe uma forma quadrática associada a esta e reciprocamente dado uma forma quadrática temos uma função quadrática. Desse modo não iremos fazer distinção entre formas e funções quadráticas.

Na verdade o que acabamos de relatar e provar se resume no seguinte teorema:

Teorema 1.3 *Uma função $h : \mathbb{F}_{q^n} \longrightarrow \mathbb{F}_q$ é uma forma quadrática se, e somente se, h é uma função quadrática.*

Um exemplo da utilização do Teorema 1.3 é o proímo resultado.

Corolário 1.4 *Sejam k e r inteiros positivos tais que $k = 2r$ e $\lambda \in \mathbb{F}_{q^k}^*$. Então a função:*

$$\begin{array}{rccc} \phi & : & \mathbb{F}_{q^k} & \longrightarrow & \mathbb{F}_q \\ & & x & \longmapsto & tr(\lambda x^{q^r+1}) \end{array}$$

é uma forma quadrática, onde $tr : \mathbb{F}_{q^k} \longrightarrow \mathbb{F}_q$ é a aplicação $\mathbb{F}_q$-linear definida por $tr(a) = a + a^q + \cdots + a^{q^{k-1}}$, chamada de traço.

Demonstração:

Pelo Teorema 1.3 basta verificarmos que ϕ é uma função quadrática, ou seja, $\phi(ax) = a^2\phi(x)$ para todo $a \in \mathbb{F}_q$ e

$$\begin{array}{rccc} B_\phi & : & \mathbb{F}_{q^k} \times \mathbb{F}_{q^k} & \longrightarrow & \mathbb{F}_q \\ & & (x, y) & \longmapsto & Q_\phi(x+y) - Q_\phi(x) - Q_\phi(y) \end{array}$$

é $\mathbb{F}_q$-bilinear simétrica.

De fato:

Primeiro observe que sendo $a^q = a$, tem-se que $a^{q^r+1} = a^2$ e portanto

$$\phi(ax) = tr(\lambda(ax)^{q^r+1}) = tr(\lambda a^{q^r+1}x^{q^r+1}) = tr(\lambda a^2 x^{q^r+1}) = a^2 tr(\lambda x^{q^r+1}) = a^2\phi(x).$$

Agora veja que

$$\begin{aligned} Q_\phi(x+y) &= tr(\lambda(x+y)^{q^r+1}) \\ &= tr(\lambda(x+y)^{q^r}(x+y)) \\ &= tr(\lambda(x^{q^r} + y^{q^r})(x+y)) \\ &= tr(\lambda x^{q^r+1}) + tr(\lambda y^{q^r+1}) + tr[\lambda(xy^{q^r} + yx^{q^r})] \\ &= Q_\phi(x) + Q_\phi(y) + tr[\lambda(xy^{q^r} + yx^{q^r})] \end{aligned}$$

Claramente $tr[\lambda(xy^{q^r} + yx^{q^r})]$ é $\mathbb{F}_q$-bilinear simétrica e temos o resultado.

□

Duas formas quadráticas são identificadas a partir da seguinte definição:

Definição 1.7 (Equivalência de Formas Quadráticas)

Sejam $f, g \in \mathbb{F}_q[x_1, \ldots, x_n]$ duas formas quadráticas. Dizemos que f é equivalente a g se existe $\mathbb{P}$ matriz $n \times n$ com coeficientes em $\mathbb{F}_q$, invertível, tal que $f(X) = g(\mathbb{P}X)$. Notação: $f \sim g$. □

É fácil ver que esta definição fornece uma relação de equivalência no conjunto das formas quadráticas sobre $\mathbb{F}_q$.

A Definição 1.7 diz que existe uma substituição linear de variáveis que leva a forma g na forma f.

Dada duas formas quadráticas f e $g \in \mathbb{F}_q[x_1, \ldots, x_n]$ equivalentes temos que para todo $b \in \mathbb{F}_q$ as equações $f(X) = b$ e $g(X) = b$ possuem o mesmo número de soluções em $\mathbb{F}_q^n$, visto que $\mathbb{P}$ estabelece uma bijeção entre seus vetores solução. Portanto equivalência de formas quadráticas preserva o número de soluções.

Suponha q ímpar e que $f \sim g$. Então por (1.3) temos $g(\mathbb{P}X) = (\mathbb{P}X)^t \mathbb{M}_g(\mathbb{P}X) = X^t \mathbb{P}^t \mathbb{M}_g(\mathbb{P}X)$ e pela condição de equivalência $g(\mathbb{P}X) = f(X) = X^t \mathbb{M}_f X$. Portando dado $f \sim g$ existe uma matriz $\mathbb{P}$, $n \times n$, invertível com coeficentes em $\mathbb{F}_q$ tal que

$$\mathbb{M}_f = \mathbb{P}^t \mathbb{M}_g \mathbb{P}. \tag{1.6}$$

Agora supondo q par e $f \sim g$ obtemos de modo análogo ao caso ímpar, utilizando a equação (1.4), que

$$\mathbb{A}_f = \mathbb{P}^t \mathbb{A}_g \mathbb{P}. \tag{1.7}$$

Desde que já indentificamos formas quadráticas é possível destacar, na nossa próxima definição, as que chamamos de não degeneradas e por conseqüência as formas bilineares associadas que são não degeneradas.

Definição 1.8 (Forma Quadrática não degenerada)

Dada uma forma quadrática f em $\mathbb{F}_q[x_1, \ldots, x_n]$ tal que $f \notin \mathbb{F}_q[x_1, \ldots, \hat{x}_i, \ldots, x_n]$ para todo $i \in \{1, \ldots, n\}$, dizemos que f é não degenerada quando não existe nenhuma forma quadrática g equivalente a f com número de variáveis menor que n, ou seja, $g \sim f$ implica que g possui n variáveis.

□

EXEMPLO 1.6 *Considere a seguinte forma quadrática* $f(x_1, x_2, x_3) = x_1^2 + x_2^2 + x_3^2$, *sobre* $\mathbb{F}_2$. *Aplique a seguinte mudança de variáveis dada pela matriz*

$$\mathbb{P} = \begin{pmatrix} 1 & 0 & 0 \\ 1 & 1 & 0 \\ 0 & 1 & 1 \end{pmatrix},$$

então definindo $g(x) = f(\mathbb{P}x)$ *obtemos*

$$g(x_1, x_2, x_3) = f(x_1, x_1 + x_2, x_2 + x_3) = x_1^2 + x_1^2 + x_2^2 + x_2^2 + x_3^2 = x_3^2.$$

Assim f *é equivalente a* g, *pela Definição* 1.7, *que só possui uma variável, e portanto* f *é degenerada.* ♢

Definição 1.9 (Forma Bilinear não degenerada e Núcleo)

Seja f *uma forma quadrática em* n *variáveis sobre* $\mathbb{F}_q$ *e* B_f *sua forma bilinear associada. Considere o conjunto* $Ker(B_f) = \{x \in \mathbb{F}_{q^n} : B_f(x, y) = 0 \text{ para todo } y \in \mathbb{F}_{q^n}\}$, B_f *é dita não degenerada quando o conjunto* $Ker(B_f)$ *é o conjunto* $\{0\}$. *Caso contrário* B_f *é dita degenerada.*

O conjunto $Ker(B_f)$ *é dito núcleo de* B_f. *Claramente* $Ker(B_f)$ *é um subespaço vetorial de* $\mathbb{F}_{q^n}$. *O número dado por* $dim(Ker(B_f))$ *é dito dimensão do núcleo de* B_f.

□

EXEMPLO 1.7 *Defina*

$$\begin{array}{rccc} B & : & \mathbb{F}_{q^n} \times \mathbb{F}_{q^n} & \longrightarrow & \mathbb{F}_q \\ & & (x, y) & \longmapsto & B(x, y) := tr(xy) \end{array}$$

onde tr *é o traço de* $\mathbb{F}_{q^n}$ *sobre* $\mathbb{F}_q$.

Claramente, pela definição do traço, B *é uma forma bilinear simétrica. Vamos calcular seu núcleo. Por definição* $Ker(B_f) = \{x \in \mathbb{F}_{q^n} : B_f(x, y) = 0 \text{ para todo } y \in \mathbb{F}_{q^n}\}$. *No apêndice A vimos que existem* $\{\alpha_1, \ldots, \alpha_n\}$, $\{\beta_1, \ldots, \beta_n\}$ *bases de* $\mathbb{F}_{q^n}$ *sobre* $\mathbb{F}_q$ *tais que*

$$tr(\alpha_i \beta_j) = \begin{cases} 1 \text{ para } i=j. \\ \\ 0 \text{ para } i \neq j \end{cases}$$

Seja $x \in \mathbb{F}_{q^n}$ *então* $x = \sum_{i=1}^{n} a_i \alpha_i$. *Fixe* $j \in \{1, \ldots, n\}$ *e temos que*

$$0 = tr(x\beta_j) = tr((\sum_{i=1}^{n} a_i \alpha_i)\beta_j) = tr(\sum_{i=1}^{n} a_i \alpha_i \beta_j) = \sum_{i=1}^{n} a_i tr(\alpha_i \beta_j) = a_j.$$

Logo $a_j = 0$ como j é arbitrário temos que $x = 0$ e portanto $Ker(B_f) = 0$ e $B(x, y) = tr(xy)$ é não degenerada. ♢

O teorema seguinte caracteriza as formas bilineares associadas que são não degeneradas.

Teorema 1.5 *Seja f uma forma quadrática em n variáveis sobre $\mathbb{F}_q$ e B_f sua forma bilinear associada. Seja $\mathbb{B}$ a representação matricial de B_f. Então são equivalentes:*

1. *B_f é não degenerada.*
2. $\det \mathbb{B} \neq 0$.

Demonstração:
Lembre que $\mathbb{B}$ corresponde a $2\mathbb{M}_f$ ou $\mathbb{A}_f + \mathbb{A}_f^t$ dependendo se q é ímpar ou par. Veja que por definição $Ker(B_f)$ é o conjunto dos $x \in \mathbb{F}_q$ tal que $x^t \mathbb{B} y = 0$ para todo $y \in \mathbb{F}_q$. Logo $Ker(B_f)$ é o conjunto dos $x \in \mathbb{F}_q$ tal que $x^t \mathbb{B} = 0$. Portanto $Ker(B_f) = 0$, se e somente se, $\det \mathbb{B} \neq 0$. Donde temos o resultado. □

É importante observar que quando q é par toda forma quadrática diagonal, $x_1^2 + \cdots + x_n^2$, tem forma bilinear associada, B_f, degenerada. De fato, se $f(x) = x^t \mathbb{A} x$ temos que $\mathbb{A}_f + \mathbb{A}_f^t$ é a matriz nula. Portanto B_f é degenerada.

Teorema 1.6 *Seja f uma forma quadrática em n variáveis sobre $\mathbb{F}_q$. Seja g forma quadrática não degenerada em r variáveis sobre $\mathbb{F}_q$ tal que $f \sim g$. Se B_g é não degenerada temos que $dim(Ker(B_f)) = n - r$.*

Demonstração:
Suponha q ímpar. Neste caso $B_f(x, y) = x^t (2\mathbb{M}_f) y$ e trivialmente temos que $dim(Ker(B_f)) = n - Posto(\mathbb{M}_f)$. Pela igualdade (1.6) temos que $\mathbb{M}_f = \mathbb{P}^t \mathbb{M}_g \mathbb{P}$, onde $\mathbb{P}$ é invertível. Disto segue que $Posto(\mathbb{M}_f) = Posto(\mathbb{M}_g)$. Como B_g é não degenerada, pelo Teorema 1.5, $Posto(\mathbb{M}_g) = r$ e temos

$$dim(Ker(B_f)) = n - Posto(\mathbb{M}_f) = n - Posto(\mathbb{M}_g) = n - r.$$

Agora suponha q par. Neste caso $B_f(x, y) = x^t (\mathbb{A}_f + \mathbb{A}_f^t) y$ e então $dim(Ker(B_f)) = n - Posto(\mathbb{A}_f + \mathbb{A}_f^t)$. Pela equação (1.7) temos $\mathbb{A}_f + \mathbb{A}_f^t = \mathbb{P}^t (\mathbb{A}_g + \mathbb{A}_g^t) \mathbb{P}$ com $\mathbb{P}$ invertível.

Donde $Posto(\mathbb{A}_f + \mathbb{A}_f^t) = Posto(\mathbb{A}_g + \mathbb{A}_g^t)$. Pelo Teorema 1.5 temos $Posto(\mathbb{A}_g + \mathbb{A}_g^t) = r$ e então

$$dim(Ker(B_f)) = n - Posto(\mathbb{A}_f + \mathbb{A}_f^t) = n - Posto(\mathbb{A}_g + \mathbb{A}_g^t) = n - r.$$

□

Para identificar formas é importante o seguinte conceito.

Definição 1.10 (Representação)

Seja $f \in \mathbb{F}_q[x_1, \ldots, x_n]$ e $b \in \mathbb{F}_q$. Dizemos que f representa b quando existe solução para $f(X) = b$. □

No sentido de identificar formas apresentamos dois lemas técnicos:

Lema 1.7 *Seja $cx_1^2 + 2b_2x_1x_2 + \cdots + 2b_nx_1x_n + h(x_2, \ldots, x_n) \in \mathbb{F}_q[x_1, \ldots, x_n]$, onde $n \geq 2$, uma forma quadrática com q ímpar, $c \neq 0$ e $h(x_2, \ldots, x_n) \in \mathbb{F}_q[x_2, \ldots, x_n]$ forma quadrática. Então*

$$cx_1^2 + 2b_2x_1x_2 + \cdots + 2b_nx_1x_n + h(x_2, \ldots, x_n) = c(x_1 + b_2c^{-1}x_2 + \cdots + b_nc^{-1}x_n)^2 + g(x_2, \ldots, x_n)$$

onde $g \in \mathbb{F}_q[x_2, \ldots, x_n]$ é forma quadrática.

Demonstração:

A demonstração segue por indução sobre n e completamento de quadrados. □

Lema 1.8 *Sejam $f \in \mathbb{F}_q[x_1, \ldots, x_n]$ uma forma quadrática, q ímpar, $n \geq 2$ e $c \in \mathbb{F}_q^*$. Se f representa c, então f é equivalente a*

$$cx_1^2 + g(x_2, \ldots, x_n)$$

onde $g \in \mathbb{F}_q[x_2, \ldots, x_n]$ é uma forma quadrática com $n - 1$ variáveis.

Demonstração:

Por hipótese existe $v = (v_1, \ldots, v_n) \in \mathbb{F}_q^n$ tal que $f(v) = c$. Como $c \neq 0$ algum v_i é diferente

de zero. Seja $\mathbb{P}$ uma matriz não singular $n \times n$, com entradas em $\mathbb{F}_q$, onde a primeira coluna é o vetor v. Temos então seguinte mudança de variáveis

$$\begin{pmatrix} y_1 \\ \vdots \\ y_n \end{pmatrix} = \mathbb{P} \begin{pmatrix} x_1 \\ \vdots \\ x_n \end{pmatrix}.$$

Faça $g(Y) = f(\mathbb{P}X)$ e temos pela equação (1.6) que $\mathbb{M}_g = \mathbb{P}^t \mathbb{M}_f \mathbb{P}$, logo escrevendo $g = \sum_{i \leq j, i=1}^{n} a_{ij} y_i y_j$ temos

$$\begin{aligned} a_{11} = (1,0,\ldots,0)\mathbb{M}_g \begin{pmatrix} 1 \\ 0 \\ \vdots \\ 0 \end{pmatrix} &= (1,0,\ldots,0)\mathbb{P}^t \mathbb{M}_f \mathbb{P} \begin{pmatrix} 1 \\ 0 \\ \vdots \\ 0 \end{pmatrix} \\ &= (v_1, v_2, \ldots, v_n)\mathbb{M}_f \begin{pmatrix} v_1 \\ \vdots \\ v_n \end{pmatrix} \\ &= f(v) = c \end{aligned}$$

e temos uma forma quadrática g cujo coeficiente do termo y_1^2 é $f(v) = c$, ou seja f é equivalente a uma forma quadrática dada por:

$$cy_1^2 + 2b_2 y_1 y_2 + \cdots + 2b_n y_1 y_n + h(y_2, \ldots, y_n) = c(y_1 + b_2 c^{-1} y_2 + \cdots + b_n c^{-1} y_n)^2 + g(y_2, \ldots, y_n).$$

A igualdade segue do Lema 1.7 com apropriados $b_i \in \mathbb{F}_q$ e formas quadráticas h, g sobre $\mathbb{F}_q$. Agora fazendo a seguinte mudança de variáveis:

$$x_1 = y_1 + b_2 c^{-1} y_2 + \cdots + b_n c^{-1} y_n,\ x_2 = y_2, \ldots, x_n = y_n$$

obtemos a forma quadrática desejada.

□

Utilizando o lema anterior e indução finita obtemos o seguinte resultado.

Teorema 1.9 *Toda forma quadrática f sobre $\mathbb{F}_q$, q ímpar, é equivalente a uma forma quadrática diagonal, a qual denotaremos por Q.*

Demonstração:

Faremos a demostração usando indução finita sobre n. Se $n = 1$ temos $f(x_1) = a_{11}x_1^2$ que já é diagonal. Suponha agora $n \geq 2$ e que o resultado é válido para todo $k \leq n-1$. Seja $f \in \mathbb{F}_q[x_1, \ldots, x_n]$ uma forma quadrática em n variavéis. Se $f \equiv 0$ é óbvio. Vamos supor f não nula. Se para algum i temos $a_{ii} \neq 0$ então f representa a_{ii}, ou caso contrário existem i, j, $i \neq j$ tal que $a_{ij} \neq 0$ e f representa $2a_{ij}$, visto que $f(c_1, \ldots, c_n) = 2a_{ij}$ quando $c_i = c_j = 1$ e $c_k = 0$. Destas considerações temos que f representa algum $a_1 \in \mathbb{F}_q^*$ e pelo lema anterior $f(x_1, \ldots, x_n) = a_1x_1^2 + g(x_2, \ldots, x_n)$. Portanto aplicando a hipótese de indução sobre a forma quadrática g temos o resultado.

□

Seja $f \in \mathbb{F}_q[x_1, \ldots, x_n]$, q ímpar, uma forma quadrática equivalente a $a_1x_1^2 + \cdots + a_nx_n^2$ onde os a_i podem ser zero. Sabemos que o posto de uma matriz é invariante pela multiplicação por uma matriz não singular. Portanto é imediato que para formas quadráticas equivalentes as suas matrizes de coeficientes possuam o mesmo posto.

Se $\mathbb{M}_f$ tem posto n é claro que f é não degenerada. E se o posto de $\mathbb{M}_f$ é igual a n segue que $\det \mathbb{M}_f \neq 0$, logo

$$\det \mathbb{M}_g = \det \mathbb{M}_f (\det \mathbb{P})^2 \tag{1.8}$$

quando $f \sim g$, pela igualdade (1.6).

Sendo f forma quadrática não degenerada em n variáveis sobre $\mathbb{F}_q$, com q par, vamos procurar uma forma quadrática g equivalente a f que tenha uma representação mais simples. Para isto precisamos do seguinte resultado:

Lema 1.10 *Seja $f \in \mathbb{F}_q[x_1, \ldots, x_n]$ uma forma quadrática não degenerada com q par. Se $n \geq 3$ então f é equivalente a*

$$x_1x_2 + g(x_3, \ldots, x_n),$$

onde $g \in \mathbb{F}_q[x_3, \ldots, x_n]$ é uma forma quadrática não degenerada.

Demonstração:

Primeiro vamos mostrar que f é equivalente a uma forma quadrática cujo coeficiente do termo x_{11}^2 é zero. Sabemos que

$$f(x_1, \ldots, x_n) = \sum_{1 \leq i \leq j \leq n} a_{ij} x_i x_j \text{ com } a_{ij} \in \mathbb{F}_q. \tag{1.9}$$

Se para algum i, $a_{ii} = 0$, basta uma mudança de variáveis e temos $a_{11} = 0$. Logo podemos assumir que para todo i temos $a_{ii} \neq 0$. Se tivermos $a_{ij} = 0$ para todos $1 \leq i \leq j \leq n$, teríamos

$$f(x_1, \ldots, x_n) = a_{11}x_1^2 + \cdots + a_{nn}x_n^2 = (a_{11}^{\frac{q}{2}} x_1 + \cdots + a_{nn}^{\frac{q}{2}} x_n)^2$$

e f seria equivalente a uma forma quadrática com uma variável, contradizendo o fato de ser não degenerada. Logo podemos, por uma reordenação das variáveis, supor que $a_{23} \neq 0$. Então

$$f(x_1, \ldots, x_n) = a_{22}x_2^2 + x_2(a_{12}x_1 + a_{23}x_3 + \cdots + a_{2n}x_n) + g_1(x_1, x_3, \ldots, x_n).$$

Fazendo a seguinte substituição linear (lembre que $a_{23} \neq 0$):

$$x_3 = a_{23}^{-1}(a_{12}y_1 + y_3 + a_{24}y_4 + \cdots + a_{2n}y_n),\ x_i = y_i \text{ para } i \neq 3.$$

Vamos obter uma forma g, equivalente a f, tal que

$$g(y_1, \ldots, y_n) = a_{22}y_2^2 + y_2y_3 + g_2(y_1, y_3, \ldots, y_n).$$

Sendo b_{11} o coeficiente de y_1^2 em g_2 e com uma nova mudança de variáveis

$$y_2 = (a_{22}^{-1}b_{11})^{\frac{q}{2}} z_1 + z_2,\ y_i = z_i \text{ para } i \neq 2$$

o coeficiente de z_1^2 é zero, como desejávamos.

Portanto podemos supor, a menos de mudança de variáveis, que f dada por (1.9) tem coeficiente $a_{11} = 0$, ou seja

$$f(x_1, \ldots, x_n) = \sum_{1 \leq i \leq j \leq n} a_{ij} x_i x_j \text{ com } a_{ij} \in \mathbb{F}_q \text{ e } a_{11} = 0.$$

Visto que f é não degenerada, algum $a_{1j} \neq 0$, vamos assumir que $a_{12} \neq 0$ e com a seguinte mudança de variáveis

$$x_2 = a_{12}^{-1}(w_2 + a_{13}w_3 + \cdots + a_{1n}w_n),\ x_i = w_i \text{ para } i \neq 2$$

transformamos f numa forma quadrática do tipo

$$w_1w_2 + \sum_{2\leq i\leq j\leq n} c_{ij}w_iw_j$$

e com uma última mudança de variáveis

$$w_1 = u_1 + c_{22}u_3 + \cdots + c_{2n}u_n,\ w_i = u_i \text{ para } i \neq 1$$

obtemos a forma quadrática equivalente

$$u_1u_2 + g(u_3, \ldots, u_n),$$

onde $g \in \mathbb{F}_q[u_3, \ldots, u_n]$ é uma forma quadrática claramente não degenerada pela construção.

□

O próximo teorema dá uma caracterização de forma quadrática não degenerada quando q é par.

Teorema 1.11 *Seja $f \in \mathbb{F}_q[x_1, \ldots, x_n]$, com q par, forma quadrática não degenerada. Se n é par então f é equivalente a*

$$x_1x_2 + x_3x_4 + \cdots + x_{n-1}x_n$$

ou a

$$x_1x_2 + x_3x_4 + \cdots + x_{n-1}x_n + x_{n-1}^2 + ax_n^2$$

onde $a \in \mathbb{F}_q$ e satisfaz $tr(a) = 1$ sendo tr definida de $\mathbb{F}_q$ sobre o seu subcorpo primo $\mathbb{F}_2$.

Demonstração:

Usando indução em n junto com o Lema 1.10 é fácil mostrar que f é equivalente a uma forma do tipo

$$x_1x_2 + x_3x_4 + \cdots + x_{n-3}x_{n-2} + bx_{n-1}^2 + cx_{n-1}x_n + dx_n^2$$

onde $b, c, d \in \mathbb{F}_q$.

Visto que f é não degenerada devemos ter $c \neq 0$. Pois caso contrário a identidade $bx_{n-1}^2 + dx_n^2 = (b^{\frac{q}{2}}x_{n-1} + d^{\frac{q}{2}}x_n)^2$ vai nos fornecer uma forma quadrática com o número de variáveis menor que n.

Se $b = 0$ temos $cx_{n-1}x_n + dx_n^2 = (cx_{n-1} + dx_n)x_n$ é equivalente a $x_{n-1}x_n$ e temos o resultado.

Se $b \neq 0$ substitua x_{n-1} por $b^{-\frac{q}{2}}x_{n-1}$ e x_n por $b^{q/2}cx_n$. Com esta mudança de variáveis temos

$$bx_{n-1}^2 + cx_{n-1}x_n + dx_n^2 \sim x_{n-1}^2 + x_{n-1}x_n + ax_n^2$$

para algum $a \in \mathbb{F}_q$. Suponha que o polinômio x^2+x+a é redutível em $\mathbb{F}_q[x]$. Logo $x^2+x+a = (x + c_1)(x + c_2), c_1, c_2 \in \mathbb{F}_q$ e portanto $x_{n-1}^2 + x_{n-1}x_n + ax_n^2 = (x_{n-1} + c_1x_n)(x_{n-1} + c_2x_n)$ é equivalente a x_nx_{n-1}. Caso $x^2 + x + a$ seja irredutível em $\mathbb{F}_q[x]$ temos pelo Corolário $A.16$ que $tr(a) = 1$ e o resultado fica estabelecido para todos os casos. □

1.3 Número de Soluções de Formas Quadráticas

Iniciamos nesta seção o estudo sobre o número de soluções em $\mathbb{F}_q^n$ de equações do tipo $f(x_1, \ldots, x_n) = b$, $b \in \mathbb{F}_q$ e f uma forma quadrática. Vamos denotar por $N(f(x_1, \ldots, x_n) = b)$ o número de soluções da equação $f(x_1, \ldots, x_n) = b$ sobre $\mathbb{F}_q$, onde consideramos somente as indeterminadas que realmente ocorrem na equação $f(x_1, \ldots, x_n) = b$. Por exemplo $N(a_1x_1^2 + a_2x_2^2 = b)$ refere-se ao número de soluções de $a_1x_1^2 + a_2x_2^2 = b$ em $\mathbb{F}_q^2$.

Vamos concentrar nossos esforços no caso em que n é par. Contudo observamos que utilizando a mesma técnica é possível determinar o número de soluções de uma forma quadrática quando n é ímpar. Contudo para nossos objetivos restringimos nossa atenção ao caso n par.

Para atingirmos nosso objetivo introduzimos o conceito de valor inteiro e um lema sobre sua soma.

Definição 1.11 (Valor Inteiro)

A função ν definida em $\mathbb{F}_q$ por

$$b \mapsto \begin{cases} -1 \ se \ b \in \mathbb{F}_q^* \\ q-1 \ se \ b=0 \end{cases}$$

é dita valor inteiro de $\mathbb{F}_q$. □

Lema 1.12 *Para todo corpo finito, $\mathbb{F}_q$, tem-se:*

$$\sum_{c\in\mathbb{F}_q}\nu(c)=0, \tag{1.10}$$

e mais ainda para todo $b\in\mathbb{F}_q$

$$\sum_{c_1+\cdots+c_m=b}\nu(c_1)\cdots\nu(c_k)=\begin{cases}0 \ \ se\ 1\leq k<m\\ \\ \nu(b)q^{m-1} \ \ se\ k=m\end{cases} \tag{1.11}$$

sendo $c_1,\ldots,c_m\in\mathbb{F}_q$.

Demonstração:

A equação dada por (1.10) é obviamente verdadeira. Para obtermos a igualdade (1.11) considere primeiro quando $1\leq k<m$ e temos

$$\begin{aligned}\sum_{c_1+\cdots+c_m=b}\nu(c_1)\cdots\nu(c_k) &= \sum_{c_1,\ldots,c_k\in\mathbb{F}_q}\nu(c_1)\ldots\nu(c_k)\cdot\sum_{c_{k+1}+\cdots+c_m=b-c_1-\cdots-c_k}1\\ &= q^{m-k-1}\sum_{c_1,\ldots,c_k\in\mathbb{F}_q}\nu(c_1)\cdots\nu(c_k)\\ &= q^{m-k-1}\left(\sum_{c_1\in\mathbb{F}_q}\nu(c_1)\right)\cdots\left(\sum_{c_k\in\mathbb{F}_q}\nu(c_k)\right)=0\end{aligned}$$

onde a última igualdade segue de (1.10).

Se $k=m$, vamos proceder por indução em m. O caso $m=1$ é trivial. Suponha a hipótese válida para $m\geq 2$. Pela primeira parte temos

$$\begin{aligned}\sum_{c_1+\cdots+c_{m+1}=b}\nu(c_1)\cdots\nu(c_m)\nu(c_{m+1}) &= \sum_{c_1+\cdots+c_{m+1}=b}\nu(c_1)\cdots\nu(c_m)[\nu(c_{m+1})+1]\\ &= \sum_{c_1,\ldots,c_m\in\mathbb{F}_q}\nu(c_1)\cdots\nu(c_m)[\nu(b-c_1-\cdots-c_m)+1]\\ &= q\sum_{c_1+\cdots+c_m=b}\nu(c_1)\cdots\nu(c_m)\end{aligned}$$

E esta última igualdade segue do fato da expressão entre colchetes ser zero, exceto quando $c_1+\cdots+c_m=b$, e neste caso $\nu(b-c_1-\cdots-c_m)=q-1$. Aplicando agora a hipótese de indução obtemos o resultado. □

Lema 1.13 *Sejam q ímpar, $b \in \mathbb{F}_q$, $a_1, a_2 \in \mathbb{F}_q^*$ e η o caractere quadrático de $\mathbb{F}_q$. Então*

$$N(a_1x_1^2 + a_2x_2^2 = b) = q + \nu(b)\eta(-a_1a_2). \tag{1.12}$$

Demonstração:

Sejam $c_1, c_2 \in \mathbb{F}_q$, aplicando o Lema 1.1 temos

$$\begin{aligned} N(a_1x_1^2 + a_2x_2^2 = b) &= \sum_{c_1+c_2=b} N(a_1x_1^2 = c_1)N(a_2x_2^2 = c_2) \\ &= \sum_{c_1+c_2=b} [1 + \eta(c_1a_1^{-1})][1 + \eta(c_2a_2^{-1})] \\ &= q + \eta(a_1)\sum_{c_1\in\mathbb{F}_q} \eta(c_1) + \eta(a_2)\sum_{c_2\in\mathbb{F}_q} \eta(c_2) + \eta(a_1a_2)\sum_{c_1+c_2\in\mathbb{F}_q} \eta(c_1c_2) \\ &= q + \eta(a_1a_2)\sum_{c\in\mathbb{F}_q} \eta(bc - c^2). \end{aligned}$$

O último somatório é igual a $\nu(b)\eta(-1)$ pelo Teorema 1.2. Donde temos o resultado.

□

Seja q ímpar. Desejamos calcular o número de soluções de $f(x_1, \ldots, x_n) = b$, onde $b \in \mathbb{F}_q$ e f é uma forma quadrática sobre $\mathbb{F}_q$. Sabemos pelo Teorema 1.9 que $f \sim Q$, Q forma quadrática diagonal. Logo podemos supor, sem perda de generalidade, que Q pode ser reescrita como $a_1x_1^2 + \cdots + a_kx_k^2$, onde $1 \leq k \leq n$ e todo $a_k \neq 0$. Como para todo $b \in \mathbb{F}_q$ o número de soluções de $a_1x_1^2 + \cdots + a_kx_k^2 = b$ em $\mathbb{F}_q^n$ é q^{n-k} vezes o número de soluções da mesma equação em $\mathbb{F}_q^k$, basta considerarmos o caso onde $k = n$, ou seja, quando f é não degenerada.

Teorema 1.14 *Seja f uma forma quadrática não degenerada sobre $\mathbb{F}_q$, q ímpar, n o número de variáveis. Se n é par então para $b \in \mathbb{F}_q$ o número de soluções da equação $f(x_1, \ldots, x_n) = b$ em $\mathbb{F}_q^n$ é*

$$q^{n-1} + \nu(b)q^{\frac{(n-2)}{2}}\eta((-1)^{\frac{n}{2}}\Delta)$$

onde η é o caractere quadrático de $\mathbb{F}_q$ e $\Delta = \det(\mathbb{M}_f)$.

Demonstração:

Seja $a_1x_1^2 + \cdots + a_nx_n^2$ a forma quadrática diagonal equivalente a f. Visto que esta equivalência preserva o número de soluções e $\eta(\det(\mathbb{M}_f)) = \eta(\det(\mathbb{M}_{a_1x_1^2+\cdots+a_nx_n^2}))$ pela equação (1.8),

basta mostrarmos o resultado para $a_1x_1^2 + \cdots + a_nx_n^2$, onde $a_i \neq 0$ para $i \in \{1, \ldots, n\}$. Seja $m = \frac{n}{2}$ temos pelos Lemas 1.12 e 1.13

$$\begin{aligned} N(a_1x_1^2 + \cdots + a_nx_n^2 = b) &= \sum_{c_1+\cdots+c_m=b} N(a_1x_1^2 + a_2x_2^2 = c_1) \cdots N(a_{n-1}x_{n-1}^2 + a_nx_n^2 = c_2) \\ &= \sum_{c_1+\cdots+c_m=b} [q + \nu(c_1)\eta(-a_1a_2)] \cdots [q + \nu(c_m)\eta(-a_{n-1}a_n)] \\ &= q^{m-1}q^m + \eta((-1)^m a_1 \cdots a_n) \sum_{c_1+\cdots+c_m=b} \nu(c_1) \cdots \nu(c_m) \\ &= q^{n-1} + \nu(b)q^{\frac{(n-2)}{2}}\eta((-1)^m a_1 \cdots a_n). \end{aligned}$$

□

Para obtermos o análogo para o caso em que q é par e n também precisamos do seguinte resultado:

Lema 1.15 *Sejam q par, a e $b \in \mathbb{F}_q$ com $tr(a) = 1$, onde o traço tr está definido de $\mathbb{F}_q$ sobre $\mathbb{F}_2$. Então*

$$N(x_1^2 + x_1x_2 + ax_2^2 = b) = q - \nu(b). \tag{1.13}$$

Demonstração:
Visto que x^2+x+a é irredutível em $\mathbb{F}_q$, pelo Corolário $A.16$, temos $x^2+x+a = (x+\alpha)(x+\alpha^q)$ com $\alpha \in \mathbb{F}_{q^2}$ e $\alpha \notin \mathbb{F}_q$ e também

$$f(x_1, x_2) = (x_1^2 + x_1x_2 + ax_2^2) = (x_1 + \alpha x_2)(x_1 + \alpha^q x_2).$$

Para cada $(c_1, c_2) \in \mathbb{F}_q^2$ obtemos que $f(c_1, c_2) = (c_1^2 + c_1x_2 + ac_2^2) = (c_1 + \alpha c_2)(c_1 + \alpha^q c_2) = (c_1 + \alpha c_2)^{q+1}$. Como $\{1, \alpha\}$ é uma base de $\mathbb{F}_{q^2}$ sobre $\mathbb{F}_q$ temos uma bijeção entre os pares ordenados (c_1, c_2) com os elementos $\gamma = c_1 + \alpha c_2 \in \mathbb{F}_{q^2}$. Portanto $N(f(x_1, x_2) = b)$ é iqual ao número de $\gamma \in \mathbb{F}_{q^2}$ tais que $\gamma^{q+1} = b$. Logo

$$N(f(x_1, x_2) = 0) = 1 = q - \nu(0)$$

Seja $b \neq 0$, como $\mathbb{F}_{q^2}^*$ é cíclico e $b^{\frac{(q^2-1)}{(q+1)}} = b^{q-1} = 1$, temos $q + 1$ elementos $\gamma \in \mathbb{F}_{q^2}$ com $\gamma^{q+1} = b$. Portanto $N(f(x_1, x_2) = b) = q + 1 = q - \nu(b)$.

□

Já tinhamos observado que $N(f(x_1,\ldots,x_n)=b)$, f forma quadrática sobre $\mathbb{F}_q$, é invariante por equivalência. Então para determinarmos $N(f(x_1,\ldots,x_n)=b)$ quando n e q são pares basta restringirmos nossa atenção ao caso do Teorema 1.11 e considerar o caso $f(x_1,\ldots,x_n)=a_1x_1^2+\cdots+a_nx_n^2$ pois esta forma é equivalente à forma x_n^2, quando q é par, e este caso não é coberto pelo Teorema 1.11.

Primeiro vamos considerar o caso mais simples:

Teorema 1.16 *Seja $b\in\mathbb{F}_q$. Se $q=2^m$ o número de soluções da equação*

$$a_1x_1^2+\cdots+a_nx_n^2=b,$$

em $\mathbb{F}_{q^n}$, chamada de equação diagonal, é dado por q^{n-1}.

Demonstração:
Primeiro veja que $a\mapsto a^2$ é um automorfismo em $\mathbb{F}_q$. Logo $a_nx^2=b$, $b\in\mathbb{F}_q$, possui somente uma solução em $\mathbb{F}_q$. Como

$$a_1x_1^2+\cdots+a_nx_n^2\sim x_n^2$$

temos que

$$N(a_1x_1^2+\cdots+a_nx_n^2=b)=q^{n-1}N(x_n^2=b)=q^{n-1}.$$

□

Teorema 1.17 *Seja $b\in\mathbb{F}_q$ com q e n pares. Então o número de soluções da equação $x_1x_2+x_3x_4+\cdots+x_{n-1}x_n=b$ em $\mathbb{F}_q^n$ é*

$$q^{n-1}+\nu(b)q^{\frac{(n-2)}{2}} \tag{1.14}$$

e o da equação $x_1x_2+x_3x_4+\cdots+x_{n-1}x_n+x_{n-1}^2+ax_n^2=b$ em $\mathbb{F}_q^n$ é

$$q^{n-1}-\nu(b)q^{\frac{(n-2)}{2}} \tag{1.15}$$

onde $a\in\mathbb{F}_q$ com $tr(a)=1$, sendo tr definido em $\mathbb{F}_q$ sobre $\mathbb{F}_2$.

Demonstração:
Consideremos inicialmente $n=2$. Observe que $N(x_1x_2=b)=q-1$ se $b\neq 0$ e

$N(x_1x_2 = b) = 2q - 1$ se $b = 0$, logo $N(x_1x_2 = b) = q + \nu(b)$ para todo $b \in \mathbb{F}_q$. Seja agora $n \geq 2$ e seja $m = \frac{n}{2}$, tome $c_1, \ldots, c_m \in \mathbb{F}_q$ tais que

$$\begin{aligned} N(x_1x_2 + \cdots + x_{n+1}x_n = b) &= \sum_{c_1+\cdots+c_m=b} N(x_1x_2 = c_1) \cdots N(x_{n-1}x_n = c_m) \\ &= \sum_{c_1+\cdots+c_m=b} [q + \nu(c_1)] \cdots [q + \nu(c_m)] \\ &= q^{m-1}q^m + \sum_{c_1+\cdots+c_m=b} \nu(c_1) \cdots \nu(c_m) \\ &= q^{n-1} + \nu(b)q^{\frac{(n-2)}{2}}. \end{aligned}$$

A última igualdade segue do Lema 1.12.

No caso restante se $n = 2$ basta usar o Lema 1.15. Seja $n \geq 4$ vamos usar o Lema 1.15 e o resultado já provado. Considere $c_1, c_2 \in \mathbb{F}_q$ tais que

$$\begin{aligned} &N(x_1x_2 + x_3x_4 + \cdots + x_{n-1}x_n + x_{n-1}^2 + ax_n^2 = b) \\ &= \sum_{c_1+c_2=b} N(x_1x_2 + x_3x_4 + \cdots + x_{n-3}x_{n-2} = c_1) \cdot N(x_{n-1}x_n + x_{n-1}^2 + ax_n^2 = c_2) \\ &= \sum_{c_1+c_2=b} [q^{n-3} + \nu(c_1)q^{\frac{(n-4)}{2}}][q - \nu(c_2)] \\ &= q^{n-1} + q^{\frac{(n-2)}{2}} \sum_{c_1 \in \mathbb{F}_q} \nu(c_1) - q^{n-3} \sum_{c_2 \in \mathbb{F}_q} \nu(c_2) - q^{\frac{(n-4)}{2}} \sum_{c_1+c_2 \in \mathbb{F}_q} \nu(c_1)\nu(c_2) \\ &= q^{n-1} - \nu(b)q^{\frac{(n-2)}{2}} \end{aligned}$$

A última igualdade é verdadeira pelo Lema 1.12. □

Portanto dado $f \in \mathbb{F}_q[x_1, \ldots, x_n]$ uma forma quadrática e $b \in \mathbb{F}_q$, a partir dos Teoremas 1.14 e 1.17, podemos determinar $N(f(x_1, \ldots, x_n) = b)$ para f não degenerada e n par. Também, a partir do Teorema 1.16 conseguimos determinar $N(f(x_1, \ldots, x_n) = b)$ quando f é diagonal e q é par.

No caso geral, quando n é par e f é degenerada, basta considerarmos g forma quadrática não degenerada equivalente a f e ultilizando os Teoremas 1.14 e 1.17 determinar $N(g(x_1, \ldots, x_k) = b)$ em $\mathbb{F}_q$, onde k e é o número variáveis de g. Donde teremos que

$$N(f(x_1, \ldots, x_n) = b) = q^{n-k}N(g(x_1, \ldots, x_k) = b)$$

em $\mathbb{F}_q^k$.

Como estamos interessados no número de soluções em $\mathbb{F}_q^n$, temos que multiplicar $N(g(x_1,\ldots,x_k) = b)$, número de soluções em $\mathbb{F}_q^k$, por q^{n-k}, onde $v = n-k$ é justamente a dimensão do núcleo da forma bilinear associada a f, pelo Teorema 1.6. Em resumo obtemos

Teorema 1.18 *Seja $f \in \mathbb{F}_q[x_1,\ldots,x_k]$ uma forma quadrática, B_f sua forma bilinear associada, v a dimensão do núcleo de B_f e N_b o número de soluções em $\mathbb{F}_q^k$ de $f(x_1,\ldots,x_k) = b$, com $b \in \mathbb{F}_q$. Se $k = 2t$ e $v = 2s$ então existe $D \in \{-1,0,1\}$ tal que*

$$N_0 = q^{2t-1} + Dq^{t+s-1}(q-1), \text{ e } N_b = q^{2t-1} - Dq^{t+s-1} \text{ quando } b \neq 0.$$

CAPÍTULO 2

Número de Soluções de uma Curva Algébrica

Neste capítulo iremos apresentar uma fórmula para o número de soluções da curva algébrica plana, sobre $\mathbb{F}_{q^k}$, definida pela equação $y^q - y = ax^s + b$ onde $a \in \mathbb{F}_{q^k}^*$, $b \in \mathbb{F}_{q^k}$, $s, k \in \mathbb{N}$ e k é número par.

Como conseqüência, deste resultado, obtemos exemplos de curvas maximais, ou seja, curvas planas cujo o número de pontos atingem a famosa cota de Weil.

As curvas maximais desempenham importante papel em Teoria dos Códigos. Também são amplamente estudadas em Teoria dos Números e Geometria Finita.

Vamos denotar por tr a função traço de $\mathbb{F}_{q^k}$ sobre $\mathbb{F}_q$.

2.1 Teorema Principal

Nesta seção vamos determinar o número de soluções da equação $y^q - y = ax^s + b$, sobre $\mathbb{F}_{q^k}$, para determinados inteiros s. A prova do resultado, sobre tal números de soluções, que apresentamos aqui é devido a J. Wolfmann e pode ser visto em [5].

Iniciamos com dois lemas que irão auxiliar na obtenção do resultado principal, e vamos concluir com outro resultado sobre número de soluções de uma equação. Na verdade é a etapa principal na demonstração do Teorema 2.3, que é o principal resultado deste capítulo, e devido a sua importâcia destacamos como um corolário.

Lema 2.1 *Se q é ímpar e $k = 2rh$ com r, h números naturais, então $m = \frac{q^k-1}{q^{2r}-1}$ possui a mesma paridade de h.*

Demonstração:

Observe que

$$m = \frac{q^k-1}{q^{2r}-1} = \frac{q^{2rh}-1}{q^{2r}-1} \equiv_2 \left(\frac{y^h-1}{y-1}\right)^2$$

sendo $y = q^r$. Visto que $\frac{y^h-1}{y-1} = y^{h-1} + y^{h-2} + \cdots + y + 1$ temos

$$m \equiv_2 y^{h-1} + y^{h-2} + \cdots + y + 1.$$

E como $y^i = q^{ri} \equiv_2 1$ para todo i natural, pois q é ímpar, obtemos

$$m \equiv_2 \underbrace{1 + \cdots + 1}_{h-1} + 1.$$

Portanto $m \equiv_2 h$ como queríamos.

□

Lembramos, segundo as notações do Teorema 1.18, que $v = dim(Ker(B_f)$ e $D \in \{-1, 0, 1\}$, onde B_f é a forma bilinear associada a uma forma quadrática f.

Lema 2.2 *Sejam k, r, h números naturais tais que $k = 2rh$ e $a \in \mathbb{F}_{q^k}$ não nulo.*

(a) A função

$$\begin{array}{rccc} \phi_a & : & \mathbb{F}_{q^k} & \longrightarrow & \mathbb{F}_q \\ & & x & \longmapsto & tr(ax^{q^r+1}) \end{array}$$

é uma forma quadrática.

(b) Seja n natural tal que $n(q^r+1) = q^k - 1$. Sejam v e D os inteiros associados a ϕ_a pelo Teorema 1.18*, então:*

Se $a^n = (-1)^h$ então $v = 2r$ e $D = (-1)^{h+1}$.

Se $a^n \neq (-1)^h$ então $v = 0$ e $D = (-1)^h$.

Demonstração:

(a) Pelo Corolário 1.4 temos que ϕ_a é uma forma quadrática e

$$\phi_a(x+y) = \phi_a(x) + \phi_a(y) + tr(a(xy^{q^r} + x^{q^r}y)).$$

sendo $\varphi(x,y) := tr(a(xy^{q^r} + x^{q^r}y))$ uma forma bilinear simétrica.

(b) Vamos caracterizar o núcleo de φ. Como $tr(ax^{q^r}y) = tr(a^{q^{k-r}}xy^{q^{k-r}}))$ obtemos $\varphi(x,y) = tr(x(ay^{q^r} + a^{q^{k-r}}y^{q^{k-r}})$. Pelo Exemplo 1.7 a forma bilinear simétrica $(x,y) \mapsto tr(xy)$ é não degenerada, disto segue que φ é não degenerada. Portanto φ é uma forma bilinear simétrica e não degenerada, dsonde temos que o núcleo de φ é o conjunto das soluções de: $ay^{q^r} + a^{q^{k-r}}y^{q^{k-r}} = 0$. Elevando esta equação a q^r-ésima potência obtemos a seguinte equação equivalente:

(1) $a^{q^r}y^{q^{2r}} + ay = 0$.

Logo o núcleo de φ é igual ao núcleo da função linear $y \mapsto a^{q^r}y^{q^{2r}} + ay$ e os elementos não nulos do $\ker\varphi$ são soluções da equação :

(2) $(y^{-1})^{q^{2r-1}} = -a^{q^r-1}$.

Considere os seguintes inteiros $m = \frac{q^k-1}{q^{2r}-1}$ e $n = \frac{q^k-1}{q^r+1}$ (n foi definido no enunciado). Se elevarmos à potência m, a equação (2), teremos uma solução em $\mathbb{F}_q^k$ se, e somente se $(-a^{q^r-1})^m = 1$. Como

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

teremos solução se, e somente se $a^n = (-1)^m$.

Se q é ímpar, pelo Lema 2.1, a paridade de m é a mesma de h. Portanto, para cada q:

(i) Se $a^n = (-1)^h$ então $dim(ker\varphi) = 2r$

(ii)Se $a^n \neq (-1)^h$ então $dim(ker\varphi) = 0$

Falta determinarmos D. Para isto considere o subgrupo M de ordem $q^r + 1$ do grupo multiplicativo $\mathbb{F}_q^*$. O conjunto das soluções de $tr(ax^{q^r+1}) = \lambda$ em $\mathbb{F}_{q^k}$ com $\lambda \neq 0$, é a união das classes αM distintas tais que $\alpha \in \mathbb{F}_{q^k}$ é solução de $tr(ax^{q^r+1}) = \lambda$. De fato: se $\alpha \in \mathbb{F}_{q^k}$ é solução e $w \in M$ temos

$$tr(a(w\alpha)^{q^r+1}) = tr(aw^{q^r+1}\alpha^{q^r+1}) = tr(a1\alpha^{q^r+1}) = \lambda$$

e temos que $m\alpha$ também é solução para todo $m \in M$. E visto que $|M| = q^r + 1$ temos que o número de soluções de $tr(ax^{q^r+1}) = \lambda$ em $\mathbb{F}_{q^k}$ é um múltiplo de $q^r + 1$. Então de acordo com o Teorema 1.18

$$q^{2t-1} - Dq^{t+s-1} \equiv 0 \bmod (q^r + 1)$$

ou, de forma equivalente,

$$q^{2rh} - Dq^{rh+s} \equiv 0 \bmod (q^r + 1).$$

No caso (i), $s = r$, usando que $q^{ir} \equiv (-1)^i \bmod (q^r + 1)$ (isto se verifica facilmente por indução em n) nós temos $D(-1)^{h+1} - 1 \equiv 0 \bmod (q^r + 1)$ e a única solução é $D = (-1)^{h+1}$.

No caso (ii), $s = 0$ e usando novamente que $q^{ir} \equiv (-1)^i \bmod (q^r + 1)$ temos $D(-1)^h - 1 \equiv 0 \bmod (q^r + 1)$ e a única solução é $D = (-1)^h$. □

Agora estamos aptos a determinar o número de soluções da equação $y^q - y = ax^s + b$ e com isto determinar o número de pontos racionais da curva algébrica plana projetiva definida por ela, sobre $\mathbb{F}_{q^k}$.

Teorema 2.3 *Seja N o número de pontos racionais da curva algébrica plana projetiva definida, sobre $\mathbb{F}_{q^k}$, pela equação $y^q - y = ax^s + b$, $a \in \mathbb{F}_{q^k}^*$, $b \in \mathbb{F}_{q^k}$ e s um número inteiro positivo. Assuma $k = 2t$ e s um divisor de $q^k - 1$. Seja n tal que $ns = q^k - 1$. Se existir um divisor r de t, $r \geq 1$, tal que $q^r \equiv -1 \bmod s$ então N é dado por uma das seguintes igualdades:*

(1) Se $a^n = \varepsilon_1$ e $tr(b) = 0$ então : $N = q^{2t} + 1 - \varepsilon(q-1)(s-1)q^t$

(2) Se $a^n = \varepsilon_1$ e $tr(b) \neq 0$ então : $N = q^{2t} + 1 + \varepsilon(s-1)q^t$

(3) Se $a^n \neq \varepsilon_1$ e $tr(b) = 0$ então : $N = q^{2t} + 1 + \varepsilon(q-1)q^t$

(4) Se $a^n \neq \varepsilon_1$ e $tr(b) \neq 0$ então : $N = q^{2t} + 1 - \varepsilon q^t$

onde $tr : \mathbb{F}_{q^k} \longrightarrow \mathbb{F}_q$, $\varepsilon = (-1)^{\frac{t}{r}}$, $\varepsilon_1 = \varepsilon^u$ e u é tal que $us = q^r + 1$.

Demonstração:

Seja C a curva algébrica plana projetiva, sobre $\mathbb{F}_{q^k}$, definida por

$$y^q - y = ax^s + b \text{ com } a, b \in \mathbb{F}_{q^k}^* \text{ e } s \in \mathbb{N} \tag{2.1}$$

e N o número de pontos racionais de C sobre $\mathbb{F}_{q^k}$. É fácil ver que C possui um único ponto no infinito e este ponto é racional. Agora para determinarmos N vamos considerar a seguinte equação sobre $\mathbb{F}_{q^k}$:

$$tr(ax^s + b) = 0, \tag{2.2}$$

sendo $tr : \mathbb{F}_{q^k} \longrightarrow \mathbb{F}_q$.
Seja $\tilde{N}$ o número de soluções de 2.2 em $\mathbb{F}_q^k$. Defina a função

$$\begin{array}{rccc} \theta & : & \mathbb{F}_{q^k} & \longrightarrow & \mathbb{F}_{q^k} \\ & & y & \longmapsto & y^q - y. \end{array}$$

Claramente θ é uma transformação $\mathbb{F}_q$-linear, com $Ker(\theta) = \mathbb{F}_q$. Donde $dim(Im\theta) = k - 1$ e como $tr(\theta(y)) = 0$ para cada $y \in \mathbb{F}_{q^k}$(Teorema $A.12$) temos que $Im(\theta)$ é exatamente o hiperplano dos elementos cujo traço é zero em $\mathbb{F}_{q^k}$. Logo (x, y) é solução de 2.1 se, e somente se, x é solução de 2.2. Agora para cada x, solução de 2.2 existem exatamente q elementos y tal que (x, y) é solução de 2.1. Somando o ponto no infinito de C, obtemos:

$$N = q\tilde{N} + 1$$

Portanto para determinarmos N, visto que o traço é linear e por 2.2, precisamos conhecer, para cada $\lambda \in \mathbb{F}_q$, o número de soluções em $\mathbb{F}_{q^k}$ da equação :

$$tr(ax^s) = \lambda \tag{2.3}$$

Lembramos que $k = 2t$, $ns = q^k - 1$ e que existe r divisor de t tal que $t = rh$, $r \geq 1$, com $q^r \equiv -1 \bmod s$. Vamos dividir o cálculo de $\tilde{N}$ em três casos em função de s.

O caso $s = 1$ é conseqüência imediata de 2.3.

O caso $s = q^r + 1$ é conseqüência imediata do Lema 2.2 e do Teorema 1.18.

O caso restante, $s \neq 1$, $s \neq q^r + 1$, é o mais trabalhoso. Para determinarmos $\tilde{N}$, nesta situação, primeiro observe que $q^r + 1$ divide $q^k - 1$. Agora vamos considerar os seguintes subgrupos cíclicos de $\mathbb{F}_{q^k}^*$:
G o subgrupo de ordem n de $\mathbb{F}_{q^k}^*$ e G' o subgrupo de ordem $n' = \frac{q^k-1}{q^r+1}$ de $\mathbb{F}_{q^k}^*$. Visto que

$\mathbb{F}_{q^k}^* =< \alpha >$, onde $|\alpha| = q^k - 1$, temos $G =< \alpha^s >$ e $G' =< \alpha^{q^r+1} >$. Como s divide $q^r + 1$, segue que G' é subgrupo de G. E como G é abeliano tome $\{a_i G'\}_{i \in I}$ o conjunto das classes modulo G' em G, onde $I = \{1, 2, \ldots, m\}$ com $m = \frac{n}{n'} = \frac{q^r+1}{s}$, sendo os a_i representantes distintos de cada classe.

Seja

$$H(\lambda) = \{x \in \mathbb{F}_{q^k} : tr(x) = \lambda\}$$

e

$$H_i(\lambda) = \{x \in \mathbb{F}_{q^k} : tr(aa_i x^{q^r+1}) = \lambda\}$$

com $N_i = \#H_i(\lambda)$.

Observe que se $x \in H(\lambda) \cap (aa_i G')$ temos que $x = aa_i g'$, com $g' \in G'$ e $tr(aa_i g') = \lambda$. Como $g' = \alpha^{j(q^r+1)}$ segue que $x \in H_i(\lambda)$. Agora para cada elemento em $H(\lambda) \cap (aa_i G')$ temos $q^r + 1$ elementos em $H_i(\lambda)$. Donde temos a seguinte relação:

$$(q^r + 1) \mid H(\lambda) \cap (aa_i G') \mid = N_i.$$

Donde temos:

$$(q^r + 1) \mid H(\lambda) \cap (aG) \mid = \sum_i^m N_i,$$

e de forma análoga

$$\tilde{N} = s \mid H(\lambda) \cap (aG) \mid$$

onde $\tilde{N}$ é número de soluções da equação 2.3.

Logo

$$\tilde{N} = \frac{s}{q^r + 1} \sum_{i=1}^{m} N_i.$$

Portanto para determinarmos $\tilde{N}$ precisamos determinar os N_i. Pelo Lema 2.2 cada N_i pode assumir dois valores dependendo se $(aa_i)^{n'} = (-1)^h$ ou $(aa_i)^{n'} \neq (-1)^h$. Suponha:

$$(aa_i)^{n'} = (-1)^h, a \in \mathbb{F}_{q^k}^*. \tag{2.4}$$

Primeiro caso: q par ou h par.

A condição 2.4 é equivalente a $(aa_i)^{n'} = 1$, ou seja $aa_i \in G'$. Mas isto se verifica se, e somente se, $a_i \equiv a^{-1} \bmod G'$. Mas existe exatamente uma solução se $a \in G$ o que significa

que $a^n = 1$ e não tem solução caso contrário.

Segundo caso: q e h ímpares.

Seja α a raíz primitiva de $\mathbb{F}_{q^k}$ e seja u tal que $us = q^r + 1$. Temos agora que a equação 2.4 é equivalente a $(aa_i)^{n'} = -1$. Visto que q é ímpar a equação $x^{n'} = -1$ admite $\alpha^{\frac{q^r+1}{2}}$ como solução e portanto o conjunto completo das soluções é $(\alpha^{\frac{q^r+1}{2}})G' = (\alpha^{\frac{us}{2}})G'$. Portanto 2.4 é equivalente a $(\alpha^{\frac{-us}{2}})a_i \in G'$ que é verdade se, e somente se, $(\alpha^{\frac{-us}{2}})a \in G$ e $a_i \equiv (\alpha^{\frac{us}{2}})a^{-1} \bmod G'$. Existe exatamente uma solução se, e somente se, $(\alpha^{\frac{-us}{2}})a \in G$ o que significa $(\alpha^{\frac{-us}{2}})^n a^n = (\alpha^{\frac{-sn}{2}})^u a^n = 1$ ou, de forma equivalente $a^n = (-1)^u$. Não existe solução caso contrário.

Donde podemos resumir os dois casos do seguinte modo: se $a \in \mathbb{F}_{q^k}^*$ e $us = q^r + 1$ então existe $i \in I$ tal que $aa_i^n = (-1)^h$ se, e somente se, $a^n = (-1)^{uh}$ e desta forma a_i é único.

Agora estamos em condições de calcular $\tilde{N}$, ou seja, o número de soluções de 2.2.

a) Se $a^n \neq (-1)^{uh}$:

Para cada $i : (aa_i)^{n'} \neq (-1)^h$ e $N_i = S(\lambda)$ com $v = 0$ e $D = (-1)^h$ (notações do Lema 2.2). Portanto

$$\tilde{N} = \frac{s}{q^r+1}(\frac{q^r+1}{s})S(\lambda) = S(\lambda).$$

b) Se $a^n = (-1)^{uh}$:

Existe somente um $i \in I$ tal que $(aa_i)^{n'} = (-1)^h$. Portanto

$$\tilde{N} = \frac{s}{q^r+1}[(\frac{q^r+1}{s} - 1)S^1(\lambda) + S^2(\lambda)]$$

onde $S^1(\lambda)$ é o número obtido no Lema 2.2 com $v = 0$, $D = (-1)^h$ e $S^2(\lambda)$ é obtido com $v = 2r$, $D = (-1)^{h+1}$. Nos encontramos o resultado do teorema considerando dois casos $\lambda = 0$ e $\lambda \neq 0$, isto é considerando $tr(b) = 0$ e $tr(b) \neq 0$, e usando $N = q\tilde{N} + 1$.

□

Nas mesmas hipóteses do Teorema 2.3 obtemos o seguinte corolário:

Corolário 2.4 *O número $N(a,b)$ de soluções em $\mathbb{F}_{q^k}$ da equação*

$$tr(ax^s + b) = 0$$

é dado por:

(1) Se $a^n = \varepsilon_1$ e $tr(b) = 0$ então : $N(a,b) = q^{2t-1} - \varepsilon(q-1)(s-1)q^{t-1}$

(2) Se $a^n = \varepsilon_1$ e $tr(b) \neq 0$ então : $N(a,b) = q^{2t-1} + \varepsilon(s-1)q^{t-1}$

(3) Se $a^n \neq \varepsilon_1$ e $tr(b) = 0$ então : $N(a,b) = q^{2t-1} + \varepsilon(q-1)q^{t-1}$

(4) Se $a^n \neq \varepsilon_1$ e $tr(b) \neq 0$ então : $N(a,b) = q^{2t-1} - \varepsilon q^{t-1}$

onde $\varepsilon = (-1)^{\frac{t}{r}}$, $\varepsilon_1 = \varepsilon^u$ e u é tal que $us = q^r + 1$.

Demonstração: Decorre diretamente da demostração do Teorema 2.3. □

2.2 Exemplos de Curvas Maximais

Nesta seção utilizamos o número de soluções da curva algébrica plana definida pela equação $y^q - y = ax^s + b$ sobre $\mathbb{F}_{q^k}$, dado pelo Teorema 2.3, para obtermos exemplos de curvas que atingem a cota de Weil.

Seja C uma curva algébrica plana (estamos supondo C absolutamente irredutível) sobre $\mathbb{F}_{q^k}$, vamos denotar por g o seu gênero. O gênero é um invariante associado à curva C, sua definição e propriedades podem ser vistas em [9], nestas notas basta sabermos que g é um número natural.

Seja $N(C)$ o número de pontos racionais da curva C. É um resultado bem conhecido devido a A. Weil que

$$q^k + 1 - 2gq^{\frac{k}{2}} \leq N(C) \leq q^k + 1 + 2gq^{\frac{k}{2}}$$

Estas cotas para $N(C)$ são conhecidas como cotas de Weil. A demonstração deste resultado pode ser vista em [9].

Definição 2.1 (Curva Maximal)

Seja C uma curva algébrica plana sobre $\mathbb{F}_{q^k}$, g seu gênero e $N(C)$ o número de seus pontos racionais. Se

$$N(C) = q^k + 1 + 2gq^{\frac{k}{2}}$$

então C é dita ser maximal. □

Observe que para termos uma curva maximal sobre $\mathbb{F}_{q^k}$ necessariamente devemos ter k par. Vejamos agora um exemplo clássico de uma curva maximal. A curva em questão é conhecida como Curva de Hermite.

EXEMPLO 2.1 *Considere a curva algébrica plana projetiva C associada ao polinômio*

$$f(x,y) = y^q + y - x^{1+q} \in \mathbb{F}_{q^2}[x,y].$$

Veja que $f^*(x,y,z) = zy^q + z^q y - x^{1+q}$ e então $d = gr(f^*) = q+1$. O gênero g de C é dado por $g = \frac{(d-1)(d-2)}{2}$, onde d é o grau de $f^*(x,y,z)$, neste caso temos $g = \frac{q(q-1)}{2}$. Para determinarmos a cardinalidade de $C(\mathbb{F}_{q^2})$ primeiro vamos contar o conjunto dos pontos no plano afim

$$\begin{aligned} C_a(\mathbb{F}_{q^2}) &= \{(x,y) \in \mathbb{F}_{q^2} \times \mathbb{F}_{q^2} : f(x,y) = 0\} \\ &= \{(x,y) \in \mathbb{F}_{q^2} \times \mathbb{F}_{q^2} : tr(y) = \mathcal{N}(x)\} \end{aligned}$$

onde tr e $\mathcal{N}$, função traço e função norma respctivamente, estão definidas em $\mathbb{F}_{q^2}$ sobre $\mathbb{F}_q$.

Como o traço é sobrejetivo temos $\#tr^{-1}(y) = q$. Logo

$$\begin{aligned} \#C_a(\mathbb{F}_{q^2}) &= \sum_{x \in \mathbb{F}_{q^2}} \#\{y \in \mathbb{F}_{q^2} : tr(y) = x^{1+q}\} \\ &= \sum_{x \in \mathbb{F}_{q^2}} \#tr^{-1}(x^{1+q}) \\ &= \sum_{x \in \mathbb{F}_{q^2}} q = qq^2 = q^3. \end{aligned}$$

Como C possui um único ponto no infinito temos que $\#C(\mathbb{F}_{q^2}) = q^3 + 1$. A cota de Weil neste caso é $q^2 + 1 + 2(\frac{q(q-1)}{2})q = q^2 + 1 + q^3 - q^2 = q^3 + 1$. Portanto a Curva de Hermite atinge a cota de Weil. ♢

Observação 2.1 *Veja que quando q é par o Exemplo acima decorre diretamente do Teorema 2.3. De fato: considere a curva algébrica projetiva definida, sobre $\mathbb{F}_{q^2}$, pela equação*

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

Onde fizemos $a = 1$, $b = 0$, $k = 2$, $t = 1 = r$ *e* $s = q + 1$ *na equação* 2.1 *do Teorema* 2.3. *Como* $q^2 - 1 = (q+1)(q-1)$ *temos que* s *divide* $q^2 - 1$ *e claramente* s *divide* $q+1$. *Portanto pelo item* (1) *do Teorema* 2.3

$$N = q^2 + 1 + (q-1)(q)q = q^3 + 1 = \#C_a(\mathbb{F}_{q^2}).$$

Agora, como nesta observação, vamos aplicar o Teorema 2.3 para obter outros exemplos de curvas maximais. Para isto vamos utilizar que o gênero g da curva algébrica plana projetiva dada pela equação $y^q - y = ax^s + b$ sobre $\mathbb{F}_{q^k}$ é $g = \frac{(q-1)(s-1)}{2}$. Este resultado pode ser visto em [9].

Corolário 2.5 *Sejam* t, r, s, g *números naturais, diferentes de zero, tais que:* r *divide* t, $q^{2t} - 1 = ns$, $q^r + 1 = us$ *e* $g = \frac{(q-1)(s-1)}{2}$, *ou seja, como no Teorema* 2.3.

(i) Se $\frac{t}{r}$ *é par então existem curvas tais que*
$N(C) = q^k + 1 - 2gq^{\frac{k}{2}}$;

(ii) Se os números q, $\frac{t}{r}$, u *são todos ímpares então existem curvas tais que*
$N(C) = q^k + 1 + 2gq^{\frac{k}{2}}$;

onde $N(C)$ *é o número de pontos racionais da curva sobre* $\mathbb{F}_{q^k}$ *de gênero* g, *sendo* $k = 2t$.

Demonstração:
(i) Sendo $\frac{t}{r}$ par é imediato que $\varepsilon = (-1)^{\frac{t}{r}} = 1$ e logo $\varepsilon_1 = \varepsilon^u = 1$. Tome $a = 1$ e temos $a^n = \varepsilon_1$.
Agora considere a seguinte curva, sobre $\mathbb{F}_{q^{2t}}$,

$$y^q - y = x^s + b$$

onde $tr(b) = 0$. Temos pela primeira igualdade do Teorema 2.3 que

$$N(C) = N = q^{2t} + 1 - (q-1)(s-1)q^t = q^{2t} + 1 - 2gq^t.$$

(ii) Sendo q, $\frac{t}{r}$, u todos ímpares temos $\varepsilon = -1$ e $\varepsilon_1 = -1$. Como $q^r + 1 = us$ temos s par pois u é ímpar e $q^r + 1$ é par. Seja α um gerador do grupo cíclico $\mathbb{F}_{q^k}^*$, tome $a = \alpha^{\frac{s}{2}}$.

Veja que $a^n = \alpha^{\frac{ns}{2}} = \alpha^{\frac{q^k-1}{2}}$. Como $(\alpha^{\frac{q^k-1}{2}})^2 = \alpha^{q^r-1} = 1$ e $\alpha^{\frac{q^k-1}{2}} \neq 1$ temos $\alpha^{\frac{q^k-1}{2}} = -1$. Logo $a^n = -1 = \varepsilon_1$.
Agora considere a seguinte curva, sobre $\mathbb{F}_{q^{2t}}$,

$$y^q - y = ax^s + b$$

onde $tr(b) = 0$. Temos pela primeira igualdade do Teorema 2.3 que

$$N(C) = N = q^{2t} + 1 + (q-1)(s-1)q^t = q^{2t} + 1 + 2gq^t.$$

□

EXEMPLO 2.2 *Seja C a curva algébrica plana dada por*

$$y^3 - y = x^4$$

sobre $\mathbb{F}_{3^{20}}$.
Sendo $q = 3$, $s = 4$, $2t = 20$ e $r = 5$ temos $q^{2t} - 1 = 3^{20} - 1 = 4(871.696.100)$, $q^r - 1 = 3^5 + 1 = 4(61)$ e $g = \frac{(q-1)(s-1)}{2} = \frac{(3-1)(4-1)}{2} = 3$. Como $\frac{t}{r} = \frac{10}{5} = 2$ segue pelo Corolário 2.5 que

$$N(C) = q^{2t} + 1 - 2gq^t = 3^{20} + 1 - 6(3^{10}) = 3.486.430.108$$

♢

Corolário 2.6 *Sejam g e r inteiros, $g \geq 0$, $r \geq 1$, tais que $2^r \equiv -1 \bmod (2g+1)$ então para todo inteiro par v, $v > 1$, e cada $q = 2^{2rv}$ existem curvas que satisfazem:*
$N(C) = q + 1 + 2g\sqrt{q}$ e $N(C) = q + 1 - 2g\sqrt{q}$.

Demonstração:
Seja $t = rv$, $k = 2t$ e $s = 2g + 1$. Como $2^r \equiv -1 \bmod s$ temos $2^{2rv} = 1 \bmod s$. Tome n e u tais que $ns = 2^{2rv} - 1$ e $us = 2^r + 1$. Como v é par temos $\varepsilon = (-1)^{\frac{t}{r}} = (-1)^v = 1$ e logo $\varepsilon_1 = \varepsilon^u = 1$. Tome $a = 1$ e temos $a^n = \varepsilon_1$.
Agora considere a seguinte curva, sobre $\mathbb{F}_{2^{2t}}$,

$$y^2 - y = x^s + b$$

onde $tr(b) = 0$. Temos pela primeira igualdade do Teorema 2.3 que

$$N(C) = N = 2^{2t} + 1 - (2-1)(2g+1-1)2^t = 2^{2t} + 1 - 2g2^t = q + 1 - 2g\sqrt{q}.$$

Considere a mesma curva com $b \in \mathbb{F}_{2^{2t}}$ tal que $tr(b) \neq 0$ e temos pela segunda igualdade do Teorema 2.3 que

$$N(C) = N = 2^{2t} + 1 + (2-1)(s-1)2^t = 2^{2t} + 1 + 2g2^t = q + 1 + 2g\sqrt{q}.$$

□

EXEMPLO 2.3 *Seja C a curva algébrica plana dada por*

$$y^2 - y = x^{11}$$

sobre $\mathbb{F}_{2^{60}}$.
Sendo $q = 2$, $s = 11$, $2t = 60$, $r = 5$, $g = 5$ e $v = 6$.
Como $2^5 + 1 = 3(11)$ e $11 = 2g + 1$ temos que $2^r \equiv -1 \bmod (2g+1)$. Portanto pelo Corolário 2.6

$$N(C) = 2^{2t} + 1 - 2g2^{\frac{k}{2}} = 2^{60} + 1 - 10(2^{30}) = 2^{31}(2^{29} - 5) + 1$$

♢

Corolário 2.7 *Se q é ímpar e $g = \frac{q-1}{2}$, $k = 2t$, $t = rv$, u e n inteiros satisfazendo as hipóteses do Teorema 2.3. Então para cada inteiro $t \geq 1$ existem curvas satisfazendo $N(C) = q^k + 1 + 2gq^{\frac{k}{2}}$ e $N(C) = q^k + 1 - 2gq^{\frac{k}{2}}$.*

Demonstração:
Vamos considerar dois casos:
(i) t par.
Neste caso faça $r = 2$ e temos $t = 2v$. Se v for par temos que $\varepsilon = (-1)^{\frac{t}{r}} = (-1)^v = 1$ e logo $\varepsilon_1 = \varepsilon^u = 1$. Tome $a = 1$ e temos $a^n = \varepsilon_1$. Agora considere a seguinte curva, sobre $\mathbb{F}_{q^{2t}}$,

$$y^q - y = x^2 + b$$

onde $tr(b) = 0$. Segue pela primeira igualdade do Teorema 2.3 que

$$N(C) = N = q^{2t} + 1 - (q-1)(2-1)q^t = q^{2t} + 1 - 2gq^t = q^k + 1 - 2gq^{\frac{k}{2}}.$$

Se v for ímpar temos $\varepsilon = (-1)^v = -1$ e $\varepsilon_1 = \varepsilon^u = (-1)^u$. Supondo u ímpar temos $\varepsilon_1 = -1$. Tome $a = 1$ e temos $a^n \neq \varepsilon_1$. Agora considere a seguinte curva, sobre $\mathbb{F}_{q^{2t}}$,

$$y^q - y = x^2 + b$$

onde $tr(b) = 0$. Pela terceira igualdade do Teorema 2.3

$$N(C) = N = q^{2t} + 1 - (q-1)(2-1)q^t = q^{2t} + 1 - 2gq^t = q^k + 1 - 2gq^{\frac{k}{2}}.$$

Supondo u par temos que $\varepsilon = -1$ e $\varepsilon_1 = 1$. Tome $a = 1$ e temos $a^n = \varepsilon_1$. Agora considere a seguinte curva, sobre $\mathbb{F}_{q^{2t}}$,

$$y^q - y = x^2 + b$$

onde $tr(b) = 0$. Pela primeira igualdade do Teorema 2.3

$$N(C) = N = q^{2t} + 1 + (q-1)(2-1)q^t = q^{2t} + 1 + 2gq^t = q^k + 1 + 2gq^{\frac{k}{2}}.$$

(ii) t é ímpar.

Faça $r = 1$ e temos $t = v$, logo v é ímpar. Portanto $\varepsilon = -1$ e $\varepsilon_1 = (-1)^u$. Se u for par temos $\varepsilon_1 = 1$. Tome $a = 1$ e temos $a^n = \varepsilon_1$. Agora considere a seguinte curva, sobre $\mathbb{F}_{q^{2t}}$,

$$y^q - y = x^2 + b$$

onde $tr(b) = 0$. Pela primeira igualdade do Teorema 2.3

$$N(C) = N = q^{2t} + 1 + (q-1)(2-1)q^t = q^{2t} + 1 + 2gq^t = q^k + 1 + 2gq^{\frac{k}{2}}.$$

Se u for ímpar temos $\varepsilon_1 = -1$. Tome $a = 1$ e temos $a^n \neq \varepsilon_1$. Agora considere a seguinte curva, sobre $\mathbb{F}_{q^{2t}}$,

$$y^q - y = x^2 + b$$

onde $tr(b) = 0$. Pela terceira igualdade do Teorema 2.3

$$N(C) = N = q^{2t} + 1 - (q-1)(2-1)q^t = q^{2t} + 1 - 2gq^t = q^k + 1 - 2gq^{\frac{k}{2}}.$$

□

EXEMPLO 2.4 *Seja C a curva algébrica plana dada por*

$$y^5 - y = x^2$$

sobre $\mathbb{F}_{5^6}$.

Onde $q = 5$, $k = 2t = 6$ e $s = 2$. Logo $t = 3$, $r = 1$, e $g = \frac{(q-1)(s-1)}{2} = \frac{5-1}{2} = 2$. Veja que

$$q^{2t} - 1 = 5^6 - 1 = 15.624 = 2(7.812) = sn,$$

$$q^r - 1 = 5 + 1 = 2(3) = su.$$

Como v e u são ímpares temos pelo Corolário 2.7 que

$$N(C) = q^{2t} + 1 - 2gq^t = 5^6 + 1 - 4(5^3) = 15.126$$

$\diamondsuit$

CAPÍTULO 3

Número de Soluções de Certas Equações Diagonais

Neste capítulo vamos considerar, sobre $\mathbb{F}_q$, equações da forma

$$a_1 x_1^{d_1} + a_2 x_2^{d_2} + \cdots + a_s x_s^{d_s} = b$$

onde $a_1, a_2, \ldots, a_s$ estão em $\mathbb{F}_q^*$, b em $\mathbb{F}_q$, e os $d_1, d_2, \ldots, d_s$ são inteiros positivos. Quando temos $d_1 = d_2 = \cdots = d_s$ podemos determinar o número de soluções, desta equação, em certos casos. Como conseqüência vamos obter exemplos de variedades projetivas cujo número de soluções atinge a cota de Weil-Deligne.

3.1 Equações Diagonais com expoente constante

Estamos interessados no número de soluções de uma equação especial. Nesta seção vamos tratar deste caso especial. Para isto vamos precisar de um resultado bastante conhecido para o caractere aditivo de $\mathbb{F}_q$, e o outro sobre a soma de determinados caracteres.

Mas primeiro vamos definir precisamente uma equação diagonal:

Definição 3.1 (Equações Diagonais)

Uma equação diagonal sobre $\mathbb{F}_q$ é uma equação da forma

$$a_1x_1^{d_1} + a_2x_2^{d_2} + \cdots + a_sx_s^{d_s} = b$$

sendo $d_1, d_2, \ldots, d_s$ inteiros positivos, $a_1, a_2, \ldots, a_s$ em $\mathbb{F}_q^*$, e b em $\mathbb{F}_q$.
Quando $d_1 = d_2 = \cdots = d_s$ dizemos equação diagonal com expoente constante sobre $\mathbb{F}_q$.

□

Lema 3.1 *Seja s um inteiro maior ou igual que 1 e q uma potência do primo p. Considere ψ_a o caractere aditivo em $\mathbb{F}_q$ definido por $\psi_a(x) = e^{(\frac{2i\pi}{p})tr(ax)}$. Então temos*

$$\prod_{i=1}^{s}\sum_{x\in\mathbb{F}_q}\psi_a(a_ix^d) = \sum_{(x_1,\ldots,x_s)\in\mathbb{F}_q^s}\prod_{i=1}^{s}\psi_a(a_ix_i^d)$$

Demonstração:

Por indução em s. Para $s = 1$ é imediato. Suponha verdadeiro para todo $n < s$ verdadeira a hipótese. Então

$$\begin{aligned}
\prod_{i=1}^{s}\sum_{x\in\mathbb{F}_q}\psi_a(a_ix^d) &= \sum_{x\in\mathbb{F}_q}\psi_a(a_1x^d)\cdots\sum_{x\in\mathbb{F}_q}\psi_a(a_sx^d)\\
&= \sum_{x\in\mathbb{F}_q}\psi_a(a_sx^d)\prod_{i=1}^{s-1}\sum_{x\in\mathbb{F}_q}\psi_a(a_ix_i^d)\\
&\overset{(1)}{=} \sum_{x\in\mathbb{F}_q}\psi_a(a_sx^d)\sum_{(x_1,\ldots,x_{s-1})\in\mathbb{F}_q^{s-1}}\prod_{i=1}^{s-1}\psi_a(a_ix_i^d)\\
&= \sum_{x\in\mathbb{F}_q}\sum_{(x_1,\ldots,x_{s-1})\in\mathbb{F}_q^{s-1}}\psi_a(a_sx^d)\prod_{i=1}^{s-1}\psi_a(a_ix_i^d)\\
&= \sum_{x\in\mathbb{F}_q}\sum_{(x_1,\ldots,x_{s-1})\in\mathbb{F}_q^{s-1}}\prod_{i=1}^{s-1}\psi_a(a_ix_i^d)\psi_a(a_sx^d)\\
&= \sum_{(x_1,\ldots,x_s)\in\mathbb{F}_q^s}\prod_{i=1}^{s-1}\psi_a(a_ix_i^d)\psi_a(a_sx_s^d)\\
&= \sum_{(x_1,\ldots,x_s)\in\mathbb{F}_q^s}\prod_{i=1}^{s}\psi_a(a_ix_i^d)
\end{aligned}$$

onde a igualdade (1) é dada pela hipótese de indução e as outras igualdades são triviais.

□

Proposição 3.2 *Seja s um inteiro, $s \geq 2$, q uma potência do primo p, e $\mathbb{F}_q$ o corpo finito de ordem q. Considere ψ_a o caractere aditivo de $\mathbb{F}_q$ definido por $\psi_a(x) = e^{(\frac{2i\pi}{p})tr(ax)}$, onde tr denota o traço de $\mathbb{F}_q$ sobre $\mathbb{F}_p$. Se N é o número de soluções $(x_1, x_2, \ldots, x_s)$ em $\mathbb{F}_q^s$ da equação*

$$a_1x_1^d + a_2x_2^d + \cdots + a_sx_s^d = b$$

então

$$N = q^{-1} \sum_{a \in \mathbb{F}_q} \psi_a(-b) \prod_{i=1}^{s} S(aa_i)$$

onde $S(a) = \sum_{x \in \mathbb{F}_q} \psi_a(x^d)$.

Demonstração:

Defina

$$\begin{array}{rccc} F : & \mathbb{F}_q^s & \longrightarrow & \mathbb{F}_q \\ & (x_1, x_2, \ldots, x_s) & \longmapsto & a_1x_1^d + a_2x_2^d + \cdots + a_sx_s^d - b. \end{array}$$

Observe que $F(x_1, x_2, \ldots, x_s) = 0$ se, e somente se, $a_1x_1^d + a_2x_2^d + \cdots + a_sx_s^d = b$ tem solução.

Primeiro vamos verificar que

$$\sum_{a \in \mathbb{F}_q} \psi_a(F(x_1, x_2, \ldots, x_s)) = \begin{cases} q & \text{se} \quad F(x_1,x_2,\ldots,x_s) = 0 \\ \\ 0 & \text{se} \quad F(x_1,x_2,\ldots,x_s) \neq 0. \end{cases}$$

Quando $F(x_1, x_2, \ldots, x_s) = 0$ o resultado é imediato.

Suponha agora $F(x_1, x_2, \ldots, x_s) \neq 0$. Chame $u = F(x_1, x_2, \ldots, x_s) \neq 0$ e observe que

$$\psi_{a+c}(u) = \psi_a(u)\psi_c(u),$$

para todo $a, c \in \mathbb{F}_q$, pois o traço é linear. Tome $c \in \mathbb{F}_q$ e veja que

$$\sum_{a \in \mathbb{F}_q} \psi_a(u) = \sum_{a \in \mathbb{F}_q} \psi_{a+c}(u) = \psi_c(u) \sum_{a \in \mathbb{F}_q} \psi_a(u).$$

Agora se $\sum_{a\in\mathbb{F}_q}\psi_a(u)\neq 0$ vamos ter $\psi_c(u)=1$ para todo $c\in\mathbb{F}_q$ e então $e^{(\frac{2i\pi}{p})tr(uc)}=1$ para todo $c\in\mathbb{F}_q$. Portanto $tr(uc)=0$ para todo $c\in\mathbb{F}_q$ com $u\neq 0$, ou seja, o traço é zero para todo elemento de $\mathbb{F}_q$. Com isto temos um absurdo pois pelo Teorema A.10 o traço é sobrejetivo. Portanto $\sum_{a\in\mathbb{F}_q}\psi_a(u)=0$ se $F(x_1,x_2,\ldots,x_s)\neq 0$ como desejavamos.

Para concluírmos o resultado considere

$$S=\sum_{(x_1,x_2,\ldots,x_s)\in\mathbb{F}_q^s}\sum_{a\in\mathbb{F}_q}\psi_a(F(x_1,x_2,\ldots,x_s)).$$

Pela observação anterior temos $S=qN$. Portanto

$$\begin{aligned}\sum_{(x_1,x_2,\ldots,x_s)\in\mathbb{F}_q^s}\sum_{a\in\mathbb{F}_q}\psi_a(F(x_1,x_2,\ldots,x_s)) &= \sum_{a\in\mathbb{F}_q}\sum_{(x_1,x_2,\ldots,x_s)\in\mathbb{F}_q^s}\psi_a(F(x_1,x_2,\ldots,x_s))\\ &= \sum_{a\in\mathbb{F}_q}\sum_{(x_1,x_2,\ldots,x_s)\in\mathbb{F}_q^s}\psi_a(a_1x_1^d+\cdots+a_sx_s^d-b)\\ &= \sum_{a\in\mathbb{F}_q}\psi_a(-b)\sum_{(x_1,x_2,\ldots,x_s)\in\mathbb{F}_q^s}\prod_{i=1}^{s}\psi_a(a_ix_i^d)\\ &= \sum_{a\in\mathbb{F}_q}\psi_a(-b)\prod_{i=1}^{s}\sum_{x\in\mathbb{F}_q}\psi_a(a_ix^d).\end{aligned}$$

A última igualdade docorre do Lema 3.1, e como $\psi_{aa_i}(x^d)=\psi_a(a_ix^d)$ obtemos o resultado fazendo $S(aa_i)=\sum_{x\in\mathbb{F}_q}\psi_a(a_ix^d)$. □

O resultado que acabamos de verificar diz que para calcular o número de soluções de uma equação diagonal com expoente constante é necessário determinarmos $\sum_{x\in\mathbb{F}_q}\psi_a(a_ix_i^d)$. Nosso próximo resultado fornece o valor deste somatório pra determinados inteiros k e s.

Lema 3.3 *Assuma $k=2t$ e que s divide p^k-1, p primo. Seja n tal que $ns=p^k-1$ e ψ_a o caractere aditivo de $\mathbb{F}_{p^k}$ definido por $\psi_a(x)=e^{(\frac{2i\pi}{p})tr(ax)}$, onde tr denota o traço de $\mathbb{F}_{p^k}$ sobre $\mathbb{F}_p$. Defina*

$$S(a)=\sum_{x\in\mathbb{F}_{p^k}}\psi_a(x^s)$$

onde $a\in\mathbb{F}_{p^k}^*$.

Caso exista um divisor positivo r de t tal que $p^r\equiv -1 \pmod s$ obtemos:

$S(a) = -\varepsilon(s-1)p^t$ para $a^n = \varepsilon_1$, e $S(a) = \varepsilon p^t$ para $a^n \neq \varepsilon_1$,
onde $\varepsilon = (-1)^{\frac{t}{r}}$ e $\varepsilon_1 = \varepsilon^u$ com $us = p^r + 1$.

Demonstração:

Seja N_λ o número de soluções de $tr(ax^s) = \lambda$, $\lambda \in \mathbb{F}_p$. Como o traço é sobrejetivo segue pelo Corolário 2.4 que para cada $\lambda \neq 0$ temos $N_\lambda = N_1$. Logo

$$S(a) = \sum_{tr(ax^s)=0} \psi_a(x^s) + \sum_{tr(ax^s)\neq 0} \psi_a(x^s).$$

Como

$$\sum_{tr(ax^s)=0} \psi_a(x^s) = \sum_{tr(ax^s)=0} 1 = N_0$$

e

$$\sum_{tr(ax^s)\neq 0} \psi_a(x^s) = N_1 \sum_{j=1}^{p-1} e^{\frac{2i\pi}{p}j} = -N_1,$$

obtemos $S(a) = N_0 - N_1$. E de acordo com o Corolário 2.4 temos dois casos a considerar:

Se $a^n = \varepsilon_1$ temos

$$S(a) = N_0 - N_1 = p^{2t-1} - \varepsilon(p-1)(s-1)p^{t-1} - p^{2t-1} + \varepsilon(s-1)p^{t-1} = -\varepsilon(s-1)p^t.$$

Se $a^n \neq \varepsilon_1$ temos

$$S(a) = N_0 - N_1 = p^{2t-1} + \varepsilon(p-1)p^{t-1} - p^{2t-1} + \varepsilon p^{t-1} = \varepsilon p^{t-1}(1+p-1) = \varepsilon p^t.$$

□

Agora estamos em condições de determinar o número de soluções de certa equação diagonal.

Teorema 3.4 *Seja p um número primo, $q = p^k$, $k = 2t$ e $\mathbb{F}_q$ o corpo finito de ordem q. Sejam $a_1, a_2, \ldots, a_s$ em $\mathbb{F}_q^*$, com $s \geq 2$, $b \in \mathbb{F}_q$ e d um divisor de $q-1$ e n tal que $nd = q-1$. Denote por N o número de soluções $(x_1, x_2, \ldots, x_s)$ em $\mathbb{F}_q^s$ da equação*

$$a_1x_1^d + a_2x_2^d + \cdots + a_sx_s^d = b.$$

Se existe um divisor r de t tal que $p^r \equiv -1 \pmod{d}$ temos:

(1) para $b = 0$, $N = q^{s-1} + \varepsilon^s q^{\frac{s}{2}-1}(q-1)d^{-1}\sum_{0}^{d-1}(1-d)^{\upsilon(j)}$,

(2) para $b \neq 0$, $N = q^{s-1} - \varepsilon^{s+1}q^{\frac{s}{2}-1}[(1-d)^{\theta(b)}q^{\frac{1}{2}} - (q^{\frac{1}{2}}-\varepsilon)d^{-1}\sum_{0}^{d-1}(1-d)^{\tau(j)}]$,

onde $\varepsilon = (-1)^{\frac{t}{r}}$, $\theta(b)$ *é o número dos* $i's$, $1 \leq i \leq s$, *que satisfazem a igualdade* $(a_i)^n = (-b)^n$, $\tau(j)$ *o número dos* $i's$, $1 \leq i \leq s$ *que satisfazem* $(a_i)^n = (\alpha^j)^n$ *(sendo* α *um gerador do grupo cíclico* $\mathbb{F}_q^*$*) e* $\upsilon(j)$ *o número dos* $i's$, *tal que* $(\alpha^j)^n(a_i)^n = \epsilon_1$.

Demonstração:

Vamos utilizar a Proposição 3.2 junto com as notações do Lema 3.3. Para $a \in \mathbb{F}_q^*$ defina $\delta(a)$ como o número dos $i's$, tal que $(aa_i)^n = \varepsilon_1$. Lembre que $S(a) = \sum_{x\in\mathbb{F}_q}\psi_a(x^s)$ e $\psi_a(x) = e^{(\frac{2i\pi}{p})tr(ax)}$, e o traço definido de $\mathbb{F}_q$ sobre $\mathbb{F}_p$. Seja $S(1) = -\varepsilon(d-1)p^t$, $S(2) = \varepsilon p^t$. Então pelo Lema 3.3 o produto $\prod_{i=1}^{s} S(aa_i)$ torna-se $S(1)^{\delta(a)}S(2)^{s-\delta(a)}$ quando $a \neq 0$. Segue então pela Proposição 3.2 que

$$\begin{aligned} qN &= \sum_{a\in\mathbb{F}_q}\psi_a(-b)\prod_{i=1}^{s}S(aa_i) \\ &= \psi_0(-b)\prod_{i=1}^{s}S(0) + \sum_{a\in\mathbb{F}_q^*}\psi_a(-b)S(1)^{\delta(a)}S(2)^{s-\delta(a)} \\ &= q^s + (S(2)^s)\sum_{a\in\mathbb{F}_q^*}(S(1)S(2)^{-1})^{\delta(a)}\psi_a(-b). \end{aligned}$$

A segunda igualdade segue de $\prod_{i=1}^{s} S(aa_i) = S(1)^{\delta(a)}S(2)^{s-\delta(a)}$ quando $a \neq 0$. A terceira igualdade vem do fato de $\psi_0(-b) = 1$ e $S(0) = q$. Como $S(2)^s = \varepsilon^s p^{st}$ e $S(1)S(2)^{-1} = 1-d$ temos

$$qN = q^s + \varepsilon^s p^{st}\sum_{a\in\mathbb{F}_q^*}(1-d)^{\delta(a)}\psi_a(-b). \tag{3.1}$$

Seja E_n o subgrupo multiplicativo de ordem n de $\mathbb{F}_q^*$ e C_j as classes módulo E_n definidas por $C_j = \alpha^j E_n$ para $j \in \{0, 1, \ldots, d-1\}$ sendo α uma raiz primitiva de $\mathbb{F}_q$. Observe que C_j é o conjunto dos $y \in \mathbb{F}_q$ tal que $y^n = \alpha^{jn}$. Portanto o somatório em 3.1 pode ser reescrito como

$$\sum_{a\in\mathbb{F}_q^*}(1-d)^{\delta(a)}\psi_a(-b)=\sum_{j=0}^{d-1}\sum_{a\in C_j}(1-d)^{\delta(a)}\psi_a(-b) \tag{3.2}$$

Seja $\upsilon(j)$ o o número dos $i's$, tal que $(\alpha^j)^n(a_i)^n = \epsilon_1$. Para todo $a \in C_j$ temos $a^n = (\alpha^j)^n$ logo $(aa_i)^n = \epsilon_1$ se, e somente se, $(\alpha^j)^n(a_i)^n = \epsilon_1$. Isto significa que $\delta(a) = \upsilon(j)$ para todo $a \in C_j$. Logo por 3.1 e 3.2 temos:

$$qN = q^s + \varepsilon^s p^{st}\sum_{j=0}^{d-1}(1-d)^{\upsilon(j)}\sum_{a\in C_j}\psi_a(-b). \tag{3.3}$$

Basta agora determinarmos $\sum_{a\in C_j}\psi_a(-b)$. Para isto vamos considerar quando $b \neq 0$ e quando $b = 0$.

(i) $b \neq 0$.

Para $\lambda \in \mathbb{F}_p$ defina

$$R_j(b,\lambda) = \#\{a \in C_j : tr(-ba) = \lambda\}$$

e

$$T_j(b,\lambda) = \#\{x \in \mathbb{F}_q : tr(-b\alpha^j x^d) = \lambda\}.$$

Se $a \in C_j$ então existe exatamente d elementos de $\mathbb{F}_q^*$ tal que $a = \alpha^j x^d$ e assim $dR_j(b,\lambda) = T_j(b,\lambda)$. Logo

$$d\sum_{a\in C_j}\psi_a(-b) = T_j(b,0) + \sum_{\lambda=1}^{p-1}T_j(b,\lambda)e^{(\frac{2i\pi}{p}\lambda)}.$$

Pela Corolário 2.4 temos que $T_j(b,\lambda)$ depende somente de $(-b\alpha^j x^d)$ e assim

$$\begin{aligned} d\textstyle\sum_{a\in C_j}\psi_a(-b) &= T_j(b,0) + T_j(b,1)\displaystyle\sum_{\lambda=1}^{p-1}e^{(\frac{2i\pi}{p}\lambda)} \\ &= T_j(b,0) + T_j(b,1)\left(-1 + \sum_{\lambda=0}^{p-1}e^{(\frac{2i\pi}{p}\lambda)}\right) \\ &= T_j(b,0) - T_j(b,1), \end{aligned}$$

a última igualdade segue do fato de $\displaystyle\sum_{\lambda=0}^{p-1}e^{(\frac{2i\pi}{p}\lambda)} = 0$ (aplicação direta do Lema 1.1). Substituindo $d\displaystyle\sum_{a\in C_j}\psi_a(-b) = T_j(b,0) - T_j(b,1)$ em 3.3 vamos obter

$$qN = q^s + d^{-1}\varepsilon^s p^{st} \sum_{j=0}^{d-1} A_j(b)(1-d)^{v(j)}, \tag{3.4}$$

onde $A_j(b) = T_j(b,0) - T_j(b,1)$.

Pelo Corolário 2.4 e pela definição de $T_j(b,\lambda)$, o número $A_j(b)$ depende somente de b e j, e do número $(b\alpha^j)^n$ ser igual a ε_1 ou não. O único caso onde $\varepsilon_1 = -1$, no Corolário 2.4, é quando p e u são ímpares. E neste caso a igualdade $ud = p^r + 1$ implica d par. Isto significa que $(\varepsilon_1)^d = (-1)^d = 1$ e portanto, pois $nd = q-1$, existe exatamente n soluções de $a^n = \varepsilon_1$. Isto é obviamente verdade se $\varepsilon_1 = 1$. Em todos os outros casos existe exatamente um único j satisfazendo $(b\alpha^j)^n = \varepsilon_1$, com $0 \leq j \leq d-1$, dito j_0. Tome $\gamma_0 = b\gamma^{j_0}$, $\gamma_1 = b\gamma^j$ com $j \neq j_0$, e seja $v_1 \in \mathbb{F}_q$ tal que $tr(v_1) = 1$, com as notações do Corolário 2.4, vamos obter:

para $j = j_0$

$$A_j(b) = A_1 = N(\gamma_0, 0) - 1 - N(\gamma_0, v_1) = -1 - \varepsilon_1(d-1)p^t$$

para $j \neq j_0$

$$A_j(b) = A_2 = N(\gamma_1, 0) - 1 - N(\gamma_1, v_1) = -1 - \varepsilon_1 p^t$$

Substituindo em 3.4 temos

$$\begin{aligned} qN &= q^s + d^{-1}\varepsilon^s p^{st}[A_1(1-d)^{v(j_0)} + A_2 \sum_{j\neq j_0}(1-d)^{v(j)}] \\ &= q^s + d^{-1}\varepsilon^s p^{st}[(A_1 - A_2)(1-d)^{v(j_0)} + A_2 \sum_{j=0}^{d-1}(1-d)^{v(j)}] \\ &= q^s + d^{-1}\varepsilon^s p^{st}[-\varepsilon d p^t (1-d)^{v(j_0)} - \varepsilon p^t \sum_{j=0}^{d-1}(1-d)^{v(j)}] \end{aligned}$$

Veja que por definição $v(j) = \{i : (\alpha^j)^n (a_i)^n = \varepsilon_1\}$, mas como vimos antes $\varepsilon_1 = \varepsilon^u$, ou seja, ε_1 é uma potência de ε. Assim, se $0 \leq j \leq d-1$, $v(j)$ é igual ao número dos $a_i's$ que pertencem somente a uma classe módulo E_n. Dessa forma podemos substituir $v(j)$ por $\tau(j)$ na última igualdade. Além disso se $j = j_0$ e como $\varepsilon_1 = (b\alpha^{j_0})^n$, o inteiro $v(j_0)$ é igual ao número dos $i's$ tal que $(a_i)^n = b^n$. Vamos denotar este último número por $\theta(b)$ e o teorema segue para $b \neq 0$.

(ii) Quando $b = 0$.

Substituindo em 3.3, obtemos

$$q^s + \varepsilon^s p^{st} \sum_{j=0}^{d-1} (1-d)^{\upsilon(j)} \sum_{a \in C_j} \psi_a(0).$$

Como $\sum_{a \in C_j} \psi_a(0) = \# \sum_{a \in C_j} 1 = \#C_j = n = \dfrac{q-1}{d}$ temos

$$qN = q^s + \varepsilon^s p^{st} \sum_{j=0}^{d-1} (1-d)^{\upsilon(j)} \frac{q-1}{d} = q^s + \varepsilon^s q^s (q-1) d^{-1} \sum_{j=0}^{d-1} (1-d)^{\upsilon(j)}.$$

□

3.2 Variedades Maximais

Dad uma equação diagonal com expoente constante em s variáveis, sobre $\mathbb{F}_q$, vimos que em certos casos é possível determinar seu número de soluções em $\mathbb{F}_q^s$.

Agora aumentando as restrições, vamos supor todos coeficientes iguais a um, é possível obtermos variedades projetivas sobre $\mathbb{F}_q$ que atigem a cota de Weil-Deligne para o número de pontos destas variedades.

Corolário 3.5 *Seja p um número primo, $q = p^k$, $k = 2t$, e $\mathbb{F}_q$ o corpo finito de ordem q. Seja N o número de soluções $(x_1, x_2, \ldots, x_s)$ em $\mathbb{F}_q^s$ da equação*

$$x_1^d + x_2^d + \cdots + x_s^d = b$$

onde $s \geq 2$, $b \in \mathbb{F}_q$ e d um divisor de $q-1$ tal que $nd = q-1$.
Se existe um divisor r de t tal que $p^r = -1 (mod\ d)$ então N é dado por:

(1) se $b = 0$, $N = q^{s-1} + \eta^s q^{\frac{s}{2}-1}(q-1)B(d,s)$,

(2) se $b \neq 0$, temos dois casos:

(i) se $b^n = 1$, $N = q^{s-1} + \eta^{s+1} q^{\frac{s}{2}-1}[(d-1)^s q^{\frac{1}{2}} - (q^{\frac{1}{2}} - \eta)B(d,s)]$,

(ii) se $b^n \neq 1$, $N = q^{s-1} + \eta^{s+1} q^{\frac{s}{2}-1}[(-1)^s q^{\frac{1}{2}} - (q^{\frac{1}{2}} - \eta)B(d,s)]$.

onde $\eta = (-1)^{\frac{t}{r}+1}$ *e* $B(d,s) = d^{-1}[(d-1)^s + (-1)^s(d-1)]$.

Demonstração:

Pelo Teorema 3.4 obtemos:

(1) para $b = 0$, $N = q^{s-1} + \varepsilon^s q^{\frac{s}{2}-1}(q-1)d^{-1}\sum_{0}^{d-1}(1-d)^{\upsilon(j)}$,

(2) para $b \neq 0$, $N = q^{s-1} + \varepsilon^s q^{\frac{s}{2}-1}(q-1)d^{-1}[(1-d)^{\theta(b)}q^{\frac{1}{2}} - (q^{\frac{1}{2}}-\varepsilon)d^{-1}\sum_{0}^{d-1}(1-d)^{\tau(j)}]$.

Portanto devemos calcular $\upsilon(j)$, $\theta(b)$ e $\tau(j)$.

Para calcular $\upsilon(j)$ temos que determinar o número dos i's que satisfazem $(\alpha^j)^n(a_i)^n = \varepsilon_1$. Como $a_i = 1$ para todo i basta verificarmos se $(\alpha^j)^n = \varepsilon_1$ tem solução. Em caso afirmativo $\upsilon(j) = s$ pois temos s coeficientes e em caso negativo $\upsilon(j) = 0$.

Mas é fácil ver que $(\alpha^j)^n = (-1)^{\frac{t}{r}u}$, $0 \leq j \leq d-1$, tem solução somente quando $j = 0$. Portanto $\upsilon(0) = s$ e $\upsilon(j) = 0$ se $j \neq 0$. E quando $b = 0$, obtemos

$$\begin{aligned} N &= q^{s-1} + \varepsilon^s q^{\frac{s}{2}-1}(q-1)d^{-1}\sum_{0}^{d-1}(1-d)^{\upsilon(j)} \\ &= q^{s-1} + \varepsilon^s q^{\frac{s}{2}-1}(q-1)d^{-1}[(1-d)^s + (d-1)] \\ &= q^{s-1} + \varepsilon^s q^{\frac{s}{2}-1}(q-1)d^{-1}(-1)^s[(d-1)^s + (-1)^s(d-1)] \\ &= q^{s-1} + (-1)^s\varepsilon^s q^{\frac{s}{2}-1}(q-1)d^{-1}[(d-1)^s + (-1)^s(d-1)] \\ &= q^{s-1} + \eta^s q^{\frac{s}{2}-1}(q-1)B(d,s), \end{aligned}$$

onde $\eta^s = (-1)^s\varepsilon^s$ e $B(d,s) = d^{-1}[(d-1)^s + (-1)^s(d-1)]$.

Agora com uma análise semelhante a de $\upsilon(j)$ vemos que $\tau(0) = s$ e $\tau(j) = 0$ se $j \neq 0$. Supondo $b^n = 1$ temos $\theta(b) = s$ e neste caso

$$\begin{aligned} N &= q^{s-1} + \varepsilon^s q^{\frac{s}{2}-1}(q-1)d^{-1}[(1-d)^{\theta(b)}q^{\frac{1}{2}} - (q^{\frac{1}{2}}-\varepsilon)d^{-1}\sum_{0}^{d-1}(1-d)^{\tau(j)}] \\ &= q^{s-1} + \varepsilon^s q^{\frac{s}{2}-1}(q-1)d^{-1}[(1-d)^s q^{\frac{1}{2}} - (q^{\frac{1}{2}}+\eta)d^{-1}(-1)^s[(d-1)^s + (-1)^s(d-1)] \\ &= q^{s-1} + \eta^{s+1}q^{\frac{s}{2}-1}[(d-1)^s q^{\frac{1}{2}} - (q^{\frac{1}{2}}-\eta)B(d,s)], \end{aligned}$$

visto que $\eta^{s+1} = (-1)^s\varepsilon^s$, $\eta = -\varepsilon$ e $B(d,s) = d^{-1}[(d-1)^s + (-1)^s(d-1)]$.

Agora supondo $b^n \neq 1$ temos $\theta(b) = 0$ e calculando N, como no caso anterior obtemos

$$N = q^{s-1} + \varepsilon^s q^{\frac{s}{2}-1}(q-1)d^{-1}[(1-d)^{\theta(b)}q^{\frac{1}{2}} - (q^{\frac{1}{2}}-\varepsilon)d^{-1}\sum_{0}^{d-1}(1-d)^{\tau(j)}].$$

□

Seja f um polinômio homogêneo de grau d em $\mathbb{F}_q[x_1, \ldots, x_s]$ e $V = Z(f)$, a variedade projetiva definida por f sobre $\mathbb{F}_q$. Considere $\tilde{N}$ o número de pontos de V sobre $\mathbb{F}_q$. Temos um resultado bastante conhecido que estabelece uma cota para $\tilde{N}$ quando V é absolutamente irredutível e não singular. Esta cota é conhecida como cota de Weil-Deligne e estabelece que

$$\left| \tilde{N} - \frac{q^{s-1}}{q-1} \right| \leq q^{(\frac{s}{2}-1)} B(d,s)$$

onde $B(d,s) = d^{-1}[(d-1)^s + (-1)^s(d-1)]$.
O próximo resultado vai nos fornecer uma família de variedades projetivas onde o número de pontos sobre $\mathbb{F}_q$, destas variedades, atigem a cota de Weil-Deligne.

Corolário 3.6 *Seja V a variedade projetiva definida por $x_1^d + x_2^d + \cdots + x_s^d$ sobre $\mathbb{F}_q$ onde $s \geq 2$, $q = p^k$ com p primo, $k = 2t$, e d é um divisor de $p^k - 1$. Seja $\tilde{N}$ o número de pontos V sobre $\mathbb{F}_q$.*
Se existe um divisor r de t tal que $p^r \equiv -1 \pmod{d}$, então $\tilde{N}$ é dado por:

Se $\frac{t}{r}$ for par e s ímpar temos

$$\tilde{N} = \frac{(q^{s-1}-1)}{(q-1)} - q^{(\frac{s}{2}-1)} B(d,s).$$

Se $\frac{t}{r}$ for ímpar temos

$$\tilde{N} = \frac{(q^{s-1}-1)}{(q-1)} + q^{(\frac{s}{2}-1)} B(d,s).$$

Demonstração:
Seja V a variedade projetiva definida por $f(x_1, \ldots, x_s) = x_1^d + \cdots + x_s^d$ sobre $\mathbb{F}_q$ (se d e q são coprimos V é absolutamente irredutível, para $s \geq 3$). Temos que V é o conjunto de pontos $(x_1 : \ldots : x_s)$ em $\mathbb{P}^{s-1}$ tal que $f(x_1, \ldots, x_s) = 0$. Agora observe que $f(0, \ldots, 0) = 0$ mas $(0 : \ldots : 0) \neq \mathbb{P}^{s-1}$ e que para toda solução $(x_1, \ldots, x_s) \neq 0$ em $\mathbb{F}_q^s$ temos que $a(x_1, \ldots, x_s)$, $a \in \mathbb{F}_q^*$ também é solução. Visto que estamos interessados em soluções em $\mathbb{P}^{s-1}$ temos

$$\tilde{N} = \frac{N-1}{q-1}$$

onde N é o número de soluções em $\mathbb{F}_{q^s}$ de $x_1^d + x_2^d + \cdots + x_s^d = 0$ dado pelo Corolário 3.5. Portanto

$$\tilde{N} - \frac{(q^{s-1}-1)}{(q-1)} = \eta^s q^{(\frac{s}{2}-1)} B(d,s)$$

com $\eta = (-1)^{\frac{t}{r}+1}$. Neste caso se $\frac{t}{r}$ é par temos $\eta^s = -1$ ou 1 de acordo s for ímpar ou par. Se $\frac{t}{r}$ é ímpar $\eta^s = 1$ e o resultado segue. □

APÊNDICE A

Corpos Finitos

Nosso objetivo, neste apêndice, é destacar alguns resultados sobre a teoria dos corpos com ênfase aos corpos finitos. Estes resultados foram utilizados ao longo do texto. Vamos nos limitar a fornecer as definições e os resultados sem demonstrações. Para maiores detalhes veja [3], [15].

Em [3] o leitor terá uma idéia de como é fecundo o universo dos corpos finitos.

A.1 Caracterização dos Corpos finitos

Nesta seção vamos caracterizar os corpos finitos e ver algumas de suas propriedades.

O primeiro exemplo de corpo finito que um estudante tem contato, na sua vida acadêmica, é o corpo dado pelo grupo quociente $\frac{Z}{pZ}$ onde p é um primo. Nos iremos denotar este corpo finito por $\mathbb{F}_p$.

Definição A.1 (Característica)

Seja K um corpo se existe n, inteiro positivo, tal que $na = 0$ para todo $a \in K$, então o menor inteiro n com esta propriedade é dito ser a característica de K, notação $n = car(K)$. Caso não exista nenhum inteiro positivo com esta propriedade a característica de K é dita ser zero. □

Teorema A.1 *Todo corpo finito possui característica prima.*

Teorema A.2 *Seja K corpo finito tal que $car(K) = p$, p primo. Então*

$$(a+b)^{p^n} = a^{p^n} + b^{p^n} \text{ e } (a-b)^{p^n} = a^{p^n} - b^{p^n}$$

para todo $a, b \in K$ e $n \in \mathbb{N}$.

Definição A.2 (Extensão) *Seja K um subcorpo do corpo L, $K \subseteq L$. Dizemos que L é uma extensão de K.* □

A dimensão do K-espaço vetorial L é dita índice da extensão L de K e denotada por $[L : K]$.

Definição A.3 (Corpo Primo) *Um corpo que não possui subcorpos próprio é chamado de corpo primo.* □

Teorema A.3 *O subcorpo primo de um corpo F é isomorfo a $\mathbb{F}_p$ ou a $\mathbb{Q}$, de acordo $car(F) = p$ ou 0.*

Teorema A.4 *Todo corpo finito F tem p^n elementos, onde p é a característica de F e $n = [F : \mathbb{F}_p]$.*

Lema A.5 *Se F é um corpo finito com q elementos, $q = p^n$, então todo $a \in F$ satisfaz $a^q = a$. Seja K um subcorpo de F, então o polinômio $x^q - x$ de $K[x]$ se fatora em $F[x]$ como*

$$x^q - x = \prod_{a \in F} (x - a)$$

e F é o corpo de fatoração de $x^q - x$ sobre K.

Teorema A.6 *Para cada primo p e cada número natural n existe um corpo finito com p^n elementos. Todo corpo finito com $q = p^n$ elementos é isomorfo ao corpo de fatoração de $x^q - x$ em $\mathbb{F}_p$.*

Teorema A.7 *Seja $\mathbb{F}_q$ o corpo finito com $q = p^n$ elementos. Então todo subcorpo de $\mathbb{F}_q$ tem p^m elementos, onde m é divisor de n. Reciprocamente se m é um divisor de n existe exatamente um subcorpo de $\mathbb{F}_q$ com p^m elementos.*

Teorema A.8 *Para todo corpo finito $\mathbb{F}_q$, o grupo multiplicativo $\mathbb{F}_q^*$ dos elementos não nulos de $\mathbb{F}_q$ é cíclico.*

Definição A.4 (Elemento Primitivo) *Um gerador do grupo cíclico $\mathbb{F}_q^*$ é chamado de elemento primitivo de $\mathbb{F}_q$.* □

Teorema A.9 *Seja $\mathbb{F}_q$ o corpo finito com extensão $\mathbb{F}_r$. Então $\mathbb{F}_r$ é uma extensão algébrica simples de $\mathbb{F}_r$ e para todo ς elemento primitivo de $\mathbb{F}_r$ temos $\mathbb{F}_q(\varsigma) = \mathbb{F}_r$.*

A.2 Funções e Bases

Nesta seção vamos definir duas importantes funções sobre um corpo finito, base dual e ver um resultado para um determinado polinômio.

Definição A.5 (Traço)

Para $a \in F = \mathbb{F}_{q^m}$ e $K = \mathbb{F}_q$, o traço de a sobre K é definido por

$$tr_{F|_K}(a) = a + a^q + \cdots + a^{q^{m-1}}.$$

□

Quando F e K estiverem claros iremos denotar $tr_{F|_K}(a)$ por $tr(a)$ e diremos apenas traço de a.

Teorema A.10 *Seja $K = \mathbb{F}_q$ e $F = \mathbb{F}_{q^m}$. Então a função $tr = tr_{F|_K}$ possui as sequintes propriedades:*

1. *$tr(\alpha) \in K$ para todo $\alpha \in F$;*
2. *tr é K-linear e sobrejetiva;*
3. *$tr(\alpha) = m\alpha$ para todo $\alpha \in K$;*
4. *$tr(\alpha^q) = tr(\alpha)$ para todo $\alpha \in F$.*

Teorema A.11 *Seja F uma extensão finita do corpo finito K. Considerando ambos como K-espaços vetoriais sobre K obtemos que toda transformação linear de F em K é da forma L_β, com $\beta \in F$, onde $L_\beta(\alpha) = tr(\beta\alpha)$ para todo $\alpha \in F$. Além disso se $\beta \neq \alpha$ temos que L_β e L_α são distintas.*

Teorema A.12 *Seja $F = \mathbb{F}_{q^m}$ uma extensão de $\mathbb{F}_q$ e $tr : F \to \mathbb{F}_q$ o traço de F sobre $\mathbb{F}_q$. Então para todo $a \in F$ temos que $tr(a) = 0$ se, e somente se, $a = b^q - b$ para algum $b \in F$.*

Definição A.6 (Norma)

Para $a \in F = \mathbb{F}_{q^m}$ e $K = \mathbb{F}_q$, a norma $N_{F|_K}$ de a de F sobre K é definida por

$$N_{F|_K}(a) = a \bullet a^q \bullet \cdots \bullet a^{q^{m-1}} = a^{\frac{(q^m-1)}{(q-1)}}.$$

□

Quando F e K estiverem claros iremos denotar $N_{F|_K}(a)$ por $N(a)$ e diremos apenas norma de a.

Teorema A.13 *Seja $N : \mathbb{F}_{q^m} \to \mathbb{F}_q$ a função norma. Então*

1. *$N(ab) = N(a)N(b)$ para todo $a, b \in \mathbb{F}_{q^m}$;*
2. *N é sobrejetiva e $N(a) = 0$ se, e somente se, $a = 0$;*
3. *$N(a) = a^m$ para todo $a \in \mathbb{F}_q$;*
4. *$N(a^q) = N(a)$ para todo $a \in \mathbb{F}_{q^m}$.*

Definição A.7 (Base Dual)

Seja K corpo finito e F uma extensão de K. Então duas bases $\{\alpha_1, \ldots, \alpha_m\}$ e $\{\beta_1, \ldots, \beta_m\}$ de F sobre K são ditas bases dual ou complementares se para $1 \leq i, j \leq m$ nos temos

$$tr_{F|_K}(\alpha_i\beta_j) = \begin{cases} 0 \text{ para } i \neq j \\ 1 \text{ para } i = j. \end{cases}$$

□

Teorema A.14 *Dado $\alpha = \{\alpha_1, \ldots, \alpha_m\}$ base de F sobre K existe $\beta = \{\beta_1, \ldots, \beta_m\}$ base de F sobre K tal que α e β são complementares.*

Teorema A.15 *Seja $a \in \mathbb{F}_q$ e p a característica de $\mathbb{F}_q$. Então $x^p - x - a$ é irredutível em $\mathbb{F}_q[x]$ se, e somente se, não tem raiz em $\mathbb{F}_q$.*

Corolário A.16 *Com a notação do Teorema A.15 o trinômio $x^p - x - a$ é irredutível em $\mathbb{F}_q[x]$ se, e somente se, $tr(a) \neq 0$, onde $tr : \mathbb{F}_q \to \mathbb{F}_p$.*

Demonstração:

Veja na página 127 da referência [3]. □

APÊNDICE B

Curvas Algébricas

Este apêndice contém definições e alguns resultados básicos sobre Curvas Algébricas Planas em especial sobre corpos finitos. Para mais detalhes e provas o leitor pode consultar [7], [8]. Neste texto a principal referência é [1].

B.1 Variedades Afim

Ao longo desta seção vamos assumir que K é um corpo algebricamente fechado.

O n-dimensional espaço afim $\mathbb{A}^n = \mathbb{A}^n(K)$ é o conjunto de todas n-uplas de elementos de K. Um elemento $P = (a_1, \ldots, a_n) \in \mathbb{A}^n$ é dito ponto de $\mathbb{A}^n$ e $a_1, \ldots, a_n$ são as coordenadas do ponto P.

Seja $K[x_1, \ldots, x_n]$ o anel dos polinômios em n variáveis sobre K. Se $f \in K[x_1, \ldots, x_n]$, um ponto $P = (a_1, \ldots, a_n) \in \mathbb{A}^n$ é dito zero de f se $f(P) = f(a_1, \ldots, a_n) = 0$.

Se f não é constante, o conjunto dos zeros de f é chamado de hipersuperfície definida por f.

Definição B.1 (Conjunto Algébrico Afim)

Seja V um subconjunto de $\mathbb{A}^n$. Se existe $S \subseteq K[x_1, \ldots, x_n]$, subconjunto de polinômios, tal que

$$V = \{P \in \mathbb{A}^n : f(P) = 0 \text{ para todo } f \in S\},$$

então V é chamado de conjunto algébrico afim de $\mathbb{A}^n$, ou simplesmente conjunto algébrico. Notação $V = Z(S)$, "zeros"de S. □

Um conjunto algébrico afim $V \subseteq \mathbb{A}^n$ é chamado de irredutível se não pode ser decomposto como $V = V_1 \cup V_2$, onde V_1 e V_2 são subconjuntos algébricos próprios de V. De forma equivalente V é irredutível se, e somente se, o ideal

$$I(V) = \{f \in K[x_1, \ldots, x_n] : f(P) = 0 \text{ para todo } P \in V\},$$

chamado de ideal de V, é primo.

B.2 Variedades Projetivas

Ao longo desta seção vamos assumir que K é um corpo algebricamente fechado.
Considere $\mathbb{A}^{n+1} \setminus \{(0, \ldots, 0)\}$ com a sequinte relação de equivalência

$$(a_1, \ldots, a_n, a_{n+1}) \sim (b_1, \ldots, b_n, b_{n+1}) \Leftrightarrow \exists\, 0 \neq \lambda \in K \text{ tal que } b_i = \lambda a_i \ \forall\ 1 \leq i \leq n+1.$$

Denotamos a classe de equivalência de $(a_1, \ldots, a_n, a_{n+1})$ por $(a_1 : \ldots : a_n : a_{n+1})$. O n-dimensional espaço projetivo $\mathbb{P}^n = \mathbb{P}^n(K)$ é o conjunto de todas as classes de equivalência

$$\mathbb{P}^n = \{(a_1 : \ldots : a_n : a_{n+1}) : a_i \in K \text{ e nem todos nulos }\}$$

Um elemento $P = (a_1 : \ldots : a_n : a_{n+1}) \in \mathbb{P}^n$ é chamado de ponto, e $a_1, \ldots, a_n, a_{n+1}$ são suas coordenadas homogêneas de P.

Seja $F \in K[x_1, \ldots, x_n, x_{n+1}]$ um polinômio homogênio de grau d, também dito forma de grau d. Um ponto $P = (a_1 : \ldots : a_n : a_{n+1}) \in \mathbb{P}^n$ é dito zero de F se, e somente se, $F(P) = F(a_1, \ldots, a_n, a_{n+1}) = 0$. Veja que está definição independe das coordenadas homogêneas de P, pois

$$F(\lambda a_1, \ldots, \lambda a_n, \lambda a_{n+1}) = \lambda^d F(a_1, \ldots, a_n, a_{n+1}),$$

donde, desde que $\lambda \neq 0$,

$$F(a_1, \ldots, a_n, a_{n+1}) = 0 \Leftrightarrow F(\lambda a_1, \ldots, \lambda a_n, \lambda a_{n+1}) = 0.$$

Definição B.2 (Conjunto Algébrico Projetivo)

Seja V um subconjunto de $\mathbb{P}^n$. Se existe um subconjunto $S \subseteq K[x_1, \ldots, x_{n+1}]$ de formas tal que

$$V = \{P \in \mathbb{P}^n : F(P) = 0 \text{ para todo } F \in S\}$$

dizemos que V é um do conjunto algébrico projetivo. □

O ideal $I(V) \subseteq K[x_1, \ldots, x_{n+1}]$ gerado pelas formas $F \in K[x_1, \ldots, x_{n+1}]$ tal que $F(P) = 0$ para todo $P \in V$, é chamado de ideal de V.

Definição B.3 (Variedade Projetiva)

Um conjunto algébrico projetivo $V \subseteq \mathbb{P}^n$ é dito irredutível se não pode ser decomposto como $V = V_1 \cup V_2$, onde V_1 e V_2 são subconjuntos algébricos projetivos de V. □

Como no caso afim $V \subseteq \mathbb{P}^n$ é irredutível se, e somente se, $I(V)$ é ideal primo de $K[x_1, \ldots, x_{n+1}]$.

B.3 Curvas e Pontos Racionais

Seja K um corpo finito. Vamos denotar por $\bar{K}$ o seu fecho algébrico.

Se $f(x, y)$ é um polinômio em $K[x, y]$, então a curva algébrica plana afim associada é definida por

$$C_a = C_a(\bar{K}) = \{(a, b) \in \bar{K} \times \bar{K} : f(a, b) = 0\}.$$

Os pontos racionais da curva plana afim associada são dados por

$$C_a(K) = \{(a, b) \in K \times K : f(a, b) = 0\}.$$

Seja agora $F(x, y, z)$ um polinômio homogêneo de grau d em $K[x, y, z]$, então a curva algébrica plana projetiva associada é definida por

$$C = C(\bar{K}) = \{(a : b : c) \in \mathbb{P}^2(\bar{K}) : f(a, b, c) = 0\}.$$

Os pontos racionais da curva plana projetiva associada são dados por

$$C = C(K) = \{(a : b : c) \in \mathbb{P}^2(K) : f(a, b, c) = 0\}.$$

Seja $f(x,y)$ um polinômio em $K[x,y]$ associamos ao polinômio f a seguinte forma em $K[x,y,z]$

$$f^*(x,y,z) := z^d f\left(\frac{x}{z}, \frac{y}{z}\right).$$

O polinômio homogêneo $f^*(x,y,z)$ é chamado de polinômio homogêneo associado a f, este processo é chamado de homogenização de f. Portanto quando nos referimos a curva algébrica plana projetiva associada ao polinômio $f(x,y)$ estamos nos referindo a curva associada ao polinômio homogêneo $f^*(x,y,z)$.

Dado um polinômio homogêneo $f(x,y,z) \in K[x,y,z]$ podemos fazer processo inverso da homgenização , ou seja, associamos ao polinômio homogêneo $f(x,y,z)$ o seguinte polinômio em $K[x,y]$

$$f_*(x,y) := f(x,y,1).$$

Este processo é chamado de desomogenização de $f(x,y,z)$.

Seja C_a a curva plana afim associada ao polinômio $f \in K[x,y]$. Tome C a curva plana projetiva associada a forma $f^* \in K[x,y,z]$ é fácil ver que $(x,y) \mapsto (x:y:1)$ é uma imersão de C_a em C. Logo para determinarmos as soluções de uma curva plana projetiva basta encontramos as soluções da curva plana afim $f(x,y)$ e depois considerar as soluções da forma $(x:y:0)$

Os pontos da forma $(x:y:0)$ são ditos pontos no infinito com relação a curva plana afim C_a.

B.4 Variedades Absolutamente Irredutíveis

Nosso principal interesse em variedades sobre corpos finitos é determinar seu número de pontos racionais. Há uma classe de variedades especiais onde este trabalho é "simplificado". E são estas variedades que vamos especificar nesta seção e fornecer alguns resultados.

Como todo polinômio $f(x,y)$ em $K[x,y]$, não constante, pode ser decomposto como produto de fatores irredutíveis, em $K[x,y]$, podemos considerar somente os polinômios irredutíveis em $K[x,y]$. Contudo $f(x,y)$ pode ser decomposto em alguma extensão de K e dessa forma, para evitar este tipo de problema, vamos considerar somente polinômios absolutamente irredutíveis em $K[x,y]$.

Definição B.4 (Polinômio Absolutamente Irredutível)

Seja $f(x_1, \ldots, x_n)$ um polinômio em $K[x_1, \ldots, x_n]$. Se $f(x_1, \ldots, x_n)$ é irredutível em $\bar{K}[x_1, \ldots, x_n]$, $\bar{K}$ fecho algébrico de K, dizemos que $f(x_1, \ldots, x_n)$ é absolutamente irredutível em $K[x_1, \ldots, x_n]$. □

Portanto quando falarmos variedade absolutamente irredutível estamos dizendo que o seu polinômio associado é absolutamente irredutível em $K[x, y]$.

Temos os seguintes resultados para determinar se um polinômio é absolutamente irredutível em $K[x, y]$.

Teorema B.1 *Seja $f(x, y) \in K[x, y]$ da seguinte forma*

$$f(x, y) = a_0 y^n + a_1(x) y^{n-1} + \cdots + a_{n-1} y + a_n(x)$$

com $a_i \in K[x]$ e $a_0 \in K^*$. Suponha que $gr(a_n(x)) = m$ é coprimo com n e que $\frac{m}{n} > \frac{gr(a_i(x))}{i}$ para $i = 1, 2, \ldots, n-1$. Então o polinômio $f(x, y)$ é absolutamente irredutível em $K[x, y]$.

Demonstração: Veja o primeiro Teorema do livro [1]. □

Teorema B.2 *Seja K um corpo arbitrário, $f \in K[x]$ com grau maior que zero, e $m \in \mathbb{N}$. Suponha que*

$$f(x) = a(x - \alpha_1)^{e_1} \cdots (x - \alpha_d)^{e_d}$$

é a fatorização de f em seu corpo de fatoração sobre K, onde $\alpha_1, \ldots, \alpha_d$ são as raízes distintas de f. Então $y^m - f(x)$ é absolutamente irredutível se, e somente se, o máximo divisor comum dos e_i e m é um.

Demonstração: Veja o Lema 6.54 do livro [3]. □

REFERÊNCIAS BIBLIOGRÁFICAS

[1] A. Garcia, *Pontos Racionais sobre Corpos Finitos*,

20^o Colóquio Brasileiro de Matemática, IMPA, 1995.

[2] I. Vainsencher, *Introdução às Curva Algébricas Planas*,

Coleção Matemática Universitária, 1996.

[3] R. Lidl and H. Niederreiter, *Finite Fields*,

Encyclopedia of Mathematics its Applications, Addison-Wesley, 1983.

[4] T. Y. Lam, *The Algebraic Theory of Quadratic Formas*,

Benjamin Reading, Mass, 1973.

[5] J. Wolfmann, *The number of points on certain curves over finite fields*,

Comm. Algebra 17, Número 8, 2055-2060, 1989.

[6] J. Wolfmann, *The number of solutions of certain diagonal equations over finite fields*,

J. Number Theory, Vol. 42, 247-257, 1992.

[7] W. Fulton, *Algebraic Curves*, Benjamin, 1969.

[8] Hartshorne, *Algebraic Geometry*, Springer, 1977.

[9] H. Stichtenoth, *Algebraic Function Fields and Codes*,
Springer Verlag, 1993.

[10] J. P. Serre, *Linear Representations of Finite Groups*,
Springer Verlag, 1977.

[11] J. Minor and D. Husemoller, *Symmetric Bilinear Formas*,
Ergebnisse der Math. 73, Springer Verlag, 1973.

[12] J. H. Conway, *The Sensual(quadritic) Form*,
The Mathematical Association of America, 1997.

[13] S. Lang, *Algebra*, Addison-Wesley, 1965.

[14] A. Garcia, *Elementos de Álgebra*, 2ed, IMPA, 2003.

[15] A. Hefez, *Códigos Corretores de Erros*, IMPA, 2002.

[16] A. Hefez, *Introdução à Geométria Projetiva*, IMPA, 1989.

[17] Y. Kitaoka, *Arithmetic of Quadratic Forms*, Cambridge, 1993.

[18] S. A. Stepanov, *Arithmetic of Algebraic Curves*, Consutants Bureau, 1994.