ALEXANDRE HENRIQUE AFONSO CAMPOS

Esteganografia do Ponto de Vista da Teoria dos Códigos

UNIVERSIDADE FEDERAL DE UBERLÂNDIA
FACULDADE DE MATEMÁTICA
2014

ALEXANDRE HENRIQUE AFONSO CAMPOS

Esteganografia do Ponto de Vista da Teoria dos Códigos

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

Área de Concentração: Matemática.
Linha de Pesquisa: Álgebra.

Orientador: Prof. Dr. Guilherme Chaud Tizziotti.

UBERLÂNDIA - MG
2014

UNIVERSIDADE FEDERAL DE UBERLÂNDIA
FACULDADE DE MATEMÁTICA
PROGRAMA DE PÓS-GRADUAÇÃO EM MATEMÁTICA
Av. João Naves de Ávila, 2121, Bloco 1F, Sala 1F 152
Campus Santa Mônica, Uberlândia - MG, CEP 38400-902

ALUNO: Alexandre Henrique Afonso Campos.

NÚMERO DE MATRÍCULA: 11212MAT001.

ÁREA DE CONCENTRAÇÃO: Matemática.

LINHA DE PESQUISA: Álgebra.

PÓS-GRADUAÇÃO EM MATEMÁTICA: Nível Mestrado.

TÍTULO DA DISSERTAÇÃO: Esteganografia do Ponto de Vista da Teoria dos Códigos.

ORIENTADOR: Prof. Dr. Guilherme Chaud Tizziotti.

Esta dissertação foi **APROVADA** em reunião pública realizada na Sala Multiuso da Faculdade de Matemática, Bloco 1F, Campus Santa Mônica, em 20 de fevereiro de 2014, às 9h00min, pela seguinte Banca Examinadora:

NOME	**ASSINATURA**
Prof. Dr. Guilherme Chaud Tizziotti Universidade Federal de Uberlândia	
Prof. Dr. Alonso Sepulveda Castellanos Universidade Federal de Uberlândia	
Prof. Dr. Rafael Peixoto Universidade Federal do Triângulo Mineiro	

Uberlândia-MG, 20 de fevereiro de 2014.

Dedicatória

Aos meus pais: José Afonso e Marli Aparecida Campos da Silva.

Agradecimentos

Agradeço à minha (agora) esposa Nalin Nóbrega Pereira Afonso, por seu companheirismo, carinho e dedicação. Ao Guilherme Chaud Tizziotti, o (também agora) pai da pequena Lis, por sua visão, críticas, elogios e por saber o melhor direcionamento. Aos meus companheiros de estudo na "salinha do mestrado", demais professores do departamento de Matemática da UFU e todos os outros que fizeram parte direta ou indiretamente deste processo.

CAMPOS, A. H. A. *Esteganografia do Ponto de Vista da Teoria dos Códigos.* 2014. 45 p. Dissertação de Mestrado, Universidade Federal de Uberlândia, Uberlândia-MG.

Resumo

A Esteganografia é um assunto que ganhou importância rapidamente no contexto da segurança da informação. Ao ser relacionada com a Teoria dos Códigos, que já estava mais desenvolvida, a pesquisa neste mérito ganhou volume. Neste trabalho, introduziremos Esteganografia e mostraremos como a Teoria dos Códigos pode facilitar seu estudo; códigos perfeitos serão associados a um tipo de protocolo esteganográfico e veremos o efeito de código em papel molhado na Esteganografia.

Palavras-chave: Esteganografia; Teoria dos Códigos; Códigos Perfeitos; Protocolos Perfeitos; Código em Papel Molhado.

CAMPOS, A. H. A. *Steganography From the Coding Theory Point of View.* 2014. 45 p. M. Sc. Dissertation, Federal University of Uberlândia, Uberlândia-MG.

Abstract

Steganography is a subject that became very important in the study of information security. When it was related to Coding Theory, which was well developed, the research on this matter rapidly increased. In this work, we will introduce Steganography and we will show how the Coding Theory can help in its study; perfect codes will be related to a kind of stegoscheme and we will see the effect of wet paper codes in Steganography.

Keywords: Steganography; Coding Theory; Perfect Codes; Perfect Stegoscheme; Wet Paper Code.

Sumário

Introdução

Esteganografia, que provém do grego "escrita escondida", é a ciência que estuda a ocultação de mensagens. Esconder uma mensagem pode ser uma forma eficiente de mantê-la em segredo, já que pode não despertar atenção. O objeto no qual se esconde a mensagem é chamado de cobertura. Basicamente, há quatro fatores principais que influenciam na eficiência da esteganografia:

1) O tipo de cobertura no qual a mensagem será imersa;

2) A escolha dos lugares da cobertura onde o segredo será escondido;

3) O método de inserção da mensagem;

4) A quantidade de mudanças que serão feitas na cobertura.

Não se deve confundir esteganografia com criptografia, cujo estudo analisa maneiras de tornar mensagens ilegíveis a terceiros pela utilização de cifras, mas não necessariamente acoberta a mensagem.

No século V a.C., Histaiacus utilizou um vetor humano para esconder uma mensagem. Ele raspou a cabeça de um mensageiro e escreveu uma mensagem encorajando Aristágoras de Mileto a se revoltar contra o rei da Pérsia e depois que o cabelo cresceu de volta, o mensageiro foi enviado. Esta foi uma situação em que o tempo não era fator primordial.

Em 460 a.C., um grego chamado Demaratus mandou uma mensagem aos espartanos alertando sobre uma invasão a ser perpetrada pelo exército de Xerxes. A mensagem foi enviada secretamente e o processo foi descrito por Heroclotus. Pelo relato, Demaratus escreveu a mensagem em madeira que foi posteriormente coberta com cera e assim, se algum guarda fosse revistar a carga, não se incomodariam com madeiras "em branco".

O Grill de Cardano, criado pelo matemático italiano Girolamo Cardano, é um método interessante e tão bem conhecido que foi utilizado pelos roteiristas, no filme Con Air - A Rota de Fuga. Para aplicar esta técnica, envia-se um texto qualquer (de preferência que faça sentido, para não despertar atenção) e dentro do texto escolhe-se caracteres que estão em determinadas posições,

combinadas entre remetente e destinatário. Para facilitar o processo de reconhecimento da mensagem, pode-se sobrepor ao texto enviado algo como um papel furado nas posições determinadas.

Exemplo: *Suponha que se queira esconder a mensagem "PRPO na cota 861"em um texto. Combinadas as posições, o remetente cria (ou encontra) um texto cuja mensagem possa ser extraída das posições indicadas. Na Figura 1, temos o texto*[1] *de cobertura (esquerda) e a seleção das posições combinadas (direita).*

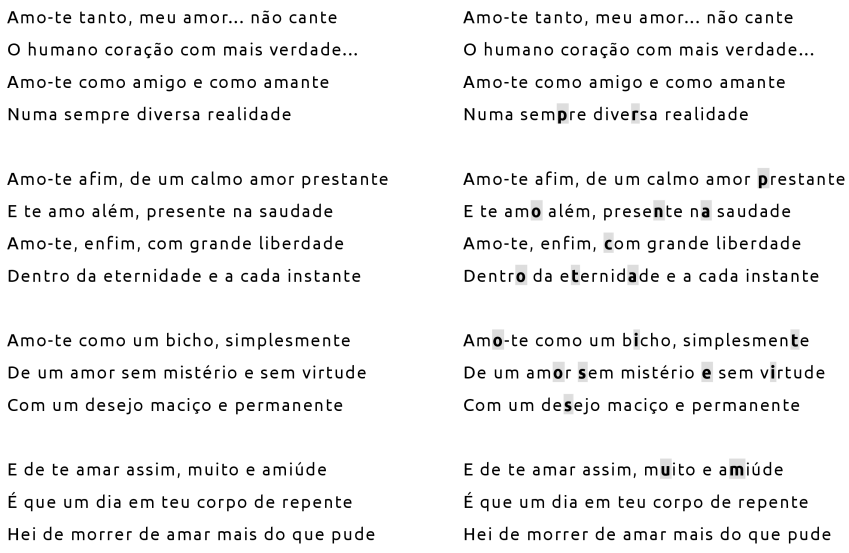

Figura 1: Imagem do texto de cobertura (esquerda) e seleção no texto (direita).

Perceba que pode ser complicado contar posições para encontrar a seleção. Pode-se criar um dispositivo (*grill*) para ser sobreposto ao texto recebido a partir de alguma referência. Na Figura 2, a referência é a primeira letra do texto (que não faz parte da mensagem).

Com este mesmo dispositivo pode-se extrair outras mensagens, contando que o texto de cobertura seja diferente ou que se altere a referência.

Apesar destes exemplos práticos, um dos trabalhos mais antigos sobre esteganografia e criptografia de que se tem notícia, do qual nasceu o termo esteganografia, é o do abade alemão Johannes Trithemius [6], publicado postumamente em 1606. O texto é uma trilogia: as duas primeiras partes sobre

[1] Soneto do Amor Total, do Vinícius de Moraes.

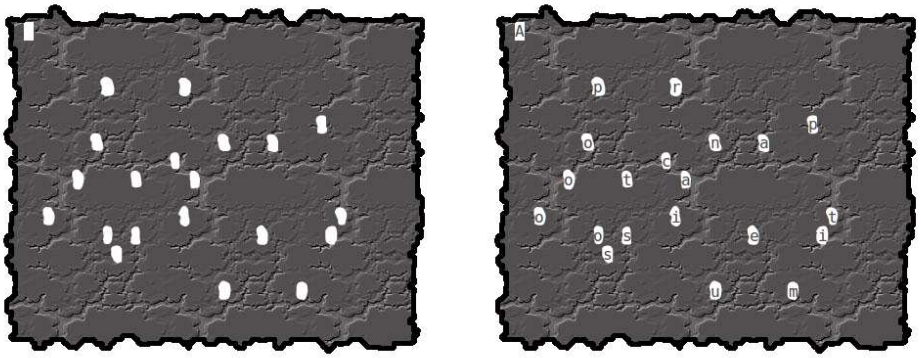

Figura 2: Dispositivo para sobreposição (esquerda) e sobreposição (direita).

esteganografia e criptografia. A terceira é sobre ocultismo e contém várias tabelas com números.

A necessidade do envio secreto de mensagens cresce em tempos de instabilidade política, por isso exemplos de esteganografia (e mesmo criptografia) estão frequentemente associados a época de conflito entre nações.

A utilização moderna da esteganografia, a digital, consiste em esconder mensagens em arquivos de computador tais como imagens ou áudios. A criação de um sistema esteganográfico contém (pelo menos) duas etapas:

1) A escolha de uma boa cobertura e como podemos inserir a mensagem da maneira mais imperceptível;

2) A criação de algoritmos eficientes para embutir e extrair a informação.

No entanto, qualquer documento eletrônico que contenha informações irrelevantes ou redundâncias pode ser utilizado como cobertura. Uma das formas bastante utilizadas de esteganografia digital é conhecida como LSB (Least Significant Bit – Bit Menos Significante em tradução livre). Na forma mais comum, seleciona-se determinado pixel[2] de uma imagem e troca-se o bit menos significante por um bit de informação.

A esteganografia também pode ser utilizada para segurança digital pela inserção de marca d'água. Para dificultar a detecção de uma mensagem inserida, estaremos interessados em como fazer o máximo de mudanças possível modificando minimamente os bits da cobertura. A teoria de códigos corretores de erros entra para aumentar a eficiência da imersão/recuperação da mensagem.

[2]Menor elemento de uma imagem. São como pequenos quadrados coloridos. Cada imagem é formada por uma sucessão de pixeis.

Com a esteganografia digital, temos basicamente dois tipos de coberturas: arquivos de imagens e textos. Para tentar detectar mensagens secretas em textos, alguns parâmetros podem ser observados:

- Frequência de letras;
- Frequência de palavras;
- Capacidade para compressão;
- Gramática, estilo de escrita e legibilidade;
- Semântica e lógica;
- Contexto da mensagem;

Estes fatores funcionam porque criar uma mensagem para esconder outra pode ser mais difícil do que parece. No exemplo do *grill* de Cardano, a mensagem de cobertura deve conter os caracteres desejados nas posições corretas. Para alcançar este intento, o remetente pode sacrificar um pouco a coesão do texto, duplicar letras ou repetir palavras, o que desperta atenção.

O próximo item elucida um pouco sobre como números podem ser associados a imagens.

Observação: *Considere que uma imagem em tons de cinza seja formada por pixeis de* 8 *bits, isto é, a imagem é uma matriz, cujo tamanho corresponde ao tamanho da imagem (exemplos comuns de são* 1024 *por* 768 *pixeis ou* 640 *por* 480 *pixeis; o primeiro número é o comprimento e o segundo a altura da imagem), em que cada entrada é um número do conjunto* $\{x \in \mathbb{Z} : 0 \leq x < 2^8\}$. *Escrevendo apropriadamente, os números deste conjunto têm* 8 *(bits) posições (*$0 = 00000000$, $1 = 00000001$, ..., $255 = 11111111$*). O preto corresponde ao número* 0 *e o branco ao número* 255. *Os números intermediários correspondem a tons de cinza claro conforme estejam mais próximos do* 255 *ou cinza escuro se estiverem próximos do* 0.

Caso a imagem seja colorida, o sistema é semelhante. Para determinar uma cor, precisamos de uma terna (x, y, z), *com* $0 <= x, y, z < 255$, *que representam as intensidades das cores vermelha, verde e azul, respectivamente (sistema RGB).*

Existem dezenas de *softwares* tanto para esconder quanto para tentar encontrar (ou recuperar) mensagens escondidas em arquivos diversos, como por exemplo o QuickStego, SecretLayer, SpamMimic ou OpenPuff.

Este trabalho está organizado da seguinte maneira: o Capítulo 1 discorre sobre código corretores de erro. O Capítulo 2 introduz protocolos esteganográficos, que são um par de aplicações, com destaque para o algoritmo F5. Do par de aplicações citadas, uma pode ser bastante difícil de ser encontrada. O Capítulo 3 é sobre como a teoria dos códigos pode facilitar o trabalho com esteganografia, sobretudo em como podemos utilizar códigos corretores de erro para encontrar a aplicação supramencionada como difícil de ser obtida. O Capítulo 4 é sobre códigos em papel molhado e como eles podem afetar a esteganografia.

Capítulo 1

Códigos Corretores de Erros

Ao se digitar uma tecla no teclado do computador, apertar um botão do controle de um video-game ou diminuir o volume da televisão, existe uma interação entre pessoas e máquinas. Estas ações, antes de serem interpretadas pelo dispositivo, devem ser transformadas em uma linguagem que um computador possa compreender. Essa linguagem é formada por palavras de um alfabeto preestabelecido e por alfabeto, entende-se um conjunto de caracteres que serão, quase sempre, algarismos.

Erros podem acontecer ao se transmitir uma mensagem por um meio ruidoso. A Teoria dos Códigos Corretores de Erro estuda maneiras de encontrar o erro e corrigir para a mensagem que deveria ter sido enviada.

1.1 Introdução

A teoria dos códigos é um assunto bem estudado e servirá de base para facilitar um estudo posterior sobre esteganografia.

1.1 Exemplo: *Considere o alfabeto* $\mathbb{F}_2 = \{0, 1\}$. *Existe uma infinidade de combinações que pode-se fazer com os dois caracteres em questão: 1, 10, 100, 101, etc. Fixado um determinado tamanho n, tem-se um número finito de palavras com este parâmetro.*

- $n = 1$ *Tem-se duas palavras:* 0 *e* 1*;*
- $n = 2$ *Quatro palavras:* 00, 01, 10 *e* 11*;*
  $\vdots$
- $n = k$ *Para cada uma das k posições, tem-se duas possibilidades:* 0 *ou* 1. *Pelo Princípio Fundamental da Contagem, o total de palavras será* 2^k.

Cada palavra poderá representar uma ação a ser interpretada: 00 *e* 01 *podem ser aumentar e diminuir o volume, respectivamente;* 10 *e* 11 *podem ser canal para cima e para baixo, respectivamente.*

Fixado um alfabeto A, no qual $\#(A) = q$, ou seja, A tem q elementos e um tamanho n, o espaço amostral de todas as palavras formadas pelos caracteres de A pode ser encarado como o espaço A^n. A definição que segue deixa claro que nem todas as palavras de A^n necessitam estar no código desejado.

1.2 Definição: *Dado um alfabeto* $A = \{a_1, a_2, ..., a_q\}$*, com* $q \in \mathbb{N}$*, um* ***código*** C *é um subconjunto de palavras de* A^n*.*

Ao se transmitir uma palavra por um meio ruidoso, erros podem acontecer e neste cenário o código anterior não é um bom código. Se se quiser aumentar o volume, ou seja, transmitir 00 e, por um erro, a palavra transmitida for 01 ou 10, como essas duas palavras pertencem ao código, não haverá indícios de que um erro foi cometido. Ao invés da detecção do erro, o televisor poderá diminuir o volume ou trocar o canal. Este exemplo simples, que causaria exasperação no quotidiano, ilustra como a transmissão exata pode ser necessária. Agora, se um médico opera um paciente com braços mecânicos, um erro poderia resultar na falha do procedimento cirúrgico.

Felizmente, existem maneiras de se detectar a presença erros. Mais ainda, em alguns casos, pode-se *corrigir* esses erros. No exemplo anterior em que

$$C = \{00, 01, 10, 11\},$$

considere o novo código

$$C_1 = \{000000, 010101, 101010, 111111\},$$

com uma correspondência termo a termo como na Tabela 1.1. Os elementos de C formam o que se chama **código-fonte**. Os que serão transmitidos, ou seja, os elementos do conjunto C_1, constituem o **código-de-canal**.

O código-de-canal é obtido considerando-se o código-fonte com alguma **redundância**, ou seja, são adicionadas partes que não são necessariamente informação, mas ajudam a corrigir possíveis erros.

As palavras do código-de-canal na Tabela 1.1 são constituída pela tripla repetição das palavras do código-fonte. Se na tentativa de transmitir 101010 ocorrer 1 erro por causa do meio ruidoso e for recebido 101110, como esta nova palavra não pertence ao código, ou seja $101110 \notin C_1$, o erro *será detectado.* Como a palavra transmitida difere quatro posições de 000000, cinco posições de 010101, uma posição de 101010 e duas posições de 111111, pode-se inferir se queria transmitir 101010. Desta forma, pode-se detectar e corrigir o erro.

Código-Fonte	Código de Canal
00	000000
01	010101
10	101010
11	111111

Tabela 1.1: Correspondência entre códigos

Após a decodificação do código-de-canal, a mensagem transmitida deveria ser 10, ou seja, aumentar o volume.

A Figura 1.1 ilustra o fluxo descrito anteriormente.

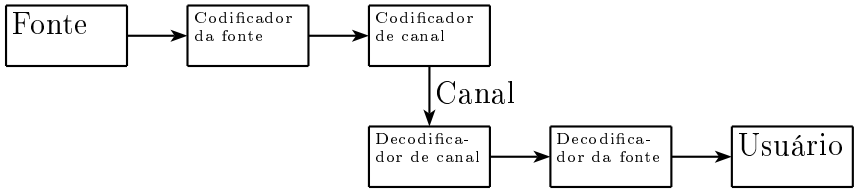

Figura 1.1: Fluxo do código

Em geral, dado um código C e uma palavra recebida r, é interessante corrigir r para a palavra em C mais próxima de r. Este tipo de decodificação é chamada de decodificação por distância mínima.

1.3 Observação: *De agora em diante, o alfabeto será um corpo finito* $\mathbb{F}_q$.

A definição que segue permite encontrar a distância entre duas palavras de um código, fundamental para correção de erros, como ficou claro na correção do código que foi feita anteriormente.

1.4 Definição: *Dado dois elementos* $u = u_1u_2...u_n$ *e* $v = v_1v_2...v_n \in \mathbb{F}_q^n$, *com* u_i *e* $v_i \in \mathbb{F}_q$, $i \in \{1, 2, ...n\}$, *a* ***Distância de Hamming*** *entre eles é definida como*

$$\mathrm{d}(u, v) = \#\{i : u_i \neq v_i, 1 \leq i \leq n\}$$

Intuitivamente, a Distância de Hamming conta quantas entradas diferentes u tem em relação a v. O nome "distância"é justificado pela próxima proposição.

1.5 Proposição: *A Distância de Hamming é uma métrica.*

Demonstração: Sejam $u = u_1...u_n$, $v = v_1...v_n$ e $w = w_1...w_n$ palavras de um código $C \subset \mathbb{F}_q^n$.

i) *Positividade:* É trivial que $\mathrm{d}(u,v) \geq 0$, já que é o número de elementos de um conjunto. Além disso, se $\mathrm{d}(u,v) = 0$, então u e v não diferem em nenhum posição, isto é, $u = v$;

ii) *Simetria:* $\mathrm{d}(u,v) = \#\{i : u_i \neq v_i, 1 \leq i \leq n\} = \#\{i : v_i \neq u_i, 1 \leq i \leq n\} = \mathrm{d}(v,u)$;

iii) *Desigualdade Triangular:* Por indução.

- $n = 1$ Tem-se $u = u_1$, $v = v_1$ e $w = w_1$. Uma, e apenas uma, das seguintes opções acontece: $u_1 = v_1$ ou $u_1 \neq v_1$. No primeiro caso, $\mathrm{d}(u,v) = 0$ e $\mathrm{d}(u,w) + \mathrm{d}(w,v) = 0$ ou 2, conforme $u_1 = w_1$ ou $u_1 \neq w_1$, respectivamente. De qualquer modo, $\mathrm{d}(u,v) \leq \mathrm{d}(u,w) + \mathrm{d}(w,v)$. No segundo caso, $\mathrm{d}(u,v) = 1$ e $\mathrm{d}(u,w) + \mathrm{d}(w,v) = 1$ ou 2. De fato, se $w_1 = u_1$, necessariamente $w_1 \neq v_1$, daí $\mathrm{d}(u,w) + \mathrm{d}(w,v) = 0 + 1 = 1$. O caso em que $w_1 = v_1$ é análogo. Tem-se $\mathrm{d}(u,w) + \mathrm{d}(w,v) = 2$ quando a dupla diferença $u_1 \neq w_1$ e $w_1 \neq u_1$ acontece.

- $n = k$ Admita, como hipótese de indução, que $\mathrm{d}_k(u,v) \leq \mathrm{d}_k(u,w) + \mathrm{d}_k(w,v)$, com $\mathrm{d}_n(u,v)$ a Distância de Hamming no espaço A^n, $u = u_1...u_k$, $v = v_1...v_k$, $w = w_1...w_k$. Agora, se for adicionada uma entrada em cada uma das palavras do código, de forma que $u = u_1...u_k u_{k+1}$, $v = v_1...v_k v_{k+1}$, $w = w_1...w_k w_{k+1}$, como a Distância de Hamming é a contagem de um conjunto (dos índices tais que uma diferença acontece), tem-se que as novas distâncias serão as mesmas somadas uma unidade, se ocorrer uma nova diferença, assim, $\mathrm{d}_k(u,v) \leq \mathrm{d}_{k+1}(u,v)$, $\forall u, v \in A^n$. Se $u_{k+1} = v_{k+1}$, então $\mathrm{d}_{k+1}(u,v) = \mathrm{d}_k(u,v) \leq \mathrm{d}_k(u,w) + \mathrm{d}_k(w,v) \leq \mathrm{d}_{k+1}(u,w) + \mathrm{d}_{k+1}(w,v)$.

■

Dada uma palavra $a \in \mathbb{F}_q^n$ e $r \in \mathbb{N}$, define-se **esfera** e **bola** de centro a e raio r, respectivamente, por

$$S(a,r) = \{u \in \mathbb{F}_q^n : \mathrm{d}(a,u) = r\} \text{ e}$$

$$B(a,r) = \{u \in \mathbb{F}_q^n : \mathrm{d}(a,u) \leq r\}$$

A próxima definição usa a noção de distância de elemento a conjunto como usual, ou seja, $\mathrm{d}(x,C) = \min\{d(x,y) | y \in C\}$.

1.6 Definição: *O* ***raio de cobertura*** *do código $C \in \mathbb{F}_q^n$ é o menor inteiro ρ tal que $\mathbb{F}_q^n = \bigcup_{x \in C} B(x,\rho)$. Podemos escrever também $\rho = \max\{\mathrm{d}(x,C) : x \in \mathbb{F}_q^n\}$.*

1.7 Proposição: *Para todo $a \in \mathbb{F}_q^n$ e $r \in \mathbb{N}$,*

$$\#S(a,r) = \binom{n}{r}(q-1)^r$$

Demonstração: Tome $a = a_1...a_n$. Uma palavra que esteja em $S(a,r)$ difere em r entradas de a. A diferença acontece em r das n entradas de a, ou seja em $\binom{n}{r}$ ocasiões. Fixado onde estão essas r diferenças, temos $q-1$ possibilidades para cada uma. Pelo Princípio Fundamental da Contagem, o total é o produto $\binom{n}{r}(q-1)^r$. ■

1.8 Proposição: *Para $r \neq r' \in \mathbb{N}$, tem-se $S(a,r) \cap S(D,r') = \emptyset$.*

Demonstração: Suponha que $b \in S(a,r) \cap S(a,r')$. Então, $\mathrm{d}(a,b) = r$ significa que a difere de b em r entradas. De $\mathrm{d}(a,b) = r'$, tem-se que a difere de b em r' entradas. Mas $r \neq r'$, absurdo. ■

Das proposições em 1.7 e 1.8, temos o resultado seguinte.

1.9 Corolário: $\#B(a,r) = \sum_{i=0}^{\lfloor r \rfloor} = \binom{n}{i}(q-1)^i$.

1.10 Observação: *Note que o número de elementos em uma esfera ou bola não depende da palavra escolhida. Podemos definir então $V_q(n,t) := \#B(x,t)$, para qualquer $x \in \mathbb{F}_q^n$, $t \in \mathbb{R}$ (o que justifica o uso da função "maior inteiro que não supera"no corolário anterior).*

1.11 Definição: *Seja $C \subset \mathbb{F}_q^n$ um código. A* ***distância mínima*** *de C é o número*

$$d = min\{\mathrm{d}(u,v) : u, v \in C \text{ e } u \neq v\}$$

Na proposição que segue, $\lfloor t \rfloor$ significa o maior inteiro que não supera $t \in \mathbb{R}$, ou seja, a parte inteira de t. Sua demonstração fará uso do fato, óbvio, $\lfloor t \rfloor \leq t$ e de agora em diante, será adotada a convenção de que $\kappa = \left\lfloor \dfrac{d-1}{2} \right\rfloor$

1.12 Proposição: *Seja $C \subset \mathbb{F}_q^n$ um código com distância mínima d. Se a e a' são palavras distintas de C, então*

$$B(a,\kappa) \cap B(a',\kappa) = \emptyset.$$

Demonstração: Suponha que $b \in B(a,\kappa) \cap B(a',\kappa)$. Então,

$$\mathrm{d}(a,a') = \mathrm{d}(a,b) + \mathrm{d}(a',b) \leq \kappa + \kappa = 2\kappa = 2\left\lfloor \frac{d-1}{2} \right\rfloor \leq 2\left(\frac{d-1}{2}\right) = d-1.$$

Absurdo, pois, por hipótese $\mathrm{d}(a,a') \geq d$. ■

1.13 Corolário: *Um código nas condições anteriores permite detectar até* $d-1$ *e corrigir até* κ *erros.*

Demonstração: Sejam a e b duas palavras do código tais que $\mathrm{d}(a,b) = d$. Se ao transmitir a palavra $a = a_1...a_n$ comete-se d erros, pode ser que se transmita a palavra b, logo, não será detectado o erro. Se se cometer até $d-1$ erros, certamente a palavra enviada não será do código, pois este tem distância mínima d e o erro será detectado. Mais ainda, pela proposição em 1.12, na bola $B(b,\kappa)$ existe uma, e apenas uma, palavra do código C, que pode-se tomar como a palavra que deveria ser transmitida. ■

1.14 Definição: *Seja* $C \subset \mathbb{F}_q^n$ *um código com distância mínima* d. *Diz-se que* C *é um* ***código perfeito*** *se* $\bigcup_{c\in C} B(c,\kappa) = \mathbb{F}_q^n$.

Em um código perfeito, qualquer palavra transmitida, mesmo que erroneamente, pode ser corrigida, pois certamente, no disco de raio κ, haverá uma única palavra que pode ser tomada como correta. Se forem cometidos mais do que κ erros, a palavra recebida será decodificada para outra que não a palavra que se queria enviar.

Um código C possui três parâmetros fundamentais $[n, M, d]$, em que n é o tamanho de cada palavra, M é o número de palavras do código e d é a distância mínima. A definição de código perfeito poderia ser dada de outra maneira:

1.15 Proposição: *Sobre* $\mathbb{F}_q$, *seja* C *um código* t*-corretor de erros, isto é, que corrige até* t *erros, tal que* $\#(C) = M$. *Temos*

$$M\sum_{i=0}^{t}\binom{n}{i}(q-1)^i \leq q^n.$$

Demonstração: As bolas de raio i centradas em palavras distintas de C são disjuntas. A soma das cardinalidades das bolas é menor que ou igual ao número de elementos do espaço todo. ■

Esta cota é chamada de **Cota de Hamming para códigos corretores de erros**

1.16 Definição: *Seja* A *um alfabeto e* $n \in \mathbb{N}$. *Diremos que*

$$F : A^n \longrightarrow A^n$$

é uma **isometria** *se* F *preserva a distância de Hamming, ou seja*

$$\mathrm{d}(F(x), F(y)) = \mathrm{d}(x,y),\ \forall x, y \in A^n.$$

1.17 Proposição: *Toda isometria de A^n é uma bijeção de A^n.*

Demonstração:
Injetividade) $F(x) = F(y) \Rightarrow 0 = \mathrm{d}(F(x), F(y)) = \mathrm{d}(x, y) \Rightarrow x = y$.
Sobrejetividade) Como A^n é finito, a função injetiva é também sobrejetiva. ■

1.18 Exemplo: *São exemplos de isometrias;*

i) Identidade;

ii) Se F é uma isometria, então F^{-1} é uma isometria;

iii) Se F e G são isometrias, então a composta $F \circ G$ também o é.

Demonstração:

i) $\mathrm{d}(Id(x), Id(y)) = \mathrm{d}(x, y)$;

ii) $\mathrm{d}(F^{-1}(x), F^{-1}(y)) = \mathrm{d}(F(F^{-1}(x)), F(F^{-1}(y))) = \mathrm{d}(x, y)$;

iii) $\mathrm{d}(F(G(x)), F(G(y))) = \mathrm{d}(G(x), G(y)) = \mathrm{d}(x, y)$.

■

1.19 Definição: *Dados dois códigos C e C' em A^n, diz-se que C' é* ***equivalente*** *a C se existe uma isometria $F : A^n \longrightarrow A^n$ tal que $F(C) = C'$.*

Para justificar o nome, a demonstração feita no exemplo em 1.18 mostra que a equivalência de códigos é uma relação de equivalência.

1.2 Códigos Lineares

1.20 Definição: *Um código $C \subset \mathbb{F}_q^n$ será chamado de* ***código linear*** *se for um subespaço vetorial de $\mathbb{F}_q^n$.*

Seja p a dimensão do código C como um $\mathbb{F}_q^n$-subespaço vetorial e seja $\{v_1, v_2, ..., v_p\}$ uma de suas bases. Tem-se que para cada $u \in C$, pode-se escrever da seguinte forma

$$u = u_1 v_1 + \cdots + u_p v_p.$$

Para cada u_i, $i \in \{1, 2, ..., p\}$, temos q possibilidades, logo,

$$\#(C) = M = q^p$$

Um código linear C com comprimento n, dimensão p e distância mínima d será denotado por um $[n, p, d]$-código.

1.21 Definição: *Dado $x \in \mathbb{F}_q^n$, define-se o* ***peso da palavra*** *x como o inteiro*

$$\omega(x) = \#\{i : x_i \neq 0, i = 1, ..., n\},$$

isto é, o número de entradas não nulas de x. Alternativamente, $\omega(x) = \mathrm{d}(x, 0)$.

1.22 Definição: *O* ***peso de um código*** *C é o inteiro*

$$\omega(C) = min\{\omega(x) : x \in C\backslash\{0\}\}$$

1.23 Proposição: *Seja $C \subset \mathbb{F}_q^n$ um código linear com distância mínima d. Temos que*

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

ii) $d = \omega(C)$

Demonstração:

i) $\omega(x - y) = \#\{i : x_i - y_i \neq 0, 1 \leq i \leq n\} = \#\{i : x_i \neq y_i, 1 \leq i \leq n\} = \mathrm{d}(x, y)$;

ii) $d = min\{\mathrm{d}(x, y) : x \neq y \in C\} = min\{\omega(x - y, 0) : x \neq y \in C\} = min\{\omega(x - y - 0) : x \neq y \in C\backslash\{0\}\}$. Chame $z = x - y$. Como $x \neq y$, tem-se $z \neq 0$. Substituindo, $d = min\{\omega(z) : 0 \neq z \in C\} = \omega(C)$.

■

Desta forma, pode-se calcular a distância mínima de um código linear com $M - 1$ cálculos. O item i) justifica o fato de a distância mínima também ser chamada de peso do código.

No que segue, há como determinar C como núcleo ou imagem de uma transformação linear.

Seja $\mathscr{B} = \{v_1, ..., v_p\}$ uma base para C. Considere a aplicação linear

$$\begin{array}{rccc} T: & \mathbb{F}_q^p & \longrightarrow & \mathbb{F}_q^n \\ & (x_1, ..., x_p) & \longmapsto & x_1v_1 + \cdots + x_pv_p \end{array}$$

Afirmação: T é injetora. De fato,

$$T(x) = T(y) \Leftrightarrow T(x) - T(y) = 0 \Leftrightarrow T(x - y) = 0 \Leftrightarrow$$

$$\Leftrightarrow T(x_1 - y_1, ..., x_p - y_p) = 0 \Leftrightarrow (x_1 - y_1)v_1 + \cdots + (x_p - y_p)v_p = 0$$

Tem-se uma combinação linear de elementos de uma base com o vetor nulo como resultado. Assim,

$$x_1 - y_1 = 0, ..., x_p - y_p = 0 \Rightarrow x_1 = y_1, ..., x_p = y_p \Rightarrow x = y.$$

Além disto, $C = Im(T)$. Por outro lado, ao se considerar $C' \subset \mathbb{F}_q^n$ tal que a soma direta $C \oplus C' = \mathbb{F}_q^n$, o código C pode ser visto como núcleo da aplicação

$$\begin{array}{rccc} H: & C \oplus C' & \longrightarrow & \mathbb{F}_q^n \\ & u + v & \longmapsto & v \end{array}$$

Para verificar se $c \in C$, basta checar se $H(v) = 0$.

1.24 Definição: *Dois códigos lineares $C, C' \subset \mathbb{F}_q^n$ são* ***linearmente equivalentes*** *se existir uma isometria linear $T : \mathbb{F}_q^n \longrightarrow \mathbb{F}_q^n$ tal que $T(C) = C'$*

1.3 Matriz Geradora

Seja $C \subset \mathbb{F}_q^n$ um código linear com parâmetros $[n, p, d]$, em que n representa o tamanho das palavras, p a dimensão do código C sobre $\mathbb{F}_q$ e d a distância mínima. Seja $\mathscr{B} = \{v_1, ..., v_p\}$ uma base para C. A matriz G cujas linhas são os vetores da base $\mathscr{B}$ é chamada de **matriz geradora do código linear**.

$$G = \begin{pmatrix} v_1 \\ \vdots \\ v_p \end{pmatrix}$$

A aplicação

$$\begin{array}{rccc} T: & \mathbb{F}_q^p & \longrightarrow & \mathbb{F}_q^n \\ & x & \longmapsto & x \cdot G \end{array}$$

pode ser vista como codificação para o código-fonte $\mathbb{F}_q^p$ na qual $Im(T)$ é o código de canal.

1.25 Definição: *Uma matriz geradora está na* ***forma padrão*** *se $G = (Id_p|A)$, em que Id_p é a matriz identidade de ordem p e A uma matriz de ordem $p \times (n - p)$.*

Esta forma é bastante conveniente pois ao se codificar $v = (v_1, ..., v_p)$, basta copiar as p primeira entradas e então calcular as $n - p$ entradas restantes.

1.26 Teorema: *Dado um código C, existe um código equivalente C' com matriz geradora na forma padrão.*

Demonstração: Ver [2, p. 92]. ■

1.4 Código Dual

1.27 Definição: *Se $C \subset \mathbb{F}_q^n$ é um código, o* ***código dual*** *de C é definido por*

$$C^{\perp} := \{v \in \mathbb{F}_q^n : \langle u, v\rangle = 0, \forall u \in C\},$$

em que $\langle u, v\rangle$ denota o produto interno usual em $\mathbb{F}_q^n$.

1.28 Lema: *Se $C \subset \mathbb{F}_q^n$ é um código linear com matriz geradora G, então*

i) $C^{\perp}$ é subespaço de $\mathbb{F}_q^n$;

ii) $x \in C^{\perp}$ se, e somente se, $Gx^t = 0$.

Demonstração:

i) Sejam u e $v \in C^{\perp}$, $\alpha \in \mathbb{F}_q$. Para qualquer $w \in C$,

$$\langle u + \alpha v, w\rangle = \langle w, v\rangle + \alpha\langle v, w\rangle = 0.$$

Claramente, $0 \in C^{\perp}$ pois $\langle 0, v\rangle = 0,\ \forall v \in \mathbb{F}_q^n$. Em particular, para $v \in C$. Logo, $C^{\perp}$ é subespaço de $\mathbb{F}_q^n$;

ii) Seja $\mathscr{B} = \{v^1, ..., v^p\}$ uma base para C.

$\Rightarrow$) $x \in C^{\perp} \Rightarrow \langle x, v\rangle = 0,\ \forall v \in C$. Em particular, $\langle x, v^i\rangle = 0,\ i = 1, ..., k$.

$$Gx^t = \begin{pmatrix} v_1^1 & v_2^1 & v_3^1 & \cdots & v_n^1 \\ v_1^2 & v_2^2 & v_3^2 & \cdots & v_n^2 \\ \vdots & \vdots & \vdots & & \vdots \\ v_1^p & v_2^p & v_3^p & \cdots & v_n^p \end{pmatrix} \begin{pmatrix} x_1 \\ x_2 \\ x_3 \\ \vdots \\ x_n \end{pmatrix} = \begin{pmatrix} \langle v^1, x\rangle \\ \langle v^2, x\rangle \\ \langle v^3, x\rangle \\ \vdots \\ \langle v^p, x\rangle \end{pmatrix} = \begin{pmatrix} 0 \\ 0 \\ 0 \\ \vdots \\ 0 \end{pmatrix}$$

$\Leftarrow$) Por hipótese,

$$Gx^t = 0 \Rightarrow \begin{pmatrix} \langle v^1, x\rangle \\ \langle v^2, x\rangle \\ \vdots \\ \langle v^p, x\rangle \end{pmatrix} = \begin{pmatrix} 0 \\ 0 \\ \vdots \\ 0 \end{pmatrix} \Rightarrow \langle x, v^i\rangle = 0,\ i = 1, ..., p.$$

Seja $u \in C$. Então, $u = u_1v^1 + \cdots + u_pv^p$. Segue que

$$\langle x, u\rangle = \langle x, u_1v^1 + \cdots + u_pv^p\rangle = u_1\langle x, v^1\rangle + \cdots + u_p\langle x, v^p\rangle =$$

$$= u_10 + \cdots + u_p0 = 0 \Rightarrow x \in C^{\perp}$$

■

Pelo lema em 1.28 *i*), $C^{\perp}$ é um código linear e será chamado de **código dual de C**.

1.29 Proposição: *Seja $C \subset \mathbb{F}_q^n$ um código linear de dimensão p com matriz geradora $G = (id_p|A)$ na forma padrão. Então:*

i) dim $C^{\perp} = n - p$;

ii) $H = (-A^t|Id_{n-p})$ é geradora de $C^{\perp}$.

Demonstração:

i) Pelo lema em 1.28, $x = (x_1, ..., x_n) \in C^{\perp} \Leftrightarrow Gx^t = 0$. Como G está na forma padrão,

$$Gx^t = \begin{pmatrix} 1 & 0 & \cdots & 0 & a_{11} & a_{12} & \cdots & a_{1(n-p)} \\ 0 & 1 & \cdots & 0 & a_{21} & a_{22} & \cdots & a_{2(n-p)} \\ \vdots & \vdots & \ddots & \vdots & \vdots & \vdots & & \vdots \\ 0 & 0 & \cdots & 1 & a_{p1} & a_{p2} & \cdots & a_{p(n-p)} \end{pmatrix} \begin{pmatrix} x_1 \\ x_2 \\ \vdots \\ x_p \\ x_{p+1} \\ x_{p+2} \\ \vdots \\ x_n \end{pmatrix} = \begin{pmatrix} 0 \\ 0 \\ \vdots \\ 0 \\ 0 \\ 0 \\ \vdots \\ 0 \end{pmatrix}$$

Seja $j \in \{1, ..., p\}$. A j-ésima linha do produto Gx^t tem a forma

$$x_j + \sum_{i=1}^{n-p} a_{ji}x_i = 0 \Rightarrow x_j = -\sum_{i=1}^{n-p} a_{ji}x_i.$$

Pode-se escrever sob a forma matricial

$$\begin{pmatrix} x_1 \\ x_2 \\ \vdots \\ x_p \end{pmatrix} = -A \begin{pmatrix} x_{p+1} \\ x_{p+2} \\ . \\ . \\ . \\ x_n \end{pmatrix}$$

Percebe-se que os elementos de $C^{\perp}$ dependem de x_i, com $1 \leq i \leq n$. Como $x_i \in \mathbb{F}_q$, tem-se q possibilidades para cada. Pelo Princípio Fundamental da Contagem, $\#(C) = q^{n-p}$, logo, sua dimensão é $n - p$;

ii) Como as $n-p$ últimas colunas de H apresentam a matriz identidade, as linhas de H são LI. Se g_j e h_i são a j-ésima e i-eśima linha de G e H, então, $\langle g_j, h_i \rangle = 0$. Portanto, o espaço vetorial gerado pelas linhas de H está contido em $C^{\perp}$. Como suas dimensões são iguais, então $C^{\perp}$ é gerado por H.

■

1.30 Proposição: *Seja C um código linear e $C^{\perp}$ gerado pela matriz H. Então, $w \in C$ se, e somente se, $H \cdot w^t = 0$.*

Demonstração: $\Rightarrow$) A geradora de $C^{\perp}$

$$H = \begin{pmatrix} v_1 \\ \vdots \\ v_{n-p} \end{pmatrix}$$

Como cada $v_i \in C^{\perp}$, então, $\langle w, v_i \rangle = 0,\ i \in \{1, ..., n-p\}$. Logo,

$$H.w^t = \begin{pmatrix} \langle v_1, w \rangle \\ \vdots \\ \langle v_{n-p}, w \rangle \end{pmatrix} = \begin{pmatrix} 0 \\ \vdots \\ 0 \end{pmatrix}.$$

$\Leftarrow$) Pode ser utilizada uma demonstração semelhante à volta do item *ii*) do lema 1.28. ■

A matriz H nas condições anteriores é chamada de **matriz teste de paridade** ou **matriz de checagem**.

1.31 Proposição: *Seja $C^{\perp}$ com matriz geradora H, dual de um código linear $C \subset \mathbb{F}_q^n$. O peso de C é maior que ou igual a s se, e somente se, quaisquer $s-1$ colunas de H são LI.*

Demonstração: $\Rightarrow$) Por hipótese, $\omega(C) \geq s$. Suponha, por absurdo, que H tenha $s-1$ colunas LD, $h^{i_1}, ..., h^{i_{s-1}}$. Assim, existem c_i não todos nulos, $i = 1, ..., s-1$, tais que $c_1 h^{i_1} + \cdots + c_{s-1} h^{i_{s-1}} = 0$. A palavra $c = (0, ..., c_1, 0, ..., c_2, ..., c_{s-1}, ...0) \in C$ (pela proposição em 1.30) e $\omega(c) \leq s-1$. Absurdo.
$\Leftarrow$) Por hipótese, quaisquer $s-1$ colunas de H são LI. Suponha, por absurdo, que o peso de C seja menor que s, ou seja, $\omega(C) \leq s-1$. Então, existe $0 \neq c = (c_1, ..., c_n) \in C$ tal que $\omega(c) \leq s-1$. Sejam $h^1, ..., h^n$ as colunas de H. Como $Hc^t = 0$,

$$\begin{pmatrix} 0 \\ \vdots \\ 0 \end{pmatrix} = H.c^t = \sum_{i=1}^{n} c_i h^i = c_1 h^1 \cdots + c_n h^n \tag{1.1}$$

Como $\omega(c)$ é o número de componentes não nulas de c, tem-se na equação (1.1), uma combinação linear não nula de no máximo $s-1$ colunas de H resultando em 0. Absurdo. Logo, o peso de C é maior que ou igual a s. ■

1.32 Teorema: *O peso do código linear C é igual a s se, e somente se, quaisquer $s-1$ colunas de H são LI e existem s colunas de H que sejam LD, em que H é a matriz teste de paridade de C.*

Demonstração: $\Rightarrow$) Por hipótese, o peso de C é s e pela proposição em 1.31, todo $s-1$ conjunto de colunas são LI. Agora, se não se tivesse que existem s colunas LD, ainda por 1.31, teria-se que $\omega(C) \geq s+1$.
$\Leftarrow$) Da proposição em 1.31, $\omega(C) \geq s$. Mas, não pode ser maior, porque então todo conjunto com s colunas seria LI. ■

1.33 Corolário: (Cota de Singleton) *Seja C um código linear com parâmetros $[n, p, d]$. Então, $d \leq n-p+1$.*

Demonstração: Da proposição em 1.23, $d = \omega(C)$. Seja H a matriz teste de paridade de C. Pela proposição em 1.31, $\omega(C) = d \leq s \Leftrightarrow s-1$ colunas de H são LI. Mas, o número máximo de colunas LI é o posto da matriz H, ou seja, sua dimensão. Pela proposição que está em 1.29, $\dim(H) = n-p$. Segue que $s-1 \leq n-p$. Como $d \leq s$, tem-se

$$d \leq n-p+1.$$

■

Os códigos em que $d = n-p+1$ são chamados de **Maximum Distance Separable** (MDS - Separados pela Distância Máxima em tradução livre).

1.5 Exemplos de Códigos Lineares

Os códigos de Hamming constituem uns dos poucos exemplos de códigos perfeitos que existem e, junto com os códigos de Golay[1], formam os únicos não triviais[2] [3, Ch. 6. §10].

1.34 Exemplo: (Código de Hamming) *O **código de Hamming** é o código cuja matriz teste de paridade, H_m de ordem $(m \times 2^m - 1)$, apresenta os elementos de $F_2^m \setminus \{0\}$ dispostos em colunas em qualquer ordem.*

[1] Para mais informações sobre códigos de Golay, veja capítulo 20 de [3].

[2] Os códigos triviais são os códigos de uma palavra apenas, o espaço $\mathbb{F}_q^n$ todo e os códigos de repetição de um código perfeito. As palavras de um código de repetição são do tipo $c = c_1 c_1 ... c_1$ em que c_1 é uma palavra de um código. O código-de-canal da Tabela 1.1 é um código perfeito de repetição induzido pelo código perfeito $\mathbb{F}_2^2$.

Existe maneira de se generalizar o código de Hamming (binário, como descrito anteriormente) para outros corpos [8, p. 202].

1.35 Exemplo: (Código de Reed-Solomon) *Considere o espaço vetorial*

$$K[X]_{p-1} = \{P \in K[X] : gr(P) \leq p-1\} \cup \{0\}.$$

Seja K um corpo e $n \in \mathbb{Z}$, $n \geq p$ e α_1, ..., $\alpha_n \in K$. A imagem da transformação linear injetora

$$\begin{array}{rccc} T: & K[X]_{p-1} & \longrightarrow & K^n \\ & P & \longmapsto & (P(\alpha_1), ..., P(\alpha_n)) \end{array}$$

é o ***Código de Reed-Solomon*** *de comprimento n, dimensão k definido por α_1, ..., α_n.*

1.36 Exemplo: (Código do Mariner 9) *Mariner 9 foi uma sonda enviada pela NASA (agência espacial estadunidense) para tirar fotos de Marte. As fotos foram recebidas em escala de cinza e teve possíveis falhas corrigidas utilizando o código desse exemplo.*

Considere a matriz

$$G = \begin{pmatrix} 1 & 1 \\ H_m & 0 \end{pmatrix},$$

na qual H_m é como no código de Hamming. O código gerado por G é o ***código de Reed-Muller*** *de primeira ordem.*

1.6 Decodificação

O processo de decodificação é uma das partes mais importantes da Teoria dos Códigos, pois é vastamente aplicado, o que cria demanda para seu estudo. No que segue, se $C \subset \mathbb{F}_q^n$ é um código linear com matriz teste de paridade H e $x \in \mathbb{F}_q^n$, chamaremos de **síndrome de x em relação a C**, ou simplesmente **síndrome**, o vetor Hx^t. Vejamos um método de decodificação.

Inicialmente, define-se o vetor erro e como sendo a diferença entre o vetor recebido r e o vetor transmitido c, isto é,

$$e = r - c$$

O peso do vetor e corresponde ao número de erros cometidos durante a transmissão da palavra. Seja H a matriz de teste de paridade do código. Como $Hc^t = 0$, temos que

$$He^t = H(r^t - c^t) = Hr^t - Hc^t = Hr^t$$

Portanto, a palavra recebida e o vetor erro têm a mesma síndrome. Denotemos por h^i a i-ésima coluna de H. Se $e = (\alpha_1, ..., \alpha_n)$, então

$$\sum_{i=1}^{n} \alpha_i h^i = He^t = Hr^t$$

1.37 Lema: *Seja C um código linear em $\mathbb{F}_q^n$ com capacidade de correção κ. Se $r \in \mathbb{F}_q^n$ e $c \in C$ são tais que $\mathrm{d}(c, r) \leq \kappa$, então existe um único vetor e com $\omega(e) \leq \kappa$, cuja síndrome é igual à síndrome de r e tal que $c = r - e$.*

Demonstração: Como $\omega(e) = \mathrm{d}(c, r) \leq \kappa$. Para provar a unicidade, sejam $e = (\alpha_1, ..., \alpha_n)$ e $e' = (\alpha'_1, ..., \alpha'_n)$ tais que $\omega(e) \leq \kappa$ e $\omega(e') \leq \kappa$ e tenham a mesma síndrome que r. Então, se H é a matriz de teste de paridade de C, temos

$$He^t = He'^t \Rightarrow \sum_{i=1}^{n} \alpha_i h^i = \sum_{i=1}^{n} \alpha'_i h^i$$

Esta última, é uma relação de dependência entre $2\kappa (\leq d-1)$ colunas de H. Como quaisquer $d-1$ colunas de H são LI, temos que $\alpha_i - \alpha'_i = 0$, e logo $e = e'$. ■

1.38 Exemplo: *Considere o código com matriz teste de paridade*

$$H = \begin{pmatrix} 1 & 0 & 1 & 0 & 0 \\ 1 & 1 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 & 1 \end{pmatrix}$$

Como, claramente, as colunas são duas a duas LI e $h^1 = h^3 + h^4$, temos que $d = 3$ e $\kappa = 1$. Portanto, para que a correção seja possível, o vetor erro deverá conter no máximo uma entrada não nula.

Seja $r = (1, 0, 1, 0, 0)$ uma palavra recebida. Primeiramente, calculamos sua síndrome.

$$He^t = Hr^t = \begin{pmatrix} 0 \\ 1 \\ 0 \end{pmatrix} = 1 \cdot h^4$$

Procuramos um vetor com apenas uma entrada não nula (igual a 1) tal que $He^t = h^4$ e disto, $e = (0, 0, 0, 1, 0)$. Consequentemente, a palavra enviada foi

$$c = r - e = (1, 0, 1, 1, 0).$$

Seja $C \subset \mathbb{F}_q^n$ um código corretor de erros com matriz teste de paridade H. sejam d a distância mínima de C e $\kappa = \lfloor \frac{d-1}{2} \rfloor$. Seja $v \in \mathbb{F}_q^n$. Defina

$$v + C = \{v + c : c \in C\}$$

1.39 Lema: *Os vetores u e v de $\mathbb{F}_q^n$ têm a mesma síndrome se, e somente se, $u \in v + C$.*

Demonstração: $Hu^t = Hv^t \Leftrightarrow H(u-v)^t = 0 \Leftrightarrow u - v \in C \Leftrightarrow u \in v + C$. ■

1.40 Proposição: *Seja C um $[n, p]$-código linear. Temos que:*

i) $v + C = v' + C \Leftrightarrow v - v' \in C$;

ii) $(v + C) \cap (v' + C) \neq \emptyset \Rightarrow v + C = v' + C$;

iii) $\bigcup\limits_{v \in \mathbb{F}_q^n} (v + C) = \mathbb{F}_q^n$;

iv) $|(v + C)| = |C| = q^p$.

Demonstração: i) $\Rightarrow$) Seja $w \in v + C$. Logo, $w = v + c$, para algum $c \in C$. Como $v + C = v' + C$, $w \in v' + C$ e existe $c' \in C$ tal que $w = v' + c'$. Portanto, $w = v + c = v' + c' \Rightarrow v - v' = c' - c$. Como c, $c' \in C$, que é um subespaço vetorial de $\mathbb{F}_q^n$, temos que $v - v' = c - c' \in C$.

$\Leftarrow$) Por hipótese, $v - v' \in C$. Seja $w \in v + C$. Temos que $w = v + c$, para algum $c \in C$. Então, $w = v' - v' + v + c = v' + \underbrace{(v - v' + c)}_{\in C}$. Assim, $w \in v' + C$. Portanto, $v + C \subset v' + C$. Analogamente, $v' + C \subset v + C$. Portanto, $v + C = v' + C$;

ii) Suponha que exista $w \in (v + C) \cap (v' + C)$. Então, $w = v + c = v' + c'$, para c, $c' \in C$. De $v + c = v' + c'$, temos que $v - v' = c' - c \in C$. Por *i*), $v - v' \in C \Rightarrow v + C = v' + C$;

iii) Seja $v \in \mathbb{F}_q^n$. Então, $v \in v + C$, já que $v = v + 0$. Logo, $\mathbb{F}_q^n = \bigcup\limits_{v \in \mathbb{F}_q^n} \{v\} \subset \bigcup\limits_{v \in \mathbb{F}_q^n} (v + C) \subset \mathbb{F}_q^n$. Segue que $\bigcup\limits_{v \in \mathbb{F}_q^n} (v + C) = \mathbb{F}_q^n$

iv) Considere a aplicação $v : C \to v + C$, $v(c) = v + c$. Essa função é bijetora. De fato, $v(c) = v(c') \Leftrightarrow v + c = v + c' \Leftrightarrow c = c'$, logo é injetora. Agora, seja $w \in v + C$. Tome $c = w - v$. Temos que $v(c) = v + w - v = w$. Portanto, é sobrejetora. Então, $|(v + C)| = |C| = q^p$.

■

Cada conjunto da forma $v+C$ é chamado de **classe lateral** de v segundo C. Fazendo $v' = 0$ em $i)$, $v + C = C \Leftrightarrow v \in C$.

1.41 Exemplo: *Seja C o $[4,2]$-código sobre $\mathbb{F}_2$ gerado pela matriz*

$$G = \begin{pmatrix} 1 & 0 & 1 & 1 \\ 0 & 1 & 0 & 1 \end{pmatrix}$$

Então, C é constituído por $v \cdot G$, com $v \in \{(0,0),(0,1),(1,0),(1,1)\}$, i.e., $C = \{(0,0,0,0),(0,1,0,1),(1,0,1,1),(1,1,1,0)\}$. As classes laterais segundo C são:

$$(0,0,0,0) + C = C$$
$$(1,0,0,0) + C = \{(1,0,0,0),(1,1,0,1),(0,0,1,1),(0,1,1,0)\}$$
$$(0,1,0,0) + C = \{(0,1,0,0),(0,0,0,1),(1,1,1,1),(1,0,1,0)\}$$
$$(0,0,1,0) + C = \{(0,0,1,0),(0,1,1,1),(1,0,0,1),(1,1,0,0)\}$$

Pelo lema em 1.39, existe uma correspondência biunívoca entre as classes laterais e síndromes.

1.42 Definição: *Um vetor de peso mínimo em uma classe lateral é chamado de **elemento líder** dessa clase.*

1.43 Proposição: *Seja C um código linear em $\mathbb{F}_q^n$, com distância mínima d. Se $u \in \mathbb{F}_q^n$ é tal que*

$$\omega(u) \leq \left\lfloor \frac{d-1}{2} \right\rfloor = \kappa,$$

então u é o único elemento líder da sua classe.

Demonstração: Suponhamos u, $v \in \mathbb{F}_q^n$, com $\omega(u)$, $\omega(v) \leq \lfloor \frac{d-1}{2} \rfloor$. Se $u \in v + C$, i.e., $u - v \in C$, então

$$\mathrm{d}(u-v,0) = \omega(u-v) \leq \omega(u) + \omega(v) \leq \left\lfloor \frac{d-1}{2} \right\rfloor + \left\lfloor \frac{d-1}{2} \right\rfloor \leq d-1.$$

Logo $u - v = 0$ e $u = v$. ■

1.44 Algoritmo: *O próximo algoritmo descreve o processo de decodificação de um código linear com matriz teste de paridade H e capacidade de correção κ.*

1) Determine S, conjunto formado por todos os elementos $u \in \mathbb{F}_q^n$ tais que $\omega(u) \leq \kappa$. Calcule as síndromes desses elementos e coloque em uma tabela;

2) Calcule a síndrome $s^t = Hr^t$, com r a palavra recebida;

3) Se s está na tabela, troque r por $r - \ell$, com ℓ o elemento líder da classe determinada por s;

4) Se s não está na tabela, então no envio da mensagem foram cometidos mais do que κ erros.

1.45 Justificativa: *Neste caso, $e = \ell$. Como as síndromes de e e da palavra recebida r são as mesmas, ao se tomar $c = r - \ell$, temos um vetor com síndrome 0, logo palavra do código, com uma correção que não ultrapassa a capacidade de correção do código, pelo peso de ℓ.*

1.46 Exemplo: *Considere o Código de Hamming da matriz teste de paridade H_3.*

$$H_3 = \begin{pmatrix} 1 & 0 & 1 & 0 & 1 & 0 & 1 \\ 0 & 1 & 1 & 0 & 0 & 1 & 1 \\ 0 & 0 & 0 & 1 & 1 & 1 & 1 \end{pmatrix}$$

As palavras que pertencem ao código são todos os vetores v de $\mathbb{F}_2^7$ tais que

$$Hv^t = \begin{pmatrix} 0 \\ 0 \\ 0 \end{pmatrix}$$

Ainda que não seja necessário para o algoritmo de decodificação, mas para fins ilustrativos, tais elementos se encontram na Tabela 1.2.

0000000	0001111	0010110	0011001
0100101	0101010	0110011	0111100
1000011	1001100	1010101	1011010
1100110	1101001	1110000	1111111

Tabela 1.2: Código gerado pela matriz teste de paridade H_3.

Como quaisquer duas colunas são LI e $h_1 + h_2 = h_3$, temos que a distância mínima é $d = 3$, logo $\kappa = 1$. Os elementos de $u \in S$, ou seja, $u \in \mathbb{F}_2^7$ tais que $\omega(u) \leq 1$ são os que contém no máximo uma entrada não nula. Esses elementos e suas síndromes estão na Tabela 1.3.

ℓ	**Síndrome**
0000000	000
0000001	111
0000010	011
0000100	101
0001000	001
0010000	110
0100000	010
1000000	100

Tabela 1.3: Líder de classe e suas síndromes.

Suponhamos que a palavra recebida (que não consta na Tabela 1.2) seja $r = 1111101$. *Sua síndrome é* $H \cdot v = 011$ *e o erro* $e = \ell = 0000010$, *de acordo com a Tabela 1.3. Logo, a palavra corrigida é* $c = r - e = 1111101 - 0000010 = 1111111$ *(que está na tabela 1.2).*

Capítulo 2

Esteganografia

2.1 Protocolos Esteganográficos

Seja s uma mensagem que queremos manter em segredo, x a cobertura onde iremos esconder a mensagem. Podemos assumir que ambas são sequências de símbolos de um corpo finito $\mathbb{F}_q$. Escreva $s = (s_1, ..., s_k) \in \mathbb{F}_q^k$ e $x = (x_1, ..., x_n) \in \mathbb{F}_q^n$.

2.1 Definição: *Sejam $k \leq n$ inteiros. Um **protocolo esteganográfico de imersão/recuperação** do tipo $[k, n]$ sobre $\mathbb{F}_q$ é um par de aplicações $\mathscr{S} = (\mathrm{e}, \mathrm{r})$, $e : \mathbb{F}_q^k \times \mathbb{F}_q^n \to \mathbb{F}_q^n$, $\mathrm{r} : \mathbb{F}_q^n \to \mathbb{F}_q^k$ tal que $\mathrm{r}(\mathrm{e}(s, x)) = s$, para todo $s \in \mathbb{F}_q^k$, $x \in \mathbb{F}_q^n$. As aplicações* e *e* r *são chamadas de **imersão** e **aplicação de recuperação**, respectivamente. O número $\rho = max\{\mathrm{d}(x, \mathrm{e}(s, x)) : s \in \mathbb{F}_q^k, x \in \mathbb{F}_q^n\}$ é o chamado **raio do protocolo**.*

Uma aplicação de imersão de um protocolo esteganográfico com raio ρ (um $[k, n, \rho]$ protocolo) permite esconder k símbolos de informações em um vetor de tamanho n trocando, no máximo ρ dos símbolos da cobertura.

2.2 Definição: *O protocolo é dito ser **próprio** se $e(s, x)$ é o elemento mais próximo a x no conjunto $\mathrm{r}^{-1}(s) = \{y \in \mathbb{F}_q^n : \mathrm{r}(y) = s\}$.*

2.3 Exemplo: *Considere o processo LSB aplicado a uma imagem. Se cada pixel é representado por h bits, podemos considerar que a cobertura é a imagem inteira; o protocolo (para cada pixel) é o par de aplicações $\mathscr{S} = (\mathrm{e}, \mathrm{r})$, com*

$$\begin{array}{rccc} \mathrm{e}: & \mathbb{F}_2 \times \mathbb{F}_2^h & \longrightarrow & \mathbb{F}_2^h \\ & (s, (x_1, ..., x_{h-1}, x_h)) & \longmapsto & (x_1, ..., x_{h-1}, s) \end{array}$$

$$\begin{array}{rccc} \mathrm{r}: & \mathbb{F}_2^h & \longrightarrow & \mathbb{F}_2 \\ & (y_1, ..., y_h) & \longmapsto & y_h \end{array}$$

Como escondemos 1 *bit de informação em uma parte da cobertura de tamanho* h *e alteremos sempre no máximo* 1 *desses* h *elementos, temos um* $[1, h, 1]$ *protocolo.*

Alternativamente, podemos ver a cobertura como sendo o conjunto de todos os bits menos significantes (os últimos, em geral). Neste caso, o par de aplicações seria

$$\begin{array}{rccc} \mathrm{e}: & \mathbb{F}_2 \times \mathbb{F}_2 & \longrightarrow & \mathbb{F}_2 \\ & (s, x) & \longmapsto & s \end{array}$$

$$\begin{array}{rccc} \mathrm{r} = id: & \mathbb{F}_2 & \longrightarrow & \mathbb{F}_2 \\ & y & \longmapsto & y \end{array}$$

Neste caso, seria um $[1, 1, 1]$ *protocolo.*

Algo que podemos considerar em um protocolo $\mathscr{S} = (\mathrm{e}, \mathrm{r})$ é a chamada **média de símbolos modificados** $\alpha = \alpha(\mathscr{S})$. Para calculá-la, consideramos a soma do número de modificações ao se esconder cada segredo em cada possibilidade da cobertura. Se for um $[k, n]$ protocolo sobre $\mathbb{F}_q$, a média é dada por

$$\alpha(\mathscr{S}) = \frac{1}{q^{kn}} \sum_{s \in \mathbb{F}_q^k} \sum_{x \in \mathbb{F}_q^n} \mathrm{d}(x, \mathrm{e}(s, x))$$

Alguns parâmetros relativos a um protocolo são:

- A **capacidade relativa** k/n, que mede os símbolos imersos por símbolo da cobertura;
- A **distorção média** (ou taxa de mudança) ρ/n, que que mede a probabilidade de que determinado símbolo na cobertura seja alterado durante o processo de imersão;
- A **eficiência da imersão**, que é a razão entre a média dos símbolos modificados e a taxa de mudança.

Quanto maior a capacidade relativa, mais informação podemos esconder na cobertura; quanto menor a distorção média, menos alterações fazemos durante a imersão. Um bom protocolo possui duas propriedades principais:

- Algoritmos eficientes para imersão e recuperação;
- Bons parâmetros, i.e., capacidade relativa grande e distorção média pequena.

2.2 Algoritmo F5

O algoritmo F5 foi desenvolvido por Westfeld [10]. Permite esconder k bits de informação em 2^k-1 bits da cobertura alterando no máximo 1 bit, ou seja, é um protocolo do tipo $[k, 2^k-1, 1]$. No que segue, $\langle x\rangle_2$ denota a expressão binária de x e, analogamente, $\langle y\rangle_{10}$ é a forma decimal de y. O i-ésimo vetor da base canônica de $\mathbb{F}_2^{2^k-1}$ é denotado por e_i e $e_0 = 0$.

Considere a aplicação (com soma vetorial em $\mathbb{F}_2$)

$$\begin{array}{rccc} \eta: & \mathbb{F}_2^k \times \mathbb{F}_2^{2^k-1} & \longrightarrow & \mathbb{N} \\ & (s,x) & \longmapsto & \left\langle s + \sum_{i=1}^{2^k-1} x_i \langle i\rangle_2 \right\rangle_{10} \end{array}$$

As aplicações de imersão e recuperação são:

$$\begin{array}{rccc} \mathrm{e}: & \mathbb{F}_2^k \times \mathbb{F}_2^{2^k-1} & \longrightarrow & \mathbb{F}_2^{2^k-1} \\ & (s,x) & \longmapsto & x + e_{\eta(s,x)} \end{array}$$

$$\begin{array}{rccc} \mathrm{r}: & \mathbb{F}_2^{2^k-1} & \longrightarrow & \mathbb{F}_2^k \\ & y & \longmapsto & \sum_{i=1}^{2^k-1} y_i \langle i\rangle_2 \end{array}$$

Vejamos que $\mathscr{S} = (\mathrm{e}, \mathrm{r})$ é realmente um protocolo esteganográfico. Observe que r é linear. De fato, se u, $v \in \mathbb{F}_2^{2^k-1}$ e $\alpha \in \mathbb{F}_2$, então, escrevendo $u = (u_1, u_2, ..., u_{2^k-1})$, $v = (v_1, v_2, ..., v_{2^k-1})$, temos:

$$\mathrm{r}(u+\alpha v) = \mathrm{r}((u_1+\alpha v_1, u_2+\alpha v_2, ..., u_{2^k-1}+\alpha v_{2^k-1})) = \sum_{i=1}^{2^k-1} (u_i+\alpha v_i)\langle i\rangle_2 =$$

$$\sum_{i=1}^{2^k-1} u_i\langle i\rangle_2 + \alpha \sum_{i=1}^{2^k-1} v_i\langle i\rangle_2 = r(u) + \alpha \mathrm{r}(v)$$

Então,

$$\mathrm{r}(\mathrm{e}(s,x)) = \mathrm{r}(x + e_{\eta(s,x)}) = \mathrm{r}(x) + \mathrm{r}(e_{\eta(s,x)}) = \sum_i x_i\langle i\rangle_2 + \langle \eta(s,x)\rangle_2 \quad (2.1)$$

Como $\eta(s,x) = \left\langle s + \sum x_i\langle i\rangle_2 \right\rangle_{10}$, temos $\langle \eta(s,x)\rangle_2 = s + \sum x_i\langle i\rangle_2$. Substituindo na equação (2.1):

$$\mathrm{r}(\mathrm{e}(s,x)) = \sum_i x_i\langle i\rangle_2 + s + \sum x_i\langle i\rangle_2 = s + 2\sum x_i\langle i\rangle_2 = s$$

2.4 Exemplo: *Suponha que queiramos esconder o segredo* $s = 011$ *dentro da cobertura* $x = 1010100$.

$$\eta(s,x) = \eta(011, 1010100) = \left\langle s + \sum_{i=1}^{7} x_i \langle i \rangle_2 \right\rangle_{10} =$$

$$\left\langle 011 + 1\cdot 001 + 0\cdot 010 + 1\cdot 011 + 0\cdot 100 + 1\cdot 101 + 0\cdot 110 + 0\cdot 111 \right\rangle_{10} = \langle 100 \rangle_{10} = 4$$

Portanto, $e_{\eta(s,x)} = 0001000$ *e daí,* $\mathrm{e}(s,x) = 1010100 + 0001000 = 1011100$.

Agora,

$$\mathrm{r}(\mathrm{e}(s,x)) = \mathrm{r}(1011100) = \sum_{i=1}^{7} y_i \langle i \rangle_2$$

$$1 \cdot 001 + 0 \cdot 010 + 1 \cdot 011 + 1 \cdot 100 + 1 \cdot 101 + 0 \cdot 110 + 0 \cdot 111 = 011 = s.$$

Capítulo 3

Códigos e Esteganografia

Para construir um protocolo, precisamos de um par de aplicações e e r tais que $\mathrm{r}(\mathrm{e}(s,x)) = s$. No caso do protocolo F5, a aplicação de recuperação é mais simples que a de imersão. Em geral, dada uma aplicação de recuperação, podemos construir uma aplicação de imersão associada que satisfaça a condição citada.

3.1 Construção de Protocolos

Seja $Y \subseteq \mathbb{F}_q^n$ e $\mathrm{d}(x,Y) := \min\{\mathrm{d}(x,y) : y \in Y\}$.

3.1 Lema: *Seja $\mathscr{S} = (e,r)$ um $[k,n,\rho]$ protocolo sobre $\mathbb{F}_q$. Então, existe um protocolo próprio $\mathscr{S}' = (e',r)$ do tipo $[k,n,\rho']$ tal que $\rho' \leq \rho$.*

Demonstração: Tome e′ como a aplicação de decodificação por distância mínima do código (subconjunto de $\mathbb{F}_q^n$) $\mathrm{r}^{-1}(s)$. Como $\mathrm{e}(s,x)$ e $\mathrm{e}'(s,x) \in \mathrm{r}^{-1}(s)$, mas e' foi tomado como distância mínima, temos $\mathrm{d}(x,\mathrm{e}'(s,x)) \leq \mathrm{d}(x,\mathrm{e}(s,x))$. O resultado segue com a definição em 2.2. ■

A próxima proposição mostra como uma aplicação de recuperação pode ser facilmente obtida.

3.2 Proposição: *Uma aplicação $\mathrm{r} : \mathbb{F}_q^n \to \mathbb{F}_q^k$ é aplicação de recuperação de um $[k,n]$ protocolo $\mathscr{S} = (\mathrm{e},\mathrm{r})$ se, e somente se, for sobrejetora. Se este protocolo for próprio, então seu raio é*

$$\rho = \max\{\mathrm{d}(x,\mathrm{r}^{-1}(s)) : x \in \mathbb{F}_q^n,\ s \in \mathbb{F}_q^k\}$$

Demonstração: $\Rightarrow$) Seja $s \in \mathbb{F}_q^k$. Como $\mathrm{r}(\mathrm{e}(s,x)) = s$, para qualquer $x \in \mathbb{F}_q^n$, seque que r é sobrejetora.

$\Leftarrow$) Se r é sobrejetora, para todo $s \in \mathbb{F}_q^k$, o conjunto $\mathrm{r}^{-1}(s)$ é não vazio. Coloque $\mathrm{e}(s,x) = y$, para algum $y \in \mathrm{r}^{-1}(s)$. Então, $\mathrm{r}(\mathrm{e}(s,x)) = \mathrm{r}(y) = s$.

No caso de o protocolo ser próprio, então $\mathrm{e}(x,s)$ é o elemento mais próximo a x em $\mathrm{r}^{-1}(s)$, ou seja, $\mathrm{d}(x,\mathrm{e}(s,x)) = \mathrm{d}(x,r^{-1}(s))$ (lembre que $\mathrm{e}(s,x) \in \mathrm{r}^{-1}(s)$). Logo,

$$\begin{aligned} \rho &= \max\{d(x,e(s,x)) : x \in \mathbb{F}_q^n,\, s \in \mathbb{F}_q^k\} \\ &= \max\{d(x,r^{-1}(s)) : x \in \mathbb{F}_q^n,\, s \in \mathbb{F}_q^k\} \end{aligned}$$

■

3.3 Corolário: *Os parâmetros $[k,n,\rho]$ de um protocolo definido sobre o $\mathbb{F}_q$ satisfazem $q^k \leq V_q(n,\rho)$ (veja a observação que está em 1.10).*

Demonstração: De acordo com o lema em 3.1, basta provar para protocolos próprios. Tome x em $\mathbb{F}_q^n$. Para todo $s \in \mathbb{F}_q^k$, existe $y \in B(x,\rho)$ tal que $r(y) = s$, logo $\#B(x,\rho) \geq \#\mathbb{F}_q^k = q^k$. ■

Esta cota é conhecida como **cota de Hamming esteganográfica**. Protocolos nos quais vale a igualdade são chamados de **protocolos perfeitos**.

Dada uma aplicação de recuperação, podemos construir a aplicação de imersão e utilizando a teoria de códigos. Associado ao protocolo $\mathscr{S} = (\mathrm{e},\mathrm{r})$, podemos considerar a família de códigos corretores de erro $\mathscr{F}_{\mathscr{S}} := (C_s = \mathrm{r}^{-1}(s) : s \in \mathbb{F}_q^k)$. Como $\mathrm{r}(\mathrm{e}(s,x)) = s$ e $\mathrm{e}(s,x) \in \mathrm{r}^{-1}(s)$, então e é a aplicação de decodificação da palavra x com respeito ao código corretor-de-erro $\mathrm{r}^{-1}(s)$. Quando o protocolo é próprio, $\mathrm{e}(s,x)$ é o elemento mais próximo à palavra x no conjunto $\mathrm{r}^{-1}(s)$ assim, o método de decodificação coincide com correção por distância mínima. Como resultado da proposição em 3.4 segue que a família de códigos como descrita forma uma partição[1] para $\mathbb{F}_q^n$.

3.4 Proposição: *Seja $\mathscr{S} = (\mathrm{e},\mathrm{r})$ um $[k,n]$-protocolo próprio. Se para cada $s \in \mathbb{F}_q^k$ considerarmos $C_s = \{x \in \mathbb{F}_q^n : \mathrm{r}(x) = s\}$, então a família $\mathscr{F}_{\mathscr{S}} = \{C_s : s \in \mathbb{F}_q^k\}$ forma uma partição para $\mathbb{F}_q^n$. Além disto, para todo $s \in \mathbb{F}_q^k$, a aplicação $\mathrm{dec}_s : \mathbb{F}_q^n \to C_s$ definida por $\mathrm{dec}_s(x) = \mathrm{e}(s,x)$ é uma aplicação de decodificação para código C_s.*

Demonstração: Como $\mathrm{r}(\mathrm{e}(s,x)) = s$, $C_s \neq \emptyset$, para qualquer $s \in \mathbb{F}_q^k$. Se $x \in C_s \cap C_{s'}$, então $\mathrm{r}(x) = s$ e $\mathrm{r}(x) = s'$. Como $\mathscr{S}$ é um protocolo, r está bem definida e $s = s'$. Pela proposição em 3.2, r é sobrejetora e logo, para $x \in \mathbb{F}_q^n$, temos $\mathrm{r}(x) = s$, para algum $s \in \mathbb{F}_q^k$ e portanto $x \in C_s$. ■

[1] Uma família $Y_1,...,Y_t \subseteq Y$ forma uma partição em Y se $Y_i \neq \emptyset$ para $1 \leq i \leq t$, os conjuntos são disjuntos dois a dois e se $y \in Y$, existe j tal que $y \in Y_j$.

3.5 Proposição: *Seja* $\{C_s : s \in \mathbb{F}_q^k\}$ *uma família de códigos que formam uma partição para* $\mathbb{F}_q^n$. *Para cada* $s \in \mathbb{F}_q^k$, *seja* dec_s *a decodificação por distância mínima para o código* C_s. *Considere as aplicações* $\mathrm{e} : \mathbb{F}_q^k \times \mathbb{F}_q^n \to \mathbb{F}_q^n$ *e* $\mathrm{r} : \mathbb{F}_q^n \to \mathbb{F}_q^k$ *definidas por* $\mathrm{e}(s,x) = \mathrm{dec}_s(x)$ *e* $\mathrm{r}(x) = s$ *se* $x \in C_s$. *Nestas condições,* $\mathscr{S} = (\mathrm{e}, \mathrm{r})$ *é* $[k,n]$*-protocolo próprio sobre* $\mathbb{F}_q$.

Demonstração: Como $\mathrm{dec}_s(x) \in C_s$, temos que $\mathrm{r}(\mathrm{e}(s,x)) = s$. Além do mais, $\mathrm{d}(x, \mathrm{e}(s,x)) = \mathrm{d}(x, \mathrm{dec}_s(x)) = \mathrm{d}(x, C_s)$, o que prova que o protocolo é próprio. ■

Utilizando estes resultados, podemos construir um protocolo esteganográfico da seguinte maneira:

1) Fixe uma aplicação de recuperação $\mathrm{r} : \mathbb{F}_q^n \to \mathbb{F}_q^k$ e considere a respectiva família[2] de códigos $\mathscr{F}_{\mathscr{S}} = (C_s = \mathrm{r}^{-1}(s) : s \in \mathbb{F}_q^k)$;

2) Para $s \in \mathbb{F}_q^k$, a aplicação de imersão e será a decodificação por distância mínima para o código $\mathrm{r}^{-1}(s)$.

3.6 Justificativa: *: Como* $\mathrm{e}(s,x) \in \mathrm{r}^{-1}(s)$ *(pela correção por distância mínima para um elemento de* $\mathrm{r}^{-1}(s)$*), temos que* $\mathrm{r}(\mathrm{e}(s,x)) = s$. *Note que poderíamos escolher* $\mathrm{e}(s,x)$ *como qualquer palavra em* $\mathrm{r}^{-1}(s)$. *A unicidade, no caso de protocolos, não é importante, apesar de o ser para a teoria dos códigos corretores de erros.*

Apesar da liberdade de poder escolher entre qualquer elemento de $\mathrm{r}^{-1}(s)$, tomamos o mais próximo de x para alterar pouco a cobertura, o que dificulta a detecção do envio da mensagem. Um protocolo construído como descrito é chamado de **protocolo baseado em códigos**. Esta construção é conhecida como **matriz de imersão**, apesar do fato de que alguns autores preferem não utilizar este termo, pois podemos não utilizar matriz alguma. O exemplo F5 como mostrado não precisou de matriz, mas podemos construir o mesmo protocolo utilizando tal recurso.

3.7 Exemplo: *No que segue,* H_3 *denota o código de Hamming de dimensão 3. Suponha que tenhamos uma aplicação de recuperação* r *como no F5 e queiramos encontrar a aplicação de imersão. Os elementos da família de*

[2]Por abuso de notação, nos referimos a $\mathscr{S}$ antes de tê-lo construído, efetivamente.

códigos são.

$$\begin{aligned} \mathrm{r}^{-1}(011) &= \{1011100, 0010000, 0011111, 0000110, \\ &\quad 0001001, 0110101, 0111010, 0100011, \\ &\quad 0101100, 1010011, 1000101, 1001010, \\ &\quad 1110110, 1111001, 1100000, 1101111\} = 0010000 + H_3 \end{aligned}$$

$$\begin{aligned} \mathrm{r}^{-1}(000) &= H_3 \\ \mathrm{r}^{-1}(001) &= 1000000 + H_3 \\ \mathrm{r}^{-1}(010) &= 0100000 + H_3 \\ \mathrm{r}^{-1}(100) &= 0001000 + H_3 \\ \mathrm{r}^{-1}(101) &= 0000100 + H_3 \\ \mathrm{r}^{-1}(110) &= 0000010 + H_3 \\ \mathrm{r}^{-1}(111) &= 0000001 + H_3 \end{aligned}$$

Note que apenas $\mathrm{r}^{-1}(000)$ *é linear - os outros são classes laterais. Suponha que queiramos esconder* $s = 011$ *em* $x = 1010100$*, como no exemplo em 2.4. Veja que em* $\mathrm{r}^{-1}(011)$*, a palavra mais próxima (distância mínima em* $\mathrm{r}^{-1}(011)$*) a* 1010100 *é* 1011100*. Tomamos* $\mathrm{e}(s, x) = 1011100$ *(na verdade, como está na justificativa em 3.6, poderíamos ter escondido* 011 *em* 1010100 *como* 1011100*, ou* 001000*, ou qualquer outra palavra de* $0010000 + H_3$*).*

Mais ainda, a recuperação de qualquer $y \in \mathrm{r}^{-1}(s)$ *coincide com o cálculo da síndrome* $H_3 \cdot y^t$*, com a seguinte ordenação para* H_3*:*

$$H_3 = \begin{pmatrix} 0 & 0 & 0 & 1 & 1 & 1 & 1 \\ 0 & 1 & 1 & 0 & 0 & 1 & 1 \\ 1 & 0 & 1 & 0 & 1 & 0 & 1 \end{pmatrix}$$

3.2 Protocolos Esteganográficos Lineares

O exemplo explicitado em 3.7 nos induz a considerar o caso em que r é linear.

3.8 Definição: *Um protocolo esteganográfico* $\mathscr{S} = (\mathrm{e}, \mathrm{r})$ *é dito* ***linear*** *se a aplicação* r *o for.*

3.9 Proposição: *Se* $\mathscr{S} = (\mathrm{e}, \mathrm{r})$ *é um* $[k, n]$*-protocolo esteganográfico linear, então* $\mathscr{C} = \mathrm{r}^{-1}(0)$ *é um código linear. Os outros códigos* $C = \mathrm{r}^{-1}(s)$*,* $s \in \mathbb{F}_q^k$*, são classes laterais.*

Demonstração: Pela definição de código linear, precisamos provar que C_0 é um subespaço de $\mathbb{F}_q^n$. Por hipótese, r é linear. Se $\beta \in \mathbb{F}_q$, u e $v \in C_0$, então $\mathrm{r}(u) = \mathrm{r}(v) = 0$ e $r(u + \beta v) = \mathrm{r}(u) + \mathrm{r}(\beta v) = \mathrm{r}(u) + \beta r(v) = 0 + 0 = 0$. Segue que $u + \beta v \in C_0$, daí C_0 é um código linear.

Dado $s \in \mathbb{F}_q^k$, considere o código $C = \mathrm{r}^{-1}(s)$. Seja $u \in C$ fixo e $v \in C$ qualquer e vejamos que $C = u + C_0$. Temos $\mathrm{r}(u) = \mathrm{r}(v) = s$. Logo, $\mathrm{r}(u - v) = 0$ e $u - v \in C_0$, portanto $C \subseteq u + C_0$. Por outro lado, se $y \in u + C_0$, então $y = u + c$, com $\mathrm{r}(c) = 0$ e $\mathrm{r}(y) = \mathrm{r}(u) + \mathrm{r}(c) = \mathrm{r}(u) = s$. Segue que $u + C_0 \in C = \mathrm{r}^{-1}(s)$. ■

3.10 Definição: *O código $C_0 = \mathrm{r}^{-1}(0)$ associado a um $[k, n]$-protocolo esteganográfico linear $\mathscr{S} = (\mathrm{e}, \mathrm{r})$ é chamado de* ***código principal*** *associado a $\mathscr{S}$ e denotado por $C_{\mathscr{S}}$. Uma matriz R de* r *(que é tal que $\mathrm{r}(x) = Rx^t$ para qualquer $x \in \mathbb{F}_q^n$, existe pois* r *é linear entre subespaços de dimensão finita e é matriz teste de paridade de $C_{\mathscr{S}}$) é chamada de* ***matriz de recuperação*** *de $\mathscr{S}$.*

No exemplo em 3.7 a matriz de recuperação é H_3 como descrita.

3.11 Proposição: *Seja C um $[n, n-k]$-código e R uma matriz teste de paridade de C. Seja* r *a aplicação cuja matriz é R. Então,* r *é aplicação de recuperação de um $[n, k, \rho]$-protocolo próprio, com ρ o raio de cobertura do código C.*

Demonstração: Como r é sobrejetora (pois R é matriz teste de paridade), de acordo com o lema em 3.1 e a proposição em 3.2, podemos construir um $[k, n]$-protocolo próprio $\mathscr{S}$. Além disso, $C_{\mathscr{S}} = C$ (pela construção sobre a matriz teste de paridade) e por consequência para todo $s \in \mathbb{F}_q^k$, temos $C_s = y_s + C$, com y_s um elemento fixo de $\mathrm{r}^{-1}(s)$. Vamos calcular o raio $\mathscr{S}$. Pela proposição em 3.2,

$$\begin{aligned} \rho(\mathscr{S}) &= \max\{\mathrm{d}(x, \mathrm{r}^{-1}(s)) : x \in \mathbb{F}_q^n,\ s \in \mathbb{F}_q^k\} \\ &= \max\{\mathrm{d}(x, y_s + C) : x \in \mathbb{F}_q^n,\ s \in \mathbb{F}_q^k\} \end{aligned}$$

Para $s \in \mathbb{F}_q^k$, seja $\rho_s = \max\{\mathrm{d}(x, y_s + C) : x \in \mathbb{F}_q^n\} = \mathrm{d}(x, y_s + c)$, para algum $c \in C$. Como a distância de Hamming é invariante pela translação, $\rho_s = \mathrm{d}(x, y_s + c) = \mathrm{d}(x - y_s, c) \leq \rho_0$; analogamente $\rho_0 \leq \rho_s$. Portanto, $\rho_s = \rho_0$. Finalmente, note que $\rho(\mathscr{S}) = \rho_0 = \max\{\mathrm{d}(x, C) : x \in \mathbb{F}_q^n\}$, que é o raio de cobertura do código C. ■

Pelos resultados anteriores, para construir um protocolo linear, podemos considerar matrizes teste de paridade de códigos lineares, obter r e tomar e como decodificação do código por distância mínima.

3.12 Algoritmo: *Dada uma matriz teste de paridade R de ordem $k \times n$ com posto tão grande quanto possível, temos uma aplicação de recuperação* r*, a distância mínima d do código associado (ver teorema em 1.32) e κ a capacidade de correção. Queremos construir a aplicação de imersão para $s \in \mathbb{F}_q^k$ e $x \in \mathbb{F}_q^n$.*

1) Defina $t := \mathrm{r}(x)$*;*

2) Coloque $c := x - \ell_t$*, com* ℓ_t *o elemento de menor peso da classe em que* t *está em relação ao código;*

3) Defina $\mathrm{e}(s, x) := \ell_s + c$*.*

3.13 Justificativa: *Como* r *é linear,* $\mathrm{r}(\mathrm{e}(s,x)) = \mathrm{r}(\ell_s + c) = \mathrm{r}(\ell_s) + \mathrm{r}(c) = s + \mathrm{r}(x - \ell_t) = s + \mathrm{r}(x) - \mathrm{r}(\ell_t) = s + \mathrm{r}(x) - \mathrm{r}(x) = s$*.*

Apesar de termos escolhido decodificação por distância mínima, a aplicação de imersão poderia ser tomada segundo qualquer método de decodificação para códigos lineares.

3.14 Exemplo: *Considere a matriz de checagem*

$$R = \begin{pmatrix} 0 & 0 & 0 & 1 & 1 & 1 & 1 \\ 0 & 1 & 1 & 0 & 0 & 1 & 1 \\ 1 & 0 & 1 & 0 & 1 & 0 & 1 \end{pmatrix}$$

Defina a aplicação de recuperação $\mathrm{r} : \mathbb{F}_2^7 \to \mathbb{F}_2^3$ *por* $\mathrm{r}(y) = R \cdot y^t$*. Temos que* r *é sobrejetora e logo, pela proposição em 3.2, é aplicação de recuperação de algum protocolo* $\mathscr{S} = (\_, \mathrm{r})$*. Vamos construir a aplicação de imersão. Considere a família de códigos* $\mathscr{F} = \{C_s : C_s = \mathrm{r}^{-1}(s),\ \text{para } s \in \mathbb{F}_2^3\}$*. Defina* $\mathrm{e} : \mathbb{F}_2^3 \times \mathbb{F}_2^7 \to \mathbb{F}_2^7$ *por* $\mathrm{e}(s,x) = y$*, com* $y \in \mathrm{r}^{-1}(s) \subset \mathbb{F}_2^7$ *tal que* $\mathrm{d}(x, \mathrm{r}^{-1}(s)) = \mathrm{d}(x,y)$*.*

Neste caso, se quisermos esconder $s = 011$ *em* 1010100 *teremos que* $\mathrm{e}(s,x) = 1011100$*.*

3.15 Lema: *Seja* $\mathscr{S} = (\mathrm{e}, \mathrm{r})$ *um* $[k,n]$*-protocolo próprio sobre* $\mathbb{F}_q$ *associado ao código* C*. Então,* $\alpha(\mathscr{S}) = \dfrac{1}{q^n} \displaystyle\sum_{x \in \mathbb{F}_q^n} \mathrm{d}(x, C)$*.*

Demonstração: Como $\mathrm{d}(x, \mathrm{e}(s,x)) = \mathrm{d}(x, \ell_s + C) = \mathrm{d}(x - \ell_s, C)$, temos

$$\sum_{x \in \mathbb{F}_q^n} \mathrm{d}(x, \mathrm{e}(s,x)) = \sum_{x \in \mathbb{F}_q^n} \mathrm{d}(x, \ell_s + C) = \sum_{y \in \mathbb{F}_q^n} \mathrm{d}(y, C)$$

Disto,

$$\alpha(\mathscr{S}) = \frac{1}{q^{k+n}} \sum_{s \in \mathbb{F}_q^k} \sum_{x \in \mathbb{F}_q^n} \mathrm{d}(x, \mathrm{e}(s,x)) = \frac{1}{q^{k+n}} \sum_{s \in \mathbb{F}_q^k} \sum_{y \in \mathbb{F}_q^n} \mathrm{d}(y, C)$$

Veja que a parte $\displaystyle\sum_{y \in \mathbb{F}_q^n} \mathrm{d}(y, C)$ independe de s para cada $s \in \mathbb{F}_q^k$ e portanto,

$$\alpha(\mathscr{S}) = \frac{1}{q^{k+n}} \left(\underbrace{\sum_{y \in \mathbb{F}_q^n} \mathrm{d}(y, C) + \cdots + \sum_{y \in \mathbb{F}_q^n} \mathrm{d}(y, C)}_{q^k \text{ vezes}} \right) = \frac{1}{q^n} \sum_{y \in \mathbb{F}_q^n} \mathrm{d}(y, C)$$

■

3.16 Proposição: *Seja $\mathscr{S} = (\mathrm{e}, \mathrm{r})$ um $[k, n]$-protocolo próprio sobre $\mathbb{F}_q$ associado ao código $\mathscr{S}$. Para $i = 0, ..., n$, seja α_i o número de líderes com peso i com respeito ao código C. Então, $\alpha(\mathscr{S}) = \dfrac{1}{q^k} \displaystyle\sum_{i=1}^{n} i\alpha_i$.*

Demonstração: Tome $x \in \mathbb{F}_q^n$. Então $x \in \ell_s + C$, para algum $s \in \mathbb{F}_q^k$. Assim, $\mathrm{d}(x, C) = \omega(\ell_s)$, pois cada palavra na classe $\ell_s + C$ está a uma mesma distância do código. As q^n palavras de $\mathbb{F}_q^n$ estão igualmente distribuídas em q^k classes, cada uma originada de uma palavra de $\mathbb{F}_q^k$, logo cada classe lateral do código contém q^{n-k} palavras.

$$\sum_{y \in \mathbb{F}_q^n} \mathrm{d}(y, C) = q^{n-k} \sum_{y \in \mathbb{F}_q^n / C} \mathrm{d}(y, C) = q^{n-k} \sum_{i=1}^{n} i\alpha_i$$

Substituindo em no lema anterior, temos o resultado[3]. ■

3.3 Códigos de Grupos

Conforme visto, ao se trabalhar com esteganografia, precisamos lidar com q^k códigos e suas respectivas aplicações de decodificação simultaneamente. O caso em que os códigos da família podem ser descritos como classes laterais de um código principal simplifica o estudo. Esta seção visa mostrar uma situação geral na qual essas condições ocorrem.

Vamos generalizar os conceitos relativos a classes em um código. Assuma que o alfabeto A é um grupo abeliano finito. Então, o produto direto A^n também é abeliano. Denote por $\star$ ambas as operações de A e A^n. Dado um elemento $x \in A^n$ e um conjunto $Y \subset A^n$, escrevemos $x \star Y = \{x \star y : y \in Y\}$.

[3] O somatório não precisa começar do 0 pois o peso da palavra líder de uma das classes é 0; a saber, a classe $0 + C = C$.

3.17 Lema: *Se A é um grupo abeliano então a distância de Hamming em A^n é invariante por translação, isto é,* $\mathrm{d}(x,y) = \mathrm{d}(x \star z, y \star z)$, *para todo* $x, y, z \in A^n$. *Como consequência, dado um subconjunto C de A^n, temos que* $\mathrm{d}(x, z \star C) = \mathrm{d}(x \star z^{-1}, C)$.

Demonstração: Sejam $x = (x_1, ..., x_n)$, $y = (y_1, ..., y_n)$, $z = (z_1, ..., z_n) \in A$. Logo, $d(x,y) = \#\{i : x_i \neq y_i\}$. Agora,

$$d(x \star z, y \star z) = \#\{i : x_i \star z_i \neq y_i \star z_i\} \tag{3.1}$$

Aplicando a lei do cancelamento em grupos abelianos para cada z_i na equação (3.1), vem que

$$\#\{i : x_i \star z_i \neq y_i \star z_i\} = \#\{i : x_i \neq y_i\} = \mathrm{d}(x,y)$$

A igualdade final é consequência imediata. ■

3.18 Definição: *Seja $C \subset A^n$ um código com q^{n-k} elementos, também um subgrupo de A^n. Dizemos que C é* ***código de grupo****.*

Considere o quociente A^n/C, cujas q^k classes possuem q^{n-k} elementos cada, $\mathscr{R} = \{z_1, ..., z_{q^k}\}$ formado por um representante de cada classe, com $z_1 \in C$. Então, $A^n/C = \{z_1 \star C, ..., z_{q^k} \star C\}$.

3.19 Proposição: *Seja C um subgrupo de A^n e $z \in A^n$. Se* dec *é uma aplicação de decodificação para C, então a aplicação $x \mapsto z \star \mathrm{dec}(x \star z^{-1})$ é uma aplicação de decodificação para $z \star C$.*

Demonstração: Tome $x \in A^n$. Como $z \star \mathrm{dec}_C(x \star z^{-1}) \in z \star C$, a aplicação está bem definida. Seja $y \in z \star C$ com a forma $y = z \star c$, para algum $c \in C$. Se $\mathrm{d}(x,y) < \mathrm{d}(x, z \star \mathrm{dec}(x \star z^{-1}))$, pelo lema em 3.17 temos que $\mathrm{d}(x \star z^{-1}, c) < \mathrm{d}(x \star z^{-1}, \mathrm{dec}(x \star z^{-1}))$, o que contraria o fato de dec ser aplicação de decodificação para C. ■

Para construir um protocolo esteganográfico, considere a aplicação bijetora $\mathrm{rec} : A^n/C \to A^k$ e estenda para $\mathrm{r} : A^n \to A^k$, $\mathrm{r} = \mathrm{rec} \circ \pi$, com $\pi : A^n \to A^n/C$ a projeção canônica. O protocolo obtido é do tipo $[k, n]$ e as aplicações de imersão e recuperação são $\mathrm{e}(s,x) = \mathrm{dec}_s(x) = z \star \mathrm{dec}(c \star z^{-1})$, com $z \in \mathrm{r}^{-1}(s)$ decodificação para C e $\mathrm{r} = \mathrm{rec}$.

3.20 Definição: *Para um subconjunto $Y \subset A^n$, o* ***raio médio*** *de Y é a média das distâncias de um vetor de A^n até Y, isto é*

$$\tilde{\rho}(Y) = \frac{1}{q^n} \sum_{x \in A^n} \mathrm{d}(x, Y)$$

Da definição de raio de cobertura, $\tilde{\rho} \leq \rho$.

3.21 Lema: *Se C é um código de grupo, então todas as classes $z \star C$ possuem o mesmo raio de cobertura e raio médio.*

Demonstração: Como $\rho = \max\{d(x, z \star C) : x \in A^n\}$, temos, pelo lema em 3.17 que $\rho = \max\{\mathrm{d}(x \star z^{-1}, C) : x \in A^n\}$, que é o raio de cobertura do código C. Quanto ao raio médio,

$$\tilde{\rho}(z \star C) = \frac{1}{q^n} \sum_{x \in A^n} d(x, z \star C) = \frac{1}{q^n} \sum_{x \in A^n} \mathrm{d}(x \star z^{-1}, C) = \frac{1}{q^n} \sum_{y \in A^n} \mathrm{d}(y, C)$$

■

3.22 Proposição: *Se C um código de grupo com q^{n-k} elementos e $\mathscr{S}$ um protocolo esteganográfico obtido por C, então,*

1) A capacidade relativa de $\mathscr{S}$ é $\alpha = k/n$;

2) O raio do protocolo de $\mathscr{S}$ é o raio de cobertura de C;

3) A distorção média de $\mathscr{S}$ é o raio médio de $C = \tilde{\rho}$.

Demonstração: Pela definição de aplicação de imersão e decodificação,

$$\mathrm{d}(x, e(s, x)) = \mathrm{d}(x \star z^{-1}, C) \tag{3.2}$$

1) Vem do fato de o protocolo ser um $[k, n]$-protocolo;

2) $\rho = \max\{\mathrm{d}(x, \mathrm{e}(s, x)) : s \in A^k, x \in A^n\} \underset{(3.2)}{=} \max\{\mathrm{d}(x \star z^{-1}, C) : x \in A^n\}$, que é o raio de cobertura do código C.

3) Consequencia imediata de 2).

■

3.23 Proposição: *Seja $S = (\mathrm{e}, \mathrm{r})$ um protocolo esteganográfico induzido por um código de grupo C. Temo que S é perfeito se, e somente se, C é perfeito.*

Demonstração: Como pela proposição em 3.22 o raio do protocolo de S é igual ao raio de cobertura de C, a cota de Hamming para códigos (proposição em 1.15) e para protocolos (proposição contida em 3.3) coincidem. ■

A última proposição deixa nítido o fato de haver tão poucos tipos de protocolos perfeitos quanto são escassos os códigos perfeitos[4]. Os únicos protocolos (lineares) perfeitos são os induzidos pelos códigos de Hamming, de Golay e os triviais.

[4]Veja o comentário no início da seção 1.5.

3.4 Protocolos Sobre Outras Estruturas

Frequentemente, os códigos estão associados ao corpo, logo grupo abeliano, $\mathbb{F}_q$ e desta forma, o exposto anteriormente se aplica. Seja $\mathrm{r} : \mathbb{Z}_q^n \to \mathbb{Z}_q^k$ um homomorfismo sobrejetor sobre $\mathbb{Z}_q$-módulos. Como $\mathbb{Z}_q^n$ e $\mathbb{Z}_q^k$ são módulos livres finitamente gerados, r pode ser dada por uma matriz H, ou seja, $\mathrm{r}(x) = Hx^t$ [1, p. 298]. O núcleo C de r é um submódulo de $\mathbb{Z}_q^n$ e $\mathbb{Z}_q^n/C \cong \mathbb{Z}_q^k$. Logo, $\#C = q^{n-k}$, C é dito ser um **código linear** sobre $\mathbb{Z}_q$ e o protocolo que surge de r é dito **protocolo linear**.

A teoria de códigos lineares sobre os anéis $\mathbb{Z}_q$ é similar. Como no caso de corpos, as classes em $\mathbb{Z}_q/C$ podem ser manipuladas em termos da aplicação r: dois vetores x, $y \in \mathbb{Z}_q^n$ pertencem à mesma classe se, e somente se, $\mathrm{r}(x) = \mathrm{r}(y)$. O líder de uma classe $x + C$ é um vetor ℓ cujo peso é mínimo entre o peso de todos os elementos de $x + C$ (algumas classes podem ter mais de um líder). Seja $\mathscr{R} = \{\ell_1, ..., \ell_{q^k}\}$ um conjunto formado por um elemento líder de cada classe. Temos que r induz uma bijeção entre $\mathscr{R} \to \mathbb{Z}_q^k$. Denote por cl a inversa desta aplicação. Para qualquer vetor $x \in \mathbb{Z}_q^n$, $\mathrm{cl}(\mathrm{r}(x))$ é um líder de $x + C$. Conhecendo $\mathscr{R}$ e a aplicação cl, temos uma decodificação para C, chamada de **algoritmo do líder da classe**.

3.24 Proposição: *A aplicação* $\mathrm{dec} : \mathbb{Z}_q^n \to C$ *dada por* $\mathrm{dec}(x) = x - \mathrm{cl}(\mathrm{r}(x))$ *é uma aplicação de decodificação para* C.

Demonstração: Como r é um homomorfismo, temos que $\mathrm{r}(x - \mathrm{cl}(\mathrm{r}(x))) = \mathrm{r}(c) - \mathrm{r}(\mathrm{cl}(\mathrm{r}(x))) = 0$ e logo $\mathrm{dec}(x) \in C$. Se existe $c \in C$ tal que $\mathrm{d}(x, c) < \mathrm{d}(x, \mathrm{dec}(x)) = \mathrm{d}(x, x - \mathrm{cl}(\mathrm{r}(x)))$, então $\omega(x - c) < \omega(\mathrm{cl}(\mathrm{r}(x))))$. Como ambos $x - c$ e $\mathrm{cl}(\mathrm{r}(x))$ pertencem à classe $x + C$, temos uma contradição. ■

3.25 Proposição: *Seja* r *a aplicação definida como anteriormente e* $\mathrm{e} : \mathbb{Z}_q^k \times \mathbb{Z}_q^n \to \mathbb{Z}_q^n$ *dada por* $\mathrm{e}(s, x) = x - \mathrm{cl}(\mathrm{r}(x) - s)$. *Então, o par* (e, r) *é um* $[n, k]$*-protocolo esteganográfico sobre* $\mathbb{Z}_q$.

Demonstração: Como $\mathrm{e}(s, x) = z + \mathrm{dec}(x - z)$, com $z = \mathrm{cl}(s)$, então

$$\begin{aligned} \mathrm{r}(\mathrm{e}(s, x)) &= r(z + \mathrm{dec}(x - z)) \\ &= \mathrm{r}(z) + \mathrm{r}(\mathrm{dec}(x - z)) \\ &= r(z) \\ &= s \end{aligned}$$

■

3.26 Proposição: *Seja* $\mathscr{S} = (\mathrm{e}, \mathrm{r})$ *um* $[n, k]$*-protocolo linear sobre* $\mathbb{Z}_q$ *e* C *o código principal associado a* $\mathscr{S}$. *Então*

(1) O raio de imersão de $\mathscr{S}$ é igual ao raio do cobertura de C;

(2) A distorção média de $\mathscr{S}$ é

$$R = \frac{1}{q^k} \sum_{\ell \in \mathscr{R}} \omega(\ell)$$

Demonstração: (1) Caso particular da proposição em 3.22;

(2) Mesmo que o lema em 3.21.

■

Se $q = p^s$ é potência de algum número primo, então existe um isomorfismo de grupos aditivos $\mathbb{F}_q \cong \mathbb{Z}_p^s$ e a teoria anterior também se aplica. Assuma que A seja um alfabeto finito com q elementos, $A = \mathbb{F}_q$ e $\mathrm{r} : \mathbb{F}_q^n \to \mathbb{F}_q^k$ seja uma aplicação sobrejetora. Então, existe uma $[k, n]$-matriz H tal que $\mathrm{r}(x) = Hx^t$. Temos que H pode ser vista como matriz teste de paridade de um $[n, n-k]$-código $C = \ker(\mathrm{r})$. O $[k, n]$-protocolo esteganográfico associado a C tem r como aplicação de recuperação e a aplicação de imersão é dada como na proposição em 3.25, ou seja

$$\mathrm{e}(s, x) = x - \mathrm{cl}(Hx^t - s)$$

Capítulo 4

Códigos em Papel Molhado

Imagine que se deseje enviar uma mensagem escrita em um papel que foi exposto a chuva e está molhado, exceto por algumas partes, no momento em que o emissor irá escrever. Para minimizar o dano ao papel e evitar que ele rasgue sobre a pressão da caneta, o emissor escolhe os lugares secos (**canal de seleção** - lugares na cobertura que conterão a mensagem escondida) para colocar o conteúdo desejado. Quando o receptor recebe o papel com a mensagem, o papel já está completamente seco e não há como saber quais lugares estavam molhados. Desta forma, emissor e receptor não compartilham o canal de seleção, e diz-se que o emissor está "escrevendo sobre papel molhado".

Quando aplicamos Teoria de Códigos e, por algum motivo, não podemos alterar determinadas posições (como no papel molhado), diz-se que estamos no caso de código em papel molhado. Mais geralmente, chama-se **Código em Papel Molhado**[1] a situação em que remetente e destinatário não compartilham o canal de seleção.

4.1 Códigos em Papel Molhado e Esteganografia

Considere que a imagem de cobertura seja $b = \{b_1, ..., b_n\}$, em que cada b_i é um pixel, para $1 \leq i \leq n$ e o conjunto $J = \{i_1, ..., i_j\} \subset \{1, ..., n\}$ que represente os índices dos pixeis que podem ser modificados. Tome M uma matriz previamente combinada (ainda que aleatória) entre remetente e

[1] Em inglês, *wet paper code*. Teoricamente poderíamos traduzir também como Código *de* Papel Molhado. Neste trabalho, optamos por Código *em* Papel Molhado porque neste caso estamos em uma situação e não em um tipo de código. Código *de* Hamming ou *de* Goppa são um tipo código. Código *em* papel molhado depende do contexto.

destinatário e suponha que vá ser enviado o segredo $s \in \mathbb{F}_2^k$ escondido em b. O remetente deve então alterar b para b' de tal forma que

$$Mb' = s. \tag{4.1}$$

O destinatário precisa resolver um sistema linear em $\mathbb{F}_2$. Chame $v = b' - b$. Os elementos não nulos de v correspondem aos bits que devem modificados para satisfazer a equação (4.1). Podemos reescrever o sistema como

$$Mv = s - Mb. \tag{4.2}$$

Neste novo sistema, existem j incógnitas v_j, $j \in J$, enquanto os outros $n-j$ valores são zero. Assim, do lado esquerdo, podemos remover de v todas as entradas nulas e de M as $n-j$ colunas correspondentes aos zeros e desta forma obteremos uma matriz H que é tal que

$$Hv = m - Mb \tag{4.3}$$

no caso em que mantemos a notação v mesmo após a remoção das entradas nulas. A matriz H possui k linhas e j coluna e o sistema tem solução quando o posto de H for igual a k.

4.1 Definição: *Seja J um conjunto de coordenadas que devem ser mantidas fixas durante a imersão, H uma $[n-k, n]$-matriz de checagem de um código C. Considere a matriz H_J obtida de H retirando-se as colunas relativas às posições de J. O código que possui H_J como matriz de checagem é chamado de* ***código reduzido*** *de C e denotado por C_J.*

Considere o conjunto $C'_J = \{c \in C : c_{j_i} = 0 \text{ para todo } j_i \in J\}$.

4.2 Proposição: *As palavras que compõe C_J são as palavras de C'_J deletadas as posições J.*

Demonstração: Chame de A o conjunto formado pelas palavras de C'_J deletadas as posições J. Queremos mostrar que $C_J = A$.
$A \subset C_J$: Seja $a = (a_1, ..., a_{n-\#(J)}) \in A$. Queremos mostrar que $H_J \cdot a^t = 0$. Ao se completar a com 0 nas posições J, renumerar e chamar o novo vetor $\overline{a}$, vemos que $\sum_{i=1}^{n}(h_i a_i) = 0$, com $a_j = 0$, para todo $j \in J$ e daí $\overline{a} \in C$. Como nas colunas de J as entradas do vetor são 0, essas não fazem diferenças na combinação linear, $a \in C_J$.
$C_J \subset A$: A matriz teste de paridade de C_J é

$$H_J = \begin{pmatrix} h_1 & h_2 & \cdots & \widehat{h_{l_1}} & \cdots & \widehat{h_{l_2}} \cdots & h_n \end{pmatrix},$$

em que as h_j, $1 \leq j \leq n$, são colunas de H e $\widehat{h_{J_i}}$, $1 \leq i \leq \#(J)$, significa a omissão das colunas. Seja $c = (c_1, ..., c_{n-\#(J)}) \in C_J$. Após adicionar 0 às posições J e fazer renumeração, temos $\overline{c} = (c_1, c_2, ..., 0, ..., c_n)$ e daí $H \cdot \overline{c}^t = 0$, ou seja, $\overline{c} \in C'_J$ e $c \in A$. ■

4.3 Exemplo: *Considere a matriz de checagem*

$$H = \begin{pmatrix} 1 & 0 & 1 & 0 & 1 & 0 \\ 1 & 1 & 0 & 0 & 1 & 1 \\ 1 & 1 & 1 & 1 & 1 & 1 \end{pmatrix}$$

O código associado a essa matriz é

$$C = \{000000, 001111, 010001, 011110, 100010, 101101, 110011, 111100\}.$$

Tome H_J obtida removendo-se a segunda e a quinta colunas

$$H_J = \begin{pmatrix} 1 & 1 & 0 & 0 \\ 1 & 0 & 0 & 1 \\ 1 & 1 & 1 & 1 \end{pmatrix}$$

O código reduzido neste caso é $C_J = \{0000, 1111\}$. Note que as únicas palavras de C a possuírem 0 *nas segunda e quinta coordenadas eram* 000000 *e* 101101.

4.2 Exemplo de Esteganografia e Códigos em Papel Molhado

Considere a matriz

$$H = \begin{pmatrix} 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ 1 & 0 & 1 & 0 & 1 & 0 & 1 & 0 \\ 0 & 1 & 1 & 0 & 0 & 1 & 1 & 0 \\ 0 & 0 & 0 & 1 & 1 & 1 & 1 & 0 \end{pmatrix}$$

O código C associado a essa matriz é como está na Tabela 4.1

00000000	00011110	00101101	00110011
01001011	01010101	01100110	01111000
10000111	10011001	10101010	10110100
11001100	11010010	11100001	11111111

Tabela 4.1: Código associado à matriz H.

Suponha que queiramos esconder $s = 1101$ em 11010110. Pelo método da distância mínima visto até os capítulos anteriores, tomaríamos $\mathrm{e}(s, x)$ como qualquer palavra no conjunto $Y = \{00010110, 11000100, 11011010, 11110111\}$, pois $\mathrm{r}^{-1}(s)$ é como na Tabela 4.2 e essas palavras estão à menor distância de x (no caso, $\mathrm{d}(y, x) = 2$ para qualquer $y \in Y$).

00001000	00010110	00100101	00111011
01000011	01011101	01101110	01110000
10001111	10010001	10100010	10111100
11000100	11011010	11101001	11110111

Tabela 4.2: Classe lateral associada a s, ou seja, $\mathrm{r}^{-1}(s)$.

No caso de Código em Papel Molhado em que não podemos, por exemplo, modificar as duas primeiras entradas, as possibilidades se restringiriam ao conjunto $\{11000100, 11011010, 11110111\}$. Se restringirmos até a terceira sem alteração, as possibilidades seriam $\{11000100, 11011010\}$. Se a restrição fosse feita às cinco primeiras entradas, não encontraríamos solução para o sistema como descrito na equação (4.1).

Capítulo 5

Conclusão

Para que se utilizem métodos esteganográficos, protocolos para esconder mensagens em imagens por exemplo, funções pouco intuitivas podem ser utilizadas. A bem desenvolvida Teoria dos Códigos facilita muito este trabalho devido ao trato com síndrome, classes laterais e outros aspectos. Vários códigos, como o Código de Hamming, código de Reed-Solomon, podem ser utilizados para este fim. O Algoritmo F5 ilustra bem como tais funções podem ser substituídas por manipulação de matrizes.

Se, por algum motivo, não pudermos alterar certas posições da mensagem original ao escondermos um segredo na cobertura, caso do código em papel molhado, podemos ter que fazer alterações grosseiras na imagem, já que nem sempre será possível utilizar método semelhante ao Bit Menos Significante. Se o número de alterações for muito restrito, pode ser que não encontremos maneira de embutir o segredo para extração futura.

O estudo moderno da Teoria dos Códigos passa pela utilização de códigos algébricos geométricos. Não encontramos, na literatura pesquisada, relação que envolva esse tipo de código com esteganografia e este campo pode se configurar em uma nova vertente para o estudo da esteganografia em trabalhos futuros.

A maioria dos exemplos de códigos presentes neste texto foram gerados de programas criados por nós na linguagem de programação Python. Nossa intenção é continuar o desenvolvimento dessas macros, uni-las e disponibilizá-las futuramente, para que outros possam utilizar e aperfeiçoar, com a mentalidade de *software open source*.

Referências Bibliográficas

[1] GARCIA, A. e LEQUAIN, Y., **Elementos de Álgebra**. 5^a edição. Rio de Janeiro, IMPA, 2010.

[2] HEFEZ, A. e VILLELA, M., **Códigos Corretores de Erros**. 2^a edição. Rio de Janeiro, IMPA, 2008.

[3] MACWILLIAMS, F. J. e SLOANE, N. J. A., **The Theory of Error-Correcting Codes**. 3^a edição. Nova Iorque, North-Holland, 1977.

[4] MUNUERA, C., **Steganography From a Coding Theory Point of View**. Algebraic Geometry modeling in Information Theory. Editado por E. Martinez-Moro. World Scientific, 2012.

[5] JUDGE, J. J., **Steganography: Past, Present, Future**. SANS Institute. Disponível em https://www.sans.org/reading-room/whitepapers/stenganography/steganography-past-present-future-552. Acesso em 01/06/2013 às 11h.

[6] TRITHEMIUS, J., **Steganographie: Ars per occultam Scripturam animi sui voluntatem absentibus aperiendi certu**. Disponível em http://www.esotericarchives.com/tritheim/stegano.htm. Acesso em 10/09/2013 às 09h.

[7] FRIDRICH, J., MIROSLAV, G. e SOUKAL, D., **Wet Paper Codes with Improved Embedding Efficiency**. Information Forensics and Security, IEEE Transactions, vol. 1, issue 1. 2006.

[8] LINT, J. H. van, **A Survey of Perfect Codes**. Rocky Mountain Jornal of Mathematics, vol. 5, número 2, Spring, 1975, pp. 199-224.

[9] ZHANG, W. e LI, S., **Steganographic Codes — a New Problem of Coding Theory**. Journal of Latex Class Files, vol. 1, número 11, 2002.

[10] WESTFELD, A., **F5 - A Steganographic Algorithm. High Capacity Despite Better Steganalysis**. Lecture Notes in Computer Science, vol. 2137, Springer, New York, 2001, pp. 289-302.

[11] **Con Air - A Rota de Fuga**. Direção: Simon West. [S.l.]: Touchstone Pictures, 1997. 1 DVD (115 min).

[12] **OpenPuff**: Software gratuito. Versão 4.00, 2012. Disponível em http://embeddedsw.net/OpenPuff_Steganography_Home.html. Acesso em 02/01/2014 às 21h.

[13] **QuickStego**: Software gratuito. Versão 1.2.0.1, 2011. Disponível em http://quick-stego.sharewarejunction.com. Acesso em 02/01/2014 às 21h.

[14] **SecretLayer**: Software pago. Versão 2.8.1, 2013. Disponível em http://www.steganographypro.com/download.php. Acesso em 02/01/2014 às 21h.

[15] **SpamMimin**: Ferramenta online. Disponível em http://www.spammimic.com. Acesso em 02/01/2014 às 22h.

Índice Remissivo