UNIVERSIDADE TECNOLÓGICA FEDERAL DO PARANÁ
PROGRAMA DE PÓS-GRADUAÇÃO EM MATEMÁTICA

DÉBORA AMANDA MARQUEZ

CÓDIGOS CORRETORES DE ERROS CLÁSSICOS E QUÂNTICOS E UMA PROPOSTA APLICADA NO ENSINO MÉDIO COM A UTILIZAÇÃO DO PROGRAMA EDUCATIVO SCRATCH

DISSERTAÇÃO

CORNÉLIO PROCÓPIO
2023

DÉBORA AMANDA MARQUEZ

CÓDIGOS CORRETORES DE ERROS CLÁSSICOS E QUÂNTICOS E UMA PROPOSTA APLICADA NO ENSINO MÉDIO COM A UTILIZAÇÃO DO PROGRAMA EDUCATIVO SCRATCH

Classical and quantum error correcting code and a proposal applied in high school using the educational program SCRATCH

Dissertação apresentada como requisito para obtenção do título de Mestre em Matemática, do Programa de Pós-Graduação em Matemática, da Universidade Tecnológica Federal do Paraná (UTFPR).

Orientador(a): Prof(a). Dr(a). Débora Aparecida Francisco Albanez

CORNÉLIO PROCÓPIO

2023

Ministério da Educação
Universidade Tecnológica Federal do Paraná
Campus Cornélio Procópio

DEBORA AMANDA MARQUEZ

CÓDIGOS CORRETORES DE ERROS CLÁSSICOS E QUÂNTICOS E UMA PROPOSTA APLICADA NO ENSINO MÉDIO COM A UTILIZAÇÃO DO PROGRAMA EDUCATIVO SCRATCH

Trabalho de pesquisa de mestrado apresentado como requisito para obtenção do título de Mestre da Universidade Tecnológica Federal do Paraná (UTFPR). Área de concentração: Matemática.

Data de aprovação: 05 de Setembro de 2023

Dra. Debora Aparecida Francisco Albanez, Doutorado - Universidade Tecnológica Federal do Paraná

Alireza Mohebi Ashtiani, - Universidade Tecnológica Federal do Paraná

Dr. Junior Cesar Alves Soares, Doutorado - Universidade do Estado de Mato Grosso (Unemat)

Documento gerado pelo Sistema Acadêmico da UTFPR a partir dos dados da Ata de Defesa em 05/09/2023.

Dedico este trabalho a minha família e aos meus amigos, pelos momentos de ausência.

AGRADECIMENTOS

Gostaria de expressar minha profunda gratidão e dedicar esta conquista aos meus pais, João Marquez *(in memoriam)* e Jovelina Alves *(in memoriam)*. Mesmo que eles não estejam mais entre nós, sua presença e influência permanecem vivas em meu coração. Seus ensinamentos e exemplos foram os alicerces que me permitiram enfrentar os desafios mais complexos desta jornada.

Ao meu marido, Ricardo Muniz, dedico uma imensa gratidão por estar ao meu lado em cada etapa desta caminhada. Você tem sido o meu porto seguro, o "ponto de convergência" que me oferece apoio incondicional, compreensão e paciência durante os momentos de ausência para dedicação aos estudos. A sua presença constante e o seu amor são o combustível que impulsionou o meu crescimento e sucesso.

À minha orientadora, Débora A. F. Albanez, expresso minha sincera gratidão. Sua orientação e dedicação foram os "coeficientes angulares" que moldaram minha trajetória acadêmica. Sou grata pela sua disponibilidade, paciência e pelo exemplo inspirador que você representa como profissional e mentora.

Por fim, gostaria de agradecer a todas as pessoas que permaneceram em minha vida, fornecendo apoio emocional, encorajamento e compreensão ao longo desta jornada. Agradeço a cada um de vocês por acreditarem em mim, por compartilharem minhas alegrias e dificuldades, e por me lembrarem constantemente que sou capaz de alcançar grandes conquistas.

Primeira Lei: Um robô não pode ferir um ser humano ou, por omissão, permitir que um ser humano sofra algum mal. Segunda Lei: Um robô deve obedecer as ordens que lhe sejam dadas por seres humanos, exceto nos casos em que tais ordens contrariem a Primeira Lei. Terceira Lei: Um robô deve proteger sua própria existência desde que tal proteção não entre em conflito com a Primeira e Segunda Leis (ASIMOV, Isaac, 1950).

RESUMO

MARQUEZ, Débora Amanda. **Códigos corretores de erros clássicos e quânticos e uma proposta aplicada no ensino médio com a utilização do programa educativo SCRATCH**. 2023. 104 f. Dissertação (Mestrado em Matemática) – Universidade Tecnológica Federal do Paraná. Cornélio Procópio, 2023.

Apresentamos neste trabalho um estudo matemático sobre os códigos corretores de erros clássicos e também os códigos corretores de erros quânticos. Os códigos corretores de erros são um tipo de código utilizado em sistemas de comunicação para detectar e corrigir erros que podem ocorrer durante a transmissão ou armazenamento de informações, oriundos de ruídos e/ou distorções nos sinais, com objetivo de que se possa recuperar a informação transmitida originalmente de forma eficiente e segura. Tais códigos trabalham basicamente adicionando redundância aos dados, de forma que seja possível a detecção e correção de tais erros. Por fim, apresentamos uma proposta aplicada ao ensino médio envolvendo teoria de códigos, com a utilização do programa educativo Scratch.

Palavras-chave: Código Cíclico. Código Linear. Código de Shor. Gamificação. Scratch.

ABSTRACT

MARQUEZ, Débora Amanda. **Classical and quantum error correcting code and a proposal applied in high school using the educational program SCRATCH**. 2023. 104 p. Dissertation (Master's in Course Name) – Universidade Tecnológica Federal do Paraná. Cornélio Procópio, 2023.

In this work, we present a mathematical approach to classical and quantum error-correcting codes. Error-correcting codes are a sort of codes used in the communication systems in order to detect and correct errors that occur during the data transmission or storage due to noise and signal distortion, aiming to recover the original transmitted information in an efficient and safe way. Such codes basically add redundancies to the data, so that the detection and correction of erros are possible. Finally, we present a proposal applied to high school involving code theory, using the educational program Scratch.

Keywords: Cyclic Code. Linear Code. Shor's Code. Gamification. Scratch.

LISTA DE ILUSTRAÇÕES

SUMÁRIO

1 INTRODUÇÃO

A comunicação e a transmissão de dados é uma parte fundamental da vida humana, pois é através dela que transmitimos nossos pensamentos, ideias e sentimentos para outras pessoas. É um processo complexo que envolve a codificação da mensagem, seu transporte e decodificação pela pessoa ou sistema receptor.

Desde o surgimento da comunicação, a busca por mecanismos confiáveis e eficientes para garantir a integridade das informações sempre foi um desafio. Nesse contexto, a Teoria da Informação, desenvolvida por Claude Shannon na década de 1940, abriu caminho para a compreensão matemática da comunicação e trouxe à tona a importância da Teoria de Códigos Corretores de Erros:

> O problema fundamental da comunicação é o de reproduzir em um ponto ou exatamente ou aproximadamente uma mensagem selecionada em outro ponto. Frequentemente as mensagens têm significado, isto é, elas se referem a ou são correlacionadas com algum sistema com certas entidades físicas ou conceituais. Estes aspectos semânticos da comunicação são irrelevantes para o problema de engenharia. ((SHANNON, 1948), p. 1).

A Teoria de Códigos Corretores de Erros desempenha um papel fundamental na transmissão, recepção bem como no armazenamento confiável de dados. Eles são projetados para detectar e corrigir erros que possam ocorrer durante a comunicação ou o armazenamento de informações, devido a interferências externas. Sua importância reside na garantia da integridade dos dados, tornando a comunicação mais segura e eficiente, estão presentes nas redes Wi-Fi que utilizamos para nos conectar à internet, nos dispositivos que armazenam músicas, filmes e dados, nos códigos QR que escaneamos com nossos smartphones, nas transmissões de dados via satélite e nas telecomunicações em geral. Segundo (MILIES, 2009), códigos são amplamente utilizados em programas espaciais da NASA[1] e do JPL[2].

Um exemplo básico de transmissão de informação é quando uma pessoa deseja transmitir a palavra “lotado” para a pessoa à sua frente, mas devido a algum tipo de interferência, a pessoa acaba escutando a palavra “bolado”. Nesse caso, a interferência é conhecida como ruído, onde refere-se a qualquer distorção ou interferência indesejada que ocorre durante a transmissão de informações. Pode ser causado por vários fatores, como sinais elétricos fracos, interferência eletromagnética, problemas na conexão física ou até mesmo falhas no processamento dos dados.

[1] NASA = National Aeronautics and Space Administration
[2] JPL = Jet Propulsion Laboratory

Para combater os efeitos do ruído na transmissão de informações, são utilizados os Códigos Corretores de Erros (CCE). Esses códigos adicionam redundância aos dados transmitidos, permitindo a detecção e correção de erros durante o processo de decodificação. Dessa forma, mesmo que ocorram alterações devido ao ruído, o receptor pode recuperar a mensagem original com base nas informações adicionais fornecidas pelos CCE.

Os Códigos Corretores de Erros Quânticos (CCEQ) é uma área de pesquisa que está abrindo portas para novas aplicações tecnológicas, possibilitando a construção de uma infraestrutura quântica que impulsionará inovações em áreas como computação, criptografia, comunicações seguras e simulação de sistemas complexos.

Assim como na teoria clássica de CCE, os CCEQ também utilizam técnicas de redundância para detectar e corrigir erros. No entanto, devido às propriedades únicas da informação quântica e às restrições impostas pelo princípio da superposição e do emaranhamento quântico, os CCEQ diferem em alguns aspectos dos Códigos Clássicos.

Mostrar aos alunos a aplicação da matemática e sua importância intrínseca no processo de transmissão e recepção de informações é fundamental para despertar o interesse e a compreensão dos conceitos matemáticos. Para (CSIKSZENTMIHALYI, 2014), a motivação e o interesse do aluno desempenham um papel crucial na assimilação e compreensão do conteúdo apresentado, fazendo com que a atitude ativa do estudante seja essencial no processo de construção do conhecimento. Ao explicitar como a matemática é utilizada na criação de CCE e na garantia da integridade das informações transmitidas, os alunos poderão constar que a matemática é uma ferramenta poderosa e relevante no mundo atual de inovações constantes, evidenciando que esta não é uma disciplina abstrata e distante da vida cotidiana, mas sim uma ciência aplicada com impacto direto em tecnologias e processos que utilizamos a cada dia com maior frequência.

A utilização de jogos digitais na educação, também conhecida como gamificação, é uma abordagem pedagógica que busca incorporar elementos de jogos no ambiente de aprendizagem. Essa prática visa tornar o processo de ensino mais engajante, motivador e eficaz, aproveitando os aspectos lúdicos e interativos dos jogos para estimular o interesse dos alunos e promover uma aprendizagem mais significativa.

> O avanço cada vez mais acelerado de dispositivos eletrônicos e a democratização do acesso à internet mudaram os fluxos informacionais, a velocidade e o alcance com que as informações são compartilhadas [...]. Sendo assim, a escola tem pela frente um enorme desafio (SILVA; SALES, 2017).

A dissertação está estruturada da seguinte forma. No segundo capítulo, são apresentadas

as preliminares de estruturas algébricas, conceitos básicos de álgebra linear e conceitos básicos de mecânica quântica. Nesse capítulo, são estabelecidas as bases teóricas necessárias para compreender os fundamentos dos CCE. Vale ressaltar que as demonstrações detalhadas dos resultados estão disponíveis nas referências citadas, uma vez que o foco principal deste trabalho é o estudo e a aplicação dos resultados dos CCE, e não a demonstração matemática rigorosa.

No terceiro capítulo, são apresentados os conceitos e resultados dos Códigos Corretores de Erros Clássicos (CCEC) e Quânticos. Serão explorados os principais conceitos e técnicas utilizadas em ambos os tipos de códigos, bem como suas propriedades e aplicações. Serão discutidos os algoritmos de codificação e decodificação, assim como as estruturas matemáticas envolvidas.

No quarto capítulo, será apresentada uma proposta de aula para o ensino médio sobre CCEC, utilizando a gamificação como estratégia pedagógica. Serão apresentados dois jogos desenvolvidos no ambiente Scratch, de autoria própria, que têm como objetivo ensinar os conceitos e as técnicas dos CCEC de forma lúdica e interativa.

2 PRELIMINARES

Neste capítulo, exploraremos alguns conceitos e resultados que dão embasamento teórico a este trabalho, tais como as estruturas algébricas de anéis e corpos que serão utilizados no estudo da Teoria de Códigos Corretores de Erros Clássicos (CCEC), tendo como referências os trabalhos de (HEFEZ; VILLELA, 2008) e (JANESCH; TANEJA, 2008). Abordaremos também alguns conceitos de Álgebra Linear, considerados essenciais para o estudo de Códigos Corretores de Erros Clássicos e para os Códigos Corretores de Erros Quânticos (CCEQ) referenciado por (AMARAL *et al.*, 2011) e (COELHO, 2001). Para o estudo de Teoria de Códigos Corretores Quânticos apresentaremos alguns conceitos de Mecânica Quântica apresentado com base nos trabalhos de (NIELSEN; CHUANG, 2002) e (AMARAL *et al.*, 2011).

2.1 ESTRUTURAS ALGÉBRICAS

Em álgebra abstrata, uma estrutura algébrica consiste num conjunto associado a uma ou mais operações sobre o conjunto que satisfazem certos axiomas (JÚNIOR, 2011), como por exemplo a comutatividade, associatividade, existência de elemento neutro, dentre outros. Estas estruturas possuem diversas propriedades essenciais para o estudo dos Códigos Corretores de Erros, enriquecendo e tornando os códigos mais eficientes. O foco dessa seção é estudar as estruturas chamadas de Anéis e Corpos.

2.1.1 Anéis e corpos

Nesta seção apresentaremos as estruturas algébricas conhecidas como anéis e corpos, com ênfase nos anéis dos números inteiros.

Definição 1. *Um anel $(A, +, \cdot)$ é um conjunto A não vazio, munido de uma operação denotada por $+$, chamada adição, e de uma operação denotada por $\cdot$, chamada multiplicação, que satisfazem as seguintes condições:*

(A1) Associatividade da adição:

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

(A2) Existência do elemento neutro para adição:

Existe um elemento chamado zero e denotado por 0*, tal que*

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

(A3) Existência do elemento inverso para adição:
Dado $a \in A$*, existe um elemento chamado simétrico de* a *e denotado por* $-a$ *tal que*

$$a + (-a) = (-a) + a = 0.$$

(A4) Comutatividade da adição:

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

(M1) Associatividade da multiplicação:

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

(M2) Existência do elemento neutro para multiplicação:
Existe um elemento chamado unidade e denotado por 1*, tal que*

$$\forall a \in A, \quad a + 1 = 1 + a = a.$$

(M3) Comutatividade da Multiplicação:

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

(AM) Distributividade da multiplicação com relação à adição:

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

Existem vários conjuntos munidos de duas operações que satisfazem os axiomas descritos acima. Por exemplo, ($\mathbb{Z}, +, \cdot$), ($\mathbb{Q}, +, \cdot$), ($\mathbb{R}, +, \cdot$) e ($\mathbb{C}, +, \cdot$) com operações usuais. O conjunto ($\mathbb{N}, +, \cdot$), não forma um anel, em virtude de não haver simétrico dos elementos, nem elemento neutro para a adição. Observe que a definição de anel não especifica a cardinalidade do conjunto, podendo este ser finito ou infinito. Os anéis finitos são escolhas vantajosas para Códigos Corretores de Erros (CCE), pois facilitam a implementação de algoritmos que realizam operações específicas que os computadores podem realizar.

Sem perda de generalidade, utilizaremos a notação simplificada de anel, ou seja, para A um anel, está subentendido $(A, +, \cdot)$. Anéis que possuem axiomas adicionais têm denominação especial, abaixo, apresentaremos um anel que possui um axioma não compartilhado por todos os anéis.

Definição 2. *Um anel A será chamado de domínio de integridade, se possuir a seguinte propriedade :*

$$\forall a, b \in A, \;\; a \neq 0 \;\; e \;\; b \neq 0 \Rightarrow a \cdot b \neq 0.$$

A propriedade acima é equivalente à seguinte:

$$\forall a, b \in A, \;\; a \cdot b = 0 \;\; \Rightarrow a = 0 \;\; \text{ou} \;\; b = 0.$$

Os anéis ($\mathbb{Z}, +, \cdot$), ($\mathbb{Q}, +, \cdot$), ($\mathbb{R}, +, \cdot$) e ($\mathbb{C}, +, \cdot$) são domínios de integridade.

Definição 3. *Um elemento a de um anel A será dito invertível se existir um elemento $b \in A$ tal que $a \cdot b = 1$. Nesse caso, dizemos que b é um inverso de a.*

Definição 4. *Um anel onde todo elemento não nulo é invertível é chamado de corpo.*

A seguir apresentaremos a definição de divisibilidade com relação aos anéis e suas propriedades, para assim, podermos definir a redutibilidade dos elementos de um anel.

Definição 5. *Sejam dados um anel A e dois elementos a e b de A, diremos que a divide b, escrevendo $a|b$, se existir um elemento $c \in A$ tal que $b = a \cdot c$. Nesse caso, diremos também a é um divisor de b, ou ainda, que b é um múltiplo de a.*

Proposição 1. *Quaisquer que sejam $a, b, c, u, \lambda, \mu \in A$ com u invertível, temos que*

(i) Se $u|a, a|0$ então $a|a$.

(ii) Se $a|u$, então a é invertível.

(iii) Se $a|b$ e $b|c$, então $a|c$.

(iv) Se $a|b$ e $a|c$, então $a|(\lambda b + \mu c)$.

Definição 6. *Dados dois elementos $a, b \in A$, diremos que a é um associado de b se existir um elemento invertível $u \in A$ tal que $a = u \cdot b$.*

Proposição 2. *Num anel A temos o seguinte:*

(i) u é associado de 1 se, e somente se, u é invertível.

(ii) Se a e b são associados, então $a|b$ e $b|a$.

(iii) $a|b$ *se, e somente se, todo associado de* a *divide todo associado de* b*, se, e somente se, algum associado de* a *divide algum associado de* b*.*

(iv) Suponhamos que A *seja um domínio de integridade. Se* $a|b$ *e* $b|a$*, então* a *e* b *são associados.*

As Proposições 1 e 2 motivam a seguinte definição:

Definição 7. *Seja* A *um anel. Diremos que um elemento não invertível* $a \in A$ *é irredutível se os únicos divisores de a são os seus associados e os elementos invertíveis de* A*.*

Em contra partida, podemos definir um elemento não invertível $a \in A$ que não é irredutível sendo dito redutível.

Definição 8. *Seja* A *um anel. Diremos que* $a \in A \setminus \{0\}$ *tal que* a *não é invertível é um elemento primo se*

$$\forall\ b, c \in A,\ \ a|b \cdot c \Rightarrow a|b\ \ \textbf{ou}\ \ a|c.$$

Generalizando os conceitos de irredutível e primo, a seguinte proposição é dada:

Proposição 3. *Num domínio de integridade todo elemento primo é irredutível.*

A aritmética modular, às vezes conhecida como álgebra do relógio, é um sistema em que os números "retrocedem"quando atingem um valor predeterminado, o módulo. Por volta de 1750, o matemático suíço Euler fez uma grande contribuição para a abordagem da congruência quando introduziu explicitamente a noção de módulo de congruência de um número natural N (DANTAS, 2016). No livro Disquisitiones Arithmeticae, publicado em 1801, Carl Friedrich Gauss desenvolveu a abordagem contemporânea da álgebra modular.

Definição 9. *Sejam* A *um anel e* $m \in A$*. Dados elementos* $a, b \in A$*, diremos que* a *é congruente a* b *módulo* m*, se* $m|(a - b)$*. Nesse caso, escreve-se,*

$$a \equiv b\ \textit{mod}\ m$$

Proposição 4. *Sejam* a, b, c, a', b' *elementos quaisquer de* A*.*

(i) $a \equiv a\ \textit{mod}\ m$

(ii) Se $a \equiv b\ \textit{mod}\ m$*, então* $b \equiv a\ \textit{mod}\ m$*.*

(iii) Se $a \equiv b\ \textit{mod}\ m$ *e* $b \equiv c\ \textit{mod}\ m$*, então* $a \equiv c\ \textit{mod}\ m$*.*

(iv) Se $a \equiv a'$ *mod* m *e* $b \equiv b'$ *mod* m*, então* $a + b \equiv a' + b'$ *mod* m *e* $a \cdot b \equiv a' \cdot b'$ *mod* m*.*

Definição 10. *A classe residual de um elemento* a *de* A*, módulo* m*, é o conjunto*

$$[a] = \{x \in A; x \equiv a \text{ mod } m\} = \{a + m \cdot \lambda; \lambda \in A\}$$

Definição 11. *Define-se* A_m *como sendo o conjunto de todas as classes residuais em* A *módulo* m*.*

Estudaremos em CCE as classes residuais de $\mathbb{Z}$ módulo m, isto é, o quociente de $m\mathbb{Z}|\mathbb{Z}$, onde

$$\mathbb{Z}_m := \{[0], [1], \ldots, [m-1].\}$$

Exemplo 1. *Seja* $m = 2$*. Logo,* $\mathbb{Z}_2 = \{[0], [1]\}$ *com as operações* $+, \cdot$ *é um Anel.*

$+$	$[0]$	$[1]$
$[0]$	$[0]$	$[1]$
$[1]$	$[1]$	$[0]$

$\times$	$[0]$	$[1]$
$[0]$	$[0]$	$[0]$
$[1]$	$[0]$	$[1]$

Proposição 5. *Quaisquer que sejam os elementos* $a, b \in A$*, temos que*

(i) $[a] = [b]$ *se, e somente se,* $m|(a - b)$*; ou seja,* $a - b \in mA$*.*

(ii) $[a] \cap [b] \neq \varnothing$ *se, e somente se,* $[a] = [b]$*.*

(iii) $A = \bigcup_{a \in A} [a]$*.*

(iv) Se A *é um domínio, existe uma bijeção entre* $[a]$ *em* mA*.*

Proposição 6. *As fórmulas* $[a] + [b] = [a + b]$ *e* $[a] \cdot [b] = [a \cdot b]$ *definem duas operações em* A_m*.*

Proposição 7. *No anel* $\mathbb{Z}$*, todo elemento irredutível é primo.*

Proposição 8. *Todo inteiro não invertível possui pelo menos um divisor primo positivo.*

Teorema 1. *0 anel* Z_m *é um corpo se, e somente se,* m *é um número primo.*

Teorema 2. *(Existência de Corpos Finitos) Para todos os números inteiros positivos* p *e* n *com* p *primo, existe um corpo com* p^n *elementos.*

Definição 12. *Sejam A um anel. Um polinômio $P(X)$ com coeficientes em A é uma expressão do tipo*

$$P(X) = \sum_{i=0}^{n} a_i X^i = a_0 + a_1 X + \ldots + a_n X^n,$$

onde n é um inteiro não negativo e os a_i são elementos de A.

Teorema 3. *O polinômio $P(X) + Q(X)$ é chamado de soma de $P(X)$ e $Q(X)$, enquanto que o polinômio $P(X) \cdot Q(X)$, também denotado por $P(X)Q(X)$, é o seu produto . Note que essas operações, quando restritas a A, coincidem com a adição e a multiplicação em A, dizemos que $A[X]$ é um anel.*

Definição 13. *Se $P(X) = \sum_{i=0}^{n} a_i X^i$ é um polinômio não nulo em $A[X]$ com $a_n \neq 0$, define-se o grau de $P(X)$ como sendo o inteiro não negativo n.*

Proposição 9. *Seja A um domínio de integridade. Temos que*

(i) Se $P(X), Q(X) \in A[X] \setminus \{0\}$, então $gr(P(X) \cdot Q(X)) = gr(P(X)) + gr(Q(X))$,

(ii) $A[X]$ é um domínio de integridade.

(iii) Os elementos invertíveis de $A[X]$ são os elementos invertíveis de A.

Definição 14. *Se $gr(P(X)) = n$ e $a_n = 1$, diremos que $P(X)$ é um polinômio mônico.*

O algoritmo de divisão entre polinômios é bastante direto, ensinado na educação básica, o que nos faz esquecer a força aritmética subjacente em ação nesse processo. A seguir, apresentaremos o algoritmo da divisão entre polinômios.

Teorema 4. *(Algoritmo da divisão) Seja $\mathbb{K}$ um corpo e $P(X), G(X) \in \mathbb{K}[X]$ com $g(x) \neq 0$. Então existem únicos polinômios $Q(X), R(X) \in \mathbb{K}[X]$ tais que*

$$P(X) = G(X)Q(X) + R(X)$$

com $R(X) = 0$ ou $gr(R(X)) < gr(G(X))$.

Exemplo 2. *Sejam os polinômios $P(x) = x^6 - 1$, $G(x) = x - 1 \in \mathbb{Z}_2$. Calculando os polinômios $Q(X), R(X) \in \mathbb{Z}_2$ pelo algoritmo da divisão, temos*

$\cancel{x^6} - 1$	$x - 1$
$\cancel{-x^6} + x^5$	$x^5 + x^4 + x^3 + x^2 + x + 1$
$\cancel{x^5} - 1$	
$\cancel{-x^5} + x^4$	
$\cancel{x^4} - 1$	
$\cancel{-x^4} + x^3$	
$\cancel{x^3} - 1$	
$\cancel{-x^3} + x^2$	
$\cancel{x^2} - 1$	
$\cancel{-x^2} + x$	
$\cancel{x - 1}$	
$\cancel{-x + 1}$	
0	

e ainda, como -1 *é raiz do polinômio* $x^5 + x^4 + x^3 + x^2 + x + 1$ *podemos dividir* $x^5 + x^4 + x^3 + x^2 + x + 1$ *por* $x + 1$. *Logo,*

$\cancel{x^5 + x^4} + x^3 + x^2 + x + 1$	$x + 1$
$\cancel{-x^5 - x^4}$	$x^4 + x^2 + 1$
$\cancel{x^3 + x^2} + x + 1$	
$\cancel{-x^3 - x^2}$	
$\cancel{x + 1}$	
$\cancel{-x - 1}$	
0	

Assim, $x^6 - 1 = (x - 1) \cdot (x + 1) \cdot (x^4 + x^2 + 1)$

Exemplo 3. *Sejam os polinômios* $P(x) = x^7 - 1$, $G(x) = x - 1 \in \mathbb{Z}_2$. *Calculando os polinômios* $Q(X), R(X) \in \mathbb{Z}_2$ *pelo algoritmo da divisão, temos*

$$
\begin{array}{r|l}
\cancel{x^7} - 1 & x - 1 \\
\hline
\cancel{-x^7} + x^6 & x^6 + x^5 + x^4 + x^3 + x^2 + x + 1 \\
\hline
\cancel{x^6} - 1 & \\
\cancel{-x^6} + x^5 & \\
\hline
\cancel{x^5} - 1 & \\
\cancel{-x^5} + x^4 & \\
\hline
\cancel{x^4} - 1 & \\
\cancel{-x^4} + x^3 & \\
\hline
\cancel{x^3} - 1 & \\
\cancel{-x^3} + x^2 & \\
\hline
\cancel{x^2} - 1 & \\
\cancel{-x^2} + x & \\
\hline
\cancel{x - 1} & \\
\cancel{-x + 1} & \\
\hline
0 &
\end{array}
$$

Assim, $x^7 - 1 = (x-1) \cdot (x^6 + x^5 + x^4 + x^3 + x^2 + x + 1)$

Teorema 5. *O máximo divisor comum* $D(X)$ *de dois polinômios, não simultaneamente nulos,* $F(X)$ *e* $G(X)$ *em* $\mathbb{K}[X]$ *existe e pode ser escrito na forma*

$$D(X) = \lambda(X) \cdot F(X) + \mu(X) \cdot G(X),$$

com $\lambda(X), \mu(X) \in \mathbb{K}$.

Proposição 10. *Sejam* $F(X), G(X), H(X) \in \mathbb{K}[X]$. *Se* $F(X) | G(X) \cdot H(X)$ *e MDC*$(F(X), G(X)) = 1$, *então* $F(X) | H(X)$.

Proposição 11. *No anel* $\mathbb{K}[X]$, *todo elemento não invertível e irredutível é primo.*

Teorema 6. *(Unicidade da fatoração) Todo polinômio mônico em* $\mathbb{K}[X]$, *não constante e não irredutível, se escreve como produto de polinômios de* $\mathbb{K}[X]$ *irredutível e mônicos. Essa escrita é única a menos da ordem dos fatores.*

Definição 15. *Seja* A *um anel e seja* $P(X) \in A[X]$. *Diremos que* $\alpha \in A$ *é uma raiz de* $P(X)$ *se* $P(\alpha) = 0$.

Proposição 12. *Sejam $\mathbb{K}$ um corpo, $P(X) \in \mathbb{K}$ e $\alpha \in \mathbb{K}[X]$. Temos que α é uma raiz de $P(X)$ se, e somente se, $(X - \alpha)$ divide $P(X)$.*

Teorema 7. *Um polinômio de grau n com coeficientes num corpo possui até n raízes distintas nesse corpo.*

Definição 16. *As classes residuais de $A = \mathbb{K}[X]$ módulo um polinômio não constante e mônico $m = P(X)$ de grau n. temos que,*

$$A_m = \mathbb{K}_{P(x)} = \{[R(X)]; R[X] \in \mathbb{K} \quad com \quad R(X) = 0, \quad ou \quad gr(R(X)) \neq n\}.$$

Proposição 13. *0 elemento $[F(X)] \in \mathbb{K}_{P(x)}$ é invertível se, MDC$(F(X), P(X)) = 1$.*

Teorema 8. *0 anel $\mathbb{K}_{P(x)}$ é um corpo se, e somente se, o polinômio $P(X)$ é irredutível.*

Teorema 9. *Seja $\mathbb{K}$ um corpo finito qualquer. Para cada número natural n, existe pelo menos um polinômio irredutível de grau n em $\mathbb{K}[X]$.*

A fatoração de polinômios redutíveis em $\mathbb{Z}$ (números inteiros) é uma tarefa difícil e não há uma solução geral que contemple qualquer polinômio. Alguns métodos conhecidos incluem o método de Euclides, o algoritmo de Berlekamp-Massey e o algoritmo de Rabin.

A fatoração de polinômios redutíveis em $\mathbb{Z}_2$ é muito mais simples, pois $\mathbb{Z}_2$ é um corpo finito. Neste caso, a fatoração pode ser realizada com algoritmos de divisão de polinômios clássicos, como o método de Euclides, que é geralmente muito mais rápido e eficiente do que os métodos utilizados para a fatoração de polinômios.

Exemplo 4. *Seja $H(X) = x^6 + x^5 + x^4 + x^3 + x^2 + x + 1$ um polinômio irredutível em $\mathbb{Z}$, porém redutível em $\mathbb{Z}_2$.*

De fato, considere que $H(X)$ pode ser fatorado. As possibilidades para a fatoração é dada por:

(i) $H(X) = (x^3 + ax^2 + bx + c) \cdot (x^3 + a'x^2 + b'x + c')$;

(ii) $H(X) = (x^4 + ax^3 + bx^2 + cx + d) \cdot (x^2 + c'x + d')$;

(iii) $H(X) = (x^5 + ax^4 + bx^3 + cx^2 + dx + e) \cdot (x + e')$.

Pela definição 13 temos que o coeficiente de maior grau dos fatores tem que ser diferente de 0. Como estamos operando em $\mathbb{Z}_2$ temos que a única possibilidade é o coeficiente de maior grau ser $[1]$, por simplicidade usaremos $[1] = 1$ e $[0] = 0$.

Para (i) *temos:*

$$x^6 + x^5 + x^4 + x^3 + x^2 + x + 1 = (x^3 + ax^2 + bx + c) \cdot (x^3 + a'x^2 + b'x + c'). \quad (1)$$

Multiplicando o segundo membro da equação, temos:

$$x^6 + a'x^5 + b'x^4 + c'x^3 + ax^5 + (a \cdot a')x^4 + (a \cdot b')x^3 + (a \cdot c')x^2 + bx^4 + (b \cdot a')x^3 \\ +(b \cdot b')x^2 + (b \cdot c')x + cx^3 + (c \cdot a')x^2 + (c \cdot b')x + c \cdot c'.$$

Colocando de forma mais visual os coeficientes com relação a x^6, x^5, x^4, x^3, x^2 *e* x *temos:*

$$x^6 : 1$$

$$x^5 : (a' + a) \quad (2)$$

$$x^4 : (b' + (a \cdot a') + b) \quad (3)$$

$$x^3 : (c' + (a \cdot b') + (b \cdot a') + c) \quad (4)$$

$$x^2 : ((a \cdot c') + (b \cdot b') + (c \cdot a')) \quad (5)$$

$$x : ((b \cdot c') + (c \cdot b')) \quad (6)$$

$$1 : c \cdot c'. \quad (7)$$

Da expressão 7 podemos afirmar que $c \cdot c' = 1$*, pois o termo independente de* $H(x)$ *é* 1*. Assim,* $c = c' = 1$*.*

Substituindo os valores de c *e* c' *na expressão 6 temos* $(b' + b)x$*. Assim* $b' = 0$ *ou* $b = 0$ *para que* $(b + b')x = 1 \cdot x = x$*.*

- *Para* $b = 0$*:*

  Temos que $b' = 1$*, assim* $c = c' = b' = 1$ *e* $b = 0$*, substituindo na expressão 5 temos* $((a \cdot c') + (b \cdot b') + (c \cdot a'))x^2 = ((a \cdot 1) + (0 \cdot 1) + (1 \cdot a'))x^2 = (a + 0 + a')x^2 = (a \cdot a')x^2$*. Logo* $a = 0$ *ou* $a' = 0$ *para que* $(a + a')x^2 = 1 \cdot x^2 = x^2$*.*

  - *Para* $a = 0$*:*

    Temos que $a' = 1$*, assim* $c = c' = b' = a' = 1$ *e* $b = a = 0$*, substituindo nas outras expressões, temos*

    Em 4: $(c' + (a \cdot b') + (b \cdot a') + c)x^3 = (1 + (0 \cdot 1) + (0 \cdot 1) + 1)x^3 = (1 + 0 + 0 + 1)x^3 = 0x^3 = 0$*.*

    Absurdo, pois o coeficiente de x^3 *em* $H(x)$ *é* 1*.*

- *Para* $a' = 0$*:*

  Temos que $a = 1$*, assim* $c = c' = b' = a = 1$ *e* $b = a' = 0$*, substituindo nas outras expressões, temos*

  Em 4: $(c' + (a \cdot b') + (b \cdot a') + c)x^3 = (1 + (1 \cdot 1) + (0 \cdot 0) + 1)x^3 = (1 + 1 + 0 + 1)x^3 = 1 \cdot x^3 = x^3$.

  Em 3: $(b' + (a \cdot a') + b)x^4 = (1 + (1 \cdot 0) + 0)x^4 = (1 + 0 + 0)x^4 = 1x^4 = x^4$.

  Em 2: $(a' + a)x^5 = (0 + 1)x^5 = 1 \cdot x^5 = x^5$.

  Portanto, $H(x) = (x^3 + x^2 + 1) \cdot (x^3 + x + 1)$.

- *Para* $b' = 0$*:*

  Temos que $b = 1$*, assim* $c = c' = b = 1$ *e* $b' = 0$*, substituindo na expressão 5 temos* $((a \cdot c') + (b \cdot b') + (c \cdot a'))x^2 = ((a \cdot 1) + (1 \cdot 0) + (1 \cdot a'))x^2 = (a + 0 + a')x^2 = (a \cdot a')x^2$. *Logo* $a = 0$ *ou* $a' = 0$ *para que* $(a + a')x^2 = 1 \cdot x^2 = x^2$.

  - *Para* $a' = 0$*:*

    Temos que $a = 1$*, assim* $c = c' = b = a = 1$ *e* $b' = a' = 0$*, substituindo nas outras expressões, temos*

    Em 4: $(c' + (a \cdot b') + (b \cdot a') + c)x^3 = (1 + (1 \cdot 0) + (1 \cdot 0) + 1)x^3 = (1 + 0 + 0 + 1)x^3 = 0x^3 = 0$.

    Absurdo, pois o coeficiente de x^3 *em* $H(x)$ *é* 1.

  - *Para* $a = 0$*:*

    Temos que $a' = 1$*, assim* $c = c' = b = a' = 1$ *e* $b' = a = 0$*, substituindo nas outras expressões, temos*

    Em 4: $(c' + (a \cdot b') + (b \cdot a') + c)x^3 = (1 + (0 \cdot 0 + (1 \cdot 1) + 1)x^3 = (1 + 0 + 1 + 1)x^3 = 1 \cdot x^3 = x^3$.

    Em 3: $(b' + (a \cdot a') + b)x^4 = (0 + (0 \cdot 1) + 1)x^4 = (0 + 0 + 1)x^4 = 1x^4 = x^4$.

    Em 2: $(a' + a)x^5 = (1 + 0)x^5 = 1 \cdot x^5 = x^5$.

    Portanto, $H(x) = (x^3 + x^2 + 1) \cdot (x^3 + x + 1)$.

  Conclui-se que $H(x) = (x^3 + x^2 + 1) \cdot (x^3 + x + 1)$.

  Vejamos ainda que $(x^3 + x^2 + 1)$ *e* $(x^3 + x + 1)$ *são polinômios irredutíveis em* $\mathbb{Z}_2$.

- *Para* $(x^3 + x^2 + 1)$*: Suponha que* $(x^3 + x^2 + 1)$ *seja redutível em* $\mathbb{Z}_2$*, assim* $(x^3 + x^2 + 1)$ *pode ser escrito como* $(x^2 + ax + b) \cdot (x + b')$.

Note que $(x^2+ax+b)\cdot(x+b') = x^3+b'x^2+ax^2+(a\cdot b')x+bx+(b\cdot b')$

$$= x^3+(b'+a)x^2+((a\cdot b')+b)x+(b\cdot b')$$

Como $(b\cdot b')=1$ *temos que* $b=b'=1$*, substituindo* b *e* b' *em* $((a\cdot b')+b)x$ *temos* $((a\cdot 1)+1)x=(a+1)x$*, com necessariamente* $a=1$*, pois o coeficiente de* x *é* 0*. Substituindo os valores de* b, b' *e* a *em* $(b'+a)x^2$*, temos* $(1+1)x^2=0x^2=0$*. Absurdo! pois o coeficiente de* x^2 *é* 1.

- *Para* (x^3+x+1) *Suponha que* (x^3+x+1) *seja redutível em* $\mathbb{Z}_2$*, assim* (x^3+x+1) *pode ser escrito como* $(x^2+ax+b)\cdot(x+b')$.

  Note que $(x^2+ax+b)\cdot(x+b') = x^3+b'x^2+ax^2+(a\cdot b')x+bx+(b\cdot b')$

  $$= x^3+(b'+a)x^2+((a\cdot b')+b)x+(b\cdot b')$$

  Como $(b\cdot b')=1$ *temos que* $b=b'=1$*, substituindo* b *e* b' *em* $((a\cdot b')+b)x$ *temos* $((a\cdot 1)+1)x=(a+1)x$*, com necessariamente* $a=0$*, pois o coeficiente de* x *é* 1*. Substituindo os valores de* b, b' *e* a *em* $(b'+a)x^2$*, temos* $(1+0)x^2=1\cdot x^2=x^2$*. Absurdo! pois o coeficiente de* x^2 *é* 0.

Como as outras possibilidades de fatoração recai em $(x^2+ax+b)\cdot(x+b')$ *em ambos os polinômios* (x^3+x^2+1) *e* (x^3+x+1)*. Podemos afirmar que* (x^3+x^2+1) *e* (x^3+x+1) *são polinômios irredutíveis em* $\mathbb{Z}_2$.

Pelo Teorema 6, temos que a fatoração $H(X)=x^6+x^5+x^4+x^3+x^2+x+1=(x^3+x^2+1)\cdot(x^3+x+1)$ *é única, não havendo necessidade de fazer os casos* (ii) *e* (iii).

Observação 1. *Pelo Exemplo 3 e 4 temos que* $x^7-1=(x-1)\cdot(x^3+x^2+1)\cdot(x^3+x+1)$

Definição 17. *Um subconjunto* I *não vazio de um anel* A *é um ideal de* A *se forem verificadas as condições:*

(i) $\forall a, b\in I, a+b\in I$;

(ii) $\forall a\in I$ *e* $\forall c\in A, ca\in I$.

Proposição 14. *Um ideal de* $\mathbb{K}$ *é da forma* $I(F(X))$*, onde* $F(X)\in\mathbb{K}[X]$.

Corolário 1. *Seja* $I\neq\{0\}$ *um ideal de* $\mathbb{K}$*. Então, existe um único polinômio mônico* $F(X)$ *em* I *(de grau mínimo), tal que* $I=I(F(X))$.

Definição 18. *Um anel onde todo ideal é principal será chamado de anel principal.*

Proposição 15. *Todo ideal de $\mathbb{K}_{P(x)}$ é da forma $I([F(X)])$, onde $F(X)$ é um divisor de $P(X)$.*

2.1.2 O corpo dos números complexos

Como em outros conjuntos numéricos, o conceito de número complexo se desenvolveu gradualmente. Algumas equações de segundo grau do tipo $x^2 + 1 = 0$, não foram resolvidas até o século XVI, porque o conceito de raiz quadrada de um número negativo era desconhecido pelos matemáticos da época. Com o passar dos anos, vários matemáticos se depararam com o mesmo problema para equações de terceira ordem, pois perceberam que o conjunto dos números reais não possuía as soluções de qualquer equação de segundo grau, tampouco possuía todas as soluções de uma equação cúbica qualquer.

Toda construção de mecânica quântica é baseada no conjunto dos números complexos, consequentemente tendo grande importância nos estudos dos CCEQ. Daremos apenas um breve resumo das principais propriedades que serão necessárias ao longo do trabalho.

Definição 19. *Um número complexo é uma expressão do tipo:*

$$z = x + iy,$$

em que x e y são números reais e i, chamado unidade imaginária, satisfaz a propriedade $i^2 = -1$. O número $x = Re(z)$ é dito a parte real de z e $y = Im(z)$ é a parte imaginária de z.

Exemplo 5. *Considere os números $z = 1 + 0i$ e $t = 2 + 7i$, é fácil observar que $z = 1 + 0i = 1 + 0 = 1$ é real e $z = 2 + 7i$ é complexo.*

Definição 20. *O conjugado do número complexo $z = x + iy$ é definido por $\overline{z} = x - iy$.*

Note que o conjugado de um número real é ele próprio.

Definição 21. *A norma de um número complexo $z = x + iy$ é definida $|z| = \sqrt{z \cdot \overline{z}} = \sqrt{x^2 + y^2}$.*

A norma de um número complexo também é chamada de *módulo* ou *valor absoluto*.

Definição 22. *Um número complexo z é chamado unitário se $|z| = 1$.*

Usando a notação $\mathbb{C} = \{x + iy; x,y \in \mathbb{R}\}$ as operações de $\mathbb{C}$ são dadas por:

- $(x_1 + y_1 i) + (x_2 + y_2 i) = (x_1 + x_2) + (y_1 + y_2)i$;

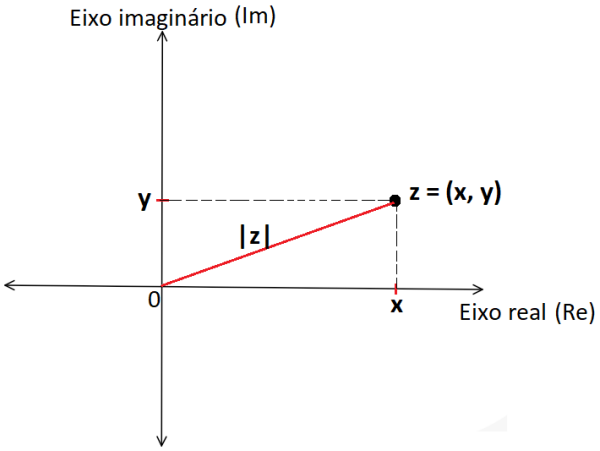
- $(x_1 + y_1 i)(x_2 + y_2 i) = (x_1 x_2 - y_1 y_2) + (x_1 y_2 + y_1 x_2)i.$

Podemos representar os números complexos geometricamente a partir de um plano semelhante ao plano cartesiano, conhecido como plano de Argand-Gauss, ou simplesmente, plano complexo. O número complexo $z = x + iy$ é representado pelo ponto (x, y), $|z|$ representa a distância euclidiana entre o ponto $(0, 0)$ e (x, y), ou seja,

$$|z| = d((x,y),(a,b)) = \sqrt{(x-0)^2 + (y-0)^2} = \sqrt{x^2 + y^2}.$$

O eixo das abscissas é chamado eixo real (Re), e o eixo das ordenadas é o eixo imaginário (Im), como apresentado na Figura 1.

Figura 1 – Representação geométrica do número z.



Fonte: Autoria própria.

2.2 CONCEITOS BÁSICOS EM ÁLGEBRA LINEAR

No decorrer desse trabalho, abordaremos os conceitos de espaços vetoriais complexos, que aparecem naturalmente em mecânica quântica e espaços vetoriais finitos estudados em CCEC.

2.2.1 Espaços vetoriais

A utilização de espaços vetoriais permite uma análise precisa da capacidade de detecção e correção de erros de um código, bem como a otimização da sua estruturada, já que cada mensagem de informação é representada por vetores . Cada mensagem de informação é representada por vetores.

Definição 23. *Sejam dados um corpo $\mathbb{K}$, cujos elementos serão chamados de escalares, e um conjunto V, cujos elementos serão chamados de vetores e serão denotados por $|v\rangle$. Diremos que V é espaço vetorial sobre $\mathbb{K}$, ou um $\mathbb{K}$-espaço vetorial, se existirem uma operação de adição em V.*

$$+ : V \times V \to V$$

$$(|v\rangle, |w\rangle) \mapsto |v\rangle + |w\rangle$$

e uma multiplicação dos elementos de V por escalares,

$$\cdot : \mathbb{K} \times V \to V,$$

$$(\lambda, |v\rangle) \mapsto \lambda \cdot |v\rangle$$

possuindo as seguintes propriedades para quaisquer $|v\rangle, |v\rangle, |v\rangle \in V$:

1. *A adição é associativa:*

$$(|u\rangle + |v\rangle) + |w\rangle = |u\rangle + (|v\rangle + |w\rangle).$$

2. *A adição é comutativa:*

$$|u\rangle + |v\rangle = |v\rangle + |u\rangle .$$

3. *Existência de elemento neutro: existe um elemento 0 em V tal que*

$$|u\rangle + 0 = |u\rangle .$$

4. *Existência de elemento inverso: dado um elemento $|u\rangle \in V$,existe um elemento $-|u\rangle$,chamado simétrico de $|u\rangle$, tal que*

$$|u\rangle + (-|u\rangle) = 0.$$

5. *Dados $\lambda, \mu \in \mathbb{K}$, vale*

$$(\lambda + \mu) \cdot |u\rangle = \lambda \cdot |u\rangle + \mu \cdot |u\rangle .$$

6. *Dados $\lambda, \mu \in \mathbb{K}$, vale*

$$\lambda \cdot (|u\rangle + |v\rangle) = \lambda \cdot |u\rangle + \lambda \cdot |v\rangle .$$

7. *Dados $\lambda, \mu \in \mathbb{K}$, vale*

$$(\lambda \cdot \mu) \cdot |u\rangle = \lambda \cdot (\mu \cdot |u\rangle).$$

8. Para todo $|u\rangle \in V$, $1 \cdot |u\rangle = |u\rangle$, *onde* 1 *é a unidade de* $\mathbb{K}$.

A notação $|\cdot\rangle$ é chamada de ket de Dirac é uma notação matemática utilizada em física quântica para representar estados quânticos que serão estudados nesse trabalho e operações matemáticas. Ela foi desenvolvida por Paul Dirac, um físico teórico britânico, e é baseada em bra-kets, que são símbolos matemáticos que representam estados quânticos. A notação de Dirac permite escrever equações quânticas de forma concisa e elegante, e é amplamente utilizada na mecânica quântica. Por convenção utilizaremos a notação de Dirac:

- Ket: $|\alpha\rangle$ (lê-se "ket alfa") é a representação do vetor coluna.
- Bra: $\langle\alpha|$ (lê-se "bra alfa") é representação do vetor linha.

Exemplo 6. *Para* $V = \mathbb{C}^2$ *sobre* $\mathbb{C}$, *seja o vetor* $|v\rangle = \begin{bmatrix} v_x \\ v_y \end{bmatrix}$ *juntamente com o* $|u\rangle = \begin{bmatrix} u_x \\ u_y \end{bmatrix}$, *serão consideradas as operações vetoriais na notação de ket é dada por:*

i) Soma: $|v\rangle + |u\rangle = \begin{bmatrix} v_x \\ v_y \end{bmatrix} + \begin{bmatrix} u_x \\ u_y \end{bmatrix} = \begin{bmatrix} v_x + u_x \\ v_y + u_y \end{bmatrix}$;

ii) Multiplicação por escalar: $\alpha\,|v\rangle = \alpha \begin{bmatrix} v_x \\ v_y \end{bmatrix} = \begin{bmatrix} \alpha v_x \\ \alpha v_y \end{bmatrix}$.

Definição 24. *Considere o espaço* $\mathbb{C}^2$ *sobre* $\mathbb{C}$ *os vetores coluna* $(1,0)$ *e* $(0,1)$ *em suas representações na notação de Dirac é dada por:* $|0\rangle = \begin{bmatrix} 1 \\ 0 \end{bmatrix}$ *e* $|1\rangle = \begin{bmatrix} 0 \\ 1 \end{bmatrix}$

O símbolo $|0\rangle$ será usado com frequência e não representa o vetor nulo do espaço vetorial em questão. Denotaremos o vetor nulo apenas pelo símbolo 0.

Exemplo 7. *O espaço vetorial* $\mathbb{R}^n$ *sobre* $\mathbb{R}$: *este é o conjunto de todas as n-upla* $(x_1, x_2, ..., x_n)$ *e* $(y_1, y_2, \ldots, y_n)$ *de números reais, com as operações de adição vetorial e multiplicação escalar dadas por:*

$$(x_1, x_2, \ldots, x_n) + (y_1, y_2, \ldots, y_n) = (x_1 + y_1, x_2 + y_2, \ldots, x_n + y_n)$$

$$\alpha \cdot (x_1, x_2, \ldots, x_n) = (\alpha x_1, \alpha x_2, \ldots, \alpha x_n)$$

onde α *é um número real.*

Exemplo 8. *O espaço vetorial de matrizes $M_{m\times n}$ sobre $\mathbb{R}$: este é o conjunto de todas as matrizes mxn com entradas reais, com as operações de adição vetorial e multiplicação escalar dadas por:*

$$A + B = [a_{ij} + b_{ij}]$$

$$\alpha A = [\alpha a_{ij}]$$

onde α é um número real.

Exemplo 9. *O espaço vetorial $\mathbb{C}^n$ sobre $\mathbb{C}$: este é o conjunto de todas as n-upla $(z_1, z_2, \ldots, z_n)$ e $(w_1, w_2, \ldots, w_n)$ de números complexos, com as operações de adição vetorial e multiplicação escalar dadas por:*

$$(z_1, z_2, \ldots, z_n) + (w_1, w_2, \ldots, w_n) = (z_1 + w_1, z_2 + w_2, \ldots, z_n + w_n)$$

$$\alpha \cdot (z_1, z_2, ..., z_n) = (\alpha z_1, \alpha z_2, \ldots, \alpha z_n)$$

onde α é um número complexo.

Definição 25. *Um subespaço vetorial S do espaço vetorial V é um subconjunto de V, tal que as seguintes propriedades são válidos:*

- $0 \in S$;
- $|x\rangle + |y\rangle \in S$ *para todo par* $|x\rangle ; |y\rangle \in S$;
- $\lambda |x\rangle \in S$ *para todo* $\lambda \in \mathbb{K}$ *e todo* $|x\rangle \in S$.

Definição 26. *Dizemos que uma expressão do tipo*

$$\alpha_1 |v_1\rangle + \ldots + \alpha_k |v_k\rangle , \alpha_i \in \mathbb{K}$$

é uma combinação linear dos vetores $|v_1\rangle , \ldots , |v_k\rangle$. Dado um conjunto de vetores dizemos que ele gera V se todo elemento de V pode ser escrito como combinação linear dos elementos desse conjunto.

Definição 27. *Dizemos que um conjunto de vetores $\{|v_1\rangle , \ldots , |v_k\rangle\} \subset V$ é linearmente independente (LI) se a equação*

$$\alpha_1 |v_1\rangle + \ldots + \alpha_k |v_k\rangle = 0$$

só admite a solução trivial $(\alpha_1, \ldots, \alpha_k) = (0, \ldots, 0)$. Caso contrário, dizemos que os vetores são linearmente dependentes (LD).

Definição 28. *Uma base para um espaço vetorial V sobre $\mathbb{K}$ é um conjunto LI*

$$\mathcal{B} = \{|v_1\rangle, \ldots, |v_k\rangle\}$$

tal que todo vetor de V é combinação linear de $\mathcal{B}$. A dimensão de V é o número de vetores em uma base, que é denotada por $dimV$ ou $dim(V)$.

Exemplo 10. *Para o espaço vetorial $\mathbb{R}^2$ sobre $\mathbb{R}$, uma base pode ser dada por $\{|1\rangle, |0\rangle\}$;*

Para o espaço vetorial $\mathbb{C}^2$ sobre $\mathbb{C}$, uma base pode ser dada por $\{|1\rangle, |0\rangle\}$;

Observe que as bases acima são as bases canônicas, ou seja, as bases formadas pelos vetores unitários. Geralmente, um espaço vetorial pode ter muitos conjuntos geradores diferentes.

Exemplo 11. *Para o espaço vetorial $\mathbb{C}^2$ sobre $\mathbb{C}$, uma base pode ser dada por*

$$\left\{ |v_1\rangle = \frac{1}{\sqrt{2}} \begin{bmatrix} 1 \\ 1 \end{bmatrix}, |v_2\rangle = \frac{1}{\sqrt{2}} \begin{bmatrix} 1 \\ -1 \end{bmatrix} \right\}.$$

pois, seja $|v\rangle = (\alpha, \beta) \in \mathbb{C}^2$, assim

$$|v\rangle = \frac{\alpha + \beta}{\sqrt{2}} |v_1\rangle + \frac{\alpha - \beta}{\sqrt{2}} |v_2\rangle.$$

2.2.2 Transformações lineares

Definição 29. *Sejam U e V espaços vetoriais. Uma aplicação $T : U \to V$ é dita uma transformação linear se dados $|u_1\rangle, |u_2\rangle \in U$ e $\lambda \in \mathbb{K}$ temos*

- $T(\lambda |u_1\rangle) = \lambda T(|u_1\rangle)$;
- $T(|u_1\rangle + |u_2\rangle) = T(|u_1\rangle) + T(|u_2\rangle)$.

Note que uma transformação linear mantém algumas características fundamentais do espaço de origem e também é conhecida como *aplicação linear* ou *mapa linear*. No caso em que o domínio e o contradomínio coincidem, ou seja $U = V$, dizemos que T é um *operador linear*, que predominará nesse trabalho.

Uma transformação linear pode transformar um espaço vetorial de dimensão 3 para um espaço de dimensão 2, como no exemplo abaixo:

Exemplo 12. *Considere a seguinte transformação linear,*

$$\begin{aligned} A: \ \mathbb{Z}_2^2 &\longrightarrow \mathbb{Z}_2^5 \\ (x_1, x_2) &\longmapsto (x_1, x_2, x_1 + x_2, x_1 - x_2, x_2). \end{aligned}$$

Aplicando a transformação Z nos elementos do conjunto $\mathbb{Z}_2^2$, obtemos

$$Z(0,1) = (0, 1, 0 + 1, 0 - 1, 1) = (0, 1, 1, 1, 1)$$

$$Z(1,0) = (1, 0, 1 + 0, 1 - 0, 0) = (1, 0, 1, 1, 0).$$

Assim, uma base para o espaço vetorial é dada por $B = \{(1, 0, 1, 1, 0),(0, 1, 1, 1, 1)\}$, gerando assim, todos os elementos do espaço vetorial $\mathbb{Z}_2^5$.

A seguir será apresentada a transformação linear no ponto de vista matricial.

Fixemos uma base $\mathcal{B} = \{|e_1\rangle, \ldots, |e_m\rangle\}$ de V e $\mathcal{F} = \{|f_1\rangle, \ldots, |f_n\rangle\}$ de U, onde V é espaço vetorial sobre $\mathbb{K}$ e U Podemos escrever um vetor $|v\rangle \in V$ na forma $|v\rangle = \sum_{i=1}^{m} v_i |e_i\rangle$, e também representá-lo na forma matricial

$$|v\rangle = \begin{bmatrix} v_1 \\ v_2 \\ \vdots \\ v_m \end{bmatrix}_{\mathcal{B}} = \begin{bmatrix} v_1, v_2, \ldots, v_m \end{bmatrix}_{\mathcal{B}}^{t}.$$

com $v_i \in V$ para todo i. Dai,

$$T(|v\rangle) = T\left(\sum_{i=1}^{m} v_i |e_i\rangle\right) = \sum_{i=1}^{m} v_i T(|e_i\rangle) = \sum_{i=1}^{m}\sum_{j=1}^{n} v_i T_{ji} |f_j\rangle)$$

onde T é uma transformação linear de V em U, com T_{ji} tal que $T(|e_i\rangle) = \sum_{j=1}^{n} T_{ji} |f_j\rangle$. Portanto podemos representar a transformação linear T por meio de uma matriz $T_{\mathcal{B},\mathcal{F}}$ com entradas T_{ij} de forma que

$$[T(|v\rangle)]_{\mathcal{F}} = T_{\mathcal{F}}^{\mathcal{B}} [v]_{\mathcal{B}}.$$

Exemplo 13. *A matriz de transformação do Exemplo 12 é dada por* $\begin{bmatrix} 1 & 0 & 1 & 1 & 0 \\ 0 & 1 & 1 & 1 & 1 \end{bmatrix}$.

Definição 30. *Considere o dual de um vetor $|v\rangle \in \mathbb{C}^n$, denotado por $\langle v|$, é o vetor transposto de $|v\rangle$ com os elementos substituídos pelos seus conjugados, ou seja $\langle v| := (|v\rangle)^\dagger = (\overline{|v\rangle})^T$.*

Exemplo 14. *Considerando o Exemplo 24, podemos concluir que o* $\langle 0| = \begin{bmatrix} 1 & 0 \end{bmatrix}$ *e* $\langle 1| = \begin{bmatrix} 0 & 1 \end{bmatrix}$.

2.2.3 Matrizes de Pauli

As matrizes de Pauli, em homenagem ao físico Wolfgang Pauli, são operadores lineares representadas por matrizes complexas 2×2 usadas na mecânica quântica que representam os três observáveis: Bit Flip, Phase Flip e Bit-Phase Flip.

As matrizes de Pauli são definidas como:

$$\sigma_i = I = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}$$

$$\sigma_x = X = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}$$

$$\sigma_y = Y = \begin{bmatrix} 0 & -i \\ i & 0 \end{bmatrix}$$

$$\sigma_z = Z = \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix}$$

Conforme veremos as matrizes de Pauli são usadas para descrever a evolução temporal de sistemas quânticos em termos de sua Hamiltoniana, que é uma função matemática que descreve a energia total do sistema. Além disso, as matrizes de Pauli são importantes para a teoria quântica de informação, onde são usadas para representar qubits, que são unidades básicas de informação quântica.

Exemplo 15. *Vejamos a ação dos operadores de Pauli nos vetores $|0\rangle$ e $|1\rangle$:*

Para o operador $\sigma_i = I$, temos:

- $I|0\rangle = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} \begin{bmatrix} 1 \\ 0 \end{bmatrix} = \begin{bmatrix} 1 \cdot 1 + 0 \cdot 0 \\ 0 \cdot 1 + 1 \cdot 0 \end{bmatrix} = \begin{bmatrix} 1 \\ 0 \end{bmatrix} = |0\rangle$
- $I|1\rangle = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} \begin{bmatrix} 0 \\ 1 \end{bmatrix} = \begin{bmatrix} 1 \cdot 0 + 0 \cdot 1 \\ 0 \cdot 0 + 1 \cdot 1 \end{bmatrix} = \begin{bmatrix} 0 \\ 1 \end{bmatrix} = |1\rangle$

Para o operador $\sigma_x = X$, temos:

- $X|0\rangle = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix} \begin{bmatrix} 1 \\ 0 \end{bmatrix} = \begin{bmatrix} 0 \cdot 1 + 1 \cdot 0 \\ 1 \cdot 1 + 10 \cdot 0 \end{bmatrix} = \begin{bmatrix} 0 \\ 1 \end{bmatrix} = |1\rangle$

- $X|1\rangle = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix} \begin{bmatrix} 0 \\ 1 \end{bmatrix} = \begin{bmatrix} 0 \cdot 0 + 1 \cdot 1 \\ 1 \cdot 0 + 0 \cdot 1 \end{bmatrix} = \begin{bmatrix} 1 \\ 0 \end{bmatrix} = |0\rangle$

Para o operador $\sigma_y = Y$, temos:

- $iY|0\rangle = \begin{bmatrix} 0 & 1 \\ -1 & 0 \end{bmatrix} \begin{bmatrix} 1 \\ 0 \end{bmatrix} = \begin{bmatrix} 0 \cdot 1 + 1 \cdot 0 \\ (-1) \cdot 1 + 0 \cdot 0 \end{bmatrix} = \begin{bmatrix} 0 \\ (-1) \end{bmatrix} = -|1\rangle$
- $iY|1\rangle = \begin{bmatrix} 0 & 1 \\ -1 & 0 \end{bmatrix} \begin{bmatrix} 0 \\ 1 \end{bmatrix} = \begin{bmatrix} 0 \cdot 0 + 1 \cdot 1 \\ (-1) \cdot 0 + 0 \cdot 1 \end{bmatrix} = \begin{bmatrix} 1 \\ 0 \end{bmatrix} = |0\rangle$

Para o operador $\sigma_z = Z$, temos:

- $Z|0\rangle = \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix} \begin{bmatrix} 1 \\ 0 \end{bmatrix} = \begin{bmatrix} 1 \cdot 1 + 0 \cdot 0 \\ 0 \cdot 1 + (-1) \cdot 0 \end{bmatrix} = \begin{bmatrix} 1 \\ 0 \end{bmatrix} = |0\rangle$
- $Z|1\rangle = \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix} \begin{bmatrix} 0 \\ 1 \end{bmatrix} = \begin{bmatrix} 1 \cdot 0 + 0 \cdot 1 \\ 0 \cdot 0 + (-1) \cdot 1 \end{bmatrix} = \begin{bmatrix} 0 \\ -1 \end{bmatrix} = -|1\rangle$

Observação 2. *No exemplo 15 é possível ver as ações dos operadores de Pauli nos vetores $|0\rangle$ e $|1\rangle$, tendo que a matriz X leva $|0\rangle$ a $|1\rangle$ e $|1\rangle$ a $|0\rangle$, ganhando assim o nome de inversão de bits; e a matriz Z deixa $|0\rangle$ invariante, e leva $|1\rangle$ a -$|1\rangle$, ganhando o termo inversão de fase.*

2.2.4 Produtos interno e externos

O produto interno é um importante conceito matemático oriundo da álgebra linear utilizado em várias ciências, incluindo física, engenharia, economia, entre outros. Em espaços vetoriais, o produto interno é uma função bilinear que mede a similaridade entre dois vetores, usado por exemplo para calcular a norma de um vetor, a distância entre dois vetores, a projeção de um vetor em outro, a ortogonalidade, entre outras aplicações. Além disso, o produto interno é uma parte importante de muitos algoritmos e teoremas em matemática e em física, incluindo os espaços de Hilbert e a teoria da relatividade.

Definição 31. *Dado um espaço vetorial V sobre $\mathbb{K}$, um produto interno é uma aplicação*

$$\langle \cdot | \cdot \rangle : V \times V \to \mathbb{K}$$

$$(|u\rangle, |v\rangle) \longmapsto \langle u|v\rangle$$

satisfazendo as seguintes propriedades: para todo $|u\rangle, |v\rangle, |w\rangle \in V$ e $\lambda, \mu \in \mathbb{K}$

- $\langle \lambda u + \mu v | w \rangle = \overline{\lambda} \langle u|w\rangle + \overline{\mu} \langle v|w\rangle$;
- $\langle u|v\rangle = \overline{\langle v|u\rangle}$;
- $\langle u|u\rangle \geq 0$;
- *Se* $\langle u|u\rangle = 0$ *então* $|u\rangle = 0$.

Definição 32. *(Espaço de Hilbert $\mathcal{H}$) Um espaço de Hilbert é um espaço vetorial munido de um produto interno completo com a norma gerada por ele.*

Definição 33. *Dizemos que dois vetores de um espaço com produto interno $|u\rangle$ e $|v\rangle$ são ortogonais se $\langle u|v\rangle = 0$. Dizemos que um conjunto $E = \{|v_1\rangle, \ldots, |v_k\rangle\}$ é ortogonal se seus elementos são dois a dois ortogonais. Dizemos que um conjunto $E = \{|v_1\rangle, \ldots, |v_k\rangle\}$ é ortonormal se é ortogonal e $\langle v_i|v_i\rangle = 1$ para todo $i = \{1, \ldots, k\}$.*

O produto externo é uma operação matemática que permite combinar dois ou mais vetores para formar um novo objeto matemático com dimensão maior. É comumente denotado como $|\ \rangle\langle\ |$. Em mecânica quântica, o produto externo é usado para descrever sistemas quânticos compostos por mais de um qubit ou sistema similar.

Proposição 16. *Muniremos o espaço $\mathbb{C}^2$ com os seguintes produtos: dados dois vetores $|\varphi\rangle, |\psi\rangle \in \mathbb{C}^n$, muniremos o espaço $\mathbb{C}$ sobre $\mathbb{C}$ com o seguinte produto interno e externo: o produto interno $\langle\varphi|\psi\rangle$ e o produto externo $|\varphi\rangle\langle\psi|$ são definidos, respectivamente, por*

$$\langle\varphi|\psi\rangle = (|\varphi\rangle)^\dagger |\psi\rangle$$

e

$$|\varphi\rangle\langle\psi| = |\varphi\rangle (|\psi\rangle)^\dagger .$$

Considerando $|\varphi\rangle = \begin{bmatrix} \alpha \\ \beta \end{bmatrix}$ e $|\psi\rangle = \begin{bmatrix} \gamma \\ \phi \end{bmatrix}$, dois vetores em $\mathbb{C}^n$, pela Definição 30 e Proposição 16 determinaremos o produto interno e externo entre esses dois vetores:

$$\langle\varphi|\psi\rangle = (|\varphi\rangle)^\dagger |\psi\rangle = \begin{bmatrix} \overline{\alpha} & \overline{\beta} \end{bmatrix} \begin{bmatrix} \gamma \\ \phi \end{bmatrix} = \overline{\alpha}\gamma + \overline{\beta}\phi;$$

e

$$|\varphi\rangle\langle\psi| = |\varphi\rangle (|\psi\rangle)^\dagger = \begin{bmatrix} \alpha \\ \beta \end{bmatrix} \begin{bmatrix} \overline{\gamma} & \overline{\phi} \end{bmatrix} = \begin{bmatrix} \alpha\overline{\gamma} & \alpha\overline{\phi} \\ \beta\overline{\gamma} & \beta\overline{\phi} \end{bmatrix}.$$

Note que, o produto interno determina um número compexo, enquanto o produto externo determina uma matriz complexa quadrada.

Definição 34. *Seja V um espaço vetorial sobre $\mathbb{K}$ com produto interno. A norma de um elemento $|v\rangle \in V$ é definida por:*

$$||v\rangle| = \sqrt{\langle v|v\rangle}$$

Exemplo 16. *Considere os vetores $|0\rangle$ e $|1\rangle$ no espaço vetorial $\mathbb{C}$, vamos determinar o produto interno, externo e a norma desses vetores. Note que,*

$$\langle 0|1\rangle = (|0\rangle)^\dagger |1\rangle = \begin{bmatrix} \overline{1} & \overline{0} \end{bmatrix} \begin{bmatrix} 0 \\ 1 \end{bmatrix} = \overline{1} \cdot 0 + \overline{0} \cdot 1 = 1 \cdot 0 + 0 \cdot 1 = 0$$

O resultado 0 indica que os vetores $|0\rangle$ e $|1\rangle$ são ortogonais.

$$|0\rangle \langle 1| = |0\rangle (|1\rangle)^\dagger = \begin{bmatrix} 1 \\ 0 \end{bmatrix} \begin{bmatrix} \overline{0} & \overline{1} \end{bmatrix} = \begin{bmatrix} 1 \cdot \overline{0} & 1 \cdot \overline{1} \\ 0 \cdot \overline{0} & 0 \cdot \overline{1} \end{bmatrix} = \begin{bmatrix} 1 \cdot 0 & 1 \cdot 1 \\ 0 \cdot 0 & 0 \cdot 1 \end{bmatrix} = \begin{bmatrix} 0 & 1 \\ 0 & 0 \end{bmatrix}.$$

e a norma do vetor $|0\rangle$ é dada por

$$\langle 0|0\rangle = (|0\rangle)^\dagger |0\rangle = \begin{bmatrix} \overline{1} & \overline{0} \end{bmatrix} \begin{bmatrix} 1 \\ 0 \end{bmatrix} = \overline{1} \cdot 1 + \overline{0} \cdot 0 = 1 \cdot 1 + 0 \cdot 0 = 1$$

Analogamente, a norma do vetor $|1\rangle$ é igual a 1. Portanto, o espaço que contém $|0\rangle$ e $|1\rangle$ é ortonormal.

Proposição 17. *(Relação de Completude) Consideremos uma base ortonormal $\{|j\rangle\} \subset V$, com $j = \{1, \ldots, dimV\}$. Qualquer vetor $|v\rangle \in V$ pode ser escrito como $|v\rangle = \sum_j v_j |j\rangle$, com $v_j = \langle j|v\rangle \in \mathbb{C}$. Assim vem que*

$$\sum_{j=1}^{dimV} |j\rangle \langle j| (|v\rangle) = \sum_{j=1}^{dimV} |j\rangle (\langle j|v\rangle) = \sum_{j=1}^{dimV} v_j |j\rangle = |v\rangle .$$

Então,

$$\sum_{j=1}^{dimV} |j\rangle \langle j| = \mathcal{I}_v$$

onde $\mathcal{I}_v |v\rangle := |v\rangle$ para todo $|v\rangle \in V$.

2.2.5 Autovetores e autovalores

Se $T : V \to V$ é um operador linear, então podemos procurar vetores não nulos satisfazendo a equação $T|v\rangle = \lambda|v\rangle$ para algum $\lambda \in \mathbb{K}$. As soluções $|v\rangle$ são conhecidas como autovetores e o respectivo λ como autovalor de T.

Considerando a representação do operador na forma matricial

$$T|v\rangle = A|v\rangle$$

temos:

- autovalores λ de T ou de A: são as raízes da equação

$$\det(A - \lambda I) = 0;$$

- autovetores $|v\rangle$ de T ou de A: para cada λ encontrado acima, são as soluções da equação $A|v\rangle = \lambda|v\rangle$ ou, equivalentemente $(A - \lambda I)|v\rangle = 0$.

Exemplo 17. *Calculemos os autovalores das matrizes de Pauli.*

- *Autovalores de I:*

$$det\left(\begin{bmatrix}1 & 0\\ 0 & 1\end{bmatrix} - \lambda\begin{bmatrix}1 & 0\\ 0 & 1\end{bmatrix}\right) = det\left(\begin{bmatrix}1-\lambda & 0\\ 0 & 1-\lambda\end{bmatrix}\right) = (1-\lambda)^2 = 0$$

Logo, $(1-\lambda)^2 = 0$, então $\lambda = 1$. Temos que os autovalores para a matriz I é dada por $\lambda_1 = 1$ e $\lambda_2 = 1$.

- *Autovalores de X:*

$$det\left(\begin{bmatrix}0 & 1\\ 1 & 0\end{bmatrix} - \lambda\begin{bmatrix}1 & 0\\ 0 & 1\end{bmatrix}\right) = det\left(\begin{bmatrix}-\lambda & 1\\ 1 & -\lambda\end{bmatrix}\right) = \lambda^2 - 1 = 0$$

Logo, $\lambda^2 - 1 = 0$, então $\lambda = \pm 1$. Temos dois autovalores para a matriz X, que são $\lambda_1 = +1$ e $\lambda_2 = -1$.

- *Autovalores de Y:*

$$det\left(\begin{bmatrix}0 & -i\\ i & 0\end{bmatrix} - \lambda\begin{bmatrix}1 & 0\\ 0 & 1\end{bmatrix}\right) = det\left(\begin{bmatrix}-\lambda & -i\\ i & -\lambda\end{bmatrix}\right) = \lambda^2 + 1 = 0$$

Logo, $\lambda^2 + 1 = 0$*, então* $\lambda = \pm i$*.Assim, temos dois autovalores para a matriz* Y*, que são* $\lambda_1 = +i$ *e* $\lambda_2 = -i$*.*

- *Autovalores de* Z*:*

$$det\left(\begin{bmatrix}1 & 0\\ 0 & -1\end{bmatrix} - \lambda\begin{bmatrix}1 & 0\\ 0 & 1\end{bmatrix}\right) = det\left(\begin{vmatrix}1-\lambda & 0\\ 0 & -1-\lambda\end{vmatrix}\right) = (1-\lambda)(-1-\lambda) = 0$$

Logo, $(1-\lambda)(-1-\lambda) = 0$*, então* $\lambda = 1$ *ou* $\lambda = -1$*. Temos dois autovalores para a matriz* Z*, que são* $\lambda_1 = +1$ *e* $\lambda_2 = -1$*.*

Vamos agora calcular os autovetores para cada autovalor. Para fazer isso, resolvemos a equação $(A - \lambda I)\,|v\rangle = 0$*, onde* $|v\rangle$ *é o autovetor correspondente ao autovalor* λ*.*

- *Autovetores de* I*: Como* $\lambda = 1$*, temos:*

$$\left(\begin{bmatrix}1 & 0\\ 0 & 1\end{bmatrix} - \begin{bmatrix}1 & 0\\ 0 & 1\end{bmatrix}\right)\begin{bmatrix}x\\ y\end{bmatrix} = \begin{bmatrix}0\\ 0\end{bmatrix}$$

Portanto,

$$\left(\begin{bmatrix}0 & 0\\ 0 & 0\end{bmatrix}\right)\begin{bmatrix}x\\ y\end{bmatrix} = \begin{bmatrix}0\\ 0\end{bmatrix}$$

Ou seja, ambos x *e* y *podem ser qualquer valor, então*

$$|v\rangle = \left\{\begin{bmatrix}x\\ y\end{bmatrix}; x \in \mathbb{C}\backslash\{0\}\right\}$$

- *Autovetores de Z: Com* $\lambda = +1$*, temos:*

$$\left(\begin{bmatrix}1 & 0\\ 0 & -1\end{bmatrix} - \begin{bmatrix}1 & 0\\ 0 & 1\end{bmatrix}\right)\begin{bmatrix}x\\ y\end{bmatrix} = \begin{bmatrix}0\\ 0\end{bmatrix}$$

Ou seja,

$$\begin{bmatrix}0\\ -2y\end{bmatrix} = \begin{bmatrix}0\\ 0\end{bmatrix}$$

Portanto, $y = 0$*. Assim*

$$|v\rangle = \left\{ \begin{bmatrix} x \\ 0 \end{bmatrix} ; x \in \mathbb{C}\backslash\{0\} \right\}$$

Para $\lambda = -1$*, temos:*

$$\left(\begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix} - \begin{bmatrix} -1 & 0 \\ 0 & -1 \end{bmatrix} \right) \begin{bmatrix} x \\ y \end{bmatrix} = \begin{bmatrix} 0 \\ 0 \end{bmatrix}$$

Logo,

$$\begin{bmatrix} 2x \\ 0 \end{bmatrix} = \begin{bmatrix} 0 \\ 0 \end{bmatrix}$$

Portanto, $2x = 0$*. Qualquer valor não nulo para* y *pode ser usado como o autovetor correspondente a* $\lambda = -1$*, isto é:*

$$|v\rangle = \left\{ \begin{bmatrix} 0 \\ y \end{bmatrix} ; x \in \mathbb{C}\backslash\{0\} \right\}$$

Usando o mesmo procedimento, os autovetores de X*,* Y *são* $\frac{1}{\sqrt{2}}\left(|0\rangle + |1\rangle\right), \frac{1}{\sqrt{2}}\left(|0\rangle - |1\rangle\right)$ *e* $\frac{1}{\sqrt{2}}\left(|0\rangle + i\,|1\rangle\right), \frac{1}{\sqrt{2}}\left(|0\rangle - i\,|1\rangle\right)$ *respectivamente.*

2.2.6 Adjuntos e operadores hermitianos

Proposição 18. *Dado um operador linear no espaço de Hilbert* $A : \mathcal{H} \to \mathcal{H}$*, existe um único operador linear* $A^\dagger$ *tal que, para todo* $|v\rangle, |w\rangle \in \mathcal{H}$*,*

$$\langle v|Aw\rangle = \left\langle A^\dagger v|w\right\rangle$$

$A^\dagger$ *é dito como adjunto (ou Hermitiano conjugado) de* A*.*

Proposição 19.

- $(A^\dagger)^\dagger = A$;
- $(AB)^\dagger = B^\dagger A^\dagger$;
- *Dado um vetor* $|v\rangle$ *define-se* $\langle v| := |v\rangle^\dagger$*. então* $(A\,|v\rangle)^\dagger = \langle v|\,A^\dagger$;
- $(|v\rangle\,\langle w|)^\dagger = |w\rangle\,\langle v|\,$;
- $(\sum_i a_i A_i)^\dagger = \sum_i \overline{a_i} A_i^\dagger$

- $A^\dagger = \overline{(A^T)} = (\overline{A})^T$

Definição 35. *Um operador é dito Hermitiano (ou auto-adjunto) se* $A^\dagger = A$.

Definição 36. *Consideremos uma base* $\{|j\rangle\} \subset W$*, com* $j = \{1, \ldots, dimW\}$*, sendo* W *um subespaço do espaço vetorial* V*. Assim, podemos construir uma base* $\{|j\rangle\} \subset V$*, com* $j = \{1, \ldots, dimV\}$ *com* $dimV \geq dimW$*. Desta forma define-se:*

$$P := \sum_{j=1}^{dimW} |j\rangle \langle j|$$

como sendo o projetor de V *sobre* W.

As seguintes propriedades são satisfeitas:

- $P^\dagger = P$
- $P^2 = P$
- $P + Q = \mathcal{I}_v$

  $$Q = \sum_{j=dimW+1}^{dimV} |j\rangle \langle j|$$

  sendo o complemento ortonormal de P.

Definição 37. *Um operador* A *é dito normal se*

$$AA^\dagger = A^\dagger A.$$

Observação 3. *Se um operador* A *é Hermitiano* $(A^\dagger = A)$*, então obviamente* A *é normal.*

Teorema 10. *(Decomposição Espectral) Dado* $A : V \to V$*,* A *é normal se, e somente se, existir uma base ortonormal de* V *na qual* A *é diagonal.*

Definição 38. *Um operador* $A : V \to V$ *é dito positivo (notação* $A \geq 0$*) se*

$$\langle v|Av\rangle \geq 0.$$

Para todo $|v\rangle \in V$ *e* $\langle v|Av\rangle > 0 \quad \forall\, |v\rangle \neq 0$*, então* A *é dito positivo definido.*

Proposição 20. *Um operador positivo* $(A \geq 0)$ *é necessariamente Hermitiano* $(A = A^\dagger)$.

Proposição 21. $A^\dagger A$ *é positivo* $A^\dagger A \geq 0$ *para qualquer operador linear* A.

Definição 39. *Um operador* $\mathcal{U} : V \to V$ *é dito unitário se*

$$\mathcal{U}^{\dagger}\mathcal{U} = \mathcal{I} = \mathcal{U}\mathcal{U}^{\dagger}$$

Apresentaremos agora o operador unitário na representação de produto externo.

Observação 4. *Consideremos uma base ortonormal* $\{|v_i\rangle\}$*, isto é,* $\langle v_i|v_j\rangle = \delta_{ij}$*. Assim* $\{|w_i\rangle\} := \{\mathcal{U}\,|v_i\rangle\}$ *também forma uma base ortonormal:*

$$\langle w_i|w_j\rangle = \langle v_i\mathcal{U}|\mathcal{U}v_j\rangle = \left\langle v_i|\mathcal{U}^{\dagger}\mathcal{U}|v_j\right\rangle = \langle v_i|v_j\rangle = \delta_{ij}$$

Exemplo 18. *Matrizes de Pauli na representação de produto interno é dada por:*

$$\sigma_i = I = |0\rangle\langle 0| + |1\rangle\langle 1|$$

$$\sigma_x = X = |0\rangle\langle 1| + |1\rangle\langle 0|$$

$$\sigma_y = Y = -i\,|0\rangle\langle 1| + i\,|1\rangle\langle 0|$$

$$\sigma_z = Z = |0\rangle\langle 0| - |1\rangle\langle 1|$$

As matrizes de Pauli são Hermitianas e unitárias.

2.2.7 Produtos tensoriais

O produto tensorial é uma operação matemática que combina dois ou mais espaços vetoriais para formar um novo espaço vetorial de dimensão superior, dotado de uma operação de composição bilinear, denotada por $\otimes$. O produto tensorial é amplamente utilizado na análise de erro e na avaliação de desempenho de códigos corretores de erros quânticos. Ele é usado para calcular a probabilidade de ocorrência de erros e para estimar o número mínimo de informações adicionais necessárias para garantir a detecção e correção de erros com precisão.

Definição 40. *Consideremos dois espaços de Hilbert* $\mathcal{V}$ *e* $\mathcal{W}$ *e bases ortonormais* $\{|v_i\rangle\} \subset \mathcal{V}$ *e* $\{|w_j\rangle\} \subset \mathcal{W}$ *com* $i = \{1, \ldots, dim\mathcal{V}\}$ *e* $j = \{1, \ldots, dim\mathcal{W}\}$*. Uma base ortonormal para o espaço produto tensorial* $\mathcal{V} \otimes \mathcal{W}$ *é definida como*

$$\{|v_i\rangle \otimes |w_j\rangle\}.$$

Temos assim que $dim\mathcal{V} \otimes \mathcal{W} = dim\mathcal{V} dim\mathcal{W}$.

Proposição 22. *Qualquer vetor* $|\psi\rangle \in \mathcal{V} \otimes \mathcal{W}$ *pode ser escrito como*

$$|\psi\rangle = \sum_{ij} c_{ij} |v_i\rangle \otimes |w_j\rangle$$

com $c_{ij} \in \mathbb{K}$*:*

Proposição 23. *As seguintes notações para produto tensorial serão utilizados:*

$$|v_i\rangle \otimes |w_j\rangle \equiv |v_i\rangle \ |w_j\rangle \equiv |v_i, w_j\rangle \equiv |v_i w_j\rangle \equiv |vw\rangle$$

Exemplo 19.

$$|0\rangle \otimes |1\rangle \equiv |01\rangle$$

$$|1\rangle \otimes |0\rangle \equiv |10\rangle$$

Proposição 24. *O produto tensorial satisfaz as seguintes propriedades de linearidade em suas duas entradas:*

i) Para $z \in \mathbb{C}$ *e* $|\psi\rangle \in \mathcal{V}$ *e* $|\phi\rangle \in \mathcal{W}$

$$z(|\psi\rangle \otimes |\phi\rangle) = (z |\psi\rangle \otimes |\phi\rangle) = |\psi\rangle \otimes (z |\phi\rangle);$$

ii) Para $|\psi\rangle, |\xi\rangle \in \mathcal{V}$ *e* $|\phi\rangle \in \mathcal{W}$

$$(|\psi\rangle + |\xi\rangle) \otimes |\phi\rangle = |\psi\rangle \otimes |\phi\rangle + |\xi\rangle \otimes |\phi\rangle ;$$

iii) Para $|\psi\rangle \in \mathcal{V}$ *e* $|\phi\rangle, |\chi\rangle \in \mathcal{W}$

$$|\psi\rangle \otimes (|\phi\rangle + |\chi\rangle) = |\psi\rangle \otimes |\phi\rangle + |\psi\rangle \otimes |\chi\rangle .$$

Definição 41. *Sejam* $\mathcal{V}, \mathcal{V}', \mathcal{W}$ *e* $\mathcal{W}'$ *espaços vetoriais sobre* $\mathbb{K}$*. Consideremos vetores* $|\psi\rangle \in \mathcal{V}$ *e* $|\phi\rangle \in \mathcal{W}$ *e operadores lineares* $A : \mathcal{V} \to \mathcal{V}'$ *e* $B : \mathcal{W} \to \mathcal{W}'$*. Define-se um operador linear* $A \otimes B : \mathcal{V} \otimes \mathcal{W} \to \mathcal{V}' \otimes \mathcal{W}'$ *como*

$$A \otimes B(|\psi\rangle \otimes |\phi\rangle) := A(|\psi\rangle) \otimes B(|\phi\rangle) \tag{8}$$

Definição 42. *De forma mais geral, a Equação 8 pode ser definida por*

$$(\sum_{ij} c_{ij} A \otimes B)(|\psi\rangle \otimes |\phi\rangle) := \sum_{ij} c_{ij} A(|\psi\rangle) \otimes B(|\phi\rangle)$$

Definição 43. *Os produtos internos nos espaços $\mathcal{V}$ e $\mathcal{W}$ podem ser usados para definir um produto em $\mathcal{V} \otimes \mathcal{W}$. Defina*

$$\left(\sum_i a_i \left| v_i \right\rangle \otimes \left| w_i \right\rangle . \sum_j b_j \left| v'_j \right\rangle \otimes \left| w'_j \right\rangle \right) = \sum_{ij} \overline{a_i} b_j \left\langle v_i | v'_j \right\rangle \left\langle w_i | w'_j \right\rangle$$

Pode-se mostrar que a função assim definida é um produto interno bem definido segundo Nielsen e Chuang (2002). A partir desse produto interno, o espaço do produto interno $\mathcal{V} \otimes \mathcal{W}$ herda a outra estrutura com a qual estamos familiarizados, como noções de adjunto, unitariedade, normalidade e Hermiticidade.

Consideremos agora o produto de Kronecker, que é uma operação matemática que permuta duas matrizes e produz uma matriz resultante. A dimensão da matriz resultante é determinada pelo número de elementos em cada matriz de entrada, como é possível ver a seguir.

Definição 44. *Considere A uma matriz $m \times n$ com entradas a_{ij}, onde $i = \{1, \ldots, m\}$ e $j = \{1, \ldots, n\}$ e B uma matriz $p \times q$. Então temos a representação matricial:*

$$A \otimes B \equiv \begin{bmatrix} a_{11}B & a_{12}B & \ldots & a_{1n}B \\ a_{21}B & a_{22}B & \ldots & a_{2n}B \\ \vdots & \vdots & \vdots & \vdots \\ a_{m1}B & a_{m2}B & \ldots & a_{mn}B \end{bmatrix}_{mp \times nq} ,$$

Notação: $A^{\otimes n} = \underbrace{A \otimes \ldots \otimes A}_{n \ parcelas}$. Exemplo $A^{\otimes 2} = A \otimes A$.

Exemplo 20. *O produto tensorial dos vetores coluna (1, 2) e (3, 4) é o vetor:*

$$\begin{bmatrix} 1 \\ 2 \end{bmatrix} \otimes \begin{bmatrix} 3 \\ 4 \end{bmatrix} = \begin{bmatrix} 1 \times 3 \\ 1 \times 4 \\ 2 \times 3 \\ 2 \times 4 \end{bmatrix} = \begin{bmatrix} 3 \\ 4 \\ 6 \\ 8 \end{bmatrix} .$$

Exemplo 21. *O produto tensorial das matrizes de Pauli X e Y é*

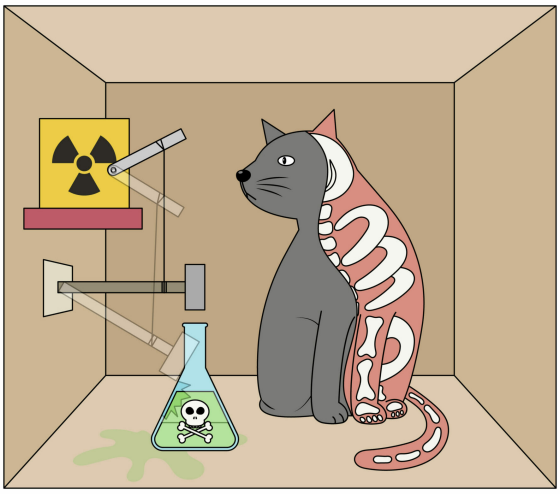
$$X \otimes Z = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix} \otimes \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix} = \begin{bmatrix} 0 \times 1 & 0 \times 0 & 1 \times 1 & 1 \times 0 \\ 0 \times 0 & 0 \times (-1) & 1 \times 0 & 1 \times (-1) \\ 1 \times 1 & 1 \times 0 & 0 \times 1 & 0 \times 0 \\ 1 \times 0 & 1 \times (-1) & 0 \times 0 & 0 \times (-1) \end{bmatrix} = \begin{bmatrix} 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & -1 \\ 1 & 0 & 0 & 0 \\ 0 & -1 & 0 & 0 \end{bmatrix} .$$

2.3 CONCEITOS BÁSICOS EM MECÂNICA QUÂNTICA

A mecânica quântica começou a ser desenvolvida no início do século XX para explicar fenômenos como a radiação eletromagnética e a estrutura dos átomos que não podiam ser explicados pela física clássica. É também a base para uma compreensão da computação quântica e da informação quântica, fornece uma descrição completamente diferente do mundo subatômico, introduzindo conceitos como a incerteza quântica, superposição de estados, emaranhamento quântico e probabilidade quântica.

Um exemplo clássico usado para ilustrar esses conceitos é o famoso “Gato de Schrödinger”. Neste experimento mental, um gato é colocado em uma caixa junto com um dispositivo que pode liberar uma substância venenosa. De acordo com a mecânica quântica, até que a caixa seja aberta e a observação seja feita, o gato está em uma superposição de estar vivo e morto ao mesmo tempo. Somente quando a caixa é aberta é que o estado do gato é definido, ilustrado na Figura 2. Esse exemplo mostra como a mecânica quântica desafia nossa intuição sobre o comportamento das partículas e nos leva a repensar nossa compreensão da realidade em níveis fundamentais.

Figura 2 – Gato de Schrödinger.



Fonte: Revista Ciência Hoje.

Os qubits, ou bits quânticos, são as unidades fundamentais da computação quântica e informação quântica. Ao contrário dos bits clássicos, que só podem representar os estados 0 e 1 de forma exclusiva, os qubits podem existir em uma superposição de ambos os estados simultaneamente. Isso significa que um qubit pode representar uma combinação linear de 0 e 1 ao mesmo tempo, proporcionando a possibilidade de executar tarefas de computação de grandes dimensões, como criptografia, inteligência artificial e análise de grandes conjuntos de dados,

muito mais rapidamente.

O primeiro postulado da mecânica quântica estabelece o espaço na qual a mecânica quântica ocorre, o espaço de Hilbert.

Postulado 1. *Existe um espaço vetorial complexo, com produto interno, associado a qualquer sistema físico fechado (sistema que não interage com outros sistemas). Um estado desse sistema é completamente descrito por um vetor unitário, chamado vetor de estado.*

O sistema mecânico quântico mais simples, o qual nos interessamos utiliza o bit quântico ou qubit. Um qubit tem um espaço de estado bidimensional, cujo espaço vetorial associado é o $\mathbb{C}^2$ sobre $\mathbb{C}$, com o produto interno usual. Uma base ortonormal para esse espaço pode ser dada pelos vetores $|0\rangle$ e $|1\rangle$. Então um **vetor de estado** arbitrário no espaço de estados pode ser escrito como

$$|\psi\rangle = a\,|0\rangle + b\,|1\rangle\,,$$

onde a e b são números complexos e a restrição $|a|^2 + |b|^2 = 1$ deve ser satisfeita. A base $\{|0\rangle\,, |1\rangle\}$ é chamada base computacional e o vetor $|\psi\rangle$ denota a superposição dos vetores $|0\rangle$ e $|1\rangle$, com amplitudes a e b.

Intuitivamente, os estados $|0\rangle$ e $|1\rangle$ são análogos aos dois valores 0 e 1 que um bit clássico pode assumir. A forma como um qubit difere de um bit clássico é que também podem existir superposições desses dois estados, na forma $a\,|0\rangle + b\,|1\rangle$, nas quais não é possível dizer que o qubit está definitivamente no estado $|0\rangle$, ou definitivamente no estado $|1\rangle$. Dizemos que qualquer combinação linear é uma superposição dos estados.

Postulado 2. *A evolução de um sistema quântico fechado é descrita por um operador linear unitário que preserva o produto interno (operador unitário). O estado $|\psi_2\rangle$ do sistema, no tempo t_1, está relacionado ao estado $|\psi_1\rangle$, no tempo t_2, através de um operador unitário $\mathcal{U}$ que depende apenas de t_1 e t_2. Ou seja,*

$$|\psi_2\rangle = \mathcal{U}\,|\psi_1\rangle\,.$$

A evolução de qualquer sistema quântico fechado pode ser descrita dessa maneira. Na seção 2.2.2 foram definidos alguns exemplos de operadores unitários (as matrizes de Pauli) que são importantes na computação quântica e na informação quântica.

As portas lógicas quânticas são operadores lineares que agem sobre estados quânticos, com o objetivo de realizar operações lógicas. A porta control NOT quântica, também conhecida como CNOT, é uma das portas lógicas quânticas mais simples e importantes, vista posteriormente.

Além da CNOT, existem outras portas lógicas importantes na mecânica quântica, como a porta de Hadamard (H), dada pelo operador unitário Hadamard, cuja representação matricial, na base computacional, é dada por

$$H = \frac{1}{\sqrt{2}} \begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix} \tag{9}$$

A porta de fase (Z), entre outras, são usadas em diversos algoritmos quânticos.

Exemplo 22. *Utilizaremos a matriz do operador unitário Hadamard aplicada na base de estados quânticos $|0\rangle$ e $|1\rangle$, transformando-os em estados superpostos. A aplicação da matriz Hadamard em cada estado é dada por:*

$$H|0\rangle = \frac{1}{\sqrt{2}} \begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix} \begin{bmatrix} 1 \\ 0 \end{bmatrix} = \frac{1}{\sqrt{2}} \begin{bmatrix} 1 \\ 1 \end{bmatrix} = \frac{1}{\sqrt{2}} \left(\begin{bmatrix} 1 \\ 0 \end{bmatrix} + \begin{bmatrix} 0 \\ 1 \end{bmatrix} \right) = \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)$$

$$H|1\rangle = \frac{1}{\sqrt{2}} \begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix} \begin{bmatrix} 0 \\ 1 \end{bmatrix} = \frac{1}{\sqrt{2}} \begin{bmatrix} 1 \\ -1 \end{bmatrix} = \frac{1}{\sqrt{2}} \left(\begin{bmatrix} 1 \\ 0 \end{bmatrix} + \begin{bmatrix} 0 \\ -1 \end{bmatrix} \right) = \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle)$$

Pelo Postulado 2 temos que, aplicando um operador unitário sobre o estado $|\psi\rangle$, o resultado ainda será uma superposição dos estados $|0\rangle$ e $|1\rangle$. Isso faz com que a quantidade de informação armazenada no estado $|\psi\rangle$ possa ser infinita. Entretanto, essa quantidade infinita de informação está no nível quântico. Para torná-la acessível no nível clássico, precisamos fazer uma medida. Para considerar esse fato, existe um terceiro postulado.

Postulado 3. *As medições quânticas são descritas por uma coleção M_m de operadores de medição. Estes são operadores que atuam no espaço de estados do sistema que está sendo medido. O índice m refere-se aos resultados de medição que podem ocorrer no experimento. Se o estado do sistema quântico for $|\psi\rangle$ imediatamente antes da medição, então a probabilidade de que o resultado m ocorra é dado por*

$$p(m) = \langle\psi| M_m^\dagger M_m |\psi\rangle , \tag{10}$$

e o estado do sistema após a medição é

$$\frac{M_m |\psi\rangle}{\sqrt{\langle\psi| M_m^\dagger M_m |\psi\rangle}} \tag{11}$$

Os operadores de medição satisfazem a equação de completude,

$$\sum_m M_m^\dagger M_m = \mathcal{I} \tag{12}$$

A equação de completude expressa o fato de que as probabilidades somam um:

$$1 = \sum_m p(m) = \sum_m \langle\psi| M_m^\dagger M_m |\psi\rangle . \tag{13}$$

Esta equação sendo satisfeita para todos $|\psi\rangle$ é equivalente à equação de completude.

Exemplo 23. *Vejamos a medição de um qubit na base computacional. Esta é uma medição em um único qubit com dois resultados definidos pelos dois operadores de medição*

$$M_0 = |0\rangle\langle 0| = \begin{bmatrix} 1 & 0 \\ 0 & 0 \end{bmatrix},$$

$$M_1 = |1\rangle\langle 1| = \begin{bmatrix} 0 & 0 \\ 0 & 1 \end{bmatrix}.$$

Observe que cada operador de medição é Hermitiano, e que $M_0^2 = M_0, M_1^2 = M_1$. Assim a relação de completude é obedecida,

$$\mathcal{I} = M_0^\dagger M_0 + M_1^\dagger M_1 = M_0 + M_1.$$

Suponha que o estado que está sendo medido seja $|\psi\rangle = a|0\rangle + b|1\rangle$. Então a probabilidade de obter o resultado da medição 0 é

$$p(0) = \langle\psi| M_0^\dagger M_0 |\psi\rangle = \langle\psi| M_0 |\psi\rangle = |a|^2 \tag{14}$$

Analogamente, a probabilidade de obter o resultado da medição 1 é $p(1) = |b|^2$. O estado após a medição nos dois casos é, portanto,

$$\frac{M_0|\psi\rangle}{|a|} = \frac{a}{|a|}|0\rangle \tag{15}$$

$$\frac{M_1|\psi\rangle}{|b|} = \frac{b}{|b|}|1\rangle . \tag{16}$$

A aplicação da matriz Hadamard transforma o estado $|0\rangle$ em um estado superposto como vimos no Exemplo 22 com probabilidade 50% de medir 0 e 50% de medir 1, e transforma o estado $|1\rangle$ em um estado superposto com probabilidade 50% de medir 0 e 50% de medir -1. De fato, sabendo que

$$H|0\rangle = \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle).$$

Pelo Postulado 3

$$p(0) = (|a|)^2 = \left(\frac{1}{\sqrt{2}}\right)^2 = \frac{1}{2}.$$

$$p(1) = (|a|)^2 = \left(\frac{1}{\sqrt{2}}\right)^2 = \frac{1}{2}.$$

Da mesma forma,

$$H\,|1\rangle = \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle).$$

Pelo Postulado 3

$$p(0) = (|a|)^2 = \left(\frac{1}{\sqrt{2}}\right)^2 = \frac{1}{2}.$$

$$p(-1) = (|a|)^2 = \left(\frac{1}{\sqrt{2}}\right)^2 = \frac{1}{2}.$$

Postulado 4. *O espaço de estados de um sistema físico composto é o produto tensorial dos espaços de estados dos sistemas físicos. Além disso, se temos sistemas numerados de* 1 *a* n*, e o sistema de número* i *é preparado no estado* $|\psi_i\rangle$*, então o estado conjunto do sistema total é* $|\psi_1\rangle \otimes |\psi_2\rangle \otimes \ldots \otimes |\psi_n\rangle$ *.*

O Postulado 4 nos permite definir associadas aos sistemas quânticos compostos, o emaranhamento. O **emaranhamento quântico** é uma propriedade da mecânica quântica que liga dois ou mais qubits de tal forma que as propriedades dos qubits não podem ser descritas independentemente. Isso significa que a medição de um qubit afeta imediatamente o estado do outro, mesmo se estiverem separados por longas distâncias. O emaranhamento é visto como uma das características mais distintivas da mecânica quântica e tem aplicações em áreas como a criptografia quântica e a computação quântica.

Exemplo 24. *Vejamos um exemplo de como fazer um estado emaranhado do tipo* $|0\rangle + |1\rangle$ *para* $|000\rangle + |111\rangle$*. Para isso, Suponha que tentamos copiar um qubit no estado desconhecido* $|\psi\rangle = a\,|0\rangle + b\,|1\rangle$*. O estado de entrada dos dois qubits pode ser escrito como*

$$[a\,|0\rangle + b\,|1\rangle]\,|0\rangle = a\,|0\rangle \otimes |0\rangle + b\,|1\rangle \otimes |0\rangle = a\,|0\rangle\,|0\rangle + b\,|1\rangle\,|0\rangle = a\,|00\rangle + b\,|10\rangle$$

A ação do CNOT, representada pelo operador unitário matriz Pauli-X, pode ser aplicado os estados de emaranhamento da seguinte forma: se o primeiro qubit estiver definido como 0*, então o segundo qubit é deixado inalterado. Se o primeiro qubit for definido como 1, o segundo qubit é invertido pela matriz de Pauli X.*

$$|00\rangle \to |00\rangle\,,\ \ |01\rangle \to |01\rangle\,,\ \ |10\rangle \to |11\rangle\,,\ \ |11\rangle \to |10\rangle$$

Assim, $a\,|00\rangle + b\,|10\rangle \rightarrow a\,|00\rangle + b\,|11\rangle$ *o qubit inicial o qual seu sucessor se baseará para permanecer inalterado ou inverter-se é chamado de controlador. Repita o mesmo procedimento, agora aplique a porta CNOT com o segundo qubit como controlador e o terceiro qubit como alvo:*

$$a\,|000\rangle + b\,|110\rangle \rightarrow a\,|000\rangle + b\,|111\rangle$$

É possível usar portas quânticas para copiar informações clássicas codificadas como $|0\rangle$ ou $|1\rangle$. No entanto, para um estado geral $|\psi\rangle$ isso não é possível, ou seja não é possível copiar estados arbitrários $|\psi\psi\rangle$. Esse fato pode ser constatado no Teorema de não-clonagem apresentados a seguir.

Teorema 11. *(Teorema da não-clonagem) É impossível para qualquer dispositivo receber um estado quântico desconhecido e arbitrário como entrada e reproduzir exatamente o mesmo estado e uma cópia dele como saída. Ou seja, é impossível clonar um estado quântico.*

A demonstração do Teorema 11 pode ser encontrado em Nielsen e Chuang (2002). Tal teorema é uma limitação fundamental na mecânica quântica, que impede a clonagem exata de estados quânticos desconhecidos, sendo necessário utilizar emaranhamento quântico. O emaranhamento permite que dois ou mais qubits se tornem interligados de forma inseparável, criando uma relação quântica única. Essa propriedade é possível porque qualquer perturbação em um qubit emaranhado afeta instantaneamente o outro qubit emaranhado, o que permite detectar erros sem perturbar a informação original. Dessa forma, o uso de emaranhamento quântico é essencial para a detecção e correção de erros, tornando os CCEQ uma ferramenta fundamental para a segurança e confiabilidade da informação quântica.

Os postulados apresentados são conceitos fundamentais da mecânica quântica. O primeiro postulado estabelece que existe um espaço vetorial complexo associado a cada sistema físico fechado e que um estado é descrito por um vetor unitário. O segundo postulado descreve a evolução de um sistema quântico fechado como sendo controlada por um operador unitário. O terceiro postulado descreve como as medições são feitas na mecânica quântica, incluindo as equações para a probabilidade de um resultado de medição e o estado do sistema após a medição. O quarto postulado descreve como o espaço de estados de sistemas compostos é dado pelo produto tensorial dos espaços de estados dos sistemas individuais. Esses postulados formam a base da teoria quântica.

3 CÓDIGOS CORRETORES DE ERROS

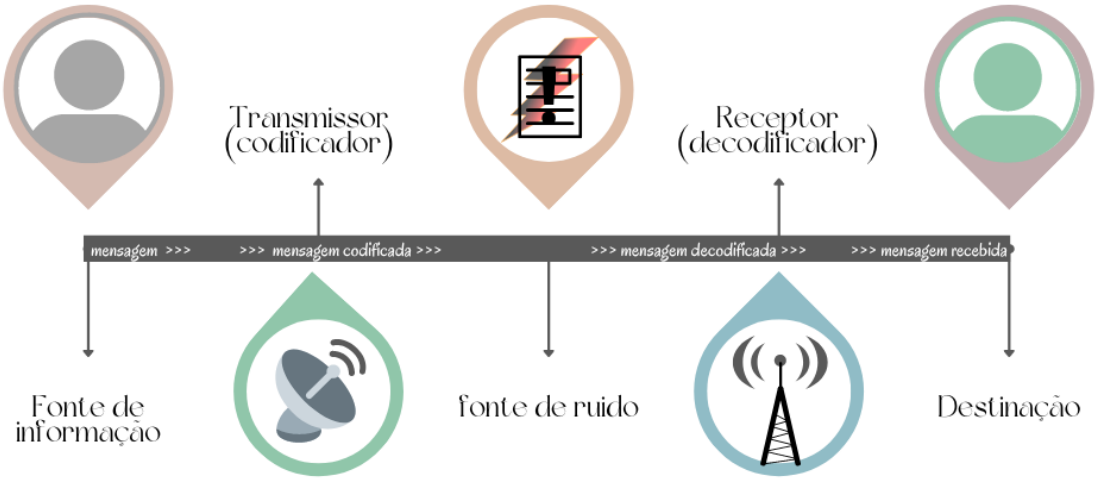
A Teoria da Informação, também conhecida como Teoria da Comunicação, é uma área da matemática e da engenharia que se dedica a estudar a quantificação, armazenamento e transmissão da informação. Ela aborda questões relacionadas à eficiência e qualidade da comunicação, incluindo a segurança da informação e a capacidade de detecção e correção de erros. Essa última é conhecida como Teoria de Códigos Corretores de Erros, a qual destina-se ao desenvolvimento de procedimentos para proteção de informações contra erros ou falhas nos processos de armazenamento e transmissão de dados, utilizando ferramentas matemáticas.

Imagine que você esteja em uma reunião importante no escritório, em que a pessoa que está falando diz coisas interessantes sobre o próximo trimestre, mas, dois colegas de trabalho começam a conversar animadamente ao seu lado e acabam tirando um pouco da sua atenção. Nessa situação, todos nós gostaríamos que por meio de alguma mágica fosse possível retirar o som da conversa de modo que apenas a voz do palestrante chegasse até os nossos ouvidos. Poderíamos imaginar que retirar os colegas da sala resolveria o problema e teríamos o caminho livre para o som da fala. No entanto, mesmo tomando esta atitude, chegariam provavelmente 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 pelo ruído, sendo uma forma de distorção ou interferência indesejada que afeta a qualidade da mensagem original, o que pode levar a erros na transmissão de informação.

De madeira mais simples, um código corretor de erros funciona codificando as informações de origem antes da transmissão da informação, e decodificando-as após a recepção. A codificação inclui a adição de informações adicionais, conhecidas como *redundância*, que permitem a detecção de erros. Se um erro for detectado durante a decodificação, ele pode ser corrigido pelo código corretor de erros, restaurando a informação original.

A figura a seguir, conhecido como diagrama de Shannon, apresenta de forma simplificada, os principais elementos envolvidos na transmissão de uma informação, também chamada de mensagem. A Figura 3 ilustra a relação entre a mensagem original, o ruído que pode interferir na transmissão e a mensagem recebida. A compreensão deste diagrama é fundamental para entender como o ruído pode afetar a qualidade da mensagem original e como a tecnologia pode ser utilizada para minimizar esses efeitos negativos.

Figura 3 – Diagrama de Shannon.



Fonte: Inspirado em Shannon (1948).

Códigos Corretores de Erros Clássicos (CCEC) e Códigos Corretores de Erros Quânticos (CCEQ) são duas abordagens para a proteção de informações contra erros. Embora compartilhem alguns princípios básicos, existem algumas diferenças importantes entre eles. Códigos Corretores de Erros Clássicos são baseados em bits, ou seja, em unidades de informação que podem ter apenas valores 0 ou 1. Em contrapartida, os Códigos Corretores de Erros Quânticos são baseados em qubits, que é o bit quântico, que pode representar 0 ou 1 ou estado de superposição e requer aspectos teóricos de álgebra linear e física quântica para seu desenvolvimento e compreensão.

3.1 CÓDIGOS CORRETORES DE ERROS CLÁSSICOS

A comunicação é um processo complexo e dinâmico que envolve a troca de informação entre duas ou mais pessoas. Mesmo com a evolução da tecnologia e a disponibilidade de novos meios de comunicação, ainda há espaço para os ruídos que podem prejudicar a precisão e a clareza da mensagem transmitida.

Existe uma ampla gama de CCEC, cada um deles projetado para atender a diferentes necessidades e demandas. Nesta análise, vamos nos concentrar em códigos lineares, em particular o código cíclico, baseado no estudo realizado em (HEFEZ; VILLELA, 2008), onde pode ser encontrado todas as demonstrações.

Para compreender a construção de um Código Corretor de Erro, é necessário conhecer alguns conceitos básicos, como alfabeto, palavra e comprimento, que serão apresentados a seguir.

Definição 45. *Código é um conjunto de símbolos usados na transmissão e recepção de mensa-*

gem.

Um conjunto finito A será chamado *alfabeto*. Denotaremos por $q = |A| \in \mathbb{N}$ o número de elementos de A. Quando o número de elementos do alfabeto de um código é q, diz-se que o código é q-ário. Como por exemplo o conjunto $\mathbb{Z}_2 = \{0,1\}$, que são os chamados códigos binários, amplamente utilizado na computação clássica, o qual utilizaremos neste trabalho.

Sequências finitas de símbolos do alfabeto chamaremos de palavras. O número de letras de uma palavra chama-se o seu comprimento. Para esse trabalho, consideraremos que todas as palavras terão o mesmo comprimento n. Estes códigos dizem-se em blocos, mas como todos os códigos que estudaremos serão em blocos, daqui em diante omitiremos esta palavra.

Exemplo 25. *Considere o seguinte exemplo de um código binário. Seja C um código que tenha quatro mensagens a ser enviadas pelo canal de comunicação de comprimento $n = 2$. No código binário, ao passar pelo codificador da fonte, as quatro mensagens, chamadas de códigos da fonte serão dadas por $C = \{00, 01, 10, 11\}$.*

Agora, apresentaremos a definição de distância de Hamming, e resultados para garantir a eficiência de um código. Richard W. Hamming foi um matemático e engenheiro de computação, conhecido por seu trabalho em codificação e Teoria da Informação.

Definição 46. *Seja $\mathbb{Z}_2$ um alfabeto e dois elementos $u = (u_1, \ldots, u_n)$ e $v = (v_1, \ldots, v_n)$ tal que $u, v \in \mathbb{Z}_2^n$, a distância de Hamming entre u e v é definida como*

$$d(u, v) = \sum_{i=1}^{n} |u_i - v_i|.$$

Observação 5. *A distância de Hamming é o número de mudanças (ou "erros") necessários para transformar uma palavra do código em outra. Em outras palavras, é o número de bits aos quais duas palavras diferem. Observe que a distância entre os elementos do código C definido no Exemplo 25 é definida como*

$$d(00{,}01) = 1, d(00{,}10) = 1, d(00{,}11) = 2, d(01{,}10) = 2, d(01{,}11) = 1 \text{ e } d(10{,}11) = 1.$$

A proposição abaixo afirma que a distância de Hamming é de fato uma métrica:

Proposição 25. *Dados $u, v \in \mathbb{Z}_2^n$, valem as seguintes propriedades:*

(i) Positividade: $d(u, v) \geq 0$, valendo a igualdade se, e somente se, $u = v$.

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

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

Dados um elemento $a \in \mathbb{Z}_2^n$ e um número real $t \geq 0$, definimos o disco e a esfera de centro em a e raio t como sendo, respectivamente, os conjuntos

$$D(a,t) = \{u \in \mathbb{Z}_2^n; d(u,a) \leq t\},$$

$$S(a,t) = \{u \in \mathbb{Z}_2^n; d(u,a) = t\},$$

Esses conjuntos são finitos e o próximo lema nos fornecerá as suas cardinalidades.

Lema 1. *Para todo $a \in \mathbb{Z}_2^n$ e todo número natural $r > 0$, temos que*

$$|D(a,r)| = \sum_{i=0}^{r} \begin{pmatrix} n \\ i \end{pmatrix} (q-1)^i.$$

onde q é o número de elementos de $\mathbb{Z}_2$.

Definição 47. *Seja C um código. A distância mínima de C é o número*

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

Exemplo 26. *Vamos considerar que o código C do Exemplo 25 ao passar pelo codificador do canal é transformado em $C = \{00101, 10110, 01001, 11010\}$, ou seja, após a implementação da redundância, o código do canal tem comprimento $n = 5$. Assim,*

$$d(00101, 10110) = 3, \qquad d(10110, 01001) = 5,$$
$$d(00101, 01001) = 2, \qquad d(10110, 11001) = 2,$$
$$d(00101, 11010) = 5, \qquad d(01001, 11010) = 3.$$

são todas as distâncias possíveis dos elementos do código. Podemos notar que pela Definição 47 que a distância mínima do código é $d = 2$.

Lema 2. *Seja C um código com distância mínima d. Se **c** e **c'** são palavras distintas de C, então*

$$D(\boldsymbol{c}, \kappa) \cap D(\boldsymbol{c'}, \kappa) = \varnothing.$$

Em um cenário de comunicação sujeito a ruídos e interferências, é comum que durante a transmissão alguns bits dos dados sejam alterados ou corrompidos, gerando erros nos dados recebidos. Os CCE são projetados de forma inteligente para detectar e corrigir tais erros, ou seja, detectar erros é identificar alterações nos dados transmitidos, enquanto corrigir erros envolve recuperar a informação original.

Teorema 12. *Seja C um código com distância mínima d. Então C pode corrigir até $\kappa = \left\lfloor \frac{d-1}{2} \right\rfloor$ erros e detectar até $d-1$ erros.*

A distância mínima é uma medida importante, pois quanto maior a distância mínima, menor a probabilidade de erro na transmissão de informação. Códigos com distância mínima alta são mais robustos a erros, pois mesmo que algum erro ocorra durante a transmissão, é mais provável que o receptor consiga corrigir o erro. Infelizmente, o código não é capaz de detectar erros com apenas uma ocorrência, pois qualquer tipo de erro resulta em uma mensagem que ainda pertence ao código. Por esse motivo, a redundância é fundamental para garantir a integridade da mensagem codificada. A demonstração do Teorema 12 pode ser encontrado em Hefez e Villela (2008).

O Exemplo 26 apresenta o código $C = \{00101, 10110, 01001, 11010\}$. A distância mínima deste código é igual a 2, o que significa que qualquer mudança em um dos bits do código resultará em pelo menos duas diferenças. A partir desta informação, podemos calcular a capacidade de correção e detecção de erros do código.

A capacidade de correção de erros é dada por $\kappa = \left\lfloor \frac{2-1}{2} \right\rfloor = \left\lfloor \frac{1}{2} \right\rfloor = 0$ erro, e a capacidade de detecção de erros é dada por $2 - 1 = 1$ erro.

Na figura 4 podemos visualizar que ao cometer um erro a mensagem recebida não pertencerá aos elementos do código, poderem não é possível saber qual é a mensagem original, visto que, tem mais de uma possibilidade com distância 1 dos elementos do código.

Assim, o código apresentado no Exemplo 26 é capaz de detectar 1 erro, mas não é capaz de corrigi-lo. Isso pode ser uma limitação significativa na eficiência da comunicação, pois erros não corrigidos podem levar a interpretações incorretas da mensagem.

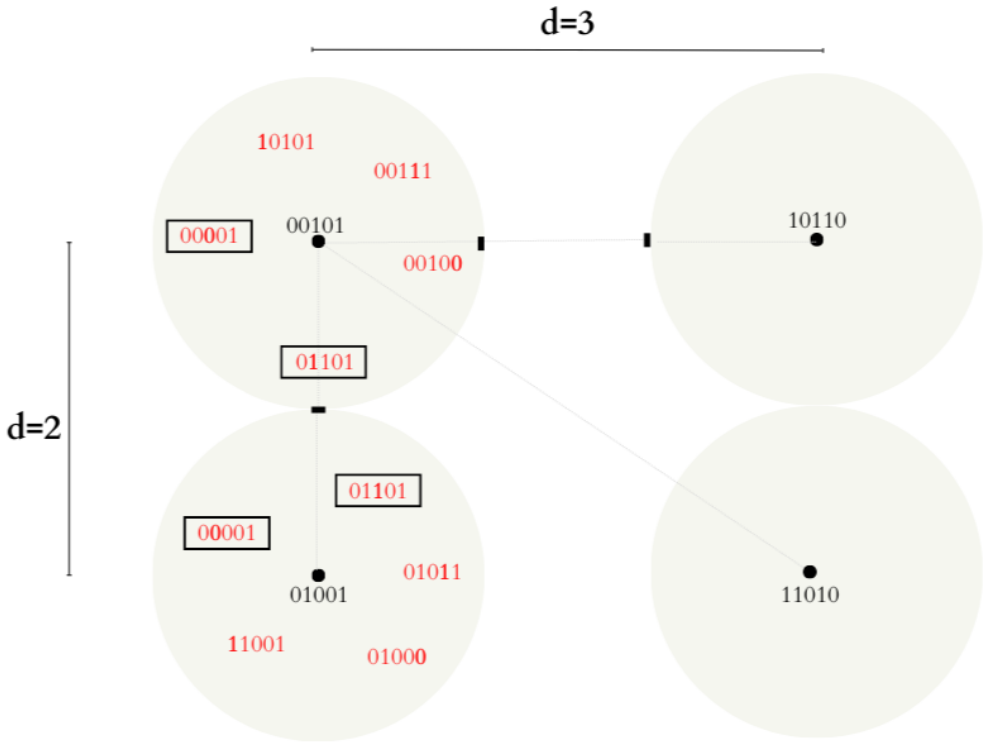
Definição 48. *Seja $C \subset A$ um código com distância mínima d, $c \in C$ palavras do código e seja $\kappa = \left\lfloor \frac{d-1}{2} \right\rfloor$. O código C será dito perfeito se*

$$\bigcup_{c \subset C} D(c, \kappa) = \mathbb{Z}_2^n.$$

Exemplo 27. *Código de Hamming (5, 2, 3). Seja C um código que tenha quatro mensagens a ser enviadas de comprimento $n = 5$, tal que $C = \{00000, 01011, 10110, 11101\}$. Assim,*

$$d(00000, 01011) = 3, \qquad d(01011, 10110) = 4,$$
$$d(00000, 10110) = 3, \qquad d(01011, 11101) = 3,$$
$$d(00000, 11101) = 4, \qquad d(10110, 11101) = 3$$

Figura 4 – Esquema da capacidade de detecção e correção de erro.



Fonte: Autoria própria.

são todas as distâncias do código. Podemos notar que pela Definição 47 a distância mínima do código é $d = 3$*. Pelo Teorema 12 a capacidade de correção de erros é dada por* $\kappa = \left\lfloor \frac{3-1}{2} \right\rfloor = \left\lfloor \frac{2}{2} \right\rfloor = 1$ *erro, e a capacidade de detecção de erros é dada por* $3 - 1 = 2$ *erros.*

A equivalência de códigos é uma relação entre dois códigos que permite que eles sejam considerados equivalentes, onde entende-se por, códigos equivalentes se pudermos transformar um no outro sem alterar suas propriedades, como sua capacidade de correção e detecção de erros. Esta transformação pode ser feita por meio de isometrias, que são funções que mantêm a distância de Hamming. Veremos a definição de equivalência de códigos e alguns resultados.

Definição 49. *Sejam* $\mathbb{Z}_2$ *um alfabeto e* n *um número natural. Diremos que uma função* $F : \mathbb{Z}_2^n \longrightarrow \mathbb{Z}_2^n$ *é uma isometria de* $\mathbb{Z}_2^n$ *se ela preserva distâncias de Hamming, isto é,*

$$d(F(\boldsymbol{x}), F(\boldsymbol{y})) = d(\boldsymbol{x}, \boldsymbol{y})$$

Para todos $x, y \in \mathbb{Z}_2^n$.

Definição 50. *Dados dois códigos* C *e* C' *em* $\mathbb{Z}_2^n$*, diremos que* C' *é equivalente a* C *se existir uma isometria* F *de* $\mathbb{Z}_2^n$ *tal que* $F(C) = C'$.

Teorema 13. *Sejam C e C' dois códigos em $\mathbb{Z}_2^n$ com $(x_1, \ldots, x_n) \in C$ elementos do código. Temos que C e C' são equivalentes se, e somente se, existem uma permutação π de $\{1, \ldots, n\}$ e bijeções $f_1, \ldots, f_n$ de A tais que*

$$C' = \{(f_{\pi(1)}(x_{\pi(1)}), \ldots, f_{\pi(n)}(x_{\pi(n)}))\}$$

O teorema acima é de extrema importância na teoria dos códigos, pois estabelece uma caracterização para códigos equivalentes. Dois códigos de comprimento n sobre um alfabeto A, cujos elementos são chamados de letras, são equivalentes se, e somente se, um deles pode ser obtido do outro mediante uma sequência de operações do tipo:

- Substituição de letras numa dada posição fixa em todas as palavras do código por meio de uma bijeção de $\mathbb{Z}_2$.
- Permutação das posições das letras em todas as palavras do código, mediante uma permutação fixa de $\{1, \ldots, n\}$.

3.1.1 Códigos Lineares

Os códigos lineares são conhecidos por sua eficiência e capacidade de corrigir erros, tornando-os uma escolha popular para aplicações críticas de comunicação.

Definição 51. *Um código $C \subset \mathbb{Z}_2^n$ será chamado de código linear se for um subespaço vetorial de $\mathbb{Z}_2^n$.*

De acordo com (WICKER; BHARGAVA, 1994), uma das principais vantagens dos códigos lineares é a facilidade de calcular sua distância mínima. Como um código linear é um subespaço vetorial, temos que o elemento neutro da adição no espaço vetorial, 0 pertence ao código C. Podemos então introduzir o seguinte:

Definição 52. *Dado $x = (x_1, x_2, \ldots, x_n) \in \mathbb{Z}_2^n$, define-se o peso de x como sendo o número inteiro*

$$\omega(x) := \left\{ \sum x_i \text{ para todo } i \text{ tal que } x_i \neq 0 \right\}.$$

Em outras palavras, temos que $\omega(x) = d(x,0)$, onde d representa a métrica de Hamming.

Definição 53. *O peso de um código linear C é o inteiro*

$$\omega(C) := \textit{min}\{\omega(x); x \in C \setminus \{0\}\}.$$

Proposição 26. *Seja $C \subset \mathbb{Z}_2^n$ um código linear com distância mínima d. Temos que*

(i) $d(x,y) = \omega(x-y),\ \forall\, x, y \in \mathbb{Z}_2^n$.

(ii) $d = \omega(C)$.

Por definição, para determinar a distância mínima de um código C que contém N palavras, é necessário calcular a distância $d(x,y)$ entre todos os $N = \frac{n(n-1)}{2}$ pares de palavras. Se o código C é linear, o teorema anterior nos informa que é suficiente calcular o peso $\omega(C)$ de $N-1$ palavras.

Exemplo 28. *Considere o código do Exemplo 26*

$$C = \{00101, 10110, 01001, 11010\}.$$

Note que calcular a distância mínima do código é determinar $\omega(C)$ de

$$N - 1 = 4 - 1 = 3$$

palavras, ou seja,

$$\omega(C)(00101 - 10110) = \omega(C)(10011) = 3;$$

$$\omega(C)(00101 - 01001) = \omega(C)(01100) = 2;$$

$$\omega(C)(00101 - 11010) = \omega(C)(11111) = 5.$$

Portando, a distância mínima de C é 2.

Definição 54. *Seja $\mathbb{Z}_2$ um corpo finito. Dois códigos lineares C e C' são linearmente equivalentes se existir uma isometria linear $T : \mathbb{Z}_2^n \longrightarrow \mathbb{Z}_2^n$ tal que $T(C) = C'$.*

Sejam $\mathbb{Z}_2$ um corpo finito com q elementos e $C \subset \mathbb{Z}_2^n$ um código linear. Chamaremos de parâmetros do código linear C à terna de inteiros (n, k, d), onde k é a dimensão de C sobre $\mathbb{Z}_2$, e d representa a distância mínima de C, que é também igual ao peso $\omega(C)$ do código C. Note que o número de elementos M de C é igual a q^k

Definição 55. *Seja $\mathcal{B} = \{v_1, \ldots, v_k\}$ uma base ordenada de C e considere a matriz G, cujas linhas são os vetores $v_i = (v_{i1}, \ldots, v_{in}), i = 1, \ldots, k$, isto é,*

$$G = \begin{bmatrix} v_1 \\ \vdots \\ v_k \end{bmatrix} = \begin{bmatrix} v_{11} & v_{12} & \ldots & v_{1n} \\ \vdots & \vdots & & \vdots \\ v_{k1} & v_{k2} & \ldots & v_{kn} \end{bmatrix}.$$

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

A *matriz geradora* de um código linear é uma matriz que descreve como cada palavra de código é formada a partir de uma combinação dos elementos do código acrescidos com suas respectivas redundâncias.

Proposição 27. *Considere a transformação linear definida por*

$$\begin{aligned} T: \ \mathbb{Z}_2^k &\longrightarrow \mathbb{Z}_2^n \\ x &\longmapsto xG \end{aligned}$$

Se $x = (x_1, \ldots, x_k)$, temos que

$$T(x) = xG = x_1v_1 + \ldots + x_kv_k,$$

logo $T(\mathbb{Z}_2^k) = C$. Podemos considerar $\mathbb{Z}_2^k$ como sendo o código fonte, C o código de canal e a transformação T, uma codificação.

Exemplo 29. *Considere a transformação linear,*

$$\begin{aligned} A: \ \mathbb{Z}_2^2 &\longrightarrow \mathbb{Z}_2^5 \\ (x_1, x_2) &\longmapsto (x_1, x_1 + x_2, x_1, x_1, x_1 + x_2). \end{aligned}$$

Aplicando a transformação A nos elementos $(1,0)$ e $(0,1)$ do conjunto $\mathbb{Z}_2^2$, obtemos

$$A(1,0) = (1, 1+0, 1, 1, 1+0) = (1, 1, 1, 1, 1), \quad A(0,1) = (0, 0+1, 0, 0, 0+1) = (0, 1, 0, 0, 1).$$

Assim, uma base para o espaço vetorial C pode ser dada por $\mathcal{B} = \{(1,1,1,1,1),(0,1,0,0,1)\}$. Podemos obter então todas as palavras com suas respectivas redundâncias a partir da matriz geradora dada por $G = \begin{bmatrix} 1 & 1 & 1 & 1 & 1 \\ 0 & 1 & 0 & 0 & 1 \end{bmatrix}$.

Agora, vamos determinar as palavras do código:

$$\begin{bmatrix} 0 & 0 \end{bmatrix} \cdot \begin{bmatrix} 1 & 1 & 1 & 1 & 1 \\ 0 & 1 & 0 & 0 & 1 \end{bmatrix} = \begin{bmatrix} 0 & 0 & 0 & 0 & 0 \end{bmatrix}$$

$$\begin{bmatrix} 0 & 1 \end{bmatrix} \cdot \begin{bmatrix} 1 & 1 & 1 & 1 & 1 \\ 0 & 1 & 0 & 0 & 1 \end{bmatrix} = \begin{bmatrix} 0 & 1 & 0 & 0 & 1 \end{bmatrix}$$

$$\begin{bmatrix} 1 & 0 \end{bmatrix} \cdot \begin{bmatrix} 1 & 1 & 1 & 1 & 1 \\ 0 & 1 & 0 & 0 & 1 \end{bmatrix} = \begin{bmatrix} 1 & 1 & 1 & 1 & 1 \end{bmatrix}$$

$$\begin{bmatrix} 1 & 1 \end{bmatrix} \cdot \begin{bmatrix} 1 & 1 & 1 & 1 & 1 \\ 0 & 1 & 0 & 0 & 1 \end{bmatrix} = \begin{bmatrix} 1 & 0 & 1 & 1 & 0 \end{bmatrix}$$

Assim, o código é dado por $C = \{00000, 11111, 01001, 10110\}$. *Sabendo que, a distância mínima de* C *é dada pelo menor valor entre essas distâncias, temos pelo Exemplo 28 que* $d = 2$, *com* $n = 5$ *o comprimento das palavras e* $k = 2$ *a dimensão de* C. *Então, o parâmetro desse código é* $(n, k, d) = (5, 2, 2)$.

Duas matrizes geradoras de um mesmo código C podem ser obtidas uma da outra por uma sequencia 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 56. *Diremos que uma matriz geradora* G *de um código* C *está na forma padrão se tivermos*

$$G = [Id_k|A],$$

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

Teorema 14. *Dado um código* C, *existe um código equivalente* C' *com matriz geradora na forma padrão.*

Exemplo 30. *Considere o código* C *do Exemplo 29, temos que a matriz geradora é dada por*

$$G = \begin{bmatrix} 1 & 1 & 1 & 1 & 1 \\ 0 & 1 & 0 & 0 & 1 \end{bmatrix} \quad L_1 - L_2 \Longrightarrow \quad G' = \begin{bmatrix} 1 & 0 & 1 & 1 & 0 \\ 0 & 1 & 0 & 0 & 1 \end{bmatrix}$$

Note que G' *está na forma padrão, ou seja,* $G' = [I|A]$ *onde* $A = \begin{bmatrix} 1 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix}$.

Definição 57. *Seja* $C \subset \mathbb{Z}_2^n$ *um código linear, definimos o complemento ortogonal de* C, *chamado de código dual, como sendo o conjunto*

$$C^{\perp} = \{v \in k^n; \langle v, u \rangle = 0, \quad \forall u \in C\}.$$

Os códigos duais são importantes no contexto dos códigos lineares, pois eles fornecem informações adicionais sobre a estrutura de um código linear e suas propriedades. Além, em muitos casos, o código dual é mais fácil de ser analisado e manipulado do que o próprio código.

Lema 3. *Se* $C \subset \mathbb{Z}_2^n$ *é um código linear, com matriz geradora* G, *então*

(i) $C^{\perp}$ *é um subespaço vetorial de* $\mathbb{Z}_2^n$*;*

(ii) $x \in C^{\perp} \iff Gx^t = 0$.

É possível corrigir erros em uma palavra do código usando uma matriz conhecida como Matriz Teste de Paridade H permitindo verificar se uma palavra pertence ou não ao código C, possibilitando a identificação e correção de erros durante a transmissão ou armazenamento de dados.

Proposição 28. *Seja* $C \subset \mathbb{Z}_2^n$ *um código de dimensão* k *com matriz geradora* $G = [Id_k|A]$*, na forma padrão. Então*

(i) *dim* $C^{\perp} = n - k$;

(ii) $H = [-A^t|Id_{n-k}]$ *é uma matriz geradora de* $C^{\perp}$.

Exemplo 31. *Pelo Exemplo 30 temos que a matriz teste de paridade é dada por*

$$H = [-A^t|I] = \begin{bmatrix} 1 & 0 & 1 & 0 & 0 \\ 1 & 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 & 1 \end{bmatrix}$$

Lema 4. *Seja* C *um código linear em* $\mathbb{Z}_2^n$*. Para toda permutação* ω *de* $\{1, \ldots, n\}$*, para todo* $c \in \mathbb{K}^*$ *e para todo* $j = 1, \ldots, n$ *temos que*

(i) $(T_\sigma(C))^{\perp} = T_\sigma(C^{\perp})$;

(ii) $(T_c^j(C))^{\perp} = T_{c^{-1}}^j(C^{\perp})$.

Proposição 29. *Sejam* C *e* D *dois códigos lineares em* $\mathbb{Z}_2^n$*. Se* C *e* D *são linearmente equivalentes, então* $C^{\perp}$ *e* $D^{\perp}$ *são linearmente equivalentes.*

Corolário 2. *Se* D *é um código lincar em* $\mathbb{Z}_2^n$ *de dimensão* k*, então* $D^{\perp}$ *é um código* $n - k$.

Lema 5. *Suponha que* C *seja um código de dimensão* k *em* $\mathbb{Z}_2^n$ *com matriz geradora* G*. Uma matriz* H *de ordem* $(n-k) \times n$*, com coeficientes em* $\mathbb{Z}_2$ *e com linhas linearmente independentes, é uma matriz geradora de* $C^{\perp}$ *se, e somente se,*

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

Corolário 3. $(C^{\perp})^{\perp} = C$.

Proposição 30. *Seja C um código linear e suponhamos que H seja uma matriz geradora de $C^{\perp}$. Temos então que*

$$v \in C \iff Hv^t = 0.$$

Proposição 31. *Seja H a matriz teste de paridade de um código C. Temos que o peso de C é maior do que ou igual a s se, e somente se, quaisquer $s-1$ colunas de H são linearmente independentes.*

Teorema 15. *Seja H a matriz teste de paridade de um código C. Temos que o peso de C é igual a s se, e somente se, quaisquer $s-1$ colunas de H são linearmente independentes e existem s colunas de H linearmente dependentes.*

Corolário 4. *(Cota de Singleton) Os parâmetros (n,k,d) de um código linear satisfazem à desigualdade*

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

Proposição 32. *Todo código de Hamming é perfeito.*

Proposição 33. *Os parâmetros do código $R(1,m)$ são $(2^m, m+1, 2^{m-1})$.*

Lema 6. *Seja C um código linear em $\mathbb{Z}_2^n$ com capacidade de correção κ. Se $r \in \mathbb{Z}_2^n$ e $c \in C$ são tais que $d(c,r) \leq \kappa$, então existe um único vetor e com $\omega(e) \leq \kappa$, cuja síndrome é igual à síndrome de r e tal que $c = r - e$.*

Algoritmo 1: decodificação em códigos corretores de um erro. Seja H a matriz teste de paridade do código C e seja r um vetor recebido. (Suponha $d \geq 3$.)
(i) Calcule Hr^t. (ii) Se $Hr^t = 0$, aceite r como sendo a palavra transmitida. (iii) Se $Hr^t = s^t \neq 0$, compare s^t com as colunas de H. (iv) Se existirem i e α tais que $s^t = \alpha h^i k$, para $\alpha \in H$, então e é a n-upla com α na posição i e zeros nas outras posições. Corrija r pondo $c = r - e$. (v) Se o contrário de (iv) ocorrer, então mais de um erro foi cometido.

Vejamos um exemplo da execução nesse algoritmo. Note que o Exemplo 29 não é possível de ser aplicado, pois a distância miníma do código é $d = 2$ e para o algoritmo é necessário que $d \geq 3$.

Exemplo 32. *Considere um código linear* $C = \{00000, 01111, 10110, 11001\}$ *dado a partir da matriz geradora* $G = \begin{bmatrix} 1 & 0 & 1 & 1 & 0 \\ 0 & 1 & 1 & 1 & 1 \end{bmatrix}$. *Note que* G *está na forma padrão, assim a matriz teste de paridade é dado por* $H = \begin{bmatrix} 1 & 1 & 1 & 0 & 0 \\ 1 & 1 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 & 1 \end{bmatrix}$.

Pela Proposição 26 temos que a distância mínima de C *é dada por*

$$\omega(00000 - 01111) = 4, \;\; \omega(00000 - 10110) = 3, \;\; \omega(00000 - 11001) = 3.$$

Assim, a distância mínima de C *é dada pelo menor valor entre essas distâncias, ou seja,* 3*, e o parâmetro desse código é* $(n, k, d) = (5, 2, 3)$.

Temos que, a capacidade de correção de erros é dada por $\kappa = \left\lfloor \frac{3-1}{2} \right\rfloor = \left\lfloor \frac{2}{2} \right\rfloor = 1$ *erro, e a capacidade de detecção de erros é dada por* $3 - 1 = 2$ *erros.*

Fazendo o processo de decodificação como orientado na Proposição 30, obteremos a síndrome igual ao vetor nulo, veja a seguir.

$$\begin{bmatrix} 1 & 1 & 1 & 0 & 0 \\ 1 & 1 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 & 1 \end{bmatrix} \cdot \begin{bmatrix} 0 \\ 0 \\ 0 \\ 0 \\ 0 \end{bmatrix} = \begin{bmatrix} 0 \\ 0 \\ 0 \end{bmatrix} \qquad \begin{bmatrix} 1 & 1 & 1 & 0 & 0 \\ 1 & 1 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 & 1 \end{bmatrix} \cdot \begin{bmatrix} 1 \\ 0 \\ 1 \\ 1 \\ 0 \end{bmatrix} = \begin{bmatrix} 0 \\ 0 \\ 0 \end{bmatrix}$$

$$\begin{bmatrix} 1 & 1 & 1 & 0 & 0 \\ 1 & 1 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 & 1 \end{bmatrix} \cdot \begin{bmatrix} 0 \\ 1 \\ 1 \\ 1 \\ 1 \end{bmatrix} = \begin{bmatrix} 0 \\ 0 \\ 0 \end{bmatrix} \qquad \begin{bmatrix} 1 & 1 & 1 & 0 & 0 \\ 1 & 1 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 & 1 \end{bmatrix} \cdot \begin{bmatrix} 1 \\ 1 \\ 0 \\ 0 \\ 1 \end{bmatrix} = \begin{bmatrix} 0 \\ 0 \\ 0 \end{bmatrix}$$

*Suponha que um erro é cometido, ou seja, a mensagem enviada é 01111 e a mensagem recebida sendo 0111**0**, ao passar pelo canal de decodificação, temos:*

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

Pelo algoritmo, temos que a síndrome s é igual a quinta coluna da matriz de paridade. E assim segue do Lema 6 que a palavra enviada foi,

$$c = r - e = 01110 - 00001 = 01111.$$

Lema 7. *Os vetores u e v de $\mathbb{Z}_2^n$ têm a mesma síndrome se, e somente se, $u \in v + C$.*

Proposição 34. *Seja C um (n,k)-código linear. Temos que*

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

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

(iii) $\cup_{v \in \mathbb{Z}_2^n}(v + C) = \mathbb{Z}_2^n$;

(iv) $|v + C| = |C| = q^k$

Definição 58. *Seja $v \in \mathbb{Z}_2^n$. Chamaremos de classe lateral o conjunto*

$$v + C = \{v + c; c \in C\}.$$

Onde,

$$v + C = C \Leftrightarrow v \in C$$

Definição 59. *Um vetor de peso mínimo numa classe lateral é chamado de elemento líder dessa classe.*

Proposição 35. *Seja C um código linear em $\mathbb{Z}_2^n$ com distância mínima d. Se $u \in \mathbb{Z}_2^n$ é tal que*

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

então u é o único elemento líder de sua classe.

Para achar líderes de classe, selecionamos todos os elementos u tais que $\omega(u) \leq \left\lfloor \frac{d-1}{2} \right\rfloor$. Cada um desses elementos é líder de uma e somente uma classe. Esses líderes são todos aqueles de peso $\leq \left\lfloor \frac{d-1}{2} \right\rfloor$.

Vamos agora discutir um algoritmo de correção de mensagem que tenham sofrido um número de erros menor ou igual à capacidade de correção do código, que é $\kappa = \left\lfloor \frac{d-1}{2} \right\rfloor$.

Determine todos os elementos de u de $\mathbb{Z}_2^n$, tal que $\omega(u) \leq \kappa$. Em seguida, calcule as síndromes desses elementos e coloque esses dados numa tabela.

Algoritmo 2: Decodificação
Seja r uma palavra recebida.
(i) Calcule a síndrome $s^t = Hr^t$.
(ii) Se s está na tabela, seja l o elemento líder da classe determinada por s; troque r por $r - l$.
(iii) Se s não está na tabela, então na mensagem recebida foram cometidos mais de κ erros.

Observação 6. *Dados r e e, respectivamente, a mensagem transmitida e o vetor erro. Como $He^t = Hr^t$, temos que a classe lateral onde e se encontra está determinada pela síndrome de r. Se $\omega(e) \leq \kappa$, temos que e é o único elemento líder de suas classe e, portanto, é conhecido e se encontra na tabela. Consequentemente, pelo Lema 6, $c = r - e = r - l$ é determinado.*

Observação 7. *Decodificar o código através do algoritmo supracitado, em síntese é calcular as síndromes e líderes antecipadamente, prevendo todos os possíveis erros.*

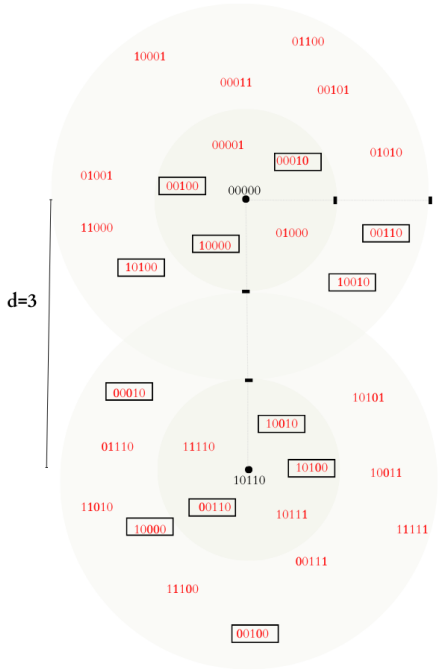
Dado o Código do Exemplo 32 temos que como a $d = 3$ os líderes são todos aqueles menores do que ou iguais a $\left\lfloor \frac{d-1}{2} \right\rfloor = 1$. Assim,

$$l = \{00000, 00001, 00010, 00100, 01000, 10000\}$$

e determinar as síndromes é considerar c como sendo uma palavra transmitida, fazendo $c + l$ temos todas as possibilidades para r, assim obter s é calcular Hr^t. Onde obtemos todos elementos da tabela supracitado como:

Líder	Síndrome
00000	000
00001	001
00010	010
00100	100
01000	111
10000	110

Figura 5 – Esquema da capacidade de detecção e correção de erros



Fonte: Autoria própria.

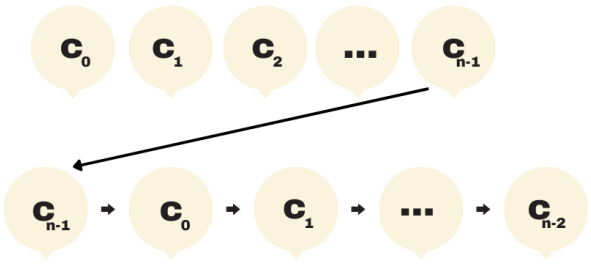
Como ilustrado na Figura 5, erros em duas posições simultaneamente o código não é capaz de corrigir, pois o código não consegue distinguir em qual posição ocorreu o erro.

3.1.2 Códigos Cíclicos

Os códigos cíclicos são uma importante classe de Códigos Corretores de Erros. Segundo (LIN; COSTELLO, 2004), os códigos cíclicos foram os primeiros códigos de bloco a serem descobertos e ainda hoje são de grande importância prática. Eles são fáceis de implementar em hardware e têm uma estrutura matemática simples que permite uma análise detalhada de seu desempenho. Alguns exemplos conhecidos de códigos cíclicos incluem os códigos de Hamming binários, os códigos de Golay, os códigos BCH, Reed-Solomon e Goppa. Devido às suas características únicas, os códigos cíclicos têm sido amplamente utilizados em diversas aplicações, incluindo sistemas de transmissão de dados via satélite, modems, redes de computadores e sistemas de armazenamento de dados.

Continuaremos representando as coordenadas de um vetor em $\mathbb{Z}_2^n$ por $(x_0, \ldots, x_{n-1})$.

Figura 6 – Esquema de uma permutação cíclica



Fonte: Autoria própria.

Chamaremos de R_n o Anel das classes residuais em $\mathbb{Z}_2[X]$ módulo X^{n-1}, isto é,

$$R_n = \mathbb{Z}_2[X]_{(X^n-1)}.$$

Temos que, todo código linear $C \subset \mathbb{Z}_2$ pode ser transportado para R_n mediante o isomorfismo ν. Considere ν uma transformação linear dada por

$$\begin{aligned} \nu : \mathbb{Z}_2^n &\longrightarrow R_n \\ (a_0, \ldots, a_{n-1}) &\longmapsto [a_0 + a_1X + a_2 + \ldots + a_{n-1}X^{n-1}]. \end{aligned}$$

Definição 60. *Um código linear $C \subset \mathbb{Z}_2^n$ será chamado de código cíclico se, para todo $c = (c_o, \ldots, c_{n-1})$ pertencente a C, o vetor $(c_{n-1}, c_o, \ldots, c_{n-2})$ pertence a C.*

Em síntese, pode-se afirmar que um código C é considerado cíclico quando uma permutação cíclica $T : C \to C$ pode ser aplicada a cada vetor $c = (c_o, \ldots, c_{n-1})$, resultando no vetor $T(c_o, \ldots, c_{n-1}) = (c_{n-1}, c_o, \ldots, c_{n-2})$, conforme ilustrado na Figura 6.

Exemplo 33. *O código*

$$C = \{0000000, 1011101, 1101110, 0110111, 1011011, 1101101, 1110110, 0111011\} \subset \mathbb{Z}_2^7$$

é cíclico, pois:

$$T(0000000) = 0000000 \in C$$

$$T(1011101) = 1101110 \in C$$

$$T(1101110) = 0110111 \in C$$

$$T(0110111) = 1011011 \in C$$

$$T(1011011) = 1101101 \in C$$

$$T(1101101) = 1110110 \in C$$

$$T(1110110) = 0111011 \in C$$

$$T(0111011) = 1011101 \in C$$

Lema 8. *Seja V um subespaço vetorial de R_n. Então, V é um ideal de R_n se, e somente se, V é fechado pela multiplicação por $[X]$.*

Teorema 16. *Um subespaço C de $\mathbb{Z}_2^n$ é um código cíclico se, e somente se, $\nu(C)$ um ideal de R_n.*

O fato de que $\nu(C)$ é um ideal de R_n significa que ele que preserva as propriedades de anel, o que pode ser útil em aplicações de codificação de dados.

Teorema 17. *Seja $I = I([g(X)])$, onde $g(X)$ é um divisor de $X^n - 1$ de grau s. Temos que $[g(X)], [Xg(X)], [X^2g(X)], \ldots, [X^{n-s-1}g(X)]$ é uma base de I como espaço vetorial sobre $\mathbb{Z}_2$.*

Qualquer elemento de I pode ser expresso como uma combinação linear de $[g(X)], [Xg(X)], [X^2g(X)], \ldots, [X^{n-s-1}g(X)]$. O teorema permite uma representação eficiente do código cíclico como uma matriz geradora em que veremos mais adiante.

Corolário 5. *Dado um código cíclico C, existe $v \in C$ tal que $C =< v >$.*

Corolário 6. *Seja $g(X) = g_0 + g_1X + \ldots + g_sX^s$ um divisor de $X^n - 1$ de grau s. Se $I = I([g(X)])$, então*

$$dim_K I = n - s,$$

e o código $C = \nu^{-1}(I)$ tem matriz geradora

$$G = \begin{bmatrix} \nu^{-1}([g(X)]) \\ \nu^{-1}([Xg(X)]) \\ \vdots \\ \nu^{-1}([X^{n-s-1}g(X)]) \end{bmatrix} = \begin{bmatrix} g_0 & g_1 & \ldots & g_s & 0 & \ldots & 0 \\ 0 & g_0 & g_1X & \ldots & g_s & \ldots & 0 \\ \vdots & \vdots & \vdots & & \vdots & & \vdots \\ 0 & \ldots & 0 & g_0 & \ldots & \ldots & g_s \end{bmatrix}$$

De acordo com o Corolário 6, qualquer ideal I de $\mathbb{Z}_2[X]$ que contém $X^n - 1$ é gerado por polinômios mônicos que dividem $X^n - 1$. Além disso, estabelece que o comprimento de cada palavra código da fonte é k e o comprimento de cada palavra do código de canal é n, então temos que $gr(g(X)) = n - k$, onde $gr(g(X))$ é o grau de $g(X)$. Isso significa que o número de bits de redundância em um código cíclico é dado pelo grau do polinômio gerador.

Exemplo 34. *Considere o código fonte dado por* $\mathbb{Z}_2^2 = \{(00), (01), (10), (11)\}$ *com*

$$v_1 = 00, v_2 = 01, v_3 = 10 \text{ e } v_4 = 11.$$

A representação dos códigos do canal na forma polinomial é dado por

$$v_1(X) = 0X + 0, v_2(X) = 0X + 1, v_3(X) = 1X + 0 \text{ e } v_4(X) = 1X + 1.$$

Vamos obter um código C *cíclico de comprimento* $n = 6$ *e dimensão* $k = 2$*. Assim,* $X^n - 1 = X^6 - 1$.

Note que, pelo Exemplo 2 o polinômio $X^6 - 1$ *sobre* $\mathbb{Z}_2^2$ *é fatorado como*

$$(X - 1) \cdot (X + 1) \cdot (X^4 + X^2 + 1).$$

Pelo Corolário 6 temos que $g(X)|X^6 - 1$*, como* $gr(g(X)) = n - k = 6 - 2 = 4$ *temos*

$$g(X) = X^4 + X^2 + 1 = X^4 + 0X^3 + X^2 + 0X + 1$$

Assim, os coeficientes de $1 + 0X + 1X^2 + 0X^3 + 1X^4$ *são utilizados para determinar a primeira linha da matriz* $g(X)$*, ou seja* 10101 *complementando de zeros até ter a quantidade de colunas igual a* n.

$$g(X) = \begin{bmatrix} 1 & 0 & 1 & 0 & 1 & 0 \\ 0 & 1 & 0 & 1 & 0 & 1 \end{bmatrix}$$

Note que $g(X)$ *está na forma padrão com* $A = \begin{bmatrix} 1 & 0 & 1 & 0 \\ 0 & 1 & 0 & 1 \end{bmatrix}$*. Vamos obter a codificação do canal para* $\mathbb{Z}_2^2 = \{00, 01, 10, 11\}$*. Logo,*

$$\begin{bmatrix} 0 & 0 \end{bmatrix} \cdot \begin{bmatrix} 1 & 0 & 1 & 0 & 1 & 0 \\ 0 & 1 & 0 & 1 & 0 & 1 \end{bmatrix} = \begin{bmatrix} 0 & 0 & 0 & 0 & 0 & 0 \end{bmatrix}$$

$$\begin{bmatrix} 0 & 1 \end{bmatrix} \cdot \begin{bmatrix} 1 & 0 & 1 & 0 & 1 & 0 \\ 0 & 1 & 0 & 1 & 0 & 1 \end{bmatrix} = \begin{bmatrix} 0 & 1 & 0 & 1 & 0 & 1 \end{bmatrix}$$

$$\begin{bmatrix} 1 & 0 \end{bmatrix} \cdot \begin{bmatrix} 1 & 0 & 1 & 0 & 1 & 0 \\ 0 & 1 & 0 & 1 & 0 & 1 \end{bmatrix} = \begin{bmatrix} 1 & 0 & 1 & 0 & 1 & 0 \end{bmatrix}$$

$$\begin{bmatrix} 1 & 1 \end{bmatrix} \cdot \begin{bmatrix} 1 & 0 & 1 & 0 & 1 & 0 \\ 0 & 1 & 0 & 1 & 0 & 1 \end{bmatrix} = \begin{bmatrix} 1 & 1 & 1 & 1 & 1 & 1 \end{bmatrix}$$

Portando, $C = \{000000, 010101, 101010, 111111\}$*, com sua representação polinomial dada por* $C = \{0, X + X^3 + X^5, 1 + X^2 + X^4, 1 + X + X^2 + X^3 + X^4 + X^5\}$.

Pela Proposição 26 temos que a distância mínima de C *é dada por*

$$\omega(00000 - 010101) = 3, \omega(00000 - 101010) = 3, \omega(00000 - 111111) = 6.$$

Assim, a distância mínima de C *é dada pelo menor valor entre essas distâncias, ou seja,* 3*, e o parâmetro desse código é* $(n, k, d) = (6, 2, 3)$.

Temos que, a capacidade de correção de erros é dada por $\kappa = \left\lfloor \frac{3-1}{2} \right\rfloor = \left\lfloor \frac{2}{2} \right\rfloor = 1$ *erro, e a capacidade de detecção de erros é dada por* $3 - 1 = 2$ *erros.*

Teorema 18. *Seja* $C = \nu^{-1}(I)$ *um código cíclico, onde* $I = I([g(X)])$*, com* $g(X)$ *um divisor de* $X^n - 1$ *de grau* s*. Então* $C^{\perp}$ *é cíclico e* $C^{\perp}\nu^{-1}(J)$*, onde* $J = I([h^*(X)])$.

Corolário 7. *A matriz teste de paridade de* $C = \nu^{-1}(I)$*, em que* $I = I([g(X)])$*, é dada por*

$$H = \begin{bmatrix} h_{n-s} & h_{n-s-1} & \dots & h_0 & 0 & \dots & 0 \\ 0 & h_{n-s} & h_{n-s-1} & \dots & h_0 & \dots & 0 \\ \vdots & \vdots & \vdots & & \vdots & & \vdots \\ 0 & \dots & 0 & h_{n-s} & \dots & \dots & h_0 \end{bmatrix}$$

onde

$$\frac{X^n - 1}{g(X)} = h_0 + h_1 X + \ldots + h_{n-s} X^{n-s}.$$

Exemplo 35. *Efetuando a divisão*

$$\begin{array}{r|l} X^6 - 1 & X^4 + X^2 + 1 \\ \hline 0 & X^2 - 1 \end{array}$$

e considerando que estamos operando em $\mathbb{Z}_2$*, temos que* $X^2 - 1 = X^2 + 1$

Assim, $h(X) = X^2 + 1$ *é polinômio de paridade de* C*. Isso implica que a matriz teste de paridade para* C *é:*

$$h(X) = \begin{bmatrix} 1 & 0 & 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 & 0 & 1 \end{bmatrix}.$$

Teorema 19. *Seja $C \subset \mathbb{Z}_2^n$ um código cíclico. Suponhamos que $C = \nu^{-1}(I)$, onde $I = I([g(X)])$, com $g(X)$ um divisor de $X^n - 1$ de grau s. Seja R a matriz $(n-s) \times s$ cuja i-ésima linha é*

$$R_i = -\mu^{-1}(r_i(X)), \quad 1 \leq i \leq n-s,$$

onde $r_i(X)$ é o resto da divisão de X^{s-1+i} por $g(X)$. Então, $(Id_{n-s}|R)$ é uma matriz geradora de C.

Teorema 20. *Seja $C \subset \mathbb{Z}_2^n$ um código cíclico gerado por um polinômio mônico $g(X)$ de graus com matriz geradora na forma padrão $(Id_{n-s}|R)$ e matriz teste de paridade $H = [Id_s| - R^t]$. Se $v = (v_0, \ldots, v_{n-1})E \in K^n$, então a síndrome de v com relação à matriz H é dada por*

$$\mu^{-1}(r(X)),$$

onde $r(X)$, é o resto da divisão de $v_0 + v_1X + \ldots + v_{n-1}X^{n-1}$ por $g(X)$.

Note que $h(X)$ não está na forma padrão. Colocando na forma padrão $H = [Id_s| - R^t]$, temos

$$h'(X) = \begin{bmatrix} 1 & 0 & 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 & 0 & 1 \end{bmatrix}$$

onde cada coluna de $h'(X)$ equivale aos restos das divisões das mensagens recebidas com erros de no máximo 2 dígitos pelo polinômio gerador $g(X) = 1 + X^2 + X^4$, ou seja, $r = \{1000, 0100, 0010, 0001, 1010, 0101\}$, em linguagem polinomial temos, $r(X) = \{1, X, X^2, X^3, 1 + X^2, X + X^3\}$, e suas respectivas síndromes $s(r(X)) = \{1, X, X^2, X^3, X^4, X^5\}$

Exemplo 36. *Dado o código do Exemplo 34*

$$C = \{000000, 010101, 101010, 111111\}.$$

Suponha que a mensagem transmitida seja 010101. *Na forma polinomial é dado por*

$$0 + 1X + 0X^2 + 1X^3 + 0X^4 + 1X^5 = X + X^3 + X^5.$$

Fazendo a divisão $\frac{c(X)}{g(X)}$, temos:

$$\begin{array}{c|c} X^5+X^3+X & X^4+X^2+1 \\ \hline 0 & X \end{array}$$

A mensagem recebida $0101010 \in \mathbb{Z}_2^6$*, pelo Teorema 19 como* $r(X)=0$ *temos que a síndrome é* 0000*, donde podemos afirmar que este vetor pertence ao código* C*.*

Suponha um erro do tipo $0\mathbf{0}0101$*, ou seja, um erro no segundo bit.*

A palavra transmitida na forma polinomial é dado por

$$0+0X+0X^2+1X^3+0X^4+1X^5=X^3+X^5.$$

Resolvendo o quociente $\frac{c(X)}{g(X)}$*, temos:*

$$\begin{array}{c|c} X^5+X^3 & X^4+X^2+1 \\ \hline -X & X \end{array}$$

A mensagem recebida $0\mathbf{0}0101 \notin \mathbb{Z}_2^6$*, como* $r(X)=X$*, temos que,* $r=0100$*, donde podemos afirmar pelo Teorema 20 que essa síndrome pertence a segunda coluna da matriz de paridade* $h'(x)$*, o que significa que houve um erro no segundo bit, com* $s(r(X))=X$*.*

Para obter a mensagem original basta calcular

$$i(X)=c(X)-s(r(X))=X^3+X^5-X=X+X^3+X^5,$$

que equivale a mensagem 010101*, onde* $i(X)$ *é a mensagem inicial e* $c(X)$ *a mensagem recebida.*

Suponha novamente um erro do tipo $10101\mathbf{1}$*, ou seja, um erro no sexto bit.*

A palavra transmitida na forma polinomial é dado por

$$1+0X+1X^2+0X^3+1X^4+1X^5=1+X^2+x^4+x^5.$$

Resolvendo o quociente $\frac{c(X)}{g(X)}$*, temos:*

$$\begin{array}{c|c} X^5+X^4+X^2+1 & X^4+X^2+1 \\ \hline X^3+X & X+1 \end{array}$$

A mensagem recebida $10101\mathbf{1} \notin \mathbb{Z}_2^6$*, como* $r(X)=X+X^3$*, temos que,* $r=0101$*, donde podemos afirmar pelo Teorema 20 que essa síndrome pertence a sexta coluna da matriz de paridade* $h'(x)$*, o que significa que houve um erro no sexto bit, com* $s(r(X))=X^5$*.*

Para obter a mensagem original basta calcular

$$i(X)=c(X)-s(r(X))=1+X^2+X^4+X^5-(X^5)=1+X^2+X^4,$$

que equivale a mensagem 101010*.*

Exemplo 37. *Considere o Código Cíclico (7, 4, 3). As mensagens que se deseja enviar são:*

$$\{SIGA, DIREITA, ESQUERDA, 1, 2, 3, 4, 5, 6, 7, 8, 9, 10\}$$

onde será codificada para o código fonte sendo

$$\{1110, 1101, 0110, 0010, 1010, 1011, 1000, 0100, 0011, 1100, 0111, 0001, 1001\}.$$

O código tem comprimento $n = 7$ e dimensão $k = 4$.

Note que, pela Observação 1 o polinômio $X^7 - 1$ sobre $\mathbb{Z}_2^2$ é fatorado como

$$X^7 - 1 = (X - 1) \cdot (X^3 + X^2 + 1) \cdot (X^3 + X + 1).$$

Pelo Corolário 6 temos que $g(X)|X^7 - 1$, como $gr(g(X)) = n - k = 7 - 4 = 3$ temos que

$$g(X) = X^3 + X^2 + 1 = 1 + 0X + 1X^2 + 1X^3 + 0X^4 + 0X^5 + 0X^6$$

ou

$$g(X) = X^3 + X + 1 = 1 + 1X + 0X^2 + 1X^3 + 0X^4 + 0X^5 + 0X^6.$$

Sem perda de generalidade, tomaremos $g(X) = X^3 + X + 1$. Assim, os coeficientes de $1 + 1X + 0X^2 + 1X^3 + 0X^4 + 0X^5 + 0X^6$ são utilizados para determinar a primeira linha da matriz $g(X)$, ou seja 1101000. Logo,

$$g(X) = \begin{bmatrix} 1 & 1 & 0 & 1 & 0 & 0 & 0 \\ 0 & 1 & 1 & 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 1 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 & 1 & 0 & 1 \end{bmatrix}$$

Note que $g(X)$ não está na forma padrão. Para deixar a matriz $g(X)$ na forma padrão, ou seja, escrever $g(X) = [I|A]$ é necessário fazer uma sequência de operações do tipo: permutação de duas linhas, multiplicação de uma linha por um escalar não nulo e adição de um múltiplo escalar de uma linha a outra. Assim,

$$g'(X) = \begin{bmatrix} 1 & 0 & 0 & 0 & 1 & 1 & 0 \\ 0 & 1 & 0 & 0 & 0 & 1 & 1 \\ 0 & 0 & 1 & 0 & 1 & 1 & 1 \\ 0 & 0 & 0 & 1 & 1 & 0 & 1 \end{bmatrix}$$

Agora, determinaremos o código do canal, ou seja, adicionando as redundâncias necessárias.

$$\begin{bmatrix}1 & 1 & 1 & 0\end{bmatrix} \cdot \begin{bmatrix}1 & 0 & 0 & 0 & 1 & 1 & 0\\ 0 & 1 & 0 & 0 & 0 & 1 & 1\\ 0 & 0 & 1 & 0 & 1 & 1 & 1\\ 0 & 0 & 0 & 1 & 1 & 0 & 1\end{bmatrix} = \begin{bmatrix}1 & 1 & 1 & 0 & 0 & 1 & 0\end{bmatrix}$$

$$\begin{bmatrix}1 & 1 & 0 & 1\end{bmatrix} \cdot \begin{bmatrix}1 & 0 & 0 & 0 & 1 & 1 & 0\\ 0 & 1 & 0 & 0 & 0 & 1 & 1\\ 0 & 0 & 1 & 0 & 1 & 1 & 1\\ 0 & 0 & 0 & 1 & 1 & 0 & 1\end{bmatrix} = \begin{bmatrix}1 & 1 & 0 & 1 & 0 & 0 & 0\end{bmatrix}$$

$$\begin{bmatrix}0 & 1 & 1 & 0\end{bmatrix} \cdot \begin{bmatrix}1 & 0 & 0 & 0 & 1 & 1 & 0\\ 0 & 1 & 0 & 0 & 0 & 1 & 1\\ 0 & 0 & 1 & 0 & 1 & 1 & 1\\ 0 & 0 & 0 & 1 & 1 & 0 & 1\end{bmatrix} = \begin{bmatrix}0 & 1 & 1 & 0 & 1 & 0 & 0\end{bmatrix}$$

$$\begin{bmatrix}0 & 0 & 1 & 0\end{bmatrix} \cdot \begin{bmatrix}1 & 0 & 0 & 0 & 1 & 1 & 0\\ 0 & 1 & 0 & 0 & 0 & 1 & 1\\ 0 & 0 & 1 & 0 & 1 & 1 & 1\\ 0 & 0 & 0 & 1 & 1 & 0 & 1\end{bmatrix} = \begin{bmatrix}0 & 0 & 1 & 0 & 1 & 1 & 1\end{bmatrix}$$

$$\begin{bmatrix}1 & 0 & 1 & 0\end{bmatrix} \cdot \begin{bmatrix}1 & 0 & 0 & 0 & 1 & 1 & 0\\ 0 & 1 & 0 & 0 & 0 & 1 & 1\\ 0 & 0 & 1 & 0 & 1 & 1 & 1\\ 0 & 0 & 0 & 1 & 1 & 0 & 1\end{bmatrix} = \begin{bmatrix}1 & 0 & 1 & 0 & 0 & 0 & 1\end{bmatrix}$$

$$\begin{bmatrix}1 & 0 & 1 & 1\end{bmatrix} \cdot \begin{bmatrix}1 & 0 & 0 & 0 & 1 & 1 & 0\\ 0 & 1 & 0 & 0 & 0 & 1 & 1\\ 0 & 0 & 1 & 0 & 1 & 1 & 1\\ 0 & 0 & 0 & 1 & 1 & 0 & 1\end{bmatrix} = \begin{bmatrix}1 & 0 & 1 & 1 & 1 & 0 & 0\end{bmatrix}$$

$$\begin{bmatrix}1 & 0 & 0 & 0\end{bmatrix} \cdot \begin{bmatrix}1 & 0 & 0 & 0 & 1 & 1 & 0\\ 0 & 1 & 0 & 0 & 0 & 1 & 1\\ 0 & 0 & 1 & 0 & 1 & 1 & 1\\ 0 & 0 & 0 & 1 & 1 & 0 & 1\end{bmatrix} = \begin{bmatrix}1 & 0 & 0 & 0 & 1 & 1 & 0\end{bmatrix}$$

$$\begin{bmatrix}0 & 1 & 0 & 0\end{bmatrix} \cdot \begin{bmatrix}1 & 0 & 0 & 0 & 1 & 1 & 0\\ 0 & 1 & 0 & 0 & 0 & 1 & 1\\ 0 & 0 & 1 & 0 & 1 & 1 & 1\\ 0 & 0 & 0 & 1 & 1 & 0 & 1\end{bmatrix} = \begin{bmatrix}0 & 1 & 0 & 0 & 0 & 1 & 1\end{bmatrix}$$

$$\begin{bmatrix}0 & 0 & 1 & 1\end{bmatrix} \cdot \begin{bmatrix}1 & 0 & 0 & 0 & 1 & 1 & 0\\ 0 & 1 & 0 & 0 & 0 & 1 & 1\\ 0 & 0 & 1 & 0 & 1 & 1 & 1\\ 0 & 0 & 0 & 1 & 1 & 0 & 1\end{bmatrix} = \begin{bmatrix}0 & 0 & 1 & 1 & 0 & 1 & 0\end{bmatrix}$$

$$\begin{bmatrix}1 & 1 & 0 & 0\end{bmatrix} \cdot \begin{bmatrix}1 & 0 & 0 & 0 & 1 & 1 & 0\\ 0 & 1 & 0 & 0 & 0 & 1 & 1\\ 0 & 0 & 1 & 0 & 1 & 1 & 1\\ 0 & 0 & 0 & 1 & 1 & 0 & 1\end{bmatrix} = \begin{bmatrix}1 & 1 & 0 & 0 & 1 & 0 & 1\end{bmatrix}$$

$$\begin{bmatrix}0 & 1 & 1 & 1\end{bmatrix} \cdot \begin{bmatrix}1 & 0 & 0 & 0 & 1 & 1 & 0\\ 0 & 1 & 0 & 0 & 0 & 1 & 1\\ 0 & 0 & 1 & 0 & 1 & 1 & 1\\ 0 & 0 & 0 & 1 & 1 & 0 & 1\end{bmatrix} = \begin{bmatrix}0 & 1 & 1 & 1 & 0 & 0 & 1\end{bmatrix}$$

$$\begin{bmatrix}0 & 0 & 0 & 1\end{bmatrix} \cdot \begin{bmatrix}1 & 0 & 0 & 0 & 1 & 1 & 0\\ 0 & 1 & 0 & 0 & 0 & 1 & 1\\ 0 & 0 & 1 & 0 & 1 & 1 & 1\\ 0 & 0 & 0 & 1 & 1 & 0 & 1\end{bmatrix} = \begin{bmatrix}0 & 0 & 0 & 1 & 1 & 0 & 1\end{bmatrix}$$

$$\begin{bmatrix}1 & 0 & 0 & 1\end{bmatrix} \cdot \begin{bmatrix}1 & 0 & 0 & 0 & 1 & 1 & 0\\ 0 & 1 & 0 & 0 & 0 & 1 & 1\\ 0 & 0 & 1 & 0 & 1 & 1 & 1\\ 0 & 0 & 0 & 1 & 1 & 0 & 1\end{bmatrix} = \begin{bmatrix}1 & 0 & 0 & 1 & 0 & 1 & 1\end{bmatrix}$$

Portanto, os elementos do código do canal são dados por,

$$\begin{aligned} C = \{&1110010, 1101000, 0110100, 0010111, 1010001, 1011100, 1000110, 0100011,\\ &0011010, 1100101, 0111001, 0001101, 1001011\}\end{aligned}$$

com sua representação polinomial dada por

$$\begin{aligned} C &= \{1+X+X^2+X^5, 1+X+X^3, X+X^2+X^4, X^2+X^4+X^5+X^6, 1+X^2 \\ &\quad +X^6, 1+X^2+X^3+X^4, 1+X^4+X^5, X+X^5+X^6, X^2+X^3+X^5, 1+X \\ &\quad +X^4+X^6, X+X^2+X^3+X^6, X^3+X^4+X^6, 1+X^3+X^5+X^6\}. \end{aligned}$$

Pela Proposição 26 temos que a distância mínima de C é dada por

$$\omega(1110010-1101000)=\omega(0011010)=3,\ \ \omega(1110010-0110100)=\omega(1000110)=3,$$

$$\omega(1110010-0010111)=\omega(1100101)=4,\ \omega(1110010-1010001)=\omega(0100011)=3,$$

$$\omega(1110010-1011100)=\omega(1010001)=3,\ \ \omega(1110010-1000110)=\omega(0110100)=3,$$

$$\omega(1110010-0100011)=\omega(1010001)=3,\ \ \omega(1110010-0011010)=\omega(1101000)=3,$$

$$\omega(1110010-1100101)=\omega(0010111)=4,\ \ \omega(1110010-0111001)=\omega(1001011)=4,$$

$$\omega(1110010-0001101)=\omega(1111111)=7,\ \ \omega(1110010-1001011)=\omega(0111001)=4.$$

Assim, a distância mínima de C é dada pelo menor valor entre essas distâncias, ou seja, 3*, e o parâmetro desse código é* $(n,k,d)=(7,4,3)$*. Temos que, a capacidade de correção de erros é dada por* $\kappa=\left\lfloor\frac{3-1}{2}\right\rfloor=\left\lfloor\frac{2}{2}\right\rfloor=1$ *erro, e a capacidade de detecção de erros é dada por* $3-1=2$ *erros.*

Vamos determinar a matriz teste de paridade, efetuando a divisão

$$\begin{array}{r|l} X^7-1 & X^3+X+1 \\ \hline 0 & X^4+X^2+X+1 \end{array}$$

assim, $h(X)=1+X+X^2+0X^3+X^4$ *é polinômio de paridade de C dados pelos coeficientes* 11101*. Pelo Corolário 7, temos que a matriz teste de paridade para C é:*

$$h(X)=\begin{bmatrix} 1 & 0 & 1 & 1 & 1 & 0 & 0 \\ 0 & 1 & 0 & 1 & 1 & 1 & 0 \\ 0 & 0 & 1 & 0 & 1 & 1 & 1 \end{bmatrix}.$$

Note que $h(X)$ não está na forma padrão. Pelo Teorema 20 temos que $h'(X)$ é dado por

$$h'(X)=\begin{bmatrix} 1 & 0 & 0 & 1 & 0 & 1 & 1 \\ 0 & 1 & 0 & 1 & 1 & 1 & 0 \\ 0 & 0 & 1 & 0 & 1 & 1 & 1 \end{bmatrix}.$$

Onde cada coluna de $h'(X)$ equivale aos restos das divisões das mensagens recebidas com erros de no máximo 2 dígitos pelo polinômio gerador $g(X) = X^3 + X + 1$, ou seja, $r(X) = \{100, 010, 001, 110, 011, 111, 101\}$, em linguagem polinomial temos,

$$r(X) = \{1, X, X^2, 1 + X, X + X^2, 1 + X + X^2, 1 + X^2\},$$

e suas respectivas síndromes

$$s(r(X)) = \{1, X, X^2, X^3, X^4, X^5, X^6\}.$$

Suponha que a mensagem transmitida seja 1110010*. Na forma polinomial é dado por*

$$1 + 1X + 1X^2 + 0X^3 + 0X^4 + 1X^5 + 0X^6 = 1 + X + X^2 + X^5.$$

Fazendo a divisão $\frac{c(X)}{g(X)}$, temos:

$$\begin{array}{r|l} X^5 + X^2 + X + 1 & X^3 + X + 1 \\ \hline 0 & X^2 - 1 \end{array}$$

A mensagem recebida $1110010 \in \mathbb{Z}_2^6$, pelo Teorema 19 como $r(X) = 0$ temos que a síndrome é 000*, donde podemos afirmar que este vetor pertence ao código C.*

Suponha um erro do tipo $1\mathbf{0}01000$*, ou seja, um erro no segundo bit. A palavra transmitida na forma polinomial é dado por*

$$1 + 0X + 0X^2 + 1X^3 + 0X^4 + 0X^5 + 0X^6 = 1 + X^3.$$

Resolvendo o quociente $\frac{c(X)}{g(X)}$, temos:

$$\begin{array}{r|l} X^3 + 1 & X^3 + X + 1 \\ \hline X & 1 \end{array}$$

a mensagem recebida $1\mathbf{0}01000 \notin \mathbb{Z}_2^7$, como $r(X) = X$, temos que, $r = 010$, donde podemos afirmar pelo Teorema 20 que essa síndrome pertence a segunda coluna da matriz de paridade $h'(x)$, o que significa que houve um erro no segundo bit, com $s(r(X)) = X$.

Para obter a mensagem original basta calcular

$$i(X) = c(X) - s(r(X)) = 1 + X^3 - X = 1 + X + X^3,$$

que equivale a mensagem 1101000*, onde $i(X)$ é a mensagem inicial e $c(X)$ a mensagem recebida.*

Suponha um erro do tipo $01101\mathbf{1}0$*, ou seja, um erro no quinto bit. A palavra transmitida na forma polinomial é dado por*

$$0 + 1X + 1X^2 + 0X^3 + 1X^4 + 1X^5 + 0X^6 = X + X^2 + X^4 + X^5.$$

Resolvendo o quociente $\frac{c(X)}{g(X)}$*, temos:*

$$\begin{array}{r|l} X^5 + X^4 + X^2 + X & X^3 + X + 1 \\ \hline X^2 + X + 1 & X^2 + X - 1 \end{array}$$

a mensagem recebida $01101\mathbf{1}0 \notin \mathbb{Z}_2^7$*, como* $r(X) = 1 + X + X^2$*, temos que,* $r = 111$*, donde podemos afirmar pelo Teorema 20 que essa síndrome pertence a sexta coluna da matriz de paridade* $h'(x)$*, o que significa que houve um erro no sexto bit, com* $s(r(X)) = X^5$*.*

Para obter a mensagem original basta calcular

$$i(X) = c(X) - s(r(X)) = X + X^2 + X^4 + X^5 - X^5 = X + X^2 + X^4,$$

que equivale a mensagem 0110100*.*

3.2 CÓDIGOS QUÂNTICOS

O ruído é um problema significativo nos sistemas de processamento de informações, podendo resultar em perda de dados e corromper informações. Embora seja ideal construir sistemas que evitem completamente o ruído, muitas vezes isso não é possível. O sucesso da implementação de um computador quântico está associado à minimização dos efeitos do ruído.

Os Códigos Corretores de Erros Quânticos são estruturas matemáticas que permitem corrigir erros que possam ocorrer durante a transmissão de informações quânticas em computadores quânticos. Alguns exemplos de Códigos Corretores de Erros Quânticos incluem o código de Shor, o código de Steane, o código de Calderbank-Shor-Steane, entre outros. Nesse trabalho abordaremos os códigos de Shor, baseados nos estudos realizados por (NIELSEN; CHUANG, 2002), onde pode ser encontrado todas as demonstrações.

Os computadores quânticos têm a capacidade de processar informações de maneira fundamentalmente diferente dos computadores eletrônicos clássicos. Isso se deve ao fato de que os qubits em um computador quântico podem existir em estados superpostos e entrelaçados, permitindo uma computação paralela mais rápida e eficiente do que os bits em um computador clássico.

Baseados na matemática da mecânica quântica, os Códigos Corretores de Erros Quânticos utilizam conceitos como superposição, entrelaçamento e noções de espaços vetoriais para garantir a correção de erros. A ideia é usar a redundância quântica para proteger o estado quântico contra erros. Isso é, distribuindo o estado quântico a ser protegido por vários qubits. As portas lógicas são usadas para manipular os qubits e realizar a correção de erro.

Para entender o código de Shor, é interessante começar com a análise de um código corretor de erros clássicos simples, como o código de repetição. Esse código consiste em repetir a informação a ser transmitida várias vezes e enviar as cópias resultantes através de um canal ruidoso.

Para ilustrar o conceito de correção de erros utilizando a técnica de repetição, podemos utilizar uma situação cotidiana como exemplo. Imagine que duas pessoas estejam conversando em um ambiente barulhento e uma delas não consegue ouvir claramente o que a outra está dizendo. Nesse caso, a pessoa que não ouviu bem pode pedir para a outra repetir o que foi dito várias vezes. Caso ainda assim não consiga entender, ela pode analisar todas as falas anteriores, que foram repetidas, para tentar deduzir a informação correta.

Esse processo é semelhante ao utilizado pelo código de repetição, que consiste em repetir a informação várias vezes e enviar as cópias resultantes através de um canal ruidoso. Quando a informação chega ao destinatário, este pode analisar as diferentes cópias para identificar a informação correta e corrigir eventuais erros de transmissão.

Neste caso, desejamos enviar um bit de um local para outro através de um canal de comunicação clássico ruidoso. O efeito do ruído no canal é inverter o bit com probabilidade $p > 0$ e transmiti-lo sem erros com probabilidade $1 - p$, o canal é conhecido como um canal simétrico binário. Podemos enviar três cópias do bit que desejamos transmitir, ou seja, 0 seria transmitido como 000 e 1 seria transmitido como 111. As cadeias de bits com redundâncias são algumas vezes chamadas de 0_L (zero lógico) e 1_L (um lógico). O conceito de "lógico"refere-se a um estado quântico que representa um valor lógico binário, como 0 ou 1.

Essa técnica funciona porque, quando recebemos as três cópias, podemos verificar se há uma maioria de 0s ou 1s e assumir que essa é a informação correta. Por exemplo, se recebemos 001, assumimos que o bit transmitido foi 0, e se recebemos 110, assumimos que o bit transmitido foi 1. A votação por maioria falha se dois ou mais bits enviados pelo canal forem invertidos.

Definição 61. *Um código corretor de erro quântico pode ser representado como uma função* $E : \mathbb{C}^{2^k} \to \mathbb{C}^{2^{kn}}$*, onde* $\mathbb{C}^{2^k}$ *e* $\mathbb{C}^{2^{kn}}$ *são espaços vetoriais complexos de dimensões* 2^k *e* 2^{kn}*,*

respectivamente. Este k qubits são designado qubits de informação são eles que devem ser protegidos de erros. Os $n-k$ qubits adicionais formam a redundância necessária para proteger a informação.

O Bit Flip, também conhecido como inversão de bit, é uma operação que altera o valor de um bit de 0 para 1 ou de 1 para 0, realizado através da aplicação da operador de Pauli-X, também conhecida como porta lógica X em um qubit. O Phase Flip, também conhecido como inversão de fase, é uma operação que altera a fase do estado quântico de um qubit, alterando o sinal da amplitude, trocando o sinal do bit de $+$ para $-$ ou de $-$ para $+$. A operação de Phase Flip é realizada através da aplicação da operador de Pauli-Z, também conhecida como porta lógica Z, em um qubit, não alterando o valor do qubit, porém alterando sua fase.

Apresentaremos a seguir o canal Bit Flip e o canal Phase Flip, antes de definir o código de Bit Flip e o código de Phase Flip.

Suponha que qubits sejam enviados através de um canal Bit Flip que os deixa inalterados com probabilidade $1-p$ e inverte os qubit à uma probabilidade p, ou seja, $|0\rangle$ para $|1\rangle$ e vice-versa. O canal Bit Flip é definido como:

$$\begin{aligned} X|0\rangle &= |1\rangle \\ X|1\rangle &= |0\rangle . \end{aligned}$$

Assim, se o estado $|\psi\rangle$ é dado por $|\psi\rangle = a|0\rangle + b|1\rangle$, então o efeito do canal Bit Flip sobre $|\psi\rangle$ será $X|\psi\rangle = a|1\rangle + b|0\rangle$.

Suponha que qubits sejam enviados através de um canal Phase Flip que os deixa inalterados com probabilidade $1-p$ e troca a fase relativa dos estados com probabilidade p, ou seja, $|0\rangle$ para $|0\rangle$ e $|1\rangle$ para $-|1\rangle$. O canal Phase Flip é definido como:

$$\begin{aligned} Z|0\rangle &= |0\rangle \\ Z|1\rangle &= -|1\rangle . \end{aligned}$$

Assim, se o estado $|\psi\rangle$ é dado por $|\psi\rangle = a|0\rangle + b|1\rangle$, então o efeito do canal Phase Flip sobre $|\psi\rangle$ será $Z|\psi\rangle = a|0\rangle - b|1\rangle$.

3.2.1 Código Bit Flip

Um dos códigos quânticos mais simples é o código de Bit Flip, que consiste em adicionar um qubit auxiliar ao qubit original e armazenar a informação de forma redundante. Se ocorrer

um erro de inversão de bit em um dos qubits, a informação pode ser recuperada a partir do outro qubit, que estará sem erro.

Suponha um canal de Bit Flip como visto anteriormente. A seguir, descreveremos as operações de codificação e decodificação de um código de Bit Flip com capacidade de correção de 1 qubit neste canal.

CODIFICAÇÃO:

Para codificarmos um qubit utilizaremos um procedimento análogo ao código de repetição clássico. Cada estado-base de um qubit $a\,|0\rangle + b\,|1\rangle$ é mapeado em um estado de 3 qubits, como apresentado no Exemplo 24, ou seja,

$$T\,|0\rangle = |000\rangle = |0_L\rangle\,;$$

$$T\,|1\rangle = |111\rangle = |1_L\rangle\,.$$

Então,

$$T\,|\psi\rangle = a\,|0_L\rangle + b\,|1_L\rangle$$

onde T é a transformação que leva $|0\rangle$ em $|0_L\rangle$ e $|1\rangle$ em $|1_L\rangle$.

O estado $|\psi\rangle = a\,|0\rangle + b\,|1\rangle$ foi perfeitamente codificado no estado,

$$|\psi\rangle = a\,|000\rangle + b\,|111\rangle\,.$$

Para a decodificação teremos duas possibilidades, uma delas utilizando projetores e a outra a composição das portas lógicas de Di Pauli.

DETECÇÃO E CORREÇÃO DO ERRO 1:

Suponha que um Bit Flip ocorreu em um dos qubits. Existe um procedimento simples de correção de erros que pode ser usado para recuperar o estado quântico.

Detecção de erro ou diagnóstico de síndrome: Em um sistema quântico que está sujeito a erros, é possível realizar uma medição para determinar qual erro ocorreu, se houver. Essa medição produz um resultado conhecido como síndrome do erro. No caso do canal Bit Flip, existem quatro síndromes de erro diferentes, que correspondem a quatro operadores de projeção distintos.

$$P_0 = |000\rangle\langle 000| + |111\rangle\langle 111| \quad \text{sem erro}$$

$$P_1 = |100\rangle\langle 100| + |011\rangle\langle 011| \quad \text{inversão do primeiro qubit}$$

$$P_2 = |010\rangle\langle 010| + |101\rangle\langle 101| \quad \text{inversão do segundo qubit}$$

$$P_3 = |001\rangle\langle 001| + |110\rangle\langle 110| \quad \text{inversão do terceiro qubit}$$

Exemplo 38. *Suponha que se deseja enviar um qubit de informação* $|\psi\rangle = a\,|0\rangle + b\,|1\rangle$ *ao codificar a mensagem, ou seja, adicionando as redundâncias temos* $|\psi\rangle = a\,|000\rangle + b\,|111\rangle$. *Suponha que um Bit Flip ocorra no primeiro qubit, então o estado corrompido é* $\psi' = a\,|100\rangle + b\,|011\rangle$. *A medida da síndrome é dada pelo operador* $\langle\psi'|P_i|\psi'\rangle$, *para* $i = 0,1,2,3$.

Sabendo que,

$$|100\rangle = |1\rangle \otimes |0\rangle \otimes |0\rangle = \begin{bmatrix} 0 \\ 1 \end{bmatrix} \otimes \begin{bmatrix} 1 \\ 0 \end{bmatrix} \otimes \begin{bmatrix} 1 \\ 0 \end{bmatrix} = \begin{bmatrix} 0 \\ 0 \\ 0 \\ 0 \\ 1 \\ 0 \\ 0 \\ 0 \end{bmatrix}$$

$$|011\rangle = |0\rangle \otimes |1\rangle \otimes |1\rangle = \begin{bmatrix} 1 \\ 0 \end{bmatrix} \otimes \begin{bmatrix} 0 \\ 1 \end{bmatrix} \otimes \begin{bmatrix} 0 \\ 1 \end{bmatrix} = \begin{bmatrix} 0 \\ 0 \\ 0 \\ 1 \\ 0 \\ 0 \\ 0 \\ 0 \end{bmatrix}$$

Então,

$$a\,|100\rangle + b\,|011\rangle = \begin{bmatrix} 0 \\ 0 \\ 0 \\ 0 \\ a \\ 0 \\ 0 \\ 0 \end{bmatrix} + \begin{bmatrix} 0 \\ 0 \\ 0 \\ b \\ 0 \\ 0 \\ 0 \\ 0 \end{bmatrix} = \begin{bmatrix} 0 \\ 0 \\ 0 \\ b \\ a \\ 0 \\ 0 \\ 0 \end{bmatrix}$$

E ainda,

$$|100\rangle\langle 100| = \begin{bmatrix}0 & 0 & 0 & 0 & 1 & 0 & 0 & 0\end{bmatrix} \otimes \begin{bmatrix}0\\0\\0\\0\\1\\0\\0\\0\end{bmatrix} = \begin{bmatrix}0&0&0&0&0&0&0&0\\0&0&0&0&0&0&0&0\\0&0&0&0&0&0&0&0\\0&0&0&0&0&0&0&0\\0&0&0&0&1&0&0&0\\0&0&0&0&0&0&0&0\\0&0&0&0&0&0&0&0\\0&0&0&0&0&0&0&0\end{bmatrix}$$

$$|011\rangle\langle 011| = \begin{bmatrix}0 & 0 & 0 & 1 & 0 & 0 & 0 & 0\end{bmatrix} \otimes \begin{bmatrix}0\\0\\0\\1\\0\\0\\0\\0\end{bmatrix} = \begin{bmatrix}0&0&0&0&0&0&0&0\\0&0&0&0&0&0&0&0\\0&0&0&0&0&0&0&0\\0&0&0&1&0&0&0&0\\0&0&0&0&0&0&0&0\\0&0&0&0&0&0&0&0\\0&0&0&0&0&0&0&0\\0&0&0&0&0&0&0&0\end{bmatrix}$$

Então,

$$|100\rangle\langle 100| + |011\rangle\langle 011| = \begin{bmatrix}0&0&0&0&0&0&0&0\\0&0&0&0&0&0&0&0\\0&0&0&0&0&0&0&0\\0&0&0&1&0&0&0&0\\0&0&0&0&1&0&0&0\\0&0&0&0&0&0&0&0\\0&0&0&0&0&0&0&0\\0&0&0&0&0&0&0&0\end{bmatrix}$$

Observe que

$$\langle\psi'|P_1|\psi'\rangle = \langle a\,|100\rangle + b\,|011\rangle\,||100\rangle\langle 100| + |011\rangle\langle 011||a\,|100\rangle + b\,|011\rangle\rangle$$

$$= \begin{bmatrix} 0 & 0 & 0 & b & a & 0 & 0 & 0 \end{bmatrix} \begin{bmatrix} 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \end{bmatrix} \begin{bmatrix} 0 \\ 0 \\ 0 \\ b \\ a \\ 0 \\ 0 \\ 0 \end{bmatrix}$$

O resultado da medição (a síndrome do erro) é 1.

Calculando a síndrome para os demais projetores, $\langle\psi'|P_0|\psi'\rangle$, $\langle\psi'|P_2|\psi'\rangle$, $\langle\psi'|P_3|\psi'\rangle$ os resultados serão 0, que era esperado pelo fato ocorrer erro sobre um único qubit.

Analogamente, supondo um erro do tipo Bit Flip no segundo qubit temos $|\psi''\rangle = a\,|010\rangle + b\,|101\rangle$, assim as síndromes são dadas por $\langle\psi''|P_0|\psi''\rangle = \langle\psi''|P_1|\psi''\rangle = \langle\psi''|P_3|\psi''\rangle = 0$ e $\langle\psi''|P_2|\psi''\rangle = 1$, supondo um erro do tipo Bit Flip no terceiro qubit temos $|\psi'''\rangle = a\,|001\rangle + b\,|110\rangle$, as síndromes são dadas por $\langle\psi'''|P_0|\psi'''\rangle = \langle\psi'''|P_1|\psi'''\rangle = \langle\psi'''|P_2|\psi'''\rangle = 0$ e $\langle\psi'''|P_3|\psi'''\rangle = 1$.

É possível estabelecer o método de recuperação do estado original por meio da análise da síndrome do erro. No caso do exemplo supracitado, o estado corrompido corresponde a $\psi' = a\,|100\rangle + b\,|011\rangle$. Nesse caso, a síndrome $\langle\psi'|P_1|\psi'\rangle = 1$ indica que a inversão do primeiro qubit é necessária para recuperar o estado original. Analogamente, a síndrome $\langle\psi''|P_2|\psi''\rangle = 1$ indica a inversão do segundo qubit e assim por diante. Para executar a inversão, é necessário aplicar o operador X no qubit correspondente. A notação X_i é usada para indicar a aplicação do operador X em um qubit específico, com i assumindo os valores 1, 2 ou 3. No entanto, é importante destacar que este procedimento não é capaz de lidar com mais de um erro no estado corrompido. Assim, recuperar o estado original de $\psi' = a\,|100\rangle + b\,|011\rangle$ é dado por

$$X_1(a\,|100\rangle + b\,|011\rangle) = a\,|000\rangle + b\,|111\rangle$$

DETECÇÃO E CORREÇÃO DE ERRO 2:

Existe uma abordagem alternativa para detectar o erro no estado recebido, ao invés de medir os quatro projetores P_0, P_1, P_2, e P_3, podemos realizar duas medições, uma do observável $Z_1Z_2 = Z \otimes Z \otimes I$ e outra do observável $Z_2Z_3 = I \otimes Z \otimes Z$. Do Exemplo 17 temos que Z

possui autovalores ± 1. Assim, Cada um desses observáveis possui autovalores ± 1, ou seja, cada medida fornecerá um autovalor para cada dois qubits de informação.

A primeira medição $Z_1 Z_2$, pode ser interpretada como uma comparação entre o primeiro e segundo qubit, analogamente, medir $Z_2 Z_3$ compara os valores do segundo e terceiro qubits. Essa medição pode ser interpretada como comparar os valores dos qubits, resultando em $+1$ se forem iguais e -1 se forem diferentes.

Combinando os resultados das duas medições, podemos determinar se ocorreu uma inversão de bit em um dos qubits e, em caso afirmativo, qual qubit foi invertido. A seguir é possível ver as possibilidades dessas medidas (síndromes): os autovalores $(Z_1 Z_2, Z_2 Z_3)$ e o qubit onde ocorreu o erro.

$$(+1, +1): \quad \text{sem erro}$$

$$(-1, +1): \quad \text{inversão do primeiro qubit}$$

$$(-1, -1): \quad \text{inversão do segundo qubit}$$

$$(+1, -1): \quad \text{inversão do terceiro qubit}$$

Exemplo 39. *Suponha que um Bit Flip ocorra no primeiro qubit, então o estado corrompido é* $\psi' = a\,|100\rangle + b\,|011\rangle$. *A medida da síndrome é dada pela medição do observável* $Z_1 Z_2$ *e* $Z_2 Z_3$. *Assim,*

$$Z_1 Z_2 (a\,|100\rangle + b\,|011\rangle) = -a\,|100\rangle - b\,|011\rangle = -(a\,|100\rangle + b\,|011\rangle) = -1.$$

E, ainda

$$Z_2 Z_3 (a\,|100\rangle + b\,|011\rangle) = a\,|100\rangle + b\,|011\rangle = +1.$$

Portanto, o resultado da síndrome é dada por $(-1, +1)$*, o que indica que houve um erro do tipo Bit Flip no primeiro qubit.*

Após a detecção de um erro, é necessário realizar a correção. Caso nenhum erro tenha ocorrido, não é necessário realizar alguma ação. Entretanto, se as sinalizações indicarem que houve um erro em algum dos qubits é necessário aplicar o operador X no qubit afetado para recuperar o estado original. Assim,

$$X_1 \psi' = a\,|000\rangle + b\,|111\rangle\,.$$

Com isso, o código será capaz de preservar o estado quântico codificado e recuperar as informações originalmente transmitidas.

Observação 8. *A medição da síndrome em ambos os casos não causam nenhuma mudança no estado antes e depois da medição da síndrome. Para garantir o sucesso das medições realizadas, é fundamental que nenhuma delas revele informações sobre as amplitudes a e b do estado quântico codificado. Essa condição é essencial para evitar que as superposições de estados quânticos sejam destruídas por alguma medição.*

3.2.2 Código Phase Flip

O código Phase Flip funciona de forma semelhante, adicionando um qubit auxiliar e armazenando a informação de forma redundante, mas dessa vez a informação é codificada em relação à fase do qubit original. Se ocorrer um erro de inversão de fase em um dos qubits, a informação pode ser recuperada a partir do outro qubit, que estará sem erro.

CODIFICAÇÃO:

Para codificarmos um qubit utilizaremos o mesmo procedimento de codificação do código Bit Flip, dado o estado-base de um qubit $a\,|0\rangle + b\,|1\rangle$ é mapeado em um estado de 3 qubits e posto um adicional de aplicar o operador Hadamard em cada qubit. Assim,

$$T\,|0\rangle = |000\rangle$$

$$T\,|1\rangle = |111\rangle$$

E,

$$T\,|\psi\rangle = a\,|000\rangle + b\,|111\rangle$$

Aplicando o operador Hadamard em cada qubit, temos

$$\begin{aligned} H(|000\rangle) &= |+++\rangle \\ &= \left(\tfrac{(|0\rangle+|1\rangle)(|0\rangle+|1\rangle)(|0\rangle+|1\rangle)}{\sqrt{2}\sqrt{2}\sqrt{2}}\right) \\ &= \left(\tfrac{(|0\rangle+|1\rangle)(|0\rangle+|1\rangle)(|0\rangle+|1\rangle)}{2\sqrt{2}}\right) \\ &= |0_L\rangle \end{aligned}$$

$$\begin{aligned} H(|111\rangle) &= |---\rangle \\ &= \left(\tfrac{(|0\rangle-|1\rangle)(|0\rangle-|1\rangle)(|0\rangle-|1\rangle)}{\sqrt{2}\sqrt{2}\sqrt{2}}\right) \\ &= \left(\tfrac{(|0\rangle-|1\rangle)(|0\rangle-|1\rangle)(|0\rangle-|1\rangle)}{2\sqrt{2}}\right) \\ &= |1_L\rangle\,. \end{aligned}$$

Então,

$$H\left|\psi\right\rangle = a\left|0_L\right\rangle + \left|1_L\right\rangle.$$

O estado $\left|\psi\right\rangle = a\left|0\right\rangle + b\left|1\right\rangle$ foi perfeitamente codificado no estado,

$$\left|\psi\right\rangle = a\left(\frac{(\left|0\right\rangle + \left|1\right\rangle)(\left|0\right\rangle + \left|1\right\rangle)(\left|0\right\rangle + \left|1\right\rangle)}{2\sqrt{2}}\right) + b\left(\frac{(\left|0\right\rangle - \left|1\right\rangle)(\left|0\right\rangle - \left|1\right\rangle)(\left|0\right\rangle - \left|1\right\rangle)}{2\sqrt{2}}\right).$$

Em resumo, a codificação do código Phase Flip ocorre em duas etapas distintas. Em primeiro lugar, os dados são codificados em três qubits, da mesma forma que ocorre no canal de Bit Flip. Em seguida, é aplicada uma porta Hadamard em cada um dos três qubits. Esse processo garante que os dados possam ser transmitidos de forma segura pelo canal de Phase Flip, sem perda de informações.

DETECÇÃO E CORREÇÃO DE ERRO:

Para detectar erros, são utilizadas as mesmas medidas projetivas que foram usadas no canal Bit Flip. No entanto, as medidas são conjugadas pelas portas de Hadamard, que são aplicadas como parte do processo de detecção de erros. Assim, P_i é levada a $H^{\otimes 3}P_iH^{\otimes 3}$ onde $H^{\otimes 3} = H \otimes H \otimes H$ e $i = \{0, 1, 2, 3\}$. Assim como no canal de Bit Flip, é possível medir as síndromes utilizando os observáveis correspondentes $H^{\otimes 3}Z_1Z_2H^{\otimes 3} = X_1X_2$ e $H^{\otimes 3}Z_2Z_3H^{\otimes 3} = X_2X_3$. Isso permite que o sistema detecte erros com mais precisão e eficiência, garantindo que a transmissão de dados ocorra de maneira segura e sem perda de informações.

Analogamente as medidas de Z_1Z_2 e Z_2Z_3 para o canal Bit Flip. A medição dos observáveis X_1X_2 e X_2X_3 compara os sinais de cada bloco de qubit, ou seja, a primeira medição X_1X_2, pode ser interpretada como uma comparação entre o sinal primeiro e segundo bloco, e medir X_2X_3 compara o sinal do segundo e terceiro bloco. Se considerarmos estados como $\left|+\right\rangle\left|+\right\rangle$ ou $\left|-\right\rangle\left|-\right\rangle$, a medida do observável X_1X_2 resultará em $+1$. No entanto, se tivermos estados do tipo $\left|+\right\rangle\left|-\right\rangle$ ou $\left|-\right\rangle\left|+\right\rangle$, a medida desse mesmo observável resultará em -1. Essas medidas são importantes para a detecção de erros e para garantir que os dados sejam transmitidos com segurança e precisão no sistema quântico.

Combinando os resultados das duas medições, podemos determinar se ocorreu uma inversão de fase em um dos qubits e, em caso afirmativo, qual qubit foi invertido com relação ao sinal (fase). A seguir é possível ver as possibilidades de resultados das medidas e os possíveis erros.

$$(+1, +1): \quad \text{sem erro}$$

$$(-1,+1): \quad \text{inversão de fase no primeiro bloco}$$

$$(-1,-1): \quad \text{inversão de fase no segundo bloco}$$

$$(+1,-1): \quad \text{inversão de fase no terceiro bloco}$$

Exemplo 40. *Suponha um erro do tipo Phase Flip ocorra no terceiro qubit, de* $|+\rangle$ *para* $|-\rangle$*, então o estado corrompido é*

$$|\psi'\rangle = a\left(\frac{(|0\rangle+|1\rangle)(|0\rangle+|1\rangle)(|0\rangle-|1\rangle)}{2\sqrt{2}}\right) + b\left(\frac{(|0\rangle-|1\rangle)(|0\rangle-|1\rangle)(|0\rangle+|1\rangle)}{2\sqrt{2}}\right).$$

A medida da síndrome é dada pela medição do observável X_1X_2 *e* X_2X_3*. Assim,*

$$\begin{aligned}
X_1X_2(|\psi'\rangle) &= X_1X_2(a\,|++-\rangle + b\,|--+\rangle) \\
&= a\left(\tfrac{(|1\rangle+|0\rangle)(|1\rangle+|0\rangle)(|0\rangle-|1\rangle)}{2\sqrt{2}}\right) + b\left(\tfrac{(|1\rangle-|0\rangle)(|1\rangle-|0\rangle)(|0\rangle+|1\rangle)}{2\sqrt{2}}\right) \\
&=^{*} a\left(\tfrac{(|0\rangle+|1\rangle)(|0\rangle+|1\rangle)(|0\rangle-|1\rangle)}{2\sqrt{2}}\right) + b\left(\tfrac{(|0\rangle-|1\rangle)(|0\rangle-|1\rangle)(|0\rangle+|1\rangle)}{2\sqrt{2}}\right) \\
&= a\,|++-\rangle + b\,|--+\rangle \\
&= +1.
\end{aligned}$$

E, ainda

$$\begin{aligned}
X_2X_3(|\psi'\rangle) &= X_2X_3(a\,|++-\rangle + b\,|--+\rangle) \\
&= a\left(\tfrac{(|0\rangle+|1\rangle)(|1\rangle+|0\rangle)(|1\rangle-|0\rangle)}{2\sqrt{2}}\right) + b\left(\tfrac{(|0\rangle-|1\rangle)(|1\rangle-|0\rangle)(|1\rangle+|0\rangle)}{2\sqrt{2}}\right) \\
&=^{\sharp} a\left(\tfrac{(|0\rangle+|1\rangle)(|0\rangle+|1\rangle)(-|0\rangle-|1\rangle)}{2\sqrt{2}}\right) + b\left(\tfrac{(|0\rangle-|1\rangle)(|0\rangle-|1\rangle)(|0\rangle+|1\rangle)}{2\sqrt{2}}\right) \\
&= -(a\,|++-\rangle + b\,|--+\rangle) \\
&= -1.
\end{aligned}$$

Observação 9. *Em* $*$ *temos,*

$$\begin{aligned}
(|1\rangle-|0\rangle)(|1\rangle-|0\rangle) &= |1\rangle\,|1\rangle - 2(|0\rangle\,|1\rangle) + |0\rangle\,|0\rangle \\
&= (|0\rangle-|1\rangle)(|0\rangle-|1\rangle)
\end{aligned}$$

Observação 10. *Em* $\sharp$ *temos,*

$$\begin{aligned}
(|1\rangle+|0\rangle)(|1\rangle-|0\rangle) &= |1\rangle\,|1\rangle - |0\rangle\,|0\rangle \\
&= (|0\rangle+|1\rangle)(|0\rangle-|1\rangle)
\end{aligned}$$

Portanto, o resultado da síndrome é dada por $(+1,-1)$*, o que indica que houve um erro do tipo Phase Flip no terceiro qubit.*

Assim como no canal Bit Flip, é possível corrigir os erros do canal de Phase Flip aplicando os mesmos operadores, mas conjugados pela matriz de Hadamard, ou seja, se for detectada uma inversão de fase em um qubit na posição i, é possível corrigir o erro aplicando o operador$Z = HXH$ sobre o qubit i. Assim,

$$Z_3 |\psi'\rangle = a \left(\frac{(|0\rangle + |1\rangle)(|0\rangle + |1\rangle)(|0\rangle + |1\rangle)}{2\sqrt{2}} \right) + b \left(\frac{(|0\rangle - |1\rangle)(|0\rangle - |1\rangle)(|0\rangle - |1\rangle)}{2\sqrt{2}} \right).$$

3.2.3 Código de Shor

Código de Shor é um algoritmo de computação quântica desenvolvido por Peter Shor em 1994. Ele é considerado um dos mais importantes algoritmos quânticos porque é capaz de calcular rapidamente a decomposição em fatores primos de números muito grandes (SHOR, 1994). Isso é importante porque a decomposição em fatores primos é uma tarefa difícil na computação clássica, e é a base para a segurança de muitos algoritmos de criptografia clássicos.

No estudo anterior, foi observado que é viável desenvolver um algoritmo capaz de detectar e corrigir erros Bit Flip e Phase Flip, desde que este ocorra em, no máximo, um único qubit. Neste momento, apresentaremos um código que permite a correção de erros quânticos arbitrários, seguindo a ideia do código de repetição e sendo eficiente para correção de no máximo 1 qubit. O código de Shor, que possui nove qubits, é uma junção dos códigos de três qubits utilizados para canais Bit Flip e Phase Flip.

CODIFICAÇÃO:

A codificação do código de Shor é iniciada com a mesma codificação do código Phase Flip. Assim, dado um qubit $a|0\rangle + b|1\rangle$ é codificado como,

$$|\psi\rangle = a|+++\rangle + b|---\rangle).$$

Em seguida, cada um desses qubits é codificado usando a codificação do código Bit Flip:

$$(|+++\rangle)|0\rangle = \left(\frac{(|00\rangle + |10\rangle)(|00\rangle + |10\rangle)(|00\rangle + |10\rangle)}{2\sqrt{2}} \right)$$

Aplicando o CNOT, temos

$$\left(\frac{(|00\rangle + |11\rangle)(|00\rangle + |11\rangle)(|00\rangle + |11\rangle)}{2\sqrt{2}} \right)$$

E, ainda

$$(|---\rangle)\,|0\rangle = \left(\frac{(|00\rangle - |10\rangle)(|00\rangle - |10\rangle)(|00\rangle - |10\rangle)}{2\sqrt{2}}\right)$$

Aplicando o CNOT, temos

$$\left(\frac{(|00\rangle - |11\rangle)(|00\rangle - |11\rangle)(|00\rangle - |11\rangle)}{2\sqrt{2}}\right)$$

Repetindo o processo novamente, teremos

$$\left(\frac{(|000\rangle + |111\rangle)(|000\rangle + |111\rangle)(|000\rangle + |111\rangle)}{2\sqrt{2}}\right) = |0_L\rangle$$
$$\left(\frac{(|000\rangle - |111\rangle)(|000\rangle - |111\rangle)(|000\rangle - |111\rangle)}{2\sqrt{2}}\right) = |1_L\rangle$$

O estado após a codificação é dado por,

$$|\psi\rangle = a\,|0_L\rangle + b\,|1_L\rangle$$

O estado $|\psi\rangle = a\,|0\rangle + b\,|1\rangle$ foi perfeitamente codificado no estado,

$$|\psi\rangle \;=\; a\left(\tfrac{(|000\rangle+|111\rangle)(|000\rangle+|111\rangle)(|000\rangle+|111\rangle)}{2\sqrt{2}}\right) + b\left(\tfrac{(|000\rangle-|111\rangle)(|000\rangle-|111\rangle)(|000\rangle-|111\rangle)}{2\sqrt{2}}\right).$$

DETECÇÃO E CORREÇÃO DE ERRO DO TIPO BIT FLIP:

Para identificar e corrigir erros de Bit Flip, é necessário utilizar as medidas dos observáveis Z_1Z_2, Z_2Z_3, Z_4Z_5, Z_5Z_6, Z_7Z_8 e Z_8Z_9. Suponhamos que ocorra um erro Bit Flip no primeiro bloco de três qubits. Realizamos a medida dos observáveis Z_1Z_2 e Z_2Z_3, e se o resultado for, respectivamente, -1 e $+1$, concluímos que o erro ocorreu no primeiro qubit e corrigimos aplicando o operador X neste qubit. O processo é análogo para erros nos outros blocos de qubits.

Exemplo 41. *Suponha que um erro de Bit Flip ocorra no segundo qubit do primeiro bloco, ou seja,*

$$|\psi'\rangle \;=\; a\left(\tfrac{(|010\rangle+|101\rangle)(|000\rangle+|111\rangle)(|000\rangle+|111\rangle)}{2\sqrt{2}}\right) + b\left(\tfrac{(|010\rangle-|101\rangle)(|000\rangle-|111\rangle)(|000\rangle-|111\rangle)}{2\sqrt{2}}\right).$$

Para detectarmos o erro é necessário aplicar as medicas dos observáveis Z_1Z_2 e Z_2Z_3. Assim,

$$\begin{aligned}
Z_1Z_2(|\psi'\rangle) &= a\left(\tfrac{(-|010\rangle-|101\rangle)(|000\rangle+|111\rangle)(|000\rangle+|111\rangle)}{2\sqrt{2}}\right)\\
&+ b\left(\tfrac{(-|010\rangle+|101\rangle)(|000\rangle-|111\rangle)(|000\rangle-|111\rangle)}{2\sqrt{2}}\right)\\
&= a\left(\tfrac{-(|010\rangle+|101\rangle)(|000\rangle+|111\rangle)(|000\rangle+|111\rangle)}{2\sqrt{2}}\right)\\
&+ b\left(\tfrac{-(|010\rangle-|101\rangle)(|000\rangle-|111\rangle)(|000\rangle-|111\rangle)}{2\sqrt{2}}\right)\\
&= -1.
\end{aligned}$$

E, ainda

$$\begin{aligned} Z_2Z_3(|\psi'\rangle) &= a\left(\frac{(-|010\rangle-|101\rangle)(|000\rangle+|111\rangle)(|000\rangle+|111\rangle)}{2\sqrt{2}}\right) \\ &+ b\left(\frac{(-|010\rangle+|101\rangle)(|000\rangle-|111\rangle)(|000\rangle-|111\rangle)}{2\sqrt{2}}\right) \\ &= a\left(\frac{-(|010\rangle+|101\rangle)(|000\rangle+|111\rangle)(|000\rangle+|111\rangle)}{2\sqrt{2}}\right) \\ &+ b\left(\frac{-(|010\rangle-|101\rangle)(|000\rangle-|111\rangle)(|000\rangle-|111\rangle)}{2\sqrt{2}}\right) \\ &= -1. \end{aligned}$$

Portanto, o resultado da síndrome é dada por $(-1,-1)$*, o que indica que houve um erro do tipo Bit Flip no segundo qubit do primeiro bloco.*

Após a detecção de um erro, é necessário realizar a correção. Caso nenhum erro tenha ocorrido, não é necessário realizar alguma ação. Entretanto, se houver um erro em algum dos qubits é necessário aplicar o operador X no qubit afetado para recuperar o estado original. Assim,

$$\begin{aligned} X_2\,|\psi'\rangle &= a\left(\frac{(|000\rangle+|111\rangle)(|000\rangle+|111\rangle)(|000\rangle+|111\rangle)}{2\sqrt{2}}\right) \\ &+ b\left(\frac{(|000\rangle-|111\rangle)(|000\rangle-|111\rangle)(|000\rangle-|111\rangle)}{2\sqrt{2}}\right) \end{aligned}$$

DETECÇÃO E CORREÇÃO DE ERRO DO TIPO PHASE FLIP:

No código de Shor quando ocorre o Phase Flip em qualquer um dos três primeiros qubits, o sinal do primeiro bloco de qubits é invertido, resultando em dois estados possíveis para o bloco. Os observáveis utilizados para a detecção e correção de erros são $X_1X_2X_3X_4X_5X_6$ e $X_4X_5X_6X_7X_8X_9$, que comparam os sinais dos blocos de três qubits para determinar em qual bloco ocorreu o erro Phase Flip. O operador Z é aplicado para corrigir o erro em qualquer um dos qubits do bloco. Essa propriedade está relacionada à não-localidade ou emaranhamento do qubit lógico. Embora os erros de inversão de fase não sejam distinguíveis, o código é corrigível, o que caracteriza a degenerescência do código.

Exemplo 42. *Suponha um erro do tipo Phase Flip ocorra no primeiro bloco, então o estado corrompido é*

$$\begin{aligned} X_2\,|\psi'\rangle &= a\left(\frac{(|000\rangle-|111\rangle)(|000\rangle+|111\rangle)(|000\rangle+|111\rangle)}{2\sqrt{2}}\right) \\ &+ b\left(\frac{(|000\rangle+|111\rangle)(|000\rangle-|111\rangle)(|000\rangle-|111\rangle)}{2\sqrt{2}}\right) \end{aligned}$$

A medida da síndrome é dada pela medição do observável $X_1X_2X_3X_4X_5X_6$ *e* $X_4X_5X_6X_7X_8X_9$*. Assim,*

$$\begin{aligned} X_1X_2X_3X_4X_5X_6(|\psi'\rangle) &= a\left(\frac{(|111\rangle-|000\rangle)(|111\rangle+|000\rangle)(|000\rangle+|111\rangle)}{2\sqrt{2}}\right) \\ &+ b\left(\frac{(|111\rangle+|000\rangle)(|111\rangle-|000\rangle)(|000\rangle-|111\rangle)}{2\sqrt{2}}\right) \\ &= -1. \end{aligned}$$

E,

$$\begin{aligned} X_4X_5X_6X_7X_8X_9(|\psi'\rangle) &= a\left(\frac{(|000\rangle+|111\rangle)(|000\rangle+|111\rangle)(|000\rangle+|111\rangle)}{2\sqrt{2}}\right) \\ &+ b\left(\frac{(|000\rangle-|111\rangle)(|000\rangle-|111\rangle)(|000\rangle-|111\rangle)}{2\sqrt{2}}\right) \\ &= +1. \end{aligned}$$

Portanto, o resultado da síndrome é dada por $(-1,+1)$*, o que indica que houve um erro do tipo Phase Flip no primeiro bloco.*

Para corrigi-lo aplicando o operador Z *sobre qualquer um dos qubits desse bloco.*

DETECÇÃO E CORREÇÃO DE ERRO DO TIPO BIT FLIP E PHASE FLIP:

O Código Shor é um método de correção de erros que pode ser utilizado para proteger a informação armazenada em qubits de computadores quânticos contra erros decorrentes de Bit Flip e Phase Flip nos qubits originais. Caso ocorra um erro de Bit Flip e Phase Flip, o código permite a detecção e correção desse erro por meio da aplicação do operador Z para Bit Flip e X para Phase Flip, ou seja, suponha um erro do tipo Bit Flip e Phase Flip no primeiro qubit, assim aplicando o operador Z_1X_1 nesse qubit, o procedimento para detectar um erro de inversão de bits detectará uma inversão de bits no primeiro qubit e o corrigirá, enquanto o procedimento para detectar um erro de inversão de fase detectará uma inversão de fase no primeiro bloco de três qubits e o corrigirá. O algoritmo de Shor não é um algoritmo de correção de erros para qubits independentes, ou seja, o código não corrige um erro de Bit Flip e Phase Flip se eles ocorrem em qubits diferentes.

4 PROPOSTA DE ATIVIDADE NO SCRATCH

Neste capítulo, propomos uma abordagem inovadora para o ensino de Códigos Corretores de Erros a estudantes do ensino médio, utilizando o Scratch. O Scratch é uma poderosa ferramenta de programação desenvolvida pelo Massachusetts Institute of Technology (MIT) com o objetivo de introduzir conceitos de programação e lógica por meio da programação em blocos para pessoas de todas as idades, especialmente crianças e jovens. O objetivo é apresentar e explorar as noções básicas de Códigos Corretores de Erros, aplicando os conceitos matemáticos relevantes apresentados nas preliminares, relacionando-os com situações do cotidiano e destacando sua aplicabilidade além do ambiente escolar.

Ao adotar o Scratch como ferramenta de aprendizado, buscamos engajar os estudantes de forma interativa e prática. Através da gamificação e atividades de programação, os alunos poderão compreender os conceitos básicos dos Códigos Corretores de Erros de maneira envolvente, desenvolvendo habilidades de resolução de problemas e pensamento lógico. O domínio dos conteúdos referentes a operações com polinômios e conceitos básicos de matrizes, permite aos estudantes compreenderem os fundamentos teóricos e aplicá-los na prática, tanto na implementação dos códigos quanto na análise de sua eficiência e capacidade de correção de erros.

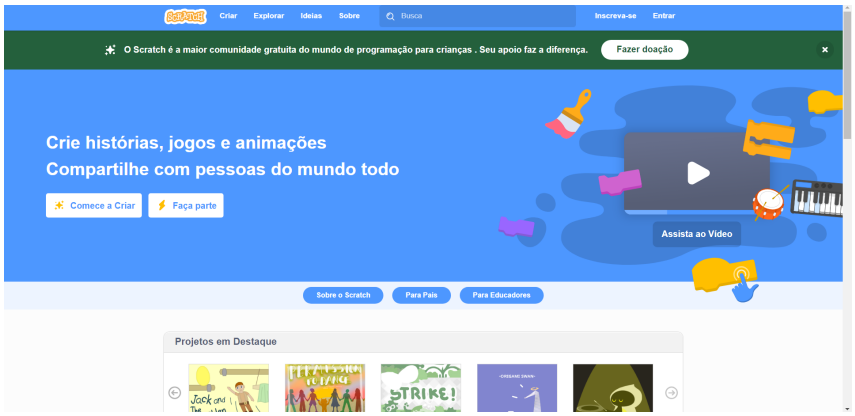
> Com o Scratch, nossa meta é levar a "Alegria da construção, orgulho da criação" para o mundo on-line, proporcionando às crianças novas maneiras de "construir", de compartilhar suas criações e de se desenvolverem como pensadoras criativas (RESNICK, 2017).

Com uma interface gráfica e intuitiva, o Scratch permite que os usuários criem projetos interativos, animações e jogos através do encaixe de blocos de código, sem a necessidade de digitar linhas de código complexas. Além disso, os usuários podem explorar e aproveitar as inúmeras produções já compartilhadas na plataforma do Scratch. Para (SANTOS; JUNIOR, 2014), os jogos eletrônicos têm o potencial de trazer benefícios aos processos educacionais, enriquecendo o ensino e aprendizagem. Independente da área de estudo, eles podem estimular o desenvolvimento do raciocínio lógico e do pensamento cognitivo.

Através dos jogos "Código de Hamming" e "Código Cíclico", desenvolvidos pelos autores nessa plataforma, os alunos serão desafiados a identificar os erros que ocorrem durante a transmissão das informações e aplicar os conceitos dos Códigos Corretores de Erros para

corrigi-los.

Figura 7 – Interface do Scratch



Fonte: Plataforma Scratch.

Na Figura 7, é possível ver a interface do Scratch, onde, na parte superior, encontram-se as opções criar, explorar, barra de pesquisa, entre outras. Para programar, basta clicar em *criar*. Caso queira conhecer mais sobre as ferramentas de blocos de programação, basta clicar em *explorar*. Os jogos apresentados e criados ao longo deste trabalho são facilmente encontrados pesquisando na barra de pesquisa os termos *Código de Hamming* e *Código Cíclico*.

A proposta de aula consiste em três momentos distintos: introdução, desenvolvimento e sistematização. Na introdução, será apresentado o primeiro jogo desenvolvido com o objetivo de apresentar a ideia de Códigos Corretos de Erros. O segundo jogo será utilizado para reforçar e consolidar os conteúdos abordados no desenvolvimento apresentados no segundo momento, proporcionando um fechamento adequado na sistematização. Ambos os jogos, criados como parte deste trabalho, têm o propósito de ilustrar e exemplificar a proposta de aula apresentada a seguir.

4.1 PROPOSTA

Tema da Aula: Corrigindo erros.

Conteúdo: Códigos Corretores de Erros.

Objeto de conhecimento: Algoritmos: modelagem de problemas e de soluções.

Habilidade da BNCC: (EM13MAT315) Investigar e registrar, por meio de um fluxograma, quando possível, um algoritmo que resolve um problema.

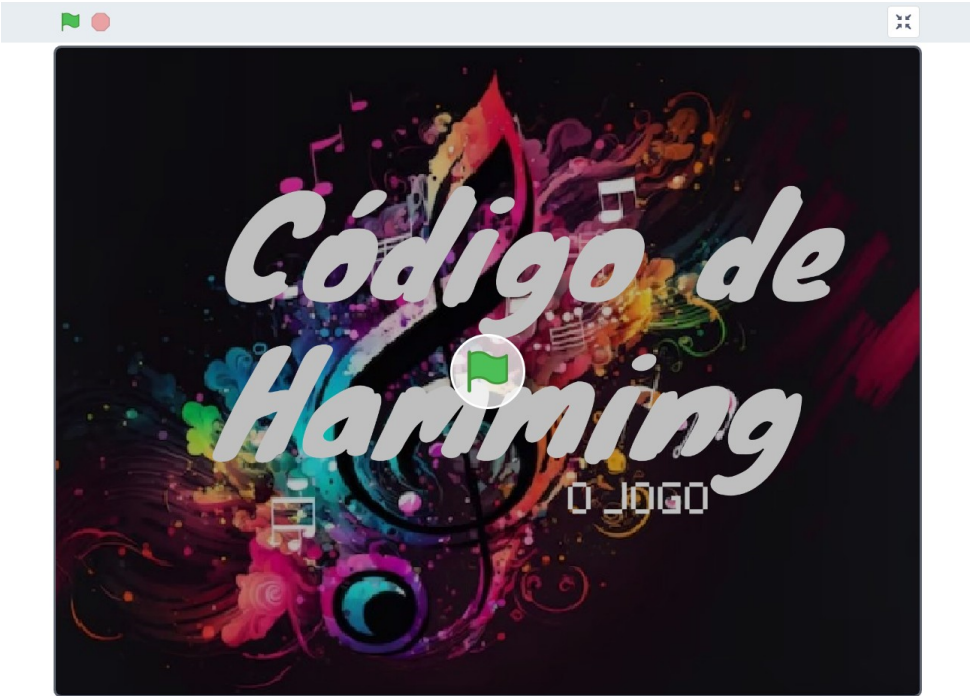
Objetivos: Aplicar os conteúdos das preliminares sobre polinômios e matrizes com os Códigos Corretores de Erros de Hamming (5, 2, 3) apresentado no Exemplo 27 e no Exemplo 37

do Código Cíclico (7, 4, 3); Usar jogos do scratch para motivar os cálculos matemáticos.

Tempo: 4 aulas

Descrição: 1º Momento (Introdução): Para o aprofundamento, o professor deve fazer a leitura dos Exemplos 27 e 37 do Capítulo 3, nos quais é possível observar os códigos com mais detalhes. Dê início à aula com a utilização do jogo "Código de Hamming" no Scratch, com o objetivo de introduzir a ideia de codificação e a eficiência de um código. Uma possibilidade é dividir a sala em grupos de, no máximo, três alunos.

Figura 8 – Tela inicial do jogo: "Código de Hamming"

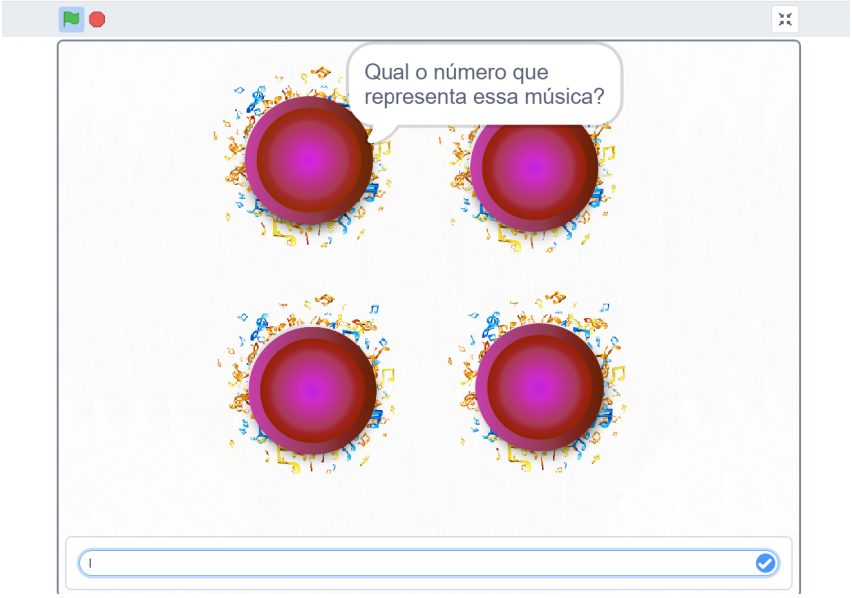


Fonte: https://scratch.mit.edu/projects/839358497/

No início do jogo, os alunos receberão as instruções, no qual eles deverão relacionar sons aos números 0 e 1. Em seguida, serão apresentadas quatro músicas em formato de toques compostas por sequências de sons representando os dígitos 0 e 1, por exemplo, uma música que represente o número 01001. Os alunos terão a tarefa de transcrever essas composições em forma de sequências de dígitos, como mostra a Figura 9. Neste momento, os alunos poderão identificar a ideia de codificação ao transformarem um som em um número.

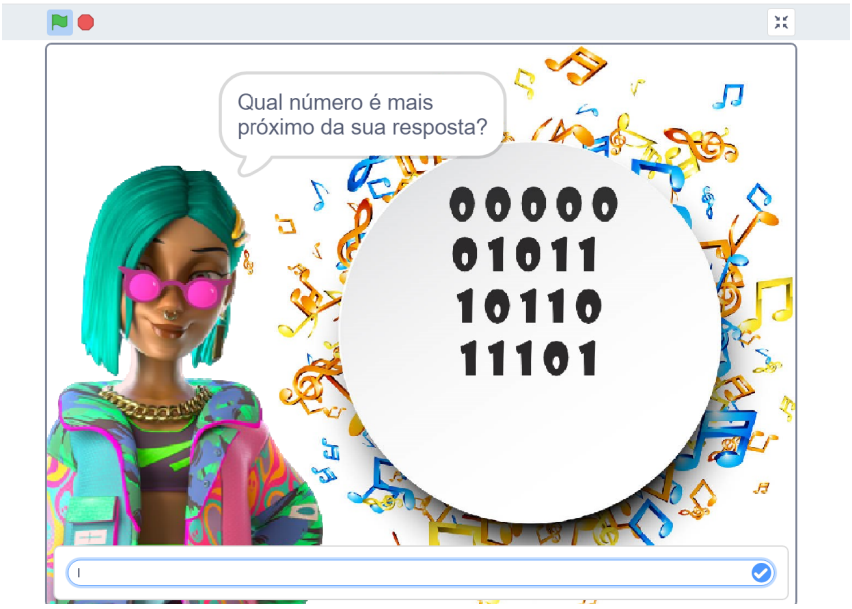
Caso o aluno não consiga colocar a resposta correta devido ao possível "ruído", uma nova tela será exibida, permitindo que o aluno ouça novamente o som e visualize todos os elementos do código, com intuito de fazer uma associação com o mais próximo possível, visto na Figura 10. Essa abordagem permite apresentar a ideia de eficiência do código com as distâncias envolvidas.

Figura 9 – Jogo: “Código de Hamming”



Fonte: Plataforma Scratch.

Figura 10 – Jogo: “Código de Hamming”



Fonte: Plataforma Scratch.

Após o término do jogo, o professor deve propor um momento de reflexão, perguntando aos alunos: Quem não conseguiu escrever o número ouvindo a música somente uma vez? O que você acredita que aconteceu? Por que você não conseguiu digitar o número correto? Tem algo a ver com o barulho?

*2º Momento (Desenvolvimento):*Em seguida apresente a seguinte reflexão:

O processo de transmissão de informações envolve a transferência de dados de um ponto para outro, seja por meio de comunicação sem fio visto na Figura 11, cabos de rede ou outros

meios de transmissão. Durante esse processo, o ruído pode ser introduzido, afetando a qualidade e integridade dos dados transmitidos. O ruído é uma interferência indesejada que pode surgir de várias fontes tais como barulho, sinais elétricos indesejados, interferência eletromagnética, falhas nos dispositivos de transmissão entre outros. O professor pode sugerir aos alunos que olhem a imagem Figura 11 e digam relatem o que está acontecendo, eles veem.

Figura 11 – Processo de transmissão de informações

Fonte: Strategy Consulting.

O professor pode relatar o ruído dentro da sala de aula, como o barulho do ventilador, os outros alunos conversando ou erros de digitação, entre outras possibilidades.

É interessante explicar aos alunos que os Códigos Corretores de Erros são mecanismos utilizados para detectar e corrigir erros introduzidos durante a transmissão ou armazenamento de dados. Mesmo que ocorra ruído e a mensagem original seja diferente da mensagem recebida, os códigos deverão ser capazes de detectar e corrigir esses erros, garantindo que, ao final da transmissão, a mensagem recebida seja igual a mensagem originalmente transmitida. Um Código Corretor de Erros consiste basicamente em adicionar redundância isto é, bits adicionais as palavras e aplicar estratégias para detectar possíveis trocas de posição dos elementos das palavras.

Explicar também que quando uma mensagem é transmitida no meio digital, as informações são convertidas em uma composição de bits, isto é, em sequências de 0's e 1's. Por exemplo, quando eles escutaram os sons, estavam codificando a mensagem e transformando os sons em dígitos. Essa conversão é necessária para que os dados possam ser representados e processados de forma eletrônica.

Para o entendimento dos alunos sobre a distância de Hamming, o professor deve motivá-los explicando que é uma maneira utilizada para medir a diferença entre duas sequências de bits, contando o número de posições em que elas diferem. Essa métrica é importante para determinar a eficiência de correção de um código. No jogo em questão, os alunos são orientados a relacionar a palavra digitada com as sequências de bits $00000, 01011, 10110, 11101$. Se a palavra digitada contiver o mínimo de erros, por exemplo, um erro de apenas um dígito em uma posição aleatória, o aluno poderá identificá-lo facilmente comparando com as palavras apresentadas.

Explore a ideia de distância e solicite aos alunos que calcule a eficiência do código utilizado no jogo. Peça as alunos para comparar dois a dois as diferenças dos bits,

$$d(0\mathbf{00}\mathbf{00}, 0\mathbf{1}0\mathbf{11}) = 3, \qquad d(\mathbf{010}1\mathbf{1}, \mathbf{10}1\mathbf{1}0) = 4,$$
$$d(\mathbf{00}\mathbf{00}0, \mathbf{1}0\mathbf{11}0) = 3, \qquad d(\mathbf{0}1\mathbf{0}\mathbf{1}1, 1\mathbf{1}\mathbf{10}1) = 3,$$
$$d(\mathbf{00}\mathbf{00}\mathbf{0}, \mathbf{11}10\mathbf{1}) = 4, \qquad d(1\mathbf{0}1\mathbf{10}, 1\mathbf{1}\mathbf{01}) = 3.$$

Note que nos exemplos acima, a menor distância é 3, ou seja, se o aluno cometer dois erros ao digitar o número, por exemplo, ao invez de digitar 00000, digitar $\mathbf{1}0\mathbf{1}00$, o aluno não conseguirá corrigir o erro com base na proximidade com a mensagem original. Isso ocorre porque 10100 pode ser considerado próximo tanto de 00000 quanto de 10110.

Em seguida, o professor deve promover um momento de diálogo e abordar as seguintes perguntas: Vocês conseguem pensar em uma situação em que seria desastroso caso uma mensagem não chegue corretamente ao seu destino? Qual é a importância dos códigos corretores de erros? Vocês conseguem identificar situações do cotidiano em que esses códigos são utilizados?

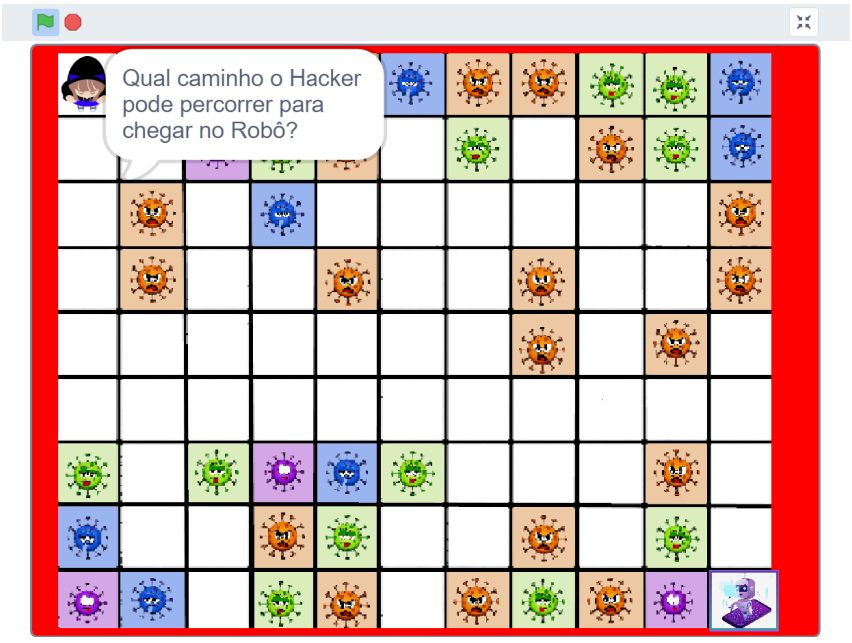
3º Momento (Sistematização): Dando continuidade a aula utilizando o jogo "Código Cíclico" no Scratch (a tela inicial do jogo é apresentado na Figura 12) com o objetivo de reforçar os conteúdos abordados até o momento e explorar a utilização de códigos corretores cíclicos. Antes de iniciar o jogo, pergunte aos alunos se eles conseguem pensar em uma situação em que os conceitos de polinômios e matrizes podem ser aplicados. Após o termino do questionamento, dê inicio ao jogo.

Na primeira parte do jogo, os alunos deverão indicar qual caminho o Hacker deve percorrer para chegar até o robô, como é possível ver na Figura 13. Os comandos disponíveis no teclado são: "Andar" (seta para baixo), "Rotacionar para Direita" (girar 90º no sentido anti-horário, seta para a direita) e "Rotacionar para Esquerda" (girar 90º no sentido horário, seta para a esquerda).

Figura 12 – Tela inicial do jogo: "Código Cíclico"

Fonte: https://scratch.mit.edu/projects/857507588/

Figura 13 – Jogo: "Código Cíclico"



Fonte: Plataforma Scratch.

As mensagens que se deseja enviar são:

$$\{SIGA, DIREITA, ESQUERDA, 1, 2, 3, 4, 5, 6, 7, 8, 9, 10\}.$$

Note que há várias possibilidades de respostas. Os alunos deverão identificar e anotar em seu caderno dois desses caminhos observados, no formato de “DIREITA” ou “ESQUERDA”, “SIGA” seguido pelo número de casas que o Hacker irá andar, alguns exemplos são: (comando 1 = “SIGA

4", comando 2 = "DIREITA SIGA 6", comando 3 = "ESQUERDA, SIGA 1", comando 4 = "DIREITA SIGA 4" e comando 5 = "ESQUERDA, SIGA 3") e (comando 1 = "SIGA 5", comando 2 = "DIREITA SIGA 6", comando 3 = "ESQUERDA, SIGA 1", comando 4 = "DIREITA SIGA 2" e comando 5 = "DIREITA, SIGA 1", comando 6 = "ESQUERDA SIGA 2" e comando 7 = "ESQUERDA, SIGA 3"). Além disso, observe que o caminho mais curto requer no mínimo 3 comandos. Eles são: comando 1 = "SIGA 5", comando 2 = "DIREITA SIGA 10" e comando 3 = "ESQUERDA, SIGA 3".

Desta forma, o professor deve apresentar aos alunos que é possível escrever o conjunto de palavras $\{SIGA, DIREITA, ESQUERDA, 1, 2, 3, 4, 5, 6, 7, 8, 9, 10\}$ da seguinte forma em termos de bits,

$$\begin{aligned} C &= \{1110010, 1101000, 0110100, 0010111, 1010001, 1011100, 1000110, 0100011, \\ &\quad 0011010, 1100101, 0111001, 0001101, 1001011\}. \end{aligned}$$

Também conseguimos representar essas palavras na forma polinomial, por exemplo, se a palavra é dada por 1110010 essa palavra é constituída pelos coeficientes do polinômio $1 + 1X + 1X^2 + 0X^3 + 0X^4 + 1X^5 + 0X^6 = 1 + X + X^2 + X^5$. Assim, todas as palavras são dadas por,

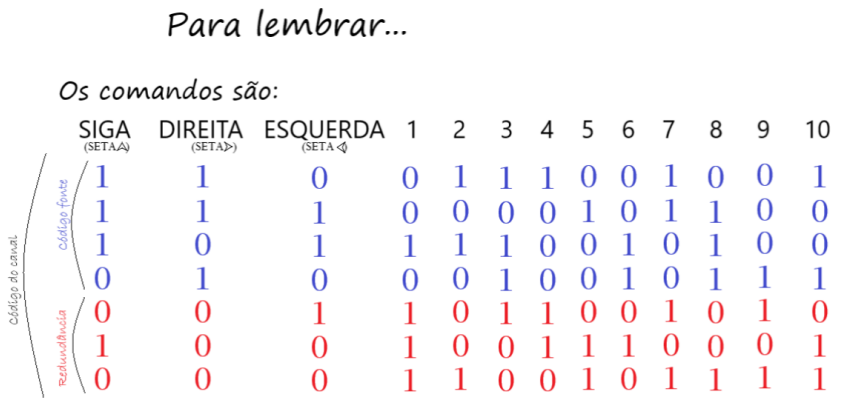
$$\begin{aligned} C &= \{1 + X + X^2 + X^5, 1 + X + X^3, X + X^2 + X^4, X^2 + X^4 + X^5 + X^6, 1 + X^2 \\ &\quad + X^6, 1 + X^2 + X^3 + X^4, 1 + X^4 + X^5, X + X^5 + X^6, X^2 + X^3 + X^5, 1 + X \\ &\quad + X^4 + X^6, X + X^2 + X^3 + X^6, X^3 + X^4 + X^6, 1 + X^3 + X^5 + X^6\}. \end{aligned}$$

O professor deverá fornecer uma "colinha" contendo a codificação do código do canal para facilitar a brincadeira, como mostrado na Figura 14, o polinômio gerador $g(X) = X^3 + X + 1$ e a matriz teste de paridade $h'(X) = \begin{bmatrix} 1 & 0 & 0 & 1 & 0 & 1 & 1 \\ 0 & 1 & 0 & 1 & 1 & 1 & 0 \\ 0 & 0 & 1 & 0 & 1 & 1 & 1 \end{bmatrix}$. Nessa segunda parte do jogo, os alunos poderão ver a funcionalidade dos Códigos Corretores de Erros que a cada mensagem inicial, é necessário realizar a codificação para que, ao passar por um canal com ruído, os efeitos desastrosos dele possam ser reduzidos por meio da detecção e/ou correção de erros.

Inicialmente, as mensagens apresentadas serão apenas mensagens codificadas, sem erros, ou seja, supõe-se que o ruído não tenha alterado nenhum dígito, conforme ilustrado na Figura 15. Os alunos receberão a mensagem codificada e terão que interpretar qual é a mensagem original, simulando o processo final descrito no diagrama apresentado na Figura 3.

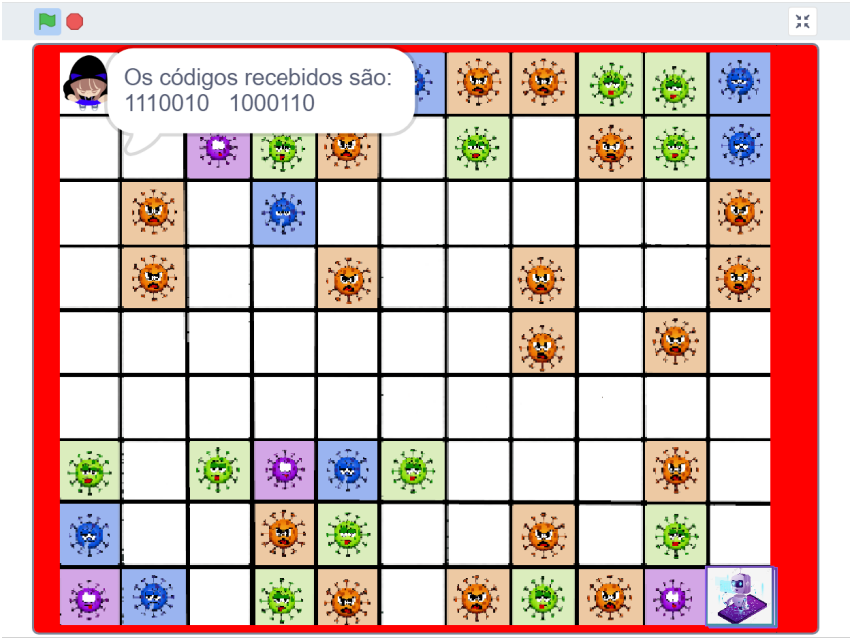
Os alunos deverão realizar as decodificações para avançar no jogo até que o Hacker encontre o robô. Neste momento, os alunos precisarão apenas relacionar os números apresentados

Figura 14 – Jogo: "Código Cíclico"



Fonte: Plataforma Scratch.

Figura 15 – Jogo: "Código Cíclico"



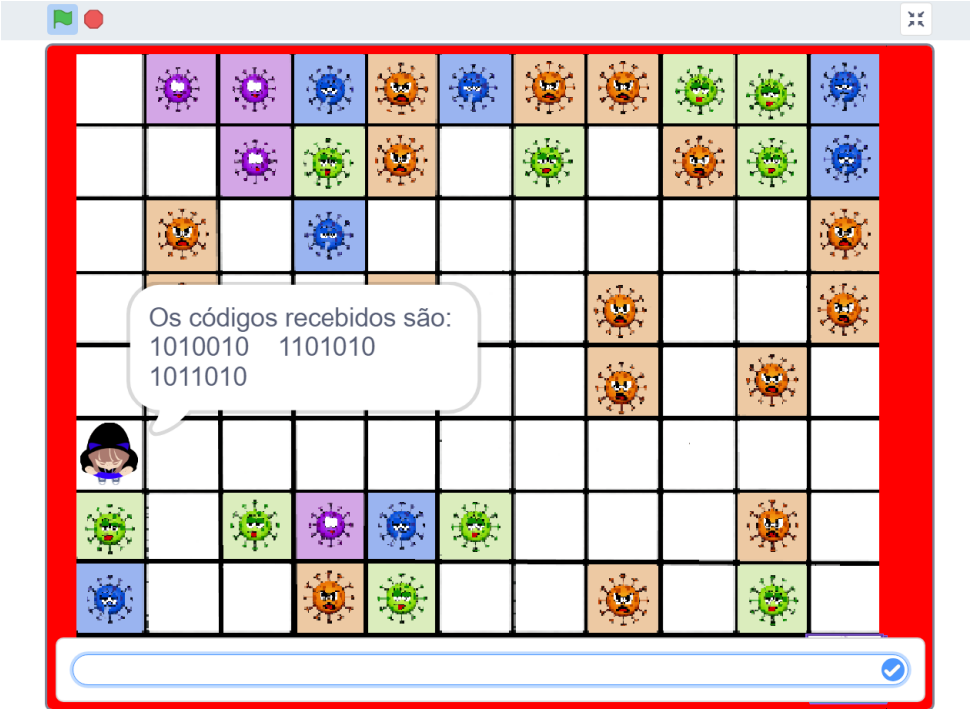
Fonte: Plataforma Scratch.

na “colinha” com as palavras “DIREITA”, “ESQUERDA” e “SIGA”, seguidas pelo número de casas que o Hacker irá andar.

Na terceira parte do jogo, os alunos serão desafiados a decodificar as mensagens, sabendo que cada uma delas possui, no máximo, um erro em alguma posição. Além disso, as posições das mensagens podem estar alteradas, sendo necessário recorrer aos conceitos de divisão de polinômios para recuperar a mensagem original. Por exemplo, veja a Figura 16. Dado o comando: $1\mathbf{0}10010, 1101\mathbf{1}0, \mathbf{1}011010$, os alunos deverão escrever essas mensagens na forma polinomial sabendo que tais mensagens são os coeficientes dos polinômios: $1+0X+X^2+0X^3+0X^4+X^5, 1+X+0X^2+X^3+0X^4+X^5, 1+0X+X^2+X^3+0X^4+X^5$ respectivamente,

isto é, $1+X^2+X^5, 1+X+X^3+X^5, 1+X^2+X^3+X^5$ respectivamente. Depois, eles deverão dividir pelo polinômio gerador $g(X)=X^3+X+1$, oriundo da fatoração de X^7-1 com $gr(g(X))=3$ visto com mais detalhes no Exemplo 37. Dessa forma, temos:

Figura 16 – Jogo: "Código Cíclico"



Fonte: Plataforma Scratch.

$$\begin{array}{r|l} X^5+X^2+1 & X^3+X+1 \\ \hline X & X^2-1 \end{array} \qquad \begin{array}{r|l} X^5+X^3+X+1 & X^3+X+1 \\ \hline X^2+X+1 & X^2 \end{array}$$

$$\begin{array}{r|l} X^5+X^3+X^2+1 & X^3+X+1 \\ \hline 1 & X^2 \end{array}$$

Os alunos poderão recuperar as mensagens iniciais somente comparando os coeficientes dos restos das divisões com as posições das colunas da matriz teste de paridade disponibilizada pelo professor dado por

$$h'(X)=\begin{bmatrix} 1 & 0 & 0 & 1 & 0 & 1 & 1 \\ 0 & 1 & 0 & 1 & 1 & 1 & 0 \\ 0 & 0 & 1 & 0 & 1 & 1 & 1 \end{bmatrix}$$

em que temos na primeira coluna 100, na segunda coluna 010, na terceira coluna 001, na quarta coluna 110, na quinta coluna 011, na sexta coluna 111 e na sétima coluna 101. Se o coeficiente do resto da divisão for 111 significa que o erro é dado na sexta posição, e para recuperar a mensagem inicial basta trocar o dígito 0 para 1 ou 1 para 0 na sexta posição.

Portanto, no exemplo anterior temos os restos $r(X) = X, 1 + X + X^2, 1$, respectivamente, o que significa que $r = 010, 111, 100$. Isso indica que as posições dos erros estão nas segunda, sexta e primeira colunas, então basta trocar os dígitos da segunda, sexta e primeira posições, ou seja, $1\mathbf{1}10010, 11010\mathbf{0}0, \mathbf{0}011010$, sendo relacionado com as palavras SIGA DIREITA 6, reescrevendo na ordem temos DIREITA SIGA 6.

Os alunos deverão realizar as decodificações para avançar no jogo até que o Hacker encontre o robô e assim finalizar o jogo. Ganha o jogo o grupo que finalizar o jogo mais rápido.

O professor pode finalizar a aula debatendo a ideia da utilização de polinômios e matrizes, mostrando aos alunos que, inicialmente, esses conceitos podem parecer sem aplicação direta, mas que, na prática, possuem diversas aplicações relevantes.

5 CONCLUSÕES E PERSPECTIVAS

Ao longo deste trabalho, exploramos a teoria preliminar dos Códigos Corretores de Erros Clássicos e Quânticos, os quais são amplamente utilizados em sistemas tecnológicos da atualidade. Além disso, apresentamos a proposta de utilizar a gamificação como estratégia de ensino no ambiente escolar, enfrentando os desafios no processo de ensino-aprendizagem. Ao ensinar os alunos sobre os Códigos Corretores de Erros, capacitamos-os a ampliar seus horizontes e explorar o potencial da matemática em diversas áreas.

No ensino médio, podemos abordar os algoritmos de codificação e decodificação de Códigos Lineares como aplicação de operações com matrizes e resolução de sistemas lineares. Os Códigos Cíclicos, por sua vez, podem ser estudados na abordagem de polinômios, exigindo o conhecimento de aritmética modular. Essa abordagem permite que os alunos compreendam a conexão entre os conceitos matemáticos e suas aplicações práticas.

No entanto, devemos reconhecer os desafios enfrentados ao elaborar jogos utilizando programação em blocos no ambiente Scratch. A necessidade de compreender a lógica da programação, organizar algoritmos e solucionar problemas pode ser intimidante no início. No entanto, nesses desafios os alunos têm a oportunidade de crescer e desenvolver suas habilidades tecnológicas.

A combinação dos Códigos Corretores de Erros Clássicos e a gamificação usado do ambiente Scratch, para aula, aplicando a matemática no cotidiano, oferecem uma abordagem inovadora para o aprendizado da matemática e o desenvolvimento de habilidades tecnológicas. Ao perceberem as aplicações práticas desses conceitos, os estudantes são incentivados a buscar conhecimentos mais avançados e a compreender como a matemática está presente em diferentes aspectos de suas vidas.

Ao introduzir jogos no contexto educacional, os alunos são estimulados a trabalhar em equipe, resolver problemas, tomar decisões e enfrentar desafios de maneira colaborativa. Os jogos proporcionam um ambiente seguro para experimentação e erro, permitindo que os alunos aprendam com suas falhas e desenvolvam estratégias para superar obstáculos.

É importante ressaltar que a jornada de aprendizagem não está isenta de desafios. Introduzir um tema novo, como o uso de códigos corretores de erros e realizar operações como divisões de polinômios para obter os resultados desejados, não é uma tarefa fácil. No entanto, é exatamente nessas dificuldades que os alunos têm a oportunidade de crescer e desenvolver suas

habilidades. É importante fornecer um ambiente de aprendizado que estimule a persistência, a criatividade e o trabalho em equipe, para que os alunos possam superar os desafios e alcançar um entendimento mais profundo dos códigos corretores de erros.

O recorte deste trabalho foi submetido para publicação na Revista Brasileira de Informática na Educação (RBIE). Uma proposta futura interessante seria elaborar um jogo que explore os Códigos Corretores de Erros Quânticos. Esse jogo poderia apresentar situações em que os jogadores são desafiados a aplicar os conceitos dos códigos quânticos para corrigir erros em informações transmitidas.

REFERÊNCIAS

AMARAL, Bárbara; BARAVIERA, Alexandre T; CUNHA, MO Terra. Mecânica quântica para matemáticos em formação. **Impa-28th Colóquio Brasileiro de Matemática**, 2011.

COELHO, Flávio Ulhoa. **Curso de Álgebra Linear, Um Vol. 34**. São Paulo: Edusp, 2001.

CSIKSZENTMIHALYI, Mihaly. **Applications of flow in human development and education**. *[S.l.]*: Springer, 2014.

DANTAS, Alexsandro Cavalcanti. O estudo de restos, congruência e divisibilidade: uma abordagem teórica aplicada ao ensino médio no brasil. Universidade Federal do Rio Grande do Norte, 2016.

HEFEZ, Abramo; VILLELA, Maria Lúcia T. **Códigos corretores de erros**. Rio de Janeiro: Instituto de Matematica Pura e Aplicada, 2008.

JANESCH, Oscar Ricardo; TANEJA, Inder J. **Álgebra I. Florianópolis: UFSC**. Florianópolis, 2008.

JÚNIOR, Sérgio Brazil. Algumas observações acerca da definição de anel a partir das bibliografias comumente utilizadas nos cursos de matemática da ufac. **ELEMENTOS**, p. 24, 2011.

LIN, Shu; COSTELLO, Daniel J. **Error Control Coding: Fundamentals and Applications**. 2. ed. New Jersey: Prentice Hall, 2004.

MILIES, César Polcino. Breve introdução à teoria dos códigos corretores de erros. **Colóquio de Matemática da Região Centro-Oeste, SBM**, p. 22, 2009.

NIELSEN, Michael A; CHUANG, Isaac. **Quantum computation and quantum information**. New York: American Association of Physics Teachers, 2002.

RESNICK, Mitchel. **Lifelong kindergarten: Cultivating creativity through projects, passion, peers, and play**. Cambridge: MIT press, 2017.

SANTOS, Wilk Oliveira dos; JUNIOR, Clovis Gomes da Silva. Uso de jogos no ensino da matemática: Uma análise entre os jogos tradicionais e os jogos digitais, baseada em pesquisa e mapeamento dos materiais encontrados na web. 2014.

SHANNON, Claude Elwood. A mathematical theory of communication. **The Bell system technical journal**, Nokia Bell Labs, v. 27, n. 3, p. 379–423, 1948.

SHOR, Peter W. Algorithms for quantum computation: discrete logarithms and factoring. *In*: IEEE. **Proceedings 35th annual symposium on foundations of computer science**. *[S.l.]*, 1994. p. 124–134.

SILVA, João Batista da; SALES, Gilvandenys Leite. Gamificação aplicada no ensino de física: um estudo de caso no ensino de óptica geométrica. **Acta Scientiae**, v. 19, n. 5, 2017.

WICKER, Stephen B.; BHARGAVA, Vijay K. **Reed-Solomon Codes and Their Applications**. New York: IEEE Press, 1994. 12 p.