UNIVERSIDADE ESTADUAL DE FEIRA DE SANTANA

Departamento de Ciências Exatas

PROFMAT - Mestrado Profissional em Matemática em Rede Nacional

Dissertação de Mestrado

CÓDIGOS CORRETORES DE ERROS: UMA PROPOSTA APLICADA AO ENSINO MÉDIO.

Aldo Brito de Jesus

Orientador: Prof. Dr. Maurício de Araujo Ferreira

Feira de Santana

Dezembro de 2021

UNIVERSIDADE ESTADUAL DE FEIRA DE SANTANA

Departamento de Ciências Exatas

PROFMAT - Mestrado Profissional em Matemática em Rede Nacional

CÓDIGOS CORRETORES DE ERROS: UMA PROPOSTA APLICADA AO ENSINO MÉDIO.

Aldo Brito de Jesus

Dissertação apresentada ao Programa de Mestrado Profissional em Matemática em Rede Nacional - PROFMAT do Departamento de Ciências Exatas, UEFS, como requisito parcial para a obtenção do título de **Mestre**.

Orientador: Prof. Dr. Maurício de Araujo Ferreira

Feira de Santana
16 de dezembro de 2021

Ficha Catalográfica - Biblioteca Central Julieta Carteado - UEFS

Jesus, Aldo Brito de

J56c Códigos corretores de erros: uma proposta aplicada ao Ensino Médio. / Aldo Brito de Jesus. – 2021.

122 f.: il.

.

Orientador: Maurício de Araujo Ferreira

Dissertação (mestrado profissional) – Universidade Estadual de Feira de Santana. Departamento de Ciências Exatas, Programa de Pós-Graduação em Matemática em Rede Nacional, Feira de Santana, 2021.

1.Códigos corretores de erros. 2.Números complexos. 3. Quatérnios de Hamilton. 4.Código de Alamouti. 5.Planílha eletrônica I. Ferreira, Maurício de Araujo, orient. II.Universidade Estadual de Feira de Santana. III. Título.

CDU: 517.9

Maria de Fátima de Jesus Moreira - Bibliotecária - CRB-5/1120

Universidade Estadual de Feira de Santana
Departamento de Ciências Exatas
Mestrado Profissional em Matemática em Rede Nacional

Ata da Sessão pública de defesa de dissertação do discente Aldo Brito de Jesus do Programa de Mestrado Profissional em Matemática em Rede Nacional da Universidade Estadual de Feira de Santana

Aos dezesseis dias do mês de dezembro de dois mil e vinte e um, às 14:00 horas, ocorreu a defesa pública não presencial, através da plataforma Google Meet, link: meet.google.com/niy-hmiq-vsk , da dissertação apresentada sob o título **"CÓDIGOS CORRETORES DE ERROS: UMA PROPOSTA APLICADA AO ENSINO MÉDIO",** do discente **Aldo Brito de Jesus**, do Programa de Mestrado Profissional em Matemática em Rede Nacional - PROFMAT da Universidade Estadual de Feira de Santana, para obtenção do título de MESTRE. A Banca Examinadora foi composta pelos professores: Maurício de Araujo Ferreira (Orientador, UEFS), Silvina Alejandra Alderete (UFOB) e Edward Landi Tonucci (UEFS). A sessão de defesa constou da apresentação do trabalho pelo discente e das arguições dos examinadores.

Em seguida, a Banca Examinadora se reuniu em sessão secreta para julgamento final do trabalho e atribuiu o conceito: aprovado.

Sem mais a tratar, foi lavrada a presente ata, que segue assinada pelos membros da Banca Examinadora e pelo Coordenador Acadêmico Institucional do PROFMAT.

Feira de Santana, 16 de dezembro de 2021.

Prof. Dr. Maurício de Araujo Ferreira (Orientador, UEFS)
Orientador

Prof.ª Dra. Silvina Alejandra Alderete (UFOB)

Edward Landi Tonucci

Prof. Dr. Edward Landi Tonucci (UEFS)

Visto do Coordenador:

Agradecimentos

Venho por meio de algumas palavras demonstrar meus sinceros agradecimentos a todas aquelas pessoas que de alguma forma contribuíram para a elaboração deste trabalho.

Agradeço primeiramente a Deus por ter me dado forças e sabedoria para chegar até aqui, sem Ele esta caminhada não seria possível. Gostaria de agradecer a minha mãe por se fazer presente em todos momentos de decisões difíceis e me apoiar em cada uma delas. Agradeço também ao meu pai, a minha companheira Ivanildes, aos meus irmão e a todos os demais familiares.

Agradeço ao professor Maurício de Araujo Ferreira por ter aceitado ser meu orientador e compartilhar um pouco do seu conhecimento comigo, sempre com paciência e muita sabedoria. Gostaria de agradecer também a todos os demais professores da UESB e do PROFMAT/UEFS que fizeram parte da minha formação até o momento e que compartilharam seus conhecimentos comigo. Em especial agradeço aos professores(as): Ana Carla Percontini da Paixão, Darlan Ferreira de Oliveira, Fabíola de Oliveira Pedreira, Kisnney Emiliano de Almeida e Maurício de Araujo Ferreira.

Gostaria ainda de demostrar meu agradecimento a todos os meus colegas do mestrado pela companhia durante as aulas e por ter compartilhado algumas experiências comigo. Em especial agradeço aos colegas Antônio Edézio de Santos de Sousa e Joãonito de Jesus Santos pelo companheirismo em todos os momentos que precisei.

Por fim, agradeço a Sociedade Brasileira de Matemática.

Resumo

Este trabalho tem por objetivo fazer um estudo sobre os códigos corretores de erros e apresentar uma proposta de abordagem deste tema no Ensino Médio, possibilitando assim que o professor utilize partes desta dissertação como material teórico para um minicurso que tenha estudantes desta etapa de ensino como público alvo. Neste trabalho fazemos uma breve revisão sobre matrizes, vetores, bases, anel, corpo, espaço vetorial e outros conteúdos que são utilizados no processo de codificação, transmissão e correção de erros em um código linear. Apresentamos os conceitos de métrica de Hamming, bits de paridade, capacidade de correção, matriz geradora e outras definições sobre a teoria dos códigos corretores de erros. Trazemos uma sequência de atividades sobre códigos de Hamming que o professor pode utilizar em sala de aula. Nas atividades, o WhatsApp é utilizado como recurso didático e as planilhas eletrônicas são exploradas para realizar algumas tarefas no processo de correção de erros. Ademais, apresentamos os números complexos como o conjunto dos pares ordenados reais munidos de duas operações, uma de adição e outra de multiplicação. Exploramos o anel dos quatérnios de Hamilton e mostramos que existe um isomorfismo entre este e um subanel do anel das matrizes com entradas complexas. Este subanel de matrizes está intimamente relacionado com o código de Alamouti que apresentamos como uma possibilidade de aprofundamento no estudo dos códigos corretores.

Palavras-chave: Códigos Corretores de Erros; Números Complexos; Quatérnios de Hamilton; Código de Alamouti; Planilha eletrônica.

Abstract

This work aims to study error-correcting codes and present a proposal to approach this topic in High School, thus enabling the teacher to use parts of this dissertation as theoretical material for a mini-course that has students from this stage of education as audiences target. In this work, we briefly review matrices, vectors, bases, ring, field, vector spaces and other contents that are used in the process of encoding, transmitting and correcting errors in a linear code. We present the concepts of Hamming metrics, parity bits, correctability, generating matrix and other definitions on the theory of error-correcting codes. We bring a sequence of activities on Hamming codes that the teacher can use in the classroom. In activities, WhatsApp is used as a teaching resource and electronic spreadsheets are used to perform some tasks in the error correction process. Furthermore, we present the complex numbers as the set of real ordered pairs with two operations, one for addition and the other for multiplication. We explore the ring of Hamilton quaternions and show that there is an isomorphism between it and a subring of the ring of matrices with complex inputs. This subring of matrices is closely related to the Alamouti code, which we present as a possibility for deepening the study of corrective codes.

Keywords: Error Correction Codes; Complex numbers; Hamilton's Quaternions; Alamouti Code; Spreadsheet.

Sumário

Introdução

A implementação do Novo Ensino Médio e a criação da Base Nacional Comum Curricular (BNCC) traz uma nova visão para o ensino da Matemática na Educação Básica. A nova proposta de ensino coloca o aluno como um ser ativo e corresponsável pelo processo de ensino e aprendizagem. O ensino da Matemática deixa de ser uma mera transmissão de conteúdos e estratégias de resolução de questões e coloca o aluno como um "ser matemático", ou seja, um ser capaz de usar e criar matemática para as demandas sociais e tecnológicas [5].

De acordo com a BNCC [5],"no Ensino Médio o foco é a construção de uma visão integrada da Matemática, aplicada à realidade em diferentes contextos." Tendo isso em vista, enxergamos os códigos corretores de erros como uma oportunidade para o professor expor a Matemática em sala de aula como parte da realidade em que vivemos e mostrar para os alunos o potencial desta área de conhecimento para o desenvolvimento de novas tecnologias. Acreditamos ainda que, o trabalho com códigos em sala de aula proporciona aos alunos a oportunidade de vivenciar o fazer matemático, investigando e propondo soluções para desafios do mundo contemporâneo, desenvolvendo assim a segunda habilidade da área de Matemática e suas Tecnologias proposta pela BNCC.

> Propor ou participar de ações para investigar desafios do mundo contemporâneo e tomar decisões éticas e socialmente responsáveis, com base na análise de problemas sociais, como os voltados a situações de saúde, sustentabilidade, das implicações da tecnologia no mundo do trabalho, entre outros, mobilizando e articulando conceitos, procedimentos e linguagens próprios da Matemática. [5]

Neste trabalho apresentamos os códigos corretores de erros por meio de uma linguagem acessível para alunos do Ensino Médio. De modo que ao trabalhar com este conteúdo em sala de aula, o professor possa usar textos da dissertação como material didático. Procuramos simplificar a linguagem matemática sem perder o formalismo. É claro que ao fazer isso, restringimos um pouco o leque de conteúdos que podem ser explorados por meio de códigos corretores, mas, acreditamos que propor uma leitura mais leve, seja uma maneira de convidar os alunos para o estudo da Matemática.

No primeiro capítulo desta dissertação, apresentamos os conceitos básicos de códigos

corretores de erros: definição, métrica de Hamming, transmissão de uma palavra, redundâncias e outros. Exibimos também alguns exemplos para facilitar o entendimento de alguns conceitos abstratos. Julgamos que o capítulo pode ser usando em sala de aula como uma breve introdução aos códigos corretores de erros.

No início do segundo capítulo definimos anel, corpo e espaço vetorial. Em seguida fazemos uma breve apresentamos dos corpos de inteiros módulo p e suas principais propriedades. Apresentamos também os Códigos de Hamming com o intuito de introduzir o estudo dos códigos lineares, que são definidos logo em seguida. Neste capítulo, muitos dos conceitos de códigos lineares foram apresentados inicialmente por meio de exemplos, desta maneira, em um primeiro momento em sala de aula, o professor do Ensino Médio pode apresentar os conceitos por meio dos exemplos sem a necessidade de recorrer a conceitos mais avançados de álgebra. E para finalizar o capítulo, apresentamos o método para correção de erros.

No terceiro capítulo, com o intuito de preparar o terreno para o capítulo seguinte, fazemos uma breve apresentação dos números complexos como sendo o espaço $\mathbb{R}^2$ munido de uma operação de adição e uma operação de multiplicação. Partindo da forma polar de um número complexo, apresentamos também uma interpretação geométrica para adição e para a multiplicação definidas em $\mathbb{R}^2$.

O quarto capítulo foge um pouco do que é proposto no Ensino Médio, nele apresentamos os Quatérnios de Hamilton e mostramos que este anel é isomorfo a um subanel do anel de matrizes de ordem 2 com coeficientes complexos, que é a base do Código de Alamouti apresentado no final do capítulo. Apesar de alguns dos conceitos apresentados neste capítulo não fazer parte do que é proposto pela base curricular do Ensino Médio, o professor pode apresentar os quatérnios apenas na sua representação matricial e explorar as propriedades herdadas dos quatérnios simplesmente como propriedades das matrizes.

Por fim, no Capítulo 5, apresentamos uma sequência didática que o professor pode aplicar para alunos do terceiro ano do Ensino Médio e/ou fazer uma adaptação para aplicar nas demais turmas, mostrando o potencial da Matemática na vida contemporânea. Nesta sequência exploramos apenas os conteúdos dos dois capítulos iniciais.

Capítulo 1

Códigos Corretores de Erros

Imagine que você seja professor de uma turma de 6º ano e esteja tentando explicar algum conteúdo para os alunos, mas, um grupo de três ou quatro crianças estão conversando baixinho no canto da sala e acabe tirando um pouco da atenção dos colegas. Nessa situação todos nós professores gostaríamos que por meio de alguma mágica fosse possível retirar o som da conversa de modo que apenas a nossa voz chegasse até os ouvidos dos alunos. Poderíamos imaginar que retirar os alunos da sala resolveria o problema e teríamos o caminho livre para o som da nossa fala. No entanto, mesmo tomando esta atitude, provavelmente chegaria ruídos dos corredores, da sala vizinha, dos carros na rua, dentre várias outras fontes de ruídos. De maneira semelhante, quando queremos enviar uma mensagem, seja por sinal analógico ou por sinal digital, existem interferências causadas pelos aparelhos usados na transmissão, pelo meio físico utilizado ou por outras fontes, de modo que é impossível que uma mensagem seja enviada e recebida sem algum tipo de problema causado por algum ruído.

Os ruídos são causados por fontes naturais, como por exemplo o sol, e também por fontes não naturais, como a turbina de um avião, o uso de um aparelho de micro-ondas, e até mesmo pelos próprios aparelhos eletrônicos utilizados na transmissão e recepção dos dados. Ao tentar sintonizar um televisor analógico ou o rádio de um carro em uma determinada frequência, é possível perceber o ruído chegando até o receptor dos aparelhos. Os pequenos chuviscos na TV ou o chiado no rádio, representam a captação de "pequenas" ondas eletromagnéticas que muitas vezes não faziam parte do sinal que foi enviado. Diferentemente do que acontece em sala de aula em muitos dos casos conseguimos fazer com que apenas o sinal enviado chegue até os nossos olhos ou ouvidos. Muitas vezes este problema é resolvido porque o sinal enviado é mais forte que o ruído, de modo que podemos corrigir os erros. O bom desempenho dos aparelhos de correção dos sinais recebidos depende da criação de algoritmos e estes dependem da existência de bons códigos corretores de erros. Um dos exemplos mais simples e corriqueiro é o código de barras. Muitas vezes em um supermercado ao aproximar o código de barras de um leitor óptico o aparelho emite um som

informando algum tipo de erro e automaticamente aproximamos o produto novamente. O mesmo acontece quando por algum motivo estamos preenchendo um formulário digital e acabamos informando um dígito do nosso CPF errado. Seria um incomodo ter que pagar mais caro por um produto ou usar um CPF diferente em uma compra pela internet. Esse tipo de situação não ocorre devido ao acréscimo de redundância no código de barras e também no CPF, neste caso a redundância é chamada de dígito verificador. Um código corretor de erros, em poucas palavras e de maneira simples, nada mais é que uma maneira organizada de acrescentar redundâncias a cada informação que queremos transmitir e/ou armazenar, de modo que seja possível utilizar os dados adicionais para recuperar a informação, detectar e corrigir os erros quando possível. Assim como no nosso sistema de escrita, os códigos corretores de erros são formados por um alfabeto, por palavras e por regras de composição das palavras. Normalmente o alfabeto é formado pelos elementos de um corpo finito e as palavras são sequências finitas destes elementos.

De acordo com [14], a Teoria dos Códigos, assim como muitos outros estudos nos diversos campos da Matemática, surgiu em meio a um conflito entre duas grandes nações, a União Soviética e o Estados Unidos durante a Guerra Fria. Em 1948 o Matemático estadunidense Claude Elwood Shannon publicou o primeiro trabalho sobre códigos corretores de erros e ficou conhecido como o pai da teoria da informação. Um outro nome ligado ao inicio da Teoria de Códigos é do Matemático estadunidense Richard Wesley Hamming, que trabalhava com um grande computador e tinha seu trabalho perdido sempre que a máquina cometia algum tipo de erro durante o armazeno de informações. Motivado pela frustração de perder todo seu trabalho sempre que ocorria um erro desse tipo, Hamming desenvolveu um dos primeiros códigos corretores de erros da história e publicou um trabalho em 1950 com conceitos fundamentais como métrica, redundância, equivalência de códigos e códigos sistemáticos. Neste trabalho veremos este código com mais detalhes. A partir da década de 70 a Teoria de Códigos passou a ser de interesse de vários engenheiros que estavam envolvidos na corrida espacial e surgiram vários outros códigos.

1.1 Códigos Corretores de Erros

No trabalho publicado em 1948, Shannon definiu a unidade de medida de informação, que chamou de bit (binary digits) e um sistema de comunicação, formado basicamente por cinco componentes: uma fonte de informação, um transmissor, um canal, um receptor e um destino, como apresentado no esquema da Figura 1.1. O código fonte, ou simplesmente a fonte, produz a mensagem a ser transmitida e envia para o transmissor que transforma a mensagem em um sinal passível de ser transmitido pelo canal, que é o meio utilizado para transmitir o sinal do transmissor até o receptor que decodifica o sinal recebido equivalente a mensagem enviada pelo transmissor, e por fim a informação é visualizada pela pessoa

ou equipamento no destino final.

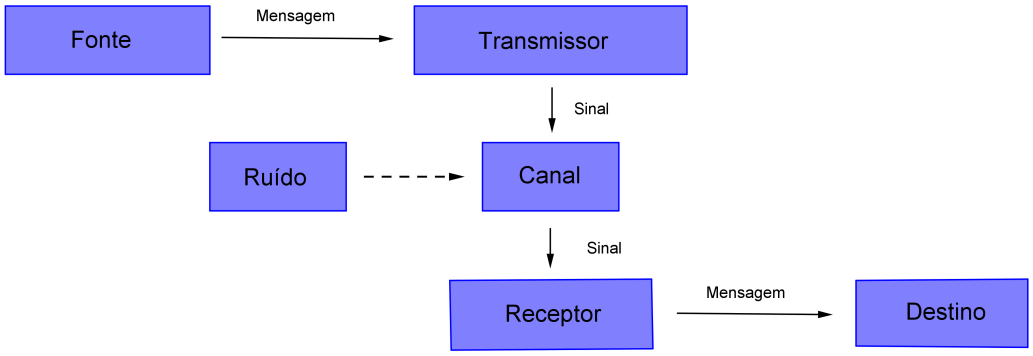

Figura 1.1: Esquema do sistema de transmissão.

Um exemplo simples de código corretor de erros é o nosso idioma. Considerando o alfabeto F formado por 23 letras mais o espaço em branco, temos uma total de 24 elementos. A maior palavra do nosso alfabeto é pneumoultramicroscopicossilicovulcanoconiótico, que possui 46 letras, assim, podemos completar as demais palavras com espaços em branco, de modo que todas elas tenham exatamente 46 elementos. Neste caso o nosso código C é um subconjunto de F^{46}, ou seja, é um subconjunto do conjunto formado por todas as sequências com 46 elementos do alfabeto F. Este código não é muito eficiente por ter palavras muito próximas umas das outras, por exemplo, as palavras BALA e MALA diferem de apenas um elemento. Assim o transmissor pode enviar a palavra BALA e, devido a interferência causada por algum ruído, chegar ao destino a palavra MALA, como representado na Figura 1.2. Como as duas palavras pertencem ao código o receptor não identificará o erro.

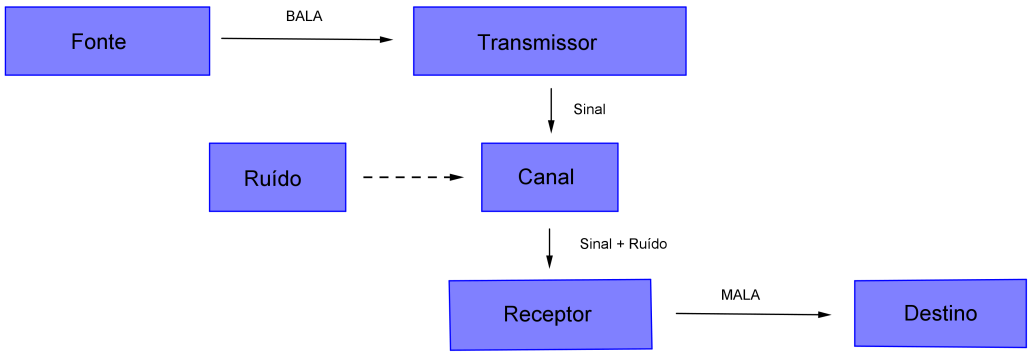

Figura 1.2: Palavra recebida com erro.

Existe também a possibilidade de ser enviada a palavra BALA e por algum motivo o receptor detectar um sinal equivalente a palavra QALA. Como esta palavra não existe em nosso idioma, o receptor saberá que a palavra está errada. Mas existem várias outras palavras que estão próxima desta, por exemplo BALA, FALA, MALA e TALA, assim o

receptor não saberá qual foi a palavra enviada e não será possível corrigir o erro. Este tipo de impossibilidade é causada devido a distância entre as palavras e a falta de informações adicionais. Veja o esquema da Figura 1.2.

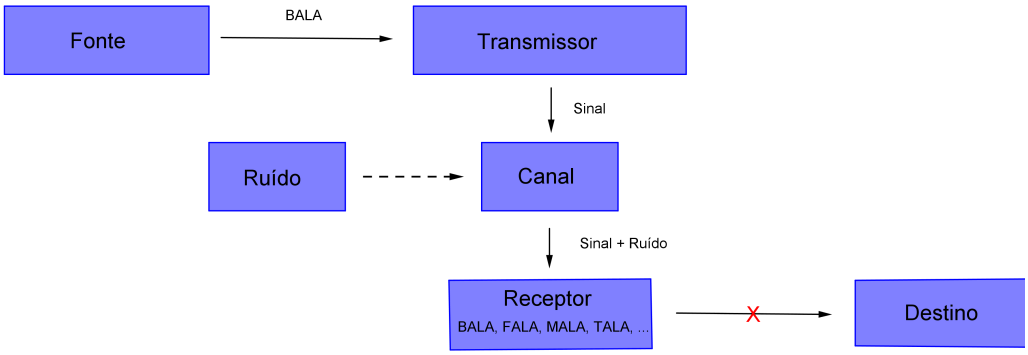

Figura 1.3: Erro sem correção.

Para resolver o problema das múltiplas substituições para palavra QALA recebida, poderíamos ter acrescentado algum tipo de redundância no sinal enviado, por exemplo, ter enviado o sinal da palavra CARAMELO junto com o sinal da palavra BALA, desta maneira, como mostra o esquema da Figura 1.4, o receptor iria detectar o sinal das palavras QALA e CARAMELO. Como as demais palavras possíveis para a correção não tem nenhum tipo de relação com a palavra CARAMELO, o receptor iria decidir corretamente por enviar a palavra BALA para o destino final. Mas note que poderíamos ter escolhido a palavra DOCE como redundância, aumentando assim apenas quatro elementos na sequência da palavra BALA. Quanto maior o comprimento das palavras, maior o custo computacional para enviar e receber as mesmas, por isso devemos nos preocupar em como acrescentar redundância nas palavras mantendo o comprimento razoavelmente pequeno.

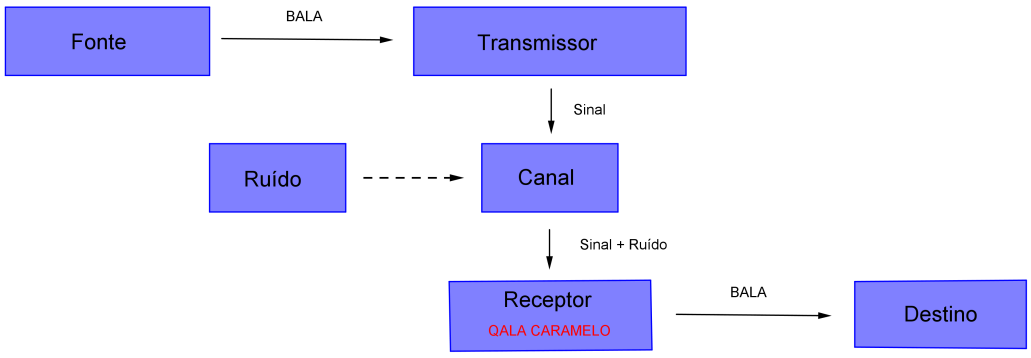

Figura 1.4: Acréscimo de redundância e correção do erro.

Um outro exemplo clássico é o código fonte $F_2^2 = \{(0,0),(0,1),(1,0),(11)\}$ de um robô que se move sobre um tabuleiro quadriculado de modo que a cada comando dado o robô se desloca de uma casa para a casa vizinha. Por simplicidade vamos representar o par

ordenado (a, b) simplesmente por ab, aqui cada palavra ab representa um comando, como descrito abaixo:

$$\begin{array}{rcl@{\qquad\qquad}rcl} \text{Leste} & \longrightarrow & 00 & \text{Norte} & \longrightarrow & 10 \\ \text{Oeste} & \longrightarrow & 01 & \text{Sul} & \longrightarrow & 11 \end{array}$$

Neste caso não temos um bom código, pois ao enviar a palavra 11 o robô poderia receber a palavra 10 e não perceber que foi cometido um erro, como no caso das palavras BALA e MALA. Precisamos então acrescentar redundâncias a cada palavra deste código de maneira organizada para que seja possível identificar e corrigir erros. Ao fazer esse acréscimo criamos uma novo código conhecido como código do canal. Podemos então, conforme Exemplo 2.32, fazer a seguinte modificação no código F_2^2:

$$\begin{array}{rcl@{\qquad\qquad}rcl} 00 & \longrightarrow & 00000 & 10 & \longrightarrow & 10110 \\ 01 & \longrightarrow & 01011 & 11 & \longrightarrow & 11101 \end{array}$$

Neste caso os dois primeiros elementos são idênticos ao que já tínhamos no código F_2^2 e os últimos são redundâncias. Assim, o código do canal é $\{00000,\ 01011,\ 10110,\ 11101\}$.

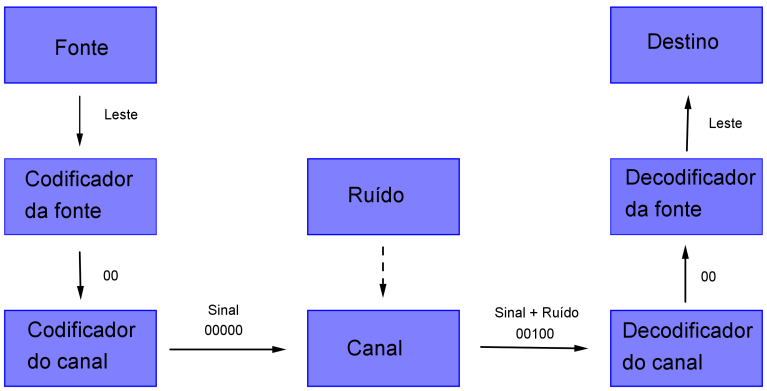

Figura 1.5: Transmissão do comando Leste com correção.

Com esse novo código fica mais fácil de corrigir possíveis erros. Por exemplo, suponha que o comando Leste deva ser enviado para o robô, primeiramente o codificador da fonte gera a palavra 00 que será transformada na palavra 00000 pelo codificador do canal e em seguida enviada. Assim, o decodificador do canal receberá um palavra que pode ser a palavra correta ou uma palavra com erro, vamos supor que o decodificador receba a palavra 00100. Ao comparar esta palavra com as demais palavras do código, o decodificador perceberá que a mesma não pertence ao código do canal, logo, concluir que ocorreu algum tipo de erro na transmissão e analisar se é possível fazer a correção. Procurando pelas palavras mais próximas, em relação a diferença entre os elementos de mesma posição, o decodificador chegará a conclusão de que a palavra enviado foi 00000 e desta maneira o

robô receberá corretamente o comando Leste, como representado na Figura 1.1.

1.2 Métrica de Hamming

Dado um alfabeto F, isto é, um conjunto com finitos elementos, denotamos o número de elementos do conjunto F por $|F|$. Em muitos dos casos o conjunto F é um corpo. Um código corretor de erros é qualquer subconjunto próprio de F^n, ou seja, é um conjunto formado por sequência com exatamente n termos, todos pertencentes ao alfabeto F.

Na seção anterior falamos em distância entre duas palavras, para formalizar este conceito vamos definir a distância de Hamming entre dois elementos do conjunto F^n.

Definição 1.1. Dados dois elementos quaisquer $u, v \in F^n$, a distância de Hamming entre $u = (u_1, u_2, ...u_i, ..., u_n)$ e $v = (v_1, v_2, ..., v_i, ..., v_n)$ é definida como

$$d(u, v) = |\{i;\ u_i \neq v_i,\ 1 \leq i \leq n\}|\,.$$

Exemplo 1.2. No código $\{00000,\ 01011,\ 10110,\ 11101\} \subset \{0, 1\}^5$, temos que

$$\begin{array}{lcllcl} d(00000, 01011) & = & 3, & d(01011, 10110) & = & 4, \\ d(00000, 10110) & = & 3, & d(01011, 11101) & = & 3, \\ d(00000, 11101) & = & 4, & d(10110, 11101) & = & 3. \end{array}$$

A distância de Hamming satisfaz as três propriedades de métrica, como veremos na proposição a seguir, por esse motivo a distância entre duas palavras como definida acima, também é conhecida como métrica de Hamming.

Proposição 1.3. *Dados $u,\ v,\ w \in F^n$, temos que*

i) Positividade: $d(u, v) \geqslant 0$, valendo a igualde se, e somente se, $u = v$;

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

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

Demonstração. O item *i)* é claro, pois o número de elementos de um conjunto é não negativo. O item *ii)* segue do fato de que $u_i \neq v_i$ se, e somente se, $v_i \neq u_i$.

Para demonstrar o item *iii)*, vamos analisar a contribuição da i-ésima coordenada para $d(u, w)$ e para a soma $d(u, v) + d(v, w)$. Observe que se $u_i \neq w_i$, então a contribuição desta coordenada para $d(u, w)$ é 1 e para $d(u, v) + d(v, w)$ é 1 ou 2, pois não podemos ter $u_i = v_i = w_i$. No caso em que $u_i = w_i$ a contribuição para $d(u, w)$ é 0 e para $d(u, v) + d(v, w)$ pode ser 0 ou 2, pois, ou $u_i = w_i = v_i$ ou $v_i \neq u_i$ e $v_i \neq w_i$. Portanto, a contribuição da i-ésima coordenada para $d(u, w)$ é menor ou igual a contribuição para

$d(u,v) + d(v,w)$. Como essas distâncias podem ser obtidos somando as contribuições de cada coordenada, chegamos a conclusão que $d(u,w) \leqslant d(u,v) + d(v,w)$. □

Muitos dos métodos de correção de erros são baseados na distância de Hamming entre duas palavras. Um dos aspectos que tornam estes métodos mais eficientes é a quantidade de palavras próximas da palavra enviada e/ou armazenada. Vamos então definir disco e esfera no conjunto F^n para formalizar a ideia de próximo e ver uma maneira de calcular a quantidade de elementos em cada um desses conjuntos.

Definição 1.4. Sejam v um elemento de F^n e $r > 0$ um número natural. Definimos o disco de raio r e centro v, como sendo o conjunto:

$$D(v,r) = \{u \in F^n \mid d(u,v) \leq r\},$$

e a esfera de raio r e centro v como sendo o conjunto:

$$S(v,r) = \{u \in F^n \mid d(u,v) = r\}.$$

Proposição 1.5. *Para todo $v \in F^n$ e todo número natural $r > 0$, temos que*

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

onde n é o comprimento das palavras e q é a quantidade de elementos do conjunto F.

Demonstração. Inicialmente note que $|D(v,r)| = \sum_{i=0}^{r} |S(v,i)|$. Vamos então calcular quantos elementos há em cada um dos conjuntos $S(v,i)$. Observe que uma palavra u pertence ao conjunto $S(v,i)$ se, e somente se, $d(u,v) = i$, ou seja, se, e somente se, u e v tem exatamente i coordenadas diferentes. Dada uma palavra v, temos $\binom{n}{i}$ maneiras de escolher as i entradas de u que serão diferentes das respectivas entradas de v e para cada uma das i coordenadas diferentes podemos escolher qualquer um dos elemento de F exceto o elemento da i-ésima coordenada de v, portanto, para cada coordenada, temos $q-1$ possibilidades. Assim, o número de elementos do conjunto $S(v,i)$ é dado por $\binom{n}{i}(q-1)^i$, de onde concluímos que $|D(v,r)| = \sum_{i=0}^{r} \binom{n}{i}(q-1)^i$. □

Exemplo 1.6. Considerando o conjunto $F^4 = \{0,1\}^4$, temos que

$$\begin{aligned}
S(0000,3) &= \{1011,\ 0111,\ 1110,\ 1101\},\\
S(0000,2) &= \{1100,\ 0011,\ 0101,\ 0110,\ 1001,\ 1010\},\\
S(0000,1) &= \{1000,\ 0100,\ 0010,\ 0001\},\\
S(0000,0) &= \{0000\}.
\end{aligned}$$

Logo, $|D(v,3)| = 15$.
E, por outro lado, temos que

$$|D(v,3)| = \sum_{i=0}^{3} \binom{4}{i}(2-1)^i = \binom{4}{0}\cdot 1^0 + \binom{4}{1}\cdot 1^1 + \binom{4}{2}\cdot 1^2 + \binom{4}{3}\cdot 1^3 = 1+4+6+4 = 15.$$

Um outro aspecto que pode tornar o processo de correção mais eficiente é a distância mínima do código. Esta característica está intimamente ligada com a quantidade de erros que é possível corrigir. Por exemplo, no código do Exemplo 1.2, temos que a distância mínima é 3 e como veremos mais na frente, neste caso é possível corrigir no máximo um erro.

Definição 1.7. Seja $\mathcal{C}$ um código, a distância miníma d de $\mathcal{C}$ é definida por

$$d = \min\{d(u,v) \mid u, v \in \mathcal{C}, \text{ com } u \neq v\}.$$

Observe que no Exemplo 1.2 calculamos a distância entre todas as palavras diferentes, fizemos um total de $\binom{4}{2} = 6$ operações. Assim, pode-se imaginar que para todo código $\mathcal{C}$, é necessário realizar $\binom{|\mathcal{C}|}{2}$ cálculos para determinar a distância mínima d. Mas, como veremos mais adiante, no caso de códigos lineares a quantidade de operações é certamente menor.

Definição 1.8. Dado um código $\mathcal{C}$ com distância mínima d definimos a cota de correção t como sendo o número natural

$$t = \left[\frac{d-1}{2}\right],$$

onde $[k]$ representa a parte inteira de um elemento k.

Proposição 1.9. *Seja $\mathcal{C}$ um código com distância mínima d. Para quaisquer duas palavras distintas $c, c' \in \mathcal{C}$, temos que*

$$D(c,t) \cap D(c',t) = \varnothing.$$

Demonstração. Suponha por contradição que exista uma palavra $v \in D(c,t) \cap D(c',t)$. Sendo assim, temos $d(c,v) \leq t$ e $d(c',v) \leq t$. Mas note que pela desigualdade triangular temos que

$$d(c,c') \leq d(c,v) + d(v,c') \leq t + t = 2t = d - 1 < d.$$

Um absurdo, pois a distância mínima do código $\mathcal{C}$ é d. Portanto, $D(c,t) \cap D(c',t) = \varnothing$. □

A proposição a seguir fornece dados numéricos relacionados a capacidade de correção de um código corretor de erros.

Proposição 1.10. *Seja $\mathcal{C}$ um código com distância mínima d. Então $\mathcal{C}$ pode corrigir no máximo $t = \left[\frac{d-1}{2}\right]$ erros e detectar $d-1$ erros.*

Demonstração. Suponha que seja enviada uma palavra c e que tenha ocorrido no mínimo um e no máximo $d-1$ erros na transmissão, assim, chegará até o receptor uma palavra r tal que $d(c,r) \leq d-1$ e portanto o decodificador saberá que a palavra r não pertence ao código $\mathcal{C}$ e concluirá que a palavra contém erros. Mas veja que, caso tenha ocorrido mais que t erros, não é possível corrigir, pois pode existir uma outra palavra c' tal que $d(c',r) \leq d-1$.

Suponha agora que a palavra r recebida contenha no máximo t erros. Neste caso temos que $d(c,r) \leq t$, assim r pertence ao disco $D(c,t)$. E dada qualquer outra palavra $c' \in \mathcal{C}$, temos que $r \notin D(c',t)$. Portanto, o decodificador concluirá que a palavra enviada foi c, pois é a palavra mais próxima de r. □

Veja que de acordo esta proposição, para maximizar a capacidade de correção de um código $\mathcal{C}$ precisamos escolher as palavras de modo que a distância mínima d seja maximizada, e desta maneira aumentar a capacidade de correção do código. Portanto, é de fundamental importância determinar a distância mínima de um código ou ter pelo menos uma estimativa para a mesma.

Uma outra maneira de melhorar a capacidade de correção e detecção de erros em um código $\mathcal{C} \subset F^n$ é escolher as palavras de modo que para toda palavra $r \in F^n$, exista uma palavra $c \in \mathcal{C}$, tal que $r \in D(c,t)$, neste caso, o código é dito perfeito, conforme Definição 1.11. Desta maneira, sempre que receber uma palavra r com erros, o decodificador será capaz de corrigir o erro. No caso em que a palavra r contém mais de t erros, a correção não estará correta. No entanto, não é simples fazer a escolha das palavras, pois existe uma relação entre a quantidade de palavras de um código, o comprimento destas palavras e a distância mínimo. Um dos problemas fundamentais da Teoria dos Códigos é estudar esta relação. Neste trabalho não entraremos em detalhes em relação a esta dependência.

Definição 1.11. Seja $\mathcal{C} \subset F^n$ um código com distância mínima d e seja $t = \left[\frac{d-1}{2}\right]$. O código $\mathcal{C}$ é dito perfeito se

$$\bigcup_{c \in \mathcal{C}} D(c,t) = F^n.$$

Exemplo 1.12. Considere o código $\mathcal{C} = \{000, 111\} \subset \{0,1\}^3$. Veja que neste código temos distância mínima $d = 3$, capacidade de correção $t = \left[\frac{3-1}{2}\right] = 1$,

$$D(000,1) = \{000, 001, 010, 100\} \text{ e } D(111,1) = \{011, 101, 110, 111\}.$$

E note ainda que,

$$D(000,1) \cup D(111,1) = \{0,1\}^3.$$

Portanto, o código $\mathcal{C}$ é perfeito.

A partir da Proposição 1.10 podemos traçar uma estratégia de correção de erros em um código utilizando apenas a métrica de Hamming. Considere o código $\mathcal{C} \subset F^n$ com distância mínima d, assim, a quantidade de erros que o código pode corrigir é $t = \left[\frac{d-1}{2}\right]$. Suponha que foi transmitida uma palavra $c \in \mathcal{C}$ e que chegou até o receptor a palavra $r \in F^n$, temos então as seguintes possibilidades:

i) Durante a transmissão foram cometidos uma quantidade de erros menor ou igual a t, neste caso podemos concluir que a palavra enviada foi c, pois é a única que satisfaz a condição $r \in D(c,t)$.

ii) Durante a transmissão foram cometidos uma quantidade de erros maior que t, neste caso $r \notin D(c,t)$, assim teremos dois casos possíveis:

1. $r \in D(c',t)$ com $c \neq c'$, neste caso concluiremos de forma incorreta que a palavra enviada foi c';

2. $r \notin D(c',t)$ para toda palavra $c' \in \mathcal{C}$, assim não poderemos corrigir o erro.

Observe que a eficiência deste método de correção de erros depende muito do canal que será utilizado para enviar o sinal e da distância mínima entre as palavras do código. Caso a probabilidade de erros seja pequena, podemos receber palavras com no máximo t erros, assim seremos capazes de fazer a correção do erro sem incertezas, no entanto, caso a quantidade de erros seja maior que t podemos corrigir a palavra de forma incorreta. Portanto, nunca teremos certeza que não houve erro no processo de correção, o máximo que teremos é uma probabilidade de acerto.

1.3 Equivalência de Códigos

No exemplo do código do robô, para possibilitar a correção de erros, utilizamos o código do Exemplo 1.2 que tem distância mínima $d = 3$ e portanto é capaz de corrigir no máximo um erro e detectar até dois. Mas, poderíamos ter escolhido o código $\{00000, 11010, 01101, 10111\}$ que também tem distância mínima $d = 3$ e além disso, fazendo a correspondência

$$00000 \longleftrightarrow 00000 \quad 01011 \longleftrightarrow 11010 \quad 10110 \longleftrightarrow 01101 \quad 11101 \longleftrightarrow 1011,$$

temos que a distância entre duas palavras quaisquer de um código é equivalente a distância entre as duas palavras correspondentes do outro. Por exemplo $d(01011, 11101) = 3$ e $d(11010, 10111) = 3$. Assim, em termos de codificação e correção de erros, os dois códigos são equivalentes.

Definição 1.13. Sejam F um alfabeto e n um número natural. Diremos que uma função $H : F^n \longrightarrow F^n$ é uma isometria de F^n se ela preserva distância de Hammning, ou seja,

se

$$d(H(u), H(v)) = d(u, v), \quad \forall\ u, v \in F^n.$$

Usaremos o conceito de isometria para definir equivalência entre dois códigos contidos em um mesmo espaço F^n. Vejamos primeiro algumas propriedades de uma isometria.

Proposição 1.14. *Toda isometria de F^n é uma bijeção de F^n.*

Demonstração. Dados $u, v \in F^n$, com $u \neq v$, suponha por contradição que $H(u) = H(v)$ e que H seja uma isometria. Assim, temos que $d(H(u), H(v)) = 0$, pois $H(u) = H(v)$. Por outro lado, como H é uma isometria, temos $d(u, v) = d(H(u), H(v)) = 0$, logo $d(u, v) = 0$, de onde segue que $u = v$. Um absurdo. Portanto, $H(u) \neq H(v)$. Mostrando assim que H é injetora. Como toda função injetora de um conjunto finito nele mesmo é também sobrejetora, concluímos que H é uma bijeção de F^n. □

Proposição 1.15. *Dado um alfabeto F, temos que*

i) A função identidade de F^n é uma isometria;

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

iii) Se H e G são isometrias de F^n, então $H \circ G$ é uma isometria de F^n.

Demonstração. Sejam F um alfabeto e $u, v \in F^n$ duas palavras quaisquer.

i) Seja $H : F^n \longrightarrow F^n$, temos então que $H(u) = u$ e $H(v) = v$, logo $d(H(u), H(v)) = d(u, v)$. Portanto, H é uma isometria;

ii) Seja $H : F^n \longrightarrow F^n$ uma isometria, segue da proposição anterior que existe H^{-1}. Além disso, temos que

$$d(H^{-1}(u), H^{-1}(v)) = d(H(H^{-1}(u)), H(H^{-1}(v))) = d(u, v).$$

Portanto, H^{-1} é uma isometria de F^n.

iii) Sejam H e G isometrias de F^n. Temos então que,

$$d(H(G(u)), H(G(v))) = d(G(u), G(v)) = d(u, v),$$

mostrando assim que $H \circ G$ é uma isometria. □

Definição 1.16. Sejam $\mathcal{C}$ e $\mathcal{C}'$ dois códigos em F^n, diremos que $\mathcal{C}'$ é equivalente a $\mathcal{C}$ se existir uma isometria H de F^n tal que $H(\mathcal{C}) = \mathcal{C}'$.

Definição 1.17. Seja $I_n = \{1, 2, 3, \cdots, n\}$ o conjunto dos n primeiros números naturais. Qualquer bijeção π do conjunto I_n nele mesmo é chamada de permutação.

Exemplo 1.18. Um exemplo simples é a isometria

$$\begin{array}{rccc} H & : & \{0,1\}^5 & \longrightarrow & \{0,1\}^5 \\ & & (v_1, v_2, v_3, v_4, v_5) & \longrightarrow & (v_5, v_4, v_3, v_2, v_1), \end{array}$$

aplicada ao código do robô $\mathcal{C} = \{00000,\ 01011,\ 10110,\ 11101\} \subset \{0,1\}^5$. Neste caso, obtemos o código $\mathcal{C}' = \{00000, 11010, 01101, 10111\}$ equivalente ao código $\mathcal{C}$.

Em geral, uma aplicação

$$\begin{array}{rccc} T_\pi & : & F^n & \longrightarrow & F^n \\ & & (v_1, v_2, \cdots, v_n) & \longrightarrow & (v_{\pi(1)}, v_{\pi(2)}, \cdots, v_{\pi(n)}), \end{array}$$

é uma isometria de F^n.

De fato, considerando as palavras $u = (u_1, u_2, \cdots, u_n), v = (v_1, v_2, \cdots, v_n) \in F^n$, para todo $1 \leq i \leq n$, caso a coordenada v_i seja diferente da coordenada u_i a coordenada $v_{\pi(i)}$ será diferente da coordenada $u_{\pi(i)}$, assim, caso a i-ésima coordenada tenha contribuição igual a 1 para $d(u, v)$, a $\pi(i)$-ésima coordenada terá também contribuição igual a 1 para $d(T_\pi(u), T_\pi(v))$.

Segue diretamente da Proposição 1.15 que a equivalência de códigos é uma relação de equivalência, isto é, satisfaz as seguintes condições:

i) Reflexiva: todo código é equivalente a si próprio;

ii) Simétrica: se $\mathcal{C}'$ é equivalente a $\mathcal{C}$ então $\mathcal{C}$ é equivalente a $\mathcal{C}'$;

iii) Transitiva: se $\mathcal{C}''$ é equivalente a $\mathcal{C}'$ e se $\mathcal{C}'$ é equivalente a $\mathcal{C}$, então $\mathcal{C}''$ é equivalente a $\mathcal{C}$.

Capítulo 2

Códigos Lineares

Nesta seção apresentaremos a classe dos códigos lineares. Neste caso, o alfabeto F é um conjunto de elementos satisfazendo as propriedades de um corpo. E o código é um subespaço vetorial. Utilizamos como referências [15], [11], [4], [7], [9] e [8].

2.1 Anéis, Corpos e Espaços Vetoriais

Definição 2.1. Uma estrutura matemática constituída por um conjunto A não vazio e um par de operações,

$$\begin{array}{rcccl} + & : & A \times A & \longrightarrow & A \\ & & (a,b) & \longmapsto & a+b. \end{array} \quad \text{e} \quad \begin{array}{rcccl} \cdot & : & A \times A & \longrightarrow & A \\ & & (a,b) & \longmapsto & a \cdot b, \end{array}$$

que chamaremos, respectivamente, de adição e multiplicação, é chamado anel comutativo com unidade se satisfaz as seguintes propriedades:
A_1. Associatividade da adição:

$$\forall\ a,b,c \in A, \qquad (a+b)+c = a+(b+c).$$

A_2. Comutatividade da adição:

$$\forall\ a,b \in A, \qquad a+b = b+a.$$

A_3. Existência de elemento neutro (chamado zero) para adição:

$$\exists\ 0_A \in A, \qquad a+0_A = 0_A + a = a, \quad \forall\ a \in A.$$

A_4. Existência de elemento inverso (chamado simétrico aditivo) para adição:

$$\forall\ a \in A,\ \exists\ -a \in A, \qquad a+(-a) = -a+a = 0_A.$$

M_1. Associatividade da multiplicação:

$$\forall\ a, b, c \in A, \qquad (a \cdot b) \cdot c = a \cdot (b \cdot c).$$

M_2. Comutatividade da multiplicação:

$$\forall\ a, b \in A, \qquad a \cdot b = b \cdot a.$$

M_3. Existência de elemento neutro (chamado unidade) para multiplicação:

$$\exists\ 1_A \in A, \qquad a \cdot 1_A = 1_A \cdot a = a, \quad \forall\ a \in A.$$

AM. Distributividade da multiplicação com relação à adição:

$$\forall\ a, b, c \in A, \qquad a \cdot (b + c) = a \cdot b + a \cdot c \ \text{ e } \ (a + b) \cdot c = a \cdot c + b \cdot c.$$

Chamamos simplesmente de anel a estrutura matemática que não goza das propriedade M_3 e M_2, mas satisfaz todas as outras propriedades da adição e multiplicação de um anel comutativo com unidade. O anel é denotado por $(A, +, \cdot)$, ou simplesmente por A quando a definição das operações estiver clara. Os elementos $a + b$ e $a \cdot b$ são chamados, respectivamente, de soma e produto de a e b. Muitas vezes omitimos o símbolo da multiplicação e escrevemos simplesmente ab para representar o produto de a e b.

Definição 2.2. Sejam $(A, +, \cdot)$ um anel e L um subconjunto não vazio de A. Diz-se que L é um subanel de A se:

i) O subconjunto L é fechado para as operações de adição e multiplicação do anel A;

ii $(L, +, \cdot)$ também é um anel.

Definição 2.3. Um anel A é chamado de domínio de integridade, se possuir a seguinte propriedade:

$$\forall\ a, b \in A, \quad a \neq 0 \text{ e } b \neq 0 \Rightarrow a \cdot b \neq 0.$$

Exemplo 2.4. Os conjuntos dos números inteiros $\mathbb{Z}$, dos números racionais $\mathbb{Q}$, dos números reais $\mathbb{R}$ e dos números complexos $\mathbb{C}$, com as operações de adição e multiplicação, são os exemplos de domínio de integridade mais conhecidos. Já o conjunto das matrizes com as operações usuais, apesar de ser um anel, não é comutativo e não é um domínio de integridade.

Definição 2.5. Um elemento a de um anel A é dito inversível se existir um elemento $b \in A$, tal que $a \cdot b = b \cdot a = 1$. Denotamos o elemento b por a^{-1} e dizemos que a^{-1} é o inverso de a.

Exemplo 2.6. Os únicos elementos inversíveis do anel $\mathbb{Z}$ são 1 e -1. Neste caso, 1 e -1 são os inversos deles mesmos. Por outro lado, todos os elementos não nulos dos anéis $\mathbb{Q}$ e $\mathbb{R}$ possuem inversos.

Definição 2.7. Um anel comutativo com unidade no qual todo elemento não nulo é inversível é chamado de corpo.

Definição 2.8. Sejam $(A, +, \cdot)$ e $(B, \oplus, \odot)$ dois anéis. Chamamos de homomorfismo de A em B a toda aplicação $f : A \to B$ tal que, para quaisquer que sejam $x, y \in A$:

$$f(x + y) = f(x) \oplus f(y) \qquad \text{e} \qquad f(x \cdot y) = f(x) \odot f(y).$$

Definição 2.9. Seja $f : A \to B$ um homomorfismo do anel A no anel B. Se f for um bijeção, então f será chamado de isomorfismo do anel A no anel B. Neste caso dizemos que os anéis A e B são isomorfos.

Na próxima seção apresentaremos os corpos de inteiros módulo p, uma classe importante de corpos no estudo e no desenvolvimento de códigos corretores de erros. Vejamos agora a definição de espaço vetorial.

Definição 2.10. Uma estrutura matemática constituída por um conjunto V não vazio, cujos elementos serão chamados de vetores, um corpo F e um par de operações,

$$\begin{array}{rccccc} + & : & V \times V & \longrightarrow & V \\ & & (u, v) & \longmapsto & u + v. \end{array} \quad \text{e} \quad \begin{array}{rccccc} \cdot & : & F \times V & \longrightarrow & V \\ & & (\alpha, u) & \longmapsto & \alpha \cdot u, \end{array}$$

que chamaremos, respectivamente, de adição e multiplicação por escalar, é chamado espaço vetorial sobre o corpo F se satisfaz as seguintes propriedades:
A_1. Associatividade da adição:

$$\forall\ u, v, w \in V, \qquad (u + v) + w = u + (v + w).$$

A_2. Comutatividade da adição:

$$\forall\ u, v \in V, \qquad u + v = v + u.$$

A_3. Existência de elemento neutro (chamado zero) para adição:

$$\exists\ 0_V \in V, \qquad u + 0_V = 0_V + u = u, \ \ \forall\ u \in V.$$

A_4. Existência de elemento inverso (chamado simétrico aditivo) para adição:

$$\forall\ u \in V,\ \exists\ -u \in V, \qquad u + (-u) = -u + u = 0_V.$$

M_1. Associatividade da multiplicação por escalar:

$$\forall\ \alpha, \beta, \in F\ \ \forall u \in V \qquad (\alpha\beta) \cdot u = \alpha(\beta \cdot u).$$

M_2. Identidade multiplicativa:

$$\forall u \in V, \qquad 1_F \cdot u = u$$

D_1. Distributividade do escalar:

$$\forall\ u, v, \in V,\ \text{e}\ \forall\ \alpha \in F, \qquad \alpha \cdot (u + v) = \alpha \cdot u + \alpha \cdot v.$$

D_2. Distributividade do vetor:

$$\forall\ u \in V,\ \text{e}\ \forall\ \alpha, \beta \in F, \qquad (\alpha + \beta) \cdot u = \alpha \cdot u + \beta \cdot u.$$

O elemento $u+v$ é chamado de soma de u e v, e o elemento $\alpha \cdot u$ é denominado produto por escalar de α por u. Representaremos o espaço vetorial simplesmente por V quando o corpo de escalares estiver subentendido.

Exemplo 2.11. Os exemplos mais comuns de espaços vetoriais são: o corpo $\mathbb{R}$, o plano $\mathbb{R}^2$ e o espaço $\mathbb{R}^3$. Nos quais a soma $u + v$ é obtida somando coordenada a coordenada e o produto por escolar $\alpha \cdot u$ é feito multiplicando α por cada um das coordenadas de u.

Exemplo 2.12. Em geral, dado um corpo F e um natural $n \geq 1$, temos que o conjunto

$$F^n = \underbrace{F \times F \times \cdots \times F}_{n\ \text{vezes}} = \{(a_1, a_2, \cdots, a_n); a_i \in F, \forall\ i = 1, 2, \cdots, n\},$$

tem uma estrutura de espaço vetorial sobre F com as operações:

$$\begin{aligned} (a_1, \cdots, a_n) + (b_1, \cdots, b_n) &= (a_1 + b_1, \cdots, a_n + b_n), \quad \forall\ (a_1, \cdots, a_n), (b_1, \cdots, b_n) \in F^n, \\ \alpha \cdot (a_1, \cdots, a_n) &= (\alpha a_1, \cdots, \alpha a_n), \qquad\qquad \forall\ \alpha \in F\ \text{e}\ \forall\ (a_1, \cdots, a_n) \in F^n. \end{aligned}$$

Uma base de um espaço vetorial V é um conjunto $\mathcal{B} \subset V$ ordenado e linearmente independente (L.I.) que gera V, ou seja, é um conjunto $\mathcal{B} = \{v_1, v_2, \cdots, v_k\}$ no qual,

$$v_i \neq \alpha_1 v_1 + \alpha_2 v_2 + \cdots + \alpha_{i-1} v_{i-1} + \alpha_{i+1} v_{i+1} + \cdots + \alpha_k v_k,$$

para quaisquer $\alpha_1, \alpha_2, \cdots, \alpha_{i-1}, \alpha_{i+1}, \cdots, \alpha_k \in F$ com $i = 1, 2, \cdots, k$, e além disso, para cada $v \in V$, existem únicos $\beta_1, \beta_2, \cdots, \beta_k \in F$, tais que,

$$v = \beta_1 v_1 + \beta_2 v_2 + \cdots + \beta_k v_k, \quad \forall\ v \in V.$$

Os elementos $\beta_1, \beta_2, \cdots, \beta_k \in F$ são as coordenadas do vetor v na base $\mathcal{B}$. Em geral a base de um espaço vetorial não é única, no entanto, todas têm a mesmas quantidade de elementos. O número k é a dimensão do espaço vetorial V.

Proposição 2.13. *Seja V um espaço vetorial de dimensão k e $\mathcal{B} = \{v_1, v_2, \cdots, v_k\}$ uma base para V. Considere o conjunto*

$$\mathcal{B}' = \{\mu_1 v_{\pi(1)}, \mu_2 v_{\pi(2)}, \cdots, \mu_j v_{\pi(j)} + \lambda v_j, \cdots, \mu_k v_{\pi(k)}\},$$

onde π é uma permutação, $j \in \{1, 2, \cdots, k\}$ e $\mu_1, \mu_2, \cdots, \mu_k, \lambda \in F$, com $\mu_1 \cdot \mu_2 \cdot ... \cdot \mu_k \neq 0$. Então, sendo $\mathcal{B}$ uma base de V, temos que $\mathcal{B}'$ também é uma base para o código V.

Demonstração. O caso em que $\lambda = 0_F$ temos que , para cada i,

$$v_i \neq \alpha_1 v_1 + \alpha_2 v_2 + \cdots + \alpha_{i-1} v_{i-1} + \alpha_{i+1} v_{1+1} + \cdots + \alpha_k v_k,$$

implica,

$$\mu_i v_{\pi(i)} \neq \alpha_{\pi(1)} \mu_1 v_{\pi(1)} + \cdots + \alpha_{\pi(i-1)} \mu_{i-1} v_{\pi(i-1)} + \alpha_{\pi(i+1)} \mu_{i+1} v_{\pi(i+1)} + \cdots + \alpha_{\pi(k)} \mu_k v_{\pi(k)},$$

pois,

$$\alpha_{\pi(1)} \mu_1 \mu_i^{-1}, \cdots, \alpha_{\pi(i-1)} \mu_{i-1} \mu_i^{-1}, \alpha_{\pi(i+1)} \mu_{i+1} \mu_i^{-1}, \cdots, \alpha_{\pi(k)} \mu_k \mu_i^{-1} \in F,$$

e dado que, para cada $v \in V$ existem,

$$\beta_1, \beta_2, \cdots, \beta_k \in F,$$

únicos, tais que,

$$v = \beta_1 v_1 + \beta_2 v_2 + \cdots + \beta_k v_k, \quad \forall\ v \in V,$$

existem,

$$\beta_1' = \beta_{\pi(1)} \mu_1^{-1}, \beta_2' = \beta_{\pi(2)} \mu_2^{-1}, \cdots, \beta_k' = \beta_{\pi(k)} \mu_k^{-1} \in F,$$

únicos, tais que,

$$v = \beta_1' v_{\pi(1)} + \beta_2' v_{\pi(2)} + \cdots + \beta_k' v_{\pi(k)}, \quad \forall\ v \in V.$$

O caso em que $\lambda \neq 0_F$, sem perda de generalidade, podemos considerar $\mu = 1$ e π como sendo função identidade, assim

$$\mathcal{B}' = \{v_1, v_2, \cdots, v_i + \lambda v_j, \cdots, v_k\}.$$

Para provar que os vetores de $\mathcal{B}'$ são linearmente independentes, suponha por contradição

que existe $v_r \in \mathcal{B}'$, tal que

$$v_r = \alpha_1 v_1 + \alpha_2 v_2 + \cdots \alpha_{r-1} v_{r-1} + \alpha_{r+1} v_{r+1} + \cdots + \alpha_k v_k.$$

Assim, se $v_r = v_i + \lambda v_j$ temos

$$v_i + \lambda v_j = \alpha_1 v_1 + \alpha_2 v_2 + \cdots \alpha_{i-1} v_{i-1} + \alpha_{i+1} v_{i+1} + \cdots + \alpha_j v_j + \cdots + \alpha_k v_k.$$

Daí,

$$v_i = \alpha_1 v_1 + \alpha_2 v_2 + \cdots \alpha_{i-1} v_{i-1} + \alpha_{i+1} v_{i+1} + \cdots + (\alpha_j - \lambda) v_j + \cdots + \alpha_k v_k,$$

com $\alpha_1, \cdots, \alpha_j - \lambda, \cdots, \alpha_k \in F$. Um absurdo.
E se, $v_r \neq v_i + \lambda v_j$, temos que

$$v_r = \alpha_1 v_1 + \cdots + \alpha_i (v_i + \lambda v_j) + \cdots \alpha_{r-1} v_{r-1} + \alpha_{r+1} v_{r+1} + \cdots + \alpha_j v_j + \cdots + \alpha_k v_k.$$

De onde segue que,

$$v_r = \alpha_1 v_1 + \cdots + \alpha_i v_i + \cdots \alpha_{r-1} v_{r-1} + \alpha_{r+1} v_{r+1} + \cdots + (\alpha_j + \lambda) v_j + \cdots + \alpha_k v_k,$$

com $\alpha_1, \cdots, \alpha_j + \lambda, \cdots, \alpha_k \in F$. Um absurdo.
Portanto, os vetores de $\mathcal{B}'$ são linearmente independentes.
Por fim, como $\mathcal{B}$ é uma base, existem $\beta_1, \cdots \beta_i \cdots, \beta_k \in F$ únicos, tais que,

$$v = \beta_1 v_1 + \beta_2 v_2 + \cdots + \beta_i v_i + \cdots + \beta_k v_k, \quad \forall\ v \in V.$$

Assim,

$$v = \beta_1 v_1 + \beta_2 v_2 + \cdots + \beta_i v_i + \cdots + \beta_i \lambda v_j - \beta_i \lambda v_j + \cdots + \beta_k v_k, \quad \forall\ v \in V.$$

Logo, existem únicos $\beta_1, \beta_2, \cdots, \beta_{j-1}, \beta_j - \beta_i \lambda, \beta_{j+1}, \cdots, \beta_k \in F$, tais que

$$v = \beta_1 v_1 + \cdots + \beta_i (v_i + \lambda v_j) + \cdots + (\beta_j - \beta_i \lambda) v_j + \cdots + \beta_k v_k, \quad \forall\ v \in V.$$

□

Esta proposição garante que dada uma base $\mathcal{B}$ para uma espaço vetorial V, podemos obter uma outra base $\mathcal{B}'$ através de uma sequência de operações do tipo:

- Permutação de dois elementos da base;
- Multiplicação de um elemento da base por um escalar não nulo;

- Substituição de um vetor da base por ele mesmo somado com um múltiplo escalar de outro vetor da base.

Um subespaço vetorial de um espaço vetorial V é um subconjunto de $L \subset V$ que, em relação as operações de V, é ainda um espaço vetorial. Uma maneira prática de verificar que o conjunto L é um subespaço de V é verificando as seguintes propriedades:

1. $0_V \in L$;
2. Se $u, v \in L$ então $u + v \in L$;
3. Se $v \in L$ então, para todo $\alpha \in F$, $\alpha v \in L$.

Dois exemplos importantes de subespaço são o núcleo e a imagem de uma transformação linear.

Definição 2.14. Sejam V e U espaços vetoriais sobre um corpo F. Uma transformação linear $A : V \to U$ é uma correspondência que associa a cada vetor $v \in V$ a um vetor $A(v) = A \cdot v = Av \in U$ de modo que seja válidas, para quaisquer $u, v \in V$ e $\alpha \in F$, as seguintes propriedades:

$$A(u + v) = Au + Av \qquad \text{e} \qquad A(\alpha \cdot v) = \alpha \cdot Av.$$

O vetor Av é a imagem do vetor v pela transformação A.

Definição 2.15. Sejam V e U espaços vetoriais sobre um corpo F e $A : V \to U$ uma transformação linear.

1. O conjunto $\text{Nuc}(A) = \{v \in V \mid A(v) = 0_U\}$ é chamado núcleo de A.

2. O conjunto $\text{Im}(A) = \{u \in U \mid \exists\ v \in V \text{ com } A(v) = u\}$ é chamado imagem de A.

Exemplo 2.16. Dada a transformação linear $A : \mathbb{R}^2 \to \mathbb{R}$, definida por $A(x, y) = y - x$, temos que,

i) $\text{Nuc}(A) = \{(x, y) \in \mathbb{R} \mid x = y\}$, isto é, a reta $y = x$;

ii) $\text{Im}(A) = \mathbb{R}$.

Proposição 2.17. *Sejam V e U espaços vetoriais sobre um corpo F e $A : V \to U$ uma transformação linear. Então, Nuc(A) é um subespaço vetorial de V e Im(A) é um subespaço vetorial de U.*

Demonstração. Note inicialmente que $0_U + A(0_V) = A(0_V) = A(0_V + 0_V) = A(0_V) + A(0_V)$, assim, $0_U + A(0_V) = A(0_V) + A(0_V)$ logo, $A(0_V) = 0_U$. De onde segue que $0_V \in \text{Nuc}(A)$ e $0_U \in \text{Im}(A)$. Além disso, dados $v, w \in \text{Nuc}(A)$ e $\alpha \in F$, temos que $A(v + w) =$

$A(v) + A(w) = 0_U + 0_U = 0_U$ e $A(\alpha \cdot v) = \alpha \cdot A(v) = \alpha \cdot 0_U = 0_U$, mostrando assim que $v + w, \alpha \cdot v \in \text{Nuc}(A)$. Por fim, observe que dados $A(v), A(w) \in \text{Im}(A)$ e $\alpha \in F$, temos que $A(v) + A(w) = A(v + w) \in \text{Im}(A)$ e $\alpha \cdot A(v) = A(\alpha \cdot v) \in \text{Im}(A)$, pois $v+w, \alpha \cdot v \in V$. Portanto, os subconjuntos $\text{Nuc}(A)$ e $\text{Im}(A)$ satisfazem as três propriedades de um subespaço vetorial. □

2.2 Corpos de Inteiros Módulo p

Apresentaremos agora o conceito de congruência módulo m, introduzida pelo Matemático Carl Friedrich Gauss por volta de 1801. Com a ideia apresentada por Gauss foi possível desenvolver um aritmética dos restos da divisão de um número inteiro pelo número fixado m.

Definição 2.18. Seja m um número inteiro maior do que 1. Diremos que dois números inteiros a e b são congruentes módulo m se quando divididos por m, a e b deixam o mesmo resto. Neste caso, escrevemos

$$a \equiv b \mod m.$$

Quando a e b não são congruentes módulo m, escrevemos

$$a \not\equiv b \mod m.$$

Exemplo 2.19. :

- $7 \equiv 12 \mod 5$, pois $7 = 1 \cdot 5 + 2$ e $12 = 2 \cdot 5 + 2$.
- $-4 \equiv 21 \mod 5$, pois $-4 = (-1) \cdot 5 + 1$ e $21 = 4 \cdot 5 + 1$.
- $35 \equiv -13 \mod 6$, pois $35 = 5 \cdot 6 + 5$ e $-13 = (-3) \cdot 6 + 5$.

Veremos agora uma proposição que muitas vezes é apresentada como definição de congruência módulo m.

Proposição 2.20. *Seja m um número inteiro maior do que 1. Temos então que,*

$$a \equiv b \mod m \text{ se, e somente se, } m \text{ divide } b - a.$$

Demonstração. Pelo algoritmo da divisão temos que $a = q_1 m + r_1$ e $b = q_2 m + r_2$, com $0 \leq r_1, r_2 \leq m - 1$. Sem perda de generalidade, vamos supor que $r_1 \leq r_2$. Temos então que,

$$b - a = (q_2 - q_1)m + (r_2 - r_1).$$

Logo, m divide $b-a$ se, e somente se, m divide $r_2 - r_1$. Como $0 \leq r_2 - r_1 \leq m-1$, temos que m divide $b-a$ se, e somente se, $r_2 - r_1 = 0$. Portanto, m divide $b-a$ se, e somente se, $r_2 = r_1$. □

Exemplo 2.21. :

- $7 \equiv 12 \mod 5$, pois $12 - 7 = 5 = 1 \cdot 5$.
- $-4 \equiv 21 \mod 5$, pois $21 - (-4) = 25 = 5 \cdot 5$.
- $35 \equiv -13 \mod 6$, pois $-13 - 35 = -48 = (-8) \cdot 6$.

Proposição 2.22. *Para quaisquer $a, b, c, d, m \in \mathbb{Z}$, com $m > 1$ temos:*

1. *(Reflexividade) $a \equiv a \mod m$;*
2. *(Simetria) se $a \equiv b \mod m$, $b \equiv a \mod m$;*
3. *(Transitividade) $a \equiv b \mod m$ e $b \equiv a \mod m$, então $a \equiv c \mod m$;*
4. *(Compatibilidade com a soma e diferença) Podemos somar e subtrair membro a membro*

$$\begin{cases} a \equiv b \mod m \\ c \equiv d \mod m \end{cases} \Rightarrow \begin{cases} a + c \equiv b + d \mod m \\ a - c \equiv b - d \mod m \end{cases}$$

   Em particular, $a \equiv b \mod m$, então $ka \equiv kb \mod m$ para todo $k \in \mathbb{Z}$.

5. *(Compatibilidade com do produto) Podemos somar e subtrair membro a membro*

$$\begin{cases} a \equiv b \mod m \\ c \equiv d \mod m \end{cases} \Rightarrow a \cdot c \equiv b \cdot d \mod m$$

   Em particular, $a \equiv b \mod m$, então $a^k \equiv b^k \mod m$ para todo $k \in \mathbb{N}$.

6. *(Cancelamento) Se $mdc(c, m) = 1$, então*

$$ac \equiv bc \bmod m \Leftrightarrow a \equiv b \mod m.$$

Demonstração. :

1. Basta observar que m divide $a - a = 0$;
2. Se $a \equiv b \mod m$, então $b - a = qm$ com q inteiro. Daí, $a - b = (-q)m$ e, portanto, $b \equiv a \mod m$;
3. Se $a \equiv b \mod m$ e $b \equiv c \mod m$, temos que $b - a = q_1 m$ e $c - b = q_2 m$, com $q_1,\ q_2 \in \mathbb{Z}$. Somando membro a membro essas duas últimas igualdades, obtemos que $c - a = (q_1 + q_2)m$. De onde concluímos que $a \equiv c \mod m$;

4. Se $a \equiv b \mod m$ e $c \equiv d \mod m$, temos que $b - a = q_1 m$ e $d - c = q_2 m$, com $q_1,\ q_2 \in \mathbb{Z}$. Somando membro a membro essas duas últimas igualdades, obtemos que $(b + d) - (a + c) = (q_1 + q_2)m$, logo $a + c \equiv b + d \mod m$. De modo análogo, temos $a - c \equiv b - d \mod m$;

5. Se $a \equiv b \mod m$ e $c \equiv d \mod m$, temos que $b-a = q_1 m$ e $d-c = q_2 m$, com $q_1,\ q_2 \in \mathbb{Z}$. E note que $bd-ac = bd-bc+bc-ac = (d-c)b+(b-a)c = q_2 mb+q_1 mc = (q_2 b+q_1 c)m$. Mostrando assim que $ac \equiv bd \mod m$.

6. Observe que $bc - ac = (b - a)c$, como $mcd(c, m) = 1$ temos que, m divide $(b - c)c$ se, e somente se, m divide $(b - c)$. Portanto, $ac \equiv bc \mod m$ se, e somente se, $a \equiv b \mod m$.

□

O três primeiros itens da propriedade nos diz que a relação de congruência módulo m é uma relação de equivalência. As demais mostram que esta relação tem um comportamento similar a relação de igualdade usual.

A proposição a seguir nos permite dividir os números inteiros em classes denominadas de classes de equivalências.

Proposição 2.23. *Todo número inteiro a é congruente módulo m a um e somente um dos números inteiros $0, 1, 2, \cdots, m - 2, m - 1$.*

Demonstração. De fato, qualquer que seja o número inteiro a, pelo algoritmo da divisão temos que $a = qm + r$, com $q, r \in \mathbb{Z}$ e $0 \leq r \leq m - 1$. De onde segue que $r = b$ para algum $b \in \{0, 1, \cdots, m - 2, m - 1\}$. Assim, $b - a = b - qm - r = -qm$, e portanto, $a \equiv b \mod m$. Pela unicidade do resto na divisão temos que b é único e precisamente igual a r. □

Vamos representar cada uma das m classes de equivalência módulo m por $\overline{x}$, com $x \in \{0, 1, \cdots, m - 2, m - 1\}$. Ou seja, $\overline{x} = \{y \in \mathbb{Z} \mid x \equiv y \mod m\}$.

Definimos o conjunto $F_m = \{\overline{0}, \overline{1}, \cdots, \overline{m-1}\}$ como sendo o conjunto das classes de equivalência módulo m. Como na divisão por m o resto da soma e da multiplicação de dois números inteiros a e b dependem, respectivamente, apenas da soma ou da multiplicação dos restos de a e b, podemos definir uma soma e uma multiplicação em F_m da seguinte maneira,

$$\overline{a} + \overline{b} = \overline{a + b} \qquad \text{e} \qquad \overline{a} \cdot \overline{b} = \overline{a \cdot b}.$$

Estas duas operações estão bem definidas, isto é, não depende da escolha dos representantes. De fato, dados $a \equiv c \mod m$ e $b \equiv d \mod m$, pela Proposição 2.22, temos que

$$a + b \equiv c + d \mod m,$$

e,

$$a \cdot b \equiv c \cdot d \mod m.$$

Exemplo 2.24. Dado o conjunto $F_4 = \{\overline{0}, \overline{1}, \overline{2}, \overline{3}\}$, temos as seguintes tábuas de adição e multiplicação:

$+$	$\overline{0}$	$\overline{1}$	$\overline{2}$	$\overline{3}$
$\overline{0}$	$\overline{0}$	$\overline{1}$	$\overline{2}$	$\overline{3}$
$\overline{1}$	$\overline{1}$	$\overline{2}$	$\overline{3}$	$\overline{0}$
$\overline{2}$	$\overline{2}$	$\overline{3}$	$\overline{0}$	$\overline{1}$
$\overline{3}$	$\overline{3}$	$\overline{0}$	$\overline{1}$	$\overline{2}$

e

$\cdot$	$\overline{0}$	$\overline{1}$	$\overline{2}$	$\overline{3}$
$\overline{0}$	$\overline{0}$	$\overline{0}$	$\overline{0}$	$\overline{0}$
$\overline{1}$	$\overline{0}$	$\overline{1}$	$\overline{2}$	$\overline{3}$
$\overline{2}$	$\overline{0}$	$\overline{2}$	$\overline{0}$	$\overline{2}$
$\overline{3}$	$\overline{0}$	$\overline{3}$	$\overline{2}$	$\overline{1}$

Observe que os elementos $\overline{0}$ e $\overline{1}$ têm, respectivamente, o mesmo comportamento que os elementos 1 e 0 na aritmética dos números inteiros. Por outro lado, diferente dos números inteiros, temos que $\overline{2} \neq \overline{0}$, no entanto, $\overline{2} \cdot \overline{2} = \overline{2 \cdot 2} = \overline{4} = \overline{0}$. Veja que o mesmo não ocorre com o exemplo a seguir.

Exemplo 2.25. Dado o conjunto $F_5 = \{\overline{0}, \overline{1}, \overline{2}, \overline{3}, \overline{4}\}$, temos as seguintes tábuas de adição e multiplicação:

$+$	$\overline{0}$	$\overline{1}$	$\overline{2}$	$\overline{3}$	$\overline{0}$
$\overline{0}$	$\overline{0}$	$\overline{1}$	$\overline{2}$	$\overline{3}$	$\overline{4}$
$\overline{1}$	$\overline{1}$	$\overline{2}$	$\overline{3}$	$\overline{4}$	$\overline{0}$
$\overline{2}$	$\overline{2}$	$\overline{3}$	$\overline{4}$	$\overline{0}$	$\overline{1}$
$\overline{3}$	$\overline{3}$	$\overline{4}$	$\overline{0}$	$\overline{1}$	$\overline{2}$
$\overline{4}$	$\overline{4}$	$\overline{0}$	$\overline{1}$	$\overline{2}$	$\overline{3}$

e

$\cdot$	$\overline{0}$	$\overline{1}$	$\overline{2}$	$\overline{3}$	$\overline{4}$
$\overline{0}$	$\overline{0}$	$\overline{0}$	$\overline{0}$	$\overline{0}$	$\overline{4}$
$\overline{1}$	$\overline{0}$	$\overline{1}$	$\overline{2}$	$\overline{3}$	$\overline{4}$
$\overline{2}$	$\overline{0}$	$\overline{2}$	$\overline{4}$	$\overline{1}$	$\overline{3}$
$\overline{3}$	$\overline{0}$	$\overline{3}$	$\overline{1}$	$\overline{4}$	$\overline{2}$
$\overline{4}$	$\overline{0}$	$\overline{4}$	$\overline{3}$	$\overline{2}$	$\overline{1}$

Observe que, dados $\overline{a}, \overline{b} \in F_5$, se $\overline{a} \neq \overline{0}$ e $\overline{b} \neq \overline{0}$ então, $\overline{a} \cdot \overline{b} \neq \overline{0}$. Esta propriedade está relacionada ao fato do número 5 ser primo.

Proposição 2.26. *Seja m um número inteiro maior que 1. O conjunto $F_m = \{\overline{0}, \overline{1}, \cdots, \overline{m-1}\}$ com as operações de adição e multiplicação definidas por,*

$$\overline{a} + \overline{b} = \overline{a+b} \qquad e \qquad \overline{a} \cdot \overline{b} = \overline{a \cdot b}, \qquad \forall\ \overline{a}, \overline{b} \in F_m,$$

forma um anel comutativo com unidade conhecido como anel dos inteiros módulo m.

Demonstração. Sejam $\overline{a}, \overline{b}, \overline{c} \in F_m$, temos que

A_1. $(\overline{a} + \overline{b}) + \overline{c} = \overline{a+b} + \overline{c} = \overline{(a+b)+c} = \overline{a+(b+c)} = \overline{a} + \overline{b+c} = \overline{a} + (\overline{b} + \overline{c})$;

A_2. $\overline{a} + \overline{b} = \overline{a+b} = \overline{b+a} = \overline{b} + \overline{a}$;

A_3. $\overline{a} + \overline{0} = \overline{0} + \overline{a} = \overline{a+0} = \overline{a}$;

A_4. $\overline{a} + \overline{m-a} = \overline{m-a} + \overline{a} = \overline{a+m-a} = \overline{m} = \overline{0}$;

M_1. $(\overline{a}\cdot\overline{b})\cdot\overline{c} = \overline{a\cdot b}\cdot\overline{c} = \overline{(a\cdot b)\cdot c} = \overline{a\cdot(b\cdot c)} = \overline{a}\cdot\overline{b\cdot c} = \overline{a}\cdot(\overline{b}\cdot\overline{c})$;

M_2. $\overline{a}\cdot\overline{b} = \overline{a\cdot b} = \overline{b\cdot a} = \overline{b}\cdot\overline{a}$;

M_3. $\overline{a}\cdot\overline{1} = \overline{1}\cdot\overline{a} = \overline{a\cdot 1} = \overline{a}$;

AM. $\overline{a}\cdot(\overline{b}+\overline{c}) = \overline{a}\cdot\overline{b+c} = \overline{a\cdot(b+c)} = \overline{ab+ac} = \overline{ab}+\overline{ac}$. □

Dado que F_m é um anel comutativo com unidade é interessante saber quais são os elementos inversíveis de F_m.

Exemplo 2.27. Observando o conjunto F_4 e a tábua de multiplicação do Exemplo 2.24, temos que não existe $\overline{a} \in F_4$ tal que $\overline{2}\cdot\overline{a} = \overline{1}$, ou seja, $\overline{2}$ não tem inverso em F_4. Por outro lado, veja que no caso do conjunto F_5, apresentado no Exemplo 2.25, todos os elementos não nulos são inversíveis.

A proposição a seguir nos diz quando um elemento $\overline{a} \in F_m$ tem inverso multiplicativo.

Proposição 2.28. *Seja m um número inteiro maior que do 1. Um elemento não nulo $\overline{a} \in F_m$, tem inverso multiplicativo em F_m se, e somente se, $mdc(a, m) = 1$.*

Demonstração. Suponha por contradição que existe $\overline{b} \in F_m$ tal que $\overline{a}\cdot\overline{b} = \overline{1}$ e que $mdc(a, m) = d > 1$. Note que $\overline{a}\cdot\overline{b} = \overline{1}$ é equivalente a dizer que $a\cdot b \equiv 1 \bmod m$, ou ainda, que existe um inteiro q tal que $ab - 1 = qm$. De onde segue que $ab - qm = 1$. Por outro lado, como $mdc(a, m) = d$, temos que existem inteiros q_1 e q_2, tais que $a = q_1 d$ e $m = q_2 d$. Substituindo esses dois valores na equação $ab - qm = 1$, obtemos que $q_1 db - qq_2 d = 1$, ou ainda, $d(q_1 b - qq_2) = 1$. Veja que temos um produto de dois inteiros resultando em 1, sendo um deles maior que 1. Um absurdo. Portanto, devemos ter $d = 1$.

Supondo agora que $mdc(a, m) = 1$, pela relação de Bézout, existem números inteiros b e q não ambos nulos tais que, $ab + mq = 1$. De onde segue que $ab - 1 = (-q)m$, logo $a\cdot b \equiv 1 \bmod m$. Portanto, $\overline{a}\cdot\overline{b} = \overline{1}$. Mostrando assim que existe o inverso do elemento $\overline{a}$. □

Esta última proposição garante que o conjunto F_p com as operações de adição e multiplicação definidas anteriormente formam um corpo para todo número primo p. De fato, dado que p é primo, temos que $mdc(p, x) = 1$ para todo $x \in \{1, 2, \cdots, p-1\}$,e portanto, todo elemento não nulo de F_p é inversível. Além disso, Uma consequência direta desta proposição é que, dados $\overline{a}, \overline{b} \in F_p$ com p primo, temos que $\overline{a}\cdot\overline{b} = \overline{0}$ se, e somente se, $\overline{a} = \overline{0}$ ou $\overline{b} = \overline{0}$. Na próxima seção usaremos o corpo $F_2 = \{\overline{0}, \overline{1}\}$ para construir o código de Hamming.

2.3 Código de Hamming

Os códigos de Hamming foram desenvolvidos por Richard W. Hamming por volta de 1950. Trata-se de uma família de códigos binários que são utilizados até hoje devido a sua baixa

complexidade e é utilizado para a correção de erros simples. Nos códigos de Hamming temos os seguintes parâmetros:

- O comprimento n das palavras é dado por $n = 2^r - 1$, com $r > 1$;
- O número de bits de informação é $k = 2^r - (r + 1)$;
- O número de bits de paridade (redundância) é $r = n - k$.

Desta maneira, ao falar do código de Hamming (n, k), ou simplesmente $ham(n, k)$, estamos nos referindo ao código cujas palavras têm comprimento n, sendo k dígitos de informação e $n - k$ dígitos de paridade.

O código de Hamming (n, k) é um subconjunto do espaço $F_2^n = \{\overline{0}, \overline{1}\}^n$. Para simplificar a notação, a partir de agora, vamos escrever simplesmente 0 e 1 no lugar de $\overline{0}$ e $\overline{1}$. Assim, por exemplo, a palavra $(\overline{0}, \overline{0}, \overline{1}, \overline{1}, \overline{0}, \overline{0}, \overline{1})$ será representada por $(0, 0, 1, 1, 0, 0, 1)$, ou simplesmente por 0011001.

Dada uma palavra $x = (x_1, x_2, x_3, \cdots, x_n) \in ham(n, k)$, temos que a i-ésima coordenada será um dígito de paridade P_α se $i = 2^{\alpha-1}$, com $\alpha \in \mathbb{N}$, e será um dígito de informação caso contrário. Por exemplo, no caso da palavra $x = (x_1, x_2, x_3, x_4, x_5, x_6, x_7) \in ham(7, 4)$, temos que x_1, x_2 e x_4 são os dígitos de paridades P_1, P_2 e P_3, respectivamente, e x_3, x_5, x_6 e x_7 são os dígitos de informação D_1, D_2, D_3 e D_4, respectivamente.

Considere a palavra $x = (x_1, x_2, x_3, \cdots, x_n) \in ham(n, k)$, temos que cada posição i, com $i \in \{1, 2, 3, \cdots, n\}$, tem uma representação binária, ou ainda, cada uma dessas posições podem ser representadas por uma sequência de r dígitos. No caso da representação das potências de 2, nesta sequência existe uma posição em que o dígito é igual a 1 e os demais são todos iguais a zero, isto é, dada a potência $2^{\alpha-1}$, temos que, em sua representação binária, o dígito da $(r-\alpha+1)$-ésima posição será igual a 1 e todos as demais iguais a 0. Por exemplo, no caso em que $n = 7$, temos $r = 3$, assim, o número $4 = 2^{3-1}$ pode ser representado por 100_2.

Seja $i = 2^{\alpha-1}$, com $\alpha \in \{1, 2, \cdots, r\}$ e $B_{j1}B_{j2}B_{j3}\cdots B_{jr}$ a representação binária da posição j. O dígito de paridade P_α que aparece na posição i da palavra v é dado pela soma de todos os dígitos de informação D_θ, que aparecem numa posição j tal que $B_{j(r-\alpha+1)} = 1$.

Exemplo 2.29. Considere a palavra $x = (x_1, x_2, x_3, x_4, x_5, x_6, x_7) \in ham(7, 4)$. Escrevendo os índices na base binária temos que,

Posição na base decimal	1	2	3	4	5	6	7
Posição na base binária	001_2	010_2	011_2	100_2	101_2	110_2	111_2
Dígito	x_1	x_2	x_3	x_4	x_5	x_6	x_7
Tipo de dígito	P_1	P_2	D_1	P_3	D_2	D_3	D_4

.

Observe que $1 = 00\mathbf{1}_2$, assim o primeiro dígito de paridade P_1 é dado pela soma de todas os dígitos de informação que aparecem em posições cuja representação na base binária apresenta o dígito 1 na posição mais a direita, que neste caso são, $3 = 01\mathbf{1}_2$, $5 = 10\mathbf{1}_2$ e $7 = 11\mathbf{1}_2$. Temos então que,

$$P_1 = x_3 + x_5 + x_7.$$

De modo análogo, temos

$$\begin{aligned} P_2 &= x_3 + x_6 + x_7, \\ P_3 &= x_5 + x_6 + x_7. \end{aligned}$$

Assim, para enviar a mensagem 1001 com 4 bits de informação usando $ham(7,4)$, temos que a palavra a ser enviada é dada por

x_1	x_2	x_3	x_4	x_5	x_6	x_7
P_1	P_2	1	P_3	0	0	1

.

Neste caso temos,

$$\begin{aligned} P_1 &= 1 + 0 + 1 = 0; \\ P_2 &= 1 + 0 + 1 = 0; \\ P_3 &= 0 + 0 + 1 = 1. \end{aligned}$$

De onde segue que a palavra a ser enviada é dada por,

x_1	x_2	x_3	x_4	x_5	x_6	x_7
0	0	1	1	0	0	1

.

No exemplo anterior, uma maneira fácil e prática de obter a palavra codificada 0011001 seria por meio da matriz da multiplicação de matrizes. Por exemplo, dada uma palavra qualquer $D_1D_2D_3D_4$ a ser transmitida, temos que a palavra $x = (x_1, x_2, x_3, x_4, x_5, x_6, x_7) \in ham(7,4)$ é dada por,

$$\underset{X_{7\times 1}}{\begin{bmatrix} v_1 \\ v_2 \\ v_3 \\ v_4 \\ v_5 \\ v_6 \\ v_7 \end{bmatrix}} = \underset{X_{7\times 1}}{\begin{bmatrix} 1\cdot D_1 + 1\cdot D_2 + 0\cdot D_3 + 1\cdot D_4 \\ 1\cdot D_1 + 0\cdot D_2 + 1\cdot D_3 + 1\cdot D_4 \\ 1\cdot D_1 + 0\cdot D_2 + 0\cdot D_3 + 0\cdot D_4 \\ 0\cdot D_1 + 1\cdot D_2 + 1\cdot D_3 + 1\cdot D_4 \\ 0\cdot D_1 + 1\cdot D_2 + 0\cdot D_3 + 0\cdot D_4 \\ 0\cdot D_1 + 0\cdot D_2 + 1\cdot D_3 + 0\cdot D_4 \\ 0\cdot D_1 + 0\cdot D_2 + 0\cdot D_3 + 1\cdot D_4 \end{bmatrix}} = \underset{G_{7\times 4}}{\begin{bmatrix} 1 & 1 & 0 & 1 \\ 1 & 0 & 1 & 1 \\ 1 & 0 & 0 & 0 \\ 0 & 1 & 1 & 1 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{bmatrix}} \cdot \underset{D_{4\times 1}}{\begin{bmatrix} D_1 \\ D_2 \\ D_3 \\ D_4 \end{bmatrix}}.$$

Veja que qualquer palavra $D_1D_2D_3D_4$ pode ser codificada apenas multiplicando a

matriz G pela matriz D. Dizemos que G é a matriz geradora do código $ham(7,4)$.

Em geral, os códigos de Hamming tem distância mínima 3, assim, pela Proposição 1.10, temos que o código é capaz de identificar até 2 erros e corrigir no máximo 1. No caso em que ocorre apenas um erro durante a transmissão, o código é capaz de detectar a posição exata onde ocorreu o erro, permitindo assim que seja feita a correção.

Para detectar o erro, no processo de decodificação é realizado o teste de verificação dos bits de paridade da palavra recebida. Sabendo exatamente como foi obtido cada um dos dígitos de paridades P_α, o decodificador consegue testar a paridade do dígito recebido. Como os dígitos são elementos do conjunto F_2, para verificar a paridade basta somar o dígito recebido com o dígito gerado a partir da palavra recebida.

Por exemplo, para verificar a paridade do dígito P_1, o decodificador soma o dígito x_1 da palavra recebida com todos os dígitos das posições i para as quais a representação binária apresenta 1 no dígito mais a direita. Assim, caso tenha ocorrido um erro em uma das posições i o resultado será diferente de 0. E desta maneira, o erro terá ocorrido em uma posição na qual o último dígito da representação decimal é igual a 1. De modo análogo, o dígito P_2 pode ser verificado e caso o resultado seja diferente de 0, saberemos que o penúltimo dígito da representação binária da posição onde ocorreu o erro também é igual a 1. Seguindo esse processo é possível encontrar a representação binária exata da posição onde o erro ocorreu.

Exemplo 2.30. Suponha que, ao enviar a palavra 0011001 tenha ocorrido um erro, de modo que a palavra recebida foi 0011011. Para detectar o erro é necessário realizar o teste de verificação de bits paridade. Neste caso, temos

	x_1		x_2		x_3		x_4		x_5		x_6		x_7		
Palavra recebida	0		0		1		1		0		1		1		
Teste P_1	$1\cdot 0$	$+$	$0\cdot 0$	$+$	$1\cdot 1$	$+$	$0\cdot 1$	$+$	$1\cdot 0$	$+$	$0\cdot 1$	$+$	$1\cdot 1$	$=$	0
Teste P_2	$0\cdot 0$	$+$	$1\cdot 0$	$+$	$1\cdot 1$	$+$	$0\cdot 1$	$+$	$0\cdot 0$	$+$	$1\cdot 1$	$+$	$1\cdot 1$	$=$	1
Teste P_3	$0\cdot 0$	$+$	$0\cdot 0$	$+$	$0\cdot 1$	$+$	$1\cdot 1$	$+$	$1\cdot 0$	$+$	$1\cdot 1$	$+$	$1\cdot 1$	$=$	1

Assim, identificando por T_α o resultado do teste de paridade para o dígito P_α, temos que a palavra $T_3T_2T_1$, conhecida como síndrome, determina a posição em que ocorreu o erro, ou seja, o número binário $T_3T_2T_1$ representa exatamente a posição onde existe um erro. Neste exemplo, temos que $110_2 = 6$, assim, o decodificador fará uma alteração no dígito x_6 e concluirá corretamente que a palavra enviada foi 0011001.

No exemplo, poderíamos ter obtido a síndrome $T_3T_2T_1$ por meio da multiplicação de

matrizes. Em geral, dada a palavra $x = (x_1, x_2, x_3, x_4, x_5, x_6, x_7) \in ham(7, 4)$, temos que

$$\underbrace{\begin{bmatrix} 1 & 0 & 1 & 0 & 1 & 0 & 1 \\ 0 & 1 & 1 & 0 & 0 & 1 & 1 \\ 0 & 0 & 0 & 1 & 1 & 1 & 1 \end{bmatrix}}_{H_{7\times 3}} \cdot \underbrace{\begin{bmatrix} x_1 \\ x_2 \\ x_3 \\ x_4 \\ x_5 \\ x_6 \\ x_7 \end{bmatrix}}_{X_{7\times 1}} = \underbrace{\begin{bmatrix} T_1 \\ T_2 \\ T_3 \end{bmatrix}}_{T_{3\times 1}}.$$

Assim, dada qualquer palavra x, podemos obter a síndrome multiplicando a matriz H pela matriz X. Dizemos que H é a matriz teste de paridade do código $ham(7, 4)$.

O código de Hamming não é o único código que pode ser obtido a partir da multiplicação de matrizes, como veremos na próxima seção, essa é uma característica dos códigos lineares. Veremos também que para cada código linear existe uma matriz teste de paridade que torna o método de detecção de erros mais simples.

2.4 Códigos Lineares

Seja F um corpo finito com q elementos. Assim, para cada $n \geq 1$, temos um espaço vetorial F^n. O corpo F é o alfabeto do código linear.

Definição 2.31. Um código $C \in F^n$ será chamado de código linear se C for um subespaço vetorial de F^n.

Exemplo 2.32. Considere a transformação linear,

$$\begin{array}{rccc} A & : & F_2^2 & \longrightarrow & F_2^5 \\ & & (x_1, x_2) & \longmapsto & (x_1, x_2, x_1, x_1 + x_2, x_2). \end{array}$$

Aplicando a transformação A nos elementos do conjunto F_2^2, obtemos

$$\begin{array}{rcrcl} (0,0) & \longmapsto & (0,0,0,0+0,0) & = & (0,0,0,0,0) \\ (0,1) & \longmapsto & (0,1,0,0+1,1) & = & (0,1,0,1,1) \\ (1,0) & \longmapsto & (1,0,1,1+0,0) & = & (1,0,1,1,0) \\ (1,1) & \longmapsto & (1,1,1,1+1,1) & = & (1,1,1,0,1). \end{array}$$

Veja que o subespaço vetorial $\mathcal{C} = \{(0,0,0,0,0), (0,1,0,1,1), (1,0,1,1,0), (1,1,1,0,1)\}$ de F_2^5 é exatamente o código do robô descrito na Seção 1.1.

Um base para o espaço vetorial $\mathcal{C}$ é dada por $\mathcal{B} = \{(1,0,1,1,0), (0,1,0,1,1)\}$, este

espaço tem dimensão 2. Todos os elementos de $\mathcal{C}$ são dados por $c = \beta_1(1,0,1,1,0) + \beta_2(0,1,0,1,1)$ com $\beta_1, \beta_2 \in F_2$. Como existe apenas duas opções de escolha para β_1 e duas para β_2 de fato existe apenas essas $2^2 = 4$ palavras no código $\mathcal{C}$.

Em geral, a quantidade de palavras de um código linear $\mathcal{C}$ depende apenas do número de elementos q do corpo F e da dimensão do espaço vetorial $\mathcal{C}$. Por exemplo, seja $\mathcal{B} = \{v_1, v_2, \cdots, v_k\}$ uma base do código linear $\mathcal{C}$, assim, qualquer palavra c pode ser escrita de maneira única como

$$c = \beta_1 v_1 + \beta_2 v_2 + \cdots + \beta_k v_k, \quad \text{com } \beta_1, \beta_2, \cdots, \beta_k \in F.$$

Observe que para cada β_i, com $i = 1, 2, \cdots, k$, existem exatamente q escolhas, portanto, o número de palavras do código linear $\mathcal{C}$ é precisamente q^k.

Definição 2.33. Seja $v = (x_1, x_2, \cdots, x_n) \in F^n$, define-se o peso do vetor v como sendo o número inteiro,

$$\omega(v) = |\{i \mid x_i \neq 0, \quad 1 \leqslant i \leqslant n\}|,$$

onde $|X|$ representa o número de elementos do conjunto X.

Definição 2.34. Seja $\mathcal{C}$ um código linear, define-se o peso do código $\mathcal{C}$ como sendo o número,

$$\omega(\mathcal{C}) = \min\{\omega(v) \mid v \in \mathcal{C} - \{0\}\}.$$

Exemplo 2.35. Considerando o código do robô $\mathcal{C}$, temos que,

$$\begin{aligned} \omega((0,0,0,0,0)) &= 0 \\ \omega((0,1,0,1,1)) &= 3 \\ \omega((1,0,1,1,0)) &= 3 \\ \omega((1,1,1,0,1)) &= 4. \end{aligned}$$

Assim, $\omega(\mathcal{C}) = 3$.

Veja que o peso do código $\mathcal{C}$ é exatamente igual a distância mínima. A proposição a seguir relaciona a ideia de peso e a métrica de Hamming.

Proposição 2.36. *Seja $\mathcal{C} \subset F^n$ um código linear com distância mínima d. Temos que*

(i) $\forall\ u, v \in F^n$, $d(u,v) = \omega(u-v)$;

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

Demonstração. (i) Sejam $u = (y_1, y_2, \cdots, y_n), v = (x_1, x_2, \cdots, x_n) \in F^n$. Por definição, temos que $d(u,v) = |\{i \mid y_i \neq x_i,\ 1 \leq i \leq n\}|$ e $\omega(u-v) = |\{i \mid (y_i - x_i) \neq 0,\ \ 1 \leqslant i \leqslant n\}|$. Veja que $y_i \neq x_i$ se, e somente se, $y_i - x_i \neq 0$, portanto, os dois conjuntos têm o mesmo número de elementos, mostrando assim que $d(u,v) = \omega(u-v)$.

(ii) Suponha por contradição que $\omega(\mathcal{C}) \neq d$, assim, $\omega(\mathcal{C}) < d$ ou $\omega(\mathcal{C}) > d$. Mas, dado que a distância mínima do código $\mathcal{C}$ é igual a d, temos que existem $u, v \in \mathcal{C}$, com $u \neq v$ e $d(u,v) = d$. Sendo $\mathcal{C}$ um código linear, temos que $u - v \in \mathcal{C}$ e, pelo item (i), $\omega(u-v) = d(u,v) = d$, portanto, o caso $\omega(\mathcal{C}) > d$ não pode ocorrer. Suponha então que $\omega(\mathcal{C}) < d$, assim, existe uma palavra $v \in \mathcal{C}$, com $v \neq 0$, tal que $\omega(v) < d$. Mas, como $0 \in \mathcal{C}$, veja que pelo item (i) temos, $d(v,0) = \omega(v-0) = \omega(v) < d$. Um absurdo, pois a distância mínima do código $\mathcal{C}$ é d. Portanto, $\omega(\mathcal{C}) = d$. □

Inicialmente para calcular a distância mínima de um código $\mathcal{C}$ era necessário realizar $\binom{|\mathcal{C}|}{2}$ operações. No caso de um código linear podemos calcular o peso de cada um dos elementos não nulos do código $\mathcal{C}$ e desta maneira determinar a distância mínima, portanto, no caso dos códigos lineares precisamos realizar apenas $|\mathcal{C}| - 1$ operações.

2.4.1 Matriz Geradora de um Código

Veremos agora como obter um código linear, ou de maneira equivalente, como obter um subespaço vetorial a partir de uma matriz geradora.

Definição 2.37. Seja $\mathcal{C}$ um código. A terna de números inteiros (n, k, d), onde n representa o comprimento das palavras do código $\mathcal{C}$, k representa a dimensão do código $\mathcal{C}$ e d representa a distância mínima de $\mathcal{C}$ é chamada de parâmetros do código.

Exemplo 2.38. Considere a transformação linear,

$$\begin{array}{rccc} A & : & F_2^3 & \longrightarrow & F_2^5 \\ & & (x_1, x_2, x_3) & \longmapsto & (x_1 + x_2 + x_3, x_2 + x_3, x_3, x_2, x_1). \end{array}$$

Aplicando a transformação A nos elementos do conjunto F_2^3, obtemos

$$\begin{array}{rcrcl} (0,0,0) & \longmapsto & (0+0+0, 0+0, 0, 0, 0) & = & (0,0,0,0,0) \\ (0,0,1) & \longmapsto & (0+0+1, 0+1, 1, 0, 0) & = & (1,1,1,0,0) \\ (0,1,0) & \longmapsto & (0+1+0, 1+0, 0, 1, 0) & = & (1,1,0,1,0) \\ (0,1,1) & \longmapsto & (0+1+1, 1+1, 1, 1, 0) & = & (0,0,1,1,0) \\ (1,0,0) & \longmapsto & (1+0+0, 0+0, 0, 0, 1) & = & (1,0,0,0,1) \\ (1,0,1) & \longmapsto & (1+0+1, 0+1, 1, 0, 1) & = & (0,1,1,0,1) \\ (1,1,0) & \longmapsto & (1+1+0, 1+0, 0, 1, 1) & = & (0,1,0,1,1) \\ (1,1,1) & \longmapsto & (1+1+1, 1+1, 1, 1, 1) & = & (1,0,1,1,1). \end{array}$$

Neste caso, temos o código linear

$$\begin{array}{rcl} \mathcal{C} & = & \{(0,0,0,0,0), (1,1,1,0,0), (1,1,0,1,0), (0,0,1,1,0), (1,0,0,0,1), \\ & & (0,1,1,0,1), (0,1,0,1,1), (1,0,1,1,1)\}, \end{array}$$

com parâmetros $(5, 3, 2)$. Veja que uma base para este código é

$$\mathcal{B} = \{(1,0,0,0,1), (1,1,0,1,0), (1,1,1,0,0)\}.$$

Fazendo $v_1 = (1,0,0,0,1)$, $v_2 = (1,1,0,1,0)$ e $v_3 = (1,1,1,0,0)$, podemos definir a transformação A em função da base $\mathcal{B}$ da seguinte maneira:

$$\begin{array}{rccc} A & : & F_2^3 & \longrightarrow & F_2^5 \\ & & (x_1, x_2, x_3) & \longmapsto & x_1v_1 + x_2v_2 + x_3v_3. \end{array}$$

Podemos ainda definir a transformação por meio de matrizes, como segue

$$\begin{array}{rccc} A & : & F_2^3 & \longrightarrow & F_2^5 \\ & & \begin{bmatrix} x_1 & x_2 & x_3 \end{bmatrix} & \longmapsto & \begin{bmatrix} x_1 & x_2 & x_3 \end{bmatrix} \cdot \begin{bmatrix} 1 & 0 & 0 & 0 & 1 \\ 1 & 1 & 0 & 1 & 0 \\ 1 & 1 & 1 & 0 & 0 \end{bmatrix}. \end{array}$$

Em geral, dado um código linear $\mathcal{C} \in F^n$, escolhendo uma base $\mathcal{B} = \{v_1, v_2, \cdots, v_k\}$ para $\mathcal{C}$, podemos obter este código por meio da transformação linear

$$\begin{array}{rccc} A & : & F^k & \longrightarrow & F^n \\ & & (x_1, x_2, \cdots, x_k) & \longmapsto & (x_1v_1 + x_2v_2 + \cdots + x_kv_k). \end{array}$$

A partir da base ordenada $\mathcal{B} = \{v_1, v_2, \cdots, v_k\}$, obtemos a matriz G a seguir, na qual cada linha i é formada pelas coordenadas do vetor v_i da base, isto é,

$$G = \begin{bmatrix} v_1 \\ v_2 \\ \vdots \\ v_k \end{bmatrix} = \begin{bmatrix} v_{11} & v_{12} & \cdots & v_{1n} \\ v_{21} & v_{22} & \cdots & v_{2n} \\ \vdots & \vdots & & \vdots \\ v_{k1} & v_{k2} & \cdots & v_{kn} \end{bmatrix}.$$

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

Considerando a transformação linear

$$\begin{array}{rccc} A & : & F^k & \longrightarrow & F^n \\ & & x & \longmapsto & xG, \end{array}$$

temos que, dado um vetor $x = (x_1, x_2, \cdots, x_k) \in F^k$,

$$A(x) = xG = x_1v_1 + x_2v_2 + \cdots + x_kv_k,$$

portanto, a imagem da transformação A é exatamente o código $\mathcal{C}$. Desta maneira, F^k

pode ser visto como o código da fonte, a aplicação A como uma codificação e $\mathcal{C} = \mathrm{Im}(A)$ o código do canal.

Exemplo 2.39. Considere a transformação A do Exemplo 2.38 e o código $\mathcal{C} = \mathrm{Im}(A)$. A matriz

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

é a matriz geradora do código $\mathcal{C}$ associada a base $\mathcal{B} = \{(1,0,0,0,1), (1,1,0,1,0), (1,1,1,0,0)\}$.

Veja que nesse exemplo, dada uma palavra $c = (c_1, c_2, c_3, c_4, c_5) \in \mathcal{C}$ é fácil encontrar a palavra $x = (x_1, x_2, x_3) \in F_2^3$, tal que $A(x) = c$, isto e, é fácil de realizar a decodificação, certamente $x = (c_5, c_4, c_3)$. Este fato ocorre devido ao tipo de matriz geradora do código. Veremos que em geral, dado um código linear qualquer, é possível obter um matriz geradora em um formato que permite simplificar o processo de decodificação, esta é uma das grandes vantagens dos códigos lineares.

Definição 2.40. Dada uma matriz G geradora de um código $\mathcal{C}$, dizemos que G está na forma padrão quando

$$G = [\mathrm{Id}_k | B],$$

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

Exemplo 2.41. Considere a transformação A do Exemplo 2.38 e o código $\mathcal{C} = \mathrm{Im}(A)$. A matriz

$$G' = \begin{bmatrix} 1 & 0 & 0 & 0 & 1 \\ 0 & 1 & 0 & 1 & 1 \\ 0 & 0 & 1 & 1 & 0 \end{bmatrix},$$

obtida a partir da matriz G é também uma matriz geradora do código $\mathcal{C}$, neste caso associada a base $\mathcal{B}' = \{(1,0,0,0,1), (0,1,0,1,1), (0,0,1,1,0)\}$. Note que G' está na forma padrão, com

$$\mathrm{Id}_3 = \begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix} \quad \text{e} \quad B = \begin{bmatrix} 0 & 1 \\ 1 & 1 \\ 1 & 0 \end{bmatrix}.$$

Para obter a matriz G' do exemplo anterior utilizamos o resultado do Proposição 2.13. Veja que,

$$\begin{aligned} (1,0,0,0,1) &= (1,0,0,0,1) \\ (0,1,0,1,1) &= (1,1,0,1,0) + 1 \cdot (1,0,0,0,1) \\ (0,0,1,1,0) &= (1,1,1,0,0) + 1 \cdot (1,1,0,1,0) \end{aligned}$$

Observação 2.42. Em geral, dada uma matriz geradora G de um código $\mathcal{C}$, podemos obter uma outra matriz geradora G' por meio de uma sequência 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.

Definição 2.43. Seja F um corpo finito e n um número natural. Dizemos que uma aplicação linear $T : F^n \longrightarrow F^n$ é uma isometria de F^n se ela preserva distâncias de Hamming, isto é, se

$$d(T(v), T(u)) = d(v, u), \quad \forall\ v, u \in F^n.$$

Definição 2.44. Seja F um corpo finito. Dois códigos lineares $\mathcal{C}$ e $\mathcal{C}'$ são linearmente equivalentes se existir uma isometria linear, $T : F^n \longrightarrow F^n$ tal que $T(\mathcal{C}) = \mathcal{C}'$.

Um exemplo simples e útil de isometria linear é a aplicação

$$\begin{array}{rccc} T_\pi & : & F^n & \longrightarrow & F^n \\ & & (v_1, v_2, \cdots, v_n) & \longrightarrow & (v_{\pi(1)}, v_{\pi(2)}, \cdots, v_{\pi(n)}), \end{array}$$

onde π é uma permutação.

É fácil ver que dado um código linear $\mathcal{C}$ com matriz geradora G, permutar as colunas da matriz G é equivalente a aplicar uma transformação T_π no código $\mathcal{C}$. Desta maneira, para toda matriz G' obtida a partir de G por meio de permutações das colunas de G, temos que o código $\mathcal{C}$ gerado pela matriz G' é linearmente equivalente ao código $\mathcal{C}$.

Proposição 2.45. *Dado um código $\mathcal{C}$ com matriz geradora G, sempre existe um código $\mathcal{C}'$ linearmente equivalente ao código $\mathcal{C}$ com matriz geradora G' na forma padrão.*

Demonstração. Para obter o código $\mathcal{C}'$, basta obter a matriz G' permutando as colunas da matriz G e aplicando operações do tipo (L1), (L2) e (L3) apresentadas na Observação 2.42. Para entender o processo veja [13]. □

Exemplo 2.46. Dado o código linear $\mathcal{C}$ definido sobre F_2 pela matriz

$$G = \begin{bmatrix} 1 & 1 & 1 & 0 & 0 & 0 & 0 \\ 1 & 0 & 0 & 1 & 1 & 0 & 0 \\ 1 & 0 & 0 & 0 & 0 & 1 & 1 \\ 0 & 1 & 0 & 1 & 0 & 1 & 0 \end{bmatrix}.$$

Fazendo as permutações,

$$C_1 \leftrightarrow C_3, \quad C_2 \leftrightarrow C_5 \ \text{ e } \ C_3 \leftrightarrow C_7.$$

nas colunas da matriz G e em seguida trocar a linha L_2 pela soma $L_2 + L_4$, obtemos a matriz

$$G' = \begin{bmatrix} 1 & 0 & 0 & 0 & 1 & 0 & 1 \\ 0 & 1 & 0 & 0 & 1 & 1 & 1 \\ 0 & 0 & 1 & 0 & 0 & 1 & 1 \\ 0 & 0 & 0 & 1 & 1 & 1 & 0 \end{bmatrix},$$

que está na forma padrão e gera um código $\mathcal{C}'$ linearmente equivalente ao código dado.

2.4.2 Códigos Duais

Os resultados apresentados até aqui são suficientes para codificar e decodificar uma mensagem por meio de um código linear. No entanto, caso ocorra algum erro é necessário que o código seja capaz de fazer a correção. Nesta seção veremos alguns resultados que servem como ferramentas para correção de erros. Iniciaremos com o exemplo a seguir:

Exemplo 2.47. Considere o código linear $\mathcal{C}$ definido sobre F_2 pela matriz

$$G = \begin{bmatrix} 1 & 0 & 0 & 0 & 1 & 0 & 1 \\ 0 & 1 & 0 & 0 & 1 & 1 & 1 \\ 0 & 0 & 1 & 0 & 0 & 1 & 1 \\ 0 & 0 & 0 & 1 & 1 & 1 & 0 \end{bmatrix}.$$

Dada uma palavra $x = (x_1, x_2, x_3, x_4, x_5, x_6, x_7)$, para saber se x é ou não uma palavra do código $\mathcal{C}$, a princípio é necessário comparar x com todas as palavras $x' \in \mathcal{C}$. Mas, assim como no código de Hamming, a partir da matriz G podemos obter uma matriz teste de paridade H. Note que a matriz G está na forma padrão $G = [\mathrm{Id}_k | B]$, desta maneira, como veremos nos próximos resultados, a matriz teste de paridade é dada por $H = \left[-B^T | \mathrm{Id}_{n-k}\right]$, onde B^T é a transposta da matriz B. Neste exemplo temos que,

$$H = \begin{bmatrix} 1 & 1 & 0 & 1 & 1 & 0 & 0 \\ 0 & 1 & 1 & 1 & 0 & 1 & 0 \\ 1 & 1 & 1 & 0 & 0 & 0 & 1 \end{bmatrix}.$$

Assim, podemos usar a matriz H para saber se determinada palavra pertence ou não ao código $\mathcal{C}$. Veja que dada uma palavra qualquer $c = (c_1, c_2, c_3, c_4) \in F_2^4$, temos que

$$\begin{bmatrix} c_1 & c_2 & c_3 & c_4 \end{bmatrix} \cdot G = \begin{bmatrix} c_1 & c_2 & c_3 & c_4 & c_1 + c_2 + c_4 & c_2 + c_3 + c_4 & c_1 + c_2 + c_3 \end{bmatrix}.$$

Logo, todas as palavra do código $\mathcal{C}$ são do tipo

$$(c_1, c_2, c_3, c_4, c_1 + c_2 + c_4, c_2 + c_3 + c_4, c_1 + c_2 + c_3).$$

E observe que,

$$\begin{bmatrix} 1 & 1 & 0 & 1 & 1 & 0 & 0 \\ 0 & 1 & 1 & 1 & 0 & 1 & 0 \\ 1 & 1 & 0 & 0 & 0 & 0 & 1 \end{bmatrix} \cdot \begin{bmatrix} c_1 \\ c_2 \\ c_3 \\ c_4 \\ c_1+c_2+c_4 \\ c_2+c_3+c_4 \\ c_1+c_2+c_3 \end{bmatrix} = \begin{bmatrix} c_1+c_1+c_2+c_2+c_4+c_4 \\ c_2+c_2+c_3+c_3+c_4+c_4 \\ c_1+c_1+c_2+c_2+c_3+c_3 \end{bmatrix} = \begin{bmatrix} 0 \\ 0 \\ 0 \end{bmatrix}.$$

Portanto, para saber se a palavra x pertence ou não ao código $\mathcal{C}$, basta multiplicar a matriz H pela matriz X^T, formada pela palavra x. Por exemplo,

$$\begin{bmatrix} 1 & 1 & 0 & 1 & 1 & 0 & 0 \\ 0 & 1 & 1 & 1 & 0 & 1 & 0 \\ 1 & 1 & 0 & 0 & 0 & 0 & 1 \end{bmatrix} \cdot \begin{bmatrix} 1 \\ 0 \\ 1 \\ 0 \\ 1 \\ 0 \\ 1 \end{bmatrix} = \begin{bmatrix} 1\cdot1+1\cdot0+0\cdot1+1\cdot0+1\cdot1+0\cdot0+0\cdot1 \\ 0\cdot1+1\cdot0+1\cdot1+1\cdot0+0\cdot1+1\cdot0+0\cdot1 \\ 1\cdot1+1\cdot0+0\cdot1+0\cdot0+0\cdot1+0\cdot0+1\cdot1 \end{bmatrix} = \begin{bmatrix} 0 \\ 1 \\ 0 \end{bmatrix}.$$

Logo, a palavra $(1,0,1,0,1,0,1)$ não pertence ao código $\mathcal{C}$.

Veremos a partir de agora alguns resultados básicos que garante a existência da matriz teste de paridade H e apresenta uma estreita relação entre a matriz H e o peso do código linear.

Definição 2.48. Sejam $a = (a_1, a_2, \cdots, a_n)$ e $b = (b_1, b_2, \cdots, b_n)$ dois vetores quaisquer de F^n . Definimos o produto interno entre a e b, como sendo o elemento $a * b \in F$, dado por

$$a * b = (a_1, a_2, \cdots, a_n) * (b_1, b_2, \cdots, b_n) = a_1b_1 + a_2b_2 + \cdots + a_nb_n.$$

Proposição 2.49. *Sejam $a = (a_1, a_2, \cdots, a_n)$, $b = (b_1, b_2, \cdots, b_n)$ e $c = (c_1, c_2, \cdots, c_n)$ três vetores quaisquer de F^n e $\lambda \in F$. Temos então que,*

1. *Simetria: $a * b = b * a$;*
2. *Bilinear: $(a + \lambda b) * c = a * c + \lambda(b * c)$.*

Demonstração. Sejam $a, b, c \in F^n$ e $\lambda \in F$, temos que

1.
$$a * b = a_1b_1 + a_2b_2 + \cdots + a_nb_n = b_1a_1 + b_2a_2 + \cdots + b_na_n = b * a.$$

2.

$$\begin{aligned}
(a+\lambda b)*c &= ((a_1,a_2,\cdots,a_n)+\lambda(b_1,b_2,\cdots,b_n))*(c_1,c_2,\cdots,c_n)\\
&= (a_1+\lambda b_1, a_2+\lambda b_2,\cdots,a_n+\lambda b_n)*(c_1,c_2,\cdots,c_n)\\
&= (a_1+\lambda b_1)c_1+(a_2+\lambda b_2)c_2+\cdots+(a_n+\lambda b_n)c_n\\
&= (a_1c_1)+\lambda(b_1c_1)+(a_2c_2)+\lambda(b_2c_2)+\cdots(a_nc_n)+\lambda(b_nc_n)\\
&= (a_1c_1)+(a_2c_2)+\cdots(a_nc_n)+\lambda\left((b_1c_1)+(b_2c_2)+\cdots+(b_nc_n)\right)\\
&= (a_1,a_2,\cdots,a_n)*(c_1,c_2,\cdots,c_n)+\lambda\left((b_1,b_2,\cdots,b_n)*(c_1,c_2,\cdots,c_n)\right)\\
&= a*c+\lambda(b*c).
\end{aligned}$$

□

Definição 2.50. Seja $\mathcal{C}\subset F^n$ um código linear. Definimos o conjunto $\mathcal{C}^\perp\subset F^n$, por

$$\mathcal{C}^\perp=\{v\in F^n \mid v*u=0,\ \forall\ u\in\mathcal{C}\}.$$

Proposição 2.51. *Se $\mathcal{C}\subset F^n$ é um código linear com matriz geradora G, então:*

1. *$\mathcal{C}^\perp$ é um subespaço vetorial de F^n;*
2. *$x\in\mathcal{C}^\perp$ se, e somente se, $Gx^T=(0,0,\cdots,0)$.*

Demonstração. Sejam $a,b\in\mathcal{C}^\perp$, $c=(c_1,c_2,\cdots,c_n)\in\mathcal{C}$ e $\alpha\in F$.

1. Note que,

   i) $(0,0,\cdots,0)*(c_1,c_2,\cdots,c_n)=0\cdot c_1+0\cdot c_2+\cdots+0\cdot c_n=0$;

   ii) $(a+b)*c=a*c+b*c=0+0=0$;

   iii) $(\alpha a)*c=\alpha(a*c)=\alpha 0=0$.

   Logo, $0_F, a+b, \alpha a\in\mathcal{C}^\perp$. Portanto, $\mathcal{C}^\perp$ é um subespaço vetorial de F^n.

2. Como as linhas de G são vetores $v_1,v_2,\cdots,v_k\in\mathcal{C}$ que formam uma base para $\mathcal{C}$, temos que

   $$Gx^T=(v_1*x,v_2*x,\cdots,v_k*x)=(0,0,\cdots,0),\qquad\forall\ x\in\mathcal{C}^\perp.$$

   E, por outro lado, dado um vetor qualquer $c\in\mathcal{C}$, temos que

   $$c=\alpha_1v_1+\alpha_2v_2+\cdots+\alpha_kv_k,\ \ \text{com}\ \ \alpha_1,\alpha_2,\cdots,\alpha_k\in F.$$

   Assim, para todo $x\in F^n$, temos

   $$x*c=x*(\alpha_1v_1+\alpha_2v_2+\cdots+\alpha_kv_k)=\alpha_1(x*v_1)+\alpha_2(x*v_2)+\cdots+\alpha_k(x*v_k).$$

Logo, se $Gx^T = (0, 0, \cdots, 0)$, temos que

$$v_1 * x = 0, v_2 * x = 0, \cdots, v_k * x = 0,$$

assim,

$$x * c = \alpha_1 0 + \alpha_2 0 + \cdots + \alpha_k 0 = 0.$$

E, portanto, $x \in \mathcal{C}^{\perp}$.

□

O subespaço vetorial $\mathcal{C}^{\perp}$ é um código linear conhecido como código dual de $\mathcal{C}$. A próxima proposição relaciona a dimensão do código $\mathcal{C}$ com a dimensão do código dual, e mostra como obter uma matriz geradora para $\mathcal{C}^{\perp}$ a partir da matriz geradora G de $\mathcal{C}$.

Proposição 2.52. *Seja $\mathcal{C} \subset F^n$ um código linear de dimensão k com matriz geradora $G = [I_k \mid B]$, na forma padrão. Então,*

1. *dim $\mathcal{C}^{\perp} = n - k$.*
2. *Uma matriz geradora para $\mathcal{C}^{\perp}$ é $H = \left[-B^T \mid I_{n-k}\right]$.*

Demonstração. Pela proposição anterior temos que $x \in \mathcal{C}^{\perp}$ se, e somente se, $Gx^T = (0, 0, \cdots, 0)$. Assim, dado um vetor $x = (x_1, x_2, \ldots, x_n) \in \mathcal{C}^{\perp}$, temos que

$$Gx^T = [I_k \mid B]\, x^T = \begin{bmatrix} 1 & 0 & \cdots & 0 & b_{(k+1)1} & b_{(k+2)1} & \cdots & b_{n1} \\ 0 & 1 & \cdots & 0 & b_{(k+1)2} & b_{(k+2)2} & \cdots & b_{n2} \\ \vdots & \vdots & \ddots & 0 & \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \cdots & 1 & b_{(k+1)k} & b_{(k+2)k} & \cdots & b_{nk} \end{bmatrix} \cdot \begin{bmatrix} x_1 \\ x_2 \\ \vdots \\ x_n \end{bmatrix} = \begin{bmatrix} 0 \\ 0 \\ \vdots \\ 0 \end{bmatrix}.$$

De onde segue que,

$$\begin{bmatrix} x_1 + b_{(k+1)1}x_{k+1} + b_{(k+2)1}x_{k+2} + \cdots + b_{n1}x_n \\ x_2 + b_{(k+1)2}x_{k+1} + b_{(k+2)2}x_{k+2} + \cdots + b_{n2}x_n \\ \vdots \\ x_k + b_{(k+1)k}x_{k+1} + b_{(k+2)k}x_{k+2} + \cdots + b_{nk}x_n \end{bmatrix} = \begin{bmatrix} 0 \\ 0 \\ \vdots \\ 0 \end{bmatrix}.$$

Assim,

$$\begin{bmatrix} x_1 \\ x_2 \\ \vdots \\ x_k \end{bmatrix} + \begin{bmatrix} b_{(k+1)1}x_{k+1} + b_{(k+2)1}x_{k+2} + \cdots + b_{n1}x_n \\ b_{(k+1)2}x_{k+1} + b_{(k+2)2}x_{k+2} + \cdots + b_{n2}x_n \\ \vdots \\ b_{(k+1)k}x_{k+1} + b_{(k+2)k}x_{k+2} + \cdots + b_{nk}x_n \end{bmatrix} = \begin{bmatrix} 0 \\ 0 \\ \vdots \\ 0 \end{bmatrix}.$$

Ou ainda,

$$\begin{bmatrix} x_1 \\ x_2 \\ \vdots \\ x_k \end{bmatrix} + \begin{bmatrix} b_{(k+1)1} & b_{(k+2)1} & \cdots & b_{n1} \\ b_{(k+1)2} & b_{(k+2)2} & \cdots & b_{n2} \\ \vdots & \vdots & \ddots & \vdots \\ b_{(k+1)k} & b_{(k+2)k} & \cdots & b_{nk} \end{bmatrix} \cdot \begin{bmatrix} x_{k+1} \\ x_{k+2} \\ \vdots \\ x_n \end{bmatrix} = \begin{bmatrix} 0 \\ 0 \\ \vdots \\ 0 \end{bmatrix}.$$

Logo,

$$\begin{bmatrix} x_1 \\ x_2 \\ \vdots \\ x_k \end{bmatrix} = - \begin{bmatrix} b_{(k+1)1} & b_{(k+2)1} & \cdots & b_{n1} \\ b_{(k+1)2} & b_{(k+2)2} & \cdots & b_{n2} \\ \vdots & \vdots & \ddots & \vdots \\ b_{(k+1)k} & b_{(k+2)k} & \cdots & b_{nk} \end{bmatrix} \cdot \begin{bmatrix} x_{k+1} \\ x_{k+2} \\ \vdots \\ x_n \end{bmatrix}.$$

Como $-B^T$ é uma matriz injetiva e o corpo F tem q elementos, temos que cada um dos valores $x_{k+1}, x_{k+2}, \cdots, x_n$ pode ser escolhido de q maneiras distintas, assim o número de elementos do espaço vetorial $\mathcal{C}^\perp$ é q^{n-k}. Portanto, a dimensão de $\mathcal{C}^\perp$ é $n-k$.

Veja ainda que cada vetor $x = (x_1, x_2, \cdots, x_n)$ de $\mathcal{C}^\perp$, pode ser escrito como

$$\begin{bmatrix} x_1 & x_2 & \ldots & x_n \end{bmatrix} = \begin{bmatrix} c_1 & c_2 & \ldots & c_{n-k} \end{bmatrix} \cdot \begin{bmatrix} -b_{(k+1)1} & -b_{(k+1)2} & \cdots & -b_{(k+1)k} & 1 & 0 \cdots 0 \\ -b_{(k+2)1} & -b_{(k+2)2} & \cdots & -b_{(k+2)k} & 0 & 1 \cdots 0 \\ \vdots & \vdots & \ddots & \vdots & \vdots & \vdots \ddots \vdots \\ -b_{n1} & -b_{n2} & \cdots & -b_{nk} & 0 & 0 \cdots 1 \end{bmatrix},$$

com, $c_1, c_2, \ldots, c_{n-k} \in F$.

Logo $\mathcal{C}^\perp$ está contido no espaço vetorial gerado pela matriz H. Como as linhas de H são vetores linearmente independentes temos que a dimensão do espaço gerado é $n-k$, e portanto, este espaço tem q^{n-k} elementos. De onde segue que o espaço gerado por $H = \left[-B^T \mid I_{n-k}\right]$ é exatamente o código linear $\mathcal{C}^\perp$. □

Proposição 2.53. *Seja $\mathcal{C}$ um código linear de dimensão k em F^n e matriz geradora G. Uma matriz H de ordem $(n-k)\times n$, com entradas em F e linhas linearmente independentes é uma matriz geradora de $\mathcal{C}^\perp$ se, e somente se,*

$$G \cdot H^T = 0.$$

Demonstração. Sejam $g_1, g_2, \cdots, g_k$ as linhas da matriz G e $h_1, h_2, \cdots, h_{n-k}$ as linhas

linearmente independentes da matriz H. Observe que

$$G \cdot H^T = \begin{bmatrix} g_1 \\ g_2 \\ \vdots \\ g_k \end{bmatrix} \cdot \begin{bmatrix} h_1 & h_2 & \dots & h_{n-k} \end{bmatrix} = \begin{bmatrix} g_1 * h_1 & g_1 * h_2 & \cdots & g_1 * h_{n-k} \\ g_2 * h_1 & g_2 * h_2 & \cdots & g_2 * h_{n-k} \\ \vdots & \vdots & \ddots & \vdots \\ g_k * h_1 & g_k * h_2 & \cdots & g_k * h_{n-k} \end{bmatrix}.$$

Assim, dado que H gera o código $\mathcal{C}^\perp$, temos que $h_1, h_2, \cdots, h_{n-k} \in \mathcal{C}^\perp$, logo, $g_j * h_i = 0$ para todo $i \in \{1, 2, \cdots, n-k\}$ e $j \in \{1, 2, \cdots k\}$, e portanto, $G \cdot H^T = 0$.

Por outro lado, como as linhas de H são linearmente independentes, temos que H gera um espaço vetorial de dimensão $n-k$. Supondo que $G \cdot H^T = 0$, para todo vetor $x \cdot H$ do código gerado por H temos que

$$G \cdot (x \cdot H)^T = G \cdot (H^T \cdot x^T) = (G \cdot H^T) \cdot x^T = 0 \cdot x^T = 0.$$

Assim, o código gerado por H está contido no código $\mathcal{C}^\perp$. Como a dimensão de $\mathcal{C}^\perp$ também é $n-k$, concluímos que o código gerado por H é exatamente o código $\mathcal{C}^\perp$. □

Proposição 2.54. *Seja $\mathcal{C}$ um código linear com matriz geradora G e suponha que H seja uma matriz geradora do código $\mathcal{C}^\perp$. Então,*

$$v \in \mathcal{C} \quad \textit{se, e somente se,} \quad Hv^T = 0.$$

Demonstração. Pela proposição anterior, temos que $G \cdot H^T = 0$. De onde segue que, $(G \cdot H^T)^T = 0^T$, logo $H \cdot G^T = 0$. E novamente pela proposição anterior, temos que G é uma matriz geradora do código $(\mathcal{C}^\perp)^\perp$. Portanto, $(\mathcal{C}^\perp)^\perp = \mathcal{C}$. Assim, pela Proposição 2.51, temos que se, $Hv^T = 0$, então $v \in (\mathcal{C}^\perp)^\perp = \mathcal{C}$. Reciprocamente, se $v \in \mathcal{C}$, então $v = xG$, daí,

$$Hv^T = H(xG)^T = H(G^T x^T) = (HG^T)x^T = 0x^T = 0.$$

□

Esta proposição mostra que para todo código linear $\mathcal{C}$, existe uma matriz teste de paridade H. Desta maneira, para saber se um vetor v pertence ao código $\mathcal{C}$ basta multiplicar a matriz H por v^T. O vetor Hv^T é chamado de síndrome de v.

Proposição 2.55. *Seja $\mathcal{C}$ um código linear com matriz geradora G e suponha que H seja uma matriz geradora do código $\mathcal{C}^\perp$. Então, se existe $x \in \mathcal{C}$ de peso $\omega(x) = s$, existem s colunas de H que são linearmente dependentes.*

Demonstração. Sejam $x = (x_1, x_2, \cdots, x_n) \in \mathcal{C}$ um vetor com peso s e $C_1, C_2, \cdots, C_n$ as colunas da matriz H. Como H é uma matriz teste de paridade, segue da Proposição 2.54

que

$$0 = Hx^T = \begin{bmatrix} C_1 & C_2 & \cdots & C_n \end{bmatrix} \begin{bmatrix} x_1 \\ x_2 \\ \vdots \\ x_n \end{bmatrix} = x_1C_1 + x_2C_2 + \cdots + x_nC_n.$$

De onde segue que,

$$x_1C_1 + x_2C_2 + \cdots + x_nC_n = 0.$$

Como $\omega(x) = s$, existem exatamente s elementos não nulos no conjunto $\{x_1, x_2, \cdots, x_n\}$, sem perda de generalidade, suponha que $x_1 \cdot x_2 \cdot \ \ldots \cdot x_s \neq 0$. Assim,

$$x_1C_1 + x_2C_2 + \cdots + x_sC_s = 0,$$

portanto,

$$C_i = -x_i^{-1}x_1C_1 - x_i^{-1}x_2C_2 - \cdots - x_i^{-1}x_{i-1}C_{i-1} - x_i^{-1}x_{i-1}C_{i-1} - \cdots - x_i^{-1}x_sC_s,$$

para todo $i \in \{1, 2, \cdots s\}$. Portanto, $\{C_1, C_2, \cdots, C_s\}$ é um conjunto L.D., mostrando assim que existem s colunas de H linearmente dependentes. □

Proposição 2.56. *Seja $\mathcal{C}$ um código linear com matriz geradora G e suponha que H seja uma matriz geradora do código $\mathcal{C}^\perp$. Se existem s colunas de H que são linearmente dependentes, então $\omega(\mathcal{C}) \leq s$.*

Demonstração. Sejam $C_1, C_2, \cdots, C_n$ as colunas da matriz teste de paridade H. Sem perda de generalidade suponha qua as colunas $C_1, C_2, \cdots, C_s$ sejam linearmente dependentes. Assim, existem escalares $x_1, x_2, \cdots x_s \in F$ não todos nulos, tais que

$$x_1C_1 + x_2C_2 + \cdots + x_sC_s = 0.$$

De onde segue que,

$$x_1C_1 + x_2C_2 + \cdots + x_sC_s + 0C_{s+1} + \cdots + 0C_n = 0,$$

logo,

$$H \cdot (x_1, x_2, \cdots, x_s, 0, \cdots, 0)^T = 0.$$

Como H é uma matriz teste de paridade, temos que $(x_1, x_2, \cdots, x_s, 0, \cdots, 0) \in \mathcal{C}$. Sendo $x_1, x_2, \cdots, x_s$ não todos nulos, temos que $\omega\left((x_1, x_2, \cdots, x_s, 0, \cdots, 0)\right) \leq s$, portanto, $\omega(\mathcal{C}) \leq s$. □

A partir destas duas últimas proposições, obtemos o resultado a seguir que usaremos para demonstrar alguns propriedades importantes no processo de decodificação.

Proposição 2.57. *Seja H uma matriz teste de paridade de um código linear $\mathcal{C}$. Então, o peso de $\mathcal{C}$ será igual a s se, e somente se, quaisquer $s-1$ colunas de H são linearmente independentes e existem s colunas de H linearmente dependentes.*

2.4.3 Decodificação

Veremos a partir de agora o processo de detecção e correção de erros num determinado código linear $\mathcal{C}$.

Definição 2.58. Seja $\mathcal{C}$ um código linear. Definimos o vetor erro e como sendo a diferença entre o vetor r recebido no destino e o vetor transmitido c, ou seja,

$$e = r - c.$$

Exemplo 2.59. Suponha que tenhamos transmitido a palavra $(1,1,0,0,1,1)$ de um código linear $\mathcal{C}$ sobre F_2 e recebido a palavra $(1,1,0,1,0,1)$. Neste caso o vetor erro é

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

Observe que neste caso o vetor erro tem peso 2, que é exatamente a quantidade de erros que ocorreu no processo de transmissão. Este fato é válido no geral . Além disso, o vetor erro e a palavra recebida estão associado ao mesmo vetor síndrome. Observe que dado um código linear $\mathcal{C}$ e uma matriz teste de paridade H, temos que

$$He^T = H(r-c)^T = H(r^T - c^T) = Hr^T - Hc^T = Hr^T - 0 = Hr^T.$$

A seguir apresentamos a proposição que permitirá construir um algoritmo para correção de erros.

Proposição 2.60. *Seja $\mathcal{C}$ um código linear contido em F^n com capacidade de correção t. Se $r \in F^n$ e $c \in \mathcal{C}$ são tais que $d(c,r) \leq t$, então existe um único vetor e com $\omega(e) \leq t$, cuja síndrome é igual à síndrome de r e tal que $c = r - e$.*

Demonstração. Considere o vetor $e = r - c$. Segue da Proposição 2.36 que $\omega(e) = \omega(r - c) = d(r,c) \leq t$, mostrando assim a existência do vetor e satisfazendo as condições da proposição. Provemos então a unicidade. Suponha que existam vetores $e = (a_1, a_2, \cdots, a_n)$ e $e' = (b_1, b_2, \cdots, b_n)$ diferentes, com síndromes iguais à de r e tais que $\omega(e) \leq t$ e $\omega(e') \leq t$. Seja H uma matriz teste de paridade do código $\mathcal{C}$ com colunas $C_1, C_2, \cdots, C_n$. Como e e

e' têm a mesma síndrome, devemos ter

$$\begin{aligned} He^T = He'^T &\Leftrightarrow a_1C_1 + a_2C_2 + \cdots + a_nC_n = b_1C_1 + b_2C_2 + b_nC_n \\ &\Leftrightarrow (a_1C_1 + a_2C_2 + \cdots + a_nC_n) - (b_1C_1 + b_2C_2 + b_nC_n) = 0 \\ &\Leftrightarrow a_1C_1 - b_1C_1 + a_2C_2 - b_2C_2 + \cdots + a_nC_n - b_nC_n = 0 \\ &\Leftrightarrow (a_1 - b_1)C_1 + (a_2 - b_2)C_2 + \cdots + (a_n - b_n)C_n = 0. \end{aligned}$$

Como $\omega(e) \leq t$ e $\omega(e') \leq t$, existem no máximo $2t$ índices i, tais que $a_i - b_i \neq 0$. E portanto, existe um conjunto formado por $2t$ ou menos colunas de H linearmente dependentes. Assim, de acordo a Proposição 2.56, devemos ter $\omega(\mathcal{C}) \leq 2t$. Por outro lado, segue da Proposição 1.10 que $2t + 1 \leq d = \omega(\mathcal{C})$. Temos então que, $\omega(\mathcal{C}) \leq 2t$ e $2t + 1 \leq \omega(\mathcal{C})$. Um absurdo. Portanto, devemos ter $e = e'$. Mostrando assim a unicidade e a validez da igualdade $c = r - e$. □

A partir da proposição acima podemos recuperar a palavra enviada c em função da palavra recebida r e do vetor erro e. No entanto, precisamos de alguma maneira determinar o vetor e. Veremos inicialmente como encontrar este vetor no caso em que o erro cometido é menor ou igual a um.

Exemplo 2.61. Considere o código linear $\mathcal{C}$ do Exemplo 2.30. Suponha que uma palavra c tenha sido enviada em determinado momento e devido ao ruído ocorreu um erro no processo de transmissão, de modo que a palavra recebida seja $r = (0, 0, 1, 1, 0, 1, 1)$.

Precisamos então determinar a posição do erro. Seja $r - c = e = (x_1, x_2, x_3, x_4, x_5, x_6, x_7)$, como a palavra foi recebida com apenas um erro, temos então apenas um $x_i \neq 0$, para $i \in \{1, 2, \cdots 7\}$.

Uma matriz teste de paridade para este código é

$$H = \begin{bmatrix} 1 & 0 & 1 & 0 & 1 & 0 & 1 \\ 0 & 1 & 1 & 0 & 0 & 1 & 1 \\ 0 & 0 & 0 & 1 & 1 & 1 & 1 \end{bmatrix}.$$

Denotando os vetores coluna da matriz H por $C_1, \cdots, C_7$, temos que

$$He^T = \begin{bmatrix} 1 & 0 & 1 & 0 & 1 & 0 & 1 \\ 0 & 1 & 1 & 0 & 0 & 1 & 1 \\ 0 & 0 & 0 & 1 & 1 & 1 & 1 \end{bmatrix} \cdot \begin{bmatrix} x_1 \\ x_2 \\ x_3 \\ x_4 \\ x_5 \\ x_6 \\ x7 \end{bmatrix} = x_i \cdot C_i.$$

Pela proposição anterior, devemos $He^T = Hr^T$. Calculando Hr^T, temos

$$Hr^T = \begin{bmatrix} 1 & 0 & 1 & 0 & 1 & 0 & 1 \\ 0 & 1 & 1 & 0 & 0 & 1 & 1 \\ 0 & 0 & 0 & 1 & 1 & 1 & 1 \end{bmatrix} \cdot \begin{bmatrix} 0 \\ 0 \\ 1 \\ 1 \\ 0 \\ 1 \\ 1 \end{bmatrix} = \begin{bmatrix} 0 \\ 1 \\ 1 \end{bmatrix} = 1 \cdot \begin{bmatrix} 0 \\ 1 \\ 1 \end{bmatrix}.$$

Comparando os dois resultados, chegamos a conclusão que $i = 6$ e $x_6 = 1$. De onde segue que $e = (0, 0, 0, 0, 0, 1, 0)$ e, portanto, a palavra enviada foi,

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

Em geral, dado um código linear $\mathcal{C}$ sobre um corpo F de comprimento n e com distância mínima $d \geq 3$, para realizar a correção de uma palavra que seja recebida com no máximo um erro, podemos utilizar a estratégia do exemplo anterior. De fato, veja que se a palavra foi recebida sem erros, temos $\omega(e) = 0$, ou seja, $e = (0, 0, \cdots, 0)$. Daí, $r = c$. E caso ocorra um erro, teremos $\omega(e) = 1$, logo, o vetor erro será do tipo $e = (0, \cdots, x_i, \cdots, 0)$, para algum $i \in 1, 2, \cdots, n$. Assim,

$$Hr^T = He^T = 0 \cdot C_1 + \cdots + x_1 \cdot C_i + \cdots + 0 \cdot C_n = x_i \cdot C_i.$$

E, a partir daí, podemos comparar $x_i \cdot C_i$ com $x_0 \cdot C_j$ para todo $x_0 \in F$ e $j = 1, 2, \cdots, n$, e determinar o valor de i e x_i.

A estratégia apresentada funciona perfeitamente em canais com ocorrência de no máximo um erro, no entanto, em canais que o número de erros aumenta, não é possível determinar diretamente a posição dos erros cometidos. Veremos então uma outra estratégia de correção para palavras recebidas com mais de 1 erro, ou seja, uma estratégia para ser usada em códigos com $t > 1$. Antes disso precisamos de algumas definições.

Definição 2.62. Seja $\mathcal{C}$ um código linear sobre o corpo F. Para todo $v \in F^n$, definimos a classe lateral de v segundo $\mathcal{C}$, como sendo o conjunto,

$$v + \mathcal{C} = \{v + c \mid c \in \mathcal{C}\}.$$

Definição 2.63. Um vetor de peso mínimo numa classe lateral é chamado de vetor líder dessa classe.

Proposição 2.64. *Dois vetores $u, v \in F^n$ têm a mesma síndrome se, e somente se, $u \in v + \mathcal{C}$.*

Demonstração. Seja H uma matriz teste de paridade do código $\mathcal{C}$. Temos então que,

$$Hu^T = Hv^T \Leftrightarrow Hu^T - Hv^T = 0 \Leftrightarrow H(u^T - v^T) = 0 \Leftrightarrow H(u-v)^T = 0 \Leftrightarrow u - v \in \mathcal{C}.$$

E veja que, se $u - v \in \mathcal{C}$, então $v + (u - v) = u \in v + \mathcal{C}$. E, reciprocamente, se $u \in v + \mathcal{C}$, existe $c \in \mathcal{C}$ tal que $u = v + c$, assim $u - v = c \in \mathcal{C}$. Portanto, $u - v \in \mathcal{C}$ se, e somente se, $u \in v + \mathcal{C}$. □

Proposição 2.65. *Sejam $u, v \in F^n$ dois vetores e $\mathcal{C}$ um código linear com parâmetros (n, k, d). Temos então as seguintes propriedades em relação às classes laterais:*

1. *$u + \mathcal{C} = v + \mathcal{C} \Leftrightarrow u - v \in \mathcal{C}$;*
2. *$(u + \mathcal{C}) \cap (v + \mathcal{C}) \neq \varnothing \Rightarrow u + \mathcal{C} = v + \mathcal{C}$;*
3. *$\bigcup_{v \in F^n} (v + \mathcal{C}) = F^n$;*
4. *$|(v + \mathcal{C})| = |\mathcal{C}| = q^k$;*
5. *O número de classes laterais segundo $\mathcal{C}$ é q^{n-k}.*

Demonstração. :

1. Como $\mathcal{C}$ é um espaço vetorial, temos que o vetor 0 pertence a $\mathcal{C}$, de onde segue que $u \in u + \mathcal{C}$. E dado que $u + \mathcal{C} = v + \mathcal{C}$, existe um $c \in \mathcal{C}$ tal que $u = v + c$, assim $u - v = c \in \mathcal{C}$. Reciprocamente, se $u - v \in \mathcal{C}$, então $v + (u - v) = u \in v + \mathcal{C}$, e, pela proposição anterior, u e v têm a mesma síndrome. Mas, se u e v têm a mesma síndrome, novamente pela proposição anterior, temos que $v \in u + \mathcal{C}$. Assim, os elementos de $u + \mathcal{C}$ e $v + \mathcal{C}$ têm a mesma síndrome, portanto pertencem a uma mesma classe lateral, de onde segue que, $u + \mathcal{C} = v + \mathcal{C}$.

2. Novamente é uma aplicação direta da proposição anterior. De fato, se $(u + \mathcal{C}) \cap (v + \mathcal{C}) \neq \varnothing$, existe um vetor w com a mesma síndrome dos vetores u e v. De onde segue que $u + \mathcal{C} = v + \mathcal{C}$.

3. É uma igualdade óbvia, pois, $v \in F^n$ e $v \in v + \mathcal{C}$.

4. Basta observar que $v + c \neq v + c'$, para todo $c \neq c'$, com $c, c' \in \mathcal{C}$.

5. Dos itens 2 e 4, temos que o número de classes laterais é dado por $\dfrac{q^n}{q^k} = q^{n-k}$.

□

Exemplo 2.66. Considere o código linear $\mathcal{C}$ sobre F_2 gerado pela matriz

$$G = \begin{bmatrix} 1 & 0 & 0 & 0 & 1 & 1 \\ 0 & 1 & 0 & 1 & 1 & 0 \\ 0 & 0 & 1 & 1 & 0 & 1 \end{bmatrix}.$$

Temos que,

$$\mathcal{C} = \{000000, 001101, 010110, 011011, 100011, 101110, 110101, 111000\}.$$

Assim, as classes laterais segundo $\mathcal{C}$ são:

$$\begin{array}{rcl} 000000 + \mathcal{C} & = & \{000000, 001101, 010110, 011011, 100011, 101110, 110101, 111000\} \\ 000001 + \mathcal{C} & = & \{000001, 001100, 010111, 011010, 100010, 101111, 110100, 111001\} \\ 000010 + \mathcal{C} & = & \{000010, 001111, 010100, 011001, 100001, 101100, 110111, 111010\} \\ 000100 + \mathcal{C} & = & \{000100, 001001, 010010, 011111, 100111, 101010, 110001, 111100\} \\ 001000 + \mathcal{C} & = & \{001000, 000101, 011110, 010011, 101011, 100110, 111101, 110000\} \\ 010000 + \mathcal{C} & = & \{010000, 011101, 000110, 001011, 110011, 111110, 100101, 101000\} \\ 100000 + \mathcal{C} & = & \{100000, 101101, 110110, 111011, 000011, 001110, 010101, 011000\} \\ 000111 + \mathcal{C} & = & \{000111, 001010, 010001, 011100, 100100, 101001, 110010, 111111\} \end{array}.$$

Neste caso uma matriz teste de paridade é,

$$H = \begin{bmatrix} 0 & 1 & 1 & 1 & 0 & 0 \\ 1 & 1 & 0 & 0 & 1 & 0 \\ 1 & 0 & 1 & 0 & 0 & 1 \end{bmatrix}.$$

Temos então a tabela abaixo que relaciona classe lateral, síndrome e líder de classe.

Classe lateral	Síndrome	Líderes
$000000 + \mathcal{C}$	000	000000
$000001 + \mathcal{C}$	001	000001
$000010 + \mathcal{C}$	010	000010
$000100 + \mathcal{C}$	100	000100
$001000 + \mathcal{C}$	101	001000
$010000 + \mathcal{C}$	110	010000
$100000 + \mathcal{C}$	011	100000
$000111 + \mathcal{C}$	111	001010, 010001, 100100

Observe que nesse exemplo, a classe lateral $000111 + \mathcal{C}$ tem mais de um líder. Na próxima proposição veremos que este fato está relacionado com a capacidade de correção

do código $\mathcal{C}$.

Proposição 2.67. *Seja $\mathcal{C} \subset F^n$ um código linear com distância mínima d. Se $u \in F^n$ é um vetor tal que $\omega(u) \leqslant \left[\frac{d-1}{2}\right] = t$, então u é o único elemento líder de sua classe lateral.*

Demonstração. Sejam $u, v \in F^n$ vetores tais que $\omega(u) \leqslant t$ e $\omega(v) \leqslant t$. Se u e v pertencem a uma mesma classe lateral, temos $u - v \in \mathcal{C}$. Mas veja que,

$$\omega(u - v) \leqslant \omega(u) + \omega(v) \leqslant t + t \leqslant d - 1.$$

Como $\omega(\mathcal{C}) = d$, devemos ter $u - v = 0$, logo, $u = v$. Portanto, u é o único elemento líder de sua classe lateral. □

Proposição 2.68. *Seja $\mathcal{C} \subset F^n$ um código linear com distância mínima d e seja $r \in F^n$. Então, existe $c \in \mathcal{C}$ tal que $d(r, c) \leqslant t$ se, e somente se, existe um vetor $e \in r + \mathcal{C}$ tal que $\omega(e) \leqslant t$. Neste caso, e é o vetor erro e a palavra enviada é $c = r - e$.*

Demonstração. Se existe $c \in \mathcal{C}$ tal que $d(r, c) \leqslant t$, temos que $-c \in \mathcal{C}$, assim, definindo $e = r - c = r + (-c)$, segue que $\omega(e) = \omega(r - c) = d(r, c) \leqslant t$ e $e \in r + \mathcal{C}$. Reciprocamente, se existe $e \in r + \mathcal{C}$ tal que $\omega(e) \leqslant t$, temos que o vetor $c = r - e$ pertence ao código $\mathcal{C}$, com $d(r, c) = \omega(r - c) = \omega(r - (r - e)) = \omega(e) \leq t$. □

Vejamos agora uma estratégia para correção de palavras recebidas com no máximo t erros.

Inicialmente devemos determinar todos os vetores $v \in F^n$, tais que $\omega(v) \leq t$. Pela Proposição 2.67, v é o único elemento líder de sua classe. Em seguida, calcular a síndrome de cada elemento v e montar uma tabela com o vetor e a respectiva síndrome. Assim, recebida uma palavra r, podemos calcular a síndrome $s^T = Hr^T$ e comparar com as síndromes da tabela. Caso a síndrome seja encontrada na tabela, o respectivo vetor v é o elemento líder da sua classe e podemos fazer a correção $c = r - v$. Caso a síndrome não seja encontrada na tabela, não será possível fazer a correção, pois foram cometidos mais de t erros.

Exemplo 2.69. (Extraído de [2]) Considere o código linear $\mathcal{C}$ sobre F_2, com parâmetros $(9, 4, 5)$ e matriz geradora

$$G = \begin{bmatrix} 1 & 1 & 1 & 1 & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 & 1 & 1 & 1 & 0 & 1 \end{bmatrix}.$$

Neste caso, o código tem capacidade de correção $t = \left[\frac{d-1}{2}\right] = \left[\frac{5-1}{2}\right] = 2$.

Suponha que este código tenha sido usado para codificar os comandos de um robô, como segue,

Comando	Fonte	Codificando	Código do Canal
Norte	00	$(0,0)\cdot G$	000000000
Sul	10	$(1,0)\cdot G$	111100010
Leste	01	$(0,1)\cdot G$	000111101
Oeste	11	$(1,1)\cdot G$	111011111.

E suponha que em determinado momento o robô tenha recebido a sequência de comandos abaixo:

$$000000011 \quad 100111101 \quad 000000000 \quad 111000111 \quad 1110000110 \quad 000111101.$$

Vejamos então como corrigir os erros e decodificar esta mensagem.
A partir da matriz teste de paridade

$$H = \begin{bmatrix} 1 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 & 1 & 1 \\ 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 1 \end{bmatrix},$$

podemos determinar a síndrome dos vetores $v \in F^n$, tais que $\omega(v) \leq t$, e montar a tabela relacionando os líderes de classe com as síndromes.

Líder	Síndrome	Líder	Síndrome
000000000	0000000	010000010	1011000
100000000	1000000	010000001	0101111
010000000	0100000	001100000	0011000
001000000	0010000	001010000	0010100
000100000	0001000	001001000	0010010
000010000	0000100	001000100	0010001
000001000	0000010	001000010	1101000
000000100	0000001	001000001	0011111
000000010	1111000	000110000	0001100
000000001	0001111	000101000	0001010
110000000	1100000	000100100	0001001
101000000	1010000	000100010	1110000
100100000	1001000	000100001	0000111
100010000	1000100	000011000	0000110
100001000	1000010	000010100	0000101
100000100	1000001	000010010	1111100
100000010	0111000	000010001	0001011
100000001	1001111	000001100	0000011
011000000	0110000	000001010	1111010
010100000	0101000	000001001	0001101
010010000	0100100	000000110	1111001
010001000	0100010	000000101	0001110
010000100	0100001	000000011	1110111.

Para a primeira palavra $r_0 = 000000011$, recebida pelo robô, temos que a síndrome s_0 é dada por,

$$s_0^T = H \cdot r_0 = \begin{bmatrix} 1 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 & 1 & 1 \\ 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 1 \end{bmatrix} \cdot \begin{bmatrix} 0 \\ 0 \\ 0 \\ 0 \\ 0 \\ 0 \\ 0 \\ 1 \\ 1 \end{bmatrix} = \begin{bmatrix} 1 \\ 1 \\ 1 \\ 0 \\ 1 \\ 1 \\ 1 \end{bmatrix}.$$

Veja que a síndrome s_0 é o último elemento da tabela acima, assim, temos o vetor erro

$e_0 = 000000011$ e podemos concluir que a primeira palavra enviado foi

$$c_0 = r_0 - e_0 = 000000011 - 000000011 = 000000000,$$

que é referente a palavra 00 do canal, e portanto, representa o comando Norte. De maneira análoga, temos

Palavra recebida(r)	Síndrome(s)	Vetor erro(e)	Palavra enviada(c)	Comando
000000011	1110111	000000011	000000000	Norte
100111101	1000000	100000000	000111101	Leste
000000000	0000000	000000000	000000000	Norte
111000111	0000110	000011000	111011111	Oeste
111000110	0001001	000100100	111100010	Sul
000111101	0000000	000000000	000111101	Leste

Capítulo 3

Corpo dos Números Complexos

Iniciaremos este capítulo com um exemplo clássico no estudo dos números complexos.

Como apresentado por [6], este exemplo está relacionado com a resolução de equações de grau 3. Considere a equação do terceiro grau,

$$x^3 - 15x - 4 = 0.$$

Veja que as soluções desta equação são $x_1 = 4, x_2 = -2+\sqrt{3}$ e $x_3 = -2-\sqrt{3}$. No entanto, no século XVI já era conhecida uma fórmula para resolução de equações de grau 3, ou seja, dada uma equação da tipo

$$x^3 + px + q = 0,$$

já era sabido que as soluções desta equação são dadas por

$$x = \sqrt[3]{-\frac{q}{2} + \sqrt{\left(\frac{q}{2}\right)^2 + \left(\frac{p}{3}\right)^2}} + \sqrt[3]{-\frac{q}{2} - \sqrt{\left(\frac{q}{2}\right)^2 + \left(\frac{p}{3}\right)^2}}.$$

E aplicando esta fórmula, obtemos que as soluções da equação acima são dadas por,

$$x = \sqrt[3]{2 + \sqrt{-121}} + \sqrt[3]{2 - \sqrt{-121}}.$$

Assim, de alguma maneira seria possível calcular $\sqrt{-121}$, pois as soluções são reais. Este fatos intrigou muitos matemáticos do século XVI e motivou o desenvolvimento da teoria dos números complexos.

3.1 Adição e multiplicação em $\mathbb{R}^2$

Veremos nesta seção que é possível definir uma operação de adição e multiplicação no espaço $\mathbb{R}^2$ de modo que a estrutura matemática resultante seja um corpo.

Considere a estrutura matemática $(\mathbb{R}^2, \oplus, \odot)$ formada pelo conjunto de pares ordenados

reais, isto é, o conjunto

$$\mathbb{R}^2 = \{(x, y) \mid x, y \in \mathbb{R}\},$$

com as seguintes operações:

$$\begin{array}{rccc} \oplus \ : & \mathbb{R}^2 \times \mathbb{R}^2 & \longrightarrow & \mathbb{R}^2 \\ & ((x_1, y_1), (x_2, y_2)) & \longmapsto & (x_1, y_1) \oplus (x_2, y_2) = (x_1 + x_2, y_1 + y_2). \end{array}$$

e,

$$\begin{array}{rccc} \odot \ : & \mathbb{R}^2 \times \mathbb{R}^2 & \longrightarrow & \mathbb{R}^2 \\ & ((x_1, y_1), (x_2, y_2)) & \longmapsto & (x_1, y_1) \odot (x_2, y_2) = (x_1x_2 - y_1y_2, x_1y_2 + y_1x_2). \end{array}$$

Vamos então mostrar que a estrutura assim definida é um corpo. É fácil de ver que o conjunto é fechado em relação a operação de adição e multiplicação definidas, isto é, dados dois elementos de $\mathbb{R}^2$ o resultado da adição e da multiplicação desses dois elementos é um elemento de $\mathbb{R}^2$. Para verificar as propriedades das operações considere os elementos $(x_1, y_1), (x_2, y_2)$ e (x_3, y_3), note que

A_1. Associatividade da adição:

$$\begin{aligned} [(x_1, y_1) \oplus (x_2, y_2)] \oplus (x_3, y_3) &= (x_1 + x_2, y_1 + y_2) \oplus (x_3, y_3) \\ &= ((x_1 + x_2) + x_3, (y_1 + y_2) + y_3) \\ &= (x_1 + (x_2 + x_3), y_1 + (y_2 + y_3)) \\ &= (x_1, y_1) \oplus (x_2 + x_3, y_2 + y_3) \\ &= (x_1, y_1) \oplus [(x_2, y_2) \oplus (x_3, y_3)]. \end{aligned}$$

A_2. Comutatividade da adição:

$$\begin{aligned} (x_1, y_1) \oplus (x_2, y_2) &= (x_1 + x_2, y_1 + y_2) \\ &= (x_2 + x_1, y_2 + y_1) \\ &= (x_2, y_2) \oplus (x_1, y_1). \end{aligned}$$

A_3. Existência de elemento neutro (chamado zero) para adição:

$$\begin{aligned} (x_1, y_1) \oplus (0, 0) &= (x_1 + 0, y_1 + 0) \\ &= (x_1, y_1). \end{aligned}$$

A_4. Existência de elemento inverso (chamado simétrico aditivo) para adição:

$$\begin{aligned} (x_1, y_1) \oplus (-x_1, -y_1) &= (x_1 + (-x_1), y_1 + (-y_1)) \\ &= (x_1 - x_1, y_1 - y_1) \\ &= (0, 0). \end{aligned}$$

M_1. Associatividade da multiplicação:

$$\begin{aligned}
[(x_1,y_1)\odot(x_2,y_2)]\odot(x_3,y_3) &= (x_1x_2-y_1y_2,x_1y_2+y_1x_2)\odot(x_3,y_3)\\
&= ((x_1x_2-y_1y_2)x_3-(x_1y_2+y_1x_2)y_3,(x_1x_2-y_1y_2)y_3\\
&\quad +(x_1y_2+y_1x_2)x_3)\\
&= (x_1x_2x_3-x_1y_2y_3-y_1x_2y_3-y_1y_2x_3,x_1x_2y_3+x_1y_2x_3\\
&\quad +y_1x_2x_3-y_1y_2y_3)\\
&= (x_1(x_2x_3-y_2y_3)-y_1(x_2y_3+y_2x_3),x_1(x_2y_3+y_2x_3)\\
&\quad +y_1(x_2x_3-y_2y_3))\\
&= (x_1,x_2)\odot(x_2x_3-y_2y_3,x_2y_3+y_2x_3)\\
&= (x_1,y_1)\odot[(x_2,y_2)\odot(x_3,y_3)]\,.
\end{aligned}$$

M_2. Comutatividade da multiplicação:

$$\begin{aligned}
(x_1,y_1)\odot(x_2,y_2) &= (x_1x_2-y_1y_2,x_1y_2+y_1x_2)\\
&= (x_2x_1-y_2y_1,x_2y_1+y_2x_1)\\
&= (x_2,y_2)\odot(x_1,y_1).
\end{aligned}$$

M_3. Existência de elemento neutro (chamado unidade) para multiplicação:

$$\begin{aligned}
(x_1,y_1)\odot(1,0) &= (x_1\cdot 1-y_1\cdot 0,x_1\cdot 0+y_1\cdot 1)\\
&= (x_1,y_1).
\end{aligned}$$

AM. Distributividade da multiplicação com relação à adição:

$$\begin{aligned}
[(x_1,y_1)\oplus(x_2,y_2)]\odot(x_3,y_3) &= (x_1+x_2,y_1+y_2)\odot(x_3,y_3)\\
&= ((x_1+x_2)x_3-(y_1+y_2)y_3,(x_1+x_2)y_3+(y_1+y_2)x_3)\\
&= (x_1x_3-y_1y_3+x_2x_3-y_2y_3,x_1y_3+y_1x_3+x_2y_3+y_2x_3)\\
&= (x_1,y_1)\odot(x_3,y_3)\oplus(x_1,y_1)\odot(x_3,y_3).
\end{aligned}$$

Chegamos então a conclusão que $(\mathbb{R}^2,\oplus,\odot)$ é um anel comutativo com unidade. Agora vamos prova a existência de inverso multiplicativo e concluir que a estrutura é um corpo. Para isto, considere o elemento não nulo $(a,b)\in\mathbb{R}^2$, neste caso temos que $a\neq 0$ ou $b\neq 0$, assim $a^2+b^2\neq 0$. Devemos então determinar, caso exista, o elemento $(x,y)\in\mathbb{R}^2$ de modo que $(a,b)\odot(x,y)=(1,0)$. Observe que,

$$(a,b)\odot(x,y)=(ax-by,ay+bx)=(1,0),$$

segue então que,

$$\begin{cases} ax-by &= 1\\ ay+bx &= 0. \end{cases}$$

Resolvendo esse sistema, obtemos que,

$$x = \frac{a}{a^2+b^2} \qquad \text{e} \qquad y = \frac{-b}{a^2+b^2}.$$

E veja que,

$$\begin{aligned}(a,b)\odot\left(\frac{a}{a^2+b^2},\frac{-b}{a^2+b^2}\right) &= \left(a\cdot\frac{a}{a^2+b^2}-b\cdot\frac{-b}{a^2+b^2}, a\cdot\frac{-b}{a^2+b^2}+b\cdot\frac{a}{a^2+b^2}\right)\\ &= \left(\frac{a^2}{a^2+b^2}+\frac{b^2}{a^2+b^2},\frac{-ba}{a^2+b^2}+\frac{ba}{a^2+b^2}\right)\\ &= \left(\frac{a^2+b^2}{a^2+b^2},\frac{-ba+ba}{a^2+b^2}\right)\\ &= (1,0).\end{aligned}$$

Portanto, todo elemento não nulo $(a,b)\in\mathbb{R}^2$ possui inverso multiplicativo, dado por,

$$\left(\frac{a}{a^2+b^2},\frac{-b}{a^2+b^2}\right).$$

Mostrando assim, que de fato a estrutura $(\mathbb{R}^2,\oplus,\odot)$ é um corpo.

Observe ainda que dado um número real α e elementos $(x_1,y_1),(x_2,y_2)\in\mathbb{R}^2$, utilizando a multiplicação por escalar usual, isto é, $\alpha(a,b)=(\alpha a,\alpha b)=(a,b)\alpha$, temos a seguinte propriedade,

$$\alpha(x_1,y_1)\odot(x_2,y_2)=(x_1,y_1)\alpha\odot(x_2,y_2)=(x_1,y_1)\odot\alpha(x_2,y_2)=(x_1,y_1)\odot(x_2,y_2)\alpha.$$

De fato, basta observar que

$$\alpha(x_1,y_1)\odot(x_2,y_2)=(\alpha x_1,\alpha y_1)\odot(x_2,y_2)=(\alpha x_1x_2-\alpha y_1y_2,\alpha x_1y_2+\alpha y_1x_2),$$

e usar as propriedades comutativa e associativa da multiplicação de números reais.

Os elementos do conjunto $\mathbb{R}^2$ podem ser naturalmente representados no plano cartesiano, de modo que as operações de adição e multiplicação tenham um significado geométrico. Como $\mathbb{R}^2$ é, também um espaço vetorial, é possível determinar uma base ordenada, de modo que todo elemento $(a,b)\in\mathbb{R}^2$ seja gerado por esta base. Um exemplo importante é a base canônica $\{(1,0),(0,1)\}$. Veja que o vetor $(1,0)$ é a unidade do corpo $(\mathbb{R}^2,\oplus,\odot)$. Assim, escrevendo $1=(1,0)$ e $i=(0,1)$, temos que

$$i^2=i\odot i=(0,1)\odot(0,1)=(0\cdot0-1,0\cdot1+1\cdot0)=(-1,0)=-(1,0)=-1.$$

Desta maneira é possível definir o corpo $(\mathbb{R}^2,\oplus,\odot)$, trocando a operação de adição '$\oplus$' pela operação de adição coordenada a coordenada '$+$' e a multiplicação '$\odot$' pela multiplicação

de modo distributivo '$\cdot$', e acrescentando a propriedade $i^2 = -1$.
De fato, veja que dados dois elementos $(x_1, y_1), (x_2, y_2) \in \mathbb{R}^2$, temos que

$$(x_1, y_1) = x_1(1,0) + y_1(0,1) = x_1 + y_1 i \qquad \text{e} \qquad (x_2, y_2) = x_2(1,0) + y_2(0,1) = x_2 + y_2 i.$$

Assim,

$$\begin{aligned}(x_1 + y_1 i) + (x_2 + y_2 i) &= (x_1 + x_2) + (y_1 + y_2)i \\ &= (x_1 + x_2)(1,0) + (y_1 + y_2)(0,1) \\ &= (x_1 + x_2, y_1 + y_2) \\ &= (x_1, y_1) \oplus (x_2, y_2),\end{aligned}$$

e,

$$\begin{aligned}(x_1 + y_1 i) \cdot (x_2 + y_2 i) &= x_1 x_2 + x_1 y_2 i + y_1 i x_2 + y_1 i y_2 i \\ &= x_1 x_2 + y_1 y_2 i^2 + x_1 y_2 i + y_1 x_2 i \\ &= x_1 x_2 - y_1 y_1 + x_1 y_2 i + y_1 x_2 i \\ &= (x_1 x_2 - y_1 y_1) + (x_1 y_2 + y_1 x_2)i \\ &= (x_1 x_2 - y_1 y_1)(1,0) + (x_1 y_2 + y_1 x_2)(0,1) \\ &= (x_1 x_2 - y_1 y_1, x_1 y_2 + y_1 x_2) \\ &= (x_1, y_1) \odot (x_2, y_2).\end{aligned}$$

Portanto, as operações '$+$' e '$\cdot$' são equivalentes as operações '$\oplus$' e '$\odot$'. Este corpo é conhecido como conjunto dos números complexos, e definido por,

$$\mathbb{C} = \{a + bi \mid a, b \in \mathbb{R}, \text{ e } i^2 = -1\}.$$

Veja que,

$$a + bi \leftrightarrow (a, b) = a(1,0) + b(0,1).$$

O subconjunto $\{a + bi \in \mathbb{C} \mid b = 0\}$ pode ser visto como uma cópia dos números reais dentro dos complexos. Desta maneira, temos que $\mathbb{R}$ está contido em $\mathbb{C}$. O que é natural, uma vez que os pontos do tipo $a + 0i$ estão sobre o eixo Ox do plano cartesiano.

O símbolo i foi utilizado pela primeira vez pelo matemático Euler nos estudos dos números do tipo $a + bi$, onde i representava $\sqrt{-1}$. Esta abordagem que fizemos, é uma abordagem atual, visto que no século XVI ainda não existiam as estruturas de anel, espaço vetorial e corpo como conhecemos hoje. O conceito de números complexos demorou séculos para ser consolidado. Na tentativa de resolver a equação que apresentamos no início do capítulo, muitos matemáticos consideraram $\sqrt{-1}$ como um número conhecido, mas não tiveram muito sucesso no estudo dos números complexos. A consolidação dos números complexos como conhecemos hoje foi estabelecida pelo matemático Carl Friedrich Gauss.

3.2 Representação Geométrica dos Números complexos

Nesta seção vamos apresentar mais algumas definições e propriedades relacionadas aos números complexos.

Como vimos na primeira seção deste capítulo, os números complexos são essencialmente pares ordenados, de modo que podemos representá-los no plano cartesiano. Neste caso, o plano cartesiano é conhecido como plano de Argand-Gauss ou plano complexo.

A primeira associação entre números complexos e pontos do plano cartesiano foi feita de forma independente pelos matemáticos Gauss e Jean Robert Argand. No plano complexo, o eixo das abscissas Ox é chamado de eixo real, e o eixo das ordenadas Oy é conhecido como eixo imaginário. Chamaremos os elementos do conjunto $\mathbb{C}$, simplesmente de números complexos.

Um número complexo $z = a + bi$ será representado no plano cartesiano pelo ponto $Z = (a, b)$.

Exemplo 3.1. Na figura abaixo temos a representação dos números complexos $z_1 = 2+3i$, $z_2 = -3 + 2i$, $z_3 = -2 - i$ e $z_4 = 2 - 2i$.

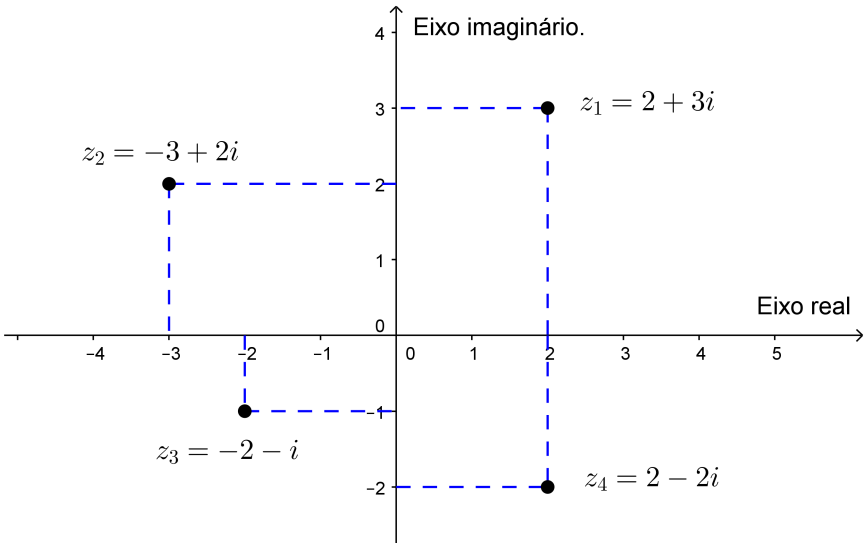

Figura 3.1: Representação geométrica.

Assim como pontos do plano que podem ser divididos em duas componentes (coordenadas), os números complexos podem ser divididos em sua parte real e sua parte imaginária. Temos então a seguinte definição:

Definição 3.2. Seja $z = a+bi$ um número complexo. Os números reais a e b são chamados, respectivamente, de parte real e parte imaginária de z, denotadas por:

$$\mathrm{Re}(z) = a \qquad \text{e} \qquad \mathrm{Im}(z) = b.$$

Com essa representação geométrica é possível perceber que a soma dos números complexos $z_1 = x_1 + y_1 i$ e $z_2 = x_2 + y_2 i$, é equivalente a soma de dois vetores com ponto inicial $(0, 0)$ e pontos finais $Z_1 = (x_1, y_1)$ e $Z_2 = (x_2, y_2)$. De modo que a regra do paralelogramo é válida para a soma de números complexos, ou seja, a soma de dois números complexos é determinado pela diagonal do paralelogramo determinado pelo vetores associados a esses números. Veja o exemplo abaixo:

Exemplo 3.3. Considere os números complexos $z_1 = 4 + i$ e $z_2 = 2 + 3i$. Temos que,

$$z_1 + z_2 = (4 + i) + (2 + 3i) = 6 + 4i.$$

Que é exatamente o ponto final do vetor determinado pela soma dos vetores $(4, 1)$ e $(2, 3)$, como mostra a Figura 3.2.

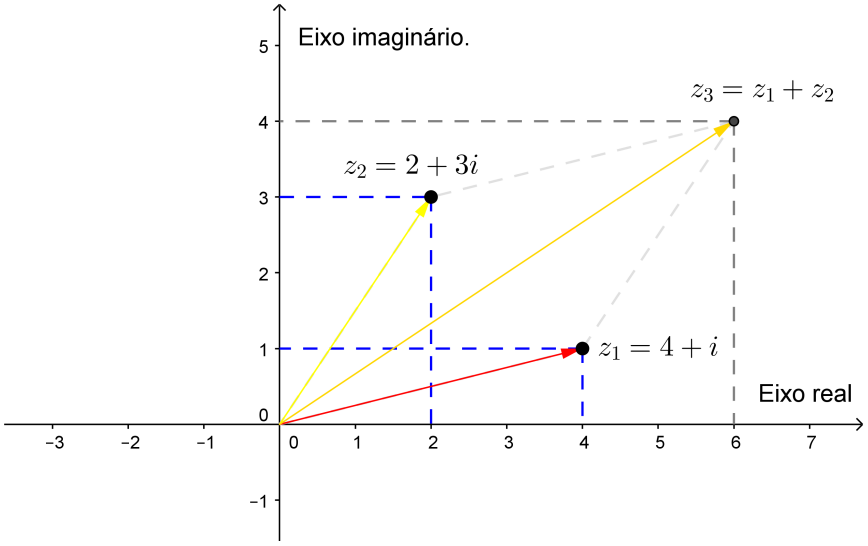

Figura 3.2: Soma de números complexos.

Definição 3.4. Seja $z = a + bi$ um número complexo. Definimos o conjugado de z como sendo o número complexo $\overline{z} = a - bi$. Geometricamente, $\overline{z}$ é o simétrico de z em relação ao eixo real, conforme Figura 3.3.

O conjugado do número $z = a + bi$ possui duas propriedades importantes em relação a operação de adição e multiplicação. Veja que

$$z + \overline{z} = (a + bi) + (a - bi) = 2a = 2 \cdot \mathrm{Re}(z),$$

$$z - \overline{z} = (a + bi) - (a - bi) = 2bi = 2 \cdot \mathrm{Im}(z),$$

e,

$$z \cdot \overline{z} = (a + bi) \cdot (a - bi) = a^2 - (bi)^2 = a^2 + b^2.$$

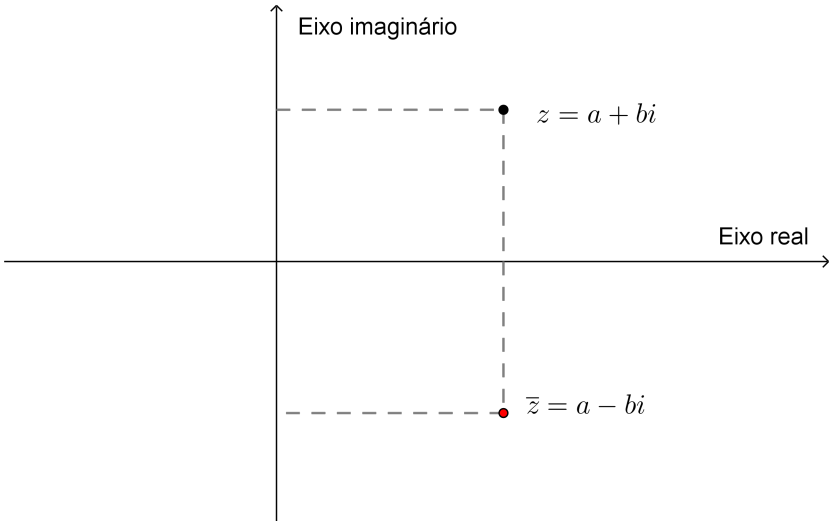

Figura 3.3: Conjugado.

Ou seja, a soma e a multiplicação do complexo z pelo seu conjugado $\overline{z}$ é sempre um número real.

Proposição 3.5. *Sejam $z = a + bi$ e $w = c + di$ dois números complexos. A conjugação tem as seguintes propriedades:*

1. $\overline{z} = 0$ *se, e somente se,* $z = 0$*;*
2. $\overline{\overline{z}} = z$*, para todo* $z \in \mathbb{C}$;
3. $\overline{z} = z$ *se, e somente se,* $z \in \mathbb{R}$*;*
4. $\overline{z \pm w} = \overline{z} \pm \overline{w}$*;*
5. $\overline{z \cdot w} = \overline{z} \cdot \overline{w}$*;*
6. $\overline{z^{-1}} = \overline{z}^{-1}$*, para todo* $z \neq 0$.

Demonstração. Considere os números complexos $z = a + bi$ e $w = c + di$. Temos então que,

1. $\overline{z} = 0 \Leftrightarrow a - bi = 0 + 0i \Leftrightarrow a = 0$ e $b = 0 \Leftrightarrow a + bi = 0 \Leftrightarrow z = 0$.
2. $\overline{\overline{z}} = \overline{a - bi} = a - (-bi) = a + bi = z$, para todo $z \in \mathbb{C}$.
3. $\overline{z} = z \Leftrightarrow a + bi = a - bi \Leftrightarrow b = -b \Leftrightarrow b = 0 \Leftrightarrow a + bi = a + 0i \Leftrightarrow z = a \Leftrightarrow z \in \mathbb{R}$.
4. $\overline{z \pm w} = \overline{(a \pm c) + (b \pm d)i} = (a \pm c) - (b \pm d)i = (a - bi) \pm (c - di) = \overline{z} \pm \overline{w}$.
5. $\overline{z \cdot w} = \overline{(a + bi) \cdot (c + di)} = \overline{(ac - bd) + (ad + bc)i} = (ac - bd) - (ad + bc)i = (ac - bd) + (-ad - bc)i = \overline{z} \cdot \overline{w}$.

6. Supondo $z \neq 0$, temos que, $\overline{z^{-1}} = \overline{\frac{a}{a^2+b^2} + \frac{-b}{a^2+b^2}i} = \frac{a}{a^2+b^2} + \frac{b}{a^2+b^2}i = \overline{z}^{-1}$.

□

Definição 3.6. Seja $z = a + bi$ um número complexo. Definimos o módulo de z como sendo o número real não negativo $|z| = \sqrt{a^2+b^2}$. O módulo de z é numericamente igual ao módulo do vetor de origem no ponto $(0,0)$ e extremidade (a,b), como representado na Figura 3.4.

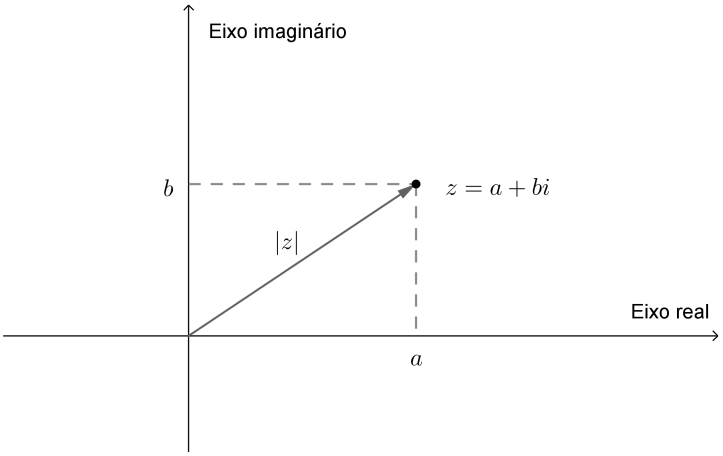

Figura 3.4: $z = a + bi$ e $|z| = \sqrt{a^2+b^2}$.

Veja que podemos usar o módulo para calcular a distância entre dois números complexos. De fato, note que dados dois números complexos $z = a + bi$ e $w = c + di$, temos que

$$|z - w| = |(a-c) + (b-d)i| = \sqrt{(a-c)^2 + (b-d)^2},$$

que é exatamente a fórmula para o cálculo da distância entre dos pontos (a,b) e (c,b) do plano cartesiano.

Exemplo 3.7. Vamos usar a definição de distância entre números complexos para determinar geometricamente os complexos z que satisfazem o sistema abaixo:

$$\begin{cases} |z-4| &= \sqrt{20} \\ |z+2| &= |z-6| \end{cases}.$$

Fazendo $z_1 = 4 + 0i$, $z_2 = -2 + 0i$ e $z_3 = 6 + 0i$, podemos reescrever o sistema da seguinte maneira:

$$\begin{cases} |z-z_1| &= \sqrt{20} \\ |z-z_2| &= |z-z_3| \end{cases}.$$

Veja que a primeira equação é satisfeita pelos complexos z cuja a distância até o complexo z_1 é constante igual a $\sqrt{20}$. Portanto, a solução da primeira equação é representada pela

circunferência de centro z_1 e raio $\sqrt{20}$. De modo semelhante, os complexos que satisfazem a outra equação são equidistantes dos complexos z_2 e z_3, neste caso, são os complexos z que estão sobre a mediatriz do segmento de reta determinado pelos complexos z_2 e z_3. Portanto, a solução do sistema é dado pelos pontos de interseção da circunferência com a mediatriz. Neste caso são os pontos z_4 e z_5, como representados na Figura 3.5.

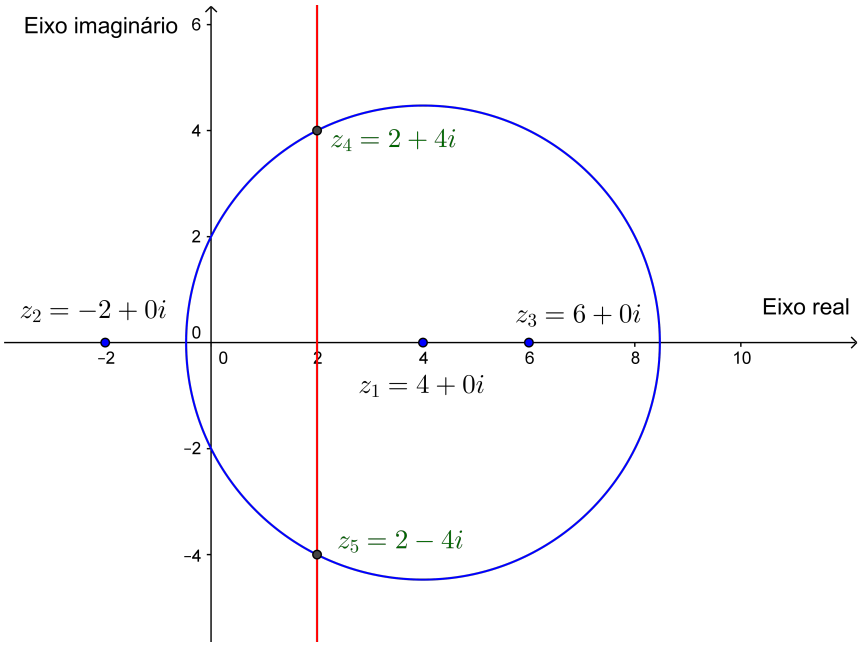

Figura 3.5: Solução geométrica do sistema.

Proposição 3.8. *Sejam $z = a + bi$ e $w = c + di$ dois números complexos. A conjugação tem as seguintes propriedades:*

1. $z \cdot \overline{z} = |z|^2$;
2. $|z| = |\overline{z}| = |-z|$;
3. $Re(z) \leq |Re(z)| \leq |z|$;
4. $Im(z) \leq |Im(z)| \leq |z|$;
5. $|z \cdot w| = |z| \cdot |w|$.

Demonstração. Considere os números complexos $z = a + bi$ e $w = c + di$. Temos então que,

1. $z \cdot \overline{z} = (a + bi) \cdot (a - bi) = a^2 - (bi)^2 = a^2 + b^2 = |z|^2$;
2. $|z| = \sqrt{a^2 + b^2} = \sqrt{a^2 + (-b)^2} = |\overline{z}| = \sqrt{a^2 + (-b)^2} = \sqrt{(-a)^2 + (-b)^2} = |-z|$;
3. $\mathrm{Re}(z) = a \leq |a| = |\mathrm{Re}(z)| = \sqrt{a^2} \leq \sqrt{a^2 + b^2} = |z|$;

4. $\text{Im}(z) = b \leq |b| = |\text{Im}(z)| = \sqrt{b^2} \leq \sqrt{a^2 + b^2} = |z|$;

5. $|z \cdot w| = \sqrt{|z \cdot w|^2} = \sqrt{(z \cdot w) \cdot \overline{(z \cdot w)}} = \sqrt{(z \cdot \overline{z}) \cdot (w \cdot \overline{w})} = \sqrt{|z|^2 \cdot |w|^2} = |z| \cdot |w|$.

□

Além das propriedades acima, o módulo de números complexos satisfaz a propriedade da desigualdade triangular, como veremos na proposição a seguir:

Proposição 3.9. *Sejam z e w dois números complexos quaisquer, temos então que,*

$$|z + w| \leq |z| + |w|,$$

valendo a igualdade se, e somente se, um dos números é múltiplo escalar real não negativo do outro.

Demonstração. Sejam z e w dois números complexos quaisquer. Observe que,

$$\begin{aligned}
|z + w|^2 &= (z + w) \cdot \overline{(z + w)} \\
&= (z + w) \cdot (\overline{z} + \overline{w}) \\
&= z \cdot \overline{z} + z \cdot \overline{w} + w \cdot \overline{z} + w \cdot \overline{w} \\
&= |z|^2 + z \cdot \overline{w} + \overline{z \cdot \overline{w}} + |w|^2 \\
&= |z|^2 + 2 \cdot \text{Re}(z \cdot \overline{w}) + |w|^2 \\
&\leq |z|^2 + 2 \cdot |\text{Re}(z \cdot \overline{w})| + |w|^2 \\
&\leq |z|^2 + 2 \cdot |z \cdot \overline{w}| + |w|^2 \\
&= |z|^2 + 2 \cdot |z| \cdot |\overline{w}| + |w|^2 \\
&= |z|^2 + 2 \cdot |z| \cdot |w| + |w|^2 \\
&= (|z| + |w|)^2 .
\end{aligned}$$

De onde segue que, $|z + w| \leq |z| + |w|$.
E, supondo $z = \alpha w$, com $\alpha \in \mathbb{R}$, temos que

$$|z + w| = |\alpha w + w| = |(\alpha + 1)w| = (\alpha + 1)|w| = \alpha|w| + |w| = |\alpha w| + |w| = |z| + |w|.$$

□

3.3 Forma Polar dos Números Complexos

Mudando as coordenadas cartesianas do ponto (a, b) para coordenadas polares, obtemos o número complexo $z = a + bi$ na sua forma polar

$$z = r \cdot (\cos(\theta) + i\text{sen}(\theta)),$$

onde $r = |z| = \sqrt{a^2 + b^2}$ e θ é o ângulo que o vetor (a, b) faz com o eixo real medido no sentido anti-horário. Como as funções seno e cosseno são periódicas, a representação polar do número complexos não é única. Basta observar que,

$$z = r \cdot (\cos(\theta) + i\text{sen}(\theta)) = r \cdot (\cos(\theta + 2k\pi) + i\text{sen}(\theta + 2k\pi)), \qquad \forall\ k \in \mathbb{Z}.$$

Cada ângulo que satisfaz a igualdade acima é chamado de argumento do número complexo z. Vamos considerar como argumento principal, ou simplesmente argumento, o número real $\theta \in [0, 2\pi[$ que satisfaz a igualdade acima. Vejamos então como determinar o argumento principal de um número complexo não nulo $z = a + bi$ qualquer.

- Se $a \neq 0$ e $b = 0$, temos que z é um número real e, portanto, está sobre o eixo real, daí, $\theta = 0$ se $a > 0$ e $\theta = \pi$ se $a < 0$;
- Se $a = 0$ e $b \neq 0$, temos que z é um imaginário puro e, portanto, está sobre o eixo imaginário, daí, $\theta = \frac{\pi}{2}$ se $b > 0$ e $\theta = \frac{3\pi}{2}$ se $b < 0$;
- Se $a \neq 0$, temos que θ é determinado pela equação;

  $$\tan(\theta) = \frac{b}{a} = \frac{\text{Im}(z)}{\text{Re}(z)},$$

  e pelo quadrante onde se encontra o ponto (a, b).

Exemplo 3.10. Dado o número complexos $z = 1 + \sqrt{3}i$, temos que,

$$\tan(\theta) = \frac{\text{Im}(z)}{\text{Re}(z)} = \frac{\sqrt{3}}{1} \quad \text{e} \quad |z| = \sqrt{1^2 + \sqrt{3}^2} = 2.$$

Logo, o argumento principal de z é $\theta = \frac{\pi}{3}$. Além disso, o ponto $(1, \sqrt{3})$ pertence ao primeiro quadrante, assim, uma representação polar para o complexo z é

$$z = 2 \cdot \left(\cos\left(\frac{\pi}{3}\right) + i\text{sen}\left(\frac{\pi}{3}\right)\right).$$

Devido a simetria de um número complexo z e seu conjugado $\overline{z}$, sendo θ um argumento para z, temos que $-\theta$ é um argumento para o complexo $\overline{z}$. De fato, dado $z = r \cdot (\cos(\theta) + i\text{sen}(\theta))$, temos que

$$\overline{z} = r \cdot (\cos(\theta) - i\text{sen}(\theta)) = r \cdot (\cos(-\theta) + i\text{sen}(-\theta)).$$

A partir da proposição a seguir veremos uma interpretação geométrica para o produto de dois números complexos.

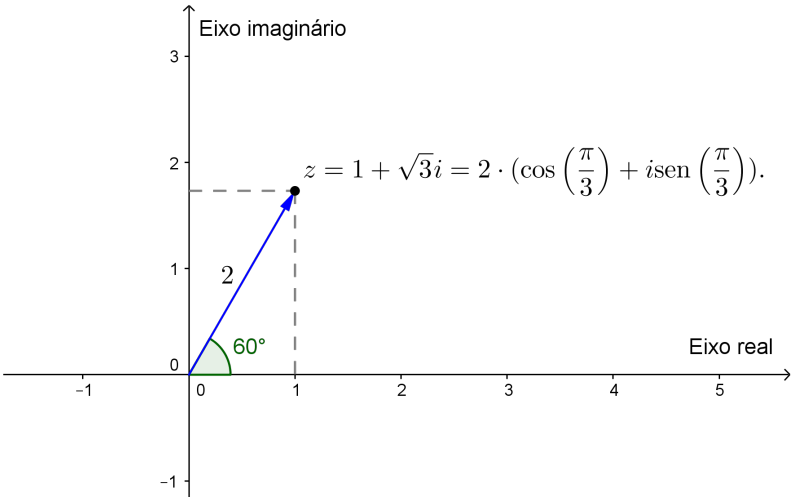

Figura 3.6: Forma polar do complexo $z = 1 + \sqrt{3}i$.

Proposição 3.11. *Sejam* $z_1 = r_1 \cdot (cos(\theta_1) + isen(\theta_1))$ *e* $z_2 = r_2 \cdot (cos(\theta_2) + isen(\theta_2))$ *dois números complexos quaisquer. Temos então que,*

$$z_1 \cdot z_2 = r_1 r_2 \cdot (cos(\theta_1 + \theta_2) + isen(\theta_1 + \theta_2)).$$

Demonstração. De fato,

$$\begin{aligned} z_1 \cdot z_2 &= r_1 \cdot (\cos(\theta_1) + i\text{sen}(\theta_1)) \cdot r_2 \cdot (\cos(\theta_2) + i\text{sen}(\theta_2)) \\ &= r_1 r_2 \cdot (\cos(\theta_1)\cos(\theta_2) + \cos(\theta_1) i\text{sen}(\theta_2) + i\text{sen}(\theta_1)\cos(\theta_2) + i\text{sen}(\theta_1) i\text{sen}(\theta_2)) \\ &= r_1 r_2 \cdot ((\cos(\theta_1)\cos(\theta_2) - \text{sen}(\theta_1)\text{sen}(\theta_2)) + (\cos(\theta_1)\text{sen}(\theta_2) + \text{sen}(\theta_1)\cos(\theta_2))) \\ &= r_1 r_2 \cdot (\cos(\theta_1 + \theta_2) + i\text{sen}(\theta_1 + \theta_2)). \end{aligned}$$

□

Exemplo 3.12. Considere os números complexos $z_1 = \sqrt{3} + i$ e $z_2 = -2\sqrt{3} + 2i$. Observe que,

$$z_1 \cdot z_2 = (\sqrt{3} + i) \cdot (-2\sqrt{3} + 2i) = -8 + 0i.$$

Por outro lado, temos que,

$$z_1 = 2 \cdot \left(\cos\left(\frac{\pi}{6}\right) + i\text{sen}\left(\frac{\pi}{6}\right)\right) \quad \text{e} \quad z_2 = 4 \cdot \left(\cos\left(\frac{5\pi}{6}\right) + i\text{sen}\left(\frac{5\pi}{6}\right)\right),$$

e, pela proposição anterior,

$$z_1 \cdot z_2 = 2 \cdot 4 \cdot \left(\cos\left(\frac{\pi}{6} + \frac{5\pi}{6}\right) + i\text{sen}\left(\frac{\pi}{6} + \frac{5\pi}{6}\right)\right) = 8 \cdot (\cos(\pi) + i\text{sen}(\pi)).$$

Observe que de fato obtemos o mesmo resultado.

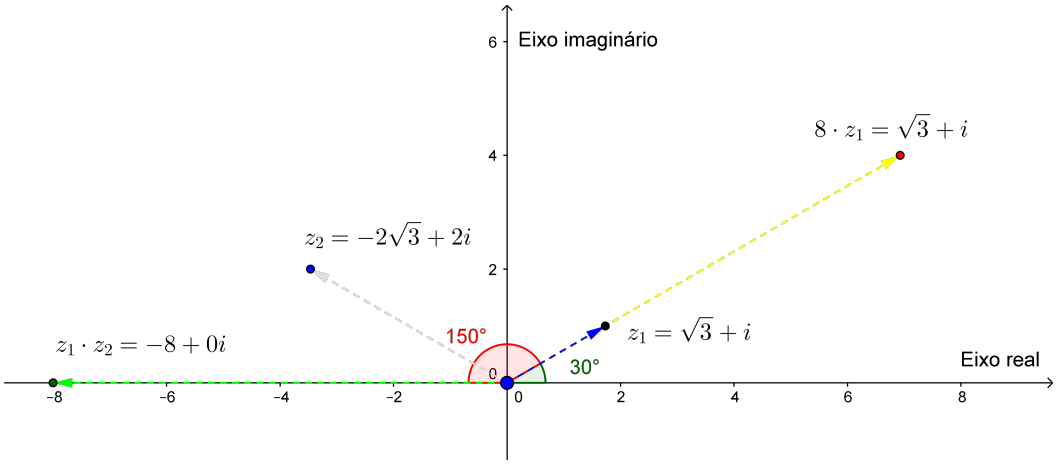

Figura 3.7: Multiplicação dos complexos $z_1 = \sqrt{3} + i$ e $z_2 = -2\sqrt{3} + 2i$.

Observe que no exemplo anterior o complexo $z_1 \cdot z_2$ pode ser obtido geometricamente por meio de uma translação, obtendo o complexo $8 \cdot z_1$, seguida de uma rotação realizada no ponto $(\sqrt{3}, 1)$ em torno da origem, como mostra a Figura 3.7. No caso em que um dos complexos tem módulo igual a 1, o produto entre os complexos z_1 e z_2 é equivalente a uma rotação, ou seja, dado $z_0 = r_0 \cdot (\cos(\theta_0) + i\text{sen}(\theta_0))$, com $\theta_0 > 0$, para qualquer complexo z, temos que $z_0 \cdot z$ é a rotação do complexo z pelo ângulo θ_0 no sentido anti-horário. Se $\theta_0 < 0$, a rotação é no sentido horário.

Utilizando indução matemática é possível mostrar que,

$$[r \cdot (\cos(\theta) + i\text{sen}(\theta))]^n = r^n \cdot (\cos(n\theta) + i\text{sen}(n\theta)),$$

para todo natural n.

Exemplo 3.13. Considere o número complexo $z = \frac{1}{2} + \frac{\sqrt{3}}{2}i$, temos que

$$z = 1 \cdot \left(\cos\left(\frac{\pi}{3}\right) + i\text{sen}\left(\frac{\pi}{3}\right)\right),$$

assim,

$$z^2 = 1^2 \cdot \left(\cos\left(2 \cdot \frac{\pi}{3}\right) + i\text{sen}\left(2 \cdot \frac{\pi}{3}\right)\right) = 1 \cdot \left(-\frac{1}{2} + \frac{\sqrt{3}}{2}\right) = -\frac{1}{2} + \frac{\sqrt{3}}{2},$$

$$z^3 = 1^3 \cdot \left(\cos\left(3 \cdot \frac{\pi}{3}\right) + i\text{sen}\left(3 \cdot \frac{\pi}{3}\right)\right) = 1 \cdot (-1 + 0) = -1 + 0i.$$

A Figura 3.13 mostra a representação geométrica das demais potências do complexo número complexos z.

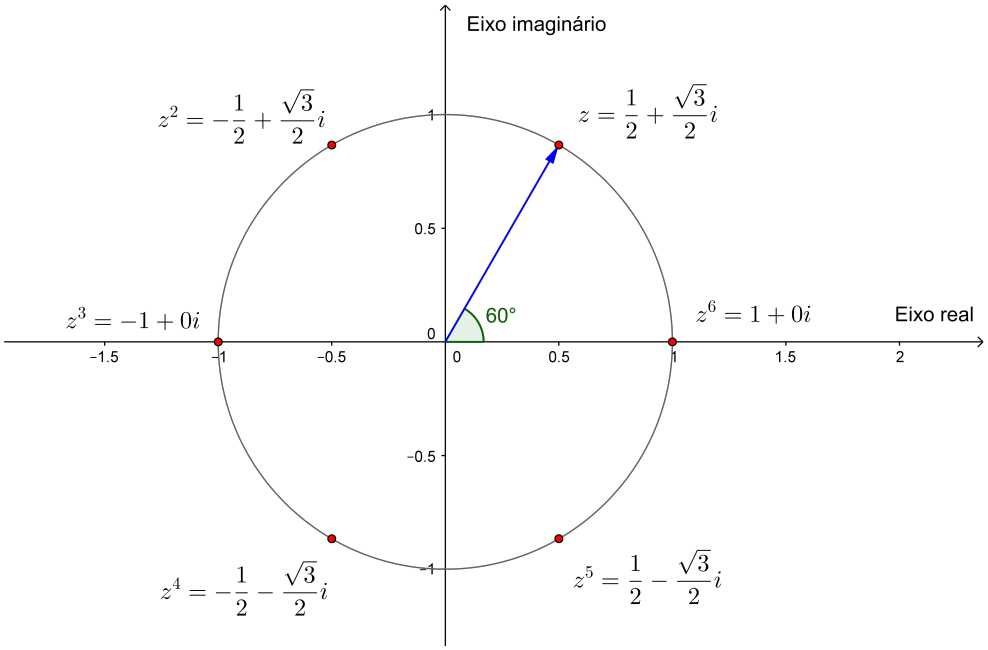

Figura 3.8: Potências do complexos $z = z = \frac{1}{2} + \frac{\sqrt{3}}{2}i$.

Capítulo 4

Códigos Corretores via Quatérnios

O conjunto dos quatérnios, com as definições de adição e multiplicação a serem definidas, introduzem no espaço euclidiano $\mathbb{R}^4$ uma estrutura algébrica similar à estrutura dos números complexos no plano $\mathbb{R}^2$. Os quatérnios foram descobertos em 1843, pelo matemático irlandês William Rowan Hamilton (1805-1865), dez anos após ter obtido o resultado que os números complexos determinam uma álgebra para os pares ordenados de números reais de modo que é possível realizar rotações por meio de multiplicações. Motivado a encontrar uma estrutura semelhante para realizar operações no espaço, Hamilton fez várias tentativas de definir uma estrutura algébrica para os ternos ordenados de modo que fosse possível realizar rotações, no entanto, chegou a conclusão que não era possível definir tal estrutura. A partir daí, o matemático irlandês passou a pensar em números com uma entrada real e três imaginárias, isto é, o que hoje conhecemos como quatérnios de Hamilton. A base da álgebra descrita por ele é a equação

$$i^2 = j^2 = k^2 = ijk = -1, \tag{4.1}$$

descoberta pelo próprio matemático em 1843 e conhecida como equação fundamental dos quatérnios [18].

A partir da equação fundamental obtemos a tábua de multiplicação (Tabela 4) dos elementos i, j e k. De imediato é possível perceber que a multiplicação é não comutativa.

$\cdot$	1	i	j	k
1	1	i	j	k
i	i	-1	k	$-j$
j	j	$-k$	-1	i
k	k	j	$-i$	-1

Tabela 4.1: Multiplicação dos elementos da base.

As principais referências que utilizamos nesta seção foram: [1], [3], [4], [12], [17] e [18].

4.1 Definições e resultados básicos

Seja $\mathbb{R}$ o corpo dos números reais. Denotamos por $\{1, i, j, k\}$ a base canônica do espaço $\mathbb{R}^4$, ou seja, a base $\{(1,0,0,0); (0,1,0,0); (0,0,1,0); (0,0,0,1)\}$. Desta maneira, um elemento $q = (q_0, q_1, q_2, q_3) \in \mathbb{R}^4$, pode ser escrito na forma $q = q_0 + q_1 i + q_2 j + q_3 k$. A partir daí, dados $q = q_0 + q_1 i + q_2 j + q_3 k$, $p = p_0 + p_1 i + p_2 j + p_3 k \in \mathbb{R}^4$ e $\alpha \in \mathbb{R}$, definimos a operação de adição de modo usual e a de multiplicação de modo distributivo, respeitando a equação fundamental dos quatérnios (4.1), isto é,

$$\alpha q + p = (\alpha q_0 + p_0) + (\alpha q_1 + p_1)i + (\alpha q_2 + p_2)j + (\alpha q_3 + p_3)k \in \mathbb{R}^4,$$

e

$$\begin{aligned}
p \cdot q &= (q_0 + q_1 i + q_2 j + q_3 k) \cdot (p_0 + p_1 i + p_2 j + p_3 k) \\
&= (q_0 p_0 + q_0 p_1 i + q_0 p_2 j + q_0 p_3 k) + (q_1 i p_0 + q_1 i p_1 i + q_1 i p_2 j + q_1 i p_3 k) \\
&\quad (q_2 j p_0 + q_2 j p_1 i + q_2 j p_2 j + q_2 j p_3 k) + (q_3 k p_0 + q_3 k p_1 i + q_3 k p_2 j + q_3 k p_3 k) \\
&= (q_0 p_0 + q_0 p_1 i + q_0 p_2 j + q_0 p_3 k) + (q_1 p_0 i + q_1 p_1 i^2 + q_1 p_2 ij + q_1 p_3 ik) \\
&\quad (q_2 p_0 j + q_2 p_1 ji + q_2 p_2 j^2 + q_2 p_3 jk) + (q_3 p_0 k + q_3 p_1 ki + q_3 p_2 kj + q_3 p_3 k^2) \\
&= (q_0 p_0 + q_0 p_1 i + q_0 p_2 j + q_0 p_3 k) + (q_1 p_0 i - q_1 p_1 + q_1 p_2 k - q_1 p_3 j) \\
&\quad (q_2 p_0 j - q_2 p_1 k - q_2 p_2 + q_2 p_3 i) + (q_3 p_0 k + q_3 p_1 j - q_3 p_2 i - q_3 p_3) \\
&= (q_0 p_0 - q_1 p_1 - q_2 p_2 - q_3 p_3) + (q_0 p_1 + q_1 p_0 + q_2 p_3 - q_3 p_2)i + \\
&\quad (q_0 p_2 - q_1 p_3 + q_2 p_0 + q_3 p_1)j + (q_0 p_3 + q_1 p_2 - q_2 p_1 + q_3 p_0)k \in \mathbb{R}^4.
\end{aligned}$$

Vejamos agora algumas propriedades em relação a adição. Considere,

$$q = q_0 + q_1 i + q_2 j + q_3 k,\ p = p_0 + p_1 i + p_2 j + p_3 k,\ r = r_0 + r_1 i + r_2 j + r_3 k \in \mathbb{R}^4,$$

temos que,

$$\begin{aligned}
q + (p + r) &= q_0 + q_1 i + q_2 j + q_3 k + (p_0 + r_0) + (p_1 + r_1)i + (p_2 + r_2)j + (p_3 + r_3)k \\
&= (q_0 + p_0 + r_0) + (q_1 + p_1 + r_1)i + (q_2 + p_2 + r_2)j + (q_3 + p_3 + r_3)k \\
&= (q_0 + p_0) + (q_1 + p_1)i + (q_2 + p_2)j + (q_3 + p_3)k + r_0 + r_1 i + r_2 j + r_3 k \\
&= (q + p) + r.
\end{aligned}$$

E,

$$\begin{aligned}
q + p &= (q_0 + p_0) + (q_1 + p_1)i + (q_2 + p_2)j + (q_3 + p_3)k \\
&= (p_0 + q_0) + (p_1 + q_1)i + (p_2 + q_2)j + (p_3 + q_3)k \\
&= p + q.
\end{aligned}$$

Sejam $0_{\mathbb{H}} = 0 + 0i + 0j + 0k$, $-q = -q_0 - q_1 i - q_2 j - q_3 k \in \mathbb{R}^4$. Segue então que

$$\begin{aligned} q + 0_{\mathbb{H}} &= (q_0 + 0) + (q_1 + 0)i + (q_2 + 0)j + (q_3 + 0)k \\ &= q_0 + q_1 i + q_2 j + q_3 k \\ &= q, \end{aligned}$$

e

$$\begin{aligned} q + (-q) &= (q_0 - q_0)(q_1 - q_1)i + (q_2 - q_2)j + (q_3 - q_3)k \\ &= 0 + 0i + 0j + 0k \\ &= 0_{\mathbb{H}}. \end{aligned}$$

Apesar de não comutativa, a multiplicação definida acima goza de algumas propriedades importantes. Vejamos primeiro um maneira alternativa para a definição da multiplicação usando conceitos de Geometria Analítica.

Proposição 4.1. *Dados $q = q_0 + q_1 i + q_2 j + q_3 k$, $p = p_0 + p_1 i + p_2 j + p_3 k \in \mathbb{R}^4$, podemos definir a multiplicação $q \cdot p$ da seguinte maneira*

$$q \cdot p = q_0 p_0 - \vec{q} * \vec{p} + q_0 \vec{p} + p_0 \vec{q} + \vec{q} \times \vec{p}.$$

Onde, $\vec{q} = (q_1, q_2, q_3)$, $\vec{p} = (p_1, p_2, p_3)$, "$*$" representa o produto interno e "$\times$" representa o produto vetorial.

Demonstração.

$$\begin{aligned} p \cdot q &= (q_0 + q_1 i + q_2 j + q_3 k) \cdot (p_0 + p_1 i + p_2 j + p_3 k) \\ &= (q_0 p_0 - q_1 p_1 - q_2 p_2 - q_3 p_3) + (q_0 p_1 + q_1 p_0 + q_2 p_3 - q_3 p_2)i + \\ &\quad (q_0 p_2 - q_1 p_3 + q_2 p_0 + q_3 p_1)j + (q_0 p_3 + q_1 p_2 - q_2 p_1 + q_3 p_0)k \\ &= (q_0 p_0 - (q_1 p_1 + q_2 p_2 + q_3 p_3)) + (q_0 p_1 i + q_0 p_2 j + q_0 p_3 k) + \\ &\quad (p_0 q_1 i + p_0 q_2 j + p_0 q_3 k) + (q_2 p_3 i + q_3 p_1 j + q_1 p_2 k - p_2 q_3 i - p_3 q_1 - p_1 q_2 k) \\ &= (q_0 p_0 - \vec{q} * \vec{p}) + q_0 \vec{p} + p_0 \vec{q} + \vec{q} \times \vec{p}. \end{aligned}$$

□

Note que na expressão $q \cdot p = (q_0 p_0 - \vec{q} * \vec{p}) + q_0 \vec{p} + p_0 \vec{q} + \vec{q} \times \vec{p}$, cometemos um abuso de notação, não faz muito sentido somar um número real com um elemento do $\mathbb{R}^3$. Usando a notação $q = q_0 + q_1 i + q_2 j + q_3 k = q_0 + \hat{q}$, temos as seguintes definições:

- q_0 representa a parte real de q e denota-se por $\mathrm{Re}(q)$;
- $\hat{q} = q_1 i + q_2 j + q_3 k$ representa a parte vetorial (parte imaginária) de q e denota-se por $\mathrm{Im}(q)$ ou $\mathrm{Vec}(q)$;
- $\vec{q} = (q_1, q_2, q_3)$ representa o vetor de $\mathbb{R}^3$ associado a parte vetorial de q. Assim, qualquer elemento q pode ser escrito como $q = q_0 + \vec{q}$.

- se $\mathrm{Re}(q) = 0$, dizemos que q é um elemento imaginário puro de $\mathbb{R}^4$.

Podemos então representar um elemento $q = q_0 + q_1 i + q_2 j + q_3 k \in \mathbb{R}^4$ utilizando sua parte real e sua parte imaginária da seguinte maneira $q = (q_0, \vec{q})$.

Provemos agora que a multiplicação é associativa. Considerando

$$q = q_0 + q_1 i + q_2 j + q_3 k,\ p = p_0 + p_1 i + p_2 j + p_3 k,\ r = r_0 + r_1 i + r_2 j + r_3 k \in \mathbb{R}^4,$$

temos que

$$\begin{aligned}
q \cdot (p \cdot r) &= (q_0, \vec{q}) \cdot (p_0 r_0 - \vec{p} * \vec{r}, p_0 \vec{r} + r_0 \vec{p} + \vec{p} \times \vec{r}) \\
&= (q_0(p_0 r_0 - \vec{p} * \vec{r}) - \vec{q} * (p_0 \vec{r} + r_0 \vec{p} + \vec{p} \times \vec{r}), q_0(p_0 \vec{r} + r_0 \vec{p} + \vec{p} \times \vec{r})) + \\
&\quad (p_0 r_0 - \vec{p} * \vec{r})\vec{q} + \vec{q} \times (p_0 \vec{r} + r_0 \vec{p} + \vec{p} \times \vec{r}) \\
&= (q_0 p_0 r_0 - q_0 \vec{p} * \vec{r} - \vec{q} * p_0 \vec{r} - \vec{q} * r_0 \vec{p} + \vec{q} * (\vec{p} \times \vec{r}), q_0 p_0 \vec{r} + q_0 r_0 \vec{p} + \\
&\quad q_0 \vec{p} \times \vec{r} + p_0 r_0 \vec{q} - (\vec{p} * \vec{r})\vec{q} + \vec{q} \times p_0 \vec{r} + \vec{q} \times r_0 \vec{p} + \vec{q} \times \vec{p} \times \vec{r}) \\
&= (q_0 p_0 r_0 - q_0 \vec{p} * \vec{r} - \vec{q} * p_0 \vec{r} - \vec{q} * r_0 \vec{p} + \vec{q} * (\vec{p} \times \vec{r}), q_0 p_0 \vec{r} + q_0 r_0 \vec{p} + \\
&\quad q_0 \vec{p} \times \vec{r} + p_0 r_0 \vec{q} - (\vec{p} * \vec{r})\vec{q} + \vec{q} \times p_0 \vec{r} + \vec{q} \times r_0 \vec{p} + (\vec{q} * \vec{r})\vec{p} - (\vec{q} * \vec{p})\vec{r})
\end{aligned}$$

e

$$\begin{aligned}
(q \cdot p) \cdot r &= (q_0 p_0 - \vec{q} * \vec{p}, q_0 \vec{p} + p_0 \vec{q} + \vec{q} \times \vec{p}) \cdot (r_0, \vec{r}) \\
&= (q_0 p_0 r_0 - \vec{q} * \vec{p} r_0 - q_0 \vec{p} * \vec{r} - p_0 \vec{q} * \vec{r} - (\vec{q} \times \vec{p}) * \vec{r}, q_0 p_0 \vec{r} - (\vec{q} * \vec{p})\vec{r} + \\
&\quad r_0 q_0 \vec{p} + r_0 p_0 \vec{q} + r_0 \vec{q} \times \vec{p} + q_0 \vec{p} \times \vec{r} + p_0 \vec{q} \times \vec{r} + \vec{q} \times \vec{p} \times \vec{r}) \\
&= (q_0 p_0 r_0 - \vec{q} * \vec{p} r_0 - q_0 \vec{p} * \vec{r} - p_0 \vec{q} * \vec{r} - (\vec{q} \times \vec{p}) * \vec{r}, q_0 p_0 \vec{r} + q_0 r_0 \vec{p} + \\
&\quad + r_0 p_0 \vec{q} - (\vec{q} * \vec{p})\vec{r} + r_0 \vec{q} \times \vec{p} + q_0 \vec{p} \times \vec{r} + p_0 \vec{q} \times \vec{r} + (\vec{q} * \vec{r})\vec{p} - (\vec{q} * \vec{p})\vec{r}) \\
&= (q_0 p_0 r_0 - q_0 \vec{p} * \vec{r} - \vec{q} * p_0 \vec{r} - \vec{q} * r_0 \vec{p} + \vec{q} * (\vec{p} \times \vec{r}), q_0 p_0 \vec{r} + q_0 r_0 \vec{p} + \\
&\quad q_0 \vec{p} \times \vec{r} + p_0 r_0 \vec{q} - (\vec{p} * \vec{r})\vec{q} + \vec{q} \times p_0 \vec{r} + \vec{q} \times r_0 \vec{p} + (\vec{q} * \vec{r})\vec{p} - (\vec{q} * \vec{p})\vec{r}).
\end{aligned}$$

Comparando as duas igualdades acima, concluímos que vale a associatividade, ou seja, que $q \cdot (p \cdot r) = (q \cdot p) \cdot r$.

Além da propriedade associativa, a multiplicação junto com a adição satisfazem as leis distributivas, isto é,

$$\begin{aligned}
q \cdot (p + r) &= (q_0, \vec{q}) \cdot (p_0 + r_0, \vec{p} + \vec{r}) \\
&= (q_0(p_0 + r_0) - \vec{q} * (\vec{p} + \vec{r}),\ q_0(\vec{p} + \vec{r}) + (p_0 + r_0)\vec{q} + \vec{q} \times (\vec{p} + \vec{r})) \\
&= (q_0 p_0 - \vec{q} * \vec{p} + q_0 r_0 - \vec{q} * \vec{r}, q_0 \vec{p} + p_0 \vec{q} + \vec{q} \times \vec{p} + q_0 \vec{r} + r_0 \vec{q} + \vec{q} \times \vec{r}) \\
&= q \cdot p + q \cdot r,
\end{aligned}$$

e modo análogo $(p + r) \cdot q = p \cdot q + r \cdot q$.

Definição 4.2. Sejam $q = q_0 + q_1 i + q_2 j + q_3 k \in \mathbb{R}^4$. O conjugado de q, denotado por $\bar{q}$,

é definido da seguinte maneira

$$\bar{q} = q_0 - q_1 i - q_2 j - q_3 k = q_0 - \hat{q} = (q_0, -\vec{q}).$$

Observe que,

$$\begin{aligned} q \cdot \bar{q} &= (q_0, \vec{q}) \cdot (q_0, -\vec{q}) \\ &= (q_0 q_0 + \vec{q} * \vec{q}, -q_0\vec{q} + q_0\vec{q} + \vec{q} \times (-\vec{q})) \\ &= (q_0^2 + q_1^2 + q_2^2 + q_3^2, \vec{0}) \\ &= q_0^2 + q_1^2 + q_2^2 + q_3^2 \\ &\geq 0, \end{aligned}$$

sendo a igualdade verdadeira apenas quando $q_0 = q_1 = q_2 = q_3 = 0$, ou seja, apenas no caso em que $q = 0_{\mathbb{H}}$. Da mesma forma, $\bar{q} \cdot q = q_0^2 + q_1^2 + q_2^2 + q_3^2$.

Definição 4.3. Seja $q = q_0 + q_1 i + q_2 j + q_3 k \in \mathbb{R}^4$, um quatérnio. Definimos a **norma reduzida** e o **módulo** de q, respectivamente, por

$$N_{red}(q) = {q_0}^2 + {q_1}^2 + {q_2}^2 + {q_3}^2 \qquad \text{e} \qquad \|q\| = \sqrt{N_{red}(q)}.$$

Estamos prontos para ver mais duas propriedades da multiplicação, a existência da unidade multiplicativa $1_{\mathbb{H}} = 1 + 0i + 0j + 0k = (1, \vec{0})$ e a existência do inverso multiplicativo $q^{-1} = \dfrac{\bar{q}}{\|q\|^2}$ de um elemento $q \neq 0$. Observe que,

$$\begin{aligned} q \cdot 1_{\mathbb{H}} &= (q_0, \vec{q}) \cdot (1, \vec{0}) \\ &= (q_0 1 + \vec{q} * \vec{0}, q_0\vec{0} + 1\vec{q} + \vec{q} \times \vec{0}) \\ &= (q_0, \vec{q}) \\ &= q \\ &= (1q_0 + \vec{0} * \vec{q}, 1\vec{q} + q_0\vec{0} + \vec{0} \times \vec{q}) \\ &= (1, \vec{0}) \cdot (q_0, \vec{q}) \\ &= 1_{\mathbb{H}} \cdot q. \end{aligned}$$

Agora, supondo $q \neq 0$, segue que

$$\begin{aligned} q \cdot \frac{\bar{q}}{\|q\|^2} &= \frac{1}{\|q\|^2} q \cdot \bar{q} \\ &= \frac{1}{\|q\|^2} \bar{q} \cdot q \\ &= \frac{1}{\|q\|^2} (q_0^2 + q_1^2 + q_2^2 + q_3^2, \vec{0}) \\ &= \frac{1}{\|q\|^2} (\|q\|^2, \vec{0}) \\ &= (1, \vec{0}). \end{aligned}$$

Chegamos então a conclusão que o espaço $\mathbb{R}^4$ com as operações de adição e multiplicação definidas acima tem uma estrutura de anel com unidade. Além disso, todo elemento diferente de zero tem um inverso multiplicativo. Este anel foi descoberto por Hamilton em 1843 e é conhecido como quatérnios de Hamilton. Denotaremos este anel por $(\mathbb{H}, +, \cdot)$, ou simplesmente por $\mathbb{H}$.

Além das propriedades da estrutura de anel com unidade, os quatérnios de Hamilton apresenta várias outras propriedades interessantes, veremos agora algumas das propriedades da norma reduzida e da conjugação de quatérnios.

Proposição 4.4. *Sejam $q = q_0 + q_1 i + q_2 j + q_3 k,\ p = p_0 + p_1 i + p_2 j + p_3 k \in \mathbb{R}^4$, dois quatérnios e $\alpha \in \mathbb{R}$ um escalar. Então,*

1. $\bar{\bar{q}} = q$;
2. $\overline{q \cdot p} = \bar{p} \cdot \bar{q}$;
3. $\overline{q + p} = \bar{q} + \bar{p}$;
4. $\overline{\alpha \cdot q} = \alpha \bar{q}$;
5. $q \cdot \bar{q} = \bar{q} \cdot q$.

Demonstração. Sejam $q = q_0 + q_1 i + q_2 j + q_3 k = (q_0, \vec{q}),\ p = p_0 + p_1 i + p_2 j + p_3 k = (p_0, \vec{p}) \in \mathbb{H}$, dois quatérnios e $\alpha \in \mathbb{R}$ um escalar.

1.
$$\bar{\bar{q}} = \overline{(q_0, -\vec{q})} = (q_0, -(-\vec{q})) = (q_0, \vec{q}) = q;$$

2.
$$\begin{aligned} \bar{p} \cdot \bar{q} &= (p_0, -\vec{p}) \cdot (q_0, -\vec{q}) \\ &= (p_0 q_0 - \vec{p} * \vec{q}, -p_0 \vec{q} - q_0 \vec{p} + \vec{p} \times \vec{q}) \\ &= (q_0 p_0 - \vec{q} * \vec{p}, -q_0 \vec{p} - p_0 \vec{q} - \vec{q} \times \vec{p}) \\ &= \overline{(q_0 p_0 - \vec{q} * \vec{p}, q_0 \vec{p} + p_0 \vec{q} + \vec{q} \times \vec{p})} \\ &= \overline{q \cdot p}; \end{aligned}$$

3.
$$\overline{q+p} = \overline{(q_0+p_0, \vec{q}+\vec{p})} = (q_0+p_0, -\vec{q}-\vec{p}) = \bar{q}+\bar{p};$$

4.
$$\overline{\alpha q} = \alpha q_0 - \alpha q_1 i - \alpha q_2 j - \alpha q_3 k = \alpha(q_0 - q_1 i - q_2 j - q_3 k) = \alpha\bar{p};$$

5.
$$q \cdot \bar{q} = N_{red}(q) = \bar{q} \cdot q.$$

□

Proposição 4.5. *Sejam* $q = q_0 + q_1 i + q_2 j + q_3 k,\ p = p_0 + p_1 i + p_2 j + p_3 k \in \mathbb{R}^4$, *dois quatérnios e* $\alpha \in \mathbb{R}$ *um escalar. Então,*

1. $\|q\|^2 = \|\bar{q}\|^2$;
2. $\|\alpha \cdot q\|^2 = \alpha^2 \cdot \|q\|^2$;
3. $\|q \cdot p\|^2 = \|q\|^2 \cdot \|p\|^2$

Demonstração. Sejam $q = q_0 + q_1 i + q_2 j + q_3 k,\ p = p_0 + p_1 i + p_2 j + p_3 k \in \mathbb{R}^4$, dois quatérnios e $\alpha \in \mathbb{R}$ um escalar.

1.
$$\|q\|^2 = q \cdot \bar{q} = \bar{q} \cdot q = \bar{q} \cdot \bar{\bar{q}} = \|\bar{q}\|^2;$$

2.
$$\begin{aligned} \|\alpha \cdot q\|^2 &= \|\alpha q_0 + \alpha q_1 i + \alpha q_2 j + \alpha q_3 k\|^2 \\ &= (\alpha q_0)^2 + (\alpha q_1)^2 + (\alpha q_2)^2 + (\alpha q_3)^2 \\ &= \alpha^2(q_0^2 + q_1^2 + q_2^2 + q_3^2) \\ &= \alpha^2 \cdot \|q\|^2; \end{aligned}$$

3.
$$\|q \cdot p\|^2 = q \cdot p \cdot \overline{q \cdot p} = q \cdot p \cdot \bar{p} \cdot \bar{q} = q \cdot \|p\|^2 \cdot \bar{q} = q \cdot \bar{q} \cdot \|p\|^2 = \|q\|^2 \cdot \|p\|^2.$$

□

4.2 Representação matricial

Nesta seção vamos estabelecer uma relação entre o anel dos quatérnios de Hamilton, o anel dos números complexos e um subanel do anel das matrizes de ordem 2 com entradas complexas. Antes disso vamos definir o conjunto dos quatérnios puros e unitários $\mathbb{H}_1^P$ por,

$$\mathbb{H}_1^P = \{q \in \mathbb{H} \mid \|q\|^2 = 1 \text{ e } \mathrm{Re}(q) = 0\}.$$

Observe que dados $q = (0, \vec{q}), p = (0, \vec{p}) \in \mathbb{H}_1^P$, temos que

$$\|q \cdot p\|^2 = \|q\|^2 \|p\|^2 = 1,$$

logo $q \cdot p \in \mathbb{H}_1$, ou seja, pertence ao conjunto dos quatérnios unitários. No entanto,

$$q \cdot p = (0, \vec{q}) \cdot (0, \vec{p}) = (0 - \vec{q} * \vec{p}, 0\vec{q} + 0\vec{p} + \vec{q} \times \vec{p}) = (-\vec{q} * \vec{p}, \vec{q} \times \vec{p}),$$

assim, teremos $q \cdot p$ puro, se $\vec{q} * \vec{p} = 0$, o que acontece se e somente se $\vec{q}$ e $\vec{p}$ forem perpendiculares.

Uma outra propriedade interessante dos quatérnios puros e unitários é que seus quadrados são sempre iguais a -1. De fato, dado $q \in \mathbb{H}_1$, temos que

$$q^2 = q \cdot q = q \cdot \bar{\bar{q}} = q \cdot \overline{-q} = -q \cdot \bar{q} = -\|q\|^2 = -1.$$

Sejam $\mathbb{C} = \{a + bi \mid a, b \in \mathbb{R}, \text{ e } i^2 = -1\}$, o anel dos números complexos, $q \in \mathbb{H}_1^P$ um quatérnio fixo e φ_q uma aplicação entre os anéis $\mathbb{C}$ e $\mathbb{H}$ definida por

$$\begin{array}{rccc} \varphi_q & : & \mathbb{C} & \longrightarrow & \mathbb{H} \\ & & a + bi & \longmapsto & \varphi_q(a + bi) = a + bq. \end{array}$$

Considere $z = a + bi,\ w = c + di \in \mathbb{C}$. Temos que,

$$\begin{aligned} \varphi_q(z) \cdot \varphi_q(w) &= (a + bq) \cdot (c + dq) \\ &= a \cdot c + a \cdot dq + bq \cdot c + bq \cdot dq \\ &= ac + adq + bcq + bdq \cdot q \\ &= ac + adq + bcq - bd \\ &= ac - bd + adq + bcq \\ &= (ac - bd) + (ad + bc)q \\ &= \varphi_q(zw) \end{aligned}$$

e

$$\begin{aligned} \varphi_q(z + w) &= \varphi_q\left((a + c) + (b + d)i\right) \\ &= (a + c) + (b + d)q \\ &= a + c + bq + dq \\ &= a + bq + c + dq \\ &= \varphi_q(z) + \varphi_q(w). \end{aligned}$$

E observe que,

$$\varphi_q(z) = 0 \Rightarrow a + bq = 0 \Rightarrow a = -bq \Rightarrow a = b = 0,$$

pois a é real e $-bq \in \mathbb{H}^P$.

Portanto, a aplicação φ_q preserva a adição e a multiplicação. Desta maneira, temos um homomorfismo injetor entre os anéis $\mathbb{C}$ e $\mathbb{H}$. Assim, $\mathbb{C}$ pode ser visto como um subanel de $\mathbb{H}$, basta tomar $q = j$, por exemplo. Além disso, a aplicação φ_q determina um subanel comutativo de $\mathbb{H}$. De fato, note que

$$\begin{aligned} \varphi_q\left((a+bi)(c+di)\right) &= \varphi_q(a+bi)\cdot\varphi_q(c+di) \\ \varphi_q\left((c+di)(a+bi)\right) &= \varphi_q(c+di)\cdot\varphi_q(a+bi), \end{aligned}$$

como,

$$(a+bi)(c+di) = (c+di)(a+bi)$$

temos,

$$\varphi_q(a+bi)\cdot\varphi_q(c+di) = \varphi_q(c+di)\cdot\varphi_q(a+bi).$$

Seja $\mathbb{C}^2 = \{(z,w) \mid z,w \in \mathbb{C}\}$ o conjunto de pares ordenados com entradas em $\mathbb{C}$, no qual definimos as operações de adição "+"e multiplicação "$\odot$"da seguinte maneira:

$$(z_1,w_1) + (z_2,w_2) = (z_1+z_2, w_1+w_2)$$

e

$$(z_1,w_1)\odot(z_2,w_2) = (z_1z_2 - w_1\overline{w_2}, z_1w_2 + w_1\overline{z_2}),$$

para todos (z_1,w_1), $(z_2,w_2) \in \mathbb{C}^2$. E seja ϕ_q uma aplicação entre $\mathbb{C}^2$ e $\mathbb{H}$ definida por

$$\begin{aligned} \phi_q \quad : \quad & \mathbb{C}^2 \longrightarrow \mathbb{H} \\ & (z,w) \longmapsto \phi_q\left((z,w)\right) = z + w\cdot q, \end{aligned}$$

onde $q \in \mathbb{H}_1^P$ é um quatérnio fixo.

Considere $z_1 = a_1 + b_1 i$, $z_2 = a_2 + b_2 i$, $w_1 = c_1 + d_1 i$ e $w_2 = c_2 + d_2 i \in \mathbb{C}$. Temos que,

$$\begin{aligned} \phi_q\left((z_1,w_1)\right) + \phi_q\left((z_2,w_2)\right) &= (z_1 + w_1\cdot q) + (z_2 + w_2\cdot q) \\ &= z_1 + z_2 + w_1\cdot q + w_2\cdot q \\ &= (z_1+z_2) + (w_1+w_2)\cdot q \\ &= \phi_q\left((z_1,w_1) + (z_2,w_2)\right). \end{aligned}$$

No entanto,

$$\begin{aligned}
\phi_q((z_1,w_1))\cdot\phi_q((z_2,w_2)) &= (z_1+w_1\cdot q)\cdot(z_2+w_2\cdot q)\\
&= z_1\cdot z_2+w_1\cdot q\cdot w_2\cdot q+w_1\cdot q\cdot z_2+z_1\cdot w_2\cdot q\\
&= z_1z_2+(c_1+d_1i)\cdot q\cdot(c_2+d_2i)\cdot q+(c_1+d_1i)\cdot q\\
&\quad\cdot(a_2+b_2i)+z_1\cdot w_2\cdot q\\
&= z_1z_2+(c_1\cdot q+d_1i\cdot q)\cdot(c_2\cdot q+d_2i\cdot q)+(c_1\cdot q\\
&\quad+d_1i\cdot q)\cdot(a_2+b_2i)+z_1w_2\cdot q\\
&= z_1z_2+c_1\cdot q\cdot c_2\cdot q+d_1i\cdot q\cdot c_2\cdot q+c_1\cdot q\cdot d_2i\cdot q\\
&\quad+d_1i\cdot q\cdot d_2i\cdot q+c_1\cdot q\cdot a_2+d_1i\cdot q\cdot a_2+c_1\cdot q\cdot b_2i\\
&\quad+d_1i\cdot q\cdot b_2i+z_1w_2q\\
&= z_1z_2+c_1c_2\cdot q^2+d_1c_2i\cdot q^2+c_1d_2\cdot q\cdot i\cdot q\\
&\quad+d_1d_2\cdot i\cdot q\cdot i\cdot q+c_1a_2\cdot q+d_1a_2i\cdot q+c_1b_2q\cdot i\\
&\quad+d_1b_2i\cdot q\cdot i+z_1w_2q\\
&= z_1z_2-c_1c_2-d_1c_2i+c_1d_2\cdot q\cdot i\cdot q+d_1d_2\cdot i\cdot q\cdot i\cdot q\\
&\quad+c_1a_2\cdot q+d_1a_2i\cdot q+c_1b_2q\cdot i+d_1b_2i\cdot q\cdot i+z_1w_2q
\end{aligned}$$

e

$$\begin{aligned}
\phi_q((z_1,w_1)\odot(z_2,w_2)) &= \phi_q((z_1z_2-w_1\overline{w_2},z_1w_2+w_1\overline{z_2}))\\
&= (z_1z_2-w_1\overline{w_2})+(z_1w_2+w_1\overline{z_2})\cdot q\\
&= z_1z_2-[(c_1c_2+d_1d_2)+(d_1c_2-c_1d_2)i]+[(c_1a_2+d_1b_2)\\
&\quad+(d_1a_2-c_1b_2)i]\cdot q+z_1w_2q\\
&= z_1z_2-c_1c_2-d_1c_2i+c_1d_2i-d_1d_2+c_1a_2q+d_1a_2i\cdot q\\
&\quad-c_1b_2i\cdot q+d_1b_2\cdot q+z_1w_2q.
\end{aligned}$$

A fim de termos,

$$\phi_q((z_1,w_1))\cdot\phi_q((z_2,w_2))=\phi_q((z_1,w_1)\odot(z_2,w_2)),$$

é necessário e suficiente que,

$$c_1d_2i-d_1d_2-c_1b_2i\cdot q+d_1d_2q=c_1d_2q\cdot i\cdot q+d_1d_2i\cdot q\cdot i\cdot q+c_1b_2q\cdot i+d_1b_2i\cdot q\cdot i.$$

Fazendo $q=j$, temos

$$\begin{aligned}
c_1d_2q\cdot i\cdot q &= c_1d_2j\cdot i\cdot j=c_1d_2(-k)\cdot j=c_1d_2i\\
d_1d_2i\cdot q\cdot i\cdot q &= d_1d_2i\cdot j\cdot i\cdot j=d_1d_2k\cdot k=-d_1d_2\\
c_1b_2q\cdot i &= c_1b_2(-k)=-c_1b_2iq\\
d_1b_2i\cdot q\cdot i &= d_1b_2i\cdot j\cdot i=d_1b_2k\cdot i=d_1b_2j.
\end{aligned}$$

Assim, para $q = j$, temos que

$$\phi_q((z_1, w_1)) \cdot \phi_q((z_2, w_2)) = \phi_q((z_1, w_1) \odot (z_2, w_2)),$$

logo, neste caso, ϕ_j preserva as operações de adição e multiplicação, portanto, ϕ_j é um homomorfismo entre $\mathbb{C}^2$ e $\mathbb{H}$. Além disso, dado $p = p_0 + p_1 i + p_2 j + p_3 k \in \mathbb{H}$, tomando $z = p_0 + p_1 i, w = p_2 + p_3 i \in \mathbb{C}$, temos

$$\phi_j((z, w)) = (p_0 + p_1 i) + (p_2 + p_3 i) \cdot j = p_0 + p_1 i + p_2 j + p_3 k,$$

logo a aplicação ϕ_j é sobrejetora.

Por fim, considerando $z = a + bi, w = c + di \in \mathbb{C}$, temos que

$$\phi_j((z, w)) = 0 \Rightarrow a + bi + cj + dk = 0 \Rightarrow a = b = c = d = 0 \Rightarrow z = w = 0.$$

Assim, dados $(z_1, w_1), (z_2, w_2) \in \mathbb{C}^2$,temos que

$$\begin{array}{rcl} \phi_j((z_1, w_1)) = \phi_j((z_2, w_2)) & \Rightarrow & \phi_j((z_1, w_1)) - \phi_j((z_2, w_2)) = 0 \\ & \Rightarrow & \phi_j((z_1 - z_2, w_1 - w_2) = 0 \\ & \Rightarrow & (z_1, w_1) = (z_2, w_2), \end{array}$$

de onde segue que a aplicação ϕ_j é injetora.

Temos então um isomorfismo entre $\mathbb{C}^2$ e $\mathbb{H}$, que será denotado por $\mathbb{C}^2 \simeq \mathbb{H}$. O elemento $\phi_j((z, w)) = z + w \cdot j$ é um quatérnio na representação de Cayley-Dickson.

A partir de agora, dado uma quatérnio $q = q_0 + q_1 i + q_2 j + q_3 k \in \mathbb{H}$, fazendo $z = q_0 + q_1 i$, $w = q_2 + q_3 i$, podemos reescrever o quatérnio q na forma $q = z + wj$, com $z, w \in \mathbb{C}$. Logo, para os quatérnios $q = z_1 + w_1 j$ e $p = z_2 + w_2 j$, podemos reescrever as operações de adição e multiplicação de quatérnios da seguinte maneira

$$\begin{array}{rcl} q + p & = & (z_1 + w_1 j) + (z_2 + w_2 j) \\ & = & (z_1, w_1) + (z_2, w_2) \\ & = & (z_1 + z_2, w_1 + w_2) \\ & = & (z_1 + z_2) + (w_1 + w_2) j \end{array}$$

e

$$\begin{array}{rcl} q \cdot p & = & (z_1 + w_1 j) \cdot (z_2 + w_2 j) \\ & = & (z_1, w_1) \odot (z_2, w_2) \\ & = & (z_1 z_2 - w_1 \overline{w_2}, z_1 w_2 + w_1 \overline{z_2}) \\ & = & (z_1 z_2 - w_1 \overline{w_2}) + (z_1 w_2 + w_1 \overline{z_2})\, j. \end{array}$$

Ou seja,

$$(z_1 + w_1 j) + (z_2 + w_2 j) = (z_1 + z_2) + (w_1 + w_2) j$$

e

$$(z_1 + w_1 j) \cdot (z_2 + w_2 j) = (z_1 z_2 - w_1 \overline{w_2}) + (z_1 w_2 + w_1 \overline{z_2})\, j.$$

Vejamos agora como relacionar quatérnios e matrizes quadradas de ordem dois com entradas no anel dos números complexos.

Considere o subconjunto $M_2^{\mathbb{H}}(\mathbb{C})$ das matrizes $M_2(\mathbb{C})$, definido por

$$M_2^{\mathbb{H}}(\mathbb{C}) = \left\{ \begin{bmatrix} z & w \\ -\overline{w} & \overline{z} \end{bmatrix} \; ; \; z, w \in \mathbb{C} \right\}.$$

Seja ψ uma aplicação de $\mathbb{H}$ em $M_2^{\mathbb{H}}$, definida por

$$z + wj \longmapsto \psi(z + wj) = \begin{bmatrix} z & w \\ -\overline{w} & \overline{z} \end{bmatrix}.$$

Dadas as matrizes

$$\begin{bmatrix} z_1 & w_1 \\ -\overline{w_1} & \overline{z_1} \end{bmatrix}, \begin{bmatrix} z_2 & w_2 \\ -\overline{w_2} & \overline{z_2} \end{bmatrix} \in M_2^{\mathbb{H}}(\mathbb{C}),$$

temos que,

$$\begin{bmatrix} z_1 & w_1 \\ -\overline{w_1} & \overline{z_1} \end{bmatrix} - \begin{bmatrix} z_2 & w_2 \\ -\overline{w_2} & \overline{z_2} \end{bmatrix} = \begin{bmatrix} z_1 - z_2 & w_1 - w_2 \\ -(\overline{w_1 - w_2}) & \overline{z_1 - z_2} \end{bmatrix} \in M_2^{\mathbb{H}}(\mathbb{C}),$$

e

$$\begin{bmatrix} z_1 & w_1 \\ -\overline{w_1} & \overline{z_1} \end{bmatrix} \cdot \begin{bmatrix} z_2 & w_2 \\ -\overline{w_2} & \overline{z_2} \end{bmatrix} = \begin{bmatrix} z_1 z_2 - w_1 \overline{w_2} & z_1 w_2 + w_1 \overline{z_2} \\ -(\overline{z_1 w_2 + w_1 \overline{z_2}}) & \overline{z_1 z_2 - w_1 \overline{w_2}} \end{bmatrix} \in M_2^{\mathbb{H}}(\mathbb{C}).$$

Portanto, $M_2^{\mathbb{H}}(\mathbb{C})$ é um subanel de $M_2(\mathbb{C})$.

Sejam $z_1 + w_1 j, z_2 + w_2 j \in \mathbb{H}$, dois quatérnios na representação de Cayley-Dickson, temos que

$$\begin{aligned} \psi(z_1 + w_1 j) + \psi(z_2 + w_2 j) &= \begin{bmatrix} z_1 & w_1 \\ -\overline{w_1} & \overline{z_1} \end{bmatrix} + \begin{bmatrix} z_2 & w_2 \\ -\overline{w_2} & \overline{z_2} \end{bmatrix} \\ &= \begin{bmatrix} z_1 + z_2 & w_1 + w_2 \\ -(\overline{w_1 + w_2}) & \overline{z_1 + z_2} \end{bmatrix} \\ &= \psi((z_1 + z_2) + (w_1 + w_2) j) \\ &= \psi((z_1 + w_1 j) + (z_2 + w_2 j)) \end{aligned}$$

e

$$\begin{aligned}
\psi(z_1 + w_1 j) \cdot \psi(z_2 + w_2 j) &= \begin{bmatrix} z_1 & w_1 \\ -\overline{w_1} & \overline{z_1} \end{bmatrix} \cdot \begin{bmatrix} z_2 & w_2 \\ -\overline{w_2} & \overline{z_2} \end{bmatrix} \\
&= \begin{bmatrix} z_1 z_2 - w_1 \overline{w_2} & z_1 w_2 + w_1 \overline{z_2} \\ -(\overline{z_1 w_2 + w_1 \overline{z_2}}) & \overline{z_1 z_2 - w_1 \overline{w_2}} \end{bmatrix} \\
&= \psi((z_1 z_2 - w_1 \overline{w_2}) + (z_1 w_2 + w_1 \overline{z_2}) j) \\
&= \psi((z_1 + w_1 j) \cdot (z_2 + w_2 j)).
\end{aligned}$$

Além disso, dada uma matriz

$$M = \begin{bmatrix} z & w \\ -\overline{w} & \overline{z} \end{bmatrix} \in M_2^{\mathbb{H}}(\mathbb{C}),$$

fazendo $q = z + wj \in \mathbb{H}$, temos que $\psi((z + wj)) = M$. E mais,

$$\psi((z + wj)) = 0 \Rightarrow \begin{bmatrix} z & w \\ -\overline{w} & \overline{z} \end{bmatrix} = 0 \Rightarrow z = w = 0 \Rightarrow q = 0.$$

Portanto, ψ é um isomorfismo entre $\mathbb{H}$ e $M_2^{\mathbb{H}}(\mathbb{C})$. Assim, um quatérnio $q = z + wj$, pode ser representado por sua matriz associada $Q = \psi(q) \in M_2^{\mathbb{H}}(\mathbb{C})$.

O anel $M_2^{\mathbb{H}}(\mathbb{C})$ goza de propriedades semelhantes ao conjunto dos quatérnios $\mathbb{H}$. Veremos a seguir mais algumas relações entres os quatérnios e as matrizes $M \in M_2^{\mathbb{H}}(\mathbb{C})$.

Proposição 4.6. *Seja $Q \in M_2^{\mathbb{H}}(\mathbb{C})$ a matriz associada ao quatérnio $q = q_0 + q_1 i + q_2 j + q_3 k \in \mathbb{H}$. Então, $\|q\|^2 = det(Q)$.*

Demonstração. De fato.

$$\begin{aligned}
\begin{vmatrix} q_0 + q_1 i & q_2 + q_3 i \\ -q_2 + q_3 i & q_0 - q_1 i \end{vmatrix} &= (q_0 + q_1 i) \cdot (q_0 - q_1 i) - (-q_2 + q_3) \cdot (q_2 + q_3 i) \\
&= {q_0}^2 + {q_1}^2 + {q_2}^2 + {q_3}^2 \\
&= \|q\|^2.
\end{aligned}$$

□

Proposição 4.7. *Seja $Q \in M_2^{\mathbb{H}}(\mathbb{C})$ a matriz associada ao quatérnio $q = q_0 + q_1 i + q_2 j + q_3 k \in \mathbb{H}$. Então, a representação matricial do quatérnio $\bar{q}$ é dada por $\overline{Q}^T$.*

Demonstração. Dado $q = q_0 + q_1 i + q_2 j + q_3 k = z + wj$, temos que $\bar{q} = q_0 - q_1 i - q_2 j - q_3 k = (q_0 - q_1 i) - (q_2 + q_3 i) j = \bar{z} - wj$.
Por outro lado, dado

$$Q = \begin{bmatrix} z & w \\ -\overline{w} & \overline{z} \end{bmatrix},$$

temos

$$\overline{Q}^T = \begin{bmatrix} \bar{z} & \overline{w} \\ -w & z \end{bmatrix}^T = \begin{bmatrix} \bar{z} & -w \\ \overline{w} & z \end{bmatrix},$$

que é exatamente a representação matricial do quatérnio $\bar{q}$. □

Corolário 4.8. *Seja $Q \in M_2^{\mathbb{H}}(\mathbb{C})$ a matriz associada ao quatérnio $q = q_0+q_1i+q_2j+q_3k \in \mathbb{H}$, tal que $\|q\|^2 \neq 0$. Então, $Q^{-1} = det(Q)^{-1} \cdot \overline{Q}^T$.*

Demonstração. Temos que,

$$\begin{aligned} Q \cdot \left(\det(Q)^{-1} \cdot \overline{Q}^T\right) &= \det(Q)^{-1} \cdot Q \cdot \overline{Q}^T \\ &= \det(Q)^{-1} \cdot \begin{bmatrix} z & w \\ -\overline{w} & \overline{z} \end{bmatrix} \cdot \begin{bmatrix} \bar{z} & -w \\ \overline{w} & z \end{bmatrix} \\ &= \det(Q)^{-1} \cdot \begin{bmatrix} z\bar{z} + w\overline{w} & -zw + wz \\ -\overline{w}\bar{z} + \bar{z}\overline{w} & \overline{w}w + \bar{z}z \end{bmatrix} \\ &= \det(Q)^{-1} \cdot \begin{bmatrix} \|z\|^2 + \|w\|^2 & 0 \\ 0 & \|z\|^2 + \|w\|^2 \end{bmatrix} \\ &= \det(Q)^{-1} \cdot \begin{bmatrix} \|q\|^2 & 0 \\ 0 & \|q\|^2 \end{bmatrix} \\ &= \det(Q)^{-1} \cdot \begin{bmatrix} \det(Q) & 0 \\ 0 & \det(Q) \end{bmatrix} \\ &= \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}. \end{aligned}$$

Como, $Q \cdot \overline{Q}^T = \overline{Q}^T \cdot Q$, concluímos que de fato $Q^{-1} = \det(Q)^{-1} \cdot \overline{Q}^T$ □

Sabemos que $\|q\|^2 = q \cdot \overline{q} = \overline{q} \cdot q$. Então, é natural esperar que as matrizes Q e $\overline{Q}^T$ estejam de alguma forma relacionadas com a norma reduzida do quatérnio q.

Definição 4.9. (Norma de Frabenius) Seja $P \in M_2(\mathbb{C})$, definimos a norma da matriz P como sendo o número real não negativo $\|P\|^2 = \mathrm{tr}(P\overline{P}^T)$. Onde $\mathrm{tr}(P)$ representa o traço da matriz P.

Observe que para $P = \begin{bmatrix} z & w \\ u & v \end{bmatrix} \in M_2(\mathbb{C})$, temos que

$$\begin{aligned} \mathrm{tr}\left(P\overline{P}^T\right) &= \mathrm{tr}\left(\begin{bmatrix} z & w \\ u & v \end{bmatrix} \cdot \begin{bmatrix} \bar{z} & \overline{u} \\ \overline{w} & \overline{v} \end{bmatrix}\right) \\ &= \mathrm{tr}\left(\begin{bmatrix} z\bar{z} + w\overline{w} & z\overline{u} + w\overline{v} \\ u\bar{z} + v\overline{w} & u\overline{u} + v\overline{v} \end{bmatrix}\right) \\ &= z\bar{z} + w\overline{w} + u\overline{u} + v\overline{v} \\ &= \|z\|^2 + \|w\|^2 + \|u\|^2 + \|v\|^2. \end{aligned}$$

No caso em que $P \in M_2^{\mathbb{H}}(\mathbb{C})$, temos $P = \begin{bmatrix} z & w \\ -\overline{w} & \overline{z} \end{bmatrix}$, assim

$$\begin{aligned} \operatorname{tr}\left(P\overline{P}^T\right) &= \operatorname{tr}\left(\begin{bmatrix} z & w \\ -\overline{w} & \overline{z} \end{bmatrix} \cdot \begin{bmatrix} \overline{z} & -w \\ \overline{w} & z \end{bmatrix}\right) \\ &= \operatorname{tr}\left(\begin{bmatrix} z\overline{z} + w\overline{w} & -zw + wz \\ -\overline{w}\overline{z} + \overline{z}\overline{w} & w\overline{w} + z\overline{z} \end{bmatrix}\right) \\ &= z\overline{z} + w\overline{w} + w\overline{w} + z\overline{z} \\ &= \|z\|^2 + \|w\|^2 + \|w\|^2 + \|z\|^2 \\ &= 2\left(\|z\|^2 + \|w\|^2\right) \\ &= 2\|p\|^2, \end{aligned}$$

onde, $p = z + wi \in \mathbb{H}$.

Portando, dado um quatérnio $q \in \mathbb{H}$ e sua matriz associada $Q \in M_2^{\mathbb{H}}(\mathbb{C})$, temos que

$$2\|q\|^2 = \|Q\|^2 = \operatorname{tr}(Q\overline{Q}^T).$$

Encerraremos esta seção com a proposição abaixo que justifica a escolha das redundância adicionadas nas palavras códigos para o esquema de Alamouti, que será apresentado na Seção 4.3.

Proposição 4.10. *Sejam u, v, r e s números complexos, com $\|r\|^2 + \|s\|^2 \neq 0$. Então, existe um único par de números complexos (z_0, w_0) que satisfaz a equação matricial*

$$\begin{bmatrix} u & v \end{bmatrix} = \begin{bmatrix} r & s \end{bmatrix} \cdot \begin{bmatrix} z & w \\ -\overline{w} & \overline{z} \end{bmatrix}.$$

Demonstração. Dada a equação matricial

$$\begin{bmatrix} u & v \end{bmatrix} = \begin{bmatrix} r & s \end{bmatrix} \cdot \begin{bmatrix} z & w \\ -\overline{w} & \overline{z} \end{bmatrix},$$

temos o seguinte sistema associado a esta equação

$$\begin{cases} u &= rz - s\overline{w} \\ v &= rw + s\overline{z} \end{cases},$$

que é equivalente ao sistema,

$$\begin{cases} u &= rz - s\overline{w} \\ \overline{v} &= \overline{s}z + \overline{r}w \end{cases},$$

que por sua vez esta associado a equação matricial

$$\begin{bmatrix} u \\ \overline{v} \end{bmatrix} = \begin{bmatrix} r & -s \\ \overline{s} & \overline{r} \end{bmatrix} \cdot \begin{bmatrix} z \\ \overline{w} \end{bmatrix}.$$

E note que,

$$\begin{aligned}
\begin{bmatrix} u \\ \overline{v} \end{bmatrix} = \begin{bmatrix} r & -s \\ \overline{s} & \overline{r} \end{bmatrix} \cdot \begin{bmatrix} z \\ \overline{w} \end{bmatrix} \quad &\Leftrightarrow \quad \begin{bmatrix} \overline{r} & s \\ -\overline{s} & r \end{bmatrix} \cdot \begin{bmatrix} u \\ \overline{v} \end{bmatrix} = \begin{bmatrix} \overline{r} & s \\ -\overline{s} & r \end{bmatrix} \cdot \begin{bmatrix} r & -s \\ \overline{s} & \overline{r} \end{bmatrix} \cdot \begin{bmatrix} z \\ \overline{w} \end{bmatrix} \\
&\Leftrightarrow \quad \begin{bmatrix} \overline{r}u + s\overline{v} \\ -\overline{s}u + r\overline{v} \end{bmatrix} = \begin{bmatrix} \overline{r}r + s\overline{s} & -\overline{r}s + s\overline{r} \\ -\overline{s}r + r\overline{s} & \overline{s}s + r\overline{r} \end{bmatrix} \cdot \begin{bmatrix} z \\ \overline{w} \end{bmatrix} \\
&\Leftrightarrow \quad \begin{bmatrix} \overline{r}u + s\overline{v} \\ -\overline{s}u + r\overline{v} \end{bmatrix} = \begin{bmatrix} \|r\|^2 + \|s\|^2 & 0 \\ 0 & \|r\|^2 + \|s\|^2 \end{bmatrix} \cdot \begin{bmatrix} z \\ \overline{w} \end{bmatrix} \\
&\Leftrightarrow \quad \begin{bmatrix} \overline{r}u + s\overline{v} \\ -\overline{s}u + r\overline{v} \end{bmatrix} = \left(\|r\|^2 + \|s\|^2\right) \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} \cdot \begin{bmatrix} z \\ \overline{w} \end{bmatrix} \\
&\Leftrightarrow \quad \frac{1}{\|r\|^2 + \|s\|^2} \begin{bmatrix} \overline{r}u + s\overline{v} \\ -\overline{s}u + r\overline{v} \end{bmatrix} = \begin{bmatrix} z \\ \overline{w} \end{bmatrix}.
\end{aligned}$$

De onde segue que o par ordenado (z_0, w_0) é dado por,

$$z_0 = \frac{\overline{r}u + s\overline{v}}{\|r\|^2 + \|s\|^2} \quad \text{e} \quad w_0 = \frac{-s\overline{u} + \overline{r}v}{\|r\|^2 + \|s\|^2}.$$

□

4.3 Código de Alamouti

Nesse exato momento, provavelmente algum aparelho eletrônico (computador, celular, televisor) da sua casa acaba de receber um pulso causado por uma onda eletromagnética carregando algum tipo de informação. Este tipo de comunicação teve seu início no século XIX com as descobertas de James Clerk Maxwell e Heinrich Hertz sobre campos eletromagnéticos e com a criação de estações de rádio feitas por Guglielmo Marconi e Ferdinand Braun de formas independentes. No mesmo período, houve também algumas contribuições do físico Nikola Tesla. Atualmente, com o avanço da tecnologia de comunicação sem fio e com a criação de aparelhos móveis, existe uma grande demanda para o uso das ondas de rádio, que trata-se de uma pequena faixa de todas as ondas disponíveis, no entanto, a banda utilizável deste espectro é limitada. Desta maneira, se faz necessário realizar estudos e desenvolver novos métodos de modulação a fim de fazer um melhor uso destas ondas, aumentando o volume e a qualidade dos dados transmitidos. Uma forma de melhorar a qualidade da transmissão de dados é utilizar sistemas com múltiplas antenas de transmissão e múltiplas antenas de recepção de sinal, porém, esses sistemas necessitam de

mais energia que os sistemas convencionais, de modo que existe uma limitação no número de antenas de recepção. Existem três tipos de configuração de sistemas com múltiplas antenas, a saber, os sistemas Single Input Multiple Output (SIMO) que usa uma antena de transmissão e múltiplas antenas de recepção, os sistemas Multiple Input Single Output (MISO) com múltiplas antenas de transmissão e uma de recepção e os sistemas Multiple Input Multiple Output (MIMO) que opera com múltiplas antenas de transmissão e múltiplas antenas de recepção.

Um grande problema da comunicação sem fio é o desvanecimento multipercurso variável com o tempo. Quando informações são transmitidas via cabos, estas viajam em um mesmo caminho, no entanto, no caso da transmissão sem fio, um mesmo sinal pode percorrer caminhos diferentes devido aos obstáculos (casas, montanhas, vegetação), e muitas vezes estes sinais podem ser duplicados ou enfraquecidos por difrações e refrações das ondas portadoras. Um exemplo claro deste tipo de desvanecimento é o som da sirene de uma ambulância, conhecido como efeito Doppler. Quando o transmissor (sirene) ou o receptor (ouvido) viajam em alta velocidade, é possível perceber uma alteração no som que chega até nossos ouvidos, isto porque a frequência percebida pode aumentar ou diminuir a depender do sentido do movimento. Neste caso temos um desvanecimento em larga escala. Uma outra situação que pode ocorrer é uma alteração no som que escutamos da sirene a depender da posição em que estamos e dos obstáculos que estão entre o transmissor e o receptor, neste caso ocorre uma degradação do sinal e temos uma desvanecimento de baixa escala.

Uma maneira de amenizar o enfraquecimento do sinal em um canal sem fio é aumentar a potência na transmissão e distribuir amplificadores ao longo dos caminhos que a portadora percorrerá, mas isso demanda um custo muito alto e muitas vezes não é viável devido ao tamanho dos amplificadores. Uma outra solução possível é receber algum tipo de feedback do destinatário em relação a qualidade do sinal recebido, mas neste caso não teríamos a velocidade de comunicação que temos nos dias atuais, pois este processo demanda mais tempo e consequentemente atraso na transmissão de uma informação.

No final da década de 1990 com a padronização do Wi-fi e com a grande demanda por meios de comunicação sem fio com um baixo custo para o mercado, o engenheiro Siavash Alamouti publicou o trabalho intitulado “A simple transmit diversity technique for wireless communications” [1], no qual foi apresentado um esquema com duas antenas de transmissão e N antenas de recepção. Esta técnica apresenta baixa complexidade computacional e não necessitava de feedback do receptor para o transmissor. Neste trabalho nos limitaremos apenas a uma breve apresentação do Código de Alamouti com duas antenas de transmissão e duas antenas de recepção.

O Código de Alamouti foi apresentado em 1998 com o intuito de atender as demandas do mercado sem a necessidade de reprojetar totalmente os sistemas já existentes. Este

código apresenta diversidade de espaço e de tempo, isto é, as antenas são separadas por uma determinada distância e os sinais são enviados em dois instantes de tempos diferentes. Assim, o sinal e uma redundância relacionada a este sinal são transmitidos por antenas diferentes e em tempos diferentes, desta maneira, mesmo que aconteça algum problema com uma das antenas em um determinado instantes de tempo, uma cópia ou pelo menos algo relacionado com o sinal original será enviado pela outra antena. Além disso, o esquema de Alamouti utiliza símbolos pilotos, isto é, símbolos previamente determinados que são transmitidos periodicamente junto com os sinais, desta maneira, ao receber estes símbolos o decodificador terá uma estimativa do desvanecimento ocorrido durante a transmissão dos demais sinais naquele período de tempo e poderá determinar os coeficientes de desvanecimento que serão utilizados para recuperar os sinais desbotados.

Considerando um esquema com duas antenas de transmissão (T_1 e T_2) e duas antenas de recepção (R_1 e R_2), temos que no tempo t, a primeira e a segunda antenas enviam, respectivamente, os sinais z_{1t} e z_{2t}. Esses sinais chegarão até as duas antenas de recepção por meio de diferentes caminhos. Cada uma dessas antenas receberão o sinal da antena T_1 e da antena T_2 acrescidos de um ruído. Desta maneira, temos que os sinais v_{1t} e v_{2t} recebidos pelas antenas R_1 e R_2, respectivamente, são

$$\begin{aligned} v_{1t} &= h_{11}z_{1t} + h_{12}z_{2t} + n_{1t} \\ v_{2t} &= h_{21}z_{1t} + h_{22}z_{2t} + n_{2t}, \end{aligned}$$

onde h_{ji} é o coeficiente de desvanecimento da antena de transmissão T_i para a antena de recepção R_j, e n_{jt} denota o ruído na R_j antena receptora no tempo t. É natural supor que existe um intervalo de tempo no qual o canal seja coerente, isto é, os coeficientes h_{ji} permanecem constantes. Existem outros trabalhos que tratam do caso em que o canal não é coerente.

Para estudar o Código de Alamouti vamos supor que seja feita uma transmissão no tempo t_1 e outra no tempo t_2 dentro do intervalo de coerência do canal. Assim, nos tempos t_1 e t_2 a antena T_1 transmite, respectivamente, os sinais z_{11}, z_{12} e T_2 transmite z_{21}, z_{22}, conforme ilustrado na Figura 4.1.
Nesse caso a antena R_1 recebe, respectivamente, os sinais

$$\begin{aligned} v_{11} &= h_{11}z_{11} + h_{12}z_{21} + n_{11} \\ v_{12} &= h_{11}z_{12} + h_{12}z_{22} + n_{12}. \end{aligned}$$

E de modo semelhante, a antena R_2 recebe os sinais

$$\begin{aligned} v_{21} &= h_{21}z_{11} + h_{22}z_{21} + n_{21} \\ v_{22} &= h_{21}z_{12} + h_{22}z_{22} + n_{22}. \end{aligned}$$

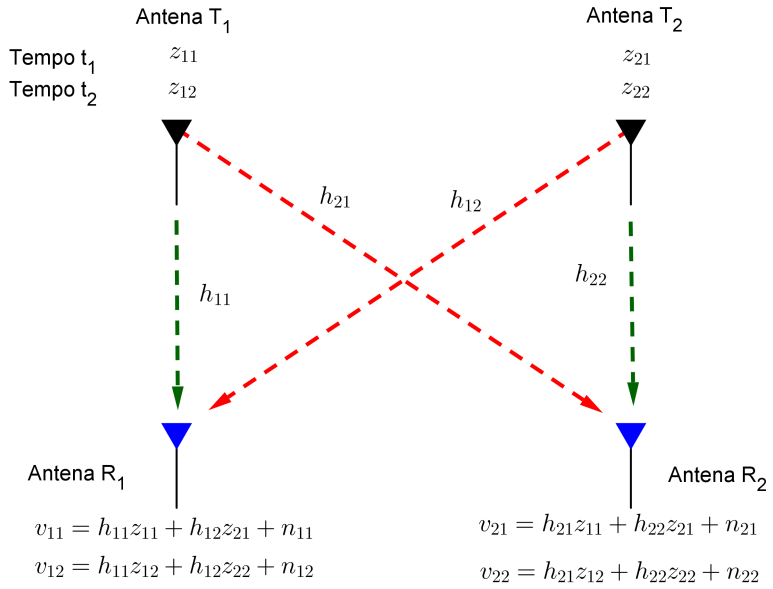

Figura 4.1: Transmissão sistema MIMO 2×2.

Podemos escrever os sinais recebidos pelas antenas R_1 e R_2 por meio da equação matricial

$$\begin{bmatrix} v_{11} & v_{12} \\ v_{21} & v_{22} \end{bmatrix} = \begin{bmatrix} h_{11} & h_{12} \\ h_{21} & h_{22} \end{bmatrix} \begin{bmatrix} z_{11} & z_{12} \\ z_{21} & z_{22} \end{bmatrix} + \begin{bmatrix} n_{11} & n_{12} \\ n_{21} & n_{22} \end{bmatrix}.$$

Veja que neste caso podemos enviar 4 sinais de informação em uma única transmissão, no entanto, diferente do esquema de Alamouti, caso ocorra algum problema em uma das antenas ou na portadora, o sinal será comprometido e não teremos condição de fazer a recuperação do mesmo. Portanto, é necessário adicionar redundâncias para ter a capacidade de recuperação de sinais.

Observe que cada antena R_i recebe no tempo t_1 dois sinais enviados de antenas diferentes e o mesmo acontece no tempo t_2. Para analisar como adicionar redundâncias, vamos fixar apenas a antena R_1 (caso 2×1 de Alamouti), assim, os sinais recebidos são dados por

$$\begin{bmatrix} v_{11} & v_{12} \end{bmatrix} = \begin{bmatrix} h_{11} & h_{12} \end{bmatrix} \begin{bmatrix} z_{11} & z_{12} \\ z_{21} & z_{22} \end{bmatrix} + \begin{bmatrix} n_{11} & n_{12} \end{bmatrix}.$$

Exemplo 4.11. Uma maneira de acrescentar redundância é repetir os sinais, ou seja, poderíamos enviar os sinais z e w no tempo t_1 e no tempo t_2 enviar os mesmos sinais apenas alterando as antenas. Este caso não funciona. Vamos supor que em determinado momento os coeficientes de desvanecimento do canal sejam $h_{11} = 1 + 0i$, $h_{12} = -1 + 0i$ e

que $n_{11} = n_{12} = 0 + 0i$. Desta maneira, os sinais recebidos são dados por

$$\begin{bmatrix} v_{11} & v_{12} \end{bmatrix} = \begin{bmatrix} 1+0i & -1+0i \end{bmatrix} \begin{bmatrix} z & w \\ w & z \end{bmatrix},$$

ou seja,

$$\begin{cases} v_{11} &= z - w \\ v_{12} &= w - z \end{cases}.$$

Mas note que,

$$\begin{cases} v_{11} &= z - w \\ v_{12} &= w - z \end{cases} \Rightarrow \begin{cases} v_{11} &= z - w \\ -v_{12} &= z - w \end{cases}.$$

E nesse caso, $v_{11} = -v_{12}$ e existem infinitos pares de números complexos (z_0, w_0) satisfazendo o sistema. Assim, é impossível determinar os sinais z e w enviados.

Exemplo 4.12. O problema do Exemplo 4.11 poderia ser resolvido enviando no tempo t_2 o sinal $-w$ no lugar do sinal w. Mas, observe que em um outro momento qualquer, os coeficientes de desvanecimento poderiam ser alterados para $h_{11} = -1 + 0i$, $h_{12} = 0 - i$ permanecendo $n_{11} = n_{12} = 0 + 0i$. Assim, os sinais recebidos seriam dados por

$$\begin{bmatrix} v_{11} & v_{12} \end{bmatrix} = \begin{bmatrix} -1+0i & 0-i \end{bmatrix} \begin{bmatrix} z & w \\ -w & z \end{bmatrix},$$

ou seja,

$$\begin{cases} v_{11} &= -z + wi \\ v_{12} &= -w - zi \end{cases}.$$

Mas note que,

$$\begin{cases} v_{11} &= -z + wi \\ v_{12} &= -w - zi \end{cases} \Rightarrow \begin{cases} v_{11} &= -z + wi \\ -v_{12}i &= -z + wi \end{cases}.$$

Chegando assim ao mesmo problema do caso anterior.

A solução encontrada por Alamouti para não ter esse tipo de problema foi enviar no tempo t_1, os sinais z e w e no tempo t_2 os sinais $-\overline{w}$ e $\overline{z}$, utilizando as antenas T_1 e T_2, respectivamente. Desta maneira, os sinais recebidos são dados por

$$\begin{bmatrix} v_{11} & v_{12} \end{bmatrix} = \begin{bmatrix} h_{11} & h_{12} \end{bmatrix} \begin{bmatrix} z & w \\ -\overline{w} & \overline{z} \end{bmatrix}.$$

Assim, supondo que h_{11} e h_{12} não são ambos nulos, segue da Proposição 4.10 que é possível determinar os sinais z e w enviados. No entanto, no processo de decodificação não podemos usar as soluções encontradas na proposição devido ao ruído acrescentado aos sinais.

A codificação para o canal MIMO com duas antenas de transmissão e duas antenas de recepção, consiste em projetar um código $C \subset M_2(\mathbb{C})$ em função dos dados a serem transmitidos. Neste caso um Código de Bloco Espaço-Tempo (SBTC), pois temos uma diversidade de tempo e uma diversidade de espaço. Assim, definimos o MIMO-SBTC de Alamouti com duas antenas de transmissão e duas antenas de recepção, que denotaremos por $\mathcal{C}$, como sendo o conjunto

$$\mathcal{C} = \left\{ X = \begin{bmatrix} z & w \\ -\overline{w} & \overline{z} \end{bmatrix} \; ; \; z, w \in \mathbb{C} \right\}.$$

Veja que na primeira linha temos os sinais enviados no tempo t_1 pelas antenas T_1 e T_2, respectivamente, e na segunda linha temos redundâncias enviadas no tempo t_2.

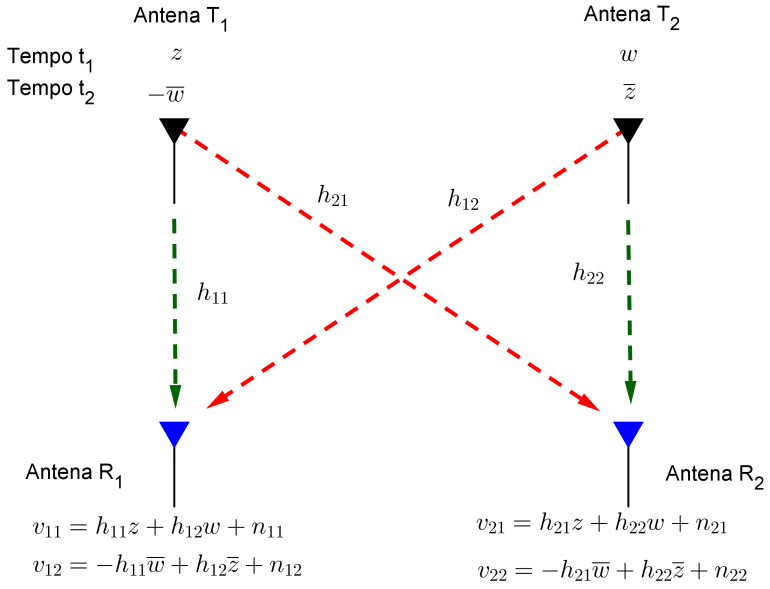

Figura 4.2: Transmissão de palavra do código $\mathcal{C}$.

Considerando agora a transmissão das palavras z e w utilizando o esquema de Alamouti, como representado na Figura 4.2, temos que os sinais recebidos, respectivamente, pelas antenas R_1 e R_2, são

$$\begin{aligned} v_{11} &= h_{11}z + h_{12}w + n_{11} \\ v_{12} &= -h_{11}\overline{w} + h_{12}\overline{z} + n_{12} \end{aligned}$$

e

$$\begin{aligned} v_{21} &= h_{21}z + h_{22}w + n_{21} \\ v_{22} &= -h_{21}\overline{w} + h_{22}\overline{z} + n_{22}. \end{aligned}$$

Ou ainda,

$$\begin{bmatrix} v_{11} & v_{12} \\ v_{21} & v_{22} \end{bmatrix} = \begin{bmatrix} h_{11} & h_{12} \\ h_{21} & h_{22} \end{bmatrix} \begin{bmatrix} z & -\overline{w} \\ w & \overline{z} \end{bmatrix} + \begin{bmatrix} n_{11} & n_{12} \\ n_{21} & n_{22} \end{bmatrix}.$$

Observe que cada matriz X do código $\mathcal{C}$ carrega dois sinais de informação escolhidos previamente.

Neste trabalho, apenas como ilustração, vamos considerar a modulação por amplitude e quadratura (QAM) e a constelação 16-QAM com a codificação ilustrada na Figura 4.3, neste caso temos 4 bits por símbolo. Constelações M-QAM: são números complexos polares representados num plano bidimensional de acordo com sua amplitude/ângulo. Note que estes símbolos foram distribuídos na constelação de modo que um ponto e seu vizinho difere de apenas um bit, no geral, para constelações QAM, os símbolos são assim distribuídos. Observe também que neste caso, dois símbolos que estão sobre uma mesma linha vertical têm sempre os mesmos dois bits iniciais iguais, e o mesmo acorre para os bits finais de símbolos sobre uma mesma reta horizontal.

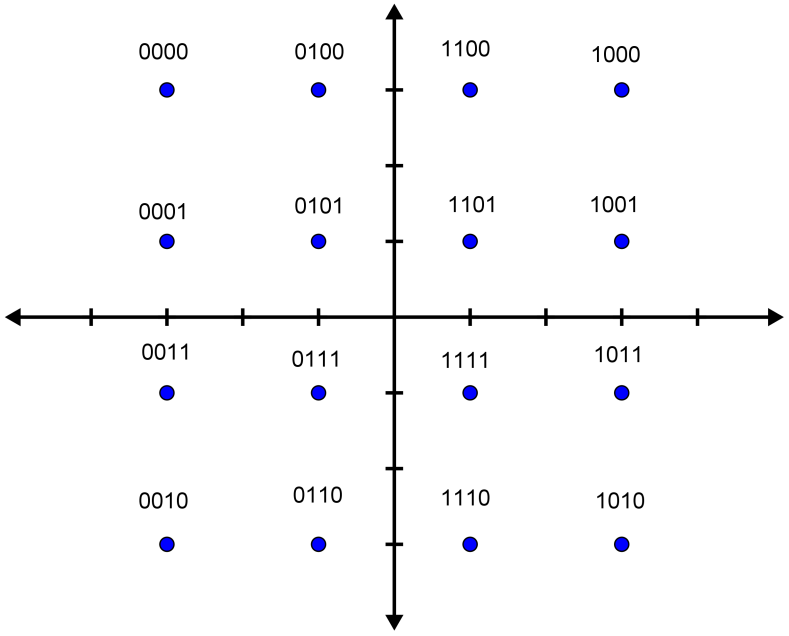

Figura 4.3: Constelação 16-QAM

A modulação QAM é feita alterando a fase e amplitude da onda e o sinal $s(t)$ enviado é uma combinação de dois sinais ortogonais, dado por

$$s(t) = S_I \cos(\omega t) + S_Q \text{sen}(\omega t).$$

Onde S_I e S_Q são as amplitudes dos sinais $S_I \cos(\omega t)$ e $S_Q \text{sen}(\omega t)$, respectivamente. Os valores de S_I e S_Q dependem do período de repetição da onda, da distância euclidiana mínima entre dois pontos da constelação e, respectivamente, das componentes x e y do par ordenado correspondente ao símbolo da constelação que queremos enviar. Dizemos que o sinal $S_I \cos(\omega t)$ está em fase e o sinal $S_Q \text{sen}(\omega t)$ está em quadratura, ou seja, existe uma defasagem de 90° em relação a fase dos dois sinais.

Na constelação 16-QAM temos que a distância euclidiana mínima entre dois pontos é 2. Supondo que o período de repetição da portadora também seja igual a 2, temos que as amplitudes S_I e S_Q dependem apenas das coordenadas x e y da constelação. Assim, para enviar o símbolo 0111, a amplitude da onda em fase e em quadratura será $-0,25$ e a fase será 225°, e para enviar o símbolo 1100 a amplitude da onda em fase será $0,25$ e da onda em quadratura $0,75$ e a fase 67°. No caso de constelações com uma quantidade maior de pontos, os valores da amplitude e das fases de dois sinais diferentes ficam mais próximos uns dos outros dificultando assim o processo de correção.

Em geral as constelações são representadas no plano complexo, de modo que cada símbolo está associado a um número complexo $z = a+bi$. No caso da constelação 16-QAM, temos que os pontos são determinados pelo produto cartesiano do conjunto $\{-3, -1, 1, 3\}$ com ele mesmo. Neste trabalho não entraremos em detalhes de como obter estas constelações. Mas, veja que os dois bits iniciais do símbolo está associado a parte real do número complexo e o dois bits finais a parte imaginária.

Exemplo 4.13. Suponha que em determinado momento os símbolos 1100 e 0111 foram enviados para o transmissor, neste caso, o modulador de sinal recebeu os números complexos $1+3i$ e $-1-i$. E, para utilizar o esquema de Alamouti, gerou os complexos $-\overline{w} = 1-i$ e $\overline{z} = 1-3i$. Assim, no tempo t_1 as antenas T_1 e T_2, respectivamente, enviaram os sinais referentes aos números complexos $1+3i$ e $-1-i$, e logo em seguida, no tempo t_2, enviaram os sinais referentes aos complexos $-\overline{w} = 1-i$ e $\overline{z} = 1-3i$. Mas, devido ao ruído, o decodificador do canal forneceu os sinais $\widetilde{z} = 1,3+2,7i$ e $\widetilde{w} = -0,7-1,2i$.

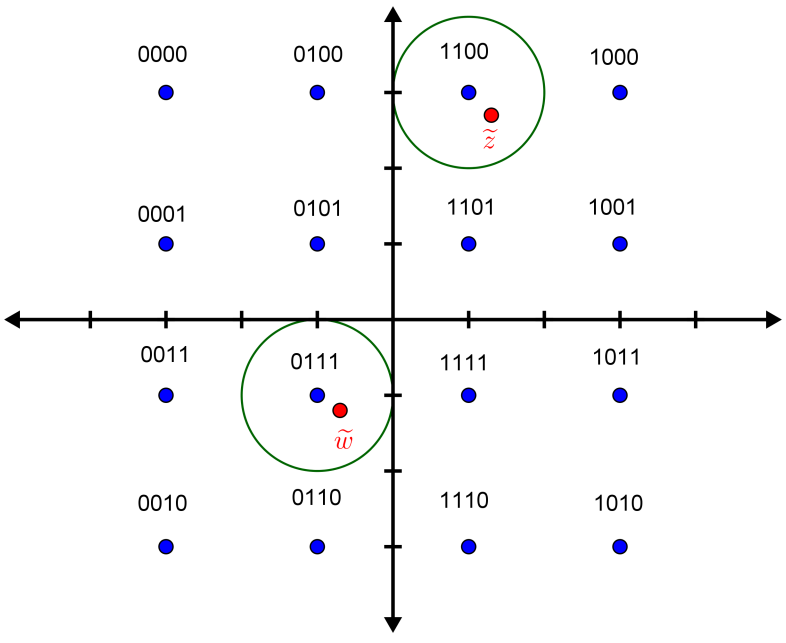

Figura 4.4: Sinais $\widetilde{z} = 1,3+2,7i$ e $\widetilde{w} = -0,7-1,2i$ fornecidos pelo decodificador.

Uma pergunta natural é como recuperar o sinal enviado? Observe que na Figura 4.4 os pontos $\widetilde{z}$ e $\widetilde{w}$ estão próximos dos pontos z e w, respectivamente. Neste caso eles estão no interior de um círculo de raio 1 centrado no sinal original. Em geral, para aumentar a probabilidade de acerto na correção de um erro desse tipo, escolhemos uma constelação cuja a distância entre dois sinais quaisquer seja maior ou igual a duas vezes o valor da variância da interferência. Desta maneira, no processo de correção podemos escolher a palavra mais próxima do sinal recebido. Como veremos a seguir, uma maneira de realizar esse processo é usando a norma de Frabenius.

Para utilizar a norma de Frabenius, em um dado momento, após receber a matriz de sinais $V = HX + N$, onde H é a matriz dos coeficientes de desvanecimento e N é a matriz dos ruídos, o decodificador precisa obter os elemento do conjunto $\mathcal{C}' = \{HX \mid X \in \mathcal{C}\}$, em seguida usar a norma para comparar a matriz V com todas as matrizes deste conjunto e por fim escolher aquela que minimiza o valor de $\|V - HX\|^2$. Este processo é conhecido como detecção por máxima verossimilhança.

Exemplo 4.14. Suponha que em um determinado momento foram transmitidos os sinais

	Antena T_1	Antena T_2
Tempo t_1	$1+3i$	$-1-i$
Tempo t_1	$1-i$	$1-3i$

do Exemplo 4.13, e que a matriz recebida foi

$$V = \begin{bmatrix} -1,9+1,8i & -1,7-6i \\ -1,9+0,3i & 1,9-4,2i \end{bmatrix}.$$

Suponha também que o estimador de canal tenha determinado

$$H = \begin{bmatrix} 1+1i & 1-i \\ 0+1i & 1-0i \end{bmatrix}.$$

Considere as matrizes

$$X_1 = \begin{bmatrix} -1+3i & -1-i \\ 1-i & -1-3i \end{bmatrix},\ X_2 = \begin{bmatrix} 1+3i & -1-i \\ 1-i & 1-3i \end{bmatrix} \text{ e } X_3 = \begin{bmatrix} 1+3i & 1-i \\ -1-i & 1-3i \end{bmatrix}.$$

Observe que,

$$\begin{aligned}
\|V - HX_1\|^2 &= \left\| \begin{bmatrix} -1,9+1,8i & -1,7-6i \\ -1,9+0,3i & 1,9-4,2i \end{bmatrix} - \begin{bmatrix} 1+1i & 1-i \\ 0+1i & 1-0i \end{bmatrix} \begin{bmatrix} -1+3i & -1-i \\ 1-i & -1-3i \end{bmatrix} \right\|^2 \\
&= \left\| \begin{bmatrix} -1,9+1,8i & -1,7-6i \\ -1,9+0,3i & 1,9-4,2i \end{bmatrix} - \begin{bmatrix} -4+0i & -4i-4 \\ -2-2i & 0-4i \end{bmatrix} \right\|^2 \\
&= \left\| \begin{bmatrix} 2,1+1,8i & 2,3-2i \\ 0,1+2,3i & 1,9-0,2i \end{bmatrix} \right\|^2 \\
&= \operatorname{tr}\left(\begin{bmatrix} 2,1+1,8i & 2,3-2i \\ 0,1+2,3i & 1,9-0,2i \end{bmatrix} \begin{bmatrix} 2,1-1,8i & 0,1-2,3i \\ 2,3+2i & 1,9+0,2i \end{bmatrix} \right) \\
&= \operatorname{tr}\left(\begin{bmatrix} 16,94 & 9.12-7,99i \\ 9,12+7,99i & 8,95 \end{bmatrix} \right) \\
&= 25,89.
\end{aligned}$$

Para X_2 temos,

$$\begin{aligned}
\|V - HX_2\|^2 &= \left\| \begin{bmatrix} -1,9+1,8i & -1,7-6i \\ -1,9+0,3i & 1,9-4,2i \end{bmatrix} - \begin{bmatrix} 1+1i & 1-i \\ 0+1i & 1-0i \end{bmatrix} \begin{bmatrix} 1+3i & -1-i \\ 1-i & 1-3i \end{bmatrix} \right\|^2 \\
&= \left\| \begin{bmatrix} -1,9+1,8i & -1,7-6i \\ -1,9+0,3i & 1,9-4,2i \end{bmatrix} - \begin{bmatrix} -2+2i & -6i-2 \\ -2 & 2-4i \end{bmatrix} \right\|^2 \\
&= \left\| \begin{bmatrix} 0,1-0,2i & 0,3+0i \\ 0,1+0,3i & -0,1-0,2i \end{bmatrix} \right\|^2 \\
&= \operatorname{tr}\left(\begin{bmatrix} 0,1-0,2i & 0,3+0i \\ 0,1+0,3i & -0,1-0,2i \end{bmatrix} \begin{bmatrix} 0,1+0,2i & 0,1-0,3i \\ 0,3+0i & -0,1+0,2i \end{bmatrix} \right) \\
&= \operatorname{tr}\left(\begin{bmatrix} 0,14 & -0,08+0,01i \\ -0,08-0,01i & 0,15 \end{bmatrix} \right) \\
&= 0,29.
\end{aligned}$$

E para X_3 segue que,

$$\begin{aligned}
\|V - HX_3\|^2 &= \left\| \begin{bmatrix} -1,9+1,8i & -1,7-6i \\ -1,9+0,3i & 1,9-4,2i \end{bmatrix} - \begin{bmatrix} 1+1i & 1-i \\ 0+1i & 1-0i \end{bmatrix} \begin{bmatrix} 1+3i & 1-i \\ -1-i & 1-3i \end{bmatrix} \right\|^2 \\
&= \left\| \begin{bmatrix} -1,9+1,8i & -1,7-6i \\ -1,9+0,3i & 1,9-4,2i \end{bmatrix} - \begin{bmatrix} -4+4i & 0-4i \\ -4+0i & 2-2i \end{bmatrix} \right\|^2 \\
&= \left\| \begin{bmatrix} 2,1-2,2i & -1,7-2i \\ 2,1+0,3i & -0,1-2,2i \end{bmatrix} \right\|^2 \\
&= \operatorname{tr}\left(\begin{bmatrix} 2,1-2,2i & -1,7-2i \\ 2,1+0,3i & -0,1-2,2i \end{bmatrix} \begin{bmatrix} 2,1+2,2i & 2,1-0,3i \\ -1,7+2i & -0,1+2,2i \end{bmatrix} \right) \\
&= \operatorname{tr}\left(\begin{bmatrix} 16,14 & 8,32-8,79i \\ 8,32+8,79i & 9,35 \end{bmatrix} \right) \\
&= 25,49.
\end{aligned}$$

É claro que podemos testar todas as matrizes HX e não encontraremos um valor menor que $0,29$ para a norma $\|V - HX\|^2$, pois, a matriz X_2 contém os sinais enviados e a taxa de erro foi pequena.

Apesar de ser eficiente, em alguns casos o processo de detecção por máxima verossimilhança demanda uma quantidade de operações inviável e um custo computacional alto. Por exemplo, neste caso temos uma total de $16^2 = 256$ matrizes no código, assim, para determinar quais foram os sinais enviados, o detector teria que fazer um total de 256 comparações. Além disso, esse número aumenta a cada vez que aumentamos a quantidade de pontos da constelação, por exemplo, no caso da constelação 256-QAM teríamos um total de $256^2 = 65536$ matrizes, portanto, o decodificador teria que realizar 65536 comparações, aumentando o consumo de energia e o tempo necessário para finalizar o processo. Assim, com o intuito de resolver o problema da quantidade de operações, seguindo as ideias de Alamouti, separamos o processo para cada um dos sinais z e w enviados.

Observe que para detectar os sinais z e w que foram enviados, podemos testar todas as combinações ordenadas (r, s) possíveis de sinais retirados da constelação 16-QAM de modo que o par (r, s) minimize o valor da expressão Δ abaixo. Assim, estaremos escolhendo, respectivamente r e s o mais próximo possível dos sinais $\widetilde{z}$ e $\widetilde{w}$ recebidos.

$$\Delta = \|v_{11} - h_{11}r - h_{12}s\|^2 + \|v_{12} + h_{11}\overline{s} - h_{12}\overline{r}\|^2 + \|v_{21} - h_{21}r - h_{22}s\|^2 + \|v_{22} + h_{21}\overline{s} - h_{22}\overline{r}\|^2 .$$

Utilizando as propriedades da norma de um número complexo, podemos expandir a

expressão acima. Note inicialmente que,

$$\begin{aligned}\|v_{11}-h_{11}r-h_{12}s\|^2 &= (v_{11}+h_{11}r-h_{12}s)(\overline{v_{11}-h_{11}r-h_{12}s})\\ &= (v_{11}-h_{11}r-h_{12}s)(\overline{v_{11}}-\overline{h_{11}}\overline{r}-\overline{h_{12}}\overline{s})\\ &= \|v_{11}\|^2+\|h_{11}\|^2\|r\|^2+\|h_{12}\|^2\|s\|^2-v_{11}\overline{h_{11}}\overline{r}-v_{11}\overline{h_{12}}\overline{s}\\ &\quad -h_{11}r\overline{v_{11}}+h_{11}r\overline{h_{12}}\overline{s}-h_{12}s\overline{v_{11}}+h_{12}s\overline{h_{11}}\overline{r},\end{aligned}$$

e

$$\begin{aligned}\|v_{12}+h_{11}\overline{s}-h_{12}\overline{r}\|^2 &= (v_{12}+h_{11}\overline{s}-h_{12}\overline{r})(\overline{v_{12}+h_{11}\overline{s}-h_{12}\overline{r}})\\ &= (v_{12}+h_{11}\overline{s}-h_{12}\overline{r})(\overline{v_{12}}+\overline{h_{11}}s-\overline{h_{12}}r)\\ &= \|v_{12}\|^2+\|h_{11}\|^2\|s\|^2+\|h_{12}\|^2\|r\|^2+v_{12}\overline{h_{11}}s-v_{12}\overline{h_{12}}r\\ &\quad +h_{11}\overline{s}\overline{v_{12}}-h_{11}\overline{s}\overline{h_{12}}r-h_{12}\overline{r}\overline{v_{12}}-h_{12}\overline{r}\overline{h_{11}}s.\end{aligned}$$

De modo análogo, temos

$$\begin{aligned}\|v_{21}-h_{21}r-h_{22}s\|^2 &= \|v_{21}\|^2+\|h_{21}\|^2\|r\|^2+\|h_{22}\|^2\|s\|^2-v_{21}\overline{h_{21}}\overline{r}-v_{21}\overline{h_{22}}\overline{s}\\ &\quad -h_{21}r\overline{v_{21}}+h_{21}r\overline{h_{22}}\overline{s}-h_{22}s\overline{v_{21}}+h_{22}s\overline{h_{21}}\overline{r},\end{aligned}$$

e

$$\begin{aligned}\|v_{22}+h_{21}\overline{s}-h_{22}\overline{r}\|^2 &= \|v_{22}\|^2+\|h_{21}\|^2\|s\|^2+\|h_{22}\|^2\|r\|^2+v_{22}\overline{h_{21}}s-v_{22}\overline{h_{22}}r\\ &\quad +h_{21}\overline{s}\overline{v_{22}}-h_{21}\overline{s}\overline{h_{22}}r-h_{22}\overline{r}\overline{v_{22}}-h_{22}\overline{r}\overline{h_{21}}s.\end{aligned}$$

Segue então que,

$$\begin{aligned}\Delta &= \|v_{11}\|^2+\|v_{12}\|^2+\|v_{21}\|^2+\|v_{22}\|^2+\|h_{12}\|^2\|s\|^2+\|h_{11}\|^2\|s\|^2+\|h_{22}\|^2\|s\|^2\\ &\quad +\|h_{21}\|^2\|s\|^2-v_{11}\overline{h_{12}}\overline{s}+h_{11}\overline{s}\overline{v_{12}}-v_{21}\overline{h_{22}}\overline{s}+h_{21}\overline{s}\overline{v_{22}}-h_{12}s\overline{v_{11}}+v_{12}\overline{h_{11}}s\\ &\quad -h_{22}s\overline{v_{21}}+v_{22}\overline{h_{21}}s-v_{11}\overline{h_{11}}\overline{r}-h_{12}\overline{r}\overline{v_{12}}-v_{21}\overline{h_{21}}\overline{r}-h_{22}\overline{r}\overline{v_{22}}-h_{11}r\overline{v_{11}}-v_{12}\overline{h_{12}}r\\ &\quad -h_{21}r\overline{v_{21}}-v_{22}\overline{h_{22}}r+\|h_{11}\|^2\|r\|^2+\|h_{12}\|^2\|r\|^2+\|h_{21}\|^2\|r\|^2+\|h_{22}\|^2\|r\|^2\\ &\quad +h_{11}r\overline{h_{12}}\overline{s}+h_{12}s\overline{h_{11}}\overline{r}-h_{11}\overline{s}\overline{h_{12}}r-h_{12}\overline{r}\overline{h_{11}}s+h_{21}r\overline{h_{22}}\overline{s}+h_{22}s\overline{h_{21}}\overline{r}-h_{21}\overline{s}\overline{h_{22}}r\\ &\quad -h_{22}\overline{r}\overline{h_{21}}s\\ &= \|v_{11}\|^2+\|v_{12}\|^2+\|v_{21}\|^2+\|v_{22}\|^2+\left(\|h_{12}\|^2+\|h_{11}\|^2+\|h_{22}\|^2+\|h_{21}\|^2\right)\|s\|^2\\ &\quad -\overline{s}\left(\overline{h_{12}}v_{11}-h_{11}\overline{v_{12}}+\overline{h_{22}}v_{21}-h_{21}\overline{v_{22}}\right)-s\left(\overline{\overline{h_{12}}v_{11}-h_{11}\overline{v_{12}}+\overline{h_{22}}v_{21}-h_{21}\overline{v_{22}}}\right)\\ &\quad -\overline{r}\left(\overline{h_{11}}v_{11}+h_{12}\overline{v_{12}}+\overline{h_{21}}v_{21}+h_{22}\overline{v_{22}}\right)-r\left(\overline{+\overline{h_{11}}v_{11}+h_{12}\overline{v_{12}}+\overline{h_{21}}v_{21}+h_{22}\overline{v_{22}}}\right)\\ &\quad +\left(\|h_{11}\|^2+\|h_{12}\|^2+\|h_{21}\|^2+\|h_{22}\|^2\right)\|r\|^2.\end{aligned}$$

Mas note que,

$$\|v_{11}\|^2+\|v_{12}\|^2+\|v_{21}\|^2+\|v_{22}\|^2,$$

não depende de r e s. Assim, para minimizar o valor de Δ, podemos minimizar simulta-

neamente os valores de Δ_s e Δ_r, onde

$$\begin{aligned}\Delta_s &= -\overline{s}\left(\overline{h_{12}}v_{11} - h_{11}\overline{v_{12}} + \overline{h_{22}}v_{21} - h_{21}\overline{v_{22}}\right) - s\left(\overline{\overline{h_{12}}v_{11} - h_{11}\overline{v_{12}} + \overline{h_{22}}v_{21} - h_{21}\overline{v_{22}}}\right)\\ &\quad + \left(\|h_{12}\|^2 + \|h_{11}\|^2 + \|h_{22}\|^2 + \|h_{21}\|^2\right)\|s\|^2,\end{aligned}$$

e

$$\begin{aligned}\Delta_r &= -\overline{r}\left(\overline{h_{11}}v_{11} + h_{12}\overline{v_{12}} + \overline{h_{21}}v_{21} + h_{22}\overline{v_{22}}\right) - r\left(\overline{\overline{h_{11}}v_{11} + h_{12}\overline{v_{12}} + \overline{h_{21}}v_{21} + h_{22}\overline{v_{22}}}\right)\\ &\quad + \left(\|h_{11}\|^2 + \|h_{12}\|^2 + \|h_{21}\|^2 + \|h_{22}\|^2\right)\|r\|^2.\end{aligned}$$

Fazendo,

$$s' = \overline{h_{12}}v_{11} - h_{11}\overline{v_{12}} + \overline{h_{22}}v_{21} - h_{21}\overline{v_{22}} \quad \text{e} \quad r' = \overline{h_{11}}v_{11} + h_{12}\overline{v_{12}} + \overline{h_{21}}v_{21} + h_{22}\overline{v_{22}},$$

temos,

$$\Delta_s = -\overline{s}s' - s\overline{s'} + \left(\|h_{12}\|^2 + \|h_{11}\|^2 + \|h_{22}\|^2 + \|h_{21}\|^2\right)\|s\|^2,$$

e

$$\Delta_r = -\overline{r}r' - r\overline{r'} + \left(\|h_{12}\|^2 + \|h_{11}\|^2 + \|h_{22}\|^2 + \|h_{21}\|^2\right)\|r\|^2.$$

Mas, observe que

$$\left\|s - s'\right\|^2 = (s - s')(\overline{s} - \overline{s'}) = s\overline{s} - s\overline{s'} - s'\overline{s} + s'\overline{s'} = \|s\|^2 + \left\|s'\right\|^2 - s\overline{s'} - s'\overline{s}.$$

Assim,

$$-s\overline{s'} - s'\overline{s} = \left\|s - s'\right\|^2 - \|s\|^2 - \left\|s'\right\|^2.$$

E, de modo análogo,

$$-r\overline{r'} - r'\overline{r} = \left\|r - r'\right\|^2 - \|r\|^2 - \left\|r'\right\|^2.$$

Temos então,

$$\Delta_s = \left\|s - s'\right\|^2 - \|s\|^2 - \left\|s'\right\|^2 + \left(\|h_{12}\|^2 + \|h_{11}\|^2 + \|h_{22}\|^2 + \|h_{21}\|^2\right)\|s\|^2,$$

e

$$\Delta_r = \left\|r - r'\right\|^2 - \|r\|^2 - \left\|r'\right\|^2 + \left(\|h_{12}\|^2 + \|h_{11}\|^2 + \|h_{22}\|^2 + \|h_{21}\|^2\right)\|r\|^2.$$

Como $\|r'\|^2$ e $\|s'\|^2$, não dependem de r e s, para minimizar o valor de Δ, podemos minimizar simultaneamente, os valores de Δ_z e Δ_w, onde

$$\Delta_z = \left\|r - r'\right\|^2 + \left(\|h_{11}\|^2 + \|h_{12}\|^2 + \|h_{21}\|^2 + \|h_{22}\|^2 - 1\right)\|r\|^2,$$

e

$$\Delta_w = \left\|s - s'\right\|^2 + \left(\|h_{11}\|^2 + \|h_{12}\|^2 + \|h_{21}\|^2 + \|h_{22}\|^2 - 1\right)\|s\|^2 .$$

Portanto, no processo de decodificação de Alamouti, o combinador gera os sinais

$$s' = \overline{h_{12}}v_{11} - h_{11}\overline{v_{12}} + \overline{h_{22}}v_{21} - h_{21}\overline{v_{22}} \quad \text{e} \quad r' = \overline{h_{11}}v_{11} + h_{12}\overline{v_{12}} + \overline{h_{21}}v_{21} + h_{22}\overline{v_{22}},$$

a partir dos sinais $v_{11},\ v_{12},\ v_{21}$ e v_{22} recebidos. Em seguida o detector de máxima verossimilhança procura na constelação os sinais r e s que minimizam os valores de Δ_z e Δ_w, respectivamente. E por fim gera as palavras associadas a cada um dos sinais r e s. Este processo é conhecido como detecção por verossimilhança.

A grande vantagem do processo de detecção por verossimilhança está na simplicidade do processo e na redução do número de operações realizadas pelo decodificador. Por exemplo, no caso da constelação 256-QAM que teríamos que fazer um total de $256^2 = 65536$ comparações, passamos a necessitar de 256 para o sinal r e 256 para o sinal s, que podem ser feitas simultaneamente. Em geral, para uma constelação 2^m-QAM, reduzimos o número de operações de m^2 para apenas $2m$. Por outro lado, observe que esse processo de correção utiliza mais fortemente os coeficientes de desvanecimento para gerar r' e s', aumentado a dependência no método em relação ao desbotamento dos sinais enviados.

Exemplo 4.15. Conside as matriz V e H do Exemplo 4.14, isto é, as matrizes

$$V = \begin{bmatrix} -1,9+1,8i & -1,7-6i \\ -1,9+0,3i & 1,9-4,2i \end{bmatrix} \quad \text{e} \quad H = \begin{bmatrix} 1+1i & 1-i \\ 0+1i & 1-0i \end{bmatrix}.$$

Neste caso, temos que

$$\begin{aligned} s' &= (1+i)(-1,92+1,8i) - (1+1i)(-1,7+6i) + (1+0i)(-1,9+0,3i) \\ &\quad -(0+1i)(1,9+4,2i) \\ &= (-3,7-0,1i) - (-7,7+4,3i) + (-1,9+0,3i) - (-4,2+1,9i) \\ &= 6,3-6i, \end{aligned}$$

e,

$$\begin{aligned} r' &= (1-i)\cdot(-1,9+1,8i) + (1-i)\cdot(-1,7+6i) + (0-i)\cdot(-1,9+0,3i) \\ &\quad + (1-0i)\cdot(1,9+4,2i) \\ &= (-0,1+3,7i) + (4,3+7,7i) + (0,3+1,9i) + (1,9+4,2i) \\ &= 6,4+17,5i. \end{aligned}$$

Para detectar os símbolos transmitidos é necessário testar cada um dos 16 símbolos. Neste caso, o detector de verossimilhança gera os valores da Tabela 4.2. Observe que ao final do processo o detector chegará a conclusão de que os sinais enviados correspondem

aos pontos $z = 1+3i$ e $w = 1-1i$, respectivamente e, portanto, os símbolos enviados foram 1100 e 1111. Desta maneira, o símbolo 1100 será enviado corretamente para o destino, no entanto, o símbolo 1111 será recebido com um erro no primeiro bit.

Este exemplo serve para mostrar que o processo de decodificação e correção por verossimilhança apresenta uma dependência dos coeficientes de desvanecimento. No próximo exemplo, veremos um caso em que o processo funciona perfeitamente. Normalmente os canais escolhidos para a transmissão de uma mensagem apresentam um tipo de desvanecimento específico, no qual o processo de correção por verossimilhança funciona com uma alta probabilidade de acerto.

Símbolo	Ponto(z)	Δ_z
0000	$-3+3i$	$388,61$
0100	$-1+3i$	$315,01$
1100	$1+3i$	**289,41**
1000	$3+3i$	$311,81$
0001	$-3+1i$	$410,61$
0101	$-1+1i$	$337,01$
1101	$1+1i$	$311,41$
1001	$3+1i$	$333,81$
0011	$-3-1i$	$480,61$
0111	$-1-1i$	$407,01$
1111	$1-1i$	$381,41$
1011	$3-1i$	$403,81$
0010	$-3-3i$	$598,61$
0110	$-1-3i$	$525,01$
1110	$1-3i$	$499,41$
1010	$3-3i$	$521,81$

Símbolo	Ponto(w)	Δ_w
0000	$-3+3i$	$257,49$
0100	$-1+3i$	$184,29$
1100	$1+3i$	$159,09$
1000	$3+3i$	$181,89$
0001	$-3+1i$	$185,49$
0101	$-1+1i$	$112,29$
1101	$1+1i$	$87,09$
1001	$3+1i$	$109,89$
0011	$-3-1i$	$161,49$
0111	$-1-1i$	$88,29$
1111	$1-1i$	**63,09**
1011	$3-1i$	$85,89$
0010	$-3-3i$	$185,49$
0110	$-1-3i$	$112,29$
1110	$1-3i$	$87,09$
1010	$3-3i$	$109,89$

Tabela 4.2: Valores gerados no teste do Exemplo 4.15.

Neste trabalho não entraremos em detalhes em relação a escolha do canal e os tipos de desvanecimento, estamos apresentando esta aplicação apenas como um convite para estudos futuros sobre códigos corretores de erros.

Exemplo 4.16. Suponha que em determinado momento os símbolos 1011 e 1111 foram enviados para o transmissor, neste caso, o modulador de sinal recebeu os números complexos $z = 3-i$ e $w = 1-i$. E, para utilizar o esquema de Alamouti, gerou os complexos $-\overline{w} = -1-i$ e $\overline{z} = 3+i$. Assim, no tempo t_1 as antenas T_1 e T_2, respectivamente, enviaram os sinais referentes aos números complexos $z = 3-i$ e $w = 1-i$, e logo em seguida, no tempo t_2, enviaram os sinais referentes aos complexos $-\overline{w} = -1-i$ e $\overline{z} = 3+i$. Além disso, suponha que

$$V = \begin{bmatrix} 1,24 + 0,076i & -0,543 - 3,206i \\ -1,9 + 0,301i & 1,112 + 2,525i \end{bmatrix} \quad \text{e} \quad H = \begin{bmatrix} 0,5 + 0,87i & -0,01 - 0,1i \\ -0,67 - 0,67 & -0,2 + 0,035i \end{bmatrix}.$$

Para detectar os símbolos transmitidos o detector de máxima verossimilhança gera os valores da Tabela 4.3. Veja que neste caso, o decodificador concluirá corretamente que os sinais enviados são referentes aos símbolos 1011 e 1111, respectivamente.

Símbolo	Ponto(z)	Δ_z
0000	$-3+3i$	125,5021
0100	$-1+3i$	84,0621
1100	$1+3i$	60,6221
1000	$3+3i$	55,1821
0001	$-3+1i$	99,7021
0101	$-1+1i$	58,2621
1101	$1+1i$	34,8221
1001	$3+1i$	29,3821
0011	$-3-1i$	91,9021
0111	$-1-1i$	50,4621
1111	$1-1i$	27,0221
1011	$3-1i$	**21,5821**
0010	$-3-3i$	102,1021
0110	$-1-3i$	60,6621
1110	$1-3i$	37,2221
1010	$3-3i$	31,7821

Símbolo	Ponto(w)	Δ_w
0000	$-3+3i$	71,505
0100	$-1+3i$	45,705
1100	$1+3i$	37,905
1000	$3+3i$	48,105
0001	$-3+1i$	45,705
0101	$-1+1i$	19,905
1101	$1+1i$	12,105
1001	$3+1i$	22,305
0011	$-3-1i$	37,905
0111	$-1-1i$	12,105
1111	$1-1i$	**4,305**
1011	$3-1i$	14,505
0010	$-3-3i$	48,105
0110	$-1-3i$	22,305
1110	$1-3i$	14,505
1010	$3-3i$	24,705

Tabela 4.3: Valores gerados no teste do Exemplo 4.16.

Capítulo 5

Proposta de Aplicação no Ensino Médio.

Neste capítulo apresentaremos uma proposta para o trabalho com códigos corretores de erros em uma turma de terceiro ano do Ensino Médio. Trata-se de uma sequências de aulas ligadas entre si, com o objetivo de apresentar e explorar os códigos corretores para introduzir vários outros conceitos da Matemática que descreveremos no decorrer do texto.

A primeira atividade trata-se de uma pequena brincadeira utilizando o WhatsApp como recurso didático e tem como objetivo fazer uma apresentação inicial sobre distância de Hamming, redundâncias e outros conceitos iniciais dos códigos corretores de erros. Na segunda atividade trabalhamos especificamente com o código de Hamming $(7, 4)$, apresentamos uma situação problema na qual os alunos devem utilizar o código $ham(7, 4)$ para codificar os comandos de um determinado robô. Na terceira e última atividade, exploramos as planilhas eletrônicas como ferramenta para fazer simulação de erros e realizar alguns procedimentos no processo de transmissão e correção das palavras no código $ham(7, 4)$, e propomos que os alunos utilizem a planilha para resolver os problemas da atividade anterior, de modo que seja possível visualizar as vantagens do uso do computador em algumas tarefas matemáticas.

5.1 Aula 1 - Corrigindo Erros

Nesta primeira aula o professor deve convidar o aluno a participar da atividade matemática. Este convite pode ser feito com uma breve apresentação sobre códigos corretores de erros semelhante ao que foi feito no Capítulo 1 deste trabalho.

- *Tema da Aula:* Corrigindo erros.
- *Conteúdo:* Códigos Corretores de Erros.

- *Competências da BNCC:* COMPETÊNCIA ESPECÍFICA 1. Utilizar estratégias, conceitos e procedimentos matemáticos para interpretar situações em diversos contextos, sejam atividades cotidianas, sejam fatos das Ciências da Natureza e Humanas, das questões socioeconômicas ou tecnológicas, divulgados por diferentes meios, de modo a contribuir para uma formação geral.

- *Habilidade da BNCC:* (EM13MAT106) Identificar situações da vida cotidiana nas quais seja necessário fazer escolhas levando-se em conta os riscos probabilísticos (usar este ou aquele método contraceptivo, optar por um tratamento médico em detrimento de outro etc.).

- *Objetivos:* Convidar o aluno a refletir sobre o uso da Matemática nos códigos corretores de erros; Conhecer os códigos corretores de erros por meio de exemplos.

- *Tempo:* 50 minutos.

- *Desenvolvimento:*

O professor deverá iniciar a aula com a brincadeira "Teclado Quebrado", que é um jogo simples, no qual cada equipe deverá corrigir erros de digitação em uma conversa no WhatsApp.

Antes de iniciar o jogo, o professor deve dividir a turma em grupos de 4 alunos. Pelo menos um membro de cada uma das equipes deve ter um smartfone com acesso a internet no qual esteja instalado o aplicativo do WhatsApp. Em seguida o educador deve criar um grupo de WhatsApp, no qual serão enviadas as mensagens, e adicionar um aluno de cada equipe. É importante que os alunos desativem o corretor ortográfico do teclado.

Na primeira rodada da disputa, o professor deverá enviar mensagens no grupo contendo um erro em alguma das palavras e as equipes deverão fazer a correção. A equipe que conseguir corrigir o erro mais rapidamente e reenviar a mensagem no grupo ganha 5 pontos. É interesse que as frases iniciais sejam de fácil correção e que gradativamente aumente a dificuldade de correção. Veja alguns exemplos de frases que o professor pode utilizar:

- O cathorro é bravo. (O cachorro é bravo);

- Comprei um helular novo. (Comprei um celular novo);

- Cortei o bolo com a maca. (Cortei o bolo com a faca);

- Tenho uma xaca leiteira. (Tenho uma vaca leiteira);

- Qual é o preço dessa kala? (Qual é o preço dessa mala);

- Na minha casa tem um xato. (Na minha casa tem um pato);

Na segunda rodada, com o intuito de deixar a correção mais difícil, o professor deve usar apenas palavras. Neste caso, cada equipe que corrigir a palavra de maneira correta ganha 10 pontos. Nesta rodada existe a possibilidade de pedir uma dica em relação a palavra, no entanto, acertos com uma dica vale apenas a metade dos pontos, ou seja, apenas 5 pontos. A dica deve ser uma outra palavra que tenha relação com a palavra que foi enviada. Esta segunda rodada é importante para que os alunos percebam que o contexto ajuda no processo de correção das palavras. Veja alguns exemplos de palavras com erros:
capendário(calendário); *coléfio* (colégio); *camepo* (camelo); *ratal* (natal); *xovo* (novo); *banata*(batata); *yala* (tala); *wola* (mola);

Na terceira rodada cada equipe deverá criar uma mensagem com no máximo um erro de digitação em cada palavra e enviar para o professor. As equipes deverão enviar também a frase corrigida. Em seguida o professor deverá enviar todas as mensagens no grupo para as equipes tentarem corrigir e reenviar. É claro que uma equipe não pode enviar a frase criada por ela mesma. Caso alguma das mensagens não seja corrigida pelas equipes, o grupo que criou a mensagem ficará com os 10 pontos da frase.

A partir das estratégias apresentadas pelos alunos para realizar o processo de correção das frases e palavras, o professor pode introduzir a ideia de redundância e e fazer uma introdução sobre os códigos corretores de erros, apresentando as dificuldades que existem no processo de transmissão de uma mensagem por meio digital e a necessidade de corrigir os erros cometidos.

Durante a discussão do problema, provavelmente os alunos vão usar em algum momento a ideia de proximidade entre duas palavras, desta maneira o professor pode apresentar a definição de métrica de Hamming e generalizar para um código qualquer. É importante que os alunos percebam que apenas a métrica de Hamming não é suficiente para realizar o processo de correção e que é necessário ter outras ferramentas. Neste momento o professor pode apresentar o código F_2^2 do robô como um outro exemplo de código no qual temos problemas com a distância entre as palavras e propor o seguinte problema:
Problema: Considere o código $\{00000,\ 01011,\ 10110,\ 11101\}$ e a codificação abaixo:

$$\begin{array}{rcrcl} \text{Leste} & \longrightarrow & 00 & \longrightarrow & 00000 \\ \text{Oeste} & \longrightarrow & 01 & \longrightarrow & 01011 \end{array} \qquad \begin{array}{rcrcl} \text{Norte} & \longrightarrow & 10 & \longrightarrow & 10110 \\ \text{Sul} & \longrightarrow & 11 & \longrightarrow & 11101. \end{array}$$

Suponha que durante a transmissão de uma mensagem para um determinado robô tenha ocorrido no máximo um erro em cada palavra. Você saberia descrever os comandos enviados para o robô que recebeu a mensagem:

$$00000\ \ 10111\ \ 11101\ \ 10000\ \ 11011\ \ 11111?$$

O professor deve explorar este problema para apresentar a necessidade de acrescentar redundâncias na palavra de um determinado código, como apresentado no Capítulo 1.

- *Materiais necessários:* Material corriqueiro do professor.
- *Avaliação:* Participação na realização das tarefas.
- *Referências:* [15], [11] e [16].

5.2 Aula 2 - Códigos de Hamming

Nesta segunda aula será necessário que os alunos tenham uma noção de base binária, neste caso, o professor pode dedicar vinte minutos da aula para fazer uma breve explanação em relação a isso. Para explicar um pouco sobre os códigos de Hamming, o professor deve utilizar o texto da Seção 2.3.

- *Tema da Aula:* Códigos de Hamming.
- *Conteúdo:* Código de Hamming $(7, 4)$.
- *Competências da BNCC:* COMPETÊNCIA ESPECÍFICA 3. Utilizar estratégias, conceitos, definições e procedimentos matemáticos para interpretar, construir modelos e resolver problemas em diversos contextos, analisando a plausibilidade dos resultados e a adequação das soluções propostas, de modo a construir argumentação consistente; COMPETÊNCIA ESPECÍFICA 4. Compreender e utilizar, com flexibilidade e precisão, diferentes registros de representação matemáticos (algébrico, geométrico, estatístico, computacional etc.), na busca de solução e comunicação de resultados de problemas.
- *Habilidades da BNCC:* (EM13MAT405) Utilizar conceitos iniciais de uma linguagem de programação na implementação de algoritmos escritos em linguagem corrente e/ou matemática.
- *Objetivos:* Conhecer os códigos de Hamming e suas aplicações; Estabelecer relações entre os códigos corretores de erros e o processo de transmissão de mensagens;
- *Tempo:* 100 minutos.
- *Desenvolvimento:*

No primeiro momento da aula o professor deve explicar o conteúdo da Seção 2.3. Após a explicação deve apresentar a seguinte situação para os alunos:

Em um determinado restaurante com 25 mesas, não existe garçom, todos os pedidos são registrados por meio do celular e um robô leva o pedido até a mesa do cliente. Para

facilitar o serviço do robô, o restaurante possui um salão em forma de quadrado, cada mesa é posicionada em um lugar fixo. Na Figura 5.1 temos uma representação da organização das mesas, onde cada quadrado do tabuleiro tem exatamente um metro de lado e cada casa verde demarca a posição de uma mesa. Por exemplo, o primeiro quadrado verde mais abaixo e mais a esquerda representa a posição da mesa $B2$.

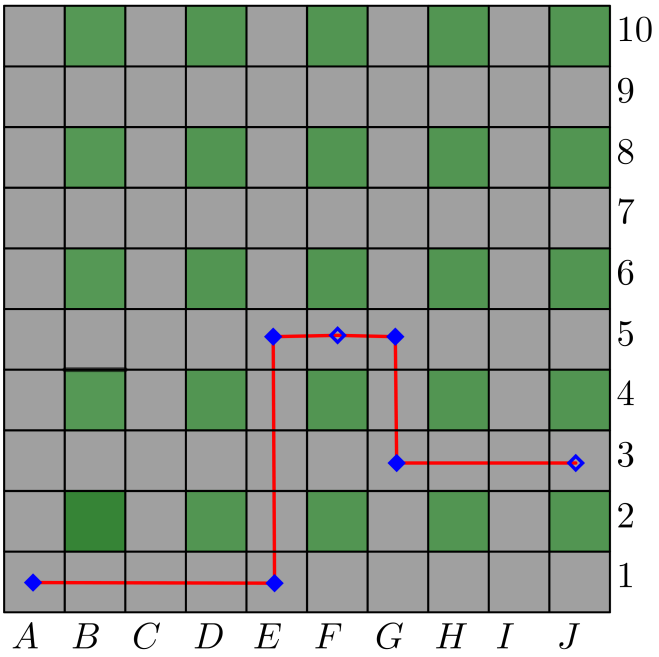

Figura 5.1: Representação do salão.

Para fazer a entrega de um pedido o robô sempre parte do centro da casa $A1$, podendo levar mais de uma pedido por vez respeitando a ordem de cada pedido, e se move de acordo com os comandos recebidos para realizar as entregas, sendo que no final sempre retorna por um dos caminhos mais curto para a posição inicial. A entrega do pedido é realizado pelo lado direito da mesa em relação aos números que aparecem no tabuleiro, isto é, sempre do lado sul. Por exemplo, no trajeto da Figura 5.1, o robô

- partiu da casa $A1$, andou quatro casas para direita, quatro casas para cima, uma casa para direita e entregou o pedido da mesa $F6$ pelo lado sul da mesa;
- andou uma casa para a direita, duas casa para baixo, três casa para direita e entregou o pedido da mesa $J4$ pelo lado sul da mesa.
- retornou para origem pelo caminho mais curto.

Seja n um número natural. Suponha que o robô obedeça aos seguintes comandos:

- $SIGA$ (para o robô andar);
- $PARE$ (para o robô parar e realizar a entrega do pedido);
- xD (para o robô andar x casas para a direita);
- xE (para o robô andar x casas para a esquerda);
- xB (para o robô andar x casas para a baixo);
- xC (para o robô andar x casas para a cima).

Assim, por exemplo, para realizar o trajeto da Figura 5.1 os comandos enviados para o robô são:

$$SIGA \quad 4 \quad D \quad 4 \quad C \quad 1 \quad D \quad PARE \quad SIGA \quad 1 \quad D \quad 2 \quad B \quad 3 \quad D \quad PARE$$

Suponha também que o robô tenha o seguinte código fonte:

COMANDOS	0	1	2	3	4	5	6	7	8	9	D	E	C	B	$SIGA$	$PARE$
	0	0	0	0	0	0	0	0	1	1	1	1	1	1	1	1
PALAVRAS	0	0	0	0	1	1	1	1	0	0	0	0	1	1	1	1
DO CÓDIGO	0	0	1	1	0	0	1	1	0	0	1	1	0	0	1	1
	0	1	0	1	0	1	0	1	0	1	0	1	0	1	0	1

Para transmitir estes comandos podemos usar o código de canal $ham(7,4)$ para o robô, ou seja, seguindo o algoritmo dos códigos de Hamming descrito na Seção 2.3, é possível acrescentar redundâncias a cada uma das palavras do código fonte do robô e obter o código de canal abaixo:

0	1	2	3	4	5	6	7	8	9	D	E	C	B	$SIGA$	$PARE$
0	1	0	1	1	0	1	0	1	0	1	0	0	1	0	1
0	1	1	0	0	1	1	0	1	0	0	1	1	0	0	1
0	0	0	0	0	0	0	0	1	1	1	1	1	1	1	1
0	1	1	0	1	0	0	1	0	1	1	0	1	0	0	1
0	0	0	0	1	1	1	1	0	0	0	0	1	1	1	1
0	0	1	1	0	0	1	1	0	0	1	1	0	0	1	1
0	1	0	1	0	1	0	1	0	1	0	1	0	1	0	1

Os alunos deverão resolver os seguintes problemas:

Problema 1: Utilizando o código de canal $ham(7,4)$, escreva uma mensagem para ser enviado ao robô que deve partir da casa $A1$ e entregar os pedidos das mesas $D8$, $J10$ e $H4$, sem retornar na origem.

Problema 2: Determine o percurso e as entregas realizadas por um robô que recebeu a seguinte mensagem sem erros:

c_1	c_2	c_3	c_4	c_5	c_6	c_7	c_8	c_9	c_{10}	c_{11}	c_{12}	c_{13}	c_{14}	c_{15}	c_{16}
0	1	1	0	0	1	1	1	0	1	1	0	0	1	1	1
0	0	0	1	1	1	0	1	0	0	0	1	1	1	0	1
1	0	1	0	1	0	1	1	1	0	1	0	1	0	1	1
0	1	1	1	1	1	1	1	0	0	1	1	1	1	1	1
1	1	0	0	1	0	0	1	1	0	0	0	1	0	0	1
1	0	1	1	0	0	1	1	1	1	1	1	0	0	1	1
0	0	0	0	0	1	0	1	0	1	0	0	0	1	0	1

Problema 3: Um robô recebeu a mensagem abaixo com no máximo um erro em cada palavra. Neste caso é possível fazer a correção e decodificar a mensagem recebida. Determine o percurso e as entregas realizadas pelo robô destacando as palavras erradas e a posição em que ocorreu o erro.

c_1	c_2	c_3	c_4	c_5	c_6	c_7	c_8	c_9	c_{10}	c_{11}	c_{12}	c_{13}	c_{14}	c_{15}	c_{16}
0	1	1	0	0	0	1	1	0	1	0	0	0	0	0	0
0	0	0	1	1	1	0	1	0	0	1	1	1	1	1	1
1	0	1	0	1	0	1	1	1	0	1	1	1	0	1	1
0	1	1	0	1	0	1	0	0	1	0	1	1	0	0	1
1	1	0	1	1	1	0	1	1	0	0	0	1	1	0	1
1	0	1	1	0	0	1	1	1	0	1	1	0	0	1	1
1	0	0	0	0	1	0	1	0	1	1	0	0	0	1	1

Problema 4: Um robô recebeu a mensagem abaixo para realizar as entregas das mesas $D4$ e $H6$, no entanto, devido algum erro de comunicação no sistema entregou um dos pedidos em uma mesa errada. Determine a mesa que recebeu o pedido errado e explique o que pode ter ocorrido para o robô ter realizado a entrega na mesa errada sem identificar o erro.

c_1	c_2	c_3	c_4	c_5	c_6	c_7	c_8	c_9	c_{10}	c_{11}	c_{12}	c_{13}	c_{14}	c_{15}	c_{16}
0	0	1	0	0	1	0	0	0	0	1	0	0	1	1	1
0	1	0	1	1	1	0	1	0	0	0	1	1	0	0	1
1	0	1	0	1	0	1	1	1	0	1	0	1	0	1	1
0	1	1	1	1	1	1	1	0	0	1	1	1	1	1	1
1	0	0	0	1	0	0	1	1	0	0	0	1	0	0	1
1	1	1	1	0	0	1	1	1	1	1	1	0	1	0	1
0	0	0	0	0	1	0	1	0	1	0	0	0	1	0	1

Problema 5: Um robô recebeu a mensagem abaixo para realizar algumas entregas, no entanto, devido algum erro de comunicação no sistema, ao sair da primeira mesa que fez a entrega e se deslocar para a segunda, acabou se chocando com uma das mesas do salão. Determine a mesa onde ocorreu o acidente e explique o que pode ter ocorrido.

c_1	c_2	c_3	c_4	c_5	c_6	c_7	c_8	c_9	c_{10}	c_{11}	c_{12}	c_{13}	c_{14}	c_{15}	c_{16}
0	0	1	1	0	1	1	1	0	1	1	0	0	1	1	1
0	1	0	0	1	1	0	1	0	1	0	1	1	1	0	1
1	0	1	0	1	0	1	1	1	0	1	0	1	0	1	1
0	1	1	1	1	1	1	1	0	1	0	1	1	1	1	1
1	0	0	1	1	0	0	1	1	1	0	0	1	0	0	1
1	1	1	0	0	0	0	1	1	0	1	1	0	0	1	1
0	0	0	0	0	1	0	1	0	0	0	0	0	0	0	1

- *Materiais necessários:* Material corriqueiro do professor.
- *Avaliação:* Atividade impressa.
- *Referências:* [15], [2] e [11]
- *Anexo:* Apêndice B.

5.3 Aula 3 - Matrizes, Planilhas e Códigos de Hamming

Este terceiro momento com os alunos tem como objetivo utilizar o computador para realizar os cálculos e as demais operações necessárias para codificar, corrigir erros e decodificar uma mensagem usando o código $ham(7,4)$. Nesta aula propomos que os alunos utilize uma máquina construída em planilha eletrônica para resolver os problemas da Seção 5.2. Os processos envolvidos na construção é necessário que os alunos tenham um conhecimento básico de lógica, planilhas, teoria de números, matrizes e geometria analítica. No Apêndice A, fazemos a descrição de como construir a máquina, mas, não indicamos que a construção e os processos envolvidos sejam trabalhados no Ensino Médio, o professor pode simplesmente disponibilizar a planilha para os alunos responder aos questionamentos. Acreditamos que esta aula, com a construção da planilha, pode ser apresentada em um minicurso sobre códigos lineares para alunos de um algum curso de Matemática que tenham cursado Teoria dos Números e Geometria Analítica .

- *Tema da Aula:* Matrizes, Planilhas e Códigos de Hamming.
- *Conteúdos:* Matrizes e Códigos de Hamming.

- *Competências da BNCC:* COMPETÊNCIA ESPECÍFICA 3. Utilizar estratégias, conceitos, definições e procedimentos matemáticos para interpretar, construir modelos e resolver problemas em diversos contextos, analisando a plausibilidade dos resultados e a adequação das soluções propostas, de modo a construir argumentação consistente; COMPETÊNCIA ESPECÍFICA 4. Compreender e utilizar, com flexibilidade e precisão, diferentes registros de representação matemáticos (algébrico, geométrico, estatístico, computacional etc.), na busca de solução e comunicação de resultados de problemas.

- *Habilidades da BNCC:* (EM13MAT405) Utilizar conceitos iniciais de uma linguagem de programação na implementação de algoritmos escritos em linguagem corrente e/ou matemática.

- *Objetivos:* Relacionar códigos de Hamming e matrizes; Usar as planilhas eletrônicas para realizar cálculos matematicos.

- *Tempo:* 100 minutos.

- *Desenvolvimento:*

Nesta aula o professor deve explicar aos alunos o funcionamento da máquina e como digitar os comandos na planilha eletrônica. Em seguida propor os problemas para que eles possam responder utilizando a planilha.

Problema 1: Usar a máquina para resolver os problemas propostos na Seção 5.2. Em seguida escrever as vantagens de utilizar o computador.

Máquina sem simulação de erros: *Clique aqui.*

Problema 2: Utilize a máquina com simulação de erros para responder de forma empírica aos seguintes questionamentos:

a) A máquina é capaz de corrigir qualquer palavra recebida com no máximo um erro?

b) Usando o código $ham(7, 4)$, no caso das palavras recebidas com até dois erros é possível saber que ocorreu erros, mas não é possível determinar a quantidade e as posições dos erros. O que pode acontecer com o robô ao receber uma palavra com exatamente dois erros?

c) O que pode acorrer com o robô ao receber uma palavra com exatamente três erros?

Observação: Para simular um novo erro basta clicar no botão enviar.

Máquina com simulação de erros: *Clique aqui.*

- *Materiais necessários:* Computador com internet e material corriqueiro do professor.

- *Avaliação:* Atividade impressa e utilização da planilha eletrônica.

- *Referências:* [15], [2] e [11]

Capítulo 6

Conclusão

Um dos grandes desafios no processo de ensino e aprendizagem é motivar os alunos para o estudo da Matemática. Boa parte dos conteúdos matemáticos trabalhados na educação básica apresentam pouca aplicabilidade no cotidiano, desta maneira, muitos alunos questionam o porquê estudar tais conteúdos. Neste trabalho apresentamos uma possibilidade para o professor trabalhar com a Matemática de maneira contextualizada com o cotidiano e, para isto, procuramos evidenciar a necessidade de ferramentas matemáticas para o desenvolvimento de novas tecnologias. Mostramos que o estudo dos códigos corretores de erros, apesar de não ser conteúdo do Ensino Médio, pode servir como motivação para o estudo de alguns conteúdos desta etapa da educação básica.

No corpo do trabalho procuramos exibir exemplos das definições e proposições apresentadas no texto, tornando assim mais fácil o entendimento dos conceitos relativos à teoria de códigos corretores de erros e possibilitando uma abordagem mais simples do conteúdo em sala de aula. Mostramos que é possível simplificar a exposição de alguns conteúdos usando uma linguagem acessível para alunos do Ensino Médio sem perder o formalismo matemático necessário para generalizar os procedimentos.

Apresentamos também uma breve introdução dos números complexos por meio de uma abordagem pouco utilizada em livros didáticos. No entanto, este conteúdo não faz parte dos conteúdos propostos pela BNCC para o Ensino Médio, mas cada instituição tem autonomia de inserir ou não o conteúdo em seu currículo. Neste trabalho mostramos que é possível aplicar os números complexos no processo de transmissão de informações, como no caso do código de Alamouti. Além disso, existem várias outras abordagens deste conteúdo que mostra a potencialidade do mesmo para modelar situações da vida contemporânea. Assim, julgamos que este conteúdo pode ser inserido em algumas turmas do Ensino Médio.

Mostramos ainda que é possível apresentar os quatérnios de Hamilton por meio de uma classe especial de matrizes com entradas complexas. E apresentamos uma aplicação direta do uso de quatérnios para a criação de um código corretor de erro. Apesar de fazer uma abordagem introdutória sobre código de Alamouti, acreditamos que a Seção 4.3 pode

servir como um convite para que alunos interessados possam aprofundar os estudos sobre códigos corretores de erros e transmissão de informações.

As atividades propostas neste trabalho servem como uma introdução aos estudos dos códigos corretores de erros em sala de aula. Procuramos introduzir recursos tecnológicos nas atividades de modo que os alunos tenham um maior interesse pelo tema e consigam visualizar na prática a utilização dos códigos corretores de erros por um computador. A máquina descrita neste trabalho permite que os alunos vejam os procedimentos realizados pelo computador para identificar e corrigir erros em uma mensagem.

Referências Bibliográficas

[1] ALAMOUTI, S. M. *Uma técnica simples de transmissão de diversidade para comunicações sem fio*. Jornal IEEE sobre áreas selecionadas em comunicações , v. 16, n. 8, pág. 1451-1458, 1998.

[2] BAHIA, F. *Um primeiro curso sobre códigos corretores de erros.* ERMAC 2010: I Encontro Regional de Matemática Aplicada e Computacional, 2010. Disponível em: <http://www.ufsj.edu.br/portal2-repositorio/File/iermac/anais/minicursos/mc8.pdf> acesso em 22 de outubro de 2021.

[3] BELFIORE, J.-C .; REKAYA, G. *Redes quaterniônicas para codificação espaço-tempo*. In: Proceedings 2003 IEEE Information Theory Workshop (Cat. No. 03EX674). IEEE, 2003. p. 267-270.

[4] BERHUY, G.; OGGIER, F. *Uma introdução às álgebras simples centrais e suas aplicações para comunicação sem fio*. American Mathematical Soc., 2013.

[5] BRASIL . *Base Nacional Comum Curricular. Ensino Médio.* Brasília: MEC. Versão final. Disponível em: http://basenacionalcomum.mec.gov.br/. Acesso em: 11 de outubro de 2021.

[6] CERRI, C.; MONTEIRO, M. S. *História dos números complexos*. CAEM-Centro de Aperfeiçoamento de Ensino de Matemática Instituto de Matemática e Estatística da USP, 2001.

[7] COELHO, F. U.; LOURENCO, M. L. *Curso de Álgebra Linear*, Um Vol. 34. [S.l.]: Edusp, 2001.

[8] DOMINGUES, H. H.; IEZZI, G. *Álgebra moderna*. reform. São Paulo: Atual, 2003.

[9] GARCIA, A. e LEQUAIN, Y. *Elementos de Álgebra* . IMPA, Rio de Janeiro, 2006. 326p.

[10] HEFEZ, A. FERNANDEZ, C. de S. *Introdução a Algebra Linear* , Rio de Janeiro: Sociedade Brasileira de Matematica, 2013. (Coleção matematica PROFMAT).

[11] HEFEZ, A.; VILLELA, M. L. T. *Códigos corretores de erros*. Instituto de Matematica Pura e Aplicada, 2008.

[12] HOLLANTI, C. et al. *Sobre a estrutura algébrica do código de prata: um código de bloco de espaço-tempo perfeito 2×2*. In: 2008 IEEE Information Theory Workshop . IEEE, 2008. p. 91-94.

[13] LIMA, E. L. *Álgebra linear*. Instituto de Matematica Pura e Aplicada, 1996.

[14] LIRA, E. H. C. de. *Códigos Corretores de Erros no Ensino Médio: um estudo sobre o Código de Hamming*. 2018. Dissertação de Mestrado. Universidade Federal Rural de Pernambuco.

[15] MILIES, C. P. *Breve introduçao a teoria dos códigos corretores de erros*. Colóquio de Matemática da Região Centro-Oeste, SBM, 2009.

[16] MILIES, C. P. *A matemática dos códigos de barras*. Artigo, USP-Departamento de Matemática, São Paulo, SP, Brasil. Recuperado em, v. 14, 2006.

[17] PINHEIRO, J. C. de M. *Caracterização de canais sem fio em ambientes generalizados de desvanecimento*. 2012.

[18] VOTO, J. *Álgebras de quaternion*. Springer Nature, 2021.

Apêndice A

Construção da Máquina

Descrevemos abaixo os passos que os alunos deverão seguir para montar a máquina capaz de simular erros de transmissão e realizar o processo de codificação, correção de erros e decodificação do código de $ham(7,4)$.

Inicialmente os alunos deverão montar a parte de geração do código. Neste caso devem seguir os seguintes passos:

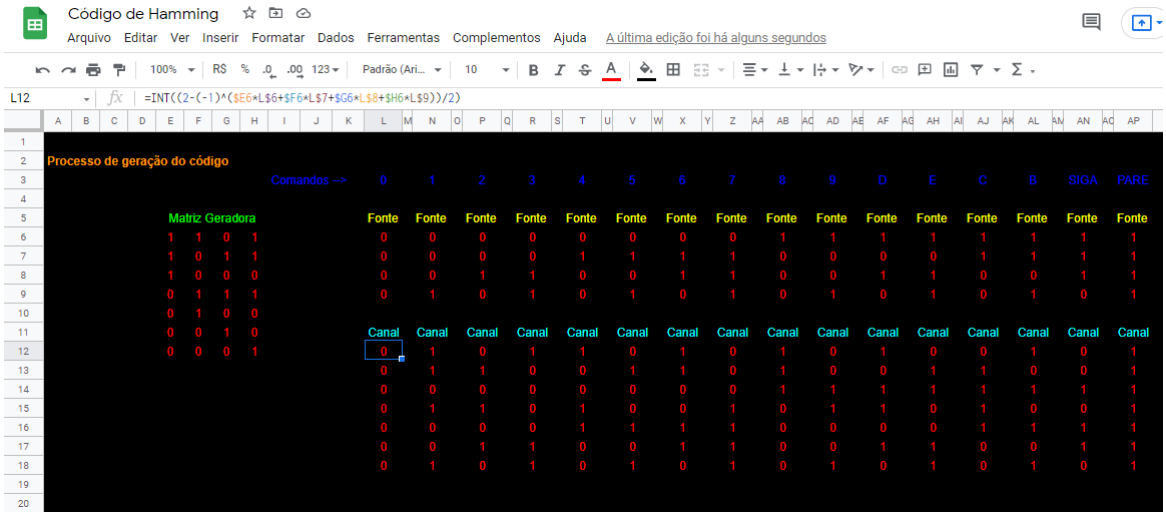

Figura A.1: Planilha: Máquina de codificação.

1º passo: Digitar a matriz $G_{7\times4}$ da Seção 2.3, que gera o código $ham(7,4)$. A primeira coluna da matriz deve iniciar na célula E6, a segunda na célula F6 e assim sucessivamente. Para identificar a matriz é possível mesclar as células E6, F6, G6 e H6 e digitar a frase: Matriz Geradora.

2º passo Na linha 3 da planilha, iniciando na célula L3 e terminando na célula AP3 e sempre saltando uma célula, digite os comandos: 0, 1, 2, $\cdots$, 8, 9, D, E, C, B, SIGA e PARE.

3º passo Na linha 5 da planilha, iniciando na célula L5 e terminando na célula AP5 e sempre saltando uma célula, digite a palavra: Fonte.

4º passo Logo abaixo de cada uma das palavras fonte digite um elemento do conjunto $F_2^4 = \{0,1\}^4$, que será uma codificação do comando correspondente que se encontra acima da palavra fonte. Sugerimos que seja usada a ordem crescente dos números na base binária.

5º passo Na linha 11 da planilha, iniciando na célula L11 e terminando na célula AP11 e sempre saltando uma célula, digite a palavra: Canal.

6º passo Na célula L12 digite a seguinte fórmula:

$$= \text{INT}((2\text{-}(\text{-}1)\hat{}\ (\$E6*L\$6+\$F6*L\$7+\$G6*L\$8+\$H6*L\$9))/2)$$

Neste caso, a expressão x_1= \$E6*L\$6+\$F6*L\$7+\$G6*L\$8+\$H6*L\$9 é referente a multiplicação entre a primeira linha da matriz geradora e a palavra do conjunto F_2^4 correspondente ao comando 1. A função INT retorna a parte inteiro do número ((2-(-1)ˆ (\$E6*L\$6+\$F6*L\$7+\$G6*L\$8+\$H6*L\$9))/2) que será 1 no caso em que x_1 é ímpar, pois neste caso temos,

$$x_1 = \frac{2-(-1)^{\text{ímpar}}}{2} = \frac{2-(-1)}{2} = \frac{2+1}{2} = \frac{3}{2} = 1,5,$$

e, 0 caso contrário, pois

$$x_1 = \frac{2-(-1)^{\text{par}}}{2} = \frac{2-1}{2} = \frac{1}{2} = 0,5.$$

6º passo Copiar a célula L12 e colar nas 6 células logo abaixo. Neste caso será codificada a primeira palavra do código.

7º passo Selecionar as células L12 até L18, copiar e colar logo abaixo de cada uma das palavras canal. Obtendo assim o código $ham(7,4)$, como mostrado na Figura A.1.

Para montar o mecanismo de codificação da mensagem a ser enviada, os alunos deverão seguir os passos abaixo:

1º passo Na linha 23 da planilha, destacar as células L23, N23, P23 e assim sucessivamente até a célula AP23. Estas células serão utilizadas para digitar a mensagem a ser enviada, sendo um comando em cada célula.

2º passo Na célula L24 digite a seguinte fórmula:

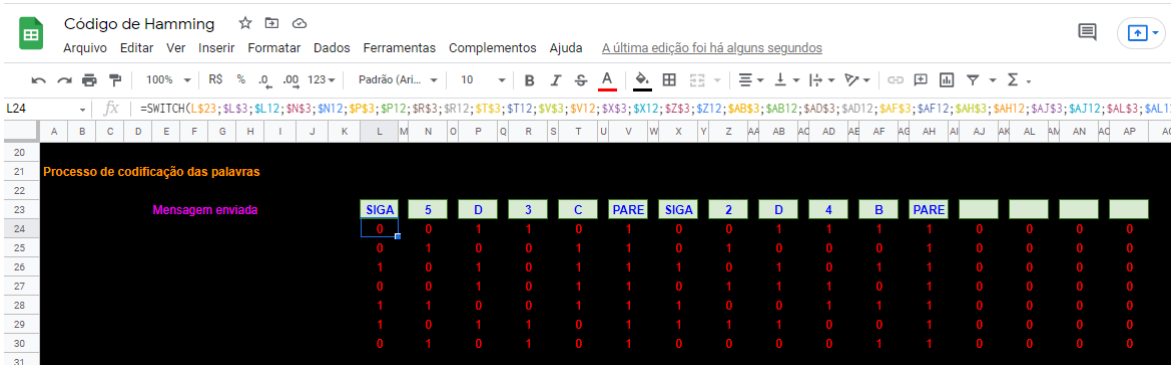

Figura A.2: Planilha: Codificação de uma mensagem.

$$=\text{SWITCH}(L\$23;\ \$L\$3;\ \$L12;\ \$N\$3;\ \$N12;\ \$P\$3;\ \$P12;\ \$R\$3;\ \$R12;\ \$T\$3;\ \$T12;\ \$V\$3;\ \$V12;\ \$X\$3;\ \$X12;\ \$Z\$3;\ \$Z12;\ \$AB\$3;\ \$AB12;\ \$AD\$3;\ \$AD12;\ \$AF\$3;\ \$AF12;\ \$AH\$3;\ \$AH12;\ \$AJ\$3;\ \$AJ12;\ \$AL\$3;\ \$AL12;\ \$AN\$3;\ \$AN12;\ \$AP\$3;\ \$AP12)$$

A função SWITCH faz uma comparação entre o comando digitado na célula L23 e os comandos digitados nas células L3, N3, $\cdots$, AN3 e AP3, e retorna a primeira entrada da palavra do código $ham(7,4)$ referente ao comando encontrado.

3º passo Copiar a célula L24 e colar na 6 células imediatamente abaixo.

4º passo Selecionar as células L24 até L30, copiar e colar logo abaixo de cada uma das células destacadas para digitação do comando, finalizando a construção do mecanismo de codificação. Veja o exemplo da Figura A.2.

Para realizar o processo de simulação de erros será necessário gerar números aleatórios na planilha, neste caso os alunos deverão criar esse mecanismo utilizando a função ALEATÓRIOENTRE. Para criar esta parte da máquina os alunos deverão seguir os seguintes passos:

1º passo Na célula L33 digitar a fórmula:

$$= \text{ALEATÓRIOENTRE}(1;100)$$

2º passo Copiar a célula L33 e colar nas células L34 e L35.

3º passo Copiar as células L33, L34 e L35 e copiar nas demais colunas que tenha o nome canal, sempre iniciando na linha 33.

Veja que para fazer a simulação de erros em uma palavra do código $ham(7,4)$, a planilha realiza os seguintes processos:

- Faz três sorteios seguidos de números em um conjunto fixado e anota os resultados.

- Forma uma sequência com os três números sorteados. Os números podem ser repetidos;

- Observa os elementos da sequência e adiciona um erro em cada uma das 'posições' sorteadas. Por exemplo, no caso da sequência (1, 4, 12), a palavra será recebida com erros nas posições 1 e 4, e no caso da sequência (2, 13, 2) a palavra será recebida com um erro na posição 2.

No caso da máquina que estamos usando, cada sorteio é feito com os número entre 1 e 100 e as palavras têm exatamente 7 posições. Neste caso, temos que a probabilidade de receber a palavra com três erros é de 0,021%, a probabilidade de receber com dois erros é aproximadamente 1,18% e a probabilidade de receber com uma erros é aproximadamente 18,4%. Para alterar estas probabilidades basta modificar o intervalo no qual os números são sorteados.

Para montar a parte mais importante da máquina, ou seja, para montar o mecanismo de detecção e correção erros, e decodificação da palavra os alunos deverão seguir os seguintes passos:

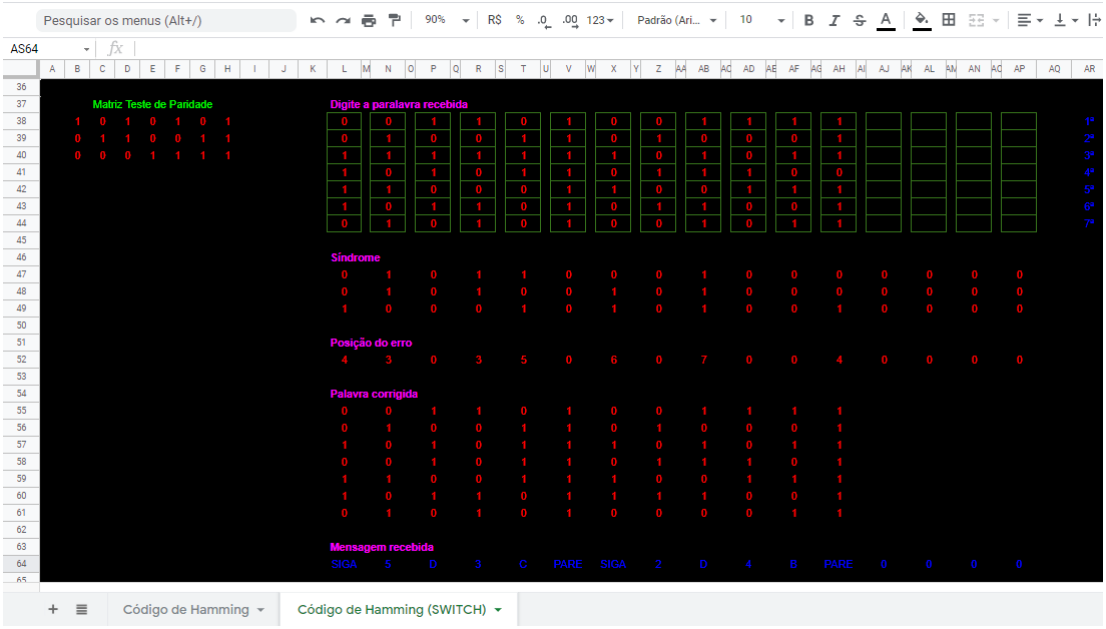

Figura A.3: Planilha: detecção e correção de erros.

1º passo Digitar a matriz teste de paridade $H_{3\times7}$ da Seção 2.3, nas linhas 38, 39, 40, iniciando na célula B38 da planilha.

2º passo Destacar as células L38 até L44, N38 até N44, P38 até P44 e assim sucessivamente até a coluna AP. Esta células servirão como entrada para as palavras recebidas.

3º passo Na célula L38 digitar a seguinte fórmula:

=SE(OU(L$33=1;L$34=1;L$35=1);ABS(L24-1);L24)

Veja que neste caso a palavra terá uma erro na primeira entrada se, no sorteio aleatório, aparecer um número igual a 1 em qualquer uma das células L33, L34 ou L35.

4º passo Na célula L39 digitar a seguinte fórmula:

=SE(OU(L$33=2;L$34=2;L$35=2);ABS(L24-1);L24)

e assim sucessivamente até a célula L44, na qual será digitada a fórmula

=SE(OU(L$33=7;L$34=7;L$35=7);ABS(L24-1);L24)

5º passo Selecionar as células L38 até L44, copiar e colar nas demais colunas onde aparece o nome canal, sempre iniciando na linha 38.

6º passo Digitar a palavra 'síndrome' na célula L46.

7º passo Na célula L47, digitar a seguinte fórmula:

=INT((2-(-1)^ ($B38*L$38 + $C38*L$39 + $D38*L$40 + $E38*L$41 + $F38*L$42 + $G38*L$43 + $H38*L$44))/2)

8º passo Copiar a célula L47 e colar nas células L48 e L49.

9º passo Selecionar as células L46, L47 E L48, copiar e colar nas demais colunas, como mostrado na Figura A.3.

10º passo Digitar a frase 'posição do erro' na célula L51.

11º passo Na célula L52, digitar a seguinte fórmula:

=L47 + L48*2 + L49*4

Esta fórmula faz a mudança de base do número binário (síndrome) para um número decimal (posição do erro).

12º passo Copiar a célula L52 e colar nas células N52, P52, $\cdots$, AN52 e AP52.

13º passo Digitar a frase 'palavra corrigida' na célula L54.

14º passo Nas células L55, L56, L57, L58, L59, L60 e L61, digitar, respectivamente, as seguintes fórmulas:

=SE(L$52=1;INT((2+(-1)^ (L38))/2);L38)
=SE(L$52=2;INT((2+(-1)^ (L39))/2);L39)
=SE(L$52=3;INT((2+(-1)^ (L40))/2);L40)
=SE(L$52=4;INT((2+(-1)^ (L41))/2);L41)
=SE(L$52=5;INT((2+(-1)^ (L42))/2);L42)
=SE(L$52=6;INT((2+(-1)^ (L43))/2);L43)
=SE(L$52=7;INT((2+(-1)^ (L44))/2);L44)

14º passo Selecionar as células L55, L56, L57, L58, L59, L60 e L61, copiar e colar nas células N55, P55, $\cdots$, AN55 e AP55.

15º passo Digitar a frase 'palavra recebida e corrigida' na célula L63.

16º passo Digitar na célula L64, a seguinte fórmula:

=SE(E(L55=$L$12; L56=$L$13; L57=$L$14; L58=$L$15; L59=$L$16; L60=$L$17; L61=$L$18); $L$3; SE(E(L55=$N$12; L56=$N$13; L57=$N$14; L58=$N$15; L59=$N$16; L60=$N$17; L61=$N$18); $N$3; SE(E(L55=$P$12; L56=$P$13; L57=$P$14; L58=$P$15; L59=$P$16; L60=$P$17; L61=$P$18); $P$3; SE(E(L55=$R$12; L56=$R$13; L57=$R$14; L58=$R$15; L59=$R$16; L60=$R$17; L61=$R$18); $R$3; SE(E(L55=$T$12; L56=$T$13; L57=$T$14; L58=$T$15; L59=$T$16; L60=$T$17; L61=$T$18); $T$3; SE(E(L55=$V$12; L56=$V$13; L57=$V$14; L58=$V$15; L59=$V$16; L60=$V$17; L61=$V$18); $V$3; SE(E(L55=$X$12; L56=$X$13; L57=$X$14; L58=$X$15; L59=$X$16; L60=$X$17; L61=$X$18); $X$3; SE(E(L55=$Z$12; L56=$Z$13; L57=$Z$14; L58=$Z$15; L59=$Z$16; L60=$Z$17; L61=$Z$18); $Z$3; SE(E(L55=$AB$12; L56=$AB$13; L57=$AB$14; L58=$AB$15; L59=$AB$16; L60=$AB$17; L61=$AB$18); $AB$3; SE(E(L55=$AD$12; L56=$AD$13; L57=$AD$14; L58=$AD$15; L59=$AD$16; L60=$AD$17; L61=$AD$18); $AD$3; SE(E(L55=$AF$12; L56=$AF$13; L57=$AF$14; L58=$AF$15; L59=$AF$16; L60=$AF$17; L61=$AF$18); $AF$3; SE(E(L55=$AH$12; L56=$AH$13; L57=$AH$14; L58=$AH$15; L59=$AH$16; L60=$AH$17; L61=$AH$18); $AH$3; SE(E(L55=$AJ$12; L56=$AJ$13; L57=$AJ$14; L58=$AJ$15; L59=$AJ$16; L60=$AJ$17; L61=$AJ$18); $AJ$3; SE(E(L55=$AL$12; L56=$AL$13; L57=$AL$14; L58=$AL$15; L59=$AL$16; L60=$AL$17; L61=$AL$18); $AL$3; SE(E(L55=$AN$12; L56=$AN$13; L57=$AN$14; L58=$AN$15; L59=$AN$16; L60=$AN$17; L61=$AN$18); $AN$3; SE(E(L55=$AP$12; L56=$AP$13; L57=$AP$14; L58=$AP$15; L59=$AP$16; L60=$AP$17; L61=$AP$18); $AP$3; "?"))))))))))))))))

Esta função faz uma comparação entre a palavra corrigida e as palavras do código $ham(7,4)$, e retorna o comando referente a palavra escolhida.

17º passo Copiar a célula L64 e colar nas células N64, P64, $\cdots$, AN64 e AP64.

Veja que no exemplo da Figura A.3, várias palavras apresentaram um erro, e mesmo assim a máquina conseguiu recuperar a mensagem.

Por fim, os alunos deverão montar a parte em que será apresentada algumas posições do robô no tabuleiro, podendo assim descrever o caminho percorrido pelo mesmo de maneira visual. O alunos deverão proceder da seguinte maneira:

1º passo Na célula L69 digitar a fórmula:

=SE(L64="SIGA";"-";"Erro")

2º passo Na célula N69 digitar a fórmula:

=SE(OU($L$69="Erro";L$64="SIGA";L$64="PARE";L$64="D";L$64="E";
L$64="B";L$64="C";L$64=0);"-";N$64)

3º passo Nas células N70, N71, $\cdots$, N77, respectivamente, digitar as fórmulas

=SE(OU(L$64=2;L$64=3;L$64=4;L$64=5;L$64=6;L$64=7;L$64=8;L$64=9);
N$69;"-")
=SE(OU(L$64=3;L$64=4;L$64=5;L$64=6;L$64=7;L$64=8;L$64=9);N$69;"-")
=SE(OU(L$64=4;L$64=5;L$64=6;L$64=7;L$64=8;L$64=9);N$69;"-")
=SE(OU(L$64=5;L$64=6;L$64=7;L$64=8;L$64=9);N$69;"-")
=SE(OU(L$64=6;L$64=7;L$64=8;L$64=9);N$69;"-")
=SE(OU(L$64=7;L$64=8;L$64=9);N$69;"-")
=SE(OU(L$64=8;L$64=9);N$69;"-")
=SE(L$64=9;N$69;"-")

4º passo Selecionar as células N70, N71, $\cdots$, N77, copiar e colar nas demais colunas em que aparece o palavra canal, sempre iniciando na linha 70.

5º passo Nas células K81, K82, K83 E K84, respectivamente, digitar as letras maiúsculas D, E, C e B.

6º passo Nas colunas L81, L82, L83 E L84, respectivamente, digitar as fórmulas:

=CONT.SE(L$69:L77;"D")
=CONT.SE(L$69:L77;"E")
=CONT.SE(L$69:L77;"C")
=CONT.SE(L$69:L77;"B")

7º passo Selecionar as células L81, L82, L83, L84, copiar e colar nas demais colunas em que aparece o palavra canal, sempre iniciando na linha 81.

8º passo Digitar a letra X na célula K66 e Y na célula K67.

9º passo Nas células L66 e L67, respectivamente, digitar as fórmulas:

=0,5+L81+L82
=0,5+L83+L84

10º passo Nas células N66 e N67, respectivamente, digitar as fórmulas:

=L66+N81+N82
=L67+N83+N84

11º passo Selecionar as células N66 e N67 copiar e colar nas demais colunas em que aparece o palavra canal, sempre iniciando na linha 66.

12º passo Digitar o número 12 nas células AR66 e AR67.

13º passo Inserir uma imagem com o tabuleiro representado o salão e as mesas, conforme Figura 5.1.

14º passo Selecionar as células K66 até AR67 e inserir um gráfico de dispersão com esses dados.

15º passo formatar o gráfico para que apareça apenas os pontos de coordenadas (x, y).

16º passo ajustar o gráfico e a imagem do tabuleiro para que os pontos apareçam exatamente nas casas do tabuleiro conforme a Figura {graficotabuleiro}.

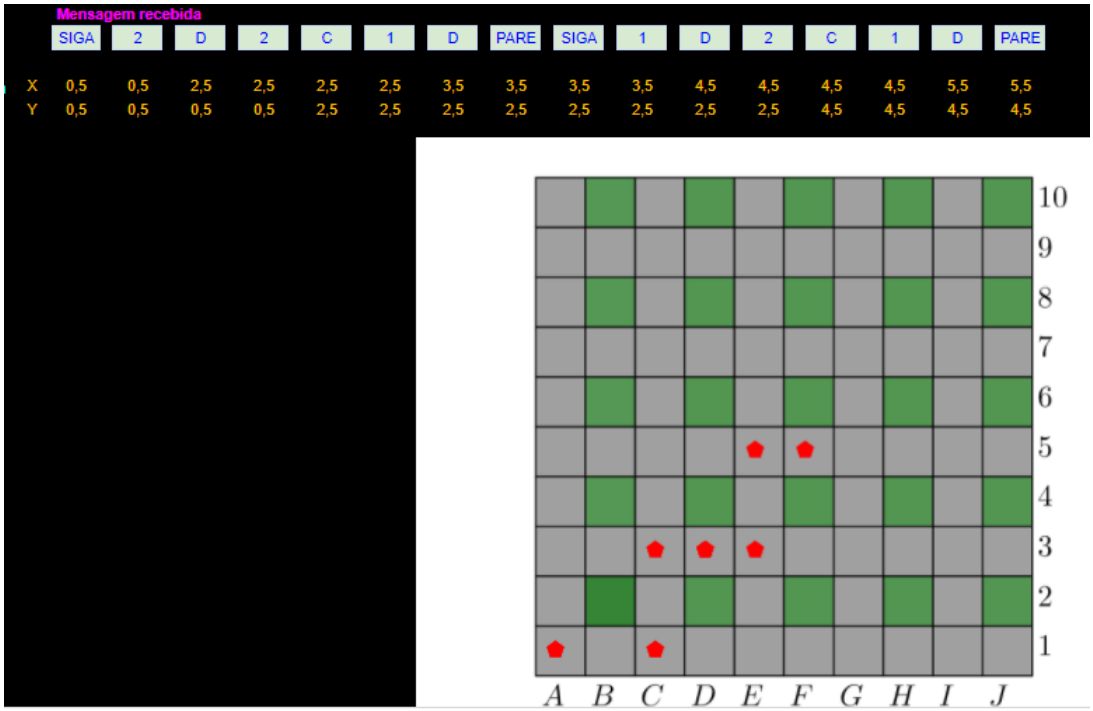

Figura A.4: Representação do movimento do robô.

Apêndice B

Representação do Salão