Ana Rachel Brito de Paula

Polinômios de Permutação e Palavras Balanceadas

CAMPINAS
2015

UNIVERSIDADE ESTADUAL DE CAMPINAS

Instituto de Matemática, Estatística
e Computação Científica

ANA RACHEL BRITO DE PAULA

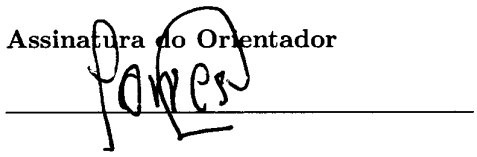
POLINÔMIOS DE PERMUTAÇÃO E PALAVRAS BALANCEADAS

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

Orientador: Fernando Eduardo Torres Orihuela

ESTE EXEMPLAR CORRESPONDE À VERSÃO FINAL DA DISSERTAÇÃO DEFENDIDA PELA ALUNA ANA RACHEL BRITO DE PAULA, E ORIENTADA PELO PROF. DR. FERNANDO EDUARDO TORRES ORIHUELA.

Assinatura do Orientador



CAMPINAS
2015

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

P281p

Paula, Ana Rachel Brito de, 1990-
Polinômios de permutação e palavras balanceadas / Ana Rachel Brito de Paula. – Campinas, SP : [s.n.], 2015.

Orientador: Fernando Eduardo Torres Orihuela.
Dissertação (mestrado) – Universidade Estadual de Campinas, Instituto de Matemática, Estatística e Computação Científica.

1. Polinômios. 2. Teoria da codificação. 3. Permutações (Matemática). 4. Análise combinatória. 5. Códigos corretores de erros (Teoria da informação). I. Torres Orihuela, Fernando Eduardo,1961-. II. Universidade Estadual de Campinas. Instituto de Matemática, Estatística e Computação Científica. III. Título.

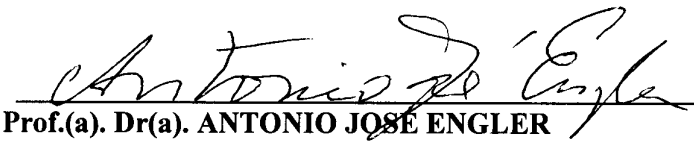
Informações para Biblioteca Digital

Título em outro idioma: Permutacion polinomias and balanced words
Palavras-chave em inglês:
Polynomials
Coding theory
Permutations (Mathematics)
Combinatorial analysis
Error-correcting codes (Information theory)
Área de concentração: Matemática Aplicada
Titulação: Mestra em Matemática Aplicada
Banca examinadora:
Fernando Eduardo Torres Orihuela
Antonio José Engler
Ercílio Carvalho da Silva
Data de defesa: 17-04-2015
Programa de Pós-Graduação: Matemática Aplicada

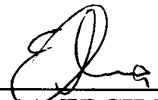
Dissertação de Mestrado defendida em 17 de abril de 2015 e aprovada

Pela Banca Examinadora composta pelos Profs. Drs.

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



Prof.(a). Dr(a). ANTONIO JOSÉ ENGLER



Prof.(a). Dr(a). ERCILIO CARVALHO DA SILVA

Abstract

The main goal in writing this dissertation is the study of the influence of the Theory of Permutation Polynomials in the context of Coding Theory via the concept of **balanced word**. Our basic reference is the paper "Permutation polynomials and applications to coding theory" by Y. Laigke-Chapury. Our plan is to introduce the basic concepts in Coding Theory, Permutation Polynomials; then we mainly consider the long-standing open Helleseth's conjecture.

Keywords: polynomials, coding , permutation.

Resumo

A dissertação "Polinômios de Permutação e Palavras Balanceadas" tem como principal objetivo estudar a influência dos polinômios de permutação na teoria de códigos mediante o conceito de **palavra balanceada**. A base do trabalho é o artigo "Permutacion polynomials and aplications to coding theory" de Yann Laigke-Chapuy. Expomos os conceitos básicos de polinômios de permutação como algumas de suas características, exemplos e métodos para identificação dos mesmos. Em seguida trataremos dos códigos lineares com ênfase nos binários explorando particularmente a conjectura de Helleseth.

Palavras-chave: polinômio, código, permutação.

Sumário

Aos meus pais.

Agradecimentos

Meu primeiro agradecimento a Deus que me mantém viva, saudável e determinada a continuar assim.

Meu melhor agradecimento aos meus pais, que sempre com muito amor me incentivaram a encarar os desafios mesmo quando isso significa ficar longe dos seus olhos.

Meu mais apaixonado agradecimento ao meu namorado Enio Romagnome, com quem nessa caminhada de pós-graduação vivi ao seu lado mais aventuras do que poderia escrever e me motivou mais do que ele próprio imagina.

Meu sincero agradecimento a meu orientador Fernando Torres, o qual eu insisto em chamar de senhor, por todo os ensinamentos, paciência e preocupação, especialmente no mês que antecedeu a defesa.

Meu fraterno agradecimento aos Amigos, especialmente os que também estão vivendo esse momento de pós, pelas experiências trocadas, pelas conversas sejam elam pessoalmente ou virtuais.

E finalmente um agradecimento a CAPES que me financiou este trabalho no último ano.

Capítulo 1

Introdução

Cada vez que se enviam dados através de determinados canais de transmissão é muito provável que erros sejam cometidos. Geralmente um dado é axiomatizado como uma sequencia finita de longitude fixa n composta de certos símbolos escolhidos de um conjunto $\mathcal{A}$, também finito, chamado de alfabeto. Assim os dados a serem transmitidos são de fato um subconjunto $\mathcal{C}$ de vetores em $\mathcal{A}^n$ o, qual e dito de código. Logo o objetivo da Teoria de Códigos é assegurar a existência de bons códigos, no sentido por exemplo de ter suficientes elementos sem afetar o custo de sua construção; também procura-se que sejam de fácil obtenção. Tradicionalmente as ferramentas que foram utilizadas provinham da Combinatória e a Teoria de Grupos. Em 1977, Goppa [**Go**] definiu os chamados Códigos Algébrico-Geométricos (atualmente ditos de códigos de Goppa Geométricos), via a Teoria de Curvas sobre corpos finitos, estabelecendo resultados novos para códigos. Escolhemos, no entanto, nessa dissertação trabalhar com códigos de corpos finitos via a Teoria de Polinômios de Permutação, pois seu estudo requer requisitos mais básico que os correspondentes a Curvas Algébricos que de fato são considerados nas diversas disciplinas de álgebra em nosso mestrado. Mais ainda os resultados principais serão considerados em corpos finitos de característica dois e o objetivo estará centrado na procura de códigos contendo *palavras balanceadas* que intuitivamente melhora a segurança na transmissão de dados. Exporemos a Conjetura de Helleseth (1976) a qual diz "intuitivamente"que os códigos desejados realiza-se basicamente como imagens de uma certa função traço. Pelo tanto nossa exposição usara fortemente a existência de polinômios de permutação particulares como certos binomiais completos tal que uma de suas parcelas é do tipo x^k, sendo k um *inteiro de Niho* o qual está relacionado com certas sequências binarias [**Niho**].

O artigo base deste trabalho é o [**Chapuy**], listado na referência. O trabalho é compreendido em dois capítulo. O primeiro trata dos preliminares sobre corpos finitos, códigos lineares, palavras balanceadas e polinômios de permutação; o segundo capítulo considera os pre-requisitos e resultados importantes para o entendimento da Conjectura de Helleseth. Finalmente prova-se essa conjetura para certos casos particulares a saber os Teoremas 5.5, 5.6 e a Proposição 5.9 em [**Chapuy**].

Boa leitura a todos.

Capítulo 2

Preliminares

Neste capítulo daremos definições exporemos resultados importante para o estudo do assunto deste trabalho.

2.1 Corpos Finitos

Definição 2.1. *Um grupo é um conjunto G munido de uma operação binária interna $*$ que satisfaz as seguintes propriedades:*

1. $\forall\ a, b, c \in G$ *temos que* $a * (b * c) = (a * b) * c$
2. $\exists\ 0 \in G$ *tal que* $\forall a \in G\ a * 0 = 0 * a = a$
3. *Para cada* $a \in G$ *existe* a^{-1} *em* G *tal que* $a * a^{-1} = a^{-1} * a = 0$.

G é dito grupo abeliano se satisfizer a propriedade 4:

4. $\forall a, b \in G$ *temos* $a * b = b * a$.

Definimos para todo elemento $a \in G$ e todo inteiro j, $a^j = \underbrace{a * \cdots * a}_{j\ vezes}$.

Um grupo G é dito cíclico se existe $a \in G$ tal que para qualquer $b \in G$ existe um inteiro j tal que $b = a^j$.

Definição 2.2. *Um anel $(R, +, \cdot)$ é um conjunto R munido de dual operações binárias internas $+$ e $\cdot$ que satisfazem:*

1. *R é um grupo abeliano em relação a $+$*
2. $\forall a, b, c \in R$ *temos* $a \cdot (b \cdot c) = (a \cdot b) \cdot c$
3. $\forall a, b, c \in R$ *temos* $a \cdot (b + c) = a \cdot b + a \cdot c$ *e* $(a + b) \cdot c = a \cdot c + b \cdot c$

Se o anel R tem outras propriedades ele ganha outro nomes, tais como:

1. *R é dito anel com identidade se existe uma identidade multiplicativa, i. é, $\exists e \in R$ tal que $\forall a \in R\ a \cdot e = e \cdot a = a$*

2. *R é dito anel comutativo se $\cdot$ é comutativo.*

3. *R é dito domínio de integridade se é comutativo com identidade $e \neq 0$ se $a \cdot b = 0$ implica que $a = 0$ ou $b = 0$*

4. *R é dito anel de divisão se $\forall a \in R \setminus \{0\}\ \exists a^{-1} \in R$ tal que $a \cdot a^{-1} = a^{-1} \cdot a = e$*

5. *Um anel de divisão comutativo é chamado de corpo, um corpo com um número finito de elementos é chamado de corpo finito.*

Seja R uma anel com identidade e, considere o homomorfismo $\phi : \mathbb{Z} \to R$ definido por $\phi(n) = n \cdot e = \underbrace{e + \cdots e}_{n\ vezes}$. Se Ker($\phi$)=$n\mathbb{Z}$ o anel R é dito de *característica positiva n. Se Ker(ϕ)= 0, R é dito de característica 0.*

Teorema 2.3. *Um corpo finito tem característica prima.*

Demonstração. Seja $\mathbb{F}$ um corpo finito. Vamos mostrar primeiro que $\mathbb{F}$ tem característica positiva.

Considere os múltiplos $e, 2e, 3e, \ldots$ da identidade e de $\mathbb{F}$. Como $\mathbb{F}$ é finito existem inteiros k e m tais que $1 \leq m < k$ e $ke = me$, ou ainda, $(m-k)e = 0$, assim $(m-k)x = (m-k)ex = 0x = 0$ para todo $x \in \mathbb{F}$ e $\mathbb{F}$ tem característica positiva.

Seja n a característica de $\mathbb{F}$. Vamos mostrar que n é primo.

Suponha que não, i. é, existem dois inteiros positivos a e b tais que $1 < a, b < n$ e $ab = n$. Então

$$0 = ne = (ab)e = (ae)(be) = 0$$

Dessa forma ou $ax = ae = 0$ ou $bx = be = 0$ para todo $x \in \mathbb{F}$ pois estamos em um corpo. Mas qualquer um dos casos contradiz a definição de característica. Portanto, n é primo. □

Um subconjunto K de um corpo F que também é um corpo com as operações induzidas é chamado subcorpo de F. Neste contexto F é dito extensão de K (Notação: $F|K$). Se $K \neq F$, K é dito subcorpo próprio de F. Observamos ainda que F é um K-espaço vetorial.

O menor subcorpo contido em um corpo F é chamado corpo primo de F. Os corpos primos são $\mathbb{Q}$ se o corpo é infinto ou $\mathbb{F}_p$, onde p é um inteiro primo, se o corpo é finito.

Teorema 2.4. *Seja F um corpo finito de característica p. Então F tem p^n elementos, onde n é a dimensão de F sobre o subcorpo primo $\mathbb{F}_p$.*

Demonstração. Defina $K = \mathbb{F}_p$. Seja $\{b_1, b_2, \ldots, b_m\}$ uma base de F sobre K. Cada elemento de F pode ser unicamente representado na forma $a_1b_1 + a_2b_2 + \cdots + a_mb_m$, onde $a_1, a_2, \ldots, a_m \in K$. Como para cada a_i há q possibilidades F tem q^m elementos. □

Mostra-se que dois corpos finitos como o mesmo número de elementos são isomorfos. A partir de agora denotaremos um corpo finito por $\mathbb{F}_q$, onde $q = p^n$ e p é a característica prima do corpo. Denotaremos ainda por $\mathbb{F}_q^*$ o grupo multiplicativo de dos elementos não nulo de $\mathbb{F}_q$

Teorema 2.5. *Para todo corpo finito $\mathbb{F}_q$ o grupo $\mathbb{F}_q^*$ é cíclico.*

Demonstração. Vamos assumir $q \geq 3$. Seja $h = q - 1$ a ordem do subgrupo $\mathbb{F}_q^*$ e $h = p_1^{r_1} p_2^{r_2} \cdots p_m^{r_m}$ a sua decomposição em fatores primos.

Para todo i, $1 \leq i \leq m$, o polinômio $x^{h/p_i} - 1$ tem no máximo h/p_i raízes sobre $\mathbb{F}_q$. Como $h/p_i < h$ existem elementos não nulos de $\mathbb{F}_q$ que não são raízes do polinômio. Seja a_i um desses elementos e $b_i = a_i^{h/p_i}$.

Nós temos que $b_i^{p_i^{r_i}} = 1$, assim a ordem de b_i é um divisor de $p_i^{r_i}$, logo é da forma $p_i^{s_i}$, onde $0 \leq s_i \leq r_i$. Por outro lado

$$b_i^{p_i^{r_i - 1}} = a_i^{h/p_i} \neq 1,$$

assim a ordem de b_i é $p_i^{r_i}$. Afirmamos que $b = b_1 b_2 \cdots b_m$ tem ordem h.

Suponha, o contrário, que ordem de b é um divisor próprio de h, dessa forma é um divisor de pelo menos um dos inteiros h/p_i, com $1 \leq i \leq m$. Vamos dizer que a ordem de b é um divisor de h/p_1. Temos então:

$$1 = b^{h/p_1} b_1^{h/p_1} b_2^{h/p_1} \cdots b_m^{h/p_1}.$$

Se $2 \leq i \leq m$, então $p_i^{r_i}$ divide h/p_1 e daí $b_i^{h/p_1} = 1$. Dessa forma $b_1^{h/p_1} = 1$, assim a ordem de b_1 divide h/p_1, o que é impossível por a ordem de b_1 é $p_1^{r_1}$.

Portanto, $\mathbb{F}_q^*$ é cíclico com gerador b. □

Definição 2.6. *Um gerador do grupo cíclico $\mathbb{F}_q^*$ é chamado de elemento primitivo de $\mathbb{F}_q$.*

2.2 Carácter

Falaremos agora sobre a função carácter. Seja G um grupo multiplicativo finito. Um carácter χ de G é um homomorfismo sobrejetivo de G sobre o grupo multiplicativo U dos números complexos de valor absoluto 1.

Entre os caracteres de G temos o carácter trivial χ_0 definido por $\chi_0(g) = 1$ para todo $g \in G$; todos os outros caracteres são chamados não triviais. Cada carácter de χ de G está associado a um carácter conjugado $\overline{\chi}$ definido por $\overline{\chi}(g) = \overline{\chi(g)},\ \forall g \in G$.

Dados $\chi_1, \chi_2, \ldots, \chi_m$ caracteres de G definimos a multiplicação de carácter como $(\chi_1 \chi_2 \cdots \chi_m)(g) = \chi_1(g)\chi_2(g)\cdots\chi_m(g)$ e denotamos $\chi^{(k)} = \underbrace{\chi \cdots \chi}_{k \text{ vezes}}$. Com essa operação o conjunto $\hat{G}$ dos caracteres G é um grupo multiplicativo com identidade χ_0. O grupo $\hat{G}$ é finito e tem ordem igual a ordem de G.

*O Teorema e Lema apresentados a seguir não serão demonstrados nesse trabalho. Suas provas podem ser vistas no livro [***Lidl** *], Teorema 5.39 e Lema 6.56, respectivamente, citado nas referências.*

Teorema 2.7. *Seja ψ um carácter multiplicativo de $\mathbb{F}_q$ e ordem $m > 1$ e $f \in \mathbb{F}_q[x]$ um polinômio mônico de grau positivo que não é a m-ésima potência de um polinômio. Seja d o número de raízes*

distintas de f em $\mathbb{F}_q$ e suponha $d \geq 2$. Então existem números complexos $\omega_1, \ldots, \omega_{d-1}$ dependendo apenas de f e ψ, tais que para qualquer inteiro positivo s temos

$$\sum_{\gamma \in \mathbb{F}_{q^s}} \psi^{(s)}(f(\gamma)) = -\omega_1^s - \cdots - \omega_{d-1}^s.$$

Lema 2.8. *Os números complexos $\omega_1, \ldots, \omega_{d-1}$ do Teorema 2.7 satisfazem $|\omega_j| \leq q^{1/2}$ para todo $1 \leq j \leq d-1$.*

Teorema 2.9. *Seja ψ um carácter multiplicativo de $\mathbb{F}_q$ e ordem $m > 1$ e $f \in \mathbb{F}_q[x]$ um polinômio mônico de grau positivo que não é a m-ésima potência de um polinômio. Seja d o número de raízes distintas de f em $\mathbb{F}_q$. Então para todo $a \in \mathbb{F}_q$ temos:*

$$\left| \sum_{c \in \mathbb{F}_q} \psi(af(c)) \right| \leq (d-1)q^{1/2}.$$

Demonstração. Suponhamos primeiro $d = 1$. Como $d = 1$ e f não é uma potência de um polinômio $f = x - \alpha$ para algum $\alpha \in \mathbb{F}_q$. Assim f é uma bijeção e $\sum_{c \in \mathbb{F}_q} \psi(af(c)) = 0$ para todo $a \in \mathbb{F}_q$. A inequação então é satisfeita para $d = 1$.

Suponhamos agora $d \geq 2$. Aplicando o Teorema 2.7 obtemos:

$$\sum_{c \in \mathbb{F}_q} \psi(af(c)) = \psi(a) \sum_{c \in \mathbb{F}_q} \psi(f(c)) = -\psi(a)(\omega_1 + \cdots + \omega_{d-1}).$$

Usando o Lema 2.8 temos que $|\omega_j| \leq q^{1/2}$ para $1 \leq j \leq d-1$, e assim obtemos a desigualdade procurada. □

2.3 Função Traço

Definiremos agora uma outra função que será muito importante para a segunda parte do nosso trabalho.

Definição 2.10. *Seja $F = \mathbb{F}_{q^m}$ uma extensão de $K = \mathbb{F}_q$. Para $\alpha \in F$ o traço $Tr_{F/K}(\alpha)$ de α sobre K é definido por*

$$Tr_{F/K}(\alpha) = \alpha + \alpha^q + \cdots + \alpha^{q^{m-1}}.$$

Se K é o subcorpo primo de F, então $Tr_{F/K}(\alpha)$ é chamado de traço absoluto de α e denotado por $Tr_F(\alpha)$.

Em outras palavras, o traço de α sobre o corpo K é a soma dos conjugados de α em relação a K.

Uma outra descrição de traço é a seguinte. Seja $f \in K[x]$ o polinômio minimal de α sobre K, seu grau d é um divisor de m. O polinômio $g(x) = f(x)^{m/d} \in K[x]$ é chamado polinômio

característico de α sobre K. As raízes de f sobre F são dadas por $\alpha, \alpha^q, \ldots, \alpha^{q^{d-1}}$, as raízes do polinômio g são exatamente os conjugados de α. Assim

$$\begin{aligned} g(x) &= x^m + a_{m-1}x^{m-1} + \cdots + a_0 \\ &= (x-\alpha)(x-\alpha^q)\cdots(x-\alpha^{q^{m-1}}), \end{aligned}$$

comparando os coeficientes temos que

$$Tr_{F/K}(\alpha) = -a_{m-1}.$$

Em particular, $Tr_{F/K}(\alpha)$ é sempre um elemento de K.

Teorema 2.11. *Sejam $K = \mathbb{F}_q$ e $F = \mathbb{F}_{q^m}$. Então a função traço $Tr_{F/K}$ satisfaz as seguintes propriedades:*

(i) $Tr_{F/K}(\alpha+\beta) = Tr_{F/K}(\alpha) + Tr_{F/K}(\beta)$ para todo $\alpha, \beta \in F$;

(ii) $Tr_{F/K}(c\alpha) = cTr_{F/K}(\alpha)$ para todo $c \in K$ e $\alpha \in F$;

(iii) $Tr_{F/K}$ é uma transformação linear sobrejetiva de F em K, onde F e K são vistos como espaços vetoriais sobre K;

(iv) $Tr_{F/K}(a) = ma$ para todo $a \in K$;

(v) $Tr_{F/K}(\alpha^q) = Tr_{F/K}(\alpha)$ para todo $\alpha \in F$.

Demonstração. (i) Para $\alpha, \beta \in F$ usando a propriedade $(\alpha+\beta)^q = \alpha^q + \beta^q$ obtemos

$$\begin{aligned} \mathrm{Tr}_{F/K}(\alpha+\beta) &= \alpha + \beta + (\alpha+\beta)^q + \cdots + (\alpha+\beta)^{q^{m-1}} \\ &= \alpha + \beta + \alpha^q + \beta^q + \cdots + \alpha^{q^{m-1}} + \beta^{q^{m-1}} \\ &= \mathrm{Tr}_{F/K}(\alpha) + \mathrm{Tr}_{F/K}(\alpha). \end{aligned}$$

(ii) Para $c \in K$ temos que $c^{q^j} = c$ para todo $j \geq 0$. Assim para $\alpha \in F$ temos

$$\begin{aligned} \mathrm{Tr}_{F/K}(c\alpha) &= c\alpha + c^q + \alpha^q + \cdots + c^{q^{m-1}}\alpha^{q^{m-1}} \\ &= c\alpha + c\alpha^q + \cdots + c\alpha^{q^{m-1}} \\ &= c\mathrm{Tr}_{F/K}(\alpha). \end{aligned}$$

(iii) As propriedade (i) e (ii) mais o fato que $\mathrm{Tr}_{F/K}(\alpha) \in K$ para todo $\alpha \in F$ garantem que $\mathrm{Tr}_{F/K}$ é uma transformação linear de F em K. Para a sobrejetividade é suficiente mostrar que existe $\alpha \in F$ tal que $\mathrm{Tr}_{F/K}(\alpha) \neq 0$, pois K como espaço vetorial sobre K tem dimensão 1.

Temos então que $\mathrm{Tr}_{F/K}(\alpha) = 0$ se, e somente se, α é raiz do polinômio $x^{q^{m-1}} + \cdots + x^q + x \in K[x]$ em F. Como o polinômios tem no máximo q^{m-1} em F e F tem q^m elementos existe $\alpha \in F$ tal que $\mathrm{Tr}_{F/K}(\alpha) \neq 0$.

(iv) Seja $a \in K$ assim $a^{q^j} = a$ para $j \geq 1$. Então

$$\begin{aligned} \mathrm{Tr}_{F/K}(a) &= a + a^q + \cdots + a^{q^{m-1}} \\ &= \underbrace{a + a + \cdots + a}_{\text{m vezes}} \\ &= ma. \end{aligned}$$

(v) Para todo $\alpha \in F$ temos que $\alpha^{q^m} = \alpha$, assim $\mathrm{Tr}_{F/K}(\alpha^q) = a^q + a^{q^2} + \cdots + a^{q^m} = \mathrm{Tr}_{F/K}(\alpha)$. $\square$

2.4 Códigos Lineares

O ponto de partida para a construção de um código corretor de erro é um conjunto finito $\mathcal{A}$ chamado de alfabeto. O número de elementos de $\mathcal{A}$ será denotado por $|\mathcal{A}|$. Um subconjunto próprio de $\mathcal{C} \subset \mathcal{A}^n$, onde n é um número natural, é chamado código corretor de erros.

O exemplo mais familiar de código é o idioma. Consideremos o alfabeto $\mathcal{A}$ formado pelas 23 letras do alfabeto da língua portuguesa junto com as vogais acentuadas, o cedilha e o espaço em branco. Temos então que qualquer palavra da língua portuguesa é um elemento do conjunto $\mathcal{A}^{27}$, onde 27 é o tamanho da maior palavra da língua. De fato a língua portuguesa é um subconjunto $\mathcal{C}$ próprio de $\mathcal{A}^{27}$. Suponhamos que escrevemos uma sequência de letras e formamos a palavra "matebática". Este não é um elemento de $\mathcal{C}$, claramente percebemos que ocorreu um erro e, neste caso, a correção é possível pois a palavra de $\mathcal{C}$ que mais se assemelha a "matebática" é "matemática".

Mas se queríamos escrever a palavra "gato" e escrevermos "galo" ou "pato" não seriamos capazes de detectar o erros. Assim o código $\mathcal{C}$ não é muito eficiente.

Hoje em dia, códigos são utilizados sempre que se deseja transmitir ou armazenar dados, garantindo a sua confiabilidade. São exemplos disso todas as comunicações via satélites, as comunicações internas de um computador, o armazenamento óptico de dados entre outros.

Vamos fazer um exemplo para ilustrar os princípios da Teoria de Código. Suponhamos que temos um robô que se move sobre um tabuleiro quadriculado, de modo que ao darmos um comando (Leste, Oeste, Norte, Sul), o robô se descola do centro de uma casa para o centro de outra contígua indicada pelo comando. Os quatro comandos são codificados como elementos de $\{0,1\} \times \{0,1\}$ como é mostrado abaixo:

$$\begin{array}{cccc} \textit{Leste} & \longmapsto & 00 & \qquad \textit{Norte} \longmapsto 10 \\ \textit{Oeste} & \longmapsto & 01 & \qquad \textit{Sul} \longmapsto 11 \end{array}$$

O código do lado direito da tabela é chamado de código fonte. Suponhamos agora que esses pares ordenados sejam transmitidos via rádio e que o sinal no caminho sofra interferências. Imaginemos que a mensagem 00 possa, na chegada, ser recebida como 01, o que faria com que o robô fosse para Oeste ao invés de Leste. O que se faz, então, é recodificar as palavras, de modo a introduzir redundâncias que permitam detectar e corrigir erros. Podemos,por exemplo, modificar o nosso código como segue:

$$\begin{array}{ccc} 00 & \longmapsto & 00000 \\ 01 & \longmapsto & 01011 \\ 10 & \longmapsto & 10110 \\ 11 & \longmapsto & 11101 \end{array}$$

Nessa recodificação, as duas primeiras posições reproduzem o código fonte, as outras três posições são redundâncias introduzidas. Este novo código é chamado de código de canal.

Suponhamos que ao transmitir a palavra 10110, por exemplo, tenhamos recebido a mensagem 11110. Comparando essa mensagem as palavras do código notamos que não lhe pertence e, portando, detectamos erros. A palavra do código que mais se aproxima da mensagem, isto é, a que tem menor número de componentes diferentes, é 10110, que é precisamente a palavra transmitida e assim fizemos uma correção. Esse esquema de transmissão e recebimento é ilustrado na figura abaixo.

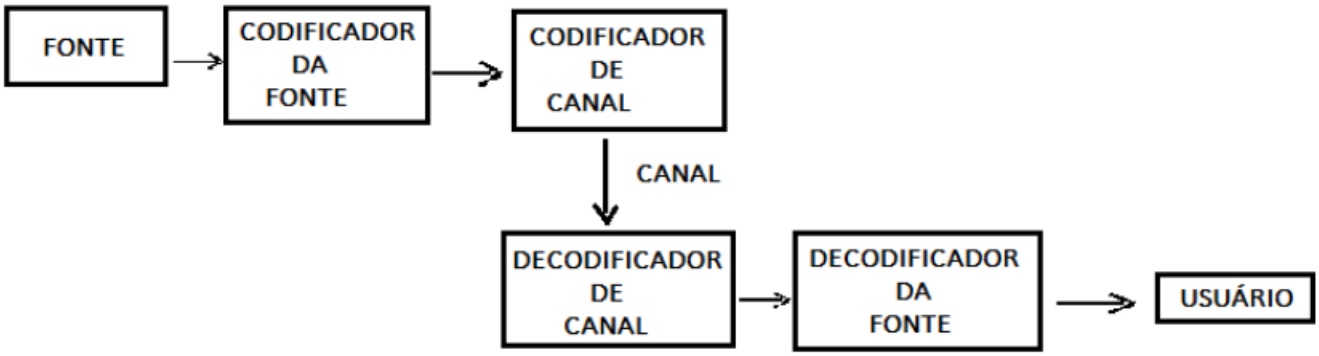


Figura 2.1: Esquema gráfico de transmissão de uma palavra

Definição 2.12. *Dados $u = (u_1, u_2, ..., u_n), v = (v_1, v_2, \ldots, v_n) \in \mathcal{A}^n$ a distância de hamming é dada por $d(u, v) = \#\{i | u_i \neq v_i,\ 1 \leq i \leq n\}$.*

Proposição 2.13. *Dados $u, v, w \in \mathcal{A}^n$ as seguintes propriedades são válidas:*

(i) Positividade: $d(u, v) \geq 0$ e $d(u, v) = 0 \Leftrightarrow u = v$;

(ii) Simetria: $d(u, v) = d(v, u)$;

(iii) Desigualdade triangular: $d(u, v) \leq d(u, w) + d(w, v)$.

Demonstração. (i) Seja M um conjunto finito qualquer, temos que $\#M \geq 0$ e $\#M = 0 \Leftrightarrow M = \emptyset$. Assim $d(u, v) \geq 0$, pois por definição $d(u, v)$ é a quantidade de elementos de um conjunto finito. Se $d(u, v) = 0$ se somente se $\{i | u_i \neq v_i,\ 1 \leq i \leq n\} = \emptyset$ e isto acontece se somente se $u = v$.

(ii)$\{i | u_i \neq v_i,\ 1 \leq i \leq n\} = \{j | v_j \neq u_j,\ 1 \leq j \leq n\}$ isso implica que $d(u, v) = d(v, u)$.

(iii) Vamos analisar a contribuição da i-ésima coordenada em $d(u, v)$, denotaremos essa contribuição por $d_i(u, v)$, assim $d(u, v) = \sum_{i=1}^{n} d_i(u, v)$. Se $u_i = v_i$, então $d_i(u, v) = 0$, temos duas possibilidades para w_i. Ou $w_i = u_i = v_i$ e assim $d_i(u, w) = d_i(w, v) = 0$, ou $w_i \neq u_i$ e teremos $d_i(u, w) = d_i(w, v) = 1$. Em qualquer um dos casos temos que $d_i(u, v) \leq d_i(u, w) + d_i(w, v)$. Se

$u_i \neq v_i$ temos duas possibilidades ou $d_i(u,w) = 0$ e $d_i(w,v) = 1$, ou $d_i(u,w) = 1$ e $d_i(w,v) = 0$. Em qualquer umas das possibilidades temos $d_i(u,w) + d_i(w,v) = 1 = d_i(u,v)$. Dessa forma $d_i(u,v) \leq d_i(u,w) + d_i(w,v)$ para todo $i \in \{1,2,...,n\}$, portando $d(u,v) \leq d(u,w) + d(w,v)$. □

Com essas propriedades temos que a distância 2.12 é uma métrica, chamada de métrica de Hamming. Dados um elemento $a \in \mathcal{A}^n$ e um número real $t > 0$, definimos o disco e a esfera de centro a e raio t respectivamente, como os conjuntos:

$$D(a,t) = \{u \in \mathcal{A}^n | d(u,a) \leq t\}$$

$$S(a,t) = \{u \in \mathcal{A}^n | d(u,a) = t\}$$

.

Lema 2.14. *Para todo $c \in \mathcal{A}^n$ e $r > 0$ natural temos que $|D(c,r)| = \sum_{i=0}^{n} \binom{n}{i}(q-1)^i$, onde $q = |\mathcal{A}|$*

Demonstração. Primeiro vamos mostrar que $|S(c,i)| = \binom{n}{i}(q-1)^i$. De fato, fixado uma entrada existem $q-1$ opções para a entrada corresponde em uma palavra diferente, fazemos isso i vezes. Existem dessa forma $\binom{n}{i}$ formas de escolhas para quais i elementos são diferentes, daí $|S(c,i)| = \binom{n}{i}(q-1)^i$.

Se $i \neq j$ então $S(c,i) \cap S(c,j) = \emptyset$. Temos ainda que $D(c,r) = \{c \in \mathcal{A}^n | d(c,a) \leq r\} = \bigcup_{i=0}^{r} S(c,i)$. Dessa forma

$$|D(c,r)| = \sum_{i=0} r|S(c,i)| = \sum_{i=0}^{r} \binom{n}{i}(q-1)^i$$

. □

Definição 2.15. *Seja $\mathcal{C}$ um código. A distância mínima de $\mathcal{C}$ é o número $d = min\{d(u,v) | u, v \in \mathcal{C}; u \neq v\}$.*

Dado d distancia mínima de $\mathcal{C}$ define-se $k = \lfloor \frac{d-1}{2} \rfloor$, onde $\lfloor t \rfloor$ é a parte inteira do número real t.

Lema 2.16. *Seja $\mathcal{C}$ um código e d sua distância mínima. Se c e c' são palavras distintas então $D(c,k) \cap D(c',k) = \emptyset$.*

Demonstração. Suponha $x \in D(c,k) \cap D(c',k)$, então $d(c,x) \leq k$ e $d(c',x) \leq k$. Assim pela desigualdade triangular temos que:

$$d(c,c') \leq d(c,x) + d(c',x) \leq 2k \leq d-1$$

Absurdo, pois $d(c,c') \geq d$. Portanto $D(c,k) \cap D(c',k) = \emptyset$. □

Teorema 2.17. *Seja $\mathcal{C}$ um código de distância mínima d e $k = \lfloor \frac{d-1}{2} \rfloor$. Então $\mathcal{C}$ pode corrigir até k erros e detectar $d-1$.*

Demonstração. Seja $b \in \mathcal{A}^n$ tal que existe $c \in \mathcal{C}$ o qual $d(c,b) \leq k$. Estão $b \in D(c,k)$, pelo Lema 2.16 este c é único, assim o erro foi corrigido.

Dado $c \in \mathcal{C}$ podemos alterar c en até $d-1$ letras sem resultar em outro elemento de $\mathcal{C}$, pois a distância mínima é d. Assim podemos detectar até $d-1$ erros. □

Definição 2.18. *Seja $\mathcal{C} \in \mathcal{A}^n$, dizemos que $\mathcal{C}$ é um código perfeito se $\bigcup_{c\in\mathcal{C}} D(c,k) = \mathcal{A}^n$.*

A partir de agora o nosso alfabeto $\mathcal{A}$ é um corpo finito $\mathbb{F}$ com q elementos. Temos então que $\mathbb{F}^n$ é um $\mathbb{F}$-espaço vetorial de dimensão n.

Definição 2.19. *Um código $\mathcal{C} \in \mathbb{F}^n$ será um código linear se for um subespaço vetorial de $\mathbb{F}^n$.*

Definição 2.20. *Dado $x \in \mathbb{F}^n$ define-se o peso de x como o número inteiro $\omega(x) := |\{i|x_i \neq 0\}|$. Em outras palavras, $\omega(x) = d(x,0)$.*

Definição 2.21. *O peso de um código linear $\mathcal{C}$ é o inteiro $\omega(\mathcal{C}) := min\{\omega(x)|x \in \mathcal{C}/\{0\}\}$.*

Proposição 2.22. *Seja $\mathcal{C} \subset \mathbb{F}^n$ um código linear com distancia mínima d. Temos que:*

(i) $\forall x, y \in \mathbb{F}^n$, $d(x,y) = \omega(x-y)$.

(ii) $d = \omega(\mathcal{C})$.

Demonstração. O item (i) é consequência imediata das definições de métrica de Hamming e de peso de um código. Para o item (ii)temos que se $x \neq y$ então $z = x - y \in \mathcal{C}/\{0\}$ e $d(x,y) = \omega(z)$. □

Em álgebra linear, conhecem-se essencialmente duas maneiras de descrever subespaços vetoriais $\mathcal{C}$ de $\mathbb{F}^n$. A primeira delas é como imagem de uma transformação linear. Obtém-se essa representação da seguinte forma.

Escolhemos uma base $\{\mathbf{v}_1, \mathbf{v}_2, \ldots, \mathbf{v}_k\}$ de $\mathcal{C}$ e consideremos a aplicação linear.

$$\begin{array}{rcl} T : \mathbb{F}^k & \to & \mathbb{F}^n \\ \mathbf{x} = (x_1, \ldots, x_k) & \mapsto & x_1\mathbf{v}_1 + x_2\mathbf{v}_2 + \ldots + x_k\mathbf{v}_k \end{array}$$

Temos que T é uma transformação linear injetiva tal que a imagem de T é $\mathcal{C}$, Portanto, dar um código $\mathcal{C} \subset \mathbb{F}^n$ é equivalente a dar uma transformação linear injetiva $T: \mathbb{F}^k \to \mathbb{F}^n$ e definir $\mathcal{C} = Im(T)$. Nessa representação torna-se fácil gerar todos os elementos de $\mathcal{C}$. Entretanto é difícil decidir se um elemento $\mathbf{v} \in \mathbb{F}^n$ pertence ou não a $\mathcal{C}$, pois, para tal é necessário resolver um sistema de n equações nas k incógnitas $x_1, \ldots, x_k$ abaixo:

$$x_1\mathbf{v}_1 + x_2\mathbf{v}_2 + \ldots + x_k\mathbf{v}_k = \mathbf{v}$$

O que tem um custo computacional muito alto.

A segunda maneira de descrever um código linear é através do núcleo de uma transformação linear. Sendo assim, considere $\mathcal{C}' \subset \mathbb{F}^n$ o complemento de $\mathcal{C}$, isto é, $\mathcal{C} \oplus \mathcal{C}' = \mathbb{F}^n$ e considere a aplicação linear

$$\begin{array}{rcl} H : \mathcal{C} \oplus \mathcal{C}' & \longrightarrow & \mathbb{F}^{n-k} \\ \mathbf{u} \oplus \mathbf{v} & \longmapsto & \mathbf{v} \end{array}$$

cujo núcleo é precisamente $\mathcal{C}$. Computacionalmente é muito mais simples decidir se um vetor $v \in \mathbb{F}^n$ pertence ou não a $\mathcal{C}$ basta verificarmos se $H(\mathbf{v}) = 0$.

Definição 2.23. *Diremos que uma função $F : \mathbb{F}^n \longrightarrow \mathbb{F}^n$ é uma isometria de $\mathbb{F}^n$ se preserva distância de Hamming, i. é, $d(F(\mathbf{x}), F(\mathbf{y})) = d(\mathbf{x}, \mathbf{y})$.*

Proposição 2.24. *Toda isometria de $\mathbb{F}^n$ é uma bijeção de $\mathbb{F}^n$.*

Demonstração. Como $\mathbb{F}^n$ é finito basta mostrarmos que se F é uma isometria F é injetivo. De fato, se $F(x) = F(y)$ então $d(x, y) = d(F(x), F(y)) = 0$ dessa forma $x = y$ e F é injetiva. □

Proposição 2.25. *1. A função identidade de $\mathbb{F}^n$ é uma isometria.*

2. Se F é uma isometria de $\mathbb{F}^n$ então F^{-1} é uma isometria.

3. Se F e G são isometria de $\mathbb{F}^n$ então $F \circ G$ é uma isometria.

Demonstração. 1. $d(x, y) = d(I(x), I(y))$, onde I é a função identidade.

2. Pela Proposição 2.24 existe F^{-1} como F é uma isometria segue que

$$d(F^{-1}(x), F^{-1}(y)) = d(F(F^{-1}(x)), F(F^{-1}(y))) = d(x, y).$$

3. Como F e G são isometrias temos que

$$d(F(G(x)), F(G(y))) = d(G(x), G(y)) = d(x, y)$$

□

Definição 2.26. *Dois códigos lineares $\mathcal{C}$ e $\mathcal{C}'$ são linearmente equivalentes se existir uma isometria linear $T : \mathbb{F}^n \longrightarrow \mathbb{F}^n$ tal que $T(\mathcal{C}) = \mathcal{C}'$.*

Dado $\mathcal{C} \subset \mathbb{F}^n$ um código linear. Chamaremos de parâmetros do código linear $\mathcal{C}$ à terna de inteiros $[n, k, d]$, onde k é a dimensão de $\mathcal{C}$ sobre $\mathbb{F}$ e d representa a distância mínima de $\mathcal{C}$.

Seja $\mathcal{B} = \{\mathbf{v}_1, \ldots, \mathbf{v}_k\}$ uma base ordenada de $\mathcal{C}$ e considere a matriz G cujas as linhas são os vetores $\mathbf{v}_i = (v_{i1}, \ldots, v_{in})$, $i = 1, \ldots, k$ isto é

$$G = \begin{pmatrix} \mathbf{v}_1 \\ \vdots \\ \mathbf{v}_k \end{pmatrix} = \begin{pmatrix} v_{11} & v_{12} & \ldots & v_{1n} \\ \vdots & \vdots & & \vdots \\ v_{k1} & v_{k2} & \ldots & v_{kn} \end{pmatrix}$$

A matriz G é chamada de matriz geradora de $\mathcal{C}$ associada a base $\mathcal{B}$.

Considere a transformação linear definida por

$$\begin{aligned} T : \mathbb{F}^k &\longrightarrow \mathbb{F}^n \\ \mathbf{x} &\longmapsto \mathbf{x}G \end{aligned}$$

Se $x = (x_1, \ldots, x_k)$ temos que $T(\mathbf{x}) = xG = x_1\mathbf{v}_1 + \ldots + x_k\mathbf{v}_k$, logo $T(\mathbb{F}^k) = \mathcal{C}$. Podemos então considerar $\mathbb{F}^k$ o código fonte, $\mathcal{C}$ o código canal e a transformação T uma codificação.

Note que a matriz G não é univocamente determinada por $\mathcal{C}$ pois ela depende da escolha da base. Lembrando que uma base de um espaço vetorial pode ser obtida de uma outra qualquer através de sequencias de operações do tipo:

- *permutação de dois elemento da base;*
- *multiplicação de elemento da base por um escalar não nulo; e*
- *substituição de um elemento da base por ele mesmo somado com um múltiplo escalar de outro elemento da base.*

*Para mais informações ver referência [***Elon** *] Segue então que duas matrizes de um mesmo código $\mathcal{C}$ podem se obtida uma da outra por uma sequências de operações do tipo:*

(L1) Permutação de duas linhas.

(L2) Multiplicação de uma linha por um escalar não nulo.

(L3) Adição de um múltiplo escalar de uma linha a outra.

Inversamente, podemos construir códigos a partir de matrizes geradoras G. Para tanto basta tomar uma matriz $k \times n$ cujas linhas são linearmente independentes e definir um código como sendo imagem da transformação linear

$$\begin{aligned} T : \mathbb{F}^k &\longrightarrow \mathbb{F}^n \\ x &\longmapsto xG. \end{aligned}$$

Definição 2.27. *Diremos que uma matriz geradora G está na forma padrão se tivermos,*

$$G = (Id_k|A),$$

onde Id_k é a matriz identidade $k \times k$ e A uma matriz $k \times (n-k)$.

Efetuando sequencias de operações sobre a matriz geradora G de um código linear $\mathcal{C}$ do tipo:

(C1) permutação de duas colunas,

(C2) multiplicação de uma coluna por um escalar não nulo,

obtemos uma matriz G' de um código $\mathcal{C}'$ equivalente a $\mathcal{C}$.

Teorema 2.28. *Dado um código $\mathcal{C}$, existe um código equivalente $\mathcal{C}'$ com matriz geradora na forma padrão.*

Demonstração. Seja G uma matriz geradora de $\mathcal{C}$. Mostraremos que com uma sequência de operações do tipo (L1), (L2), (L3) e (C1) podemos colocar G na forma padrão.

Suponhamos

$$G = \begin{pmatrix} g_{11} & g_{12} & \dots & g_{1n} \\ \vdots & \vdots & & \vdots \\ gk1 & g_{k2} & \dots & g_{kn} \end{pmatrix}.$$

Como a primeira linha de G é não nula, por meio dde (C1), podemos supor $q_{11} \neq 0$. Agora multiplicamos a primeira linha por g_{11}^{-1}, podemos por 1 no lugar de g_{11}.

Somando à segunda, terceira, etc. linhas a primeira linha multiplicada respectivamente por $-g_{21}, -g_{31}$, etc. obtemos uma matriz

$$\begin{pmatrix} 1 & b_{12} & \dots & b_{1n} \\ 0 & b_{22} & \dots & b_{2n} \\ \vdots & \vdots & & \vdots \\ 0 & b_{k2} & \dots & b_{kn} \end{pmatrix}.$$

Agora na segunda linha da matriz certamente tem um elemento não nulo que por meio da operação (C1) pode ser colocado na segunda linha e segunda coluna. Multiplicando a segunda linha pelo inverso desse elemento e usando operações (L3) obtemos a matriz

$$\begin{pmatrix} 1 & 0 & c_{13} & \dots & c_{1n} \\ 0 & 1 & c_{23} & \dots & c_{2n} \\ \vdots & \vdots & \vdots & & \vdots \\ 0 & 0 & c_{k3} & \dots & c_{kn} \end{pmatrix}.$$

E assim sucessivamente até encontrarmos uma matriz na forma padrão $G' = (Id_k|A)$. □

2.4.1 Códigos Balanceados

Vamos agora direcionar o nosso foco para alfabetos binários, $\mathcal{A} = \{0, 1\}$. Uma palavra binária, forma apenas por 0 e 1, de comprimento m é dita balanceada se contém exatamente $m/2$ zeros e $m/2$ uns.

Definição 2.29. *Uma palavra binária é dita balanceada se contém tantos zeros quanto uns, isto é, se x é uma palavra balanceada então $\omega(x) = m/2$.*

Um código balanceado com n o número de entradas que nos dão a informação e p o número de redundâncias é um conjunto de palavras balanceadas de comprimento $m = p + n$. Códigos balanceados tem a propriedade que nenhuma palavra está 'contida' em outra, i. é, as posições dos 1 de uma palavra nunca será um subconjunto das posições de 1 de uma outra palavra.

2.5 Polinômios de Permutação

Os polinômios de permutação, daqui para frente referidos apenas como PP, podem historicamente serem traçados até Gauss em seu estudo sobre sistema completo de resíduos. Entretanto, os primeiro estudo sistemático de Polinômios de Permutação foram feitos por Hermite (1863) para corpos primos e em seguida generalizado por Dickson (1897) para corpos finitos. O interesse atual em Polinômios de Permutação é sua relação com a criptografia. Apesar da atenção dada aos polinômios de permutação identifica-los não é tarefa fácil e ainda não existe um algoritmo eficiente para a construção dos mesmos.

Lema 2.30. *Para qualquer $\varphi : \mathbb{F}_q \longrightarrow \mathbb{F}_q$ existe um único polinômio $f \in \mathbb{F}_q[x]$ de grau máximo $q-1$ que satisfaz $\varphi(c) = f(c), \forall c \in \mathbb{F}_q$.*

Demonstração. (Existência) Considere o polinômio dado por $f(x) = \sum_{c \in \mathbb{F}_q} \varphi(c)[1-(x-c)^{q-1}]$ temos que:

$$f(x) = \varphi(c)[1-(x-c)^{q-1}] + \varphi(c_2)[1-(x-c_2)^{q-1}] + ... + \varphi(c_{q-1})[1-(x-c_{q-1})^{q-1}]$$

Fazendo $x = c$ temos que $f(c) = \varphi(c)$. Isso completa a primeira parte.

(Unicidade) Suponha $f, g \in \mathbb{F}_q[x]$ com graus iguais a $q-1$ e $f(c) = g(c) = \varphi(c) \forall c \in \mathbb{F}_q$ e $f \neq g$. Assim, $gr(f-g) \leq q-1$. Como $f \neq g$, segue que $f - q \neq 0$, dessa forma $f-g$ tem no máximo $q-1$ raízes, contradição pois $(f-g)(c) = 0 \forall c \in \mathbb{F}_q$. □

Lema 2.31. *Para qualquer $f, g \in \mathbb{F}_q[x]$, $f(c) = g(c), \forall c \in \mathbb{F}_q$ se, e somente se, $f(x) \equiv g(x) \pmod{x^q - x}$.*

Demonstração. Pelo algoritmo da divisão temos que

$$f(x) - g(x) = h(x)(x^q - x) + r(x)$$

, com $h, r \in \mathbb{F}_q[x]$ e $\partial(r) < q$. Suponha que $f(c) = g(c), \forall c \in \mathbb{F}_q$, assim como $c^q = c$ temos que $r(c) = 0 \ \forall c \in \mathbb{F}_q$ portando $r(x) = 0$ e $f(x) \equiv g(x) \pmod{x^q - x}$. Suponha agora que $f(x) \equiv g(x) \pmod{x^q - x})$ assim $r(x) = 0$ e $f(c) - g(c) = 0 \ \forall c \in \mathbb{F}_q$. □

Lema 2.32. *O polinômio $f \in \mathbb{F}_q[x]$ é um PP se,e somente se, as seguintes condições são equivalentes:*

1. *a função $f : c \mapsto f(c)$ é sobrejetiva;*
2. *a função $f : c \mapsto f(c)$ é injetiva;*
3. *$f(x) = a$ tem uma solução em $\mathbb{F}_q$ para todo $a \in \mathbb{F}_q$*
4. *$f(x) = a$ tem uma única solução para cada $a \in \mathbb{F}_q$*

Lema 2.33. *Sejam $a_0, a_1, ..., a_{q-1}$ elementos de $\mathbb{F}_q$. São equivalentes as seguintes afirmações:*

(i) $a_0, a_1, ..., a_{q-1}$ *são distintos;*

(ii) $\sum_{i=0}^{q-1} a_1^t = \begin{cases} 0, & t = 0,\ 1,\ ...,\ q\text{-}2; \\ -1, & t = q\text{-}1. \end{cases}$.

Demonstração. Para $i \in \{0, 1, ..., q-1\}$ considere o polinômio

$$g_i(x) = 1 - \sum_{j=0}^{q-1} a_i^{q-1-j} x^j.$$

Temos que $g_i(a_i) = 1$ e $g_i(b) = 0$ com $b \in \mathbb{F}_q; b \neq a_i$. Dessa forma o polinômio

$$g(x) = \sum_{i=0}^{q-1} g_i(x) = -\sum_{j=0}^{q-1} (\sum_{i=0}^{q-1} a_i^{q-1-j}) x^j$$

leva cada elemento de $\mathbb{F}_q$ em 1 se, e somente se, $\{a_0, a_1, \ldots, a_n\} = \mathbb{F}_q$ o que é equivalente a (i). Como $\partial(g) < q$, pelo Lema 2.31 o polinômio g leva cada elemento de $\mathbb{F}_q$ em 1 se, e somente, $g(x) = 1$ o que é equivalente a (ii). □

A seguir veremos estudaremos critérios para obtermos polinômios de permutação.

Teorema 2.34 (Critério de Hermites)**.** *Seja $\mathbb{F}_q$ um corpo de característica p. Então $f \in \mathbb{F}_q$ é um polinômio de permutação de $\mathbb{F}_q$ se somente se valem as seguintes condições:*

(i) f tem uma única raiz em $\mathbb{F}_q$;

(ii) para todo $t \in \{1, ..., q-2\}$ e $t \not\equiv 0 \pmod p$ temos que $g(x) \equiv f(x)^t \pmod{x^q - x}$ tem grau menor ou igual a $q-2$

Demonstração. Para cada $1 \leq t \leq$ temos que $f(x)^t \pmod{x^q - x} = \sum_{i=0}^{q-1} b_i^{(t)} x^i$. Pelo Lema 2.30 temos que $b_{q-1}^{(t)} = \sum_{c \in \mathbb{F}_q} f(c)^t$.

$\Rightarrow$ Suponha que f é PP. (i) vale de imediato. Temos ainda que $\mathbb{F}_q = \{f(c) | c \in \mathbb{F}_q\}$ assim pelo Lema 2.33 2.4 $b_{q-1}^{(t)} = 0$ se $t \in \{1, 2, ..., q-2\}$ e $b_{q-1}^{(t)} = -1$ se $t = q-1$, logo (ii) e satisfeita.

$\Leftarrow$ Suponha que (i) e (ii) valem, por (i) temos que $\sum_{c \in \mathbb{F}_q} f(c)^{q-1} = -1$ e por (ii) $\sum_{c \in \mathbb{F}_q} f(c)^t = 0$ com $1 \leq t \leq q-2,\ t \not\equiv 0 \pmod p$. Suponha que $t \equiv 0 \pmod p \Rightarrow t = t' p^j$, com $1 \leq t \leq q-2$. Segue que:

$$\sum f(c)^t = \sum f(c)^{t' p^j} = (\sum f(c) t')^{p^j} = 0.$$

Assim pelo Lema 2.33 $\{f(c) | c \in \mathbb{F}_q\} = \mathbb{F}_q$ e f é um polinômio de permutação. □

Corolário 2.35. *Se $d > 1$ e $d | q-1$, então não existe nenhum PP em $\mathbb{F}_q$ de grau d.*

Teorema 2.36. *$f \in \mathbb{F}_q[x]$ é um PP se somente se $\sum_{c \in \mathbb{F}_q} \chi(f(c)) = 0$, $\forall \chi$ caráter aditivo não trival de $\mathbb{F}_q$.*

Demonstração. Suponha primeiro que f é PP, então $\sum_{c\in\mathbb{F}_q}\chi(f(c)) = \sum_{c\in\mathbb{F}_q}\chi(c) = 0$, pelas propriedades de caráter.

Suponha agora que $\chi_\circ$ o caráter trivial e $\sum_{c\in\mathbb{F}_q}\chi(f(c)) = 0$, $\forall\chi \neq \chi_\circ$. Vamos mostrar que existe um único $x \in \mathbb{F}_q$ tal que $f(x) = a$ para um $a \in \mathbb{F}_q$ fixado. Para tanto utilizar a teoria de caráter. O número de $x \in \mathbb{F}_q$ que satisfaz $f(x) = a$ é dado por:

$$N(a) = \frac{1}{q}\sum_{c\in\mathbb{F}_q}\sum_{\chi}\chi(f(c))\overline{\chi(a)}.$$

Segue que:

$$\begin{aligned} N(a) &= \frac{1}{q}\sum_{c\in\mathbb{F}_q}(\chi_\circ(f(c))\overline{\chi_\circ(a)} + \sum_{\chi\neq\chi_\circ}\chi(f(c))\overline{\chi(a)}) \\ &= \frac{1}{q}\sum_{c\in\mathbb{F}_q}\chi_\circ(f(c))\overline{\chi_\circ(a)} + \frac{1}{q}\sum_{\chi\neq\chi_\circ}\overline{\chi(a)}\sum_{c\in\mathbb{F}_q}\chi(f(c)) \\ &= \frac{q}{q} \\ &= 1. \end{aligned}$$

Portanto, f é PP. □

Teorema 2.37. *(i) Todo polinômio linear em $\mathbb{F}_q$ é um PP*

(ii) $x^n \in \mathbb{F}_q[x]$ é PP se somente se $mdc(n, q-1) = 1$.

Teorema 2.38. *Seja $\mathbb{F}_q$ com característica p. Então o p-polinômio $L(x) = \sum_{i=0}^{m} a_i x^{p^i} \in \mathbb{F}_q[x]$ é um PP se somente se $L(x)$ tem apenas 0 como raiz dm $\mathbb{F}_q$.*

Demonstração. Temos que $L : \mathbb{F}_q \longrightarrow \mathbb{F}_q$ é linear. Assim se 0 é a unica raiz, L é injetiva, portando bijetiva logo é um PP □

O teorema a seguir nos dá uma caracterização se um tipo específico de polinômio é uma permutação.

Teorema 2.39 (Wan-Lidl)**.** *Sejam m e r inteiros positivos tais que m divide $q-1$. Seja $\alpha \in \mathbb{F}_q$ um elemento primitivo e $P \in \mathbb{F}_q[x]$. Então $Q = x^r P(x^{\frac{q-1}{m}})$ é um PP de $\mathbb{F}_q$ se somente se satisfaz as seguintes condições:*

1. $mdc(r, \frac{q-1}{m}) = 1$
2. $\forall i;\ 0 \leq i < m,\ P(\alpha^{i\frac{q-1}{m}}) \neq 0$
3. $\forall i,\ j;\ 0 \leq i < j < m,\ Q(\alpha^i)^{\frac{q-1}{m}} \neq Q(\alpha^j)^{\frac{q-1}{m}}$.

Demonstração. Definiremos $\psi : \mathbb{F}_q^* \longrightarrow \mathbb{Z}/d\mathbb{Z}$ dado por:

$$\psi(x) \equiv \text{Ind}_\alpha(x) \pmod{m}.$$

Onde $\text{Ind}_\alpha(x) \equiv b \pmod{q-1}$ tal que $\alpha^b = x$. Definimos ainda $\omega = \alpha^{\frac{q-1}{m}}$

ψ é um homomorfismo pois $x, y \in \mathbb{F}_q^*$ temos que:

$$\begin{aligned}
\psi(xy) &\equiv \text{Ind}_\alpha(xy) \pmod{m} \\
&\equiv (\text{Ind}_\alpha(x) + \text{Ind}_\alpha(y)) \pmod{m} \\
&\equiv \text{Ind}_\alpha(x) \pmod{m} + \text{Ind}_\alpha(y) \pmod{m} \\
&= \psi(x) + \psi(y).
\end{aligned}$$

Podemos observar também que $x^{\frac{q-1}{m}} = \alpha^{\text{Ind}_\alpha(x)\frac{q-1}{m}} = \omega^{\text{Ind}_\alpha(x)}$. Como $\omega^m = 1$, concluímos que

$$x^{\frac{q-1}{m}} = \omega^{\psi(x)}.$$

Afirmação: $\psi\left(\frac{P(\omega^i)}{P(\omega^j)}\right) \not\equiv r(j-i) \pmod{m} \Rightarrow Q(\alpha^i)^{\frac{q-1}{m}} \neq Q(\alpha^j)^{\frac{q-1}{m}}$.

Mostraremos a afirmação pela contra-positiva. Suponhamos então que $Q(\alpha^i)^{\frac{q-1}{m}} = Q(\alpha^j)^{\frac{q-1}{m}}$. Note que

$$Q(\alpha^i)^{\frac{q-1}{m}} = (\alpha^{ir} P(\alpha^{i\frac{q-1}{m}}))^{\frac{q-1}{m}} = \omega^{ir} P(\omega^i)^{\frac{q-1}{m}}$$

. Assim temos que:

$$\begin{aligned}
\omega^{ir} P(\omega^i)^{\frac{q-1}{m}} &= \omega^{jr} P(\omega^j)^{\frac{q-1}{m}} \\
\left(\frac{P(\omega^i)}{P(\omega^j)}\right)^{\frac{q-1}{m}} &= \omega^{r(j-i)} \\
\omega^{\psi\left(\frac{P(\omega^i)}{P(\omega^j)}\right)} &= \omega^{r(j-i)} \\
\psi\left(\frac{P(\omega^i)}{P(\omega^j)}\right) &\equiv r(j-i) \pmod{m}
\end{aligned}$$

Afirmação demonstrada seguiremos para a demonstração do teorema.

Suponha que Q é um PP. Assim a equação $Q(x) = 0$ possui uma única solução $x = 0$ dessa forma o item *2* é satisfeito. Com isso satisfeito temos que Q é um PP se somente se $\text{Ind}_\alpha(Q(\alpha^k)) \pmod{q-1}$ com $0 \leq K \leq q-2$ são distintos. Escrevemos então:

$$k = i + mj, 0 \leq i \leq m-1,\ 0 \leq j \leq \frac{q-1}{m}$$

A forma especial de Q implica:

$$\begin{aligned}
\text{Ind}_\alpha(Q(\alpha^k)) &= r(i+mj) + \text{Ind}_\alpha(P(\omega^i)) \\
&= m(rj) + mi + \text{Ind}_\alpha(P(\omega^i))
\end{aligned}$$

Da última equação segue que $\text{Ind}_\alpha(Q(\alpha^k))$ com $k \in \{0, 1, ..., q-1\}$ é um sistema completo de resíduos módulo $q-1$ se somente se $\text{mdc}(r, \frac{q-1}{m}) = 1$ e $ri + \text{Ind}_\alpha(Q(\alpha^i))$ for um sistema de completo de resíduos módulo m, mas isso é equivalente a dizer que se $0 \leq i < j \leq m$ então $\psi\left(\frac{P(\omega^i)}{P(\omega^j)}\right) \not\equiv r(j-i) \pmod{m}$. Assim *1* e *3* são satisfeitas. □

Vamos agora definir um tipo particular de polinômios, os polinômios de Dickson. Para tanto precisamos ter em mãos algumas definições e propriedades. Sejam $x_1 e x_2$ indeterminadas e $k \in \mathbb{N}$, temos que em qualquer anel comutativo vale:

$$x_1^k + x_2^k = \sum_{j=1}^{\llcorner \frac{k}{2} \lrcorner} \frac{k}{k-j} \binom{k-j}{j} (-x_1 x_2)^j (x_1 + x_2)^{k-2j}.$$

Para a elemento de um anel comutativo definimos o Polinômio de Dickson $g_k(x, a)$ por:

$$g_k(x, a) = \sum_{j=0}^{\lfloor \frac{k}{2} \rfloor} \frac{k}{k-j} \binom{k-j}{j} (-a)^j x^{k-2j}$$

Considerando $g_k(x, a)$ sobre um corpo $\mathbb{F}$, valem as seguintes propriedades:

- $g_k(y + \frac{a}{y}, a) = y^k + \frac{a^k}{y^k}$
- $g_k(x, ab^2) = b^k g_h(b^{-1}x, a)$.

Com isso podemos mostrar o teorema:

Teorema 2.40. *O polinômio de Dickson $g_k(x, a)$ com $a \in \mathbb{F}_q^*$ é um polinômio de permutação se somente se $mdc(k, q^2 - 1) = 1$.*

Demonstração. ($\Leftarrow$) Suponha que $\text{mdc}(k, q^2 - 1) = 1$. Sejam $b, c \in \mathbb{F}_q$ tais que $g_k(b, a) = g_k(c, a)$. Existem β e $\gamma \in \mathbb{F}_q^*$ tais que $b = \beta + a\beta^{-1}$ e $c = \gamma + a\gamma - 1$. Pela propriedade anterior temos que:

$$\beta^k + a^k \beta^{-k} = \gamma^k + a^k \gamma^{-k} \Leftrightarrow (\beta^k + \gamma^k)(\beta^k \gamma^k - a^k) = 0 \Rightarrow \beta^k = \gamma^k \text{ ou } \beta^k = (a\gamma^{-1})^k$$

Como x^k é um polinômio de permutação, pois mdc(k,q-1)=1 temos que $\beta = \gamma$ ou $\beta = a\gamma^{-1}$ em qualquer um dos casos $b = c$ e $g_k(x, a)$ é um PP.

($\Rightarrow$) Seja $\text{mdc}(k, q^2 - 1) = d > 1$. Suponhamos primeiro que d é par. Dessa forma q é ímpar e k é par, então $g_k(x, a)$ contém apenas potências pares de x e assim $g_k(c, a) = g_k(-c, a)$. Mas $c \neq -c$ contradizendo a hipótese de $g_k(x, a)$ ser um PP.

Suponhamos agora que d é ímpar. Então existe um primo impar r que divide d. Dessa forma d divide k, e $q - 1$ ou $q + 1$ é divisível por r, temos então dois casos.

No primeiro caso a equação $x^r = 1$ tem r soluções em $\mathbb{F}_q$, daí existe $b \in \mathbb{F}_q$, $b \neq 1$, a com $b^r = 1$. Como $b^k = 1$ e pela definição de Polinômio de Dickson

$$g_k(b + ab^{-1}, a) = 1 + a^k = g(1 + a, a).$$

Como $b + ab^{-1} = 1 + a$ implicaria $b = 1$ ou $b = a$, temos que $b + ab^{-1} \neq 1 + a$ e assim $g_k(x, a)$ não é um PP.

No segundo caso, seja $\gamma \in \mathbb{F}_{q^2}$ solução de $x^{q+1} = a$. Como $x^r = 1$ tem r soluções em $\mathbb{F}_{q^2}$, então existe $\beta \in \mathbb{F}_{q^2}, \beta \neq 1, a\gamma^{-2}$ com $\beta^r = 1$. Dessa forma $\beta^{q+1} = 1$ e $\beta^k = 1$, segue que:

$$g_k(\gamma + a\gamma^{-1}, a) = g_k(\beta\gamma + a(\beta\gamma)^{-1}, a)$$

Temos ainda que, $\gamma a \gamma^{-1} = \gamma + \gamma^q \in \mathbb{F}_q$ e $\beta\gamma + a(\beta\gamma)^{-1} = \beta\gamma + (\beta\gamma)^q \in \mathbb{F}_q$, e ainda $\beta\gamma + a(\beta\gamma)^{-1} \neq \gamma + a\gamma^{-1}$. Então $g_k(x, a)$ não é um PP. □

Corolário 2.41. *Se $a \in \mathbb{F}_q^*$ e $mdc(k, q^2-1) = 1$, então*

$$\sum_{c \in \mathbb{F}_q} \chi(g_k(c, a)) = 0$$

para todo carácter não trivial de $\mathbb{F}_q$.

Demonstração. Como $g_k(x, a)$ é um PP pelo Teorema 2.40 nós temos:

$$\sum_{c \in \mathbb{F}_q} \chi(g_k(c, a)) = \sum_{c \in \mathbb{F}_q} \chi(c)$$

pelo Teorema 2.9 obtemos o resultado. □

Falaremos agora dos binômios de permutação. O nosso primeiro resultado é um corolário do Teorema 2.39.

Corolário 2.42. *Sejam p um primo e m e ℓ naturais. Seja k a ordem de p em $\mathbb{Z}/m\mathbb{Z}$. Tome $q = p^{k\ell m}$ e r relativamente primo com $q-1$. Se $a \in \mathbb{F}_{p^{k\ell}}$, o binômios $X^r(X^{\frac{q-1}{m}} + a)$ é um PP se somente se $(-a)^m \neq 1$.*

Agora um lema técnico.

Lema 2.43. *Sejam k, ℓ e p inteiros positivos. Seja ainda m divisor de $p^k - 1$ e r relativamente primo com $p^{k\ell m} - 1$, então $mdc(p^{k\ell m} - 1, \frac{p^{k\ell m - 1}}{m} + r) = 1$.*

Demonstração. Seja $q = p^{k\ell m}$, notamos que:

$$\begin{aligned} \frac{q-1}{m} &= \frac{p^k - 1}{m} \sum_{i=0}^{\ell m - 1} [(p^k - 1) + 1]^i \\ &\equiv \frac{p^k - 1}{m} \sum_{i=0}^{\ell m - 1} 1 \pmod{m} \\ &\equiv 0 \pmod{m} \end{aligned}$$

Assim se m divide $p^k - 1$ também divide $\frac{q-1}{m}$. $q-1$ e $\frac{q-1}{m}$ têm os mesmos divisores primos, seja d um desses divisores. Dessa forma d divide $\frac{q-1}{m}$, mas não divide r já que este é relativamente primo com $q-1$. Dessa forma o lema está provado. □

Com o Lema 2.43 temos que os monômios $X^{r+\frac{q-1}{m}}$ e aX^r são permutações desde que seus expoentes sejam relativamente primos com $q-1$.

Queremos agora encontrar permutações completas, isto é, permutações f tais que $f(x) + x$ também é uma permutação. Na verdade queremos encontrar permutações polinomiais completas de um modelo específico.

Teorema 2.44. *Sejam p primo, m e ℓ naturais e k a ordem de p em $\mathbb{Z}/m\mathbb{Z}$. Tome $q = p^{k\ell m}$ e r um inteiro positivo relativamente primo com $q-1$. Assumindo $a \in \mathbb{F}_{p^{k\ell}}$ tal que $(-a)^m \neq 1$. Os polinômios $P = X(X^{\frac{q-1}{m}} + a)$ e $Q = aX^{\frac{q-1}{m}+1}$ são permutações completas.*

Demonstração. Pelo Corolário 2.42, P é uma permutação. Como $a \in \mathbb{F}_{p^{k\ell}}$ tal que $(-a)^m \neq 1$ então $a+1$ também satisfaz essa condição, assim novamente pelo Corolário 2.42 $P+X$ é uma permutação. Q é uma permutação pelo Lema 2.43. E finalmente, $Q+X$ é uma permutação pelo Corolário 2.42. □

Podemos obter uma família de polinômios de permutação da forma $X^r(X^{\frac{q-1}{m}}+a)$ para valores específicos de a. A pergunta natural é quantos polinômios da forma $X^r(X^{\frac{q-1}{m}}+a)$ são permutações.

Definição 2.45. $\mathcal{B}(q,m,r) = \{a \in \mathbb{F}_q^* \mid X^r(X^{\frac{q-1}{m}}+a)$ *é uma permutação*$\}$ *e* $N(q,m,r) = \#\mathcal{B}(q,m,r)$.

Daremos agora um limitante superior para $N(q,m,r)$

Teorema 2.46. *Sejam q potência de um primo p, r um inteiro positivo relativamente primo com $q-1$ e m um divisor de $q-1$, então:*

$$\left| N(q,m,r) - \frac{m!}{m^m} q \right| \leq m! \left(\frac{1}{m^m} + (m-2) \right) \sqrt{q} + (m+1)! \,.$$

Demonstração. Considere $\mathcal{G}$ o subgrupo cíclico de $\mathbb{F}_q^*$ de ordem m e tome β gerador de $\mathcal{G}$. Seja ω um primitivo da m-ésima raiz da unidade em $\mathbb{C}$.

Denotaremos por ϕ a aplicação de $\mathcal{G}$ no conjunto das raízes m-ésimas da unidade em $\mathbb{C}$ $\phi(\beta^i) = \omega^i$ estendido com $\phi(0) = 0$.

Para $a \in \mathbb{F}_q$, o teorema 2.39 garante que $Q_a(x) = x^r(x^{\frac{q-1}{m}}+a)$ é uma permutação se,e somente se, as duas condições a seguir são satisfeitas:

$$\forall i, 0 \leq i < m, \beta^i + a \neq 0 \text{ o que é equivalente a } (-a)^m \neq 1 \tag{2.5.1}$$

$$\text{A função } \begin{cases} \{1,\ldots,m\} \longrightarrow \{1,\ldots,m\} \\ i \longmapsto \log_\beta(Q_a(\alpha^i)^{\frac{q-1}{m}}) \end{cases} \text{ é uma permutação.} \tag{2.5.2}$$

Para $f : \{1,\ldots,m\} \longrightarrow \{1,\ldots,m\}$ definimos

$$P_f(X_1,\ldots,X_m) = \prod_{i=0}^{m} \left(\sum_{j=0}^{m-1} [X_i \omega^{-f(i)}]^j \right). \tag{2.5.3}$$

Seja Ψ o caráter $x \mapsto \phi(x^{\frac{q-1}{m}})$. Para $x = (x_1,\ldots,x_m)$ uma m-upla de elementos em $\mathbb{F}_q^*$, usaremos a notação $\Psi(x) = (\Psi(x_1),\ldots,\Psi(x_m))$. Temos então:

$$P_f(\Psi(x)) = \begin{cases} m^m, & \text{se } f(i) = \log_\beta(x_i^{\frac{q-1}{m}}) \text{ para todo i;} \\ 0, & \text{caso contrário.} \end{cases} \tag{2.5.4}$$

Seja $\mathcal{S}$ o conjunto das permutações de $\{1, ldots, m\}$. Note que de acordo com 2.5.4

$$\frac{1}{m^m} \sum_{\sigma \in \mathcal{S}} P_\sigma(\Psi(Q_a(\alpha),\ldots,Q_a(\alpha^m))) = \begin{cases} 1, & \text{se 2.5.2 é satisfeita;} \\ 0, & \text{caso contrario.} \end{cases} \tag{2.5.5}$$

Dessa forma

$$N(q,m,r) = \frac{1}{m^m} \sum_{\substack{a\in\mathbb{F}_q^* \\ (-a)^m\neq 1}} \sum_{\sigma\in\mathcal{S}} P_\sigma(\Psi(Q_a(\alpha),\ldots,Q_a(\alpha^m))) \tag{2.5.6}$$

Queremos encontrar uma estimativa para essa soma.

Seja $\mathcal{M}(P)$ o conjunto dos monômios de P, para um monômio M definimos $ind(M)$ como o número de indeterminadas que aparecem em M. O carácter Ψ é multiplicativo. Assim:

$$M\circ\Psi(x_1,\ldots,x_m) = \Psi\circ M(x_1,\ldots,x_m).$$

Para qualquer $\sigma\in\mathcal{S}$ temos:

$$\begin{aligned}\left|\sum_{a\in\mathbb{F}_q} P_\sigma(\Psi(Q_a(\alpha),\ldots,Q_a(\alpha^m))) - q\right| &= \left|\sum_{a\in\mathbb{F}_q}\sum_{\substack{M\in\mathcal{M}(P)\\ ind(M)=k}} M(\Psi(Q_a(\alpha),\ldots,Q_a(\alpha^m)))\right| \\ &\leq \sum_{k=1}^{m}\sum_{\substack{M\in\mathcal{M}(P)\\ ind(M)=k}}\left|\sum_{a\in\mathbb{F}_q}\Psi(M(Q_a(\alpha),\ldots,Q_a(\alpha^m)))\right|.\end{aligned}$$

Se $M=\prod_{i\in I} X_i^{k_i}$ nós obtemos:

$$M(Q_a(\alpha),ldots,Q_a(\alpha^m)) = \prod_{i\in I}[\alpha^{ir}(\beta^i+a)]^{k_i}$$

o qual visto como um polinômio com indeterminada a tem exatamente $\#I = ind(M)$ raízes que são $\{-\beta^i | i\in I\}$. Elas tem multiplicidade k_i que é estritamente menor que m. Usando o Teorema 2.9 na soma de carácter nós obtemos:

$$\left|\sum_{a\in\mathbb{F}_q} P_\sigma(\Psi(Q_a(\alpha),\ldots,Q_a(\alpha^m))) - q\right| \leq \sum_{k=1}^{m}\sum_{\substack{M\in\mathcal{M}(p)\\ ind(M)=k}}(k-1)\sqrt{q}. \tag{2.5.7}$$

Temos ainda que cada indeterminada aparece apenas em um dos m termos do produto 2.5.3 que define P, temos que $\#\{M\in\mathcal{M}(P) | ind(M)=k\} = (m-1)^k\binom{m}{k}$ e então:

$$\left|\sum_{a\in\mathbb{F}_q} P_\sigma(\Psi(Q_a(\alpha),\ldots,Q_a(\alpha^m))) - q\right| \leq \left(\sum_{k=1}^{m}(m-1)^k\binom{m}{k}(k-1)\right)\sqrt{q}. \tag{2.5.8}$$

A clássica fórmula para coeficientes binomiais $k\binom{m}{k} = m\binom{m-1}{k-1}$ nos dá:

$$\begin{aligned}\sum_{k=1}^{m}(m-1)^k\binom{m}{k}(k-1) &= m\sum_{k=1}^{m}(m-1)^k\binom{m-1}{k-1} - \sum_{k=1}^{m}(m-1)^k\binom{m}{k} \\ &= m(m-1)m^{m-1} - (m^m-1) \\ &= 1+m^m(m-2).\end{aligned}$$

Somando a inequação 2.5.8 para $\sigma \in \mathcal{S}$ nós obtemos

$$\begin{aligned}
\left| N(q,m,r) - \frac{m!}{m^m} q \right| &= \frac{1}{m^m} \left| \sum_{\sigma \in \mathcal{S}} \left(\sum_{\substack{a \in \mathbb{F}_q^* \\ (-a)^m \neq 1}} P_\sigma(\Psi(Q_a(\alpha), \ldots, Q_a(\alpha^m))) - q \right) \right| \\
&\leq \frac{1}{m^m} \sum_{\sigma \in \mathcal{S}} \left(\left| \sum_{a \in \mathbb{F}_q} P_\sigma(\Psi(Q_a(\alpha), \ldots, Q_a(\alpha^m))) - q \right| \right. \\
&+ \left. \left| \sum_{\{a | (-a)^m = 1\} \cup \{0\}} P_\sigma(\Psi(Q_a(\alpha), \ldots, Q_a(\alpha^m))) \right| \right) \\
&\leq \frac{m!}{m^m}(1 + m^m(m-2))\sqrt{q} + \sum_{\sigma \in \mathcal{S}} \sum_{\{a | (-a)^m = 1\} \cup \{0\}} 1 \\
&\leq \frac{m!}{m^m}(1 + m^m(m-2))\sqrt{q} + m!\,(m+1)
\end{aligned}$$

e isso completa a prova. □

Corolário 2.47. *Sejam p, q, r e m como no teorema anterior. Assumindo que $q > (1+\frac{m+1}{m^{m+2}})^2 m^{2m+2}$. Então existe $a \in \mathbb{F}_q^*$ tal que $X^r(X^{\frac{q-1}{m}} + a)$ é uma permutação de $\mathbb{F}_q$.*

Demonstração. A existência desse a é equivalente a $N(q,m,r) > 0$. Pelo teorema 2.46 uma condição suficiente para isto é:

$$0 < \frac{1}{m^m} q - \left(\frac{1}{m^m} + (m-2) \right) \sqrt{q} - (m+1).$$

A maior raiz desse grau para o polinômio é:

$$\frac{m^{m+1}}{2} \left(\left(1 + \frac{1}{m^{m-1}} - \frac{2}{m} \right) + \sqrt{\left(1 + \frac{1}{m^{m-1}} - \frac{2}{m} \right)^2 + 4\frac{m+1}{m^{m+2}}} \right)$$

o qual é menor que

$$\frac{m^{m+1}}{2} \left(1 + \sqrt{1 + 4\frac{m+1}{m^{m+2}}} \right).$$

Usando o fato que $\sqrt{1+x} < 1 + \frac{x}{2}$ obtemos

$$m^{m+1} \left(1 + \frac{m+1}{m^{m+2}} \right)$$

um limitante inferior para $\sqrt{q}$. Este limitante dá o nosso resultado. □

Depois de todos esses resultados estamos prontos para discutir a Conjectura de Helleseth.

Capítulo 3

Conjectura de Helleseth

A partir de agora estaremos trabalhando no corpo $\mathbb{F}_{2^n}$ com n inteiro positivo. Para qualquer função binária $f : \mathbb{F}_{2^n} \longrightarrow \mathbb{F}_2$ podemos associar sua imagem a palavra $(f(x))_{x\in\mathbb{F}_{2^n}}$. Isso significa que quem ordenaremos os elementos de $\mathbb{F}_{2^n}$ fixando um elemento primitivo α.

Definição 3.1. *Seja f uma função binária. Usaremos a notação $(f(x))_{x\in\mathbb{F}_{2^n}}$ para a palavra binária $f(0)f(\alpha)\cdots f(\alpha^{2^n-1})$.*

Nosso interesse em palavras binárias é uma questão criptográfica pois palavras balanceadas, ver Definição 2.29 revelam menos do código fonte do que outros tipos de palavras.

A seguir consideraremos o corpo $\mathbb{F}_{2^n}$ como um espaço vetorial de dimensão n sobre $\mathbb{F}_2$. Um elemento $a \in \mathbb{F}_{2^n}$ pode ser visto como uma n-upla de elementos $a_i \in \mathbb{F}_2$, e uma função $F : \mathbb{F}_{2^n} \longrightarrow \mathbb{F}_{2^n}$ como uma n-upla de funções binárias f_i, i. é, $F = (f_1, \ldots, f_n)$ com $f_i : \mathbb{F}_{2^n} \longrightarrow \mathbb{F}_2$.

*A próxima proposição dá uma caraterização de funções de permutação baseada no conceito de palavra balanceada, sua demonstração pode ser vista na referência [**Lidl**] no item 7.17.*

Proposição 3.2. *Utilizando a notação acima, F é uma permutação de $\mathbb{F}_{2^n}$ se somente se para todo $a \in \mathbb{F}_{2^n}^*$ a palavra*

$$(a_1 f_1(x) + \cdots + a_n f_n(x))_{x\in\mathbb{F}_{2^n}}$$

é uma palavra balanceada.

3.1 Conjectura de Helleseth

Conjectura 3.3 (Conjectura de Helleseth)**.** *Para todo inteiro k relativamente primo com $2^n - 1$, existe $a \in \mathbb{F}_{2^n}^*$ tal que $(Tr(x^k + ax))_{x\in\mathbb{F}_{2^n}}$ é uma palavra balanceada, onde $Tr(\alpha) = Tr_{\mathbb{F}_{2^n}}$.*

A Conjectura original é mais geral, trata não somente do caso 2 mas sim de um p primo qualquer.

A Proposição 3.2 nos diz que se x^k+ax é um polinômio de permutação, então $(Tr(x^k+ax))_{x\in\mathbb{F}_{2^n}}$ é uma palavra balanceada. Assim achar binômios de permutação é uma forma de responder parcialmente a Conjectura de Helleseth.

Teorema 3.4. *Seja $q = 2^{s\ell m}$, ℓ inteiro positivo, m um divisor de $q-1$ e s a ordem de 2 em $\mathbb{Z}/m\mathbb{Z}$. Então a Conjectura 3.3 é satisfeita para $k = \frac{q-1}{m} + 1$.*

Demonstração. Observe que

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

assim pelo Corolário 2.42 é suficiente mostrar que existe $a \in \mathbb{F}_{2^{k\ell}}$ tal que $(-a^m) \neq 1$.

De fato, $(-a^m) = 1$ se, e somente se, a é raiz de $g(x) = x^m + 1$. Mas g possui exatamente m raízes em $\mathbb{F}_{2^{k\ell}}$ assim existe $a \in \mathbb{F}_{2^{k\ell}}$ que não é raiz de g.

Dessa forma $x^k + ax$ é um PP e $(\mathrm{Tr}(x^k + ax))$ é uma palavra balanceada pela Proposição **??**. □

Teorema 3.5. *Para todo $m \geq 2$, para todo $n \geq 2\log_2\left(1 + \frac{m+1}{m^{m+2}}\right) + (2m+2)\log_2(m)$ tal que m divide $2^n - 1$. a Conjectura de Helleseth é satisfeita para $k = \frac{2^n-1}{m} + 1$.*

Demonstração. Seja $q = 2^n$ temos então por hipótese que $q > \left(1 + \frac{m+1}{m^{m+2}}\right)^2 m^{2m+2}$ assim pelo Corolário 2.47 existe $a \in \mathbb{F}_q^*$ tal que $x^k + ax$ é um PP e assim a conjectura é satisfeita pela proposição **??**. □

3.2 Expoentes de Niho

Definição 3.6. *Seja $n = p^{2t} - 1$ e k um inteiro positivo menor que n. Então k é um expoente de Niho se, e somente se, satisfaz as seguinte condições:*

- $Mdc(k, n) = 1$
- $k \notin \{1, p, p^p, \ldots, p^{t-1}\}$
- $k \equiv p^j \pmod{p^t - 1}$ *para algum* $j, 0 \leq j \leq t-1$.

Alguns números que são expoentes de Niho satisfazem a Conjectura de Helleseth.

Proposição 3.7. *O número $\frac{p^{2t}-1}{m} + 1$ é um expoente de Niho em $\mathbb{F}_{p^{2t}}$ se, e somente, m divide $p^t + 1$.*

Demonstração. Escrevendo $q = p^{2t}$, nós temos:

$$\begin{aligned} \frac{q-1}{m} + 1 = \lambda(p^t - 1) + p^j \quad &\Leftrightarrow \quad q - 1 + m = \lambda(p^t - 1)m + p^j m \\ &\Leftrightarrow \quad m = \frac{(p^t - 1)(p^t + 1)}{\lambda(p^t - 1) + p^j - 1}. \end{aligned}$$

Com $j = 0$, obtemos o resuldado. □

Usando os resultados obtidos sobre binômios de permutação na sessão 2.3 nós obtemos mais expoentes de Niho.

Proposição 3.8. *Sejam m e ℓ inteiros positivos, s a ordem de 2 em $\mathbb{Z}/m\mathbb{Z}$. Tome $q = 2^{s\ell m}$. Se m divide $1 + \sqrt{q}$ então*

$$k = \frac{q-1}{m} + 1$$

é um expoente de Niho e existe $a \in \mathbb{F}_q^*$ tal que a palavra $(Tr(x^k + ax))_{x\in\mathbb{F}_q}$ é balanceada.

Demonstração. A Proposição 3.7 garante que k é um expoente de Niho, enquanto o Corolário 2.42 nós dá um $a \in \mathbb{F}_q^*$ tal que $(x^k + ax)$ é um polinômio de permutação, pela Proposição 3.2 $(\mathrm{Tr}(x^k + ax))_{x\in\mathbb{F}_q}$ é uma palavra balanceada. □

Bibliografia

[Chapuy] Yann Laigle-Chapuy, "Permutation polynomials and applications to coding theory", Finite Fields and Their Applications, v.13,p. 58–70", 2007.

[Wan-Lidl] Daqing Wan and Rudolf Lidl, "Permutation polynomials of the Form $x^r f(x^{(q-1)/d})$ and Their Group Structure", Monatshefte für Mathematik, v.112,p.149–163, 1991.

[Lidl] Rudolf Lidl and Harald Niederreiter, "Finite Fields", Cambridge University Press, 1977.

[Abramo] Abramo Hefez and Maria Lúcia T. Villela,"Códigos Corretores de Erros ", IMPA, 2002.

[Elon] Elon Lages Lima, "Álgebra Linear", "IMPA", 1996.

[Katz] Daniel J. Katz, "Proof of a Conjecture of Helleseth: Maximal Linear Recursive Sequences of Period $2^{2^n} - 1$ Never Have Three-Valued Cross-Correlation", arXiv:1105.2291v2, 2011.

[Helleseth] Tor Helleseth, "Some results about the cross-correlation functions between two maximal linear sequences", Discrete Mathematics, v. 16, p.209–232, 1976.

[Niho] Y. Niho, "Multi-valued cross-correlation function between two maximal linear recursive sequences, Tese de Doutorado, University of Southern California, Los Angeles, CA, 1975

[Knuth] Donald E, Knuth, "Efficient Balanced Codes", IEEE Transactions on Information Theory, v. 32, p. 51–53, 1986.