Universidade Estadual de Campinas
Instituto de Matemática, Estatística e Computação Científica
Departamento de Matemática

Dissertação de Mestrado

Formas quadráticas, pesos de Hamming generalizados e curvas algébricas

Diogo Bruno Fernandes Negreiros

Orientador: Prof. Dr. Paulo Roberto Brumatti

Campinas-SP
Julho, 2011

Formas quadráticas, pesos de Hamming generalizados e curvas algébricas

Este exemplar corresponde à redação final da dissertação devidamente corrigida e defendida por Diogo Bruno Fernandes Negreiros e aprovada pela comissão julgadora.

Campinas, 18 de julho de 2011

Prof. Dr. Paulo Roberto Brumatti
Orientador

Banca examinadora:

1. Prof. Dr. Paulo Roberto Brumatti
2. Prof. Dr. Fernando Eduardo Torres Orihuela
3. Prof. Dr. Cícero Fernandes de Carvalho

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

FICHA CATALOGRÁFICA ELABORADA POR
MARIA FABIANA BEZERRA MÜLLER - CRB8/6162
BIBLIOTECA DO INSTITUTO DE MATEMÁTICA, ESTATÍSTICA E
COMPUTAÇÃO CIENTÍFICA - UNICAMP

N312f

Negreiros, Diogo Bruno Fernandes, 1983-
Formas quadráticas, pesos de Hamming generalizados e curvas algébricas / Diogo Bruno Fernandes Negreiros. – Campinas, SP: [s.n.], 2011.

Orientador: Paulo Roberto Brumatti.
Dissertação (mestrado) – Universidade Estadual de Campinas, Instituto de Matemática, Estatística e Computação Científica.

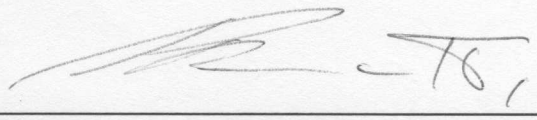
1. Corpos finitos (Álgebra). 2. Formas quadráticas. 3. Códigos de controle de erros (Teoria da informação). 4. Peso generalizado de Hamming. 5. Curvas algébricas. I. Brumatti, Paulo Roberto, 1950-. II. Universidade Estadual de Campinas. Instituto de Matemática, Estatística e Computação Científica. III. Título.

Informações para Biblioteca Digital

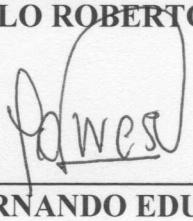
Título em inglês: Quadratic forms, generalized Hamming weights and algebraic curves
Palavras-chave em Inglês:
Finite fields (Algebra)
Quadratic forms
Algebraic curves
Generalized Hamming weight
Área de concentração: Matemática
Titulação: Mestre em Matemática
Banca examinadora:
Paulo Roberto Brumatti [Orientador]
Fernando Eduardo Torres Orihuela
Cícero Fernandes de Carvalho
Data da defesa: 18-07-2011
Programa de Pós Graduação: Matemática

Dissertação de Mestrado defendida em 18 de julho de 2011 e aprovada

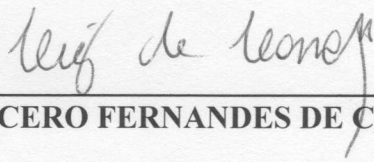
Pela Banca Examinadora composta pelos Profs. Drs.



Prof.(a). Dr(a). PAULO ROBERTO BRUMATTI



Prof. (a). Dr (a). FERNANDO EDUARDO TORRES ORIHUELA



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

Resumo

Este texto tem como objetivo o estudo de um tipo de código que possui relações com as teorias de curvas algébricas e de formas quadráticas. Começaremos introduzindo as definições e resultados sobre as três teorias que serão necessárias a este estudo. Depois apresentaremos os códigos a serem estudados bem como as relações entre seus sub-códigos e curvas algébricas e entre suas palavras e formas quadráticas. Observando que sub-códigos de peso mais baixo correspondem a curvas com mais pontos, nos dedicaremos a obter um processo para a descoberta de sub-códigos de peso mínimo dentro deste tipo de código. Tal processo será possível através de investigações sobre as formas quadráticas associadas a palavras. Finalizaremos com exemplos de aplicações do processo em alguns códigos, o que permite também calcular seus pesos de Hamming generalizados de ordem mais baixa.

Abstract

This text's objective is the study of a kind of code wich has relations with the theories of algebraic curves and quadratic forms. We start by introducing definitions and results about the three theories we will need in such study. Later, we present the codes wich will be studied along with relations between its subcodes and algebraic curves and between its words and quadratic forms. Noting that lower weight subcodes correspond to curves with more points, we research a process to find minimum weight subcodes in this kind of code. This process will be possible through investigations on the quadratic forms related to words. Finally we set examples of applications of the process on some codes, and that gives us their lower order generalized Hamming weights.

Agradecimentos

Agradeço:

Minha mãe e meu pai por me incentivarem e darem as condições necessárias aos meus estudos, e também a minha irmã pela ajuda financeira no momento em que eu mais necessitei.

A toda minha família por serem as pessoas agradáveis, divertidas e amorosas que são, renovando meu ânimo a cada visita.

Ao professor Brumatti por sua paciência e atenção ao me orientar neste trabalho.

Aos colegas de curso, tanto da graduação quanto da pós por tornarem os momentos de estudo mais eficientes e agradáveis.

À CAPES e ao CNPq pelo apoio financeiro.

Sumário

Introdução

Curvas algébricas e códigos lineares são dois objetos matemáticos tradicionalmente interligados. Neste trabalho veremos que também é possível utilizar a teoria de formas quadráticas para se obter informações adicionais sobre os dois temas. O entrelaçamento entre as três teorias abordadas neste texto será feito através de um tipo de código binário peculiar, o qual será um sub-código de um código de Reed-Muller perfurado. Os pesos das palavras deste código estarão relacionadas ao número de pontos de curvas planas de Artin-Schreier. Com base nesta relação, estabeleceremos uma nova entre pesos de sub-códigos e número de pontos de curvas, que desta vez não serão mais planas. Observando que sub-códigos de peso mais baixo serão ligados a curvas com mais pontos, torna-se interessante calcular os pesos de Hamming generalizados deste código. Esta tarefa será facilitada pela criação de sub-códigos de peso mínimo, o que será feito através da criação de formas quadráticas que induzem palavras de peso mínimo dentro do nosso código.

No primeiro capítulo definiremos e apresentaremos a teoria que se fará necessária sobre os três conceitos a serem trabalhados: curvas algébricas, códigos lineares e formas quadráticas sobre um corpo de característica 2. E como tudo será feito sobre corpos finitos, explicitaremos também alguma teoria a respeito. A maioria dos resultados serão apenas citados, com exceção das seções referentes a códigos e formas quadráticas. Sobre a teoria de códigos serão elaborados resultados visando facilitar o cálculo dos pesos de Hamming generalizados. Já no caso da teoria de formas quadráticas, como a característica 2 não é tão facilmente abordada bibliograficamente, teremos sobre ela algumas demonstrações.

Já no segundo capítulo, apresentaremos o código que é o tema central deste texto, o qual será determinado por dois números naturais m e h, com $h \leq m/2$. Uma vez escolhidos estes dois números, toma-se o conjunto dos polinômios linearizados, com coeficientes no corpo com 2^m elementos, cujos

graus são limitados por 2^h e o código está completamente determinado por este conjunto. Este capítulo também incluirá as relações das palavras deste código com as curvas de Artin-Schreier e com funções quadráticas, bem como a construção de curvas ligadas a sub-códigos, junto com a fórmula que liga o peso destes ao número de pontos daquelas.

Concluiremos com o terceiro capítulo onde será elaborado um método para se obter sub-códigos de peso mínimo no nosso código. Este método consiste em construir um conjunto de funções quadráticas que induzem palavras de peso mínimo e avaliar a dimensão do código constituído por estas palavras. Serão necessárias abordagens ligeiramente diferentes quanto à escolha de m, nos casos deste número ser par ou ímpar. Também ilustraremos a aplicação do método com alguns exemplos para certas escolhas de h, incluindo exemplos mais específicos ainda onde escolhe-se h e m.

O texto aqui escrito foi baseado no artigo [G-V 3], de Gerald van der Geer e Marcel van der Vlugt. Também foram utilizados conteúdos dos artigos [G-V 1] e [G-V 2] dos mesmos autores, já que muito do primeiro artigo citado se baseia neles.

Capítulo 1

Noções básicas

Faremos neste capítulo a introdução dos conceitos básicos que serão explorados e interligados neste trabalho: as curvas algébricas, os códigos lineares e as formas quadráticas. Antes de tudo, porém, precisaremos introduzir alguns conceitos sobre corpos finitos.

1.1 Corpos finitos

Como este trabalho será todo desenvolvido sobre corpos finitos, vários resultados sobre o assunto serão necessários, os quais serão apresentados aqui junto com a notação que adotaremos para os objetos relacionados ao tema. A referência básica para o assunto é [L-N].

Todo corpo finito é uma extensão algébrica finita do corpo $\mathbb{Z}_p$ das classes de congruência módulo p, onde p é um primo. Sendo extensão algébrica, ele é também um espaço vetorial sobre $\mathbb{Z}_p$, tendo, portanto, p^m elementos, onde m é a sua dimensão. Denotaremos por $\mathbf{F}_q$ o corpo com q elementos, onde $q = p^m$ para algum primo p e um número natural m. Desta forma escreveremos $\mathbf{F}_p$ no lugar de $\mathbb{Z}_p$. Podemos utilizar esta notação sem problemas pois o corpo com q elementos é único a menos de isomorfismo. Outra característica importante de $\mathbf{F}_q$ como extensão algébrica de $\mathbf{F}_p$ é que este é o corpo de raízes do polinômio $X^q - X \in \mathbf{F}_p[X]$.

Dado um corpo finito $\mathbf{F}_q$, qualquer extensão finita deste é um corpo $\mathbf{F}_{q^n}$ com n natural, ou seja, um corpo com p^{mn} elementos. Por outro lado temos também que qualquer sub-corpo de $\mathbf{F}_q$ é um corpo $\mathbf{F}_{p^n}$ onde n divide m.

Dado $\mathbf{F}_{q^n}$ extensão de $\mathbf{F}_q$, o grupo dos $\mathbf{F}_q$-automorfismos de $\mathbf{F}_{q^n}$ é cíclico de ordem n, gerado pelo automorfismo $\sigma : \mathbf{F}_{q^n} \to \mathbf{F}_{q^n}$ definido por $\sigma(x) = x^q$. Um parâmetro importante relacionando $\mathbf{F}_{q^n}$ a $\mathbf{F}_q$ é a chamada *função traço*, definida por:

$$\begin{aligned} Tr_{\mathbf{F}_{q^n}/\mathbf{F}_q} : \mathbf{F}_{q^n} &\to \mathbf{F}_q \\ x &\mapsto \sum_{j=0}^{n-1} \sigma^j(x) = \sum_{j=0}^{n-1} x^{q^j}. \end{aligned}$$

Esta função exercerá um papel central neste texto, e algumas das características dela que serão úteis se encontram na proposição abaixo, que é fruto dos Teoremas 2.23, 2.25 e 2.26 de [L-N].

Proposição 1.1.1: *Dado $\mathbf{F}_{q^n}$ extensão de $\mathbf{F}_q$, a função $Tr_{\mathbf{F}_{q^n}/\mathbf{F}_q}$ satisfaz:*

1. *$Tr_{\mathbf{F}_{q^n}/\mathbf{F}_q}$ é uma transformação linear sobrejetiva quando consideramos os dois corpos como $\mathbf{F}_q$-espaços vetoriais.*
2. *$Tr_{\mathbf{F}_{q^n}/\mathbf{F}_q}(\alpha) = 0$ se, e somente se, $\alpha = \beta^q + \beta$ para algum $\beta \in \mathbf{F}_{q^n}$.*
3. *$Tr_{\mathbf{F}_{q^n}/\mathbf{F}_p}(x) = Tr_{\mathbf{F}_q/\mathbf{F}_p}[Tr_{\mathbf{F}_{q^n}/\mathbf{F}_q}(x)]$ para cada $x \in \mathbf{F}_{q^n}$.*

Como a função que mais utilizaremos será $Tr_{\mathbf{F}_q/\mathbf{F}_p}$, esta será tratada apenas por Tr.

1.2 Curvas algébricas

Apresentaremos brevemente aqui o conceito de curvas algébricas, que serão apresentadas como um caso particular de conjuntos algébricos. Também será enunciado um critério para o isomorfismo entre variedades algébricas.

Dado um corpo $\mathbf{K}$ denotaremos por $\mathbb{A}^n(\mathbf{K})$ o conjunto das n-uplas de elementos de $\mathbf{K}$. $\mathbb{A}^n(\mathbf{K})$ (ou $\mathbb{A}^n$ quando estiver claro qual é o corpo em questão) será chamado o *n-espaço afim* sobre $\mathbf{K}$. Em particular nos referimos a $\mathbb{A}^2$ por *plano afim*. Chamamos *conjunto algébrico afim* sobre $\mathbf{K}$ a um conjunto do tipo

$$V(I) = \{(a_1, \ldots, a_n) \in \mathbb{A}^n(\mathbf{K});\ f(a_1, \ldots, a_n) = 0\ \forall f \in I\}$$

onde I é um ideal de $\mathbb{B} = \mathbf{K}[X_1, \ldots, X_n]$. Dado um conjunto algébrico afim V, definimos o ideal $\mathcal{I}(V)$ em $\mathbb{B}$ por

$$\mathcal{I}(V) = \{f(X_1, \ldots, X_n) \in \mathbb{B};\ f(a_1, \ldots, a_n) = 0\ \forall (a_1, \ldots, a_n) \in V\}.$$

Temos que $V(\mathcal{I}(V)) = V$. Mais ainda, $\mathcal{I}(V)$ é o maior ideal I que cumpre $V(I) = V$. Quando $\mathcal{I}(V)$ é um ideal primo, chamamos V de *variedade algébrica afim* ou, mais sucintamente, apenas *variedade*. Dadas duas variedades V e W em $\mathbb{A}^m$ e $\mathbb{A}^n$, respectivamente, uma função $f : V \to W$ é dita uma *função polinomial* se existem polinômios $p_1, \ldots, p_n \in \mathbf{K}[X_1, \ldots, X_m]$ tais que

$$f(a_1, \ldots, a_m) = (p_1(a_1, \ldots, a_m), \ldots, p_n(a_1, \ldots, a_m))$$

para cada $(a_1, \ldots, a_m) \in V$. Dizemos que V e W são *isomorfas* quando existem funções polinomiais $f : V \to W$ e $g : W \to V$ tais que $f \circ g$ e $g \circ f$ são as identidades em V e W, respectivamente. A cada conjunto algébrico afim V está associado o anel $\mathbf{K}[V] = \mathbb{B}/\mathcal{I}(V)$, que recebe o nome de *anel de coordenadas de V*. Assim, quando V é uma variedade, $\mathbf{K}[V]$ é um domínio de integridade. Abaixo enunciamos o resultado, de uso comum, que caracteriza o fato de duas variedades algébricas serem isomorfas.

Proposição 1.2.1: *Duas variedades algébricas afins são isomorfas se, e somente se, seus anéis de coordenadas são* $\mathbf{K}$*-isomorfos.*

A *dimensão* de um conjunto algébrico V é definida como a dimensão de Krull de $\mathbf{K}[V]$. Um conjunto algébrico de dimensão 1 é chamado de *curva algébrica*, ou apenas *curva*. Quando tal curva está definida no plano afim, a chamamos de *curva algébrica plana*. No caso em que V é uma variedade algébrica, o Teorema da normalização de Noether diz que a dimensão de V é dada pelo grau de transcendência, sobre $\mathbf{K}$, do corpo de frações de $\mathbf{K}[V]$. Além disso, a uma variedade algébrica de dimensão 1 chamamos *curva algébrica irredutível*.

Toda curva plana $C = V(I)$ pode ser definida a partir de uma equação

$$f(X, Y) = 0,$$

onde f é um polinômio tal que $I = (f)$, ou seja,

$$C = \{(x, y) \in \mathbf{K}^2;\ f(x, y) = 0\}.$$

Evidentemente a curva C será irredutível quando f for irredutível. Mais geralmente, todo conjunto algébrico $V = V(I) \subset \mathbb{A}^n$ pode ser definido a partir de um sistema

$$\begin{cases} f_1(X_1, \ldots, X_n) = 0 \\ \vdots \\ f_k(X_1, \ldots, X_n) = 0 \end{cases}$$

com $f_1, \ldots, f_k$ polinômios tais que $I = (f_1, \ldots, f_k)$. Uma boa referência para o que acabamos de descrever é o livro [F].

1.3 Códigos

O objeto principal deste texto é um código linear, um conceito que será apresentado nesta seção. Estamos principalmente interessados nos pesos de Hamming generalizados, que como o próprio nome já diz, são a generalização do peso mínimo, um importante invariante de um código.

Dados $n \in \mathbb{N}$ e um conjunto finito $\mathbf{A}$, que chamaremos de *alfabeto*, uma *palavra* de tamanho n é um elemento de $\mathbf{A}^n$. Um *código* de tamanho n sobre $\mathbf{A}$ é um subconjunto não vazio de $\mathbf{A}^n$. Vejamos agora duas definições centrais na teoria de códigos.

Definição 1.3.1: Em um código $C \subset \mathbf{A}^n$:

1. A distância de Hamming é a função

$$\begin{aligned} d : & C \times C \to \{0, \ldots, n\} \\ & (x, y) \mapsto \#\{i \in \{1, \ldots, n\};\ x_i \neq y_i\}. \end{aligned}$$

2. A distância mínima de um código é o mínimo que a distância de Hamming assume entre duas palavras distintas deste código.

Como a função acima é uma métrica em $\mathbf{A}^n$, um código forma um espaço métrico quando considerada sobre ele a distância de Hamming. Em um código corretor de erros, sua distância mínima d é um parâmetro importante pois nele é possível corrigir até $[d - 1/2]$ erros de uma palavra recebida.

Quando o alfabeto é um corpo finito $\mathbb{F}_q$ e o código é um sub-espaço vetorial de $(\mathbb{F}_q)^n$, dizemos que este é um código *linear* de tamanho n. A um

sub-espaço vetorial de um código linear chamamos *sub-código*. Seja $\mathscr{C}$ um código linear de tamanho n sobre $\mathbf{F}_q$. Chamamos $w(c) = d(c, 0)$ o *peso* da palavra c de $\mathscr{C}$, e o *peso mínimo de* $\mathscr{C}$ o mínimo que a função peso admite nas palavras não nulas. Temos então que em $\mathscr{C}$ o seu peso mínimo é igual à sua distância mínima. Também podemos definir o peso de um sub-código $\mathscr{D}$ de $\mathscr{C}$ da seguinte forma:

$$w(\mathscr{D}) = \#\{i \in \{1, \ldots, n\};\ \exists\ c \in \mathscr{D} \text{ tal que } c_i \neq 0\}.$$

Finalmente, definimos o *r-ésimo peso de Hamming generalizado* de $\mathscr{C}$ por

$$d_r(\mathscr{C}) = min\{w(\mathscr{D});\ \mathscr{D} \text{ sub-espaço } r\text{-dimensional de } \mathscr{C}\}.$$

A seguir teremos o primeiro dos dois únicos resultados apresentados nesta seção, os quais nos darão uma vantagem computacional.

Proposição 1.3.2: *Para cada $\mathscr{D}$ sub-código de $\mathscr{C}$ vale*

$$w(\mathscr{D}) = \frac{1}{q^d - q^{d-1}} \sum_{c \in \mathscr{D}} w(c),$$

onde $d = dim(\mathscr{D})$.

Demonstração: Seja $\pi_i : (\mathbf{F}_q)^n \to \mathbf{F}_q$ para cada $i \in \{1, \ldots, n\}$ a projeção na i-ésima coordenada e $\rho : \mathbf{F}_q \to \mathbb{Z}_{\geq 0}$ definido por $\rho(x) = 1$, se $x \neq 0$, e $\rho(0) = 0$. Deste modo, para cada $c \in (\mathbf{F}_q)^n$,

$$w(c) = \sum_{i=1}^{n} \rho \circ \pi_i(c).$$

Agora tomando $Z = \{i \in \{1, \ldots, n\};\ \pi_i(c) = 0\ \forall c \in \mathscr{D}\}$ temos que $i \notin Z$ implica $dim(ker(\pi_i) \cap \mathscr{D}) = d - 1$, ou seja, $\#ker(\pi_i) \cap \mathscr{D} = q^{d-1}$, e assim

$$\sum_{c \in \mathscr{D}} \rho \circ \pi_i(c) = q^d - q^{d-1}.$$

Com isso

$$\begin{aligned}\sum_{c\in\mathscr{D}} w(c) &= \sum_{c\in\mathscr{D}}\sum_{i=1}^{n} \rho\circ\pi_i(c)\\ &= \sum_{i=1}^{n}\sum_{c\in\mathscr{D}} \rho\circ\pi_i(c)\\ &= \sum_{i\notin Z}\sum_{c\in\mathscr{D}} \rho\circ\pi_i(c)\\ &= \sum_{i\notin Z}(q^d - q^{d-1})\\ &= w(\mathscr{D})(q^d - q^{d-1}).\end{aligned}$$

□

Quando num sub-código toda palavra não nula tiver o peso mínimo do código, o chamaremos de um *sub-código de peso mínimo*. É fácil ver que sub-códigos de um sub-código de peso mínimo também são de peso mínimo. Ainda a respeito desta definição temos o corolário abaixo.

Corolário 1.3.3: *Se em $\mathscr{C}$ existe um sub-código $\mathscr{D}$ de peso mínimo e dimensão r, então vale a seguinte fórmula:*

$$d_r(\mathscr{C}) = \frac{q^r - 1}{q^r - q^{r-1}} d_1(\mathscr{C}).$$

Demonstração: Basta observar que se $c \in \mathscr{C} \setminus \{0\}$ tem o peso mínimo, então

$$d_1(\mathscr{C}) = w(\mathbf{F}_q \cdot c) = w(c)$$

e

$$d_r(\mathscr{C}) = w(\mathscr{D}) = \frac{1}{q^r - q^{r-1}} \sum_{d\in\mathscr{D}} w(d) = \frac{q^r - 1}{q^r - q^{r-1}} w(c)$$

□

Os códigos que exploraremos neste trabalho são todos pertencentes à família dos códigos de Reed-Muller, que serão apresentados agora. Tomando a função de avaliação

$$\begin{aligned}\beta : \mathbf{F}_q[X_1,\ldots,X_m] &\to (\mathbf{F}_q)^{q^m}\\ f &\mapsto (f(v))_{v\in(\mathbf{F}_q)^m},\end{aligned}$$

e o conjunto

$$P_r = \{f \in \mathbf{F}_q[X_1,\ldots,X_m];\ grau(f) \leq r\},$$

definimos o *código de Reed-Muller* de r-ésima ordem sobre $\mathbf{F}_q$ de comprimento q^m por

$$\mathscr{R}(r,m) = \beta(P_r).$$

Este conjunto é de fato um código linear pois a aplicação avaliação é $\mathbf{F}_q$-linear. Fazendo uma ligeira alteração nesta aplicação de modo a obter

$$\beta^*(f) = (f(v))_{v\in(\mathbf{F}_q)^m\setminus\{0\}},$$

podemos definir o código de comprimento $q^m - 1$

$$\mathscr{R}^*(r,m) = \beta^*(P_r),$$

que chamaremos de *código de Reed-Muller perfurado*.

1.4 Formas quadráticas sobre um corpo de característica 2

Existe uma vasta bibliografia abordando a teoria de formas quadráticas. Porém, como o caso de interesse é sobre um corpo de característica 2, que nem todos os livros escolhem contemplar, aqui serão desenvolvidos alguns resultados sobre o assunto.

Uma *n-forma quadrática* sobre um corpo $\mathbf{K}$ é um polinômio homogêneo de grau 2 em até n variáveis com coeficientes neste corpo ou o polinômio nulo, ou seja, um polinômio da forma

$$\sum_{\substack{i=1\\ j\geq i}}^{n} a_{ij}X_iX_j,$$

onde os coeficientes $a_{ij} \in \mathbf{K}$ estão unicamente determinados. Deste modo, uma n-forma quadrática pode ser vista como k-forma quadrática para cada $k > n$, o que faz sentido já que sempre podemos incluir $\mathbf{K}[X_1,\ldots,X_n]$ em $\mathbf{K}[X_1,\ldots,X_{n+1}]$.

Mais abrangente que o conceito de forma quadrática é o de função quadrática, o qual será mais utilizado neste texto do que o anterior. Dados V um $\mathbf{K}$-espaço vetorial e $\varphi : V \to \mathbf{K}$ uma função, dizemos que φ é uma *função quadrática* se ela satisfaz as condições:

(i) $\forall (a, x) \in \mathbf{K} \times V$, $\varphi(ax) = a^2\varphi(x)$;

(ii) $B_\varphi(x, y) = \varphi(x + y) - \varphi(x) - \varphi(y)$ define uma forma bilinear simétrica de $V \times V$ em $\mathbf{K}$.

Neste caso nos referimos ao par (V, φ) por *espaço quadrático*. É fácil ver que se tivermos α e β funcionais lineares de V em $\mathbf{K}$ e definirmos, para cada $x \in V$, $\varphi(x) = \alpha(x) \cdot \beta(x)$, então (V, φ) forma um espaço quadrático. Dada uma n-forma quadrática Q tem-se que

$$\begin{aligned} Q : \quad \mathbf{K}^n \quad &\to \quad \mathbf{K} \\ (x_1, \ldots, x_n) &\mapsto Q(x_1, \ldots, x_n), \end{aligned}$$

é uma função quadrática, a qual será frequentemente tratada como a própria forma, uma vez que duas formas quadráticas são iguais se, e somente se, elas coincidem como funções. Também é verdade que cada função quadrática cujo domínio é $\mathbf{K}^n$ determina uma única n-forma quadrática, um fato que será verificado mais a frente no caso de corpos de característica 2.

Chamamos dois espaços quadráticos (V, φ) e (W, ψ) de *isométricos*, denotado por $(V, \varphi) \sim (W, \psi)$, quando existe um isomorfismo $T : V \to W$ tal que $\varphi = \psi \circ T$. Além disso, duas n-formas quadráticas Q e R serão ditas *equivalentes*, ou $Q \sim R$, quando tivermos $(\mathbf{K}^n, Q) \sim (\mathbf{K}^n, R)$. Em outras palavras, duas formas quadráticas são equivalentes se existe uma mudança linear não singular de variáveis que transforma uma na outra. Chamamos de *posto* da forma quadrática Q o inteiro não negativo

$$min\{n \in \mathbb{Z}_{\geq 0};\ \text{existe R } n\text{-forma quadrática tal que } Q \sim R\}.$$

Além disso, uma n-forma quadrática é dita *degenerada* se seu posto é menor que n. Extenderemos este conceito para espaços quadráticos dizendo que uma função quadrática $\varphi : V \to \mathbf{K}$ é degenerada quando existe um isomorfismo $T : \mathbf{K}^n \to V$, $n = dim\ V$, tal que $\varphi \circ T$ não depende de x_n.

Dadas (V, φ) e (W, ψ) espaços quadráticos sobre $\mathbf{K}$ podemos definir

$$\begin{aligned} \varphi \oplus \psi : V \oplus W &\to \mathbf{K} \\ v + w &\mapsto \varphi(v) + \psi(w) \end{aligned}$$

e assim temos o espaço quadrático $(V \oplus W, \varphi \oplus \psi)$.

Consideremos de agora em diante $\mathbf{K}$ um corpo com característica 2. Comecemos verificando um resultado já prometido anteriormente.

Proposição 1.4.1: *Dada $\varphi : \mathbf{K}^n \to \mathbf{K}$ função quadrática existe uma única n-forma quadrática Q_φ tal que*

$$\varphi(x_1, \ldots, x_n) = Q_\varphi(x_1, \ldots, x_n) \ \forall (x_1, \ldots, x_n) \in \mathbf{K}^n.$$

Demonstração: Considere $e_1, \ldots, e_n$ a base canônica de $\mathbf{K}^n$ e B_φ a forma bilinear simétrica associada a φ. Agora tome para cada $(i, j) \in \{1, \ldots, n\}^2$ com $j \geq i$

$$a_{ij} = \begin{cases} \varphi(e_i), \text{ se } i = j \\ B_\varphi(e_i, e_j), \text{ se } j > i \end{cases}$$

Tomando

$$Q_\varphi(X_1, \ldots, X_n) = \sum_{\substack{i=1 \\ j \geq i}}^{n} a_{ij} X_i X_j$$

temos que para cada $(x_1, \ldots, x_n) \in \mathbf{K}^n$

$$\begin{aligned} \varphi(x_1, \ldots, x_n) &= \varphi\left(\sum_{i=1}^{n} x_i e_i\right) \\ &= \varphi(x_1 e_1) + \varphi\left(\sum_{i=2}^{n} x_i e_i\right) + B\left(x_1 e_1, \sum_{i=2}^{n} x_i e_i\right) \\ &= a_{11} x_1^2 + \varphi\left(\sum_{i=2}^{n} x_i e_i\right) + \sum_{j=2}^{n} a_{1j} x_1 x_j \end{aligned}$$

e prosseguindo com o mesmo raciocínio chegamos a

$$\begin{aligned} \varphi(x_1, \ldots, x_n) &= \sum_{i=1}^{n} a_{ii} x_i^2 + \sum_{i=1}^{n-1} \sum_{j=i+1}^{n} a_{ij} x_i x_j \\ &= \sum_{i=1}^{n} \sum_{j \geq i}^{n} a_{ij} x_i x_j \\ &= Q_\varphi(x_1, \ldots, x_n). \end{aligned}$$

□

Chamamos B_φ, definida em (ii), de forma bilinear associada a (V, φ). Para cada S sub-espaço vetorial de V, definimos o sub-espaço ortogonal a S por

$$S^\perp = \{x \in V; \ B_\varphi(x, y) = 0 \ \forall y \in S\}.$$

Chamamos o radical de φ, ou $rad\ \varphi$, o conjunto $V^\perp$.

Teorema 1.4.2: *Dado (V, φ) espaço quadrático sobre $\mathbf{K}$ e $U \subset V$ sub-espaço tal que $V = U \oplus rad\ \varphi$. Então tem-se:*

1. *$rad\ (\varphi|_U) = \{0\}$*
2. *$rad\ \varphi$ é soma ortogonal de sub-espaços unidimensionais;*
3. *U é soma ortogonal de sub-espaços bidimensionais.*

Demonstração: Para se provar 1 basta observar que $rad\ \varphi|_U = (rad\ \varphi) \cap U$. O item 2 é consequência imediata do fato de qualquer base de $rad\ \varphi$ ser ortogonal.
A prova de 3. será feita por indução sobre a dimensão de U. Se $dim(U) = 0$ não há nada a fazer. Supondo $dim(U) > 0$ e tomando $v_1 \in U \setminus \{0\}$, como $v_1 \notin rad\ \varphi|_U$, existe $v_2 \in U$ tal que $B_\varphi(v_1, v_2) \neq 0$. Além disso,

$$B_\varphi(v_1, v_1) = \varphi(v_1 + v_1) + \varphi(v_1) + \varphi(v_1) = 0,$$

logo v_1 e v_2 são linearmente independentes, por onde segue que o sub-espaço $U_1 = \mathbf{F}_q \cdot v_1 + \mathbf{F}_q \cdot v_2$ tem dimensão 2. Tomando $U_2 = {U_1}^\perp \cap U$ temos $U = U_1 \oplus U_2$. Daí segue que $rad\ \varphi|_{U_2} = 0$ e aplicando a hipótese de indução em U_2 temos o resultado. □

Esta descrição de V em sub-espaços ortogonais é útil pois para cada $x \in V$, se $y \in rad\ \varphi$, então

$$\varphi(x + y) = \varphi(x) + \varphi(y) + B_\varphi(x, y) = \varphi(x) + \varphi(y),$$

donde temos que $\varphi = \varphi|_U \oplus \varphi|_{rad\ \varphi}$ para cada U tal que $V = rad\ \varphi \oplus U$. Tal observação será útil na demonstração da próxima proposição.

Proposição 1.4.3: *Uma função quadrática $\varphi : V \to \mathbf{K}$ é degenerada se, e somente se, existe $z \in rad\ \varphi \setminus \{0\}$ tal que $\varphi(z) = 0$.*

Demonstração: Suponha que existe $T : \mathbf{K}^n \to V$ isomorfismo linear tal que $\psi = \varphi \circ T$ independe de x_n. Como

$$\psi(x_1, \ldots, x_{n-1}, x_n) = \psi(x_1, \ldots, x_{n-1}, 0)$$

para todo $(x_1, \ldots, x_{n-1}, x_n) \in \mathbf{K}^n$,

$$\psi(0, \ldots, 0, 1) = \psi(0, \ldots, 0, 0) = 0.$$

Então tomando $z = T(0, \ldots, 0, 1)$, temos que $\varphi(z) = 0$ e

$$\begin{aligned} B_\varphi(x, z) &= \varphi(x + z) + \varphi(x) + \varphi(z) \\ &= \varphi(T(T^{-1}(x) + T^{-1}(z))) + \varphi(x) \\ &= \psi(T^{-1}(x) + (0, \ldots, 0, 1)) + \varphi(x) \\ &= \psi(T^{-1}(x)) + \varphi(x) \\ &= \varphi(T(T^{-1}(x))) + \varphi(x) \\ &= \varphi(x) + \varphi(x) = 0, \end{aligned}$$

para cada $x \in \mathbf{K}^n$, ou seja, $z \in rad\ \varphi$. Agora para a volta, tome $U \subset V$ tal que $V = rad\ \varphi \oplus U$, $T_1 : \mathbf{K}^m \to U$ e $T_2 : \mathbf{K}^{n-m} \to rad\ \varphi$ isomorfismos. Segue que

$$\begin{aligned} T : \quad \mathbf{K}^n \quad &\to V \\ (x_1, \ldots, x_n) &\mapsto T_1(x_1, \ldots, x_m) + T_2(x_{m+1}, \ldots, x_n) \end{aligned}$$

é isomorfismo e $\varphi \circ T = \varphi \circ T_1 + \varphi \circ T_2$. Portanto, podemos nos restringir ao caso em que $rad\ \varphi = V$. Neste caso, tomando $v_1, \ldots, v_n$ base de V e $d_i = \varphi(v_i)$, temos para cada $(x_1, \ldots, x_n) \in \mathbf{K}^n$

$$\varphi\left(\sum_{i=1}^{n} x_i v_i\right) = \sum_{i=1}^{n} d_i x_i^2.$$

Com isso, se $\varphi(z) = 0$ com $z \neq 0$, e aqui podemos supor $z = \sum_{i=1}^{n} z_i v_i$ com $z_n \neq 0$,

$$\sum_{i=1}^{n} d_i z_i^2 = 0.$$

Considerando

$$\begin{aligned} T : \quad \mathbf{K}^n \quad &\to V \\ (x_1, \ldots, x_n) &\mapsto \sum_{i=1}^{n-1} \left(x_i + \frac{z_i}{z_n} x_n\right) v_i \ + x_n v_n \end{aligned}$$

temos para cada $(x_1, \ldots, x_n) \in \mathbf{K}^n$

$$\begin{aligned}\varphi(T(x_1, \ldots, x_n)) &= \sum_{i=1}^{n-1} d_i \left(x_i + \frac{z_i}{z_n} x_n \right)^2 + d_n x_n^2 \\ &= \sum_{i=1}^{n} d_i x_i^2 + \frac{x_n^2}{z_n^2} \sum_{i=1}^{n-1} d_i z_i^2 \\ &= \sum_{i=1}^{n} d_i x_i^2 + \frac{x_n^2}{z_n^2} d_n z_n^2 \\ &= \sum_{i=1}^{n-1} d_i x_i^2 \end{aligned}$$

□

Os resultados apresentados até aqui foram baseados na seção 1.4 de [P]. Também utilizaremos, para cada n-forma quadrática Q, a notação $N(Q)$ para a cardinalidade do conjunto solução da equação $Q(X_1, \ldots, X_n) = 0$. A proposição enunciada abaixo é derivada dos Teoremas 6.30 e 6.32 de [L-N] e não será demonstrada neste texto.

Teorema 1.4.4: *Seja Q uma n-forma quadrática não degenerada sobre $\mathbf{F}_q$. Se n é ímpar,*

$$Q \sim X_1X_2 + X_3X_4 + \ldots + X_{n-2}X_{n-1} + X_n^2$$

e $N(Q) = q^{n-1}$. Se n é par, então

$$Q \sim X_1X_2 + X_3X_4 + \ldots + X_{n-1}X_n,$$

e $N(Q) = q^{n-1} + (q-1)q^{(n-2)/2}$ ou

$$Q \sim X_1X_2 + X_3X_4 + \ldots + X_{n-1}X_n + X_{n-1}^2 + aX_n^2,$$

e $N(Q) = q^{n-1} - (q-1)q^{(n-2)/2}$, onde $a \in \mathbf{F}_q$ satisfaz $Tr(a) = 1$.

Como não trataremos apenas de formas quadráticas não degeneradas, precisaremos da proposição abaixo.

Proposição 1.4.5: *Sejam Q uma n-forma quadrática sobre $\mathbf{F}_q$ de posto k e R uma k-forma tal que $Q \sim R$. Então $N(Q) = q^{n-k}N(R)$.*

Demonstração: Tomando T automorfismo linear de $(\mathbf{F}_q)^n$ tal que $R = Q \circ T$, como a função quadrática induzida por R não depende das $n - k$ últimas coordenadas, o conjunto solução de $Q \circ T(X_1, \ldots, X_n) = 0$ é dado por

$$\{(x_1, \ldots, x_n) \in (\mathbf{F}_q)^n;\ R(x_1, \ldots, x_k) = 0\}$$

e este conjunto está em bijeção com $N(Q)$. □

Podemos adotar, para uma função quadrática $\varphi : V \to \mathbf{K}$,

$$N(\varphi) = \#\{x \in V;\ \varphi(x) = 0\}.$$

Para generalizar os dois resultados acima para funções quadráticas basta tomar um isomorfismo $T : \mathbf{K}^n \to V$ e considerar a função quadrática $\varphi \circ T$, que terá uma forma quadrática associada, pela Proposição 1.4.1, equivalente a φ. As soluções desta forma quadrática serão trazidas à função quadrática original por intermédio de T.

Capítulo 2

O código $\mathscr{C}_h$

Este capítulo se dedicará à construção de um tipo particular de código e ao estudo de suas relações com as teorias de curvas algébricas e formas quadráticas. Tais relações permitem um intercâmbio de informações entre sub-códigos deste código e algumas curvas algébricas. Fazemos aqui a breve apresentação deste código para tratar das relações com as outras teorias nas seções que seguirão. Seja $q = 2^m$ com $1 < m \in \mathbb{N}$. Para algum $0 < h \leq [m/2]$ considere

$$R_h = \left\{ \sum_{i=0}^{h} a_i X^{2^i};\ a_i \in \mathbf{F}_q \right\}.$$

Este conjunto, por ser um espaço vetorial sobre $\mathbf{F}_q$, também o é sobre $\mathbf{F}_2$. Os polinômios que o constituem são ditos linearizados pois $f \in R_h$ implica

$$f(x+y) = f(x) + f(y)\ \forall x, y \in \mathbf{F}_q.$$

Temos então o código binário de tamanho $q-1$

$$\mathscr{C}_h = \{\mathcal{C}_R = (Tr[xR(x)])_{x \in \mathbf{F}_q^*};\ R \in R_h\}$$

sobre o qual trabalharemos de aqui em diante até o final do capítulo.

2.1 Códigos e curvas

Palavras de $\mathscr{C}_h$ se identificam com curvas planas assim como sub-códigos de dimensão d com curvas em $\mathbb{A}^{d+1}$. Estas identificações ligam sub-códigos de

peso menor a curvas com mais pontos.

A cada palavra $\mathcal{C}_R$ deste código associamos a curva de Artin-Schreier C_R em $\mathbb{A}^2(\mathbf{F}_q)$ definida pela equação

$$Y^2 + Y = XR(X).$$

Verificamos a irredutibilidade do polinômio $Y^2+Y+XR(X)$ observando que para termos um polinômio do tipo $Y^2+Y+f(X)$ redutível sobre $(\mathbf{F}_q[X])[Y]$ deve existir $g(X) \in \mathbf{F}_q[X]$ tal que $g(X)^2 + g(X) = f(X)$, implicando num $f(X)$ de grau par. A associação feita entre $\mathcal{C}_R$ e C_R se justifica em virtude da proposição abaixo.

Proposição 2.1.1:

$$w(\mathcal{C}_R) = q - \frac{\#C_R}{2}$$

Demonstração: Sabemos que

$$\#C_R = \sum_{x \in \mathbf{F}_q} \#\{y \in \mathbf{F}_q;\ xR(x) = y^2 + y\}.$$

Porém, observe que o polinômio Y^2+Y tem 2 raízes, 0 e 1. Além disso, para cada $t \in \mathbf{F}_q$, se $y^p + y = t$, então $(y+1)^2 + (y+1) = t$. Ou seja, o polinômio $Y^2 + Y + t$, quando tem raízes em $\mathbf{F}_q$, tem exatamente 2. Segue pelo item 2 do Teorema 1.1.1 que

$$\#\{y \in \mathbf{F}_q;\ xR(x) = y^2 + y\} = \begin{cases} 2, & \text{se } Tr[xR(x)] = 0, \\ 0, & \text{se } Tr[xR(x)] \neq 0. \end{cases}$$

Tem-se então que

$$\begin{aligned} \#C_R &= 2(\#\{x \in \mathbf{F}_q;\ Tr[xR(x)] = 0\}) \\ &= 2(1 + \#\{x \in {\mathbf{F}_q}^*;\ Tr[xR(x)] = 0\}). \end{aligned}$$

E como

$$w(\mathcal{C}_R) = q - 1 - \#\{x \in \mathbf{F}_q^*;\ Tr[xR(x)] = 0\},$$

conseguimos

$$\#C_R = 2(q - w(\mathcal{C}_R)).$$ □

Também para um sub-código $\mathscr{D}$ de $\mathscr{C}_h$ associamos uma curva. Tomando $\mathcal{C}_{R_1}, \ldots, \mathcal{C}_{R_t}$ base de $\mathscr{D}$, definimos a curva afim $C^{(\mathscr{D})} \subset \mathbb{A}^{t+1}(\mathbf{F}_q)$ dada pelo sistema

$$\begin{cases} Y_1^2 + Y_1 &= XR_1(X) \\ & \vdots \\ Y_t^2 + Y_t &= XR_t(X). \end{cases}$$

Porém, esta definição depende da escolha de uma base. É necessário saber até onde a curva está determinada por esta escolha.

Lema 2.1.2: *A curva $C^{(\mathscr{D})}$, a menos de isomorfismo, independente da base de $\mathscr{D}$.*

Demonstração: Sejam $\mathcal{C}_{R_1}, \ldots, \mathcal{C}_{R_t}$ e $\mathcal{C}_{S_1}, \ldots, \mathcal{C}_{S_t}$ bases de $\mathscr{D}$. Devemos ter $R_1, \ldots, R_t$ linearmente independentes, já que a função $R \mapsto (Tr[xR(x)])_{x \in \mathbf{F}_q^*}$ é $\mathbf{F}_2$-linear. O mesmo ocorre para $S_1, \ldots, S_t$, portanto, temos

$$\begin{pmatrix} R_1 \\ \vdots \\ R_t \end{pmatrix} = A \begin{pmatrix} S_1 \\ \vdots \\ S_t \end{pmatrix}.$$

para algum $A \in GL(t, \mathbf{F}_2) \subset GL(t, \mathbf{F}_q)$. Com isso, consideremos o homomorfismo induzido da $\mathbf{F}_q$-transformação linear

$$\varphi : \mathbf{F}_q[X, Y_1, \ldots, Y_t] \to \mathbf{F}_q[X, Y_1, \ldots, Y_t]$$

definida por $\varphi \mid_{\mathbf{F}_q[X]} = Id$ e

$$\begin{pmatrix} \varphi(Y_1) \\ \vdots \\ \varphi(Y_t) \end{pmatrix} = A \begin{pmatrix} Y_1 \\ \vdots \\ Y_t \end{pmatrix}.$$

Este será automorfismo, já que o seu inverso pode ser obtido de maneira semelhante utilizando A^{-1} no lugar de A. Agora tome, em $\mathbf{F}_q[X, Y_1, \ldots, Y_s]$, I o ideal gerado pelos polinômios $Y_i^2 + Y_i + XR_i(X)$, e J o gerado pelos

polinômios $Y_i^2 + Y_i + XS_i(X)$. Como

$$\begin{pmatrix} \varphi(Y_1^2 + Y_1 + XR_1(X)) \\ \vdots \\ \varphi(Y_t^2 + Y_t + XR_t(X)) \end{pmatrix} = A \begin{pmatrix} Y_1^2 + Y_1 \\ \vdots \\ Y_t^2 + Y_t \end{pmatrix} + X \begin{pmatrix} R_1(X) \\ \vdots \\ R_t(X) \end{pmatrix}$$
$$= A \begin{pmatrix} Y_1^2 + Y_1 + XS_1(X) \\ \vdots \\ Y_t^2 + Y_t + XS_t(X) \end{pmatrix}$$

e $A \in GL(t, \mathbf{F}_q)$,

$$\varphi\left(\sum_{i=1}^{t} \mathbf{F}_q \cdot [Y_i^2 + Y_i + XR_i(X)]\right) = \sum_{i=1}^{t} \mathbf{F}_q \cdot [Y_i^2 + Y_i + XS_i(X)],$$

donde, por φ ser automorfismo, segue que $\varphi(I) = J$. Temos então o isomorfismo entre $\mathbf{F}_q[X, Y_1, \ldots, Y_s]/I$ e $\mathbf{F}_q[X, Y_1, \ldots, Y_s]/J$, que são os anéis de coordenadas de $C^{(\mathscr{D})}$ com as bases $\mathcal{C}_{R_1}, \ldots, \mathcal{C}_{R_t}$ e $\mathcal{C}_{S_1}, \ldots, \mathcal{C}_{S_t}$, respectivamente. □

Desta vez, relacionamos a curva determinada por $\mathscr{D}$ e seu peso.

Proposição 2.1.3: *Dado $\mathscr{D}$ sub-código de dimensão t de $\mathscr{C}_h$, a cardinalidade da curva $C^{(\mathscr{D})}$ definida por este código e seu peso satisfazem a equação*

$$w(\mathscr{D}) = q - \frac{\#C^{(\mathscr{D})}}{2^t}$$

Demonstração: Sejam $Z = \{x \in \mathbf{F}_q^*;\ \pi_x(\mathcal{C}) = 0\ \forall \mathcal{C} \in \mathscr{D}\}$ e $z = \#Z$. Assim, $w(\mathscr{D}) = q - 1 - z$. Tem-se

$$\begin{aligned} x \in Z &\Leftrightarrow Tr[xR(x)] = 0\ \forall R \in \mathbf{F}_2 \cdot R_1 + \ldots + \mathbf{F}_2 \cdot R_t \\ &\Leftrightarrow \#\{(y_1, \ldots, y_t) \in (\mathbf{F}_q)^t;\ xR_i(x) = y_i^2 + y_i\ \forall i \in \{1, \ldots, t\}\} \neq 0 \\ &\Leftrightarrow \#\{(y_1, \ldots, y_t) \in (\mathbf{F}_q)^t;\ xR_i(x) = y_i^2 + y_i\ \forall i \in \{1, \ldots, t\}\} = 2^t. \end{aligned}$$

Com isso

$$\begin{aligned}
\#C^{(\mathscr{D})} &= \sum_{x\in\mathbf{F}_q} \#\{(y_1,\ldots,y_t)\in(\mathbf{F}_q)^t;\ xR_i(x)=y_i^2+y_i,\ 1\le i\le t\} \\
&= 2^t + \sum_{x\in\mathbf{F}_q^*} \#\{(y_1,\ldots,y_t)\in(\mathbf{F}_q)^t;\ xR_i(x)=y_i^2+y_i,\ 1\le i\le t\} \\
&= 2^t + \sum_{x\in Z} 2^t \\
&= 2^t(1+z)
\end{aligned}$$

□

Conclui-se então que quanto mais baixo for o peso de um sub-código mais pontos a curva relacionada a este terá.

2.2 Códigos e formas quadráticas

Aqui serão ligadas palavras a funções quadráticas de maneira bem direta, relacionando os pesos daquelas ao número de soluções destas.

A uma palavra não nula $\mathcal{C}_R \in \mathscr{C}_h$ também podemos associar a função quadrática sobre $\mathbf{F}_2$, com domínio em $\mathbf{F}_q$, definida por

$$Q_R(x) = Tr[xR(x)],$$

uma vez que

$$B_R(x,y) = Tr[xR(y) + yR(x)]$$

é bilinear simétrica. Portanto, se fixarmos um isomorfismo de $(\mathbf{F}_2)^m$ em $\mathbf{F}_q$, temos pela Proposição 1.4.1 que cada Q_R pode ser representado por um polinômio homogêneo de grau 2 em $\mathbf{F}_2[X_1,\ldots,X_m]$. Assim podemos ver que $\mathscr{C}_h$ é sub-código do código binário $\mathscr{R}^*(2^h,m)$.

Temos de imediato que

$$w(\mathcal{C}_R) = q - N(Q_R)$$

que combinando com a Proposição 2.1.1 leva a

$$\#C_R = 2N(Q_R).$$

Agora vamos investigar o radical das funções quadráticas obtidas desta maneira.

Proposição 2.2.1: *rad* Q_R *tem dimensão* w *com* $(m-w)$ *par.*

Demonstração: Segue do item 3 do Teorema 1.4.2. □

Proposição 2.2.2: *Se* $R = \sum_{i=0}^{h} a_i X^{2^i} \in R_h$, *então*

$$rad\ Q_R = \{x \in \mathbf{F}_q;\ E(x) = 0\},$$

onde $E(X) = (R(X))^{2^h} + \sum_{i=0}^{h} (a_i X)^{2^{h-i}}$.

Demonstração: Para cada i,

$$Tr\left[a_i x y^{2^i}\right] = Tr\left[(a_i x y^{2^i})^{2^{m-i}}\right] = Tr\left[(a_i x)^{2^{m-i}} y\right],$$

portanto,

$$Tr[xR(y)] = \sum_{i=0}^{h} Tr\left[a_i x y^{2^i}\right] = \sum_{i=0}^{h} Tr\left[(a_i x)^{2^{m-i}} y\right] = Tr\left[\sum_{i=0}^{h} (a_i x)^{2^{m-i}} y\right]$$

donde segue que

$$Tr[xR(y) + yR(x)] = Tr\left[y\left\{\sum_{i=0}^{h} (a_i x)^{2^{m-i}} \quad + R(x)\right\}\right].$$

Daí temos que $x \in rad\ Q_R$ se, e somente se,

$$\sum_{i=0}^{h} (a_i x)^{2^{m-i}} + R(x) = 0,$$

que equivale a

$$\sum_{i=0}^{h} (a_i x)^{2^{h-i}} + (R(x))^{2^h} = 0$$ □

Corolário 2.2.3: *Para cada* $R \in R_h \setminus \{0\}$, $dim(rad\ Q_R) \leq d + h$ *onde* 2^d *é o grau de* R.

Demonstração: O polinômio $E(X)$ tem grau 2^{d+h}, daí $\#rad\ Q_R \leq 2^{d+h}$, ou seja, $dim(rad\ Q_R) \leq d + h$. □

O espaço vetorial $rad\ Q_R$ contém o sub-espaço

$$\Omega_R = \{x \in rad\ Q_R;\ Q_R(x) = 0\},$$

que não é necessariamente nulo pois estamos trabalhando sobre um corpo de característica 2. Sobre a dimensão de Ω temos:

Proposição 2.2.4: *Sejam $w = dim(rad\ Q)$ e $\omega = dim(\Omega)$. Temos:*

1. *$\omega = w$ ou $\omega = w - 1$.*

2. *Se $R \in R_h \setminus \{0\}$, então o posto de Q_R é dado por $m - \omega$.*

Demonstração: 1. Segue do fato de de $Q_R|_{rad\ Q_R}$ ser um funcional linear.
2. Decorre da Proposição 1.4.3. □

Agora uma consequência das generalizações para funções quadráticas do Teorema 1.4.4 e da Proposição 1.4.5 :

Teorema 2.2.5: *Seja $w = dim(rad\ Q_R)$. Se Q_R tem posto $m-w+1$ (ímpar),*

$$Q_R \sim X_1X_2 + \ldots + X_{m-w-1}X_{m-w} + X^2_{m-w+1},$$

e $N(Q_R) = 2^{w-1} \cdot 2^{m-w} = q/2$. E se Q_R tem posto $m - w$ (par),

$$Q_R \sim X_1X_2 + \ldots + X_{m-w-1}X_{m-w}$$

e $N(Q_R) = 2^w \cdot (2^{m-w-1} + 2^{(m-w-2)/2}) = (q + \sqrt{q2^w})/2$, ou

$$Q_R \sim X_1X_2 + \ldots + X_{m-w-1}X_{m-w} + X^2_{m-w-1} + X^2_{m-w}$$

e $N(Q_R) = 2^w \cdot (2^{m-w-1} - 2^{(m-w-2)/2}) = (q - \sqrt{q2^w})/2$.

Capítulo 3

Construção de sub-códigos de peso mínimo

Neste capítulo investigaremos o código $\mathscr{C}_h$ para encontrar nele sub-códigos de peso baixo. Para a construção deste código binário devemos escolher o subconjunto R_h dentro de $\mathbf{F}_q[X]$ com $q = 2^m$ e são necessárias abordagens diferentes para quando este m é par ou ímpar.

3.1 O caso m ímpar

Esta seção trará uma série de resultados que culminarão num processo para a construção de sub-códigos de peso mínimo dentro de $\mathscr{C}_h$ através de formas quadráticas que se identificarão com palavras neste código.

Para esta seção consideraremos m ímpar com $m \geq 3$. Encontramos sub-códigos de peso mínimo em $\mathscr{C}_h$, com $0 < h \leq (m-1)/2$ através da observação que segue.

Proposição 3.1.1: *Dados $0 \leq w \leq 2h-1$ com $(m-w)$ par e um conjunto $\{a_i, b_i; i \in \{1, \ldots, (m-w)/2\}\} \subset \mathbf{F}_q$ linearmente independente sobre $\mathbf{F}_2$, a expressão*

$$\sum_{i=1}^{(m-w)/2} Tr(a_i x)Tr(b_i x), \tag{3.1.1}$$

é uma função quadrática, a qual é equivalente à forma $X_1X_2+\ldots+X_{m-w-1}X_{m-w}$ e tem $(q+\sqrt{q2^w})/2$ zeros em $\mathbf{F}_q$.

Demonstração: Começamos tomando para cada $i \in \{1, \ldots, (m-w)/2\}$

$$\varphi_i : \begin{array}{ccc} \mathbf{F}_q & \to & \mathbf{F}_2 \\ x & \mapsto & Tr(a_i x) \end{array} \quad \text{e} \quad \psi_i : \begin{array}{ccc} \mathbf{F}_q & \to & \mathbf{F}_2 \\ x & \mapsto & Tr(b_i x) \end{array}.$$

Como cada uma destas funções é $\mathbf{F}_2$-linear, $\varphi_i \cdot \psi_i$ é função quadrática para cada i, donde segue que (3.1.1) também o é. Agora observando que para qualquer $\{\alpha_i, \beta_i;\ i \in \{1, \ldots, w\}\} \subset \mathbf{F}_2$

$$\begin{aligned} & \sum_{i=1}^{(m-w)/2} \alpha_i \varphi_i + \beta_i \psi_i = 0 \\ \Leftrightarrow & \sum_{i=1}^{(m-w)/2} Tr\left[(\alpha_i a_i + \beta_i b_i)x\right] = 0 \ \forall x \in \mathbf{F}_q \\ \Leftrightarrow & \sum_{i=1}^{(m-w)/2} (\alpha_i a_i + \beta_i b_i) = 0 \\ \Leftrightarrow & \alpha_i = \beta_i = 0 \ \forall i \in \{1, \ldots, (m-w)/2\}, \end{aligned}$$

segue que $A = \{\varphi_i, \psi_i;\ i \in \{1, \ldots, (m-w)/2\}\}$ é um conjunto $\mathbf{F}_2$-linearmente independente de funcionais lineares. Tomando $\tau_i : \mathbf{F}_q \to \mathbf{F}_2$ funcional linear para cada $i \in \{1, \ldots, w\}$ de tal forma que $A \cup \{\tau_i;\ i \in \{1, \ldots, w\}\}$ forme uma base do espaço dual de $\mathbf{F}_q$, temos que a transformação linear

$$\begin{aligned} T : \mathbf{F}_q &\to (\mathbf{F}_2)^m \\ x &\mapsto (\varphi_1(x), \psi_1(x), \ldots, \varphi_{(m-w)/2}(x), \psi_{(m-w)/2}(x), \tau_1(x), \ldots, \tau_w(x)) \end{aligned}$$

é injetiva, já que se todas as coordenadas se anulassem para algum $x \in \mathbf{F}_q^*$, teríamos $\tau(x) = 0$ para todo τ no dual de $\mathbf{F}_q$, que seria um absurdo. Portanto T é o isomorfismo que nos dá a equivalência desejada. O número de zeros segue do Teorema 2.2.5. □

De agora em diante chamaremos $Q(a_1, \ldots, a_{(m-w)/2}, b_1, \ldots, b_{(m-w)/2})$, ou mais simplesmente $Q(a, b)$, à função quadrática definida em (3.1.1). Ao ser avaliada em $\mathbf{F}_q^*$, esta função quadrática define uma palavra em $(\mathbf{F}_2)^{q-1}$, a qual frequentemente será tratada como a própria função. Assim, quando o conjunto $\{a_1, \ldots, a_{(m-w)/2}, b_1, \ldots, b_{(m-w)/2}\}$, que será denotado por $\{a, b\}$, é linearmente independente, temos pela proposição anterior que:

$$w(Q(a, b)) = (q - \sqrt{q2^w})/2. \tag{3.1.2}$$

Podemos encontrar palavras de $\mathscr{C}_h$ escolhendo o conjunto $\{a, b\}$ de acordo com o resultado abaixo.

Proposição 3.1.2: *Se o conjunto* $\{a_i, b_i;\ i \in \{1, \ldots, (m-w)/2\}\} \subset \mathbf{F}_q$ *satisfaz o sistema*

$$\sum_{i=1}^{(m-w)/2} ({a_i}^{2^j} b_i + a_i {b_i}^{2^j}) = 0 \tag{3.1.3}$$

para cada $j \in \{h+1, \ldots, (m-1)/2\}$, *então* $Q(a, b) \in \mathscr{C}_h$.

Demonstração: Começamos observando que para cada $a, b, x \in \mathbf{F}_q$

$$Tr(ax)Tr(bx) = Tr(Tr(ax)bx) = Tr\left(\sum_{j=0}^{m-1} a^{2^j} b x^{2^j+1}\right).$$

E como, para cada j,

$$\begin{aligned} Tr(a^{2^j} b x^{2^j+1}) &= Tr[(a^{2^j} b x^{2^j+1})^{2^{m-j}}] \\ &= Tr(a b^{2^{m-j}} x^{2^{m-j}+1}), \end{aligned}$$

obtemos

$$\begin{aligned} Tr\left(\sum_{j=\frac{m+1}{2}}^{m-1} a^{2^j} b x^{2^j+1}\right) &= Tr\left(\sum_{j=\frac{m+1}{2}}^{m-1} a b^{2^{m-j}} x^{2^{m-j}+1}\right) \\ &= Tr\left(\sum_{j=1}^{\frac{m-1}{2}} a b^{2^j} x^{2^j+1}\right), \end{aligned}$$

por onde chegamos a

$$\begin{aligned} Tr(ax)Tr(bx) &= Tr\left(\sum_{j=0}^{m-1} a^{2^j} b x^{2^j+1}\right) \\ &= Tr\left(\sum_{j=0}^{\frac{m-1}{2}} a^{2^j} b x^{2^j+1}\right) + Tr\left(\sum_{j=\frac{m+1}{2}}^{m-1} a^{2^j} b x^{2^j+1}\right) \\ &= Tr\left(\sum_{j=0}^{\frac{m-1}{2}} a^{2^j} b x^{2^j+1}\right) + Tr\left(\sum_{j=1}^{\frac{m-1}{2}} a b^{2^j} x^{2^j+1}\right) \\ &= Tr\left(abx^2 + \sum_{j=1}^{\frac{m-1}{2}} (a^{2^j} b + a b^{2^j}) x^{2^j+1}\right). \end{aligned}$$

Daí concluímos que

$$\sum_{i=1}^{(m-w)/2} Tr(a_i x)Tr(b_i x)$$
$$= Tr\left[\left(\sum_{i=1}^{(m-w)/2} a_i b_i\right)x^2 + \sum_{j=1}^{\frac{m-1}{2}}\left(\sum_{i=1}^{(m-w)/2} {a_i}^{2^j} b_i + a_i {b_i}^{2^j}\right)x^{2^j+1}\right]$$

e, como o polinômio entre colchetes pertence a R_h se, e somente se, satisfaz (3.1.3), temos o resultado. □

Corolário 3.1.3: *Para um conjunto* $\{a_1, \ldots, a_{(m-w)/2}\} \in \mathbf{F}_q$ *fixo, as palavras* $Q(a,b)$ *induzidas pelas soluções* $(b_1, \ldots, b_{(m-w)/2})$ *de (3.1.3) formam um subcódigo de* $\mathscr{C}_h$.

Demonstração: Para a fixo, as equações de (3.1.3) são polinômios linearizados nas variáveis b_i. Daí, se (a,b) e (a,c) são soluções, $(a, b+c)$ também é. Agora basta observar que

$$Q(a, b+c)(x) = Q(a,b)(x) + Q(a,c)(x)\ \forall x \in \mathbf{F}_q.$$ □

Consideremos, de agora em diante, $w = 2h-1$, já que assim, se conseguirmos satisfazer as hipóteses da Proposição 3.1.1, obtemos, por (3.1.2), $Q(a,b)$ com o menor peso possível. Agora seja

$$M = (m-w)/2 = (m-2h+1)/2.$$

Neste caso (3.1.3) nos dá $\frac{m-1}{2} - h = M - 1$ equações em M incógnitas b_i. Fixaremos agora um conjunto $\{a_1, \ldots, a_M\}$ linearmente independente sobre $\mathbf{F}_2$ e assumiremos que o sistema de equações (3.1.3) não é vazio, ou seja, $h < (m-1)/2$.

Proposição 3.1.4: *O sistema (3.1.3) tem pelo menos q soluções* $(b_1, \ldots, b_M)$ *em* $(\mathbf{F}_q)^M$.

Demonstração: Como o sistema (3.1.3) é homogêneo, podemos supor $a_1 = 1$. Agora para cada $j \in \{1, \ldots, m\}$ ficamos com a equação

$${b_1}^j + b_1 = \sum_{i=2}^{M} a_i {b_i}^{2^j} + {a_i}^{2^j} b_i$$

e, se aplicarmos a substituição $b_1 = b_1' + \sum_{i=2}^{M} \sqrt[2^j]{a_i} b_i$, obtemos

$$\left(b_1' + \sum_{i=2}^{M} \sqrt[2^j]{a_i} b_i \right)^{2^j} + b_1' + \sum_{i=2}^{M} \sqrt[2^j]{a_i} b_i = \sum_{i=2}^{M} a_i {b_i}^{2^j} + {a_i}^{2^j} b_i$$

$${b_1'}^{2^j} + b_1' + \sum_{i=2}^{M} a_i b_i^{2^j} + \sqrt[2^j]{a_i} b_i = \sum_{i=2}^{M} a_i {b_i}^{2^j} + {a_i}^{2^j} b_i$$

$${b_1'}^{2^j} + b_1' = \sum_{i=2}^{M} \left(a_i^{2^j} + \sqrt[2^j]{a_i} \right) b_i.$$

Se $a_i^{2^j} + \sqrt[2^j]{a_i} \neq 0$ para algum i, esta equação tem q^{M-1} soluções, já que a aplicação linear

$$(b_2, \ldots, b_M) \mapsto \sum_{i=2}^{M} \left(a_i^{2^j} + \sqrt[2^j]{a_i} \right) b_i$$

é sobrejetiva, tendo portanto q^{M-2} elementos em seu núcleo, donde segue que, para cada $b_i' \in \mathbf{F}_q$, exatamente q^{M-2} elementos de $(\mathbf{F}_q)^{M-1}$ têm ${b_i'}^{2^j} + b_i'$ como imagem. Agora se $a_i^{2^j} + \sqrt[2^j]{a_i} = 0$ para todo i, o número de soluções da equação é sq^{M-1} onde s é o número de raízes de $X^{2^j} + X$. Observe que $s \geq 2$, pois 0 e 1 são raízes deste polinômio. Sendo assim, para cada j, temos um conjunto solução com q^{M-1} ou mais elementos. Como cada um destes conjuntos é um $\mathbf{F}_2$-espaço vetorial, cada um deles tem ao menos dimensão $m(M-1)$ sobre $\mathbf{F}_2$. Segue que o espaço solução do sistema tem dimensão superior a[1]

$$(M-1)^2 m - (M-2)Mm = (M^2 - 2M + 1 - M^2 + 2M)m = m. \quad \square$$

O peso de uma palavra $\mathcal{C}_R$ de $\mathscr{C}_h$ é $q/2$ se Q_R tem posto ímpar. Agora se Q_R tem posto par, dado por $m - v$ com $v = dim(rad\ Q_R)$, então $\mathcal{C}_R$ tem peso $(q + \sqrt{q2^v})/2$ ou $(q - \sqrt{q2^v})/2$. Como devemos ter v ímpar com $v \leq 2h$, o peso mínimo de $\mathscr{C}$ tem a cota inferior $(q - \sqrt{q2^{2h-1}})/2$, que é atingida se encontrarmos uma palavra $Q(a, b)$ com $\{a, b\}$ tendo posto $2M$ sobre $\mathbf{F}_2$ e satisfazendo (3.1.3). Esta cota inferior será útil na proposição que segue.

[1]Estamos usando aqui que se $(V_i)_{i=1}^k$ são sub-espaços de W, então

$$dim(\cap_{i=1}^k V_i) \geq \sum_{i=1}^k dim(V_i) - (k-1)dim(W).$$

Proposição 3.1.5: *Dado $k \leq M$, sejam $\{c_1, \ldots, c_k\} \subset \mathbf{F}_q$ um conjunto $\mathbf{F}_2$-linearmente independente e $\{d_1, \ldots, d_k\} \subset \mathbf{F}_q$ tal que a função quadrática definida pela expressão*

$$\sum_{i=1}^{k} Tr(c_i x)Tr(d_i x)$$

induz uma palavra pertencente a $\mathscr{C}_h$. Se $\{c_i, d_i;\ i \in \{1, \ldots, k\}\}$ for linearmente dependente, o que é necessariamente verdade para $k < M$, então, para cada $j \in \{1, \ldots, k\}$, d_j é combinação linear dos c_i's.

Demonstração: Ter $k < M$ implica em elementos c_i, d_i linearmente dependentes pois, caso contrário, teríamos, pela Proposição 3.1.1 e pela igualdade $2k = m - 2[h + (M - k)] + 1$, uma palavra de peso $(q - \sqrt{2q^{2(h+M-k)-1}})/2$, menor que a cota inferior encontrada. Agora para o resultado principal, podemos supor sem perda de generalidade $j = 1$, já que estamos livres para fazer uma reordenação de índices. Sejam, para cada $i \in \{1, \ldots, k\}$, φ_i e ψ_i os funcionais de $\mathbf{F}_q$ em $\mathbf{F}_2$ definidos por $\varphi(x) = Tr(c_i x)$ e $\psi_i(x) = Tr(d_i x)$. Desta forma temos

$$\sum_{i=1}^{M} Tr(c_i x)Tr(d_i x) = \sum_{i=1}^{M} \varphi(x)\psi_i(x).$$

Tomemos $\{\gamma_1, \ldots, \gamma_k, \delta_1, \ldots, \delta_{k-1}\} \subset \mathbf{F}_2$ tais que

$$d_k = \sum_{i=1}^{k-1}(\gamma_i c_i + \delta_i d_i) \quad + \gamma_k c_k,$$

para obtermos

$$\psi_k = \sum_{i=1}^{k-1}(\gamma_i \varphi_i + \delta_i \psi_i) \quad + \gamma_k \varphi_k.$$

Assim temos que

$$\begin{aligned}\sum_{i=1}^{k} \varphi_i\psi_i &= \sum_{i=1}^{k-1} \varphi_i\psi_i \quad + \varphi_k \left(\sum_{i=1}^{k-1} \gamma_i\varphi_i + \delta_i\psi_i \quad + \gamma_k\varphi_k \right) \\ &= \sum_{i=1}^{k-1} \varphi_i\psi_i \quad + \sum_{i=1}^{k-1} \gamma_i\varphi_i\varphi_k \quad + \sum_{i=1}^{k-1} \delta_i\psi_i\varphi_k \quad + \gamma_k\varphi_k^2.\end{aligned}$$

E como

$$\sum_{i=1}^{k-1} \varphi_i\psi_i \quad + \sum_{i=1}^{k-1} \gamma_i\varphi_i\varphi_k = \sum_{i=1}^{k-1} \varphi_i(\psi_i + \gamma_i\varphi_k)$$

e

$$\sum_{i=1}^{k-1} \delta_i\psi_i\varphi_k = \sum_{i=1}^{k-1} \delta_i\varphi_k(\psi_i + \gamma_i\varphi_k) \quad + \sum_{i=1}^{k-1} \gamma_i\delta_i\varphi_k^2,$$

$$\begin{aligned}\sum_{i=1}^{k} \varphi_i\psi_i &= \sum_{i=1}^{k-1} \varphi_i(\psi_i + \gamma_i\varphi_k) \quad + \sum_{i=1}^{k-1} \delta_i\varphi_k(\psi_i + \gamma_i\varphi_k) \quad + \sum_{i=1}^{k-1} \gamma_i\delta_i\varphi_k^2 \quad + \gamma_k\varphi_k^2 \\ &= \sum_{i=1}^{k-1} (\varphi_i + \delta_i\varphi_k)(\psi_i + \gamma_i\varphi_k) \quad + \left(\gamma_k + \sum_{i=1}^{k-1} \gamma_i\delta_i\right)\varphi_k^2.\end{aligned}$$

Porém, observe que

$$[\varphi_k(x)]^2 = [Tr(c_k x)]^2 = Tr[(c_k x)^2] = Tr(x c_k^2 x),$$

para cada $x \in \mathbf{F}_q$, portanto, φ_k^2 induz uma palavra de $\mathscr{C}_h$. Por isso, também pertence a este código a palavra induzida por

$$\sum_{i=1}^{k-1} [\varphi_i(x) + \delta_i\varphi_k(x)][\psi_i(x) + \gamma_i\varphi_k(x)] = \sum_{i=1}^{k-1} Tr\left(c_i^{(1)}x\right) Tr\left(d_i^{(1)}\right),$$

onde $c_i^{(1)} = c_i + \delta_i c_k$ e $d_i^{(1)} = d_i + \gamma_i c_k$ para cada $i \in \{1, \ldots, k-1\}$. Utilizando o que já foi discutido no começo desta demonstração vemos que o conjunto $A_1 = \left\{c_i^{(1)}, d_i^{(1)}; i \in \{1, \ldots, k-1\}\right\}$ é linearmente dependente. Assim, podemos repetir o mesmo procedimento, passando sempre por conjuntos linearmente dependentes, até chegar ao conjunto $A_{k-1} = \{c_1^{(k-1)}, d_1^{(k-1)}\}$. Mas observe que $c_1^{(k-1)} = c_1 + L_1(c_2, \ldots, c_k)$ e $d_1^{(k-1)} = d_1 + L_2(c_2, \ldots, c_k)$, onde L_1 e L_2 são transformações $\mathbf{F}_2$-lineares de $(\mathbf{F}_q)^{k-1}$ em $\mathbf{F}_q$. Se $d_1^{(k-1)} = 0$ já temos o resultado. Agora para $d_1^{(k-1)} \neq 0$, a dependência linear de A_{k-1} implica

$$c_1^{(k-1)} + d_1^{(k-1)} = 0,$$

ou seja,

$$d_1 = c_1 + L_1(c_2, \ldots, c_k) + L_2(c_2, \ldots, c_k). \qquad \square$$

Corolário 3.1.6: *Seja $(b_1, \ldots, b_M)$ solução de (3.1.3). Se $\{a_1, \ldots, a_M, b_1\}$ é linearmente independente, então $\{a, b\}$ também o é.*

Agora sejam S o $\mathbf{F}_2$-espaço vetorial de soluções $(b_1, \ldots, b_M)$ de (3.1.3) para o conjunto $\{a_1, \ldots, a_M\}$ $\mathbf{F}_2$-linearmente independente fixado anteriormente e V sua imagem sobre $\mathbf{F}_q$ pela projeção na primeira coordenada.

Teorema 3.1.7: *Se $r = dim_{\mathbf{F}_2}(V) - M > 0$ então existe em $\mathscr{C}_h$ um subcódigo de peso mínimo de dimensão r.*

Demonstração: Como $r = dim_{\mathbf{F}_2}(V) - M > 0$ existem $b_1^{(1)}, \ldots, b_1^{(r)}$ em V tais que o conjunto $\{a_1, \ldots, a_M, b_1^{(1)}, \ldots, b_1^{(r)}\}$ é linearmente independente. Pelo Corolário 3.1.6 cada $b_1^{(j)}$ induz uma palavra

$$\mathcal{C}_j = Q(a_1, \ldots, a_M, b_1^{(j)}, \ldots, b_M^{(j)})$$

de peso mínimo em $\mathscr{C}_h$. Verifiquemos agora que o espaço gerado por estas palavras tem dimensão r. Sejam $\beta_1, \ldots, \beta_r \in \mathbf{F}_2$ tais que

$$\sum_{j=1}^{r} \beta_j \mathcal{C}_j = 0.$$

Escrevendo $d_i = \sum_{j=1}^{r} \beta_j b_i^{(j)}$ para cada $i \in \{1, \ldots, M\}$ temos que $(d_1, \ldots, d_M) \in S$ e

$$\begin{aligned}\sum_{j=1}^{r} \beta_j \sum_{i=1}^{M} Tr(a_i x) Tr(b_i^{(j)} x) &= \sum_{i=1}^{M} Tr(a_i x) Tr\left[\left(\sum_{j=1}^{r} \beta_j b_i^{(j)}\right) x\right] \\ &= \sum_{i=1}^{M} Tr(a_i x) Tr(d_i x) = 0\end{aligned}$$

para todo $x \in \mathbf{F}_q$. Daí temos pela Proposição 3.1.1 que $\{a_1, \ldots, a_M, d_1, \ldots, d_M\}$ é linearmente dependente sobre $\mathbf{F}_2$, donde segue pelo Corolário 3.1.6 que $\{a_1, \ldots, a_M, d_1\}$ também o é. Então existem $\alpha_1, \ldots, \alpha_M, \delta \in \mathbf{F}_2$ não todos nulos tais que

$$\sum_{i=1}^{M} \alpha_i a_i \quad + \delta d_1 = 0.$$

Observe que devemos ter $\delta \neq 0$, já que os a_i's já são linearmente independentes. Mas daí temos

$$\sum_{i=1}^{M} \alpha_i a_i + \sum_{j=1}^{r} \delta \beta_j b_1^{(j)} = 0$$

implicando $\alpha_i = \delta\beta_j = 0$ para todo i e j. Conclui-se então que $\beta_j = 0$ para todo j. □

A Proposição 3.1.4 nos dá $dim_{\mathbf{F}_2} S \geq m$. A proposição seguinte nos dará uma cota inferior para $dim_{\mathbf{F}_2} V$.

Proposição 3.1.8: *Seja $(b_1, \ldots, b_M) \in S$. Então $(b_1, b'_2, \ldots, b'_M) \in S$ se, e somente se, existe uma matriz simétrica A, $(M-1)\times(M-1)$, com entradas em $\mathbf{F}_2$ tal que $(b'_2, \ldots, b'_M) = (b_2, \ldots, b_M) + (a_2, \ldots, a_M)A$.*

Demonstração: Suponhamos primeiro $(b_1, b'_2, \ldots, b'_M) \in S$. Com isso, como $(0, b_2 + b'_2, \ldots, b_M + b'_M) \in S$, temos que

$$\sum_{i=2}^{M} Tr(a_i x) Tr(b_i + b'_i x)$$

representa uma palavra em $\mathscr{C}_h$. Portanto, pela Proposição 3.1.5, para cada $i \in \{2, \ldots, M\}$ existem $\alpha_{ij} \in \mathbf{F}_2$ tais que

$$b_i + b'_i = \sum_{j=2}^{M} \alpha_{ij} a_j.$$

Então temos que

$$\begin{aligned}
\sum_{i=2}^{M} Tr(a_i x) Tr(b_i + b'_i x) &= \sum_{i=2}^{M} Tr(a_i x) Tr\left(\sum_{j=2}^{M} \alpha_{ij} a_j x\right) \\
&= \sum_{i=2}^{M} \sum_{j=2}^{M} Tr(a_i x) Tr(\alpha_{ij} a_j x) \\
&= \sum_{i=2}^{M} \alpha_{ii} Tr(a_i x)^2 \\
&+ \sum_{i=2}^{M-1} \sum_{j=i+1}^{M} \left[Tr(a_i x) Tr(\alpha_{ij} a_j x) + Tr(a_j x) Tr(\alpha_{ji} a_i x) \right].
\end{aligned}$$

Mas para cada (i,j)

$$\begin{aligned} Tr(a_ix)Tr(\alpha_{ij}a_jx) + Tr(a_jx)Tr(\alpha_{ji}a_ix) &= (\alpha_{ij} + \alpha ji)Tr(a_ix)Tr(a_jx) \\ &= Tr(a_ix)Tr[(\alpha_{ij} + \alpha_{ji})a_jx] \end{aligned}$$

e como, para cada i, $Tr(a_ix)^2$ representa uma palavra em $\mathscr{C}_h$, o mesmo ocorre para

$$\sum_{i=2}^{M-1}\sum_{j=i+1}^{M} Tr(a_ix)Tr(\beta_{ij}a_jx) = \sum_{i=2}^{M-1} Tr(a_ix)Tr\left[\left(\sum_{j=i+1}^{M}\beta_{ij}\right)x\right],$$

onde $\beta_{ij} = \alpha_{ij} + \alpha_{ji}$ para cada (i,j). Segue mais uma vez da Proposição 3.1.5 que para cada $k \in \{2,\ldots,M-1\}$ o conjunto $\left\{a_2,\ldots,a_{M-1},\sum_{j=k+1}^{M}\beta_{ij}a_j\right\}$ é linearmente dependente. Fixemos então um $k < M-1$ e tomemos $\gamma_2,\ldots,\gamma_M$ não todos nulos em $\mathbf{F}_2$ tais que

$$\sum_{i=2}^{M-1}\gamma_i a_i \quad + \gamma_M\left(\sum_{j=k+1}^{M}\beta_{kj}a_j\right) = 0.$$

Daí segue que

$$\sum_{i=2}^{k}\gamma_i a_i \quad + \sum_{i=k+1}^{M-1}(\gamma_i a_i + \gamma_M\beta_{ki})a_i \quad + \gamma_M\beta_{kM}a_M = 0$$

e como não podemos ter $\gamma_M = 0$, $\beta_{kM} = 0$. Observe que para $k = M-1$ chegamos à igualdade acima sem o somatório do meio, que leva à mesma conclusão. Portanto temos $\beta_{kM} = 0$ para cada $k \in \{2,\ldots,M-1\}$. Assim temos em $\mathscr{C}_h$ a palavra induzida por

$$\sum_{i=2}^{M-2} Tr(a_ix)Tr\left(\sum_{j=i+1}^{M-1}\beta_{ij}a_jx\right).$$

Explorando esta expressão da mesma maneira que fizemos anteriormente, chegamos a $\beta_{k(M-1)} = 0$ para todo k. Fazendo este processo sucessivamente chegamos finalmente até $\beta_{23} = 0$, mostrando que a matriz A é simétrica. Agora para a volta seja $A = (c_{ij})_{i,j=2}^{M}$ matriz simétrica. Assim

$$(b_2,\ldots,b_M) + (a_2,\ldots,a_M)A = \left(b_2 + \sum_{k=2}^{M}a_kc_{k2},\ldots,b_M + \sum_{k=2}^{M}a_kc_{kM}\right).$$

Substituindo diretamente em (3.1.3) obtemos para cada $j \in \{h+1, \ldots, M\}$

$$a_1 b_1^{2^j} + a_1^{2^j} b_1 + \sum_{i=2}^{M} \left[a_i^{2^j} \left(b_i + \sum_{k=1}^{M} a_k c_{ki} \right) + a_i \left(b_i + \sum_{k=1}^{M} a_k c_{ki} \right)^{2^j} \right]$$

$$= a_1 b_1^{2^j} + a_1^{2^j} b_1 + \sum_{i=2}^{M} \left[a_i^{2^j} b_i + a_i^{2^j} \left(\sum_{k=2}^{M} a_k c_{ki} \right) + a_i b_i^{2^j} + a_i \left(\sum_{k=2}^{M} a_k c_{ki} \right)^{2^j} \right]$$

$$= \sum_{i=1}^{M} \left(a_i^{2^j} b_i + a_i b_i^{2^j} \right) + \sum_{i=2}^{M} \sum_{k=2}^{M} \left(a_i^{2^j} a_k c_{ki} + a_i a_k^{2^j} c_{ki} \right),$$

onde o somatório à esquerda já é nulo por hipótese. Só resta observar que

$$\sum_{i=2}^{M} \sum_{k=2}^{M} c_{ki} \left(a_i^{2^j} a_k + a_i a_k^{2^j} \right)$$

$$= \sum_{i=1}^{M} c_{ii} \left(a_i^{2^j} a_i + a_i a_i^{2^j} \right)$$

$$+ \sum_{i=2}^{M-1} \sum_{k=i+1}^{M} \left[c_{ki} \left(a_i^{2^j} a_k + a_i a_k^{2^j} \right) + c_{ik} \left(a_k^{2^j} a_i + a_k a_i^{2^j} \right) \right] = 0 \qquad \square$$

Como podemos escolher as $M(M-1)$ entradas para esta matriz A, temos:

Corolário 3.1.9: $dim_{\mathbf{F}_2}(V) = dim_{\mathbf{F}_2}(S) - \frac{M(M-1)}{2} \geq m - \frac{M(M-1)}{2}$

3.2 Aplicando o processo para m ímpar

Agora utilizaremos os resultados obtidos na seção anterior para determinar sub-códigos de peso mínimo dentro de $\mathscr{C}_h$ e, a partir destes, obter curvas cujo número de pontos será conhecido.

Seja $q = 2^m$ com $m \geq 3$ ímpar. Para vários valores de $0 < h \leq (m-1)/2$, tomaremos

$$w = 2h - 1 \quad e \quad M = (m - 2h + 1)/2.$$

Além disso chamaremos de S o conjunto das soluções $(b_1, \ldots, b_M)$ do sistema (3.1.3) com o w já determinado, e também de V a projeção de S na primeira coordenada.

O caso $h = (m-1)/2$

Neste caso $M = 1$. Como o sistema (3.1.3) é vazio, pela Proposição 3.1.1, temos que para cada $b \in \mathbf{F}_q \setminus \mathbf{F}_2$ a palavra de tamanho $q-1$ induzida pela função quadrática $Tr(x)Tr(bx)$ de $\mathbf{F}_q$ em $\mathbf{F}_2$ está em $\mathscr{C}_h$ e tem peso $(q - \sqrt{q2^w})/2 = 2^{m-2}$, que é o peso mínimo deste código. Então tomando $\{b^{(1)}, \ldots, b^{(m-1)}\} \subset \mathbf{F}_q \setminus \mathbf{F}_2$ linearmente independente sobre $\mathbf{F}_2$ e chamando $\mathcal{C}_i$ a palavra induzida por $Tr(x)Tr(b^{(i)}x)$, temos que o sub-código $\mathscr{D}_{m-1}$, gerado por estas palavras, é de peso mínimo e tem dimensão $m-1$. Tomando para cada $r \in \{1, \ldots, m-2\}$ um sub-código $\mathscr{D}_r \subset \mathscr{D}_{m-1}$ de dimensão r, podemos formular a proposição que segue.

Proposição 3.2.1: *Os pesos de Hamming generalizados do código binário* $\mathscr{C}_{(2m-1)/2}$ *de comprimento* $2^m - 1$ *satisfazem*

$$d_r(\mathscr{C}_{(m-1)/2}) = (2^r - 1) \cdot 2^{m-r-1}$$

para cada $r \in \{1, \ldots, m-1\}$.

Demonstração: Como já temos para cada r um sub-código de peso mínimo com esta dimensão, do Corolário 1.3.3 segue que

$$d_r(\mathscr{C}_{(m-1)/2}) = (2^r - 1)d_1(\mathscr{C}_{(m-1)/2})/(2^r - 2^{r-1}).$$

Como $d_1(\mathscr{C}_{(m-1)/2}) = 2^{m-2}$ e $2^r - 2^{r-1} = 2^{r-1}$ temos o resultado. □

Como para cada $r \in \{1, \ldots, m-1\}$ temos

$$d_r(\mathscr{C}_{(m-1)/2}) = w(\mathscr{D}_r),$$

a Proposição 2.1.3 nos dá

$$\#C^{(\mathscr{D}_r)} = 2^r[2^m - (2^r - 1) \cdot 2^{m-r-1}] = 2^{m-1}(2^r + 1).$$

O caso $h = (m-3)/2$

Para este caso consideraremos $m \geq 5$. Temos então $M = 2$ e tomando $\{1, a_2\}$ com $a_2 \in \mathbf{F}_q \setminus \mathbf{F}_2$ o sistema (3.1.3) consiste apenas na equação

$$b_1^{2^{(m-1)/2}} + b_1 = a_2 b_2^{2^{(m-1)/2}} + a_2^{2^{(m-1)/2}} b_2.$$

Daí, fazendo a substituição $b_1 = b_1' + a_2^{(m+1)/2} b_2$, ela se transforma em

$$b_1' + b_1'^{\,2^{(m-1)/2}} = \left(a_2^{(m+1)/2} + a_2^{(m-1)/2}\right) b_2.$$

Como $\left(a_2^{(m+1)/2} + a_2^{(m-1)/2}\right) = a_2^{(m-1)/2}(a_2 + 1) \neq 0$, observa-se diretamente que o conjunto S das soluções (b_1, b_2) do sistema possui q soluções , ou seja, $dim_{\mathbf{F}_2}(S) = m$. Combinando esta informação com o Corolário 3.1.9 obtemos $dim_{\mathbf{F}_2}(V) = m - 1$. Nos valendo desta informação, podemos formular a proposição abaixo.

Proposição 3.2.2: *Os pesos de Hamming generalizados do código binário* $\mathscr{C}_{(m-3)/2}$ *de comprimento* $2^m - 1$ *satisfazem*

$$d_r(\mathscr{C}_{(m-3)/2}) = (2^r - 1) \cdot 3 \cdot 2^{m-r-2}$$

para cada $r \in \{1, \ldots, m-3\}$.

Demonstração: Pelo Teorema 3.1.7, para cada $r \in \{1, \ldots, m-3\}$, existe um sub-código de peso mínimo e dimensão r em $\mathscr{C}_{(m-3)/2}$. Como o peso mínimo deste código é $(q - \sqrt{q2^{m-4}}) = 3 \cdot 2^{m-2}$, basta aplicar a Proposição 2.1.3. □

Assim como no caso anterior, determinamos os sub-códigos de peso mínimo $\mathscr{D}_r$ para cada $r \in \{1, \ldots, m-3\}$ e obtemos

$$\#C^{(\mathscr{D}_r)} = 2^r[2^m - (2^r - 1) \cdot 3 \cdot 2^{m-r-2}] = 2^{m-2}(2^r + 3).$$

O caso $h = (m-5)/2$

Tomaremos agora $m \geq 7$. Temos agora $M = 3$. Fixando $\{1, a_1, a_2\}$ linearmente independente sobre $\mathbf{F}_2$, o sistema (3.1.3) é formado pelas equações:

$$b_1 + b_1^{2^{(m-3)/2}} = \sum_{i=2}^{3} a_i^{2^{(m-3)/2}} b_i + a_i b_i^{2^{(m-3)/2}}$$
$$b_1 + b_1^{2^{(m-1)/2}} = \sum_{i=2}^{3} a_i^{2^{(m-1)/2}} b_i + a_i b_i^{2^{(m-1)/2}}.$$

Basta aplicar o Corolário 3.1.9 para verificarmos que $dim_{\mathbf{F}_2}(V) \geq m - 3$, seguindo pelo Teorema 3.1.7 que existe um sub-código de peso mínimo e

dimensão r para cada $r \in \{1, \ldots, m-6\}$. Porém, pode-se escolher os elementos a_2 e a_3 de forma a obter uma solução de (3.1.3) com cardinalidade superior à q garantida pela Proposição 3.1.4, o que assegura a existência de sub-códigos de peso mínimo de dimensões superiores. Ilustraremos este fato com um exemplo.

3.2.3 Exemplo: Para $m = 9$ e $h = 2$ temos o sistema:

$$b_1 + b_1^8 = a_2^8 b_2 + a_2 b_2^8 + a_3^8 b_3 + a_3 b_3^8 \tag{3.2.1}$$
$$b_1 + b_1^{16} = a_2^{16} b_2 + a_2 b_2^{16} + a_3^{16} b_3 + a_3 b_3^{16}. \tag{3.2.2}$$

E se escolhermos $\{1, a_2, a_3\}$ uma base de $\mathbf{F}_8$ sobre $\mathbf{F}_2$, (3.2.1) pode ser reescrita como

$$b_1 + b_1^8 = a_2 b_2 + a_2^8 b_2^8 + a_3 b_3 + a_3^8 b_3^8,$$

ou seja,

$$b_1 + a_2 b_2 + a_3 b_3 + (b_1 + a_2 b_2 + a_3 b_3)^8 = 0.$$

Daí temos $\{(b_1, b_2, b_3) \in (\mathbf{F}_{512})^3;\ b_1 + a_2 b_2 + a_3 b_3 \in \mathbf{F}_8\}$ como conjunto solução de (3.2.1). Com isto em mente, para auxiliar a contagem de soluções do sistema, vamos tomar $\mu \in \mathbf{F}_8$ e fazer a substituição $b_1 = \mu + a_2 b_2 + a_3 b_3$ em (3.2.2), obtendo

$$(a_2 + a_2^2)(b_2 + b_2^{16}) + (a_3 + a_3^2)(b_3 + b_3^{16}) + \mu + \mu^2 = 0.$$

Utilizando que $(a_2 + a_2^2) \neq 0$, já que $a_2 \in \mathbf{F}_8 \setminus \mathbf{F}_2$, tomamos

$$c = (a_2 + a_2^2)^{-1}(a_3 + a_3^2) \qquad \text{e} \qquad d = (a_2 + a_2^2)^{-1}(\mu + \mu^2)$$

para ficar com a equação equivalente

$$b_2 + b_2^{16} + c(b_3 + b_3^{16}) + d = 0.$$

Podemos reduzir o grau em b_3 fazendo a substituição $b_2 = b_2' + c^{32} b_3$, que nos dá

$$b_2' + {b_2'}^{16} + (c + c^{32}) b_3 + d = 0.$$

Mas como $c \in \mathbf{F}_8$, $c^{32} = c^2$, daí devemos ter o coeficiente de b_3 não nulo, já que o contrário implicaria em $c = 1$, ou seja $a_2 + a_2^2 = a_3 + a_3^2$, que por sua vez implicaria $a_2 + a_3 \in \mathbf{F}_2$, contrariando a independência linear entre 1, a_2 e a_3. Portanto cada escolha de b_2 em $\mathbf{F}_{512}$ determina unicamente o elemento

b_3 satisfazendo a equação acima, ou seja, ela possui exatamente 512 soluções. Como temos uma equação como esta determinada para cada $\mu \in \mathbf{F}_8$, e a escolha de μ determina unicamente b_1, concluímos que o sistema em questão possui $8 \cdot 512$ soluções (b_1, b_2, b_3), ou seja, $dim_{\mathbf{F}_2}(S) = 12$. Daí o Corolário 3.1.9 e o Teorema 3.1.7 atestam a existência do sub-código de peso mínimo $\mathscr{D}_6$ de dimensão 6. Como o peso mínimo do sub-código $\mathscr{C}_2$ de tamanho 511 é $2^5 \cdot 7$, verificamos, como nos casos anteriores, as igualdades

$$d_r(\mathscr{C}_2) = (2^r - 1)2^{6-r} \cdot 7$$

para cada $r \in \{1, \ldots, 6\}$. Escolhendo mais uma vez $\mathscr{D}_r$ o sub-código de peso mínimo e dimensão r, obtemos também

$$\#C^{(\mathscr{D}_r)} = 2^6 \cdot (2^r + 7).$$

3.3 O caso m par

De maneira análoga ao que foi feito na Seção 3.1, serão desenvolvidos agora resultados que servirão de instrumentos para a construção de sub-códigos de peso baixo em $\mathscr{C}_h$, desta vez para m par. Porém, surgirão algumas complicações que exigirão certas adaptações.

Nesta seção tomaremos um inteiro $m \geq 4$ par e consideraremos o código $\mathscr{C}_h$ com $1 < h < m/2$. Não há dificuldade em trazer a Proposição 3.1.1 para este caso e juntando-a com os comentários que a seguem temos:

Proposição 3.3.1: *Dados $0 \leq w \leq 2h$ com $(m - w)$ par e um conjunto $\{a_i, b_i \in \mathbf{F}_q;\ i \in \{1, \ldots, (m-w)/2\}\}$ linearmente independente sobre $\mathbf{F}_2$, a expressão*

$$\sum_{i=1}^{(m-w)/2} Tr(a_i x)Tr(b_i x)$$

define uma palavra em $(\mathbf{F}_2)^{q-1}$ de peso $(q - \sqrt{q2^w})/2$.

Já o critério para que a palavra induzida pertença a $\mathscr{C}_h$, apesar de continuar essencialmente o mesmo, exige um pouco de cuidado em sua demonstração, como veremos a seguir.

Proposição 3.3.2: *Se os elementos $a_i, b_i \in \mathbf{F}_q$, com $i \in \{1, \ldots, (m-w)/2\}$ satisfazem o sistema*

$$\sum_{i=1}^{(m-w)/2} (a_i{}^{2^j} b_i + a_i b_i{}^{2^j}) = 0 \tag{3.3.1}$$

para $j \in \{h+1, \ldots, m/2\}$ então a palavra induzida por $\sum_{i=1}^{(m-w)/2} Tr(a_i x)Tr(b_i x)$ está em $\mathscr{C}_h$.

Demonstração: Tomando $a, b, x \in \mathbf{F}_q$ e utilizando as igualdades

$$Tr(ax)Tr(bx) = Tr\left(\sum_{j=0}^{m-1} a^{2^j} b x^{2^j+1}\right)$$

e

$$Tr\left(a^{2^j} b x^{2^j+1}\right) = Tr\left(a b^{2^{m-j}} x^{2^{m-j}+1}\right)$$

retiradas da Proposição 3.1.2 chegamos, através de manipulações semelhantes às desta proposição, a

$$Tr(ax)Tr(bx) = Tr\left[abx^2 + a^{2^{m/2}} b x^{2^{m/2}+1} + \sum_{j=1}^{m/2-1} \left(a^{2^j} b + a b^{2^j}\right) x^{2^j+1}\right].$$

Segue daí, para cada $x \in \mathbf{F}_q$, a igualdade

$$\sum_{i=1}^{(m-w)/2} Tr(a_i x)Tr(b_i x)$$

$$= Tr\left[\sum_{i=1}^{\frac{m-w}{2}} a_i b_i x^2 + \sum_{i=1}^{\frac{m-w}{2}} a_i^{2^{m/2}} b_i x^{2^{m/2}+1} + \sum_{j=1}^{\frac{m}{2}-1} \sum_{i=1}^{\frac{m-w}{2}} \left(a_i^{2^j} b_i + a_i b_i^{2^j}\right) x^{2^j+1}\right].$$

Aplicando a condição (3.3.1) nos $j \in \{h+1, \ldots, m/2-1\}$ obtemos

$$\sum_{i=1}^{(m-w)/2} Tr(a_i x)Tr(b_i x) = Tr\left(xR(x) + S(x)\right),$$

onde

$$R(X) = \sum_{i=1}^{(m-w)/2} a_i b_i X + \sum_{j=1}^{h} \sum_{i=1}^{(m-w)/2} \left(a_i^{2^j} b_i + a_i b_i^{2^j}\right) X^{2^j} \in R_h$$

e

$$S(X) = \sum_{i=1}^{(m-w)/2} a_i^{2^{m/2}} b_i X^{2^{m/2}+1}.$$

Aparentemente não temos tudo do que precisávamos para garantir o resultado, porém (3.3.1) para $j = m/2$ significa que

$$\begin{aligned} S(x)^{2^{m/2}} &= \left(\sum_{i=1}^{(m-w)/2} a_i^{2^{m/2}} b_i x^{2^{m/2}+1} \right)^{2^{m/2}} \\ &= \left(\sum_{i=1}^{(m-w)/2} a_i b_i^{2^{m/2}} x^{1+2^{m/2}} \right) \\ &= \left(\sum_{i=1}^{(m-w)/2} a_i^{2^{m/2}} b_i x^{2^{m/2}+1} \right) = S(x) \end{aligned}$$

e utilizamos isto para verificar que

$$Tr_{\mathbf{F}_q/\mathbf{F}_{\sqrt{q}}}[S(x)] = S(x) + S(x)^{\sqrt{q}} = S(x) + S(x)^{2^{m/2}} = 0.$$

Conclui-se pelo item 3 da Proposição 1.1.1 que

$$Tr\left(S(x)\right) = Tr_{\mathbf{F}_{\sqrt{q}}/\mathbf{F}_2}\left\{ Tr_{\mathbf{F}_q/\mathbf{F}_{\sqrt{q}}}[S(x)] \right\} = 0,$$

e como consequência temos

$$\sum_{i=1}^{(m-w)/2} Tr(a_i x) Tr(b_i x) = Tr[xR(x)]. \qquad \square$$

Como uma palavra $\mathcal{C}_R \in \mathscr{C}_h$ tem peso $q/2$, se Q_R tem posto ímpar, $(q - \sqrt{q2^v})/2$ ou $(q + \sqrt{q2^v})/2$, se Q_R tem posto par dado por $m - v$, onde $v = dim(rad\ Q_R)$, e $v \leq 2h$, chegamos à cota inferior $(q - \sqrt{q2^{2h}})$ para o peso mínimo do código em questão. Então vamos fixar desta vez $w = 2h$ e $M = (m - 2h)/2$ para podermos atingir este peso mínimo com palavras criadas através da Proposição 3.3.1, tomando um conjunto linearmente independente $\{a_1, \ldots, a_M\}$, sempre podendo escolher $a_1 = 1$, e obtendo o conjunto $\{b_1, \ldots, b_M\}$ resolvendo (3.3.1) nas variáveis b_i's. Porém, desta vez

este sistema tem M equações e M incógnitas, o que impossibilita um resultado análogo à Proposição 3.1.4. O conjunto S formado pelas soluções $(b_1, \ldots, b_M)$ de (3.3.1) também são um sub-espaço vetorial de $(\mathbf{F}_q)^m$, entretanto, não temos uma cota inferior para a sua dimensão, como temos no caso ímpar.

Seguindo com o trabalho de adaptar os resultados da Seção 3.1, temos abaixo um enunciado idêntico ao da Proposição 3.1.5 e cuja demonstração será praticamente a mesma.

Proposição 3.3.3: *Dado $k \leq M$, sejam $\{c_1, \ldots, c_k\} \subset \mathbf{F}_q$ um conjunto $\mathbf{F}_2$-linearmente independente e $\{d_1, \ldots, d_k\} \subset \mathbf{F}_q$ tal que a função quadrática definida pela expressão*

$$\sum_{i=1}^{k} Tr(c_i x) Tr(d_i x)$$

induz uma palavra pertencente a $\mathscr{C}_h$. Se $\{c_i, d_i;\ i \in \{1, \ldots, k\}\}$ for linearmente dependente, o que é necessariamente verdade para $k < M$, então, para cada $j \in \{1, \ldots, k\}$, d_j é combinação linear dos c_i's.

Demonstração: Idem à da Proposição 3.1.5, com exceção de que agora temos $2k = m - 2[h + (M-k)]$, portanto um conjunto $\{c_i, d_i;\ i \in \{1, \ldots, k\}\}$ linearmente dependente dá origem a uma palavra de peso $(q - \sqrt{q 2^{2[h+(M-k)]}})/2$, mantendo a contradição com a cota inferior de $\mathscr{C}_h$. □

Corolário 3.3.4: *Seja $(b_1, \ldots, b_M)$ solução de (3.1.3). Se $\{a_1, \ldots, a_M, b_1\}$ é linearmente independente, então $\{a, b\}$ também o é.*

Definindo também para este caso V a projeção de S na primeira coordenada, podemos enunciar, também com o enunciado igual ao do Teorema 3.1.7, o principal resultado da seção.

Teorema 3.3.5: *Se $r = dim_{\mathbf{F}_2}(V) - M > 0$ então existe em $\mathscr{C}_h$ um subcódigo de peso mínimo de dimensão r.*

Demonstração: Como o Teorema 3.1.7 utiliza apenas a Proposição 3.1.5 e o Corolário 3.1.6, basta substituir estes pela Proposição 3.3.3 e pelo Corolário 3.3.4, respectivamente. □

Nada impede uma adaptação sem alterações da Proposição 3.1.8, porém a falta de uma cota inferior para S enfraquece o que corresponde ao Corolário 3.1.9 neste caso.

Proposição 3.3.6: *Seja* $(b_1, \ldots, b_M) \in S$. *Então* $(b_1, b'_2, \ldots, b'_M) \in S$ *se, e somente se, existe uma matriz simétrica* A, $(M-1) \times (M-1)$, *com entradas em* $\mathbf{F}_2$ *tal que* $(b'_2, \ldots, b'_M) = (b_2, \ldots, b_M) + (a_2, \ldots, a_M)A$.

Demonstração: Idêntica à demonstração com a Proposição 3.3.3, a Proposição 3.3.4 e o sistema (3.3.1) nos lugares da Proposição 3.1.5, da Proposição 3.1.6 e (3.1.3), respectivamente. □

Corolário 3.3.7: $dim_{\mathbf{F}_2}(V) = dim_{\mathbf{F}_2}(S) - \frac{M(M-1)}{2}$

3.4 Aplicando o processo para m par

Assim como foi feito para o caso onde m era ímpar, trabalharemos nesta seção exemplos de utilização dos resultados obtidos na que precede.

Tomemos um inteiro par $m \geq 4$ e $q = 2^m$. Para os valores de $0 < h < m/2$ que serão tomados, diremos que

$$w = 2h \quad e \quad M = (m - 2h)/2.$$

Também chamaremos de S o espaço vetorial das soluções $(b_1, \ldots, b_M)$ de (3.3.1) para o w definido acima e V a projeção de S na primeira coordenada.

O caso $h = (m-2)/2$

Neste caso $w = m-2$ e $M = 1$. O sistema (3.3.1) consiste apenas na equação

$$b_1 + b_1^{2^{m/2}} = 0,$$

para a qual as soluções são os elementos de $\mathbf{F}_{\sqrt{q}}$, ou seja, $dim(S) = m/2$. Daí, para cada $b \in \mathbf{F}_{\sqrt{q}}$, a palavra induzida por $Tr(x)Tr(bx)$ tem peso $q/4$, que é o mínimo para este código. Como consequência do Teorema 3.3.5, já que neste caso $S = V$, existe um sub-código, de peso mínimo e dimensão $(m-2)/2$, $\mathscr{D}_{(m-2)/2} \subset \mathscr{C}_h$. Tomando sub-códigos $\mathscr{D}_r \subset \mathscr{D}_{(m-2)/2}$ de dimensão r para cada $r \in \{1, \ldots, (m-4)/2\}$, como fizemos em casos em que m era ímpar, chegamos ao resultado abaixo.

Proposição 3.4.1: *Para cada* $r \in \{1, \ldots, (m-2)/2\}$, *os pesos de Hamming generalizados do código binário* $\mathscr{C}_{(m-2)/2}$ *de tamanho* $m-1$ *satisfazem*

$$d_r(\mathscr{C}_{(m-2)/2}) = (2^r - 1) \cdot 2^{m-r-1}.$$

Segue então que para cada r

$$\#C^{(\mathscr{D}_r)} = 2^{m-1}(2^r + 1).$$

O caso $h = (m-4)/2$

Suponhamos agora $m \geq 6$. Temos $w = m-4$, $M = 2$ e o sistema (3.3.1) é

$$\begin{aligned} b_1^{2^{m/2-1}} + b_1 &= a_2 b_2^{m/2-1} + a_2^{m/2-1} b_2 \\ b_1^{2^{m/2}} + b_1 &= a_2 b_2^{m/2} + a_2^{m/2} b_2. \end{aligned}$$

Fazendo a transformação $b_1 = b_1' + a^{2^{m/2}} b_2$ obtemos

$$b_1'^{\,2^{m/2-1}} + b_1' = (a_2 + a_2^{2^{m-1}}) b_2^{m/2-1} + (a_2^{m/2-1} + a_2^{m/2}) b_2 \qquad (3.4.1)$$

$$b_1'^{\,2^{m/2}} + b_1' = (a_2 + a_2^{2^m}) b_2^{m/2} + (a_2^{m/2} + a_2^{m/2}) b_2 = 0. \qquad (3.4.2)$$

A equação (3.4.2) implica $b_1' \in \mathbf{F}_{\sqrt{q}}$. Podemos simplificar (3.4.1) se escolhermos $a_2 \in \mathbf{F}_4 \setminus \mathbf{F}_2$. Neste caso, como $X^4 + X = (X^2 + X)(X^2 + X + 1)$, a_2 deve ser raiz de $X^2 + X + 1$, ou seja, $a_2^2 + a_2 = 1$. Agora observe que, para cada $k \in \mathbb{N}$,

$$a_2^{2^{2k}} = a_2^{4^k} = a_2 \quad e \quad a_2^{2^{2k+1}} = \left(a_2^{4k}\right)^2 = a_2^2.$$

Segue daí que $a_2^{2^{m-1}} = a_2^2$, donde temos que o coeficiente de $b_2^{m/2-1}$ em (3.4.1) é igual a 1. O mesmo ocorre para o de b_2, já que $(m/2-1)$ e $m/2$ são números consecutivos. Com isto verifica-se que a equação (3.4.1) é da forma

$$b_1'^{\,2^{m/2-1}} + b_1' = b_2^{2^{m/2-1}} + b_2.$$

Fazendo a substituição $c = b_1' + b_2$ ficamos com a equação

$$c^{2^{(m-2)/2}} + c = 0$$

a ser resolvida em $\mathbf{F}_q$. Portanto devemos ter c raiz de algum polinômio $p(X) \in \mathbf{F}_2[X]$ irredutível e divisor de $X^{2^{(m-2)/2}} + X$. Como $p(X)$ terá também que dividir $X^q + X$, seu grau é limitado superiormente por d, o máximo divisor comum entre m e $(m-2)/2$. Como $m - 2[(m-2)/2] = 2$, $d \leq 2$. Se $d = 1$, ou seja, $m = 4k$ com $k \in \mathbb{N}$, as únicas soluções para c são 1 e 0, donde segue que $b_2 = b_1' + \mathbf{F}_2$. E se $d = 2$, ou seja, $m = 4k + 2$ com $k \in \mathbb{N}$, como o único polinômio irredutível de grau 2 em $\mathbf{F}_2[X]$ é o que tem como raízes os

elementos de $\mathbf{F}_4 \setminus \mathbf{F}_2$, verifica-se que $b_2 = b_1 + \mathbf{F}_4$. Conclui-se então que o sistema (3.3.1) tem $2\sqrt{q} = 2^{(m+2)/2}$ soluções, quando m é divisível por 4, ou $4\sqrt{q} = 2^{(m+4)/2}$ soluções, caso contrário.

O peso mínimo de $\mathscr{C}_h$ é $2^{m-3} \cdot 3$ e com as informações acima obtemos S com dimensão $(m+2)/2$ ou $(m+4)/2$, donde segue, pelo Corolário 3.3.7, que os possíveis valores para a dimensão de V são $m/2$ ou $(m+2)/2$. Tomando os sub-códigos $\mathscr{D}_r \subset \mathscr{C}_h$ como no exemplo anterior, desta vez com $1 \leq r \leq m/2$, para m divisível por 4, ou $1 \leq r \leq (m+2)/2$, caso contrário, formulamos o resultado seguinte:

Proposição 3.4.2: *Os pesos de Hamming generalizados do código binário* $\mathscr{C}_{(m-4)/2}$ *de tamanho* $2^m - 1$ *satisfazem*

$$d_r(\mathscr{C}_{(m-4)/2}) = (2^r - 1)2^{m-r-2} \cdot 3$$

para cada $r \in \{1, \ldots, m/2\}$. *Além disso, se* m *não for divisível por 4, também vale a mesma equação para* $r = (m+2)/2$.

Aplicando aqui a Proposição 2.1.3 temos para cada $1 \leq r \leq m/2$, e também para $r = (m+2)/2$ no caso m não for divisível por 4,

$$\#C^{(\mathscr{D}_r)} = 2^{m-2}(2^r + 3).$$

Notação

Aqui se encontra a notação que não foi definida no decorrer do texto:

- $\mathbb{N} = \{1, 2, 3, \ldots\}$ e $\mathbb{Z}_{\geq 0} = \{0, 1, 2, 3, \ldots\}$.
- Dado um conjunto finito A, $\#A$ será a cardinalidade deste conjunto.
- Para cada x número real, $[x]$ representa o maior inteiro menor ou igual a x.
- Dado um corpo $\mathbf{K}$, $\mathbf{K}^*$ denota o conjunto $\mathbf{K}\backslash\{0\}$, enquanto $\mathbf{K}[X_1, \ldots, X_n]$ é o anel de polinômios nas variáveis $X_1, \ldots, X_n$.
- Dado V espaço vetorial sobre um corpo $\mathbf{K}$, para quaisquer U e W sub-espaços vetoriais de V, $U + W$ denotará o também sub-espaço $\{u + w;\ u \in U \text{ e } w \in W\}$. Além disso, para cada $v \in V$, $\mathbf{K} \cdot v$ representará o sub-espaço gerado por v, ou seja, o conjunto $\{k \cdot v;\ k \in \mathbf{K}\}$
- Dado um anel $\mathbf{R}$ e $r_1, \ldots, r_n \in \mathbf{R}$, $(r_1, \ldots, r_n)$ é o ideal gerado pelos elementos r_i, ou seja, o conjunto $\{s_1 \cdot r_1 + \ldots + s_n \cdot r_n;\ s_1, \ldots, s_n \in \mathbf{R}\}$.

Referências Bibliográficas

[G-V 1] Gerard van der Geer e Marcel van der Vlugt, Reed-Muller codes and supersingular curves I, Compositio Mathematica 84 (1992), 333-367.

[G-V 2] Gerard van der Geer e Marcel van der Vlugt, Fibre products of Artin-Schreier curves and generalized Hamming weights of codes, Journal of Combinational Theory Series A 70 (1995), 337-348

[G-V 3] Gerard van der Geer e Marcel van der Vlugt, Quadratic Forms, Generalized Hamming Weights of Codes and Curves with Many Points, Journal of Number Theory 59 (1996), 20-36

[F] W. Fulton, Algebraic Curves, Benjamin, 2008

[G-L] Jacobus H. van Lint e Gerald van der Geer, Introduction to Coding Theory and Algebraic Geometry

[L-N] Rudolf Lidl e Harald Niederreiter, Finite fields, "Encycl. Math. Appl." Vol. 20, Addison-Wesley, Reading, MA, 1983.

[P] Albrecht Pfister: Quadratic Forms with Applications to Algebraic Geometry and Topology, "London Mathematical Society Lecture Note Series; 217", 1995